**1. Management within your organization has defined a use case to**

**support confidentiality of PII stored in a database. Which of the following**

**solutions will BEST meet this need?**

A. Hashing

B. Digital signature

C. Encryption

D. Smart card

**2. Management has implemented a policy stating that messages sent**

**between upper-level executives must arrive without any changes. The IT**

**department is tasked with implementing technical controls to meet this**

**need. Which security goal does this policy address?**

A. Confidentiality

B. Integrity

C. Availability

D. Authentication

**3. Your organization recently implemented two servers that act as failover**

**devices for each other. Which security goal is your organization pursuing?**

A. Obfuscation

B. Integrity

C. Confidentiality

D. Availability

**4. You are tasked with improving the overall security for a database server.**

**Which of the following is a preventive control that will assist with this goal?**

A. Disabling unnecessary services

B. Identifying the initial baseline configuration

C. Monitoring logs for trends

D. Implementing a backup and restoration plan

**5. An IT department recently had its hardware budget reduced, but the**

**organization still expects them to maintain availability of services. Which**

**of the following choices would BEST help them maintain availability with**

**a reduced budget?**

A. Failover clusters

B. Virtualization

C. Bollards

D. Hashing

**6. You want to test new security controls before deploying them. Which**

**of the following technologies provides the MOST flexibility to meet this**

**goal?**

A. Baselines

B. Hardening techniques

C. Virtualization technologies

D. Patch management programs

**7. You suspect that traffic in your network is being rerouted to an**

**unauthorized router within your network. Which of the following**

**command-line tools would help you narrow down the problem?**

A. ping

B. tracert

C. ipconfig

D. netstat

**8. The First Bank of Springfield has been experiencing widespread**

**fraud recently. Attackers are transferring funds out of customer accounts**

**to other banks. The bank began requiring customers to obtain credentials**

**in person at the bank. However, this hasn’t reduced the number of**

**fraudulent transactions. After reviewing available logs, investigators**

**determined that these fraudulent transactions are conducted with the**

**customer’s actual credentials. Which of the following security controls**

**should be strengthened to reduce these incidents?**

A. Authentication

B. Identification

C. Accounting

D. Authorization

**9. An outside security auditor recently completed an in-depth security**

**audit on your network. One of the issues he reported was related to**

**passwords. Specifically, he found the following passwords used on the**

**network: Pa$$, 1@W2, and G7bT3. Which of the following should be**

**changed to avoid the problem shown with these passwords?**

A. Password complexity

B. Password length

C. Password history

D. Password reuse

**10. When you log on to your online bank account, you are also able to**

**access a partner’s credit card site, check-ordering services, and a mortgage**

**site without entering your credentials again. Which of the following does**

**this describe?**

A. SSO

B. Same sign-on

C. SAML

D. Kerberos

**11. Your network uses an authentication service based on the X.500**

**specification. When encrypted, it uses TLS. Which authentication service**

**is your network using?**

A. SAML

B. Diameter

C. Kerberos

D. LDAP

**12. You’re asked to identify who is accessing a spreadsheet containing**

**employee salary data. Detailed logging is configured correctly on this file.**

**However, you are unable to identify a specific person who is accessing**

**the file. Which of the following is the MOST likely reason?**

A. Shared accounts are not prohibited.

B. Guest accounts are disabled.

C. Permissions for the file were assigned to a group.

D. Account lockout has been enabled.

**13. Interns from a local college frequently work at your company. Some**

**interns work with the database developers, some interns work with the**

**web application developers, and some interns work with both developers.**

**Interns working with the database developers require specific privileges,**

**and interns working with the web application developers require different**

**privileges. Which of the following is the simplest method to meet these**

**requirements?**

A. Use generic accounts.

B. Create user-based privileges.

C. Use group-based privileges.

D. Grant the interns access to the Guest account.

**14. You are configuring a file server used to share files and folders among**

**employees within your organization. However, employees should not be**

**able to access all folders on this server. Which of the following choices is**

**the BEST method to manage security for these folders?**

A. Assign permissions to each user as needed.

B. Wait for users to request permission and then assign the

appropriate permissions.

C. Delegate authority to assign these permissions.

D. Use security groups with appropriate permissions.

**15. The Retirement Castle uses groups for ease of administration and**

**management. They recently hired Jasper as their new accountant. Jasper**

**needs access to all the files and folders used by the Accounting department.**

**Which of the following should the administrator do to give Jasper**

**appropriate access?**

A. Create an account for Jasper and add the account to the Accounting

group.

B. Give Jasper the password for the Guest account.

C. Create an account for Jasper and use rule-based access control

for accounting.

D. Create an account for Jasper and add the account to the

Administrators group.

**16. You need to send several large files containing proprietary data to a**

**business partner. Which of the following is the BEST choice for this task?**

A. FTP

B. SNMPv3

C. SFTP

D. SRTP

**17. Your organization is planning to establish a secure link between one of**

**your mail servers and a business partner’s mail server. The connection will**

**use the Internet. Which protocol is the BEST choice?**

A. TLS

B. SMTP

C. HTTP

D. SSH

**18. Bart is adding a DMZ into his organization’s network. Which of the**

**following is the BEST description of why he would do so?**

A. To increase security for servers accessed from public networks

B. To provide a secure physical location for networking equipment

C. To lure attackers to a fake server or fake network

D. To cache data retrieved from a web server

**19. Your organization wants to prevent employees from accessing file**

**sharing web sites. Which of the following choices will meet this need?**

A. Content inspection

B. Malware inspection

C. URL filter

D. Web application firewall

**20. Your organization hosts several web servers in a web farm. They have**

**recently been attacked, resulting in unacceptable downtime. Management**

**wants to implement a solution that will provide protection for the web**

**farm and include load balancing to improve the overall performance of the**

**web farm. Which of the following will BEST meet this need?**

A. Stateless firewall

B. Stateful firewall

C. Web application firewall

D. Host-based firewall

**21. Management suspects that employees have been sending proprietary**

**data out of the network via email. They want to implement a solution that**

**will detect and block similar incidents in the future. Which of the**

**following is the BEST choice to meet this need?**

A. Mail gateway

B. UTM appliance

C. Forward proxy

D. Reverse proxy

**22. You are tasked with configuring a switch so that it separates VoIP and**

**data traffic. Which of the following provides the BEST solution?**

A. NAC

B. DMZ

C. SRTP

D. VLAN

**23. Your organization hosts an e-commerce business that has become quite**

**Successful recently. It includes a web farm and a database server within the**

**DMZ. IT management is concerned that there isn’t enough staff working**

**around the clock to protect these servers. Which of the following would**

**provide the BEST automated protection for these servers?**

A. NIDS and HIDS

B. NIPS and HIPS

C. SIEM and NIPS

D. SIEM and NIDS

**24. Management is concerned about malicious activity and wants to**

**implement a security control that will detect unusual traffic on the**

**network. Which of the following is the BEST choice to meet this goal?**

A. Network-based firewall

B. Signature-based IDS

C. Anomaly-based IDS

D. Honeynet

**25. Of the following choices, what can you use to divert malicious**

**attacks on your network away from valuable data to worthless, fabricated**

**data?**

A. IPS

B. Proxy server

C. Web application firewall

D. Honeypot

**26. Your organization frequently has guests visiting in various**

**conference rooms throughout the building. These guests need access to the**

**Internet via the wireless network, but should not be able to access internal**

**network resources. Employees need access to both the internal network and**

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

A. NAT

B. DMZ

C. VPN

D. 802.1x

**27. Management asks you if you can modify the wireless network to**

**prevent users from easily discovering it. Which of the following would you**

**modify to meet this goal?**

A. CCMP

B. WPA2 Enterprise

C. SSID broadcast

D. MAC address filter

**28. Marge, a security administrator, is tasked with ensuring that all devices**

**have updated virus definition files before they can access network resources.**

**Which of the following technologies would help her accomplish this goal?**

A. NIDS

B. NAC

C. DLP

D. DMZ

**29. Your organization is hosting a wireless network with an 802.1x server**

**using PEAP. On Thursday, users report they can no longer access the**

**wireless network, but they could access it on the previous day.**

**Administrators verified the network configuration matches the baseline,**

**there aren’t any hardware outages, and the wired network is operational.**

**Which of the following is the MOST likely cause for this problem?**

A. The RADIUS server certificate expired.

B. DNS is providing incorrect host names.

C. DHCP is issuing duplicate IP addresses.

D. MAC filtering is enabled.

**30. Lisa has created an application on her development computer. She**

**wants to test it on a Linux-based computer she commonly uses for testing.**

**However, she wants to ensure it is isolated when she tests it. Which of the**

**following is the BEST solution to meet her needs?**

A. Use chroot.

B. Sideload the application.

C. Use FDE.

D. Use chmod.

**31. Your organization recently purchased some laptops that include a**

**TPM. Which of the following BEST identifies what the TPM provides?**

A. Detection of unauthorized data transfers

B. A hardware root of trust

C. Sandboxing

D. An external security device used to store cryptographic keys

**32. Your organization has recently rented access to computing resources**

**via a cloud. Administrators within your organization apply patches to the**

**operating system. Which of the following choices BEST describes this**

**cloud deployment model?**

A. Community

B. Software as a Service

C. Infrastructure as a Service

D. Hybrid

**33. Homer noticed that several generators within the nuclear power plant**

**have been turning on without user interaction. Security investigators**

**discovered that an unauthorized file was installed, causing these**

**generators to start at timed intervals. Further, they determined this file**

**was installed during a visit by external engineers. What should Homer**

**recommend to mitigate this threat in the future?**

A. Create an internal CA.

B. Implement WPA2 Enterprise.

C. Implement patch management processes.

D. Configure the SCADA within a VLAN.

**34. Management wants to ensure that employees do not print any**

**documents that include customer or employee PII. Which of the following**

**solutions would meet this goal?**

A. HSM

B.TPM

C. VLAN

D. DLP

**35. A tech company recently discovered an attack on its organization,**

**resulting in a significant data breach of customer data. After investigating**

**the attack, they realized it was very sophisticated and likely originated**

**from a foreign country. Which of the following identifies the MOST**

**likely threat actor in this attack?**

A. Hacktivist

B. APT

C. Competitors

D. Insiders

**36. A recent antivirus scan on a server detected a Trojan. A technician**

**removed the Trojan, but a security administrator expressed concern that**

**unauthorized personnel might be able to access data on the server. The**

**security administrator decided to check the server further. Of the**

**following choices, what is the administrator MOST likely looking for on**

**this server?**

A. Backdoor

B. Logic bomb

C. Rootkit

D. Botnet

**37. After Marge turned on her computer, she saw a message indicating**

**that unless she made a payment, her hard drive would be formatted. What**

**does this indicate?**

A. Keylogger

B. Ransomware

C. Backdoor

D. Trojan

**38. An organization’s security policy requires employees to place all**

**discarded paper documents in containers for temporary storage. These**

**papers are later burned in an incinerator. Which of the following attacks**

**are these actions MOST likely trying to prevent?**

A. Shoulder surfing

B. Tailgating

C. Vishing

D. Dumpster diving

**39. Users in your organization have reported receiving a similar email**

**from the same sender. The email included a link, but after recent training**

**on emerging threats, all the users chose not to click the link. Security**

**investigators determined the link was malicious and was designed to**

**download ransomware. Which of the following BEST describes the**

**email?**

A. Phishing

B. Spear phishing

C. Spam

D. Vishing

**40. Your local library is planning to purchase new computers that patrons**

**can use for Internet research. Which of the following are the BEST**

**choices to protect these computers? (Select TWO.)**

A. Mantrap

B. Anti-malware software

C. Cable locks

D. Disk encryption

**41. You are troubleshooting an intermittent connectivity issue with a**

**webserver. After examining the logs, you identify repeated connection**

**attempts from various IP addresses. You realize these connection attempts**

**are overloading the server, preventing it from responding to other**

**connections. Which of the following is MOST likely occurring?**

A. DDoS attack

B. DoS attack

C. Amplification attack

D. Salting attack

**42. You are reviewing security controls and their usefulness. You notice**

**that account lockout policies are in place. Which of the following attacks**

**will these policies thwart? (Select TWO.)**

A. DNS poisoning

B. Replay

C. Brute force

D. Buffer overflow

E. Dictionary

**43. Security analysts recently discovered that users in your organization**

**are inadvertently installing malware on their systems after visiting the**

**comptai.org web site. Users have a legitimate requirement to visit the**

**comptia.org web site. Which of the following is the MOST likely**

**explanation for this activity?**

A. Smurf

B. Typo squatting

C. Fuzzing

D. Replay

**44. An attacker recently attacked a web server hosted by your company.**

**After investigation, security professionals determined that the attacker**

**used a previously unknown application exploit. Which of the following**

**BEST identifies this attack?**

A. Buffer overflow

B. Zero-day attack

C. Man-in-the-browser

D. Session hijacking

**45. While reviewing logs for a web application, a developer notices that**

**it has crashed several times reporting a memory error. Shortly after it**

**crashes, the logs show malicious code that isn’t part of a known**

**application. Which of the following is MOST likely occurring?**

A. Buffer overflow

B. ARP poisoning

C. Privilege escalation

D. Replay

**46. Management at your organization is planning to hire a development**

**firm to create a sophisticated web application. One of their primary goals**

**is to ensure that personnel involved with the project frequently**

**collaborate with each other throughout the project. Which of the**

**following is an appropriate model for this project?**

A. Waterfall

B. SDLC

C. Agile

D. Secure DevOps

**47. Your organization is preparing to deploy a web-based application,**

**which will accept user input. Which of the following will BEST test the**

**reliability of this application to maintain availability and data integrity?**

A. Model verification

B. Input validation

C. Error handling

D. Dynamic analysis

**48. An attacker has launched several successful XSS attacks on a web**

**application within your DMZ. Which of the following are the BEST**

**choices to protect the web server and prevent this attack? (Select TWO.)**

A. Dynamic code analysis

B. Input validation

C. Code obfuscation

D. WAF

E. Normalization

**49. Ziffcorp is developing a new technology that they expect to become a**

**huge success when it’s released. The CIO is concerned about someone**

**stealing their company secrets related to this technology. Which of the**

**following will help the CIO identify potential dangers related to the loss of**

**this technology?**

A. Threat assessment

B. Vulnerability assessment

C. Privacy threshold assessment

D. Privacy impact assessment

**50. You are performing a risk assessment and you need to calculate the**

**average expected loss of an incident. Which of the following value**

**combinations would you MOST likely use?**

A. ALE and ARO

B. ALE and SLE

C. SLE and ARO

D. ARO and ROI

**51. You recently completed a vulnerability scan on your network. It**

**reported that several servers are missing key operating system patches.**

**However, after checking the servers, you’ve verified the servers have**

**these patches installed. Which of the following BEST describes this?**

A. False negative

B. Misconfiguration on servers

C. False positive

D. Non-credentialed scan

**52. You want to identify all the services running on a server in your**

**network. Which of the following tools is the BEST choice to meet this**

**goal?**

A. Penetration test

B. Protocol analyzer

C. Sniffer

D. Port scanner

**53. Lisa needs to identify if a risk exists within a web application and**

**identify potential misconfigurations on the server. However, she should**

**passively test the security controls. Which of the following is the BEST**

**choice to meet her needs?**

A. Perform a penetration test.

B. Perform a port scan.

C. Perform a vulnerability scan.

D. Perform traffic analysis with a sniffer.

**54. A network administrator needs to identify the type of traffic and**

**packet flags used in traffic sent from a specific IP address. Which of the**

**following is the BEST tool to meet this need?**

A. SIEM

B. Netcat

C. Protocol analyzer

D. Vulnerability scan

**55. Lisa has been hired as a penetration tester by your organization to test**

**the security of a web server. She wants to identify the operating system and**

**get some information on services and applications used by the server.**

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

A. SIEM

B. Netcat

C. Tcpdump

D. Gray box test

**56. An organization wants to provide protection against malware attacks.**

**Administrators have installed antivirus software on all computers.**

**Additionally, they implemented a firewall and an IDS on the network.**

**Which of the following BEST identifies this principle?**

A. Implicit deny

B. Layered security

C. Least privilege

D. Flood guard

**57. A security professional needs to identify a physical security control**

**that will identify and authenticate individuals before allowing them to**

**pass, and restrict passage to only a single person at a time. Which of the**

**following should the professional recommend?**

A. Tailgating

B. Smart cards

C. Biometrics

D. Mantrap

**58. Your company’s web site experiences a large number of client**

**requests during certain times of the year. Which of the following could**

**your company add to ensure the web site’s availability during these times?**

A. Fail-open cluster

B. Certificates

C. Web application firewall

D. Load balancing

**59. Which of the following is the LOWEST cost solution for fault**

**tolerance?**

A. Load balancing

B. Round-robin scheduling

C. RAID

D. Warm site

**60. Employees access a secure area by entering a cipher code, but this**

**code does not identify individuals. After a recent security incident,**

**management has decided to implement a key card system that will identify**

**individuals who enter and exit this secure area. However, the installation**

**might take six months or longer. Which of the following choices can the**

**organization install immediately to identify individuals who enter or exit**

**the secure area?**

A. Mantrap

B. Access list

C. CCTV

D. Bollards

**61. An organization has decided to increase the amount of customer data**

**it maintains and use it for targeted sales. The privacy officer has**

**determined that this data is PII. Which type of assessment should be**

**completed to ensure the organization is complying with applicable laws**

**and regulations related to this data?**

A. Privacy impact assessment

B. Privacy threshold assessment

C. Threat assessment

D. Supply chain assessment

**62. A security technician runs an automated script every night designed**

**to detect changes in files. Of the following choices, what are the MOST**

**LIKELY protocols used in this script?**

A. PGP and SHA

B.ECC and HMAC

C. AES and Twofish

D. SHA and HMAC

**63. An application requires users to log on with passwords. The**

**application developers want to store the passwords in such a way that it**

**will thwart rainbow table attacks. Which of the following is the BEST**

**solution?**

A. SHA

B. Blowfish

C. ECC

D. Bcrypt

**64. Which of the following cryptography concepts indicates that**

**ciphertext is significantly different than plaintext after it has been**

**encrypted?**

A. Diffusion

B. Obfuscation

C. Collision

D. Confusion

**65. Your organization is investigating possible methods of sharing**

**encryption keys over a public network. Which of the following is the BEST**

**choice?**

A. CRL

B. PBKDF2

C. Hashing

D. ECDHE

**66. An application developer is working on the cryptographic elements of**

**an application. She needs to implement an encryption algorithm that**

**provides both confidentiality and data authenticity. Which of the following**

**cipher modes supports these goals?**

A. CTM

B.CBC

C. ECB

D. GCM

**67. An organization hosts several web servers in a web farm used for ecommerce. Due to recent attacks, management is concerned that attackers might try to redirect web site traffic, allowing the attackers to impersonate their e-commerce site. Which of the following methods will address this issue?**

A. Stapling

B. Perfect forward secrecy

C. Pinning

D. Key stretching

**68. Users within an organization frequently access public web servers**

**using HTTPS. Management wants to ensure that users can verify that**

**certificates are valid even if the public CAs are temporarily unavailable.**

**Which of the following should be implemented to meet this need?**

A. OCSP

B.CRL

C. Private CA

D. CSR

**69. A security auditor discovered that several employees in the**

**Accounting department can print and sign checks. In her final report, she**

**recommended restricting the number of people who can print checks and**

**the number of people who can sign them. She also recommended that no**

**one should be authorized to print and sign checks. Which security policy**

**does this describe?**

A. Discretionary access control

B. Rule-based access control

C. Separation of duties

D. Job rotation

**70. Your organization includes a software development division within**

**the IT department. One developer writes and maintains applications for**

**the Sales and Marketing departments. A second developer writes and**

**maintains applications for the Payroll department. Once a year, they have**

**to switch roles for at least a month. What is the purpose of this practice?**

A. To enforce a separation of duties policy

B. To enforce a mandatory vacation policy

C. To enforce a job rotation policy

D. To enforce an acceptable use policy

**71. Your organization is considering storage of sensitive data with a**

**cloud provider. Your organization wants to ensure the data is encrypted**

**while at rest and while in transit. Which type of interoperability**

**agreement can your organization use to ensure the data is encrypted while**

**in transit?**

A. SLA

B.BPA

C. MOU

D. ISA

**72. You work as a help-desk professional in a large organization. You**

**have begun to receive an extraordinary number of calls from employees**

**related to malware. Using common incident response procedures, which of**

**the following should be your FIRST response?**

A. Preparation

B. Identification

C. Eradication

D. Recovery

**73. An incident response team is following typical incident response**

**procedures. Which of the following phases is the BEST choice for**

**analyzing an incident with a goal of identifying steps to prevent a**

**reoccurrence of the incident?**

A. Preparation

B. Identification

C. Eradication

D. Lessons learned

**74. You are helping your organization create a security policy for**

**incident response. Which of the following choices is the BEST choice to**

**include when an incident requires confiscation of a physical asset?**

A. Ensure hashes are taken first.

B. Ensure witnesses sign an AUP.

C. Maintain the order of volatility.

D. Keep a record of everyone who took possession of the physical

asset.

**75. Security personnel confiscated a user’s workstation after a security**

**incident. Administrators removed the hard drive for forensic analysis, but**

**left it unattended for several hours before capturing an image. Which of**

**the following could prevent the company from taking the employee to**

**court over this incident?**

A. Witnesses were not identified.

B. A chain of custody was not maintained.

C. An order of volatility was not maintained.

D. A hard drive analysis was not complete.