**1. Homer needs to send an email to his supervisor with an attachment**

**that includes proprietary data. He wants to maintain the confidentiality of**

**this data. Which of the following choices is the BEST choice to meet his**

**needs?**

A. Digital signature

B. Encryption

C. Steganography

D. Hashing

**2. You are the security administrator in your organization. You want to**

**ensure that a file maintains integrity. Which of the following choices is the**

**BEST solution to meet your goal?**

A. Steganography

B. Encryption

C. Hash

D. AES

**3. Which of the following accurately identifies primary security control**

**types?**

A. Role-based and discretionary

B. Technical and administrative

C. Confidentiality and availability

D. Encryption and hashing

**4. You recently started a new job in information technology security.**

**Your primary responsibilities are to monitor security logs, analyze trend**

**reports, and install CCTV systems. Which of the following choices BEST**

**identifies your responsibilities? (Select TWO.)**

A. Hardening systems

B. Detecting security incidents

C. Preventing incidents

D. Implementing monitoring controls

**5. A security expert is identifying and implementing several different**

**physical deterrent controls to protect an organization’s server room.**

Which of the following choices would BEST meet this objective?

A. Using hardware locks

B. Utilizing data encryption

C. Performing a vulnerability assessment

D. Training users

**6. An organization is implementing a feature that allows multiple**

**servers to operate on a single physical server. Which of the following is**

**the feature being implemented?**

A. Virtualization

B. IaaS

C. Cloud computing

D. DLP

**7. Lisa is using a Linux computer to monitor network traffic. She**

**connected the computer to the mirror port of a switch and started the**

**logging software. However, she found that the only traffic being collected**

**is traffic to or from the Linux computer. She wants to collect all traffic**

**going through the switch. Which of the following actions should she take?**

A. Run the command ipconfig eth0 promisc.

B. Run the command ifconfig eth0 promisc.

C. Reconfigure the switch.

D. Connect the computer to a router.

**8. Management has updated the security policy and it has changed the**

**requirements for the password policy. The password policy needs to**

**ensure that users change their passwords regularly and they cannot reuse**

**their passwords. Which of the following settings need to be configured?**

**(Select THREE.)**

A. Maximum password age

B. Password length

C. Password history

D. Password complexity

E. Minimum password age

**9. Your organization has implemented a system that stores user**

**credentials in a central database. Users log on once with their credentials.**

**They can then access other systems in the organization without logging on**

**again. Which of the following does this describe?**

A. Federation

B. SAML

C. Single sign-on

D. Biometrics

**10. You are modifying a configuration file used to authenticate Linux**

**accounts against an external server. The file includes phrases such as**

**DC=Server1 and DC=Com. Which authentication service is the external**

**server MOST likely using?**

A. Diameter

B. RADIUS

C. LDAP

D. SAML

**11. A network includes a ticket-granting ticket server. Which of the**

**following choices is the primary purpose of this server?**

A. Authentication

B. Identification

C. Authorization

D. Access control

**12. Your organization has a strict policy requiring administrators to**

**disable user accounts during the exit interview. This provides several**

**security benefits. Which of the following choices BEST identifies a**

**security benefit of this practice?**

A. Ensures that user security keys are retained

Ensures that user files are retained

C. Ensures that the account can be enabled again if the employee

returns

D. Ensures that users cannot log on remotely

**13. An administrator needs to grant users access to different servers**

**based on their job functions. Which access control model is the BEST**

**choice to use?**

A. Discretionary access control

B. Mandatory access control

C. Role-based access control

D. Rule-based access control

**14. You configure access control for users in your organization. Some**

**departments have a high employee turnover, so you want to simplify**

**account administration. Which of the following is the BEST choice?**

A. User-assigned privileges

B. Group-based privileges

C. Domain-assigned privileges

D. Network-assigned privileges

**15. The Mapple organization is creating a help-desk team to assist**

**employees with account issues. Members of this team need to create and**

**modify user accounts and occasionally reset user passwords. Which of**

**the following is the BEST way to accomplish this goal?**

A. Give each help-desk employee appropriate privileges

individually.

B. Add members of the help-desk team to a security group that has

the appropriate privileges.

C. Add each member of the help-desk team to the administrator

group within the domain.

D. Assign attributes to members of the group and give these

attributes appropriate privileges.

**16. Lisa wants to manage and monitor the switches and routers in her**

**network. Which of the following protocols would she use?**

A. NAT

B. SRTP

C. SNMPv3

D. DNSSEC

**17. Your organization has several switches within the network. You need to**

**implement a security control to prevent unauthorized access to these**

**switches. Which of the following choices BEST meets this need?**

A. Disable unused ports.

B. Implement an implicit deny rule.

C. Disable STP.

D. Enable SSH.

**18. A network technician incorrectly wired switch connections in your**

**organization’s network. It effectively disabled the switch as though it was**

**a victim of a denial-of-service attack. Which of the following should be**

**done to prevent this in the future?**

A. Install an IDS.

B. Only use Layer 2 switches.

C. Install SNMPv3 on the switches.

D. Implement STP or RSTP.

**19. Your network currently has a dedicated firewall protecting access to**

**a web server. It is currently configured with only the following two rules in the ACL:**

**PERMIT TCP ANY**

**ANY 443 PERMIT**

**TCP ANY ANY 80**

**You have detected DNS requests and zone transfer requests coming**

**through the firewall and you need to block them. Which of the following**

**would meet this goal? (Select TWO. Each answer is a full solution.)**

A. Add the following rule to the firewall: DENY TCP ALL ALL 53.

B. Add the following rule to the firewall: DENY UDP ALL ALL 53.

C. Add the following rule to the firewall: DENY TCP ALL ALL 25.

D. Add the following rule to the firewall: DENY IP ALL ALL 53.

E. Add an implicit deny rule at the end of the ACL.

**20. Your organization wants to combine some of the security controls used**

**to control incoming and outgoing network traffic. At a minimum, the**

**solution should include malware inspection, content inspection, and a**

**DDoS mitigator. Which of the following BEST meets this goal?**

A. VLAN

B. NAT

C. UTM

D. DNSSEC

**21. Your email server is getting overloaded with spam and much of it is**

**malicious. You need to implement a solution that can help reduce the**

**amount of spam reaching the email server. Which of the following is the**

**BEST choice?**

A. Reverse proxy

B. Media gateway

C. Web application firewall

D. Mail gateway

**22. Your organization has a dedicated classroom used for teaching**

**computer classes. Students include internal employees and visiting guests.**

**Security administrators recently discovered that students were unplugging**

**the network cable from some classroom computers and plugging the**

**network cable into their laptop computers, giving them access to network**

**resources. Which of the following is the BEST solution to prevent this**

**activity?**

A. Flood guard

B. VLAN

C. Port security

D. Loop protection

**23. A HIDS reported a vulnerability on a system based on a known**

**attack. After researching the alert from the HIDS, you identify the**

**recommended solution and begin applying it. What type of HIDS is in**

**use?**

A. Network-based

B. Signature-based

C. Heuristic-based

D. Anomaly-based

**24. After recently adding additional network devices, administrators**

**noticed an increased workload related to their IDS. Which of the**

**following can cause an increased workload from incorrect reporting?**

A. False negatives

B. False positives

C. Signature-based IDS

D. Behavioral-based IDS

**25. Lenny noticed a significant number of logon failures for**

**administrator accounts on the organization’s public web site. After**

**investigating it further, he notices that most of these attempts are from IP**

**addresses assigned to foreign countries. He wants to implement a solution**

**that will detect and prevent similar attacks. Which of the following is the**

**BEST choice?**

A. Add a flood guard to the network.

B. Block all traffic from foreign countries.

C. Implement an IPS.

D. Disable the administrator accounts.

**26. You are assisting a small business owner in setting up a public**

**wireless hot spot for her customers. Which of the following actions is**

**MOST appropriate for this hot spot?**

A. Using Open mode

B. Enabling MAC filtering

C. Disabling SSID broadcast

D. Installing directional antennas

**27. Jasper is setting up an 802.11ac network at the Retirement Castle. He**

**wants to provide the highest level of security. Which of the following**

**would BEST meet his needs?**

A. WPA2 with AES

B. WPA2 with TKIP

C. WPA2 with SSL

D. WPA2 with MD5

**28. You are planning a wireless network for a business. A core**

**requirement is to ensure that the solution encrypts user credentials when**

**users enter their usernames and passwords. Which of the following BEST**

**meets this requirement?**

A. WPA2-PSK

B. WPA2 using CCMP

C. WPS with EAP-FAST

D. WPA2 with EAP-TTLS

**29. An attacker can access email contact lists on your smartphone. What**

**type of attack is this?**

A. Bluesnarfing

B. Bluejacking

C. Captive portal

D. WPS

**30. An organization is hosting a VPN. Management wants to ensure that all**

**VPN clients are using up-to-date operating systems and antivirus software.**

**Which of the following would BEST meet this need?**

A. NAT

B. NAC

C. VLAN

D. DMZ

**31. A network administrator needs to update the operating system on**

**switches used within the network. Assuming the organization is following**

**standard best practices, what should the administrator do first?**

A. Submit a request using the baseline configuration process.

B. Submit a request using the incident management process.

C. Submit a request using the change management process.

D. Submit a request using the application patch management process.

**32. What functions does an HSM include?**

A. Reduces the risk of employees emailing confidential

information outside the organization

B. Provides webmail to clients

C. Provides full drive encryption

D. Generates and stores keys used with servers

**33. The Shelbyville Nuclear Power Plant stores some data in the cloud**

**using its own resources. The Springfield school system also has a cloud**

**using its own resources. Later, the two organizations decide to share some**

**of the educational data in both clouds. Which of the following BEST**

**describes the cloud created by these two organizations?**

A. Community

B. Private

C. Public

D. PaaS

**34. Ziffcorp is planning to eliminate its current BYOD policy and instead**

**implement a COPE deployment model. You’re asked to provide input for**

**the new policy. Which of the following concepts are appropriate for this**

**policy?**

A. Encryption on employee-owned devices

B. HSM

C. ISA

D. Remote wipe

**35. Your organization is planning to implement a CYOD policy. Which of**

**the following security controls will help protect data by isolating it?**

A. Encrypt sensitive data

B. Storage segmentation

C. Full device encryption

D. Rooting

**36. Bart recently launched an attack on a company web site using scripts**

**he found on the Internet. Which of the following BEST describes Bart as**

**a threat actor?**

A. Insider

B. Hacktivist

C. Script kiddie

D. Nation-state

**37. Recently, malware on a computer at the Monty Burns Casino**

**destroyed several important files after it detected that Homer was no**

**longer employed at the casino. Which of the following BEST identifies**

**this malware?**

A. Logic bomb

B.Rootkit

C. Backdoor

D. Adware

**38. A security administrator at a shopping mall discovered two wireless**

**cameras pointing at an automatic teller machine. These cameras were not**

**installed by mall personnel and are not authorized. What is the MOST**

**likely goal of these cameras?**

A. Tailgating

B. Dumpster diving

C. Vishing

D. Shoulder surfing

**39. Maggie reports that she keeps receiving unwanted emails about**

**mortgages. What does this describe?**

A. Phishing

B. Spear phishing

C. Spam

D. Vishing

**40. Your organization has been receiving a significant amount of spam**

**with links to malicious web sites. You want to stop the spam. Of the**

**following choices, which provides the BEST solution?**

A. Add the domain to a block list.

B. Use a URL filter.

C. Use a MAC filter.

D. Add antivirus software.

**41. Lisa received an email advertising the newest version of a popular**

**smartphone. She’s been looking for this smartphone, but can’t find it**

**anywhere else. This email includes a malicious link. Which of the**

**following principles is the email sender employing?**

A. Authority

B. Intimidation

C. Scarcity

D. Trust

**42. An IDS alerts on increased traffic. Upon investigation, you realize it**

**is due to a spike in network traffic from several sources. Assuming this is**

**malicious, which of the following is the MOST likely explanation?**

A. A smurf attack

B. A spoofing attack

C. A DoS attack

D. A DDoS attack

**43. An application on one of your database servers has crashed several**

**times recently. Examining detailed debugging logs, you discover that just**

**prior to crashing, the database application is receiving a long series of x90**

**characters. What is MOST likely occurring?**

A. SQL injection

B. Buffer overflow

C. XML injection

D. Zero-day

**44. A review of a web application discovered that the application is not**

**performing boundary checking. Which of the following should the web**

**developer add to this application to resolve this issue?**

A. XSRF

B. XSS

C. Input validation

D. Fuzzing

**45. Web developers are implementing error handling in a web site**

**application. Which of the following represents a best practice for this?**

A. Displaying a detailed error message but logging generic

information on the error

B. Displaying a generic error message but logging detailed

information on the error

C. Displaying a generic error message and logging generic

information on the error

D. Displaying a detailed error message and logging detailed

information on the error

**46. Developers have created an application that users can download and**

**install on their computers. Management wants to provide users with a**

**reliable method of verifying that the application has not been modified.**

**Which of the following methods provides the BEST solution?**

A. Code signing

B. Input validation

C. Code obfuscation

D. Stored procedures

**47. Some protocols include timestamps and sequence numbers. These**

**components help protect against what type of attacks?**

A. Amplification

B. Replay

C. SYN flood

D. Salting

**48. Looking at logs for an online web application, you see that someone**

**has entered the following phrase into several queries:**

**‘ or ‘1’=’1’ --**

**Which of the following provides the BEST protection against this attack?**

A. Normalization

B. Proper error handling

C. Removing dead code

D. Stored procedures

**49. You need to calculate the ALE for a server. The value of the server is**

**$3,000 and it has failed 10 times in the past year. Each time it failed, it**

**resulted in a 10 percent loss. What is the ALE?**

A. $300

B. $500

C. $3,000

D. $30,000

**50. A recent vulnerability scan reported that a web application server is**

**missing some patches. However, after inspecting the server, you realize**

**that the patches are for a protocol that administrators removed from the**

**server. Which of the following is the BEST explanation for this disparity?**

A. False negative

B. False positive

C. Lack of patch management tools

D. The patch isn’t applied

**51. You suspect that a database server used by a web application does not**

**have current patches. Which of the following is the BEST action to take to**

**verify the server has up-to-date patches?**

A. Network mapping

B. Port scan

C. Protocol analyzer

D. Vulnerability scan

**52. You suspect that a user is running an unauthorized AP within the**

**organization’s building. Which of the following tools is the BEST choice**

**to see if an unauthorized AP is operating on the network?**

A. Rogue system

B. Wireless scanner

C. Password cracker

D. Penetration test

**53. Your organization outsourced development of a software module to**

**modify the functionality of an existing proprietary application. The**

**developer completed the module and is now testing it with the entire**

**application. What type of testing is the developer performing?**

A. White box

B. Black box

C. Gray box

D. Black hat

**54. Your coworker tells you how recent attacks on the network have been**

**disrupting services and network connectivity. He suggests that you use**

**Nmap to run a vulnerability scan on the network and identify**

**vulnerabilities. Which of the following should you do FIRST?**

A. Create a network map.

B. Locate a network map.

C. Obtain an administrative account to run a credentialed scan.

D. Obtain authorization.

**55. Your organization’s security policy states that administrators should**

**follow the principle of least privilege. Which of the following tools can**

**ensure that administrators are following the policy?**

A. Permission auditing review

B. Risk assessment

C. Vulnerability assessment

D. Threat assessment

**56. You need to secure access to a data center. Which of the following**

**choices provides the BEST physical security to meet this need? (Select**

**THREE.)**

A. Biometrics

B. Cable locks

C. Mantrap

D. CCTV

**57. Your company wants to control access to a restricted area of the**

**building by adding an additional physical security control that includes**

**facial recognition. Which of the following provides the BEST solution**?

A. Bollards

B. Guards

C. Retina scanners

D. Cameras

**58. An organization needs to improve fault tolerance to increase data**

**availability. However, the organization has a limited budget. Which of the**

**following is the BEST choice to meet the organization’s needs?**

A. RAID

B. Backup system

C. Hot and cold aisles

D. UPS

**59. You need to modify the network infrastructure to increase availability**

**of web-based applications for Internet clients. Which of the following**

**choices provides the BEST solution?**

A. Load balancing

B. Proxy server

C. UTM

D. Content inspection

**60. Your backup policy for a database server dictates that the amount of**

**time needed to restore backups should be minimized. Which of the**

**following backup plans would BEST meet this need?**

A. Full backups on Sunday and incremental backups on the other six

days of the week

B. Full backups on Sunday and differential backups on the other six

days of the week

C. Incremental backups on Sunday and differential backups on the

other six days of the week

D. Differential backups on Sunday and incremental backups on the

other six days of the week

**61. After a recent attack causing a data breach, an executive is analyzing**

**the financial losses. She determined that the attack is likely to cost at least**

**$1 million. She wants to ensure that this information is documented for**

**future planning purposes. In which of the following is she MOST likely to**

**document it?**

A. DRP

B.BIA

C. HVAC

D. RTO

**62. An organization is considering an alternate location as part of its**

**continuity of operations plan. It wants to identify a solution that provides**

**the shortest recovery time. Which of the following is the BEST choice?**

A. Cold site

B. Warm site

C. Hot site

D. Off-site backups

**63. You need to identify a method that can be used for data integrity.**

**Which of the following choices will meet your needs?**

A. AES

B. DES

C. RC4

D. SHA

**64. Users in your organization sign their emails with digital signatures.**

**Which of the following provides integrity for these digital signatures?**

A. Hashing

B. Encryption

C. Non-repudiation

D. Private key

**65. Network administrators in your organization need to administer**

**firewalls, security appliances, and other network devices. These devices**

**are protected with strong passwords, and the passwords are stored in a file**

**listing these passwords. Which of the following is the BEST choice to**

**protect this password list?**

A. File encryption

B. Database field encryption

C. Full database encryption

D. Whole disk encryption

**66. An application developer needs to use an encryption protocol to**

**encrypt credit card data within a database used by the application. Which**

**of the following would be the FASTEST, while also providing strong**

**confidentiality?**

A. AES-256

B. DES

C. Blowfish

D. SHA-2

**67. A developer is creating an application that will encrypt and decrypt**

**data on mobile devices. These devices don’t have a lot of processing**

**power. Which of the following cryptographic methods has the LEAST**

**overhead and will work with these mobile devices?**

A. Elliptic curve

B. 3DES

C. PBKDF2

D. Bcrypt

**68. Your organization hosts a web site used only by employees. The web**

**site uses a certificate issued by a private CA and the network downloads a**

**CRL from the CA once a week. However, after a recent compromise,**

**security administrators want to use a real-time alternative to the CRL.**

**Which of the following will BEST meet this need?**

A. DSA

B. HMAC

C. CSR

D. OCSP

**69. You need to request a certificate for a web server. Which of the**

**following would you MOST likely use?**

A. CA

B.CRL

C. CSR

D. OCSP

**70. Your organization recently updated a security policy. It states that**

**duties of network administrators and application developers must be**

**separated. Which of the following is the MOST likely result of**

**implementing this policy?**

A. One group develops program code and the other group deploys

the code.

B. One group develops program code and the other group modifies

the code.

C. One group deploys program code and the other group administers

databases.

D. One group develops databases and the other group modifies

databases.

**71. Your organization wants to prevent damage from malware. Which of**

**the following phases of common incident response procedures is the**

**BEST phase to address this?**

A. Preparation

B. Identification

C. Containment

D. Lessons learned

**72. A forensic expert is preparing to analyze a hard drive. Which of the**

**following should the expert do FIRST?**

A. Capture an image.

B. Identify the order of volatility.

C. Create a chain of custody document.

D. Take a screenshot.

**73. An administrator recently learned of a suspected attack on a Florida based web server from IP address 72.52.206.134 at 01:45:43 GMT.**

**However, after investigating the logs, he doesn’t see any traffic from that**

**IP at that time. Which of the following is the MOST likely reason why the**

**administrator was unable to identify the traffic?**

A. He did not account for time offsets.

B. He did not capture an image.

C. The IP address has expired.

D. The logs were erased when the system was rebooted.

**74. Social engineers have launched several successful phone-based**

**attacks against your organization resulting in several data leaks. Which of**

**the following would be MOST effective at reducing the success of these**

**attacks?**

A. Implement a BYOD policy.

B. Update the AUP.

C. Provide training on data handling.

D. Implement a program to increase security awareness.

**75. Security personnel recently released an online training module**

**advising employees not to share specific personal information on social**

**media web sites that they visit. Which of the following is this advice**

**MOST likely trying to prevent?**

A. Spending time on non-work-related sites

B. Phishing attack

C. Cognitive password attacks

D. Rainbow table attack