Exam : SY0-101

Title : Security+

Ver : 04-11-05

QUESTION 1
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

Explanation:
There is no such thing as a SAC (Subjective Access Control) list.

QUESTION 2
Access control decisions are based on responsibilities that an individual user or process has in an organization.
This best describes:

A. MAC (Mandatory Access Control)
B. RBAC (Role Based Access Control)
C. DAC (Discretionary Access Control)
D. None of the above.

Answer: B

Explanation:
The RBAC model allows a user to act in a certain predetermined manner based on the role the user holds in the organization. Users can be assigned certain roles system wide.
Reference: Security + (SYBEX) page 12

QUESTION 3
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

Explanation:
The DAC model allows the owner of a resource to establish privileges to the information they own. The DAC model would allow a user to share a file or use a file that someone

else has shared. The DAC model establishes an ACL that identifies the users who have authorization to that information. This allows the owner to grant or revoke access to individuals or groups of individuals based on the situation. This model is dynamic in nature and allows information to be shared easily between users.
Reference: Security + (SYBEX) page 12

QUESTION 4
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

Explanation:
In a DAC model, network users have some flexibility regarding how information is accessed. This model allows users to dynamically share information with other users. The process allows a more flexible environment, but it increases the risk of unauthorized disclosure of information. Administrators will have a more difficult time ensuring that information access is controlled and that only appropriate access is given.
Reference: Security + (SYBEX) page 440

QUESTION 5
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

Explanation:
Access control lists enable devices in your network to ignore requests from specified users or systems, or grant certain network capabilities to them. ACLs allow a stronger set of access controls to be established in your network. The basic process of ACL control allows the administrator to design and adapt the network to deal with specific security threats.
Reference: Security + (SYBEX) page 235

QUESTION 6

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,-, - Marketing: -, Write, - Other Read, Write, -

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

Explanation:

The Owner is allowed to: Read, Write, & Execute

User A is allowed to: Read, Write, & -

Sales is allowed to: Read, -, -

Marketing is allowed to: -, Write, -

Others are allowed to: Red, Write, -

And User B is allowed to do nothing! -,-,-(None)

QUESTION 7

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

Explanation:

Each distinct department (sales, marketing, management, and production) has their own role in the company, which probably includes using the: filer server, print server, and mail server. So it would be wise to create roles for each department.

QUESTION 8

DAC (Discretionary Access Control) system operates which following statement:

A. Files that don't have an owner CAN NOT be modified.
B. The administrator of the system is an owner of each object.
C. The operating system is an owner of each object.
D. Each object has an owner, which has full control over the object.

Answer: D

Explanation:
The DAC model allows the owner of a resource to establish privileges to the information they own. The DAC model would allow a user to share a file or use a file that someone else has shared. The DAC model establishes an ACL that identifies the users who have authorized to that information. This allows the owner to grant or revoke access to individuals or group of individuals based on the situation. This model is dynamic in nature and allows information to be shared easily between users.
Reference: Security + (SYBEX) page 12

QUESTION 9

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

Explanation:
Mandatory Access Control is a strict hierarchical model usually associated with governments. All objects are given security labels known as sensitivity labels and are classified accordingly. Then all users are given specific security clearances as to what they are allowed to access.
Reference: Security + (SYBEX) page

QUESTION 10

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

Explanation:
The MAC model is a static model that uses a predefined set of access privileges to files on the system. The system administrator establishes these parameters and associates them with an account, files or resources. The MAC model can be very restrictive.
Reference: Security + (SYBEX) page 11

QUESTION 11
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

Explanation:
Mandatory Access Control is a strict hierarchical model, first developed by governments and it is based on classifying data on importance and categorizing data by department. Users receive specific security clearances to access this data. For instance, the most important piece of data would have the highest classification, where only the President would of that department would have access; while the least important resources would be classified at the bottom where everyone in the organization including the janitors could access it.

QUESTION 12
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

Explanation:
Mandatory Access Control is a strict hierarchical model, first developed by governments and it is based on classifying data on importance and categorizing data by department. Users receive specific security clearances to access this data. For instance, the most important piece of data would have the highest classification, where only the President would of that department would have access; while the least important resources would be classified at the bottom where everyone in the organization including the janitors could access it.

QUESTION 13
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

Explanation:
The word lattice is used to describe the upper and lower level bounds of a user' access permission.
1.2 Recognize and be able to differentiate and explain the following methods of authentication
* Kerberos
* CHAP (Challenge Handshake Authentication Protocol)
* Certificates
* Username / Password
* Tokens
* Multi-factor
* Mutual

QUESTION 14
Which type of password generator is based on challenge-response mechanisms?

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

Answer: A

Explanation:
An synchronous password generator, has an authentication server that generates a challenge (a large number or string) which is encrypted with the private key of the token device and has that token device's public key so it can verify authenticity of the request (which is independent from the time factor). That challenge can also include a hash of transmitted data, so not only can the authentication be assured; but also the data integrity.

QUESTION 15
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

Explanation:
A self service password reset is a system where if an individual user forgets their password, they can reset it on their own (usually by answering a secret question on a web prompt, then receiving a new temporary password on a pre-specified email address) without having to call the help desk. For a system with many users, this will significantly reduce the help desk call volume.

QUESTION 16
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

Explanation:
A one time password is simply a password that has to be changed every time you log on; effectively making any intercepted password good for only the brief interval of time before the legitimate user happens to login themselves. So by chance, if someone were to intercept a password it would probably already be expired, or be on the verge of expiration within a matter of hours.

QUESTION 17
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

Explanation:
A common authentication technique whereby an individual is prompted (the challenge) to provide some private information (the response). Most security systems that rely on smart cards are based on challenge-response. A user is given a code (the challenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.
Reference:
http://www.webopedia.com/TERM/C/challenge_response.html

QUESTION 18
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
Time synchronization is crucial because Kerberos uses server and workstation time as part of the authentication process.

QUESTION 19
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

Explanation:
The actual verification of a client's identity is done by validating an authenticator. The authenticator contains the client's identity and a timestamp.
To insure that the authenticator is up-to-date and is not an old one that has been captured by an attacker, the timestamp in the authenticator is checked against the current time. If the timestamp is not close enough to the current time (typically within five minutes) then the authenticator is rejected as invalid. Thus, Kerberos requires your system clocks to be loosely synchronized (the default is 5 minutes, but it can be adjusted in Version 5 to be whatever you want).
Reference:
http://www.faqs.org/faqs/kerberos-faq/general/section-22.html

---

QUESTION 20
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

Explanation:
If the key distribution centre is down, all of other systems dependent on those keys won't be able to function.

QUESTION 21
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

Explanation:
CHAP is commonly used to encrypt passwords. It provides for on-demand authentication within an ongoing data transmission, that is repeated at random intervals during a session. The challenge response uses a hashing function derived from the Message Digest 5 (MD5) algorithm.

QUESTION 22
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

Explanation:
Symmetric key authentication

QUESTION 23
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

Explanation:
CHAP performs the handshake process when first establishing a connection; and then at random intervals during the transaction session.

QUESTION 24
Regarding security, biometrics are used for.

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

Answer: D

Explanation:
Biometrics devices use physical characteristics to identify the user.
Reference: Security + (SYBEX) page 18

QUESTION 25
Currently, the most costly method of an authentication is the use of:

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

Answer: C

Explanation:
Biometrics
These technologies are becoming more reliable, and they will become widely used over the next few years. Many companies use smart cards as their primary method of access control. Implementations have been limited in many applications because of the high cost associated with these technologies.
Reference: Security + (SYBEX) page 265

QUESTION 26
Which of the following provides the strongest authentication?

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

Answer: C

Explanation:
Biometrics is the use of authenticating a user by scanning on of their unique physiological body parts. Just like in the movies, a user places their hand on a finger print scanner or they put their eyes against a retinal scanner. If the image matches what's on the database, it authenticates the user. Since a persons fingerprint, blood vessel print, or retinal image is unique the only way the system can authenticate is if the proper user is there. The only way an unauthorized user to get access is to physically kidnap the authorized user and force them through the system. For this reason, biometrics are the strongest (and the costliest) for of authentication.

QUESTION 27
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

Explanation:
Features that make web surfing more exciting like: ActiveX, Java, JavaScript, CGI scripts, and cookies all poise security concerns. Disabling them (which is as easy as setting your browser security level to High) is the best method of securing a web browser, since its simple, secure, and within every users reach.

QUESTION 28
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

Explanation:
Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system.
Reference: Security + (SYBEX) page 135

QUESTION 29
When a session is initiated between the Transport Control Program (TCP) client and server in a network, a very small buffer space exist 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

Explanation:
SYN flood is a DoS attack in which the hacker sends a barrage of SYN packets. The receiving station tries to respond to each SYN request for a connection, thereby tying up all the resources. All incoming connections are rejected until all current connections can be established. Change this if you want but in the SYN flood the hacker sends a SYN packet to the receiving station with a spoofed return address of some broadcast address on their network. The receiving station sends out this SYN packets (pings the broadcast address) which causes multiple servers or stations to respond to the ping, thus overloading the originator of the ping (the receiving station). Therefore, the hacker may send only 1 SYN packet, whereas the network of the attacked station is actually what does the barrage of return packets and overloads the receiving station.
Reference: Security + (SYBEX) page 530

QUESTION 30
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: MTU packets that are bigger than the maximum size the underlying layer can handle 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.

QUESTION 31
The action of determining which 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

Explanation:
Fingerprinting is the act of inspecting returned information from a server (ie. One method is ICMP Message quoting where 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.

QUESTION 32
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

Explanation:
Malicious port scanning is an attempt to find an unused port that the system won't acknowledge. Several programs now can use port scanning for advanced host detection and operating system fingerprinting. With knowledge of the operating system, the hacker can look up known vulnerabilities and exploits for that particular system.

QUESTION 33
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
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.

QUESTION 34
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

Explanation:
Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system. This exploitation is usually a result of a programming error in the development of the software.
Reference: Security + (SYBEX) page 135

QUESTION 35
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

Explanation:
SYN flood is a DoS attack in which the hacker sends a barrage of SYN packets. The receiving station tries to respond to each SYN request for a connection, thereby tying up all the resources. All incoming connections are rejected until all current connections can be established.
Reference: Security + (SYBEX) page 530

QUESTION 36
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 over whelming the bandwidth of a particular server or router.
D. an individual e-mail address list being used to distribute a virus.

Answer: C

Explanation:
A distributed denial of service attack takes place from within, and is usually the doing of a disgruntled worker. They set up a zombie software that takes over numerous servers, and routers within the network to overwhelm the systems bandwidth.
A and B are incorrect because a DDoS doesn't fail or shut down the servers, it merely compromises them.
Reference: Security + (SYBEX) page

QUESTION 37
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

Explanation:
The SYN flood attack works when a source system floods and end system with TCP SYN requests, but intentionally does not send out acknowledgements (ACK). Since TCP needs confirmation, the receiving computer is stuck with half-open TCP sessions, just waiting for acknowledgement so it can reset the port. Meanwhile the connection buffer is being overflowed, making it difficult or impossible for valid users to connect, therefore their service is denied.

QUESTION 38
As the Security Analyst for the Certkiller .com network, you become aware that your systems may be under attack. This kind of attack is a DoS attack and the exploit sends 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

Explanation:
Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system.
Reference: Security + (SYBEX) page 135

QUESTION 39
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

Explanation:
DOS attacks prevent access to resources by users authorized to use those resources. An attacker may attempt to bring down an e-commerce website to prevent or deny usage by legitimate customers.
Reference: Security + (SYBEX) page 53

QUESTION 40
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

Explanation:
Since backdoor's are publicly marketed/distributed software applications, they are characterized by having a trade name.

QUESTION 41
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

Explanation:
The TCP/IP (Transmission Control Protocol/Internet Protocol) session state is altered in a way that intercepts legitimate packets and allows a third party host to insert acceptable packets. Thus hijacking the conversation, and continuing the conversation under the disguise of the legitimate party, and taking advantage of the trust bond.

QUESTION 42
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 allows 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

Explanation:
A detailed site on how to hijack a TCP/IP a session can be found at:
http://staff.washington.edu/dittrich/talks/qsm-sec/script.html

---

QUESTION 43
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

Explanation:
TCP/IP's connection orientated nature, and lack of natural security makes it easy to hijack a session by spoofing.

QUESTION 44
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 RFC19lS reserved space.

A. SYN (Synchronize) flooding
B. spoofing
C. DoS (Denial of Service) attacks
D. dictionary attacks

Answer: B

Explanation:
By having strict addressing filters; an administrator prevents a spoofed address from gaining access.

QUESTION 45
Providing false information about the source of an attack is known as:

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

Answer: B

Explanation:
A spoofing attack is simple an attempt by someone or something masquerading as someone else. This type of attack is usually considered an access attack.
Reference: Security + (SYBEX) page 56

QUESTION 46
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

Explanation:
A spoofing attack is simply an attempt by someone or something masquerading as someone else.
Reference: Security + (SYBEX) page 56

QUESTION 47
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

Explanation:
IP Spoofing
A hacker trying to gain access to a network by pretending his or her machine has the same network address as the internal network.
Reference: Security + (SYBEX) page 515

QUESTION 48
Which of the following results in a domain name server resolving the domain name to a different and wrong IP (Internet Protocol) address and thus misdirecting Internet traffic?
A) DoS (Denial of Service)
B) Spoofing
C) brute force attack
D) reverse DNS (Domain Name Service)

Answer: B

Explanation:
Spoofing is when you forge the source address of traffic, so it appears to come from somewhere else, preferably somewhere safe and trustworthy. Web spoofing is a process where someone creates a convincing copy of a legitimate website or a portion of the world wide web, so that when someone enters a site that they think is safe, they end up communicating directly with the hacker. To avoid this you should rely on certificates, IPSEC, and set up a filter to block internet traffic with an internal network address.

QUESTION 49
Forging an IP (Internet Protocol) address to impersonate another machine is best defined as:

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

Answer: B

Explanation:
The word spoofing was popularized in the air-force. When a fighter jet notices an enemy missile (air-to-air or surface-to-air) coming, the pilot will fire off a flair or a chaff (depending on whether or not the missile is heat seeking or radar guided) to spoof (trick) the missile into going after the wrong target. IP spoofing works the same way, and is commonly used by computer hackers because it's easy to implement, it takes advantage of someone else's trust relationship, it makes it harder to identify the source of the true attack, and it focuses attention away to an innocent 3rd party.

QUESTION 50
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

Explanation:
Spoofing is the process of trying to deceive, or to spoof, someone into believing that a source address is coming from somewhere else.
Incorrect answers:
Social engineering deals with the human aspect of gaining access and passwords.
TCP/IP hijacking requires an existing session.
Smurfing is a legitimate kind of DoS attack, that does involve spoofing, however it doesn't match the above description.

QUESTION 51
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

Explanation:
A birthday attack is based on the principle that amongst 23 people, the probability of 2 of them having the same birthday is greater the 50%. By that rational if an attacker examines the hashes of an entire organizations passwords, they'll come up with some common denominators.

QUESTION 52
The greater the keyspace and complexity of a password, the longer an attack may take to crack the password.

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

Answer: B

Explanation:
A brute force attack is when a computer program try's EVERY single keystroke combination until it cracks the password. If you had a bike lock or a brief case with three combinations of numbers (0-9), there were 999 possible choices, so if you started at 000

and worked your way up you could attempt every number in about 20 minutes and eventually crack the lock. A computer keyboard has millions of possibilities, but since computers can enter thousands and even millions of keys a second, a brute force attack can be successful in a matter of hours. Each keyspace exponentially increases the possible answer choices, so passwords that are extremely short can be cracked within an hour but passwords beyond eight characters require time and computer resources that are usually beyond a brute force hackers patience and financial motives.

QUESTION 53

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

Explanation:
A dictionary attack is an attack which uses a dictionary of common words to attempt to find the password of a user.
Reference: Security + (SYBEX) page 58

QUESTION 54

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

Explanation:
A dictionary attack is a preliminary brute force attempt at guessing a password. Dictionary attacks work on the principle that most people choose a simple word or phrase as a password. By having a computer try every word, or phrase in a dictionary; most passwords can be hacked in a matter of hours. Since passwords become exponentially

more difficult to crack with each character, passwords greater then 8 characters consume excessive time and resources to crack.

QUESTION 55
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

Explanation:
The method used in these attacks places a piece of software between a server and the user. The software intercepts and then sends the information to the server. The server responds back to the software, thinking it is the legitimate client. The attacking software then sends this information on to the server, etc. The man in the middle software may be recording this information, altering it, or in some other way compromising the security of your system.
Reference: Security + (SYBEX) page 57

QUESTION 56
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

Explanation:
PKI is a two-key system. Messages are encrypted with a public key. Messages are decrypted with a private key. If you want to send an encrypted message to someone, you would request their public key. You would encrypt the message using their public key and send it to them. They would then use their private key to decrypt the message.
Reference: Security + (SYBEX) page 331

QUESTION 57
What is the best defense against man in the middle attacks?

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

Answer: B

QUESTION 58
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

A. Birthday
B. Brute force
C. Man-in-the-middle
D. Smurf

Answer: B

Explanation: Brute force attacks are performed with tools that cycle through many possible character, number, and symbol combinations to guess a password. Since the token allows offline checking of PIN, the cracker can keep trying PINS until it is cracked.

QUESTION 59
What is called an attach where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets?
A.) SYN flood attack
B.) Smurf attack
C.) Ping of Dead Attack
D.) Denial of Service (DOS) Attack

Answer: B

QUESTION 60
Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?
A.) Differential cryptanalysis
B.) Differential linear cryptanalysis
C.) Birthday attack
D.) Statistical attack

Answer: C
Attacks Against One-Way Hash Functions: A good hashing algorithm should not produce the same hash value for two different messages. If the algorithm does produce the same value for two distinctly different messages, this is referred to as a collision. If an attacker

finds an instance of a collision, he has more information to use when trying to break the cryptographic methods used. A complex way of attacking a one-way hash function is called the birthday attack. Now hold on to your had while we go through this -- it is a bit tricky. In standard statistics, a birthday paradox exists. It goes something like this:
How many people must be in the same room for the chance to be greater than even that another person has the same birthday as you?

Answer: 253
How many people must be in the same room for the chance to be greater than even that at least two people share the same birthday?

Answer: 23
This seems a bit backwards, but the difference is that in the first instance, you are looking for someone with a specific birthday date, which matches yours. In the second instance, you are looking for any two people who share the same birthday. There is a higher probability of finding two people who share a birthday than you finding another person sharing your birthday -- thus, the birthday paradox.
....This means that if an attacker has one hash value and wants to find a message that hashes to the same hash value, this process could take him years. However, if he just wants to find any two messages with the same hashing value, it could take him only a couple hours. .....The main point of this paradox and this section is to show how important longer hashing values truly are. A hashing algorithm that has a larger bit output is stronger and less vulnerable to brute force attacks like a birthday attack.

QUESTION 61
Which of the following attacks focus on cracking passwords?

A. SMURF
B. Spamming
C. Teardrop
D. Dictionary

Answer: D

Explanation:
Dictionaries may be used in a cracking program to determine passwords. A short dictionary attack involves trying a list of hundreds or thousands of words that are frequently chosen as passwords against several systems. Although most systems resist such attacks, some do not. In one case, one system in five yielded to a particular dictionary attack.

QUESTION 62
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

Explanation:
Viruses get into your computer in one of three ways. They may enter your computer on a contaminated floppy or CD-ROM, through e-mail, or as a part of another program.
Reference: Security + (SYBEX) page 76

QUESTION 63
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

Explanation:
In such a scenario the most rational answer is to tell your network administrator. Most network administrators don't have much to do most of the day, so they live for an opportunity like this.
Incorrect Answers:
Deleting the file wouldn't be good, because deleting a file doesn't necessarily eliminate a problem, as it could put it to your email trash folder, or to your recycle bin. This will give you a false sense of security, and work against the process of containment.
Copying the email to all distribution lists, is another mistake, because if indeed the email does contain a virus, you'll only spread it.
Ignoring the problem isn't a good problem, although virus hoaxes are common, all it takes is one real virus to cause a mini-disaster.

QUESTION 64
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

Explanation:
If a virus threat is for real, the major anti-virus players like Symantec, McAfee, or Sophos will know about it before you, and they will have details on their sites.
Incorrect answers:
Searching for and deleting a file is not only a waste of time with today's OS's complex directory systems, but its also ineffective. One can miss a file, the file could be hidden, the wrong file can be deleted, and worst of all: when you delete a file it doesn't realy get completely deleted, instead it gets sent to a 'recycle bin.'
Broadcasting an alert and creating panic isn't the right thing to do, because it will waste bandwidth, and perhaps terrorizing the users is the original intent of the attack.
The act of locating and downloading a patch isn't just time consuming, but there's a chance that the patch itself could be the virus, or the process of resetting the computer could activate the virus.

QUESTION 65
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

Explanation:
A worm is different from a virus. Worms reproduce themselves, are self-contained and do not need a host application to be transported. The Trojan Horse program may be installed as part of an installation process. They do not reproduce or self replicate.
Reference: Security + (SYBEX) page 83+85

QUESTION 66
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

Explanation:
Worms are dangerous because they can enter a system by exploiting a 'hole' in an operating system. They don't' need a host file, and they don't need any user intervention

to replicate by themselves. Some infamous worms were: Morris, Badtrans, Nimda, and Code Red.

QUESTION 67

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

Explanation:
A logic bomb is a special kind of virus or Trojan horse that is set to go off following a preset time interval, or following a pre-set combination of keyboard strokes. Some unethical advertisers use logic bombs to deliver the right pop-up advertisement following a keystroke, and some disgruntled employees set up logic bombs to go off to sabotage their companies computers if they feel termination is imminent.

QUESTION 68

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

QUESTION 69

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

Explanation:
A Trojan horse attaches itself to another file, such as a word processing document. Trojan horses may also arrive as part of an e-mail for free game, software, or other file. When the Trojan horse activates and performs its task, it infects all of the word processing or template files. Consequently, every new file will carry the Trojan horse. The Trojan horse may not be visible because it masks itself inside of a legitimate program.
Reference: Security + (SYBEX) page 80

QUESTION 70
A piece of code that appears to do something useful while performing a harmful and unexpected function like stealing passwords is a:

A. Virus
B. Logic bomb
C. Worm
D. Trojan horse

Answer: D

Explanation:
Trojan horses are programs that enter a system or network under the guise of another program. A Trojan Horse may be included as an attachment or as part of an installation program. The Trojan Horse could create a back door or replace a valid program during installation. The Trojan Program would then accomplish its mission under the guise of another program. Trojan Horses can be used to compromise the security of your system and they can exist on a system for years before they are detected.
Reference: Security + (SYBEX) page 84

QUESTION 71
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

Explanation:
A virus is a piece of software designed to infect a computer system. The virus may do nothing more than reside on the computer. A virus may also damage the data on your hard disk, destroy your operating system, and possibly spread to other systems.
Reference: Security + (SYBEX) page 76

QUESTION 72
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

Explanation:
A virus is a piece of software designed to infect a computer system. I can go into this further, but the answer is obvious.
Reference: Security + (SYBEX) page 76

QUESTION 73
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

Explanation:
A virus can do many things and including itself in a program is one of them. A virus is a program intended to damage a computer system.
Reference: Security + (SYBEX) page 533

QUESTION 74
A virus that hides itself by intercepting disk access requests is:

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

Answer: B

Explanation:
A stealth virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the stealth virus redirects commands around itself in order to avoid detection. An infected

file may report a file size different from what is actually present in order to avoid detection.
Reference: Security + (SYBEX) page 80

QUESTION 75
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

Explanation:
Replication mechanism: To replicate a virus needs to attach itself to the right code, where it can replicate and spread past security systems into other systems.
Activation mechanism: Most virus's require the user to actually do something. During the 80's and early 90's most virus's were activated when you booted from a floppy disk, or inserted a new floppy disk into an infected drive. Nowadays most computer virus's come as email forwards, and they require the user to execute.
Objective: Many virus's have no objective at all, but some have the objective to delete data, hog up memory, or crash the system.

QUESTION 76
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

Explanation:
The only preventative measure in dealing with social engineering attacks is to educate your users and staff to never give out passwords and user Ids over the phone, via e-mail, or to anyone who is not positively verified as being who they say they are.
Reference: Security + (SYBEX) page 87

QUESTION 77
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

Explanation:
Social engineering is a process where an attacker attempts to acquire information about your network and system by talking to people in the organization. A social engineering attack may occur over the phone, by e-mail, or by a visit.
Reference: Security + (SYBEX) page 87

QUESTION 78
Which of the following is most commonly used by an intruder to gain unauthorizedaccess to a system?

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

Answer: D

Explanation:
Social engineering is a process where an attacker attempts to acquire information about your network and system by talking to people in the organization. A social engineering attack may occur over the phone, by e-mail, or by a visit.
The answer is not written in the book, but the easiest way to gain information would be social engineering.
Reference: Security + (SYBEX) page 87

QUESTION 79
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

Explanation:
A seems to be the best answer. The other answers involving objects and social engineering are verbal attacks.

QUESTION 80
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

Explanation:
Social engineering is any means of using people to seek out information. These people practice espionage to: break in without detection, disguise themselves in, trick others into giving them access, or trick others into giving them information.

QUESTION 81
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

Explanation:
Because of human rights laws, it is unlawful to use technology to directly control people's emotions and behaviors. For this reason social engineering attacks can not be deterred through technical means.

QUESTION 82
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

Explanation:
Social engineering attacks work because of the availability heuristic, law of reciprocity, and law of consistency. In the past people have had experiences where a co-worker with a legitimate problem asked for help and been grateful for it. So by consistency, they feel the urge to help others again the way they've helped out somebody in the past. By availability, when someone asks for help, they associate that ask for help for every legitimate cry for help, and times when they needed help themselves and were helped; so

essentially they're being a good Samaritan. If an awareness program were to be implemented where employees could be aware of social engineering tactics, they would be more likely to think about them, and be more suspect of an attack when someone does ask for a favor. With this knowledge in intuition, an employee will make a smarter decision.

QUESTION 83

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

Explanation:
Social engineering is using deception to engineer human emotions into granting access.

QUESTION 84

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

Explanation:
Social engineering is a process where an attacker attempts to acquire information about your network and system by talking to people in the organization. A social engineering attack may occur over the phone, be e-mail, or by a visit.
Reference: Security + (SYBEX) page 87

QUESTION 85
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

Explanation:
The only preventative measure in dealing with social engineering attacks is to educate your users and staff to never give out passwords and user Ids over the phone, via e-mail, or to anyone who is not positively verified as being who they say they are.
Reference: Security + (SYBEX) page 87

QUESTION 86
What network mapping tool uses ICMP (Internet Control Message Protocol)?

A. port scanner.
B. map scanner.
C. ping scanner.
D. share scanner.

Answer: C

Explanation:
Ping confirms a connection by sending and receiving ICMP packets.

QUESTION 87
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

Explanation:
A TCP/IP network makes many of the ports available to outside users through the router. These ports will respond in a predictable manner when queried. An attacker can systematically query a network to determine which services and ports are open. This process is called port scanning, and it can reveal a great deal about your network. Port scans can be performed both internally and externally. Many routers, unless configured

appropriately, will let all of the protocols pass through them.
Reference: Security + (SYBEX) page 69

QUESTION 88
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

Explanation:
In SYN scanning, a TCP SYN packet is sent to the port(s) to be scanned. If the port responds with a TCP SYN ACK packet, then the port is listening. If it replies with a TCP RST packet, then it is not.

QUESTION 89
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

Explanation:
IPSec works at the network layer of the OSI layer model and is a key factor in VPNs.

QUESTION 90
Which tunneling protocol only works on IP networks?

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

Answer: C

Explanation:
Point-to-Point Tunneling Protocol
You can access a private network through the Internet or other public network by using a

virtual private network (VPN) connection with the Point-to-Point Tunneling Protocol (PPTP).
Developed as an extension of the Point-to-Point Protocol (PPP), PPTP tunnels and/or encapsulates, IP, IPX, or NetBEUI protocols inside of PPP datagrams
PPTP does not require a dial-up connection. It does, however, require IP connectivity between your computer and the server.
Not B: L2TP is an industry-standard Internet tunneling protocol with roughly the same functionality as the Point-to-Point Tunneling Protocol (PPTP). Like PPTP, L2TP encapsulates Point-to-Point Protocol (PPP) frames, which in turn encapsulate IP, IPX, or NetBEUI protocols

---

QUESTION 91
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

Explanation:
L2TP uses UDP port 1701 while PPTP uses TCP port 1723

QUESTION 92
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. SMTP (Simple Mail Transfer Protocol) and L2TP (Layer Two Tunneling Protocol).

Answer: C

Explanation:
PPTP and L2TP are both VPN tunneling protocols. L2TP is more sophisticated and gaining more popularity.

Incorrect answers:
PPP is an encapsulation protocol usually associate with ISDN and SLIP s an old protocol used for direct serial line connections between two computers.

QUESTION 93
A network administrator is having difficulty establishing aL2TP (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 All (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

Explanation:
The most secure firewall configuration is one in which the firewall permits only IKE and IPSec traffic to flow between the specific IP addresses of the peers. However, if these addresses are not static, or if there are many addresses, a less secure configuration might be required to permit IPSec and IKE traffic to flow between subnets.
When a firewall or filtering router exists between IPSec peers, it must be configured to forward IPSec traffic on UDP source and destination port 500, IP protocol 50 (ESP), or IP protocol 51 (AH).
Reference:
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/enus/dnsbj_ips_schx.asp

QUESTION 94
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
IPSec provides secure authentication and encryption of data and headers. IPSec can work in tunneling mode or transport mode. In tunneling mode, the data or payload and message headers are encrypted. Transport mode encrypts only the payload.
Reference: Security + (SYBEX) page 127

QUESTION 95
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

Explanation:
Point to point tunneling protocol was originally proposed by Microsoft and its associates and it works by embedding its very own network protocol within the TCP/IP packets.

QUESTION 96
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

Explanation:
It's obvious that L2TP and PPTP are tunneling protocols because the word tunneling is in

the acronyms for their name, but IPSec is also considered a tunneling protocol because it creates a secure tunnel connection.

QUESTION 97
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

Explanation:
Since RADIUS keeps its credentials and keys in a centralized database, it's ideal for a large population of remote users. RADIUS authenticates the dial-in user by means of a private symmetric key; and stores a user profile to grant user authorization.

QUESTION 98
What port does TACACS use?

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

Answer: D
TACACS uses both TCP and UDP port 49.

QUESTION 99
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

Explanation:

SSH uses port 22 and TCP for connections.
Reference: Security + (SYBEX) page 127

QUESTION 100
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

Explanation:
Secure Shell is like telnet in the sense that an administrator may enter commands into a remote server, except that it uses an encrypted and authenticated connection [(RSA) cryptography for connection and authentication; and IDEA, Blowfish, or DES for data stream encryption.] instead of Telnet's cleartext.

QUESTION 101
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

Explanation:
Internet Message Access Protocol is an email feature that is similar to POP3 but has the ability to search for key words while the messages are on the mail server. The current version of IMAP (IMAP4) uses port 143 and TCP for connection.
Reference: Security + (SYBEX) page 130

QUESTION 102
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.
Answers A

Explanation:
Using a 3rd party email relay can put you in an advantage of getting unnecessary spam. Anyone on the internet can relay an unsolicited email through an SMTP server, and the message will appear to be legitimate coming from the email server, and it makes it much more difficult to trace the spammer.

QUESTION 103
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
Answers B

Explanation:
Secure MIME (S/MIME) is a standard used for encrypting e-mail. S/MIME can also contain signature data. S/MIME provides encryption, integrity, and authentication when used in conjunction with PKI.
Reference: Security + (SYBEX) page 368

QUESTION 104
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

Explanation:
What differentiates S/MIME from MIME is that it uses RSA asymmetric encryption and it relies on a digital certificate for authentication.

QUESTION 105
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

Explanation:
Microsoft Exchange Server 5.0 & 5.5 had a vulnerability that made it suspect to crashes following a malformed MIME header. Patches have since been released.

QUESTION 106
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

Explanation:
Secure MIME (S/MIME) is a standard used for encrypting e-mail. S/MIME can also contain signature data. S/MIME provides encryption, integrity, and authentication when used in conjunction with PKI.
Reference: Security + (SYBEX) page 368

QUESTION 107
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
Secure MIME (S/MIME) is a standard used for encrypting e-mail. S/MIME can also contain signature data. S/MIME provides encryption, integrity, and authentication when used in conjunction with PKI.
Reference: Security + (SYBEX) page 368

QUESTION 108
What technical impact may occur due to the receipt of large quantifies of spam?

A. DoS (Denial of Service).

B. processor underutilization.
C. reduction in hard drive space requirements.
D. increased network throughput.

Answer: A

Explanation:
In systems where no email filters are set up, it is possible for some users to receive over a hundred unsolicited emails a day! If every user on a network received that much email, the human time necessary to sort through those emails will be Herculean. The system resources required to: process, download, and store such email can potentially reduce a networks availability to zero; thus denying service.

QUESTION 109
What statement is most true about viruses and hoaxes?

A. Hoaxes can create as much damage as a real virus.
B. Hoaxes are harmless pranks and should be ignored.
C. Hoaxes can help educate user about a virus.
D. Hoaxes carry a malicious payload and can be destructive.

Answer: A

Explanation: Hoaxes do have the possibility of causing as much damage as viruses. Many hoaxes instruct the recipient to forward the message to everyone that they know and thus causes network congestion and heavy e-mail activity. Hoaxes also often instruct the user to delete files on their computer that may cause their computer or a program to quit functioning.

QUESTION 110
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

Explanation:
Many newer viruses spread using email. The infected system includes an attachment to any e-mail that you send to another user. The recipient opens this file thinking it is something you legitimately sent them. When they open the file, the virus infects the

target system. Many times the virus is in an executable attachment.
Reference: Security + (SYBEX) page 78

QUESTION 111
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

Explanation:
Although answer choices B,C,D have a degree of truth to them; the BEST answer is A. Email hoaxes often create unnecessary traffic because they ask users to forward an email to everyone in address book, and whether it is a computer virus or a blind, crippled, starving, cancer victim child suffering from Herpes it creates undue panic and emotion in the work setting.

QUESTION 112
PGP uses which of the following to encrypt data?
A.) An asymmetric scheme
B.) A symmetric scheme
C.) a symmetric key distribution system
D.) An asymmetric key distribution

Answer: B

QUESTION 113
Which of the following mail standards relies on a "Web of Trust"?
A.) Secure Multipurpose Internet Mail extensions (S/MIME)
B.) Pretty Good Privacy (PGP)
C.) MIME Object Security Services (MOSS)
D.) Privacy Enhanced Mail (PEM)

Answer: B
"PGP does not use a hierarchy of Cas, or any type of formal trust certificates, but relies on a "web of trust" in its key management approach. Each user generates and distributes his or her public key, and users sign each other's public keys, which creates a community of users who trust each other. This is different than the CA approach where no one trusts each other, they only trust the CA.

QUESTION 114
Which of the following will let a security administrator allow only if HTP (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

Explanation:
A proxy server is a server that is situated between a client and a server; that intercessors requests. Proxy servers are used for two reasons:
• To filter requests, so a strict parent or company can prevent their kids or employees from viewing the wrong sties.
• The increase performance, so multiple users accessing the same information (like a school, or a library,) can fetch common information from the proxy server.

QUESTION 115
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

Explanation:
The symbol: *.* is known as a wild card mask, and just like in poker when a file matches a wild card anything goes. By deleting the wild card, it prevents ANY email server (including the SPAM servers) from relaying information.

QUESTION 116
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

Explanation:
An email relay will essentially make your mail server invisible to the internet, so you can protect yourself from port scans, virus's, and arbitrary access.

QUESTION 117
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

Explanation:
If someone can find a way to relay email through the relay server, they can send thousands of unsolicited emails a day without the recipients having a way to pinpoint the source.

QUESTION 118
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

Explanation:
Since only clear unencrypted text is being sent across the world through multitudes of WAN equipment and routers; it is easy for someone to sniff your conversation and eavesdrop on every single word you type.

QUESTION 119
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 UDP (User Datagram Protocol) port 25 to all inbound connections.
D. Open TCP (Transmission Control Protocol) port 25 to all inbound and outbound connections.

Answer: D

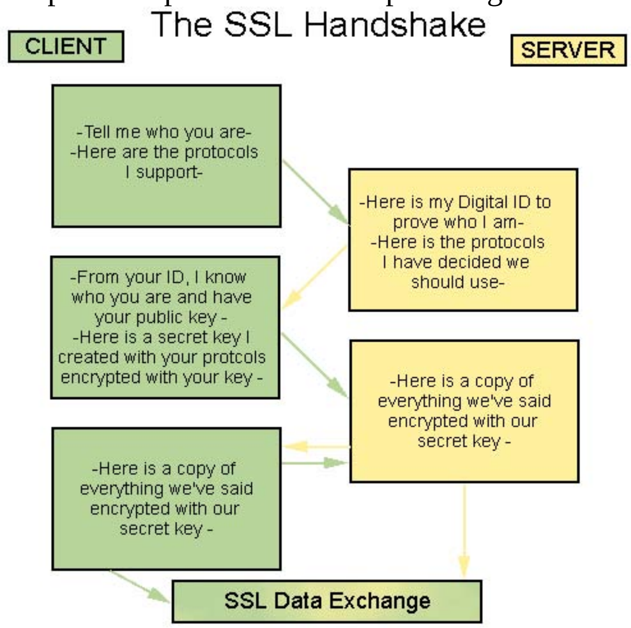
Explanation:
TCP port 25 is reserved for SMTP while port 110 is for POP3.

QUESTION 120
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

Explanation:
Graphical explanation of 6 steps to Digital Handshake for SSL


The SSL Handshake
CLIENT
SERVER
-Tell me who you are- -Here are the protocols I support-
-Here is my Digital ID to prove who I am- -Here is the protocols I have decided we should use-
-From your ID, I know who you are and have your public key - -Here is a secret key I created with your protcols encrypted with your key -
-Here is a copy of everything we've said encrypted with our secret key -
-Here is a copy of everything we've said encrypted with our secret key -
SSL Data Exchange

Note: The handshake begins when a browser connects to an SSL-enabled server, and asks the server to send back its identification, a digital certificate that usually contains the server name, the trusted certifying authority, and the server public encryption key. The browser can contact the server of the trusted certifying authority and confirm that the certificate is authentic before proceeding.

The browser then presents a list of encryption algorithms and hashing functions (used to generate a number from another); the server picks the strongest encryption that it also supports and notifies the client of the decision.

In order to generate the session keys used for the secure connection, the browser uses the server public key from the certificate to encrypt a random number and send it to the server. The client can encrypt this data, but only the server can decrypt it: this is the one fact that makes the keys hidden from third parties, since only the server and the client have access to this data.

The server replies with more random data (which doesn't have to be encrypted), and then both parities use the selected hash functions on the random data to generate the session keys. This concludes the handshake and begins the secured connection, which is encrypted and decrypted with the session keys.

The SSL handshake allows the establishment of a secured connection over an insecure channel. Even if a third party were to listen to the conversation, it would not be able to obtain the session keys. The process of creating good random numbers and applying hash functions can be quite slow, but usually the session keys are cached, so the handshake occurs only on the first connection between the parties.

This process works on top of HTTP, so its portable to any platform that supports it, and is in principle applicable to other protocols as well (Welling 2001, p.334). The process described is part of SSL version 2.0, but version 3.0 is supposed to replace it soon. Another standard, Transport Layer Security (TSL) is still in draft and is supposed to replace SSL in the future.

QUESTION 121

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

Explanation:

The Secure Socket Layer is used to establish a secure communication connection between two TCP-based machines. This protocol uses the handshake method. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key. The session is secure after this process.

Reference: Security + (SYBEX) page 365

QUESTION 122

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

Explanation: The Secure Sockets Layer (SSL) protocol uses both asymmetric and symmetric key exchange. It uses asymmetric keys for the SSL handshake. During the handshake, the master key, is encrypted with the receivers public passes from the client to the server. The client and server make their own session keys using the master key. The session keys encrypt and decrypt data for the remainder of the session. Symmetric key exchange occurs during the exchange of the cipher specification, or encryption level.

QUESTION 123

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
SSL Handshake Protocol
runs before any application data is transmitted
provides mutual authentication
establishes secret encryption keys
establishes secret MAC keys

QUESTION 124

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

Explanation:
The Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines.
Reference: Security + (SYBEX) page 365

QUESTION 125
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

Explanation:
The Secure Socket Layer is used to establish a secure communication connection between two TCP-based machines. This protocol uses the handshake method. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key. The session is secure after this process.
Reference: Security + (SYBEX) page 365

QUESTION 126
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

Explanation:
SSL comes in two strengths, 40-bit and 128-bit, which refer to the length of the "session key" generated by every encrypted transaction. The longer the key, the more difficult it is to break the encryption code.
Reference: http://wp.netscape.com/security/techbriefs/ssl.html

QUESTION 127
Which of the following is a protocol generally used for secure web transactions?

A. S/MIME (Secure Multipurpose Internet Mail Extensions)

B. XML (Extensible Makeup Language)
C. SSL (Secure Sockets Layer)
D. SMTP (Simple Mail Transfer Protocol)

Answer: C

Explanation:
The Secure Socket Layer is used to establish a secure communication connection between two TCP-based machines. This protocol uses the handshake method. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key. The session is secure after this process.
Reference: Security + (SYBEX) page 365

QUESTION 128
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 HTTP (Hypertext Transfer Protocol) while HTTPS (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.
Answers B

Explanation:
SSL on its own works at the session layer (layer 5) so it has more versatility in protocols that it supports.

QUESTION 129
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

Explanation:
For an SSL connection to compete, the web client and server should have a trusted certificate to confirm authenticity.
A shared password, address on the same subnet, and a common operating system are ludicrous answers because they defy the reason why SSL exists.

QUESTION 130
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

Explanation:
There are three versions of SSL out right now: SSL v.2, SSL v.3, and TLSv1 which is still going through standardization. SSL v.2 ensures encrypted data between client and serer. The server can authenticate the client, and the client can option to authenticate the server. SSL v.3 was enhanced for security and efficiency. It includes data compression, the ability of either the client or server requesting a renegotiation of the ciphers and shared key at any moment, and the use of certificate chains.

QUESTION 131
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

Explanation:
Secure Sockets Layer is secure, so it would be natural to assume that it uses the connection orientated TCP instead of UDP. Secondly, TCP port 80 is HTTP, which stands for (hyper text transfer protocol) TCP port 443 is HTTPS which stands for hyper text transfer protocol over secure socket layer'

QUESTION 132
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

Explanation:
Regardless of whether or not you use Netscape Navigator or Microsoft Internet Explorer, if you come across a page with a security certificate and an SSL connection (most likely for banking, investments, or purchases) you will have secure access.

QUESTION 133
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

Explanation:
SSL is associated with secure transactions (credit card purchases and online banking) over your web browser, so naturally it operates between the top two layers of the OSI model.

QUESTION 134
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

Explanation:
Answer A seems to be the most correct of these answer.
B. Is incorrect because IM client are not Trojan Horses, but they can be compromised by Trojan Horses.

C. Is incorrect because the answer would make IM secure.
D. All IM messaging system that transverse the Internet uses it as a medium.

QUESTION 135
Users of Instant Messaging clients are especially prone to what?

A. Theft of root user credentials.
B. Disconnection from the file server.
C. Hostile code delivered by file transfer.
D. Slow Internet connections.
E. Loss of email privileges.
F. Blue Screen of Death errors.

Answer: C

Explanation:
IM clients can also be compromised by malicious code, Trojan Horse programs, and traditional DoS attacks.
Reference: Security + (SYBEX) page 197

QUESTION 136
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

Explanation:
Instant messaging was created for speed and simplicity. They wanted a program that was feature rich, but not memory intensive so more people could be online more often. Since the text is unencrypted, it's very easy for someone to eavesdrop on a message, hijack the conversation and send a virus that's disguised as an innocent graphic file.

QUESTION 137
Instant Messaging is most vulnerable to:

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

Answer: D

Explanation:
Since instant messenger conversations are sent unencrypted (in clear-text) it's very easy for someone to use a sniffer on the line to eavesdrop on the entire conversation.

QUESTION 138
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

Explanation:
When you're online and you execute an ActiveX control; the only thing that can control it, are the individual user settings of the current user.
Reference: Security + (SYBEX) page

QUESTION 139
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

Explanation:
ActiveX components are downloaded to the client hard disk, potentially allowing additional security breaches. Web browsers can be configured so that they require confirmation to accept an ActiveX control.
Reference: Security + (SYBEX) page 135

QUESTION 140
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

Explanation:
ActiveX controls are digitally signed with an Authenticode signature, verified by a Certificate Authority. The controls are restricted by that signature only, not by the web browser settings.

QUESTION 141
Which of the following can be used to track a user's browsing habits on the Internet and may contain usernames and passwords?

A. Digital certificates
B. Cookies
C. ActiveX controls
D. Web server cache

Answer: B

Explanation:
Cookies are text files that a browser maintains on the user's hard disk. A cookie will typically contain information about the user. Cookies are used to provide persistent, customized web experience for each visit.
Cookies do contain username and passwords for each site you visit or login into.
Reference: Security + (SYBEX) page 135

QUESTION 142
Which of the following is an HTI'P (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)/l.0 Caching.
D. vCard v3.0.
Answers B

Explanation:
Cookies were originally developed by Netscape as a convenience feature to save user settings across multiple sites, servers, and webpages. For example, some cookies save passwords and login information so a user doesn't have to enter it everytime they visit a page. Since cookies contain valuable information like: user name, IP address, browser, and operating system a hacker can use cookie information for spoofing.

QUESTION 143
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

Explanation:
Common Gateway Interface is an older form of scripting that was used extensively in early web systems. CGI scripts could be used to capture data from a user using simple forms. The CGI script ran on the web server, and it interacted with the client browser. CGI is frowned upon in new applications because of its security issues, but it still widely used in older systems.
Although the answer is not given in the paragraph from the book, the answer would be D.
Reference: Security + (SYBEX) page 136

QUESTION 144
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

Explanation:
Common Gateway Interface is an older form of scripting that was used extensively in early web systems. CGI scripts could be used to capture data from a user using simple forms. The CGI script ran on the web server, and it interacted with the client browser. CGI is frowned upon in new applications because of its security issues, but it still widely used in older systems.
Reference: Security + (SYBEX) page 136

QUESTION 145
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

Explanation:

Transport Layer Security is an end-to-end encryption protocol that is similar to and based on SSL version 3.0 except it uses stronger encryption, and not entirely interoperable. It is specified in ISO 10736 as part of the transport layer in a protocol stack; defined in RFC 2246.

QUESTION 146
LDAP (Lightweight Directory Access Protocol) requires what ports by default?

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

Answer: A

Explanation:
The 'well known' LDAP ports are 389 for LDAP and 636 for LDAP SSL.

QUESTION 147
The start of the LDAP (Lightweight Directory Access Protocol) directory is called the:

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

Answer: B

Explanation:
LDAP directories are arranged as trees. Below the topmost 'root' node, country information appears, followed by entries for companies, states or national organizations. Next comes entries for organizational units, such as branch offices and departments. Finally we locate individuals, which in X.500 and LDAP include people, shared resources such as printers, and documents. An LDAP directory server thus makes it possible for a corporate user to find the information resources she needs anywhere on the enterprise network.
Reference: http://www.intranetjournal.com/foundation/ldap.shtml

---

QUESTION 148
LDAP (Lightweight Directory Access Protocol) directories are arranged as:

A. linked lists.
B. trees.
C. stacks.
D. queues.

Answer: B

Explanation:
Directories are displayed best as directory tree's, so naturally LDAP uses tree's. LDAP is based from an object-orientated access model built to directory enabled networking (DEN) standards.

QUESTION 149
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

Explanation:
FTP has a major flaw. The user ID and password are not encrypted and are subject to packet capture.
Reference: Security + (SYBEX) page 138

QUESTION 150
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

Explanation:
Early FTP servers did not offer security. Security was based on the honor system. Most logons to an FTP site used the anonymous logon. By convention, the logon ID was the user's email address, and the password was anonymous.
Reference: Security + (SYBEX) page 137

QUESTION 151
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

Explanation:
Anonymous FTP is based on good faith. But if it used to take advantage of the nonsecure logon, then answer C would seem to be the best answer.

QUESTION 152
A FTP (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

Explanation:
In some implementations of FTP daemons, the PORT command can be misused to open a connection to a port of the attacker's choosing on a machine that the attacker could not have accessed directly. There have been ongoing discussions about this problem (called "FTP bounce") for several years, and some vendors have developed solutions for this problem.
For more detailed information on this FTP Bounce attack refer to the hyperlink.
Reference: http://www.cert.org/advisories/CA-1997-27.html

QUESTION 153
What ports does FTP (File Transfer Protocol) use?

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

Answer: A

Explanation:
In basic FTP operations, port 20 is the data port and port 21 is the command port.

QUESTION 154
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

Explanation:
In basic FTP operations, port 20 is the data port and port 21 is the command port.

QUESTION 155
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.

QUESTION 156
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

Explanation:
802.11b
The 802.11b standard provides for bandwidth of up to 11Mbps in the 2.4GHz frequency spectrum.
Reference: Security + (SYBEX) page 193

QUESTION 157
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

Explanation:
The 802.11 standard describes the communication that occurs in wireless local area networks (LANs). The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP.
WEP relies on a secret key that is shared between a mobile station (eg. a laptop with a wireless ethernet card) and an access point (ie. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe; however, no commercial system we are aware of has mechanisms to support such techniques.
Reference: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

---

QUESTION 158
Which of the following provides privacy, data integrity and authentication for handled 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.

QUESTION 159
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

Explanation:
Since most wireless devices are low in: memory, processing power, and bandwidth capability creating a security mechanism is a difficult task. WTLS is the method security for WAP (Wireless Application Protocol) and it provides transport layer security directly between a wireless device and the WAP gateway.

QUESTION 160
A protocol specified in IEEE (Institute of Electrical and Electronics Engineers) 802.11b intended to provide a WLAN (Wireless Local Area Network) with the level of security associated with a LAN (Local Area Network) is:

A. WEP (Wired Equivalent Privacy)
B. ISSE (Information Systems Security Engineering)
C. ISDN (Integrated Services Digital Network)
D. VPN (Virtual Private Network)

Answer: A

Explanation:
Wired Equivalent Privacy is a wireless protocol designed to provide privacy equivalent to that of a wired network.
Reference: Security + (SYBEX) page 372

QUESTION 161
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

Explanation:
If every access point is secured to WEP standards, the entire range covered by the

wireless system will be encrypted to a security level that equals a conventional wired network, thus preventing sniffing and unauthorized 'drive by' access.

QUESTION 162
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

Explanation:
The 802.11 standard describes the communication that occurs in wireless local area networks (LANs). The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP.
WEP relies on a secret key that is shared between a mobile station (eg. a laptop with a wireless ethernet card) and an access point (ie. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe; however, no commercial system we are aware of has mechanisms to support such techniques.
Reference: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

---

QUESTION 163
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 that that of wired LANs (Local Area Networks).
D. Allow radio frequencies to penetrate walls.

Answer: A

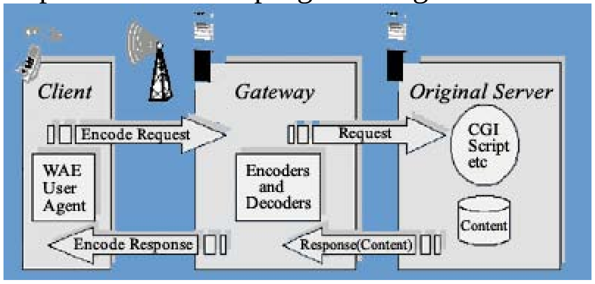
Explanation:
Wired Equivalent Privacy is a wireless protocol designed to provide privacy equivalent to that of a wired network.
Reference: Security + (SYBEX) page 372

QUESTION 164
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:



QUESTION 165
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

Explanation:
Vulnerability scanners are tools that were designed to remotely assess your network by finding vulnerabilities on your systems before the bad guys do.
Vulnerability scanning looks for vulnerabilities in your network before anyone has a chance to exploit them. The vulnerabilities might exist on your network as a whole (open TCP ports or unneeded services), on your servers, or on workstations.
A vulnerability scanner will examine your system and compare it to a database of known vulnerabilities, then report the vulnerabilities it finds on each system. The report will also tell you how to fix the vulnerabilities, such as altering configuration files or downloading security patches from a vendor.

QUESTION 166
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

Explanation:
Packet sniffers are used to capture, monitor and analyze traffic. There legitimate purpose is to find traffic flow problems and bottlenecks for the sake of network optimization. However, hackers use the to capture data, to use in replay attacks.

QUESTION 167
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. hoats.allow
D. hosts.deny

Answer: B

Explanation:
The shadow password format, is popular in Linux. A shadowed password remains readable on the outside, but instead of a password it contains placeholders composed of 9 fields which include a username, an encrypted password, and seven different time dependent fields.

QUESTION 168
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

Explanation:
B is wrong because hardware and software are usually used in a wide array by different vendors.

QUESTION 169
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

Explanation:
Leaving additional network services enabled may cause difficulties and can create vulnerabilities in your network. As much as possible, configure your network devices as restrictively as you can.
Reference: Security + (SYBEX) page 235

QUESTION 170
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

Explanation:

A successful attack on the right server can give you credentials like: usernames, addresses, and password hashes for many users over many systems.

QUESTION 171
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 his 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

Explanation:
Switches were originally designed to segment networks to make communications more efficient. Unless traffic is sent to the broadcast address, a switch will not forward traffic out all ports.

QUESTION 172
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

Explanation:
Geography and architecture can effect wireless availability and integrity. It would be crucial to perform a site survey first, to locate any geographical and architectural obstacles so they can be accommodated.

QUESTION 173
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

Explanation:
Access control lists enable devices in your network to ignore requests from specified users or systems, or grant certain network capabilities to them. ACLs allow a stronger set of access controls to be established in your network. The basic process of ACL control allows the administrator to design and adapt the network to deal with specific security threats.
Reference: Security + (SYBEX) page 235

QUESTION 174
Sensitive data traffic can be confined to workstations on a specific subnet using privilege policy based tables in a:

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

Answer: A

Explanation:
A router with an access control list is a powerful line of defense against users on the outside, and users on the inside.

QUESTION 175
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

Explanation:
In IPSec the payload and the header are known as the ESP (Encapsulating Security Payload) and AH (Authentication Header).

QUESTION 176
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

Explanation:
What good is a firewall without any kind of policy or configuration policy to be implemented?

QUESTION 177
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 lDS (Intrusion Detection System)
D. a client based IDS (Intrusion Detection System)

Answer: A

Explanation:
A network based Intrusion Detection System is not limited to a single server or network segment like a host based IDS, it monitors all the traffic over the entire network

---

QUESTION 178
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

Explanation:
Stateful Packet Filter-Stateful Inspection
This type of firewall combines the speed of packet filters with the enhanced security of stored session information typified by proxies. While traffic is being forwarded through the firewall, stateful inspections of the packets create slots in session flow tables. These tables contain source and destination IP addresses, port numbers, and TCP protocol information. Before traffic can travel back through the firewall, stateful inspections of the packets are cross-referenced to the session flow tables for an existing connection slot. If a match is found in the tables, the packets are forwarded; otherwise, the packets are dropped or rejected. The Cisco PIX firewall uses stateful inspection as its primary method to control traffic flow.

Reference:
http://www.informit.com/articles/article.asp?p=101741&seqNum=3

QUESTION 179
The basic strategy that should be used when configuring the rules fore secure firewall is:

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

Answer: D

Explanation:
It's safer and easier to deny everybody and work to allow some; then it is to allow everybody and work to deny some. Always deny by default, because you'll never know what you can overlook or forget.

QUESTION 180
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 CAN NOT be authenticated, authorized or accounted for.
D. a firewall CAN NOT inspect encrypted traffic.

Answer: D

Explanation:
A firewall can't inspect traffic once it is channeled into a VPN. When a firewall sees a VPN channel, it considers it as already passing security checks. The firewall does not have the ability to see through the encrypted channel.

QUESTION 181
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

Explanation:
Sniffers can be mitigated using a Switch. The switch is intelligent and sends the data only to the destination address. Sniffers usually work in a LAN using a hub.

QUESTION 182
The best protection against the abuse of remote maintenance of PBX (Private Branch Exchange) system is to:

A. Keep maintenance features turned off until needed
B. Insists on strong authentication before allowing remote maintenance
C. Keep PBX (Private Branch Exchange) in locked enclosure and restrict access to only a few people.
D. Check to see if the maintenance caller is on the list of approved maintenance personnel

Answer: B

Explanation: Only authenticated access should be allowed.

QUESTION 183
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

Explanation:
During the late 1980's before call display, it was very common for pranksters to phone up pizza delivery restaurants and fraudulently order pizzas to unsuspected peoples houses. The American pizza industry (led by Pizza Hut and Domino's) applied the security mechanism of callback to authenticate fraudulent orders from legitimate orders. During the order, they'd ask for the customer's phone number and phone them back to confirm the order. This simple security measure saved the pizza industry millions of dollars, and it's the exact same security measure that dial up modems can use to authenticate remote users.

QUESTION 184
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

Explanation:
A war dialer picks up modems that are connected to a phone jack on a network. By using a war dialer, you can find a connected modem and call into it to gain remote access to a computer. This is very 1980s, but it still works. For remote access purposes, a war dialer would be the best choice here.

QUESTION 185
A mobile sales force requires remote connectivity in order to access shared files and email 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

Explanation:
A virtual private network is exactly what it sounds. The salesmen can log on to the internet, go to the VPN service providers sign on page, and from there they will virtual access to a private network that is safe, secure, and encrypted.

QUESTION 186
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

Explanation:
Switches don't send all traffic on the segment to every port so conventional sniffing methods don't work.

QUESTION 187
Intrusion detection systems typically consist of two parts, a console and a:

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

Answer: A

Explanation:
Sensor's are installed at various locations of the network to sense an intruder, which reports the information back to a console so an administrator can be informed of the details of the intrusion.

QUESTION 188
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: A

Explanation:
A multi-homed (also called dual homed) firewall only means it is a single bastion server with 2 NIC cards (thus dual or multi-homed) which is the least expensive of the methods to implement. If it is compromised, they gain access to the network so the correct answer is not "C". Your explanation describes the DMZ as the answer but you must have thought multi-homed was referring to a screened gateway (router - server - router setup).

QUESTION 189
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 no 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.

QUESTION 190
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

Explanation:
The obvious choice to this question is C. I do not know of any network that allows everyone administrative controls.

QUESTION 191
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: D

Explanation:
You can use a switch to segment a specific network or subnet by using VLANs.

QUESTION 192
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

Explanation:
Active response involves taking an action based upon an attack or threat. The goal of an active response would be to take the quickest action possible to reduce the potential impact of an event. Terminating connections, processes, or sessions are responses that may occur in the event of an unauthorized connection.

A and C are wrong for obvious reasons.
Reference: Security + (SYBEX) page 181

QUESTION 193
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

Explanation:
Spoofed e-mails will not be detected by the IDS.

QUESTION 194
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

Explanation:
Host based IDS solutions are made up of programs and processes running on a host, server, or workstation that monitor event logs, application logs, port access, and other process to identify suspicious behavior or signatures associated with an attack. They differ from network based IDS that seek: string signatures, port signatures, and header signatures.

QUESTION 195
What is a common DISADVANTAGE of employing an IDS (Intrusion Detection System)?

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

Answer: A

Explanation:

A false positive is when legitimate traffic is picked up as an intruder. If this happens too often then the IDS is not working properly.

QUESTION 196
Which of the following statements is true about network based lDSs (Intrusion Detection System)?

A. Network based lDSs (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 lDSs (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 lDSs (Intrusion Detection System) are usually passive devices that listen on a network wire without interfering with the normal operation of a network.

Answer: D

Explanation:
In a passive system, the IDS detects a potential security breach, logs the information and signals an alert. In a reactive system, the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source.

QUESTION 197
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

Explanation:
Network based Intrusion Detection System work by examining ALL packets for known attack signatures, even DoS attacks as they happen.

QUESTION 198
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

Explanation:
Fiber-optic, as a media, is relatively secure because it cannot be easily tapped. It is the strongest media available to defeat EMI and RFI in my opinion.
Reference: Security + (SYBEX) page 147

QUESTION 199
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

Explanation:
Fiber optic cable, as a media, is relatively secure because it cannot be easily tapped. It is the strongest media available to defeat EMI and RFI in my opinion.
Reference: Security + (SYBEX) page 147

QUESTION 200
What media provides the best protection against electromagnetic interference?
A) coaxial cable
B) UTP (Unshielded Twisted Pair)
C) STP (Shielded Twisted Pair)
D) fiber optic cable

Answer: D

Explanation:
Fiber optic cables are not affected by electromagnetic interference or radio frequency interference and it is difficult to eavesdrop; because they don't work the same way as conventional cables. They're made out of glass (which is an insulator) and transmit pulses of light through that glass.

QUESTION 201
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

Explanation:
IPSec provides secure authentication and encryption of data and headers. IPSec can work in Tunneling mode or Transport mode. In Tunneling mode, the data or payload and message headers are encrypted. Transport mode encrypts only the payload.
Reference: Security + (SYBEX) page 127

QUESTION 202
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

Explanation:
A VLAN allows you to create groups of users and systems and segment them on the network. This segmentation allows you to hide segments of the network from other segments and control access. You can think of a VLAN as a good way to contain network traffic. VLANS are created by using a switch, and switched networks mitigate against sniffers.
Reference: Security + (SYBEX) page 28

QUESTION 203
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: B

Explanation:
Implement a VLAN (Virtual Local Area Network) to restrict network access is the best answer. VLAN's would restrict access only to their local VLAN, and this would require less administrative overhead than setting up firewalls at each subnet. They are also hardware based (at the switch and MAC level) Firewalls are used so that external users (outside the organization cannot get in), whereas VLAN's are used within an organization to provide security.

QUESTION 204
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

Explanation:
Tunneling refers to the ability to create a virtual dedicated connection between two systems or network. The tunnel is created between the two ends by encapsulating the data in a mutually agreed upon protocol for transmission.
Reference: Security + (SYBEX) page 29

QUESTION 205
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

Explanation:
IPSec provides secure authentication and encryption of data and headers. IPSec can work in tunneling mode or transport mode. In tunneling mode, the data or payload and message headers are encrypted. Transport modes encrypt only the payload.
Reference: Security + (SYBEX) page 127

QUESTION 206
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

Explanation:
Civil engineers build tunnels to allow one direction of traffic flow to be protected against another traffic flow. They will build a tunnel under a river, or underneath a highway. Network engineers use tunneling to protect a data flow from the elements of the internet. They tunnel by placing secure encrypted IP packets into a non-secure IP packet.

QUESTION 207
Tunneling is best described as the act of encapsulating:

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

Answer: B

Explanation:
IPSec Tunneling
When used alone for interoperability scenarios, IPSec performs Layer 3 tunneling, meaning the tunneled payload is a Network Layer packet. The entire IP packet is encapsulated and encrypted for transfer by one of the IPSec security protocols:
ESP Tunnel Mode
The inner IP header (the original packet header) usually carries the ultimate source and destination addresses, while the outer IP header contains the address of a security gateway. The Signed area indicates where the packet has been protected with integrity. The Encrypted area indicates what information is encrypted for confidentiality. The original header is placed after the ESP header. The entire packet is appended with an ESP trailer prior to encryption. Everything following the ESP header, except for the ESP authentication trailer, is encrypted, including the original header because it is now considered to be part of the data portion. The entire packet is then encapsulated. The information in the new IP header is used to route the packet from origin to the next destination; usually a security gateway.

QUESTION 208
The primary purpose of NAT (Network Address Translation) is to:

A. Translate IP (Internet Protocol) addresses into user friendly names.
B. Hide internal hosts from the public network.
C. Use on public IP (Internet Protocol) address on the internal network as a name server.
D. Hide the public network from internal hosts.

Answer: B

Explanation:
NAT effectively hides your network from the world. This makes it much harder to determine what systems exist on the other side of the router.
Reference: Security + (SYBEX) page 29

QUESTION 209
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

Explanation:
172.16.0.0 is a private IP address that can be NAT to a IP address.

QUESTION 210
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: A
NAT and PAT can be configured for static and dynamic address translation.

QUESTION 211
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
A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network.

QUESTION 212
A company's web server is configured for the following services: HTTP (Hypertext Transfer Protocol), SSL (Secure Sockets Layer), FTP (Pile 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

Explanation:
Port 80 is used by HTTP
Port 443 is used by HTTPS (HTTP over SSL)
Port 21 is used by FTP, and
Port 25 is used by SMTP

QUESTION 213
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

Explanation:
Network address translation will allow you to connect multiple computers to the internet with just one IP address, because it works as an agent between the internal network and

the outside networks.
Reference: Security + (SYBEX) page 185

QUESTION 214
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

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.
Short for demilitarized zone, a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. The term comes from military use, meaning a buffer area between two enemies.
Reference:
http://www.webopedia.com/TERM/D/DMZ.html

QUESTION 215
A DMZ (Demilitarized Zone) typically contains:

A. A customer account database
B. Staff workstations
C. A FTP (File Transfer Protocol) server
D. A SQL (Structured Query Language) based database server

Answer: C

Explanation:
A DMZ is an area where you can place a public server for access by people you might not trust otherwise. By isolating a server in a DMZ, you can hide or remove access to other areas of your network.
A FTP server can be used by people from outside of your network and should be placed in the DMZ.
Reference: Security + (SYBEX) page 26

QUESTION 216
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.

QUESTION 217
The general philosophy for DMZ's is that:
A.) any system on the DMZ can be compromised because it's accessible from the Internet
B.) any system on the DMZ cannot be compromised because it's not accessible from the Internet
C.) some systems on the DMZ can be compromised because they are accessible from the Internet
D.) any system on the DMZ cannot be compromised because it's by definition 100% safe and not accessible from the Internet

Answer: A

QUESTION 218
NetBus and Back Orifice are each considered an example of a(n):

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

Explanation:
Illicit servers are also known as 'backdoors.' They allow system access without using a security check.

QUESTION 219
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

Explanation:
An active intrusion detection response is to begin taking action against the intruder as soon as the breach is detected. Te principles are: detection (collect additional information), deflection (change the environment), and countermeasures (take action against the intruder).
So changing the environment to spoof the attacker and hide your valuable resources; and collecting details about the source of the intrusion and the type of intrusion to gather evidence for prosecution and future system hardening are all components of active intrusion detection.

QUESTION 220
Incorrectly detecting authorized access as an intrusion or attack is called a false:

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

Answer: B

Explanation: False intrusion is a false alarm, when there is no need of any alarm.
Not C: A false positive is when legitimate traffic is picked up as an intruder.

QUESTION 221
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

Explanation:
When the hull of a ship ruptures, the crew seals the locks to contain the damage. When a population is exposed to a disease like SARS, those infected are quarantined to contain further infection. When a network's security is breached, it may take a while to fix the problem, and in the panic it's possible to actually spread the damage further, so the most

important initial step is to contain the breach to minimize damage and ease reconstruction.

QUESTION 222
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.

QUESTION 223
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

Explanation:
A deception active response fools the attacker into thinking the attack is succeeding while monitoring the activity and potentially redirecting the attacker to a system that is designed to be broken. This allows the operator or administrator to gather data about how the attack is unfolding and what techniques are being used in the attack. This process is referred to as sending them to the honey pot.
Reference: Security + (SYBEX) page 183

QUESTION 224
A honey pot is _____.

A. A false system or network to attract attacks away from your real network.
B. A place to store passwords.
C. A sage haven for your backup media.
D. Something that exist only in theory.

Answer: A

Explanation:
A honey pot is a computer that has been designed as a target for computer attacks. The benefit of a honey pot system is that it will draw attackers away from a higher value system or it will allow administrators to gain intelligence about an attack strategy.
Reference: Security + (SYBEX) page 185

QUESTION 225
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

Explanation:
A honey pot is a computer that has been designed as a target for computer attacks.
Reference: Security + (SYBEX) page 185

QUESTION 226
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 honey pot is a computer that has been designed as a target for computer attacks. The benefit of a honey pot system is that it will draw attackers away from a higher valued systems or it will allow administrators to gain intelligence about an attack strategy.
Reference: Security + (SYBEX) page 185

QUESTION 227
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

Explanation:
A honey pot is a computer that has been designed as a target for computer attacks. The benefit of a honey pot system is that it will draw attackers away from a higher valued systems or it will allow administrators to gain intelligence about an attack strategy.
Reference: Security + (SYBEX) page 185

QUESTION 228
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.
Answers B

Explanation:
A honey pot is a computer that has been designed as a target for computer attacks. The benefit of a honey pot system is that it will draw attackers away from a higher valued systems or it will allow administrators to gain intelligence about an attack strategy.
Reference: Security + (SYBEX) page 185

QUESTION 229
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

Explanation:
If someone intentionally severs a T1 cable you have a serious incidence on your hands.
An attack like this should be considered when planning incident response.

QUESTION 230
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

Explanation:
TCP wrappers are an additional method of providing security against unwelcome visitors. In a Solaris environment there's a TCP daemon called inted which responds to TCP/IP connections and initiates the right program to furnish the needs of that request. A TCP wrapper, wraps itself around this daemon with a tcpd program which logs the incoming request first, putting up an optional layer of access control that can allow or deny a request depending on where its from.

QUESTION 231
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

QUESTION 232
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 beams 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

Explanation:
Internet Message Access Protocol v4 uses port 143 and TCP for connections. POP3 uses

port 110 and TCP for connections and therefore can be filtered out to decrease unnecessary exposure.
Reference: Security + (SYBEX) page 130

QUESTION 233
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

Explanation:
Renaming the administrator account name and disabling the guest account will reduce the risk of a computer being attacked.

QUESTION 234
What port does SNMP use?

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

Answer: B
SNMP uses UDP port 161

QUESTION 235
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

Explanation:
Objects are what the user constructs (ie: tables, columns, views, domains).
Actions are the operations performed on the objects. (ie: select, insert, delete, reference)
Users invoke the actions on the objects.

QUESTION 236
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

Explanation:
Ports 20 and 21 are used for FTP. If you only allow outbound connections, you will allow a hacker to download the contents of your server (good if you are in advertising, and your server is full of promotional materials) but never upload anything detrimental or malicious to it.

QUESTION 237
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

Explanation:
An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program). Microsoft Windows NT/2000, Novell's NetWare, Digital's OpenVMS, and Unix-based systems are among the operating systems that use access control lists. The list is implemented differently by each operating system.
Reference:
www.whatis.com

QUESTION 238
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

Explanation:
Hackers perform port scans to find out which of the 65,536 ports are being used in hope of finding an application with a vulnerability. By uninstalling and disabling any program or processes that aren't really necessary, one greatly reduces the likelihood of an attack.

QUESTION 239
What is one advantage of the NTFS file system over the FAT16 and FAT32 file systems?

A. Integral support for streaming audio files.
B. Integral support for UNIX compatibility.
C. Integral support for dual-booting with Red Hat Linux.
D. Integral support for file and folder level permissions.

Answer: D

Explanation:
The NTFS was introduced with Windows NT to address security problems. With NTFS files, directories, and volumes can each have their own security.
Reference: Security + (SYBEX) page 229

QUESTION 240
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 ll0 at the firewall.

Answer: A

Explanation:
DHCP works over UDP ports 67 and 68.

QUESTION 241
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

Explanation:
If a domain name server allows zone transfer, it will allow another DNS server (one from a different domain) to access its DNS library of IP addresses and names; which could fall into a hackers hands if he were to pose as a DNS server.

QUESTION 242
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

Explanation:
DNS reverse lookup takes a numbered IP address and converts it to a domain name. This is a very easy process, and there are free reverse DNS lookup services online. With reverse DNS a spammer won't be able to hide.

QUESTION 243
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

Explanation:
SSL is used to secure a connection between a web user and a web server for transactions like: banking, securities, and ecommerce.

QUESTION 244
What is a common type of attack on web servers?

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

Answer: B

Explanation:
Buffer overflow occur when an application receives more data that it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system.
Reference: Security + (SYBEX) page 135

QUESTION 245
What functionality should be disallowed between a DNS (Domain Name) server and untrusted node?

A. name resolutions
B. reverse ARP (Address Resolution Protocol) requests
C. system name resolutions
D. zone transfers

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

QUESTION 246
How should a primary DNS (Domain Name Service) server be configured toprovide 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

Explanation:
If a DNS server was only configured to handle DNS and nothing else, the only type of packets that could take up any resources will be domain name requests. Overwhelming an entire servers, services with domain name requests alone is an engineering feat.

QUESTION 247
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

Explanation:
Software patches are good for network security, because they are developed the fix known vulnerabilities. So even if everything's operating normally, a patch is still very beneficial. When you patch an operating system, there's always a risk that something can go wrong which can compromise your data and server operation. It would be wise to backup your data BEFORE, installing a patch, and it would also be wise to test the patch on your least important servers first.

QUESTION 248
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

Explanation:
Platform hardening procedures can be categorized into three basic areas:
• The first area to address is removing unused software and processes from the workstations. The services and processes may create opportunities for exploitation.
• The second are involves ensuring that all services and applications are up-to-date and configured in the most secure manner allowed. This may include assigning passwords, limiting access, and restricting capabilities.
• The third area to address involves the minimization of information dissemination about the operating system, services, and capabilities of the system.
Reference: Security + (SYBEX) page 120

QUESTION 249
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

Explanation:
The Sybex book discusses application hardening and refers this to the web, FTP, and Email servers. The question refers to programming new applications. Although I could not find any information in the book about programming hardening, I would say that answer B is the best choice out of the four answers.

QUESTION 250
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

Explanation:
Operating system hardening is easy when you know of a well documented patch or hotfix. When you're hardening an operating system for the unexpected, it's a long task.

QUESTION 251
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

Explanation:

This seems to be the best choice out of the four answers. By hashing the passwords, they will be encrypted.

QUESTION 252
How many bits are employed when using hash encryption?

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

Answer: C

Explanation:
Reference: Security + (SYBEX) page 183

QUESTION 253
What kind of encryption does Block Cipher have?

A. Symmetric
B. Asymmetric
C. Both symmetric and asymmetric

Answer: A

Explanation:
There are two main types of symmetric ciphers: block ciphers and stream ciphers.

QUESTION 254
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

Explanation:
Digital signatures are used to authenticate asymmetric keys.

QUESTION 255
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

Explanation:
The asymmetric algorithms are used to encrypt two different keys; a public key and a private key.

QUESTION 256
Non-repudiation is based on what type of key infrastructure?

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

Answer: C

Explanation:
Non-repudiation is unique to asymmetric systems, because the private key is exclusive to one party only.
Exam cram pages 182-183
Reference: Security + (SYBEX) page

QUESTION 257
Which two of the following are symmetric-key algorithms used for encryption?

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

Answer: A, B

Explanation:
Symmetric key encryption comes in two categories:
- block cipher (encrypt a number of bits as a single unit)
- stream cipher (encrypts single bits of plain text one bit at a time)

QUESTION 258
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

Explanation:
Here are some of the common standard that use symmetric algorithm.

- DES
- AES has replaced DES as the current standard, and it uses the Rijindael algorithm.
- 3DES
- CAST
- RC
- Blowfish
- IDEA

Reference: Security + (SYBEX) page 321-322

QUESTION 259
By definition, how many keys are needed to lock and unlock data using symmetrickey encryption?

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

Answer: C

Explanation:
Symmetrical Keys present a difficult challenge to both key management and security perspective. The loss or compromise of a symmetrical key compromises the entire system. Single key systems are entirely dependant on the privacy of the key. This key requires special handling and security. Make sure that symmetrical keys are never divulged. Symmetrical keys should be transmitted using secure out-of-band methods.
Reference: Security + (SYBEX) page 385-386

QUESTION 260
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

Explanation:
Asymmetric algorithm uses two keys to encrypt and decrypt data. These keys are referred to as the public and private key. The public key can be used by the sender to encrypt a message, and the private key can be used by the sender to encrypt a message, and the private key can be used by the receiver to decrypt the message.
Reference: Security + (SYBEX) page 322

QUESTION 261
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

Explanation:
Four popular asymmetric systems are in use today:
- RSA
- Diffie-hellman
- ECC
- El Gamal

Reference: Security + (SYBEX) page 324

QUESTION 262
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 someone aside from the intended parties gets the key, privacy has been compromised. Symmetric algorithms have the advantage of not consuming too much computing power.

QUESTION 263
During the digital signature process, asymmetric cryptography satisfies what security requirement?

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

Answer: D

QUESTION 264
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

Explanation:
A digital signature validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.
Reference: Security + (SYBEX) page 327

QUESTION 265
The primary DISADVANTAGE of symmetric cryptography is:

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

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

QUESTION 266
File encryption using symmetric cryptography satisfies what security requirement?

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

Answer: A

Explanation:
"The first goal of cryptography is confidentiality". Since file encryption using symmetric cryptography is a form of cryptography, it would make sense it would meet the confidentiality requirement.
Reference: Syngress Security Study guide, Page 513

QUESTION 267
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 was designed by the NSA.

QUESTION 268
Which of the following statements identifies a characteristic of a symmetric algorithm?

A. Performs a fast transformation of data relative to other cryptographic methods.
B. Regardless of the size of the user's input data, the size of the output data is fixed.
C. Is relatively slow in transforming data when compared to other cryptographic methods.
D. Includes a one way function where it is computationally infeasible for another entity to determine the input data from the output data.

Answer: A

Explanation:
Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A private key is simply a key that is not disclosed to people who are not

authorized to use the encryption system. The disclosure of a private key breaches the security of the encryption system.
By having the secret key, that would mean you will be authenticated to received the file or data that.
Reference: Security + (SYBEX) page 320

QUESTION 269
Which of the following is an example of an asymmetric encryption algorithm?
A) RC4 (Rivest Cipher 4)
B) IDEA (International Data Encryption Algorithm)
C) MD5 (Message Digest 5)
D) RSA (Rivest Shamir Adelmann)

Answer: D

Explanation:
RSA is the only asymmetric encryption algorithm (the others are symmetric).

QUESTION 270
What kind of attack is a hashed password vulnerable to?

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

Answer: B

Explanation:
A hashed password cannot be guessed, or reversed engineered. Hashing is a number used for data integrity also known as checksum, not encryption of password.
As you can see the hash value is just a single number. The hash value cannot be used to derive the meaning of the original message.
Note: If a hash was stolen off the wire using a man in the middle attack, it would do him no good. The reason is that the hash can represent several different words. The hash can not be used to crack a password or message, it is used to verify or to store on a server as opposed to plain text. But a password can still be guessed using a dictionary or brute force. Here is how a hash is arrived at.
Password: this
ASCll Values t = 116, h = 104, i = 105, s = 115 (These values are multiplied by 2 to get the calculated number, which would be 232, 208, 210, 230. These numbers are added together then divided by 10. (232+208+210+230)/10 This gives you a hash of 80, but there are other number/ letter combinations that would give you this one way hash. So it can not be used to crack the password.
Reference Security+ (Sybex) page 313.

Hashed Password or Password-Verifier
Passwords stored in a database should be stored in a one-way hashed form, to prevent casual retrieval of the information. Since passwords are often vulnerable to dictionary attack, preventing unauthorized access to this data thus remains a high priority. In general, the requirement for secure host storage is characteristic of all mutual authentication cryptographic systems. Alternative public-key methods are especially sensitive to the theft of a stored private key.

QUESTION 271
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

Explanation:
A digital signature validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.
Reference: Security + (SYBEX) page 327

QUESTION 272
Which of the following hash functions generates a 160-bit output?

A. MD4 (Message Digest 4).
B. MD5 (Message Digest 5).
C. UDES (Data Encryption Standard).
D. SHA-1 (Secure Hashing Algorithm 1).

Answer: D

Explanation:
The SHA-1 algorithm produces a 160-bit hash value. SHA has been updated; the new standard is SHA-1.
Reference: Security + (SYBEX) page 319

QUESTION 273
Data integrity is best achieved using a(n)

A. Asymmetric cipher
B. Digital certificate
C. Message digest

D. Symmetric cipher

Answer: C

Explanation:
The Message Digest Algorithm is another algorithm that creates a hash value. MDA uses a one-way hash. The hash value is used to help maintain integrity.
Reference: Security + (SYBEX) page 319

QUESTION 274
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

Explanation:
The goal of integrity is the make sure that the data being worked with is actually correct data.
Reference: Security + (SYBEX) page 22

QUESTION 275
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

Explanation:
The goal of integrity is the make sure that the data being worked with is actually correct data.
Reference: Security + (SYBEX) page 22

QUESTION 276
What two functions does IPSec perform? (Choose two)

A. Provides the Secure Shell (SSH) for data confidentiality.
B. Provides the Password Authentication Protocol (PAP) for user authentication.
C. Provides the Authentication Header (AH) for data integrity.

D. Provides the Internet Protocol (IP) for data integrity.
E. Provides the Nonrepudiation Header (NH) for identity integrity.
F. Provides the Encapsulation Security Payload (ESP) for data confidentiality.

Answer: C, F

Explanation:
IPSec is a security protocol that provides authentication and encryption across the Internet. IPSec can use AH or ESP.
Reference: Security + (SYBEX) page 371

QUESTION 277
Message authentication codes are used to provide which service?

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

Answer: A

Explanation:
A common method of verifying integrity involves adding a Message Authentication Code to the message. The MAC is derived from the message and a key. This process ensures the integrity of the message.
Reference: Security + (SYBEX) page 326

QUESTION 278
The most common form of authentication is the use of:

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

Answer: C

Explanation:
Password authentication is common on every operating system, and every restricted website. The sheer number of password authentication dwarves all the other options all put together. Passwords are easy to implement, users are accustomed to them, and the only equipment necessary is a keyboard.

QUESTION 279
Which of the following makes a token based authentication system very difficult to attack?

A) a token uses a digital certificate
B) a token is something that is physically possessed
C) a token can only be used by one time
D) a token can only be used by the intended owner

Answer: C

Explanation: Sybex Security+ Page 15, The authentication system creates a token every time a user or a session begins. At the completion of a session, the token is destroyed.

QUESTION 280
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

Explanation:
Multi-Factor
When two or more of these access methods are included as a part of the authentication process, you are implementing a multi-factor system.
Reference: Security + (SYBEX) page 17

QUESTION 281
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

Explanation:
The purpose is so that a user can gain access to all of the applications and systems they need when they log on with a single sign-on.
Reference: Security + (SYBEX) page 434

QUESTION 282
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.

QUESTION 283
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

Explanation:
The goal of confidentiality is to prevent or minimize unauthorized access and disclosure of data and information.
Reference: Security + (SYBEX) page 22

QUESTION 284
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

Explanation:

Access control prevents users from accessing information and resources that they're not supposed to; hence controlling access. Authentication is to authenticate that the user who does gain access is the right user. Confidentiality is the function of giving privacy, data integrity is the process of replicating the data perfectly.

QUESTION 285
The protection of data against unauthorized access or disclosure is an example of what?

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

Answer: A

Explanation:
The goal of confidentiality is to prevent or minimize unauthorized access and disclosure of data and information.
Reference: Security + (SYBEX) page 22

QUESTION 286
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

Explanation:
Access control defines how users and systems communicate and in what manner. Three basic models are used to explain access control.
Reference: Security + (SYBEX) page 11

QUESTION 287
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

Explanation:
Security measures and countermeasures are used for confidentiality, integrity, availability and accountability.

QUESTION 288
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

Explanation:
Data integrity is when the message received is exactly the same as the message sent.

QUESTION 289
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

Explanation:
The design goals of a security topology must deal with issues of confidentiality, integrity, availability and accountability. You will often see the confidentiality, integrity and availability referred to as the CIA of network security. The accountability is equally important.
Reference: Security + (SYBEX) page 22

QUESTION 290
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

Explanation:
The principle of non-repudiation is used in secure email, and ecommerce to give people confidence in their transaction.

- Irrefutable proof that the data came from where it claims to be from
- Irrefutable proof that the data was submitted
- Irrefutable proof that the data was delivered
- Irrefutable proof that the data was received

QUESTION 291
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

Explanation:
Non-repudiation is an encryption process that is used to confirm that an email actually: comes from where the source says it's from, that it was submitted and delivered without being altered, and that the recipient actually opened it.

QUESTION 292
Many intrusion detection systems look for known patterns or _____ to aid in detecting attacks.

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

Answer: B

Explanation:
IDS can detect two types of traffic patterns. Misuse-Detection IDS is primarily focused on evaluating attacks based on attack signatures and audit trails. Anomaly-Detection IDS focuses on abnormal traffic patterns.
Reference: Security + (SYBEX) page 177-178

QUESTION 293
Digital signatures can be used for which of the following?

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

Answer: D

Explanation:
Digital signatures provide authentication and integrity in their own right, but also provide non-repudiation for proof of origin. Non-repudiation is proof that can be clearly demonstrated to a third party. Since a sender uses their own unique private asymmetric key, this provides proof that they indeed generate the message.

QUESTION 294
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

Explanation:
A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.
References:
www.whatis.com

QUESTION 295
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

Explanation:
The public key is the only key that's made public.

QUESTION 296
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

Explanation:
A certificate practice statement (CPS) is legal document that describes how the CA (Certificate Authority) manages the certificates it issue.

QUESTION 297
A CPS (Certificate Practice Statement) is a legal document that describes a CA's (Certificate Authority's) ___________:

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

Answer: C

Explanation:
A Certification Practice Statement is a public statement of the practices a company uses for issuing and validating certificates and for supporting reliance on their certificates. The company outlines why there certificates are good, and brag about the details of their features, and their liability limits.

QUESTION 298
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

Explanation:
The fields of X509 are:

- Version
- Serial Number
- Signature Algorithm Identifier
- Issuer
- Validity Period
- Subject Name
- Subject Public Key Information
- Extension Field

QUESTION 299
Which of the following correctly identifies some of the contents of a 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: C

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
C
A. 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

QUESTION 300
Most certificates used for authentication are based on what standard?

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

Answer: D

Explanation:
"The most widely used standard for digital certificates is X.509."
Reference:
http://www.webopedia.com/TERM/D/digital_certificate.html

QUESTION 301
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

Explanation:
This is not discussed in the book so much, but you can find online more information on software publisher certificate. The answer A is correct.

QUESTION 302
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

Explanation:
Web browsers like Internet Explorer and Netscape Navigator are capable of abiding by a

trust list; which is a list of sites that are confirmed to be safe and have their valid certificates embedded to prove it.

QUESTION 303
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

Explanation:
A smart card is a type of badge or card that can allow access to multiple resources including buildings, parking lots, and computers. The card itself usually contains a small amount of memory that can be used to store permissions and access information.
Answer C is least likely to be a smart card.
Reference: Security + (SYBEX) page 18 + 154

QUESTION 304
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

Explanation:
The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. The CA marks the certificate as revoked. This information is published in the CRL and becomes available using OCSP.
Reference: Security + (SYBEX) page 338

QUESTION 305
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

Explanation:
A digital certificate is like a virtual identification card issued by a certification authority (CA) that establishes your credentials when doing web based transactions. Digital certificates contain a name, serial number, validity period, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the CA's digital signature so that a recipient can verify that the certificate is real.

QUESTION 306
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

Explanation:
A certificate revocation list is a list kept by a certificate authority that lists off sites who's certificates have expired, or been revoked for security breaches. The problem with them is that, although it is possible to get an immediate response, the data that is on the list has up to a 24 hour update delay. For this reason Online Certificate Status Protocol (OCSP) is better.

QUESTION 307
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

Explanation:
Certification revocation is the process of revoking a certification before it expires. A certificate may need to be revoked because it was stolen, an employee moved on to a new company, or someone has had their access revoked.
Reference: Security + (SYBEX) page 337

QUESTION 308
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
Definition of Policy - course of action, guiding principle, or procedure considered expedient, prudent, or advantageous.

QUESTION 309
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

Explanation:
Any document that serves as the vehicle on which it is used as a guideline is a policy.
4.4 Identify and be able to differentiate different cryptographic standards and protocols (7 questions)

QUESTION 310
The defacto IT (Information Technology) security evaluation criteria for the international community is called?

A. Common Criteria
B. Global Criteria
C. TCSEC (Trusted Computer System Evaluation Criteria)
D. ITSEC (Information Technology Security Evaluation Criteria)

Answer: A
Reference: Standards for Security in E-Business Activities.

QUESTION 311
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

Explanation:
AES has replaced DES as the current standard, and it uses the Rijindael algorithm
Reference: Security + (SYBEX) page 22

QUESTION 312
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:
MD5 is the newest version of the algorithm. MD5 produces a 128-bit hash, but the algorithm is more complex than its predecessors and it offers greater security.
Reference: Security + (SYBEX) page 320

QUESTION 313
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

Explanation:
IPSec is an IETF protocol, and it does use an AH and ESP for network security.

QUESTION 314
What has 160-Bit encryption?

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

D. Blowfish

Answer: C
HMAC-SHA-1 uses a 160-bit secret key.

QUESTION 315
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

Explanation:
Also known as an exponential key agreement, the Diffie-Hellman algorithm allows two sides to agree to an exclusive secret key between them, with no prior arrangements. When the keys are exchanged they are done so secretively, then verified to confirm it reaches the right recipient.

QUESTION 316
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.

QUESTION 317
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

Explanation:

The sender uses their private key to 'sign' the message, but the receiver uses their 'public' key to verify the signature on the message.

QUESTION 318

Which protocol is used to negotiate and provide authenticated keying material forsecurity 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

Explanation:
IPSec supports the Internet Key Exchange protocol which is a key management standard used to specify speerate key protocols to be used during dta encryption. IKE functions within the Internet Security Association and Key Managemnet Protocol (ISAKMP), which defines the payloads used to exchange key aand authentication data appended to each packet.

QUESTION 319

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

Explanation:
Dual key pair support is critical for applications that utilize both encryption and digital signatures. An end user needs one key pair for encryption and another for digital signing so that the encryption key pair can be backed up without compromising the integrity of the user's digital signatures.

QUESTION 320

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

Explanation:
If User A sends User B a message that only User B can read, we can assume that they're using a asymmetric encryption algorithm. User A has to use User B's public key, because User B's private key is private.

QUESTION 321
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

Explanation:
A certificate is really nothing more than a mechanism that associates the public key with an individual.
Reference: Security + (SYBEX) page 332

QUESTION 322
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

Explanation:
The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. The CA marks the certificate as revoked. This information is published in the CRL and becomes available using OCSP.
Reference: Security + (SYBEX) page 338

QUESTION 323
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: A

QUESTION 324
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

Explanation:
The private key is what the user uses, to encrypt the data. Once someone has the private key in 'their hands' they can easily extract the public key (which is out in the open) then decrypt the message perfectly.

QUESTION 325
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

Explanation:
The PKI is a system that provides for exchange of data over a network, by way of a secure asymmetric key system. The most popular company in America that does this is VeriSign.

QUESTION 326
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

Explanation:
If all the keys are stored in one place, under the watch of a limited number of people; the more a hacker will have to gain by infiltrating that particular key depository, and the more financial incentive he'll have to stage an elaborate attack, including social engineering to capitalize on the volume of a centralized facility.

QUESTION 327
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

Explanation:
Here's an example; if you want want to digitally sign an email, your special email client will give you a hash, your PRIVATE KEY will encrypt the hash, and when the recipient of your email receives the email they will use their software to hash the message, then use your PUBLIC KEY to decrypt the hash, and it the hashes match the message is valid.

QUESTION 328
A block cipher is an example of which of the following encryption algorithms?
A) asymmetric key
B) public key
C) symmetric key
D) unkeyed

Answer: C

Explanation:
A block cipher is a symmetric key encryption that takes a number of bits and encrypts them as a single unit. Some popular block ciphers are: DES, 3DES, AES (Rijndael), Blowfish, IDEA, RC2, RC5,RC6, CAST,MARS, Serpent, Twofish.

QUESTION 329
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

Explanation:
In centralized key management the certificate authority has complete control over the entire process. Many users aren't comfortable with someone else having access to their private keys, and don't feel personally secure with this solution.

QUESTION 330
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

Explanation:
Incorrect:
Deleting a key isn't necessarily a good idea because one day in the future, you may need the key again. Recycling keys or submitting to a key repository isn't necessary because a cryptographic key isn't a physical key made out of metal.

QUESTION 331
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

Explanation:
Smart cards are used for authentication, and in this example the smart card authenticated that the owner of the card was the one authorized to use that particular workstation.

QUESTION 332
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

Explanation:
Digital certificates contain public keys, so that the public can verify authenticity.

QUESTION 333
What access control principle requires that every user or process is given the most restricted privileges?

A. Control permissions
B. Least privilege
C. Hierarchical permissions
D. Access mode

Answer: B

Explanation:
The access control principle of least privilege is about giving each user's the bare minimum amount of access, just enough so they can perform their task and nothing else. So by limiting employee access from the inside, security will be easier to implement, and the risk of social engineering attacks or mistakes are reduced.

QUESTION 334
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

Explanation:
The Bell-LaPadula model is a formal state transition model of computer security policy that describes a set of access control rules.
In this formal model, the entities in a computer system are divided into abstract sets of subjects and objects. The notion of a secure state is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system is secure.
A system state is defined to be "secure" if the only permitted access modes of subjects to

objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object, and a determination is made as to whether the subject is authorized for the specific access mode. The clearance/classification scheme is expressed in terms of a lattice.

This security model is directed toward security (rather than data integrity) and is characterized by the phrase: "no read up, no write down". Compare Biba model.

With Bell-LaPadula, users can only create content at or above their own security level (secret researchers can create secret or top-secret files but may not create public files). Conversely, users can only view content at or below their own security level (secret researchers can view public or secret files, but may not view top-secret files).

See, ITsecurity.com (2003). Bell-LaPadula Security Model. Retrieved May 19, 2004 from http://www.itsecurity.com/dictionary/bell.htm

Reference:

http://en.wikipedia.org/wiki/Bell-LaPadula_model

QUESTION 335

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

Explanation:

Role based access control is also known as discretionary access control. Different company operations have a list of potential resources, and within this department there are numerous potential roles each requiring access to some of the operations resources, and within each role fits multiple users who perform the same role.

QUESTION 336

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

Explanation:
Biometric systems are those that use some kind of unique biological identifier to identify a person. Some of these unique identifiers include fingerprints, patterns on the retina, and handprints, and DNA scanners, and they can be used as part of the access control mechanisms.
Usernames, passwords and PINs are not apart of biometrics.
Reference: Security + (SYBEX) page 265

QUESTION 337
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 threat 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

Explanation:
This is the only answer that can be true.

A. Is false, because why would a repair of the window increase the threat.
B. Is false, because with a repair, there is no vulnerability.
C. If the window is not repaired, then the threat will increase not decrease.
Reference: Security + (SYBEX) page 87

QUESTION 338
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

Explanation:
Piggybacking is when an intruder waits for a legitimate user to enter a door, sneaks up

behind them, and follows them in during the brief window of time. It is a popular method of access in spy and detective movies. Since security guards are famous for not paying attention, closed-circuit television requires a security guard to monitor, and biometrics are just an elaborate 'key' that has no additional protection against piggybacking; the best solution is a man trap. A man trap is a holding cell between two entry points, similar to a revolving door. Only one person can fit in at once, and a person has to wait alone in that man trap before a security guard can let them in.

QUESTION 339
Turnstiles, double entry doors, mantraps 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

Explanation:
Piggybacking is an espionage tactic commonly used in the movies. The hero or the villain hides by a secure entrance, and waits for an unknowing authorized user to enter. When the authorized user enters, they use stealth to sneak behind them and gain access without the authorized user even knowing. Other forms of piggybacking take advantage of human altruism. An unauthorized person will put on a disguise and carry a heavy box to the door, where the authorized user will try to do the right thing, and prop the door open for them.

QUESTION 340
Which one does not use Smart Card Technology?

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

Answer: A

Explanation:
Why would a CD player use a Smart card? This is a pretty easy answer.

QUESTION 341
Certkiller .com 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

Explanation:
Keep in mind that cost and the best level of security is asked for. To keep all the servers in one room, along with the vital components with a security measure added to the room will provide what is asked for.

QUESTION 342
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: D

Explanation:
Strong passwords are not a part of physical security.
Reference: Security + (SYBEX) page 258

QUESTION 343
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

Explanation:
The objective of a physical barrier is to prevent access to computers and networks. The other answers refer to detection and not prevention.
Reference: Security + (SYBEX) page 259

QUESTION 344
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

Explanation:
The best answer is
A. By reducing the overall opportunity for an intrusion to occur is pretty general but equally important.

QUESTION 345
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. fireproof doors that can be easily opened if an alarm is sounded.

Answer: A

Explanation:
If there's a fire, the smart thing to do would be to perform an emergency system shutdown. Equipment that gets shut down properly will be less likely to spread the fire, and equipment that's shut down properly is more likely to preserve its data.
Incorrect answers:
A sprinkler system wouldn't necessarily be good for electronic equipment, as water isn't recommended for electrical fires (C02, dry chemical, or halon is appropriate for electrical fires), and it will damage electrical equipment.
Non flammable materials in the room are good, but smoke or heat from another room can still damage equipment.
Answer D is a trick question, because fireproof doors should be closed on an alarm, not opened.

QUESTION 346
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

Explanation:
A differential backup is similar in function to an incremental backup, but it only backs up any files that have been altered since the last full backup.
Reference: Security + (SYBEX) page 413

QUESTION 347
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

Explanation:
A cold site is a physical location that a business has access to in case of an emergency, where they can start from scratch and rebuild a new enterprise following a disaster. It is called a cold site not because the facility isn't heated, but because it's the opposite of a hot site. A hot site already contains functioning: servers, mainframes, switches, cables, routers, workstations, telephones, jacks, desks, and chairs so a company can set up tentative operations quickly. Most companies have service contracts and opt for a cold site or a hot site depending on the importance of their operations.

QUESTION 348
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

Explanation:
A hot site is a location that can provide operations within hours of a failure. This type of site would have servers, networks and telecommunications in place to reestablish service in a very short amount of time.
Reference: Security + (SYBEX) page 418

QUESTION 349
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, a structured approach to disaster recovery is prepared for the organization.

QUESTION 350
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

Explanation:
If you already have the most critical components of your operation set up and running at an alternate site, you should begin relocation at the original site with the least critical process. That way, if something does go wrong at the original, or if following the disaster something wasn't fixed properly, you won't risk disrupting critical operations again.

QUESTION 351
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

Explanation:
This is a tough question as well. Answer B seems to be the best answer out of the four. Penetration testing will not occur without risk assessment. And the other two answers are not really good choices.

QUESTION 352
Documenting change levels and revision information is most useful for:

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

Answer: C

Explanation:
Disaster recovery is the ability to recover system operations after a disaster. One of the key aspects of disaster recovery planning is designing a comprehensive backup plan. This includes backup storage, procedures and maintenance.
Reference: Security + (SYBEX) page 405

QUESTION 353
Which of the following is expected network behavior?

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

Explanation:
There will always be variations of traffic load. The other three answers are suspicious traffic.

QUESTION 354
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

Explanation:
Business Continuity Planning is the process of implementing policies, controls, and procedures to counteract the effects of losses, outages, or failures of critical business processes.
Reference: Security + (SYBEX) page 276

QUESTION 355
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 starts working, and then drops to 60 degrees when it stops 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

Explanation: The expansion and contraction that occurs during the normal heating and cooling cycles of your system can cause chips and cards, over time, to inch loose from sockets or slots.

QUESTION 356
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

Explanation:
RAID is a technology that uses multiple disks to provide fault tolerance.
Reference: Security + (SYBEX) page 404

QUESTION 357
A primary drawback to using shared storage clustering for high availability and disaster recover 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 Disks) 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

Explanation:
Storing primary infrastructure and your backup infrastructure in the same geographical location, isn't very safe because in the unlikely event of a natural disaster, a war, an insurrection, a labour act of transcendental civil disobedience, both units will be in a position of compromise.

QUESTION 358
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

Explanation:
By reducing the lifetime of a password, the user must change the password, thus making the attacker start over on guessing the password.

QUESTION 359
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 of atleast one nonalpha.
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

Explanation:
If a user gets a difficult password that they can't remember, there's a certain chance that they will forget the password or compromise security by writing down their password on

a Post It note on their keyboard. Since the user won' be able to reset the password themselves they'll have to make regular trips to help desk for a new password, and with regular disgruntled users getting emotional over passwords, the risk of social engineering increases.

QUESTION 360
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: C

Explanation:
With the assumption that the screen saver is password protected.
Incorrect answers:
If you leave the computer unattended a social engineer could walk by, and view your sensitive material. If you turn off your monitor, they can easily turn it back on.

QUESTION 361
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

Explanation:
This means that a process has no more privileges than necessary to be able to fulfill its functions.
Reference: CISSP Certification (All-in-one) SHON Harris page 209
(The CISSP and Security + exams are closely related)

QUESTION 362
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

Explanation:
Due Care policies identify what level of care is used to maintain the confidentiality of private information. These policies specify how information is to be handled. The objectives of Due Car policies are to protect and safeguard customer and/or client records.
Reference: Security + (SYBEX) page 428

QUESTION 363
A need to know security policy would grant access based on:

A. Least privilege
B. Less privilege
C. Loss of privilege
D. Singe privilege

Answer: A

Explanation:
The need to know policies allow people in an organization to withhold the release of classified or sensitive information from others in the company. The more people have access to sensitive information, the more likely it is that this information will be disclosed to unauthorized personnel. A need to know policy is not intended to prohibit people from accessing information they need; it is meant to minimize unauthorized access.
I could not find the word " least privilege" in this book, but the term in used in the CISSP book. Answer A is correct and is the correct term that is used, the others are not.
Reference: Security + (SYBEX) page

QUESTION 364
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

Explanation:
There are many policies for companies these days. Considering the question refers to a user security policy, the users and staff need to know the policy. This is a tricky question

with many close answers. I would say D would be the best choice, but make your best decision.

QUESTION 365
Companies without an acceptable use policy may give their employees an expectation of

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

Answer: C

Explanation:
Acceptable Use policies deal primarily with computers and information provided by the company. Your policy should clearly stipulate what activities are allowed and what activities are not allowed. Having an acceptable use policy in place eliminates any uncertainty regarding what is and what isn't allowed in your organization.
Reference: Security + (SYBEX) page 425+426

QUESTION 366
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

Explanation:
The CSO of a company usually drafts a policy on information security, which should reflect managements attitude towards security and productivity.

QUESTION 367
What is generally the most overlooked element of security management?

A. Security awareness
B. Intrusion detection
C. Risk assessment
D. Vulnerability control

Answer: A

Explanation:
Security awareness and education are critical to the success of a security effort. Security awareness and education include explaining policies, standards, procedures, and guidelines to both users and management.
The book does not imply that it is over looked, but answer
A. seems to be the best choice
here. Use your best judgement with this question.
Reference: Security + (SYBEX) page 474

QUESTION 368
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

Explanation:
Detection systems fall under two categories; anomaly detection and misuse detection. If network behavior use deviates from normal use it's an anomaly. If behavior matches a known scenario, it's misuse. If a company knows their employees are visiting unauthorized pornographic web sites, and they want to detect that 'known' behavior they are in need of misuse detection.

QUESTION 369
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

Explanation:
Countless employees have compromised their business applications by installing computer games, and pornographic movies. To avoid such a problem all you have to do is to get employees to agree on a sensible use policy for personal files so they can know before hand what they are allowed to install.

QUESTION 370
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

Explanation:
In the hosting business, every company aims for 100% availability in their service level agreements, and usually offer concessions for times of reduced availability. Sadly, these agreements have exceptions which include: scheduled network maintenance, hardware maintenance, software maintenance, virus attacks, hacker attacks, force majeure, labour actions, war, insurrections, sabotage, and past due accounts on your part.

QUESTION 371
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:
Separation of duties policies are designed to reduce the risk of fraud and prevent other losses in an organization. A good policy will require more than one person to accomplish key processes.
Reference: Security + (SYBEX) page 428

QUESTION 372
Computer forensics experts collect and analyze data using which of the following guidelines so as to minimize data loss?

A. Evidence
B. Chain of custody
C. Chain of command
D. Incident response

Answer: B

Explanation:
The chain of custody is a log of the history of evidence that has been collected. This log should catalog every event from the time the evidence is collected.
Reference: Security + (SYBEX) page 457

QUESTION 373
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

Explanation:
Dumpster diving is a very common physical access method. Companies generate a huge amount of paper in the normal course of events. Most of the information eventually winds up in dumpsters or recycle bins. These dumpsters may contain information that is highly sensitive in nature. In high security government environments, sensitive papers are either shredded or burned. Most businesses do not do this.
Reference: Security + (SYBEX) page 51

QUESTION 374
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

Explanation:
When people create complex passwords that they can't remember, or are in a situation where they need multiple passwords they have a tendency of writing their passwords down. Usually on a notepad, a Post It note, or on their desk ledger.

QUESTION 375
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

Explanation:
System access requests don't reveal too much information. They are a card that an employee fills that requests the types of resources they want access to, and the privileges they want. All a hacker can learn from them is that from the moment the request was dated, that particular user did not have those privileges
Incorrect answers:
A document that contains any clues to a company's internal or external addressing scheme or a configuration or system map is of value because they are all hard clues that can help a hacker 'blueprint' the network structure. Old passwords also have value to them, because they give a hacker a glimpse at password characteristics. (How many characters? Are dictionary words used? How often are passwords changed? Does the administrator or the user choose them?)

QUESTION 376
A system administrator discovers suspicious activity that might indicate a computer crime. The administrator should first:

A. refer to the companies 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

Explanation:
For the sake of containment and awareness, whenever an administrator discovers suspicious activity, before making a move he should refer to the companies incident response plan, since different security policies require different plans of attack.

QUESTION 377
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

Explanation:
The question doesn't ask what method can be used to best secure the emails, or what will

best prevent the transmission of nonessential email. It asks what action will discourage the employees, so the correct answer is to create a network security policy that defines what kind of email use constitutes the term misuse.

QUESTION 378
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

Explanation:
When an employee signs an acceptable use policy they basically waive their right to privacy and give express written consent to having their computer searched at the employers discretion.
5.5 Explain the following concepts of privilege management
* user / Group / Role Management
* Single Sign-on
* Centralized vs. Decentralized
* Auditing (Privilege, Usage, Escalation)
* MAC /DAC / RBAC (Mandatory Access Control / Discretionary Access Control / Role Based Access Control) (10 questions)

QUESTION 379
As the Security Analyst for your company's network, you want to implement Single Sign-on technology.
What benefit can you expect to get when implementing Single Sign-on?

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

Explanation:
The purpose is so a user can gain access to all of the applications and systems they need when they log on with a single sign-on.
Reference: Security + (SYBEX) page 434

QUESTION 380
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

Explanation:
The key word is decentralized, so the best answer would be B.
Reference: Security + (SYBEX) page 432

QUESTION 381
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

Explanation:
In order to have access to information to files or systems, you need to be authenticated.

QUESTION 382
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

Explanation:
The point of a security audit is to test the existing security policies and procedures to see how they fare against new forms of attack.
Incorrect answers:
Security audits aren't necessary to review a company's existing resources, and security goals are an abstract that the CTO notes following a board meeting.
A mission statement is a long sentence that philosophizes the company's goals.
Ethic codes are voluntary moral standards placed by management.

QUESTION 383
Clients in Company A can view web sites that have been created for them, but CAN NOT 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

Explanation:
By having the authority to access the controlled sites, you will be allowed to navigate them. If they are not configured correctly or you do not have privileged access, you will not be allowed to navigate that site.

QUESTION 384
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

Explanation:
Audit trails are a record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions. Most accounting systems and database management systems include an audit trail component. In addition, there are separate audit trail software products that enable network administrators to monitor use of network resources.
Reference:
http://www.webopedia.com/TERM/A/audit_trail.html

QUESTION 385
Why are unique user IDs critical in the review of audit trails?

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

Explanation:
With a unique user ID you'll have soft evidence on the timing and the action any accessed user accomplishes. When a user known that they are being tracked, they think twice about doing something they shouldn't do.

QUESTION 386
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

Explanation:
A user obtaining access to a resource they would not normally be able to access. This is done inadvertently by running a program with SUID (Set User ID) or SGID (Set Group ID) permissions - or by temporarily becoming another user.
Reference: Security + (SYBEX) page 522

QUESTION 387
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

Explanation:
Role based access control contains components of MAC (mandatory access control) and DAC (discretionary access control), and is characterized by its use of profiles. A profile is a specific role that a group of employees perform in a function and the resources they need access to. When an employee is hired he is put into a profile, and when the entire profile of workers needs more or less resources they can all be facilitated together.

QUESTION 388
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

Explanation:
Strict control over subjects and objects by way of access control lists, and a hierarchical list of who's allowed to access what resources is a characteristic of Mandatory Access Control.

QUESTION 389
You are promoting user awareness in forensics, so users will know what to do when incidents occur with their computers. Which of the following tasks should you instruct users to perform when an incident occurs? (Choose all that apply)

A. Shut down the computer.
B. Contact the incident response team.
C. Documents what they see on the screen.
D. Log off the network.

Answer: B, C

Explanation:
The best choices would be B and C. When an incident occurs, the best things to do are to document what is going on and call the incident response team. By logging off the network, you can damage evidence. If the system is being attacked over the internet, then shutting the system down will corrupt the data and evidence.
Reference: Security + (SYBEX) page 456

QUESTION 390
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

Explanation:
Answer A is correct to stop anyone from corrupting the evidence.
Answer B is incorrect, because you would want the incident response team there.
Answer C is incorrect, because that would corrupt any evidence that is stored in RAM.
Answer D is correct to stop all activity to the hacker.

QUESTION 391
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

Explanation:
Preservation of evidence requires limited access. Answer A and B are the best choice.
Answer C is wrong, because many incidents that occur in a computer system, especially Internet attacks, will only show up in system RAM while the system is running. Answer D is wrong, because you should not touch anything until the authorities arrive.
Reference: Security + (SYBEX) page 456-458

QUESTION 392
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 is 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

Explanation:

A cyclic redundancy check is a hash function used to verify packet integrity. It makes a checksum out of redundant data and appends a Frame Check Sequence on the frame. A CRC is calculated before and after data transmission and duplication to confirm integrity. Cyclic redundancy checks are very easy to implement, they take very little overhead, and their ability of confirming data integrity is high enough that you can trust it for court evidence.

QUESTION 393

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

Explanation:
You want evidence usable if it is needed for a trial. It is a good idea to seal evidence into a bag and identify the date, time, and person who collected it. This bag-and-tag process makes tampering with the evidence more difficult.
Reference: Security + (SYBEX) page 458

QUESTION 394

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

Explanation:
The chain of custody is a log of the history of evidence that has been collected. This log should catalog every event from the time the evidence is collected.
Reference: Security + (SYBEX) page 457

QUESTION 395
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 that 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

Explanation:
1. 9 Data policy
2. 8 Internet connection
3. 7 personnel
4. 5 software

QUESTION 396
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

Explanation:
Single Loss Expectancy is the cost of a single loss when it occurs.
Reference: Security + (SYBEX) page 470

QUESTION 397
You have identified a number of risks to which your company's assets are exposed, and want to implement policies, procedures, and various security measures.
In doing so, what will be your objective?

A. Eliminate every threat that may affect the business.
B. Manage the risks so that the problems resulting from them will be minimized.
C. Implement as many security measures as possible to address every risk that an asset may be exposed to.

D. Ignore as many risks as possible to keep costs down.

Answer: B

Explanation:
Answer B would be the best benefit to the policy for your company to adjust more or less to certain needs depending on the risk.
Answer A is wrong because not every threat can be fixed.
Answer C is wrong because it may cost more money to address every risk than what the company makes.
Answer D is obviously wrong.

QUESTION 398
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

Explanation:
Answer C is correct because there is no way to bullet proof a computer's security. There are too many variables to consider.

QUESTION 399
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 businessfunctionality.
C. to identify how much it will cost to implement counter measures.
D. to delegate responsibility.

Answer: B

Explanation:
Hypothetically speaking, a company can spend millions on security and still not be 100% secure, while some companies can spend virtually nothing on security but because of the nature of their business, they won't be at risk of losing anything. Risk analysis is to find out exactly how much security is worth to you, and how much security you can get for how much its worth.

QUESTION 400
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

Explanation:
An impact analysis is when you plan out a worst case disaster scenario and illustrate just how much business a company can lose; then estimate the price of the best solution. From there you start compromising, with a cost factor analysis to factor out how much a solution and its risk reduction benefits would cost versus the probability of lost business and peace of mind. During which the company formally decides how much downtime they can afford to lose, and ends up implementing a solution accordingly.

QUESTION 401
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

Explanation:
Recovery is equally as important a step as the original backup. What good is an up to date backup file, if it can't be recovered properly? Sadly, most system administrators make the assumption that their recovery will work flawlessly and fail to test their recovery procedures.

QUESTION 402
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: B

QUESTION 403
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

Explanation:
Operating system manufacturers pride themselves in having a secure system, and the instant they realize that there's a security breach they assign a team on it to develop a security patch. Or when they make new software release (Linux kernels seam to be updated every other day) they try to fix all known vulnerabilities. Since the older an operating system is, the more time a hacker's have to seek vulnerabilities. A simple security patch that takes a couple of minutes to download and install is the difference between having a secure network and having a system made completely useless by a worm.

QUESTION 404
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

Explanation:
If you have any security controls (firewalls) that you think are working and are not, then there can be a vulnerability.

QUESTION 405
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

Explanation:
The insurance business is also known as the risk assessment business.

QUESTION 406
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

Explanation:
Penetration testing is the act of gaining access
Reference: Security + (SYBEX) page 521

QUESTION 407
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 an IDS (Intrusion Detection System)

Answer: A

Explanation:
Performing a vulnerability assessment is one of the most effective way to find holes in the network. The other answers limit your assessment.

QUESTION 408
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
Answers B

Explanation:

If a company relies on a system for its day to day business; they owe it to their shareholders and customers to protect their data. Usually the more important the company, the more incentive there is for an attack; so vulnerability assessment isn't a form of insecurity. Any site is vulnerable to a hacker, so vulnerability assessments are rarely done in vain.

QUESTION 409
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 (possibly C)

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

QUESTION 410
Company intranets, newsletters, posters, login banners and e-mails would be good tools to utilize in a security:
investigation
awareness program
policy review
control test

Answer: B

Explanation:
Advertisement techniques are used to bring product awareness to a consumer; likewise advertising techniques can also be used to bring awareness to security programs.
Reference: Security + (SYBEX) page

QUESTION 411
Security training should emphasize that the weakest links in the security of an organization are typically:

A. Firewalls
B. Polices
C. Viruses
D. People

Answer: D

Explanation:

People would be the weakest link out of these 4 answers, because they may not follow the policies or configure the firewall correctly. Viruses are not in a security organization.

QUESTION 412
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
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.

QUESTION 413
Appropriate documentation of a security incident is important for each of the following reasons EXCEPT:

A. The documentation serves as 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

Explanation:
There is no documentation on who should be fired for an incident.

QUESTION 414
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

Explanation:
Keeping track of system events and asset inventories is an important aspect of security.

System logs tell us what is happening with the systems on the network. These logs should be periodically reviewed and cleared. Logs tend to fill up and become hard to work with. It is a good practice to review system logs on a weekly basis to look for unusual errors, activities, or events.
Reference: Security + (SYBEX) page 463

QUESTION 415
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

Explanation:
The answer asks for the most common system goal. So the correct answer isn't about what system logging can do, or should do, but what ALL system logging accomplishes. The most basic form of system logging is a pen and paper sign on, where a user logs their name, the system they use, their purpose, and the time they begin and end. So if a future incidence happens, one could go into the logs, and narrow down who could have witnessed it or been present.

QUESTION 416
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

Explanation:
Keeping track of system events and asset inventories is an important aspect of security. System logs tell us what is happening with the systems on the network. These logs should be periodically reviewed and cleared. Logs tend to fill up and become hard to work with. It is a good practice to review system logs on a weekly basis to look for unusual errors, activities, or events.
Reference: Security + (SYBEX) page 463

QUESTION 417
What standard security protocol provides security and privacy in a WLAN (Wireless Local Area Network)?

A. SWP (Secure WLAN Protocol)
B. WEP (Wired Equivalent Privacy)
C. SSL (Secure Sockets Layer)
D. S/MIME (Secure Multipurpose Internet Mail Extensions)

Answer: B

QUESTION 418
It is most difficult to eavesdrop on which of the following types of network cabling?

A. fiber optic cable
B. coaxial cable
C. UDP (Unshielded Twisted Pair)
D. STP (Shielded Twisted Pair)

Answer: A

QUESTION 419
Which of the following is the best reason for a CA (Certificate Authority) to revoke a certificate?

A. The user's certificate has been idle for two months.
B. The user has relocated to another address.
C. The user's private key has been compromised.
D. The user's public key has been compromised.

Answer: C

QUESTION 420
Which of the following would best protect the confidentiality and integrity of an email message?

A. SHA-1 (Secure Hashing Algorithm 1)
B. IPSec (Internet Protocol Security)
C. Digital signature
D. S/MIME (Secure Multipurpose Internet Mail Extensions)

Answer: D

QUESTION 421
Being able to verify that a message received has not been modified in transit is defined as:

A. authorization
B. non-repudiation
C. integrity

D. cryptographic mapping

Answer: C

QUESTION 422
The first step in establishing a disaster recovery plan is to:

A. Get budgetary approval for the plan.
B. Agree on the objectives of the plan.
C. List possible alternative sites to be used in a disaster event.
D. Prioritize processes requiring immediate attention in a disaster event.

Answer: B

QUESTION 423
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

QUESTION 424
A program appearing to be useful that contains additional hidden code that allows unauthorized individuals to exploit or destroy data is commonly known as a:

A. virus
B. Trojan horse
C. Worm
D. Back door

Answer: B

QUESTION 425
A sound security policy will define:

A. What is considered an organization's assets.
B. What attacks are planned against the organization.
C. How an organization compares the others in security audits.
D. Weaknesses in competitor's systems.

Answer: A

QUESTION 426
When securing a DNS (Domain Name Service) server, and shutting down all unnecessary ports, which port should NOT be shut down?

A. 21
B. 23
C. 53
D. 55

Answer: C

QUESTION 427
Creation of an information inventory is mist vulnerable when:

A. Localizing license based attacks.
B. Trying to reconstruct damaged systems.
C. Determining virus penetration within an enterprise.
D. Terminating employees for security policy violations.

Answer: B

QUESTION 428
A team organized for the purpose of handling security crises is called a(n):

A. computer information team
B. security resources team
C. active detection team
D. incident response team

Answer: D

QUESTION 429
There are a number of ports in TCP/IP (Transmission Control Protocol/Internet Protocol) that can be scanned, exploited, or attached.
How many ports are vulnerable to such operations?

A. 32
B. 1,024
C. 65,535
D. 16,777,216

Answer: C