CompTIA SY0-101

Security+

Q&A with explanations

Version 19.0

Leading The Way
in IT Testing And Certification Tools

www.testking.com

Important Note Please
Read Carefully

Study Tips
This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Further Material
For this exam www.Testking.in also provides:
- Online Testing. Practice the questions in an exam environment.
- Sybex, Syngress, McGraw-Hill, Wrox... eBooks for all certification.
- Teaching material such as M.O.C (Microsoft Official Curriculum), Cisco Academy
- Simulator and software for self-study.

All available or will listing at: http://www.TestKing.in

Latest Version
We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for One Year after the purchase. You should check www.TestKing.in 3-4 days before the scheduled exam date.

For most updates, it is enough just to print the new questions at the end of the new version, not the whole document.

Table of Contents

Total number of questions: 429

Topic 1, General Security Concepts (91 questions)

1.1 Recognize and be able to differentiate and explain the various access control models. (13 questions)

QUESTION NO: 1
Which of the following is NOT a valid access control mechanism?

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:
The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). There is no SAC (Subjective Access Control) list.

Incorrect Answers:
C: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). MAC is based on predefined access privileges to a resource.
A: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). DAC is based on the owner of the resource allowing other users access to that resource.
D: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). RBAC is based on the role or responsibilities users have in the organization.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION NO: 2
Which of the following best describes an access control mechanism in which access control decisions are based on the responsibilities that an individual user or process has in an organization?

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

Answer: B
Explanation:
Access control using the RBAC model is based on the role or responsibilities users have in the organization. These usually reflect the organization's structure and can be implemented system wide.

Incorrect Answers:
A: Access control using the MAC model is based on predefined access privileges to a resource.
C: Access control using the DAC model is based on the owner of the resource allowing other users access to that resource.
D: Access control using the RBAC model is based on the role or responsibilities users have in the organization.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION NO: 3
Which of the following best describes an access control mechanism that allows the data owner to create and administer access control?

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 control access privileges to that resource. This model is dynamic in nature and allows the owner of the resource to grant or revoke access to individuals or groups of individuals.

Incorrect Answers:
A: Access control using the MAC model is based on predefined access privileges to a resource.
B: Access control using the RBAC model is based on the role or responsibilities users have in the organization.
C: Access control using the LBAC model is based on a list of users and the privileges they have been granted to an object. This list is usually created by the administrator.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10, 668.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION NO: 4
Which of the following is an inherent flaw in the DAC (Discretionary Access Control) model?

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:
The DAC model is more flexible than the MAC model. It allows the owner of a resource to control access privileges to that resource. Thus, access control is entirely at the digression of the owner, as is the resource that is shared. In other words, there are no security checks to ensure that malicious code is not made available for sharing.

References:

Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p. 720.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 393.

QUESTION NO: 5
Which of the following access control methods 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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 13, 216, 219

QUESTION NO: 6
You work as the security administrator at TestKing.com. You set permissions on a file object in a network operating system which uses DAC (Discretionary Access Control). The ACL (Access Control List) of the file is as follows:

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

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

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:
ACLs have a list of users and their associated access that they have been granted to a resource such as a file. When a user attempts to access a resource the ACL is checked to see if the user has the required privileges, if the required privileges are not found, access is denied. In this ACL, User B does not have an associated access privilege to the resource. Therefore User B has no permissions on the resource and will not be able to access it.

Incorrect Answers:
B, C, D: In this ACL, User B does not have an associated access privilege to the resource. Therefore User B has absolutely no permissions on the resource.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 13, 211
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 9-10.

QUESTION NO: 7
You work as the security administrator at TestKing.com. TestKing has a RBAC (Role Based Access Control) compliant system for which you are planning the security implementation. There are three types of resources including files, printers, and mailboxes and four distinct departments with distinct functions including Sales, Marketing, Management, and Production in the system. Each department needs access to different resources. Each user has a workstation. Which roles should you create 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:

Access control using the RBAC model is based on the role or responsibilities users have in the organization. These roles usually reflect the organization's structure, such as its division into different departments, each with its distinct role in the organization. Thus the RBAC model could be based on the different departments.

Incorrect Answers:
A: The RBAC model is based on user roles, not on resource roles such as file, printer, and mailbox roles. These resource roles might not reflect the different departments' access requirements to them.
C: The RBAC model is based on user roles, not on a division between users and machines. Grouping all users together does not differentiate between the different access requirements of different users based on the role that those users fulfill in the organization.
D: By implementing allow access and deny access roles, we would create only two options: access to all resources or no access. This does not differentiate between the different access requirements of different users based on the role that those users fulfill in the organization.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION NO: 8
With regard to DAC (Discretionary Access Control), which of the following statements are true?

A. Files that don't have an owner CANNOT 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 control access privileges to that resource. Thus, access control is entirely at the digression of the owner who has full control over the resource.

Incorrect Answers:
A: Each file does have an owner, which is the user that created the file, or the user to whom the creator of the file has transferred ownership.

B: The creator of the resource is the owner of that resource, not the administrator. C:
The creator of the resource is the owner of that resource, not the operating system.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 9-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION NO: 9
Which of the following are used to make access decisions 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.

Incorrect Answers:
A: DAC uses an Access Control List (ACL) that identifies the users who have been granted access to a resource.
B: DAC is based on the ownership of a resource. The owner of the resource controls access to that resource.
C: RBAC is based on group membership, which would reflect both the role users fulfill in the organization and the structure of the organization.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-9.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION NO: 10
Which of the following access control methods allows access control decisions to be based on security labels associated with each data item and each user?

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:
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.

Incorrect Answers:
A: RBAC is based on group membership, which would reflect both the role users fulfill in the organization and the structure of the organization.
C: LBAC is based on a list of users and the privileges they have been granted to an object. This list is usually created by the administrator.
D: DAC is based on the ownership of a resource. The owner of the resource controls access to that resource.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION NO: 11
Which of the following access control methods relies on 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:
MAC is a strict hierarchical mode that is based on classifying data on importance and categorizing data by department. Users receive specific security clearances to access this data.

Incorrect Answers:
A: RBAC is based on the role users fulfill in the organization.
B: There is no NDAC.
D: DAC is based on the ownership of a resource. The owner of the resource controls access to that resource.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION NO: 12
Which of the following is a characteristic of MAC (Mandatory Access Control)?

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

Answer: A
Explanation:
MAC is a strict hierarchical mode that is based on classifying data on importance and categorizing data by department. Users receive specific security clearances to access this data.

Incorrect Answers:
B: DAC is based on ownership of a resource. The owner of the resource controls access to that resource.
C, D: DAC and LBAC use Access Control Lists (ACL) that identifies the users who have been granted access to a resource.

References:

Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION NO: 13
Which of the following terms best 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 bounds of a user's access permission. In other words, a user's access differs at different levels. It describes a hierarchical model that is based on classifying data on sensitivity and categorizing it at different levels. Users must have the correct level of security clearances to access the data. This is the system that MAC is based on.

Incorrect Answers:
B: TheBell La-Padula model prevents a user from accessing information that has a higher security rating than that which the user is authorized to access. It also prevents information from being written to a lower level of security. Thus this model is based on classification which is used in MAC. However, it is not the best answer.
C: TheBIBA model is similar to the Bell La-Padula model but is more concerned with information integrity.
D: TheClark and Wilson model prevents the direct access of data. Data can only be accessed through applications that have predefined capabilities. This prevents unauthorized modification, errors, and fraud from occurring. This does not describe MAC.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 455, 267-269.

1.2 Recognize and be able to differentiate and explain the various methods of authentication. (13 questions)

QUESTION NO: 1
Which of the following password generators 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.**

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 1

QUESTION NO: 2
Which of the following password management systems is designed to provide for a large number of users?

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.

Incorrect answers:

B: Locally saved password management systems are not designed for large networks and large amounts of users.
C: A multi-factor system is when two or more access methods are included as part of the authentication process. This would be impractical with a large number of users.
D: Synchronized password would pose a serious threat for any amount of users.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 2

QUESTION NO: 3
Which of the following provides 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.

Incorrect Answers:
A: VPN tunnels through the Internet to establish a link between two remote private networks. However, these connections are not considered secure unless a tunneling protocol, such as PPTP, and an encryption protocol, such as IPSec is used.
B: PPTP is a tunneling protocol. It does not provide encryption which could mitigate against interception.
D: Complex password requirements make the password more difficult to crack using brute force and dictionary attacks. However, it does not protect the password from being intercepted.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 22-26, 105-108.

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp.112-114

QUESTION NO: 4
Which of the following best 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.

Incorrect Answers:
B: Challenge-response sessions do not generate random login IDs but random challenges. C: Challenge-response sessions do not rely on special hardware devices to generate the challenge or the response. The computer system does this. D: The purpose of authentication is to determine if the owner should be authenticated.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 20-21.
http://www.webopedia.com/TERM/C/challenge_response.html

QUESTION NO: 5
Which of the following must be deployed for Kerberos to function correctly?

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

Answer: D
Explanation:
Time synchronization is crucial because Kerberos uses server and workstation time as part of the authentication process. Kerberos authentication uses a Key Distribution Center (KDC) to orchestrate the process. The KDC authenticates the principle (which can be a user, a program, or a system) and provides it with a ticket. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another principle. Kerberos is quickly becoming a common standard in network environments. Its only significant weakness is that the KDC can be a single point of failure. If the KDC goes down, the authentication process will stop.

Incorrect answers:
A: This is irrelevant.
B: Time synchronization is more important in Kerberos.
C: Tokens devices are not as essential to Kerberos as time synchronization is.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.17

QUESTION NO: 6
Why are clocks used in a Kerberos authentication system?

A. To ensure proper connections.
B. To ensure tickets expire correctly.
C. To generate the seed value for the encryptions keys.
D. 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).

Incorrect answers:
A: Proper connections are not dependant on time synchronization. C: Generating seed value for encryption keys are not time related. D: You do not need time synchronization for benchmark and set optimal encryption algorithms.

References:
http://www.faqs.org/faqs/kerberos-faq/general/section-22.html

QUESTION NO: 7
Which of the following factors must be considered when implementing Kerberos authentication?

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.

Incorrect answers:
A: This will not prevent Kerberos from functioning. B: This will not prevent Kerberos from functioning. D: Encryption is part of Kerberos. No passwords are sent in clear text.

Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.17

QUESTION NO: 8
You work as the security administrator at TestKing.com. You want to ensure that only encrypted passwords are used during authentication. Which authentication protocol should you use?

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.

Incorrect answers:
A: PPTP is a tunneling protocol. It does not provide encryption.
B: SMTP is a protocol for sending e-mail between SMTP servers.
C: Kerberos is an authentication scheme that uses tickets (unique keys) embedded within messages.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.112

QUESTION NO: 9
Which of the following are the 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:
Kerberos authentication uses a Key Distribution Center (KDC) to orchestrate the process. The KDC authenticates the principle (which can be a user, a program, or a system) and provides it with a ticket. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another principle.

Incorrect answers:
B: SAM is not required.
C: There is no need for an application database or system manager.
D: A privilege server and not a system manager are necessary.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp.16-17

QUESTION NO: 10
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.

Incorrect answers:
B: CHAP also challenges for a handshake during the connection. C:
CHAP also challenges for a handshake after the initial connection. D:
CHAP also challenges for a handshake during connections.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.15

QUESTION NO: 11
For which of the following can biometrics be used?

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

Answer: D
Explanation:
Biometrics devices use physical characteristics to identify the user.

Incorrect answers:
A: Accountability does not require physical characteristics of users.
B: Certification does not require physical characteristics of users. C:
Authorization is not the same as authentication.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 18-19

QUESTION NO: 12
Which of the following is the most costly method of an authentication?

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.

Incorrect answers:
A, B, D: Passwords, tokens and shared secrets are in use in most companies since they are not as costly as biometrics.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 18-19, 265

QUESTION NO: 13
Which of the following provides the strongest form of 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.

Incorrect answers:
A: Tokens are not as reliable as biometrics.
B: Usernames and passwords can be intercepted.
D: One time passwords is not the strongest form of authentication among the choices given.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 18-19, 265

1.3 Identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols (3 questions)

QUESTION NO: 1
Which of the following represents the best method for securing 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 pose 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.

Incorrect answers:
A: As newer versions one expects them to be better than the predecessors. However, this is not the best method to secure a web browser.
C: VPN tunnels through the Internet to establish a link between two remote private networks. However, these connections are not considered secure unless a tunneling protocol, such as PPTP, and an encryption protocol, such as IPSec is used.
D: This does not represent the best method for securing a web browser.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp.112-114

QUESTION NO: 2
How many ports in TCP/IP (Transmission Control Protocol/Internet Protocol) are vulnerable to being scanned, exploited, or attached?

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

Answer: C
Explanation:
Internet Control Message Protocol (ICMP) abuse and port scans represent known attack signatures. The Ping utility uses ICMP and is often used as a probing utility prior to an attack or may be the attack itself. If a host is being bombarded with ICMP echo requests or other ICMP traffic, this behavior should set off the IDS. Port scans are a more devious form of attack/reconnaissance used to discover information about a system. Port scanning is not an attack but is often a precursor to such activity. Port scans can be sequential, starting with port 1 and scanning to port 65535, or random. A knowledge-based IDS should recognize either type of scan and send an alert.

Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 7
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 67

QUESTION NO: 3
Which of the following ports does a DNS (Domain Name Service) server require?

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

Answer: C
Explanation:
Port 53 is used for Domain Name System (DNS) Name Queries

Incorrect answers:
A: Ports 20 and 21 are associated with FTP, where 20 are used for file transfer data and 21 for command and control data.
B: Telnet uses port 23.
D: DHCP makes use of port 55.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Appendix B http://www.iana.org/assignments/port-numbers

1.4 Recognize various types of attacks and specify the appropriate actions to take to mitigate vulnerability and risk. (34 questions)

QUESTION NO: 1
Which of the following 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.

Incorrect answers:
A: A brute force attack is an attempt to guess passwords until a successful guess occurs. C: A man-in-the-middle attack is an attack that occurs when someone/thing that is trusted intercepts packets and retransmits them to another party. D

: WinNuke or Blue Screen of Death is a Windows-based attack that affects only computers running Windows NT 3.51 or 4. It is caused by the way the Windows NT TCP/IP stack handles bad data in the TCP header.
Instead of returning an error code or rejecting the bad data, it sends NT to the Blue Screen of Death (BSOD). Figuratively speaking, the attack "nukes" the computer.
E: A SYN flood attack forces a victim system to use up one of its finite number of connections for each connection the initiator opens. Because these requests arrive so quickly, the victim system has no time to free dangling, incomplete connections before all its resources are consumed.
F: A spoofing attack is simply an attempt by someone or something masquerading as someone else. This type of attack is usually considered an access attack.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, **p** 135

QUESTION NO: 2
Which of the following attacks exploits the session initiation between the Transport Control Program (TCP) client and server in a network?

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.

Incorrect answers: A

: Buffer overflow attacks, as the name implies, attempt to put more data (usually long input strings) into the buffer than it can hold.
C: A smurf attack is an attack caused by pinging a broadcast to a number of sites with a false "from" address. When the hosts all respond to the ping, they flood the false "from" site with echoes.
D: A birthday attack is a probability method of finding similar keys in MD5.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 530

QUESTION NO: 3
Which of the following attacks uses ICMP (Internet Control Message Protocol) and improperly formatted MTUs (Maximum Transmission Unit) to crash a target computer?

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.
Remember that 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.

Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 52

QUESTION NO: 4
Which of the following determines which operating system is installed on a system by analyzing its response to certain network traffic?

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.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 67

QUESTION NO: 5
Malicious port scanning determines the

A. computer name
B. fingerprint of the operating system
C. 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.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 3

QUESTION NO: 6
Which of the following fingerprinting techniques exploits 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.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 70

QUESTION NO: 7
Which of the following type of attacks exploits poor programming techniques and lack of code review?

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.

Incorrect answers:
A: CGI scripts were used to capture data from a user using simple forms. Vulnerabilities in CGI are its inherent ability to do what it is told. If a CGI script is written to wreak havoc (or carries extra code added to it by a miscreant) and it is executed, your systems will suffer.
B: A birthday attack is a probability method of finding similar keys in MD5.
D: A dictionary attack cycles through known words in a dictionary file, testing the user's password to see whether a match is made.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 135

QUESTION NO: 8
Which of the following network attacks misuses TCP's (Transmission Control Protocol) three way handshake to overload servers and deny access to legitimate users?

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.

Incorrect answers:
A: A man-in-the-middle attack is an attack that occurs when someone/thing that is trusted intercepts packets and retransmits them to another party.
B

: A smurf attack is an attack caused by pinging a broadcast to a number of sites with a false "from" address. When the hosts all respond to the ping, they flood the false "from" site with echoes.
C: A teardrop attack is a DoS attack that uses large packets and odd offset values to confuse the receiver and help facilitate a crash.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 530

QUESTION NO: 9
Which of the following is most common method of accomplishing DDoS (Distributed Denial of Service) attacks?

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 zombie software that takes over numerous servers and routers within the network to overwhelm the systems bandwidth.

A and B are incorrect because
Incorrect answers:
A, **B:** Distributed Denial of Service (DDoS) attack is a derivative of a DoS attack in which multiple hosts in multiple locations all focus on one target. DDoS doesn't fail or shut down the servers, it merely compromises them. D: This is another method that can be used, but this method is not as common as option C.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 1

QUESTION NO: 10
Which of the following is a DoS (Denial of Service) attack that exploits TCP's (Transmission Control Protocol) three-way handshake for new connections?

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.

Incorrect answers:
B: The ping of death crashes a system by sending Internet Control Message Protocol (ICMP) packets that are larger than the system can handle.
C: A Land attack exploits a behavior in several operating systems and their respective TCP/IP stacks.
D: Buffer overflow attacks, as the name implies, attempt to put more data into the buffer than it can hold.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 52

QUESTION NO: 11
Which of the following is a DoS exploit that sends more traffic to a node than anticipated?

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.

Incorrect answers:
A: The ping of death crashes a system by sending Internet Control Message Protocol (ICMP) packets that are larger than the system can handle.
C: 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 company's computers if they feel termination is imminent.
D: A smurf attack uses IP spoofing and broadcasting to send a ping to a group of hosts in a network.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 135

QUESTION NO: 12
Which of the following is a security breach 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.

Incorrect answers:
A: A Certificate Revocation List (CRL) is a list of digital certificate revocations that must be regularly downloaded to stay current.

C: An Access Control List (ACL) is a list of rights that an object has to resources in the network.
D: A Message Digest Algorithm (MDA) is an algorithm that creates a hash value. The hash **value is also used to help maintain integrity. There are several versions of MD; the most** common are MD5, MD4, and MD2.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 53

QUESTION NO: 13
Loki, NetCaZ, Masters Paradise and NetBus are examples of 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.

Incorrect answers:
A: A brute force attack is an attempt to guess passwords until a successful guess occurs.
B: A spoofing attack is simply an attempt by someone or something masquerading as someone else. This type of attack is usually considered an access attack.
D: A man-in-the-middle attack is an attack that occurs when someone/thing that is trusted intercepts packets and retransmits them to another party.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.54

QUESTION NO: 14
What is usually the goal of TCP (transmission Control Protocol) session hijacking?

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.

Incorrect answers:
B: TCP sequence number attacks occur when an attacker takes control of one end of a TCP session.
C: Port identification is not the aim of TCP session hijacking.
D: Identifying source addresses is not the aim of TCP session hijacking.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.69

QUESTION NO: 15
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 IP (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

Incorrect answers:
B: Creating new IP addresses is not the aim of TCP/IP session hijacking.
C: Inserting packets as the server is not the aim of TCP/IP session hijacking. Furthermore the session state does get altered.
D: The session state does not remain unaltered.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.69

QUESTION NO: 16
What characteristic of TCP/IP (transmission Control Protocol/Internet Protocol) does TCP/IP (transmission Control Protocol/Internet Protocol) session hijacking exploit?

A. The fact that TCP/IP (transmission Control Protocol/Internet Protocol) has no authentication mechanism, thus allowing a clear text password of 16 bytes
B. The fact that TCP/IP (transmission Control Protocol/Internet Protocol) allows packets to be tunneled to an alternate network
C. The fact that TCP/IP (transmission Control Protocol/Internet Protocol) has no authentication mechanism, and therefore allows connectionless packets from anyone
D. The fact that TCP/IP (transmission Control Protocol/Internet Protocol) 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.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.69

QUESTION NO: 17
Which of the following attacks can be mitigated against by implementing the following ingress/egress traffic filtering?

*** 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.

Incorrect answers:
A: A SYN flood forces a victim system to use up one of its finite number of connections for each connection the initiator opens.
C: Dos attacks can also be a result of SYN flooding.
D: A dictionary attack cycles through known words in a dictionary file, testing the user's password to see whether a match is made.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 1

QUESTION NO: 18
In which of the following attacks does the attacker pretend to be a legitimate user?

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

Answer: B
Explanation:
A spoofing attack is simply an attempt by someone or something masquerading as someone else. This type of attack is usually considered an access attack.

Incorrect answers:
A: Aliasing is a type of backdoor attack where an existing user who already has privileges often creates the back door account, which is set up to look like a normal user's account and given a high-level privilege that allows an attacker to come in under an alias.
C: Flooding techniques are used to overload the state table and effectively cause the firewall to shut down or reboot.
D: Redirecting is more of a deception active response that 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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 56

QUESTION NO: 19
Which of the attacks can involve the misdirection of the domain name resolution and 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.

Incorrect answers:
A: Denial of service(DoS) attacks prevent access to resources by users authorized to use those resources.
C: A brute force attack is an attempt to guess passwords until a successful guess occurs. This type of attack usually occurs over a long period. It can be accomplished by applying every possible combination of characters that could be the key.
D

: Reverse DNS involves using an IP address to find a domain name, rather than using a domain name to find an IP address (normal DNS). PTR records are used for the reverse lookup, and often this is used to authenticate incoming connections.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 56

QUESTION NO: 20
In an IP (Internet Protocol) spoofing attack, what field of an IP (Internet Protocol) packet does the attacker manipulate?

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

Answer: B
Explanation:
In IP Spoofing a hacker tries to gain access to a network by pretending his or her machine has the same network address as the internal network.

Incorrect answers:
The source port field is the port that is addressed on the destination.
The destination address field is the port to where data is being sent.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, **p** 515

QUESTION NO: 21
You are the network administrator at TestKing.com. You discover that your domain name server is resolving the domain name to the wrong IP (Internet Protocol) address and thus misdirecting Internet traffic. You suspect a malicious attack. Which of the following would you suspect?

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.

Incorrect answers:
A: Denial of service(DoS) attacks prevent access to resources by users authorized to use those resources.
C: A brute force attack is an attempt to guess passwords until a successful guess occurs. This type of attack usually occurs over a long period. It can be accomplished by applying every possible combination of characters that could be the key.
D: Reverse DNS involves using an IP address to find a domain name, rather than using a domain name to find an IP address (normal DNS). PTR records are used for the reverse lookup, and often this is used to authenticate incoming connections.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 54

QUESTION NO: 22
What is the process of forging an IP (Internet Protocol) address to impersonate another machine called?

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.

Incorrect answers:
A: TCP/IP hijacking, also known as active sniffing, involves the attacker gaining access to a host in the network and logically disconnecting it from the network.
C: A man-in-the-middle attack is an attack that occurs when someone/thing that is trusted intercepts packets and retransmits them to another party.
D: A replay attack can be any attack where the data is retransmitted repeatedly. In one such possibility, a user can replay a web session and visit sites intended only for the original user.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 54

QUESTION NO: 23
You are the security administrator at TestKing.com. You detect intruders accessing your internal network. The source IP (Internet Protocol) addresses originate from trusted networks. What type of attack are you experiencing?

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:
A: Social engineering deals with the human aspect of gaining access and passwords.
B: TCP/IP hijacking requires an existing session.
C:

Smurfing is a legitimate kind of DoS attack that does involve spoofing, however it doesn't match the above description.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 85-86.

QUESTION NO: 24
What is an attack whereby two different messages using the same hash function produce a common message digest known as?

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.

Incorrect answers:
A: A man-in-the-middle attack is an attack that occurs when someone/thing that is trusted intercepts packets and retransmits them to another party.
B & D: Ciphertext can be used in brute force attacks as well. If the cryptographic formula is known, the attack can concentrate on breaking the cipher used more efficiently than pure guessing.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 312

QUESTION NO: 25
Which of the following can be deterred against by increasing the keyspace and complexity of a 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. A dictionary attack is an attack that uses words from a database (dictionary) to test against passwords until a match is found. This is not a complexity issue.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 86

QUESTION NO: 26
Which type of attack can easily break a user's password if the user uses simple and meaningful things such as pet names or birthdays for their passwords?

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.

Incorrect answers:
B: A brute force attack is an attempt to guess passwords until a successful guess occurs. This type of attack usually occurs over a long period. It can be accomplished by applying every possible combination of characters that could be the key.
C: A spoofing attack is an attempt by someone or something to masquerade as someone else.
D: This is rather similar to brute force attacks.
E: This is an attack that occurs when someone/thing that is trusted intercepts packets and retransmits them to another party.
F: There is no such attack.
G: Role-Based Access Control (RBAC) models approach the problem of access control based on established roles in an organization. It is not an attack.
H: A replay attack is any attack where the data is retransmitted repeatedly. In one such possibility, a user can replay a web session and visit sites intended only for the original user.
I: This is the name of a virus (possibly?)

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 58

QUESTION NO: 27
What should the minimum length of a password be to deter dictionary password cracks?

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

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.

Reference:

Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 3

QUESTION NO: 28
In which of the following does someone use an application to capture and manipulate packets as they are passing through your network?

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.

Incorrect answers:
A: This is a derivative of a DoS attack in which multiple hosts in multiple locations all focus on one target.
B: A back door is an opening left in a program application (usually by the developer) that allows additional access to data. Typically, these are created for debugging purposes and aren't **documented. Before the product ships, the back doors are closed; when they aren't closed,** security loopholes exist. This is what gets to be exploited.
C: A spoofing attack is an attempt by someone or something to masquerade as someone else.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 57

QUESTION NO: 29
Which of the following is the best defense against 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.

Incorrect answers:
A: This is a LAN that allows users on different switch ports to participate in their own network separate from, but still connected to, the other stations on the same or connected switch. Who is to say that the perpetrator is not one of the users in the private separate network?
B: PPTP encapsulates virtual network packets into PPP, which are, in turn, encapsulated into generic routing encapsulation (GRE) packets and transmitted in the form of IP datagrams between the parties. Meaning that after the tunnel is created data gets to be transferred, however, this does not prevent man in the middle attacks.
D: A smart card is a type of badge or card that gives you access to resources including buildings, parking lots, and computers. It contains information about your identity and access privileges. Each area or computer has a card scanner or a reader in which you insert your card. But this will not prevent man in the middle attacks.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, **p** 331

QUESTION NO: 30
Which of the following is the best defense against man in the middle attacks?

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

Answer: B
Explanation:
Encryption makes the intercepted data unreadable to the interceptor.

Incorrect answers:
A: A firewall will not prevent a man in the middle attack.
C: Authentication only happens during logon and the attack could occur when already logged on. In some instances authentication is not present.
D: Passwords are usually only used when logging on. This is not a good enough defense.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 86

QUESTION NO: 31
You are the security administrator at TestKing.com. All TestKing users have a token and 4-digit personal identification number (PIN) that are used to access their computer systems. The token performs off-line checking for the correct PIN. To which of the following type of attack is TestKing vulnerable?

A. Birthday
B. Brute force
Q 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.

Incorrect answers:
A: This type of attack is also an access attack, but it can be used as the starting point for a modification attack.
C: A man-in-the-middle attack is commonly used to gather information in transit between two hosts.
D: A smurf attack uses IP spoofing and broadcasting to send a ping to a group of hosts in a network.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter 1

QUESTION NO: 32
What is an attack in which 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 called?

A. SYN flood attack
B. Smurf attack
C. Ping of Dead Attack
D. Denial of Service (DOS) Attack

Answer: B
Explanation:
A smurf attack uses IP spoofing and broadcasting to send a ping to a group of hosts in a network.

Incorrect answers:
A: A SYN flood attack is a common DoS attack that involves opening as many TCP sessions as possible.
C: The ping of death crashes a system by sending Internet Control Message Protocol (ICMP) packets that are larger than the system can handle.
D: Denial of service (DoS) attacks prevents access to resources by users authorized to use those resources.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 52-57.

QUESTION NO: 33
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
Explanation:
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, it 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.

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.

Incorrect answers:
A & **B:** Any type of Cryptanalysis is the study and practice of finding weaknesses in ciphers. D: This is actually a Mathematical attack that uses mathematical modeling and statistical analysis to determine how the system operates. These types of attacks depend on intercepting large amounts of data and methodically attempting to decrypt the messages using one of the methods previously described.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 312

QUESTION NO: 34
Which of the following attacks attempts to crack 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.

Incorrect answers:
A: A smurf attack uses IP spoofing and broadcasting to send a ping to a group of hosts in a network.
B: Spam is unsolicited e-mail and bogs down network bandwidth; puts additional stress on email systems; wastes employee productivity; and above all is extremely frustrating to everyone, consuming time and sometimes money.
C: A teardrop attack is a DoS attack that uses large packets and odd offset values to confuse the receiver and help facilitate a crash.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 57.

1.5 Recognize the various types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk. (15 questions)

QUESTION NO: 1
Which of the following is an effective method of preventing computer viruses from spreading?

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.

Incorrect answers:
A: This will pose a more serious risk.
C: Preventing the execution of .vbs files will not prevent virus infection.
D: Host based IDS installation is not as effective as scanning e-mail attachments.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 76

QUESTION NO: 2
What would a user's best plan of action be on receiving an e-mail message warning of a virus that may have accidentally been sent in the past, and suggesting that the user to delete a specific file if it appears on the user's computer?

A. Check for the file and delete it immediately.
B. Check for the file, delete it 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:
A: 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.
B: Copying the email to all distribution lists, is another mistake, because if indeed the email does contain a virus, you'll only spread it.
D: 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.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 79

QUESTION NO: 3
What should a network administrator's first course of action be on receiving an e-mail alerting him to the presence of a virus on the system if a specific executable file exists?

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:
B: 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 really get completely deleted, instead it gets sent to a 'recycle bin.'
C: 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.
D: 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.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 79

QUESTION NO: 4
Which of the following is the major difference between a worm and a Trojan horse?

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.

Incorrect answers:

A: The main difference between a worm and a Trojan horse is not the way they are being spread, but rather the self replicating aspect of worms.
C: Both can be malicious.
D: There are differences of which the worms ability to replicate itself is the distinguishing factor.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 83, 85

QUESTION NO: 5
Which of the following can 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.

Incorrect answers:
A: A virus is a piece of software designed to infect a computer system. A virus may also damage the data on your hard disk, destroy your operating system, and possibly spread to other systems.
B: 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.
C: Designed to take advantage of holes in security, worms are similar in function and behavior to viruses, Trojan horses, and logic bombs-with the exception that they are self-replicating.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 80

QUESTION NO: 6
What type of program will record system keystrokes in a text file and e-mail it to the author, and will also delete system logs every five days or whenever a backup is performed?

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 company's computers if they feel termination is imminent.

Incorrect answers:
A: A virus is a piece of software designed to infect a computer system. A virus may also damage the data on your hard disk, destroy your operating system, and possibly spread to other systems.
B: A back door is not an attack in its own right; it allows a user to enter a system from a different interface or with different credentials.
D: Designed to take advantage of holes in security, worms are similar in function and behavior to viruses, Trojan horses, and logic bombs-with the exception that they are self-replicating.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 80

QUESTION NO: 7
The system administrator of the company has resigned. When the administrator's user ID is deleted, the system suddenly begins deleting files. What type of malicious code is this?

A. Logic bomb
B. Virus
C. Trojan horse

D. Worm

Answer: A
Explanation:
A Logic bomb is a virus or Trojan horse that is built to go off when a particular event occurs or a certain amount of time passes, in this case when the system administrator user ID was deleted.

Incorrect answers:
B: A virus is a piece of software designed to infect a computer system. A virus may also damage the data on your hard disk, destroy your operating system, and possibly spread to other systems.
C: 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.
D: Designed to take advantage of holes in security, worms are similar in function and behavior to viruses, Trojan horses, and logic bombs-with the exception that they are self-replicating.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 80

QUESTION NO: 8
What is an application that appears to perform a useful function but instead contains some sort of malicious code called?

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.

Incorrect answers:
A: Designed to take advantage of holes in security, worms are similar in function and behavior to viruses, Trojan horses, and logic bombs-with the exception that they are self-replicating. B: A SYN flood is connection-oriented protocol TCP that has a process called a three-way handshake. C: A virus is a piece of software designed to infect a computer system. A virus may also damage the data on your hard disk, destroy your operating system, and possibly spread to other systems. E: It is really a virus or Trojan horse that is built to go off when a particular event occurs or a certain amount of time passes.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 80

QUESTION NO: 9
What is a piece of code that appears to do something useful while performing a harmful and unexpected function like stealing passwords called?

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.

Incorrect answers:
A: 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. B

: It is really a virus or Trojan horse that is built to go off when a particular event occurs or a certain amount of time passes.
C: Designed to take advantage of holes in security, worms are similar in function and behavior to viruses, Trojan horses, and logic bombs-with the exception that they are self-replicating.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 84

QUESTION NO: 10
What is a piece of malicious code that has no productive purpose but can replicate itself and exist only to damage computer systems or create further vulnerabilities called?

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.

Incorrect answers:
A: It is really a virus or Trojan horse that is built to go off when a particular event occurs or a certain amount of time passes.
B: Designed to take advantage of holes in security, worms are similar in function and behavior to viruses, Trojan horses, and logic bombs-with the exception that they are self-replicating.
C: A Trojan horse could be useful.
D: A SYN flood is connection-oriented protocol TCP that has a process called a three-way handshake.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 76

QUESTION NO: 11
Which of the following is used to describe an autonomous agent that copies itself into one or more host programs, then propagates when the host is run?

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.

Incorrect answers:
A: A Trojan horse appears to be useful software, but code is hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code.
B: A back door is not an attack in its own right; it allows a user to enter a system from a different interface or with different credentials.
C: It is really a virus or Trojan horse that is built to go off when a particular event occurs or a certain amount of time passes.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 76

QUESTION NO: 12
What is a program that can infect other programs by modifying them to include a version of it called?

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.

Incorrect answers:
A: This is an inherent characteristic of viruses. A software virus is a small chunk of code designed to attach to other code. It typically has a dual purpose: It needs to replicate, and it typically has some other purpose or action that it takes when triggered to do so.
C: A Trojan horse appears to be useful software, but code is hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code.
D: It is really a virus or Trojan horse that is built to go off when a particular event occurs or a certain amount of time passes.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 533

QUESTION NO: 13
What type of virus can hides itself by intercepting disk access requests?

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 so as to avoid detection. An infected file may report a file size different from what is actually present in order to avoid detection.

Incorrect answers:
A: A multipartite virus infects multiple locations on a system. These viruses typically infect memory first and then copy themselves to multiple other locations, such as the boot sector of each hard disk, files, and executables on the system.
C: Stealth viruses are also called interrupt interceptors.
D: A polymorphic virus, or mutating virus, changes or mutates as it copies itself to other files or programs. The goal is to make it difficult to detect and remove the virus.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 80
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 1

QUESTION NO: 14
Which of the following are 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 viruses require the user to actually do something. During the 80's and early 90's most viruses 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 viruses have no objective at all, but some have the objective to delete data, hog up memory, or crash the system.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 1

QUESTION NO: 15
What is a program that appears to be useful but contains hidden code that allows unauthorized individuals to exploit or destroy data is commonly known?

A. A virus
B. A Trojan horse
C. A worm
D. A back door

Answer: B
Explanation:
A Trojan horse appears to be useful software (and in fact may be), but code is hidden inside that will attack your system directly or allow the system to be infiltrated by the originator of the code

Incorrect answers:
A: A software virus, in similar fashion, is a small chunk of code designed to attach to other code. It typically has a dual purpose: It needs to replicate, and it typically has some other purpose or action that it takes when triggered to do so.
C: Worms are similar in function and behavior to viruses, Trojan horses, and logic bombs-with the exception that they are self-replicating.
D: A backdoor is an opening left in a program application (usually by the developer) that allows additional access to data.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter 1

1.6 Understand the concept of and know how to reduce the risks of social engineering (10 questions)

QUESTION NO: 1
With regards to the use of Instant Messaging, which of the following type of attack can best be guarded against by user awareness training?

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

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.

Incorrect answers:
B: Instant Messaging is not a measure for combating the risk of stealth attacks.
C: Ambush attacks cannot be combated through Instant Messaging.

D: A multi-pronged attack can be combated using technical means.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 87

QUESTION NO: 2
What is the most common method of social engineering?

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.

Incorrect answers:
A: This is not social engineering.
C: This option is also a form of social engineering, but not as common as calling users and asking for information.
D: This is not specific enough to be called social engineering.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 87

QUESTION NO: 3
What do intruders use most often to gain unauthorized-access 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.

Incorrect answers:
A: A brute force attack is an attempt to guess passwords until a successful guess occurs. This type of attack usually occurs over a long period.
B: Logging of keystrokes involves being at the workstation itself.
C: 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. This involves too much effort compared to social engineering.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 57, 87

QUESTION NO: 4
Which of the following measures can be used to guard against 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.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.83

QUESTION NO: 5
Which of the following is an example of the theft of network passwords without the use of software tools?

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.

Incorrect answers:
A: A Trojan is a software "code" used to infiltrate a network, like the installation of zombie software used for remote control attacks.
C: Sniffing is an application that captures all traffic traveling past a network interface attached to some network.
D: Hacking is both hardware and software based.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter 2

QUESTION NO: 6
Which of the following type of attack CANNOT 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 cannot be deterred through technical means.

Incorrect answers:
A: To prevent this type of attack you need to put technical measures in place that forces users to make use of difficult passwords.
B: In this attack, a third system is placed between two hosts (electronically) already communicating or currently in the process of setting up a communication channel. Positive mutual authentication between the end points of a given session is probably the best way to prevent these attacks. Certificates can be used for mutual authentication.
C: The Denial of service attack can be deterred through technical means because they make a target machine unavailable as the result of a buffer overrun and a crash. These DoS attacks are not application specific and can be prevented by a firewall.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter 3

QUESTION NO: 7
Why do social engineering attacks often 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.

Incorrect answers:
A: Social engineering does not rely on passwords only. This can be accessed through human emotive pleas.
C: Multiple logins is not the cause of social engineering.
D: Audit logs are irrelevant when considering social engineering attack success.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.83

QUESTION NO: 8
In which of the following would an attacker impersonate a dissatisfied customer of a company and requesting a password change on the customer's account?

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.

Incorrect answers:
A: SNMP agents are used in hostile code.
C: In IP Spoofing a hacker can impersonate a valid service by sourcing traffic using the service's IP address or name.
D:A man-in-the-middle attack is commonly used to gather information in transit between two hosts.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter 3

QUESTION NO: 9

You are the network administrator at TestKing.com. During a routing site audit of TestKing's wireless network, you discover an unauthorized Access Point under the desk of Sales department user. 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 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.

Incorrect answers:
A: A SYN flood, forces a victim system to use up one of its finite number of connections for each connection the initiator opens.
B: Distributed denial of service attacks are multicell attacks.
C: A man-in-the-middle attack is commonly used to gather information in transit between two hosts.
D: In this attack, the source system sends a flood of SYN requests and never sends the final ACK, creating a half-open TCP session.
E: In IP Spoofing a hacker can impersonate a valid service by sourcing traffic using the service's IP address or name.
G: A replay attack is similar in part to a man-in-the-middle attack. In this instance, an attacker intercepts traffic between two end points and retransmits or replays it later.
H: Phone tag is not the same as social engineering.
I: You are not a victim of a Halloween attack in this case.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 87
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter 3

QUESTION NO: 10
Which of the following is the most effective defense against a social engineering attack?

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

Answer: D
Explanation:
Social engineering is the method of using human intelligence methods to gain access or information about your organization. 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.

Incorrect answers:
A: Marking documents is not a human intelligence method of gaining password information. B: Escorting will prevent guests from talking to users to gain access to their password, etc. but this does not mean that you can escort them 24/7.
C: A badge security system does not prevent malicious individuals from gaining access to a valid badge.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 83

1.7 Understand the concept and significance of auditing, logging and system scanning (3 questions)

QUESTION NO: 1
Which of the following network mapping tools 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.

Incorrect answers:
A: Port scan is an automated procedure of initiating sessions on every specified TCP port to see whether the host replies.
B: Map scanning is mainly used to identify targets for attack.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter 3

QUESTION NO: 2
What can an attacker can determine which network services are enabled on a target system?

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 the protocols pass through them.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 69

QUESTION NO: 3

What type of port scan is used to determine which 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.

Incorrect answers:
B: TCP connect scans are used to identify potential targets and services. This type of scan utilizes the full TCP three-way handshake.
C: When a basic firewall or router blocks other TCP scans, the TCP FIN scan can be used. It is used to identify listening TCP ports based on a response, or lack of a response, to a finish (FIN) packet.
D: A TCP scan designed to penetrate firewalls and filtering routers is the TCP NULL scan. A NULL scan is similar to the XMAS scan in that TCP sequence numbers are zero, but the NULL scan passes no flags at all.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 1

Topic 2, Communication Security (79 questions)

2.1 Recognize and understand the administration of the various types of remote access technologies. (12 questions)

QUESTION NO: 1
Which of the following is a VPN (Virtual Private Network) protocol that operates at the Network Layer (Layer 3) of the OSI (Open Systems Interconnect) model?

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.

Incorrect answers:
A: PPP is a full-duplex line protocol that supersedes SLIP (Serial Line Internet Protocol) often used in dial-up connections operating at layer 2.
B: SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.
C: L2TP is a tunneling protocol that adds functionality to PPP. This protocol was created by Microsoft and Cisco and is often used with virtual private networks (VPNs) operating at layer 2.

Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 5, Lesson 2

QUESTION NO: 2
Which of the following is a tunneling protocol that only works on IP networks?

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

Answer: C
Explanation:
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). It was 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.

Incorrect answers:
A: IPX is a connectionless, routable network protocol based on the Xerox XNS architecture. It's the default protocol for versions of NetWare before NetWare 5 and operates at the Network layer of the OSI model and is responsible for addressing and routing packets to workstations or servers on other networks.
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
D: SSH is a replacement for rlogin in Unix/Linux that includes security. rlogin allowed one host to establish a connection with another with no real security being employed SSH replaces it with slogin and digital certificates.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 122

QUESTION NO: 3
On a firewall, which ports must be open in order to support L2TP (Layer Two Tunneling Protocol) and PPTP (Point-to-Point Tunneling Protocol) connections respectively?

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 port 1723 and TCP for connections.

Incorrect answers:
A: TCP port 635 is used by RLZ Dbase and UDP port 654 is used by OADV.
B: TCP port 749 is used for Kerberos Admin, UDP port 781 is used by HP Performance data collector.
D: This is used by RADIUS accounting.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 120
http://www.iana.org/assignments/port-numbers

QUESTION NO: 4
Which of the following are VPN (Virtual Private Network) tunneling protocols? (Choose two)

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

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

Incorrect answers:
A: PPP is an encapsulation protocol usually associated with ISDN.
B: SLIP is an old protocol used for direct serial line connections between two computers.
D: Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail between SMTP servers.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 120

QUESTION NO: 5
In addition to opening the appropriate L2TP (Layer Two Tunneling Protocol) and IKE (Internet Key Exchange) transport layer ports on the perimeter router and firewall, what steps 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 a client and the firewall?

A. The perimeter router and firewall must allow inbound protocol number 51 for ESP (Encapsulating Security Payload) encapsulated IPSec (Internet Protocol Security) traffic
B. The perimeter router and firewall must allow inbound protocol number 49 for ESP (Encapsulating Security Payload) encapsulated IPSec (Internet Protocol Security) traffic
C. The perimeter router and firewall must allow inbound protocol numbers 50 and 51 for ESP (Encapsulating Security Payload) and All (Authentication Header) encapsulated IPSec (Internet Protocol Security) traffic
D. The perimeter router and firewall must 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).

Incorrect answers:
A: This alone will not allow traffic flow between a client and a firewall.
B: This option will not allow AH and ESP IPSec traffic between client and firewall.
D: Port 53 is used for DNS server lookups and SQL client name lookup.

References:

http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=

QUESTION NO: 6
Which of the following can be 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.

Incorrect answers:
A: ESP is a header used to provide a mix of security services in IPv4 and IPv6. ESP can be used alone or in combination with the IP Authentication Header (AH). But this is not enough to authenticate and encrypt IP traffic.
B: S/MIME) is a standard used for encrypting e-mail not IP traffic.
D: IPv2 does not authenticate and encrypt IP traffic.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 127

QUESTION NO: 7
Which of the following 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:
Tunneling refers creating a virtual dedicated connection between two systems or networks. You create the tunnel between the two ends by encapsulating the data in a mutually-agreed-upon protocol for transmission. In most tunnels, the data passed through the tunnel appears at the other side as part of the network. 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.

Incorrect answers:
A: PPP is not a tunneling protocol and as such cannot be used to create a VPN.
C, D: These protocols are not used in the creation of a VPN.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 30-31

QUESTION NO: 8
Which of the following are VPN (Virtual Private Network) 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:
Tunneling refers creating a virtual dedicated connection between two systems or networks. You create the tunnel between the two ends by encapsulating the data in a mutually-agreed-upon protocol for transmission. In most tunnels, the data passed through the tunnel appears at the other side as part of the network. 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.

Incorrect answers:
A, C: SSL is not a tunneling protocol.
B: PPP is not a tunneling protocol.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 30-32

QUESTION NO: 9

What is the biggest benefit to using RADIUS (Remote Authentication Dial-in User Service) for a multi-site VPN (Virtual Private Network) that supports a large number 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.**

Incorrect answers:
B: This is incorrect.
C: This is incorrect as a database is used in RADIUS.
D: There is no replication of user database as RADIUS gives you a single source for the authentication to take place.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 121-122

QUESTION NO: 10
On a firewall, which ports must be open in order to support TACACS?

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

Answer: D
Explanation:

TACACS uses both TCP and UDP port 49.

Incorrect answers:
A: This port is used for FTP's control channel.
B: UDP port 161 is used by SNMP. C: Port 53
is used for DNS.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 64
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 2

QUESTION NO: 11
On a firewall, which ports must be open in order to support SSH (Secure Shell)?

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.

Incorrect answers:
B: UDP port 69 is used for TFTP.
C, D: Port 17 is used for the quote of the day and port 179 is used for Border gateway protocol. SSH does not require the use of these ports for functionality.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 64,127
http://www.iana.org/assignments/port-numbers

QUESTION NO: 12
Which of the following is an 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.
SSH is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also provides alternative, security-equivalent, programs for such Unix standards as Telnet, FTP, and many other communications-oriented programs. SSH is now available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other clear text-oriented programs in the Unix environment. SSH uses port 22 and TCP for connections.

Incorrect answers:
A: The Data Encryption Standard (DES) is a strong and efficient algorithm based on a 56-bit key. (Strong refers to the fact that it's hard to break.) DES has several modes that offer security and integrity. However, it has become a little dated as a result of advances in computer technology, and it's being replaced. For its time, it was one of the best standards available. B: This cannot be used as an alternative to Telnet. D: This is not an alternative to Telnet.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 120

2.2 Recognize and understand the administration of various email security concepts. (15 questions)

QUESTION NO: 1
On a firewall, which ports must be open in order to support IMAP4?

A. 80
B. 3869

C. 21
D. 110
E. 143
F. 443

Answer: E
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.

Incorrect answers:
A: port 80 is meant for HTTP.
B: Port 3869 is used for hp OVSAM MgmtServer Disco and is thus not meant for IMAP4.
C: Port 21 is the command port for FTP.
D: Port 110 is for POP3
F: Port 443 for HTTPS.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 64,130
http://www.iana.org/assignments/port-numbers

QUESTION NO: 2
What is the main DISADVANTAGE of using a third party mail relay?

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

Answer: A
Explanation:
Using a third 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.

Incorrect answers:

B: Relay actually lends itself to being exploited by unsolicited spammers.
C: This is not the main disadvantage of a relay.
D: The relay does not restrict spammers from gaining access.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 129

QUESTION NO: 3
What is the purpose of S/MIME (Secure Multipurpose Internet Mail Extensions)?

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

Answer: 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.

Incorrect answers:
A: S/MIME is meant to encrypt messages and files, not user names and profiles.
C: A VPN is a private network that provides security over an otherwise unsecure environment. This is not what S/MIME does.
D: It is not only outbound messages that are encrypted.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 330

QUESTION NO: 4
What do you require in order to use S/MIME (Secure Multipurpose Internet Mail Extensions)?

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

Incorrect answers:
B: You need a digital certificate and not a server side certificate.
C: This is not necessary for S/MIME.
D: You need a digital certificate with S/MIME instead.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 330

QUESTION NO: 5
What are the possible results of a malformed MIME (Multipurpose Internet Mail Extensions) header?

A. It can create a back door that will allow an attacker free access to a company's private network.
B. It can create a virus that infects a user's computer.
C. It can cause an unauthorized disclosure of private information.
D. It can 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.

Incorrect answers:
A: It does not create a backdoor. This is usually the result of a Trojan horse. B: Viruses are not created due to malformed MIME. C: This is not a result of malformed MIME.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 330

QUESTION NO: 6
Which of the following is often used to encrypt e-mail messages?

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.

Incorrect answers:
B: BINDING allows zone transfers to be signed.
C: DES is a strong and efficient algorithm based on a 56-bit key. But it has been replaced.
D: SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 368

QUESTION NO: 7
Which of the following represents the greatest benefit of using S/MIME /Secure Multipurpose Internet Mail Extension)?

A. It allows users to send encrypted and digitally sign e-mail messages.
B. It allows users to send anonymous e-mails.
C. It allows users to send e-mails with a return receipt.
D. It expedites the delivery of e-mail.

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.

Incorrect answers:
B: S/MIME allows for digitally signed, more secure e-mail, anonymity is thus out of the question.
C: This is not an S/MIME benefit.
D: This is not the main benefit of S/MIME.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 368

QUESTION NO: 8
Which of the following is a possible technical impact of receiving 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.**

Incorrect answers:
B: Processor underutilization usually occurs when the buffer overflows. C: DoS will occur before you experience hard drive space reduction. D: This is a secondary result of spamming.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 221

QUESTION NO: 9
With regard to viruses and hoaxes, which of the following is TRUE? (Choose the best answer)

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.

Incorrect answers:
B: Hoaxes are not harmless and can in fact cause a lot of damage. C:
It does not educate users. D: This is false.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 79
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 6, Lesson 1

QUESTION NO: 10
Which types of attachments should be filtered from e-mails to minimize the danger of viruses?

A. Text files.
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.

Incorrect answers:
A, B, C: These types of files also pose a threat, but not as big a threat as executable files.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 78

QUESTION NO: 11
Which of the following 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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 79

Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 6, Lesson 1

QUESTION NO: 12
Which of the following does PGP use to encrypt data?

A. An asymmetric scheme
B. A symmetric scheme
C. a symmetric key distribution system
D. An asymmetric key distribution

Answer: A
Explanation:
PGP is a shareware implementation of RSA encryption. Pretty Good Privacy (PGP) is a set of software tools that allows you to encrypt, decrypt, and digitally sign computer data and e-mail. PGP's encryption and decryption services are asymmetric.

Incorrect answers:
B, C, and D: 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 secret key-sometimes referred to as a private key-is a key that isn't disclosed to people who aren't authorized to use the encryption system. The disclosure of a private key breaches the security of the encryption system. If a key is lost or stolen, the entire process is breached. DES, 3DES, CAST, RC, Blowfish and IDEA Blowfish are all examples of encryption using a symmetric scheme.
Asymmetric algorithms use two keys to encrypt and decrypt data. These keys are referred to as the public key and the private key. The public 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. As you may recall, symmetrical systems require the key to be private between the two parties. With asymmetric systems, each circuit has one key. RSA, Diffie-Hellman, ECC and El Gamal are examples of encryption using asymmetrical schemes.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 292-294
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 6, Lesson 1

QUESTION NO: 13
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
Explanation:
"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.

Incorrect answers:
A: S/MIME contains signature data. It uses the PKCS #7 standard (Cryptographic Message Syntax Standard) and is the most widely supported standard used to secure e-mail communications.
C: MIME is the predecessor of S/MIME.
D: PEM is created with three digital signature algorithms.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 292-294
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 6, Lesson 1

QUESTION NO: 14
Which of the following defines the ability to verify that an e-mail message received has not been modified in transit?

A. Authorization
B. Non-repudiation
C. Integrity

D. Cryptographic mapping

Answer: C
Explanation:
The goal of integrity is to verify that information being used is accurate and hasn't been tampered with. Integrity is coupled with accountability to ensure that data is accurate and that a final authority exists to verify this, if needed.

Incorrect answers:
A: Authorization has to do with an access to issue.
B: Non-repudiation The ability (by whatever means) to verify that data was seen by an intended party. It makes sure they received the data and can't repudiate (dispute) that it arrived.
D: Cryptographic mapping does not verify whether e-mail has been tampered with or not.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 286

QUESTION NO: 15
Which of the following would best protect the confidentiality and integrity of an e-mail 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
Explanation:
Secure Multipurpose Internet Mail Extensions (S/MIME) is a standard used for encrypting e-mail.
S/MIME contains signature data. It uses the PKCS #7 standard (Cryptographic Message Syntax Standard) and is the most widely supported standard used to secure e-mail communications.

Incorrect answers:
A: The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. The SHA is a one-way hash that provides a hash value that can be used with an encryption protocol B: IPSec is a set of protocols that enable encryption, authentication, and integrity over IP.

C: A digital signature is an electronic signature whose sole purpose is to authenticate the sender.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 330

2.3 Recognize and understand the administration of the various internet security concepts. (31 questions)

QUESTION NO: 1
You work as the security administrator at TestKing.com. You want to configure the TestKing network to allow only HTTP (Hypertext Transfer Protocol) traffic for outbound Internet connections. You also want to set permissions to allow only certain users to browse the web. Which of the following should you use?

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

Answer: C
Explanation:
A proxy server is a type of server that makes a single Internet connection and services requests **on behalf of many users. It 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.

Incorrect answers:
A: A proxy server would be more suited to the needs of the company.
B: A protocol analyzer is not used to set permissions to allow only certain users access to browse the web.
D

: A stateful firewall not only examine packets at the Network layer, but also gather information about the packet's communications session from all layers to determine whether a packet is valid in the context in which it is received. But this is all proxy-able.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 463

QUESTION NO: 2
You work as the security administrator at TestKing.com. You notice that an e-mail server is currently relaying e-mail (including spam) for any e-mail server requesting relaying. On further investigation you discover the existence of /etc/mail/relay domains. How should you modify 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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 129-130

QUESTION NO: 3
What is the main purpose of an e-mail relay server?

A. It is used to block all spam, which allows the e-mail system to function more efficiently without the additional load of spam.
B. It is used to prevent viruses from entering the network.

C. It is used to defend the primary e-mail server and limit the effects of any attack.
D. It is used to 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, viruses, and arbitrary access.

Incorrect answers:
A: This is but one function of how it can be used.
B: This will not prevent viruses from entering the network.
D: It cannot eliminate vulnerabilities.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 129-130

QUESTION NO: 4
Why should e-mail server be configured to prevent e-mail relay?

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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 129-130

QUESTION NO: 5

Which of the following can 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.

Incorrect answers:
B: Port scanning is when an attacker can systematically query your network to determine which services and ports are open.
C: This is the study and practice of finding weaknesses in ciphers.
D: Reverse engineering is the process of re-creating the functionality of an item by first deciding what the result is and then creating something from scratch that serves the same purpose.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 183-184

QUESTION NO: 6
On a firewall, which ports must be open in order to support e-mail communication using SMTP (Simple Mail Transfer Protocol)?

A. TCP (Transmission Control Protocol) port 110 to all inbound and outbound connections.
B. UDP (User Datagram Protocol) port 110 to all inbound connections.
C. UDP (User Datagram Protocol) port 25 to all inbound connections.
D. 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.

Incorrect answers:
A, B, C: SMTP is a protocol for sending e-mail between SMTP servers. Whereas POP3 is the protocol used to download e-mail from an SMTP e-mail server to a network client.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 64

QUESTION NO: 7
How many steps are used during the SSL (Secure Sockets Layer) handshake process?

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

Answer: B
Explanation:
SSL establishes a stateful connection negotiated by a handshaking procedure between client and server. During this handshake, the client and server exchange the specifications for the cipher that will be used for that session. 1. The handshake begins when a browser connects to an SSL-enabled server, and asks the (2) 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); (3) 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. (4) 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.

(5) The server replies with more random data (which doesn't have to be encrypted), and (6) then both parties 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.

Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 4

QUESTION NO: 8
What will the SSL (Secure Sockets Layer) enabled server do first when a user clicks to browse a secure page?

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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 365

QUESTION NO: 9
Which of the following types of encryption does SSL (Secure Sockets Layer) 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.

Incorrect answers:
A: SSL makes use of symmetric key exchange not asymmetric keys.
C: Public keys are not necessarily symmetric and neither is it used in SSL.
D: Secret encryption does not mean symmetric key exchange which is used by SSL.

Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 4

QUESTION NO: 10
Which of the following steps in the SSL (Secure Socket Layer) protocol allows for client and server authentication, MAC (Mandatory Access Control) and encryption algorithm negotiation, and selection of cryptographic keys?

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

Answer: D
Explanation:
SSL Handshake Protocol
* runs before any application data is transmitted
* provides mutual authentication
* establishes secret encryption keys
* establishes secret MAC keys

Incorrect answers:
A: Handshake protocol occurs before alert protocol.
B: The change cipher spec protocol only occurs after the application protocol.
C: Record protocol encompasses the handshake, alert and change cipher spec protocols in SSL.

Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 4
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 178

QUESTION NO: 11
Which of the following protocols is used to encrypt 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.

Incorrect answers:
A: IP Security (IPSec) is a security protocol that provides authentication and encryption across the Internet.
B: HTTP is the protocol used for communication between a web server and a web browser. Communication is not encryption.
D: A VPN is a system that uses the public Internet as a backbone for a private interconnection (network) between locations.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 365

QUESTION NO: 12

Which of the following protocols does a web server use 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.

Incorrect answers:
A: TCP/IP) is the protocol suite developed by the DoD in conjunction with the Internet. It was designed as an internetworking protocol suite that could route information around network failures.
B: ActiveX is a technology implemented by Microsoft that allows customized controls, icons, and other features to increase the usability of web-enabled systems.
C: IP Security (IPSec) is a security protocol that provides authentication and encryption across the Internet.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 365

QUESTION NO: 13
In which lengths are SSL (Secure Sockets Layer) session keys available? (Choose two)

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

Answer: A. C

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:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 4
http ://wp.netscape. com/security/techbriefs/ssl .html

QUESTION NO: 14
Which of the following protocols is used to 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.

Incorrect answers:
A: Secure Multipurpose Internet Mail Extensions (S/MIME) is a standard used for encrypting e-mail.
B: XML can be used to generate standard or fully customized content rich Web pages, documents, and applications. XML is used to provide widely accessible services and data to end users, exchange data among applications, and capture and represent data in a large variety of custom and standard formats.
D: SMTP is a protocol for sending e-mail between SMTP servers.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 365

QUESTION NO: 15
Which of the following represents the main advantage of using 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.

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

Incorrect answers:
A: This is not the main advantage.
C: This is not an advantage when both have the same capability.
D: This is an advantage, but not the main difference and advantage between SSL and HTTPS.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION NO: 16
What does a web client and server require in order for an SSL (Secure Sockets Layer) connection to be established between them automatically?

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

Incorrect answers:
A: A shared password is not the way in which SSL allows a secure connection to be established. C: An address on the same subnet does not necessarily mean an automatic connection. D: A common operating system does not automatically mean a connection.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION NO: 17
Which of the following is a key function introduced SSLv3.0 (Secure Sockets Layer version 3.0)?

A. The ability to act as a CA (Certificate Authority).
B. The ability to force client side authentication via digital certificates.
C. The ability to use x.400 certificates.
D. The ability to 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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION NO: 18
On a firewall, which ports must be open in order to support SSL (Secure Sockets Layer)?

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'

Incorrect answers:
A: UDP port 80 is meant for HTTP.
B: TCP port 80 is used for HTTP without the secure socket layer.
D: UDP port 69 is used for TFTP.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 2

QUESTION NO: 19
Which of the following allows 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. None of the above.

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.

Incorrect answers:
B: Integrated web with NOS security do not guarantee secure access.
C: SSL only would be browser or vendor specific. D: This is irrelevant.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION NO: 20
Between which layers of the OSI (Open Systems Interconnection) model does SSL (Secure Sockets Layer) operate? (Choose all that apply)

A. The Application Layer.
B. The Transport Layer
C. The Network Layer
D. The Data Link Layer
E. The Physical Layer

Answer: A, B
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. SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.

Incorrect answers:
C, D and E: The OSI model and SSL operates between the application layer and the transport layer not the Network, Data Link or Physical layers.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION NO: 21
What makes Instant Messaging 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 EVI 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.
Instant messaging is a form of immediate e-mail that takes place between two or more users. IM clients are often prone to hostile code (usually in the form of file transfers) and subject to social engineering attacks, wherein a hacker plays upon the culpability of a user to get what they need.

Incorrect answers:
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 EVI messaging system that transverse the Internet uses it as a medium.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 21

QUESTION NO: 22
Which of the following is the greatest vulnerability of using Instant Messaging clients?

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:
Instant Messaging (IM) enables users to communicate in real-time using text messages and to exchange files (pictures, music, and so on) with one another. Thus EVI clients can also be compromised by malicious code, Trojan Horse programs, and traditional DoS attacks. IM clients are often prone to hostile code (usually in the form of file transfers) and subject to social engineering attacks, wherein a hacker plays upon the culpability of a user to get what they need.

Incorrect answers:
A: This is a result of spoofing.
B: This could result from a buffer overflow attack.
D: Slow internet connection could be ping of death attack results.
E: Loss of e-mail privileges is dependent on company policy.
F: Blue screen of Death errors is the result of a Winnuke attack.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 21

QUESTION NO: 23
Which of the following is the biggest problem associated with Instant Messaging?

A. It is widely deployed and difficult to control.
B. It was created without security in mind.
C. It is easily spoofed.
D. It is 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.

Incorrect answers:
A: Other real time communication was designed with security in mind as well and is probable just as widely used.
C: A spoofing attack is an attempt by someone or something to masquerade as someone else. But in Instant Messaging this is not necessarily an attack. It could also be a safety measure.
D: Messaging is not necessarily file sharing.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 21

QUESTION NO: 24
Which of the following is Instant Messaging 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.

Incorrect answers:
A: DoS attacks are the result of flood attacks.
B: Fraud attacks do not usually result from Instant Messaging.
C: Stability? This is irrelevant in this case.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 21
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 2

QUESTION NO: 25
With which privileges are ActiveX control executed?

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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 128

QUESTION NO: 26
Which of the following is responsible for displaying an install dialog box for 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.

Incorrect answers:
B: This is not how ActiveX dialog boxes are installed.
C: The sandbox is a set of rules used when creating a Java applet that prevents certain functions when the applet is sent as part of a web page. This is not responsible for installing dialog boxes.
D: Negotiation between client and server is not how ActiveX dialog boxes are installed.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 135

QUESTION NO: 27
Which of the following are used to prove where ActiveX controls originated from?

A. Encryption.
B. Their location on the web server.
C. SSL (Secure Sockets Layer).
D. Digital signatures.

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.

Incorrect answers:
A: Encryption does not reveal origin.
B: Location of ActiveX controls on the Web server will not reveal where the controls originated from.
C: SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 128,135
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 2

QUESTION NO: 28
Which of the following can be used to track a user's browsing habits on the Internet?

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.

Incorrect answers:
A: Digital certificates are used in authentication not user browsing habit tracking.
C: ActiveX objects are system components that can be initialized and scripted from a variety of environments, including HTML-formatted email messages. ActiveX objects are versatile and can do nearly anything, depending on how they are written. But they are not used to track browsing habits.
D: Web server cache is not used to track user browser habits.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 128,135

QUESTION NO: 29
Which of the following can be 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.

Answer: 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 every time 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.

Incorrect answers:
A, **C:** HTTPS is a combination of HTTP with Secure Socket Layer (SSL) to make for a secure connection.IT is the protocol used for communication between a web server and a web browser.
D: This is not used to retain data connection and user information, etc.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION NO: 30
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 a doubtful choice 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.**

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 136

Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 5

QUESTION NO: 31
When hosting a web server with CGI (Common Gateway Interface) scripts, which permissions should the directories for public view have?

A. Read
B. Execute
C. Read and Write
D. Read, Write, and Execute
E. Full Control

Answer: B
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.

Incorrect answers:
A, C& D: CGI scripts are executed on the server and as such should have the execute permission in directories for public view.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 136, 217
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 5

2.4 Recognize and understand the administration of the various directory security concepts. (4 questions)

QUESTION NO: 1
Which of the following is 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.**

Incorrect answers:
B: MPLS (Multi-Protocol Label Switching) is not similar to SSLv3.
C: Strong authentication over LDAP v3 is provided through Simple Authentication and Security Layer (SASL) communications defined in RFC 2222. This is not similar to SSLv3
D: Multi-Layer Switching is not the same as SSLv3.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

QUESTION NO: 2
On a firewall, which ports must be open in order to allow LDAP (Lightweight Directory Access Protocol) traffic?

A. 389 and 636
B. 389 and 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.

Incorrect answers:
B: Port 139 is the NetBIOS session service port.

C: NetBIOS services occurs via ports 137, 138, and 139
D: Port 139 is the NetBIOS session service port.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 64
http://www.iana.org/assignments/port-numbers

QUESTION NO: 3
What is the start of the LDAP (Lightweight Directory Access Protocol) directory called?

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

Answer: B
Explanation:
LDAP directories are arranged as trees. The top of the hierarchy is called the LDAP root. 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.

Incorrect answers:
A: The top of the hierarchy is called the root and not the head.
C: This top is known as the root.
D: The whole directory is arranged as trees. And the top is called the root.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2 http: //www. intranetj ournal. com/foundati on/l dap. shtml

QUESTION NO: 4

How are LDAP (Lightweight Directory Access Protocol) directories arranged?

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

Answer: B
Explanation:
Directories are displayed best as directory trees, so naturally LDAP uses trees. LDAP is based from an object-orientated access model built to directory enabled networking (DEN) standards. The top of the hierarchy is called the LDAP root. The LDAP root server creates the hierarchy and the rest of the structure (and resources) branch out from that location. LDAP uses objects to represent computers, user accounts, shared resources, services, and so on.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

2.5 Recognize and understand the administration of the various file transfer protocols and concepts. (6 questions)

QUESTION NO: 1
Which of the following is vulnerable to having username and password information intercepted by packet sniffing?

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.

Incorrect answers:

A: Secure Shell (SSH) is a replacement for rlogin in Unix/Linux that includes security. rlogin **allowed one host to establish a connection with another with no real security being employed;** SSH replaces it with slogin and digital certificates.
B: Secure Socket Layer (SSL) is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.
D: Secure Hypertext Transfer Protocol (S-HTTP) is a protocol used for secure communications between a web server and a web browser.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 130

QUESTION NO: 2
How can you ensure that only authorized users can access a FTP (File Transfer Protocol) 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.

Incorrect answers:
A: Blind FTP is synonymous to anonymous FTP and allowing blind FTP is not the way to ensure that only authorized users access the FTP server.
C: Redirection will not prevent unauthorized access.
D: This is impractical as it will not prevent unauthorized access.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 1
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 137

QUESTION NO: 3
Should you enabling anonymous FTP (File Transfer Protocol) read/write access, which of the following could occur?

A. An upload and download directory for each user.
B. Detailed logging information for each user.
C. The 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 non-secure logon, then answer C would seem to be the best answer.

Incorrect answers:
A: This is the legitimate use of an FTP site.
B: You need to have a logon for any FTP (without anonymous access enabled) you want to access.
D: This is not the answer.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 1

QUESTION NO: 4
What is the purpose of a FTP (File Transfer Protocol) bounce attack?

A. Exploiting a buffer overflow vulnerability on the FTP (File Transfer Protocol) server
B. Rebooting the FTP (File Transfer Protocol) server
C. Storing and distributing malicious code
D. Establishing a connection between the FTP (File Transfer Protocol) server and another computer

Answer: D
Explanation:

FTP bounce is a method that attackers use to protect their identity when scanning your network, by bouncing the scan off a vulnerable FTP server. 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.

Incorrect answers:
A: In an attack, the buffer overflow condition can be used to damage files, change data, acquire confidential information, or execute code on the target computer. The attacker might even be able to gain full control over the target system.
B: Rebooting the server is not the aim of a FTP bounce attack.
C: The primary aim of a FTP bounce attack is to establish an illegitimate connection not storing and distributing malicious code. This is secondary.

References:
http://www.cert.org/advisories/CA-1997-27.html
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 1

QUESTION NO: 5
On a firewall, which ports must be open in order to allow FTP (File Transfer Protocol) traffic?

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.

Incorrect answers:
B: Port 25 is for SMTP. Port 110 is for POP3
C: Port 80 is used by HTTP (used for the World Wide Web) and port 443 for HTTPS (used for secure web connections)
D: Ports 161 and 162 are used for SNMP messages and traps respectively.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 64
http://www.iana.org/assignments/port-numbers

QUESTION NO: 6
Which of the following ports are used to access FTP (File Transfer Protocol)?

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.

Incorrect answers:
A: Port 80 is used by HTTP (used for the World Wide Web) and port 443 for HTTPS (used for secure web connections) C: Port 23 is used by Telnet. D: Port 80 is used by HTTP.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 64
http://www.iana.org/assignments/port-numbers

2.6 Recognize and understand the administration of the various wireless technologies and concepts. (11 questions)

QUESTION NO: 1
Which of the following do attackers most often use 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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 109

QUESTION NO: 2
What is the maximum data transmission rate of IEEE (Institute of Electrical and Electronics Engineers) 802.11b?

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:
The 802.1 1b standard provides for bandwidth of up to 1 1Mbps in the 2.4GHz frequency spectrum.

Incorrect answers:
A, B: This is below the maximum bandwidth that can be accommodated by 802.1 1b. D: This is above the maximum bandwidth that 802.1 1b can accommodate.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 193

QUESTION NO: 3
Which of the following can 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.

Incorrect answers:
A: ESP is a header used to provide a mix of security services in IPv4 and IPv6. ESP can be used alone or in combination with the IP Authentication Header (AH).
C: Transport Layer Security (TLS) is a protocol whose purpose is to verify that secure communications between a server and a client remain secure. Not exactly prevention of intruders.
D: SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer. It does not prevent intruders from intruding.

References:
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

QUESTION NO: 4
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.

Incorrect answers:
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.
B: Wireless systems frequently use the Wireless Access Protocol (WAP) for network communications.
C: An electronic transaction is not the same as providing the means for secure communication insofar as privacy, data integrity and authentication is concerned.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 177-179

QUESTION NO: 5
Between which of the following does WTLS (Wireless Transport Layer Security) provides security services?

A. A Web server.
B. A mobile device.
C. A Wireless client.
D. A Wireless network interface card.
E. A WAP (Wireless Application Protocol) gateway

Answer: B, E
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 security layer of the Wireless Applications Protocol (WAP). WTLS provides authentication, encryption, and data integrity for wireless devices between a wireless device and the WAP gateway.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 177-178

QUESTION NO: 6
Which of the following provides a WLAN (Wireless Local Area Network) with the level of security associated with a LAN (Local Area Network)?

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.

Incorrect answers:
B: This is not the method to supply security to a WLAN akin to a LAN.
C: ISDN is a telecommunications standard that is used to digitally send voice, data, and video signals over the same lines.
D: VPN is a system that uses the public Internet as a backbone for a private interconnection (network) between locations. This is not WLAN with the security levels akin to a LAN.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 372

QUESTION NO: 7
What should be done to secure the wireless network environment that uses access points as repeaters?

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.

Incorrect answers:
A: Making use of complex passwords is not the same as repeaters.
B: Ensuring that wireless cards are used is not the same as providing security in the form of repeaters. This in fact might enhance the danger.
D: Adhoc mode is the same as a point-to-point (ad-hoc or wireless bridge), a network created when two devices are brought within transmission range of each other. This is not the same as security.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 186

QUESTION NO: 8
In a wireless network that uses WEP (Wired Equivalent Privacy) to provide wireless security, which of the following may authenticate to an 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:
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. Server authentication requires the workstation to authenticate against the server (access point).

Incorrect answers:
A: This option should be more specific and mention from where the administrator operates from.
B: This is not true as this would make a farce of security.
C: Only users within the company are not correct since WEP applies to mobile users and the option should rather state users with the correct WEP key.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 117
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

QUESTION NO: 9
What is the purpose of WEP (Wired Equivalent Privacy)?

A. To provide a WLAN (Wireless Local Area Network) with the same level of security as a wired LAN (Local Area Network).
B. To provide a collision preventive method of media access for a WLAN (Wireless Local Area Network).
C. To provide a WLAN (Wireless Local Area Network) with a wider access area that that of a wired LAN (Local Area Network).
D. To allow radio frequencies to penetrate walls.

Answer: A
Explanation:
WEP is a security protocol for 802.1 1b (wireless) networks that attempts to establish the same security for them as would be present in a wired network. It is designed to provide privacy equivalent to that of a wired network.

Incorrect answers:
B: Providing collision prevention is not the purpose of WEP.

C: WEP is a security protocol, not a WLAN extender.
D: The purpose of WEP is not to allow radio frequencies to penetrate walls. That is just the way in which it is used.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 335

QUESTION NO: 10
On which of the following is the WAP (Wireless Application Protocol) programming model based?

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:
Wireless networking is not unlike networking on cable. Computers can be connected to form a client/server network. Hubs and switches can be used to connect network segments and allow communications over a broader area.
WAP systems communicate using a WAP gateway system. The gateway converts information back and forth between HTTP and WAP, as well as encodes and decodes between the security protocols.

Incorrect answers:
A: There must be a gateway between client and server. WEP is intended to provide the security for WAP.
B: This is not how WAP works.
C: The wireless interface card is not the same as a gateway.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 179

QUESTION NO: 11
Which of the following can be used to provide 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
Explanation:
WEP is a security protocol for 802.1 1b (wireless) networks that attempts to establish the same security for them as would be present in a wired network. It is designed to provide privacy equivalent to that of a wired network.

Incorrect answers:
A: SWP is a method of securing wireless networks that is beginning to gain momentum and acceptance.
C: SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.
D: S M I M E provides email privacy using encryption and authentication via digital signatures.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, p. 335

Topic 3, Infrastructure Security (88 questions)

3.1 Understand security concerns and concepts of the various types of devices. (33 questions)

QUESTION NO: 1
What type of program highlights the vulnerabilities of servers on the network to various exploits and suggests ways to mitigate the vulnerabilities?

A. Intrusion detection
B. Port scanner

C. Vulnerability scanner
D. Trojan scanner

Answer: C
Explanation:
A vulnerability assessment uses a set of tools to identify vulnerabilities in a network. It usually works by scanning the network for IP hosts and identifying the different services running on the computers on the network. Each service is then probed to test the service for its security against known vulnerabilities. These tools then reports the vulnerabilities it finds on each computer, their level of risk, and suggests methods for mitigating these risks.

Incorrect Answers:
A: Intrusion diction systems detect possible attacks by monitoring network behavior, scanning packet header information, and examining the contents of packets. It does not check for vulnerabilities.
B: Port scanning and sniffers are often used as part of a vulnerability assessment; however, on their own, they do not report methods for mitigating against risks.
D: There is no such thing as a Trojan scanner.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 422.
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 301.

QUESTION NO: 2
Which of the following can be used to review network traffic and determine which services are running on the network?

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

Answer: A
Explanation:
Packet sniffers are used to capture, monitor and analyze network traffic. There legitimate purpose is to find traffic flow problems and bottlenecks. However, hackers use it to capture data, to use in replay attacks.

Incorrect Answers:
B: Intrusion diction systems detect possible attacks by monitoring network behavior, scanning packet header information, and examining the contents of packets. It does not check for vulnerabilities.
C: A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network.
D: A router interconnects two discontiguous or dissimilar networks. It does not review traffic.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 422.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 67.

QUESTION NO: 3
You work as a security administrator at TestKing.com. You are reconfiguring a UNIX server so as to make it less susceptible to an attacker obtaining the user account passwords. You decide to have the encrypted passwords contained within a file that is readable only by root. What is a common name for this file?

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

Answer: B
Explanation:
The shadow password file is a UNIX file that contains password related user information, including the encrypted user passwords. This file is readable only by superuser and/or members of a specified group that has root access because the file is only readable by root.

Incorrect Answers:
A: The passwd file is a UNIX file used to store user information for each user on the system. This information includes the user's login name and an encrypted version of the user's password. Although the passwords are encrypted, the passwrd file has general read permission, so the file may be read by any authenticated users or process. C, D:

The hosts.allow and hosts.deny files are access control lists that control the systems that are allowed or denied specified services. The hosts are identified by their IP addresses or host names.

References:
Bozidar Levi, UNIX Administration - A Comprehensive Sourcebook for Effective Systems and Network Management, Boca Raton (FL), CRC Press, 2002, pp. 170-171, 195-198, 364.

QUESTION NO: 4
Which of the following is NOT a valid reason for supporting the recommendation that only essential services be provided by a particular host, and any unnecessary services be disabled?

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:
All services are part of the operating system and do not require additional software. Furthermore, services are optimized to run on a computer that meets the minimum system requirements for the operating system. Therefore no additional hardware is required. However, additional hardware and software can be used to supplement certain services but this is not a requirement.

Incorrect Answers:
A: All unnecessary services should be disabled as each service running on a server has its own vulnerabilities that could be exploited.
C: Unnecessary services would generate unnecessary logging. Thus disabling unnecessary services will reduce logging.
D: Some firewalls, especially software based firewalls can only block well known ports. Thus, if an unnecessary service does not use a well known port, the firewall will not be able to control access to that port.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 115-117, 201-216.

QUESTION NO: 5
You work as a security administrator at TestKing.com. On examining the server's list of protocols that are bound and active on each network interface card, you notice a relatively large number of protocols. What should you do 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.

Incorrect Answers:
A: All unnecessary port or services should be disabled as each unnecessary port or services have its own vulnerabilities that can be exploited.
B: On most operating systems, a default protocol suite is installed during installation of the operating system. After the operating system is installed, the administrator should disable unnecessary protocols so as to harden the computer against attack.
D: Port filtering can block access to a port. However, protocols can be mapped to different ports.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 115-117, 201-216.

QUESTION NO: 6

Why are single servers often the targets of attack?

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

Answer: C
Explanation:
In a single server environment, all user credentials are stored on one server. A successful attack on that server will thus give the attacker access to usernames, addresses, and password hashes for all network users.

Incorrect Answers:
A: A single server may contain launch scripts but this is not likely.
B: Each computer on a network, regardless if they are servers or workstations, will contain security policy settings.
D: Master encryption keys are only created in a PKI system. It is unlikely that a single server network will use a PKI system.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 115-117, 201-216.

QUESTION NO: 7
You work as a security administrator at TestKing.com. A network administrator has just replaced a hub with a switch. When you use software to sniff packets from the network, you notice that you can detect communication only between his computer and the servers on the network. You cannot detect communications between other network clients and the servers. The network administrator assures you that the switch is functioning properly. What is the most likely cause of this problem?

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. For this reason, sniffers cannot be used on a switched network.

Incorrect Answers:
B: VLANS can be implemented to segment a network using one switch. In this system, the ports a grouped into a virtual LAN. Thus VLANS are switched networks. Sniffers cannot be used on a switched network because they do not use broadcast addresses.
C: Sniffers cannot be used on a switched network, regardless of the software configuration. D: Sniffers can be used only in the local segment. They cannot be used on a switched network because they do not use broadcast addresses.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 67, 114.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp. 78, 92.

QUESTION NO: 8
What should be performed before implementing a wireless solution?

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 affect 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.

Incorrect Answers:
A: Ad hoc mode allows two wireless devices to communicate directly with each other without the need for a wireless access point.
B: Ensuringstrong passwords will improve authentication but will not prevent interception of packet.
C: Wireless solutions can consist of Wi-Fi devices and Bluetooth enabled devices.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 180.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 219.

QUESTION NO: 9
Which of the following security mechanisms can be used to control the flow of packets traveling through routers?

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

Answer: C
Explanation:
ACLs control access to resources based on user permissions or IP address. On a router, an ACL can allow or deny a machine access to a network based on the machine's IP address.

Incorrect Answers:
C: OSPF policies can also be used to control the flow of packets traveling through routers. There are two OSPF policies: OSPF Accept Policies and OSPF Announce Policies. OSPF Accept Policies can be configured to prevent the forwarding of packets to external networks. OSPF Announce Policies can be prevent the advertising of external routes. However, these can only be applied to OSPF enabled routes. B, D: There is not such thing as fault tolerance tables or packet locks.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 216.
http://www.rhyshaden.com/ospf.htm

QUESTION NO: 10
In which of the following can privilege policy based tables be used to confine sensitive data traffic to workstations on a specific subnet?

A. A router.
B. A server.
C. A modem.
D. A 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. It can be configured to prevent or allow specific systems from accessing a network based to the system's IP addresses, thus controlling the flow of data.

Incorrect Answers:
B: Datatraffic passes through a router rather than a server and is controlled at the router.
C: A modem is used for remote access and does not support the configuration of security policies.
D: A VPN is a remote access method that tunnels through an insecure, public network. It is not a privilege policy based table.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 105-107, 112-114, 216.

QUESTION NO: 11
In a VPN (Virtual Private Network), which of the following will be encrypted by using IPSec (Internet Protocol Security) in the tunnel mode?

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).

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 112-114.

QUESTION NO: 12
What is the first step in implementing a firewall?

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:
A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network. The first step in implementing a firewall is to develop a firewall policy that defines how the firewall should filter traffic and the types of traffic that should be blocked or allowed.

Incorrect Answers:
A, **B:** The firewall policy should define which types of traffic and which ports should be permitted and which should be blocked.
D: There is no effective defense against a DDoS attack.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 76.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 100-104.

QUESTION NO: 13
Which of the following is the best IDS (Intrusion Detection System) to monitor the entire network?

A. A network based IDS (Intrusion Detection System).
B. A host based IDS (Intrusion Detection System).

C. A user based IDS (Intrusion Detection System).
D. A client based IDS (Intrusion Detection System).

Answer: A
Explanation:
An intrusion detection system (IDS) monitors inbound and outbound network traffic on a host or network in order to detect an attempted intrusion. This can be either a host based IDS, which monitors traffic to and from a single host, or a network based IDS, which monitors network traffic. Thus, network based IDS is not limited to a single server but monitors the traffic over the entire network

Incorrect Answers:
B: A host based IDS monitors traffic to and from a single host, which can be a server or a workstation.
C, D: There is no user based or client based IDS.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 162-164.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 422-432.

QUESTION NO: 14
What does a firewall use to ensure that each packet is part of an established TCP (Transmission Control Protocol) session?

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

Answer: C
Explanation:
A stateful inspection firewall uses a state table to keep track of every communications channel at all levels of the network. This provides additional security in connectionless protocols such as User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP).

Incorrect Answers:

A: A packet filtering firewall block or permits traffic of a particular type. It does not track the session to which the packet belongs.
B: There is no such thing as a stateless inspection firewall; only a stateful inspection firewall, a packet filtering firewall and a proxy firewall.
D: Circuit-level gateways operate at the OSI session layer to monitor TCP handshaking to decide whether session requests should be allowed or denied. It does not track other TCP packets or other protocols.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 100-104.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 331-341.
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 115.
http ://www.informit. com/articles/article.asp?p= 101741 &seqNum=3

QUESTION NO: 15
What is the basic strategy for configuring the rules for a secure firewall?

A. Permit all.
B. Deny all.
C. Default permit.
D. Default deny.

Answer: D
Explanation:
A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network. It should be configured to allow only explicitly permitted. All types of traffic and ports that are not explicitly permitted, should be denied by default.

A: A permit all policy would make a firewall obsolete as the purpose of a firewall is to block unwanted traffic.
B: A deny all policy will mean that no traffic is allowed through the firewall. This will effective prevent traffic between the trusted internal network and the external network.
C: A default permit policy would be a vulnerability as it means that ports and types of traffic that have not been explicitly allowed or blocked would be allowed to pass through the firewall.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 100-104.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341.

QUESTION NO: 16
Which of the following is a security consideration that is introduced by a VPN (Virtual Private Network)?

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

Answer: D
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.

Incorrect Answers:
A: VPNtraffic is tunneled through the public network and cannot be intercepted.
B: Encrypted data cannot easily be decrypted.
C: A tunneled connection can be authenticated via RADIUS. Once connected, the normal network management systems can be used for authorization and accounting.

Reference:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 76.

QUESTION NO: 17
Which of the following can be used to limit hostile sniffing on a LAN (Local Area Network)?

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

D. A firewall.

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. For this reason, sniffers cannot be used on a switched network.

Incorrect Answers:
B: An Ethernet hub transmits traffic out all ports. For this reason it does not prevent sniffing.
C: A CSU/DSU is a connection device for digital serial connections such as T1. It does not prevent sniffing.
D: A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network. However, a firewall does not prevent sniffing on the internal network.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 100-104.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341.
David Groth and Toby Skandier, Network+ Study Guide, 4th Edition, San Francisco, Sybex, p 36.

QUESTION NO: 18
Which of the following represents the best protection against the abuse of remote maintenance of PBX (Private Branch Exchange) system?

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: A
Explanation:

PBX systems are maintained by the vendor of the system. This is accomplished through remote maintenance. You can prevent an attacker from exploiting a PBX system by turning off maintenance features until the vendor informs you that maintenance is required.

Incorrect Answers:
B: Maintenance is performed by the vendor which would not have a user account in your network. Therefore authentication is not possible.
C: Limiting physical access to the PBX system will not defend it against remote attacks.
D: Checking to see if a caller is on a list would require unnecessary administrative overhead and would be inefficient.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 354.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 80.

QUESTION NO: 19
Which of the following security mechanisms can be applied to modems to better authenticate remote users?

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

Answer: D
Explanation:
Callback is security measure that can be implemented in remote access authentications. When a user connects to the modem, the modem calls the user back at a predefined telephone number. This limits remote access to the network.

Incorrect Answers:
A: A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network. It cannot be applied to a modem.
B, C: A modem is a network connection device. Encryption cannot be applied to devices, only to **data; neither can SSH, which is also an encryption system.**

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 100-104.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341, 352-353.

QUESTION NO: 20
Which of the following method would most likely allow an attacker that is attempting to penetrate a company's network through its remote access system to gain access?

A. War dialer.
B. Trojan horse.
C. DoS (Denial of Service).
D. Worm.

Answer: A
Explanation:
A war dialer is a program that dials a block of telephone numbers in the attempt to fins a remote access computer to connect to. Although advances in telecom technology has made it easier to identify war dialers, war dialer remain a threat to remote access systems

Incorrect Answers:
B: A Trojan horse is a piece of malicious code that is included in a useful looking program. It is used to create backdoors into systems. This type of attack usually does not require remote access but an Internet connection.
C: A DoS attack attempts to affect the availability of network resources and serviced. This type of attack usually does not require remote access but an Internet connection.
D: A worm is a program that replicates itself by means of computer networks. It resides in active memory and is usually spread via e-mail.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 56, 71, 80, 82, 100, 202.

QUESTION NO: 21
You work as a security administrator at TestKing.com. Mobile users require remote connectivity in

orderto access shared files and e-mail on the corporate network. All mobile uses have laptops equipped with Ethernet adapters. Some also have modems. What is the best remote access solution to allow all mobile users 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 VPN is a network connection that tunnels through a public network, providing the same level of security as a local connection. When the salesmen create a VPN connection, they will be required to authenticate to the VPN server. Once authenticated, they will virtual access to a private network that is safe, secure, and encrypted. However, their access to resources on the private network will be determined by their permissions on those resources.

Incorrect Answers:
A: ISDN is used mainly for Internet connectivity but can be used for remote access. However, this would require an ISDN modem.
B: Dial-up is a remote access method that requires the use of modems in both the remote access **clients and the remote access server. Not all laptops have modems; therefore this option will not** meet the needs of all laptop users.
C: SSL is a website technology used to secure communication between a browser and a web server. It is not used for remote access.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 105-108, 119, 258, 353. Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 110, 112-114, 325.

QUESTION NO: 22
Which of the following is the 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 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. For this reason, sniffers cannot be used on a switched network.

Incorrect Answers:
A: An intrusion detection system (IDS) monitors inbound and outbound network traffic on a host or network in order to detect an attempted intrusion.
B: Promiscuous mode allows a network card to intercept all traffic on the network, not just the traffic intended for it. Disabling promiscuous mode will ensure that the network card does not intercept traffic. However, this does not prevent sniffing.
C: An Ethernet hub transmits traffic out all ports. For this reason it does not prevent sniffing.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 67, 100-104.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341.
David Groth and Toby Skandier, Network+ Study Guide, 4th Edition, San Francisco, Sybex, p 36.

QUESTION NO: 23
Which two parts does an IDS (Intrusion Detection Systems) typically consist of? (Choose two)

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

Answer: B D
Explanation:
An IDS has a number of components including a sensor and an analyzer. The sensor collects the data which is then passed on to the analyzer. The analyzer analyzes the data for suspicious activity. When suspicious activity is identified, an alert is sent to the operator either via e-mail or a console.

Incorrect Answers:
A: A router connects two networks, including two disparate networks. C: A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that **enters and/or leaves a network. A firewall is not part of an IDS system; however, an IDS can be** used in conjunction with a firewall to increase security.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 162-164.

QUESTION NO: 24
What is the main advantage of using a multi-homed firewall?

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

Answer: C
Explanation:
A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network. A multi-homed firewall has two or more network cards. This allows for the distinction between multiple networks and allows for the creation of a demilitarized zone (DMZ). The DMZ hosts publicly accessible servers, such as web or FTP. The firewall provides secured but public access to the DMZ, while blocking access to the private network. If the multi-homed firewall is compromised, only the systems in the DMZ will be exposed.

Incorrect Answers:
A: A multi-homed firewall is simply a firewall that has multiple network cards. Network cards are relatively inexpensive. However, this is not the main advantage of multi-homed firewalls. A firewall is a security device. Therefore, a multi-homed firewalls ability to create a distinction between different networks is more important.
B: A multi-homed firewall would require filters on all network cards, thus increasing the complexity of filtering while also increasing security.
D: **It** would not be possible for the attacker to circumvent the second firewall as it would be configured to block all traffic to the private network.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 76.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 100-104.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341.

QUESTION NO: 25
Which of the following is the best defense 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:
In IP Spoofing attacks the attacker attempts to gain access to the internal network by using an IP address that matches the internal network address, thus pretending his or her computer is on the internal network. This attack can be prevented by implementing ingress IP address filtering at the network perimeter. This will block inbound traffic from the outside.

Incorrect Answers:
A: IDS uses known attack signatures and anomalies in network traffic behavior to detect intruders. It does not detect spoofed IP addresses.
B: A DMZ is a network zone that holds servers and resources that need to be accessible to a public network. This DMZ is usually separated from the internal network by a firewall. D: IP address filtering can mitigate against IP spoofing.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 78.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 54-55.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 65-67.

QUESTION NO: 26
Which of the following is usually NOT included in security requirements for servers?

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:
Granting any user administrative privileges would allow any user full control over the system and would render that administrative account obsolete. This would not be a good security measure.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 259.

QUESTION NO: 27
You work as a security administrator at TestKing.com. You need to confine sensitive data traffic to a specific subnet. Which of the following could you use?

A. A router.
B. A server.
C. A switch.
D. A 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. It can be configured to prevent or allow specific systems from accessing a network based to the system's IP addresses, thus controlling the flow of data.

Incorrect Answers:
B: Datatraffic passes through a router rather than a server and is controlled at the router.
C: You can use a switch to segment a specific network or subnet by using VLANs. This however does not confine traffic to only that segment.

D: A VPN is a remote access method that tunnels through an insecure, public network. It is not confine network traffic.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 105-107, 112-114, 216.

QUESTION NO: 28
What may an active detection IDS system perform when it discovers an unauthorized connection attempt? (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.

Incorrect Answers:
A: Informing the attacker of his or her activities would not prevent the exploitation of the system.
C: Providing the attacker with a usernames and passwords for administrative accounts would entirely compromise the system.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 162-164.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 422-432.

QUESTION NO: 29
Which of the following

attacks 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:
An intrusion detection system (IDS) monitors inbound and outbound network traffic on a host or network in order to detect an attempted intrusion. E-mail messages are not network traffic, therefore spoofed emails will not be detected by the IDS.

Incorrect Answers:
A, **B, D:** An intrusion detection system (IDS) monitors inbound and outbound network traffic on a host or network in order to detect an attempted intrusion. This includes DoS attacks, port scans, and vulnerability exploits.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 162-164.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 422-432.

QUESTION NO: 30
What are servers or workstations that run programs and utilities for recording probes and attacks against them called?

A. Firewalls.
B. Host based IDS (Intrusion Detection System).
C. Proxies.
D. Active targets.

Answer: B
Explanation:

An intrusion detection system (IDS) monitors inbound and outbound network traffic on a host or network in order to detect an attempted intrusion. 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.

Incorrect Answers:
A: A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network.
C: A proxy is a type of firewall that prevents direct communication between a host on the internal network and a host on the external network.
D: There is not such thing as an active agent; perhaps in the CIA, but not in computer security anyway.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 100-104, 162-164.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 331-341, 422-432.

QUESTION NO: 31
Which of the following is a DISADVANTAGE of employing an IDS (Intrusion Detection System)?

A. False positives.
B. Throughput decreases.
C. Compatibility.
D. Administration.

Answer: A
Explanation:
An intrusion detection system (IDS) monitors inbound and outbound network traffic on a host or network in order to detect an attempted intrusion. Sometimes an IDS will mistake legitimate traffic for an intrusion. This is called a false positive.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 95.

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 162-164, 173-174.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 422-432.

QUESTION NO: 32
With regard to network based lDSs (Intrusion Detection Systems), which of the following statements is true?

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

Answer: D
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.

Incorrect answers:
A, **B, C:** Network based IDSs are usually passive and do not interfere with the normal operation of the network.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 422-432.

QUESTION NO: 33
What type of system will examine all packets on an internal network for known attack signatures?

A. A vulnerability scanner.

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

Answer: D
Explanation:
An intrusion detection system (IDS) monitors inbound and outbound network traffic on a host or network in order to detect an attempted intrusion. This can be either a host based IDS, which monitors traffic to and from a single host, or a network based IDS, which monitors network traffic. Thus, network based IDS is not limited to a single server but monitors the traffic over the entire network

Incorrect Answers:
A: Avulnerability scanner is used to detect and report known vulnerabilities in a network. It does not monitor network traffic.
B: A packet filter is a type of firewall that filters out types of network traffic that it is configured to block. It does not monitor the traffic for known attack signatures but simply drops it if that type of traffic is blocked.
C: A host based IDS monitors traffic to and from a single host, which can be a server or a workstation.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 162-164.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 422-432.
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 301.

3.2 Understand the security concerns for the various types of media. (5 questions)

QUESTION NO: 1
Which of the following network media types is most immune to eavesdropping and electromagnetic interference?

A. STP (Shielded Twisted Pair) cable.
B. UTP (Unshielded Twisted Pair) cable.
C. Coaxial cable.
D. Fiber-optic cable.

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.

Incorrect answers:
A, B: UTP and STP cabling isn't as secure as coax since it can be easily tapped into, and it's used primarily for internal wiring. It's more difficult to splice into a twisted pair cable, but three-way breakout boxes are easy to build or buy.
C: Coax is present in many older networks and tends to provide reliable service once it's installed. However, if a terminator, NIC card, T-connector, or inline connector malfunctions or becomes disconnected, the entire segment of wire in that network will malfunction, and network services will cease operation. Coax can fail when handled.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 132-135

QUESTION NO: 2
Which of the following media types provides the lowest risk to RF (Radio Frequency) eavesdropping?

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

Answer: B
Explanation:
Fiber optic cable is relatively secure because it cannot be easily tapped. It is the strongest media available to defeat EMI and RFI in my opinion.

Incorrect answers: A

: Coax is present in many older networks and tends to provide reliable service once it's installed. Coax can fail when handled. Because the electrical signal is conducted by a single core wire, someone can easily tap the wire by piercing the sheath. He would then be able to eavesdrop on the conversations of all the hosts attached to the segment because 10BASE-2 coaxial cabling implements broadband transmission technology and assumes many hosts connected to the same wire.
C: Twisted pair cabling isn't as secure as fiber optic since it can be easily tapped into, and it's used primarily for internal wiring. It's more difficult to splice into a twisted pair cable, but three-way breakout boxes are easy to build or buy.
D: Unbounded cabling does not provide protection against RF eavesdropping.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 132-135

QUESTION NO: 3
Which of the following media types provides the most 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 is designed for short- and long-range transmissions at speeds higher than 1Gbps. It uses light pulses for signal transmission, making it immune to RFI and EMI.

Incorrect answers:
A: Because the electrical signal is conducted by a single core wire, someone can easily tap the wire by piercing the sheath. He would then be able to eavesdrop on the conversations of all the hosts attached to the segment because 10BASE-2 coaxial cabling implements broadband transmission technology and assumes many hosts connected to the same wire.
B: UTP has no shielding and is prone to radio frequency interference (RFI) and electromagnetic **interference (EMI); however, its installation is relatively simple and its cost low.**
C: STP cable has a single shield around all the pairs. STP wraps a shield, like a coax, over the wires, but is also vulnerable to interference from electromagnets and radio frequency.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 132-135

QUESTION NO: 4
Which of the following media types provides the least protection against electromagnetic interference?

A. Coaxial cable.
B. UTP (Unshielded Twisted Pair).
C. STP (Shielded Twisted Pair).
D. Fiber optic cable.

Answer: B
Explanation:
UTP has no shielding and is prone to radio frequency interference (RFI) and electromagnetic **interference (EMI); however, its installation is relatively simple and its cost low.**

Incorrect answers:
A: Coax is used in many older networks and tends to provide reliable service once it's installed. Coax can fail when handled and can be affected by electromagnetic interference and radio frequency interference.
C: STP cable has a single shield around all the pairs. STP wraps a shield, like a coax, over the wires, but is also vulnerable to interference from electromagnets and radio frequency. D: 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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 132-135

QUESTION NO: 5
On which of the following types of network cabling is eavesdropping the MOST difficult?

A. Fiber optic cable.

B. Coaxial cable.
C. UTP (Unshielded Twisted Pair).
D. STP (Shielded Twisted Pair).

Answer: A
Explanation:
As far as security is concerned, fiber cabling eliminates the tapping of electrical signals that is possible in the case of twisted pair and coax. Tapping fiber cable without service interruption and specially constructed equipment is impossible, which makes stealing service or eavesdropping on traffic significantly more difficult.

Incorrect answers:
B: Because the electrical signal is conducted by a single core wire, someone can easily tap the wire by piercing the sheath. He would then be able to eavesdrop on the conversations of all the hosts attached to the segment because 10BASE-2 coaxial cabling implements broadband transmission technology and assumes many hosts connected to the same wire. C, D: UTP has no shielding and is prone to radio frequency interference (RFI) and **electromagnetic interference (EMI); however, its installation is relatively simple and its cost low.** Both UTP and STP can be tapped, although it is physically a little trickier than tapping coaxial cable because of the physical structure of STP and UTP cable. The major difference from coaxial cable is the connection method. Whereas coaxial cable runs from computer to computer, twisted pair cabling runs from computer to concentrator-hub, repeater, bridge, switch, Multi-Station Access Unit (MSAU), and so on. Therefore, the service is more vulnerable to abuse and theft in those concentration spots.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 132-135

3.3 Understand the concepts behind the various kinds of Security Topologies. (17 questions)

QUESTION NO: 1
You work as the security administrator at TestKing.com. You want to establish a secure connection between headquarters and a branch office over a public network. In which mode should you configure the router at each location to use IPSec (Internet Protocol Security)?

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.

Incorrect answers:
A: The mode that IPSec operate in is either transport- or tunnel mode.
C: Transport mode encrypts only the payload.
D: The mode that IPSec operate in is either transport- or tunnel mode.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 127

QUESTION NO: 2
Which of the following can be used to mitigate against sniffers and decrease broadcast traffic?

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.

Incorrect answers: A

: A virtual private network (VPN) is a private network connection that occurs through a public network. This in itself is not a measure to decrease broadcast traffic.
B: A demilitarized zone (DMZ) is an area where you can place a public server for access by people you might not trust otherwise. It is not used to mitigate against sniffers.
D: A RADIUS server can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether an incoming caller is authorized. In a large network with many connections, this allows a single server to perform all authentications. But this will not decrease broadcast traffic.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 28, 112

QUESTION NO: 3
You work as the network administrator at TestKing.com. You want to restrict internal access to other parts of the network. Your solution will be hardware based and must be implemented with the least amount of administrative effort. Which of the following would be your 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.

Incorrect answers:
A: Firewalls are used to keep external users from intruding. This is not the best solution under the circumstances.
C

: A proxy firewall can be thought of as an intermediary between your network and any other **network. Used to process requests from an outside network; the proxy firewall examines the data** and makes rules-based decisions about whether the request should be forwarded or refused. The proxy intercepts all the packages and reprocesses them for use internally. This process includes hiding IP addresses. However, this is not a hardware based solution as is required by the question.
D: Implementing a VLAN is not what is required in this case as it is not hardware based.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, pp. 102, 112

QUESTION NO: 4
What is the process by which remote users make a secure connection to internal resources after establishing an Internet connection called?

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. For example: a VPN or even SSL.

Incorrect answers:
A, C and D: Channeling, throughput and forwarding is not used when establishing a secure Internet connection to internal resources.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 29

QUESTION NO: 5

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.

Incorrect answers:
A: Authentication Header (AH) is a header used to provide connectionless integrity and data origin authentication for IP datagrams, and used to provide protection against replays. B: SSH is a replacement for rlogin in Unix/Linux that includes security. D: DES is a block cipher algorithm used for encryption.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 127

QUESTION NO: 6
Tunneling is _____

A. the process of 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. the process of 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 ordinary/non-secure IP packets into encrypted/secure IP packets.

Incorrect answers:
B: Tunneling is not meant to burrow through firewalls. It is meant to provide safe passage for ordinary non-secure packets into encrypted secure packets.
C: It is not a matter of time, but rather a matter of having a safe way of passing data packets. D: The tunnel itself does not capture data.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, p. 30

QUESTION NO: 7
Which of the following best describes tunneling?

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

Answer: B
Explanation:
Tunneling refers creating a virtual dedicated connection between two systems or networks. You create the tunnel between the two ends by encapsulating the data in a mutually-agreed-upon protocol for transmission. In most tunnels, the data passed through the tunnel appears at the other side as part of the network. Tunneling sends private data across a public network by placing (encapsulating) that data into other packets. Most tunnels are virtual private networks (VPNs).

Incorrect answers:
A: This is a vice versa description of tunneling.
C: This is not correct as ordinary non-secure data gets encapsulated inside of encrypted/secure IP packets.
D: This is not what tunneling does; this is normal clear text messaging.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, pp. 30-32

QUESTION NO: 8
What is the primary purpose of NAT (Network Address Translation)?

A. To translate IP (Internet Protocol) addresses into user friendly names.
B. To hide internal hosts from the public network.
C. To use on public IP (Internet Protocol) address on the internal network as a name server.
D. To 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.

Incorrect answers:
A: The primary purpose of NAT is to hide internal hosts, not translating IP addresses into user friendly names.
C: This is not the primary purpose of NAT.
D: This would actually defeat the purpose of NAT.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, p. 29

QUESTION NO: 9
When connecting the following IP (Internet Protocol) address schemes to the Internet, which one will require NAT (Network Address Translation)?

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:

The NAT server provides IP addresses to the hosts or systems in the network and tracks inbound and outbound traffic. A company that uses NAT presents a single connection to the network. This connection may be through a router or a NAT server. The only information that an intruder will be able to get is that the connection has a single address. 172.16.0.0 is a private IP address that can be NAT to a IP address.

Incorrect answers:
A, **C, D:** These addresses do not require NAT when connecting to the Internet. The private address ranges are:
10.0.0.0-10.255.255.255
172.16.0.0-172.31.255.255
192.168.0.0-192.168.255.255

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, p. 28

QUESTION NO: 10
Which of the following can be used to accomplish NAT (Network Address Translation)?

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
Explanation:
Both NAT and PAT can be configured for static and dynamic address translation.

Incorrect answers:
B, C and D: Network Address Translation (NAT) - IP proxy is a server that acts as a go-between for clients accessing the Internet. All communications look as if they originated from a proxy server because the IP address of the user making a request is hidden. A proxy server takes on responsibility for providing services between the internal and external network. However, the proxy server can actually be the server providing the services or it can create a separate connection to the requested server. In this way, a proxy server can be used to hide the addressing scheme of the internal network.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, p. 29

QUESTION NO: 11
What is the area in which a system administrator would place the web server to isolate it from other servers on the network called?

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

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

Incorrect answers:
A: A honey pot is a system designed to entice or entrap an attacker. Enticement means inviting or luring an attacker to the system. Entrapment is the process of encouraging an attacker to perform an act, even if they don't want to do it.
B: A Hybrid subnet is not meant for isolating a web server from the other servers on a network.
D: A virtual local area network (VLAN) allows you to create groups of users and systems and segment them on the network. This segmentation lets you hide segments of the network from other segments and thereby control access.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, pp. 28, 185

QUESTION NO: 12

You work as the network administrator at TestKing.com. You want to configure a new web server to provide HTTP (Hypertext Transfer Protocol), SSL (Secure Sockets Layer), FTP (Pile Transfer Protocol), and SMTP (Simple Mail Transfer Protocol) services. The web server will be placed into a DMZ (Demilitarized Zone). Which standard ports must you open on the firewall 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

Incorrect answers:
A: Port 119 TCP is used by Network News Transfer Protocol (NNTP). Port 23 is used by Telnet. Ports 21 and 80 would be a necessity.
B: Ports 443 and 21 would be useful in setting up the web server. Port 119 TCP is used by Network News Transfer Protocol (NNTP). Port 1250 is used for swldy-sias.
D: Only port 110 would not be essential as it is used for POP version 3

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Appendix B
http://www.iana.org/assignments/port-numbers

QUESTION NO: 13
When connecting a network to the Internet, which of the following will ensure that the internal network IP (Internet Protocol) addresses are not compromised?

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.

Incorrect answers:
A: A honey pot is a bogus system set up to attract and slow down a hacker.
C: A VPN is a system that uses the public Internet as a backbone for a private interconnection (network) between locations.
D: A screened network will not necessarily ensure that the internal network IP addresses are not compromised.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, **p** 185

QUESTION NO: 14
Which of the following best 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.
It is 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.

Incorrect answers:

A: This is not what a DMZ is meant to function as.
C: Based on this option then your whole DMZ would compromise the company network.
D: This is not the purpose of a DMZ.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 26
http://www.webopedia.com/TERM/D/DMZ.html

QUESTION NO: 15
Which of the following would be placed in a DMZ (Demilitarized Zone)?

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.

Incorrect answers:
A: The customers will not feel confident in your company as some of their confidential information will be exposed.
B: Staff workstations are not meant to be in a DMZ.
D: Your SQL based database server might hold confidential information that should not be open for scrutiny.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 26

QUESTION NO: 16

Which of the following best describes an extranet?

A. An area or zone set aside for business to store extra servers for internal use.
B. An area or zone accessible to the general public for accessing the business' web site.
C. An area or zone that allows a business to securely transact with other businesses.
D. An area or zone 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 that are trustworthy. An extranet allows you to connect to a partner via a private network or a connection using a secure communications channel using the Internet.

Incorrect answers:
A: An extranet's purpose is not extra storage space.
B: An extranet is meant for transactions and not for the general public to access the site.
D: An extranet is not meant to serve as storage space.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide Second Edition, Sybex Publishing, Alameda, 2004, p. 27

QUESTION NO: 17
Which of the following is the general philosophy behind a DMZ?

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
Explanation:

A DMZ (demilitarized zone) is an area in a network that allows restrictive access to untrusted users and isolates the internal network from access by external users and systems. It does so by using routers and firewalls to limit access to sensitive network resources.

Incorrect answers:
B: A demilitarized zone is accessible from the Internet. C:
This is partly true. D: This is not correct.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide Second Edition, Sybex Publishing, Alameda, 2004, p. 28

3.4 Differentiate the various types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system. (12 questions)

QUESTION NO: 1
Which of the following would NetBus and Back Orifice be an example of?

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

Answer: B
Explanation:
Illicit servers are also known as 'backdoors.' They allow system access without using a security check.
An illicit server is an application/program that shouldn't be there but is operating on the network, and one that is commonly used to gain unauthorized control by allowing someone to bypass normal authentication. NetBus is one of the best-known examples of an illicit server.

Incorrect answers:
A: A virus is a program intended to damage a computer system. Sophisticated viruses are encrypted and hide in a computer and may not appear until the user performs a certain action or until a certain date. For example worms and phage viruses. C: A spoofing attack is an attempt by someone or something to masquerade as someone else.

D: This is exactly the opposite of an illicit server.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide Second Edition, Sybex Publishing, Alameda, 2004, p. 251

QUESTION NO: 2
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.

Incorrect answers:
A: Maintaining the environment would be contradictory to the aim of the intrusion.
B: Only alerting the manager is not what intrusion detection is about. D: It will not discard information.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide Second Edition, Sybex Publishing, Alameda, 2004, p. 115

QUESTION NO: 3
What is it called when an authorized access is detected as an intrusion or attack?

A. A false negative
B. A false intrusion
C. A false positive
D. A false alarm

Answer: B
Explanation:
False intrusion is a false alarm, when there is no need of any alarm.

Incorrect answers:
A: This is a false negative acknowledgments of intrusion in an intrusion detection system, which means an intrusion has occurred but the IDS discarded related events or traces as false signals.
C: A false positive is a false affirmative acknowledgment of intrusion, which means an intrusion detection has incorrectly identified certain events or traces as signaling an attack or intrusion when no such attack or intrusion is underway. Thus, a false positive is a false alarm. A false positive is when legitimate traffic is picked up as an intruder.
D: False alarms can happen if the facility is in a remote location, wildlife and even the wind can set off sound-based motion sensors. These alarms are comprised of microphones and monitoring chips that react when sound is produced in the monitored area, above a preset threshold (this is the area where adjustments can be made). These devices should be used in conjunction with other mechanisms, such as cameras, to help prevent reactions to normal events such as deer, dogs, cats, and the occasional stiff breeze.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 4

QUESTION NO: 4
Which of the following is the most important step that should be taken in response to a security breach?

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.

Incorrect answers:
A: Encryption should have been used as a preventative measure. B: Authentication could have prevented a security breach. D: Intrusion already occurred due to the security breach.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 9

QUESTION NO: 5
Which of the following involves the process of analyzing log files after an attack has started?

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.

Incorrect answers:
A: Active detection mechanisms involve some action taken by the intrusion detection system in response to a suspicious activity or an intrusion (in essence, it is reactive detection). B, C: Covert or overt detection is not the process of analyzing log files after the commencement of an attack.

Reference:
Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 4

QUESTION NO: 6
You work as the security administrator at TestKing.com. TestKing has been receiving a high volume of attacks on the testking.com web site. You want to collect information on the attackers so that legal action can be taken. Which of the following can you use to accomplish this?

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.

Incorrect answers:
A: A demilitarized zone (DMZ) is a method of placing web and other servers that serve the general public outside the firewall and, therefore, isolating them from internal network access. C: A firewall is a combination of hardware and software that protects a network from attack by hackers who could gain access through public networks, including the Internet. D: A new subnet is not going to allow you to collect information from attackers.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 183

QUESTION NO: 7
What is a honey pot?

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.

Incorrect answers:
B: To store passwords in a honey pot would be foolhardy.
C: This is what you would like to keep away from being attacked. Besides the honey pot is somewhat of a decoy.
D: It does exist.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, **p** 185

QUESTION NO: 8
Can honey pots be used to preventing attackers from gaining access to critical systems?

A. Yes
B. No
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.

Incorrect answers:
B: The whole idea of a honey pot is to lure attackers away from the real critical systems. C: This is somewhat obscure.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 185

QUESTION NO: 9
What is a server that is used to attract a potential intruder's attention called?

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.

Incorrect answers:
B, C and D: A server that is used to attract attention away from the real stuff is called a honey pot and not a lame duck, teaser or pigeon.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 185

QUESTION NO: 10
What information do 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.

Incorrect answers: A

: An internal user is not necessarily an intruder. Besides you would presumably know all the internal users.
C: Data within the network is not what the honey pot is supposed to gain intelligence from. D: This is not data from a possible attacker. Besides you would already have the information if the attach is from within the network.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 185

QUESTION NO: 11
Which of the following is a decoy system that is designed to divert an attacker from accessing critical systems while collecting information about the attacker's activity?

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

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.

Incorrect answers:
A: A demilitarized zone (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.
C: An intrusion detector is an item/application performing intrusion detection.
D: A screened host is a router that is in front of a server on the private network. Typically, this server does packet filtering before reaching the firewall/proxy server that services the internal network.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 28, 185

QUESTION NO: 12
When would a severed T1 line most likely be considered?

A. When planning data recovery.
B. When planning off site storage.
C. When planning media destruction.
D. When planning incident response.

Answer: D
Explanation:
Telecommunications technology is developing to the point where all communications occur via data links to phone companies using standard data transmission technologies, such as T1 or T3. This means that both voice and data communications are occurring over the same network connection to a phone company or a provider. This allows a single connection for all communications to a single provider of these services. If someone intentionally severs a T1 cable you have a serious incident on your hands. An attack like this should be considered when planning incident response.

Incorrect answers:
A: Data recovery can be effected through backups and a severed T1 line would not be relevant. B: Offsite storage would not be affected by a severed T1 line. C: Media destruction is not reliant on a T1 line.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 111

3.5 Understand the various concepts of Security Baselines, be able to explain what a Security Baseline is and understand the implementation and configuration of each kind of intrusion detection system. (21 questions)

QUESTION NO: 1
What is the main purpose of TCP (Transmission Control Protocol) wrappers?

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.

Incorrect answers:
A: Wrappers do not prevent IP spoofing.
C: Encryption is not a TCP wrapper's main function.
D: TCP wrappers' main purpose is not to perform sniffing in troubleshooting.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishers, 2004, p. 209

QUESTION NO: 2
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
Explanation:

LDAP utilizes an object-oriented access model defined by the Directory Enabled Networking (DEN) standard, which is based on the Common Information Model (CIM) standard. Buffer overflow vulnerabilities, Format string vulnerabilities may result in unauthorized access to enact commands on the LDAP server or impair its normal operation, and improperly formatted requests may be used to create an effective denial of service (DoS) attack against the LDAP **server, preventing it from responding to normal requests; are the vulnerabilities of LDAP.** However, it is certainly not inferior to SNMP.

Incorrect answers:
A: Mapping into a directory is part of DEN.
C: It does act as an object oriented information model.
D: This statement is true about directory enabled networking.

Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 5

QUESTION NO: 3
You work as the security administrator at TestLing.com. When you perform a port scan against your server you discover four open TCP (Transmission Control Protocol) ports: 25, 110, 143 and 389. You want to close all unnecessary ports to decrease unnecessary exposure. However, TestKing users must be able to connect to the corporate network 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 ports you filter out 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.

Incorrect answers:
A: SMTP makes use of port 25. C: Port 143 is used for HTTPS. D: LDAP (SSL) makes use of this port.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 130
http://www.iana.org/assignments/port-numbers

QUESTION NO: 4
For security purposes, which of the following should be implemented after installing a new operating system?

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, because administrator accounts typically have full rights to all network resources.

Incorrect answers:
A: This can be done after application has been installed.
B: The guest account is not as vulnerable or exploitable as an administrator account.
D: Creating a secure administrator account is still an administrator account that can be exploited if it is not renamed after installing a new operating system.

Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 11

QUESTION NO: 5
On a firewall, which port should be open to allow SNMP traffic?

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

Answer: B
Explanation:
SNMP uses UDP port 161

Incorrect answers:
A: Port 21 is used for FTP.
C: DNS client to server lookup uses this port.
D: Port 49 is not used for SNMP traffic, it is used for Login Host Protocol (TACACS).

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 130
http://www.iana.org/assignments/port-numbers

QUESTION NO: 6
Which of the following are the three entities of the SQL (Structured Query Language) security model? (Choose three)

A. tables
B. actions
C. objects
D. users

Answer: B, C, D
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.

Incorrect answers: A

: A database is a collection of objects such as tables, views, and stored procedures. In other word, tables are user constructs.

Reference:
Kalen Delaney, Inside Microsoft SQL Server 2000, Microsoft Press, Redmond, 2000, Part 2, Chapter 3

QUESTION NO: 7
You work as the security administrator at TestKing.com. TestKing employees often download files from a FTP (File Transfer Protocol) server. You are in the process of installing a firewall. How you configure the firewall?

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.

Incorrect answers:
A, **B:** Port 119 is used by Network News Transfer protocol. Thus you should not use it to set up a FTP server, whether inbound or outbound.
C: Since it is an FTP server, you need not open the port to inbound connections. Else it will defeat the purpose of having an FTP service.

Reference:
http://www.iana.org/assignments/port-numbers

QUESTION NO: 8
Which of the following associates users and groups to certain rights to use, read, write, modify, or execute objects on the system?

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 Open VMS, and Unix-based systems are among the operating systems that use access control lists. The list is implemented differently by each operating system.

Incorrect answers:
A: This is a two-key encryption system wherein messages are encrypted with a private key and decrypted with a public key.
C: This signature validates the integrity of the message and the sender.
D: A CRL is a list of digital certificate revocations that must be regularly downloaded to stay current.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 216
www.whatis.com

QUESTION NO: 9
Which of the following can limit exposure and vulnerability exposed by port scans?

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 65,535 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.

Incorrect answers:
A, B and C: Disabling all the unnecessary programs and processes is the best way of safeguarding yourself against vulnerabilities that can be exploited via port scans.

Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 7
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 67

QUESTION NO: 10
Which of the following represents an advantage of using 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.

Incorrect answers:
A, B and C: Unlike any of the FAT file systems, NTFS supports file-and folder-level permissions. FAT file systems provide complete access locally to the entire FAT partition. **Network access can be achieved regardless of the file system used; therefore, answer B is** incorrect. Support for multiple operating systems is not a feature of NTFS over FAT file **systems; therefore, answer C is incorrect. Streaming video is not a function of the type of file system; therefore, answer A is incorrect.**

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 229

QUESTION NO: 11
How can a DHCP (Dynamic Host Configuration Protocol) service be secured?

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

Answer: A
Explanation:
DHCP works over UDP ports 67 and 68.

Incorrect answers:
B: This will just block DNS client server lookup.
C: This will only block SMPT. D: This will block
POP3.

Reference:
http://www.iana.org/assignments/port-numbers

QUESTION NO: 12
Which of the following can help secure DNS (Domain Name Service) information?

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:

A DNS zone is an area in the DNS hierarchy that is managed as a single unit. 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 hackers' hands if they** were to pose as a DNS server.

Incorrect answers:
A: Blocking all unnecessary traffic will not help secure DNS information.
C: Password changes are not meant to secure DNS information.
D: The default password, whether changed or not, will not secure DNS information.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

QUESTION NO: 13
You work as an e-mail administrator at TestKing.com. You want prevent malicious users from sending e-mails from non-existent domains. What should you do?

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.

Incorrect answers:
B: In forward lookup zones, DNS servers map FQDNs to IP addresses. Forward lookup zones thus answer queries to resolve FQDNs to IP addresses. This will not prevent malicious users sending you e-mail from non-existent domains.
C: As DNS servers make recursive queries on behalf of clients, they temporarily cache resource records. These cached records contain information acquired in the process of answering queries on behalf of a client. Later, when other clients place new queries that request information matching cached resource records, the DNS server can use the cached information to answer these queries. This is thus not a preventative measure.

D: There are no reoccurring queries on a DNS server.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

QUESTION NO: 14
What is SSL (Secure Sockets Layer) used for?

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

Incorrect answers:
A, B and C: SSL is used for secure communications between a web browser and web servers not for file and print servers, RADIUS or AAA.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishers, 2004, p. 126

QUESTION NO: 15
Which of the following 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.

Incorrect answers:
A: A birthday attack is a type of brute force attack and does not so common on your web server per se.
C: E-Mail servers are usually susceptible to spam attacks.
D: Brute force attacks work by trying to randomly guess a password repeatedly against a known account ID. This is not a common web server attack.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishers, 2004, pp. 129,135

QUESTION NO: 16
Which of the following should be prevented 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
Explanation:
Users who can start zone transfers from your server can list all of the records in your zones.

Incorrect answers:
A: Name resolution is a function of DNS, you cannot prevent it.
B: IP address to MAC address resolution occurs through ARP Request and Reply messages. The reverse, MAC to IP resolution, uses Reverse ARP (RARP) Requests and Replies.
C: Name resolution is a function of DNS, you cannot prevent it.

Reference:

Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

QUESTION NO: 17
You work as a security administrator at TestKing .com. You want to secure you primary DNS (Domain Name Service) server against DoS (Denial of Service) attacks and hackers. How should you configure the primary DNS (Domain Name Service)?

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 server's services with domain name requests alone is an engineering feat.

Incorrect answers:
A: This will cause the DNS server to be obsolete and as such is not an option.
C: This will interfere with the functioning of the DNS server.
D: This is not how you secure your DNS server against DoS attacks and hackers.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

QUESTION NO: 18
What should be a system administrator's line of action when a patch is released for a server?

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.

Incorrect answers:
A: This is not advisable because the patch could be a backdoor attack. C: This is not what a patch is meant for. A Patch could be useful. D: Backing up after installing the patch is foolhardy.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 117

QUESTION NO: 19
When disabling services to harden a machine against external attacks, what process should be followed?

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.
Basically this means do some research insofar as services and their dependencies are concerned for your system.

Incorrect answers:
A: DHCP is meant to assign IP addresses and should not be disabled.
B: This does not mean that you will be protected against external attacks. This is only disabling any service as this option suggests.
D: This would be irrelevant as this option suggests that you do actually put financial operations at risk.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 117-120

QUESTION NO: 20
Which of the following represents the best way to harden an application that is developed in house?

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 Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishers, Alameda, 2004, book discusses application hardening and refers this to the web, FTP, and E-mail 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 NO: 21
When securing a server, which of the following would require the most effort 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.

Incorrect answers:
B: Configuring the network in terms of documentation is not half as daunting as hardening an OS due to the lack of documentation.
C: Security policy creation is not as dependant on documentation as hardening of the OS is.
D: You will be hardening the OS when installing the latest hot fixes and patches and thus available documentation is not so crucial in this case.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 210

Topic 4, Basics of Cryptography (84 questions)

4.1 Be able to identify and explain the different kinds of cryptographic algorithms. (22 questions)

QUESTION NO: 1
Which of the following represents the best method of protecting passwords stored on the authentication server?

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.

Incorrect answers:
A: Storing any password in clear text is foolhardy.
C, D: These methods do not represent the best ways to protect passwords that are stored on the authentication server.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 2
With regard to hash encryption, which of the following is true?

A. Hash encryption uses 32 bits.
B. Hash encryption uses 64 bits.
C. Hash encryption uses 128 bits.
D. Hash encryption uses 256 bits.

Answer: C
Explanation:
Hashing produces a 128 bit message digest (hash), very fast, appropriate for medium security usage, e.g. MD4 and MD5. Only SHA-1, also a hash encryption produces a 160 bit message digest (hash), standard for the U.S. government, but slower than MD5.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 287-292

Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 3
Which type of encryption does Block Cipher provide?

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.

Incorrect answers:
B: Block cipher does not provide asymmetric encryption.
C: Only symmetric encryption is provided by Block cipher, not both.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 4
For which of the following can digital signatures be used?

A. Encryption.
B. Asymmetric key.
C. Symmetric key encryption.
D. Public key decryption.

Answer: B
Explanation:

Digital signatures are used to authenticate asymmetric keys.

Incorrect answers:
A: You do not necessary have to make use of digital signatures for encryption. C: Symmetric key encryption does not require digital signatures. D: Digital signatures are not used for Public key encryption.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 5
In the file encryption process, what is the asymmetric algorithm is used for?

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

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

Incorrect answers:
B: It is not the file contents that are encrypted by the asymmetric algorithm.
C: Certificates does not get encrypted in the asymmetric algorithm file encryption process.
D: Hash results are not encrypted in the file encryption process of asymmetric algorithms.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 6
On which of the following key infrastructures is non-repudiation based?

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.

Incorrect answers:
A: Symmetric systems are not non-repudiation based.
B: A distributed trust is not non-repudiation.
D: User-centric systems are not non-repudiation based.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1
Kirk Hausman, Diane Barrett, Martin Weiss, and Ed Tittel, Security+ Certification Exam Cram 2, Indianapolis, Que, 2003, pp. 182-183

QUESTION NO: 7
Which of the following symmetric-key algorithms are used for encryption? (Choose two)

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)

Incorrect answers:
C: Public keys are used with asymmetric encryption algorithms.
D: Secret or Private keys are used in asymmetric encryption algorithms.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 8
What type of encryption algorithm is Advanced Encryption Standard (AES) an example of?

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 and IDEA

Incorrect answers:
A: Wireless Transport Layer Security (WTLS) is the security layer of the Windows Application Protocol
C

: When two or more access methods are included as part of the authentication process, you're implementing a multi-factor system. A system that uses smart cards and passwords is referred to as a two-factor authentication system.
D: Four popular asymmetric systems are in use today are RSA, Diffie-hellman, ECC and El Gamal

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 9
When using symmetric-key encryption, how many keys are needed to encrypt and decrypt data?

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.

Incorrect answers:
A: You only need one key with symmetric encryption.
B: Two keys are used in asymmetric encryption.
D: At least a key is necessary to encrypt and decrypt.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298

Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 10
With regard to asymmetric cryptography, which of the following are true?

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.

Incorrect answers:
B: This is not a necessarily true with asymmetric cryptography. Any of the asymmetric algorithms can be used.
C: Asymmetric cryptography provides a method to validate an individual.
D: It is not limited to a session key.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 11
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

Incorrect answers:
A: CAST is a symmetric encryption algorithm. B:
RC5 is a symmetric encryption algorithm. D:
SHA-1 is a hashing algorithm.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 12
Which of the following types of encryption algorithms is IDEA (International Data Encryption Algorithm), Blowfish, RC5 (Rivest Cipher 5) and CAST-128 examples of?

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.

In 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.

Incorrect answers:
B: Asymmetric encryption algorithms include RSA, Diffie-Hellman and elliptic curve cryptography.
C: Some common hash algorithms currently in use include the MD4, MD5, and SHA-1 algorithms.
D: Elliptic curve is an example of asymmetric encryption algorithm.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 13
In the digital signature process, which of the following security requirements does asymmetric cryptography satisfy?

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

Answer: D
Explanation:
Authentication requires a user to provide some proof or credential that represents something they know, something they have, or something they are before allowing access to your company's resources.

Incorrect answers:
A: Because there is a public key and a private key, the public key can be provided to anyone that you want to send you encrypted information, but only you can decrypt that information. This helps ensure data confidentiality.

B: Access Control is the means of giving or restricting user access to network resources. This is usually accomplished through the use of an ACL (Access Control List).
C: Data integrity refers to the level of confidence that data won't be jeopardized and will be kept secret. 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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress Publishing, 2002, p 513

QUESTION NO: 14
What does an asymmetric algorithm encrypt when a user digitally signs a document?

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

Answer: D
Explanation:
The digital signature is derived from a hash process known only by the originator. 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.

Incorrect answers:
A: Secret pass keys are not encrypted when using digital signatures in an asymmetric algorithm.
B: File content is not encrypted by an asymmetric algorithm when digital signatures are used. C: The document is digitally signed and not the certificates.

Reference:

Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 2925-298

QUESTION NO: 15
What is the primary DISADVANTAGE of symmetric cryptography?

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

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

Incorrect answers:
A: The algorithms used with symmetric encryption are relatively fast, so they impact system performance less and are good for encrypting large amounts of data (for instance, data on a hard disk or data being transmitted across a remote access link).
C: Symmetric algorithms are difficult to decipher without the correct algorithm; therefore they are not easy to break. Well-tested symmetric algorithms such as 3DES and AES are nearly impossible to decipher without the correct key.
D: Memory management does not fall into the disadvantages of symmetric cryptography category.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 292-293

QUESTION NO: 16

Which of the following security requirements does file encryption using symmetric cryptography satisfy?

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.

Incorrect answers:
B: Access Control is the means of giving or restricting user access to network resources. This is usually accomplished through the use of an ACL (Access Control List).
C: Data integrity refers to the level of confidence that data won't be jeopardized and will be kept secret. 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.
D: Authentication requires a user to provide some proof or credential that represents something they know, something they have, or something they are before allowing access to your company's resources.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 7, Lesson 1
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress Publishing, 2002, p 513

QUESTION NO: 17
Which of the following encryption schemes relies on the sender and receiver using 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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 292-293

QUESTION NO: 18
Which of the following statements describes 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.

Incorrect answers:
B: This is not true as the size of data input determines the size of data output.
C: This is relative for all algorithms.
D: A symmetric algorithm requires both ends to have the same key and is thus not a one-way function.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 292-293

QUESTION NO: 19
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).

Incorrect answers:
A: RC4 is a symmetric encryption algorithm with variable key length, stream cipher, effectively in public domain.
B: IDEA is a symmetric encryption algorithm with 128-bit key, requires licensing for commercial use.
C: MD5 is the newest version of the MD4 algorithm. It produces a 128-bit hash, but not an example of asymmetric encryption algorithm.

Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 294
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION NO: 20
Which of the following kinds of attacks 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:
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 cannot be used to crack the password.
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. But a password can still be guessed using adictionary or brute force.

Incorrect answers:
A: 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 cannot be used to **crack a password or message; it is used to verify or to store on a server as opposed to plain text.**
C: Reverse engineering is the process of re-creating the functionality of an item by first deciding what the result is and then creating something from scratch that serves the same purpose. Hashed passwords will thus not be vulnerable. D: Hashed passwords are not susceptible to DoS attacks.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 57

QUESTION NO: 21

In the digital signature process, which of the following security requirements does hashing satisfy?

A. Non-repudiation.
B. Access control.
C. Data integrity.
D. Authentication.

Answer: C
Explanation:
Data integrity refers to the level of confidence that data won't be jeopardized and will be kept secret. 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.

Incorrect answers:
A: Non-repudiation is the ability (by whatever means) to verify that data was seen by an intended party. It makes sure they received the data and can't repudiate (dispute) that it arrived. B: Access Control is the means of giving or restricting user access to network resources. This is usually accomplished through the use of an ACL (Access Control List).
D: Authentication requires a user to provide some proof or credential that represents something they know, something they have, or something they are before allowing access to your company's resources.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 7, Lesson 1

QUESTION NO: 22
Which of the following hash schemes 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.

Incorrect answers:
A: MD4 produces a 128 bit message digest. B: MD5 produces a 128 bit message digest. C: DES is a 56-bit key not considered strong enough for today's standards, relatively slow.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 291-292
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

4.2 Understand how cryptography addresses the various security concepts. (21 questions)

QUESTION NO: 1
Which of the following can best be used to achieve data integrity?

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.

Incorrect answers:
A, D: A cipher is a method used to encode characters to hide their value. Ciphering is the process of using a cipher to encode a message.
B: A digital certificate is an electronic credential used to authenticate users.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 291-293

QUESTION NO: 2
Which of the following best describes 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.

Incorrect answers:
A: This sounds more like availability rather than integrity.
C: This is not what data integrity is about.
D: It is not meant to indicate the security level of data, but rather than data is tamper-free.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 22-23

QUESTION NO: 3
Which of the following is an assurance that a message has not been altered in transit?

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.

Incorrect answers:
B: Static assurance is not the assurance that a message had not been tampered with.
C: Dynamic assurance is not to make sure that messages had been tampered with.
D: Cyclical check sequence is an error-checking method in data communications that runs a formula against data before transmission. Not an assurance that the message is tamper free.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 23

QUESTION NO: 4
Which of the following does IPSec (IP Security) provide? (Choose two)

A. Secure Shell (SSH) for data confidentiality.
B. Password Authentication Protocol (PAP) for user authentication.
C. Authentication Header (AH) for data integrity.
D. Internet Protocol (IP) for data integrity.
E. Nonrepudiation Header (NH) for identity integrity.
F. 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.

Incorrect answers:
A, B, D and E: These are not provided by IPSec.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 120-121

QUESTION NO: 5
Which of the following services do message authentication codes provide?

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.

Incorrect answers:
B: Fault recovery is not provided through message authentication.
C: Key recovery is not a purpose of message authentication.
D: Acknowledgement is not a purpose of message authentication.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 61, 296

QUESTION NO: 6
Which of the following is the most common form of authentication?

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.

Incorrect answers:
A: Certificates authentication is not as common as password authentication.
B: Tokens can be pricier than passwords and thus not a popular as passwords.
D: Biometric are too expensive and as such is not in such to the same scale as passwords.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 16
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 7, Lesson 1

QUESTION NO: 7
Why is 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: B
Explanation:
A token is a device that can be issued to a user for use in the authentication process. For example, there are token devices that, when enabled, synchronize with a server. Think of a token as a small piece of data that holds a sliver of information about the user. With a token being a physical possession it makes it hard to attack.

Tokens are difficult to duplicate and are generally tamper resistant. Some can be carried with you for use on any workstation, although others require appropriate hardware peripherals and software on a workstation. Although tokens offer reliable security, they can be costly and difficult to deploy in an enterprise environment.

Tokens can either provide a one-time-use password or store information about the user. The user information can be a certificate and a password, as with smart cards. Smart card technologies provide strong security through encryption as well as access control. Smart cards require a reader that is used when the authentication is required.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 16
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 7, Lesson 1

QUESTION NO: 8
What type of authentication provides an additional layer of security when a stored key and memorized password are not strong enough?

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.

Incorrect answers:
A: Mutual authentication is when both the user and the resource authenticate to each other. But is is not an additional layer of security.
C: Biometrics does not represent an additional security layer.
D: Certificate authentication is not synonymous with the provision of an additional layer of security.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 17, 244

QUESTION NO: 9
Which of the following authentication problems is addressed by a single sign on process?

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

Answer: D
Explanation:
One of the big problems that larger systems must deal with is the need to access multiple systems or applications. This may require a user to remember multiple accounts and passwords. The purpose of a single sign-on (SSO) is to give users access to all the applications and systems they need when they log on with a single sign-on.

Incorrect answers:
A: Authorization through multiple servers is not what a single sign on is meant for.
B: Multiple domains are irrelevant in this case.
C: Multifactor authentication is when two or more access methods are included as part of the authentication process, you're implementing a multi-factor system.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 17, 388

QUESTION NO: 10
Which of the following is NOT a major component of ISAKMP (Internet Security Association and Key Management Protocol)?

A. Authentication of peers.
B. Threat management.
C. Communication management.
D. Security association creation and management.
E. Cryptographic key establishment and management.

Answer: C
Explanation: The four major functional components of ISAKMP are: Authentication of communications peers, Threat mitigation. Security association creation and management and Cryptographic key establishment and management; thus rendering communication management NOT a major component of ISAKMP.

Incorrect answers:
A, **B,D and** E: These are all major components of SAKMP.

Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 9

QUESTION NO: 11
You work as the security administrator at TestKing.com. The CEO at TestKing wants to send an e-mail message to a business partner. The CEO does not want anyone else to have the ability to read the e-mail message. Which tenet of information security is the CEO 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.

Incorrect answers:
A: Authentication is to authenticate that the user who does gain access is the right user.
B: Integrity is the process of replicating the data perfectly.
D: Non-repudiation main purpose is to prevent one or the other party from denying actions they carried out.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 112-114

QUESTION NO: 12
In a VPN (Virtual Private Network), which of the following are used to restrict 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.**

Incorrect answers:
B: Authentication is to authenticate that the user who does gain access is the right user.
C: Confidentiality is the function of giving privacy.
D: Data integrity is the process of replicating the data perfectly.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 112-114

QUESTION NO: 13
What is the protection of data against unauthorized access or disclosure is an example of?

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.

Incorrect answers:
B: Integrity is the level of confidence to make sure that the data being worked with is the correct data.
C: Signing is similar to certifying.
D: Hashing refers to performing a calculation on a message and converting it into a numeric hash value.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 22-25, 267, 285

QUESTION NO: 14
Which of the following services 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.

Incorrect answers:
A: Data integrity is the level of confidence to make sure that the data being worked with is the correct data.
B: Data confidentiality is to prevent or minimize unauthorized access to and disclosure of data and information.
C: Data authentication is to allow only the correct credentials to have access.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 22-25, 267

QUESTION NO: 15
What is the primary purpose of technical security measures and countermeasures?

A. The prevention of unauthorized access, unauthorized modification, and denial of authorized access.
B. The prevention of interoperability of the framework, unauthorized modification, and denial of authorized access.
C. The prevention of potential discovery of access, interoperability of the framework, and denial of authorized access.
D. The prevention of interoperability of the framework, unauthorized modification, and unauthorized access.

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

Incorrect answers:
B: Prevention of the interoperability of the framework is not a direct concern of security measures.
C: The prevention of potential discovery of access is not the primary purpose of technical security measures.
D: Interoperability of the framework is not a direct concern of security measures.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 308

QUESTION NO: 16

Which of the following ensures that an e-mail message was not tampered with while in transit?

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. It is the level of confidence to make sure that the data being worked with is the correct data.

Incorrect answers:
A: The goal of confidentiality is to prevent or minimize unauthorized access to and disclosure of data and information.
B: Authentication is to allow only the correct credentials to have access.
D: Non-repudiation main purpose is to prevent one or the other party from denying actions they carried out.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 22-25

QUESTION NO: 17
Why is the control of access to information systems and associated networks necessary?

A. For the preservation of their authenticity, confidentiality, integrity and availability.
B. For the preservation of their integrity and availability.
C. For the preservation of their confidentiality, integrity and availability.
D. For the preservation of their 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.

Incorrect answers:
A: Integrity, availability and confidentially can be preserved through access control. Authenticity can occur through many other methods.
B: It more for more than mere integrity and availability.
D: Integrity is another necessary factor that is missing from this option.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 211

QUESTION NO: 18
What is the general purpose of non-repudiation?

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

Incorrect answers:
A: Non-repudiation is not meant to protect from virus transmission to computers on the same network.

B: Protection from DoS attacks cannot be mitigated with non-repudiation.
D: This is also part of the benefits of non-repudiation; however, the crux of non-repudiation is rather to prevent the sender from denying that communication did in fact occur.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 299

QUESTION NO: 19
Which of the following security processes allows a recipient 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.

Incorrect answers:
A: Authentication does not allow the recipient to verify the originator of an e-mail. B: Integrity has to de with the content and not so much the originator of the email. D: Confidentiality is not there to be used to verify the originator of an e-mail message.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 297

QUESTION NO: 20
What do most intrusion detection systems look for in order to detect attacks? (Chose two)

A. Patterns
B. Viruses
C. Signatures
D. Hackers
E. Mal ware

Answer: A, C
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.

Incorrect answers:
B: They do not make use of viruses to detect attacks.
D: IDS cannot go and look for hackers to look for attacks. They need to look at patterns and signatures in order to detect a hacker.
E: IDS does not make use of malware to detect attacks.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 115-117

QUESTION NO: 21
Which of the following do digital signatures provide for?

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 generated the message.

Incorrect answers:
A, **B and C:** Digital certificates makes provision for non-repudiation and not for availability, encryption of decryption.

Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 3
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 297

4.3 Understand and be able to explain the PKI (Public Key Infrastructure) concepts. (17 questions)

QUESTION NO: 1
Which of the following represents the main purpose of digital certificates?

A. To bind a public key to the identity of the signer and recipient.
B. To bind a private key to the identity of the signer and recipient.
C. To bind a public key to the entity that holds the corresponding private key.
D. To bind a private key to the entity that holds the corresponding public key.

Answer: C
Explanation:
A digital certificate is the public key with an individual. It is issued by a certification authority (CA) and 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.

Incorrect Answers:
A, B: A certificate associates the public key with an individual. This has nothing to do with any intended recipient. Furthermore, a PKI system is based on the continued security of the user's private key. This key must never leave the possession of the owner.
D: A certificate associates the public key with an individual. The user's private key must never leave the possession of the owner.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 272.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 305.

QUESTION NO: 2
When applying to the CA (Certificate Authority) for a certificate, what must a user supply the CA (Certificate Authority) with?

A. The user's public key.
B. The intended recipient's public key.
C. The public keys of the user and his intended recipient.
D. The public and private keys of the user and his intended recipient.

Answer: A
Explanation:
A certificate associates the public key with an individual. Therefore the user must submit proof of identity and his or her public key.

Incorrect Answers:
B, C, D: A certificate associates the public key with an individual. This has nothing to do with any intended recipient. Furthermore, a PKI system is based on the continued security of the user's private key. This key must never leave the possession of the owner.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 272.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 305.

QUESTION NO: 3
Which of the following represents good practice when 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.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 538-539.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 301.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 131.

QUESTION NO: 4
Which of the following is described in a CPS (Certificate Practice Statement)?

A. A CA's (Certificate Authority's) class level issuing process.
B. A CA's (Certificate Authority's) copyright notice.
C. A CA's (Certificate Authority's) procedures.
D. A CA's (Certificate Authority's) asymmetric encryption schema.

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

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 538-539.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 301.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 131.

QUESTION NO: 5
With regard to a X509 v.3 certificate, which of the following is NOT a field?

A. private key
B. issuer
C. serial number
D. subject

Answer: A
Explanation:
The X.509 has a Version field, a Serial Number field, a Signature Algorithm Identifier field, an Issuer field, a Validity Period field, a Subject Name field, a Subject Public Key Information field, and an Extension Field. It does not have a private key field.

Incorrect Answers:
B: X.509 does have an Issuer field.
C: X.509 does have a Serial Number field.
D: X.509 does have a Subject Name field.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 304-305.

QUESTION NO: 6
Which of the following correctly identifies 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 private 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 has a Version field, a Serial Number field, a Signature Algorithm Identifier field, an Issuer field, a Validity Period field, a Subject Name field, a Subject Public Key Information field, and an Extension Field. It does not have a private key field.

Incorrect Answers:
A: X.509 does not have an Object Identifiers field or the location of user's electronic identity. B: X.509 does not have a private key field.
D: X.509 does not have the serial number of the CA (Certificate Authority) certificate, and the CRL (Certificate Revocation List) entry point.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 304-305.
http://csrc.nist.gov/pki/panel/santosh/tsld002.htm

QUESTION NO: 7
On which of the following standards are most certificates that are used for authentication based?

A. ISO19278
B. X.500
C. RFC 1205
D. X.509 v3

Answer: D
Explanation:
The most widely used digital certificates standard is the X.509 version 3.

Incorrect Answers:
A: There is no ISO 19278 certificate standard.
B: X.500 is a standard for hierarchical directory structures. LDAP is based on the X.500 standard.
C: RFC 1205 describes the IBM 5250 Telnet interface.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 224, 304-305.
http://www.faqs.org/rfcs/rfc1205.html

QUESTION NO: 8

With regard to the Internet, which of the following best describes pop-up browser window which validates the identity of the ActiveX developer?

A. Authenticode
B. Web server certificate
C. CA (Certificate Authority) certificate
D. Server certificate

Answer: A
Explanation:
Authenticode is based on certificate technology which allows ActiveX components to be validated by the web server.

Incorrect Answers:
B: A web server certificate allows a website to enable SSL communication.
C: A CA (Certificate Authority) certificate associates a public key with a CA, verifying the identity of the CA and the validity of the certificates that the CA issues.
D: A server certificate is used to validate the identity of a server to a client.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128.
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 49, 283.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 21-22.

QUESTION NO: 9
Of which of the following trust models is an embedded root certificates within web browsers an example?

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.

Incorrect Answers:
A: In a bridge trust model, a peer-to-peer relationship exists between the root CAs. This enables cross-certification as it allows the root CAs to communicate with each other. This trust model allows a certification process to be established between organizations or departments.
B: The mesh trust model combines the bridge model and the hierarchical model, expanding the bridge model by supporting multiple paths and multiple root CAs. Each root CA can cross-certify with the other root CAs in the mesh.
C: In a hierarchical trust model a root CA provides the certification information for intermediate CAs, which only trust information provided by the root CA. The intermediate CAs issue certificates to other entities.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 306-310.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 134.

QUESTION NO: 10
Which of the following represent acceptable use of smart card technology? (Choose all that apply)

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

Answer: A, B, D
Explanation:
A smart card is a hardware device that can be used for authentication purposes, including authentication user access to mobile telephones, satellite television access cards, credit cards and token cards.

Incorrect Answers:
C: There is no such thing as a PKI token card. PKI uses software based certificates and keys, not cards.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 6, 17, 300-301.

QUESTION NO: 11
Which of the following is 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.

Incorrect Answers:
A, **B:** Only certificates that have been revoked are published in the CRL, not certificates that have expired or that are pending renewal.
C: Certificates would not be issued without a valid CA (Certificate Authority) signature.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 131-132.

QUESTION NO: 12
Which of the following can be contained in a digital certificates?

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 associates the public key with an individual. Therefore the user must submit proof of identity and his or her public key. The fields contained in a certificate include a Version field, a Serial Number field, a Signature Algorithm Identifier field, an Issuer field, a Validity Period field, a Subject Name field, a Subject Public Key Information field, and an Extension Field. It does not have a private key field.

Incorrect Answers:
A, **B:** A digital certificate does not contain any private key information. A PKI system is based on the continued security of the private keys. These key must never leave the possession of the owner. Furthermore, certificate's revocation information is published in a Certificate Revocation List (CRL).
C: Certificate's revocation information is published in a Certificate Revocation List (CRL), not in the digital certificate.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 272.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 131-132, 305.

QUESTION NO: 13
With regard to CRLs (Certificate Revocation Lists), which of the following are true?

A. A CLR (Certificate Revocation List) query that receives a response in near real time indicates that high availability equipment is used.
B. A CLR (Certificate Revocation List) query that receives a response in near real time implies that a fault tolerant database is being used.
C. A CLR (Certificate Revocation List) query that receives a response in near real time does not guarantee that fresh data is being returned.
D. A CLR (Certificate Revocation List) query that receives a response in near real time 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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 131-132.

QUESTION NO: 14
Which of the following is issued when a private key becomes compromised before the certificate's normal expiration?

A. A certificate enrollment list
B. A certificate expiration list
C. A certificate revocation list
D. A certificate 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.

Incorrect Answers:
A, **B, D:** There is not certificate enrollment list, certificate expiration list, or certificate validation list.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2002, pp 305-306.

QUESTION NO: 15
Which of the following PKI documents outlines the PKI's use, management and deployment?

A. PKI policy.

B. PKI procedure.
C. PKI practice.
D. Best practices guideline.

Answer: A
A PKI policy defines a course of action and is a guiding principle or procedure for using, managing and deploying certificates.

Incorrect Answers:
B, D: There are two PKI documents. The PKI policy and the certificate practice statements. There are no PKI procedure document or a best practices guideless document for PKI. C: A certificate practice statement defines how a CA will manage the certificates it issues.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 538-539.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 301.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 131.

QUESTION NO: 16
Which of the following PKI documents facilitates common interoperability standards and common assurance criteria on an industry wide basis?

A. PKI policy.
B. PKI procedure.
C. PKI practice.
D. PKI process.

Answer: A
Explanation:
Any document that serves as the vehicle on which it is used as a guideline is a policy.

Incorrect Answers:
B, D: There are two PKI documents. The PKI policy and the certificate practice statements. There are no PKI procedure or PKI process documents.
C: A certificate practice statement defines how a CA will manage the certificates it issues.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 538-539.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 301.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 131.

QUESTION NO: 17
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
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. For this reason, the private key must never leave the possession of its owner.

Incorrect Answers:
A: Lack of use is not a reason for revocation.
B: A certificate links a user's public key to the identity of that user and is not dependant on the user's address.
D: The user's public key is the 'shared' portion of the private/public key pair. It is used by recipients to verify the data.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 306.

4.4 Identify and be able to differentiate different cryptographic standards and protocols (8 questions)

QUESTION NO: 1

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

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

Answer: A
The Common Criteria is the defacto IT (Information Technology) security evaluation criteria for the international community. Before the Common Criteria, different criteria were used in America and in Europe. The criterion used in the USA was called the Trusted Computer Systems Evaluation Criteria (TCSEC), or Orange Book, and was developed by the U.S. Department of Defense while the criterion used in Europe was the Information Technology Security Evaluation Criteria (ITSEC). The Common Criteria is the result of efforts to combine these two.

Incorrect Answers:
B: There is no such thing as a Global Criteria.
C: Prior to the Common Criteria, the Trusted Computer Systems Evaluation Criteria (TCSEC), or Orange Book, was used in the USA and differed from the criteria used in Europe.
D: Prior to the Common Criteria, the Information Technology Security Evaluation Criteria (ITSEC) was used in Europe and differed from the criteria used in the USA.

References:
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 62.

QUESTION NO: 2
What algorithm does AES (Advanced Encryption Standard) use?

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

Answer: A
Explanation:
AES uses the Rijindael algorithm.

Incorrect Answers:
B: There is no Nagle algorithm
C: Spanning Tree is used in routing it is not an algorithm.
D: The Public Key Infrastructure (PKI) is based on certificates and keys. It is not an algorithm.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 503-504.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 293.

QUESTION NO: 3
Which of the following is 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?

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

Answer: D
Explanation:
MD5 is take a variable length of data input and produces a hash that is always equal to128-bits, regardless of the length of the input data.

Incorrect Answers:
A: IPSec is not an algorithm.
B: The RSA algorithm is a public-key encryption system for both encryption and digital signatures.
C: Blowfish is a block cipher algorithm that uses a 64-bit block of data to create the hash.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 120.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 293.

QUESTION NO: 4

Which of the following IETF (Internet Engineering Task Force) protocols use 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. AH is used to provide data integrity while ESP is used to provide authenticity and integrity of the data payload.

Incorrect Answers:
A, **C, D:** SSL, HTTPS and SSH does not use AH and ESP. Only IPSec uses AH and ESP.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 120.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 297.

QUESTION NO: 5
Which of the following provides 160-bit encryption?

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

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

Incorrect Answers:
A, **B:** MD-2, MD-4 and MD-5 provide 128-bit encryption.
D: Blowfish provides 64-bit encryption.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 511, 512.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 291, 293.

QUESTION NO: 6
What does the Diffie-Hellman algorithm allow?

A. Access to digital certificate stores from a 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.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 507-508.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 295, 445.

QUESTION NO: 7
Which of the following encryption algorithms is based on Rijndael?

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

Answer: A
Explanation:

Advanced Encryption Standard (AES) uses the Rijndael block cipher algorithm.

Incorrect Answers:
B, C: 3DES and DES are not based on Rijndael.
D: Skipjack is the algorithm that was used in the Clipper Chip.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 503-504, 554.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 293.

QUESTION NO: 8
Which of the following 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
Explanation:
IPSec is an IETF protocol, and it does use an AH and ESP. AH is used to provide data integrity while ESP is used to provide authenticity and integrity of the data payload.

Incorrect Answers:
B, C, D: SSL, TLS and PPTP does not use AH and ESP. Only IPSec uses AH and ESP.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 120.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 297.

4.5 Understand and be able to explain the various Key Management and Certificate Lifecycle concepts. (16 questions)

QUESTION NO: 1
Which of the following encryption keys 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:
A digital signature validates the authenticity of the message by verifying the source of the message. This is known as non-repudiation. The digital signature also ensures that the message was not altered in transit by using hashing. The sender or signer uses his or her private key to hash the message. Once the recipient receives the message he or she uses the signer's public key to verify the hash.

Incorrect Answers:
B: The signer's private key is used to sign the message. It never leaves the possession of the **signer; hence it is referred to as the private key.**
C, D: The same key pair must be used to validate the message. Since the signer uses his own private key to sign the message, the recipient must use the signer's public key to verify it. The sender cannot use the recipient's key to sign the message as this would not prove the identity of the sender.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 515-516.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 297.

QUESTION NO: 2
Which of the following negotiates and provides authenticated keying material for-security associations in a secure manner?

A. ISAKMP (Internet Security Association and Key Management Protocol)
B. ESP (Encapsulating Security Payload)

C. SSH (Secure Shell)
D. SKEME (Secure Key Exchange Mechanism)

Answer: A
Explanation:
IPSec uses (ISAKMP) as its security association manager. It is used to negotiate and provide authenticated keying material for security associations in a secured manner.

Incorrect Answers:
B: IPSec uses ESP to provide data encryption to ensure the authenticity and integrity of the data payload.
C: SSH is used to secure access to remote systems and replaces the standard Telnet, rlogin, rsh, and rcp commands. It uses public key cryptography to provide session encryption.
D: There is not such thing as SKEME.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 118, 120, 121-122.

QUESTION NO: 3
With regard to non-repudiation, which of the following uses distinct key pairs to separate confidentiality services from integrity services?

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.

Incorrect Answers:
A: There is no such thing as a discrete key pair. C:

Key escrow is used for recovery purposes. It is a storage process by which copies of private keys and/or secret keys are retained by a centralized management system as a means of insurance or recovery in the event of a disaster.
D: A foreign key is used in relational databases to ensure the integrity of data in the database. It is not used to provide network security.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 553-554.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, **p** 138.

http://www.verisign.com/products-services/security-services/pki/pki-security/public-key-infrastructure/

QUESTION NO: 4
Which of the following must be used to encrypt an e-mail to ensure that only the intended recipient can read it?

A. The intended recipient's public key.
B. The intended recipient's private key.
C. The sender's public key.
D. The sender's private key.

Answer: A
Explanation:
Ensuring that only the intended recipient can read an e-mail message is referred to as authenticating the recipient. To authenticate the recipient in private/public key cryptography, the sender must use the recipient's public key to encrypt message. This forces authentication of the recipient as only the recipient can posses the corresponding private key to decrypt the message.

Incorrect Answers:
B: The sender cannot be in possession of the recipient's private key as a private key never leaves the possession of its owner. Therefore the sender cannot use the recipient's private key to encrypt the message.
C, D: The sender's private key can be used to hash the message so as to allow the recipient to use the sender's public key to verify the identity of the sender. This authenticates the sender, not the recipient.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 127.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 515-516.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 297.

QUESTION NO: 5
Which of the following must a user submit to a trusted CA (Certificate Authority) when applying for a certificate?

A. A private key.
B. A public key.
C. A password.
D. A Kerberos key.

Answer: B
Explanation:
A certificate associates the public key with an individual. Therefore the user must submit proof of identity and their public key.

Incorrect Answers:
A: To ensure the validity of the private/public key pair, the user's private key must never leave the possession of its owner. Only the user's public key may be made available.
C: The PKI system does not use passwords. It uses certificates.
D: Kerberos is used for authentication purposes, not certificate purposes.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 272.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 305.

QUESTION NO: 6
When implementing a PKI (Public Key Infrastructure), which of the following are two common methods 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:
CRL and OCSP are used in certificate revocation. This process begins when the CA is notified that a particular certificate needs to be revoked. The CA marks the certificate as revoked by publishing it in the certificate revocation list (CRL). The information is published in the CRL and becomes available using the Online Certificate Status Protocol (OCSP).

Incorrect Answers:
A: An access control list (ACL) is used to control access to network resources for authenticated users and does not require the implementation of a PKI while Pretty Good Privacy (PGP) is uses to provide security for e-mail messages.
B: Certificate revocation lists (CRLs) are used in PKI but not Protocol Independent Multicasting (PIM), which is a routing protocol.
D: RSA and MD5 are encryption algorithms used to encrypt data transmissions.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 124, 216, 292-292, 294, 305-306.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 128-135, 393, 540-541.

QUESTION NO: 7
Which of the following factors influences the lifespan of a public key certificate and its associated keys?

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

As with passwords, the longer a certificate key is used, the greater is the possibility that it would be compromised. Therefore certificates have an expiration date or lifespan. Upon reaching the expiration date, the certificate will no longer be valid.

Incorrect Answers:
B: Security should be of greater concern than cost. C:
Certificates have key lengths not hash lengths. D:
Data is not openly available on the PKI system.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 344.

QUESTION NO: 8
When is the integrity of a cryptographic system considered to be compromised?

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. For this reason, the private key must never leave the possession of its owner.

Incorrect Answers:
A: The purpose for which the key is used does not determine its status as being compromised. B: The user's public key is the 'shared' portion of the private/public key pair. It is used by recipients to verify the data.
D: The validity of the data source can only be compromised if the private key used to encrypt that data is compromised.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 306.

QUESTION NO: 9
Which of the following is a pervasive system whose services are implemented and delivered using public key technologies?

A. A public key cryptography scheme.
B. A public key distribution authority.
C. A public key exchange.
D. A public key 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 companies that do this are VeriSign and Thwate.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 532-534.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 300-301.

QUESTION NO: 10
Which of the following is a primary concern of centralized key management systems?

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.

Incorrect Answers: B:

Although certificates must be accessible to users who need to validate a owner of a certificates identity, this is not the primary concern of a PKI system. The security of the keys is more important. As soon as keys are compromised, the entire system fails. C: Keys must be secure at all times. Making the key repository publicly accessible will compromise the keys stored there. D: Certificates are used to identify a user's public key. This information cannot be kept confidential.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 532-534.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 300-301.

QUESTION NO: 11
Which of the following does a recipient use, together with the hash value, to verify a digital signature?

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

Answer: C
Explanation:
A digital signature validates the authenticity of the message by verifying the source of the message. This is known as non-repudiation. The digital signature also ensures that the message was not altered in transit by using hashing. The sender or signer uses his or her private key to hash the message. Once the recipient receives the message he or she uses the signer's public key to verify the hash.

Incorrect Answers:
A: The signer's private key is used to sign the message. It never leaves the possession of the **signer; hence it is referred to as the private key.**
B, D: The same key pair must be used to validate the message. Since the signer uses his own private key to sign the message, the receiver must use the signer's public key to verify it. The sender cannot use the receiver's key to sign the message as this would not prove the identity of the sender.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 515-516.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 297.

QUESTION NO: 12
Which of the following encryption algorithms is a block cipher an example of?

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 block of data and encrypts it as a single unit. Some popular block ciphers are: DES, 3DES, AES (Rijndael), Blowfish, IDEA, RC2, RC5, RC6, CAST, MARS, Serpent, Twofish.

Incorrect Answers:
A: A block cipher is a symmetric key encryption method that uses shared or secret keys. It does not use asymmetrical keys.
B: A block cipher is a symmetric key encryption method that uses shared or secret keys. These keys are referred to as private keys, not public keys.
D: Block cipher encryption does make use of keys.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 500-505.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 293.

QUESTION NO: 13
Which of the following is a public key infrastructure model where certificates are issued and revoked via a CA (Certificate Authority) an example of?

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

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.

Incorrect Answers:
A, **B, D:** The only PKI models are the centralized model and the hierarchical model.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 533-534.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 301-302.

QUESTION NO: 14
What should be done with a cryptographic system's keys when they are no longer needed?

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

Answer: A
Explanation:
PKI keys should remain secure at all times. If a key is no longer required, it should be taken out of usage and stored securely, or it should be destroyed.

Incorrect Answers:
B: Deleting a key from the system's storage mechanism does not ensure that the key is secure. The key may still be on the user's computer where is would be vulnerable. C: Keys are not recycled. They are issued to a specific user and are used to identify that user as the author of a document.

D: A key repository is an escrow system that is used to restore a key in case of a disaster. It does not ensure that the key will be taken out of use.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 342, 344-345.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 556, 560.

QUESTION NO: 15
What security service is provided by using a smart card containing a private key when you log onto a workstation?

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.

Incorrect Answers:
B, C, D: A smart card is a physical hardware device that a user uses a proof of his or her identity when authenticating to a system and consists of a single secret or private key. Because of this it cannot provide confidentiality, integrity or non-repudiation as these require a public/private key pair which is software based.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 17-18, 143, 313, 340, 345.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 21, 381.

QUESTION NO: 16
Which of the following keys is contained in a digital certificate?

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

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

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 118, 121-122.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 227.

Topic 5, Operational / Organizational Security (87 questions)

5.1 Understand the application of the various concepts of physical security. (13 questions)

QUESTION NO: 1
Which of the following access control principle dictates that every user be given the most restricted privileges?

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

Answer: B
Explanation:
The principle of least privilege states that every user should be granted the most restrictive level of access that would allow them to perform their work, and no more.

Incorrect Answers: A:

Access control permissions are used to grant users access to network resources. They are not access control principles.
C: Thereare no hierarchical permissions, though there is a hierarchical trust model, which refers to security certificates and is not an access control principle.
D: Access control modes are the methods used to ensure that users can only access resources that they are authorized to access.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 451-452.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 265.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 6.

QUESTION NO: 2
Which four elements does the BellLa-Padula access control model consist of?

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 La-Padula access control model is designed to prevent unauthorized access to classified information and prevents users from accessing information that has a higher security rating than they are authorized to access. The model also prevents information from being written to a lower level of security.

In this model, the entities in a computer system are divided into abstract sets of subjects and objects. The system 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.

With Bell-LaPadula, users can only create content at or above their own security level and can only view content at or below their own security level.

Incorrect Answers:
B: The Bell La-Padula access control model uses security levels, not groups or roles.
C: The Bell La-Padula access control model uses security levels, not permissions.
D: The Bell La-Padula access control model uses subjects and objects, not groups and roles.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 267.
http://en.wikipedia.org/wiki/Bell-LaPadula_model
http ://www.itsecurity. com/dictionary /bell .htm

QUESTION NO: 3
With regard to RBAC (Role Based Access Control), which of the following 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:
Access control using the RBAC model is based on the role or responsibilities users have in the organization. These roles usually reflect the organization's structure, such as its division into different departments, each with its distinct role in the organization. Users with the same responsibility and who perform the same functions in an organization are grouped together in one role. Each role are allowed the level of access required to perform the operations that comprises their responsibility within the organization.

Incorrect Answers:
A, **B, C:** RBAC is based on multiple users, multiple roles and multiple operations. With a single role, all users will have the same access levels.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 6.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 13.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 10.

QUESTION NO: 4
Which of the following 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 authentication uses biological features, such as fingerprints, patterns on the retina, and handprints. These features are unique to each individual and can be used to identify the person.

Incorrect Answers:
A: Biometrics refers biological features that are unique to each individual. Usernames and passwords are not biological features.
B, D: PIN numbers are not biological features.

References:
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 41.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 26.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 19
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 14-15.

QUESTION NO: 5
You notice that the lock to the window of an office that is adjacent to the server room is broken. Because it is not your office you tell the resident of the office to contact the maintenance department and have it fixed. You however do not 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:
If the window is not repaired, the threat that someone may use it to gain access will increase as more people become aware of the vulnerability.

Incorrect Answers:
A: Having the windows **repaired would not increase the threat; instead, the threat will be** reduced.
B: Having the windows repaired would reduce the threat. Thus the threat will not remain constant.
C: If the window is not repaired, the threat will increase as more people become aware of the vulnerability. It will not decrease.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 5.

QUESTION NO: 6
Which of the following provides the best protection against physical piggybacking?

A. Mantrap.
B. Security guard.
C. CCTV (Closed-Circuit Television).
D. Biometrics.

Answer: A
Explanation:
Piggybacking is a process of gaining access to a physical location without passing through authentication systems. It occurs when one user authenticates successfully to the physical building and wittingly or unwittingly allows another user into the building without requiring the second user to authenticate to the system. A mantrap can be used to prevent piggybacking. A mantrap is a holding cell between two entry points. It usually requires visual identification, and allows only one or two people into the facility at a time.

Incorrect Answers:
B: Although security guards can prevent piggybacking, security guard which is prone to human error and may lack vigilance. Thus, this is not the best defense against piggybacking.

C: CCTV plays an important role in auditing and can be used to prevent unauthorized access. However, this is dependent to the vigilance of a security guard which is prone to human error. Thus, this is not the best defense against piggybacking.
D: Biometrics is an authentication method that uses biological features that are unique to each individual to identify that individual. However, piggybacking is when a user authenticates successfully to the physical building and allows another user in without requiring authentication for the second user.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 238.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 152.

QUESTION NO: 7
Which of the following do turnstiles, double entry doors, mantraps and security guards help to prevent?

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 a process of gaining access to a physical location without passing through authentication systems. It occurs when one user authenticates successfully to the physical building and wittingly or unwittingly allows another user into the building without requiring the second user to authenticate to the system. Turnstiles, which allow only one person through at a time, double entry doors, security and mantraps can be used to prevent piggybacking. A man trap is a holding cell between two entry points. It usually requires visual identification, and allows only one or two people into the facility at a time.

Incorrect Answers:
B, C, D: Turnstiles, double entry doors, mantraps and security guards are elements of physical access security. They are not elements of an authorization security system and do not prevent the unauthorized retrieval of information or impersonation

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 238.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 152.

QUESTION NO: 8
Which of the following does NOT use Smart Card Technology?

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

Answer: A
Explanation:
CD players do not have security features and would not require the use of a Smart card.

Incorrect Answers:
B, D: Smart cards are usually used in mobile devices such as cell phones, hand held computers, and laptops. They are used to authenticate the user to the mobile device. C: Satellite cards use smart card technology to authenticate the user.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 6, 17, 300-301.

QUESTION NO: 9
You work as the security administrator at TestKing.com. TestKing.com consists of a main building with two smaller branch offices. The main building and branch offices are connected with fast links. Company policy dictates that each building has security measures that require visitors to sign in, and all employees are required to wear identification badges at all times. You want to physically 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:

Placing all the servers along with the vital components in one room would allow us to implement physical security measures to one room. This will provide the best level of security at the lowest cost and is viable because all TestKing branch offices are connected with fast links.

Incorrect Answers:

B, C, D: We want to keep the cost of physically securing the servers and vital components at a minimum. This means keeping the number of locations that require securing to a minimum. Placing all the servers and vital components in one room meet this requirement.

QUESTION NO: 10

Which of the following does 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:

Physical security refers to the physical access to the device. Strong passwords will not prevent physical access to the device.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 258

QUESTION NO: 11
Which of the following is an example of a physical access barrier?

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 physical access to computers and networks. This is can be accomplished through security guards

Incorrect Answers:
A, **D:** Motion detectors and video surveillance, while detecting unauthorized access, do not prevent unauthorized access.
B: Personnel traffic pattern management does not prevent unauthorized access.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 582-584.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 237-243.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 151-152.

QUESTION NO: 12
When considering physical security, which of the following is of the greatest importance?

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 primary aim of physical security is to reduce the opportunity of an intrusion by preventing physical access to resources. This can be accomplished by physical barriers such as burglar bars, security guards, and locked doors.

Incorrect Answers:
B: The primary aim of physical security is to reduce the opportunity of an intrusion by preventing physical access to resources
C: While being able to identify an intruder is a consideration in any security design, it is not the primary objective. The primary objective is to prevent unauthorized access.
D: Assess the impact of crime zoning and environmental considerations are not the primary concern of physical security.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 576-582.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 5.

QUESTION NO: 13
Which of the following should be included as part of a fire protection plan for a computer room?

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 is 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 is shut down properly is more likely to preserve its data.

Incorrect Answers:
B: A computer room would contain sensitive electronic equipment which would be damaged by a sprinkler system. Furthermore, the water from a sprinkler system could cause an electrical short that could lead to secondary fires, loss of equipment and loss of data. C: Although the use of non flammable materials in the computer room would be a good idea, smoke or heat from a nearby fire could still damage equipment.

D: Although fireproof doors can be used to contain a fire to one side of the fireproof door, they will not protect equipment in the computer room if the fire originates in that room. Furthermore, to effective contain the fire to one side of the fireproof door, it should remain closed.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 248, 251-253.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 154-155.

5.2 Understand the security implications of disaster recovery. (7 questions)

QUESTION NO: 1
Which of the following backup methods will backup only those files that were modified or created since the last full backup?

A. Copy
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 added or altered since the last full backup.

Incorrect Answers:
A: A copy backup backs up all the files on the system regardless of the archive attribute. Thus files that have been previously backed up in a Full backup will also be included in the copy backup.
C: Incremental backups are similar in function to differential backups but will backup only the files that have been added or modified since the last incremental backup rather than the last full backup.
D: Archive backups are similar to copy backups in that they backup all the files on the system regardless of the archive attribute. Thus files that have been previously backed up in a Full backup will also be included in the archive backup. A difference is that the archive backup compresses the backed up data.

References:

Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 685-686.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 368-369.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 156-157.

QUESTION NO: 2
Which of the following best describes the term cold site?

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 contains no equipment, and no communication links. It requires the complete creation of a network from scratch following a disaster. Often, a cold site requires weeks to configure. Although a cold site is the least costly, it makes recovery nearly impossible.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 692-693.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 375.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 157-158.

QUESTION NO: 3
Which of the following is 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?**

A. A cold site.
B. A warm site.
C. A mirrored site.
D. A hot site.

Answer: D
Explanation:
A hot site is a location that can be activated to provide critical functions within hours of a failure. It would have servers, networks and communication links in place to re-establish service in a very short amount of time.

Incorrect Answers:
A: A cold site is a physical location that contains no equipment, and no communication links. It requires the complete creation of a network from scratch following a disaster. Often, a cold site requires weeks to configure.
B: A warm site is a compromise between a hot site and a cold site. It provides some of the capabilities of a hot site, but it requires more administrative work to configure systems to resume operations.
C: There is no such thing as a mirrored site.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 692-693.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 374-375.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 157-158.

QUESTION NO: 4
Which of the following 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.

Incorrect Answers:

A: It is not always necessary to recover all systems as workstations usually do not hold critical data. These systems can be rebuilt rather than recovered.
B: Critical systems should be included in the disaster recover plan rather than systems identified by the board of directors, the president or the owner.
C: Financial systems and human resources systems would probably be included as they are usually critical systems. However, this is not the best answer as other critical systems should also be included. These critical systems would be identified in a formal risk analysis process.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 693-695.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 156.

QUESTION NO: 5
You work as the network administrator at TestKing.com. A fire has devastated the server room. Fortunately you have an alternate site. What is the first process you should resume at the original site?

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.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 692-693.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 374-375.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 157-158.

QUESTION NO: 6
Which of the following is typically included in a DRP (Disaster Recovery Plan)?

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

Answer: B
Explanation:
A preliminary risk analysis is performed in a Disaster Recovery Plan 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.

Incorrect Answers:
A: Penetration testing would indirectly be part of a Disaster Recovery Plan as it would be part of risk assessment. However, risk assessment would be the better answer. C, D: A Disaster Recovery Plan is concerned with reestablishing operations after a disaster. It would thus be primarily concerned with bringing systems back online rather than network attacks and access controls lists.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 692-693.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 374-375.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 157-158.

QUESTION NO: 7
For which of the following tasks is documenting change levels and revision information the most useful?

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.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, Alameda, Sybex, 2003, p 405.

5.3 Understand the security implications of the various topics of business continuity. (5 questions)

QUESTION NO: 1
Which of the following is acceptable and 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:
In any network there will always be variations of traffic load as this is dependent on usage patterns.

Incorrect Answers:
A: Traffic coming from or going to unexpected locations is not expected and not acceptable. B: Non-standard or malformed packets/protocol violations are suspicious traffic that may indicate an attempted network attack.
C: Repeated, failed connection attempts are suspicious traffic that may indicate unauthorized access attempts.

QUESTION NO: 2
Which of the following must a well defined business continuity plan consist of? (Choose all that apply)

A. Risk and analysis.
B. Maintenance and audit.

C. Business impact analysis.
D. Budgeting and acceptance.
E. Training and awareness.
F. Integration and validation.
G. Strategic planning and mitigation.
H. Documentation and security labeling.

Answer: A, B, C, E, F, G
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.

Incorrect Answers:
D, H: Budgeting and acceptance, and documentation and security labeling are usually not part of a business continuity plan

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 695-697.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 253-257.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 159-160.

QUESTION NO: 3
What problem may result from temperature fluctuations of between 60 and 90 degrees? (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. This is referred to as chip creep.

Incorrect Answers:
A: High humidity levels, rather than fluctuations in temperature, can increase electrostatic discharge
B: Power outages are not caused by fluctuations in temperature.
D: Poor air quality can cause problems related to ESD and fluctuations in temperature. However, poor air quality does not result from fluctuations in temperature.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 588.

QUESTION NO: 4
Which of the following technical solutions 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 for the hard disk subsystem, and thus high availability in the event of a hard disk failure.

Incorrect Answers:
A: UPD is a connection orientated protocol. It does not provide redundancy and does not ensure high availability in the event of a failure.
B: An anti-virus solution prevents the spread of viruses but it does not provide redundancy and does not ensure high availability in the event of a failure.
D: Firewalls protect an internal network from attacks originating from outside that network. It does provide redundancy and does not ensure high availability in the event of a failure.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 359-363.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 698-700.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 160-161.

QUESTION NO: 5
Which of the following is the main disadvantage of using shared storage clustering for high availability and disaster recover?

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, is not very safe because in the unlikely event of a natural disaster, a war, an insurrection, a labor act of transcendental civil disobedience, both units will be in a position of compromise.

5.4 Understand the concepts and uses of the various types of policies and procedures. (23 questions)

QUESTION NO: 1
Reducing which of the following will reduce the probability that a password can be guessed?

A. The password length.
B. The password lifetime.
C. The password's encryption level.
D. The password's alphabet set.

Answer: B
Explanation:
Passwords should be changed after a period of time. This prevents users from using one password indefinitely and reduces the opportunity for hackers to guess the password.

Incorrect Answers: A,
D:

Longerpassword lengths and more complex alphabet sets make it more difficult for hackers to crack a password by using dictionary attacks of brute force attacks.
C: Password encryption prevents hackers from using intercepted passwords. It does not reduce the likelihood that passwords could be guessed.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 76-77, 647-648.

QUESTION NO: 2
Which of the following would reduce the level of security of a network?

A. Passwords must be greater than six characters and consist of at least one non-alpha.
B. All passwords are set to expire at regular intervals and users are required to choose new passwords that have not been used before.
C. Complex passwords that users CANNOT 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.

Incorrect Answers:
A: Strong passwords with long password lengths and complex character sets will improve network security as it will make it more difficult for a hacker to crack a user's password.
B: A password lifetime policy will increase network security by reducing the opportunity for a hacker to guess a user's password.
D: An account lockout policy will improve network security by locking out a user account after a set number of failed logon attempts. A number of failed logon attempts would indicate a possible attempt to crack an account's password.

References:

Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 76-77, 647-648.

QUESTION NO: 3
Which of the following is the best course of action for the user who currently has sensitive material displayed on his monitor and now needs to leave 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:
A user can ensure that sensitive material on his monitor is not accessible by unauthorized users by waiting for the screensaver to come on before leaving the area. However, the screen saver should be password protected.

Incorrect Answers:
A: If you leave the computer unattended a social engineer could walk by, and view your sensitive material.
B: If you turn off your monitor, they can easily turn it back on.
D: A policy for securing sensitive data usually refers to the secure storage of data.

QUESTION NO: 4
Which of the following security principals entails the practice of providing each user only the access they require to perform their job?

A. Least privilege
B. Defense in depth
C. Separation of duties
D. Access control

Answer: A
Explanation:

The principle of least privilege states that every user should be granted the most restrictive level of access that would allow them to perform their work, and no more.

Incorrect Answers:
B: Defense-in-depth is the use of multiple security mechanisms to provide multiple barriers that will slow down attackers, and make it easier to detect and respond to attacks.
C: Separation of Duties is designed to reduce the risk of fraud and prevent other losses in an organization. It allows one person to perform a part of a key process, thus requiring more than one person to complete the process.
D: Access control is the process of granting users access to network resources. It is not an access control principle.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 229, 451-452.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 265, 383.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 6, 164.

QUESTION NO: 5
Which of the following best describes the term "due care"?

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 defines the level of care that level of care that a reasonable person would exercise in a given situation, and is used to address problems of negligence. This includes the level of care that is required to maintain the confidentiality of private information and specifies how such information is to be handled. It is designed to provide protection from security violations and injury to assets and personnel.

Incorrect Answers:
B: Due Care is meant to address problems of negligence. This cannot take place on a scheduled basis but on an ongoing basis.
C:

AlthoughDue Care does refer to the protection from injury to equipment and supplies, it is not technical in nature but legal in nature. It refers to the level of care that a reasonable person would exercise in a given situation. D: Due Care is meant to address problems of negligence rather than shared passwords.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 640-642.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 383.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 164.

QUESTION NO: 6
On which of the following principles would a need to know security policy would grant access be based?

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 sensitive information from others in the company that do not need to know the information. It is not intended to **prohibit people from accessing information they need; it is meant to minimize unauthorized** access. This is akin to the principle of least privilege, which states that every user should be granted the most restrictive level of access that would allow them to perform their work, and no more.

Incorrect Answers:
B, C, D: There is no less privilege, loss of privilege or single privilege principle.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 640-642.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 383.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 164.

QUESTION NO: 7
To whom of the following should a policy maker provide documentation when making changes to a user security policy?

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

Answer: D
Explanation:
A user security policy would affect all employees at a company. In addition, all employees will have to be aware of the new policy so as to adhere to it. Thus, the new user security policy should be made available to the whole staff.

This question requires a distinction between network users, which are all users of a network, including administrators and would be akin to all staff, and a default network group called Users which do not have administrative privileges.

Incorrect Answers:
A: A user security policy would affect all employees at a company. In addition, all employees will have to be aware of the new policy so as to adhere to it. Thus, the new user security policy should be made available to the whole staff and not just the security administrator.
B: A user security policy would affect all employees at a company. In addition, all employees will have to be aware of the new policy so as to adhere to it. Thus, the new user security policy should be made available to the whole staff and not just the auditors.
C: In this scenario, users should refer to all network users, which is akin to all staff members, rather than the default network group called Users, which do not have administrative privileges.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 271.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 163.

QUESTION NO: 8

Which expectation would a company without an acceptable use policy give their employees?

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

Answer: C
Explanation:
An acceptable use policy deals primarily with computers and information provided by the company. It stipulates what activities a user is allowed and what activities they are not allowed, as well as the monitoring of these activities. A crucial aspect of an acceptable use policy is lack of user privacy as an acceptable use policy is enforced through check that the user has not violated the policy. If your organization does not have an acceptable use policy, it opens itself to potential invasion of privacy lawsuits.

Incorrect Answers:
A, **B, D:** An acceptable use policy indicates that a user has no privacy and that a company has the right to monitor system and resource usage. Thus a lack of an acceptable usage policy would give the users a sense of privacy rather than a sense of intrusion, audits or prosecution.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, **p** 381.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 163.

QUESTION NO: 9
Which of the following must the implementation of access control devices and technologies reflect?

A. The organization's ACLs (Access Control List).
B. The organization's access control matrixes.
C. The organization's information security policies.
D. The organization's internal control procedures.

Answer: C
Explanation:

The Chief Security Officer of a company usually drafts a policy on information security, which should reflect management's attitude towards security and productivity.

QUESTION NO: 10
Which of the following 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. However, security awareness is the most overlooked element of security management.

Incorrect Answers:
B, C, D: Security awareness rather than intrusion diction, risk assessment, and vulnerability control is the most overlooked element of security management.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 174-175.

QUESTION NO: 11
What type of detection entails the tracking of personnel who visit unauthorized web sites?

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.

Incorrect Answers:
A: Abusedetection refers to the destruction of resources
C: Anomaly detection refers to unusual behavior.
D: Site filtering can be implemented at a firewall to prevent users from visiting unauthorized web sites. This, however, is not a diction system.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 163-164.

QUESTION NO: 12
You work as the network administrator at TestKing.com. You need to issue a TestKing employee with a laptop computer which is to be used to connect remotely to the corporate network. You want to ensure that the user does not install personal applications on the laptop. What must you do?

A. Users should not be given laptop computers in order to prevent this type of occurrence.
B. The user should be given instructions as to what is allowed to be installed.
C. The hard disk should be made read only.
D. Biometrics should be 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 to an acceptable use policy so they can know before hand what activities they are allowed and what activities they are not allowed.

Incorrect Answers:
A: Not giving the user a laptop could be counter productive as it would mean that the employee would not be able to work remotely.
C:

Should the hard disk be made read only, the user would only be able to access files on the system. He or she would not be able to make changes to the files and thus would not be able to accomplish their tasks
D: Biometrics and authentication do not control authorization and thus cannot be used to control what a user is and is not allowed.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, **p** 381.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 163.

QUESTION NO: 13
Which of the following should 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.

Incorrect Answers:
A, **C:** In a network an application server, availability as well as performance would be required as these would be productivity issues.
D: In most case a company would want to implement its own security.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 649-650.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 376-378.

QUESTION NO: 14
Which of the following best describes the term "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 is designed to reduce the risk of fraud and prevent other losses in an organization. It allows one person to perform a part of a key process, thus requiring more than one person to complete the process.

Incorrect Answers:
B, C: The principle of least privilege states that every user should be granted the most restrictive level of access that would allow them to perform their work, and no more. This principle can also be applied to providing users with only information that they require to perform their jobs.
D: Screening employees before assigning them to a position is part of risk assessment rather than a "separation of duties".

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 229, 451-452.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 265, 383.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 6, 164.

QUESTION NO: 15
Which of the following guidelines do computer forensics experts use to collect and analyze data while minimizing data loss?

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

Answer: B
Explanation:
The chain of custody documents the history of evidence that has been collected from the moment evidence is discovered through to the presentation of the evidence in court.

Incorrect Answers:
A: Evidence collected during the investigation of the crime is used as proof in determining possible guilt. However, for evidence to be presentable in court, the forensic expert must be able to show that the evidence was handled egitimately, that the evidence was properly preserved, and that the evidence was collected properly. The chain of custody is used to accomplish this. C: A chain of command indicated the hierarchical organization of a company. It is not relevant to the preservation of evidence.
D: Incident response refers to the process of identifying, investigating, repairing, documenting, and adjusting procedures to prevent the reoccurrence of an incident. It does not refer to the collection and analysis of data by forensic experts.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 602-609.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 385, 406-409.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 101-102, 170-171.

QUESTION NO: 16
Which of the following 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 the process of scavenging through trash in a search for clues trash for clues to users' passwords and other sensitive information. The secure disposal and destruction of waste can prevent dumpster diving. This includes the shredding and incineration of printed material, and the incineration, crushing, or magnetic destruction of storage media.

Incorrect Answers:
A, **C:** Additional security staff and surveillance equipment will not be able to prevent dumpster diving once the trash has been removed from the site.
D: Emptying the trash can frequently will not prevent dumpster diving at the location where the trash is taken to. Thus the vulnerability would remain.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 49.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 72.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 165.

QUESTION NO: 17
Which of the following does an attacker hope to acquire by searching through trash? (Choose all that apply)

A. Process lists.
B. Boot sectors.
C. Old passwords.
D. Virtual memory.
E. Network diagrams.
F. IP (Internet Protocol) address lists.

Answer: C, E, F
Explanation:
During dumpster diving, a potential attacker would search for clues about the network. These would include network diagrams, IP address lists, user passwords, etc.

Incorrect Answers:
A: Process lists are of little use to an attacker and would not be something an attacker would search for during dumpster diving.
B: Boot sectors are of little use to an attacker and would not be something an attacker would search for during dumpster diving.

D: Virtual memory is space on a hard disk drive that is used when system RAM is full. It is erased as soon as the application that required the data held in virtual memory is closed.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 49.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 72.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 165.
David Groth and Dan Newland, et al, A+ Complete Study Guide, Second Edition, San Francisco, 2001, pp 455-456, 569-570, 839.

QUESTION NO: 18
Which of the following would an attacker NOT be concerned with when searching through trash?

A. An IP (Internet Protocol) address.
B. System configuration or network map.
C. Old passwords.
D. System access requests.

Answer: D
Explanation:
During dumpster diving, a potential attacker would search for clues about the network. These would include network diagrams, IP address lists, user passwords, etc. However, system access requests would not reveal 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: An IP address would be of value to a potential hacker as it gives them an indication of the network being used. It also gives them the address of a system to attack.
B: Aconfiguration or system map is of value to a potential hacker because they can help the hacker 'blueprint' the network structure.
C: Old passwords would be of value to a potential hacker because they give the hacker an indication of how strong the password is, including the password length, the character sets used, and possibility the password lifetime.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 49.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 72.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 165.

QUESTION NO: 19
What should a system administrator do first on discovering suspicious activity that might indicate a computer crime?

A. Refer to the company's 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, his or her first step should be to refer to the company's incident response plan. The incident response plan defines and describes the procedures to perform in the event of an incident. It is designed to limit damage caused by the incident, to recover the environment as quickly as possible, and to gather information about the incident and the perpetrator in order to prevent a reoccurrence and pursue legal prosecution

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 172-177, 385-386.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 101-102.

QUESTION NO: 20
Which of the following is the best method of discouraging employees from misusing company e-mail?

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:
E-mail usage cannot effectively be controlled by mechanism such as permissions as users often require access to e-mail to perform their job functions. Thus, the user needs to take responsibility for their use of the company's e-mail system. The best way to accomplish this would be though a usage policy, which is one of the elements of a network security policy.

Incorrect Answers:
A: Access control lists define the permissions users have to network resources such as files, folders, printers and computers. It does not control the use of a company's e-mail system.
C: Strong authentication would control user access to the network system or to a server. It does not control e-mail usage. Furthermore, users would probably require access to e-mail in their job functions thus users would need to be authenticated to the e-mail server. Once authenticated, the system has no further control over the use of the e-mail system.
D: E-mail encryption is on a per user basis. Each user would need to encrypt his or her e-mail. Thus the user can still misuse the company's e-mail system by sending unencrypted e-mail messages.

QUESTION NO: 21
Which of the following is an acceptable interpretation of a use policy signed by an employee?

A. The employee's written refusal for allowing an employer to search an employee's workstation.
B. The employee's written policy for allowing an employer to search an employee's workstation.
C. The employee's written guideline for allowing an employer to search an employee's workstation.
D. The employee's written consent for allowing an employer to search an employee's workstation.

Answer: D
Explanation:

An acceptable use policy deals primarily with computers and information provided by the company. It stipulates what activities a user is allowed and what activities they are not allowed, as well as the monitoring of these activities. A crucial aspect of an acceptable use policy is lack of user privacy as an acceptable use policy is enforced through check that the user has not violated the policy. 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 employer's discretion.

Incorrect Answers:
A: An acceptable use policy stipulates what activities a user is allowed and what activities they are not allowed, as well as the monitoring of these activities by searching an employee's workstation. By signing the policy a user would be giving their consent rather than their refusal.
B, C: An acceptable use policy is a company policy rather than a user's policy or a user's guideline.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, **p** 381.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 163.

QUESTION NO: 22
What will a sound security policy define?

A. An organization's assets.
B. Attacks that are planned against the organization.
C. How an organization compares the others in security audits.
D. Weaknesses in competitor's systems.

Answer: A
A security policy is concerned with the protection of company assets, including systems, data, networks, and staff.

Incorrect Answers:
B: It is most unlikely that an organization would be aware of attacks that are planed against it. Further more, a security policy would define procedures that are to be followed in response to an attack rather than the attack itself.
C, D: A security policy is not concerned with the security levels at a rival organization and is comparative.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 9.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 635

QUESTION NO: 23
When is the creation of an information inventory MOST vulnerable?

A. When localizing license based attacks.
B. When trying to reconstruct damaged systems.
C. When determining virus penetration within an enterprise.
D. When terminating employees for security policy violations.

Answer: B

5.5 Explain the various concepts of privilege management. (10 questions)

QUESTION NO: 1
Which of the following is an advantage that can be gained when implementing a Single Sign-on technology?

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:
A single sign-on allows a user to authenticate one to the system, allowing them to access all of the applications and systems they have permissions to without requiring them to authenticate to each resource.

Incorrect Answers:
A: A single sign-on allows a user to authenticate one to the system, not twice.
B:

Thesingle sign-on is an authentication process, which allows users to log on to the system. It is not an authorization system. An authorization system uses permissions to determine which resources an authenticated user is able to access, and their levels of access. C: Thesingle sign-on is an authentication process, which allows users to log on to the system. It does not provide authenticated users with permissions to perform operations.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 388-389.

QUESTION NO: 2
Where are user accounts and passwords stored in a decentralized privilege management environment?

A. On a central authentication server.
B. On each individual server.
C. On no more than two servers.
D. On a server configured for decentralized management.

Answer: B
Explanation:
In a decentralized management system, user accounts and passwords stored on each server throughout the network.

Incorrect Answers:
A, D: A single server cannot be configured for decentralized management as management would then be centralized on one server.
C: In a decentralized management system, user accounts and passwords stored on each server in the network. Depending on the size of the network, this would probably be more than two servers.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 389.

QUESTION NO: 3

Which of the following describes a user who has accessed a system using a valid user ID and password combination?

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

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

QUESTION NO: 4
The review of which of the following does an IT (Information Technology) security audit generally focus on?

A. Exiting resources and goals
B. Exiting policies and procedures
C. Exiting mission statements
D. Exiting 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:
A: Security audits are not necessary to review a company's existing resources and security goals are an abstract that the CTO notes following a board meeting.
C: A mission statement is a long sentence that philosophizes the company's goals.
D: Ethic codes are voluntary moral standards placed by management.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 467.

QUESTION NO: 5
Which of the following reasons might prevent clients from navigating web sites that have been created for them?

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 the correct access privileges, you will not be allowed to navigate that site.

Incorrect Answers:
B: A DMZ is a security zone that is separated from the internal network by one or more firewalls. However, servers in the DMZ is accessible from the internal network and from the internet.
C: Sites that have IP filtering will prevent access to that site rather. However, users are not able to navigate the site. We can therefore assume that they can access the site.
D: Heavy traffic would make it difficult to navigate the site as bandwidth usage would be high. However, site navigation would be slow rather than impossible.

References:
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, pp. 365-366.

QUESTION NO: 6
Which of the following is the collection of information that includes login, file access, other various activities, and actual or attempted legitimate and unauthorized violations?

A. An audit.
B. An ACL (Access Control List).
C. An audit trail.
D. A 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.

Incorrect Answers:
A: An audit is similar to an audit trail but is a bit more ambiguous as it can also refer to the process of testing security measures, etc. An audit trail would be more accurate. B: An access control list is used to control access to network resources. It lists users that have access to a resource and the type of permissions that have been granted to them on that resource. D: The syslog records system events rather than log on and file access information.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 32-33, 166.
http://www.webopedia.com/TERM/A/audit_trail.html

QUESTION NO: 7
Unique user IDs are critical in the review of audit trails because they

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

Answer: B
Explanation:
Each user account has a unique user ID associated with it. These IDs uniquely identify an authenticated user, allowing you to track user activity once the user has logged on to the system. Thus, the user can be held accountable for his or her actions.

Incorrect Answers:
A: User IDs cannot easily be altered. However, this does not explain their usefulness in audit trails.
C: User IDs do not show which files were changed, but which user account was used to change a file.
D: User IDs do not trigger corrective controls. They uniquely identify a user account.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 14.

QUESTION NO: 8
An attack in which a user logs into a server with his user account, executes a program and then performed activities only available to an administrator is an example of which of the following?

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.

Incorrect Answers:
A: A Trojan horse is a malicious program that may be included as an attachment or as part of a useful installation program. It can be used to create a back door or replace a valid program during installation.
C: A back door is a program or configuration that is designed to allow unauthenticated access to a system. These can be legitimate applications such as Symantec's PC Anywhere, or malicious code such as Sub Seven or T0rnkit.
D: Removing a security policy would not provide a user with more privileges as permissions and privileges needs to be explicitly granted.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 80, 388.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 30, 169. Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 80.

QUESTION NO: 9
Which of the following provides different groups of employees with different rights to files based on the group's needs?

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:
Access control using the RBAC model is based on the role or responsibilities users have in the organization. These usually reflect the organization's structure and can be implemented system wide.

Incorrect Answers:
A: Access control using the DAC model is based on the owner of the resource allowing other users access to that resource.
C: Access control using the MAC model is based on predefined access privileges to a resource.
D: Access control lists contain user names and their associated access permissions to resources. They form the basis for access control models but are not access control models by themselves.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION NO: 10
Which of the following security methods entails enabling 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:

Access control using the MAC model is based on predefined access privileges to a resource this is strict control over subjects and objects by way of access control lists, and a hierarchical list of which users are allowed to access which resources.

Incorrect Answers:
B: Access control using the DAC model is based on the owner of the resource allowing other users access to that resource.
C: Access control using the RBAC model is based on the role or responsibilities users have in the organization. These usually reflect the organization's structure and can be implemented system wide.
D: There is not such thing as a Subjective Access Control model.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

5.6 Understand the concepts of the various topics of forensics. (7 questions)

QUESTION NO: 1
In forensics, which of the following tasks should be performed 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:
When an incident occurs, the first thing that should be done is to document what is going on and notify the incident response team.

Incorrect Answers:
A, **D:** By logging off the network or shutting the system down would corrupt the data and destroy the evidence, particularly data stored in RAM.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 172-177, 385-386.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 101-102.

QUESTION NO: 2
When arriving at a crime scene in which a hacker is accessing unauthorized data on a file server from across the network, what should you do? (Choose all that apply)

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:
You would want to prevent to possible contamination of evidence. This would be best achieved by preventing people other than the incident response team from entering the room. You could disconnect the network cable to prevent the hacker from gaining further data as this will not corrupt evidence.

Incorrect Answers:
B: When an incident occurs, the first thing that should be done is to document what is going on and notify the incident response team.
C: Shuttingdown the server would corrupt any evidence that is stored in RAM. This would result in a loss of evidence.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 172-177, 385-386.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 101-102.

QUESTION NO: 3
After securing a crime scene in which a hacker is accessing unauthorized data on a file server from across the network, what can you so 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:
When an incident occurs, the first thing that should be done is to document what is going on and notify the incident response team. You could document what is the incident by photographing information displayed on the monitors or by writing down messages displayed by the computer.

Incorrect Answers:
C: Shuttingdown the server would corrupt any evidence that is stored in RAM. This would result in a loss of evidence.
D: You should not touch or remove anything from the scene until the incident response team arrives.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 172-177, 385-386.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 101-102.

QUESTION NO: 4
In forensics, which of the following tasks should be done to ensure an exact duplicate of data obtained in an investigation is made?

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.

Incorrect Answers:
B: You should not alter any aspect of the data, including changing file attributes.
C: Comparing files on a individual basis would be time consuming.
D: Imagingsoftware does make accurate copies, though the copies could be corrupt.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 603-607.

QUESTION NO: 5
You work as a crime scene technician at TestKing.com. You arrive with an investigator at a crime scene, which of the following tasks will you be responsible for?

A. Ensuring that any documentation and evidence is handed over to the investigator.
B. Reestablishing a perimeter as new evidence presents itself.
C. Establishing a chain of command.
D. Tagging, bagging, and inventorying 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.

Incorrect Answers:
A, **B:** The investigator is responsible for gathering evidence, and reestablishing perimeters as new evidence is uncovered.
C: Achain of command id not required for the preservation of evidence.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 408.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 608.

QUESTION NO: 6

Which of the following avoids the allegations that the evidence may have been tampered with when it was unaccounted for?

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

Answer: B
Explanation:
The chain of custody documents the history of evidence that has been collected from the moment evidence is discovered through to the presentation of the evidence in court.

Incorrect Answers:
A: A chain of command indicated the hierarchical organization of a company. It is not relevant to the preservation of evidence.
C: There is no such thing as a chain of jurisdiction.
D: Evidence collected during the investigation of the crime is used as proof in determining possible guilt. However, for evidence to be presentable in court, the forensic expert must be able to show that the evidence was handled legitimately, that the evidence was properly preserved, and that the evidence was collected properly. The chain of custody is used to accomplish this.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 602-609.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 385, 406-409.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 101-102, 170-171.

QUESTION NO: 7
Which of the following are responsible for handling security crises?

A. Computer information team.
B. Security resources team.
C. Active detection team.
D. Incident response team.

Answer: D

An incident response team is responsible for responding to incidents in which security may be breached.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 172-177, 385-386.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 101-102.

5.7 Understand and be able to explain the various concepts of risk identification. (15 questions)

QUESTION NO: 1
You work as the security administrator at testKing.com. You need to create asset protection policies. The manager of the IT department has provided you with a list of assets that have importance weighted on a scale of 1 to 10 with 10 having the highest importance. Internet connectivity has an importance of 8, servers have an importance of 9, workstations have an importance of 7, software has an importance of 5 and personnel has an importance of 6. Based on the weights, what is the orderin which you will generate new policies?

A. Internet policy, server security, workstation security policy, personnel safety policy, software policy.
B. Server security policy, Internet policy, workstation security policy, software policy, personnel safety policy.
C. Software policy, personnel safety policy, workstation security policy, Internet policy, server security policy.
D. Server security policy, Internet policy, workstation security policy, personnel safety policy, software policy.

Answer: D
Explanation:
You should generate policies for the most important assets first. In this scenario, servers have the highest importance, followed by Internet connectivity, workstations, personnel and then software.

Incorrect Answers:
A: Policies should be generated for the most important assets first. In this scenario, servers have a higher level of importance than Internet connectivity. Thus, a server security policy should be generated before an Internet plicy. B:

Policies should be generated for the most important assets first. In this scenario, personnel has a higher importance than software. Thus policies for personnel should be generated before policies for software.
C: Policies should be generated for the most important assets first, not for the least important assets. In this scenario, servers have the highest importance, followed by Internet connectivity, workstations, personnel and then software.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 791-792.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 172.

QUESTION NO: 2
You work as the security analyst at TestKing.com. You are currently compiling estimates on the financial impact of a risk occurring 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:
SLE, which is an abbreviation for Single Loss Expectancy, is the cost of a single loss when it occurs.

Incorrect Answers:
A: ARO, which is the Annualized Rate of Occurrence, is based on the likelihood of an event occurring one or more times within a year.
C: ALE, which is the Annual Loss Expectancy, is cost of all events likely to occur within a year. It is calculated by multiplying the SLE by the ARO.
D: Asset identification is the process of identifying assets and prioritizing their importance.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 256
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 172.

QUESTION NO: 3
What will be the objective of implementing policies, procedures, and various security measures once you have identified a number of risks to which your company's assets are exposed?

A. Eliminating every threat that may affect the business.
B. Managing the risks so that the problems resulting from them will be minimized.
C. Implementing as many security measures as possible to address every risk that an asset may be exposed to.
D. Ignoring as many risks as possible to keep costs down.

Answer: B
Explanation:
The purpose of risk analysis is to prepare for the possibility of risks occurring so as to minimize the effect of such events and recovering from them.

Incorrect Answers:
A: Some environmental threats can be minimized but not eliminated.
C: Implementing countermeasure against all risks, especially environmental risks such as earthquakes and hurricanes, would require a large amount of capital and may not make economic sense.
D: If risks are to be ignored, then there is no need for a risk analysis.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 33-35.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 172.

QUESTION NO: 4
Which of the following is a fundamental risk management assumption?

A. Computers can never be completely secure until all vendor patches are installed.
B. Computers can never be completely secure unless they have a variable password.
C. Computers can never be completely secure.
D. Computers can never be completely secure unless they have only one user.

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

Incorrect Answers:
A: Vendor patches are reactive attempt to fix vulnerabilities. They are not proactive. Thus other as yet unknown vulnerabilities might remain.
B: Passwords can be cracked, guessed or spoofed.
D: Computers can never be secure, regardless of the how many people use it.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 33-35.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 172.

QUESTION NO: 5
With regard to computer security, what is an organization's primary purpose in conducting risk analysis?

A. To identify vulnerabilities to the computer systems within the organization.
B. To quantify the impact of potential threats in relation to the cost of lost business-functionality.
C. To identify how much it will cost to implement counter measures.
D. To delegate responsibility.

Answer: B
Explanation:
The purpose of risk analysis is to prepare for the possibility of risks occurring so as to minimize the effect of such events, as well as the cost involved in recovering from them.

Incorrect Answers:
A: Identifying which vulnerabilities a system may be exposed to is one aspect of risk analysis. Risk analysis is also concerned with environmental risks, the costs of recovering from an event and the impact an event might have should it occur.
C: Identifying cost to implement counter measures is one aspect of risk analysis. Risk analysis is also concerned with environmental risks, vulnerabilities, and the impact an event might have should it occur.
D: Risk analysis in not concerned with delegating responsibility.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 33-35.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 172.

QUESTION NO: 6
Which of the following is the best reason to perform a business impact analysis as part of the business continuity planning process?

A. To test the veracity of data obtained from risk analysis.
B. To obtain formal agreement on maximum tolerable downtime.
C. To create the framework for designing tests to determine efficiency of business continuity plans.
D. To 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.

Incorrect Answers:
A: A risk analysis is the second component of a business continuity plan. It is concerned with the probability of asset loss while a business impact analysis is concerned with critical business processes.
C, D: A business impact analysis is a component of a business continuity plan. It is concerned with critical business processes.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 253-254.

QUESTION NO: 7

You work as the system administrator at TestKing.com. You have just performed a backup of the data on a server. Under which of the following conditions will the data on the server still be at risk?

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

Answer: A
Explanation:
Recovery is equally as important a step as the original backup. Sadly, most system administrators make the assumption that their recovery will work flawlessly and fail to test their recovery procedures.

Incorrect Answers:
B: Reliable backups and recovery can be performed, regardless of whether users are logged on.
C: Keeping backup media on an off-site location is a good security precaution incase a natural disaster occurs.
D: If a failure occurs during the backup, then the data was always at risk. The failure would **prevent the backup from being created; hence we cannot then speak of the data still being at risk** as we have not moved beyond that.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 690-696.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 363-368.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 156.

QUESTION NO: 8
Which of the following will be MOST affected by missing audit log entries?

A. The ability to recover destroyed data.
B. The ability to legally prosecute an attacker.
C. The ability to evaluate system vulnerabilities.
D. The ability to create reliable system backups.

Answer: B
Audit logs play an important role in audit trails. They allow administrators to identify the user account used to perpetrate an attack and possibly prosecute the guilty party. Should the audit logs be lost or altered, thie will not be possible.

Incorrect Answers:
A, **D:** Auditlogs are not used for data backup or recovery purposes. C:
Auditlogs are used in audit trains, not in risk analysis.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 27-28, .
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 101, 102.

QUESTION NO: 9
Which of the following preventative measures should an administrator adopt to reduce vulnerabilities on a web server?

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:
Web servers must be accessible to internet users. Therefore it is not possible to protect them by using traditional techniques such as IP filtering or placing them behind firewalls. The best way to protect such servers is by ensuring that the latest security updates and patches are installed on the servers. These updates and patches are provided by the operating system vendor.

Incorrect Answers:
A: Depending on the amount of traffic that a web server could receive, the use of packet sniffing would require great overhead.
C: Auditing a web server is not really practical given the amount of audited data that would be collected.
D: The web server should need to be accessible to the Internet. Blocking incoming DNS requests to the server would make it impossible for users to access the server.

References:

Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 245, 478.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 217.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 108.

QUESTION NO: 10
Which of the following will ensure that security controls in a system do NOT become vulnerabilities?

A. If the security controls are designed and implemented by the system vendor.
B. Adequately testing the security controls.
C. If the security controls are implemented at the application layer in the system.
D. If the security controls are designed to use multiple factors of authentication.

Answer: B
Explanation:
Any security controls, which include firewalls IDS systems, should be tested to ensure that they meet the organizations requirements. Untested security controls which may have been incorrectly configured would represent a potential vulnerability.

Incorrect Answers:
A, **C:** The vendor that designs and implements the security control, or the OSI layer at which the security control operates, will not lead to a vulnerability.
D: Multifactorauthentication is more secure and would not create a vulnerability.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 249.

QUESTION NO: 11
With regard to the ARO, where can you find specific data that can be used for risk assessment?

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:
ARO, which is the Annualized Rate of Occurrence, is based on the likelihood of an event occurring one or more times within a year. This can be based on historical data. Most companies take insurance against disasters and would instigate an insurance claim in the event of such an occurrence. Thus, the insurance business would be a good source of information.

Incorrect Answers:
B: Stockbrokers deal with shares and share prices, not asset loss.
C: Asset loss of software and equipment are assets do not appear in manuals.
D: ARO cannot be accurately predicted but risk analysis and risk management is not concerned with accuracy, but probability.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 256
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 172.

QUESTION NO: 12
At which of the following stages 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 similar to system scanning and vulnerability scanning. It is used to determine if all known security vulnerabilities have been correctly addressed by producing an audit report listing all of the vulnerabilities of the system.

Incorrect Answers:
B, D: There is no such thing as control testing or discovery testing.
C:

Audit planning is not related to vulnerability testing. Auditing is used to trace the user that violates a system while vulnerability testing is used to ensure that violations via known vulnerabilities do not occur.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 33.

QUESTION NO: 13
You work as a network administrator at TestKing.com. You want to test the network for security vulnerabilities. Which of the following is the MOST effective method you can use to determine what security holes reside on a network?

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:
A vulnerability assessment is a set of tools that are used to identify vulnerabilities in a network. It usually works by scanning the network for IP hosts and identifying the different services running on the hosts. Each service then probed to test the service for its security against known vulnerabilities.

Incorrect Answers:
B, C: Port scanning and sniffers are often used as part of a vulnerability assessment, however, on their own, they do not expose all known vulnerabilities.
D: An IDS does not detect vulnerabilities. It used known patterns of attacks and deviations from normal network behavior to identify possible attacks.

References:
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 301.

QUESTION NO: 14
Which of the following does a company demonstrate by having a security vulnerability assessment performed on systems that it relies on?

A. That the site CANNOT be hacked.
B. A commitment to protecting data and customers.
C. Insecurity on the part of the organization.
D. A needless fear of attack.

Answer: B
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.

Incorrect Answers:
A: It is not possible to create a hack proof system. It is only possible to ensure that known vulnerabilities are not used to hack a system. No precautions can be taken against as yet unknown vulnerabilities.
C, D: In today's interconnected networks, the threat of hackers is real. Taking precaution against hackers does not constitute a needless fear or insecurity on the part of the organization.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, **P11.**

QUESTION NO: 15
When are privileged accounts MOST vulnerable?

A. Immediately after a successful remote login.
B. Immediately after a privileged user is terminated.
C. Immediately after a default installation is performed.
D. Immediately after a full system backup is performed.

Answer: B
Explanation:
When a disgruntled administrator is fired the system is most vulnerable until the fired administrator's user account is deleted. While his or her account is still operable, the fired administrator could login remotely and wreck havoc to the system.

Incorrect Answers:

A: Remote login is normal in a network environment. They do pose a security risk but there should be secure authentication methods in place for these logins.
C: Permissions must be explicitly granted. If permissions are not granted, then there are no permissions. During the default installation, the Administrator's account is the one with the most default permissions. These accounts are usually renamed to increase their security. However, this account is still protected by a password which the administrator enters during the installation. D: Permissions must be explicitly granted. If permissions are not granted, then there are no permissions. No permissions are granted during backup and once the backup is restored, the permissions are retained.

References:
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 401.

5.8 Understand the security relevance of the education and training of end users, executives and human resources. (3 questions)

QUESTION NO: 1
In which of the following can company intranets, newsletters, posters, login banners and e-mails be used?

A. In a security investigation.
B. In a security awareness program.
C. In a security policy review.
D. In a security control test.

Answer: B
Explanation:
Intranets, newsletters, posters, login banners and e-mails are advertising techniques that can be used to raise security awareness, especially newsletters and e-mails.

Incorrect Answers:
A, **D:** Advertising techniques such as login banners and posters usually do not form part of a security investigation or a security control test.
C: A security policy review would use the policy itself, not advertising techniques.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416.

QUESTION NO: 2
Which of the following is typically the weakest links in the security of an organization?

A. Firewalls
B. Policies
C. Viruses
D. Human beings

Answer: D
Explanation:
People are the weakest link in any security organization. They are prone to human error, errors in judgment, and lack of vigilance. Furthermore, they do not always follow correct procedures, do not always adhere to policies, and could misconfigure security devices such as firewalls.

Incorrect Answers:
A: A correctly configured firewall protects an internal network from attackers on an external network, such as the Internet. These however, are still dependant on humans configuring them correctly. Thus human beings rather than the firewall are the weak link here.
B: Policies have to be adhered to and implemented correctly. It is not the policy that is a weak link, but the people that must adhere to them, or implement them that are.
C: Viruses are not part of a security organization

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 72-73.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 290.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 31.

QUESTION NO: 3
Which of the following is the MOST effective way of protecting users against social engineering?

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 is a type of attack that exploits human behavior in an attempt to trick the victim into performing some activity or revealing some information that they should not. It can take many forms including, skillfully worded websites, clever e-mail messages, personnel impersonations and acting. There is no fool proof defense against social engineering though its threat can be minimized through security awareness campaigns and education and training campaigns.

Incorrect Answers:
B: Socialengineering is not a network based attack. Therefore firewall, which protects an internal network from attacks originating from an external network, cannot guard against it. C: Social engineering cannot be prevented through authentication methods. D: Socialengineering is not a network based attack. Therefore IDS, which uses known patterns and signatures of network attacks and deviations in network behavior, cannot detect it.

References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 72.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 243-244.

5.9 Understand and explain the various documentation concepts. (4 questions)

QUESTION NO: 1
Which of the following does NOT explain why appropriate documentation of a security incident is important?

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 NO: 2
What must a system administrator do to ensure that system logging is an effective security measure?

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.

Incorrect Answers:
B: Circular logging overwrites data once the log file becomes full. This ensures that the log file does not become too large. However, some data would be lost.
C: Configuring the system to shutdown when the logs are full will ensure that logging will **always take place; however, if the log is not review then there is no point in ensuring that** logging does take place.
D: SNMP Traps allows network management systems to interoperate using SNMP. However, this does not make logging an effective tool.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 84.

QUESTION NO: 3
Which of the following is the MOST common goal of operating system logging?

A. Determining the amount of time employees spend using various applications.
B. Keeping a record of system events.
C. Providing details of what systems have been compromised.
D. Providing details of which systems are interconnected.

Answer: B
Explanation:
System logging records system events.

Incorrect Answers:
A: Monitoring application usage is not a common purpose for system logging.
C: System logging can provide information on what systems have been compromised. It, however, accomplishes this through recording system events.
D: **System logging does not provide information on interconnectivity between systems; it** provides information on systems events.

References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 33.

QUESTION NO: 4
You work as the security administrator at TestKing.com. You want to maximize the effectiveness of system logging. What should you do?

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.

Incorrect Answers:
A: Encrypting the log files will ensure that the log files are not compromised; however, this is of no use if the logs are not monitored and reviewed regularly.
B: Rotating the log files is of no use if the logs are not monitored and reviewed regularly.
C: Printing and copying log files are meaningless if the logs are not monitored and reviewed.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 84.