

ALL ■ IN ■ ONE

CompTIA Security+™

EXAM GUIDE
Second Edition

Gregory White
Wm. Arthur Conklin
Dwayne Williams
Roger Davis
Chuck Cothren



New York • Chicago • San Francisco • Lisbon
London • Madrid • Mexico City • Milan • New Delhi
San Juan • Seoul • Singapore • Sydney • Toronto

McGraw-Hill is an independent entity from CompTIA. This publication and CD may be used in assisting students to prepare for the CompTIA Security+ Exam. Neither CompTIA nor McGraw-Hill warrants that use of this publication and CD will ensure passing any exam. CompTIA is a registered trademark of CompTIA in the United States and/or other countries.

- Authentication mechanisms ensure that only valid users are provided access to the computer system or network.
- The three general methods used in authentication involve the users providing either something they know, something they have, or something unique about them (something they are).

Questions

To further help you prepare for the Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the list of correct answers at the end of the chapter.

1. Which access control mechanism provides the owner of an object the opportunity to determine the access control permissions for other subjects?
 - A. Mandatory
 - B. Role-based
 - C. Discretionary
 - D. Token-based
2. What is the most common form of authentication used?
 - A. Biometrics
 - B. Tokens
 - C. Access card
 - D. Username/password
3. A retinal scan device is an example of what type of authentication mechanism?
 - A. Something you know
 - B. Something you have
 - C. Something about you/something you are
 - D. Multifactor authentication
4. Which of the following is true about the security principle of *implicit deny*?
 - A. In a given access control situation, if a rule does not specifically allow the access, it is by default denied.
 - B. It incorporates both access-control and authentication mechanisms into a single device.
 - C. It allows for only one user to an object at a time; all others are denied access.
 - D. It bases access decisions on the role of the user, as opposed to using the more common access control list mechanism.

5. From a security standpoint, what are the benefits of *job rotation*?
 - A. It keeps employees from becoming bored with mundane tasks that might make it easier for them to make a mistake without noticing.
 - B. It provides everybody with a better perspective of the issues surrounding security and lessens the impact of losing any individual employee since others can assume their duties.
 - C. It keeps employees from learning too many details related to any one position thus making it more difficult for them to exploit that position.
 - D. It ensures that no employee has the opportunity to exploit a specific position for any length of time without risk of being discovered.
6. What was described in the chapter as being essential in order to implement mandatory access controls?
 - A. Tokens
 - B. Certificates
 - C. Labels
 - D. Security classifications
7. The CIA of security includes
 - A. Confidentiality, integrity, authentication
 - B. Certificates, integrity, availability
 - C. Confidentiality, inspection, authentication
 - D. Confidentiality, integrity, availability
8. *Security through obscurity* is an approach to security that is sometimes used but that is dangerous to rely on. It attempts to do the following:
 - A. Protect systems and networks by using confusing URLs to make them difficult to remember or find.
 - B. Protect data by relying on attackers not being able to discover the hidden, confusing, or obscure mechanisms being used as opposed to employing any real security practices or devices.
 - C. Hide data in plain sight through the use of cryptography.
 - D. Make data hard to access by restricting its availability to a select group of users.
9. The fundamental approach to security in which an object has only the necessary rights and privileges to perform its task with no additional permissions is a description of
 - A. Layered security
 - B. Least privilege
 - C. Role-based security
 - D. Kerberos

10. Which access control technique discussed relies on a set of rules to determine whether access to an object will be granted or not?
 - A. Role-based access control
 - B. Object and rule instantiation access control
 - C. Rule-based access control
 - D. Discretionary access control
11. The security principle that ensures that no critical function can be executed by any single individual (by dividing the function into multiple tasks that can't all be executed by the same individual) is known as
 - A. Discretionary access control
 - B. Security through obscurity
 - C. Separation of duties
 - D. Implicit deny
12. The ability of a subject to interact with an object describes
 - A. Authentication
 - B. Access
 - C. Confidentiality
 - D. Mutual authentication
13. Information security places the focus of security efforts on
 - A. The system hardware
 - B. The software
 - C. The user
 - D. The data
14. In role-based access control, which of the following is true?
 - A. The user is responsible for providing both a password and a digital certificate in order to access the system or network.
 - B. A set of roles that the user may perform will be assigned to each user, thus controlling what the user can do and what information he or she can access.
 - C. The focus is on the confidentiality of the data the system protects and not its integrity.
 - D. Authentication and nonrepudiation are the central focus.
15. Using different types of firewalls to protect various internal subnets is an example of
 - A. Layered security
 - B. Security through obscurity

- C. Diversity of defense
- D. Implementing least privilege for access control

Answers

1. C. Discretionary access control provides the owner of an object the opportunity to determine the access control permissions for other subjects.
2. D. Username/password is the single most common authentication mechanism in use today.
3. C. A retinal scan is an example of a biometric device, which falls into the category of something about you/something you are.
4. A. The basic premise of implicit deny is that an action is allowed only if a specific rule states that it is acceptable, making A the most correct answer.
5. B. While both C and D may indeed bear a semblance of truth, they are not the primary reasons given as benefits of rotating employees through jobs in an organization. The reasons discussed included ensuring that no single individual alone can perform security operations, plus the benefit of having more employees understand the issues related to security.
6. C. Labels were discussed as being required for both objects and subjects in order to implement mandatory access controls. D is not the correct answer, because mandatory access controls are often used to implement various levels of security classification but security classifications are not needed in order to implement MAC.
7. D. Don't forget that even though authentication was described at great length in this chapter, the A in the CIA of security represents availability, which refers to the hardware and data being accessible when the user wants it.
8. B. Answer B describes the more general definition of this flawed approach, which relies on attackers not being able to discover the mechanisms being used in the belief that if it is confusing or obscure enough, it will remain safe. The problem with this approach is that once the confusing or obscure technique is discovered, the security of the system and data can be compromised. Security must rely on more than just obscurity to be effective. A does at some level describe activity that is similar to the concept of security through obscurity, but it is not the best answer.
9. B. This description describes least privilege. Layered security refers to using multiple layers of security (such as at the host and network layers) so that if an intruder penetrates one layer, they still will have to face additional security mechanisms before gaining access to sensitive information.
10. C. Rule-based access control relies on a set of rules to determine whether access to an object will be granted or not.

11. C. The separation of duties principle ensures that no critical function can be executed by any single individual.
12. B. Access is the ability of a subject to interact with an object.
13. D. Information security places the focus of the security efforts on the data (information).
14. B. In role-based access controls, roles are assigned to the user. Each role will describe what the user can do and the data or information that can be accessed to accomplish that role.
15. C. This is an example of diversity of defense. The idea is to provide different types of security and not rely too heavily on any one type of product.

Chapter Review

In this chapter, the organizational aspects of computer security were reviewed along with the role that policies, procedures, standards, and guidelines play in it. Taken together, these documents outline the security plan for the organization. Various factors that affect the security of the organization were discussed, including logic access controls and organizational security policies. Social engineering was discussed along with both the direct and indirect methods used. The best defense against all social engineering attacks consists of an active training and awareness program for employees.

Questions

To further help you prepare for the Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the list of correct answers at the end of the chapter.

1. Which type of social engineering attack utilizes voice messaging to conduct the attack?
 - A. Phishing
 - B. War dialing
 - C. Vishing
 - D. War driving
2. Social engineering attacks work well because the individual who is the target of the attack/attempt
 - A. Is often not very intelligent and can't recognize the fact that a social engineering attempt is being attempted.
 - B. Often either genuinely wants to help or is trying to avoid a confrontation, depending on the attacker's specific tack.
 - C. Is new to the organization and can't tell that the story he is being fed is bogus.
 - D. Knows the attacker.
3. From a security standpoint, why should an organization consider a policy of mandatory vacations?
 - A. To ensure that employees are not involved in illicit activity that they are attempting to hide.
 - B. Because employees who are tired are more prone to making errors.
 - C. To provide an opportunity for security personnel to go through their desks and computer systems.
 - D. To keep from having lawsuits filed against the organization for adverse working conditions.

4. Select all of the following that are examples of personally identifiable information:
 - A. An individual's name
 - B. A national identification number
 - C. A license plate number
 - D. A telephone number
 - E. A street address
5. A hoax can still be a security concern because
 - A. It may identify a vulnerability that others can then decide to use in an attack.
 - B. It shows that an attacker has the contact information for an individual who might be used in a later attack.
 - C. It can result in a user performing some action that could lead to a compromise or that might adversely affect the system or network.
 - D. A hoax is never a security concern—that is why it is called a hoax.
6. How should CDs and DVDs be disposed of?
 - A. By shredding using a paper shredder designed also to shred CDs and DVDs.
 - B. By using a commercial grade degausser.
 - C. By overwriting the disk with 0s, then 1s, and then a random character.
 - D. There is no approved way of disposing of this type of media, so they must be archived in a secure facility.
7. What type of attack consists of looking through an individual's or organization's trash for sensitive information?
 - A. Phishing
 - B. Vishing
 - C. Shoulder surfing
 - D. Dumpster diving
8. What type of attack can involve an attacker setting up a camera to record the entries individuals make on keypads used for access control?
 - A. Phishing
 - B. Shoulder surfing
 - C. Dumpster diving
 - D. Vishing

9. Which of the following should be included in a password policy?
 - A. An explanation of how complex the password should be (i.e., what types of characters a password should be made up of)
 - B. The length of time the password will be valid before it expires
 - C. A description on how passwords should be distributed and protected
 - D. All of the above
10. What is the best method of preventing successful phishing attacks?
 - A. Firewalls that can spot and eliminate the phishing e-mails.
 - B. Blocking sites where phishing originates.
 - C. A viable user training and awareness program.
 - D. There is no way to prevent successful phishing attacks.
11. What type of attack uses e-mails with a convincing story to encourage users to provide account or other sensitive information?
 - A. Vishing
 - B. Shoulder surfing
 - C. Dumpster diving
 - D. Phishing
12. The reason for providing a group access control policy is
 - A. It provides a mechanism for individual users to police the other members of the group.
 - B. It provides an easy mechanism to identify common user restrictions for members of the group. This means that individual profiles for each user don't have to be created but instead each is identified as a member of the group with its associated group profile/policies.
 - C. It is the only way to identify individual user access restrictions.
 - D. It makes it easier for abnormal behaviors to be identified, as a group norm can be established.
13. Which of the following is a high-level, broad statement of what the organization wants to accomplish?
 - A. Policy
 - B. Procedure
 - C. Guideline
 - D. Standard

Answers

1. **C.** Vishing is basically a variation of phishing that uses voice communication technology to obtain the information the attacker is seeking. Vishing takes advantage of the trust that most people place in the telephone network. The users are unaware that using Voice over IP (VoIP) technology, attackers can spoof calls from legitimate entities. Voice messaging can be compromised and used in these attempts.
2. **B.** Social engineering works because people generally truly want to help an individual asking for assistance or because they are trying to avoid a confrontation. They also work because people generally want to believe that the individual really is who he claims to be, even if that's not actually the case. The target's intelligence isn't an important factor; anybody can fall prey to an adept social engineer. Being new to an organization can certainly make it easier for an attacker to convince a target that he is entitled to the information requested, but it is not a requirement. Long-time employees can just as easily provide sensitive information to a talented social engineer. The target and attacker generally do not know each other in a social engineering attack, so **D** is not a good answer.
3. **A.** A frequent characteristic of employees who are involved in illicit activities is their reluctance to take a vacation. A prime security reason to require mandatory vacations is to discourage illicit activities in which employees are engaged.
4. **A, B, C, D, E.** All of these are examples of personally identifiable information. Any information that can be used to identify an individual uniquely falls into this category.
5. **C.** A hoax can cause a user to perform some action, such as deleting a file that the operating system needs. Because of this, hoaxes can be considered legitimate security concerns.
6. **A.** Shredders that are designed to destroy CDs and DVDs are common and inexpensive. A degausser is designed for magnetic media, not optical. Writing over with 0s, 1s, and a random character is a method that can be used for other magnetic media but not CDs or DVDs.
7. **D.** This is a description of dumpster diving. From a security standpoint, you should be concerned with an attacker being able to locate information that can help in an attack on the organization. From an individual perspective, you should be concerned about the attacker obtaining information such as bank account or credit card numbers.
8. **B.** This is a description of a shoulder surfing method. Other methods include simply looking over a person's shoulder as she enters code or using binoculars to watch from a distance.

9. **D.** All three of these were mentioned as part of what a password policy should include.
10. **C.** While research is being conducted to support spotting and eliminating phishing e-mails, no effective method is currently available to do this. It may be possible to block some sites that are known to be hostile, but again this is not effective at this time since an e-mail could come from anywhere and its address can be spoofed anyway. There might be some truth to the statement (**D**) that there is no way to prevent successful phishing attacks, because users continue to fall for them. The best way to prevent this is an active and viable user training and awareness program.
11. **D.** This is a description of phishing, which is a type of social engineering attack as are the other options. Vishing employs the use of the telephone network. Shoulder surfing involves the attacker attempting to observe a user entering sensitive information on a form, keypad, or keyboard. Dumpster diving involves the attacker searching through the trash of an organization or individual to find useful and sensitive information.
12. **B.** Groups and domains provide a mechanism to organize users in a logical way. Individuals with similar access restrictions can be placed within the same group or domain. This greatly eases the process of account creation for new employees.
13. **A.** This is the definition of a policy. Procedures are the step-by-step instructions on how to implement policies in an organization.

- I treasure and will defend equality, justice and respect for others.
- I will not participate in any form of discrimination, whether due to race, color, national origin, ancestry, sex, sexual orientation, gender/sexual identity or expression, marital status, creed, religion, age, disability, veteran's status, or political ideology.

Chapter Review

From a system administrator's position, complying with cyber-laws is fairly easy. Add warning banners to all systems that enable consent to monitoring as a condition of access. This will protect you and the firm during normal routine operation of the system. Safeguard all personal information obtained in the course of your duties and do not obtain unnecessary information merely because you can get it. With respect to the various privacy statutes that are industry specific—GLB, FCRA, ECPA, FERPA, HIPAA—refer to your own institution's guidelines and policies. When confronted with aspects of the U.S. Patriot Act, refer to your company's general counsel, for although the act may absolve you and the firm of responsibility, this act's implications with respect to existing law are still unknown. And in the event that your system is trespassed upon (hacked), you can get federal law enforcement assistance in investigating and prosecuting the perpetrators.

Questions

To further help you prepare for the Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the list of correct answers at the end of the chapter.

1. The VP of IS wants to monitor user actions on the company's intranet. What is the best method of obtaining the proper permissions?
 - A. A consent banner displayed upon login
 - B. Written permission from a company officer
 - C. Nothing, because the system belongs to the company
 - D. Written permission from the user
2. Your Social Security number and other associated facts kept by your bank are protected by what law against disclosure?
 - A. The Social Security Act of 1934
 - B. The Patriot Act of 2001
 - C. The Gramm-Leach-Bliley Act
 - D. HIPAA

3. Breaking into another computer system in the United States, even if you do not cause any damage, is regulated by what laws?
 - A. State law, as the damage is minimal
 - B. Federal law under the Identity Theft and Assumption Deterrence Act
 - C. Federal law under Electronic Communications Privacy Act (ECPA) of 1986
 - D. Federal law under the Patriot Act of 2001
4. Export of encryption programs is regulated by the
 - A. U.S. State Department
 - B. U.S. Commerce Department
 - C. U.S. Department of Defense
 - D. National Security Agency
5. For the FBI to install and operate Carnivore on an ISP's network, what is required?
 - A. A court order specifying specific items being searched for
 - B. An official request from the FBI
 - C. An impact statement to assess recoverable costs to the ISP
 - D. A written request from an ISP to investigate a computer trespass incident
6. True or false: Digital signatures are equivalent to notarized signatures for all transactions in the United States.
 - A. True for all transactions in which both parties agree to use digital signatures
 - B. True only for non-real property transactions
 - C. True only where governed by specific state statute
 - D. False, as the necessary laws have not yet passed
7. The primary factor(s) behind data sharing compliance between U.S. and European companies is/are
 - A. Safe Harbor Provision
 - B. European Data Privacy Laws
 - C. U.S. FTC enforcement actions
 - D. All of the above
8. True or false: Writing viruses and releasing them across the Internet is a violation of law.
 - A. Always true. All countries have reciprocal agreements under international law.
 - B. Partially true. Depends on laws in country of origin.
 - C. False. Computer security laws do not cross international boundaries.

- D. Partially true. Depends on the specific countries involved, for the author of the virus and the recipient.
9. Publication of flaws in encryption used for copy protection is a potential violation of
- A. HIPAA
 - B. U.S. Commerce Department regulations
 - C. DMCA
 - D. National Security Agency regulations
10. Violation of DMCA can result in
- A. Civil fine
 - B. Jail time
 - C. Activity subject to legal injunctions
 - D. All of the above

Answers

1. A. A consent banner consenting to monitoring resolves issues of monitoring with respect to the Electronic Communications Privacy Act (ECPA) of 1986.
2. C. The Gramm-Leach-Bliley Act governs the sharing of privacy information with respect to financial institutions.
3. D. The Patriot Act of 2001 made computer trespass a felony.
4. B. Export controls on commercial encryption products are administered by the Bureau of Industry and Security (BIS) in the U.S. Department of Commerce.
5. B. The Patriot Act of 2001 mandated ISP compliance with the FBI Carnivore program.
6. A. Electronic digital signatures are considered valid for transactions in the United States since the passing of the Electronic Signatures in Global and National Commerce Act (E-Sign) in 2001.
7. D. All of the above. The primary driver is European data protection laws as enforced on U.S. firms by FTC enforcement through the Safe Harbor provision mechanism.
8. D. This is partially true, for not all countries share reciprocal laws. Some common laws and reciprocity issues exist in certain international communities—for example, European Union—so some cross-border legal issues have been resolved.
9. C. This is a potential violation of the Digital Millennium Copyright Act of 1998 unless an exemption provision is met.

10. D. All of the above have been attributed to DMCA, including the jailing of a Russian programmer who came to the United States to speak at a security conference. See w2.eff.org/IP/DMCA/?f=20010830_eff_dmca_op-ed.html.

a boot sector encryption method that protects data on the Vista operating system. BitLocker utilizes AES encryption to encrypt every file on the hard drive automatically. All encryption occurs in the background, and decryption occurs seamlessly when data is requested. The decryption key can be stored in the Trusted Platform Module (TPM) or on a USB key.

Chapter Review

Cryptography is in many ways the key to security in many systems. The progression of technology has allowed systems to be built to retrieve the secrets of others. More and more information is being digitized and then stored and sent via computers. Storing and transmitting valuable data and keeping it secure can be best accomplished with encryption.

In this chapter, you have seen the message digest one-way functions for passwords and message integrity checks. You have also examined the symmetric encryption algorithms used for encrypting data at high speeds. Finally, you have learned about the operation of asymmetric cryptography that is used for key management and digital signatures. These are three distinct types of encryption with different purposes.

The material presented in this chapter is based on current algorithms and techniques. When implemented properly, they will improve security; however, they need to be updated as encryption strength decays. Encryption is based on traditionally difficult mathematical problems, and it can keep data secure only for a limited amount of time, as technology for solving those problems improves—for example, encryption that was incredibly effective 50 years ago is now easily broken. However, current encryption methods can provide a reasonable assurance of security.

Questions

To further help you prepare for the Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the list of correct answers at the end of the chapter.

1. What is the biggest drawback to symmetric encryption?
 - A. It is too easily broken.
 - B. It is too slow to be easily used on mobile devices.
 - C. It requires a key to be securely shared.
 - D. It is available only on UNIX.
2. What is Diffie-Hellman most commonly used for?
 - A. Symmetric encryption key exchange
 - B. Signing digital contracts
 - C. Secure e-mail
 - D. Storing encrypted passwords

3. What is AES meant to replace?
 - A. IDEA
 - B. DES
 - C. Diffie-Hellman
 - D. MD5
4. What kind of encryption cannot be reversed?
 - A. Asymmetric
 - B. Hash
 - C. Linear cryptanalysis
 - D. Authentication
5. What is public key cryptography a more common name for?
 - A. Asymmetric encryption
 - B. SHA
 - C. An algorithm that is no longer secure against cryptanalysis
 - D. Authentication
6. How many bits are in a block of the SHA algorithm?
 - A. 128
 - B. 64
 - C. 512
 - D. 1024
7. How does elliptical curve cryptography work?
 - A. It multiplies two large primes.
 - B. It uses the geometry of a curve to calculate three points.
 - C. IT shifts the letters of the message in an increasing curve.
 - D. It uses graphs instead of keys.
8. A good hash function is resistant to what?
 - A. Brute-forcing
 - B. Rainbow tables
 - C. Interception
 - D. Collisions
9. How is 3DES an improvement over normal DES?
 - A. It uses public and private keys.
 - B. It hashes the message before encryption.
 - C. It uses three keys and multiple encryption and/or decryption sets.
 - D. It is faster than DES.

10. What is the best kind of key to have?
 - A. Easy to remember
 - B. Long and random
 - C. Long and predictable
 - D. Short
11. What makes asymmetric encryption better than symmetric encryption?
 - A. It is more secure.
 - B. Key management is part of the algorithm.
 - C. Anyone with a public key could decrypt the data.
 - D. It uses a hash.
12. What kinds of encryption does a digital signature use?
 - A. Hashing and asymmetric
 - B. Asymmetric and symmetric
 - C. Hashing and symmetric
 - D. All of the above
13. What does differential cryptanalysis require?
 - A. The key
 - B. Large amounts of plaintext and ciphertext
 - C. Just large amounts of ciphertext
 - D. Computers able to guess at key values faster than a billion times per second
14. What is a brute-force attack?
 - A. Feeding certain plaintext into the algorithm to deduce the key
 - B. Capturing ciphertext with known plaintext values to deduce the key
 - C. Sending every key value at the algorithm to find the key
 - D. Sending two large men to the key owner's house to retrieve the key
15. What is key escrow?
 - A. Printing out your private key
 - B. How Diffie-Hellman exchanges keys
 - C. When the government keeps a copy of your key
 - D. Rijndael

Answers

1. C. In symmetric encryption, the key must be securely shared. This can be complicated because long keys are required for good security.
2. A. Diffie-Hellman is most commonly used to protect the exchange of keys used to create a connection using symmetric encryption. It is often used in Transport Layer Security (TLS) implementations for protecting secure web pages.
3. B. AES, or Advanced Encryption Standard, is designed to replace the old U.S. government standard DES.
4. B. Hash functions are one-way and cannot be reversed to provide the original plaintext.
5. A. Asymmetric encryption is another name for public key cryptography.
6. C. 512 bits make up a block in SHA.
7. B. Elliptical curve cryptography uses two points to calculate a third point on the curve.
8. D. A good hash algorithm is resistant to collisions, or two different inputs hashing to the same value.
9. C. 3DES uses multiple keys and multiple encryption or decryption rounds to improve security over regular DES.
10. B. The best encryption key is one that is long and random, to reduce the predictability of the key.
11. B. In public key cryptography, only the private keys are secret, so key management is built into the algorithm.
12. A. Digital signatures use hashing and asymmetric encryption.
13. B. Differential cryptanalysis requires large amounts of plaintext and ciphertext.
14. C. Brute-forcing is the attempt to use every possible key to find the correct one.
15. C. When the government keeps a copy of your private key, this is typically referred to as key escrow.

Questions

1. When a user wants to participate in a PKI, what component does he or she need to obtain, and how does that happen?
 - A. The user submits a certification request to the CA.
 - B. The user submits a key pair request to the CRL.
 - C. The user submits a certification request to the RA.
 - D. The user submits proof of identification to the CA.
2. How does a user validate a digital certificate that is received from another user?
 - A. The user will first see whether her system has been configured to trust the CA that digitally signed the other user's certificate and will then validate that CA's digital signature.
 - B. The user will calculate a message digest and compare it to the one attached to the message.
 - C. The user will first see whether her system has been configured to trust the CA that digitally signed the certificate and then will validate the public key that is embedded within the certificate.
 - D. The user will validate the sender's digital signature on the message.
3. What is the purpose of a digital certificate?
 - A. It binds a CA to a user's identity.
 - B. It binds a CA's identity to the correct RA.
 - C. It binds an individual to an RA.
 - D. It binds an individual to a public key.
4. What steps does a user take to validate a CA's digital signature on a digital certificate?
 - A. The user's software creates a message digest for the digital certificate and decrypts the encrypted message digest included within the digital certificate. If the decryption performs properly and the message digest values are the same, the certificate is validated.
 - B. The user's software creates a message digest for the digital signature and encrypts the message digest included within the digital certificate. If the encryption performs properly and the message digest values are the same, the certificate is validated.
 - C. The user's software creates a message digest for the digital certificate and decrypts the encrypted message digest included within the digital certificate. If the user can encrypt the message digest properly with the CA's private key and the message digest values are the same, the certificate is validated.

- D. The user's software creates a message digest for the digital signature and encrypts the message digest with its private key. If the decryption performs properly and the message digest values are the same, the certificate is validated.
5. What is a bridge CA, and what is its function?
- A. It is a hierarchical trust model that establishes a root CA, which is the trust anchor for all other CAs.
 - B. It is an entity that creates and maintains the CRL for several CAs at one time.
 - C. It is a CA that handles the cross-certification certificates for two or more CAs in a peer-to-peer relationship.
 - D. It is an entity that validates the user's identity information for the RA before the request goes to the CA.
6. Why would a company implement a key archiving and recovery system within the organization?
- A. To make sure all data encryption keys are available for the company if and when it needs them
 - B. To make sure all digital signature keys are available for the company if and when it needs them
 - C. To create session keys for users to be able to access when they need to encrypt bulk data
 - D. To back up the RA's private key for retrieval purposes
7. Within a PKI environment, where does the majority of the trust actually lie?
- A. All users and devices within an environment trust the RA, which allows them to indirectly trust each other.
 - B. All users and devices within an environment trust the CA, which allows them to indirectly trust each other.
 - C. All users and devices within an environment trust the CRL, which allows them to indirectly trust each other.
 - D. All users and devices within an environment trust the CPS, which allows them to indirectly trust each other.
8. Which of the following properly explains the *m of n control*?
- A. This is the process a user must go through to properly register for a certificate through the RA.
 - B. This ensures that a certificate has to be fully validated by a user before he can extract the public key and use it.
 - C. This is a control in key recovery to enforce separation of duties.
 - D. This is a control in key recovery to ensure that the company cannot recover a user's key without the user's consent.

9. Which of the following is not a valid field that could be present in an X.509 version 3 digital certificate?
 - A. Validity dates
 - B. Serial number
 - C. Extensions
 - D. Symmetric key
10. To what does a certificate path pertain?
 - A. All of the digital certificates that need to be validated before a received certificate can be fully validated and trusted
 - B. All of the digital certificates that need to be validated before a sent certificate can be properly encrypted
 - C. All of the digital certificates that need to be validated before a user trusts her own trust anchor
 - D. All of the digital certificates that need to be validated before a received certificate can be destroyed
11. Which of the following certificate characteristics was expanded upon with version 3 of the X.509 standard?
 - A. Subject
 - B. Extensions
 - C. Digital signature
 - D. Serial number
12. What is a certification practices statement (CPS), and what is its purpose?
 - A. A CPS outlines the steps a CA goes through to validate identities and generate certificates. Companies should review this document to ensure that the CA follows the necessary steps the company requires and provides the necessary level of protection.
 - B. A CPS outlines the steps a CA goes through to communicate with other CAs in other states. Companies should review this document to ensure that the CA follows the necessary steps the company requires and provides the necessary level of protection.
 - C. A CPS outlines the steps a CA goes through to set up an RA at a company's site. Companies should review this document to ensure that the CA follows the necessary steps the company requires and provides the necessary level of protection.
 - D. A CPS outlines the steps a CA goes through to become a business within a vertical market. Companies should review this document to ensure that the CA follows the necessary steps the company requires and provides the necessary level of protection.

13. Which of the following properly describes what a public key infrastructure (PKI) actually is?
 - A. A protocol written to work with a large subset of algorithms, applications, and protocols
 - B. An algorithm that creates public/private key pairs
 - C. A framework that outlines specific technologies and algorithms that must be used
 - D. A framework that does not specify any technologies, but provides a foundation for confidentiality, integrity, and availability services
14. Once an individual validates another individual's certificate, what is the use of the public key that is extracted from this digital certificate?
 - A. The public key is now available to use to create digital signatures.
 - B. The user can now encrypt session keys and messages with this public key and can validate the sender's digital signatures.
 - C. The public key is now available to encrypt future digital certificates that need to be validated.
 - D. The user can now encrypt private keys that need to be transmitted securely.
15. Why would a digital certificate be added to a certificate revocation list (CRL)?
 - A. If the public key had become compromised in a public repository
 - B. If the private key had become compromised
 - C. If a new employee joined the company and received a new certificate
 - D. If the certificate expired
16. What is an online CRL service?
 - A. End-entities can send a request containing a serial number of a specific certificate to an online CRL service. The online service will query several CRL distribution points and respond with information about whether the certificate is still valid or not.
 - B. CAs can send a request containing the expiration date of a specific certificate to an online CRL service. The online service will query several other RAs and respond with information about whether the certificate is still valid or not.
 - C. End-entities can send a request containing a public key of a specific certificate to an online CRL service. The online service will query several end-entities and respond with information about whether the certificate is still valid or not.
 - D. End-entities can send a request containing a public key of a specific CA to an online CRL service. The online service will query several RA distribution points and respond with information about whether the CA is still trustworthy or not.

17. If an extension is marked as critical, what does this indicate?
 - A. If the CA is not programmed to understand and process this extension, the certificate and corresponding keys can be used for their intended purpose.
 - B. If the end-entity is programmed to understand and process this extension, the certificate and corresponding keys cannot be used.
 - C. If the RA is not programmed to understand and process this extension, communication with the CA is not allowed.
 - D. If the end-entity is not programmed to understand and process this extension, the certificate and corresponding keys cannot be used.
18. How can users have faith that the CRL was not modified to present incorrect information?
 - A. The CRL is digitally signed by the CA.
 - B. The CRL is encrypted by the CA.
 - C. The CRL is open for anyone to post certificate information to.
 - D. The CRL is accessible only to the CA.
19. When would a certificate be suspended, and where is that information posted?
 - A. It would be suspended when an employee leaves the company. It is posted on the CRL.
 - B. It would be suspended when an employee changes his or her last name. It is posted on the CA.
 - C. It would be suspended when an employee goes on vacation. It is posted on the CRL.
 - D. It would be suspended when a private key is compromised. It is posted on the CRL.
20. What does cross certification pertain to in a PKI environment?
 - A. When a company uses an outsourced service provider, it needs to modify its CPS to allow for cross certification to take place between the RA and CA.
 - B. When two end-entities need to communicate in a PKI, they need to exchange certificates.
 - C. When two or more CAs need to trust each other so that their end-entities can communicate, they will create certificates for each other.
 - D. A RA needs to perform a cross certification with a user before the certificate registration is terminated.

Answers

1. **C.** The user must submit identification data and a certification request to the registration authority (RA). The RA validates this information and sends the certification request to the certificate authority (CA).
2. **A.** A digital certificate is validated by the receiver by first determining whether her system has been configured to trust the CA that digitally signed the certificate. If this has been configured, the user's software uses the CA's public key and validates the CA's digital signature that is embedded within the certificate.
3. **D.** A digital certificate vouches for an individual's identity and binds that identity to the public key that is embedded within the certificate.
4. **A.** The user's software calculates a message digest for the digital certificate and decrypts the encrypted message digest value included with the certificate, which is the digital signature. The message digest is decrypted using the CA's public key. If the two message digest values match, the user knows that the certificate has not been modified in an unauthorized manner, and since the encrypted message digest can be decrypted properly with the CA's public key, the user is assured that this CA created the certificate.
5. **C.** A bridge CA is set up to handle all of the cross-certification certificates and traffic between different CAs and trust domains. A bridge CA is used instead of requiring all of the CAs to authenticate to each other and create certificates with one another, which would end up in a full mesh configuration.
6. **A.** To protect itself, the company will make backups of the data encryption keys its employees use for encrypting company information. If an employee is no longer available, the company must make sure that it still has access to its own business data. Companies should not need to back up digital signature keys, since they are not used to encrypt data.
7. **B.** The trust anchor for a PKI environment is the CA. All users and devices trust the CA, which allows them to indirectly trust each other. The CA verifies and vouches for each user's and device's identity, so these different entities can have confidence that they are communicating with specific individuals.
8. **C.** The m of n control is the part of the key recovery software that allows a certain number of people to be involved with recovering and reconstructing a lost or corrupted key. A certain number of people (n) are allowed to authenticate to the software, which will allow them to participate in the key recovery process. Not all of those people may be available at one time, however, so a larger number of people (m) need to be involved with the process. The system should not allow only one person to carry out key recovery, because that person could then use the keys for fraudulent purposes.
9. **D.** The first three values are valid fields that are used in digital certificates. Validity dates indicate how long the certificate is good for, the serial number

is a unique value used to identify individual certificates, and extensions allow companies to expand the use of their certificates. A public key is included in the certificate, which is an asymmetric key, not a symmetric key.

10. **A.** The certificate path is all of the certificates that must be validated before the receiver of a certificate can validate and trust the newly received certificate. When a user receives a certificate, she must obtain the certificate and public key of all of the CAs until she comes to a self-signed certificate, which is the trusted anchor. So the user must validate each of these certificates until the trusted anchor is reached. The path between the receiver and a trusted anchor is referred to as the certificate path. This is a hierarchical model of trust, and each rung of the trust model must be verified before the end user's certificate can be validated and trusted.
11. **B.** The X.509 standard is currently at version 3, which added more extension capabilities to digital certificates and which added more flexibility for companies using PKIs. Companies can define many of these extensions to mean specific things that are necessary for their proprietary or customized environment and software.
12. **A.** The CPS outlines the certificate classes the CA uses and the CA's procedures for verifying end-entity identities, generating certificates, and maintaining the certificates throughout their lifetimes. Any company that will be using a specific CA needs to make sure it is going through these procedures with the level of protection the company would require of itself. The company will be putting a lot of trust in the CA, so the company should do some homework and investigate how the CA actually accomplishes its tasks.
13. **D.** A PKI is a framework that allows several different types of technologies, applications, algorithms, and protocols to be plugged into it. The goal is to provide a foundation that can provide a hierarchical trust model, which will allow end-entities to indirectly trust each other and allow for secure and trusted communications.
14. **B.** Once a receiver validates a digital certificate, the embedded public key can be extracted and used to encrypt symmetric session keys, encrypt messages, and validate the sender's digital signatures.
15. **B.** Certificates are added to a CRL the public/private key pair should no longer be bound to a specific person's identity. This can happen if a private key is compromised, meaning that it was stolen or captured—this would mean someone else could be using the private key instead of the original user, so the CRL is a protection mechanism that will alert others in the PKI of this incident. Certificates can be added to the CRL if an employee leaves the company or is no longer affiliated with the company for one reason or another. Expired certificates are not added to CRLs.
16. **A.** Actually getting the data on the CRLs to end-entities is a huge barrier for many PKI implementations. The environment can have distribution points

set up, which provide centralized places that allow the users' systems to query to see whether a certificate has been revoked or not. Another approach is to push down the CRLs to each end-entity or to use an online service. The online service will do the busy work for the end-entity by querying all the available CRLs and returning a response to the end-entity indicating whether the certificate has been revoked or not.

17. D. Digital certificates have extensions that allow companies to expand the use of certificates within their environments. When a CA creates a certificate, it is certifying the key pair to be used for a specific purpose (for digital signatures, data encryption, validating a CA's digital signature, and so on). If a CA adds a critical flag to an extension, it is stating that the key pair can be used only for the reason stated in the extension. If an end-entity receives a certificate with this critical flag set and cannot understand and process the marked extension, the key pair cannot be used at all. The CA is stating, "I will allow the key pair to be used only for this purpose and under these circumstances." If an extension is marked noncritical, the end-entity does not have to be able to understand and process that extension.
18. A. The CRL contains all of the certificates that have been revoked. Only the CA can post information to this list. The CA then digitally signs the list to ensure that any modifications will be detected. When an end-entity receives a CRL, it verifies the CA's digital signature, which tells the end-entity whether the list has been modified in an unauthorized manner and guarantees that the correct CA signed the list.
19. C. A certificate can be suspended if it needs to be temporarily taken out of production for a period of time. If an employee goes on vacation and wants to make sure no one can use his certificate, he can make a suspension request to the CA, which will post the information to the CRL. The other answers in this question would require the certificate to be revoked, not suspended, and a new certificate would need to be created for the user.
20. C. Cross certification means that two or more CAs create certificates for each other. This takes place when two trust domains, each with their own CA, need to be able to communicate—a trusted path needs to be established between these domains. Once the first CA validates the other CA's identity and creates a certificate, it then trusts this other CA, which creates a trusted path between the different PKI environments. The trust can be bidirectional or unidirectional.

rity policies and practices can be developed in 12 areas. Various types of publications are available from NIST such as those found in the FIPS series.

Questions

1. Which organization created PKCS?
 - A. RSA
 - B. IEEE
 - C. OSI
 - D. ISO
2. Which of the following is not part of a public key infrastructure?
 - A. Certificates
 - B. Certificate revocation list (CRL)
 - C. Substitution cipher
 - D. Certificate authority (CA)
3. Which of the following is used to grant permissions using rule-based, role-based, and rank-based access controls?
 - A. Attribute Certificate
 - B. Qualified Certificate
 - C. Control Certificate
 - D. Operational Certificate
4. Transport Layer Security consists of which two protocols?
 - A. TLS Record Protocol and TLS Certificate Protocol
 - B. TLS Certificate Protocol and TLS Handshake Protocol
 - C. TLS Key Protocol and TLS Handshake Protocol
 - D. TLS Record Protocol and TLS Handshake Protocol
5. Which of the following provides connection security by using common encryption methods?
 - A. TLS Certificate Protocol
 - B. TLS Record Protocol
 - C. TLS Layered Protocol
 - D. TLS Key Protocol
6. Which of the following provides a method for implementing a key exchange protocol?
 - A. EISA

- B. ISA
 - C. ISAKMP
 - D. ISAKEY
7. A relationship in which two or more entities define how they will communicate securely is known as what?
- A. Security association
 - B. Security agreement
 - C. Three-way agreement
 - D. Three-way handshake
8. The entity requesting an SA sets what?
- A. Initiator cookie
 - B. Process ID
 - C. Session number
 - D. Session ID
9. What protocol is used to establish a CA?
- A. Certificate Management Protocol
 - B. Internet Key Exchange Protocol
 - C. Secure Sockets Layer
 - D. Public Key Infrastructure
10. What is the purpose of XKMS?
- A. Encapsulates session associations over TCP/IP
 - B. Extends session associations over many transport protocols
 - C. Designed to replace SSL
 - D. Defines services to manage heterogeneous PKI operations via XML
11. Which of the following is a secure e-mail standard?
- A. POP3
 - B. IMAP
 - C. S/MIME
 - D. SMTP
12. Secure Sockets Layer uses what port to communicate?
- A. 143
 - B. 80
 - C. 443
 - D. 53

Answers

1. A. RSA Laboratories created Public Key Cryptography Standards (PKCS).
2. C. The substitution cipher is not a component of PKI. The substitution cipher is an elementary alphabet-based cipher.
3. A. An Attribute Certificate (AC) is used to grant permissions using rule-based, role-based, and rank-based access controls.
4. D. Transport Layer Security consists of the TLS Record Protocol, which provides security, and the TLS Handshake Protocol, which allows the server and client to authenticate each other.
5. B. The TLS Record Protocol provides connection security by using common encryption methods, such as DES.
6. C. The Internet Security Association and Key Management Protocol (ISAKMP) provides a method for implementing a key exchange protocol and for negotiating a security policy.
7. A. During a security association, the client and the server will list the types of encryption of which they are capable and will choose the most secure encryption standard that they have in common.
8. A. The entity requesting a security association will request an initiator cookie.
9. A. The Certificate Management Protocol is used to establish a CA.
10. D. XML Key Management Specification (XKMS) allows services to manage PKI via XML, which is interoperable across different vendor platforms.
11. C. Secure/Multipurpose Internet Mail Extensions (S/MIME) is a secure e-mail standard. Other popular standards include Pretty Good Privacy (PGP) and OpenPGP.
12. C. SSL's well-known port is 443. SSL was developed by Netscape.

reduces false positives by trying to match the supplied biometric with the one that is associated with the supplied token. This prevents the computer from seeking a match using the entire database of biometrics. Using multiple factors is one of the best ways to ensure proper authentication and access control.

Chapter Review

Physical Security is required to maintain the security of information systems. Any person with malicious intent who gains physical access to a computer system can cause significant damage. If a person can gain physical access, almost no information security safeguard can truly protect valuable information.

You have seen how access controls can provide legitimate access while denying intruders. However, you have also seen how these systems are increasingly computer- and network-based, which can cause a separate path of attack to be generated. Physical access can be compromised through the use of information systems. As the tendency to use the IP network increases for every device in the organization, more and more inter-linked systems will require interlinked security requirements. This is the concept of *convergence*, which can apply to security as well as voice, video, and data.

Questions

1. The feature that could allow a CD to load malicious code is called what?
 - A. A false negative
 - B. A CD-Key
 - C. A MBR, or Master Boot Record
 - D. Auto-run
2. Why is water not used for fire suppression in data centers?
 - A. It would cause a flood.
 - B. Water cannot put out an electrical fire.
 - C. Water would ruin all the electronic equipment.
 - D. Building code prevents it.
3. Which one is not a unique biometric?
 - A. Fingerprint
 - B. Eye retina
 - C. Hand geometry
 - D. Shoulder-to-waist geometry
4. Why is physical security so important to good network security?
 - A. Because encryption is not involved

- B. Because physical access defeats nearly all network security measures
 - C. Because an attacker can steal biometric identities
 - D. Authentication
5. How does multiple-factor authentication improve security?
- A. By using biometrics, no other person can authenticate.
 - B. It restricts users to smaller spaces.
 - C. By using a combination of authentications, it is more difficult for someone to gain illegitimate access.
 - D. It denies access to an intruder multiple times.
6. Why is access to an Ethernet jack a risk?
- A. A special plug can be used to short out the entire network.
 - B. An attacker can use it to make a door entry card for himself.
 - C. Wireless traffic can find its way onto the local area network.
 - D. It allows access to the internal network.
7. When a biometric device has a false positive, it has done what?
- A. Generated a positive charge to the system for which compensation is required
 - B. Allowed access to a person who is not authorized
 - C. Denied access to a person who is authorized
 - D. Failed, forcing the door it controls to be propped open
8. Why does an IP-based CCTV system need to be implemented carefully?
- A. Camera resolutions are lower.
 - B. They don't record images; they just send them to web pages.
 - C. The network cables are more easily cut.
 - D. They could be remotely attacked via the network.
9. Which of the following is a very simple physical attack?
- A. Using a custom RFID transmitter to open a door
 - B. Accessing an Ethernet jack to attack the network
 - C. Outright theft of the computers
 - D. Installing a virus on the CCTV system
10. A perfect bit-by-bit copy of a drive is called what?
- A. Drive picture
 - B. Drive image
 - C. Drive copy
 - D. Drive partition

11. What about physical security makes it more acceptable to other employees?
 - A. It is more secure.
 - B. Computers are not important.
 - C. It protects the employees themselves.
 - D. It uses encryption.
12. On whom should a company perform background checks?
 - A. System administrators only
 - B. Contract personnel only
 - C. Background checks are not needed outside of the military
 - D. All individuals who have unescorted physical access to the facility
13. What is a common threat to token-based access controls?
 - A. The key
 - B. Demagnetization of the strip
 - C. A system crash
 - D. Loss or theft of the token
14. Why should security guards get cross-training in network security?
 - A. They are the eyes and ears of the corporation when it comes to security.
 - B. They are the only people in the building at night.
 - C. They are more qualified to know what a security threat is.
 - D. They have the authority to detain violators.
15. Why can a USB flash drive be a threat?
 - A. They use too much power.
 - B. They can bring malicious code past other security mechanisms.
 - C. They can be stolen.
 - D. They can be encrypted.

Answers

1. D. Auto-run allows CDs to execute code automatically.
2. C. Electronic components would be ruined by a water-based fire-suppression system.
3. D. Shoulder-to-waist geometry is not unique. All the other examples are biometrics that are unique.
4. B. Physical access to a computer system will almost always defeat any security measures put in place on the system.

5. C. Multiple-factor authentication gives an attacker several systems to overcome, making the unauthorized access of systems much more difficult.
6. D. An exposed Ethernet jack available in a public place can allow access to the internal network, typically bypassing most of the network's security systems.
7. B. A false positive means the system granted access to an unauthorized person based on a biometric being *close* to an authorized person's biometric.
8. D. Any device attached to the IP network can be attacked using a traditional IP-based attack.
9. C. The theft of a computer is a very simple attack that can be carried out surprisingly effectively. This allows an attacker to compromise the stolen machine and its data at his leisure.
10. B. A drive image is a perfect copy of a drive that can then be analyzed on another computer.
11. C. Physical security protects the people, giving them a vested interest in its support.
12. D. All unescorted people entering the facility should be background checked.
13. D. The loss or theft of the token is the most common and most serious threat to the system; anyone with a token can access the system.
14. A. Security guards are the corporation's eyes and ears and have a direct responsibility for security information.
15. B. USB drives have large storage capacities and can carry some types of malicious code past traditional virus filters.

ized users out and monitor activity. Taken together, these pieces can make a secure network that is efficient, manageable, and effective.

Questions

To further help you prepare for the Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the list of correct answers at the end of the chapter.

1. Switches operate at which layer of the OSI model?
 - A. Physical layer
 - B. Network layer
 - C. Data link layer
 - D. Application layer
2. UTP cables are terminated for Ethernet using what type of connector?
 - A. A BNC plug
 - B. An Ethernet connector
 - C. A standard phone jack connector
 - D. An RJ-45 connector
3. Coaxial cable carries how many physical channels?
 - A. Two
 - B. Four
 - C. One
 - D. None of the above
4. The purpose of a DMZ in a network is to
 - A. Provide easy connections to the Internet without an interfering firewall
 - B. Allow server farms to be divided into similar functioning entities
 - C. Provide a place to lure and capture hackers
 - D. Act as a buffer between untrusted and trusted networks
5. Network access control is associated with which of the following?
 - A. NAP
 - B. IPsec
 - C. IPv6
 - D. NAT
6. The purpose of twisting the wires in twisted-pair circuits is to
 - A. Increase speed

- B. Increase bandwidth
 - C. Reduce crosstalk
 - D. Allow easier tracing
7. The shielding in STP acts as
- A. A physical barrier strengthening the cable
 - B. A way to reduce interference
 - C. An amplifier allowing longer connections
 - D. None of the above
8. Microsoft NAP permits
- A. Restriction of connections to a restricted subnet only
 - B. Checking of a client OS patch level before a network connection is permitted
 - C. Denial of a connection based on client policy settings
 - D. All of the above
9. One of the greatest concerns addressed by physical security is preventing unauthorized connections having what intent?
- A. Sniffing
 - B. Spoofing
 - C. Data diddling
 - D. Free network access
10. SNMP is a protocol used for which of the following functions?
- A. Secure e-mail
 - B. Secure encryption of network packets
 - C. Remote access to user workstations
 - D. Remote access to network infrastructure
11. Firewalls can use which of the following in their operation?
- A. Stateful packet inspection
 - B. Port blocking to deny specific services
 - C. NAT to hide internal IP addresses
 - D. All of the above
12. SMTP is a protocol used for which of the following functions?
- A. E-mail
 - B. Secure encryption of network packets
 - C. Remote access to user workstations

- D. None of the above
- 13. Microwave communications are limited by
 - A. Speed—the maximum for microwave circuits is 1 Gbps
 - B. Cost—microwaves take a lot of energy to generate
 - C. Line of sight—microwaves don't propagate over the horizon
 - D. Lack of standard operation protocols for widespread use
- 14. USB-based flash memory is characterized by
 - A. Expensive
 - B. Low capacity
 - C. Slow access
 - D. None of the above
- 15. Mobile devices connected to networks include what?
 - A. Smart phones
 - B. Laptops
 - C. MP3 music devices
 - D. All of the above

Answers

1. C. Switches operate at layer 2, the data link layer of the OSI model.
2. D. The standard connector for UTP in an Ethernet network is the RJ-45 connector. An RJ-45 is larger than a standard phone connector.
3. C. A coaxial connector carries one wire, one physical circuit.
4. D. A DMZ based topology is designed to manage the different levels of trust between the Internet (untrusted) and the internal network (trusted).
5. A. NAP (Network Access Protection) is one form of network access control.
6. C. The twist in twisted-pair wires reduces crosstalk between wires.
7. B. The shielding on STP is for grounding and reducing interference.
8. D. Microsoft Network Access Protection (NAP) enables the checking of a system's health and other policies prior to allowing connection.
9. A. Sniffing is the greatest threat, for passwords and accounts can be captured and used later.
10. D. The Simple Network Management Protocol is used to control network devices from a central control location.
11. D. Firewalls can do all of these things.

12. A. SMTP, the Simple Mail Transfer Protocol, is used to move e-mail across a network.
13. C. Microwave energy is a line-of-sight transmission medium; hence, towers must not be spaced too far apart or the horizon will block transmissions.
14. D. USB-based flash memory is low cost, fast, and high capacity—currently 32GB.
15. D. Almost any digital memory-containing device can find its way onto a network.

Chapter Review

Many methods can be used to achieve security under remote access conditions, and the number is growing as new protocols are developed to meet the ever-increasing use of remote access. From the beginnings of Telnet, to IPv6 with built-in IPsec, the options are many, but the task is basically the same. Perform the functions of authentication, authorization, and accounting while providing message and data security from outside intervention.

Table 9-1 shows some remote access support solutions.

TCP Port Number	UDP Port Number	Keyword	Protocol
20		FTP-Data	File Transfer (Default Data)
21		FTP	File Transfer Control
22		SSH	Secure Shell Login
23		TELNET	Telnet
25		SMTP	Simple Mail Transfer
37	37	TIME	Time
49	49	TACACS+	TACACS+ login
53	53	DNS	Domain Name Server
65	65	TACACS+	TACACS+ database service
88	88	Kerberos	Kerberos
500	500	ISAKMP	ISAKMP protocol
512		rexec	
513		rlogin	UNIX rlogin
	513	rwho	UNIX Broadcast Naming Service
514		rsh	UNIX rsh and rep
	514	SYSLOG	UNIX system logs
614	614	SSHELL	SSL Shell
	1645	RADIUS	RADIUS: Historical
	1646	RADIUS	RADIUS: Historical
	1701	L2TP	L2TP
1723	1723	PPTP	PPTP
1812	1812	RADIUS	RADIUS authorization
1813	1813	RADIUS-actg	RADIUS accounting

Table 9-1 Common TCP/UDP Remote Access Networking Port Assignments

Some of the remote access solutions have a hardware component (such as L2F and RADIUS), some have software (SSH and PPTP), and some have both (VPN and IPsec), depending on the vendor's implementation and system requirements. Your choice of a remote access solution will depend on several factors, including security requirements, the type of network, the type of clients, required access methods, scalability, existing authentication mechanisms, and cost. Each system has its strengths and weaknesses, and when properly employed, each can be used effectively within its own limitations. There is no best solution at the present time, but as the Internet advances and IPv6 is adopted, IPsec will move up the list into a prime spot and provide a significant number of these required services as part of the TCP/IPv6 protocol suite.

Questions

To further help you prepare for the Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the list of correct answers at the end of the chapter.

1. PPP provides for
 - A. Network control of printers over a parallel port
 - B. Encapsulation of datagrams across serial point-to-point connections
 - C. An obsolete layer protocol from before the Internet
 - D. A service to establish VPNs across the Internet
2. Authentication is typically based upon what? (Select all that apply.)
 - A. Something a user possesses
 - B. Something a user knows
 - C. Something measured on a user, such as a fingerprint
 - D. None of the above
3. Passwords are an example of
 - A. Something you have
 - B. Something you know
 - C. A shared secret
 - D. None of the above
4. Which of these protocols is used for carrying authentication, authorization, and configuration (accounting) information between a network access server and a shared authentication server?
 - A. IPsec
 - B. VPN
 - C. SSH
 - D. RADIUS

5. On a VPN, traffic is encrypted and decrypted at
 - A. Endpoints of the tunnel only
 - B. Users' machines
 - C. Each device at each hop
 - D. The data link layer of access devices
6. What protocol is used for TACACS+?
 - A. UDP
 - B. NetBIOS
 - C. TCP
 - D. Proprietary
7. What protocol is used for RADIUS?
 - A. UDP
 - B. NetBIOS
 - C. TCP
 - D. Proprietary
8. Which protocols are natively supported by Microsoft Windows XP and Vista for use in securing remote connections?
 - A. SSH
 - B. PPTP
 - C. IPsec
 - D. RADIUS
9. What are the foundational elements of an access control system?
 - A. Passwords, permissions, cryptography
 - B. Shared secrets, authorization, authenticators
 - C. Authentication, permissions, user IDs
 - D. Identification, authorization, authentication
10. IPsec provides which options as security services?
 - A. ESP and AH
 - B. ESP and AP
 - C. EA and AP
 - D. EA and AH
11. Secure Shell uses which port to communicate?
 - A. TCP port 80
 - B. UDP port 22

- C. TCP port 22
 - D. TCP port 110
12. Elements of Kerberos include which of the following:
- A. Tickets, ticket granting server, ticket authorizing agent
 - B. Ticket granting ticket, authentication server, ticket
 - C. Services server, Kerberos realm, ticket authenticators
 - D. Client to server ticket, authentication server ticket, ticket
13. To establish an PPTP connection across a firewall, you must do which of the following?
- A. Do nothing; PPTP does not need to cross firewalls by design.
 - B. Do nothing; PPTP traffic is invisible and tunnels past firewalls.
 - C. Open a UDP port of choice and assign to PPTP.
 - D. Open TCP port 1723.
14. To establish an L2TP connection across a firewall, you must do which of the following?
- A. Do nothing; L2TP does not cross firewalls by design.
 - B. Do nothing; L2TP tunnels past firewalls.
 - C. Open a UDP port of choice and assign to L2TP.
 - D. Open UDP port 1701.
15. IPsec can provide which of the following types of protection?
- A. Context protection
 - B. Content protection
 - C. Both context and content protection
 - D. Neither context nor content protection

Answers

- 1. B. PPP supports three functions: encapsulate datagrams across serial links; establish, configure, and test links using LCP; and establish and configure different network protocols using NCP.
- 2. A, B, and C. Authentication is commonly performed with passwords, something you know; tokens, something you have; and biometrics, such as fingerprints.
- 3. B. Passwords are defined as something you know, and are not to be shared.
- 4. D. RADIUS is a protocol for performing authentication, authorization, and accounting. It involves an information exchange between a network access

server, which desires authentication of specific connections, and a shared authentication server.

5. **A.** A virtual private network (VPN) is a secure communications protocol that encrypts traffic between two endpoints of a tunnel. At each endpoint of the secure VPN tunnel, the traffic is either encrypted or decrypted, depending on whether the traffic is going into or out of the tunnel.
6. **C.** TACACS+ is TCP-based and uses port 49.
7. **A.** RADIUS has been officially assigned UDP ports 1812 for RADIUS Authentication and 1813 for RADIUS Accounting by the Internet Assigned Number Authority (IANA). However, previously, ports 1645–Authentication and 1646–Accounting were used unofficially and became the default ports assigned by many RADIUS client/server implementations of the time. The tradition of using 1645 and 1646 for backward compatibility continues to this day. For this reason, many RADIUS server implementations monitor both sets of UDP ports for RADIUS requests. Microsoft RADIUS servers default to 1812 and 1813, but Cisco devices default to the traditional 1645 and 1646 ports.
8. **B** and **C.** Both PPTP and IPsec are supported by Microsoft Windows operating systems. IPsec is more resource intensive, but also more versatile, and it allows greater flexibility in connections.
9. **D.** Access control systems need three main components: identification, authorization, and authentication.
10. **A.** IPsec utilizes Encapsulating Security Payload (ESP) and Authentication Headers (AH).
11. **C.** SSH initiates conversations over TCP port 22.
12. **B.** Kerberos works using tickets. A ticket granting ticket is one type of ticket obtained from the authentication server.
13. **D.** PPTP uses TCP port 1723 to establish communications, so this port must be open across a firewall for PPTP to function correctly.
14. **D.** L2TP uses UDP port 1701 to establish communications, so this port must be open across a firewall for L2TP to function correctly.
15. **C.** IPsec can provide both context and content protection by using both ESP and AH.

even though the data is tunneled through, IP addresses are still sent in the clear, giving an attacker information about what and where your VPN endpoint is.

Another phenomenon of wireless is borne out of its wide availability and low price. All the security measures of the wired and wireless network can be defeated by the rogue AP. Typically added by a well-intentioned employee trying to make their lives more convenient, the AP was purchased at a local retailer. When installed, it works fine, but it typically will have no security installed. Since the IT department doesn't know about it, it is an uncontrolled entry point into the network.

Occasionally an attacker gains physical access to an organization, and will install a rogue AP to maintain network access. In either case, access needs to be removed. The most common way to control rogue AP is some form of wireless scanning to ensure only legitimate wireless is in place at an organization. While complete wireless IDS systems will detect APs, this can also be done with a laptop and free software.

802.11 has enjoyed tremendous growth because of its ease of use and popularity, but that growth is threatened by many organizational rules prohibiting its use due to security measures. As you have seen here, the current state of wireless security is very poor, making attacking wireless a popular activity. With the addition of strong authentication and better encryption protocols, wireless should become both convenient and safe.

Chapter Review

Wireless is a popular protocol that has many benefits but a certain number of risks. Wireless offers local network access to anyone within range. The lack of physical control over the medium necessitates the careful configuration of the security features available. 802.11 has brought inexpensive wireless networking to homes and small businesses. Weak encryption was a problem in early versions of the standard, but current implementations perform better. 3G mobile phones allow you to carry the Internet in your pocket, but it can also allow an attacker to pickpocket your e-mails and contacts through Bluetooth.

Questions

To further help you prepare for the Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the list of correct answers at the end of the chapter.

1. What encryption method does WEP use to try to ensure confidentiality of 802.11 networks?
 - A. MD5
 - B. AES
 - C. RC4
 - D. Diffie-Hellman

2. How does WTLS ensure integrity?
 - A. Sender's address
 - B. Message authentication codes
 - C. Sequence number
 - D. Public key encryption
3. What two key lengths does WEP support?
 - A. 1024 and 2048
 - B. 104 and 40
 - C. 512 and 256
 - D. 24 and 32
4. Why does the SSID provide no real means of authentication?
 - A. It cannot be changed.
 - B. It is only 24 bits.
 - C. It is broadcast in every beacon frame.
 - D. SSID is not an authentication function.
5. The 802.1X protocol is a new protocol for Ethernet
 - A. Authentication
 - B. Speed
 - C. Wireless
 - D. Cabling
6. Why does WTLS have to support shorter key lengths?
 - A. WAP doesn't need high security.
 - B. The algorithm cannot handle longer key lengths.
 - C. Key lengths are not important to security.
 - D. WTLS has to support devices with low processor power and limited RAM.
7. Why is 802.11 wireless such a security problem?
 - A. It has too powerful a signal.
 - B. It provides access to the physical layer of Ethernet without a person needing physical access to the building.
 - C. All the programs on wireless are full of bugs that allow buffer overflows.
 - D. It draws too much power and the other servers reboot.

8. What protocol is WTLS trying to secure?
 - A. WAP
 - B. WEP
 - C. GSM
 - D. SSL
9. Why should wireless have strong two-way authentication?
 - A. Because you want to know when an attacker connects to the network.
 - B. Because wireless is especially susceptible to a man-in-the-middle attack.
 - C. Wireless needs authentication to prevent users from adding their home computers.
 - D. Two-way authentication is needed so an administrator can ask the wireless user a set of questions.
10. Why is attacking wireless networks so popular?
 - A. There are more wireless networks than wired.
 - B. They all run Windows.
 - C. It's easy.
 - D. It's more difficult and more prestigious than other network attacks.
11. How are the security parameters of WTLS chosen between two endpoints?
 - A. Only one option exists for every parameter.
 - B. The client dictates all parameters to the server.
 - C. The user codes the parameters through DTMF tones.
 - D. The WTLS handshake determines what parameters to use.
12. What is bluejacking?
 - A. Stealing a person's mobile phone
 - B. Sending an unsolicited message via Bluetooth
 - C. Breaking a WEP key
 - D. Leaving your Bluetooth in discoverable mode
13. How does 802.11n improve network speed?
 - A. Wider bandwidth
 - B. Higher frequency
 - C. Multiple in multiple out
 - D. Both A and C

14. Bluebugging can give an attacker what?
 - A. All of your contacts
 - B. The ability to send “shock” photos
 - C. Total control over a mobile phone
 - D. A virus
15. Why is it important to scan your own organization for wireless?
 - A. It can detect rogue access points.
 - B. It checks the installed encryption.
 - C. It finds vulnerable mobile phones.
 - D. It checks for wireless coverage.

Answers

1. C. WEP uses the RC4 stream cipher.
2. B. WTLS uses a message authentication code generated with a one-way hash algorithm.
3. B. WEP currently supports 104 and 40, though it is sometimes packaged as 64-bit and 128-bit encryption. The initialization vector takes up 24 bits, leaving the 40- and 104-bit key strings.
4. C. The SSID, or service set identifier, attempts to provide an authentication function, but because it is broadcast in every frame, it is trivial for an attacker to break.
5. A. Authentication; 802.1X is the new EAP framework for strong authentication over Ethernet networks.
6. D. WAP is designed to be used with small mobile devices, usually with low processor power and limited RAM, so it must support lower grade encryption.
7. B. The 802.11 protocol provides physical layer access without a person needing to have physical access to the building, thus promoting drive-by and parking lot attacks.
8. A. WTLS is an attempt to secure the Wireless Application Protocol, or WAP.
9. B. Wireless is not connected to any physical medium, making it especially vulnerable to a man-in-the-middle attack.
10. C. Attacking wireless networks is extremely popular because it’s easy—the majority of wireless networks have no security installed on them. This allows anyone to connect and have practically full access to the network.
11. D. The WTLS handshake lets both endpoints exchange capabilities, and then the parameters are agreed upon.

12. B. Bluejacking is a term used for the sending of unauthorized messages to another Bluetooth device.
13. D. The “n” protocol uses both wider bandwidth and multiple-input and multiple-output techniques to increase speed several times over the “g” protocol.
14. C. Bluebugging give an attacker total control over a mobile phone.
15. A. Scanning detects rogue access points.

that will automatically block suspicious or malicious traffic before it reaches its intended destination, and many vendors call these Intrusion Prevention Systems (IPSs).

Firewalls are security devices that protect an organization's network perimeter by filtering traffic coming into the organization based on an established policy. They can be simple packet filtering devices or can have more advanced application layer filtering capabilities. Personal software firewalls are software packages that help protect individual systems by controlling network traffic coming into and out of that individual system.

Antivirus technologies scan network traffic, e-mail, files, and removable media for malicious code. Available in software and appliance form, they provide a necessary line of defense against the massive amount of malicious code roaming the Internet.

Proxies service client requests by forwarding requests from users to other servers. Proxies can be used to help filter and manage network traffic, particularly web browsing. Proxies are often combined with a content-filtering capability that administrators can use to block access to malicious or inappropriate content. Many organizations and users also employ pop-up blockers, mechanisms that prevent the annoying ads that appear in new browser windows as you visit certain web pages.

Protocol analyzers, often called sniffers, are tools that capture and decode network traffic. Analyzers must be able to see and capture network traffic to be effective, and many switch vendors support network analysis through the use of mirroring or span ports. Network traffic can also be viewed using network taps, a device for replicating network traffic passing across a physical link.

Honeypots are specialized forms of intrusion detection that involve setting up simulated hosts and services for attackers to target. Honeypots are based on the concept of luring attackers away from legitimate systems by presenting more tempting or interesting systems that, in most cases, appear to be easy targets. By monitoring activity within the honeypot, security personnel are better able to identify potential attackers along with their tools and capabilities.

Questions

1. What are the three types of event logs generated by Windows NT and 2000 systems?
 - A. Event, Process, and Security
 - B. Application, User, and Security
 - C. User, Event, and Security
 - D. Application, System, and Security
2. What are the two main types of intrusion detection systems?
 - A. Network-based and host-based
 - B. Signature-based and event-based
 - C. Active and reactive
 - D. Intelligent and passive

3. The first commercial, network-based IDS product was
 - A. Stalker
 - B. NetRanger
 - C. IDES
 - D. RealSecure
4. What are the two main types of IDS signatures?
 - A. Network-based and file-based
 - B. Context-based and content-based
 - C. Active and reactive
 - D. None of the above
5. A passive, host-based IDS
 - A. Runs on the local system
 - B. Does not interact with the traffic around it
 - C. Can look at system event and error logs
 - D. All of the above
6. Which of the following is *not* a capability of network-based IDS?
 - A. Can detect denial-of-service attacks
 - B. Can decrypt and read encrypted traffic
 - C. Can decode UDP and TCP packets
 - D. Can be tuned to a particular network environment
7. An active IDS can
 - A. Respond to attacks with TCP resets
 - B. Monitor for malicious activity
 - C. A and B
 - D. None of the above
8. Honeypots are used to
 - A. Attract attackers by simulating systems with open network services
 - B. Monitor network usage by employees
 - C. Process alarms from other IDSs
 - D. Attract customers to e-commerce sites
9. Egress filtering is used to detect SPAM that is
 - A. Coming into an organization
 - B. Sent from known spammers outside your organization

- C. Leaving an organization
 - D. Sent to mailing lists in your organization
10. Preventative intrusion detection systems
- A. Are cheaper
 - B. Are designed to stop malicious activity from occurring
 - C. Can only monitor activity
 - D. Were the first types of IDS
11. Which of the following is not a type of proxy?
- A. Reverse
 - B. Web
 - C. Open
 - D. Simultaneous
12. IPS stands for
- A. Intrusion processing system
 - B. Intrusion prevention sensor
 - C. Intrusion prevention system
 - D. Interactive protection system
13. A protocol analyzer can be used to
- A. Troubleshoot network problems
 - B. Collect network traffic statistics
 - C. Monitor for suspicious traffic
 - D. All of the above
14. True or False: Windows Defender is available with every version of the Windows operating system.
- A. True
 - B. False
15. Heuristic scanning looks for
- A. Normal network traffic patterns
 - B. Viruses and spam only
 - C. Firewall policy violations
 - D. Commands or instructions that are not normally found in application programs

Answers

1. **D.** The three main types of event logs generated by Windows NT and 2000 systems are Application, System, and Security.
2. **A.** The two main types of intrusion detection systems are network-based and host-based. Network-based systems monitor network connections for suspicious traffic. Host-based systems reside on an individual system and monitor that system for suspicious or malicious activity.
3. **B.** The first commercial network-based IDS product was NetRanger, released by Wheelgroup in 1995.
4. **B.** The two main types of IDS signatures are context-based and content-based. Context-based signatures examine traffic and how that traffic fits into the other traffic around it. A port scan is a good example of a context-based signature. A content-based signature looks at what is inside the traffic, such as the contents of a specific packet.
5. **D.** A passive, host-based IDS runs on the local system, cannot interfere with traffic or activity on that system, and would have access to local system logs.
6. **B.** A network-based IDS typically cannot decrypt and read encrypted traffic. This is one of the principle weaknesses of network-based intrusion detection systems.
7. **C.** An active IDS can perform all the functions of a passive IDS (monitoring, alerting, reporting, and so on) with the added ability of responding to suspected attacks with capabilities such as sending TCP reset messages to the source and destination IP addresses.
8. **A.** Honeypots are designed to attract attackers by providing what appear to be easy, inviting targets. The honeypot collects and records the activity of attackers and their tools.
9. **C.** Egress filtering is performed to detect and stop SPAM from leaving your organization. Mail is checked as it leaves your organization.
10. **B.** Preventative intrusion detection systems are designed to “prevent” malicious actions from having any impact on the targeted system or network. For example, a host-based preventative IDS may intercept an attacker's buffer overflow attempt and prevent it from executing. By stopping the attack, the IDS prevents the attacker from affecting the system.
11. **D.** Reverse, Web, and Open are all types of proxies discussed in the chapter. Simultaneous is not a type of known proxy.
12. **C.** IPS stands for intrusion prevention system.

13. **D.** A protocol analyzer is a very flexible tool and can be used for network traffic analysis, statistics collection, and monitoring and identification of suspicious or malicious traffic.
14. **B.** False. Windows Defender is available for Windows XP, Vista, Windows Server 2003, and Windows Server 2008.
15. **D.** Heuristic scanning typically looks for commands or instructions that are not normally found in application programs.

typically consists of removing samples and default materials, preventing reconnaissance attempts, and ensuring the software is patched and up to date. Group policies are a method for managing the settings and configurations of many different users and systems.

Questions

1. Which of the following steps is part of the hardening process for operating systems?
 - A. Removing unnecessary applications and utilities
 - B. Disabling unneeded services
 - C. Setting appropriate permissions on files
 - D. All of the above
2. Group policies can be applied to
 - A. Users and systems
 - B. Only to the local system
 - C. Only to users
 - D. Only to systems
3. Buffer overflow attacks are best defeated by
 - A. Removing sample files
 - B. Selecting strong passwords
 - C. Setting appropriate permissions on files
 - D. Installing the latest patches
4. Which of the following is a disciplined approach to the acquisition, testing, and implementation of operating system and application updates?
 - A. Security templates
 - B. Patch management
 - C. System hardening
 - D. System baselining
5. Traffic filtering is used to
 - A. Scan incoming web requests for malformed code
 - B. Restrict access to ports and services
 - C. Prevent buffer overflows
 - D. Optimize the flow of time-sensitive traffic
6. File permissions under UNIX consist of what three types?
 - A. Modify, read, and execute
 - B. Full control, read-only, and run

- C. Write, read, and open
 - D. Read, write, and execute
7. The **netstat** command
- A. Lists active network connections
 - B. Provides the status of all hardware interfaces
 - C. Shows open files and directories
 - D. All of the above
8. Security templates can be used to configure settings in the following areas:
- A. Restricted Groups, User Rights, and Memory Usage
 - B. User Rights, System Services, and Disk Usage
 - C. System Services, Registry Permissions, and Restricted Groups
 - D. Disk Usage, File Permissions, and Bandwidth Usage
9. The **inetd** daemon
- A. Listens for incoming connections
 - B. Starts the appropriate service when required
 - C. Runs at system startup
 - D. All of the above
10. To provide an immediate solution addressing a specific vulnerability, a vendor may release
- A. A hotfix
 - B. A service pack
 - C. A patch
 - D. None of the above
11. Network Access Quarantine Control allows administrators to
- A. Block malicious or suspicious traffic on wireless connections
 - B. Prevent computers from connecting to the network until their configuration has been reviewed and deemed "safe"
 - C. Filter out viruses, malware, and Trojans
 - D. Restrict traffic from systems using non-Microsoft operating systems
12. Password security consists of
- A. Selecting a password with at least eight characters, at least one change in case, and at least one number or nonalphanumeric character
 - B. Storing the password in your wallet or purse
 - C. Using the same password on every system
 - D. Changing passwords at least once a year

13. TCP wrappers
 - A. Verify checksums on every packet entering or leaving the system
 - B. Help prioritize network traffic for optimal throughput
 - C. Help restrict access to the local system
 - D. None of the above
14. Ensuring software is patched and up to date is important for
 - A. Operating systems
 - B. Network devices
 - C. Applications
 - D. All of the above
15. Security templates are
 - A. A collection of security settings
 - B. A method of managing patches
 - C. Application-specific security features
 - D. Available only on domain controllers

Answers

1. D. All of the steps mentioned (removing unnecessary applications, disabling unnecessary services, and setting appropriate permissions on files) are part of the hardening process. Leaving out any of these steps could result in an insecure system.
2. A. Group policies can be applied to both users and systems.
3. D. The best defense against buffer overflows is to apply the appropriate patches or fixes that eliminate the buffer overflow condition.
4. B. Patch management is a disciplined approach to the acquisition, testing, and implementation of operating system and application updates.
5. B. Traffic filtering is used to restrict access to ports and services. This helps control who has access to network services and which services they may access.
6. D. File permissions under UNIX consist of read, write, and execute.
7. A. The **netstat** (network statistics) command lists information about active network connections.
8. C. Security templates can be used to configure settings in all of the following areas: Account Policies, Event Log settings, File Permissions, Registry Permissions, Restricted Groups, System Services, and User Rights.

9. **D.** The Internet superserver daemon, `inetd`, performs all of the functions listed. This helps prevent other services from using system resources until they need to do so.
10. **A.** Immediate solutions designed to address a specific vulnerability are usually called hotfixes. Patches and service packs tend to be larger, they are released on a slower timetable, and they often contain fixes for many different problems.
11. **B.** Network Access Quarantine Control enables administrators to prevent computers from connecting to the network until their configuration has been reviewed and deemed “safe.” This capability can help prevent the spread of viruses and malware.
12. **A.** Password security consists of selecting a password with at least eight characters, at least one change in case, and at least one number or nonalphanumeric character.
13. **C.** TCP wrappers help restrict access to the local system by controlling what systems are allowed to connect to what services. This functionality is typically implemented in the `hosts.allow` and `hosts.deny` files on a specific system.
14. **D.** Ensuring software is patched and up to date is important for *every* piece of software and network equipment.
15. **A.** Security templates are a collection of security settings that can be applied to systems to increase their security posture.

tion, to DDoS attacks, which can incorporate thousands of penetrated systems in an attack on a targeted system or network.

In addition to guarding against human attackers, you must try to prevent various forms of malicious software from attacking your system. Security auditing and assessments can be used to measure an organization's current security posture. It is important that you understand the various types of attacks that could affect your organization to plan how you will address them, should they occur.

Questions

To further help you prepare for the Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the list of correct answers at the end of the chapter.

1. A SYN flood is an example of what type of attack?
 - A. Malicious code
 - B. Denial-of-service
 - C. Man-in-the-middle
 - D. Spoofing
2. An attack in which the attacker simply listens for all traffic being transmitted across a network, in the hope of viewing something such as a user ID and password combination, is known as
 - A. A man-in-the-middle attack
 - B. A denial-of service-attack
 - C. A sniffing attack
 - D. A backdoor attack
3. Which attack takes advantage of a trusted relationship that exists between two systems?
 - A. Spoofing
 - B. Password guessing
 - C. Sniffing
 - D. Brute-force
4. In what type of attack does an attacker resend the series of commands and codes used in a financial transaction to cause the transaction to be conducted multiple times?
 - A. Spoofing
 - B. Man-in-the-middle
 - C. Replay
 - D. Backdoor

5. The trick in both spoofing and TCP/IP hijacking is in trying to
 - A. Provide the correct authentication token.
 - B. Find two systems between which a trusted relationship exists.
 - C. Guess a password or brute-force a password to gain initial access to the system or network.
 - D. Maintain the correct sequence numbers for the response packets.
6. Rootkits are challenging security problems because
 - A. They can be invisible to the operating system and end user.
 - B. Their true functionality can be cloaked, preventing analysis.
 - C. They can do virtually anything an operating system can do.
 - D. All of the above.
7. The ability of an attacker to crack passwords is directly related to the method the user employed to create the password in the first place, as well as
 - A. The length of the password
 - B. The size of the character set used in generating the password
 - C. The speed of the machine cracking the password
 - D. The dictionary and rules used by the cracking program
8. A piece of malicious code that must attach itself to another file to replicate itself is known as
 - A. A worm
 - B. A virus
 - C. A logic bomb
 - D. A Trojan
9. A piece of malicious code that appears to be designed to do one thing (and may in fact do that thing) but that hides some other payload (often malicious) is known as
 - A. A worm
 - B. A virus
 - C. A logic bomb
 - D. A Trojan
10. An attack in which an attacker attempts to lie and misrepresent himself in order to gain access to information that can be useful in an attack is known as
 - A. Social science
 - B. White-hat hacking
 - C. Social engineering
 - D. Social manipulation

11. The first step in an attack on a computer system consists of
 - A. Gathering as much information about the target system as possible
 - B. Obtaining as much information about the organization in which the target lies as possible
 - C. Searching for possible exploits that can be used against known vulnerabilities
 - D. Searching for specific vulnerabilities that may exist in the target's operating system or software applications
12. The best way to minimize possible avenues of attack for your system is to
 - A. Install a firewall and check the logs daily.
 - B. Monitor your intrusion detection system for possible attacks.
 - C. Limit the information that can be obtained on your organization and the services that are run by your Internet-visible systems.
 - D. Ensure that all patches have been applied for the services that are offered by your system.
13. A war-driving attack is an attempt to exploit what technology?
 - A. Fiber-optic networks whose cables often run along roads and bridges
 - B. Cellular telephones
 - C. The public switched telephone network (PSTN)
 - D. Wireless networks
14. How can you protect against worms of the type that Robert Morris unleashed on the Internet?
 - A. Follow the same procedures you'd use to secure your system from a human attacker.
 - B. Install antivirus software.
 - C. Ensure that no executable attachments to e-mails are executed unless their integrity has been verified.
 - D. Monitor for changes to utilities and other system software.
15. Malicious code that is set to execute its payload on a specific date or at a specific time is known as
 - A. A logic bomb
 - B. A Trojan horse
 - C. A virus
 - D. A time bomb

Answers

1. B. A SYN flood attack involves launching a large number of SYN packets at a system. In TCP, the response to this is a SYN/ACK, and the system then waits for an ACK to complete the three-way handshake. If no ACK is received, the system will wait until a time-out occurs, and then it will release the connection. If enough SYN packets are received (requesting that communication be set up) the system can fill up and not process any more requests. This is a type of DoS attack.
2. C. Sniffing consists of a person simply listening to all traffic on a network. It takes advantage of the friendly nature of the network, in which systems are only supposed to grab and examine packets that are destined to them. Sniffing looks at all packets traveling across the network.
3. A. One form of spoofing attack attempts to take advantage of the trusted relationship that may exist between two systems. This trusted relationship could mean that users on one system will not be required to authenticate themselves when accessing the other system; the second system trusts the first to have performed any necessary authentication. If packets are formed that claim to have come from one of the trusted systems, the target can be fooled into performing actions as if an authorized user had sent them.
4. C. This is the description of a replay attack.
5. D. Getting the correct sequence number is the tricky part of any attempt to spoof or take over a session. This is made easy if the attacker can observe (sniff) the network traffic. If, however, the attacker is external to the network, the task is much more complicated.
6. D. Rootkits have almost unlimited power over an infected system. They can cloak themselves from detection and hide their true nature.
7. D. This is a tricky question. All of the answers have a bearing on the ability of the attacker to crack the password, but, as discussed in the text, the dictionary and rule set used will make or break the attempt (unless an attacker *wants* to try a brute-force attack, which is generally his last option). The size of the password will certainly have a bearing, but the difference between brute-forcing a 13-character password and a 14-character password is not important—neither will be accomplished in the lifetime of the attacker. The same can be said of the size of the character set used to generate the password. The more characters that are available, the larger the number of passwords that must be tried in order to brute-force it—but attackers try to stay away from using brute-force attacks. The speed of the machine will have some bearing, but speed will make little difference if the attacker uses a brute-force attack, since he still won't crack it in time to take advantage of it. If the

- attacker can pick a good dictionary and rule set, he can probably crack the password (remember that users have a tendency to select poor passwords).
8. **B.** This answer defines a virus. This is the distinguishing aspect of a virus that separates it from other forms of malicious code, especially worms.
 9. **D.** This describes a Trojan (or Trojan horse). A virus that is attached to another file and that appears to be that file may also hide a malicious payload, but the description provided is traditionally used to describe a Trojan.
 10. **C.** This is a description of social engineering. The term *white-hat hacking* is often used to refer to authorized penetration tests on a network.
 11. **B.** The first step is generally acknowledged to be to gather as much information about the organization as possible. This information can then be used in social engineering attacks that can result in the revelation of even more information, or even access to the system. If access can be obtained without having to run any exploits, the attacker's chance of discovery is minimized. The second step is to gather information about the specific systems and networks—details on the actual hardware and software that is being used. It is not until both of these steps have been accomplished that possible vulnerabilities and tools to exploit them can be determined. This sequence may differ if the attacker is not targeting a specific system, but is instead looking for systems that are vulnerable to a specific exploit. In this case, the attacker would probably be searching for a vulnerability first, and then for a tool that exploits it, and he may never even consider the organization that is being targeted.
 12. **C.** To minimize the avenues of attack, you need to limit the information that can be obtained and the number of services you offer. The more services that are available, the greater the number of possible avenues that can be exploited. It is important to install patches, but this doesn't minimize the avenues; it protects specific avenues from attack. The use of firewalls and intrusion detection systems is important, but monitoring them doesn't aid in minimizing the avenues of attack (though a properly administered firewall can help to limit the exposure of your network).
 13. **D.** War-driving is an attempt to locate wireless networks whose access area extends into publicly accessible space.
 14. **A.** The Morris worm used the same type of techniques to penetrate the systems that human attackers use. Therefore, if you protect the system against one, you are protecting it against the other. Installing an antivirus package and not allowing executable attachments to e-mail to be executed are good ideas, but they address the other type of worm, not the Morris type of Internet worm. Monitoring the system for changes to utilities and other system software is

also a good idea, but it is reactive in nature and discovering these changes means the individual or worm has already penetrated your system. Your goal should be to try to prevent this in the first place.

15. D. This defines a time bomb. The more general term *logic bomb* is sometimes used, but this term generally refers to a piece of software that is set to execute when some specified event occurs. When that event is a date or time, we often refer to the malicious code as a time bomb.

Trillian is a third-party chat client program that works with multiple chat networks; its most significant feature is that it can encrypt the chat messages, on AIM and ICQ networks, that the client sends to the server. While this does not help with file-sharing problems, it will provide confidentiality in one direction. To protect the method of file exchange, the clients will have to be changed to integrate a virus scanner. These solutions and others should be applied widely to ensure that IM will occur securely.

Instant messaging is an application that can increase productivity by saving communication time, but it's not without risks. The protocol sends messages in plaintext and thus fails to preserve their confidentiality. It also allows for sharing of files between clients, allowing a backdoor access method for files. There are some methods to minimize security risks, but more development efforts are required before IM is ready to be implemented in a secure fashion. The best ways in which to protect yourself on an IM network are similar to those for almost all Internet applications: Avoid communication with unknown persons, avoid running any program you are unsure of, and do not write anything you wouldn't want posted with your name on it.

Chapter Review

E-mail is one of the oldest and most popular applications on the Internet. Security was not a primary concern when it was created, and many extensions to the protocol, while greatly increasing the functionality to users, have increased security problems. The MIME extensions allowed file attachments and HTML mail, which allowed the e-mail transfer of viruses and Trojan programs. E-mail software that is capable of interpreting HTML also opened the door for self-installing e-mail worms. E-mail also offers simple annoyances, such as unwanted commercial spam and the hoax e-mails that never seem to die out. Worst of all is the complete lack of privacy and weak authentication inherent in e-mail. S/MIME and PGP attempt to reduce some of the limitations of e-mail, providing privacy, integrity, and authentication. Instant messaging is a newer protocol, but it carries similar risks for malicious software. Both e-mail and IM share the weakness of being a clear text protocol subject to interception. Both protocols need to be implemented with care to maintain security.

Questions

1. What is spam?
 - A. Unsolicited commercial e-mail
 - B. A Usenet archive
 - C. A computer virus
 - D. An encryption algorithm
2. How does the Realtime Blackhole List help fight spam?
 - A. It is a universal Internet receptacle for spam.
 - B. It maintains current signatures of all available spam for download.

- C. It takes all spam and returns it to the sender.
 - D. It maintains a list of spam sources against which e-mail servers can check messages.
3. How many bits are needed in a symmetric encryption algorithm to give decent protection from brute-force attacks?
- A. 24 bits
 - B. 40 bits
 - C. 56 bits
 - D. 128 bits
4. How do some instant messaging programs cause problems for intrusion detection systems?
- A. They can scan for open ports trying to find a server.
 - B. They force the IDS to decode your conversations.
 - C. They force the IDS to shut down.
 - D. They run on Windows PCs.
5. What makes e-mail hoaxes popular enough to keep the same story floating around for years?
- A. They are written by award-winning authors.
 - B. The story prompts action on the reader's part.
 - C. The story will grant the user good luck only if he or she forwards it on.
 - D. The hoax e-mail forwards itself.
6. What is greylisting?
- A. E-mail messages are temporarily rejected so that the sender is forced to resend.
 - B. E-mail messages are run through a strong set of filters before delivery.
 - C. E-mail messages are sent through special secure servers.
 - D. E-mail is sent directly from the local host to the remote host, bypassing servers entirely.
7. Why do PGP and S/MIME need public key cryptography?
- A. Public keys are necessary to determine whether the e-mail is encrypted.
 - B. The public key is necessary to encrypt the symmetric key.
 - C. The public key unlocks the password to the e-mail.
 - D. The public key is useless and gives a false sense of privacy.
8. What symmetric encryption protocols does S/MIME support?
- A. AES and RC4

- B. IDEA and 3DES
 - C. 3DES and RC2
 - D. RC4 and IDEA
9. Why is HTML e-mail dangerous?
- A. It can't be read by some e-mail clients.
 - B. It sends the content of your e-mails to web pages.
 - C. It can allow launching of malicious code from the preview pane.
 - D. It is the only way spam can be sent.
10. What is a Trojan horse program?
- A. A program that encrypts e-mail for security
 - B. A program that appears legitimate but is actually malicious code
 - C. A program that runs only on a single computer
 - D. A program that self-compiles before it runs
11. Why is S/MIME sometimes considered unsecured?
- A. It doesn't actually encrypt the e-mail.
 - B. It can send unsigned e-mails.
 - C. It uses inferior Triple DES encryption.
 - D. It can be used with only 40-bit ciphers.
12. If they are both text protocols, why is instant messaging traffic riskier than e-mail?
- A. More viruses are coded for IM.
 - B. IM has no business purpose.
 - C. IM traffic has to travel outside of the organization to a server.
 - D. Emoticons.
13. What makes spam so popular as an advertising medium?
- A. Its low cost per impression
 - B. Its high rate of return
 - C. Its ability to canvass multiple countries
 - D. Its quality of workmanship
14. What is one of the popular Trojan horse payloads?
- A. Word processor
 - B. Web server
 - C. Remote control programs

15. What is a potential security problem with key escrow?
- A. The key gets lost.
 - B. Someone could add a key to your encryption and then distribute the key.
 - C. The key could contain a Trojan horse.
 - D. Key escrow requires 40-bit keys.

Answers

1. A. Spam is unsolicited commercial e-mail.
2. D. The Realtime Blackhole List is a list of sources known to send spam, and e-mail servers can use it to perform checks against the source of e-mail. If the source matches, often the e-mail is simply dropped from the server.
3. D. 128 bits is the current requirement to provide decent security from brute-force attacks against the key.
4. A. Some instant messaging programs can look like an internal port scan when trying to find a server, causing the IDS to alert you even when an actual attack is not occurring.
5. B. Hoax e-mails work by prompting action on the user's part. Typically the action is to forward the e-mail to everyone the reader knows, sometimes to right some moral injustice.
6. A. Greylisting is a temporary rejection of e-mail to force the remote server to resend the message. Since spammers will not follow the RFC specifications, they will not perform resending.
7. B. The public key is used to encrypt the symmetric key, which is then used to encrypt the message contents, because encrypting the entire message would take too much processing power.
8. C. S/MIME supports 3DES and RC2.
9. C. HTML e-mail can carry embedded instructions to download or run scripts that can be launched from the preview pane in some e-mail programs, without requiring that the user actively launch the attached program.
10. B. A Trojan horse program looks like a legitimate game or video but actually carries malicious code.
11. D. S/MIME currently supports a 40-bit cipher to perform the symmetric encryption, and this is considered unsecured by some, as 128 bits should be the minimum on symmetric keys.
12. C. IM protocols require the traffic travel to the hosting server, so two users in an organization are sending the traffic to an outside server and back when communicating via IM.

13. A. Spam is popular simply because of its low cost. Spam can be sent to thousands of people for less than a cent per reader.
14. C. Remote control programs, such as SubSeven and Back Orifice, are popular Trojan horse programs because they give the attacker access to all the resources of the machine.
15. B. Because key escrow involves adding an additional private key to your original private key in the encryption routine, if an attacker is able to add a key without your knowledge, he can secretly decode all your messages.

Chapter Review

This chapter covered a lot of web technologies that have been developed in response to challenges presented by the massive interconnectivity and data sharing available across the Internet and the World Wide Web. The need for an easy way to handle the complexities of encryption and decryption led to the development of the SSL protocol series and then the TLS series. This session-layer protocol allows for the addition of authentication and data integrity checking for all activities that occur at lower levels, including TCP/IP functionality. SSL/TLS provides seamless integration through SSL/TLS-aware software, alleviating the user from tedious setups and data manipulation.

The WWW has become a major forum for data exchange, and with this widespread application of computing came the need to retrieve attribute information rapidly from data stores for identifying users, resources, and other hierarchical data structures. Directory technologies were thus born from database technologies, providing methods to accomplish these narrowly defined data storage and retrieval tasks. FTP, a longtime protocol used on the Internet, continues to thrive and also has a secure form, the SSH-enabled SFTP.

One of the new possibilities enabled by the Internet's high degree of interconnectivity is downloadable application code that operates in a browser environment. Developers are using web browsers as user interfaces. Standard functionality and user familiarity make web browsers a good choice for many application interfaces. To enable this extensible use, browsers are now designed to be extended via plug-ins and scripting functions. These extensions offer much in the way of functionality and also introduce new levels of security concerns. Java applets, JavaScript, and ActiveX technologies are some of the examples of new methods that enable developers to write browser-based applications. For more complex work, server-side implementations also exist, such as CGI and server-side scripts.

Cookies aren't just for snacking anymore; they have spread with the Internet and act as tiny data stores on computers everywhere. These small text files are essential little pieces of code that help to maintain state between web pages and web applications, and they can significantly enhance functionality for browser-based applications. As with any technology that offers to increase functionality, cookies also introduce security concerns that need to be understood and managed appropriately.

Questions

1. A cookie is
 - A. A piece of data in a database that enhances web browser capability
 - B. A small text file used in some HTTP exchanges
 - C. A segment of script to enhance a web page
 - D. A favorite snack of web developers, so they named a program after it
2. The use of certificates in SSL is similar to
 - A. A receipt proving purchase

- B. Having a notary notarize a signature
 - C. A historical record of a program's lineage
 - D. None of the above
3. SSL can be used to secure
- A. POP3 traffic
 - B. HTTP traffic
 - C. SMTP traffic
 - D. All of the above
4. SFTP uses which method to secure its transmissions?
- A. IPsec
 - B. VPN
 - C. SSH
 - D. SSL
5. Security for JavaScript is established by whom?
- A. The developer at the time of code development.
 - B. The user at the time of code usage.
 - C. The user through browser preferences.
 - D. Security for JavaScript is not necessary—the Java language is secure by design.
6. ActiveX can be used for which of the following purposes?
- A. Add functionality to a browser
 - B. Update the operating system
 - C. Both A and B
 - D. Neither A nor B
7. CGI has a weakness in its implementation because
- A. It offers almost unlimited operating system access and functionality on a UNIX box.
 - B. It is limited to Windows operating systems only.
 - C. It is difficult to program in.
 - D. It has a proprietary interface.
8. The keyword **[secure]** in a cookie
- A. Causes the system to encrypt its contents
 - B. Prevents it from passing over HTTP connections
 - C. Tells the browser that the cookie is a security upgrade
 - D. None of the above

9. Code signing is used to
 - A. Allow authors to take artistic credit for their hard work
 - B. Provide a method to demonstrate code integrity
 - C. Guarantee code functionality
 - D. Prevent copyright infringement by code copying
10. SSL provides which of the following functionality?
 - A. Data integrity services
 - B. Authentication services
 - C. Data confidentiality services
 - D. All of the above
11. SSL uses which port to carry HTTPS traffic?
 - A. TCP port 80
 - B. UDP port 443
 - C. TCP port 443
 - D. TCP port 8080
12. High security browsers can use what to validate SSL credentials for a user?
 - A. AES encrypted links to a root server
 - B. An extended validation SSL certificate
 - C. MD-5 hashing to ensure integrity
 - D. SSL v. 3.0
13. To establish an SSL connection for e-mail and HTTP across a firewall, you must
 - A. Open TCP ports 80, 25, 443, and 223
 - B. Open TCP ports 443, 465, and 995
 - C. Open a TCP port of choice and assign it to all SSL traffic
 - D. Do nothing; SSL tunnels past firewalls
14. Directories are characterized by
 - A. Being optimized for read-only data
 - B. Being optimized for attribute type data
 - C. More functionality than a simple database
 - D. Better security model than a database
15. To prevent the use of cookies in a browser, a user must
 - A. Tell the browser to disable cookies via a setup option.
 - B. Delete all existing cookies.

- C. All of the above.
- D. The user need do nothing—by design, cookies are necessary and cannot be totally disabled.

Answers

1. B. Cookies are small pieces of ASCII text used in HTTP transfers to exchange data between client and server.
2. B. A certificate acts as an electronic notary, providing a method of determining authenticity through a third party.
3. D. SSL can be used to secure all of the above—SPOP3 is POP3 secured, HTTPS is secure HTTP, and SSMTP is secure SMTP.
4. C. SFTP uses SSH to enable secure file transfers.
5. C. JavaScript security is ultimately the responsibility of the end user, and the options exist in browsers to select various security levels or even disable it altogether.
6. C. ActiveX can be used to create all kinds of software and modifications to existing software. ActiveX is technology that can be used to create complex application logic that is then embedded into other container objects such as a web browser.
7. A. Unlimited access to operating system functionality makes many CGI scripts security hazards to the system, and special care is required in their design and implementation.
8. B. Cookies with the [secure] tag are only passed by browsers over HTTPS connections.
9. B. Code signing includes data integrity checking through a hash value.
10. D. SSL provides all of the above.
11. C. HTTPS traffic is connection oriented (TCP) and carried over port 443 by default.
12. B. Extended validation SSL certificate is signed by the CA to prove authenticity.
13. B. HTTP uses 443, SSMTP uses 465, and SPOP3 uses 995.
14. B. Directories are used primarily for reading attribute type data to support fast lookups and searches.
15. C. The user must do both A and B. A will prevent future cookies from interacting, but B is necessary to stop cookies already downloaded from being passed back to the server on subsequent visits.

such as the periodic creation of system backups, the use of RAID technology, and areas where redundant products or services should be considered.

Questions

1. A business impact assessment is designed to do which of the following?
 - A. Determine the impact your business has on other organizations.
 - B. Determine the impact your business has on local, regional, and national economies.
 - C. Determine the effect your corporate security strategy has on the way you conduct your operations.
 - D. Determine which processes, systems, and people are critical to the operation of your organization.
2. A good backup plan will include which of the following?
 - A. The critical data needed for the organization to operate
 - B. Any software that is required to process the organization's data
 - C. Specific hardware to run the software or to process the data
 - D. All of the above
3. Which backup strategy backs up only the files and software that have changed since the last full backup?
 - A. Full
 - B. Differential
 - C. Incremental
 - D. Delta
4. Which of the following is *not* a consideration in calculating the cost of a backup strategy?
 - A. The cost of the backup media
 - B. The storage costs for the backup media
 - C. The probability that the backup will be needed
 - D. The frequency with which backups are created
5. Which of the following is the name for a fully configured environment similar to the normal operating environment that can be operational immediately to within a few hours?
 - A. Hot site
 - B. Warm site
 - C. Online storage system
 - D. Backup storage facility

6. Which of the following is considered an issue with long-term storage of magnetic media, as discussed in the chapter?
 - A. Tape media can be used a limited number of times before it degrades.
 - B. Software and hardware evolve, and the media stored may no longer be compatible with current technology.
 - C. Both of the above.
 - D. None of the above.
7. Which of the following is the best approach to take for potential short-term loss of electrical power?
 - A. Don't worry about it. If it is short term, the systems will be back up in at most a few minutes, and processing can resume.
 - B. Install an uninterruptible power supply (UPS) to allow processing to continue while you wait for power to be restored. If it will take longer than a few minutes, the supply will allow you to gracefully bring the system down so no loss of information is suffered.
 - C. Install a backup power generator and maintain a supply of fuel for it.
 - D. Have the power company install a backup power line into your facility.
8. What other common utility is it important to consider when developing your recovery plans?
 - A. Water
 - B. Gas
 - C. Communications
 - D. Television/cable
9. RAID stands for
 - A. Replacement Array of Identical Disks
 - B. Replacement Array of Inexpensive Disks
 - C. Redundant Array of Identical Devices
 - D. Redundant Array of Inexpensive Disks
10. Which RAID technique uses an array of identical disks with all data copied to each of the disks?
 - A. RAID 0
 - B. RAID 1
 - C. RAID 4
 - D. RAID 5

11. Which of the following is a reason to maintain a supply of spare parts (hardware and software)?
 - A. Products fail but newer versions may not be compatible with older versions.
 - B. Buying multiple copies of products will reduce the overall cost.
 - C. Insurance companies that provide insurance against data loss require it.
 - D. In the case of a security incident, law enforcement agencies can seize your original equipment so you'll need to have extra copies to maintain business continuity.
12. Developing a DRP, BCP, and backup policy is just one step in preparing for a disaster. What other step needs to be taken?
 - A. Once developed, the plans should be exercised to make sure that they are complete and that all individuals know their responsibilities.
 - B. The plans need to be provided to the organization's insurance provider to ensure that they are sufficient to cover the needs of the organization.
 - C. The plans should be published on the Internet to share with others who can learn from the organization's experience.
 - D. An independent contractor should be consulted to ensure that the plans are complete and adequate.

Answers

1. **D.** This is the description of what a business impact assessment is supposed to accomplish. It is important to emphasize that the BIA not only includes the systems (hardware and software) needed by the organization, but any supplies or specific individuals that are critical for the operation of the organization.
2. **D.** All of these are important. Having copies of your data will not be useful if specialized software is required to process it and if specialized hardware is needed to run the special software. You must consider all of these in your backup plan.
3. **B.** This is the definition of a differential backup. In an incremental backup, the data and software that has changed since the last full or incremental backup is saved. A delta backup saves only those portions of the files that have changed, instead of the entire file.
4. **C.** This was a tricky question. The probability that the backup will be needed is a factor in determining the optimal backup frequency, but it was not discussed as part of the cost of the backup strategy. It is also a figure that can be used in a risk analysis to determine the optimum strategy.

5. A. This is the definition of a hot site.
6. C. Both A and B were identified as issues that must be considered when planning your long-term storage strategy.
7. B. Purchasing and using a UPS is the best strategy to address short-term power loss. It allows for continued operation if the loss is brief or lets you bring the system down without loss of data. Generators are expensive to purchase and maintain and are not appropriate for short-term power loss. They may be essential for long-term loss of power in installations where this is likely and processing is critical. Ignoring the issue (answer A) is not a good approach as even a brief loss in power can disrupt processing and cause loss of data. Installing a second power line is also not a reasonable answer.
8. C. Communications (whether telephone or wireless) is critical for organizations today. Water and gas may be important, especially for long-term utility interruption, but they are generally not considered as important as communications, where even a short-term loss can be disastrous. While loss of television or cable may result in you missing your favorite show, it generally is not considered as crucial to business (unless the cable also supplies your Internet connectivity and is relied on for business operations).
9. D. This is the original definition for this acronym, but Redundant Array of Independent Disks is also now used.
10. B. This is the description for RAID 1. This technique is more expensive than other techniques as the total capacity for the entire RAID implementation is the capacity of a single disk.
11. A. Older equipment and software may not be compatible with newer versions, which could mean that business continuity is lost if a product fails. Having spare parts enables you to bring systems back up more quickly without problems associated with compatibility issues.
12. A. This is the best answer. Every plan should be tested to ensure that it is complete and so that key individuals in the plan know their parts and can accomplish assigned tasks. Exercising a plan can also identify items that are required in the event of a disaster but that are not required during normal business operations. The other answers may all have elements that could be partially correct but are not the best answer. Insurance companies may indeed want to know that the organization has a BCP, DRP, and backup plan, but this is not the best answer. Sharing information between organizations certainly is a practice that can help raise the level of preparedness across an industry, but sharing specifics about your plan is not advisable and could lead to a security breach. Contractors might be able to help develop a plan and can provide valuable assistance, but they are not required in the process if your organization has sufficient expertise.

Interrelationship digraphs A method for identifying cause-and-effect relationships by clearly defining the problem to be solved, identifying the key elements of the problem, and then describing the relationships between each of the key elements.

Pareto charts A histogram that ranks the categories in a chart from most frequent to least frequent, thus facilitating risk prioritization.

PERT (program evaluation and review technique) charts A diagram depicting interdependencies between project activities, showing the sequence and duration of each activity. When complete, the chart shows the time necessary to complete the project and the activities that determine that time (the critical path). The earliest and latest start and stop times for each activity and available slack times can also be shown.

Risk management plan A comprehensive plan documenting how risks will be managed on a given project. It contains processes, activities, milestones, organizations, responsibilities, and details of each major risk management activity and how it is to be accomplished. It is an integral part of the project management plan.

Risks Really Don't Change, But They Can Be Mitigated

One final thought to keep in mind is that the risk itself doesn't really change, no matter what actions are taken to mitigate that risk. A high risk will always be a high risk. However, actions can be taken to reduce the impact of that risk if it occurs.

Chapter Review

Risk management is a key management process that must be used at every level, whether managing a project, a program, or an enterprise. Managing risk is important in keeping a business competitive and must be done by managers at all levels. Both qualitative and quantitative risk assessment approaches must be used to manage risk effectively, and a number of approaches were presented in this chapter. Understand that it is impossible to conduct a purely quantitative risk assessment, but it is possible to conduct a purely qualitative risk assessment.

Questions

1. Which of the following correctly defines qualitative risk management?
 - A. The loss resulting when a vulnerability is exploited by a threat
 - B. To reduce the likelihood of a threat occurring

- C. The process of subjectively determining the impact of an event that affects a project, program, or business
 - D. The process of objectively determining the impact of an event that affects a project, program, or business
2. Which of the following correctly defines risk?
- A. The risks still remaining after an iteration of risk management
 - B. The possibility of suffering harm or loss
 - C. The loss resulting when a vulnerability is exploited by a threat
 - D. Any circumstance or event with the potential to cause harm to an asset
3. Single loss expectancy (SLE) can best be defined by which of the following equations?
- A. $SLE = \text{asset value} * \text{exposure factor}$
 - B. $SLE = \text{annualized loss expectancy} * \text{annualized rate of occurrence}$
 - C. $SLE = \text{asset value} * \text{annualized rate of occurrence}$
 - D. $SLE = \text{annualized loss expectancy} * \text{exposure factor}$
4. Which of the following correctly defines annualized rate of occurrence?
- A. On an annualized basis, the frequency with which an event is expected to occur
 - B. How much an event is expected to cost per year
 - C. A measure of the magnitude of loss of an asset
 - D. Resources or information an organization needs to conduct its business
5. Which of the following are business risks?
- A. Business continuity management
 - B. Fraud
 - C. Contract management
 - D. Treasury management
 - E. All of the above
 - F. None of the above
6. The Basel Committee defines operational risk as which of the following?
- A. Risk of default of outstanding loans
 - B. Risk of losses due to fluctuations of market prices
 - C. The possibility of suffering harm or loss
 - D. Risk from disruption by people, systems, processes, or disasters
7. Which of the following are *not* assets?
- A. Hardware

- B. Inventory
- C. Equipment or software failure
- D. Cash
- E. All of the above
- F. None of the above

For questions 8 and 9, assume the following: The asset value of a small distribution warehouse is \$5 million, and this warehouse serves as a backup facility. Its complete destruction by a disaster would take away about 1/5 of the capability of the business. Also assume that this sort of disaster is expected to occur about once every 50 years.

8. Which of the following is the calculated single loss expectancy (SLE)?
 - A. SLE = \$25 million
 - B. SLE = \$1 million
 - C. SLE = \$2.5 million
 - D. SLE = \$5 million
9. Which of the following is the calculated annualized loss expectancy (ALE)?
 - A. ALE = \$50,000
 - B. ALE = \$20,000
 - C. ALE = \$1 million
 - D. ALE = \$50 million
10. When discussing qualitative risk assessment versus quantitative risk assessment, which of the following is true?
 - A. It is impossible to conduct a purely quantitative risk assessment, and it is impossible to conduct a purely qualitative risk assessment.
 - B. It is possible to conduct a purely quantitative risk assessment, but it is impossible to conduct a purely qualitative risk assessment.
 - C. It is possible to conduct a purely quantitative risk assessment, and it is possible to conduct a purely qualitative risk assessment.
 - D. It is impossible to conduct a purely quantitative risk assessment, but it is possible to conduct a purely qualitative risk assessment.

Answers

1. C. Qualitative risk management is the process of *subjectively* determining the impact of an event that affects a project, program, or business. A defines impact, B defines mitigation, and D defines quantitative risk assessment.
2. B. Risk is the possibility of suffering harm or loss. A defines residual risk, C defines impact, and D defines threat.

3. A. SLE is the value of the asset multiplied by the exposure factor.
4. A. Annualized rate of occurrence is defined as the frequency with which an event is expected to occur on an annual basis. Answer B defines annualized loss expectancy. Answer C defines exposure factor. Answer D defines asset.
5. E. All listed items are business risks.
6. D. The Basel Committee defines operational risk as risk from disruption by people, systems, processes, or disasters. Answer A defines credit risk. Answer B defines market risk. Answer C defines risk.
7. C. Equipment or software failure is a threat. All other answers are examples of assets.
8. B. $SLE = \text{asset value } (\$5 \text{ million}) * \text{exposure factor } (1/5) = \1 million .
9. B. $ALE = SLE (\$1 \text{ million}) * \text{annualized rate of occurrence } (1/50) = \$20,000$.
10. D. A purely quantitative risk assessment is not achievable because it is impossible to define and quantitatively measure all factors. On the other hand, a risk assessment that qualitatively evaluates risk is possible.

- **Level 3: Defined** The process is managed (as defined in level 2) but is tailored from the organization's standard set of processes, according to the organization's tailoring guidelines.
- **Level 4: Quantitatively Managed** The process is a defined process (see level 3) and uses statistical evaluation and quantitative objectives to control and manage the process.
- **Level 5: Optimizing** Key business processes are quantitatively managed (level 4) and improved by understanding root causes of variation. Improvements can be both incremental and innovative.



EXAM TIP To complete your preparations for the Security+ exam, it is recommended that you consult SEI's web site (www.sei.cmu.edu/cmmi) for specific CMMI definitions. Be sure that you understand the differences between capability levels and maturity levels as defined in CMMI.

Change management is a key process to implementing the CMMI in an organization. For example, if an organization is at CMMI level 0, it probably has no formal change management processes in place. At level 3, an organization has a defined change management process that is followed and tailored to the specific project needs. At level 5, the change management process is a routine, quantitatively evaluated part of improving software products and implementing innovative ideas. In order for an organization to effectively manage software development, operation, and maintenance, it should have effective change management processes in place.

Chapter Review

Change management is an essential management tool and control mechanism. The key concept of segregation of duties ensures that no single individual or organization possesses too much control in a process. Therefore, it helps prevent errors and fraudulent or malicious acts. The elements of change management (configuration identification, configuration control, configuration status accounting, and configuration auditing), coupled with a defined process and a change control board, will provide management with proper oversight of the software lifecycle. Once such a process and management oversight exists, the company will be able to use CMMI to move from ad hoc activities to a disciplined software management process.

Questions

1. An upgrade to a software package resulted in errors that had been corrected in the previously released upgrade. This type of problem could have been prevented by
 - A. The system administrator making the changes instead of the developer

- B. Proper change management procedures being used when changing the object code
 - C. The use of an object-oriented design approach rather than a rapid prototyping design approach
 - D. Proper change management procedures when changing the source code
2. Change management procedures are established to
- A. Ensure continuity of business operations in the event of a major disruption
 - B. Ensure that changes in business operations caused by a major disruption are properly controlled
 - C. Add structure and control to the development of software systems
 - D. Identify threats, vulnerabilities, and mitigating actions that could impact an organization
3. Which of the following is *not* a principle of separation of duties?
- A. Software development, testing, quality assurance, and production should be assigned to different individuals.
 - B. Software developers should have access to production data and source code files.
 - C. Software developers and testers should be restricted from accessing “live” production data.
 - D. The functions of creating, installing, and administering software programs should be assigned to different individuals.
4. Why should end users not be given access to program source code?
- A. It could allow an end user to implement the principle of least privilege.
 - B. It helps lessen the opportunity of exploiting software weaknesses.
 - C. It assists in ensuring an independent and objective testing environment.
 - D. It ensures testing and quality assurance perform their proper functions.
5. Configuration status accounting consists of
- A. The process of controlling changes to items that have been baselined
 - B. The process of identifying which assets need to be managed and controlled
 - C. The process of verifying that the configuration items are built and maintained properly
 - D. The procedures for tracking and maintaining data relative to each configuration item in the baseline
6. Configuration identification consists of
- A. The process of controlling changes to items that have been baselined

- B. The process of identifying which assets need to be managed and controlled
 - C. The process of verifying that the configuration items are built and maintained properly
 - D. The procedures for tracking and maintaining data relative to each configuration item in the baseline
7. Which position is responsible for moving executable code to the test/QA or production systems?
- A. System administrator
 - B. Developer
 - C. Manager
 - D. Quality assurance
8. Which computer security technology is used to ensure the integrity of executable code?
- A. Host-based intrusion detection systems
 - B. Firewalls
 - C. Gateways
 - D. Network-based intrusion detection systems
9. In the Software Engineering Institute's Capability Maturity Model Integration (CMMI), which of the following correctly defines Level 3, Defined?
- A. Statistical evaluation and quantitative objectives are used to control and manage the process.
 - B. The process satisfies process area goals but is not institutionalized.
 - C. The process is managed but is tailored from the organization's standard set of processes.
 - D. The process has a supporting infrastructure and is monitored, controlled, reviewed, and evaluated.
10. In the Software Engineering Institute's Capability Maturity Model Integration (CMMI), which of the following correctly defines Level 2, Managed?
- A. Statistical evaluation and quantitative objectives are used to control and manage the process.
 - B. Key business processes are quantitatively managed and improved by understanding root causes of variation.
 - C. The process is managed but is tailored from the organization's standard set of processes.
 - D. The process has a supporting infrastructure and is monitored, controlled, reviewed, and evaluated.

Answers

1. **D.** Reappearing errors are likely caused by a developer not using the most recent version of the source code. Answer **A** is wrong because proper segregation of duties states that the developer is responsible for changing software programs, not the system administrator. Answer **B** is wrong because the source code will be recompiled, not the object code. Answer **C** is wrong because the design approach would not have caused this problem.
2. **C.** The fundamental purpose of software change management is to add structure and control to the software development process. Answers **A** and **B** are incorrect because software change management does not apply directly to ensuring business continuity. Answer **D** is incorrect; this is the definition of risk management.
3. **B.** Programmers should not be given direct access to production data or files. All the other answers are principles of segregation of duties, as outlined in the chapter.
4. **B.** If end users have access to source code, they could possibly view, identify, and abuse errors or weaknesses in the source code. Answer **A** is incorrect because the principle of least privilege does not directly apply here. Answer **C** is incorrect because end user access to program source code is not directly related to the testing environment. Answer **D** is incorrect because end user access to program source code is not directly related to the testing and quality assurance functions.
5. **D.** Configuration status accounting consists of the procedures for tracking and maintaining data relative to each configuration item in the baseline. Answers **A**, **B**, and **C** are the definitions of configuration control, configuration identification, and configuration auditing, respectively.
6. **B.** Configuration identification consists of the process of identifying which assets need to be managed and controlled. Answers **A**, **C**, and **D** are the definitions of configuration control, configuration auditing, and configuration status accounting, respectively.
7. **A.** The system administrator should be the only person allowed to move executables. The developer modifies the source code, the manager approves moving the executable to the production system, and quality assurance tests the executables.
8. **A.** Host-based intrusion detection systems create and maintain a database of the size and content of executable modules. Firewalls filter IP traffic; gateways also filter traffic, and network-based intrusion detection systems monitor IP traffic.

9. C. Level 3, Defined means that the process is managed but is tailored from the organization's standard set of processes. Answers A, B, and D are the definitions of Level 4, Quantitatively Managed; Level 1, Performed; and Level 2, Managed, respectively.
10. D. Level 2, Managed means the process has a supporting infrastructure and is monitored, controlled, reviewed, and evaluated. Answers A, B, and C are the definitions of Level 4, Quantitatively Managed; Level 5, Optimizing; and Level 3, Defined, respectively.

Access control is a specific part of privilege management, more specifically the part that deals with user access. The four main models of access control are mandatory access control, discretionary access control, role-based access control, and rule-based access control. Mandatory access control is based on the sensitivity of the information or process itself. Discretionary access control uses file permissions and access lists to restrict access based on a user's identity or group membership. Role-based access control restricts access based on the user's assigned role or roles. Rule-based access control restricts access based on a defined set of rules established by the administrator.

The Windows operating system uses permissions and rights to control how users and groups interact with the operating system. Permissions are used to control what actions a user or group can take on a file or folder. Rights are used to control a user's or group's ability to interact with the system itself.

Questions

1. Privilege management applies to
 - A. Files, resources, and users
 - B. Users, physical locations, and resources
 - C. Users, physical locations, and processes
 - D. Applications, systems, and security
2. A user ID is
 - A. A unique identifier assigned to each user
 - B. A form of privilege management
 - C. A unique identifier given to each process
 - D. A type of system command
3. Role management is based on
 - A. The user ID
 - B. The group to which a user is assigned
 - C. A job or function
 - D. The rights associated with the root user
4. Single sign-on
 - A. Works for only one user
 - B. Requires only one user ID and password
 - C. Groups like users together
 - D. Requires the user to log in to each resource one time
5. Compared to decentralized management, centralized management
 - A. Typically requires less training and fewer resources

- B. Brings control to a central location
 - C. Is easier to audit and manage
 - D. All of the above
6. Records showing which users accessed a computer system and what actions they performed are called
- A. User rights
 - B. System and event logs
 - C. Audit trails
 - D. Permissions
7. Minimum password age is
- A. The number of days a password must be used before it can be changed
 - B. The number of days a password can be used
 - C. The number of days before the password becomes inactive
 - D. The number of days before a password must be changed
8. The three types of auditing are
- A. Privilege, usage, and escalation
 - B. User, system, and application
 - C. File, process, and media
 - D. None of the above
9. In the context of privilege management, MAC stands for
- A. Media access control
 - B. Monetary audit control
 - C. Mandatory access control
 - D. None of the above
10. Under discretionary access control,
- A. File access is controlled by permissions.
 - B. Owners can change permissions of their own files.
 - C. File permissions may consist of owner, group, and world.
 - D. All of the above.
11. In role-based access control
- A. Resources are assigned to individual user IDs
 - B. Access is granted based on job function
 - C. Files are labeled with sensitivity levels
 - D. Users are divided into groups

12. A domain password policy
 - A. Tells users how to safeguard their passwords
 - B. Specifies the minimum length of a password
 - C. Determines when passwords should be used
 - D. Controls access to resources based on time of day

Answers

1. A. Privilege management is the process of restricting a user's ability to interact with the computer system, including files and resources.
2. A. A user ID is a unique identifier assigned to each user of a computer system. It allows the system to distinguish one user from another as well as determine what information, applications, and resources a particular user can access.
3. C. Role management is based on jobs and functions, not specific groups or users.
4. B. Single sign-on requires only one user ID and password. The user logs on to the SSO server once, and the SSO server then performs any additional authentication tasks for the user.
5. D. When compared to decentralized management, centralized management typically requires less training and fewer resources, brings control to a central location, and is easier to audit and manage.
6. C. Records showing which users accessed a computer system and what actions they performed are called audit trails.
7. A. Minimum password age is the number of days that must pass before a password can be changed.
8. A. The three main types of auditing discussed were privilege, usage, and escalation.
9. C. MAC stands for mandatory access control, which is the process of controlling access to information based on the sensitivity of that information and whether or not the user is operating at the appropriate sensitivity level and has the authority to access that information.
10. D. Under discretionary access control, file access is controlled by permissions. Owners can change their files' permissions when they want to, and file permissions in UNIX operating systems consist of different privileges for owner, group, and world.
11. B. In role-based access control, access to files and resources is usually assigned by job function. For example, a person with a "backup operator" role would be assigned the rights and privileges needed to perform that function.
12. B. A domain password policy specifies the minimum length of a password. Answers A and C should be part of the organizational password policy.

only assist the reader during Security+ exam preparations but will also help in the discovery of potential violations of laws or corporate policies.

Questions

1. Which of the following correctly defines evidence as being sufficient?
 - A. The evidence is material to the case or has a bearing to the matter at hand.
 - B. The evidence is presented in the form of business records, printouts, and so on.
 - C. The evidence is convincing or measures up without question.
 - D. The evidence is legally qualified and reliable.
2. Which of the following correctly defines direct evidence?
 - A. The knowledge of the facts is obtained through the five senses of the witness.
 - B. The evidence consists of tangible objects that prove or disprove a fact.
 - C. The evidence is used to aid the jury and may be in the form of a model, experiment, chart, or the like, offered to prove an event occurred.
 - D. It is physical evidence that links the suspect to the scene of a crime.
3. Which of the following correctly defines demonstrative evidence?
 - A. The evidence is legally qualified and reliable.
 - B. The evidence consists of tangible objects that prove or disprove a fact.
 - C. The evidence is used to aid the jury and may be in the form of a model, experiment, chart, or the like, offered to prove an event occurred.
 - D. The evidence is in the form of business records, printouts, manuals, and so on.
4. Which of the following correctly defines the best evidence rule?
 - A. The evidence is legally qualified and reliable.
 - B. Courts prefer original evidence rather than a copy to ensure that no alteration of the evidence (intentional or unintentional) has occurred.
 - C. The evidence is used to aid the jury and may be in the form of a model, experiment, chart, or the like, offered to prove an event occurred.
 - D. Physical evidence that links the suspect to the scene of a crime.
5. Which of the following correctly defines the exclusionary rule?
 - A. The knowledge of the facts is obtained through the five senses of the witness.
 - B. The evidence consists of tangible objects that prove or disprove a fact.

- C. The evidence is used to aid the jury and may be in the form of a model, experiment, chart, or the like, offered to prove an event occurred.
 - D. Any evidence collected in violation of the Fourth Amendment is not admissible as evidence.
6. Which of the following is the *most* rigorous investigative method?
- A. Build a new system that completely images the suspect system.
 - B. Verify software on the suspect system and use that software for investigation.
 - C. Examine the suspect system using its software without verification.
 - D. Use a dedicated forensic workstation.
7. Which of the following correctly defines slack space?
- A. The space on a disk drive that is occupied by the boot sector
 - B. The space located at the beginning of a partition
 - C. The remaining clusters of a previously allocated file that are available for the operating system to use
 - D. The unused space on a disk drive when a file is smaller than the allocated unit of storage (such as a cluster)
8. Which of the following correctly defines the process of acquiring evidence?
- A. Dump the memory, power down the system, create an image of the system, and analyze the image.
 - B. Power down the system, dump the memory, create an image of the system, and analyze the image.
 - C. Create an image of the system, analyze the image, dump the memory, and power down the system.
 - D. Dump the memory, analyze the image, power down the system, and create an image of the system.
9. If you are investigating a computer incident, and you need to remove the disk drive from a computer and replace it with a copy so the user doesn't know it has been exchanged, how many copies of the disk should you make, and how should they be used?
- A. Three copies: One to replace the drive removed, one to be used for file authentication, and one for analysis.
 - B. Four copies: One to replace the drive removed; one is marked, sealed, logged, and stored with the original, unmodified disk as evidence; one is for file authentication; and one is for analysis.
 - C. Five copies: One to replace the drive removed; one is marked, sealed, logged, and stored with the original, unmodified disk as evidence; one is

for file authentication; one is for analysis; and one is for holding message digests.

D. Four copies: One to replace the drive removed; one is marked, sealed, logged, and stored with the original, unmodified disk as evidence; one is for file authentication; and one is for holding message digests.

10. Which of the following correctly describes the hashing concept?
- A. A method of verifying that data has been completely deleted from a disk
 - B. A method of overwriting data with a specified pattern of 1s and 0s on a disk
 - C. An algorithm that applies mathematical operations to a data stream to calculate a unique number based on the information contained in the data stream
 - D. A method used to keep an index of all files on a disk

Answers

1. C is the correct definition. Answer A defines relevant evidence. Answer B defines documentary evidence. Answer D defines competent evidence.
2. A is the correct definition. Answer B defines real evidence. Answer C defines demonstrative evidence. Answer D defines real evidence.
3. C is the correct definition. Answer A defines competent evidence. Answer B defines real evidence. Answer D defines documentary evidence.
4. B is the correct definition. Answer A defines competent evidence. Answer C defines demonstrative evidence. Answer D defines real evidence.
5. D is the correct definition. Answer A defines direct evidence. Answer B defines real evidence. Answer C defines demonstrative evidence.
6. D. Answers A and B are other methods on the rigor spectrum. Answer C is the least rigorous method.
7. D. Answers A and B are contrived definitions. Answer C defines free space.
8. A. The other answers are not in the correct order.
9. B. The other answers are contrived responses.
10. C is the correct definition. The other answers are contrived responses.

OSI Model and Internet Protocols

In this appendix, you will

- Learn about the OSI model
- Review the network protocols associated with the Internet

Networks are interconnected groups of computers and specialty hardware designed to facilitate the transmission of data from one device to another. The basic function of the network is to allow machines and devices to communicate with each other in an orderly fashion.

Networking Frameworks and Protocols

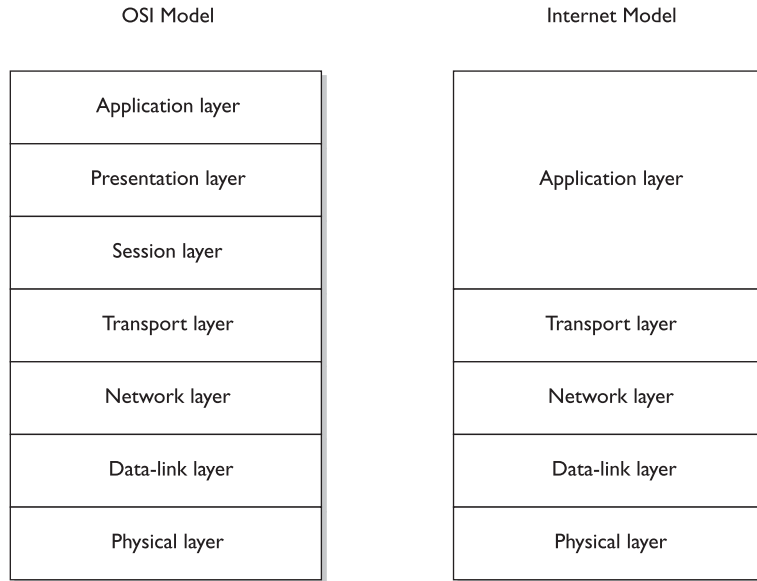
Today's networks consist of a wide variety of types and sizes of equipment from multiple vendors. To ensure an effective and efficient transfer of information between devices, agreements as to how the transfer should proceed between vendors are required.

The term *protocol* refers to a standard set of rules developed to facilitate a specific level of functionality. In networking, a wide range of protocols have been developed, some proprietary and some public, to facilitate communication between machines. Just as speakers need a common language to communicate, or they must at least understand each other's language, computers and networks must agree on a common protocol.

Communication requires that all parties have a common understanding of the object under discussion. If the object is intangible or not present, each party needs some method of referencing items in such a way that the other party understands. A *model* is a tool used as a framework to give people common points of reference when discussing items. Mathematical models are common in science, because they give people the ability to compare answers and results. In much the same way, models are used in many disciplines to facilitate communication. Network models have been developed by many companies as ways to communicate among engineers what specific functionality is occurring when and where in a network.

As the Internet took shape, a series of protocols was needed to ensure interoperability across this universal network structure. The Transmission Control Protocol (TCP),

Figure B-1
OSI and Internet
network models



the direct communication path is shown as a bold line between the two physical layers. All data between the boxes traverses this line. The dotted lines between higher layers represent virtual connections, and the associated activities and protocols are also listed

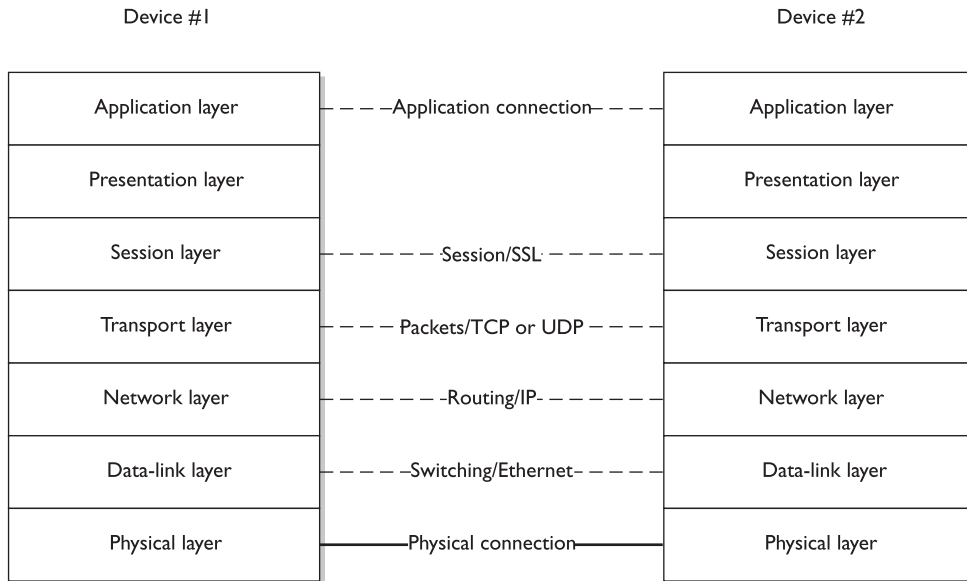


Figure B-2 Network model communication paths

for most layers (the protocols are also listed in Table B-1). These dotted lines are virtual—data does not actually cross them, although it appears as though it does. The true path of data is down to the physical layer and back up to the same layer on another machine.

Application Layer

The application layer is the typical interface to the actual application being used. This is the layer of the communication stack that is typically responsible for initiating the request for communication. For example, Internet Explorer is an application program that operates in the application layer using HTTP to move data between systems. This layer represents the user’s access to the system and the network. While it appears that the application is communicating directly with an application on another machine, this is actually a *virtual* connection. The application layer is also sometimes referred to as layer 7 in the OSI model. Several protocols are commonly found in the application layer, including Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and Simple Network Management Protocol (SNMP).

In the OSI model, the application layer actually communicates with the presentation layer only on its own machine. In the Internet model, the immediate level below the application layer is the transport layer, and this is the only layer directly called by the application layer in this model. As a result of the “missing” presentation and session layers in the Internet model, the functionality of these OSI layers is performed by the application layer.

The session layer functionality present in the Internet model’s application layer includes the initiation, maintenance, and termination of logical sessions between endpoints in the network communication. The session layer functionality also includes session level accounting and encryption services. The presentation layer functionality of the OSI model is also included in the Internet model’s application layer, specifically functionality to format the display parameters of the data being received. Any other functions not specifically included in the lower layers of the Internet model are specifically included in the application layer.

Layer	Commonly Used Protocols
Application	HTTP, SNMP, SMTP, FTP, Telnet
Presentation	XDR
Session	SSL, TLS
Transport	TCP, UCP
Network	IP, ICMP
Data-link	IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring), ARP, RARP
Physical	IEEE 802.3 (Ethernet) hardware, IEEE 802.5 (Token Ring) hardware

Table B-1 Common Protocols by OSI Layer

Presentation Layer

The presentation layer gets its name from its primary function: preparing for the presentation of data. It is responsible for preparing the data for different interfaces on different types of terminals or displays so the application does not have to deal with this task. Data compression, character set translation, and encryption are found in this layer.

The presentation layer communicates with only two layers—the application layer above it and the session layer below it. The presentation layer is also known as layer 6 of the OSI model.

Session Layer

The primary responsibility of the session layer is the managing of communication sessions between machines. The management functions include initiating, maintaining, and terminating sessions. Managing a session can be compared to making an ordinary phone call. When you dial, you initiate a session. The session must be maintained in an open state during the call. At the completion of the call, you hang up and the circuit must be terminated. As each session can have its own parameters, the session layer is responsible for setting them up, including security, encryption, and billing or accounting functions.

The session layer communicates exclusively with the presentation layer above it and the transport layer below it. The session layer is also known as layer 5 of the OSI model.

Transport Layer

The transport layer is responsible for dealing with the end-to-end transport of data across the network connection. To perform this task, the transport layer handles data entering and leaving the network through logical connections. It can add and use address-specific information, such as ports, to accomplish this task. A *port* is an address-specific extension that enables multiple simultaneous communications between machines. Should the data transmission be too large for a single-packet transport, the transport layer manages breaking up the data stream into chunks and reassembling it. It ensures that all packets are transmitted and received, and it can request lost packets and eliminate duplicate packets. Error checking can also be performed at this level, although this function is usually performed at the data-link layer.

Protocols can be either connection oriented or connectionless. If the protocol is connection oriented, the transport layer manages the connection information. In the case of TCP, the transport layer manages missing packet retransmission requests via the sliding window algorithm.

The transport layer communicates exclusively with the session layer above it and the network layer below it. The transport layer is also known as layer 4 of the OSI model.

Network Layer

The network layer is responsible for routing packets across the network. Routing functions determine the next best destination for a packet and will determine the full address of the target computer if necessary. Common protocols at this level include IP and Internet Control Message Protocol (ICMP).

The network layer communicates exclusively with the transport layer above it and the data-link layer below it. The network layer is also known as layer 3 of the OSI model.

Data-Link Layer

The data-link layer is responsible for the delivery and receipt of data from the hardware in layer 1, the physical layer. Layer 1 only manipulates a stream of bits, so the data-link layer must convert the packets from the network layer into bit streams in a form that can be understood by the physical layer. To ensure accurate transmission, the data-link layer adds end-of-message markers onto each packet and also manages error detection, correction, and retransmission functions. This layer also performs the media-access function, determining when to send and receive data based on network traffic. At this layer, the data packets are technically known as *frames*, although many practitioners use *packet* in a generic sense.

The data-link layer communicates exclusively with the network layer above it and the physical layer below it. The data-link layer is also known as layer 2 of the OSI model, and it is where LAN switching based on machine address functionality occurs.

Physical Layer

The physical layer is the realm of communication hardware and software, where 1s and 0s become waves of light, voltage levels, phase shifts, and other physical entities as defined by the particular transmission standard. This layer defines the physical method of signal transmission between machines in terms of electrical and optical characteristics. The physical layer is the point of connection to the outside world via standard connectors, again determined by signal type and protocol.

The physical layer communicates with the physical layer on other machines via wire, fiber-optics, or radio waves. The physical layer also communicates with the data-link layer above it. The physical layer is also referred to as OSI layer 1.

Internet Protocols

To facilitate cross-vendor product communication, protocols have been adopted to standardize methods. The Internet brought several new protocols into existence, a few of which are commonly used in routing of information. Two protocols used at the transport layer are TCP and UDP, whereas IP is used at the network layer. In each session, one transport layer protocol and one network layer protocol is used, making the pairs TCP/IP and UDP/IP.

TCP

TCP is the primary transport protocol used on the Internet today, accounting for more than 80 percent of packets on the Internet.

TCP begins by establishing a virtual connection through a mechanism known as the TCP *handshake*. This handshake involves three signals: a SYN signal sent to the target, a SYN/ACK returned in response, and then an ACK sent back to the target to complete the circuit. This establishes a virtual connection between machines over which the data will be transported, and that is why TCP is referred to as being *connection oriented*.

TCP is classified as a reliable protocol and will ensure that packets are sent, received, and ordered using sequence numbers. Some overhead is associated with the sequencing of packets and maintaining this order, but for many communications, this is essential, such as in e-mail transmissions, HTTP, and the like.

TCP has facilities to perform all the required functions of the transport layer. TCP has congestion- and flow-control mechanisms to report congestion and other traffic-related information back to the sender to assist in traffic-level management. Multiple TCP connections can be established between machines through a mechanism known as *ports*. TCP ports are numbered from 0 to 65,535, although ports below 1024 are typically reserved for specific functions. TCP ports are separate entities from UDP ports and can be used at the same time.

UDP

UDP is a simpler form of transport protocol than TCP. UDP performs all of the required functionality of the transport layer, but it does not perform the maintenance and checking functions of TCP. UDP does not establish a connection and does not use sequence numbers. UDP packets are sent via the “best effort” method, often referred to as “fire and forget,” because the packets either reach their destination or they are lost forever. It offers no retransmission mechanism, which is why UDP is called an unreliable protocol.

UDP does not have traffic-management or flow-control functions as TCP does. This results in much lower overhead and makes UDP ideal for streaming data sources, such as audio and video traffic, where latency between packets can be an issue. Essential services such as Dynamic Host Configuration Protocol (DHCP) and Domain Name Service (DNS) use UDP, primarily because of the low overhead. When packets do get lost, which is rare in modern networks, they can be resent.

Multiple UDP connections can be established between machines via ports. UDP ports are numbered from 0 to 65,535, although ports below 1024 are typically reserved for specific functionality. UDP ports are separate entities from TCP ports and can be used at the same time.

IP

IP is a connectionless protocol used for routing messages across the Internet. Its primary purpose is to address packets with IP addresses, both destination and source, and