







- C. TCSEC (Trusted Computer System Evaluation Criteria)
- D. ITSEC (Information Technology Security Evaluation Criteria)

Answer: A

Q15. You are running cabling for a network through a boiler room where the furnace and some other heavy machinery reside. You are concerned about interference from these sources.

Which of the following types of cabling provides the best protection from interference in this area?

- A. STP
- B. UTP
- C. Coaxial
- D. Fiber-optic

Answer: D

Q16. When evidence is acquired, a log is started that records who had possession of the evidence for a specific amount of time. This is to avoid allegations that the evidence may have been tampered with when it was unaccounted for, and to keep track of the tasks performed in acquiring evidence from a piece of equipment or materials.

What is the term used to describe this process?

- A. Chain of command.
- B. Chain of custody.
- C. Chain of jurisdiction.
- D. Chain of evidence.

Answer: B

Q17. Following a disaster, while returning to the original site from an alternate site, the first process to resume at the original site would be the:

- A. Least critical process
- B. Most critical process.
- C. Process most expensive to maintain at an alternate site.
- D. Process that has a maximum visibility in the organization.

Answer: A

Q18. User A needs to send a private e-mail to User B. User A does not want anyone to have the ability to read the e-mail except for User B, thus retaining privacy.

Which tenet of information security is User A concerned about?

- A. Authentication

- B. Integrity
- C. Confidentiality
- D. Non-repudiation

Answer: C

Q19. What kind of attack are hashed password vulnerable to?

- A. Man in the middle.
- B. Dictionary or brute force.
- C. Reverse engineering.
- D. DoS (Denial of Service)

Answer: B

Q20. Active detection IDS systems may perform which of the following when a unauthorized connection attempt is discovered? (Choose all that apply.)

- A. Inform the attacker that he is connecting to a protected network.
- B. Shut down the server or service.
- C. Provide the attacker the usernames and passwords for administrative accounts.
- D. Break of suspicious connections.

Answer: B, D

Q21. You are the first to arrive at a crime scene in which a hacker is accessing unauthorized data on a file server from across the network.

To secure the scene, which of the followings actions should you perform?

- A. Prevent members of the organization from entering the server room.
- B. Prevent members of the incident response team from entering the server room.
- C. Shut down the server to prevent the user from accessing further data.
- D. Detach the network cable from the server to prevent the user from accessing further data.

Answer: A, D

Q22. An application that appears to perform a useful function but instead contains some sort of malicious code is called a \_\_\_\_\_.

- A. Worm
- B. SYN flood
- C. Virus
- D. Trojan Horse
- E. Logic Bomb

Answer: D

Q23. You have been alerted to the possibility of someone using an application to capture and manipulate packets as they are passing through your network.

What type of threat does this represent?

- A. DDos
- B. Back Door
- C. Spoofing
- D. Man in the Middle

Answer: D

Q24. Access controls that are created and administered by the data owner are considered:

- A. MACs (Mandatory Access Control)
- B. RBACs (Role Based Access Control)
- C. LBACs (List Based Access Control)
- D. DACs (Discretionary Access Control)

Answer: D

Q25. Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies.

What type of encryption is it from the list below?

- A. WTLS
- B. Symmetric
- C. Multifactor
- D. Asymmetric

Answer: B

Q26. When securing a FTP (File Transfer Protocol) server, what can be done to ensure that only authorized users can access the server?

- A. Allow blind authentication.
- B. Disable anonymous authentication.
- C. Redirect FTP (File Transfer Protocol) to another port.
- D. Only give the address to users that need access.

Answer: B

Q27. Asymmetric cryptography ensures that:

- A. Encryption and authentication can take place without sharing private keys.
- B. Encryption of the secret key is performed with the fastest algorithm available.
- C. Encryption occurs only when both parties have been authenticated.

D. Encryption factoring is limited to the session key.

Answer: A

Q28. A program that can infect other programs by modifying them to include a version of itself is a:

- A. Replicator
- B. Virus
- C. Trojan horse
- D. Logic bomb

Answer: B

Q29. The protection of data against unauthorized access or disclosure is an example of what?

- A. Confidentiality
- B. Integrity
- C. Signing
- D. Hashing

Answer: A

Q30. If a private key becomes compromised before its certificate's normal expiration, X.509 defines a method requiring each CA (Certificate Authority) to periodically issue a signed data structure called a certificate:

- A. Enrollment list
- B. Expiration list
- C. Revocation list
- D. Validation list

Answer: C

Q31. What transport protocol and port number does SSH (Secure Shell) use?

- A. TCP (Transmission Control Protocol) port 22
- B. UDP (User Datagram Protocol) port 69
- C. TCP (Transmission Control Protocol) port 179
- D. UDP (User Datagram Protocol) port 17

Answer: A

Q32. What design feature of Instant Messaging makes it extremely insecure compared to other messaging systems?

- A. It is a peer-to-peer network that offers most organizations virtually no control over it.

- B. Most IM clients are actually Trojan Horses.
- C. It is a centrally managed system that can be closely monitored.
- D. It uses the insecure Internet as a transmission medium.

Answer: A

Q33. John wants to encrypt a sensitive message before sending it to one of his managers.

Which type of encryption is often used for e-mail?

- A. S/MIME
- B. BIND
- C. DES
- D. SSL

Answer: A

Q34. In a decentralized privilege management environment, user accounts and passwords are stored on:

- A. One central authentication server.
- B. Each individual server.
- C. No more than two servers.
- D. One server configured for decentralized management.

Answer: B

Q35. Many intrusion detection systems look for known patterns or \_\_\_\_\_ to aid in detecting attacks.

- A. Viruses
- B. Signatures
- C. Hackers
- D. Malware

Answer: B

Q36. Providing false information about the source of an attack is known as:

- A. Aliasing
- B. Spoofing
- C. Flooding
- D. Redirecting

Answer: B

Q37. You are assessing risks and determining which asset protection policies to create first. Another member of the IT staff has provided you with a list of assets, which have

importance weighted on a scale of 1 to 10. Internet connectivity has an importance of 8, data has an importance of 9, personnel have an importance of 7, and software has an importance of 5.

Based on the weights, what is the order in which you will generate new policies?

- A. Internet policy, data security, personnel safety policy, software policy.
- B. Data security policy, Internet policy, software policy, personnel safety policy.
- C. Software policy, personnel safety policy, Internet policy, data security policy.
- D. Data security policy, Internet policy, personnel safety policy, software policy.

Answer: D

Q38. You are compiling estimates on how much money the company could lose if a risk occurred one time in the future.

Which of the following would these amounts represent?

- A. ARO
- B. SLE
- C. ALE
- D. Asset identification

Answer: B

Q39. When visiting an office adjacent to the server room, you discover the lock to the window is broken. Because it is not your office you tell the resident of the office to contact the maintenance person and have it fixed. After leaving, you fail to follow up on whether the window was actually repaired.

What affect will this have on the likelihood of a threat associated with the vulnerability actually occurring?

- A. If the window is repaired, the likelihood of the thread occurring will increase.
- B. If the window is repaired, the likelihood of the threat occurring will remain constant.
- C. If the window is not repaired the, the likelihood of the threat occurring will decrease.
- D. If the window is not repaired, the likelihood of the threat occurring will increase.

Answer: D

Q40. A company consists of a main building with two smaller branch offices at opposite ends of the city. The main building and branch offices are connected with fast links so that all employees have good connectivity to the network.

Each of the buildings has security measures that require visitors to sign in, and all employees are required to wear identification badges at all times. You want to protect servers and other vital equipment so that the company has the best level of security at the lowest possible cost.

Which of the following will you do to achieve this objective?

- A. Centralize servers and other vital components in a single room of the main building, and add security measures to this room so that they are well protected.
- B. Centralize most servers and other vital components in a single room of the main building, and place servers at each of the branch offices. Add security measures to areas where the servers and other components are located.
- C. Decentralize servers and other vital components, and add security measures to areas where the servers and other components are located.
- D. Centralize servers and other vital components in a single room in the main building. Because the building prevents unauthorized access to visitors and other persons, there is no need to implement physical security in the server room.

Answer: A

Q41. Which of the following backup methods copies only modified files since the last full backup?

- A. Full
- B. Differential
- C. Incremental
- D. Archive

Answer: B

Q42. When examining the server's list of protocols that are bound and active on each network interface card, the network administrator notices a relatively large number of protocols.

Which actions should be taken to ensure network security?

- A. Unnecessary protocols do not pose a significant to the system and should be left intact for compatibility reasons.
- B. There are no unneeded protocols on most systems because protocols are chosen during the installation.
- C. Unnecessary protocols should be disabled on all server and client machines on a network as they pose great risk.
- D. Using port filtering ACLs (Access Control List) at firewalls and routers is sufficient to stop malicious attacks on unused protocols.

Answer: C

Q43. An administrator notices that an e-mail server is currently relaying e-mail (including spam) for any e-mail server requesting relaying. Upon further investigation the administrator notices the existence of /etc/mail/relay domains. What modifications should the administrator make to the relay domains file to prevent relaying for non-explicitly named domains?

- A. Move the .\* entry to the bottom of the relay domains file and restart the e-mail process.

- B. Move the .\* entry to the top of the relay domains file and restart the e-mail process.
- C. Delete the .\* entry in the relay domains file and restart the e-mail process.
- D. Delete the relay domains file from the /etc/mail folder and restart the e-mail process.

Answer: C

Q44. A recent audit shows that a user logged into a server with their user account and executed a program. The user then performed activities only available to an administrator.

This is an example of an attack?

- A. Trojan horse
- B. Privilege escalation
- C. Subseven back door
- D. Security policy removal

Answer: B

Q45. Users who configure their passwords using simple and meaningful things such as pet names or birthdays are subject to having their account used by an intruder after what type of attack?

- A. Dictionary attack
- B. Brute Force attack
- C. Spoofing attack
- D. Random guess attack
- E. Man in the middle attack
- F. Change list attack
- G. Role Based Access Control attack
- H. Replay attack
- I. Mickey Mouse attack

Answer: A

Q46. By definition, how many keys are needed to lock and unlock data using symmetric-key encryption?

- A. 3+
- B. 2
- C. 1
- D. 0

Answer: C

Q47. A autonomous agent that copies itself into one or more host programs, then propagates when the host is run, is best described as a:

- A. Trojan horse
- B. Back door
- C. Logic bomb
- D. Virus

Answer: D

Q48. What are access decisions based on in a MAC (Mandatory Access Control) environment?

- A. Access control lists
- B. Ownership
- C. Group membership
- D. Sensitivity labels

Answer: D

Q49. A company uses WEP (Wired Equivalent Privacy) for wireless security. Who may authenticate to the company's access point?

- A. Only the administrator.
- B. Anyone can authenticate.
- C. Only users within the company.
- D. Only users with the correct WEP (Wired Equivalent Privacy) key.

Answer: D

Q50. Notable security organizations often recommend only essential services be provided by a particular host, and any unnecessary services be disabled.

Which of the following does NOT represent a reason supporting this recommendation?

- A. Each additional service increases the risk of compromising the host, the services that run on the host, and potential clients of these services.
- B. Different services may require different hardware, software, or a different discipline of administration.
- C. When fewer services and applications are running on a specific host, fewer log entries and fewer interactions between different services are expected, which simplifies the analysis and maintenance of the system from a security point of view.
- D. If a service is not using a well-known port, firewalls will not be able to disable access to this port, and an administrator will not be able to restrict access to this service.

Answer: B

Q51. Of the following services, which one determines what a user can change or view?

- A. Data integrity
- B. Data confidentiality
- C. Data authentication

D. Access control

Answer: D

Q52. One way to limit hostile sniffing on a LAN (Local Area Network) is by installing:

- A. An ethernet switch.
- B. An ethernet hub.
- C. A CSU/DSU (Channel Service Unit/Data Service Unit).
- D. A firewall.

Answer: A

Q53. Packet sniffing can be used to obtain username and password information in clear text from which one of the following?

- A. SSH (Secure Shell)
- B. SSL (Secure Sockets Layer)
- C. FTP (File Transfer Protocol)
- D. HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer)

Answer: C

Q54. Documenting change levels and revision information is most useful for:

- A. Theft tracking
- B. Security audits
- C. Disaster recovery
- D. License enforcement

Answer: C

Q55. IMAP4 requires port \_\_\_\_\_ to be open.

- A. 80
- B. 3869
- C. 22
- D. 21
- E. 23
- F. 25
- G. 110
- H. 143
- I. 443

Answer: H

Q56. As the Security Analyst for your companies network, you become aware that your systems may be under attack. This kind of attack is a DOS attack and the exploit send more traffic to a node than anticipated.

What kind of attack is this?

- A. Ping of death
- B. Buffer Overflow
- C. Logic Bomb
- D. Smurf

Answer: B

Q58. As the Security Analyst for your companies network, you want to implement AES. What algorithm will it use?

- A. Rijndael
- B. Nagle
- C. Spanning Tree
- D. PKI

Answer: A

Q59. Forensic procedures must be followed exactly to ensure the integrity of data obtained in an investigation. When making copies of data from a machine that us being examined, which of the following tasks should be done to ensure it is an exact duplicate?

- A. Perform a cyclic redundancy check using a checksum or hashing algorithm.
- B. Change the attributes of data to make it read only.
- C. Open files on the original media and compare them to the copied data.
- D. Do nothing. Imaging software always makes an accurate image.

Answer: A

Q60. As the Security Analyst for your companies network, you want to implement Single Signon technology.

What benefit can you expect to get when implementing Single Signon?

- A. You will need to log on twice at all times.
- B. You can allow for system wide permissions with it.
- C. You can install multiple applications.
- D. You can browse multiple directories.

Answer: D

Q61. What technology was originally designed to decrease broadcast traffic but is also beneficial in reducing the likelihood of having information compromised by sniffers?

- A. VPN (Virtual Private Network)
- B. DMZ (Demilitarized Zone)
- C. VLAN (Virtual Local Area Network)
- D. RADIUS (Remote Authentication Dial-in User Service)

Answer: C

Q62. When a user clicks to browse a secure page, the SSL (Secure Sockets Layer) enabled server will first:

- A. Use its digital certificate to establish its identity to the browser.
- B. Validate the user by checking the CRL (Certificate Revocation List).
- C. Request the user to produce the CRL (Certificate Revocation List).
- D. Display the requested page on the browser, then provide its IP (Internet Protocol) address for verification

Answer: A

Q63. A \_\_\_\_\_ occurs when a string of data is sent to a buffer that is larger than the buffer was designed to handle.

- A. Brute Force attack
- B. Buffer overflow
- C. Man in the middle attack
- D. Blue Screen of Death
- E. SYN flood
- F. Spoofing attack

Answer: B

Q64. Which of the following describes the concept of data integrity?

- A. A means of determining what resources a user can use and view.
- B. A method of security that ensures all data is sequenced, and numbered.
- C. A means of minimizing vulnerabilities of assets and resources.
- D. A mechanism applied to indicate a data's level of security.

Answer: B

Q65. After installing a new operating system, what configuration changes should be implemented?

- A. Create application user accounts.
- B. Rename the guest account.
- C. Rename the administrator account, disable the guest accounts.
- D. Create a secure administrator account.

Answer: C

Q66. You are explaining SSL to a junior administrator and come up to the topic of handshaking.

How many steps are employed between the client and server in the SSL handshake process?

- A. Five
- B. Six
- C. Seven
- D. Eight

Answer: B

Q67. The term "due care" best relates to:

- A. Policies and procedures intended to reduce the likelihood of damage or injury.
- B. Scheduled activity in a comprehensive preventative maintenance program.
- C. Techniques and methods for secure shipment of equipment and supplies.
- D. User responsibilities involved when sharing passwords in a secure environment.

Answer: A

Q68. At what stage of an assessment would an auditor test systems for weaknesses and attempt to defeat existing encryption, passwords and access lists?

- A. Penetration
- B. Control
- C. Audit planning
- D. Discovery

Answer: A

Q69. Controlling access to information systems and associated networks is necessary for the preservation of their:

- A. Authenticity, confidentiality, integrity and availability.
- B. Integrity and availability.
- C. Confidentiality, integrity and availability.
- D. Authenticity, confidentiality and availability.

Answer: C

Q70. The start of the LDAP (Lightweight Directory Access Protocol) directory is called the:

- A. Head
- B. Root
- C. Top
- D. Tree

Answer: B

Q71. What type of authentication may be needed when a stored key and memorized password are not strong enough and additional layers of security is needed?

- A. Mutual
- B. Multi-factor
- C. Biometric
- D. Certificate

Answer: B

Q72. Dave is increasing the security of his Web site by adding SSL (Secure Sockets Layer).

Which type of encryption does SSL use?

- A. Asymmetric
- B. Symmetric
- C. Public Key
- D. Secret

Answer: B

Q73. In context of wireless networks, WEP (Wired Equivalent Privacy) was designed to:

- A. Provide the same level of security as a wired LAN (Local Area Network).
- B. Provide a collision preventive method of media access.
- C. Provide a wider access area than that of wired LANs (Local Area Network).
- D. Allow radio frequencies to penetrate walls.

Answer: A

Q74. What are two common methods when using a public key infrastructure for maintaining access to servers in a network?

- A. ACL and PGP.
- B. PIM and CRL.
- C. CRL and OCSP.
- D. RSA and MD2

Answer: C

Q75. What is the greatest benefit to be gained through the use of S/MIME (Secure Multipurpose Internet Mail Extension)? The ability to:

- A. Encrypted and digitally sign e-mail messages.

- B. Send anonymous e-mails.
- C. Send e-mails with a return receipt.
- D. Expedite the delivery of e-mail.

Answer: A

Q76. While performing a routing site audit of your wireless network, you discover an unauthorized Access Point placed on your network under the desk of Accounting department security. When questioned, she denies any knowledge of it, but informs you that her new boyfriend has been to visit her several times, including taking her to lunch one time.

What type of attack have you just become a victim of?

- A. SYN Flood.
- B. Distributed Denial of Service.
- C. Man in the Middle attack.
- D. TCP Flood.
- E. IP Spoofing.
- F. Social Engineering
- G. Replay attack
- H. Phone tag
- I. Halloween attack

Answer: F

Q77. A collection of information that includes login, file access, other various activities, and actual or attempted legitimate and unauthorized violations is a(n):

- A. Audit
- B. ACL (Access Control List)
- C. Audit trail
- D. Syslog

Answer: C

Q78. You are the first person to respond to the scene of an incident involving a computer being hacked. After determining the scope of the crime scene and securing it, you attempt to preserve evidence at the scene.

Which of the following tasks will you perform to preserve evidence? (Choose all that apply.)

- A. Photograph any information displayed on the monitors of computers involved in the incident.
- B. Document any observation or messages displayed by the computer.
- C. Shut down the computer to prevent further attacks that may modify data.
- D. Gather up manuals, nonfunctioning devices, and other materials and equipment in the area so they are ready for transport.

Answer: A, B

Q79. A well defined business continuity plan must consist of risk and analysis, business impact analysis, strategic planning and mitigation, training and awareness, maintenance and audit and:

- A. Security labeling and classification.
- B. Budgeting and acceptance.
- C. Documentation and security labeling.
- D. Integration and validation.

Answer: D

Q80. Which of the following media types is most immune to RF (Radio Frequency) eavesdropping?

- A. Coaxial cable
- B. Fiber optic cable
- C. Twisted pair wire
- D. Unbounded

Answer: B

Q81. A piece of malicious code that can replicate itself has no productive purpose and exist only to damage computer systems or create further vulnerabilities is called a?

- A. Logic Bomb
- B. Worm
- C. Trojan Horse
- D. SYN flood
- E. Virus

Answer: E

Q82. How many bits are employed when using has encryption?

- A. 32
- B. 64
- C. 128
- D. 256

Answer: C

Q83. You are the first person to arrive at a crime scene. An investigator and crime scene technician arrive afterwards to take over the investigation.

Which of the following tasks will the crime scene technician be responsible for performing?

- A. Ensure that any documentation and evidence they possessed is handled over to the investigator.

- B. Reestablish a perimeter as new evidence presents itself.
- C. Establish a chain of command.
- D. Tag, bag, and inventory evidence.

Answer: D

Q84. Which of the following is an example of an asymmetric algorithm?

- A. CAST (Carlisle Adams Stafford Tavares)
- B. RC5 (Rivest Cipher 5)
- C. RSA (Rivest Shamir Adelman)
- D. SHA-1 (Secure Hashing Algorithm 1)

Answer: C

Q85. Honey pots are useful in preventing attackers from gaining access to critical system. True or false?

- A. True
- B. False
- C. It depends on the style of attack used.

Answer: A

Q86. You are researching the ARO and need to find specific data that can be used for risk assessment.

Which of the following will you use to find information?

- A. Insurance companies
- B. Stockbrokers
- C. Manuals included with software and equipment.
- D. None of the above. There is no way to accurately predict the ARO.

Answer: A

Q87. Data integrity is best achieved using a(n)

- A. Asymmetric cipher
- B. Digital certificate
- C. Message digest
- D. Symmetric cipher

Answer: C

Q88. In order for a user to obtain a certificate from a trusted CA (Certificate Authority), the user must present proof of identity and a:

- A. Private key
- B. Public key
- C. Password
- D. Kerberos key

Answer: B

Q89. Which of the following is a technical solution that supports high availability?

- A. UDP (User Datagram Protocol)
- B. Anti-virus solution
- C. RAID (Redundant Array of Independent Disks)
- D. Firewall

Answer: C

Q90. You have decided to implement biometrics as part of your security system. Before purchasing a locking system that uses biometrics to control access to secure areas, you need to decide what will be used to authenticate users.

Which of the following options relies solely on biometric authentication?

- A. Username and password.
- B. Fingerprints, retinal scans, PIN numbers, and facial characteristics.
- C. Voice patterns, fingerprints, and retinal scans.
- D. Strong passwords, PIN numbers, and digital imaging.

Answer: C

Q91. Which of the following results in a domain name server resolving the domain name to a different and thus misdirecting Internet traffic?

- A. DoS (Denial of Service)
- B. Spoofing
- C. Brute force attack
- D. Reverse DNS (Domain Name Service)

Answer: B

Q92. Which two of the following are symmetric-key algorithms used for encryption?

- A. Stream-cipher
- B. Block
- C. Public
- D. Secret

Answer: A, B

Q93. While connected from home to an ISP (Internet Service Provider), a network administrator performs a port scan against a corporate server and encounters four open TCP (Transmission Control Protocol) ports: 25, 110, 143 and 389. Corporate users in the organization must be able to connect from home, send and receive messages on the Internet, read e-mail by means of the IMAPv.4 (Internet Message Access Protocol version 4) protocol, and search into a directory services database for user e-mail addresses, and digital certificates. All the e-mail related services, as well as the directory server, run on the scanned server.

Which of the above ports can be filtered out to decrease unnecessary exposure without affecting functionality?

- A. 25
- B. 110
- C. 143
- D. 389

Answer: B

Q94. A high profile company has been receiving a high volume of attacks on their web site. The network administrator wants to be able to collect information on the attacker(s) so legal action can be taken.

What should be implemented?

- A. A DMZ (Demilitarized Zone)
- B. A honey pot
- C. A firewall
- D. A new subnet

Answer: B

Q95. When a session is initiated between the Transport Control Program (TCP) client and server in a network, a very small buffer space exists to handle the usually rapid "hand-shaking" exchange of messages that sets up the session.

What kind of attack exploits this functionality?

- A. Buffer Overflow
- B. SYN Attack
- C. Smurf
- D. Birthday Attack

Answer: B

Q96. A primary drawback to using shared storage clustering for high availability and disaster recovery is:

- A. The creation of a single point of vulnerability.

- B. The increased network latency between the host computers and the RAID (Redundant Array of Independent Disk) subsystem.
- C. The asynchronous writes which must be used to flush the server cache.
- D. The highest storage capacity required by the RAID (Redundant Array of Independent Disks) subsystem.

Answer: A

Q97. What kind of attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss but the lack of legitimate use of that system?

- A. CRL
- B. DOS
- C. ACL
- D. MD2

Answer: B

Q98. A problem with air conditioning is causing fluctuations in temperature in the server room. The temperature is rising to 90 degrees when the air conditioner stops working, and then drops to 60 degrees when it starts working again.

The problem keeps occurring over the next two days. What problem may result from these fluctuations? (Select the best answer.)

- A. Electrostatic discharge
- B. Power outages
- C. Chip creep
- D. Poor air quality

Answer: C

Q99. In order to establish a secure connection between headquarters and a branch office over a public network, the router at each location should be configured to use IPSec (Internet Protocol Security) in \_\_\_\_\_ mode.

- A. Secure
- B. Tunnel
- C. Transport
- D. Data link

Answer: B

Q100. Giving each user or group of users only the access they need to do their job is an example of which security principal.

- A. Least privilege
- B. Defense in depth

- C. Separation of duties
- D. Access control

Answer: A

Q101. When an ActiveX control is executed, it executes with the privileges of the:

- A. Current user account
- B. Administrator account
- C. Guest account
- D. System account

Answer: A

Q102. Which of the following is the best description of "separation of duties"?

- A. Assigning different parts of tasks to different employees.
- B. Employees are granted only the privileges necessary to perform their tasks.
- C. Each employee is granted specific information that is required to carry out the job function.
- D. Screening employees before assigning them to a position.

Answer: A

Explanation: A task needs several people involved as a method of checks and balances.

Q103. Which of the following is a popular VPN (Virtual Private Network) protocol operating at OSI (Open Systems Interconnect) model Layer 3?

- A. PPP (Point-to-Point Protocol)
- B. SSL (Secure Sockets Layer)
- C. L2TP (Layer Two Tunneling Protocol)
- D. IPSec (Internet Protocol Security)

Answer: D

Q104. The system administrator has just used a program that highlighted the susceptibility of several servers on the network to various exploits. The program also suggested fixes.

What type of program was used?

- A. Intrusion detection
- B. Port scanner
- C. Vulnerability scanner
- D. Trojan scanner

Answer: C

Q105. What fingerprinting technique relies on the fact that operating systems differ in the amount of information that is quoted when ICMP (Internet Control Message Protocol) errors are encountered?

- A. TCP (Transmission Control Protocol) options.
- B. ICMP (Internet Control Message Protocol) error message quenching.
- C. Fragmentation handling.
- D. ICMP (Internet Control Message Protocol) message quoting.

Answer: D

Explanation: **ICMP Message quoting:** The ICMP quotes back part of the original message with every ICMP error message. Each operating system will quote definite amount of message to the ICMP error messages. The peculiarity in the error messages received from various types of operating systems helps us in identifying the remote host's OS.

Q106. An extranet would be best defined as an area or zone:

- A. Set aside for business to store extra servers for internal use.
- B. Accessible to the general public for accessing the business' web site.
- C. That allows a business to securely transact with other businesses.
- D. Added after the original network was built for additional storage.

Answer: C

Explanation: An extranet is a private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company.

Q107. What authentication problem is addressed by single sign on?

- A. Authorization through multiple servers.
- B. Multiple domains.
- C. Multi-factor authentication.
- D. Multiple usernames and passwords.

Answer: D

Q108. An administrator is concerned with viruses in e-mail attachments being distributed and inadvertently installed on user's workstations. If the administrator sets up and attachment filter, what types of attachments should be filtered from e-mails to minimize the danger of viruses.

- A. Text file
- B. Image files
- C. Sound files
- D. Executable files

Answer: D

Q109. Which protocol is typically used for encrypting traffic between a web browser and web server?

- A. IPsec (Internet Protocol Security)
- B. HTTP (Hypertext Transfer Protocol)
- C. SSL (Secure Sockets Layer)
- D. VPN (Virtual Private Network)

Answer: C

Q110. Incorrectly detecting authorized access as an intrusion or attack is called a false:

- A. Negative
- B. Intrusion
- C. Positive
- D. Alarm

Answer: C

Q111. When hardening a machine against external attacks, what process should be followed when disabling services?

- A. Disable services such as DHCP (Dynamic Host Configuration Protocol) client and print servers from servers that do not use/serve those functions.
- B. Disable one unnecessary service after another, while reviewing the effects of the previous action.
- C. Research the services and their dependencies before disabling any default services.
- D. Disable services not directly related to financial operations.

Answer: C

Q112. Message authentication codes are used to provide which service?

- A. Integrity
- B. Fault recovery
- C. Key recovery
- D. Acknowledgement

Answer: A

Q113. IDEA (International Data Encryption Algorithm), Blowfish, RC5 (Rivest Cipher 5) and CAST-128 are encryption algorithms of which type?

- A. Symmetric
- B. Asymmetric
- C. Hashing
- D. Elliptic curve

Answer: A

Explanation: A few well-known examples of symmetric encryption algorithms are: DES, Triple-DES (3DES), IDEA, CAST-128, BLOWFISH, RC5, and TWOFISH.

Note: When using symmetric algorithms, both parties share the same key for en- and decryption. To provide privacy, this key needs to be kept secret. Once somebody else gets to know the key, it is not safe any more. Symmetric algorithms have the advantage of not consuming too much computing power.

Q114. An example of a physical access barrier would be:

- A. Video surveillance
- B. Personnel traffic pattern management
- C. Security guard
- D. Motion detector

Answer: C

Q115. Which of the following is likely to be found after enabling anonymous FTP (File Transfer Protocol) read/write access?

- A. An upload and download directory for each user.
- B. Detailed logging information for each user.
- C. Storage and distribution of unlicensed software.
- D. Fewer server connections and less network bandwidth utilization.

Answer: C

Q116. Currently, the most costly method of an authentication is the use of:

- A. Passwords
- B. Tokens
- C. Biometrics
- D. Shared secrets

Answer: C

Q117. Which systems should be included in a disaster recover plan?

- A. All systems.
- B. Those identified by the board of directors, president or owner.
- C. Financial systems and human resources systems.
- D. Systems identified in a formal risk analysis process.

Answer: D

Explanation: A preliminary risk analysis is performed to identify business critical applications and functions. Once those functions have been identified and documented, we prepared a structured approach to disaster recovery for the organization.

Q118. Security requirements for servers DO NOT typically include:

- A. The absence of vulnerabilities used by known forms of attack against server hosts.
- B. The ability to allow administrative activities to all users.
- C. The ability to deny access to information on the server other than that intended to be available.
- D. The ability to disable unnecessary network services that may be built into the operating system or server software.

Answer: B

Q119. An administrator of a web server notices many port scans to a server. To limit exposure and vulnerability exposed by these port scans the administrator should:

- A. Disable the ability to remotely scan the registry.
- B. Leave all processes running for possible future use.
- C. Close all programs or processes that use a UDP (User Datagram Protocol) or TCP (Transmission Control Protocol) port.
- D. Uninstall or disable any programs or processes that are not needed for the proper use of the server.

Answer: D

Q120. Privileged accounts are most vulnerable immediately after a:

- A. Successful remote login.
- B. Privileged user is terminated.
- C. Default installation is performed.
- D. Full system backup is performed.

Answer: B

Explanation: A fired domain admin could easily RAS or VPN in and wreck havoc if his/her privileged account is not disabled.

Q121. What is the advantage of a multi-homed firewall?

- A. It is relatively inexpensive to implement.
- B. The firewall rules are easier to manage.
- C. If the firewall is compromised, only the systems in the DMZ (Demilitarized Zone) are exposed.
- D. An attacker must circumvent two firewalls.

Answer: C

Q122. A password security policy can help a system administrator to decrease the probability that a password can be guessed by reducing the password's:

- A. Length
- B. Lifetime
- C. Encryption level
- D. Alphabet set

Answer: B

Q123. What is the best defence against man in the middle attacks?

- A. A firewall
- B. Strong encryption
- C. Strong authentication
- D. Strong passwords

Answer: C

Explanation: A man in the middle (MITM) attack, means that someone places himself in the communication channel between the two parties already at the time of certificate exchange. When a party sends its public key to the other, the MITM takes this key and replaces it by his own. The other party thinks the key just received came from the expected sender, but in fact it comes from the MITM. That's the reasons why public keys should be signed by a trusted authority (a.k.a. "trust center" or "certificate authority").

Q124. One of the most effective ways for an administrator to determine what security holes reside on a network is to:

- A. Perform a vulnerability assessment.
- B. Run a port scan.
- C. Run a sniffer.
- D. Install and monitor and IDS (Intrusion Detection System)

Answer: A

Q125. An inherent flaw of DAC (Discretionary Access Control) relating to security is:

- A. DAC (Discretionary Access Control) relies only on the identity of the user or process, leaving room for a Trojan horse.
- B. DAC (Discretionary Access Control) relies on certificates, allowing attackers to use those certificates.
- C. DAC (Discretionary Access Control) does not rely on the identity of a user, allowing anyone to use an account.
- D. DAC (Discretionary Access Control) has no known security flaws.

Answer: A

Q126. What is the most common method used by attackers to identify the presence of an 801.11b network?

- A. War driving
- B. Direct inward dialing
- C. War dialing
- D. Packet driving

Answer: A

Explanation: War driving is the practice of literally driving around looking for free connectivity from Wi-Fi networks.

Incorrect Answers:

- B: Does not apply.
- C: In war dialing combinations of numbers are tested to find network back doors via modem.
- D: Does not apply.

Q127. Analyzing log files after an attack has started as an example of:

- A. Active detection
- B. Overt detection
- C. Covert detection
- D. Passive detection

Answer: D

Explanation: Passive intrusion detection systems involve the manual review of event logs and application logs. The inspection involves analysis and detection of attack patterns in event log data.

Q128. A malformed MIME (Multipurpose Internet Mail Extensions) header can:

- A. Create a back door that will allow an attacker free access to a company's private network.
- B. Create a virus that infects a user's computer.
- C. Cause an unauthorized disclosure of private information.
- D. Cause an e-mail server to crash.

Answer: D

Q129. When a user digitally signs a document an asymmetric algorithm is used to encrypt:

- A. Secret passkeys
- B. File contents
- C. Certificates
- D. Hash results

Answer: D

Q130. The best way to harden an application that is developed in house is to:

- A. Use an industry recommended hardening tool.
- B. Ensure that security is given due considerations throughout the entire development process.
- C. Try attacking the application to detect vulnerabilities, then develop patches to fix any vulnerabilities found.
- D. Ensure that the auditing system is comprehensive enough to detect and log any possible intrusion, identifying existing vulnerabilities.

Answer: B

Q131. The best method to use for protecting a password stored on the server used for user authentication is to:

- A. Store the server password in clear text.
- B. Hash the server password.
- C. Encrypt the server password with asymmetric keys.
- D. Encrypt the server password with a public key.

Answer: B

Q132. During the digital signature process, asymmetric cryptography satisfied what security requirement?

- A. Confidentiality
- B. Access control
- C. Data integrity
- D. Authentication

Answer: D

Q133. Which encryption scheme relies on both the sender and receiver to use different keys to encrypt and decrypt messages?

- A. Symmetric
- B. Blowfish
- C. Skipjack
- D. Asymmetric

Answer: D

Explanation: Asymmetric Encryption is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt.

Incorrect Answers:

- A: In symmetric encryption the message can be encrypted and decrypted using the same key.

- B: Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA.
- C: Skipjack is the encryption algorithm contained in the Clipper chip, and it was designed by the NSA.

Q134. For system logging to be an effective security measure, an administrator must:

- A. Review the logs on a regular basis.
- B. Implement circular logging.
- C. Configure the system to shutdown when the logs are full.
- D. Configure SNMP (Simple Network Management Protocol) traps for logging events.

Answer: A

Q135. The most effective way an administrator can protect users from social engineering is:

- A. Education
- B. Implement personal firewalls.
- C. Enable logging on at user's desktops.
- D. Monitor the network with an IDS (Intrusion Detection System)

Answer: A

Explanation: **Social engineering:** An outside hacker's use of psychological tricks on legitimate users of a computer system, in order to gain the information (usernames and passwords) he needs to gain access to the system.

Q136. With regards to the use of Instant Messaging, which of the following type of attack strategies is effectively combated with user awareness training?

- A. Social engineering
- B. Stealth
- C. Ambush
- D. Multi-prolonged

Answer: A

Q137. The process by which remote users can make a secure connection to internal resources after establishing an Internet connection could correctly be referred to as:

- A. Channeling
- B. Tunneling
- C. Throughput
- D. Forwarding

Answer: B

Q138. Appropriate documentation of a security incident is important for each of the following reasons EXCEPT:

- A. The documentation serves as a lessons learned which may help avoid further exploitation of the same vulnerability.
- B. The documentation will server as an aid to updating policy and procedure.
- C. The documentation will indicate who should be fired for the incident.
- D. The documentation will server as a tool to assess the impact and damage for the incident.

Answer: C

Q139. How can an e-mail administrator prevent malicious users from sending e-mails from non-existent domains?

- A. Enable DNS (Domain Name Service) reverse lookup on the e-mail server.
- B. Enable DNS (Domain Name Service) forward lookup on the e-mail server.
- C. Enable DNS (Domain Name Service) recursive queries on the DNS (Domain Name Service) server.
- D. Enable DNS (Domain Name Service) reoccurring queries on the DNS (Domain Name Service)

Answer: A

Q140. A network attack that misuses TCP's (Transmission Control Protocol) three way handshake to overload servers and deny access to legitimate users is called a:

- A. Man in the middle.
- B. Smurf
- C. Teardrop
- D. SYN (Synchronize)

Answer: D

Q141. Which of the following options describes a challenge-response session?

- A. A workstation or system that generates a random challenge string that the user enters when prompted along with the proper PIN (Personal Identification Number).
- B. A workstation or system that generates a random login ID that the user enters when prompted along with the proper PIN (Personal Identification Number).
- C. A special hardware device that is used to generate random text in a cryptography system.
- D. The authentication mechanism in the workstation or system does not determine if the owner should be authenticated.

Answer: A

Q142. Assuring the recipient that a message has not been altered in transit is an example of which of the following:

- A. Integrity
- B. Static assurance
- C. Dynamic assurance
- D. Cyclical check sequence

Answer: A

Q143. A server placed into service for the purpose of attracting a potential intruder's attention is known as a:

- A. Honey pot
- B. Lame duck
- C. Teaser
- D. Pigeon

Answer: A

Explanation: A honeypot is a system which uses fake server and send alarms when some "bad guy" try to exploit some bug. The goal is to learn how black-hats probe for and exploit a system. By learning their tools and methods, you can then better protect your network and systems.

Q144. An organization is implementing Kerberos as its primary authentication protocol. Which of the following must be deployed for Kerberos to function properly?

- A. Dynamic IP (Internet Protocol) routing protocols for routers and servers.
- B. Separate network segments for the realms.
- C. Token authentication devices.
- D. Time synchronization services for clients and servers.

Answer: D

Explanation: Time synchronization is crucial because Kerberos uses server and workstation time as part of the authentication process.

Q145. The action of determining with operating system is installed on a system simply by analyzing its response to certain network traffic is called:

- A. OS (Operating System) scanning.
- B. Reverse engineering.
- C. Fingerprinting
- D. Host hijacking.

Answer: C

Q146. One of the factors that influence the lifespan of a public key certificate and its associated keys is the:

- A. Value of the information it is used to protect.
- B. Cost and management fees.
- C. Length of the asymmetric hash.
- D. Data available openly on the cryptographic system.

Answer: C

Q147. A DRP (Disaster Recovery Plan) typically includes which of the following:

- A. Penetration testing.
- B. Risk assessment.
- C. DoS (Denial of Service) attack.
- D. ACLs (Access Control List).

Answer: B

Q148. When a change to user security policy is made, the policy maker should provide appropriate documentation to:

- A. The security administrator.
- B. Auditors
- C. Users
- D. All staff.

Answer: D

Q149. A major difference between a worm and a Trojan horse program is:

- A. Worms are spread via e-mail while Trojan horses are not.
- B. Worms are self replicating while Trojan horses are not.
- C. Worms are a form of malicious code while Trojan horses are not.
- D. There is no difference.

Answer: B

Q150. A common algorithm used to verify the integrity of data from a remote user through the creation of a 128-bit hash from a data input is:

- A. IPSec (Internal Protocol Security)
- B. RSA (Rivest Shamir Adelman)
- C. Blowfish
- D. MD5 (Message Digest 5)

Answer: D

Explanation: The MD5 hashing algorithm that creates a 128-bit hash value.

Q151. A network administrator wants to restrict internal access to other parts of the network. The network restrictions must be implemented with the least amount of administrative overhead and must be hardware based.

What is the best solution?

- A. Implement firewalls between subnets to restrict access.
- B. Implement a VLAN (Virtual Local Area Network) to restrict network access.
- C. Implement a proxy server to restrict access.
- D. Implement a VPN (Virtual Private Network).

Answer: A

Q152. Which one of the following would most likely lead to a CGI (Common Gateway Interface) security problem?

- A. HTTP (Hypertext Transfer Protocol) protocol.
- B. Compiler or interpreter that runs the CGI (Common Gateway Interface) script.
- C. The web browser.
- D. External data supplied by the user.

Answer: D

Q153. What is the best method of reducing vulnerability from dumpster diving?

- A. Hiring additional security staff.
- B. Destroying paper and other media.
- C. Installing surveillance equipment.
- D. Emptying the trash can frequently.

Answer: B

Q154. SSL (Secure Sockets Layer) session keys are available in what two lengths?

- A. 40-bit and 64-bit.
- B. 40-bit and 128-bit.
- C. 64-bit and 128-bit.
- D. 128-bit and 1,024-bit.

Answer: B

Q155. Which of the following is expected network behaviour?

- A. Traffic coming from or going to unexpected locations.
- B. Non-standard or malformed packets/protocol violations.
- C. Repeated, failed connection attempts.
- D. Changes in network performance such as variations in traffic load.

Answer: D

Q156. Which of the following steps in the SSL (Secure Socket Layer) protocol allows for client and server authentication, MAC (Mandatory Access Control) and encryption algorithm negotiation, and selection of cryptographic keys?

- A. SSL (Secure Sockets Layer) alert protocol.
- B. SSL (Secure Sockets Layer) change cipher spec protocol.
- C. SSL (Secure Sockets Layer) record protocol.
- D. SSL (Secure Sockets Layer) handshake protocol.

Answer: D

Explanation: SSL Handshake Protocol

- run before any application data is transmitted
- provides mutual authentication
- establishes secret encryption keys
- establishes secret MAC keys

Q157. Which of the following correctly identifies some of the contents of an user's X.509 certificate?

- A. User's public key, object identifiers, and the location of the user's electronic identity.
- B. User's public key, the CA (Certificate Authority) distinguished name, and the type of symmetric algorithm used for encryption.
- C. User's public key, the certificate's serial number, and the certificate's validity dates.
- D. User's public key, the serial number of the CA (Certificate Authority) certificate, and the CRL (Certificate Revocation List) entry point.

Answer: B

Explanation: The X.509 standard defines what information can go into a certificate, and describes how to write it down (the data format). All X.509 certificates have the following data, in addition to the signature:

**Version:**

**Serial Number:** The entity that created the certificate, the CA, is responsible for assigning it a serial number to distinguish it from other certificates it issues.

**Signature Algorithm Identifier:**

**Issuer Name:** The X.500 name of the entity that signed the certificate. This is normally a CA. Using this certificate implies trusting the entity that signed this certificate.

**Validity Period:**

**Subject Name:**

**Subject Public Key Information:** This is the public key of the entity being named, together with an algorithm identifier which specifies which public key crypto system this key belongs to and any associated key parameters.

Reference: <http://csrc.nist.gov/pki/panel/santosh/tsld002.htm>

Q158. What is the best method of defence against IP (Internet Protocol) spoofing attacks?

- A. Deploying intrusion detection systems.
- B. Creating a DMZ (Demilitarized Zone).
- C. Applying ingress filtering to routers.
- D. There is not a good defense against IP (Internet Protocol) spoofing.

Answer: C

Explanation: IP Spoofing attacks that take advantage of the ability to forge (or "spoof") IP address can be prevented by implementing Ingress and Egress filtering on the network perimeter.

Q159. A need to know security policy would grant access based on:

- A. Least privilege
- B. Less privilege
- C. Loss of privilege
- D. Single privilege

Answer: A

Q160. Which tunneling protocol only works on IP networks?

- A. IPX
- B. L2TP
- C. PPTP
- D. SSH

Answer: B

Q161. What functionality should be disallowed between a DNS server and untrusted node?

- A. name resolutions
- B. reverse ARP requests
- C. system name resolutions
- D. zone transfers

Answer: D

Explanation: Users who can start zone transfers from your server can list all of the records in your zones.

Q162. Which access control method provides the most granular access to protected objects?

- A. Capabilities
- B. Access control lists
- C. Permission bits
- D. Profiles

Answer: B

Q163. The primary DISADVANTAGE of symmetric cryptography is:

- A. Speed
- B. Key distribution
- C. Weak algorithms
- D. Memory management

Answer: B

Explanation: In symmetric encryption the message can be encrypted and decrypted using the same key.

Q164. What port does SNMP use?

- A. 21
- B. 161
- C. 53
- D. 49

Answer: B

Explanation: SNMP uses UDP port 161

Q165. What port does TACACS use?

- A. 21
- B. 161
- C. 53
- D. 49

Answer: D

Explanation: TACACS uses both TCP and UDP port 49.

Q166. What would NOT improve the physical security of workstations?

- A. Lockable cases, keyboards, and removable media drives.
- B. Key or password protected configuration and setup.
- C. Password required to boot.
- D. Strong passwords.

Answer: A

Q167. What are the four major components of ISAKMP (Internet Security Association and Key Management Protocol)?

- A. Authentication of peers, threat management, communication management, and cryptographic key establishment.
- B. Authentication of peers, threat management, communication management, and cryptographic key establishment and management.
- C. Authentication of peers, threat management, security association creation and management cryptographic key establishment and management.
- D. Authentication of peers, threat management, security association creation and management and cryptographic key management.

Answer: C

Explanation: The four major functional components of ISAKMP are:

- Authentication of communications peers.
- Threat mitigation.
- Security association creation and management.
- Cryptographic key establishment and management.

Q168. An attacker can determine what network services are enabled on a target system by:

- A. Installing a rootkit on the target system.
- B. Checking the services file.
- C. Enabling logging on the target system.
- D. Running a port scan against the target system.

Answer: D

Q169. What type of attack CANNOT be detected by an IDS (Intrusion Detection System)?

- A. DoS (Denial of Service)
- B. Exploits of bugs or hidden features
- C. Spoofed e-mail
- D. Port scan

Answer: C

Q170. Which of the following provides privacy, data integrity and authentication for handles devices in a wireless network environment?

- A. WEP (Wired Equivalent Privacy)
- B. WAP (Wireless Application Protocol)
- C. WSET (Wireless Secure Electronic Transaction)
- D. WTLS (Wireless Transport Layer Security)

Answer: D

Explanation: Short for Wireless Transport Layer Security. WTLS is the security layer of the WAP, providing privacy, data integrity and authentication for WAP services.

Not A: WEP is one of the most popular features available for a Wireless LAN. It is used to encrypt and decrypt data signals transmitted between Wireless LAN devices. In essence, WEP makes a wireless LAN link as secure as a wired link. However, WTLS

Q171. An effective method of preventing computer viruses from spreading is to:

- A. Require root/administrator access to run programs.
- B. Enable scanning of e-mail attachments.
- C. Prevent the execution of .vbs files.
- D. Install a host based IDS (Intrusion Detection System)

Answer: B

Q172. A PKI (Public Key Infrastructure) document that serves as the vehicle on which to base common interoperability standards and common assurance criteria on an industry wide basis is a certificate:

- A. Policy
- B. Practice
- C. Procedure
- D. Process

Answer: A

Q173. The integrity of a cryptographic system is considered compromised if which of the following conditions exist?

- A. A 40-bit algorithm is used for a large financial transaction.
- B. The public key is disclosed.
- C. The private key is disclosed.
- D. The validity of the data source is compromised.

Answer: C

Q174. The system administrator concerned about security has designated a special area in which to place the web server away from other servers on the network. This area is commonly known as the?

- A. Honey pot
- B. Hybrid subnet
- C. DMZ (Demilitarized Zone)
- D. VLAN (Virtual Local Area Network)

Answer: C

Explanation: A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network.

Q175. A document written by the CEO that outlines PKI use, management and deployment is a...

- A. PKI policy
- B. PKI procedure
- C. PKI practice
- D. best practices guideline

Answer: A

Explanation: Definition of Policy - course of action, guiding principle, or procedure considered expedient, prudent, or advantageous.

Q176. Which one does not use Smart Card Technology?

- A. CD Player
- B. Cell Phone
- C. Satellite Cards
- D. Handheld Computer

Answer: A

Q177. Regarding security, biometrics are used for.

- A. Accountability
- B. Certification
- C. Authorization
- D. Authentication

Answer: D

Q178. What is the most effective social engineering defence strategy?

- A. Marking of documents
- B. Escorting of guests
- C. Badge security system
- D. Training and awareness

Answer: D

Q179. Missing audit log entries most seriously affect an organization's ability to:

- A. Recover destroyed data.
- B. Legally prosecute an attacker.
- C. Evaluate system vulnerabilities.
- D. Create reliable system backups.

Answer: C

Explanation: The audit trail lets you detect suspicious activity from both outsiders and insiders and provides you with important evidence to use against intruders.

Q180. File encryption using symmetric cryptography satisfies what security requirement?

- A. Confidentiality
- B. Access control
- C. Data integrity
- D. Authentication

Answer: D

Q181. A security administrator tasked with confining sensitive data traffic to a specific subnet would do so by manipulating privilege policy based tables in the networks:

- A. Server
- B. Router
- C. VPN (Virtual Private Network)
- D. Switch

Answer: B

Q182. Security training should emphasize that the weakest links in the security of an organization are typically:

- A. Firewalls
- B. Policies
- C. Viruses
- D. People

Answer: D

Q183. IEEE (Institute of Electrical and Electronics Engineers) 802.11b is capable of providing data rates of to:

- A. 10 Mbps (Megabits per second)
- B. 10.5 Mbps (Megabits per second)
- C. 11 Mbps (Megabits per second)
- D. 12 Mbps (Megabits per second)

Answer: C

Q184. The standard encryption algorithm based on Rijndael is known as:

- A. AES (Advanced Encryption Standard)
- B. 3DES (Triple Data Encryption Standard)
- C. DES (Data Encryption Standard)
- D. Skipjack

Answer: A

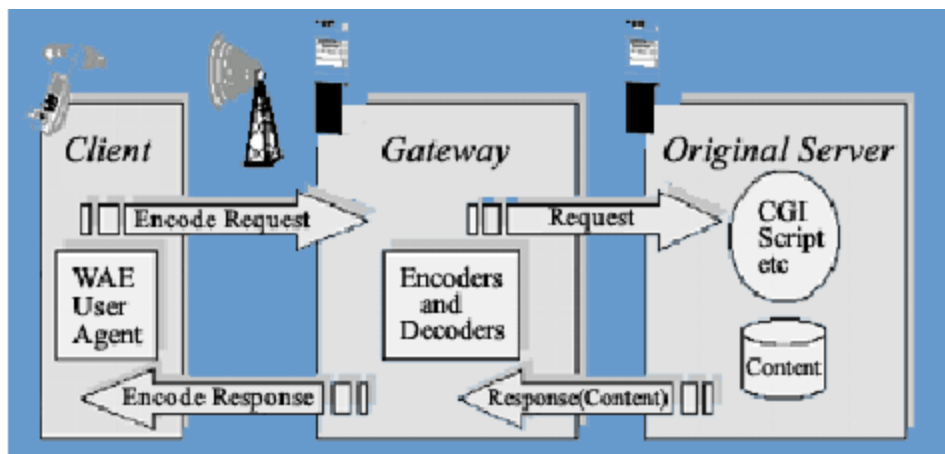
Explanation: Rijndael is a symmetric-key block cipher. After a competition Rijndael was selected as the successor to DES and became the Advanced Encryption Standard, or AES.

Q185. The WAP (Wireless Application Protocol) programming model is based on the following three elements:

- A. Client, original server, WEP (Wired Equivalent Privacy)
- B. Code design, code review, documentation
- C. Client, original server, wireless interface card
- D. Client, gateway, original server

Answer: D

Explanation: WAP programming model:



Q186. Technical security measures and countermeasures are primary intended to prevent:

- A. Unauthorized access, unauthorized modification, and denial of authorized access.
- B. Interoperability of the framework, unauthorized modification, and denial of authorized access.
- C. Potential discovery of access, interoperability of the framework, and denial of authorized access.
- D. Interoperability of the framework, unauthorized modification, and unauthorized access.

Answer: A

Q187. Poor programming techniques and lack of code review can lead to which of the following type of attack?

- A. CGI (Common Gateway Interface) script
- B. Birthday
- C. Buffer overflow

D. Dictionary

Answer: C

Q188. Security controls may become vulnerabilities in a system unless they are:

- A. Designed and implemented by the system vendor.
- B. Adequately tested.
- C. Implemented at the application layer in the system.
- D. Designed to use multiple factors of authentication.

Answer: B

Q189. Which of the following is NOT a characteristic of DEN (Directory Enabled Networking)?

- A. It is mapped into the directory defined as part of the LDAP (Lightweight Directory Access Protocol).
- B. It is inferior to SNMP (Simple Network Management Protocol).
- C. It is an object oriented information model.
- D. It is an industry standard indicating how to construct and store information about a network's users, applications and data.

Answer: B

Q190. A network attack method that uses ICMP (Internet Control Message Protocol) and improperly formatted MTUs (Maximum Transmission Unit) to crash a target computer is known as a:

- A. Man in the middle attack
- B. Smurf attack
- C. Ping of death attack
- D. TCP SYN (Transmission Control Protocol / Synchronized) attack

Answer: C

Explanation: The Ping of Death attack involved sending IP packets of a size greater than 65,535 bytes to the target computer. IP packets of this size are illegal, but applications can be built that are capable of creating them. Carefully programmed operating systems could detect and safely handle illegal IP packets, but some failed to do this.

Note: Packets that are bigger than the maximum size the underlying layer can handle (the MTU) are fragmented into smaller packets, which are then reassembled by the receiver. For ethernet style devices, the MTU is typically 1500.

Incorrect Answers:

- A: A man in the middle attack allows a third party to intercept and replace components of the data stream.
- B: The "smurf" attack, named after its exploit program, is one of the most recent in the category of network-level attacks against hosts. A perpetrator sends a large amount of

ICMP echo (ping) traffic at IP broadcast addresses, all of it having a spoofed source address of a victim.

D: In a TCP SYN attack a sender transmits a volume of connections that cannot be completed. This causes the connection queues to fill up, thereby denying service to legitimate TCP users.

Q191. Which of the following is considered the best technical solution for reducing the threat of a man in the middle attack?

- A. Virtual LAN (Local Area Network)
- B. GRE (Generic Route Encapsulation) tunnel IPIP (Internet Protocol-within-Internet Protocol Encapsulation Protocol)
- C. PKI (Public Key Infrastructure)
- D. Enforcement of badge system

Answer: C

Q192. Access controls based on security labels associated with each data item and each user are known as:

- A. MACs (Mandatory Access Control)
- B. RBACs (Role Based Access Control)
- C. LBACs (List Based Access Control)
- D. DACs (Discretionary Access Control)

Answer: A

Q193. What is NOT an acceptable use for smart card technology?

- A. Mobile telephones
- B. Satellite television access cards
- C. A PKI (Public Key Infrastructure) token card shared by multiple users
- D. Credit cards

Answer: C

Q194. Which of the following access control models introduces user security clearance and data classification?

- A. RBAC (Role Based Access Control).
- B. NDAC (Non-Discretionary Access Control).
- C. MAC (Mandatory Access Control).
- D. DAC (Discretionary Access Control).

Answer: C

Q195. A wireless network with three access points, two of which are used as repeaters, exists at a company. What step should be taken to secure the wireless network?

- A. Ensure that employees use complex passwords.
- B. Ensure that employees are only using issued wireless cards in their systems.
- C. Ensure that WEP (Wired Equivalent Privacy) is being used.
- D. Ensure that everyone is using adhoc mode.

Answer: C

Q196. How are clocks used in a Kerberos authentication system?

- A. The clocks are synchronized to ensure proper connections.
- B. The clocks are synchronized to ensure tickets expire correctly.
- C. The clocks are used to generate the seed value for the encryptions keys.
- D. The clocks are used to benchmark and set the optimal encryption algorithm.

Answer: B

Q197. What are three measures which aid in the prevention of a social engineering attack?

- A. education, limit available information and security policy.
- B. education, firewalls and security policy.
- C. security policy, firewalls and incident response.
- D. security policy, system logging and incident response.

Answer: A

Q198. Which of the following would be most effective in preventing network traffic sniffing?

- A. deploy an IDS (Intrusion Detection System).
- B. disable promiscuous mode.
- C. use hubs instead of routers.
- D. use switches instead of hubs.

Answer: D

Q199. Non-repudiation is based on what type of key infrastructure?

- A. symmetric.
- B. distributed trust.
- C. asymmetric.
- D. user-centric.

Answer: C

Q200. The first step in effectively implementing a firewall is:

- A. blocking unwanted incoming traffic.

- B. blocking unwanted outgoing traffic.
- C. developing a firewall policy.
- D. protecting against DDoS (Distributed Denial of Service) attacks.

Answer: C

Q201. LDAP (Lightweight Directory Access Protocol) requires what ports by default?

- A. 389 and 636
- B. 389 and 139
- C. 636 and 137
- D. 137 and 139

Answer: A

Q202. In the context of the Internet; what is tunneling? Tunneling is:

- A. using the Internet as part of a private secure network
- B. the ability to burrow through three levels of firewalls
- C. the ability to pass information over the internet within the shortest amount of time
- D. creating a tunnel which can capture data

Answer: A

Q203. Which of the following is required to use S/MIME (Secure Multipurpose Internet Mail Extensions)?

- A. digital certificate.
- B. server side certificate.
- C. SSL (Secure Sockets Layer) certificate.
- D. public certificate.

Answer: A

Q204. Non-repudiation is generally used to:

- A. protect the system from transmitting various viruses, worms and Trojan horses to other computers on the same network.
- B. protect the system from DoS (Denial of Service) attacks.
- C. prevent the sender or the receiver from denying that the communication between them has occurred.
- D. ensure the confidentiality and integrity of the communication.

Answer: C

Q205. Which of the following is typically included in a CRL (Certificate Revocation List)?

- A. certificates that have had a limited validity period and have expired.

- B. certificates that are pending renewal.
- C. certificates that are considered invalid because they do not contain a valid CA (Certificate Authority) signature.
- D. certificates that have been disabled before their scheduled expiration.

Answer: D

Q206. Company intranets, newsletters, posters, login banners and e-mails would be good tools to utilize in a security:

- A. investigation
- B. awareness program
- C. policy review
- D. control test

Answer: B

Q207. Using distinct key pairs to separate confidentiality services from integrity services to support non-repudiation describes which one of the following models?

- A. discrete key pair.
- B. dual key pair.
- C. key escrow.
- D. foreign key.

Answer: B

Q208. What IETF (Internet Engineering Task Force) protocol uses AH (Authentication Header) and ESP (Encapsulating Security Payload) to provide security in a networked environment?

- A. SSL (Secure Sockets Layer).
- B. IPSec (Internet Protocol Security).
- C. HTTPS (Secure Hypertext Transfer Protocol).
- D. SSH (Secure Shell).

Answer: B

Q209. Which of the following is the best IDS (Intrusion Detection System) to monitor the entire network?

- A. a network based IDS (Intrusion Detection System)
- B. a host based IDS (Intrusion Detection System)
- C. a user based IDS (Intrusion Detection System)
- D. a client based IDS (Intrusion Detection System)

Answer: A

Q210. One of the primary concerns of a centralized key management system is that

- A. keys must be stored and distributed securely
- B. certificates must be made readily available
- C. the key repository must be publicly accessible
- D. the certificate contents must be kept confidential

Answer: A

Q211. What has 160-Bit encryption?

- A. MD-5
- B. MD-4
- C. SHA-1
- D. Blowfish

Answer: C

Q212. A CPS (Certificate Practice Statement) is a legal document that describes a CA's (Certificate Authority):

- A. class level issuing process.
- B. copyright notice.
- C. procedures.
- D. asymmetric encryption schema.

Answer: C

Q213. FTP (File Transfer Protocol) is accessed through what ports?

- A. 80 and 443.
- B. 20 and 21.
- C. 21 and 23.
- D. 20 and 80.

Answer: B

Q214. In a typical file encryption process, the asymmetric algorithm is used to?

- A. encrypt symmetric keys.
- B. encrypt file contents.
- C. encrypt certificates.
- D. encrypt hash results.

Answer: A

Q215. An IT (Information Technology) security audit is generally focused on reviewing existing:

- A. resources and goals
- B. policies and procedures
- C. mission statements
- D. ethics codes

Answer: B

Q216. Instant Messaging is most vulnerable to:

- A. DoS (Denial of Service).
- B. fraud.
- C. stability.
- D. sniffing.

Answer: D

Q217. Loki, NetCaZ, Masters Paradise and NetBus are all considered what type of attack?

- A. brute force
- B. spoofing
- C. back door
- D. man in the middle

Answer: C

Q218. The use of embedded root certificates within web browsers is an example of which of the following trust models?

- A. bridge.
- B. mesh.
- C. hierarchy.
- D. trust list.

Answer: D

Q219. A security consideration that is introduced by a VPN (Virtual Private Network) is:

- A. an intruder can intercept VPN (Virtual Private Network) traffic and create a man in the middle attack.
- B. captured data is easily decrypted because there are a finite number of encryption keys.
- C. tunneled data CANNOT be authenticated, authorized or accounted for.
- D. a firewall CANNOT inspect encrypted traffic.

Answer: D

Q220. Impersonating a dissatisfied customer of a company and requesting a password change on the customer's account is a form of:

- A. hostile code.
- B. social engineering.
- C. IP (Internet Protocol) spoofing.
- D. man in the middle attack.

Answer: B

Q221. A system administrator discovers suspicious activity that might indicate a computer crime. The administrator should first:

- A. refer to incident response plan.
- B. change ownership of any related files to prevent tampering.
- C. move any related programs and files to non-erasable media.
- D. set the system time to ensure any logged information is accurate.

Answer: A

Q222. DDoS (Distributed Denial of Service) is most commonly accomplished by:

- A. internal host computers simultaneously failing.
- B. overwhelming and shutting down multiple services on a server.
- C. multiple servers or routers monopolizing and overwhelming the bandwidth of a particular server or router.
- D. an individual e-mail address list being used to distribute a virus.

Answer: C

Q223. Which is of greatest importance when considering physical security?

- A. reduce overall opportunity for an intrusion to occur
- B. make alarm identification easy for security professionals
- C. barricade all entry points against unauthorized entry
- D. assess the impact of crime zoning and environmental considerations in the overall design

Answer: A

Q224. An attack whereby two different messages using the same hash function produce a common message digest is also known as a:

- A. man in the middle attack.
- B. ciphertext only attack.
- C. birthday attack.
- D. brute force attack.

Answer: C

Q225. In a RBAC (Role Based Access Control) contexts, which statement best describes the relation between users, roles and operations?

- A. multiple users, single role and single operation.
- B. multiple users, single role and multiple operations.
- C. single user, single role and single operation.
- D. multiple users, multiple roles and multiple operations.

Answer: D

Q226. The flow of packets traveling through routers can be controlled by implementing what type of security mechanism?

- A. ACL (Access Control List)
- B. fault tolerance tables
- C. OSPF (Open Shortest Path First) policy
- D. packet locks

Answer: A

Q227. Which security architecture utilizes authentication header and/or encapsulating security payload protocols?

- A. IPSec (Internet Protocol Security).
- B. SSL (Secure Sockets Layer).
- C. TLS (Transport Layer Security).
- D. PPTP (Point-to-Point Tunneling Protocol).

Answer: A

Q228. The goal of TCP (transmission Control Protocol) hijacking is:

- A. taking over a legitimate TCP (transmission Control Protocol) connection
- B. predicting the TCP (transmission Control Protocol) sequence number
- C. identifying the TCP (transmission Control Protocol) port for future exploitation
- D. identifying source addresses for malicious use

Answer: A

Q229. What are the three entities of the SQL (Structured Query Language) security model?

- A. actions, objects and tables
- B. actions, objects and users
- C. tables, objects and users
- D. users, actions and tables

Answer: B

Q230. What is the greatest advantage to using RADIUS (Remote Authentication Dial-in User Service) for a multi-site VPN (Virtual Private Network) supporting a large population of remote users?

- A. RADIUS (Remote Authentication Dial-in User Service) provides for a centralized user database.
- B. RADIUS (Remote Authentication Dial-in User Service) provides for a decentralized user database.
- C. No user database is required with RADIUS (Remote Authentication Dial-in User Service).
- D. User database is replicated and stored locally on all remote systems.

Answer: A

Q231. Which of the following is the best protection against an intercepted password?

- A. VPN (Virtual Private Network).
- B. PPTP (Point-to-Point Tunneling Protocol).
- C. one time password.
- D. complex password requirement.

Answer: C

Q232. Which of the following is used to authenticate and encrypt IP (Internet Protocol) traffic?

- A. ESP (Encapsulating Security Payload)
- B. S/MIME (Secure Multipurpose Internet Mail Extensions)
- C. IPSec (Internet Protocol Security)
- D. IPv2 (Internet Protocol version 2)

Answer: C

Q233. An administrator is configuring a server to make it less susceptible to an attacker obtaining the user account passwords. The administrator decides to have the encrypted passwords contained within a file that is readable only by root. What is a common name for this file?

- A. passwd
- B. shadow
- C. hosts.allow
- D. hosts.deny

Answer: B

Q234. What port scanning technique is used to see what ports are in a listening state and then performs a two way handshake?

- A. TCP (transmission Control Protocol) SYN (Synchronize) scan

- B. TCP (transmission Control Protocol) connect scan
- C. TCP (transmission Control Protocol) fin scan
- D. TCP (transmission Control Protocol) null scan

Answer: A

Q235. When hosting a web server with CGI (Common Gateway Interface) scripts, the directories for public view should have:

- A. execute permissions
- B. read and write permissions
- C. read, write, and execute permissions
- D. full control permissions

Answer: A

Q236. When User A applies to the CA (Certificate Authority) requesting a certificate to allow the start of communication with User B, User A must supply the CA (Certificate Authority) with

- A. User A's public key only
- B. User B's public key only
- C. User A's and User B's public keys
- D. User A's and User B's public and private keys

Answer: A

Q237. Performing a security vulnerability assessment on systems that a company relies on demonstrates:

- A. that the site CAN NOT be hacked
- B. a commitment to protecting data and customers
- C. insecurity on the part of the organization
- D. a needless fear of attack

Answer: B

Q238. The Diffie-Hellman algorithm allows:

- A. access to digital certificate stores from s-certificate authority.
- B. a secret key exchange over an insecure medium without any prior secrets.
- C. authentication without the use of hashing algorithms.
- D. multiple protocols to be used in key exchange negotiations.

Answer: B

Q239. Which of the following type of attack CAN NOT be deterred solely through technical means?

- A. dictionary.
- B. man in the middle.
- C. DoS (Denial of Service).
- D. social engineering.

Answer: D

Q240. TCP/IP (transmission Control Protocol/Internet Protocol) hijacking resulted from exploitation of the fact that TCP/IP (transmission Control Protocol/Internet Protocol):

- A. has no authentication mechanism, thus allowing a clear text password of 16 bytes
- B. allows packets to be tunneled to an alternate network
- C. has no authentication mechanism, and therefore allows connectionless packets from anyone
- D. allows a packet to be spoofed and inserted into a stream, thereby enabling commands to be executed on the remote host

Answer: D

Q241. Intruders are detected accessing an internal network The source IP (Internet Protocol) addresses originate from trusted networks. The most common type of attack in this scenario in

- A. social engineering
- B. TCP/IP (Transmission Control Protocol/Internet Protocol) hijacking
- C. smurfing
- D. spoofing

Answer: D

Q242. A user wants to send e-mail and ensure that the message is not tampered with while in transit Which feature of modern cryptographic systems will facilitate this?

- A. confidentiality.
- B. authentication.
- C. integrity.
- D. non-repudiation.

Answer: C

Q243. What must be done to maximize the effectiveness of system logging?

- A. encrypt log files
- B. rotate log files
- C. print and copy log files
- D. review and monitor log files

Answer: D

Q244. Turnstiles, double entry doors and security guards are all prevention measures for which type of social engineering?

- A. piggybacking
- B. looking over a co-worker's shoulder to retrieve information
- C. looking through a co-worker's trash to retrieve information
- D. impersonation

Answer: A

Q245. WTLS (Wireless Transport Layer Security) provides security services between a mobile device and a:

- A. WAP (Wireless Application Protocol) gateway.
- B. web server.
- C. wireless client.
- D. wireless network interface card.

Answer: A

Q246. When a potential hacker looks through trash, the most useful items or information that might be found include all except:

- A. an IP (Internet Protocol) address.
- B. system configuration or network map.
- C. old passwords.
- D. system access requests.

Answer: D

Q247. A public key is a pervasive system whose services are implemented and delivered using public key technologies that include CAs (Certificate Authority), digital certificates, non-repudiation, and key history management.

- A. cryptography scheme.
- B. distribution authority.
- C. exchange.
- D. infrastructure.

Answer: D

Q248. In cryptographic operations, digital signatures can be used for which of the following systems?

- A. encryption.
- B. asymmetric key.

- C. symmetric and encryption.
- D. public and decryption.

Answer: B

Q249. Which of the following programs is able to distribute itself without using a host file?

- A. virus.
- B. Trojan horse.
- C. logic bomb.
- D. worm.

Answer: D

Q250. A network administrator is having difficulty establishing a L2TP (Layer Two Tunneling Protocol) VPN (Virtual Private Network) tunnel with IPsec (Internet Protocol Security) between a remote dial-up client and the firewall, through a perimeter router. The administrator has confirmed that the clients and firewall's IKE (Internet Key Exchange) policy and IPsec (Internet Protocol Security) policy are identical. The appropriate L2TP (Layer Two Tunneling Protocol) and IKE (Internet Key Exchange) transport layer ports have also been allowed on the perimeter router and firewall. What additional step must be performed on the perimeter router and firewall to allow AH (Authentication Header) and ESP (Encapsulating Security Payload) tunnel-encapsulated IPsec (Internet Protocol Security) traffic to flow between the client and the firewall?

- A. configure the perimeter router and firewall to allow inbound protocol number 51 for ESP (Encapsulating Security Payload) encapsulated IPsec (Internet Protocol Security) traffic
- B. configure the perimeter router and firewall to allow inbound protocol number 49 for ESP (Encapsulating Security Payload) encapsulated IPsec (Internet Protocol Security) traffic
- C. configure the perimeter router and firewall to allow inbound protocol numbers 50 and 51 for ESP (Encapsulating Security Payload) and AH (Authentication Header) encapsulated IPsec (Internet Protocol Security) traffic
- D. configure the perimeter router and firewall to allow inbound protocol numbers 52 and 53 for AH (Authentication Header) and ESP (Encapsulating Security Payload) encapsulated IPsec (Internet Protocol Security) traffic

Answer: C

Q251. Digital signatures can be used for which of the following?

- A. availability.
- B. encryption.
- C. decryption.
- D. non-repudiation.

Answer: D

Q252. The basic strategy that should be used when configuring the rules for secure

firewall is:

- A. permit all.
- B. deny all.
- C. default permit.
- D. default deny .

Answer: D

Q253. An employer gives an employee a laptop computer to use remotely. The user installs personal applications on the laptop and overwrites some system files. How might this have been prevented with minimal impact on corporate productivity?

- A. Users should not be given laptop computers in order to prevent this type of occurrence.
- B. The user should have received instructions as to what is allowed to be installed.
- C. The hard disk should have been made read only.
- D. Biometrics should have been used to authenticate the user before allowing software installation.

Answer: B

Q254. Which security method is in place when the administrator of a network enables access lists on the routers to disable all ports that are not used?

- A. MAC (Mandatory Access Control).
- B. DAC (Discretionary Access Control).
- C. RBAC (Role Based Access Control).
- D. SAC (Subjective Access Control).

Answer: A

Q255. Which of the following would NOT be considered a method for managing the administration of accessibility?

- A. DAC (Discretionary Access Control) list.
- B. SAC (Subjective Access Control) list.
- C. MAC (Mandatory Access Control) list.
- D. RBAC (Role Based Access Control) list.

Answer: B

Q256. Which of the following hash functions generates a 160-bit output?

- A. MD4 (Message Digest 4).
- B. MD5 (Message Digest5).
- C. UDES (Data Encryption Standard).
- D. SHA-1 (Secure Hashing Algorithm 1).

Answer: D

Q257. What is the first step before a wireless solution is implemented?

- A. ensure ad hoc mode is enabled on the access points.
- B. ensure that all users have strong passwords.
- C. purchase only Wi-Fi (Wireless Fidelity) equipment.
- D. perform a thorough site survey.

Answer: D

Q258. Intrusion detection systems typically consist of two parts, a console and as

- A. sensor
- B. router
- C. processor
- D. firewall

Answer: A

Q259. Which of the following keys is contained in a digital certificate?

- A. public key.
- B. private key.
- C. hashing key.
- D. session key.

Answer: A

Q260. An attacker attempting to penetrate a company's network through its remote access system would most likely gain access through what method?

- A. war dialer.
- B. Trojan horse.
- C. DoS (Denial of Service).
- D. worm.

Answer: A

Q261. A company's web server is configured for the following services: HTTP (Hypertext Transfer Protocol), SSL (Secure Sockets Layer), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol). The web server is placed into a DMZ (Demilitarized Zone). What are the standard ports on the firewall that must be opened to allow traffic to and from the server?

- A. 119,23,21,80.
- B. 443, 119,21,1250.
- C. 80,443,21,25.
- D. 80,443, 110,21.

Answer: C

Q262. An attacker manipulates what field of an IP (Internet Protocol) packet in an IP (Internet Protocol) spoofing attack?

- A. version field.
- B. source address field.
- C. source port field.
- D. destination address field.

Answer: B

Q263. Administrators currently use telnet to remotely manage several servers. Security policy dictates that passwords and administrative activities must not be communicated in clear text. Which of the following is the best alternative to using telnet?

- A. DES (Data Encryption Standard).
- B. S-Telnet.
- C. SSH (Secure Shell).
- D. PKI (Public Key Infrastructure).

Answer: C

Q264. How many characters should the minimum length of a password be to deter dictionary password cracks?

- A. 6.
- B. 8.
- C. 10.
- D. 12.

Answer: B

Q265. A VPN (Virtual Private Network) using IPSec (Internet Protocol Security) in the tunnel mode will provide encryption for the:

- A. one time pad used in handshaking.
- B. payload and message header.
- C. hashing algorithm and all e-mail messages.
- D. message payload only.

Answer: B

Q266. A DoS (Denial of Service) attack which takes advantage of TCP's (Transmission Control Protocol) three way handshake for new connections is known as:

- A. SYN (Synchronize) flood.

- B. ping of death attack.
- C. land attack.
- D. buffer overflow attack.

Answer: A

Q267. The Bell La-Padula access control model consists of four elements. These elements are

- A. subjects, objects, access modes and security levels.
- B. subjects, objects, roles and groups.
- C. read only, read/write, write only and read/write/delete.
- D. groups, roles, access modes and security levels.

Answer: A

Q268. How should a primary DNS (Domain Name Service) server be configured to provide the best security against DoS (Denial of Service) and hackers?

- A. disable the DNS (Domain Name Service) cache function.
- B. disable application services other than DNS (Domain Name Service).
- C. disable the DNS (Domain Name Service) reverse lookup function.
- D. allow only encrypted zone transfer to a secondary DNS (Domain Name Service) server.

Answer: B

Q269. What type of security process will allow others to verify the originator of an e-mail message?

- A. authentication.
- B. integrity.
- C. non-repudiation.
- D. confidentiality.

Answer: C

Q270. Which of the following protocols is used by web servers to encrypt data?

- A. TCP/IP (transmission Control Protocol/Internet Protocol)
- B. ActiveX
- C. IPSec (Internet Protocol Security)
- D. SSL (Secure Sockets Layer)

Answer: D

Q271. Of the following, what is the primary attribute associated with e-mail hoaxes?

- A. E-mail hoaxes create unnecessary e-mail traffic and panic in non-technical users.
- B. E-mail hoaxes take up large amounts of server disk space.
- C. E-mail hoaxes can cause buffer overflows on the e-mail server.
- D. E-mail hoaxes can encourage malicious users.

Answer: A

Q272. Most certificates used for authentication are based on what standard?

- A. 1S019278
- B. X.500
- C. RFC 1205
- D. X.509 v3

Answer: D

Q273. What type of security mechanism can be applied to modems to better authenticate remote users?

- A. firewalls
- B. encryption
- C. SSH (Secure Shell)
- D. callback

Answer: D

Q274. NAT (Network Address Translation) can be accomplished with which of the following?

- A. static and dynamic NAT (Network Address Translation) and PAT (Port Address Translation)
- B. static and hide NAT (Network Address Translation)
- C. static and hide NAT (Network Address Translation) and PAT (Port Address Translation)
- D. static, hide, and dynamic NAT (Network Address Translation)

Answer: C

Q275. In order for an SSL (Secure Sockets Layer) connection to be established between a web client and server automatically, the web client and server should have a(n):

- A. shared password
- B. certificate signed by a trusted root CA (Certificate Authority)
- C. address on the same subnet
- D. common operating system

Answer: B

Q276. Despite regular system backups a significant risk still exists if:

- A. recovery procedures are not tested
- B. all users do not log off while the backup is made
- C. backup media is moved to an off-site location
- D. an administrator notices a failure during the backup process

Answer: A

Q277. Malicious code is installed on a server that will e-mail system keystrokes stored in a text file to the author and delete system logs every five days or whenever a backup is performed. What type of program is this?

- A. virus.
- B. back door.
- C. logic bomb.
- D. worm.

Answer: C

Q278. The public key infrastructure model where certificates are issued and revoked via a CA (Certificate Authority) is what type of model?

- A. managed
- B. distributed
- C. centralized
- D. standard

Answer: C

Q279. The best reason to perform a business impact analysis as part of the business continuity planning process is to:

- A. test the veracity of data obtained from risk analysis
- B. obtain formal agreement on maximum tolerable downtime
- C. create the framework for designing tests to determine efficiency of business continuity plans
- D. satisfy documentation requirements of insurance companies covering risks of systems and data important for business continuity

Answer: B

Q280. A FEP (File Transfer Protocol) bounce attack is generally used to

- A. exploit a buffer overflow vulnerability on the FTP (File Transfer Protocol) server
- B. reboot the FTP (File Transfer Protocol) server
- C. store and distribute malicious code
- D. establish a connection between the FTP (File Transfer Protocol) server and another computer

Answer: D

Q281. A security designer is planning the implementation of security mechanisms in a RBAC (Role Based Access Control) compliant system. The designer has determined that there are three types of resources in the system including files, printers, and mailboxes. The organization has four distinct departments with distinct functions including Sales, Marketing, Management, and Production. Each department needs access to different resources. Each user has a workstation. Which roles should be created to support the RBAC (Role Based Access Control) model?

- A. file, printer, and mailbox roles
- B. sales, marketing, management, and production roles
- C. user and workstation roles
- D. allow access and deny access roles

Answer: B

Q282. Malicious port scanning is a method of attack to determine which of the following?

- A. computer name
- B. the fingerprint of the operating system
- C. the physical cabling topology of a network
- D. user ID and passwords

Answer: B

Q283. What should be done to secure a DHCP (Dynamic Host Configuration Protocol) service?

- A. block ports 67 and 68 at the firewall.
- B. block port 53 at the firewall.
- C. block ports 25 and 26 at the firewall.
- D. block port 110 at the firewall.

Answer: A

Q284. As a security administrator, what are the three categories of active responses relating to intrusion detection?

- A. collect additional information, maintain the environment, and take action against the intruder
- B. collect additional information, change the environment, and alert the manager
- C. collect additional information, change the environment, and take action against the intruder
- D. discard any additional information, change the environment, and take action against the intruder

Answer: C

Q285. What protocol should be used to prevent intruders from using access points on a wireless network?

- A. ESP (Encapsulating Security Payload)
- B. WEP (Wired Equivalent Privacy)
- C. TLS (Transport Layer Security)
- D. SSL (Secure Sockets Layer)

Answer: B

Q286. What is the main advantage SSL (Secure Sockets Layer) has over HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer)?

- A. SSL (Secure Sockets Layer) offers full application security for HTITP (Hypertext Transfer Protocol) while H'ITPS (Hypertext Transfer Protocol over Secure Sockets Layer) does not.
- B. SSL (Secure Sockets Layer) supports additional application layer protocols such as FTP (File Transfer Protocol) and NNTP (Network News Transport Protocol) while HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer) does not.
- C. SSL (Secure Sockets Layer) and HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer) are transparent to the application.
- D. SSL (Secure Sockets Layer) supports user authentication and HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer) does not.

Answer: B

Q287. During the digital signature process, hashing provides a means to verify what security requirement?

- A. non-repudiation.
- B. access control. .
- C. data integrity.
- D. authentication.

Answer: C

Q288. Which of the following often requires the most effort when securing a server due to lack of available documentation?

- A. hardening the OS (Operating System)
- B. configuring the network
- C. creating a proper security policy
- D. installing the latest hot fixes and patches

Answer: A

Q289. In order for User A to send User B an e-mail message that only User B can read, User A must encrypt the e-mail with which of the following keys?

- A. User B's public key
- B. User B's private key
- C. User A's public key
- D. User A's private key

Answer: A

Q290. What does the message recipient use with the hash value to verify a digital signature?

- A. signer's private key
- B. receiver's private key
- C. signer's public key
- D. receiver's public key

Answer: C

Q291. As it relates to digital certificates, SSLv3.0 (Secure Sockets Layer version 3.0) added which of the following key functionalities? The ability to;

- A. act as a CA (Certificate Authority).
- B. force client side authentication via digital certificates.
- C. use x.400 certificates.
- D. protect transmissions with 1024-bit symmetric encryption.

Answer: B

Q292. In responding to incidents such as security breaches, one of the most important steps taken is:

- A. encryption.
- B. authentication.
- C. containment.
- D. intrusion.

Answer: C

Q293. SSL (Secure Sockets Layer) is used for secure communications with:

- A. file and print servers.
- B. RADIUS (Remote Authentication Dial-in User Service) servers.
- C. AAA (Authentication, Authorization, and Administration) servers.
- D. web servers.

Answer: D

Q294. Which of the following statements is true about network based IDSs (Intrusion

Detection System)?

- A. Network based IDSs (Intrusion Detection System) are never passive devices that listen on a network wire-without interfering with the normal operation of a network.
- B. Network based IDSs (Intrusion Detection System) are usually passive devices that listen on a network wire while interfering with the normal operation of a network.
- C. Network based IDSs (Intrusion Detection System) are usually intrusive devices that listen on a network wire while interfering with the normal operation of a network.
- D. Network based IDSs (Intrusion Detection System) are usually passive devices that listen on a network wire without interfering with the normal operation of a network.

Answer: D

Q295. What physical access control most adequately protects against physical piggybacking?

- A. man trap.
- B. security guard.
- C. CCTV (Closed-Circuit Television).
- D. biometrics.

Answer: A

Q296. Which of the following provides the strongest authentication?

- A. token
- B. username and password
- C. biometrics
- D. one time password

Answer: C

Q297. What is the best method to secure a web browser?

- A. do not upgrade, as new versions tend to have more security flaws.
- B. disable any unused features of the web browser.
- C. connect to the Internet using only a VPN (Virtual Private Network) connection.
- D. implement a filtering policy for illegal, unknown and undesirable sites.

Answer: B

Q298. What is the primary DISADVANTAGE of a third party relay?

- A. Spammers can utilize the relay.
- B. The relay limits access to specific users.
- C. The relay restricts the types of e-mail that maybe sent.
- D. The relay restricts spammers from gaining access.

Answer: A

Q299. A network administrator wants to connect a network to the Internet but does not want to compromise internal network IP (Internet Protocol) addresses. What should the network administrator implement?

- A. a honey pot
- B. a NAT (Network Address Translation)
- C. a VPN (Virtual Private Network)
- D. a screened network

Answer: B

Q300. Which of the following methods may be used to exploit the clear text nature of an instant-Messaging session?

- A. packet sniffing.
- B. port scanning. .
- C. cryptanalysis.
- D. reverse engineering.

Answer: A

Q301. A user receives an e-mail from a colleague in another company. The e-mail message warns of a virus that may have been accidentally sent in the past, and warns the user to delete a specific file if it appears on the user's computer. The user checks and has the file. What is the best next step for the user?

- A. Delete the file immediately.
- B. Delete the file immediately and copy the e-mail to all distribution lists.
- C. Report the contents of the message to the network administrator.
- D. Ignore the message. This is a virus hoax and no action is required.

Answer: C

Q302. When implementing Kerberos authentication, which of the following factors must be accounted for?

- A. Kerberos can be susceptible to man in the middle attacks to gain unauthorized access.
- B. Kerberos tickets can be spoofed using replay attacks to network resources.
- C. Kerberos requires a centrally managed database of all user and resource passwords.
- D. Kerberos uses clear text passwords.

Answer: C

Q303. Which of the following protocols is most similar to SSLv3 (Secure Sockets Layer version 3)?

- A. TLS (transport Layer Security).
- B. MPLS (Multi-Protocol Label Switching).
- C. SASL (Simple Authentication and Security Layer).
- D. MLS (Multi-Layer Switching).

Answer: A

Q304. A CRL (Certificate Revocation List) query that receives a response in near real time:

- A. indicates that high availability equipment is used.
- B. implies that a fault tolerant database is being used.
- C. does not guarantee that fresh data is being returned.
- D. indicates that the CA (Certificate Authority) is providing near real time updates.

Answer: C

Q305. Which of the following is a VPN (Virtual Private Network) tunneling protocol?

- A. AH (Authentication Header).
- B. SSH (Secure Shell).
- C. IPSec (Internet Protocol Security).
- D. DES (Data Encryption Standard).

Answer: C

Q306. What ports does FFP (File Transfer Protocol) use?

- A. 20 and 21.
- B. 25 and 110.
- C. 80 and 443.
- D. 161 and 162.

Answer: A

Q307. A decoy system that is designed to divert an attacker from accessing critical systems while collecting information about the attacker's activity, and encouraging the attacker to stay on the system long enough for administrators to respond is known as:

- A. DMZ (Demilitarized Zone).
- B. honey pot.
- C. intrusion detector.
- D. screened host.

Answer: B

Q308. What is the default transport layer protocol and port number that SSL (Secure Sockets Layer) uses?

- A. UDP (User Datagram Protocol) transport layer protocol and port 80
- B. TCP (Transmission Control Protocol) transport layer protocol and port 80
- C. TCP (Transmission Control Protocol) transport layer protocol and port 443
- D. UDP (User Datagram Protocol) transport layer protocol and port 69

Answer: C

Q309. The greater the keyspace and complexity of a password, the longer a attack may take to crack the password.

- A. dictionary
- B. brute force
- C. inference
- D. frontal

Answer: B

Q310. Which two protocols are VPN (Virtual Private Network) tunneling protocols?

- A. PPP (point-to-Point Protocol) and SLIP (Serial Line Internet Protocol).
- B. PPP (Point-to-Point Protocol) and PPTP (Point-to-Point Tunneling Protocol).
- C. L2TP (Layer Two Tunneling Protocol) and PPTP (Point-to-Point Tunneling Protocol).
- D. SMIP (Simple Mail Transfer Protocol) and L2TP (Layer Two Tunneling Protocol).

Answer: C

Q311. An e-mail is received alerting the network administrator to the presence of a virus on the system if a specific executable file exists. What should be the first course of action?

- A. Investigate the e-mail as a possible hoax with a reputable anti-virus vendor.
- B. Immediately search for and delete the file if discovered.
- C. Broadcast a message to the entire organization to alert users to the presence of a virus.
- D. Locate and download a patch to repair the file.

Answer: A

Q312. A minor configuration change which can help secure DNS (Domain Name Service) information is:

- A. block all unnecessary traffic by using port filtering.
- B. prevent unauthorized zone transfers.
- C. require password changes every 30 days.
- D. change the default password.

Answer: B

Q313. What determines if a user is presented with a dialog box prior to downloading an ActiveX component?

- A. the user's browser setting.
- B. the <script> meta tag.
- C. the condition of the sandbox.
- D. the negotiation between the client and the server.

Answer: A

Q314. ActiveX controls to prove where they originated.

- A. are encrypted.
- B. are stored on the web server.
- C. use SSL (Secure Sockets Layer).
- D. are digitally signed.

Answer: D

Q315. A virus that hides itself by intercepting disk access requests is:

- A. multipartite.
- B. stealth.
- C. interceptor.
- D. polymorphic.

Answer: B

Q316. Which of the following needs to be included in a SLA (Service Level Agreement) to ensure the availability of server based resources rather than guaranteed server performance levels?

- A. network
- B. hosting
- C. application
- D. security

Answer: B

Q317. When does CHAP (Challenge Handshake Authentication Protocol) perform the handshake process?

- A. when establishing a connection and at anytime after the connection is established.
- B. only when establishing a connection and disconnecting.
- C. only when establishing a connection.
- D. only when disconnecting.

Answer: A

Q318. Part of a fire protection plan for a computer room should include:

- A. procedures for an emergency shutdown of equipment.
- B. a sprinkler system that exceeds local code requirements.
- C. the exclusive use of non-flammable materials within the room.
- D. the fireproof doors that can be easily opened if an alarm is sounded.

Answer: A

Q319. Which of the following is an HTTP (Hypertext Transfer Protocol) extension or mechanism used to retain connection data, user information, history of sites visited, and can be used by attackers for spoofing an on-line identity?

- A. HTTPS (Hypertext Transfer Protocol over SSL).
- B. cookies.
- C. HTTP (Hypertext Transfer Protocol)/1.0 Caching.
- D. vCard v3.0.

Answer: B

Q320. What should a firewall employ to ensure that each packet is part of an established TCP (Transmission Control Protocol) session?

- A. packet filter.
- B. stateless inspection.
- C. stateful like inspection.
- D. circuit level gateway.

Answer: C

Q321. Which of the following is most commonly used by an intruder to gain unauthorized access to a system?

- A. brute force attack.
- B. key logging.
- C. Trojan horse.
- D. social engineering.

Answer: D

Q322. Management wants to track personnel who visit unauthorized web sites. What type of detection will this be?

- A. abusive detection.
- B. misuse detection.
- C. anomaly detection.
- D. site filtering.

Answer: B

Q323. Which of the following best describes TCP/IP (Transmission Control Protocol/Internet Protocol) session hijacking?

- A. The TCP/IP (Transmission Control Protocol/Internet Protocol) session state is altered in a way that intercepts legitimate packets and allow a third party host to insert acceptable packets.
- B. The TCP/IP (Transmission Control Protocol/Internet Protocol) session state is altered allowing third party hosts to create new IF (Internet Protocol) addresses.
- C. The TCP/IP (Transmission Control Protocol/Internet Protocol) session state remains unaltered allowing third party hosts to insert packets acting as the server.
- D. The TCP/IP (Transmission Control Protocol/Internet Protocol) session state remains unaltered allowing third party hosts to insert packets acting as the client.

Answer: A

Q324. What is a common DISADVANTAGE of employing an IDS (Intrusion Detection System)?

- A. false positives.
- B. throughput decreases.
- C. compatibility.
- D. administration.

Answer: A

Q325. System administrators and hackers use what technique to review network traffic to determine what services are running?

- A. sniffer.
- B. IDS (Intrusion Detection System).
- C. firewall.
- D. router.

Answer: A

Q326. What is a good practice in deploying a CA (Certificate Authority)?

- A. enroll users for policy based certificates.
- B. create a CPS (Certificate Practice Statement).
- C. register the CA (Certificate Authority) with a subordinate CA (Certificate Authority).
- D. create a mirror CA (Certificate Authority) for fault tolerance.

Answer: B

Q327. Single servers are frequently the targets of attacks because they contain:

- A. application launch scripts.
- B. security policy settings.
- C. credentials for many systems and users.
- D. master encryption keys.

Answer: C

Q328. Sensitive data traffic can be confined to workstations on a specific subnet using privilege policy based tables in as:

- A. router.
- B. server.
- C. modem.
- D. VPN (Virtual Private Network).

Answer: A

Q329. What is the most common goal of operating system logging?

- A. to determine the amount of time employees spend using various applications.
- B. to keep a record of system usage.
- C. to provide details of what systems have been compromised.
- D. to provide details of which systems are interconnected.

Answer: B

Q330. When a patch is released for a server the administrator should:

- A. immediately download and install the patch.
- B. test the patch on a non-production server then install the patch to production.
- C. not install the patch unless there is a current need.
- D. install the patch and then backup the production server.

Answer: B

Q331. An e-mail relay server is mainly used to:

- A. block all spam, which allows the e-mail system to function more efficiently without the additional load of spam.
- B. prevent viruses from entering the network.
- C. defend the primary e-mail server and limit the effects of any attack.
- D. eliminate e-mail vulnerabilities since all e-mail is passed through the relay first.

Answer: C

Q332. What network mapping tool uses ICMP (Internet Control Message Protocol)?

- A. port scanner.

- B. map scanner.
- C. ping scanner.
- D. share scanner.

Answer: C

Q333. Which of the following will let a security administrator allow only if ITP (Hypertext Transfer Protocol) traffic for outbound Internet connections and set permissions to allow only certain users to browse the web?

- A. packet filtering firewall.
- B. protocol analyzer.
- C. proxy server.
- D. stateful firewall.

Answer: C

Q334. The most common form of authentication is the use of:

- A. certificates.
- B. tokens.
- C. passwords.
- D. biometrics.

Answer: C

Q335. What are the three main components of a Kerberos server?

- A. authentication server, security database and privilege server.
- B. SAM (Sequential Access Method), security database and authentication server.
- C. application database, security database and system manager.
- D. authentication server, security database and system manager.

Answer: A

Q336. Which of the following IP (Internet Protocol) address schemes will require NAT (Network Address Translation) to connect to the Internet?

- A. 204.180.0.0/24
- B. 172.16.0.0/24
- C. 192.172.0.0/24
- D. 172.48.0.0/24

Answer: B

Q337. Which of the following is NOT a field of a X509 v.3 certificate?

- A. private key

- B. issuer
- C. serial number
- D. subject

Answer: A

Q338. Servers or workstations running programs and utilities for recording probes and attacks against them are referred to as:

- A. firewalls.
- B. host based IDS (Intrusion Detection System).
- C. proxies
- D. active targets.

Answer: B

Q339. To reduce vulnerabilities on a web server, an administrator should adopt which preventative measure?

- A. use packet sniffing software on all inbound communications.
- B. apply the most recent manufacturer updates and patches to the server.
- C. enable auditing on the web server and periodically review the audit logs.
- D. block all DNS (Domain Naming Service) requests coming into the server.

Answer: B

Q340. When a cryptographic system's keys are no longer needed, the keys should be:

- A. destroyed or stored in a secure manner
- B. deleted from the system's storage mechanism
- C. recycled
- D. submitted to a key repository

Answer: A

Q341. Which of the following terms represents a MAC (Mandatory Access Control) model?

- A. Lattice
- B. Bell La-Padula
- C. BIBA
- D. Clark and Wilson

Answer: A

Q342. LDAP (Lightweight Directory Access Protocol) directories are arranged as:

- A. linked lists.

- B. trees.
- C. stacks.
- D. queues.

Answer: B

Q343. Which of the following is the greatest problem associated with Instant Messaging?

- A. widely deployed and difficult to control.
- B. created without security in mind.
- C. easily spoofed.
- D. created with file sharing enabled.

Answer: B

Q344. The term cold site refers to:

- A. a low temperature facility for long term storage of critical data
- B. a location to begin operations during disaster recovery
- C. a facility seldom used for high performance equipment
- D. a location that is transparent to potential attackers

Answer: B

Q345. Sensitive material is currently displayed on a user's monitor. What is the best course of action for the user before leaving the area?

- A. The user should leave the area. The monitor is at a personal desk so there is no risk.
- B. turn off the monitor
- C. wait for the screen saver to start
- D. refer to the company's policy on securing sensitive data

Answer: D

Q346. The theft of network passwords without the use of software tools is an example of:

- A. Trojan programs.
- B. social engineering.
- C. sniffing.
- D. hacking.

Answer: B

Q347. An alternate site configured with necessary system hardware, supporting infrastructure and an on site staff able to respond to an activation of a contingency plan 24 hours a day, 7 days a week is a:

- A. cold site.

- B. warm site.
- C. mirrored site.
- D. hot site.

Answer: D

Q348. Which type of password generator is based on challenge-response mechanisms?

- A. asynchronous
- B. synchronous
- C. cryptographic keys
- D. smart cards

Answer: A

Q349. Which of the following is a characteristic of MACs (Mandatory Access Control):

- A. use levels of security to classify users and data
- B. allow owners of documents to determine who has access to specific documents
- C. use access control lists which specify a list of authorized users
- D. use access control lists which specify a list of unauthorized users

Answer: A

Q350. S/MIME (Secure Multipurpose Internet Mail Extensions) is used to:

- A. encrypt user names and profiles to ensure privacy
- B. encrypt messages and files
- C. encrypt network sessions acting as a VPN (Virtual Private Network) client
- D. automatically encrypt all outbound messages

Answer: B

Q351. What are three characteristics of a computer virus?

- A. find mechanism, initiation mechanism and propagate
- B. learning mechanism, contamination mechanism and exploit
- C. search mechanism, connection mechanism and integrate
- D. replication mechanism, activation mechanism and objective

Answer: D

Q352. Which of the following are tunneling protocols?

- A. IPSec (Internet Protocol Security), L2TP (Layer Two Tunneling Protocol), and SSL (Secure Sockets Layer)
- B. IPSec (Internet Protocol Security), L2TP (Layer Two Tunneling Protocol), and PPP (Point-to-Point Protocol)

- C. L2TP (Layer Two Tunneling Protocol), PPTP (Point-to-Point Tunneling Protocol), and SSL (Secure Sockets Layer)
- D. PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol), and IPSec (Internet Protocol Security)

Answer: D

Q353. What are TCP (Transmission Control Protocol) wrappers used for?

- A. preventing IP (Internet Protocol) spoofing
- B. controlling access to selected services
- C. encrypting TCP (Transmission Control Protocol) traffic
- D. sniffing TCP (Transmission Control Protocol) traffic to troubleshoot

Answer: B

Q354. A user logs onto a workstation using a smart card containing a private key. The user is verified when the public key is successfully factored with the private key. What security service is being provided?

- A. authentication.
- B. confidentiality.
- C. integrity.
- D. non-repudiation.

Answer: A

Q355. What technical impact may occur due to the receipt of large quantities of spam?

- A. DoS (Denial of Service).
- B. processor underutilization.
- C. reduction in hard drive space requirements.
- D. increased network throughput.

Answer: A

Q356. An administrator wants to set up a system for an internal network that will examine all packets for known attack signatures. What type of system will be set up?

- A. vulnerability scanner
- B. packet filter
- C. host based IDS (Intrusion Detection System)
- D. network based IDS (Intrusion Detection System)

Answer: D

Q357. A password management system designed to provide availability for a large number of users includes which of the following?

- A. self service password resets
- B. locally saved passwords
- C. multiple access methods
- D. synchronized passwords

Answer: A

Q358. What is a common type of attack on web servers?

- A. birthday.
- B. buffer overflow.
- C. spam.
- D. brute force.

Answer: B

Q359. While surfing the Internet a user encounters a pop-up window that prompts the user to download a browser plug-in. The pop-up window is a certificate which validates the identity of the plug-in developer. Which of the following best describes this type of certificate?

- A. software publisher certificate
- B. web certificate
- C. CA (Certificate Authority) certificate
- D. server certificate

Answer: A

Q360. What is the major reason that social engineering attacks succeed?

- A. strong passwords are not required
- B. lack of security awareness
- C. multiple logins are allowed
- D. audit logs are not monitored frequently

Answer: B

Q361. Which authentication protocol could be employed to encrypt passwords?

- A. PPTP (Point-to-Point Tunneling Protocol)
- B. SMTP (Simple Mail Transfer Protocol)
- C. Kerberos
- D. CHAP (Challenge Handshake Authentication Protocol)

Answer: D

Q362. Which protocol is used to negotiate and provide authenticated keying material for security associations in a protected manner?

- A. ISAKMP (Internet Security Association and Key Management Protocol)
- B. ESP (encapsulating Security Payload)
- C. 5511 (Secure Shell)
- D. SKEME (Secure Key Exchange Mechanism)

Answer: A

Q363. E-mail servers have a configuration choice which allows the relaying of messages from one e-mail server to another. An e-mail server should be configured to prevent e-mail relay because:

- A. untraceable, unwanted e-mail can be sent
- B. an attacker can gain access and take over the server
- C. confidential information in the server's e-mail boxes can be read using the relay
- D. the open relay can be used to gain control of nodes on additional networks

Answer: A

Q364. A mobile sales force requires remote connectivity in order to access shared files and e-mail on the corporate network. All employees in the sales department have laptops equipped with ethernet adapters. Some also have modems. What is the best remote access solution to allow all sales employees to access the corporate network?

- A. ISDN (Integrated Services Digital Network)
- B. dial-up
- C. SSL (Secure Sockets Layer)
- D. VPN (Virtual Private Network)

Answer: D

Q365. Which of the following four critical functions of a VPN (Virtual Private Network) restricts users from using resources in a corporate network?

- A. access control
- B. authentication
- C. confidentiality
- D. data integrity

Answer: A

Q366. How are honey pots used to collect information? Honey pots collect:

- A. IP (Internet Protocol) addresses and identity of internal users
- B. data on the identity, access, and compromise methods used by the intruder.
- C. data regarding and the identity of servers within the network.
- D. IP (Internet Protocol) addresses and data of firewalls used within the network.

Answer: B

Q367. How must a firewall be configured to only allow employees within the company to download files from a FTP (File Transfer Protocol) server?

- A. open port 119 to all inbound connections.
- B. open port 119 to all outbound connections.
- C. open port 20/21 to all inbound connections.
- D. open port 20/21 to all outbound connections.

Answer: D

Q368. Tunneling is best described as the act of encapsulating:

- A. encrypted/secure IF packets inside of ordinary/non-secure IF packets.
- B. ordinary/non-secure IF packets inside of encrypted/secure IP packets.
- C. encrypted/secure IP packets inside of encrypted/non-secure IF packets.
- D. ordinary/secure IF packets inside of ordinary/non-secure IF packets.

Answer: B

Q369. Clients in Company A can view web sites that have been created for them, but CANNOT navigate in them. Why might the clients not be able to navigate in the sites?

- A. The sites have improper permissions assigned to them.
- B. The server is in a DMZ (Demilitarized Zone).
- C. The sites have IP (Internet Protocol) filtering enabled.
- D. The server has heavy traffic.

Answer: A

Q370. An acceptable use policy signed by an employee can be interpreted as an employee's written for allowing an employer to search an employee's workstation.

- A. refusal.
- B. policy.
- C. guideline.
- D. consent.

Answer: D

Q371. What protocol can be used to create a VPN (Virtual Private Network)?

- A. PPP (Point-to-Point Protocol).
- B. PPTP (Point-to-Point Tunneling Protocol).
- C. SLIP (Serial Line Internet Protocol).
- D. ESLIP (Encrypted Serial Line Internet Protocol).

Answer: B

Q372. The information that governs and associates users and groups to certain rights to use, read, write, modify, or execute objects on the system is called a(n):

- A. public key ring.
- B. ACL (Access Control List).
- C. digital signature.
- D. CRL (Certificate Revocation Lists).

Answer: B

Q373. A fundamental risk management assumption is, computers can NEVER be completely.

- A. secure until all vendor patches are installed.
- B. secure unless they have a variable password.
- C. secure.
- D. secure unless they have only one user.

Answer: C

Q374. An administrator is setting permissions on a file object in a network operating system which uses DAC (Discretionary Access Control). The ACL (Access Control List) of the file follows:

Owner: Read,	Write, Execute	User A: Read,
Write, -	User B: -, -, - (None)	Sales: Read, -, -
Write, -	Other Read, Write, -	Marketing: -, -

User "A" is the only owner of the file. User "B" is a member of the Sales group. What effective permissions does User "B" have on the file with the above access list?

- A. User B has no permissions on the file.
- B. User B has read permissions on the file.
- C. User B has read and write permissions on the file.
- D. User B has read, write and execute permissions on the file.

Answer: A

Q375. A user who has accessed an information system with a valid user ID and password combination is considered a(n):

- A. manager
- B. user
- C. authenticated user
- D. security officer

Answer: C

Q376. Which security method should be implemented to allow secure access to a web page, regardless of the browser type or vendor?

- A. certificates with SSL (Secure Sockets Layer).
- B. integrated web with NOS (Network Operating System) security.
- C. SSL (Secure Sockets Layer) only.
- D. secure access to a web page is not possible.

Answer: A

Q377. The most common method of social engineering is:

- A. looking through users' trash for information
- B. calling users and asking for information
- C. e-mailing users and asking for information
- D. e-mail

Answer: B

Q378. Why are unique user IDs critical in the review of audit trails?

- A. They CANNOT be easily altered.
- B. They establish individual accountability.
- C. They show which files were changed.
- D. They trigger corrective controls.

Answer: B

Q379. A police department has three types of employees: booking officers, investigators, and judges. Each group of employees is allowed different rights to files based on their need. The judges do not need access to the fingerprint database, the investigators need read access and the booking officers need read/write access. The booking officer would need no access to warrants, while an investigator would need read access and a judge would need read/write access. This is an example of:

- A. DAC (Discretionary Access Control) level access control.
- B. RBAC (Role Based Access Control) level access control.
- C. MAC (Mandatory Access Control) level access control.
- D. ACL (Access Control List) level access control.

Answer: B

Q380. The main purpose of digital certificates is to bind a

- A. public key to the identity of the signer and recipient

- B. private key to the identity of the signer and recipient
- C. public key to the entity that holds the corresponding private key
- D. private key to the entity that holds the corresponding public key

Answer: C

Q381. A perimeter router is configured with a restrictive ACL (Access Control List). Which transport layer protocols and ports must be allowed in order to support L2TP (Layer Two Tunneling Protocol) and PPTP (Point-to-Point Tunneling Protocol) connections respectively, through the perimeter router?

- A. TCP (Transmission Control Protocol) port 635 and UDP (User Datagram Protocol) port 654
- B. TCP (Transmission Control Protocol) port 749 and UDP (User Datagram Protocol) port 781
- C. UDP (User Datagram Protocol) port 1701 and TCP (transmission Control Protocol) port 1723
- D. TCP (Transmission Control Protocol) port 1812 and UDP (User Datagram Protocol) port 1813

Answer: C

Q382. Digital certificates can contain which of the following items:

- A. the CA's (Certificate Authority) private key.
- B. the certificate holder's private key.
- C. the certificate's revocation information.
- D. the certificate's validity period.

Answer: D

Q383. The system administrator of the company has terminated employment unexpectedly. When the administrator's user ID is deleted, the system suddenly begins deleting files. This is an example of what type of malicious code?

- A. logic bomb
- B. virus
- C. Trojan horse
- D. worm

Answer: A

Q384. A network administrator has just replaced a hub with a switch. When using software to sniff packets from the networks, the administrator notices conversations the administrator's computer is having with servers on the network, but can no longer see conversations taking place between other network clients and servers. Given that the switch is functioning properly, what is the most likely cause of this?

- A. With the exception of broadcasts, switches do not forward traffic out all ports.

- B. The switch is setup with a VLAN (Virtual Local Area Network) utilizing all ports.
- C. The software used to sniff packets is not configured properly.
- D. The sniffer's Ethernet card is malfunctioning.

Answer: A

Q385. Which encryption key is used to verify a digital signature?

- A. the signer's public key.
- B. the signer's private key.
- C. the recipient's public key.
- D. the recipient's private key.

Answer: A

Q386. NetBus and Back Orifice are each considered an example of a(n):

- A. virus.
- B. illicit server.
- C. spoofing tool.
- D. allowable server.

Answer: B

Q387. Companies without an acceptable use policy may give their employees an expectation of

- A. intrusions
- B. audits
- C. privacy
- D. prosecution

Answer: C

Q388. Implementation of access control devices and technologies must fully reflect an organization's security position as contained in its:

- A. ACLs (Access Control List)
- B. access control matrixes
- C. information security policies
- D. internal control procedures

Answer: C

Q389. Searching through trash is used by an attacker to acquire data such as network diagrams, IP (Internet Protocol) address lists and:

- A. boot sectors.

- B. process lists.
- C. old passwords.
- D. virtual memory.

Answer: C

Q390. Discouraging employees from misusing company e-mail is best handled by:

- A. enforcing ACLs (Access Control List).
- B. creating a network security policy.
- C. implementing strong authentication.
- D. encrypting company e-mail messages.

Answer: B

Q391. Forging an IP (Internet Protocol) address to impersonate another machine is best defined as:

- A. TCP/IP (Transmission Control Protocol/Internet Protocol) hijacking.
- B. IF (Internet Protocol) spoofing.
- C. man in the middle.
- D. replay.

Answer: B

Q392. When setting password rules, which of the following would LOWER the level of security of a network?

- A. Passwords must be greater than six characters and consist at least one non-alpha.
- B. All passwords are set to expire at regular intervals and users are required to choose new passwords that have not been used before.
- C. Complex passwords that users CAN NOT remotely change are randomly generated by the administrator and given to users.
- D. After a set number of failed attempts the server will lock out any user account forcing the user to call the administrator to re-enable the account.

Answer: C

Q393. A severed T1 line is most likely to be considered in planning.

- A. data recovery.
- B. off site storage.
- C. media destruction.
- D. incident response.

Answer: D

Q394. An organization's primary purpose in conducting risk analysis in dealing with

computer security is:

- A. to identify vulnerabilities to the computer systems within the organization.
- B. to quantify the impact of potential threats in relation to the cost of lost business functionality.
- C. to identify how much it will cost to implement counter measures.
- D. to delegate responsibility.

Answer: B

Q395. Which of the following most accurately describes a DMZ (Demilitarized Zone)?

- A. an application program with a state that authenticates the user and allows the user to be categorized based on privilege
- B. a network between a protected network and an external network in order to provide an additional layer of security
- C. the entire area between the network of origin and the destination network.
- D. an application that allows the user to remove any offensive of an attacker

Answer: B

Q396. SSL (Secure Sockets Layer) operates between which two layers of the OSI (Open Systems Interconnection) model?

- A. application and transport
- B. transport and network
- C. network and data link
- D. data link and physical

Answer: A

Q397. What is a network administrator protecting against by ingress/egress filtering traffic as follows: Any packet coming into the network must not have a source address of the internal network. Any packet coming into the network must have a destination address from the internal network Any packet leaving the network must have a source address from the internal network. Any packet leaving the network must not have a destination address from the internal networks Any packet coming into the network or leaving the network must not have a source or destination address of a private address or an address listed in RFC1918 reserved space.

- A. SYN (Synchronize) flooding
- B. spoofing
- C. DoS (Denial of Service) attacks
- D. dictionary attacks

Answer: B

Q398. How must a firewall be configured to make sure that a company can communicate with other companies using SMTP (Simple Mail Transfer Protocol) e-mail?

- A. Open TCP (Transmission Control Protocol) port 110 to all inbound and outbound connections.
- B. Open UDP (User Datagram Protocol) port 110 to all inbound connections.
- C. Open UUP (User Datagram Protocol) port 25 to all inbound connections.
- D. Open TOP (Transmission Control Protocol) port 25 to all inbound and outbound connections.

Answer: D