1. The Chief Security Officer (CSO) for a datacenter in a hostile environment, is concerned about protecting the facility from car bomb attacks. Which of the following BEST would protect the building from this threat? (Choose two.)
A. Dogs
B. Fencing
C. CCTV
D. Guards
E. Bollards
F. Lighting

2. Users can authenticate to a company's web applications using their credentials form a popular social media site. Which of the following poses the greatest risk with this integration?
A. Malicious users can exploit local corporate credentials with their social media credentials
B. Changes to passwords on the social media site can be delayed from replicating to the company
C. Data loss from the corporate servers can create legal liabilities with the social media site
D. Password breaches to the social media affect the company application as well

3. A corporation has experienced several media leaks of proprietary data on various web forums. The posts were made during business hours and it is believed that the culprit is posting during work hours from a corporate machine. The Chief Information Officer (CIO) wants to scan internet traffic and keep records for later use in legal proceedings once the culprit is found. Which of the following provides the BEST solution?
A. Protocol analyzer
B. NIPS
C. Proxy server
D. HIDS

4. The security administrator runs an rpm verify command which records the MD5 sum, permissions, and timestamp of each file on the system. The administrator saves this information to a separate server. Which of the following describes the procedure the administrator has performed?
A. Host software base-lining
B. File snapshot collection
C. TPM
D. ROMDB verification

5. Users are trying to communicate with a network but are unable to do so. A network administrator sees connection attempts on port 20 from outside IP addresses that are being blocked. How can the administrator resolve this?
A. Enable stateful FTP on the firewall
B. Enable inbound SSH connections
C. Enable NETBIOS connections in the firewall
D. Enable HTTPS on port 20

6. In order to enter a high-security datacenter, users are required to speak the password into a voice recognition system. Ann a member if the sales department over hears the password and upon speaks it into the system. The system denies her entry and alerts the security team. Which of the following is the MOST likely reason for her failure to enter the data center?
A. An authentication factor
B. Discretionary access
C. Time of day restrictions
D. Least privilege restrictions

7. Given the following list of corporate access points, which of the following attacks is MOST likely underway if the company wireless network uses the same wireless hardware throughout?
MAC SID
00:01:AB:FA:CD:34Corporate AP
00:01:AB:FA:CD:35Corporate AP
00:01:AB:FA:CD:36Corporate AP
00:01:AB:FA:CD:37Corporate AP
00:01:AB:FA:CD:34Corporate AP

A. Packet sniffing

B. Evil Twin
C. WPS attack
D. Rogue access point

8. A system administrator has noticed network performance issues and wants to gather performance data from the gateway router. Which of the following can be used to perform this action?
A. SMTP
B. iSCSI
C. SNMP
D. IPSec

9. Which of the following technologies was developed to allow companies to use less-expensive storage while still maintaining the speed and redundancy required in a business environment?
A. RAID
B. Tape Backup
C. Load Balancing
D. Clustering

10. Joe a technician is tasked with finding a way to test operating system patches for a wide variety of servers before deployment to the production environment while utilizing a limited amount of hardware resources. Which of the following would provide the BEST environment for performing this testing?
A. OS hardening
B. Application control
C. Virtualization
D. Sandboxing

11. Which of the following is replayed during wireless authentication to exploit a weal key infrastructure?
A. Preshared keys
B. Ticket exchange
C. Initialization vectors
D. Certificate exchange

12. A new security policy being implemented requires all email within the organization be digitally signed by the author using PGP. Which of the following would needs to be created for each user?
A. A certificate authority
B. A key escrow
C. A trusted key
D. A public and private key

13. Which of the following authentication provides users XML for authorization and authentication?
A. Kerberos
B. LDAP
C. RADIUS
D. SAML

14. A company wants to prevent end users from plugging unapproved smartphones into PCs and transferring data. Which of the following would be the BEST control to implement?
A. MDM
B. IDS
C. DLP
D. HIPS

15. The ore-sales engineering team needs to quickly provide accurate and up-to-date information to potential clients. This information includes design specifications and engineering data that is developed and stored using numerous applications across the enterprise. Which of the following authentication technique is MOST appropriate?
A. Common access cards
B. TOTP
C. Single sign-on
D. HOTP

16. A network engineer is configuring a VPN tunnel connecting a company's network to a business partner. Which of the following protocols should be used for key exchange?

A. SHA-1
B. RC4
C. Blowfish
D. Diffie-Hellman

17. Which of the following types of cloud computing would be MOST appropriate if an organization required complete control of the environment?
A. Hybrid Cloud
B. Private cloud
C. Community cloud
D. Community cloud
E. Public cloud

18. The database server used by the payroll system crashed at 3 PM and payroll is due at 5 PM. Which of the following metrics is MOST important is this instance?
A. ARO
B. SLE
C. MTTR
D. MTBF

19. Which of the following is an attack designed to activate based on time?
A. Logic Bomb
B. Backdoor
C. Trojan
D. Rootkit

20. A network security engineer notices unusual traffic on the network from a single IP attempting to access systems on port 23. Port 23 is not used anywhere on the network. Which of the following should the engineer do to harden the network from this type of intrusion in the future?
A. Disable unnecessary services on servers
B. Disable unused accounts on servers and network devices
C. Implement password requirements on servers and network devices
D. Enable auditing on event logs

21. Which of the following documents outlines the responsibility of both participants in an agreement between two organizations?
A. RFC
B. MOU
C. RFQ
D. SLA

22. Users in the HR department were recently informed that they need to implement a user training and awareness program which is tailored to their department. Which of the following types of training would be the MOST appropriate for this department?
A. Handing PII
B. Risk mitigation
C. Input validation
D. Hashing

23. Which of the following incident response plan steps would MOST likely engaging business professionals with the security team to discuss changes to existing procedures?
A. Recovery
B. Incident identification
C. Isolation / quarantine
D. Lessons learned
E. Reporting

24. A company is starting to allow employees to use their own personal devices without centralized management. Employees must contact IT to have their devices configured to use corporate email; access is also available to the corporate cloud-based servers. Which of the following is the BEST policy to implement under these circumstances?
A. Acceptable use policy
B. Security policy
C. Group policy
D. Business Agreement policy

25. Which of the following BEST explains Platform as a Service?
A. An external entity that provides a physical or virtual instance of an installed

operating system
B. A third party vendor supplying support services to maintain physical platforms and servers
C. An external group providing operating systems installed on virtual servers with web applications
D. An internal group providing physical server instances without installed operating systems or support

26. One of the senior managers at a company called the help desk to report to report a problem. The manager could no longer access data on a laptop equipped with FDE. The manager requested that the FDE be removed and the laptop restored from a backup. The help desk informed the manager that the recommended solution was to decrypt the hard drive prior to reinstallation and recovery. The senior manager did not have a copy of the private key associated with the FDE on the laptop. Which of the following tools or techniques did the help desk use to avoid losing the data on the laptop?
A. Public key
B. Recovery agent
C. Registration details
D. Trust Model

27. An employee in the accounting department recently received a phishing email that instructed them to click a link in the email to view an important message from the IRS which threatened penalties if a response was not received by the end of the business day. The employee clicked on the link and the machine was infected with malware. Which of the following principles BEST describes why this social engineering ploy was successful?
A. Scarcity
B. Familiarity
C. Social proof
D. Urgency

28. A security technician received notification of a remotely exploitable vulnerability affecting all multifunction printers firmware installed throughout the organization. The vulnerability allows a malicious user to review all the documents processed by the affected printers. Which of the following compensating controls can the security technician to mitigate the security risk of a sensitive document leak?
A. Create a separate printer network
B. Perform penetration testing to rule out false positives
C. Install patches on the print server
D. Run a full vulnerability scan of all the printers

29. A systems administrator has made several unauthorized changes to the server cluster that resulted in a major outage. This event has been brought to the attention of the Chief Information Office (CIO) and he has requested immediately implement a risk mitigation strategy to prevent this type of event from reoccurring. Which of the following would be the BEST risk mitigation strategy to implement in order to meet this request?
A. Asset Management
B. Change Management
C. Configuration Management
D. Incident Management

30. An incident occurred when an outside attacker was able to gain access to network resources. During the incident response, investigation security logs indicated multiple failed login attempts for a network administrator. Which of the following controls, if in place could have BEST prevented this successful attack?
A. Password history
B. Password complexity
C. Account lockout
D. Account expiration

31. Joe needs to track employees who log into a confidential database and edit files. In the past, critical files have been edited, and no one admits to making the edits. Which of the following does Joe need to implement in order to enforce accountability?
A. Non-repudiation
B. Fault tolerance
C. Hashing
D. Redundancy

32. A new mobile banking application is being developed and uses SSL / TLS certificates but penetration tests show that it is still vulnerable to man-in-the-middle attacks, such as DNS hijacking. Which of the following would mitigate this attack?
A. Certificate revocation
B. Key escrow
C. Public key infrastructure
D. Certificate pinning

33. One month after a software developer was terminated, the helpdesk started receiving calls that several employees' computers were being infected with malware. Upon further research, it was determined that these employees had downloaded a shopping toolbar. It was this toolbar that downloaded and installed the errant code. Which of the following attacks has taken place?
A. Logic bomb
B. Cross-site scripting
C. SQL injection
D. Malicious add-on

34. Which of the following would an attacker use to generate and capture additional traffic prior to performing an IV attack?
A. DNS poisoning
B. DDoS
C. Replay attack
D. Dictionary attack

35. An administrator has concerns regarding the company's server rooms Proximity badge readers were installed, but it is discovered this is not preventing unapproved personnel from tailgating into these area. Which of the following would BEST address this concern?
A. Replace proximity readers with turn0based key locks
B. Install man-traps at each restricted area entrance
C. Configure alarms to alert security when the areas are accessed
D. Install monitoring cameras at each entrance

36. Which of the following would be a reason for developers to utilize an AES cipher in CCM mode (Counter with Chain Block Message Authentication Code)?
A. It enables the ability to reverse the encryption with a separate key
B. It allows for one time pad inclusions with the passphrase
C. Counter mode alternates between synchronous and asynchronous encryption
D. It allows a block cipher to function as a steam cipher

37. One of the findings of risk assessment is that many of the servers on the data center subnet contain data that is in scope for PCI compliance, Everyone in the company has access to these servers, regardless of their job function. Which of the following should the administrator do?
A. Segment the network
B. Use 802.1X
C. Deploy a proxy sever
D. Configure ACLs
E. Write an acceptable use policy

38. Various employees have lost valuable customer data due to hard drives failing in company provided laptops. It has been discovered that the hard drives used in one model of laptops provided by the company has been recalled by the manufactory. The help desk is only able to replace the hard drives after they fail because there is no centralized record of the model of laptop given to each specific user. Which of the following could have prevented this situation from occurring?
A. Data backups
B. Asset tracking
C. Support ownership
D. BYOD policies

39. Attempting to inject 50 alphanumeric key strokes including spaces into an application input field that only expects four alpha characters in considered which of the following attacks?
A. XML injection
B. Buffer overflow
C. LDAP Injection
D. SQL injection

40. An organization is required to log all user internet activity. Which of the following would accomplish this requirement?
A. Configure an access list on the default gateway router. Configure the default gateway router to log all web traffic to a syslog server
B. Configure a firewall on the internal network. On the client IP address configuration, use the IP address of the firewall as the default gateway, configure the firewall to log all traffic to a syslog server
C. Configure a proxy server on the internal network and configure the proxy server to log all web traffic to a syslog server
D. Configure an access list on the core switch, configure the core switch to log all web traffic to a syslog server

41. An agent wants to create fast and efficient cryptographic keys to use with Diffie-Hellman without using prime numbers to generate the keys. Which of the following should be used?
A. Elliptic curve cryptography
B. Quantum cryptography
C. Public key cryptography
D. Symmetric cryptography

42. Joe an application developer is building an external facing marketing site. There is an area on the page where clients may submit their feedback to articles that are posted. Joe filters client-side JAVA input. Which of the following is Joe attempting to prevent?
A. SQL injections
B. Watering holes
C. Cross site scripting
D. Pharming

43. A video surveillance audit recently uncovered that an employee plugged in a personal laptop and used the corporate network to browse inappropriate and potentially malicious websites after office hours. Which of the following could BEST prevent a situation like this form occurring again?
A. Intrusion detection
B. Content filtering
C. Port security
D. Vulnerability scanning

44. A server administrator notes that a fully patched application often stops running due to a memory error. When reviewing the debugging logs they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describes?
A. Malicious add-on
B. SQL injection
C. Cross site scripting
D. Zero-day

45. A resent OS patch caused an extended outage. It took the IT department several hours to uncover the cause of the issue due to the system owner who installed the patch being out of the office. Which of the following could help reduce the likelihood of this situation occurring in the future?
A. Separation of duties
B. Change management procedures
C. Incident management procedures
D. User rights audits and reviews

46. The Chief Information Security Officer (CISO) is concerned that users could bring their personal laptops to work and plug them directly into the network port under their desk. Which of the following should be configured on the network switch to prevent this from happening?
A. Access control lists
B. Loop protection
C. Firewall rule
D. Port security

47. Ann a network administrator has been tasked with strengthening the authentication of users logging into systems in area containing sensitive information. Users log in with usernames and passwords, following by a retinal scan. Which of the following could

she implement to add an additional factor of authorization?
A. Requiring PII usage
B. Fingerprint scanner
C. Magnetic swipe cards
D. Complex passphrases

48. In an environment where availability is critical such as Industrial control and SCADA networks, which of the following technologies in the MOST critical layer of defense for such systems?
A. Log consolidation
B. Intrusion Prevention system
C. Automated patch deployment
D. Antivirus software

49. A security manager installed a standalone fingerprint reader at the data center. All employees that need to access the data center have been enrolled to the reader and local reader database is always kept updates. When an employee who has been enrolled uses the fingerprint reader the door to the data center opens. Which of the following does this demonstrate? (Choose three.)
A. Two-factor authentication
B. Single sign-on
C. Something you have
D. Identification
E. Authentication
F. Authorization

50. A network technician is configuring clients for VLAN access. The network address for the sales department is 192.168.0.64 with a broadcast address of 192.168.0.71. Which of the following IP address/subnet mask combinations could be used to correctly configure a client machine in the sales department?
A. 192.168.0.64/29
B. 192.168.0.66/27
C. 192.168.0.67/29
D. 192.168.0.70/28

51. The help desk is experiencing a higher than normal amount of calls from users reporting slow response from the application server. After analyzing the data from a packet capturing tool, the head of the network engineering department determines that the issue is due, in part from the increase of personnel recently hired to perform application development. Which of the following would BEST assist in correcting this issue?
A. Load balancer
B. Spam filter
C. VPN Concentrator
D. NIDS

52. Two organizations want to share sensitive data with one another from their IT systems to support a mutual customer base. Both organizations currently have secure network and security policies and procedures. Which of the following should be the PRIMARY security considerations by the security managers at each organization prior to sharing information? (Choose three.)
A. Physical security controls
B. Device encryption
C. Outboarding/Offboarding
D. Use of digital signatures
E. SLA/ISA
F. Data ownership
G. Use of smartcards or common access cards
H. Patch management

53. A company's password and authentication policies prohibit the use of shared passwords and transitive trust. Which of the following if implemented would violate company policy? (Choose two.)
A. Discretionary access control
B. Federation
C. Single sign-on
D. TOTP
E. Two-factor authentication

54. Which of the following types of attacks is based on coordinating small slices of a task across multiple systems?
A. DDos
B. Spam
C. Spoofing
D. Dos

55. A system security analyst wants to capture data flowing in and out of the enterprise. Which of the following would MOST likely help in achieving this goal?
A. Taking screenshots
B. Analyzing Big Data metadata
C. Analyzing network traffic and logs
D. Capturing system image

56. The security manager reports that the process of revoking certificates authority is too slow and should be automated. Which of the following should be used to automate this process?
A. CRL
B. GPG
C. OCSP
D. Key escrow

57. A user attempts to install a new and relatively unknown software program recommended by a colleague. The user is unable to install the program, dispute having successfully installed other programs previously. Which of the following is MOST likely the cause for the user's inability to complete the installation?
A. Application black listing
B. Network Intrusion Prevention System
C. Group Policy
D. Application White Listing

58. A company needs to provide web-based access to shared data sets to mobile users, while maintaining a standardized set of security controls. Which of the following technologies is the MOST appropriate storage?
A. Encrypted external hard drives
B. Cloud storage
C. Encrypted mobile devices
D. Storage Area Network

59. An employee's mobile device associates with the company's guest WiFi SSID, but then is unable to retrieve email. The email settings appear to be correct. Which of the following is the MOST likely cause?
A. The employee has set the network type to WPA instead of WPA2
B. The network uses a captive portal and requires a web authentication
C. The administrator has blocked the use of the personal hot spot feature
D. The mobile device has been placed in airplane mode

60. A malicious individual used an unattended customer service kiosk in a busy store to change the prices of several products. The alteration was not noticed until several days later and resulted in the loss of several thousand dollars for the store. Which of the following would BEST prevent this from occurring again?
A. Password expiration
B. Screen locks
C. Inventory control
D. Asset tracking

61. In order to enter a high-security data center, users are required to speak the password into a voice recognition system. Ann, a member of the sales department, overhears the password and later speaks it into the system. The system denies her entry and alerts the security team. Which of the following is the MOST likely reason for her failure to enter the data center?
A. An authentication factor
B. Discretionary Access
C. Time of Day Restrictions
D. Least Privilege Restrictions

62. A company requires that all users enroll in the corporate PKI structure and digitally sign all emails. Which of the following are primary reasons to sign emails with digital certificates? (Choose two.)

A. To establish non-repudiation
B. To ensure integrity
C. To prevent SPAM
D. To establish data loss prevention
E. To protect confidentiality
F. To establish transport encryption

63. The Chief Information Officer (CIO) has asked a security analyst to determine the estimated costs associated with each potential breach of their database that contains customer information. Which of the following is the risk calculation that the CIO is asking for?
A. Impact
B. SLE
C. ARO
D. ALE

64. A security assurance officer is preparing a plan to measure the technical state of a customer's enterprise. The testers employed to perform the audit will be given access to the customer facility and network. The testers will not be given access to the details of custom developed software used by the customer. However the testers with have access to the source code for several open source applications and pieces of networking equipment used at the facility, but these items will not be within the scope of the audit. Which of the following BEST describes the appropriate method of testing or technique to use in this scenario? (Choose two.)
A. Social engineering
B. All source
C. Black box
D. Memory dumping
E. Penetration

65. Which of the following authentication services combines authentication and authorization in a use profile and use UDP?
A. LDAP
B. Kerberos
C. TACACS+
D. RADIUS

66. A security administrator is designing an access control system, with an unlimited budget, to allow authenticated users access to network resources. Given that a multifactor authentication solution is more secure, which of the following is the BEST combination of factors?
A. Retina scanner, thumbprint scanner, and password
B. Username and password combo, voice recognition scanner, and retina scanner
C. Password, retina scanner, and proximity reader
D. One-time password pad, palm-print scanner, and proximity photo badges

67. The access control list (ACL) for a file on a server is as follows:
User: rwx
User: Ann: r- -
User: Joe: r- -

Group: rwx
Group: sales: r-x

Other: r-x

Joe and Ann are members of the Human Resources group. Will Ann and Joe be able to run the file?
A. No since Ann and Joe are members of the Sales group owner of the file
B. Yes since the regular permissions override the ACL for the file
C. No since the ACL overrides the regular permissions for the file
D. Yes since the regular permissions and the ACL combine to create the effective permissions on the file

68. Using a protocol analyzer, a security consultant was able to capture employee's credentials. Which of the following should the consultant recommend to the company, in order to mitigate the risk of employees credentials being captured in the same manner in the future?
A. Wiping of remnant data

B. Hashing and encryption of data in-use
C. Encryption of data in-transit
D. Hashing of data at-rest

69. A Company has recently identified critical systems that support business operations. Which of the following will once defined, be the requirement for restoration of these systems within a certain period of time?
A. Mean Time Between Failure
B. Mean Time to Restore
C. Recovery Point Objective
D. Recovery Time Objective

70. The software developer is responsible for writing the code and promoting from the development network to the quality network. The network administrator is responsible for promoting code to the application servers. Which of the following practices are they following to ensure application integrity?
A. Job rotation
B. Implicit deny
C. Least privilege
D. Separation of duties

71. Ann is traveling for business and is attempting to use the hotel's wireless network to check for new messages. She selects the hotel's wireless SSID from a list of networks and successfully connects. After opening her email client and waiting a few minutes, the connection times out. Which of the following should Ann do to retrieve her email messages?
A. Change the authentication method for her laptop's wireless card from WEP to WPA2.
B. Open a web browser and authenticate using the captive portal for the hotel's wireless network.
C. Contact the front desk and have the MAC address of her laptop added to the MAC filter on the hotel's wireless network.
D. Change the incoming email protocol from IMAP to POP3.

72. Which of the following password attacks involves attempting all kinds of keystroke combinations on the keyboard with the intention to gain administrative access?
A. Dictionary
B. Hybrid
C. Watering hole
D. Brute Force

73. Ann, a security administrator, is strengthening the security controls of the company's campus. Her goal is to prevent people from accessing open locations that are not supervised, such as around the receiving dock. She is also concerned that employees are using these entry points as a way of bypassing the security guard at the main entrance. Which of the following should Ann recommend that would BEST address her concerns?
A. Increase the lighting surrounding every building on campus
B. Build fences around campus with gates at entrances
C. Install cameras to monitor the unsupervised areas
D. Construct bollards to prevent vehicle entry in non-supervised areas

74. While an Internet café a malicious user is causing all surrounding wireless connected devices to have intermittent and unstable connections to the access point. Which of the following is MOST likely being used?
A. Evil Twin
B. Interference
C. Packet sniffer
D. Rogue AP

75. A password audit has revealed that a significant percentage if end-users have passwords that are easily cracked. Which of the following is the BEST technical control that could be implemented to reduce the amount of easily "crackable" passwords in use?
A. Credential management
B. Password history
C. Password complexity
D. Security awareness training

76. While working on a new project a security administrator wants to verify the integrity of the data in the organizations archive library. Which of the following is

the MOST secure combination to implement to meet this goal? (Choose two.)
A. Hash with SHA
B. Encrypt with Diffie-Hellman
C. Hash with MD5
D. Hash with RIPEMD
E. Encrypt with AES

77. A company has been attacked and their website has been altered to display false information. The security administrator disables the web server service before restoring the website from backup. An audit was performed on the server and no other data was altered. Which of the following should be performed after the server has been restored?
A. Monitor all logs for the attacker's IP
B. Block port 443 on the web server
C. Install and configure SSL to be used on the web server
D. Configure the web server to be in VLAN 0 across the network

78. A security administrator suspects that an employee in the IT department is utilizing a reverse proxy to bypass the company's content filter and browse unapproved and non-work related sites while at work. Which of the following tools could BEST be used to determine how the employee is connecting to the reverse proxy?
A. Port scanner
B. Vulnerability scanner
C. Honeypot
D. Protocol analyzer

79. Joe, a company's network engineer, is concerned that protocols operating at the application layer of the OSI model are vulnerable to exploitation on the network. Which of the following protocols should he secure?
A. SNMP
B. SSL
C. ICMP
D. NetBIOS

80. Ann a security technician receives a report from a user that is unable to access an offsite SSN server. Ann checks the firewall and sees the following rules:
Allow TCP 80
Allow TCP 443
Deny TCP 23
Deny TCP 20
Deny TCP 21

Which of the following is preventing the users from accessing the SSH server?
A. Deny TCP 20
B. Deny TCP 21
C. Deny TCP 23
D. Implicit deny

81. An administrator uses a server with a trusted OS and is configuring an application to go into production tomorrow, In order to make a new application work properly, the administrator creates a new policy that labels the application and assigns it a security context within the trusted OS. Which of the following control methods is the administrator using by configuring this policy?
A. Time based access control
B. Mandatory access control
C. Role based access control
D. Rule based access control

82. A security administrator has been tasked with assisting in the forensic investigation of an incident relating to employee misconduct. The employee's supervisor believes evidence of this misconduct can be found on the employee's assigned workstation. Which of the following choices BEST describes what should be done? (Choose two.)
A. Record time as offset as required and conduct a timeline analysis
B. Update antivirus definitions and conduct a full scan for infected files
C. Analyze network traffic, system, and file logs
D. Create an additional local admin account on that workstation to conduct work from
E. Delete other user profiles on the system to help narrow down the search space
F. Patch the system before reconnecting it to the network

83. Joe a web developer wants to make sure his application is not susceptible to cross-site request forgery attacks. Which of the following is one way to prevent this type of attack?
A. The application should always check the HTTP referrer header
B. The application should always check the HTTP Request header
C. The application should always check the HTTP Host header
D. The application should always use SSL encryption

84. A custom PKI application downloads a certificate revocation list (CRL) once per day. Management requests the list be checked more frequently. Which of the following is the BEST solution?
A. Refresh the CA public key each time a user logs in
B. Download the CRK every 60 seconds
C. Implement the OCSP protocol
D. Prompt the user to trust a certificate each time it is used

85. A rogue programmer included a piece of code in an application to cause the program to halt at 2:00 PM on Monday afternoon when the application is most utilized. This is Which of the following types of malware?
A. Trojan
B. Virus
C. Logic Bomb
D. Botnets

86. After connecting to the corporate network a user types the URL if a popular social media website in the browser but reports being redirected to a login page with the corporate logo. Which of the following is this an example of?
A. LEAP
B. MAC filtering
C. WPA2-Enterprise
D. Captive portal

87. The Quality Assurance team is testing a third party application. They are primarily testing for defects and have some understanding of how the application works. Which of the following is the team performing?
A. Grey box testing
B. White box testing
C. Penetration testing
D. Black box testing

88. A user Ann has her assigned token but she forgotten her password. Which of the following appropriately categorizes the authentication factor that will fail in this scenario?
A. Something you do
B. Something you know
C. Something you are
D. Something you have

89. An employee from the fire Marshall's office arrives to inspect the data center. The operator allows him to bypass the multi-factor authentication to enter the data center. Which of the following types of attacks may be underway?
A. Impersonation
B. Hoax
C. Tailgating
D. Spoofing

90. A company recently received accreditation for a secure network, In the accreditation letter, the auditor specifies that the company must keep its security plan current with changes in the network and evolve the systems to adapt to new threats. Which of the following security controls will BEST achieve this goal?
A. Change management
B. Group Policy
C. Continuous monitoring
D. Credential management

91. A cyber security administrator receives a list of IPs that have been reported as attempting to access the network. To identify any possible successful attempts across the enterprise, which of the following should be implemented?

A. Monitor authentication logs
B. Disable unnecessary accounts
C. Time of day restrictions
D. Separation of duties

92. Which of the following exploits either a host file on a target machine or vulnerabilities on a DNS server in order to carry out URL redirection?
A. Pharming
B. Spoofing
C. Vishing
D. Phishing

93. Ann a new small business owner decides to implement WiFi access for her customers. There are several other businesses nearby who also have WiFi hot spots. Ann is concerned about security of the wireless network and wants to ensure that only her customers have access. Which of the following choices BEST meets her intent of security and access?
A. Enable port security
B. Enable WPA
C. Disable SSID broadcasting
D. Enable WEP

94. A security engineer is tasked with encrypting corporate email. Which of the following technologies provide the MOST complete protection? (Choose two.)
A. PGP/GPG
B. S/MIME
C. IPSEC
D. Secure POP3
E. IMAP
F. HMAC

95. Which of the following is the GREATEST security concern of allowing employees to bring in their personally owned tablets and connecting to the corporate network?
A. Tablet network connections are stored and accessible from the corporate network
B. The company's attack surface increases with the non-corporate devices
C. Personally purchased media may be available on the network for others to stream
D. Encrypted tablets are harder to access to determine if they are infected

96. Searching for systems infected with malware is considered to be which of the following phases of incident response?
A. Containment
B. Preparation
C. Mitigation
D. Identification

97. A technician has deployed a new VPN concentrator. The device needs to authenticate users based on a backend directory service. Which of the following services could be run on the VPN concentrator to perform this authentication?
A. Kerberos
B. RADIUS
C. GRE
D. IPSec

98. A webpage displays a potentially offensive advertisement on a computer. A customer walking by notices the displayed advertisement and files complaint. Which of the following can BEST reduce the likelihood of this incident occurring again?
A. Clean-desk policies
B. Screen-locks
C. Pop-up blocker
D. Antispyware software

99. Which of the following is an attack designed to activate based on date?
A. Logic bomb
B. Backdoor
C. Trojan
D. Rootkit

100. A malicious user has collected the following list of information:
-- 192.168.1.5 OpenSSH-Server_5.8

-- 192.168.1.7 OpenSSH-Server_5.7
-- 192.168.1.9 OpenSSH-Server_5.7

Which of the following techniques is MOST likely to gather this type of data?
A. Banner grabbing
B. Port scan
C. Host scan
D. Ping scan