1. Which of the following types of malware is designed to provide access to a system when normal authentication fails?
A. Rootkit
B. Botnet
C. Backdoor
D. Adware

2. Ann is concerned that the application her team is currently developing is vulnerable to unexpected user input that could lead to issues within the memory is affected in a detrimental manner leading to potential exploitation. Which of the following describes this application threat?
A. Replay attack
B. Zero-day exploit
C. Distributed denial of service
D. Buffer overflow

3. Which of the following can be used for both encryption and digital signatures?
A. 3DES
B. AES
C. RSA
D. MD5

4. A user tries to visit a web site with a revoked certificate. In the background a server from the certificate authority only sends the browser revocation information about the domain the user is visiting. Which of the following is being used by the certificate authority in this exchange?
A. CSR
B. Key escrow
C. OCSP
D. CRL

5. Joe wants to employ MD5 hashing on the company file server. Which of the following is Joe trying to achieve?
A. Availability
B. Confidentiality
C. Non repudiation
D. Integrity

6. By hijacking unencrypted cookies an application allows an attacker to take over existing web sessions that do not use SSL or end to end encryption. Which of the following choices BEST mitigates the security risk of public web surfing? (Choose two.)
A. WPA2
B. WEP
C. Disabling SSID broadcasting
D. VPN
E. Proximity to WIFI access point

7. The security administration team at a company has been tasked with implementing a data-at-rest solution for its company storage. Due to the large amount of storage the Chief Information Officer (CISO) decides that a 128-bit cipher is needed but the CISO also does not want to degrade system performance any more than necessary. Which of the following encryptions needs BOTH of these needs?
A. SHA1
B. DSA
C. AES
D. 3DES

8. A company has a BYOD policy that includes tablets and smart phones. In the case of a legal investigation, which of the following poses the greatest security issues?
A. Recovering sensitive documents from a device if the owner is unable or unwilling to cooperate
B. Making a copy of all of the files on the device and hashing them after the owner has provided the PIN
C. Using GPS services to locate the device owner suspected in the investigation
D. Wiping the device from a remote location should it be identified as a risk in the investigation

9. After several thefts a Chief Executive Officer (CEO) wants to ensure unauthorized do not have to corporate grounds or its employees. The CEO just approved new budget line

items for fences, lighting, locks and CCTVs. Which of the following is the primary focus?
A. Safety
B. Confidentiality
C. Availability
D. Integrity

10. Which of the following steps in incident response procedures entails of the incident and identification of knowledge gained that can be applied to future handling of incidents?
A. Recovery procedures
B. Escalation and notification
C. Reporting
D. Lessons learned

11. Which of the following automated or semi-automated software testing techniques relies on inputting large amounts of random data to detect coding errors or application loopholes?
A. Fuzzing
B. Black box
C. Fault injection
D. SQL injection

12. A company's BYOD policy requires the installation of a company provide mobile agent on their on their personally owned devices which would allow auditing when an employee wants to connect a device to the corporate email system. Which of the following concerns will MOST affect the decision to use a personal device to receive company email?
A. Personal privacy
B. Email support
C. Data ownership
D. Service availability

13. A penetration tester is measuring a company's posture on social engineering. The penetration tester sends a phishing email claiming to be from IT asking employees to click a link to update their VPN software immediately. Which of the following reasons would explain why this attack could be successful?
A. Principle of Scarcity
B. Principle of Intimidation
C. Principle of Urgency
D. Principle of liking

14. A new employee has joined the accounting department and is unable to access the accounting server. The employee can access other network resources and the Internet. Other accounting employees are able to access the accounting server without any issues. Which of the following is the MOST likely issue?
A. The server's IDS is blocking the new employee's connection
B. The workstation is unable to join the domain
C. The server's drive is not mapped on the new employee's workstation
D. The new account is not in the proper role-based profile

15. Joe a sales employee is connecting to a wireless network and has entered the network information correctly. His computer remains connected to the network but he cannot access any resources on the network. Which of the following is the MOST likely cause of this issue?
A. The encryption is too strong
B. The network SSID is disabled
C. MAC filtering is enabled
D. The wireless antenna power is set too low

16. Which of the following is used to inform users of the repercussions of releasing proprietary information?
A. OLA
B. SLA
C. NDA
D. MOU

17. A review of administrative access has discovered that too many accounts have been granted administrative rights. Which of the following will alert the security team when elevated access is applied?
A. Establishing user access reviews

B. Establishing user based privileges
C. Establishing monitoring on accounts
D. Establishing group based privileges

18. When an authorized application is installed on a server, the application triggers an alert on the HIDS. This is known as a:
A. Vulnerability
B. False negative
C. False positive
D. Threat vector

19. In which of the following scenarios would it be preferable to implement file level encryption instead of whole disk encryption?
A. A server environment where the primary security concern is integrity and not file recovery
B. A cloud storage environment where multiple customers use the same hardware but possess different encryption keys
C. A SQL environment where multiple customers access the same database
D. A large datacenter environment where each customer users dedicated hardware resources

20. For high availability which of the following would be MOST appropriate for fault tolerance?
A. RAID 0
B. Clustering
C. JBOD
D. Load Balancing

21. When implementing a Public Key Infrastructure, which of the following should the sender use to digitally sign a document?
A. A CSR
B. A private key
C. A certificate authority
D. A public key

22. A military base wants to incorporate biometrics into its new security measures, but the head of security does not want them to be the sole method of authentication. For unmanned entry points, which of the following solutions would work BEST?
A. Use voice print and a bollard
B. Use a retina scanner and a thumbprint
C. Use CCTV and a PIN
D. Use a retina scan and a PIN code

23. Ann, a security administrator, wants to limit access to the wireless network. Which of the following can be used to do this without using certificates?
A. Employ EAP-TLS
B. Employ PEAP on all laptops
C. Enable MAC filtering
D. Disable SSID broadcasting

24. A user has an Android smartphone that supports full device encryption. However when the user plugs into a computer all of the files are immediately accessible. Which of the following should the user do to enforce full device confidentiality should the phone be lost or stolen?
A. Establish a PIN passphrase
B. Agree to remote wipe terms
C. Generate new media encryption keys
D. Download the encryption control app from the store

25. The network manager has obtained a public IP address for use with a new system to be available via the internet. This system will be placed in the DMZ and will communicate with a database server on the LAN. Which of the following should be used to allow fir proper communication between internet users and the internal systems?
A. VLAN
B. DNS
C. NAT
D. HTTP
E. SSL

26. After a new RADIUS server is added to the network, an employee is unable to connect

to the company's WPA2-Enterprise WIFI network, which is configured to prompt for the employee's network username and password. The employee reports receiving an error message after a brief connection attempt, but is never prompted for credentials. Which of the following issues could be causing the problem?

A. The employee's account is locked out in the directory service
B. The new RADIUS server is overloading the wireless access point
C. The new RADIUS server's certificate is not trusted by the employee's PC
D. The employee's account is disabled in the RADIUS server's local database

27. Ann the security administrator has been reviewing logs and has found several overnight sales personnel are accessing the finance department's network shares. Which of the following security controls should be implemented to BEST remediate this?

A. Mandatory access
B. Separation of duties
C. Time of day restrictions
D. Role based access

28. A fiber company has acquired permission to bury a fiber cable through a famer's land. Which of the following should be in the agreement with the farmer to protect the availability of the network?

A. No farm animals will graze near the burial site of the cable
B. No digging will occur near the burial site of the cable
C. No buildings or structures will be placed on top of the cable
D. No crops will be planted on top of the cable

29. The programmer confirms that there is potential for a buffer overflow on one of the data input fields in a corporate application. The security analyst classifies this as a (N).

A. Threat
B. Risk
C. Attack
D. Vulnerability

30. A security technician would like to use ciphers that generate ephemeral keys for secure communication. Which of the following algorithms support ephemeral modes? (Choose two.)

A. Diffie-Hellman
B. RC4
C. RIPEMO
D. NTLMv2
E. PAP
F. RSA

31. A security technician would like an application to use random salts to generate short lived encryption leys during the secure communication handshake process to increase communication security. Which of the following concepts would BEST meet this goal?

A. Ephemeral keys
B. Symmetric Encryption Keys
C. AES Encryption Keys
D. Key Escrow

32. A security administrator wishes to implement a method of generating encryption keys from user passwords to enhance account security. Which of the following would accomplish this task?

A. NTLMv2
B. Blowfish
C. Diffie-Hellman
D. PBKDF2

33. A security technician wants to improve the strength of a weak key by making it more secure against brute force attacks. Which of the following would achieve this?

A. Blowfish
B. Key stretching
C. Key escrow
D. Recovery agent

34. A recent audit had revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the

security posture during deployment? (Choose two.)
A. Deploy a honeypot
B. Disable unnecessary services
C. Change default passwords
D. Implement an application firewall
E. Penetration testing

35. A local hospital with a large four-acre campus wants to implement a wireless network so that doctors can use tablets to access patients' medical data. The hospital also wants to provide guest access to the internet for hospital patients and visitors in select areas. Which of the following areas should be addressed FIRST?
A. MAC filters
B. Site Survey
C. Power level controls
D. Antenna types

36. After making a bit-level copy of compromised server, the forensics analyst Joe wants to verify that he bid not accidentally make a change during his investigation. Which of the following should he perform?
A. Take a hash of the image and compare it to the one being investigated
B. Compare file sizes of all files prior to and after investigation
C. Make a third image and compare it to the second image being investigated
D. Compare the logs of the copy to the actual server

37. Which of the following attacks is generally initiated from a botnet?
A. Cross site scripting attack
B. HTTP header injection
C. Distributed denial of service
D. A war driving attack

38. A network security analyst has confirmed that the public facing web server has been compromised. Which of the following stages if the Incident Handling Response does this describe?
A. Analyzing
B. Recovering
C. Identification
D. Mitigation

39. Deploying compensating security controls is an example of:
A. Risk avoidance
B. Risk mitigation
C. Risk transference
D. Risk acceptance

40. A web startup wants to implement single sign-on where its customers can log on to the site by using their personal and existing corporate email credentials regardless of which company they work for. Is this directly supported by SAML?
A. No not without extensive partnering and API integration with all required email providers
B. Yes SAML is a web based single sign-on implementation exactly fir this purpose
C. No a better approach would be to use required email providers LDAP or RADIUS repositories
D. Yes SAML can use oauth2 to provide this functionality out of the box

41. A security administrator is installing a single camera outside in order to detect unauthorized vehicles in the parking lot. Which of the following is the MOST important consideration when deploying a CCTV camera to meet the requirement?
A. Training
B. Expense
C. Resolution
D. Field of view

42. A system administrator wants to configure a setting that will make offline password cracking more challenging. Currently the password policy allows upper and lower case characters a minimum length of 5 and a lockout after 10 invalid attempts. Which of the following has the GREATEST impact on the time it takes to crack the passwords?
A. Increase the minimum password length to 8 while keeping the same character set
B. Implement an additional password history and reuse policy
C. Allow numbers and special characters in the password while keeping the minimum

length at 5
D. Implement an account lockout policy after three unsuccessful logon attempts

43. Establishing a method to erase or clear memory is an example of securing which of the following?
A. Data in transit
B. Data at rest
C. Data in use
D. Data in motion

44. Joe processes several requisitions during the day and during the night shift they are approved by Ann. This is an example of which of the following?
A. Separation of duties
B. Discretionary access
C. Mandatory access
D. Time of day restrictions

45. A security administrator would like to write an access rule to block the three IP addresses given below. Which of the following combinations should be used to include all of the given IP addresses?
192.168.12.255
192.168.12.227
192.168.12.229
A. 192.168.12.0/25
B. 192.168.12.128.28
C. 192.168.12.224/29
D. 192.168.12.225/30

46. After installing a new Linux system, the administrator runs a command that records the size, permissions, and MD5 sum of all the files on the system. Which of the following describes what the administrator is doing?
A. Identifying vulnerabilities
B. Design review
C. Host software baselining
D. Operating system hardening

47. An intrusion has occurred in an internet facing system. The security administrator would like to gather forensic evidence while the system is still in operation. Which of the following procedures should the administrator perform FIRST on the system?
A. Make a drive image
B. Take hashes of system data
C. Collect information in RAM
D. Capture network traffic

48. Which of the following wireless standards is backwards compatible with 802.11g?
A. 802.11a
B. 802.11b
C. 802.11n
D. 802.1q

49. Joe uses his badge to enter the server room, Ann follows Joe entering without using her badge. It is later discovered that Ann used a USB drive to remove confidential data from a server. Which of the following principles is potentially being violated? (Choose two.)
A. Clean desk policy
B. Least privilege
C. Tailgating
D. Zero-day exploits
E. Data handling

50. The below report indicates that the system is MOST likely infected by which of the following?
Protocol -- LOCAL IP -- FOREIGN IP -- STATE
TCP -- 0.0.0:445 -- 0.0.0.0:0 -- Listening
TCP -- 0.0.0.0:3390 -- 0.0.0.0:0 -- Listening
A. Trojan
B. Worm
C. Logic bomb
D. Spyware

51. A security administrator is required to submit a detailed implementation plan and back out plan to get approval prior to updating the firewall and other security devices. Which of the following types of risk mitigation strategies is being followed?
A. Change management
B. Routine audit
C. Rights and permissions review
D. Configuration management

52. Which of the following authentication services uses a default TCP of 389?
A. SAML
B. TACACS+
C. Kerberos
D. LDAP

53. A software company sends their offsite backup tapes to a third party storage facility. TO meet confidentiality the tapes should be:
A. Labeled
B. Hashed
C. Encrypted
D. Duplicated

54. Ann, a technician, wants to implement a single protocol on a remote server which will enable her to encrypt and proxy all of her traffic though the remote server via SOCKS5. Which of the following should Ann enable to support both encryption and proxy services?
A. SSH
B. IPSEC
C. TLS
D. HTTPS

55. Ann, a system analyst, discovered the following log. Which of the following or techniques does this indicate?
{bp1@localmachine}$ Is-al
Total 12
Drwxrwxr-x
A. Protocol analyzer
B. Port scanner
C. Vulnerability
D. Banner grabbing

56. A company discovers an unauthorized device accessing network resources through one of many network drops in a common area used by visitors. The company decides that is wants to quickly prevent unauthorized devices from accessing the network but policy prevents the company from making changes on every connecting client. Which of the following should the company implement?
A. Port security
B. WPA2
C. Mandatory Access Control
D. Network Intrusion Prevention

57. The helpdesk is receiving numerous reports that a newly installed biometric reader at the entrance of the data center has a high of false negatives. Which of the following is the consequence of this reported problem?
A. Unauthorized employees have access to sensitive systems
B. All employees will have access to sensitive systems
C. No employees will be able to access the datacenter
D. Authorized employees cannot access sensitive systems

58. A software developer places a copy of the source code for a sensitive internal application on a company laptop to work remotely. Which of the following policies is MOST likely being violated?
A. Clean desk
B. Data handling
C. Chain of custody
D. Social media

59. While testing a new host based firewall configuration a security administrator inadvertently blocks access to localhost which causes problems with applications

running on the host. Which of the following addresses refer to localhost?
A. ::0
B. 127.0.0.0
C. 127.0.0.1
D. 127.0.0/8
E. 127::0.1

60. A user has reported inadvertently sending an encrypted email containing PII to an incorrect distribution group. Which of the following potential incident types is this?
A. Data sharing
B. Unauthorized viewing
C. Data breach
D. Unauthorized access

61. A company is exploring the option of letting employees use their personal laptops on the internal network. Which of the following would be the MOST common security concern in this scenario?
A. Credential management
B. Support ownership
C. Device access control
D. Antivirus management

62. A security engineer discovers that during certain times of day, the corporate wireless network is dropping enough packets to significantly degrade service. Which of the following should be the engineer's FIRST step in troubleshooting the issues?
A. Configure stronger encryption
B. Increase the power level
C. Change to a higher gain antenna
D. Perform a site survey

63. A security administrator is reviewing the web logs and notices multiple attempts by users to access:
http://www.comptia.org/idapsearch?user-

Having identified the attack, which of the following will prevent this type of attack on the web server?
A. Input validation on the web server
B. Block port 389 on the firewall
C. Segregate the web server by a VLAN
D. Block port 3389 on the firewall

64. A breach at a credit card company resulted in customers credit card information being exposed . The company has conducted a full forensic investigation and identified the source of the breach. Which of the following should the company do NEXT?
A. Move to the incident identification phase
B. Implement the risk assessment plan
C. Implement damage and loss control procedures
D. Implement first responder processes

65. Joe a user upon arriving to work on Monday morning noticed several files were deleted from the system. There were no records of any scheduled network outages or upgrades to the system. Joe notifies the security department of the anomaly found and removes the system from the network. Which of the following is the NEXT action that Joe should perform?
A. Screenshots of systems
B. Call the local police
C. Perform a backup
D. Capture system image

66. The user of a news service accidently accesses another user's browsing history. From this the user can tell what competitors are reading, querying, and researching. The news service has failed to properly implement which of the following?
A. Application white listing
B. In-transit protection
C. Access controls
D. Full disk encryption

67. A system requires administrators to be logged in as the "root" in order to make administrator changes. Which of the following controls BEST mitigates the risk

associated with this scenario?
A. Require that all administrators keep a log book of times and justification for accessing root
B. Encrypt all users home directories using file-level encryption
C. Implement a more restrictive password rotation policy for the shared root account
D. Force administrator to log in with individual accounts and switch to root
E. Add the administrator to the local group

68. A defense contractor wants to use one of its classified systems to support programs from multiple intelligence agencies. Which of the following MUST be in place between the intelligence agencies to allow this?
A. A DRP
B. An SLA
C. A MOU
D. A BCP

69. A penetration tester was able to obtain elevated privileges on a client workstation and multiple servers using the credentials of an employee. Which of the following controls would mitigate these issues? (Choose two.)
A. Separation of duties
B. Least privilege
C. Time of day restrictions
D. Account expiration
E. Discretionary access control
F. Password history

70. Which of the following is considered the MOST effective practice when securing printers or scanners in an enterprise environment?
A. Routine vulnerability scanning of peripherals
B. Install in a hardened network segment
C. Turn off the power to the peripherals at night
D. Enable print sharing only from workstations

71. After a few users report problems with the wireless network, a system administrator notices that a new wireless access point has been powered up in the cafeteria. The access point has the same SSID as the corporate network and is set to the same channel as nearby access points. However, the AP has not been connected to the Ethernet network. Which of the following is the MOST likely cause of the user's wireless problems?
A. AP channel bonding
B. An evil twin attack
C. Wireless interference
D. A rogue access point

72. A network technician at a company, Joe is working on a network device. He creates a rule to prevent users from connecting to a toy website during the holiday shopping season. This website is blacklisted and is known to have SQL injections and malware. Which of the following has been implemented?
A. Mandatory access
B. Network separation
C. Firewall rules
D. Implicit Deny

73. Company XYZ has suffered leaks of internally distributed confidential documents. Ann the network security analyst has been tasked to track down the culprit. She has decided to embed a four letter string of characters in documents containing proprietary information. Which of the following initial steps should Ann implement before sending documents?
A. Store one of the documents in a honey pot
B. Start antivirus scan on all the suspected computers
C. Add a signature to the NIDS containing the four letter string
D. Ask employees to report suspicious behaviors

74. Which of the following should a company deploy to prevent the execution of some types of malicious code?
A. Least privilege accounts
B. Host-based firewalls
C. Intrusion Detection systems
D. Application white listing

75. An administrator is investigating a system that may potentially be compromised and sees the following log entries on the router.
Jul 15 14:47:29.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) - > 10.10.1.5 (6667), 3 packets.
Jul 15 14:47:38.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) - > 10.10.1.5 (6667), 6 packets.
Jul 15 14:47:45.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) - > 10.10.1.5 (6667), 8 packets.

Which of the following BEST describes the compromised system?
A. It is running a rogue web server
B. It is being used in a man-in-the-middle attack
C. It is participating in a botnet
D. It is an ARP poisoning attack

76. Ann the IT director wants to ensure that as hoc changes are not making their way to the production applications. Which of the following risk mitigation strategies should she implement in her department?
A. Change management
B. Permission reviews
C. Incident management
D. Perform routine audits

77. Which of the following would allow users from outside of an organization to have access to internal resources?
A. NAC
B. VLANS
C. VPN
D. NAT

78. Which of the following is BEST described by a scenario where management chooses not to implement a security control for a given risk?
A. Mitigation
B. Avoidance
C. Acceptance
D. Transference

79. When confidentiality is the primary concern which of the following types of encryption should be chosen?
A. Digital Signature
B. Symmetric
C. Asymmetri
D. Hashing

80. A Windows- based computer is infected with malware and is running too slowly to boot and run a malware scanner. Which of the following is the BEST way to run the malware scanner?
A. Kill all system processes
B. Enable the firewall
C. Boot from CD/USB
D. Disable the network connection

81. Ann a member of the Sales Department has been issued a company-owned laptop for use when traveling to remote sites. Which of the following would be MOST appropriate when configuring security on her laptop?
A. Configure the laptop with a BIOS password
B. Configure a host-based firewall on the laptop
C. Configure the laptop as a virtual server
D. Configure a host-based IDS on the laptop

82. A security technician has removed the sample configuration files from a database server. Which of the following application security controls has the technician attempted?
A. Application hardening
B. Application baselines
C. Application patch management
D. Application input validation

83. Data confidentiality must be enforces on a secure database. Which of the following

controls meets this goal? (Choose two.)
A. MAC
B. Lock and key
C. Encryption
D. Non-repudiation
E. Hashing

84. A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site do not record any footage. Which of the following types of controls was being used?
A. Detective
B. Corrective
C. Deterrent
D. Preventive

85. A network security administrator is trying to determine how an attacker gained access to the corporate wireless network. The network is configured with SSID broadcast disabled. The senior network administrator explains that this configuration setting would only have deterred an unsophisticated attacker because of which of the following?
A. The SSID can be obtained with a wireless packet analyzer.
B. The required information can be brute forced over time.
C. Disabling the SSID only hides the network from other WAPs.
D. The network name could be obtained through a social engineering campaign.

86. Joe a system administrator receives reports that users attempting to reach the corporate website are arriving at an unfamiliar website instead. An investigation by a forensic analyst found that the name server log has several corporate IP addresses that were changed using Joe's credentials. Which of the following is this attack called?
A. Xmas attack
B. DNS poisoning
C. Web server attack
D. Spoofing attack

87. Joe a technician initiated scans if the company's 10 routers and discovered that half if the routers were not changed from their default configuration prior installed on the network. Which of the following would address this?
A. Secure router configuration
B. Implementing 802.1x
C. Enabling loop protection
D. Configuring port security

88. An employee attempts to go to a well-known bank site using the company-standard web browser by correctly typing in the address of the site into the web browser. The employee is directed to a website that looks like the bank's site but is not the actual bank site. The employee's user name and password are subsequently stolen. This is an example of which of the following?
A. Watering hole attack
B. Cross-site scripting
C. DNS poisoning
D. Man-in-the-middle attack

89. A user authenticates to a local directory server. The user then opens a virtualization client to connect to a virtual server. Instead of supplying a username/password combination, the user simply checks a "use directory credentials" checkbox to authenticate to the virtual server. Which of the following authentication types has been utilized?
A. Transitive trust
B. Common access card
C. Multifactor authentication
D. Single sign-on

90. The new Chief Information Officer (CIO) of company ABC, Joe has noticed that company XWY is always one step ahead with similar products. He tasked his Chief Security Officer to implement new security controls to ensure confidentiality of company ABC's proprietary data and complete accountability for all data transfers. Which of the following security controls did the Chief Security Officer implement to BEST meet these requirements? (Choose Two)
A. Redundancy
B. Hashing

C. DRP
D. Digital Signatures
E. Encryptions

91. A worker dressed in a fire suppression company's uniform asks to be let into the server room to perform the annual check in the fire extinguishers. The system administrator allows the worker into the room, only to discover hours later that the worker was actually a penetration tester. Which of the following reasons allowed the penetration tester to access the server room?
A. Testing the fire suppression system represented a critical urgency
B. The pen tester assumed the authority of a reputable company
C. The pen tester used an intimidation technique on the administrator
D. The administrator trusted that the server room would remain safe

92. A company uses port security based on an approved MAC list to secure its wired network and WPA2 to secure its wireless network. Which of the following prevents an attacker from learning authorized MAC addresses?
A. Port security prevents access to any traffic that might provide an attacker with authorized MAC addresses
B. Port security uses certificates to authenticate devices and is not part of a wireless protocol
C. Port security relies in a MAC address length that is too short to be cryptographically secure over wireless networks
D. Port security encrypts data on the network preventing an attacker form reading authorized MAC addresses

93. A security technician is implementing PKI on a Network. The technician wishes to reduce the amount of bandwidth used when verifying the validity of a certificate. Which of the following should the technician implement?
A. CSR
B. Key escrow
C. OSCR
D. CRL

94. The network security manager has been notified by customer service that employees have been sending unencrypted confidential information via email. Which of the following should the manager select to BEST detect and provide notification of these occurrences?
A. DLP
B. SSL
C. DEP
D. UTM

95. While troubleshooting a new wireless 802.11 ac network an administrator discovers that several of the older systems cannot connect. Upon investigation the administrator discovers that the older devices only support 802.11 and RC4. The administrator does not want to affect the performance of the newer 802.11 ac devices on the network. Which of the following should the administrator do to accommodate all devices and provide the MOST security?
A. Disable channel bonding to allow the legacy devices and configure WEP fallback
B. Configure the AP in protected mode to utilize WPA2 with CCMP
C. Create a second SSID on the AP which utilizes WPA and TKIP
D. Configure the AP to utilize the 5Gh band only and enable WEP

96. A security administrator is troubleshooting an authentication issues using a network sniffer. The security administrator reviews a packet capture of the authentication process and notices that authentication is performed using extensible markup over SOAP. Which of the following authentication services is the security administrator troubleshooting?
A. SAML
B. XTACACS
C. Secure LDAP
D. RADIUS

97. Given a class C network a technician has been tasked with creating a separate subnet for each of the eight departments in the company. Which of the following network masks would allow for each department to have a unique network space and what is the maximum number of hosts each department could have?
A. Network 255.255.255.192, 62 hosts

B. Network 255.255.255.224, 30 hosts
C. Network 255.255.255.240, 16 hosts
D. Network 255.255.255.248, 32 hosts

98. A software security concern when dealing with hardware and devices that have embedded software or operating systems is:
A. Patching may not always be possible
B. Configuration support may not be available
C. These is no way to verify if a patch is authorized or not
D. The vendor may not have a method for installation of patches

99. A major medical corporation is investigating deploying a web based portal for patients to access their medical records. The medical corporation has a long history of maintaining IT security but is considering having a third party vendor create the web portal. Which of the following areas is MOST important for the Chief Information Security Officer to focus on when reviewing proposal from vendors interested in creating the web portal?
A. Contractor background check
B. Confidentiality and availability
C. Redundancy and privacy
D. Integrity and confidentiality

100. Which of the following authentication methods requires the user, service provider and an identity provider to take part in the authentication process?
A. RADIUS
B. SAML
C. Secure LDAP
D. Kerberos