D - 1N

1. A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?
[✓ A.] It can protect multiple domains
B. It provides extended site validation
C. It does not require a trusted certificate authority
D. It protects unlimited subdomains

2. After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition. Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Choose two.)
A. Monitor VPN client access
B. Reduce failed login out settings
[✓ C.] Develop and implement updated access control policies
D. Review and address invalid login attempts
E. Increase password complexity requirements
[✓ F.] Assess and eliminate inactive accounts

3. A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle. Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?
A. Architecture review
B. Risk assessment
C. Protocol analysis
[✓ D.] Code review

4. A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts. Which of the following subnets would BEST meet the requirements?
A. 192.168.0.16 255.25.255.248
[✓ B.] 192.168.0.16/28
C. 192.168.1.50 255.255.25.240
D. 192.168.2.32/27

5. A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops. These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network. Which of the following should be implemented in order to meet the security policy requirements?
A. Virtual desktop infrastructure (IDI)
B. WS-security and geo-fencing
C. A hardware security module (HSM)
D. RFID tagging system
[✓ E.] MDM software
F. Security Requirements Traceability Matrix (SRTM)

6. The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN. Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?
A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
B. Create a user training program to identify the use of email and perform regular audits to ensure compliance
[✓ C.] Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

7. A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network. Which of the following security measures did the technician MOST likely implement to cause this

Scenario?

[✓ A.] Deactivation of SSID broadcast
B. Reduction of WAP signal output power
C. Activation of 802.1X with RADIUS
D. Implementation of MAC filtering
E. Beacon interval was decreased

8. A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production. Which of the following would the deficiencies?

A. Mandatory access controls
B. Disable remote login
[✓ C.] Host hardening
D. Disabling services

9. Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field. Which of the following has the application programmer failed to implement?

A. Revision control system
B. Client side exception handling
[✓ C.] Server side validation
D. Server hardening

10. An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware the attacker is provided with access to the infected machine. Which of the following is being described?

[✓ A.] Zero-day exploit
B. Remote code execution
C. Session hijacking
D. Command injection

A

11. A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine. Which of the following can be implemented to reduce the likelihood of this attack going undetected?

[✓ A.] Password complexity rules
[✓ B.] Continuous monitoring

Ans given: B

C. User access reviews
D. Account lockout policies

12. A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening. In order to implement a true separation of duties approach the bank could:

[✓ A.] Require the use of two different passwords held by two different individuals to open an account
B. Administer account creation on a role based access control approach
C. Require all new accounts to be handled by someone else other than a teller since they have different duties
D. Administer account creation on a rule based access control approach

13. A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day. Which of the following could the security administrator implement to reduce the risk associated with the finding?

A. Implement a clean desk policy
B. Security training to prevent shoulder surfing
[✓ C.] Enable group policy based screensaver timeouts

D. Install privacy screens on monitors

14. Company policy requires the use if passphrases instead if passwords. Which of the following technical controls MUST be in place in order to promote the use of passphrases?
A. Reuse
B
[✓ B. Length]
C. History
D. Complexity

15. During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could best prevent this from occurring again?
A. Credential management
B. Group policy management
C. Acceptable use policy
[✓ D. Account expiration policy]

? 16. Which of the following should identify critical systems and components?
A. MOU
B. BPA
C. ITCP business Continuity Planning
[✓ D. BCP]

17. Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?
[✓ A. Logic bomb]
B. Trojan
C. Scareware
D. Ransomware

18. A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks?
A. SQL injection
B. Header manipulation
[✓ C. Cross-site scripting]
D. Flash cookie exploitation

19. Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures. Which of the following should be implemented to this issue?
A. Decrease the room temperature
[✓ B. Increase humidity in the room]
C. Utilize better hot/cold aisle configurations
D. Implement EMI shielding

20. A portable data storage device has been determined to have malicious firmware. Which of the following is the BEST course of action to ensure data confidentiality?
A. Format the device
B. Re-image the device
[✓ C. Perform virus scan in the device]
D. Physically destroy the device

21. A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable. Which of the following MUST be implemented to support this requirement?
A. CSR
B. OCSP
[✓ C. CRL] Certificate Revocation List
D. SSH

22. A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients. Which of the following is being used?
[✓ A. Gray box vulnerability testing]
B. Passive scan

C. Credentialed scan

D. Bypassing security controls

23. The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws. Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

A. Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers

B. Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data intransit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location

[✓ C.] Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations

D. Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

24. While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does notappear to be within the bounds of the organizations Acceptable Use Policy. Which of the following tool or technology would work BEST for obtaining more information on this traffic?

A. Firewall logs

[✓ B.] IDS logs

C. Increased spam filtering

D. Protocol analyzer

25. A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the BEST way to accomplish this?

[✓ A.] Enforce authentication for network devices

B. Configure the phones on one VLAN, and computers on another

C. Enable and configure port channels

D. Make users sign an Acceptable use Agreement

26. An administrator has concerns regarding the traveling sales team who works primarily from smart phones. Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

[✓ A.] Enable screensaver locks when the phones are not in use to prevent unauthorized access

~~B.~~ Configure the smart phones so that the stored data can be destroyed from a centralized location

C. Configure the smart phones so that all data is saved to removable media and kept separate from the device

D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered

27. A user of the wireless network is unable to gain access to the network. The symptoms are:

Unable to connect to both internal and Internet resources
The wireless icon shows connectivity but has no network access
The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.

Which of the following is the MOST likely cause of the connectivity issues?

[✓ A.] The wireless signal is not strong enough

B. A remote DDoS attack against the RADIUS server is taking place

C. The user's laptop only supports WPA and WEP

D. The DHCP scope is full

E. The dynamic encryption key did not update while the user was offline

28. A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to

provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls. Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Choose Three)

A. Password complexity policies
B. Hardware tokens
C. Biometric systems
[✓ D.] Role-based permissions
E. One time passwords
[✓ F.] Separation of duties
G. Multifactor authentication
H. Single sign-on
[✓ I.] Lease privilege

29. A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot reenable the setting without the knowledge of the user. Which of the following mobile device capabilities should the user disable to achieve the stated goal?

A. Device access control
B. Location based services
C. Application control
[✓ D.] GEO-Tagging

30. A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile date first. Which of the following is the order in which Joe should collect the data?

~~A.~~ CPU cache, paging/swap files, RAM, remote logging data
B. RAM, CPU cache. Remote logging data, paging/swap files
C. Paging/swap files, CPU cache, RAM, remote logging data
[✓ D.] CPU cache, RAM, paging/swap files, remote logging data

31. An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/ administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP. Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

A. Use a honeypot
[✓ B.] Disable unnecessary services
C. Implement transport layer security
D. Increase application event logging

32. A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another. Which of the following should the security administrator do to rectify this issue?

A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
[✓ B.] Recommend classifying each application into like security groups and segmenting the groups from one another
C. Recommend segmenting each application, as it is the most secure approach
D. Recommend that only applications with minimal security features should be segmented to protect them

33. A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code. Which of the following assessment techniques is BEST described in the analyst's report?

A. Architecture evaluation
B. Baseline reporting
C. Whitebox testing
[✓ D.] Peer review

34. An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for

identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are. The controls used by the receptionist are in place to prevent which of the following types of attacks?
A. Tailgating
B. Shoulder surfing
[✓ C. Impersonation]
D. Hoax

35. A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resources. There cannot be a possibility of any equipment being damaged in the test. Which of the following has the administrator been tasked to perform?
A. Risk transference
B. Penetration test
C. Threat assessment
[✓ D. Vulnerability assessment]

36. A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshootingprocess, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on thelocal machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?
A. Transitive access
B. Spoofing
[✓ C. Man-in-the-middle]
D. Replay

37. Which of the following use the SSH protocol?
A. Stelnet
[✓ B. SCP]
C. SNMP
D. FTPS SSL/TLS
E. SSL
[✓ F. SFTP]

38. A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?
A. Utilizing a single question for password recovery
[✓ B. Sending a PIN to a smartphone through text message]
C. Utilizing CAPTCHA to avoid brute force attacks
D. Use a different e-mail address to recover password

39. A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability. In order to prevent similar situations in the future, the company should improve which of the following?
[✓ A. Change management procedures]
B. Job rotation policies
C. Incident response management
D. Least privilege access controls

40. A computer on a company network was infected with a zero-day exploit after an employee accidentally opened an email thatcontained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidentallyopened it. Which of the following should be done to prevent this scenario from occurring again in the future?
A. Install host-based firewalls on all computers that have an email client installed
B. Set the email program default to open messages in plain text
[✓ C. Install end-point protection on all computers that access web email]
D. Create new email spam filters to delete all messages from that sender

41. A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage. Which of the following should be implemented?
A. Recovery agent

B. Ocsp
[✓ C.] Crl
D. Key escrow

42. An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection. Which of the following AES modes of operation would meet this integrity-only requirement?
[✓ A.] HMAC
B. PCBC
C. CBC
D. GCM
E. CFB

No Right Answer

43. The chief security officer (CSO) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs. Which of the following is the best solution for the network administrator to secure each internal website?
[✓ A.] Use certificates signed by the company CA
B. Use a signing certificate as a wild card certificate
C. Use certificates signed by a public ca
D. Use a self-signed certificate on each internal server

44. A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base. Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?
A. Peer review
B. Component testing
[✓ C.] Penetration testing
D. Vulnerability testing

45. Which of the following encrypts data a single bit at a time?
[✓ A.] Stream cipher
B. Steganography
C. 3DES
D. Hashing

46. A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access. Which of the following would be the BEST course of action?
A. Modify all the shared files with read only permissions for the intern.
[✓ B.] Create a new group that has only read permissions for the files.
C. Remove all permissions for the shared files.
D. Add the intern to the "Purchasing" group.

47. A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected. To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?
A. MAC filtering
B. Virtualization
[✓ C.] OS hardening
D. Application white-listing

48. Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work?
A. Taking pictures of proprietary information and equipment in restricted areas.
B. Installing soft token software to connect to the company's wireless network.
C. Company cannot automate patch management on personally-owned devices.
[✓ D.] Increases the attack surface by having more target devices on the company's campus

Ans given. A

49. Which of the following is the summary of loss for a given year?
A. MTBF
[✓ B.] ALE
C. SLA
D. ARO

50. A Security Officer on a military base needs to encrypt several smart phones that will be going into the field. Which of the following encryption solutions should be deployed in this situation?
A. Elliptic curve
B. One-time pad
C. 3DES
[✓ D.] AES-256

51. An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week. Which of the following would be the BEST method of updating this application?
[✓ A.] Configure testing and automate patch management for the application.
B. Configure security control testing for the application.
C. Manually apply updates for the application when they are released.
D. Configure a sandbox for testing patches before the scheduled monthly update.

52. A technician must configure a firewall to block external DNS traffic from entering a network. Which of the following ports should they block on the firewall?
[✓ A.] 53
B. 110
C. 143
D. 443

53. A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols. Which of the following summarizes the BEST response to the programmer's proposal?
A. The newly developed protocol will only be as secure as the underlying cryptographic algorithms used.
[✓ B.] New protocols often introduce unexpected vulnerabilities, even when developed with otherwise secure and tested algorithm libraries.
C. A programmer should have specialized training in protocol development before attempting to design a new encryption protocol.
D. The obscurity value of unproven protocols against attacks often outweighs the potential for introducing new vulnerabilities.

54. The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device. Which of the following categories BEST describes what she is looking for?
A. ALE
B. MTTR
C. MTBF
[✓ D.] MTTF

55. A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet. Which of the following should be used in the code? (Choose two.)
A. Escrowed keys
B. SSL symmetric encryption key
[✓ C.] Software code private key
D. Remote server public key
[✓ E.] OCSP

56. XYZ Company has a database containing personally identifiable information for all its customers. Which of the following options would BEST ensure employees are only viewing information associated to the customers they support?
A. Auditing
[✓ B.] Access Control
C. Encryption
D. Data ownership

57. A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange

white markings in different areas of the parking lot. The person is attempting which of the following types of attacks?

A. Jamming

[✓ B.] War chalking

C. Packet sniffing

D. Near field communication

58. Joe, the security administrator, sees this in a vulnerability scan report:
"The server 10.1.2.232 is running Apache 2.2.20 which may be vulnerable to a mod_cgi exploit."

Joe verifies that the mod_cgi module is not enabled on 10.1.2.232. This message is an example of:

A. a threat.

[✓ B.] a risk.

Answer given D

C. a false negative.

[✓ D.] a false positive.

59. A system administrator is configuring a site-to-site VPN tunnel. Which of the following should be configured on the VPN concentrator during the IKE phase?

Internet Key Exchange

A. RIPEMD

B. ECDHE

[✓ C.] Diffie-Hellman

D. HTTPS

60. Ann, a security administrator, has been tasked by the Chief Information Officer (CIO) to have the company's application servers tested using black box methodology. Which of the following BEST describes what Ann has been asked to do?

A. Verify the server's patch level and attempt various knows exploits that might be possible due to missing security updates.

B. Simulate an external attack where the attackers have been provided with user access privileges on the server.

C. Organize the application developers to attempt to compromise their servers by entering invalid data into their entry fields.

[✓ D.] Simulate an external attack where the attackers have no information regarding the software or systems in place.

61. A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks. Which of the following is the reason the manager installed the racks this way?

A. To lower energy consumption by sharing power outlets

[✓ B.] To create environmental hot and cold isles

C. To eliminate the potential for electromagnetic interference

D. To maximize fire suppression capabilities

62. Phishing emails frequently take advantage of high-profile catastrophes reported in the news. Which of the following principles BEST describes the weakness being exploited?

[✓ A.] Intimidation

B. Scarcity

C. Authority

D. Social proof

63. Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network. This is MOST likely which of the following types of attacks?

[✓ A.] Vishing

B. Impersonation

C. Spim

D. Scareware

64. An administrator discovers the following log entry on a server:

```
Nov 12 2013 00:23:45 httpd[2342]: GET
/app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow
```

Which of the following attacks is being attempted?

A. Command injection

B. Password attack

C. Buffer overflow

[✓ D.] Cross-site scripting

65. A security team wants to establish an Incident Response plan. The team has never experienced an incident. Which of the following would BEST help them establish plans and procedures?
[✓ A.] Table top exercises
B. Lessons learned
C. Escalation procedures
[✓ D.] Recovery procedures

66. Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?
A. Protocol analyzer
[✓ B.] Vulnerability scan
C. Penetration test
D. Port scanner

67. Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?
A. Cloud computing
B. Virtualization
C. Redundancy
D. Application control

68. A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN. Which of the following protocols should be used?
[✓ A.] RADIUS
B. Kerberos
C. LDAP
D. MSCHAP

69. A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion. Which of the following technologies would BEST be suited to accomplish this?
A. Transport Encryption
B. Stream Encryption
C. Digital Signature
[✓ D.] Steganography

70. A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database Which of the following risk mitigation strategies should have been implemented when the supervisor was demoted?
[✓ A.] Incident management
B. Routine auditing
C. IT governance
D. Monthly user rights reviews

71. Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?
A. War chalking
[✓ B.] Bluejacking
C. Bluesnarfing
D. Rogue tethering

72. Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation?
A. An ephemeral key was used for one of the messages
B. A stream cipher was used for the initial email; a block cipher was used for the reply
C. Out-of-band key exchange has taken place
[✓ D.] Asymmetric encryption is being used

73. Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message. Which of the following principles of social engineering made this attack successful?

[✓ A.] Authority
B. Spamming
C. Social proof
D. Scarcity

74. Which of the following is the LEAST secure hashing algorithm?
A. SHA1
B. RIPEMD
[✓ C.] MD5
D. DES

75. An employee uses RDP to connect back to the office network. If RDP is misconfigured, which of the following security exposures would this lead to?
A. A virus on the administrator's desktop would be able to sniff the administrator's username and password.
B. Result in an attacker being able to phish the employee's username and password.
C. A social engineering attack could occur, resulting in the employee's password being extracted.
[✓ D.] A man in the middle attack could occur, resulting the employee's username and password being captured.

76. During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall. Which of the following will the audit team most 1 likely recommend during the audit out brief?
A. Discretionary access control for the firewall team
[✓ B.] Separation of duties policy for the firewall team
C. Least privilege for the firewall team
D. Mandatory access control for the firewall team

77. Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?
A. NAC
B. VLAN
[✓ C.] DMZ
D. Subnet

78. An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server. Which of the following will most likely fix the uploading issue for the users?
A. Create an ACL to allow the FTP service write access to user directories
[✓ B.] Set the Boolean SELinux value to allow FTP home directory uploads
C. Reconfigure the FTP daemon to operate without utilizing the PASV mode
D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

79. An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity. Which of the following actions will help detect attacker attempts to further alter log files?
A. Enable verbose system logging
B. Change the permissions on the user's home directory
[✓ C.] Implement remote syslog
D. Set the bash_history log file to "read only"

80. A global gaming console manufacturer is launching a new gaming platform to its customers. Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?
[✓ A.] Firmware version control
B. Manual software upgrades
C. Vulnerability scanning
[✓ D.] Automatic updates
E. Network segmentation
F. Application firewalls

81. An audit has revealed that database administrators are also responsible for

auditing database changes and backup logs. Which of the following access control methodologies would BEST mitigate this concern?

A. Time of day restrictions
B. Principle of least privilege
C. Role-based access control
[✓ D.] Separation of duties

82. Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications. Which of the following best describes what she will do?

[✓ A.] Enter random or invalid data into the application in an attempt to cause it to fault
B. Work with the developers to eliminate horizontal privilege escalation opportunities
C. Test the applications for the existence of built-in- back doors left by the developers
D. Hash the application to verify it won't cause a false positive on the HIPS.

83. Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop. Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?

A. full-disk encryption
[✓ B.] Host-based firewall
C. Current antivirus definitions
D. Latest OS updates

84. An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times. Which of the following describes this type of attack?

A. Integer overflow attack
B. Smurf attack
[✓ C.] Replay attack
D. Buffer overflow attack
E. Cross-site scripting attack

85. An organization is moving its human resources system to a cloud services provider. The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords. Which of the following options meets all of these requirements?

A. Two-factor authentication
B. Account and password synchronization
C. Smartcards with PINS
[✓ D.] Federated authentication

86. The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?

A. Implement deduplication at the network level between the two locations
[✓ B.] Implement deduplication on the storage array to reduce the amount of drive space needed
C. Implement deduplication on the server storage to reduce the data backed up
D. Implement deduplication on both the local and remote servers

87. A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?

[✓ A.] Set up the scanning system's firewall to permit and log all outbound connections
B. Use a protocol analyzer to log all pertinent network traffic
C. Configure network flow data logging on all scanning system
D. Enable debug level logging on the scanning system and all scanning tools used.

88. Which of the following best describes the initial processing phase used in mobile device forensics?

[✓ A.] The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
B. The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
C. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
D. The phone and storage cards should be examined as a complete unit after examining

the removable storage cards separately.

89. Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain \. Which of the following tools would aid her to decipher the network traffic?
A. Vulnerability Scanner
B. NMAP
C. NETSTAT
[✓ D.] Packet Analyzer

90. An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?
A. Find two identical messages with different hashes
B. Find two identical messages with the same hash
C. Find a common has between two specific messages
[✓ D] Find a common hash between a specific message and a random message

91. The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administor has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled. Which of the following would further obscure the presence of the wireless network?
A. Upgrade the encryption to WPA or WPA2
B. Create a non-zero length SSID for the wireless router
C. Reroute wireless users to a honeypot
[✓ D] Disable responses to a broadcast probe request

92. Which of the following should be used to implement voice encryption?
A. SSLv3
B. VDSL Secure real-time Transport Protocol
[✓ C.] SRTP
D. VoIP

93. During an application design, the development team specifics a LDAP module for single sign-on communication with the company's access control database. This is an example of which of the following?
A. Application control
B. Data in-transit
C. Identification
[✓ D.] Authentication

94. After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?
A. Time-of-day restrictions
B. Change management
C. Periodic auditing of user credentials
[✓ D.] User rights and permission review

95. A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA inorder to verify:
[✓ A.] Performance and service delivery metrics
B. Backups are being performed and tested
C. Data ownership is being maintained and audited
D. Risk awareness is being adhered to and enforced

96. Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?
[✓ A.] Calculate the ALE
B. Calculate the ARO
C. Calculate the MTBF
D. Calculate the TCO

97. A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list. Which of the following BEST describes this type of IDS?
[✓ A.] Signature based
B. Heuristic
C. Anomaly-based

D. Behavior-based

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

99. During a data breach cleanup it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?
A. Reporting
[✓ B.] Preparation
C. Mitigation
D. Lessons Learned

100. New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority. In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?
[✓ A.] Fail safe
B. Fault tolerance
C. Fail secure
D. Redundancy