Chapter 3

Implementation

THE COMPTIA SECURITY+ EXAM SY0-601 TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **3.1 Given a scenario, implement secure protocols**
- ✓ **3.2 Given a scenario, implement host or application security solutions**
- ✓ **3.3 Given a scenario, implement secure network designs**
- ✓ **3.4 Given a scenario, install and configure wireless security settings**
- ✓ **3.5 Given a scenario, implement secure mobile solutions**
- ✓ **3.6 Given a scenario apply cybersecurity solutions to the cloud**
- ✓ **3.7 Given a scenario, implement identity and account management controls**
- ✓ **3.8 Given a scenario, implement authentication and authorization solutions**
- ✓ **3.9 Given a scenario, implement public key infrastructure**

1. Adam is setting up a public key infrastructure (PKI) and knows that keeping the passphrases and encryption keys used to generate new keys is a critical part of how to ensure that the root certificate authority remains secure. Which of the following techniques is not a common solution to help prevent insider threats?
   - **A.** Require a new passphrase every time the certificate is used.
   - **B.** Use a split knowledge process for the password or key.
   - **C.** Require dual control.
   - **D.** Implement separation of duties.

2. Naomi is designing her organization's wireless network and wants to ensure that the design places access points in areas where they will provide optimum coverage. She also wants to plan for any sources of RF interference as part of her design. What should Naomi do first?
   - **A.** Contact the FCC for a wireless map.
   - **B.** Conduct a site survey.
   - **C.** Disable all existing access points.
   - **D.** Conduct a port scan to find all existing access points.

3. Chris is preparing to implement an 802.1X-enabled wireless infrastructure. He knows that he wants to use an Extensible Authentication Protocol (EAP)-based protocol that does not require client-side certificates. Which of the following options should he choose?
   - **A.** EAP-MD5
   - **B.** PEAP
   - **C.** LEAP
   - **D.** EAP-TLS

4. What term is commonly used to describe lateral traffic movement within a network?
   - **A.** Side-stepping
   - **B.** Slider traffic
   - **C.** East-west traffic
   - **D.** Peer interconnect

5. Charlene wants to use the security features built into HTTP headers. Which of the following is not an HTTP header security option?
   - **A.** Requiring transport security
   - **B.** Preventing cross-site scripting
   - **C.** Disabling SQL injection
   - **D.** Helping prevent MIME sniffing

6. Charlene wants to provision her organization's standard set of marketing information to mobile devices throughout her organization. What MDM feature is best suited to this task?
   - **A.** Application management
   - **B.** Remote wipe

C. Content management

D. Push notifications

7. Denny wants to deploy antivirus for his organization and wants to ensure that it will stop the most malware. What deployment model should Denny select?

A. Install antivirus from the same vendor on individual PCs and servers to best balance visibility, support, and security.

B. Install antivirus from more than one vendor on all PCs and servers to maximize coverage.

C. Install antivirus from one vendor on PCs and from another vendor on the server to provide a greater chance of catching malware.

D. Install antivirus only on workstations to avoid potential issues with server performance.

8. When Amanda visits her local coffee shop, she can connect to the open wireless without providing a password or logging in, but she is immediately redirected to a website that asks for her email address. Once she provides it, she is able to browse the Internet normally. What type of technology has Amanda encountered?

A. A preshared key

B. A captive portal

C. Port security

D. A Wi-Fi protected access

9. Charles has been asked to implement DNSSEC for his organization. Which of the following does it provide?

A. Confidentiality

B. Integrity

C. Availability

D. All of the above

10. Sarah has implemented an OpenID-based authentication system that relies on existing Google accounts. What role does Google play in a federated environment like this?

A. An RP

B. An IdP

C. An SP

D. An RA

11. Ian needs to connect to a system via an encrypted channel so that he can use a command-line shell. What protocol should he use?

A. Telnet

B. HTTPS

C. SSH

D. TLS

12. Casey is considering implementing password key devices for her organization. She wants to use a broadly adopted open standard for authentication and needs her keys to support that. Which of the following standards should she look for her keys to implement, in addition to being able to connect via USB, Bluetooth, and NFC?

A. SAML

B. FIDO

C. ARF

D. OpenID

13. Nadia is concerned about the content of her emails to her friend Danielle being read as they move between servers. What technology can she use to encrypt her emails, and whose key should she use to encrypt the message?

A. S/MIME, her private key

B. Secure POP3, her public key

C. S/MIME, Danielle's public key

D. Secure POP3, Danielle's private key

14. What type of communications is SRTP most likely to be used for?

A. Email

B. VoIP

C. Web

D. File transfer

15. Olivia is implementing a load-balanced web application cluster. Her organization already has a redundant pair of load balancers, but each unit is not rated to handle the maximum designed throughput of the cluster by itself. Olivia has recommended that the load balancers be implemented in an active/active design. What concern should she raise as part of this recommendation?

A. The load balancer cluster cannot be patched without a service outage.

B. The load balancer cluster is vulnerable to a denial-of-service attack.

C. If one of the load balancers fails, it could lead to service degradation.

D. None of the above

16. What two ports are most commonly used for FTPS traffic?

A. 21, 990

B. 21, 22

C. 433, 1433

D. 20, 21

17. What occurs when a certificate is stapled?

- **A.** Both the certificate and OCSP responder are sent together to prevent additional retrievals during certificate path validation.
- **B.** The certificate is stored in a secured location that prevents the certificate from being easily removed or modified.
- **C.** Both the host certificate and the root certificate authority's private key are attached to validate the authenticity of the chain.
- **D.** The certificate is attached to other certificates to demonstrate the entire certificate chain.

18. Greg is setting up a public key infrastructure (PKI). He creates an offline root certificate authority (CA) and then needs to issue certificates to users and devices. What system or device in a PKI receives certificate signing requests (CSRs) from applications, systems, and users?

- **A.** An intermedia CA
- **B.** An RA
- **C.** A CRL
- **D.** None of the above

19. Mark is responsible for managing his company's load balancer and wants to use a load-balancing scheduling technique that will take into account the current server load and active sessions. Which of the following techniques should he choose?

- **A.** Source IP hashing
- **B.** Weighted response time
- **C.** Least connection
- **D.** Round robin

20. During a security review, Matt notices that the vendor he is working with lists their IPSec virtual private network (VPN) as using AH protocol for security of the packets that it sends. What concern should Matt note to his team about this?

- **A.** AH does not provide confidentiality.
- **B.** AH does not provide data integrity.
- **C.** AH does not provide replay protection.
- **D.** None of the above; AH provides confidentiality, authentication, and replay protection.

21. Michelle wants to secure mail being retrieved via the Post Office Protocol Version 3 (POP3) because she knows that it is unencrypted by default. What is her best option to do this while leaving POP3 running on its default port?

- **A.** Use TLS via port 25.
- **B.** Use IKE via port 25.
- **C.** Use TLS via port 110.
- **D.** Use IKE via port 110.

22. Daniel works for a mid-sized financial institution. The company has recently moved some of its data to a cloud solution. Daniel is concerned that the cloud provider may not support the same security policies as the company's internal network. What is the best way to mitigate this concern?

A. Implement a cloud access security broker.

B. Perform integration testing.

C. Establish cloud security policies.

D. Implement security as a service.

23. The company that Angela works for has deployed a Voice over IP (VoIP) environment that uses SIP. What threat is the most likely issue for their phone calls?

A. Call interception

B. Vishing

C. War dialing

D. Denial-of-service attacks

24. Alaina is concerned about the security of her NTP time synchronization service because she knows that protocols like TLS and BGP are susceptible to problems if fake NTP messages were able to cause time mismatches between systems. What tool could she use to quickly protect her NTP traffic between Linux systems?

A. An IPSec VPN

B. SSH tunneling

C. RDP

D. A TLS VPN

25. Ramon is building a new web service and is considering which parts of the service should use Transport Layer Security (TLS). Components of the application include:

1. Authentication

2. A payment form

3. User data, including address and shopping cart

4. A user comments and reviews section

Where should he implement TLS?

A. At points 1 and 2, and 4

B. At points 2 and 3, and 4

C. At points 1, 2, and 3

D. At all points in the infrastructure

26. Katie's organization uses File Transfer Protocol (FTP) for contractors to submit their work product to her organization. The contractors work on sensitive customer information, and then use organizational credentials provided by Katie's company to log in and transfer the information. What sensitive information could attackers gather if they were able to capture the network traffic involved in this transfer?

A. Nothing, because FTP is a secure protocol

B. IP addresses for both client and server

C. The content of the files that were uploaded

D. Usernames, passwords, and file content

27. What security benefits are provided by enabling DHCP snooping or DHCP sniffing on switches in your network?

A. Prevention of malicious or malformed DHCP traffic

B. Prevention of rogue DHCP servers

C. Collection of information about DHCP bindings

D. All of the above

28. Aaron wants to use a certificate for the following production hosts:

```
www.example.com
blog.example.com
news.example.com
```

What is the most efficient way for him to provide Transport Layer Security (TLS) for all of these systems?

A. Use self-signed certificates.

B. Use a wildcard certificate.

C. Use an EV certificate.

D. Use an SSL certificate.

29. Cassandra is concerned about attacks against her network's Spanning Tree Protocol (STP). She wants to ensure that a new switch introduced by an attacker cannot change the topology by asserting a lower bridge ID than the current configuration. What should she implement to prevent this?

A. Enable BridgeProtect.

B. Set the bridge ID to a negative number.

C. Disable Spanning Tree protocol.

D. Enable Root Guard.

30. Charles finds a PFX formatted file on the system he is reviewing. What is a PFX file capable of containing?

A. Only certificates and chain certificates, not private keys

B. Only a private key

C. A server certificate, intermediate certificates, and the private key

D. None of the above, because PFX files are used for certificate requests only

31. Which device would most likely process the following rules?

```
PERMIT IP ANY EQ 443
DENY IP ANY ANY
```

A. NIPS

B. HIPS

C. Content filter

D. Firewall

32. Ted wants to use IP reputation information to protect his network and knows that third parties provide that information. How can he get this data, and what secure protocol is he most likely to use to retrieve it?

A. A subscription service, SAML

B. A VDI, XML

C. A subscription service, HTTPS

D. An FDE, XML

33. What does setting the secure attribute for an HTTP cookie result in?

A. Cookies will be stored in encrypted form.

B. Cookies will be sent only over HTTPS.

C. Cookies will be stored in hashed form.

D. Cookies must be accessed using a cookie key.

34. Charles wants to use IPSec and needs to be able to determine the IPSec policy for traffic based on the port it is being sent to on the remote system. Which IPSec mode should he use?

A. IPSec tunnel mode

B. IPSec IKE mode

C. IPSec PSK mode

D. IPSec transport mode

35. Wi-Fi Protected Setup (WPS) includes four modes for adding devices to a network. Which mode has significant security concerns due to a brute-force exploit?

A. PIN

B. USB

C. Push button

D. Near-field communication

36. Claire wants to check whether a certificate has been revoked. What protocol is used to validate certificates?

A. RTCP

B. CRBL

C. OCSP

D. PKCRL

37. Nick is responsible for cryptographic keys in his company. What is the best way to deauthorize a public key?

A. Send out a network alert.

B. Delete the digital certificate.

C. Publish that certificate in the CRL.

D. Notify the RA.

38. What two connection methods are used for most geofencing applications?

A. Cellular and GPS

B. USB and Bluetooth

C. GPS and Wi-Fi

D. Cellular and Bluetooth

39. Gabriel is setting up a new e-commerce server. He is concerned about security issues. Which of the following would be the best location to place an e-commerce server?

A. DMZ

B. Intranet

C. Guest network

D. Extranet

40. Janelle is the security administrator for a small company. She is trying to improve security throughout the network. Which of the following steps should she take first?

A. Implement antimalware on all computers.

B. Implement acceptable use policies.

C. Turn off unneeded services on all computers.

D. Set password reuse policies.

41. Ben is responsible for a new application with a worldwide user base that will allow users to sign up to access existing data about them. He would like to use a method of authentication that will permit him to verify that users are the correct people to match up with their accounts. How can he validate these users?

A. Require that they present their Social Security number.

B. Require them to use a federated identity via Google.

C. Require them to use knowledge-based authentication.

D. Require them to validate an email sent to the account they signed up with.

42. Jason wants to implement a remote access virtual private network (VPN) for users in his organization who primarily rely on hosted web applications. What common VPN type is best suited to this if he wants to avoid deploying client software to his end-user systems?

A. A TLS VPN

B. An RDP (Remote Desktop Protocol) VPN

C. An Internet Control Message Protocol (ICMP) VPN

D. An IPSec VPN

43. Juan is a network administrator for an insurance company. His company has a number of traveling salespeople. He is concerned about confidential data on their laptops. What is the best way for him to address this?

A. FDE

B. TPM

C. SDN

D. DMZ

44. Which design concept limits access to systems from outside users while protecting users and systems inside the LAN?

A. DMZ

B. VLAN

C. Router

D. Guest network

45. Nina wants to use information about her users like their birth dates, addresses, and job titles as part of her identity management system. What term is used to describe this type of information?

A. Roles

B. Factors

C. Identifiers

D. Attributes

46. Megan is preparing a certificate signing request (CSR) and knows that she needs to provide a CN for her web server. What information will she put into the CN field for the CSR?

A. Her name

B. The hostname

C. The company's name

D. The fully qualified domain name of the system

47. Which of the following is the equivalent of a VLAN from a physical security perspective?

A. Perimeter security

B. Partitioning

C. Security zones

D. Firewall

48. Nelson uses a tool that lists the specific applications that can be installed and run on a system. The tool uses hashes of the application's binary to identify each application to ensure that the application matches the filename provided for it. What type of tool is Nelson using?

A. Antivirus

B. Blacklisting

C. Antimalware

D. Whitelisting

49. Which type of firewall examines the content and context of each packet it encounters?

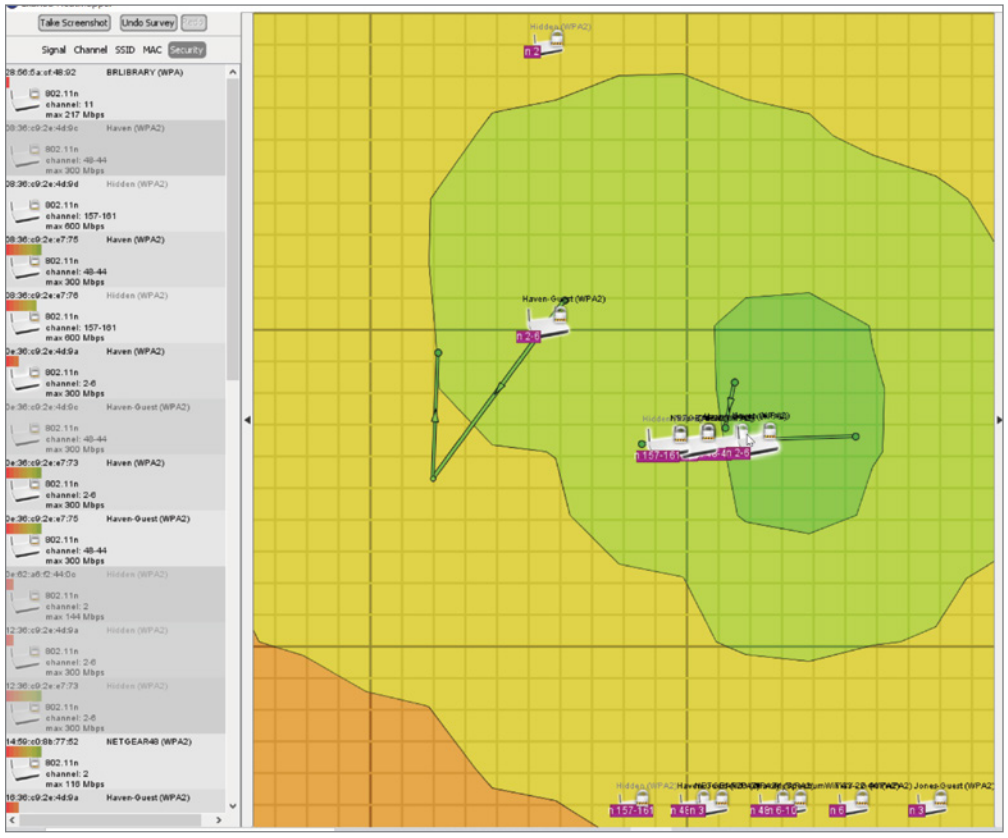
A. Packet filtering firewall

B. Stateful packet filtering firewall

C. Application layer firewall

D. Gateway firewall

50. As part of his wireless network deployment efforts, Scott generates the image shown here. What term is used to describe this type of visualization of wireless networks?



A. A heatmap

B. A network diagram

C. A zone map

D. A DMZ

51. You're designing a new network infrastructure so that your company can allow unauthenticated users connecting from the Internet to access certain areas. Your goal is to protect the internal network while providing access to those areas. You decide to put the web server on a separate subnet open to public contact. What is this subnet called?

A. Guest network

B. DMZ

C. Intranet

D. VLAN

52. Madhuri's web application converts numbers that are input into fields by specifically typing them and then applies strict exception handling. It also sets a minimum and maximum length for the inputs that it allows and uses predefined arrays of allowed values for inputs like months or dates. What term describes the actions that Madhuri's application is performing?

A. Buffer overflow prevention

B. String injection

C. Input validation

D. Schema validation

53. You're outlining your plans for implementing a wireless network to upper management. What wireless security standard should you adopt if you don't want to use enterprise authentication but want to provide secure authentication for users that doesn't require a shared password or passphrase?

A. WPA3

B. WPA

C. WPA2

D. WEP

54. Brandon wants to ensure that his intrusion prevention system (IPS) is able to stop attack traffic. Which deployment method is most appropriate for this requirement?

A. Inline, deployed as an IPS

B. Passive via a tap, deployed as an IDS

C. Inline, deployed as an IDS

D. Passive via a tap, deployed as an IPS

55. You are the chief security officer (CSO) for a large company. You have discovered malware on one of the workstations. You are concerned that the malware might have multiple functions and might have caused more security issues with the computer than you can currently detect. What is the best way to test this malware?

A. Leave the malware on that workstation until it is tested.

B. Place the malware in a sandbox environment for testing.

C. It is not important to analyze or test it; just remove it from the machine.

D. Place the malware on a honeypot for testing.

56. You are trying to increase security at your company. You're currently creating an outline of all the aspects of security that will need to be examined and acted on. Which of the following terms describes the process of improving security in a trusted OS?

A. FDE

B. Hardening

C. SED

D. Baselining

57. Melissa's website provides users who access it via HTTPS with a Transport Layer Security (TLS) connection. Unfortunately, Melissa forgot to renew her certificate, and it is presenting users with an error. What happens to the HTTPS connection when a certificate expires?

A. All traffic will be unencrypted.

B. Traffic for users who do not click OK at the certificate error will be unencrypted.

C. Trust will be reduced, but traffic will still be encrypted.

D. Users will be redirected to the certificate authority's site for a warning until the certificate is renewed.

58. Isaac is reviewing his organization's secure coding practices document for customer-facing web applications and wants to ensure that their input validation recommendations are appropriate. Which of the following is not a common best practice for input validation?

A. Ensure validation occurs on a trusted server.

B. Validate all client-supplied data before it is processed.

C. Validate expected data types and ranges.

D. Ensure validation occurs on a trusted client.

59. Frank knows that the systems he is deploying have a built-in TPM module. Which of the following capabilities is not a feature provided by a TPM?

A. A random number generator

B. Remote attestation capabilities

C. A cryptographic processor used to speed up SSL/TLS

D. The ability to bind and seal data

60. What is the primary use of hashing in databases?

A. To encrypt stored data, thus preventing exposure

B. For indexing and retrieval

C. To obfuscate data

D. To substitute for sensitive data, allowing it to be used without exposure

61. Hans is a security administrator for a large company. Users on his network visit a wide range of websites. He is concerned they might get malware from one of these many websites. Which of the following would be his best approach to mitigate this threat?

A. Implement host-based antivirus.

B. Blacklist known infected sites.

C. Set browsers to allow only signed components.

D. Set browsers to block all active content (ActiveX, JavaScript, etc.).

62. Zarmeena has implemented wireless authentication for her network using a passphrase that she distributes to each member of her organization. What type of authentication method has she implemented?

A. Enterprise

B. PSK

C. Open

D. Captive portal

63. Olivia is building a wireless network and wants to implement an Extensible Authentication Protocol (EAP)-based protocol for authentication. What EAP version should she use if she wants to prioritize reconnection speed and doesn't want to deploy client certificates for authentication?

A. EAP-FAST

B. EAP-TLS

C. PEAP

D. EAP-TTLS

64. You work at a large company. You are concerned about ensuring that all workstations have a common configuration, that no rogue software is installed, and that all patches are kept up to date. Which of the following would be the most effective for accomplishing this?

A. Use VDI.

B. Implement restrictive policies.

C. Use an image for all workstations.

D. Implement strong patch management.

65. Naomi has deployed her organization's cloud-based virtual datacenters to multiple Google datacenter locations around the globe. What does this design provide for her systems?

A. Resistance to insider attacks

B. High availability across multiple zones

C. Decreased costs

D. Vendor diversity

66. Patrick wants to deploy a virtual private networking (VPN) technology that is as easy for end users to use as possible. What type of VPN should he deploy?

A. An IPSec VPN

B. An SSL/TLS VPN

C. An HTML5 L2TP VPN

D. An SAML VPN

67. Olivia is responsible for web application security for her company's e-commerce server. She is particularly concerned about XSS and SQL injection. Which technique would be most effective in mitigating these attacks?

A. Proper error handling

B. The use of stored procedures

C. Proper input validation

D. Code signing

68. Isaac wants to prevent corporate mobile devices from being used outside of his company's buildings and corporate campus. What mobile device management (MDM) capability should he use to allow this?

A. Patch management

B. IP filtering

C. Geofencing

D. Network restrictions

69. Sophia wants to test her company's web application to see if it is handling input validation and data validation properly. Which testing method would be most effective for this?

A. Static code analysis

B. Fuzzing

C. Baselining

D. Version control

70. Alaina has implemented an HSM. Which of the following capabilities is not a typical HSM feature?

A. Encryption and decryption for digital signatures

B. Boot attestation

C. Secure management of digital keys

D. Strong authentication support

71. Cynthia wants to issue contactless cards to provide access to the buildings she is tasked with securing. Which of the following technologies should she deploy?

A. RFID

B. Wi-Fi

C. Magstripe

D. HOTP

72. Alaina wants to prevent bulk gathering of email addresses and other directory information from her web-exposed LDAP directory. Which of the following solutions would not help with this?

A. Using a back-off algorithm

B. Implementing LDAPS

C. Requiring authentication

D. Rate limiting queries

73. Alaina has been told that her organization uses a SAN certificate in their environment. What does this tell Alaina about the certificate in use in her organization?

A. It is used for a storage area network.

B. It is provided by SANS, a network security organization.

C. The certificate is part of a self-signed, self-assigned namespace.

D. The certificate allows multiple hostnames to be protected by the same certificate.

74. Edward is responsible for web application security at a large insurance company. One of the applications that he is particularly concerned about is used by insurance adjusters in the field. He wants to have strong authentication methods to mitigate misuse of the application. What would be his best choice?

A. Authenticate the client with a digital certificate.

B. Implement a very strong password policy.

C. Secure application communication with Transport Layer Security (TLS).

D. Implement a web application firewall (WAF).

75. Sarah is the CIO for a small company. The company uses several custom applications that have complicated interactions with the host operating system. She is concerned about ensuring that systems on her network are all properly patched. What is the best approach in her environment?

A. Implement automatic patching.

B. Implement a policy that has individual users patch their systems.

C. Delegate patch management to managers of departments so that they can find the best patch management for their departments.

D. Immediately deploy patches to a test environment; then as soon as testing is complete, have a staged rollout to the production network.

76. Gary uses a wireless analyzer to perform a site survey of his organization. Which of the following is not a common feature of a wireless analyzer's ability to provide information about the wireless networks around it?

A. The ability to show signal strength of access points on a map of the facility

B. The ability to show the version of the RADIUS server used for authentication

C. The ability to show a list of SSIDs available in a given location

D. The ability to show the version of the 802.11 protocol (n, ac, ax)

77. Emiliano is a network administrator and is concerned about the security of peripheral devices. Which of the following would be a basic step he could take to improve security for those devices?

A. Implement FDE.

B. Turn off remote access (SSH, Telnet, etc.) if not needed.

C. Utilize fuzz testing for all peripherals.

D. Implement digital certificates for all peripherals.

78. What type of code analysis is manual code review?

A. Dynamic code review

B. Fagan code review

C. Static code review

D. Fuzzing

79. Samantha has used ssh-keygen to generate new SSH keys. Which SSH key should she place on the server she wants to access, and where is it typically stored on a Linux system?

A. Her public SSH key, `/etc/`

B. Her private SSH key, `/etc/`

C. Her public SSH key, `~/.ssh`

D. Her private SSH key, `~/.ssh`

80. Ixxia is a software development team manager. She is concerned about memory leaks in code. What type of testing is most likely to find memory leaks?

A. Fuzzing

B. Stress testing

C. Static code analysis

D. Normalization

81. What IP address does a load balancer provide for external connections to connect to web servers in a load-balanced group?

A. The IP address for each server, in a prioritized order

B. The load balancer's IP address

C. The IP address for each server in a round-robin order

D. A virtual IP address

82. What term describes random bits that are added to a password before it is hashed and stored in a database?

A. Flavoring

B. Rainbow-armor

C. Bit-rot

D. Salt

83. Victor is a network administrator for a medium-sized company. He wants to be able to access servers remotely so that he can perform small administrative tasks from remote locations. Which of the following would be the best protocol for him to use?

A. SSH

B. Telnet

C. RSH

D. SNMP

84. Dan configures a resource-based policy in his Amazon account. What control has he deployed?

A. A control that determines who has access to the resource, and the actions they can take on it

B. A control that determines the amount that service can cost before an alarm is sent

C. A control that determines the amount of a finite resource that can be consumed before an alarm is set

D. A control that determines what an identity can do

85. Charlene's company uses rack-mounted sensor appliances in their datacenter. What are sensors like these typically monitoring?

A. Temperature and humidity

B. Smoke and fire

C. Power quality and reliability

D. None of the above

86. Laurel is reviewing the configuration for an email server in her organization and discovers that there is a service running on TCP port 993. What secure email service has she most likely discovered?

A. Secure POP3

B. Secure SMTP

C. Secure IMAP (IMAPS)

D. Secure MIME (SMIME)

87. What type of topology does an ad hoc wireless network use?

A. Point-to-multipoint

B. Star

C. Point-to-point

D. Bus

88. What is the primary advantage of allowing only signed code to be installed on computers?

A. It guarantees that malware will not be installed.

B. It improves patch management.

C. It verifies who created the software.

D. It executes faster on computers with a Trusted Platform Module (TPM).

89. Samantha has been asked to provide a recommendation for her organization about password security practices. Users have complained that they have to remember too many passwords as part of their job and that they need a way to keep track of them. What should Samantha recommend?

A. Recommend that users write passwords down near their workstation.

B. Recommend that users use the same password for sites with similar data or risk profiles.

C. Recommend that users change their standard passwords slightly based on the site they are using.

D. Recommend a password vault or manager application.

90. Matt has enabled port security on the network switches in his building. What does port security do?

A. Filters by MAC address

B. Prevents routing protocol updates from being sent from protected ports

C. Establishes private VLANs

D. Prevents duplicate MAC addresses from connecting to the network

91. Tom is responsible for VPN connections in his company. His company uses IPSec for VPNs. What is the primary purpose of AH in IPSec?

A. Encrypt the entire packet.

B. Encrypt just the header.

C. Authenticate the entire packet.

D. Authenticate just the header.

92. Miles wants to ensure that his internal DNS cannot be queried by outside users. What DNS design pattern uses different internal and external DNS servers to provide potentially different DNS responses to users of those networks?

A. DNSSEC

B. Split horizon DNS

C. DMZ DNS

D. DNS proxying

93. Abigail is responsible for setting up a network-based intrusion prevention system (NIPS) on her network. The NIPS is located in one particular network segment. She is looking for a passive method to get a copy of all traffic to the NIPS network segment so that it can analyze the traffic. Which of the following would be her best choice?

A. Using a network tap

B. Using port mirroring

C. Setting the NIPS on a VLAN that is connected to all other segments

D. Setting up a NIPS on each segment

94. Amanda wants to allow users from other organizations to log in to her wireless network. What technology would allow her to do this using their own home organization's credentials?

A. Preshared keys

B. 802.11q

C. RADIUS federation

D. OpenID Connect

95. Nathan wants to ensure that the mobile devices his organization has deployed can only be used in the company's facilities. What type of authentication should he deploy to ensure this?

A. PINs

B. Biometrics

C. Context-aware authentication

D. Content-aware authentication

96. Which of the following best describes a TPM?

A. Transport Protection Mode

B. A secure cryptoprocessor

C. A DNSSEC extension

D. Total Patch Management

97. Janice is explaining how IPSec works to a new network administrator. She is trying to explain the role of IKE. Which of the following most closely matches the role of IKE in IPSec?

A. It encrypts the packet.

B. It establishes the SAs.

C. It authenticates the packet.

D. It establishes the tunnel.

98. What certificate is most likely to be used by an offline certificate authority (CA)?

A. Root

B. Machine/computer

C. User

D. Email

99. Emily manages the IDS/IPS for her network. She has a network-based intrusion prevention system (NIPS) installed and properly configured. It is not detecting obvious attacks on one specific network segment. She has verified that the NIPS is properly configured and working properly. What would be the most efficient way for her to address this?

A. Implement port mirroring for that segment.

B. Install a NIPS on that segment.

C. Upgrade to a more effective NIPS.

D. Isolate that segment on its own VLAN.

100. Dana wants to protect data in a database without changing characteristics like the data length and type. What technique can she use to do this most effectively?

A. Hashing

B. Tokenization

C. Encryption

D. Rotation

101. Elenora is responsible for log collection and analysis for a company with locations around the country. She has discovered that remote sites generate high volumes of log data, which can cause bandwidth consumption issues for those sites. What type of technology could she deploy to each site to help with this?

A. Deploy a log aggregator.

B. Deploy a honeypot.

C. Deploy a bastion host.

D. None of the above

102. Dani is performing a dynamic code analysis technique that sends a broad range of data as inputs to the application she is testing. The inputs include data that is both within the expected ranges and types for the program and data that is different and, thus, unexpected by the program. What code testing technique is Dani using?

A. Timeboxing

B. Buffer overflow

C. Input validation

D. Fuzzing

103. Tina wants to ensure that rogue DHCP servers are not permitted on the network she maintains. What can she do to protect against this?

A. Deploy an IDS to stop rogue DHCP packets.

B. Enable DHCP snooping.

C. Disable DHCP snooping.

D. Block traffic on the DHCP ports to all systems.

104. Endpoint detection and response has three major components that make up its ability to provide visibility into endpoints. Which of the following is not one of those three parts?

A. Data search

B. Malware analysis

C. Data exploration

D. Suspicious activity detection

105. Isabelle is responsible for security at a mid-sized company. She wants to prevent users on her network from visiting job-hunting sites while at work. Which of the following would be the best device to accomplish this goal?

A. Proxy server

B. NAT

C. A packet filter firewall

D. NIPS

106. What term describes a cloud system that stores, manages, and allows auditing of API keys, passwords, and certificates?

A. A cloud PKI

B. A cloud TPM

C. A secrets manager

D. A hush service

107. Fred is building a web application that will receive information from a service provider. What open standard should he design his application to use to work with many modern third-party identity providers?

A. SAML

B. Kerberos

C. LDAP

D. NTLM

108. You are responsible for an e-commerce site. The site is hosted in a cluster. Which of the following techniques would be best in assuring availability?

A. A VPN concentrator

B. Aggregate switching

C. An SSL accelerator

D. Load balancing

109. What channels do not cause issues with channel overlap or overlap in U.S. installations of 2.4 GHz Wi-Fi networks?

A. 1, 3, 5, 7, 9, and 11

B. 2, 6, and 10

C. 1, 6, and 11

D. Wi-Fi channels do not suffer from channel overlap.

110. Ryan is concerned about the security of his company's web application. Since the application processes confidential data, he is most concerned about data exposure. Which of the following would be the most important for him to implement?

A. WAF

B. TLS

C. NIPS

D. NIDS

111. Which of the following connection methods only works via a line-of-sight connection?

A. Bluetooth

B. Infrared

C. NFC

D. Wi-Fi

112. Carole is responsible for various network protocols at her company. The Network Time Protocol has been intermittently failing. Which of the following would be most affected?

A. Kerberos

B. RADIUS

C. CHAP

D. LDAP

113. You are selecting an authentication method for your company's servers. You are looking for a method that periodically reauthenticates clients to prevent session hijacking. Which of the following would be your best choice?

A. PAP

B. SPAP

C. CHAP

D. OAuth

114. Naomi wants to deploy a firewall that will protect her endpoint systems from other systems in the same security zone of her network as part of a zero-trust design. What type of firewall is best suited to this type of deployment?

A. Hardware firewalls

B. Software firewalls

C. Virtual firewalls

D. Cloud firewalls

115. Lisa is setting up accounts for her company. She wants to set up accounts for the Oracle database server. Which of the following would be the best type of account to assign to the database service?

A. User

B. Guest

C. Admin

D. Service

116. Gary wants to implement EAP-based protocols for his wireless authentication and wants to ensure that he uses only versions that support Transport Layer Security (TLS). Which of the following EAP-based protocols does not support TLS?

A. LEAP

B. EAP-TTLS

C. PEAP

D. EAP-TLS

117. Manny wants to download apps that aren't in the iOS App Store, as well as change settings at the OS level that Apple does not normally allow to be changed. What would he need to do to his iPhone to allow this?

A. Buy an app via a third-party app store.

B. Install an app via side-loading.

C. Jailbreak the phone.

D. Install Android on the phone.

118. Many smartcards implement a wireless technology to allow them to be used without a card reader. What wireless technology is frequently used to allow the use of smartcards for entry-access readers and similar access controls?

A. Infrared

B. Wi-Fi

C. RFID

D. Bluetooth

119. Carl has been asked to set up access control for a server. The requirements state that users at a lower privilege level should not be able to see or access files or data at a higher privilege level. What access control model would best fit these requirements?

A. MAC

B. DAC

C. RBAC

D. SAML

120. Jack wants to deploy a network access control (NAC) system that will stop systems that are not fully patched from connecting to his network. If he wants to have full details of system configuration, antivirus version, and patch level, what type of NAC deployment is most likely to meet his needs?

A. Agentless, preadmission

B. Agent-based, preadmission

C. Agentless, postadmission

D. Agent-based, postadmission

121. Claire has been notified of a zero-day flaw in a web application. She has the exploit code, including a SQL injection attack that is being actively exploited. How can she quickly react to prevent this issue from impacting her environment if she needs the application to continue to function?

A. Deploy a detection rule to her IDS.

B. Manually update the application code after reverse-engineering it.

C. Deploy a fix via her WAF.

D. Install the vendor provided patch.

122. Eric wants to provide company-purchased devices, but his organization prefers to provide end users with choices among devices that can be managed and maintained centrally. What mobile device deployment model best fits this need?

A. BYOD

B. COPE

C. CYOD

D. VDI

123. Derek is in charge of his organization's certificate authorities and wants to add a new certificate authority. His organization already has three certificate authorities operating in a mesh: A. South American CA, B. the United States CA, and C, the European Union CA. As they expand into Australia, he wants to add D. the Australian CA. Which CAs will Derek need to issue certificates to from D. to ensure that systems in the Australian domain are able to access servers in A, B, and C's domains?

A. He needs all the other systems to issue D certificates so that his systems will be trusted there.

B. He needs to issue certificates from D to each of the other CAs systems and then have the other CAs issue D a certificate.

C. He needs to provide the private key from D to each of the other CAs.

D. He needs to receive the private key from each of the other CAs and use it to sign the root certificate for D.

124. Claire is concerned about an attacker getting information regarding network devices and their configuration in her company. Which protocol should she implement that would be most helpful in mitigating this risk while providing management and reporting about network devices?

A. RADIUS

B. TLS

C. SNMPv3

D. SFTP

125. Ben is using a tool that is specifically designed to send unexpected data to a web application that he is testing. The application is running in a test environment, and configured to log events and changes. What type of tool is Ben using?

A. A SQL injection proxy

B. A static code review tool

C. A web proxy

D. A fuzzer

126. Eric is responsible for his organization's mobile device security. They use a modern mobile device management (MDM) tool to manage a BYOD mobile device environment. Eric needs to ensure that the applications and data that his organization provides to users of those mobile devices remain as secure as possible. Which of the following technologies will provide him with the best security?

A. Storage segmentation

B. Containerization

C. Full-device encryption

D. Remote wipe

127. Murali is looking for an authentication protocol for his network. He is very concerned about highly skilled attackers. As part of mitigating that concern, he wants an authentication protocol that never actually transmits a user's password, in any form. Which authentication protocol would be a good fit for Murali's needs?

A. CHAP

B. Kerberos

C. RBAC

D. Type II

128. As part of the certificate issuance process from the CA that her company works with, Marie is required to prove that she is a valid representative of her company. The CA goes through additional steps to ensure that she is who she says she is and that her company is legitimate, and not all CAs can issue this type of certificate. What type of certificate has she been issued?

A. An EV certificate

B. A domain-validated certificate

C. An organization validation certificate

D. An OCSP certificate

129. Mark wants to provide a wireless connection with the highest possible amount of bandwidth. Which of the following should he select?

A. LTE cellular

B. Bluetooth

C. NFC

D. 802.11ac Wi-Fi

130. What is the primary advantage of cloud-native security solutions when compared to third-party solutions deployed to the same cloud environment?

A. Lower cost

B. Better security

C. Tighter integration

D. All of the above

131. Ed needs to securely connect to a DMZ from an administrative network using Secure Shell (SSH). What type of system is frequently deployed to allow this to be done securely across security boundaries for network segments with different security levels?

A. An IPS

B. A NAT gateway

C. A router

D. A jump box

132. You work for a social media website. You wish to integrate your users' accounts with other web resources. To do so, you need to allow authentication to be used across different domains, without exposing your users' passwords to these other services. Which of the following would be most helpful in accomplishing this goal?

A. Kerberos

B. SAML

C. OAuth

D. OpenID

133. Christina wants to ensure that session persistence is maintained by her load balancer. What is she attempting to do?

A. Ensure that all of a client's requests go to the same server for the duration of a given session or transaction.

B. Assign the same internal IP address to clients whenever they connect through the load balancer.

C. Ensure that all transactions go to the current server in a round-robin during the time it is the primary server.

D. Assign the same external IP address to all servers whenever they are the primary server assigned by the load balancer.

134. Tara is concerned about staff in her organization sending email with sensitive information like customer Social Security numbers (SSNs) included in it. What type of solution can she implement to help prevent inadvertent exposures of this type of sensitive data?

A. FDE

B. DLP

C. S/MIME

D. POP3S

135. Jennifer is considering using an infrastructure as a service cloud provider to host her organization's web application, database, and web servers. Which of the following is not a reason that she would choose to deploy to a cloud service?

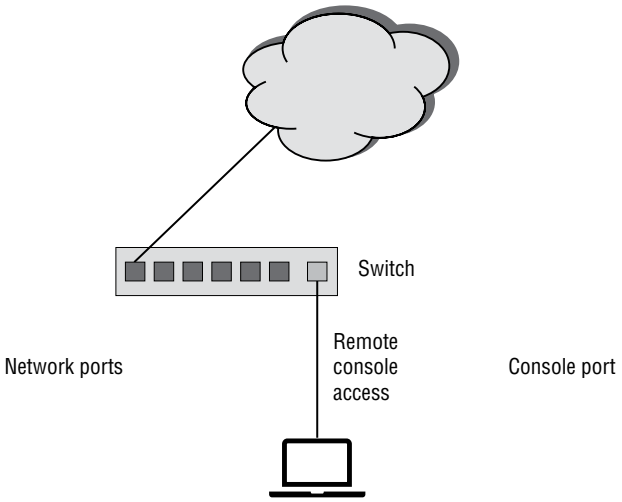
A. Support for high availability

B. Direct control of underlying hardware

C. Reliability of underlying storage

D. Replication to multiple geographic zones

136. This image shows an example of a type of secure management interface. What term describes using management interfaces or protected alternate means to manage devices and systems?



A. A DMZ

B. Out-of-band management

C. In-band management

D. A TLS

137. Chris has provided the BitLocker encryption keys for computers in his department to his organization's security office so that they can decrypt computers in the event of a breach of investigation. What is this concept called?

A. Key escrow

B. A BitLocker Locker

C. Key submission

D. AES jail

138. Marek has configured systems in his network to perform boot attestation. What has he configured the systems to do?

A. To run only trusted software based on previously stored hashes using a chained boot process

B. To notify a BOOTP server when the system has booted up

C. To hash the BIOS of the system to ensure that the boot process has occurred securely

D. To notify a remote system or management tool that the boot process was secure using measurements from the boot process

139. You have been asked to find an authentication service that is handled by a third party. The service should allow users to access multiple websites, as long as they support the third-party authentication service. What would be your best choice?

A. OpenID

B. Kerberos

C. NTLM

D. Shibboleth

140. Which of the following steps is a common way to harden the Windows registry?

A. Ensure the registry is fully patched.

B. Set the registry to read-only mode.

C. Disable remote registry access if not required.

D. Encrypt all user-mode registry keys.

141. Lois is designing the physical layout for her wireless access point (WAP) placement in her organization. Which of the following items is not a common concern when designing a WAP layout?

A. Determining construction material of the walls around the access points

B. Assessing power levels from other access points

C. Performing a site survey

D. Maximizing coverage overlap

142. Gabby has been laid off from the organization that she has worked at for almost a decade. Mark needs to make sure that Gabby's account is securely handled after her last day of work. What can he do to her account as an interim step to best ensure that files are still accessible and that the account could be returned to use if Gabby returns after the layoff?

A. Delete the account and re-create it when it is needed.

B. Disable the account and reenable it if it is needed.

C. Leave the account active in case Gabby returns.

D. Change the password to one Gabby does not know.

143. Mason is responsible for security at a company that has traveling salespeople. The company has been using ABAC for access control to the network. Which of the following is an issue that is specific to ABAC and might cause it to incorrectly reject logins?

A. Geographic location

B. Wrong password

C. Remote access is not allowed by ABAC.

D. Firewalls usually block ABAC.

144. Darrell is concerned that users on his network have too many passwords to remember and might write down their passwords, thus creating a significant security risk. Which of the following would be most helpful in mitigating this issue?

A. Multifactor authentication

B. SSO

C. SAML

D. LDAP

145. Frank is a security administrator for a large company. Occasionally, a user needs to access a specific resource that they don't have permission to access. Which access control methodology would be most helpful in this situation?

A. Mandatory access control (MAC)

B. Discretionary access control (DAC)

C. Role-based access control

D. Rule-based access control

146. Ed is designing the security architecture for his organization's move into an infrastructure as a service cloud environment. In his on-site datacenter, he has deployed a firewall in front of the datacenter network to protect it, and he has built rules that allow necessary services in, as well as outbound traffic for updates and similar needs. He knows that his cloud environment will be different. Which of the following is not a typical concern for cloud firewall designs?

A. Segmentation requirements for virtual private clouds (VPCs)

B. Hardware access for updates

C. The cost of operating firewall services in the cloud

D. OSI layers and visibility of traffic to cloud firewalls

147. Amelia is looking for a network authentication method that can use digital certificates and does not require end users to remember passwords. Which of the following would best fit her requirements?

A. OAuth

B. Tokens

C. OpenID

D. RBAC

148. Damian has designed and built a website that is accessible only inside of a corporate network. What term is used to describe this type of internal resource?

A. An intranet

B. An extranet

C. A DMZ

D. A TTL

149. The firewall that Walter has deployed looks at every packet sent by systems that travel through it, ensuring that each packet matches the rules that it operates and filters traffic by. What type of firewall is being described?

A. Next generation

B. Stateless

C. Application layer

D. Stateful

150. Nancy wants to protect and manage her RSA keys while using a mobile device. What type of solution could she purchase to ensure that the keys are secure so that she can perform public key authentication?

A. An application-based PKI

B. An OPAL-encrypted drive

C. A MicroSD HSM

D. An offline CA

151. Oliver needs to explain the access control scheme used by both the Windows and Linux filesystems. What access control scheme do they implement by default?

A. Role-based access control

B. Mandatory access control

C. Rule-based access control

D. Discretionary access control

152. Stefan just became the new security officer for a university. He is concerned that student workers who work late on campus could try to log in with faculty credentials. Which of the following would be most effective in preventing this?

A. Time-of-day restrictions

B. Usage auditing

C. Password length

D. Credential management

153. Next-generation firewalls include many cutting-edge features. Which of the following is not a common next-generation firewall capability?

A. Geolocation

B. IPS and/or IDS

C. Sandboxing

D. SQL injection

154. Greg knows that when a switch doesn't know where a node is, it will send out a broadcast to attempt to find it. If other switches inside its broadcast domain do not know about the node, they will also broadcast that query, and this can create a massive amount of traffic that can quickly amplify out of control. He wants to prevent this scenario without causing the network to be unable to function. What port-level security feature can he enable to prevent this?

A. Use ARP blocking.

B. Block all broadcast packets.

C. Enable storm control.

D. None of the above

155. Isaac is designing his cloud datacenter's public-facing network and wants to properly implement segmentation to protect his application servers while allowing his web servers to be accessed by customers. What design concept should he apply to implement this type of secure environment?

A. A reverse proxy server

B. A DMZ

C. A forward proxy server

D. A VPC

156. Jennifer is concerned that some people in her company have more privileges than they should. This has occurred due to people moving from one position to another and having cumulative rights that exceed the requirements of their current jobs. Which of the following would be most effective in mitigating this issue?

A. Permission auditing

B. Job rotation

C. Preventing job rotation

D. Separation of duties

157. Susan has been tasked with hardening the systems in her environment and wants to ensure that data cannot be recovered from systems if they are stolen or their disk drives are stolen and accessed. What is her best option to ensure data security in these situations?

A. Deploy folder-level encryption.

B. Deploy full-disk encryption.

C. Deploy file-level encryption.

D. Degauss all the drives.

158. Chloe has noticed that users on her company's network frequently have simple passwords made up of common words. Thus, they have weak passwords. How could Chloe best mitigate this issue?

A. Increase minimum password length.

B. Have users change passwords more frequently.

C. Require password complexity.

D. Implement Single Sign-On (SSO).

159. Which Wi-Fi protocol implements simultaneous authentication of equals (SAE) to improve on previous security models?

A. WEP

B. WPA

C. WPA2

D. WPA3

160. Megan wants to set up an account that can be issued to visitors. She configures a kiosk application that will allow users in her organization to sponsor the visitor, set the amount of time that the user will be on-site, and then allow them to log into the account, set a password, and use Wi-Fi and other services. What type of account has Megan created?

A. A user account

B. A shared account

C. A guest account

D. A service account

161. Henry wants to deploy a web service to his cloud environment for his customers to use. He wants to be able to see what is happening and stop abuse without shutting down the service if customers cause issues. What two things should he implement to allow this?

A. An API gateway and logging

B. API keys and logging via an API gateway

C. An API-centric IPS and an API proxy

D. All of the above

162. Patrick has been asked to identify a UTM appliance for his organization. Which of the following capabilities is not a common feature for a UTM device?

A. IDS and or IPS

B. Antivirus

C. MDM

D. DLP

163. A companywide policy is being created to define various security levels. Which of the following systems of access control would use documented security levels like Confidential or Secret for information?

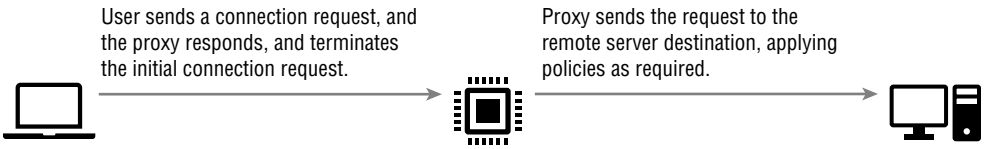
A. RBAC

B. MAC

C. DAC

D. BAC

164. This image shows a type of proxy. What type of proxy is shown?



A. A forward proxy

B. A boomerang proxy

C. A next generation proxy

D. A reverse proxy

165. Gurvinder is reviewing log files for authentication events and notices that one of his users has logged in from a system at his company's home office in Chicago. Less than an hour later, the same user is recorded as logging in from an IP address that geo-IP tools say comes from Australia. What type of issue should he flag this as?

A. A misconfigured IP address

B. An impossible travel time, risky login issue

C. A geo-IP lookup issue

D. None of the above

166. Users in your network are able to assign permissions to their own shared resources. Which of the following access control models is used in your network?

A. DAC

B. RBAC

C. MAC

D. ABAC

167. Cynthia is preparing a new server for deployment and her process includes turning off unnecessary services, setting security settings to match her organization's baseline configurations, and installing patches and updates. What is this process known as?

A. OS hardening

B. Security uplift

C. Configuration management

D. Endpoint lockdown

168. John is performing a port scan of a network as part of a security audit. He notices that the domain controller is using secure LDAP. Which of the following ports would lead him to that conclusion?

A. 53

B. 389

C. 443

D. 636

169. Chris wants to securely generate and store cryptographic keys for his organization's servers, while also providing the ability to offload TLS encryption processing. What type of solution should he recommend?

A. A GPU in cryptographic acceleration mode

B. A TPM

C. A HSM

D. A CPU in cryptographic acceleration mode

170. Tracy wants to protect desktop and laptop systems in her organization from network attacks. She wants to deploy a tool that can actively stop attacks based on signatures, heuristics, and anomalies. What type of tool should she deploy?

A. A firewall

B. Antimalware

C. HIDS

D. HIPS

171. Which of the following access control methods grants permissions based on the user's position in the organization?

A. MAC

B. RBAC

C. DAC

D. ABAC

172. What does UEFI measured boot do?

A. Records how long it takes for a system to boot up

B. Records information about each component that is loaded, stores it in the TPM, and can report it to a server

C. Compares the hash of every component that is loaded against a known hash stored in the TPM

D. Checks for updated versions of the UEFI, and compares it to the current version; if it is measured as being too far out of date, it updates the UEFI

173. Kerberos uses which of the following to issue tickets?

A. Authentication service

B. Certificate authority

C. Ticket-granting service

D. Key distribution center

174. Maria wants to ensure that her wireless controller and access points are as secure as possible from attack via her network. What control should she put in place to protect them from brute-force password attacks and similar attempts to take over her wireless network's hardware infrastructure?

A. Regularly patch the devices.

B. Disable administrative access.

C. Put the access points and controllers on a separate management VLAN.

D. All of the above

175. Marcus wants to check on the status of carrier unlocking for all mobile phones owned by and deployed by his company. What method is the most effective way to do this?

A. Contact the cellular provider.

B. Use an MDM tool.

C. Use a UEM tool.

D. None of the above; carrier unlock must be verified manually on the phone.

176. Michael wants to implement a zero-trust network. Which of the following steps is not a common step in establishing a zero trust network?

A. Simplify the network.

B. Use strong identity and access management.

C. Configure firewalls for least privilege and application awareness.

D. Log security events and analyze them.

177. Samantha is looking for an authentication method that incorporates the X.509 standard and will allow authentication to be digitally signed. Which of the following authentication methods would best meet these requirements?

A. Certificate-based authentication

B. OAuth

C. Kerberos

D. Smartcards

178. Your company relies heavily on cloud and SaaS service providers such as `salesforce.com`, Office365, and Google. Which of the following would you have security concerns about?

A. LDAP

B. TACACS+

C. SAML

D. Transitive trust

179. What is the primary difference between MDM and UEM?

A. MDM does not include patch management.

B. UEM does not include support for mobile devices.

C. UEM supports a broader range of devices.

D. MDM patches domain machines, not enterprise machines.

180. Kathleen wants to implement a zero-trust network design and knows that she should segment the network. She remains worried about east/west traffic inside the network segments. What is the first security tool she should implement to ensure hosts remain secure from network threats?

A. Antivirus

B. Host-based firewalls

C. Host-based IPS

D. FDE

181. Gary is designing his cloud infrastructure and needs to provide a firewall-like capability for the virtual systems he is running. Which of the following cloud capabilities acts like a virtual firewall?

A. Security groups

B. Dynamic resource allocation

C. VPC endpoints

D. Instance awareness

182. Derek has enabled automatic updates for the Windows systems that are used in the small business he works for. What hardening process will still need to be tackled for those systems if he wants a complete patch management system?

A. Automated installation of Windows patches

B. Windows Update regression testing

C. Registry hardening

D. Third-party software and firmware patching

183. Theresa implements a network-based IDS. What can she do to traffic that passes through the IDS?

A. Review the traffic based on rules and detect and alert about unwanted or undesirable traffic.

B. Review the traffic based on rules and detect and stop traffic based on those rules.

C. Detect sensitive data being sent to the outside world and encrypt it as it passes through the IDS.

D. All of the above

184. Murali is building his organization's container security best practices document and wants to ensure that he covers the most common items for container security. Which of the following is not a specific concern for containers?

A. The security of the container host

B. Securing the management stack for the container

C. Insider threats

D. Monitoring network traffic to and from the containers for threats and attacks

185. Gary's organization uses a NAT gateway at its network edge. What security benefit does a NAT gateway provide?

A. It statefully blocks traffic based on port and protocol as a type of firewall.

B. It can detect malicious traffic and stop it from passing through.

C. It allows systems to connect to another network without being directly exposed to it.

D. It allows non-IP-based addresses to be used behind a legitimate IP address.

186. Fred sets up his authentication and authorization system to apply the following rules to authenticated users:

- Users who are not logging in from inside the trusted network must use multifactor authentication.
- Users whose devices have not passed a NAC check must use multifactor authentication.
- Users who have logged in from geographic locations that are more than 100 miles apart within 15 minutes will be denied.

What type of access control is Fred using?

A. Geofencing

B. Time-based logins

C. Conditional access

D. Role-based access

187. Henry is an employee at Acme Company. The company requires him to change his password every three months. He has trouble remembering new passwords, so he keeps switching between just two passwords. Which policy would be most effective in preventing this?

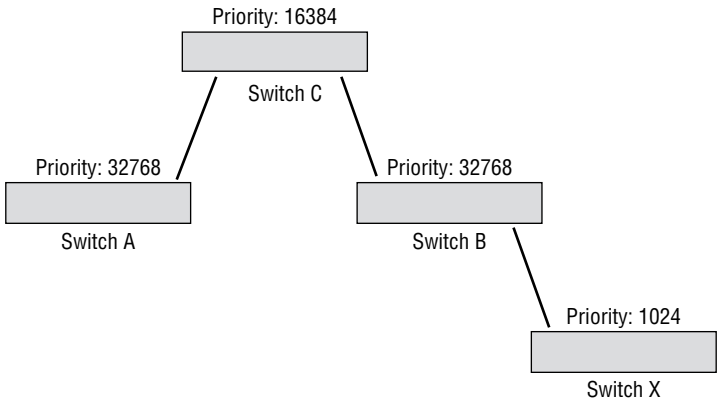
A. Password complexity

B. Password history

C. Password length

D. Multifactor authentication

188. The following image shows a scenario where Switch X is attached to a network by an end user and advertises itself with a lower spanning tree priority than the existing switches. Which of the following settings can prevent this type of issue from occurring?



A. 802.11n

B. Port recall

C. RIP guard

D. BPDU guard

189. Tracy wants to limit when users can log in to a standalone Windows workstation. What can Tracy do to make sure that an account called "`visitor`" can only log in between 8 a.m. and 5 p.m. every weekday?

A. Running the command `net user visitor /time:M-F,8am-5pm`

B. Running the command `netreg user visitor -daily -working-hours`

C. Running the command `login limit:daily time: 8-5`

D. This cannot be done from the Windows command line.

190. Sheila is concerned that some users on her network may be accessing files that they should not—specifically, files that are not required for their job tasks. Which of the following would be most effective in determining if this is happening?

A. Usage auditing and review

B. Permissions auditing and review

C. Account maintenance

D. Policy review

191. In which of the following scenarios would using a shared account pose the least security risk?

A. For a group of tech support personnel

B. For guest Wi-Fi access

C. For students logging in at a university

D. For accounts with few privileges

192. Mike's manager has asked him to verify that the certificate chain for their production website is valid. What has she asked Mike to validate?

A. That the certificate has not been revoked

B. That users who visit the website can verify that the site and the CAs in the chain are all trustworthy

C. That the encryption used to create the certificate is strong and has not been cracked

D. That the certificate was issued properly and that prior certificates issued for the same system have also been issued properly

193. Maria is responsible for security at a small company. She is concerned about unauthorized devices being connected to the network. She is looking for a device authentication process. Which of the following would be the best choice for her?

A. CHAP

B. Kerberos

C. 802.11i

D. 802.1X

194. Which wireless standard uses CCMP to provide encryption for network traffic?

A. WPA2

B. WEP

C. Infrared

D. Bluetooth

195. Charles is a CISO for an insurance company. He recently read about an attack wherein an attacker was able to enumerate all the network devices in an organization. All this was done by sending queries using a single protocol. Which protocol should Charles secure to mitigate this attack?

A. SNMP

B. POP3

C. DHCP

D. IMAP

196. Magnus is concerned about someone using a password cracker on computers in his company. He is concerned that crackers will attempt common passwords in order to log in to a system. Which of the following would be best for mitigating this threat?

A. Password age restrictions

B. Password minimum length requirements

C. Account lockout policies

D. Account usage auditing

197. Lucas is looking for an XML-based open standard for exchanging authentication information. Which of the following would best meet his needs?

A. SAML

B. OAuth

C. RADIUS

D. NTLM

198. Joshua is looking for an authentication protocol that would be effective at stopping session hijacking. Which of the following would be his best choice?

A. CHAP

B. PAP

C. TACACS+

D. RADIUS

199. Greg's company has a remote location that uses an IP-based streaming security camera system. How could Greg ensure that the remote location's networked devices can be managed as if they are local devices and that the traffic to that remote location is secure?

A. An as-needed TLS VPN

B. An always-on TLS VPN

C. An always-on IPSec VPN

D. An as-needed IPSec VPN

200. What does the OPAL standard specify?

A. Online personal access licenses

B. Self-encrypting drives

C. The origin of personal accounts and libraries

D. Drive sanitization modes for degaussers

201. What does Unified Extensible Firmware Interface (UEFI) Secure Boot do?

A. It protects against worms during the boot process.

B. It validates a signature for each binary loaded during boot.

C. It validates the system BIOS version.

D. All of the above

202. Derek is trying to select an authentication method for his company. He needs one that will work with a broad range of services like those provided by Microsoft and Google so that users can bring their own identities. Which of the following would be his best choice?

A. Shibboleth

B. RADIUS

C. OpenID Connect

D. OAuth

203. Jason is considering deploying a network intrusion prevention system (IPS) and wants to be able to detect advanced persistent threats. What type of IPS detection method is most likely to detect the behaviors of an APT after it has gathered baseline information about normal operations?

A. Signature-based IPS detections

B. Heuristic-based IPS detections

C. Malicious tool hash IPS detections

D. Anomaly-based IPS detections

204. What component is most often used as the foundation for a hardware root of trust for a modern PC?

A. The CPU

B. A TPM

C. A HSM

D. The hard drive or SSD

205. Dennis wants to deploy a firewall that can provide URL filtering. What type of firewall should he deploy?

A. A packet filter

B. A stateful packet inspection firewall

C. A next-generation firewall

D. None of the above

206. Waleed's organization uses a combination of internally developed and commercial applications that they deploy to mobile devices used by staff throughout the company. What type of tool can he use to handle a combination of bring-your-own-device phones and corporate tablets that need to have these applications loaded onto them and removed from them when their users are no longer part of the organization?

A. MOM

B. MLM

C. MIM

D. MAM

207. Charlene is preparing a report on the most common application security issues for cloud applications. Which of the following is not a major concern for cloud applications?

A. Local machine access leading to compromise

B. Misconfiguration of the application

C. Insecure APIs

D. Account compromise

208. The CA that Samantha is responsible for is kept physically isolated and is never connected to a network. When certificates are issued, they are generated then manually transferred via removable media. What type of CA is this, and why would Samantha's organization run a CA in this mode?

A. An online CA; it is faster to generate and provide certificates.

B. An offline CA; it is faster to generate and provide certificates.

C. An online CA; it prevents potential exposure of the CA's root certificate.

D. An offline CA; it prevents potential exposure of the CA's root certificate.

209. Susan has configured a virtual private network (VPN) so that traffic destined for systems on her corporate network is routed over the VPN but traffic sent to other destinations is sent out via the VPN user's local network. What is this configuration called?

A. Half-pipe

B. Full-tunnel

C. Split-tunnel

D. Split horizon

210. Adam has experienced problems with users plugging in cables between switches on his network, which results in multiple paths to the same destinations being available to systems on the network. When this occurs, the network experiences broadcast storms, causing network outages. What network configuration setting should he enable on his switches to prevent this?

A. Loop protection

B. Storm watch

C. Sticky ports

D. Port inspection

211. Charles is concerned that users of Android devices in his company are delaying OTA updates. Why would Charles be concerned about this, and what should he do about it?

A. OTA updates patch applications, and a NAC agent would report on all phones in the organization.

B. OTA updates update device encryption keys and are necessary for security, and a PKI would track encryption certificates and keys.

C. OTA updates patch firmware and updates phone configurations, and an MDM tool would provide reports on firmware versions and phone settings

D. OTA updates are sent by phones to report on online activity and tracking, and an MDM tool receives OTA updates to monitor phones

212. Ben is preparing to implement a firewall for his network and is considering whether to implement an open source firewall or a proprietary commercial firewall. Which of the following is not an advantage of an open source firewall?

A. Lower cost

B. Community code validation

C. Maintenance and support

D. Speed of acquisition

213. Barbara wants to implement WPA3 Personal. Which of the following features is a major security improvement in WPA3 over WPA2?

A. DDoS monitoring and prevention

B. Per-channel security

C. Brute-force attack prevention

D. Improvements from 64-bit to 128-bit encryption

214. Isaac wants to implement mandatory access controls on an Android-based device. What can he do to accomplish this?

A. Run Android in single-user mode.

B. Use SEAndroid.

C. Change the Android registry to MAC mode.

D. Install MACDroid.

215. Greg has implemented a system that allows users to access accounts like administrator and root without knowing the actual passwords for the accounts. When users attempt to use elevated accounts, their request is compared to policies that determine if the request should be allowed. The system generates a new password each time a trusted user requests access, and then logs the access request. What type of system has Greg implemented?

A. A MAC system

B. A PAM system

C. A FDE system

D. A TLS system

216. Alaina has issued Android tablets to staff in her production facility, but cameras are banned due to sensitive data in the building. What type of tool can she use to control camera use on all of her organization's corporate devices that she issues?

A. MDM

B. DLP

C. OPAL

D. MMC

217. Olivia wants to enforce a wide variety of settings for devices used in her organization. Which of the following methods should she select if she needs to manage hundreds of devices while setting rules for use of SMS and MMS, audio and video recording, GPS tagging, and wireless connection methods like tethering and hotspot modes?

A. Use baseline settings automatically set for every phone before it is deployed using an imaging tool.

B. Require users to configure their phones using a lockdown guide.

C. Use a UEM tool and application to manage the devices.

D. Use a CASB tool to manage the devices.

218. John wants to deploy a solution that will provide content filtering for web applications, CASB functionality, DLP, and threat protection. What type of solution can he deploy to provide these features?

A. A reverse proxy

B. A VPC gateway

C. An NG SWG

D. A next-gen firewall

219. Brian wants to limit access to a federated service that uses Single Sign-On based on user attributes and group membership, as well as which federation member the user is logging in from. Which of the following options is best suited to his needs?

A. Geolocation

B. Account auditing

C. Access policies

D. Time-based logins

220. Sharif uses the `chmod` command in Linux to set the permissions to a file using the command `chmod 700 example.txt`. What permission has he set on the file?

A. All users have write access to the file.

B. The user has full access to the file.

C. All users have execute access to the file.

D. The user has execute access to the file.

221. Patrick regularly connects to untrusted networks when he travels and is concerned that an on-path attack could be executed against him as he browses websites. He would like to validate certificates against known certificates for those websites. What technique can he use to do this?

A. Check the CRL.

B. Use certificate pinning.

C. Compare his private key to their public key.

D. Compare their private key to their public key.

222. What is the most common format for certificates issued by certificate authorities?

A. DER

B. PFX

C. PEM

D. P7B

223. Michelle's organization uses self-signed certificates throughout its internal infrastructure. After a compromise, Michelle needs to revoke one of the self-signed certificates. How can she do that?

A. Contact the certificate authority and request that they revoke the certificate.

B. Add the certificate to the CRL.

C. Remove the certificate from the list of whitelisted certificates from each machine that trusts it.

D. Reissue the certificate, causing the old version to be invalidated.

224. Which of the following is not a common way to validate control over a domain for a domain-validated X.509 certificate?

A. Changing the DNS TXT record

B. Responding to an email sent to a contact in the domain's WHOIS information

C. Publishing a nonce provided by the certificate authority as part of the domain information

D. Changing the IP addresses associated with the domain

225. Fiona knows that SNMPv3 provides additional security features that previous versions of SNMP did not. Which of the following is not a security feature provided by SNMPv3?

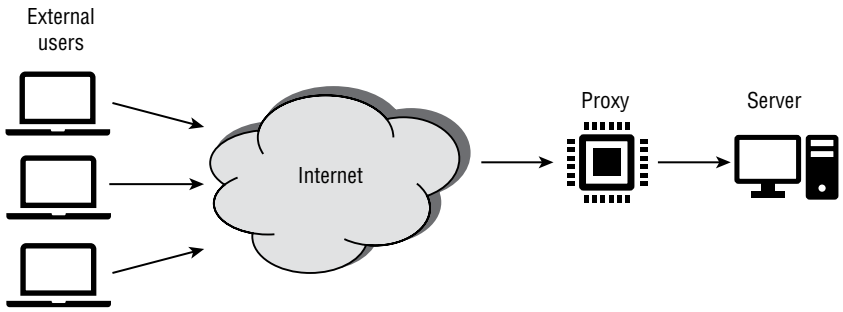
A. SQL injection prevention

B. Message integrity

C. Message authentication

D. Message confidentiality

226. The following figure shows a proxy in use. In this usage model, the proxy receives a connection request, and then connects to the server and forwards the original request. What type of proxy is this?



A. A reverse proxy

B. A round-robin proxy

C. A next-generation proxy

D. A forward proxy