P- 3 IV

chief information officer (CIO) of a major company intends to increase employee ectivity and productivity by issuing employees mobile devices with access to their erprise email, calendar, and contacts. The solution the CIO intends to use requires PKI that automates the enrollment of mobile device certificates. Which of the following, when implemented and configured securely, will meet the CIO's requirement?

A. OCSP
[✓ B. SCEP]
C. SAML
D. OSI

2. An attacker impersonates a fire marshal and demands access to the datacenter under the threat of a fine. Which of the following reasons make this effective? (Choose two.)

A. Consensus
[✓ B. Authority]
[✓ C. Intimidation]
D. Trust
E. Scarcity

3. In the course of troubleshooting wireless issues from users, a technician discovers that users are connecting to their home SSIDs while at work. The technician scans but detects none of those SSIDs. The technician eventually discovers a rouge access point that spoofs any SSID request. Which of the following allows wireless use while mitigating this type of attack?

[✓ A. Configure the device to verify access point MAC addresses.]
B. Disable automatic connection to known SSIDs.
C. Only connect to trusted wireless networks.
D. Enable MAC filtering on the wireless access point.

4. Which of the following describes the implementation of PAT?

A. Translating the source and destination IPS, but not the source and destination ports
B. A one to one persistent mapping between on private IP and one Public IP
C. Changing the priority of a TCP stream based on the source address
[✓ D. Associating multiple public IP addresses with one private address]

5. Which of the following forms of software testing can best be performed with no knowledge of how a system is internally structured or functions? (Choose Two.)

A. Boundary testing
B. White box
[✓ C. Fuzzing]
[✓ D. Black box]
E. Grey Box

6. A load balancer has the ability to remember which server a particular client is using and always directs that client to the same server. This feature is called:

A. Cookie tracking
B. URL filtering
[✓ C. Session affinity]
D. Behavior monitoring

7. A company has recently begun to provide internal security awareness for employees. Which of the following would be used to demonstrate the effectiveness of the training?

[✓ A. Metrics]
B. Business impact analysis
C. Certificate of completion
D. Policies

8. Users in an organization are experiencing when attempting to access certain websites. The users report that when they type in a legitimate URL, different boxes appear on the screen, making it difficult to access the legitimate sites. Which of the following would best mitigate this issue?

[✓ A. Pop-up blockers]
B. URL filtering
C. Antivirus
D. Anti-spam

9. A company hires a penetration testing team to test its overall security posture. The organization has not disclosed any information to the penetration testing team and has allocated five days for testing. Which of the following types of testing will the penetration testing team have to conduct?

A. Static analysis
B. Gray Box
C. White box
[✓ D. Black box]

10. A web administrator has just implemented a new web server to be placed in production. As part of the company's security plan, any new system must go through a security test before it is placed in production. The security team runs a port scan resulting in the following data:

```
  21 tcp open FTP
  23 tcp open Telnet
  22 tcp open SSH
  25 UDP open smtp
  110 tcp open pop3
  443 tcp open https
```

Which of the following is the BEST recommendation for the web administrator?
A. Implement an IPS
[✓ B. Disable unnecessary services]
C. Disable unused accounts
D. Implement an IDS
E. Wrap TELNET in SSL

11. Which of the following best describes the reason for using hot and cold aisles?
[✓ A. To ensure air exhaust from one aisle doesn't blow into the air intake of the next aisle]
B. To ensure the dewpoint stays low enough that water doesn't condensate on equipment
C. To decrease amount of power wiring that is run to each aisle
D. Too maintain proper humidity in the datacenter across all aisles

12. An organization has an internal PKI that utilizes client certificates on each workstation. When deploying a new wireless network, the security engineer has asked that the new network authenticate clients by utilizes the existing client certificates. Which of the following authentication mechanisms should be utilized to meet this goal?
A. EAP-FAST
B. LEAP
C. PEAP
[✓ D. EAP-TLS]

13. An attacker is attempting to insert malicious code into an installer file that is available on the internet. The attacker is able to gain control of the web server that houses both the installer and the web page which features information about the downloadable file. To implement the attack and delay detection, the attacker should modify both the installer file and the:
A. SSL certificate on the web server
B. The HMAC of the downloadable file available on the website
C. Digital signature on the downloadable file
[✓ D. MD5 hash of the file listed on the website]

14. After receiving the hard drive from detectives, the forensic analyst for a court case used a log to capture corresponding events prior to sending the evidence to lawyers. Which of the following do these actions demonstrate?
[✓ A. Chain of custody]
B. Order if volatility
C. Data analysis
D. Tracking man hours and expenses

15. A group of users from multiple departments are working together on a project and will maintain their digital output in a single location. Which of the following is the BEST method to ensure access is restricted to use by only these users?
A. Mandatory access control
B. Rule-based access
[✓ C. Group based privileges]
D. User assigned privileges

16. Which of the following technologies when applied to android and iOS environments, can an organization use to add security restrictions and encryption to existing mobile applications? (Choose Two)
[✓ A. Mobile device management]

B. Containerization
[✓ C.] Application whitelisting
D. Application wrapping
E. Mobile application store

17. Mobile tablets are used by employees on the sales floor to access customer data. Ann a customer recently reported that another customer was able to access her personal information on the tablet after the employee left the area. Which of the following would BEST prevent these issues from reoccurring?
[✓ A.] Screen Locks
B. Full-device encryption
C. Application control
D. Asset tracking

18. An application developer has coded a new application with a module to examine all user entries for the graphical user interface. The module verifies that user entries match the allowed types for each field and that OS and database commands are rejected before entries are sent for further processing within the application. These are example of:
A. Input validation
[✓ B.] SQL injection
C. Application whitelisting
D. Error handling

19. Ann, a security administrator is hardening the user password policies. She currently has the following in place:

Passwords expire every 60 days
Password length is at least eight characters
Passwords must contain at least one capital letter and one numeric character
Passwords cannot be reused until the password has been changed eight times

She learns that several employees are still using their original password after the 60-day forced change. Which of the following can she implement to BEST mitigate this?
A. Lower the password expiry time to every 30days instead of every 60 days
B. Require that the password contains at least one capital, one numeric, and one special character
C. Change the re-usage time from eight to 16 changes before a password can be repeated
[✓ D.] Create a rule that users can only change their passwords once every two weeks

20. Which of the following BEST describes disk striping with parity?
A. RAID 0
B. RAID 1
C. RAID 2
[✓ D.] RAID 5

21. Which of the following will allow the live state of the virtual machine to be easily reverted after a failed upgrade?
A. Replication
B. Backups
C. Fault tolerance
[✓ D.] Snapshots

22. An organization currently uses FTP for the transfer of large files, due to recent security enhancements, is now required to use a secure method of file transfer and is testing both SFTP and FTPS as alternatives. Which of the following ports should be opened on the firewall in order to test the two alternatives? (Choose Two)
[✓ A.] TCP 22
B. TCP 25
C. TCP 69
D. UDP 161
[✓ E.] TCP 990
F. TCP 3380

23. Which of the following types of malware, attempts to circumvent malware detection by trying to hide its true location on the infected system?
[✓ A.] Armored virus
B. Ransomware
C. Trojan
D. Keylogger

24. An attacker went to a local bank and collected disposed paper for the purpose of collecting data that could be used to steal funds and information from the bank's customers. This is an example of:

A. Impersonation

B. Whaling

[✓ C.] Dumpster diving

D. Hoaxes

25. An employee reports work was being completed on a company owned laptop using a public wireless hot-spot. A pop-up screen appeared and the user closed the pop-up. Seconds later the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?

[✓ A.] Ransomware

B. Rootkit

C. Scareware

D. Spyware

26. A small IT security form has an internal network composed of laptops, servers, and printers. The network has both wired and wireless segments and supports VPN access from remote sites. To protect the network from internal and external threats, including social engineering attacks, the company decides to implement stringent security controls. Which of the following lists is the BEST combination of security controls to implement?

A. Disable SSID broadcast, require full disk encryption on servers, laptop, and personally owned electronic devices, enable MAC filtering on WAPs, require photographic ID to enter the building.

[✓ B.] Enable port security; divide the network into segments for servers, laptops, public and remote users; apply ACLs to all network equipment; enable MAC filtering on WAPs; and require two-factor authentication for network access.

C. Divide the network into segments for servers, laptops, public and remote users; require the use of one time pads for network key exchange and access; enable MAC filtering ACLs on all servers.

D. Enable SSID broadcast on a honeynet; install monitoring software on all corporate equipment' install CCTVs to deter social engineering; enable SE Linux in permissive mode.

27. A security analyst is working on a project team responsible for the integration of an enterprise SSO solution. The SSO solution requires the use of an open standard for the exchange of authentication and authorization across numerous web based applications. Which of the following solutions is most appropriate for the analyst to recommend in this scenario?

[✓ A.] SAML

B. XTACACS

C. RADIUS

D. TACACS+

E. Secure LDAP

28. A thief has stolen mobile device and removed its battery to circumvent GPS location tracking. The device user is a four digit PIN. Which of the following is a mobile device security control that ensures the confidentiality of company data?

A. Remote wiping

B. Mobile Access control

[✓ C.] Full device encryption

D. Inventory control

29. A user has called the help desk to report an enterprise mobile device was stolen. The technician receiving the call accesses the MDM administration portal to identify the device's last known geographic location. The technician determines the device is still communicating with the MDM. After taking note of the last known location, the administrator continues to follow the rest of the checklist. Which of the following identifies a possible next step for the administrator?

A. Remotely encrypt the device

B. Identify the mobile carrier's IP address

C. Reset the device password

[✓ D.] Issue a remote wipe command

30. A risk management team indicated an elevated level of risk due to the location of a corporate datacenter in a region with an unstable political climate. The chief

information officer (CIO) accepts the recommendation to transition the workload to an alternate datacenter in a more stable region. Which of the following forms of risk mitigation has the CIO elected to pursue?

A. Deterrence
B. Transference
[✓ C. Avoidance]
D. Acceptance
E. sharing

31. During a recent audit, the auditors cited the company's current virtual machine infrastructure as a concern. The auditors cited the fact that servers containing sensitive customer information reside on the same physical host as numerous virtual machines that follow less stringent security guild lines. Which of the following would be the best choice to implement to address this audit concern while maintain the current infrastructure?

A. Migrate the individual virtual machines that do not contain sensitive data to separate physical machines
B. Implement full disk encryption on all servers that do not contain sensitive customer data
C. Move the virtual machines that contain the sensitive information to a separate host
[✓ D. Create new VLANs and segment the network according to the level of data sensitivity]

32. A switch is set up to allow only 2 simultaneous MAC addresses per switch port. An administrator is reviewing a log and determines that a switch ort has been deactivated in a conference room after it detected 3 or more MAC addresses on the same port. Which of the following reasons could have caused this port to be disabled?

A. A pc had a NIC replaced and reconnected to the switch
B. An ip telephone has been plugged in
C. A rouge access point was plugged in
[✓ D. An arp attack was launched from a pc on this port]

33. A network administrator was to implement a solution that will allow authorized traffic, deny unauthorized traffic and ensure that appropriate ports are being used for a number of TCP and UDP protocols. Which of the following network controls would meet these requirements?

[✓ A. Stateful firewall]
B. Web security gateway
C. URL filter
D. proxy server
E. web application firewall

34. Client computers login at specified times to check and update antivirus definitions using a dedicated account configured by the administrator. One day the clients are unable to login with the account, but the server still responds to ping requests. The administrator has not made any changed. Which of the following most likely happened?

A. Group policy is blocking the connection attempts
B. The administrator account has been disabled
C. The switch port for the server has died
[✓ D. The password on the account has expired]

35. In performing an authorized penetration test of an organization's system security, a penetration tester collects information pertaining to the application versions that reside on a server. Which of the following is the best way to collect this type of information?

A. Protocol analyzer
[✓ B. Banner grabbing]
C. Port scanning
D. Code review

36. A company is deploying an new video conferencing system to be used by the executive team for board meetings. The security engineer has been asked to choose the strongest available asymmetric cipher to be used for encryption of board papers, and chose the strongest available stream cipher to be configured for video streaming. Which of the following ciphers should be chosen? (Choose two)

[✓ A. RSA]
[✓ B. RC4]
C. 3DES
D. HMAC
E. SJA-256

37. Joe has hired several new security administrators and have been explaining the4 design of the company's network. He has described the position and descriptions of the company's firewalls, IDS sensors, antivirus server, DMZs, and HIPS. Which of the following best describes the incorporation of these elements?
A. Load balancers
[✓ B.] Defense in depth
C. Network segmentation
D. UTM security appliance

38. A security administrator is selecting an MDM solution for an organization, which has strict security requirements for the confidentiality of its data on end user devices. The organization decides to allow BYOD, but requires that users wishing to participate agree to the following specific device configurations; camera disablement, password enforcement, and application whitelisting. The organization must be able to support a device portfolio of differing mobile operating systems. Which of the following represents the MOST relevant technical security criteria for the MDM?
A. Breadth of support for device manufacturers' security configuration APIS
[✓ B.] Ability to extend the enterprise password polices to the chosen MDM
C. Features to support the backup and recovery of the stored corporate data
D. Capability to require the users to accept an AUP prior to device onboarding

39. Employees are reporting that they have been receiving a large number of emails advertising products and services. Links in the email direct the users' browsers to the websites for the items being offered. No reports of increased virus activity have been observed. A security administrator suspects that the users are the targets of:
A. A watering hole attack
B. Spear phishing
C. A spoofing attack
[✓ D.] A spam campaign

40. An employee finds a USB drive in the employee lunch room and plugs the drive into a shared workstation to determine who owns the drive. When the drive is inserted, a command prompt opens and a script begins to run. The employee notifies a technician, who determines that data on a server have been compromised. This is an example of:
A. Device removal
B. Data disclosure
[✓ C.] Incident identification
D. Mitigation steps

41. A chief information officer (CIO) is concerned about PII contained in the organization's various data warehouse platforms. Since not all of the PII transferred to the organization is required for proper operation of the data warehouse application, the CIO requests the in needed PII data be parsed and securely discarded. Which of the following controls would be MOST appropriate in this scenario?
A. Execution of PII data identification assessments
B. Implementation of data sanitization routines
C. Encryption of data-at-rest
D. Introduction of education programs and awareness training
[✓ E.] Creation of policies and procedures

42. The security administrator receives a service ticket saying a host based firewall is interfering with the operation of a new application that is being tested in delevopment. The administrator asks for clarification on which ports need to be open. The software vendor replies that it could use up to 20 ports and many customers have disabled the host based firewall. After examining the system the administrator sees several ports that are open for database and application servers that only used locally. The vendor continues to recommend disabling the host based firewall. Which of the following is the best course of action for the administrator to take?
A. Allow ports used by the application through the network firewall
B. Allow ports used externally through the host firewall
C. Follow the vendor recommendations and disable the host firewall
[✓ D.] Allow ports used locally through the host firewall

43. A corporate wireless guest network uses an open SSID with a captive portal to authenticate guest users. Guests can obtain their portal password at the service desk. A security consultant alerts the administrator that the captive portal is easily bypassed, as long as one other wireless guest user is on the network. Which of the following attacks did the security consultant use?

A. ARP poisoning
B. DNS cache poisoning
[✓ C.] MAC spoofing
D. Rouge DHCP server

44. A company requires that all wireless communication be compliant with the Advanced encryption standard. The current wireless infrastructure implements WEP + TKIP. Which of the following wireless protocols should be implemented?
A. CCMP
~~B.~~ 802.1x
C. 802.3
[✓ D.] WPA2
E. AES

45. A security analyst, while doing a security scan using packet capture security tools, noticed large volumes of data images of company products being exfiltrated to foreign IP addresses. Which of the following is the FIRST step in responding to scan results?
[✓ A.] Incident identification
B. Implement mitigation
C. Chain of custody
D. Capture system image

46. An administrator deploys a WPA2 Enterprise wireless network with EAP-PEAP-MSCHAPv2. The deployment is successful and company laptops are able to connect automatically with no user intervention. A year later, the company begins to deploy phones with wireless capabilities. Users report that they are receiving a warning when they attempt to connect to the wireless network from their phones. Which of the following is the MOST likely cause of the warning message?
A. Mutual authentication on the phone is not compatible with the wireless network
[✓ B.] The phones do not support WPA2 Enterprise wireless networks
C. User certificates were not deployed to the phones
D. The phones' built in web browser is not compatible with the wireless network
E. Self-signed certificates were used on the RADIUS servers

47. An attacker has gained access to the company's web server by using the administrator's credentials. The attacker then begins to work on compromising the sensitive data on other servers. Which off the following BEST describes this type of attack?
A. Privilege escalation A & B?
[✓ B.] Client-side attack
C. Man-in-the-middle
D. Transitive access

48. A security technician is concerned there4 is not enough security staff available the web servers and database server located in the DMZ around the clock. Which of the following technologies, when deployed, would provide the BEST round the clock automated protection?
A. HIPS & SIEM
B. NIPS & HIDS
C. HIDS& SIEM
[✓ D.] NIPS&HIPS

49. Which of the following best describes the objectives of succession planning?
A. To identify and document the successive order in which critical systems should be reinstated following a disaster situation
[✓ B.] To ensure that a personnel management plan is in place to ensure continued operation of critical processes during an incident
C. To determine the appropriate order in which contract internal resources, third party suppliers and external customers during a disaster response
D. To document the order that systems should be reinstated at the primary site following a failover operation at a backup site.

50. A system administrator wants to use open source software but is worried about the source code being comprised. As a part of the download and installation process, the administrator should verify the integrity of the software by:
A. Creating a digital signature of the file before installation
B. Using a secure protocol like HTTPS to download the file
[✓ C.] Checking the has against an official mirror that contains the same file

D. Encryption any connections the software makes

51. The chief security officer (CSO) has reported a rise in data loss but no break-ins have occurred. By doing which of the following would the CSO MOST likely to reduce the number of incidents?
A. Implement protected distribution
B. Employ additional firewalls
[✓ C.] Conduct security awareness training
D. Install perimeter barricades

52. In an effort to test the effectiveness of an organization's security awareness training, a penetrator tester crafted an email and sent it to all of the employees to see how many of them clicked on the enclosed links. Which of the following is being tested?
~~A.~~ How many employees are susceptible to a SPAM attack
B. How many employees are susceptible to a cross-site scripting attack
[✓ C.] How many employees are susceptible to a phishing attack
D. How many employees are susceptible to a vishing attack

53. Devices on the SCADA network communicate exclusively at Layer 2. Which of the following should be used to prevent unauthorized systems using ARP-based attacks to compromise the SCADA network?
A. Application firewall L7
B. IPSec - L3
C. Hardware encryption. L1
[✓ D] VLANS - L2

54. When information is shared between two separate organizations, which of the following documents would describe the sensitivity as well as the type and flow of the information?
A. SLA
[✓ B.] ISA
C. BPA
D. MOA

55. Joe noticed that there is a larger than normal account of network on the printer VLAN of his organization, causing users to have to wait a long time for a print job. Upon investigation Joe discovers that printers were ordered and added to the network without his knowledge. Which of the following will reduce the risk of this occurring again in the future?
A. Log analysis
B. Loop protection
C. Access control list
[✓ D.] Rule-based management

56. Jo an employee reports to the security manager that several files in a research and development folder that only JOE has access to have been improperly modified. The modified data on the files in recent and the modified by account is Joe's. The permissions on the folder have not been changed, and there is no evidence of malware on the server hosting the folder or on Joe's workstation. Several failed login attempts to Joe's account were discovered in the security log of the LDAP server. Given this scenario, which of the following should the security manager implement to prevent this in the future?
A. Generic account prohibition
[✓ B)] Account lockout
C. Password complexity
D. User access reviews

57. A user contacts the help desk after being unable to log in to a corporate website. The user can log into the site from another computer in the next office, but not from the PC. The user's PC was able to connect earlier in the day. The help desk has user restart the NTP Network Time Protocol service. Afterwards the user is able to log into the website. The MOST likely reason for the initial failure was that the website was configured to use which of the following authentication mechanisms?
A. Secure LDAP
B. RADIUS
C. NTLMv2
[✓ D.] Kerberos

58. A security analyst has been investigating an incident involving the corporate website. Upon investigation, it has been determined that users visiting the corporate website would be automatically redirected to a, malicious site. Further investigation on the corporate website has revealed that the home page on the corporate website has been altered to include an unauthorized item. Which of the following would explain why users are being redirected to the malicious site?

[✓ A.] DNS poisoning
~~B.~~ XSS
C. Iframe
D. Session hijacking

59. A news and weather toolbar was accidently installed into a web browser. The toolbar tracks users' online activities and sends them to a central logging server. Which of the following attacks took place?

A. Man-in-the-browser
B. Flash cookies
C. Session hijacking
D. Remote code execution
[✓ E.] Malicious add-on

60. A project manager is working with an architectural firm that focuses on physical security. The project manager would like to provide requirements that support the primary goal of safely. Based on the project manager's desires, which of the following controls would the BEST to incorporate into the facility design?

A. Biometrics
[✓ B.] Escape routers
C. Reinforcements
D. Access controls

61. While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security controls?

A. MAC spoofing
B. Pharming
C. Xmas attack
[✓ D.] ARP poisoning

62. An administrator wants to configure a switch port so that it separates voice and data traffic. Which of the following MUST be configured on the switch port to enforce separation of traffic?

A. DMZ
[✓ B.] VLAN
C. Subnetting
D. NAC

63. A company must send sensitive data over a non-secure network via web services. The company suspects that competitors are actively trying to intercept all transmissions. Some of the information may be valuable to competitors, even years after it has been sent. Which of the following will help mitigate the risk in the scenario?

[✓ A.] Digitally sign the data before transmission
B. Choose steam ciphers over block ciphers
[✓ C.] Use algorithms that allow for PFS   Perfect forward Secrecy
D. Enable TLS instead of SSL
E. Use a third party for key escrow

64. When implementing a mobile security strategy for an organization which of the following is the MOST influential concern that contributes to that organization's ability to extend enterprise policies to mobile devices?

A. Support for mobile OS
B. Support of mobile apps
C. Availability of mobile browsers
[✓ D.] Key management for mobile devices

65. Software developers at a company routinely make changes to production systems they maintain based on code deliveries that are only peer reviewed and are not rigorously tested by the test engineering group. These changes frequently result in a loss of service. Which of the following risk migration controls or strategies should be implemented to prevent these ad hoc changes from occurring in the future?

A. Threat modeling

B. User rights reviews
C. Change management
[✓ D.] Trust modeling

66. A system administrator runs a network inventory scan every Friday at 10:00 am to track the progress of a large organization's operating system upgrade of all laptops. The system administrator discovers that some laptops are now only being reported as IP addresses. Which of the following options is MOST likely the cause of this issue?
A. HIDS
B. Host-based firewalls rules
C. All the laptops are currently turned off
[✓ D.] DNS outage

67. A security administrator working for a law enforcement organization is asked to secure a computer system at the scene of a crime for transport to the law enforcement forensic facility. In order to capture as mush evidence as possible, the computer system has been left running. The security administrator begins information by image which of the following system components FIRST?
A. NVRAM
[✓ B.] RAM
C. TPM
D. SSD

68. A new employee has been hired to perform system administration duties across a large enterprise comprised of multiple separate security domains. Each remote location implements a separate security domain. The new employee has successfully responded to and fixed computer issues for the main office. When the new employee tries to perform work on remote computers, the following messages appears. You need permission to perform this action. Which of the following can be implemented to provide system administrators with the ability to perform administrative tasks on remote computers using their uniquely assigned account?
[✓ A.] Implement transitive trust across security domains
B. Enable the trusted OS feature across all enterprise computers
C. Install and configure the appropriate CA certificate on all domain controllers
D. Verify that system administrators are in the domain administrator group in the main office

69. Which of the following metrics is important for measuring the extent of data required during backup and recovery?
A. MOU
B. ARO
[✓ C.] ALE
D. RPO

70. A project manager is evaluating proposals for a cloud commuting project. The project manager is particularly concerned about logical security controls in place at the service provider's facility. Which of the following sections of the proposal would be MOST important to review, given the project manager's concerns?
A. CCTV monitoring
B. Perimeter security lighting system
[✓ C.] Biometric access system
D. Environmental system configuration

71. A security administrator would like to ensure that some members of the building's maintenance staff are only allowed access to thefacility during weekend hours. Access to the facility is controlled by badge swipe and a man trap. Which of the following options will BEST accomplish this goal?
A. CCTV
B. Security Guard
[✓ C.] Time of day restrictions
D. Job rotation

72. A security manager received reports of several laptops containing confidential data stolen out of a lab environment. The lab is not a high security area and is secured with physical key locks. The security manager has no information to provide investigators related to who may have stolen the laptops. Which of the following should the security manager implement to improve legal and criminal investigations in the future?
A. Motion sensors

B. Mobile device management
[✓ C. CCTV]
D. Cable locks
E. Full-disk encryption

73. During a Linux security audit at a local college, it was noted that members of the dean's group were able to modify employee records in addition to modifying student records, resulting in an audit exception. The college security policy states that the dean's group should only have the ability to modify student records. Assuming that the user and group ownerships are in place, which of the following sets of permissions should have been assigned to the directories containing the employee records?
A. R-x---rwx
B. Rwxr wxrwx
[✓ C. Rwx----wx]
[✓ D. Rwxrwxr--]

74. An employee reports work was being completed on a company-owned laptop using a public wireless hot-spot. A pop-up screen appeared, and the user closed the pop-up. Seconds later, the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?
[✓ A. Ransomware]
B. Rootkit
C. Scareware
D. Spyware

75. Which of the following can be mitigated with proper secure coding techniques?
A. Input validation
B. Error handling
C. Header manipulation
[✓ D. Cross-site scripting]

76. Which of the following attacks initiates a connection by sending specially crafted packets in which multiple TCP flags are set to 1?
A. Replay
B. Smurf
[✓ C. Xmas]
D. Fraggle

77. A Company transfers millions of files a day between their servers. A programmer for the company has created a program that indexes and verifies the integrity of each file as it is replicated between servers. The programmer would like to use the fastest algorithm to ensure integrity. Which of the following should the programmer use?
A. SHA1
B. RIPEMD
C. DSA
[✓ D. MD5]

78. A system administrator is conducting baseline audit and determines that a web server is missing several critical updates. Which of the following actions should the administrator perform first to the issue?
[✓ A. Open a service ticket according to the patch management plan]
B. Disconnect the network interface and use the administrative management console to perform the updates
C. Perform a backup of the server and install the require patches
D. Disable the services for the web server but leave the server alone pending patch updates

79. The IT department has been tasked with reducing the risk of sensitive information being shared with unauthorized entities from computers it is saved on, without impeding the ability of the employees to access the internet. Implementing which of the following would be the best way to accomplish this objective?
A. Host-based firewalls
[✓ B. DLP]
C. URL filtering
D. Pop-up blockers

80. A server crashes at 6 pm. Senior management has determined that data must be restored within two hours of a server crash. Additionally, a loss of more than one hour

worth of data is detrimental to the company's financial well-being. Which of the following is the RTO?

A. 7pm
[✓ B.] 8pm
C. 9pm
D. 10pm

81. To mitigate the risk of intrusion, an IT Manager is concerned with using secure versions of protocols and services whenever possible. In addition, the security technician is required to monitor the types of traffic being generated. Which of the following tools is the technician MOST likely to use?

A. Port scanner
[✓ B.] Network analyzer
C. IPS
D. Audit Logs

82. An administrator is implementing a new management system for the machinery on the company's production line. One requirement is that the system only be accessible while within the production facility. Which of the following will be the MOST effective solution in limiting access based on this requirement?

A. Access control list
B. Firewall policy
[✓ C.] Air Gap
D. MAC filter

83. A risk assessment team is concerned about hosting data with a cloud service provider (CSP) which of the following findings would justify this concern?

A. The CPS utilizes encryption for data at rest and in motion
[✓ B.] The CSP takes into account multinational privacy concerns
C. The financial review indicates the company is a startup
D. SLA state service tickets will be resolved in less than 15 minutes

84. A company wishes to prevent unauthorized employee access to the data center. Which of the following is the MOST secure way to meet this goal?

A. Use Motion detectors to signal security whenever anyone entered the center
B. Mount CCTV cameras inside the center to monitor people as they enter
[✓ C.] Install mantraps at every entrance to the data center in conjunction with their badges
D. Place biometric readers at the entrances to verify employees' identity

85. A company hosts a web server that requires entropy in encryption initialization and authentication. To meet this goal, the company would like to select a block cipher mode of operation that allows an arbitrary length IV and supports authenticated encryption. Which of the following would meet these objectives?

A. CFB
[✓ B.] GCM
C. ECB
D. CBC

86. A chief information security officer (CISO) is providing a presentation to a group of network engineers. In the presentation, the CISO presents information regarding exploit kits. Which of the following might the CISO present?

[✓ A.] Exploit kits are tools capable of taking advantage of multiple CVEs
B. Exploit kits are vulnerability scanners used by penetration testers
C. Exploit kits are WIFI scanning tools that can find new honeypots
D. Exploit kits are a new type of malware that allow attackers to control their computers

87. During a company-wide initiative to harden network security, it is discovered that end users who have laptops cannot be removed from the local administrator group. Which of the following could be used to help mitigate the risk of these machines becoming compromised?

~~A.~~ Security log auditing
[✓ B.] Firewalls
C. HIPS
D. IDS

88. An administrator receives a security alert that appears to be from one of the company's vendors. The email contains information and instructions for patching a serious flaw that has not been publicly announced. Which of the following can an employee use to validate the authenticity if the email?

A. Hashing algorithm
B. Ephemeral Key
C. SSL certificate chain
D. Private key
[✓ E.] Digital signature

89. A project team is developing requirements of the new version of a web application used by internal and external users. The application already features username and password requirements for login, but the organization is required to implement multifactor authentication to meet regulatory requirements. Which of the following would be added requirements will satisfy the regulatory requirement? (Choose three.)
[✓ A.] Digital certificate
B. Personalized URL
C. Identity verification questions
[✓ D.] Keystroke dynamics
[✓ E.] Tokenized mobile device
F. Time-of-day restrictions
G. Increased password complexity
H. Rule-based access control

90. A bank is planning to implement a third factor to protect customer ATM transactions. Which of the following could the bank implement?
A. SMS
B. Fingerprint
[✓ C.] Chip and Pin
D. OTP

91. Which of the following internal security controls is aimed at preventing two system administrators from completing the same tasks?
A. Least privilege
[✓ B.] Separation of Duties
C. Mandatory Vacation
D. Security Policy

92. An administrator performs a risk calculation to determine if additional availability controls need to be in place. The administrator estimates that a server fails and needs to be replaced once every 2 years at a cost of $8,000. Which of the following represents the factors that the administrator would use to facilitate this calculation?
A. ARO= 0.5; SLE= $4,000; ALE= $2,000
[✓ B.] ARO=0.5; SLE=$8,000; ALE=$4,000 Annual rate of occurrence
C. ARO=0.5; SLE= $4,000; ALE=$8,000
D. ARO=2; SLE= $4,000; ALE=$8,000
E. ARO=2; SLE= $8,000; ALE= $16,000

93. A security administrator needs to implement a technology that creates a secure key exchange. Neither party involved in the key exchange will have pre-existing knowledge of one another. Which of the following technologies would allow for this?
A. Blowfish
B. NTLM
[✓ C.] Diffie-Hellman
D. CHAP

94. A technician has been assigned a service request to investigate a potential vulnerability in the organization's extranet platform. Once the technician performs initial investigative measures, it is determined that the potential vulnerability was a false-alarm. Which of the following actions should the technician take in regards to the findings?
A. Write up the findings and disable the vulnerability rule in future vulnerability scans
B. Refer the issue to the server administrator for resolution
C. Mark the finding as a false-negative and close the service request
[✓ D.] Document the results and report the findings according to the incident response plan

95. A security administrator is using a software program to test the security of a wireless access point. After running the program for a few hours, the access point sends the wireless secret key back to the software program. Which of the following attacks is this an example of?
A. WPS
B. IV

[✓ C.] Deauth
D. Replay

96. A user, Ann, has been issued a smart card and is having problems opening old encrypted email. Ann published her certificates to the local windows store and to the global address list. Which of the following would still need to be performed?
[✓ A.] Setup the email security with her new certificates
B. Recover her old private certificate
C. Reinstall her previous public certificate
D. Verify the email address is associated with her certificate

97. Which of the following is a best practice when setting up a client to use the LDAPS protocol with a server?
A. The client should follow LDAP referrals to other secure servers on the network
[✓ B.] The client should trust the CA that signed the server's certificate
C. The client should present a self-signed certificate to the server
D. The client should have access to port 389 on the server

98. A network manager needs a cost-effective solution to allow for the restoration of information with a RPO of 24 hours. The disaster recovery plan also requires that backups occur within a restricted timeframe during the week and be take offsite weekly. Which of the following should the manager choose to BEST address these requirements?
[✓ A.] Daily incremental backup to tape
B. Disk-to-disk hourly server snapshots
C. Replication of the environment at a hot site
D. Daily differential backup to tape
E. Daily full backup to tape

99. Given the following set of firewall rules:

```
  From the inside to outside allow source any destination any port any
  From inside to dmz allow source any destination any port tcp-80
  From inside to dmz allow source any destination any port tcp-443
```

Which of the following would prevent FTP traffic from reaching a server in the DMZ from the inside network?
[✓ A.] Implicit deny
B. Policy routing
C. Port forwarding
D. Forwarding proxy

100. During a routine configuration audit, a systems administrator determines that a former employee placed an executable on an application server. Once the system was isolated and diagnosed, it was determined that the executable was programmed to establish a connection to a malicious command and control server. Which of the following forms of malware is best described in the scenario?
A. Logic bomb
[✓ B.] Rootkit
C. Back door
D. Ransomware