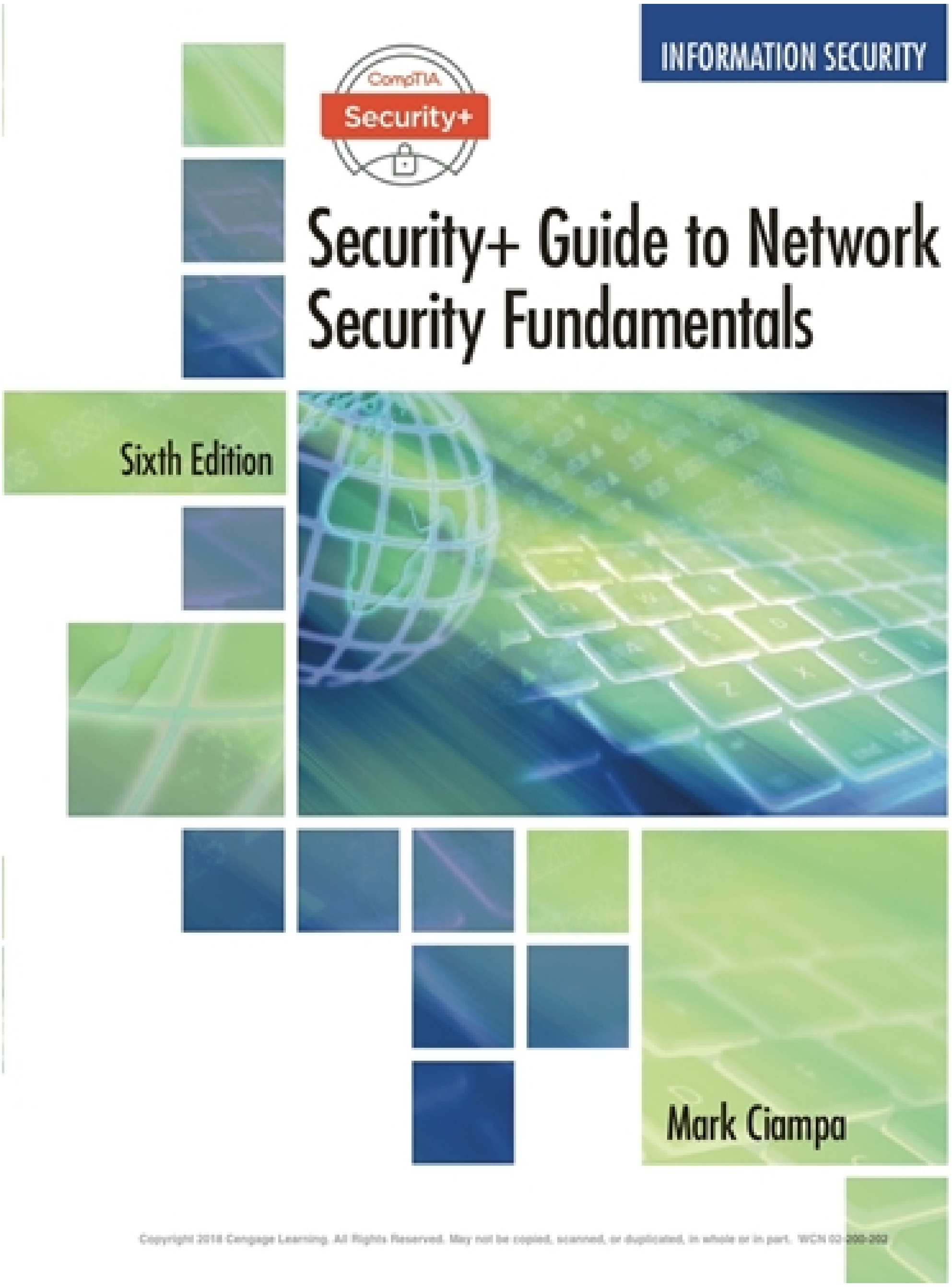
Solutions for CompTIA Security Guide to Network Security Fundamentals 6th Edition by Ciampa


INFORMATION SECURITY
CompTIA
Security+
Security+ Guide to Network Security Fundamentals
Sixth Edition
Mark Ciampa
Copyright 2018 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. WCN 02-200-202

Solutions

Ciampa, *Security+ Guide to Networking Fundamentals*, 6th ed.

9781337288781

Solutions for Review Questions

Chapter 1

1. Ian recently earned his security certification and has been offered a promotion to a position that requires him to analyze and design security solutions as well as identifying users' needs. Which of these generally recognized security positions has Ian been offered?

A. **Security administrator**

B. Security technician

C. Security officer

D. Security manager

2. Alyona has been asked by her supervisor to give a presentation regarding reasons why security attacks continue to be successful. She has decided to focus on the issue of widespread vulnerabilities. Which of the following would Alyona NOT include in her presentation?

A. Large number of vulnerabilities

B. End-of-life systems

C. Lack of vendor support

D. Misconfigurations

3. Tatyana is discussing with her supervisor potential reasons why a recent attack was successful against one of their systems. Which of the following configuration issues would NOT covered?

A. Default configurations

B. Weak configurations

C. Vulnerable business processes

D. Misconfigurations

4. What is a race condition?

A. When a vulnerability is discovered and there is a race to see if it can be patched before it is exploited by attackers.

B. **When two concurrent threads of execution access a shared resource simultaneously, resulting in unintended consequences.**

C. When an attack finishes its operation before antivirus can complete its work.

D. When a software update is distributed prior to a vulnerability being discovered.

5. Which the following is NOT a reason why it is difficult to defend against today's attackers?

A. Delays in security updating

B. Greater sophistication of defense tools

C. Increased speed of attacks

D. Simplicity of attack tools

6. Which of the following is NOT true regarding security?

A. Security is a goal.

B. Security includes the necessary steps to protect from harm.

C. Security is a process.

D. Security is a war that must be won at all costs.

7. Adone is attempting to explain to his friend the relationship between security and convenience. Which of the following statements would he use?

A. "Security and convenience are not related."

B. "Convenience always outweighs security."

C. "Security and convenience are inversely proportional."

D. "Whenever security and convenience intersect, security always wins."

8. Which of the following ensures that only authorized parties can view protected information?

A. Authorization

B. Confidentiality

C. Availability

D. Integrity

9. Which of the following is NOT a successive layer in which information security is achieved?

A. Products

B. People

C. Procedures

D. Purposes

10. Complete this definition of information security: *That which protects the integrity, confidentiality, and availability of information _____.*

A. *on electronic digital devices and limited analog devices that can connect via the Internet or through a local area network.*

B. *through a long-term process that results in ultimate security.*

C. *using both open-sourced as well as supplier-sourced hardware and software that interacts appropriately with limited resources.*

D. *through products, people, and procedures on the devices that store, manipulate, and transmit the information.*

11. Which of the following is an enterprise critical asset?

A. System software

B. Information

C. Outsourced computing services

D. Servers, routers, and power supplies

12. Gunnar is creating a document that explains risk response techniques. Which of the following would he NOT list and explain in his document?

A. Extinguish risk

B. Transfer risk

C. Mitigate risk

D. Avoid risk

13. Which act requires banks and financial institutions to alert their customers of their policies in disclosing customer information?

A. Sarbanes-Oxley Act (Sarbox)

B. Financial and Personal Services Disclosure Act

C. Health Insurance Portability and Accountability Act (HIPAA)

D. Gramm-Leach-Bliley Act (GLBA)

14. Why do cyberterrorists target power plants, air traffic control centers, and water systems?

A. These targets are government-regulated and any successful attack would be considered a major victory.

B. These targets have notoriously weak security and are easy to penetrate.

C. They can cause significant disruption by destroying only a few targets.

D. The targets are privately owned and cannot afford high levels of security.

15. Which tool is most commonly associated with nation state threat actors?

A. Closed-Source Resistant and Recurrent Malware (CSRRM)

B. **Advanced Persistent Threat (APT)**

C. Unlimited Harvest and Secure Attack (UHSA)

D. Network Spider and Worm Threat (NSAWT)

16. An organization that practices purchasing products from different vendors is demonstrating which security principle?

A. Obscurity

B. Diversity

C. Limiting

D. Layering

17. What is an objective of state-sponsored attackers?

A. To right a perceived wrong

B. To amass fortune over of fame

C. To spy on citizens

D. To sell vulnerabilities to the highest bidder

18. Signe wants to improve the security of the small business where she serves as a security manager. She determines that the business needs to do a better job of not revealing the type of computer, operating system, software, and network connections they use. What security principle does Signe want to use?

A. Obscurity

B. Layering

C. Diversity

D. Limiting

19. What are industry-standard frameworks and reference architectures that are required by external agencies known as?

A. Compulsory

B. Mandatory

C. Required

D. Regulatory

20. What is the category of threat actors that sell their knowledge of vulnerabilities to other attackers or governments?

A. Cyberterrorists

B. Competitors

C. **Brokers**

D. Resource managers

Chapter 2

21. Which of the following is not a primary trait of malware?

A. diffusion

B. circulation

C. infection

D. concealment

22. Which type of malware requires a user to transport it from one computer to another?

A. worm

B. rootkit

C. adware

D. **virus**

23. Which type of mutation completely changes a virus from its original form by rewriting its own code whenever it is executed?

A. betamorphic

B. oligomorphic

C. polymorphic

D. metamorphic

24. Ebba received a message from one of her tech support employees. In violation of company policy, a user had downloaded a free program to receive weather reports, but the program had also installed malware on the computer that gave the threat actor unrestricted access to the computer. What type of malware had been downloaded?

A. virus

B. ransomware

C. RAT

D. Trojan

25. Linnea's father called her to say that a message suddenly appeared on his screen that says his software license has expired and he must immediately pay $500 to have it renewed before control of the computer will be returned to him. What type of malware is this?

A. persistent virusware

B. Trojanware

C. **blocking ransomware**

D. lockoutware

26. Astrid's computer screen suddenly says that all files are now locked until money is transferred to a specific account, at which time she will receive a means to unlock the files. What type of malware has infected her computer?

A. Bitcoin malware

B. **Crypto-malware**

C. Blocking virus

D. Networked worm

27. What is the name of the threat actor's computer that gives instructions to an infected computer?

A. **Command and control (C&C) server**

B. Resource server

C. Regulating Net Server (RNS)

D. Monitoring and Infecting (M&I) server

28. Which of these could NOT be defined as a logic bomb?

A. If the company's stock price drops below $100, then credit Juni's account with 10 additional years of retirement credit.

B. Erase all data if Matilda's name is removed from the list of employees.

C. Reformat the hard drive three months after Sigrid left the company.

D. Send spam email to Moa's inbox on Tuesday.

29. Which of the following is NOT correct about a rootkit?

A. A rootkit is able to hide its presence or the presence of other malware.

B. A rootkit accesses "lower layers" of the operating system.

C. **A rootkit is always the payload of a Trojan.**

D. The risk of a rootkit is less today than previously.

30. Which of these is a general term used for describing software that gathers information without the user’s consent?

A. gatherware

B. adware

C. **spyware**

D. scrapeware

31. Which statement regarding a keylogger is NOT true?

A. Keyloggers can be used to capture passwords, credit card numbers, or personal information.

B. **Software keyloggers are generally easy to detect**.

C. Hardware keyloggers are installed between the keyboard connector and computer keyboard USB port.

D. Software keyloggers can be designed to send captured information automatically back to the attacker through the Internet.

32. A watering hole attack is directed against _____.

A. wealthy individuals

B. a smaller group of specific users

C. all users of a large corporation

D. attackers who send spam

33. _____ sends phishing messages only to wealthy individuals.

A. Whaling

B. Spear phishing

C. Target phishing

D. Microing

34. Lykke receives a call while working at the helpdesk from someone who needs his account reset immediately. When Lykke questions the caller, he says, “If you don’t reset my account immediately, I will call your supervisor!” What psychological approach is the caller attempting to use on Lykke?

A. Familiarity

B. Scarcity

C. Intimidation

D. Consensus

35. Hedda pretends to be the help desk manager and calls Steve to trick him into giving her his password. What social engineering attack has Hedda performed?

A. aliasing

B. duplicity

C. impersonation

D. luring

36. How can an attacker use a hoax?

A. **A hoax could convince a user that a bad Trojan is circulating and that he should change his security settings.**

B. By sending out a hoax, an attacker can convince a user to read his email more often.

C. A user who receives multiple hoaxes could contact his supervisor for help.

D. Hoaxes are not used by attackers today.

37. Which of these items retrieved through dumpster diving would NOT provide useful information?

A. calendars

B. organizational charts

C. memos

D. books

38. _____ is following an authorized person through a secure door.

A. Tagging

B. Tailgating

C. Backpacking

D. Caboosing

39. Each of these is a reason why adware is scorned EXCEPT _____.

A. it displays objectionable content

B. it displays the attacker's programming skills

C. it can interfere with a user's productivity

D. it can cause a computer to crash or slow down

40. What is the term used for a threat actor who controls multiple bots in a botnet?

A. bot herder

B. zombie shepherd

C. rogue IRC

D. cyber-robot

Chapter 3

1. <EOCMULT_first>The Hashed Message Authentication Code (HMAC) _____.

E. <EOCMULTA_first>encrypts only the message

F. <EOCMULTA>encrypts only the key

G. encrypts the key and the message

H. encrypts the DHE key only

2. What is the latest version of the Secure Hash Algorithm?

A. SHA-2

B. SHA-3

C. SHA-4

D. SHA-5

3. Alexei was given a key to a substitution cipher. The key showed that the entire alphabet was rotated 13 steps. What type of cipher is this?

A. AES

B. XAND13

C. **ROT13**

D. Alphabetic

4. Abram was asked to explain to one of his coworkers the XOR cipher. He showed his coworker an example of adding two bits, 1 and 1. What is the result of this sum?

A. 2

B. 1

C. **0**

D. 16

5. Which of the following key exchanges uses the same keys each time?

A. Diffie-Hellman-RSA (DHRSA)

B. Diffie-Hellman Ephemeral (DHE)

C. **Diffie-Hellman (DH)**

D. Elliptic Curve Diffie-Hellman (ECDH)

6. Public key systems that generate random public keys that are different for each session are called _____.

A. Public Key Exchange (PKE)

B. **perfect forward secrecy**

C. Elliptic Curve Diffie-Hellman (ECDH)

D. Diffie-Hellman (DH)

7. What is data called that is to be encrypted by inputting it into a cryptographic algorithm?

A. opentext

B. plaintext

C. cleartext

D. ciphertext

8. Which of these is NOT a basic security protection for information that cryptography can provide?

A. authenticity

B. risk loss

C. integrity

D. confidentiality

9. Which areas of a file *cannot* be used by steganography to hide data?

A. in areas that contain the content data itself

B. in the file header fields that describe the file

C. in data that is used to describe the content or structure of the actual data

D. in the directory structure of the file system

10. Proving that a user sent an email message is known as _____.

A. non-repudiation

B. repudiation

C. integrity

D. availability

11. A(n) _____ is not decrypted but is only used for comparison purposes.

A. key

B. stream

C. digest

D. algorithm

12. Which of these is NOT a characteristic of a secure hash algorithm?

A. Collisions should be rare.

B. A message cannot be produced from a predefined hash.

C. The results of a hash function should not be reversed.

D. The hash should always be the same fixed size.

13. Alyosha was explaining to a friend the importance of protecting a cryptographic key from cryptoanalysis. He said that the key should not relate in a simple way to the cipher text. Which protection is Alyosha describing?

A. diffusion

B. confusion

C. integrity

D. chaos

14. Which of these is the strongest symmetric cryptographic algorithm?

A. Data Encryption Standard

B. Triple Data Encryption Standard

C. **Advanced Encryption Standard**

D. RC 1

15. If Bob wants to send a secure message to Alice using an asymmetric cryptographic algorithm, which key does he use to encrypt the message?

A. Alice’s private key

B. Bob’s public key

C. Alice’s public key

D. Bob’s private key

16. Egor wanted to use a digital signature. Which of the following benefits will the digital signature not provide?

A. verify the sender

B. prove the integrity of the message

C. verify the receiver

D. enforce nonrepudiation

17. Illya was asked to recommend the most secure asymmetric cryptographic algorithm to his supervisor. Which of the following did he choose?

A. SHA-2

B. ME-312

C. BTC-2

D. RSA

18. At a staff meeting one of the technicians suggested that the enterprise protect its new web server by hiding it and not telling anyone where it is located. Iosif raised his hand and said that security through obscurity was a poor idea. Why did he say that?

A. It is an unproven approach and has never been tested.

B. It would be too costly to have one isolated server by itself.

C. **It would be essentially impossible to keep its location a secret from everyone**.

D. It depends too heavily upon non-repudiation in order for it to succeed.

19. What is a characteristic of the Trusted Platform Module (TPM)?

A. It provides cryptographic services in hardware instead of software

B. It allows the user to boot a corrupted disk and repair it

C. It is available only on Windows computers running BitLocker

D. It includes a pseudorandom number generator (PRNG)

20. Which of these has an onboard key generator and key storage facility, as well as accelerated symmetric and asymmetric encryption, and can back up sensitive material in encrypted form?

A. Trusted Platform Module (TPM)

B. Hardware Security Module (HSM)

C. self-encrypting hard disk drives (SED)

D. encrypted hardware-based USB devices

Chapter 4

Review Questions

1. Which of the following is NOT a method for strengthening a key?

A. Randomness

B. Cryptoperiod

C. Length

D. Variability

2. Which of the following block ciphers XORs each block of plaintext with the previous block of ciphertext before being encrypted?

A. Electronic Code Book (ECB)

B. Galois/Counter (GCM)

C. Counter (CTR)

D. **Cipher Block Chaining (CBC)**

3. What entity calls in crypto modules to perform cryptographic tasks?

A. Certificate Authority (CA)

B. OCSP Chain

C. Intermediate CA

D. **Crypto service provider**

4. ______ are symmetric keys to encrypt and decrypt information exchanged during the session and to verify its integrity.

A. Encrypted signatures

B. **Session keys**

C. Digital certificates

D. Digital digests

5. Which of these is considered the strongest cryptographic transport protocol?

A. **TLS v1.2**

B. TLS v1.0

C. SSL v2.0

D. SSL v2.0

6. The strongest technology that would assure Alice that Bob is the sender of a message is a(n) _____.

A. digital signature

B. encrypted signature

C. digest

D. **digital certificate**

7. A digital certificate associates _____.

I. a user’s public key with his private key

J. the user’s identity with his public key

K. a user’s private key with the public key

L. a private key with a digital signature

8. Digital certificates can be used for each of these EXCEPT _____.

A. to verify the authenticity of the Registration Authorizer

B. to encrypt channels to provide secure communication between clients and servers

C. to verify the identity of clients and servers on the Web

D. to encrypt messages for secure email communications

9. An entity that issues digital certificates is a _____.

E. Certificate Signatory (CS)

F. Digital Signer (DS)

G. **Certificate Authority (CA)**

H. Signature Authority (SA)

10. A centralized directory of digital certificates is called a(n) _____.

A. Digital Signature Permitted Authorization (DSPA)

B. Digital Signature Approval List (DSAP)

C. Certificate Repository (CR)

D. Authorized Digital Signature (ADS)

11. ______ performs a real-time lookup of a digital certificate’s status.

A. Certificate Revocation List (CRL)

B. Real-Time CA Verification (RTCAV)

C. **Online Certificate Status Protocol (OCSP)**

D. CA Registry Database (CARD)

12. What is a value that can be used to ensure that hashed plaintext will not consistently result in the same digest?

E. algorithm

F. initialization vector (IV)

G. nonce

H. **salt**

13. Which digital certificate displays the name of the entity behind the website?

A. Online Certificate Status Certificate

B. Extended Validation (EV) Certificate

C. Session Certificate

D. X.509 Certificate

14. Which trust model has multiple CAs, one of which acts as a facilitator?

A. **Bridge**

B. Hierarchical

C. Distributed

D. Web

15. Which statement is NOT true regarding hierarchical trust models?

A. It is designed for use on a large scale.

B. The root signs all digital certificate authorities with a single key.

C. It assigns a single hierarchy with one master CA.

D. The master CA is called the root.

16. Public key infrastructure (PKI) _____.

A. generates public/private keys automatically

B. creates private key cryptography

C. is the management of digital certificates

D. requires the use of an RA instead of a CA

17. A(n) _____ is a published set of rules that govern the operation of a PKI.

A. signature resource guide (SRG)

B. enforcement certificate (EF)

C. certificate practice statement (CPS)

D. **certificate policy (CP)**

18. Which of these is NOT part of the certificate life cycle?

A. expiration

B. revocation

C. **authorization**

D. creation

19. _____ refers to a situation in which keys are managed by a third party, such as a trusted CA.

E. Key authorization

F. Key escrow

G. Remote key administration

H. Trusted key authority

20. _____ is a protocol for securely accessing a remote computer.

E. Transport Layer Security (TLS)

F. Secure Shell (SSH)

G. Secure Sockets Layer (SSL)

H. Secure Hypertext Transport Protocol (SHTTP)

Chapter 5

Review Questions

1. Which attack intercepts communications between a web browser and the underlying computer?

A. man-in-the-middle (MITM)

B. man-in-the-browser (MITB)

C. replay

D. ARP poisoning

2. Olivia was asked to protect the system from a DNS poisoning attack. What are the locations she would need to protect?

A. Web server buffer and host DNS server

B. Reply referrer and domain buffer

C. Web browser and browser add-on

D. **Host table and external DNS server**

3. Newton is concerned that attackers could be exploiting a vulnerability in software to gain access to resources that the user normally would be restricted from accessing. What type of attack is he worried about?

A. **Privilege escalation**

B. Session replay

C. Scaling exploit

D. Amplification

4. Which of the following adds new functionality to the web browser so that users can play music, view videos, or display special graphical images within the browser?

A. Extensions

B. Scripts

C. **Plug-ins**

D. Add-ons

5. An attacker who manipulates the maximum size of an integer type would be performing what kind of attack?

A. **integer overflow**

B. buffer overflow

C. number overflow

D. heap overflow

6. What kind of attack is performed by an attacker who takes advantage of the inadvertent and unauthorized access built through three succeeding systems that all trust one another?

A. **privilege escalation**

B. cross-site attack

C. horizontal access attack

D. transverse attack

7. Which statement is correct regarding why traditional network security devices cannot be used to block web application attacks?

A. The complex nature of TCP/IP allows for too many ping sweeps to be blocked.

B. Web application attacks use web browsers that cannot be controlled on a local computer.

C. Network security devices cannot prevent attacks from web resources.

D. **Traditional network security devices ignore the content of HTTP traffic, which is the vehicle of web application attacks**.

8. What is the difference between a DoS and a DDoS attack?

A. DoS attacks are faster than DDoS attacks

B. DoS attacks use fewer computers than DDoS attacks

C. DoS attacks do not use DNS servers as DDoS attacks do

D. DoS attacks user more memory than a DDoS attack

9. John was explaining about an attack that accepts user input without validating it and uses that input in a response. What type of attack was he describing?

A. SQL

B. XSS

C. XSRF

D. DDoS DNS

10. Which attack uses the user's web browser settings to impersonate that user?

A. XDD

B. XSRF

C. Domain hijacking

D. Session hijacking

11. What is the basis of an SQL injection attack?

A. to expose SQL code so that it can be examined

B. to have the SQL server attack client web browsers

C. to insert SQL statements through unfiltered user input

D. to link SQL servers into a botnet

12. Which action cannot be performed through a successful SQL injection attack?

A. discover the names of different fields in a table

B. reformat the web application server's hard drive

C. display a list of customer telephone numbers

D. erase a database table

13. Attackers who register domain names that are similar to legitimate domain names are performing _____.

A. Address resolution

B. HTTP manipulation

C. HTML squatting

D. URL hijacking

14. What type of attack involves manipulating third-party ad networks?

A. Session advertising

B. **Malvertising**

C. Clickjacking

D. Directory traversal

15. Why are extensions, plug-ins, and add-ons considered to be security risks?

A. They are written in Java, which is a weak language.

B. **They have introduced vulnerabilities in browsers**.

C. They use bitcode.

D. They cannot be uninstalled.

16. What is a session token?

A. XML code used in an XML injection attack

B. a random string assigned by a web server

C. another name for a third-party cookie

D. a unique identifier that includes the user's email address

17. Which of these is not a DoS attack?

A. SYN flood

B. DNS amplification

C. smurf attack

D. push flood

18. What type of attack intercepts legitimate communication and forges a fictitious response to the sender?

A. SIDS

B. interceptor

C. **MITM**

D. SQL intrusion

19. A replay attack _____.

A. can be prevented by patching the web browser

B. is considered to be a type of DoS attack

C. makes a copy of the transmission for use at a later time

D. replays the attack over and over to flood the server

20. DNS poisoning _____.

A. floods a DNS server with requests until it can no longer respond

B. is rarely found today due to the use of host tables

C. **substitutes DNS addresses so that the computer is automatically redirected to another device**

D. is the same as ARP poisoning

Chapter 6

Review Questions

1. Isabella is a security support manager for a large enterprise. In a recent meeting, she was asked which of the standard networking devices already present on the network could be configured to supplement the specific network security hardware devices that were recently purchased. Which of these standard networking devices would Isabella recommend?

A. router

B. hub

C. virtual private network

D. SIEM device

2. Ximena noticed that Sofia had created a network bridge on her new laptop between the unsecured wireless network and the organization's secure intranet. Ximena explained to Sofia the problem associated with setting up the bridge. What did Ximena tell Sofia?

A. A bridge will block packets between two different types of networks.

B. A bridge cannot be used on any Internet connection.

C. A bridge would block packets from reaching the Internet.

D. **A bridge could permit access to the secure wired network from the unsecured wireless network**

3. Which of these would NOT be a filtering mechanism found in a firewall ACL rule?

A. source address

B. direction

C. date

D. protocol

4. Which of the following devices can identify the application that send packets and then make decisions about filtering based on it?

A. Internet content filter

B. **application-based firewall**

C. reverse proxy

D. web security gateway

5. Which function does an Internet content filter NOT perform?

A. **intrusion detection**

B. URL filtering

C. malware inspection

D. content inspection

6. How does network address translation (NAT) improve security?

A. It filters based on protocol.

B. **It discards unsolicited packets.**

C. It masks the IP address of the NAT device.

D. NATs do not improve security.

7. Francisco was asked by a student intern to explain the danger of a MAC flooding attack on a switch. What would Francisco say?

A. Once the MAC address table is full the switch functions like a network hub.

B. A MAC flooding attack with filter to the local host computer’s MAC-to-IP address tables and prevent these hosts from reaching the network.

C. In a defense of a MAC flooding attack network routers will freeze and not permit any incoming traffic.

D. A MAC flooding attack will prevent load balances from identifying the correct VIP of the servers.

8. Which device is easiest for an attacker to take advantage of to capture and analyze packets?

A. router

B. hub

C. switch

D. load balancer

9. Sebastian was explaining to his supervisor why the enterprise needed to implement port security. His supervisor asked what security action a flood guard could do when a MAC flooding attack occurred. Which of the following was NOT an answer that was given by Sebastian?

A. Ignore the new MAC addresses while allowing normal traffic from the single pre-approved MAC address

B. Cause the device to enter a fail-open mode.

C. Record new MAC addresses up to a specific limit

D. Block the port entirely

10. Which statement regarding a demilitarized zone (DMZ) is NOT true?

A. It can be configured to have one or two firewalls.

B. It typically includes an email or web server.

C. It provides an extra degree of security.

D. It contains servers that are used only by internal network users.

11. Which statement about network address translation (NAT) is true?

A. It substitutes MAC addresses for IP addresses.

B. It can be stateful or stateless.

C. It can be found only on core routers.

D. It removes private addresses when the packet leaves the network.

12. Which of these is NOT used in scheduling a load balancer?

A. The IP address of the destination packet

B. Data within the application message itself

C. Round-robin

D. Affinity

13. In which of the following configurations are all the load balancers always active?

A. **Active-active**

B. Active-passive

C. Passive-active-passive

D. Active-load-passive-load

14. Which device intercepts internal user requests and then processes those requests on behalf of the users?

A. Forward proxy server

B. Reverse proxy server

C. Host detection server

D. Intrusion prevention device

15. Raul was asked to configure the VPN to preserve bandwidth. Which configuration would he choose?

A. Split tunnel

B. Full tunnel

C. Narrow tunnel

D. Wide tunnel

16. Which device watches for attacks and sounds an alert only when one occurs?

A. firewall

B. network intrusion detection system (NIDS)

C. network intrusion prevention system (NIPS)

D. proxy intrusion device

17. Which of the following is a multipurpose security device?

A. Hardware security module

B. Unified Threat Management (UTM)

C. Media gateway

D. Intrusion Detection/Prevention (ID/P)

18. Which of the following CANNOT be used to hide information about the internal network?

A. network address translation (NAT)

B. a protocol analyzer

C. a subnetter

D. a proxy server

19. What is the difference between a network intrusion detection system (NIDS) and a network intrusion prevention system (NIPS)?

A. A NIDS provides more valuable information about attacks.

B. There is no difference; a NIDS and a NIPS are equal.

C. **A NIPS can take actions more quickly to combat an attack.**

D. A NIPS is much slower because it uses protocol analysis.

20. Which is the most secure type of firewall?

A. stateless packet filtering

B. stateful packet filtering

C. network intrusion detection system replay

D. reverse proxy analysis

Chapter 7

Review Questions

1. Which of the following TCP/IP protocols do not relate to security?

A. **IP**

B. SNMP

C. HTTPS

D. FTP

2. Aideen sent an email to her supervisor explaining the Domain Name System Security Extensions (DNSSEC). Which of the following statements would Aideen have NOT included in her email?

A. It is fully supported in BIND9.

B. It adds additional resource records.

C. It adds message header information.

D. **It can prevent a DNS transfer attack**.

3. What is the recommended secure protocol for voice and video applications?

A. **Secure Real-time Transport Protocol (SRTP)**

B. Hypertext Transport Protocol Secure (HTTPS)

C. Network Time Protocol (NTP)

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

4. Which type of log can provide details regarding requests for specific files on a system?

A. audit log

B. event log

C. access log

D. SysFile log

5. Which type of device log contains the most beneficial security data?

A. **firewall log**

B. email log

C. switch log

D. router log

6. Which type of cloud is offered to specific organizations that have common concerns?

A. public cloud

B. hybrid cloud

C. private cloud

D. **community cloud**

7. Which of these is NOT correct about an SSL accelerator?

A. It can be a separate hardware card that inserts into a web server

B. It can be a separate hardware module

C. It should reside between the user’s device and the web servers

D. **It can only handle the SSL protocol.**

8. Catriona needed to monitor network traffic. She did not have the resources to install an additional device on the network. Which of the following solutions would meet her needs?

A. Network tap

B. Port mirroring

C. Aggregation switch

D. Correlation engine

9. Which version of Simple Network Management Protocol (SNMP) is considered the most secure?

A. SNMPv2

B. SNMPv3

C. SNMPv4

D. SNMPv5

10. Which Domain Name System (DNS) attack replaces a fraudulent IP address for a symbolic name?

A. DNS replay

B. DNS masking

C. DNS poisoning

D. DNS forwarding

11. Which of these is the most secure protocol for transferring files?

A. FTPS

B. TCP

C. SFTP

D. FTP

12. Which of the following can be used to prevent a buffer overflow attack?

A. DEP

B. FIM

C. VPN

D. DNS

13. Which of the following is NOT a service model in cloud computing?

A. Software as a Service (SaaS)

B. **Hardware as a Service (HaaS)**

C. Platform as a Service (PaaS)

D. Infrastructure as a Service (IaaS)

14. Eachna is showing a new security intern the log file from a firewall. Which of the following entries would she tell him do not need to be investigated?

A. suspicious outbound connections

B. IP addresses that are being rejected and dropped

C. successful logins

D. IP addresses that are being rejected and dropped

15. Which type of hypervisor does not run on an underlying operating system?

A. **Type I**

B. Type II

C. Type III

D. Type IV

16. Which application stores the user's desktop inside a virtual machine that resides on a server and is accessible from multiple locations?

A. Application cell

B. Container

C. VDE

D. VDI

17. Kyle asked his supervisor which type of computing model was used when the enterprise first started. She explained that the organization purchased all the hardware and software necessary to run the company. What type of model was she describing to Kyle?

A. Virtual services

B. Off-premises

C. **On-premises**

D. Hosted services

18. DNSSEC adds additional _____ and message header information, which can be used to verify that the requested data has not been altered in transmission.

A. **resource records**

B. field flags

C. hash sequences

D. zone transfers

19. What functions of a switch does a software defined network separate?

A. Host and virtual

B. **Control plane and physical plane**

C. RAM and hard drive

D. Network level and resource level

20. Which of the following is NOT a security concern of virtualized environments?

A. Virtual machines must be protected from both the outside world and from other virtual machines on the same physical computer.

B. Physical security appliances are not always designed to protect virtual systems.

C. **Virtual servers are less expensive than their physical counterparts**.

D. Live migration can immediately move one virtualized server to another hypervisor.</EOCMULTA></EOCMULTA_first></EOCMULT_first>

Chapter 8

Review Questions

1. Which technology is predominately used for contactless payment systems?

A. near field communication (NFC)

B. wireless local area network (WLAN)

C. Bluetooth

D. Radio Frequency ID (RFID)

2. Which of these Bluetooth attacks involves accessing unauthorized information through a Bluetooth connection?

A. **Bluesnarfing**

B. Bluejacking

C. Bluecreeping

D. Bluestealing

3. What is a difference between NFC and RFID?

A. NFC is based on wireless technology while RFID is not.

B. RFID is faster than NFC.

C. **RFID is designed for paper-based tags while NFC is not.**

D. NFC devices cannot pair as quickly as RFID devices.

4. Which of these technologies is NOT found in a wireless router?

A. **access point**

B. router

C. dynamic host configuration protocol (DHCP) server

D. firewall

5. Why is a rogue AP a security vulnerability?

A. It uses the weaker IEEE 80211i protocol.

B. It conflicts with other network firewalls and can cause them to become disabled.

C. **It allows an attacker to bypass- -network security configurations.**

D. It requires the use of vulnerable wireless probes on all mobile devices.

6. Which of these is NOT a risk when a home wireless router is not securely configured?

A. Only a small percentage of the total traffic can be encrypted.

B. An attacker can steal data from any folder with file sharing enabled.

C. User names, passwords, credit card numbers, and other information sent over the WLAN could be captured by an attacker.

D. Malware can be injected into a computer connected to the WLAN.

7. Which of these Wi-Fi Protected Setup (WPS) methods is vulnerable?

A. Push-Button method

B. PIN method

C. piconet method

D. NFC method

8. Flavio visits a local coffee shop on his way to school and accesses its free Wi-Fi. When he first connects, a screen appears that requires him to first agree to an Acceptable Use Policy (AUP) before continuing. What type of AP has he encountered?

A. **captive portal**

B. web-based portal

C. rogue portal

D. authenticated portal

9. Which of the following is NOT a wireless peripheral protection option?

A. Update or replacing any vulnerable device

B. Switch to a more fully tested Bluetooth model

C. **Install a network sensor to detect an attack**

D. Substitute a wired device

10. The primary design of a(n) ______ is to capture the transmissions from legitimate users.

A. rogue access point

B. WEP

C. evil twin

D. Bluetooth grabber

11. Which of these is a vulnerability of MAC address filtering?

A. APs use IP addresses instead of MACs.

B. The user must enter the MAC.

C. **MAC addresses are initially exchanged unencrypted**.

D. Not all operating systems support MACs.

12. Which of these is NOT a limitation of turning off the SSID broadcast from an AP?

A. Turning off the SSID broadcast may prevent users from being able to freely roam from one AP coverage area to another.

B. Some versions of operating systems favor a network that broadcasts an SSID over one that does not.

C. Users can more easily roam from one WLAN to another.

D. The SSID can easily be discovered, even when it is not contained in beacon frames, because it still is transmitted in other management frames sent by the AP.

13. What is the primary weakness of wired equivalent privacy (WEP)?

A. It functions only on specific brands of APs.

B. **Its usage creates a detectable pattern**.

C. It slows down a WLAN from 104 Mbps to 16 Mbps.

D. Initialization vectors (IVs) are difficult for users to manage.

14. WPA replaces WEP with _____.

A. WPA2

B. **Temporal Key Integrity Protocol (TKIP)**

C. Cyclic Redundancy Check (CRC)

D. Message Integrity Check (MIC)

15. Adabella was asked by her supervisor to adjust the frequency spectrum settings on a new AP. She brought up the configuration page and looked through the different options. Which of the following frequency spectrum settings would she NOT be able to adjust?

A. Frequency band

B. Channel selection

C. **RFID spectrum**

D. Channel width

16. A wireless LAN controller (WLC) was recently installed, and now Kelsey needs to purchase several new APs to be managed by it. Which type of AP should he purchase?

A. **Controller AP**

B. Standalone AP

C. Fat AP

D. Any type of AP can be managed by a WLC.

17. AES-CCMP is the encryption protocol standard used in _____.

A. WPA

B. WPA2

C. IEEE 802.11

D. NFC

18. Elijah was asked by a student intern to explain the Extensible Authentication Protocol (EAP). What would be the best explanation of EAP?

A. It is the transport protocol used in TCP/IP for authentication

B. It is a framework for transporting authentication protocols

C. It is a subset of WPA2

D. It is a technology used by IEEE 802.11 for encryption

19. Minh has been asked to recommend an EAP for a system that uses both passwords and tokens with TLS. Which should she recommend?

A. EAP-TLS

B. EAP-TTLS

C. EAP-SSL

D. EAP-FAST

20. Which of these is NOT a type of wireless AP probe?

A. wireless device probe

B. WNIC probe

C. dedicated probe

D. AP probe

Chapter 9

1. Which of the following is NOT a reason why supply chain infections are considered especially dangerous?

A. If the malware is planted in the ROM firmware of the device this can make it difficult or sometimes even impossible to clean an infected device.

B. Users are receiving infected devices at the point of purchase and are completely unaware that a brand new device may be infected.

C. It is virtually impossible to closely monitor every step in the supply chain.

D. **Supply chains take advantage of the trusted “chain of trust” concept.**

2. Which type of operating system runs on a firewall, router, or switch?

A. Server OS

B. **Network OS**

C. Device OS

D. Resource OS

3. Which of the following is NOT designed to prevent individuals from entering sensitive areas but instead is intended to direct traffic flow?

A. **Barricade**

B. Fencing

C. Roller barrier

D. Type V controls

4. Which of the following is NOT a motion detection method?

A. Magnetism

B. Radio frequency

C. Moisture

D. Infrared

5. Which type of residential lock is most often used for keeping out intruders?

A. Encrypted key lock

B. Keyed entry lock

C. Privacy lock

D. Passage lock

6. A lock that extends a solid metal bar into the door frame for extra security is the _____.

A. triple bar lock

B. deadman’s lock

C. full bar lock

D. deadbolt lock

7. Which statement about a mantrap is true?

A. It is illegal in the United States.

B. It monitors and controls two interlocking doors to a room.

C. It is a special keyed lock.

D. It requires the use of a cipher lock.

8. Which of the following is NOT a typical OS security configuration?

A. Employing least functionality

B. Restricting patch management

C. Disabling default accounts/passwords

D. Disabling unnecessary ports and services

9. Which of the following can be used to secure a laptop or mobile device?

A. Mobile connector

B. Cable lock

C. Mobile chain

D. Security tab

10. Which of the following is NOT a characteristic of an alarmed carrier PDS?

A. Requires periodic visual inspections

B. Uses continuous monitoring

C. Carrier can be hidden above the ceiling

D. Eliminates the need to seal connections

11. Which of the following is NOT a memory vulnerability?

A. DLL injection

B. Pointer deference

C. Buffer overflow

D. Variable overflow

12. Which stage is a “quality assurance” test that verifies the code functions as intended?

A. Production stage

B. Testing stage

C. Staging stage

D. Development stage

13. Which model uses a sequential design process?

A. **Waterfall model**

B. Rigid model

C. Agile model

D. Secure model

14. What allows for a single configuration to be set and then deployed to many or all users?

A. Snap-In Replication (SIR)

B. Active Directory

C. Group Policy

D. Command Configuration

15. Which of the following is a cumulative package of all patches?

A. Rollup

B. **Service pack**

C. Patch

D. Hotfix

16. Which of the following is NOT an advantage to an automated patch update service?

A. Administrators can approve or decline updates for client systems, force updates to install by a specific date, and obtain reports on what updates each computer needs.

B. Downloading patches from a local server instead of using the vendor's online update service can save bandwidth and time because each computer does not have to connect to an external server.

C. **Users can disable or circumvent updates just as they can if their computer is configured to use the vendor's online update service**.

D. Specific types of updates that the organization does not test, such as hotfixes, can be automatically installed whenever they become available.

17. How can an SDIO card be made secure?

A. **Using the security mechanisms on a standard Wi-Fi network**.

B. Turning on patch updates to the SDIO card.

C. Requiring a username before accessing the SDIO card.

D. SDIO cards are natively secure and no security settings are needed.

18. How does heuristic detection detect a virus?

A. A virtualized environment is created and the code is executed in it.

B. A string of bytes from the virus is compared against the suspected file.

C. **The bytes of a virus are placed in different "piles" and then used to create a profile**.

D. The virus signature file is placed in a suspended chamber before streaming to the CPU.

19. Which of these is a list of approved email senders?

A. Blacklist

B. Whitelist

C. Bluelist

D. Yellowlist

20. Which of the following types of testing uses unexpected or invalid inputs?

A. Stress testing

B. **Dynamic analysis**

C. Static analysis

D. Runtime testing

Chapter 10

Review Questions

1. Which technology is NOT a core feature of a mobile device?

A. physical keyboard

B. small form factor

C. local non-removable data storage

D. data synchronization capabilities

2. Agape was asked to make a recommendation regarding short-range wireless technologies to be supported in a new conference room that was being renovated. Which of the following would she NOT consider due to its slow speed and its low deployment levels today?

A. ANT

B. Bluetooth

C. **Infrared**

D. NFC

3. Calista is designing the specifications for new laptop computers to be purchased by her company. She is comparing the different types and sizes of USB connections found on the devices. Which type USB connection would she NOT find on a laptop?

A. Type D

B. Mini

C. Micro

D. Standard

4. In her job interview, Xiu asks about the company policy regarding smartphones. She is told that employees may choose from a limited list of approved devices but that she must pay for the device herself; however, the company will provide her with a monthly stipend. Which type of enterprise deployment model does this company support?

A. BYOD

B. COPE

C. **CYOD**

D. Corporate-owned

5. Pakpao has been asked to provide research regarding a new company initiative to add Android smartphones to a list of approved devices. One of the considerations is how frequently the smartphones receive firmware OTA updates. Which of the following reasons would Pakpao NOT list in his report as a factor in the frequency of Android firmware OTA updates?

A. Both OEMs and wireless carriers are hesitant to distribute Google updates because it limits their ability to differentiate themselves from competitors if all versions of Android start to look the same through updates.

B. Because many of the OEMs had modified Android, they are reluctant to distribute updates that could potentially conflict with their changes.

C. **Wireless carriers are reluctant to provide firmware OTA updates because of the bandwidth it consumes on their wireless networks.**

D. Because OEMs and wireless carriers want to sell as many devices as possible, they have no financial incentive to update mobile devices that users would then continue to use indefinitely.

6. What is the process of identifying the geographical location of a mobile device?

A. geotracking

B. **geolocation**

C. geoID

D. geomonitoring

7. Which of these is NOT a risk of connecting a mobile device to a public network?

A. Public networks are beyond the control of the employee’s organization.

B. Replay attacks can occur on public networks.

C. Public networks may be susceptible to man-in-the-middle attacks.

D. Public networks are faster than local networks and can spread malware more quickly to mobile devices.

8. Paavo was reviewing a request by an executive for a new subnotebook computer. The executive said that he wanted USB OTG support and asked Paavo's opinion regarding its security. What would Paavo tell him about USB OTG security?

A. USB OTG uses strong security and the executive should have no concerns.

B. Subnotebooks do not support USB OTG.

C. An unsecured mobile device could infect other tethered mobile devices or the corporate network.

D. **Connecting a mobile device as a peripheral to an infected computer could allow malware to be sent to that device.**

9. A friend of Ukrit told him that he has just downloaded and installed an app that allows him to circumvent the built-in limitations on his Apple iOS smartphone. What is this called?

A. Rooting

B. Sideloading

C. **Jailbreaking**

D. Ducking

10. Which of the following technologies provides for pictures, video, or audio to be included in text messages?

A. MMS

B. QR

C. SMS

D. ANT

11. What prevents a mobile device from being used until the user enters the correct passcode?

A. swipe identifier (SW-ID)

B. screen lock

C. screen timeout

D. touch swipe

12. Gaetan has attempted to enter the passcode for his mobile device but keeps entering the wrong code. Now he is asked to enter a special phrase to continue. Which configuration setting is enabled on Gaetan's mobile device?

A. reset to factory settings

B. extend lockout period

C. enable high security

D. lock device

13. What does containerization do?

A. It splits operating system functions only on specific brands of mobile devices.

B. It places all keys in a special vault.

C. It slows down a mobile device to half speed.

D. It separates personal data from corporate data.

14. What allows a device to be managed remotely?

A. **mobile device management (MDM)**

B. mobile application management (MAM)

C. mobile resource management (MRM)

D. mobile wrapper management (MWM)

15. Which of these is NOT a security feature for locating a lost or stolen mobile device?

A. remote lockout

B. **last known good configuration**

C. alarm

D. thief picture

16. What enforces the location in which an app can function by tracking the location of the mobile device?

A. location resource management

B. geofencing

C. GPS tagging

D. Graphical Management Tracking (GMT)

17. Which of these is considered the strongest type of passcode to use on a mobile device?

A. **password**

B. PIN

C. fingerprint swipe

D. draw connecting dots pattern

18. Jabez needs to alert through an SMS text message those corporate users who have a specific brand and type of mobile device regarding a serious malware incident. What technology will she use?

A. MCM

B. COPE

C. MAM

D. push notification services

19. Which tool manages the distribution and control of apps?

A. MAM

B. MDM

C. MCM

D. MFM

20. Which type of OS is typically found on an embedded system?

A. SoC

B. RTOS

C. OTG

D. COPE

Chapter 11

1. Which authentication factor is based on a unique talent that a user possesses?

A. What you have

B. What you are

C. What you do

D. What you know

2. Which of these is NOT a characteristic of a weak password?

A. A common dictionary word

B. **A long password**

C. Using personal information

D. Using a predictable sequence of characters

3. Each of the following accounts should be prohibited EXCEPT:

A. Shared accounts

B. Generic accounts

C. **Privileged accounts**

D. Guest accounts

4. Ilya has been asked to recommend a federation system technology that is an open source federation framework that can support the development of authorization protocols. Which of these technologies would he recommend?

A. **OAuth**

B. Open ID Connect

C. Shibboleth

D. NTLM

5. How is key stretching effective in resisting password attacks?

A. **It takes more time to generate candidate password digests**.

B. It requires the use of GPUs.

C. It does not require the use of salts.

D. The license fees are very expensive to purchase and use it.

6. Which of these is NOT a reason why users create weak passwords?

A. A lengthy and complex password can be difficult to memorize.

B. A security policy requires a password to be changed regularly.

C. Having multiple passwords makes it hard to remember all of them.

D. **Most sites force users to create weak passwords even though they do not want to**.

7. What is a hybrid attack?

A. An attack that uses both automated and user input

B. An attack that combines a dictionary attack with a mask attack

C. A brute force attack that uses special tables

D. An attack that slightly alters dictionary words

8. A TOTP token code is generally valid for what period of time?

A. Only while the user presses SEND

B. For as long as it appears on the device

C. For up to 24 hours

D. Until an event occurs

9. What is a token system that requires the user to enter the code along with a PIN called?

A. Single-factor authentication system

B. Token-passing authentication system

C. Dual-prong verification system

D. Multifactor authentication system

10. Which of these is a U.S. Department of Defense (DoD) smart card that is used for identification of active-duty and reserve military personnel?

A. Personal Identity Verification (PIV) card

B. Secure ID Card (SIDC)

C. Common Access Card (CAC)

D. Government Smart Card (GSC)

11. Which of the following should NOT be stored in a secure password database?

A. Iterations

B. Password digest

C. Salt

D. Plaintext password

12. Creating a pattern of where a user accesses a remote web account is an example of which of the following?

A. Keystroke dynamics

B. **Geolocation**

C. Time-Location Resource Monitoring (TLRM)

D. Cognitive biometrics

13. Timur was making a presentation regarding how attackers break passwords. His presentation demonstrated the attack technique that is the slowest yet most thorough attack that is used against passwords. Which of these password attacks did he demonstrate?

A. Dictionary attack

B. Hybrid attack

C. Custom attack

D. **Brute force attack**

14. Which human characteristic is NOT used for biometric identification?

A. Retina

B. Iris

C. Height

D. Fingerprint

15. _____ biometrics is related to the perception, thought processes, and understanding of the user.

A. **Cognitive**

B. Standard

C. Intelligent

D. Behavioral

16. Using one authentication credential to access multiple accounts or applications is known as _____.

A. **single sign-on**

B. credentialization

C. identification authentication

D. federal login

17. What is a disadvantage of biometric readers?

A. Speed

B. Cost

C. Weight

D. Standards

18. Which type of password attack is a more targeted brute force attack that uses placeholders for characters in certain positions of the password?

A. Rainbow attack

B. Mask attack

C. Rule attack

D. Pass the hash attack

19. Why should the account lockout threshold not be set too low?

A. It could decrease calls to the help desk.

B. The network administrator would have to reset the account manually.

C. The user would not have to wait too long to have her password reset.

D. **It could result in denial of service (DoS) attacks**.

20. Which one-time password is event-driven?

A. HOTP

B. TOTP

C. ROTP

D. POTP

Chapter 12

1. What is the current version of TACACS?

A. XTACACS

B. TACACS+

C. TACACS v9

D. TRACACS

2. How is the Security Assertion Markup Language (SAML) used?

A. **It allows secure web domains to exchange user authentication and authorization data.**

B. It is a backup to a RADIUS server.

C. It is an authenticator in IEEE 802.1x.

D. It is no longer used because it has been replaced by LDAP.

3. A RADIUS authentication server requires the ________ to be authenticated first.

A. authenticator

B. user

C. authentication server

D. **supplicant**

4. Which of the following is NOT true regarding how an enterprise should handle an orphaned or dormant account?

A. A formal procedure should be in place for disabling accounts for employees who are dismissed, resign, or retire from the organization.

B. Access should be ended as soon as the employee is no longer part of the organization.

C. Logs should be monitored because current employees are sometimes tempted to use an older dormant account instead of their own account.

D. All orphaned and dormant accounts should be deleted immediately whenever they are discovered.

5. With the development of IEEE 802.1x port security, what type of authentication server has seen even greater usage?

A. RADIUS

B. Lite RDAP

C. DAP

D. RDAP

6. Which of the following is NOT part of the AAA framework?

A. Authentication

B. Access

C. Authorization

D. Accounting

7. What is the version of the X.500 standard that runs on a personal computer over TCP/IP?

A. Lite RDAP

B. DAP

C. LDAP

D. IEEE X.501

8. Raul has been asked to serve as the individual to whom day-to-day actions have been assigned by the owner. What role is Raul taking?

A. Privacy officer

B. End-user

C. **Custodian**

D. Operator

9. Which access control model is the most restrictive?

A. DAC

B. MAC

C. Role-Based Access Control

D. Rule-Based Access Control

10. Which type of access control model uses predefined rules that makes it flexible?

A. **ABAC**

B. DAC

C. MAC

D. Rule-Based Access Control

11. Which can be used to establish geographical boundaries where a mobile device can and cannot be used?

A. **Location-based policies**

B. Restricted access control policies

C. Geolocation policies

D. Mobile device policies

12. Which statement about Rule-Based Access Control is true?

A. It requires that a custodian set all rules.

B. It is considered obsolete today.

C. It dynamically assigns roles to subjects based on rules.

D. It is considered a real-world approach by linking a user's job function with security.

13. Which of the following would NOT be considered as part of a clean desk policy?

A. Do not share passwords with other employees.

B. Lock computer workstations when leaving the office.

C. Place laptops in a locked filing cabinet.

D. Keep mass storage devices locked in a drawer when not in use.

14. Which of these is a set of permissions that is attached to an object?

A. Access control list (ACL)

B. Subject Access Entity (SAE)

C. Object modifier

D. Security entry designator

15. Which Microsoft Windows feature provides group-based access control for centralized management and configuration of computers and remote users who are using Active Directory?

A. Windows Registry Settings

B. AD Management Services (ADMS)

C. Group Policy

D. Resource Allocation Entities

16. What can be used to provide both file system security and database security?

A. RBASEs

B. LDAPs

C. CHAPs

D. **ACLs**

17. What is the least restrictive access control model?

A. DAC

B. ABAC

C. MAC

D. Rule-Based Access Control

18. What is the secure version of LDAP?

A. LDAPS

B. Secure DAP

C. X.500

D. 802.1x

19. Which of the following is the Microsoft version of EAP?

A. EAP-MS

B. **MS-CHAP**

C. PAP-MICROSOFT

D. AD-EAP

20. Which of the following involves rights given to access specific resources?

A. Identification

B. **Access**

C. Authorization

D. Accounting

Chapter 13

1. <EOCMULT_first>At what point in a vulnerability assessment would an attack tree be utilized?

A. <EOCMULTA_first>Vulnerability appraisal

B. <EOCMULTA>Risk assessment

C. Risk mitigation

D. Threat evaluation

2. Which of the following is NOT true about privacy?

A. Today, individuals can achieve any level of privacy that is desired.

B. Privacy is difficult due to the volume of data silently accumulated by technology.

C. Privacy is freedom from attention, observation, or interference based on your decision.

D. Privacy is the right to be left alone to the degree that you choose.

3. Which of the following is NOT a risk associated with the use of private data?

A. Individual inconveniences and identity theft

B. Associations with groups

C. Statistical inferences

D. **Devices being infected with malware**

4. Which of the following is NOT an issue raised regarding how private data is gathered and used?

A. The data is gathered and kept in secret.

B. **By law, all encrypted data must contain a “backdoor” entry point**.

C. Informed consent is usually missing or is misunderstood.

D. The accuracy of the data cannot be verified.

5. Which of the following is a systematic and methodical evaluation of the exposure of assets to attackers, forces of nature, and any other entity that could cause potential harm?

A. **Vulnerability assessment**

B. Penetration test

C. Vulnerability scan

D. Risk appraisal

6. Which of these should NOT be classified as an asset?

A. Business partners

B. Buildings

C. Employee databases

D. Accounts payable

7. Which of the following command-line tools tests a connection between two network devices?

A. Netstat

B. Ping

C. Nslookup

D. Ifconfig

8. Which statement regarding vulnerability appraisal is NOT true?

A. **Vulnerability appraisal is always the easiest and quickest step**.

B. Every asset must be viewed in light of each threat.

C. Each threat could reveal multiple vulnerabilities.

D. Each vulnerability should be cataloged.

9. Which of the following constructs scenarios of the types of threats that assets can face to learn who the attackers are, why they attack, and what types of attacks may occur?

A. Vulnerability prototyping

B. Risk assessment

C. Attack assessment

D. Threat modeling

10. Which of the following tools is a Linux command-line protocol analyzer?

A. Wireshark

B. Tcpdump

C. IP

D. Arp

11. Which of the following is a command-line alternative to Nmap?

A. **Netcat**

B. Statnet

C. Mapper

D. Netstat

12. Which of these is NOT a state of a port that can be returned by a port scanner?

A. Open

B. **Busy**

C. Blocked

D. Closed

13. Which of the following data sensitivity labels is the highest level of data sensitivity?

A. Ultra

B. **Confidential**

C. Private

D. Secret

14. Which of the following data sensitivity labels has the lowest level of data sensitivity?

A. Unrestricted

B. **Public**

C. Free

D. Open

15. Which of the following is NOT a function of a vulnerability scanner?

A. Detects which ports are served and which ports are browsed for each individual system

B. Alerts users when a new patch cannot be found

C. Maintains a log of all interactive network sessions

D. Detects when an application is compromised

16. Which of the following must be kept secure as mandated by HIPAA?

A. PII

B. **PHI**

C. PHIL

D. PLILP

17. Which statement regarding a honeypot is NOT true?

A. It is typically located in an area with limited security.

B. It is intentionally configured with security vulnerabilities.

C. **It cannot be part of a honeynet**.

D. It can direct an attacker’s attention away from legitimate servers.

18. Which of the following sends “probes” to network devices and examines the responses to evaluate whether a specific device needs remediation?

A. **Active scanner**

B. Probe scanner

C. Passive scanner

D. Remote scanner

19. If a tester is given the IP addresses, network diagrams, and source code of customer applications, the tester is using which technique?

A. Black box

B. White box

C. Gray box

D. Blue box

20. If a software application aborts and leaves the program open, which control structure is it using?

A. Fail-safe

B. Fail-secure

C. **Fail-open**

D. Fail-right

Chapter 14

1. Raul has been asked to help develop an outline of procedures to be followed in the event of a major IT incident or an incident that directly impacts IT. What type of planning is this?

A. Disaster recovery planning

B. IT contingency planning

C. Business impact analysis planning

D. Risk IT planning

2. Dilma has been tasked with creating a list of potential employees to serve in an upcoming tabletop exercise. Which employees will be on her list?

A. All employees

B. Individuals on a decision-making level

C. Full-time employees

D. Only IT managers

3. What is the average amount of time that it will take a device to recover from a failure that is not a terminal failure?

A. **MTTR**

B. MTBR

C. MTBF

D. MTTI

4. Which of the following is NOT a category of fire suppression systems?

A. Water sprinkler system

B. Wet chemical system

C. Clean agent system

D. Dry chemical system

5. Which of the following is NOT required for a fire to occur?

A. A chemical reaction that is the fire itself

B. A type of fuel or combustible material

C. A spark to start the process

D. Sufficient oxygen to sustain the combustion

6. An electrical fire like that which would be found in a computer data center is known as what type of fire?

A. Class A

B. Class B

C. Class C

D. Class D

7. Which level of RAID uses disk mirroring and is considered fault-tolerant?

A. Level 1

B. Level 2

C. Level 3

D. Level 4

8. What is the amount of time added to or subtracted from Coordinated Universal Time to determine local time?

A. **Time offset**

B. Civil time

C. Daylight savings time

D. Greenwich Mean Time (GMT)

9. What does the abbreviation RAID represent?

A. Redundant Array of IDE Drives

B. Resilient Architecture for Interdependent Discs

C. Redundant Array of Independent Drives

D. Resistant Architecture of Inter-Related Data Storage

10. Which of these is an example of a nested RAID?

A. Level 1-0

B. Level 0-1

C. Level 0+1

D. Level 0/1

11. A(n) _____ is always running off its battery while the main power runs the battery charger.

A. secure UPS

B. backup UPS

C. off-line UPS

D. on-line UPS

12. Which type of site is essentially a duplicate of the production site and has all the equipment needed for an organization to continue running?

A. Cold site

B. Warm site

C. **Hot site**

D. Replicated site

13. Which of the following can a UPS NOT perform?

A. **Prevent certain applications from launching that will consume too much power**

B. Disconnect users and shut down the server

C. Prevent any new users from logging on

D. Notify all users that they must finish their work immediately and log off

14. Which of these is NOT a characteristic of a disaster recovery plan (DRP)?

A. It is updated regularly.

B. It is a private document used only by top-level administrators for planning.

C. It is written.

D. It is detailed.

15. What does an incremental backup do?

A. Copies all files changed since the last full or incremental backup

B. Copies selected files

C. Copies all files

D. Copies all files since the last full backup

16. Which question is NOT a basic question to be asked regarding creating a data backup?

A. What media should be used?

B. How long will it take to finish the backup?

C. Where should the backup be stored?

D. What information should be backed up?

17. The chain of _____ documents that the evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt the evidence.

A. forensics

B. evidence

C. custody

D. control

18. What is the maximum length of time that an organization can tolerate between data backups?

A. Recovery time objective (RTO)

B. Recovery service point (RSP)

C. Recovery point objective (RPO)

D. Optimal recovery timeframe (ORT)

19. Margaux has been asked to work on the report that will analyze the exercise results with the purpose of identifying strengths to be maintained and weaknesses to be addressed for improvement. What report will she be working on?

A. Identification of critical systems report

B. Containment report

C. Business continuity report

D. **After-action report**

20. When an unauthorized event occurs, what is the first duty of the cyber-incident response team?

A. To log off from the server

B. **To secure the crime scene**

C. To back up the hard drive

D. To reboot the system

Chapter 15

1. <EOCMULT_first>Which of the following threats would be classified as the actions of a hactivist?

A. <EOCMULTA_first>External threat

B. <EOCMULTA>Internal threat

C. Environmental threat

D. Compliance threat

2. Which of these is NOT a response to risk?

A. mitigation

B. transference

C. **resistance**

D. avoidance

3. Agnella was asked to create a report that listed the reasons why a contractor should be provided penetration testing authorization. Which of the follow would she NOT list in her report?

A. Legal authorization

B. Indemnification

C. Limit retaliation

D. **Access to resources**

4. Which of the following risk control types would use video surveillance systems and barricades to limit access to secure sites?

A. operational

B. managerial

C. **technical**

D. strategic

5. Which of the following approaches to risk calculation typically assigns a numeric value (*1–10*) or label (*High*, *Medium*, or *Low*) represents a risk?

A. **Quantitative risk calculation**

B. Qualitative risk calculation

C. Rule-based risk calculation

D. Policy-based risk calculation

6. Which of the following is the average amount of time that it will take a device to recover from a failure that is not a terminal failure?

A. MTTF

B. MTTR

C. FIT

D. MTBF

7. Which of the following covers the procedures of managing object authorizations?

A. Asset management

B. Task management

C. Privilege management

D. Threat management

8. Which statement does NOT describe a characteristic of a policy?

A. Policies define appropriate user behavior.

B. Policies identify what tools and procedures are needed.

C. Policies communicate a unanimous agreement of judgment.

D. Policies may be helpful if it is necessary to prosecute violators.

9. Tomassa is asked to determine the expected monetary loss every time a risk occurs. Which formula will she use?

A. AV

B. ARO

C. ALE

D. SLE

10. What is a collection of suggestions that should be implemented?

A. Policy

B. Guideline

C. Standard

D. Code

11. Simona needs to research a control that attempts to discourage security violations before they occur. Which control will she research?

A. Deterrent control

B. Preventive control

C. Detective control

D. Corrective control

12. Which statement is NOT something that a security policy must do?

A. State reasons why the policy is necessary.

B. **Balance protection with productivity**.

C. Be capable of being implemented and enforced.

D. Be concise and easy to understand.

13. What describes is the ability of an enterprise data center to revert to its former size after expanding?

A. Scalability

B. Elasticity

C. Contraction

D. Reduction

14. Which policy defines the actions users may perform while accessing systems and networking equipment?

A. End-user policy

B. Acceptable use policy

C. Internet use policy

D. User permission policy

15. While traveling abroad, Giuseppe needs to use public Internet café computers to access the secure network. Which of the following non-persistence tools should he use?

A. Snapshot

B. Live boot media

C. Revert to known state

D. Secure Configuration

16. Bria is reviewing the company's updated personal email policy. Which of the following will she NOT find in it?

A. Employees should not use company email to send personal email messages.

B. Employees should not access personal email at work.

C. Employees should not forward company emails to a personal email account.

D. **Employees should not give out their company email address unless requested.**

17. For adult learners, which approach is often preferred?

A. Pedagogical

B. Andragogical

C. Institutional

D. Proactive

18. Which of the following is NOT a security risk of social media sites for users?

A. Personal data can be used maliciously.

B. Users may be too trusting.

C. Social media security is lax or confusing.

D. Social media sites use popup ads.

19. Which of the following is NOT a time employee training should be conducted?

A. After monthly patch updates.

B. When a new computer is installed.

C. During an annual department retreat.

D. When an employee is promoted.

20. Bob needs to create an agreement between his company and a third-party organization that demonstrates a “convergence of will” between the parties so that they can work together. Which type of agreement will Bob use?

A. SLA

B. BPA

C. ISA

D. **MOU**

Chapter 1

Introduction to Security

At a Glance

Instructor's Manual Table of Contents

Lecture Notes

Overview

Chapter 1 introduces security fundamentals that form the basis of the Security+ certification. It begins by examining the current challenges in computer security and why it is so difficult to achieve. It then describes information security in more detail to illustrate why it is important. Finally, the chapter looks at who is responsible for these attacks and what the fundamental defenses against attackers are.

Chapter Objectives

- Explain the challenges of securing information
- Define information security and explain why it is important
- Identify the types of threat actors that are common today
- Describe how to defend against attacks

Teaching Tips

Challenges of Securing Information

1. Explain that there is no simple solution to securing information. This can be seen through the different types of attacks that users face today, as well as the difficulties in defending against these attacks.

Today's Security Attacks

1. Describe some recent security attacks, such as the following:
   a. A reporter drove a Jeep Cherokee while two security researchers 10 miles away remotely connected to it and started manipulating its controls.
   b. United Airlines passenger who tampered with the Seat Electronic Box to connect to other system on the plane.
   c. Half a billion Yahoo accounts were compromised by attacker who gained unauthorized access to its web servers.
   d. USB Killer device.
   e. WINVote voting machine vulnerabilities .
   f. VTech accounts that included information on 6.4 million children were hacked .
   g. IRS Get Transcript program was hacked.

2. Mention that security statistics bear witness to the continual success of attackers:
   a. From 2005-2017 over 907 million electronic data records in the U.S. had been breached.

Teaching Tip	Phishing Web sites are well known for suddenly appearing and then disappearing to reduce the risk of being traced. The average time a site is online is only four days according to the APWG (www.antiphishing.org).

Teaching Tip	The US-CERT security bulletin is available at www.us-cert.gov/cas/bulletins/.

Reasons for Successful Attacks

1. Discuss the following reasons behind successful attacks:
   a. Widespread vulnerabilities
   b. Configuration issues
   c. Poorly designed software
   d. Hardware limitations
   e. Enterprise-based issues

Difficulties in Defending against Attacks

1. Describe the following difficulties in defending against attacks:
   a. Universally connected devices
   b. Increased speed of attacks
   c. Greater sophistication of attacks
   d. Availability and simplicity of attack tools
   e. Faster detection of vulnerabilities
   f. Delays in security updating
   g. Weak security update distribution
   h. Distributed attacks
   i. Use of personal devices
   j. User confusion

2. Table 1-2 summarizes these difficulties.

What Is Information Security?

1. Mention that knowing why information security is important today and who the attackers are is beneficial. Point out that knowing the terminology used can be helpful when creating defenses for computers.

Understanding Security

1. Explain that security can be considered as a state of freedom from a danger or risk. This state or condition of freedom exists because protective measures are established and maintained.

2. Use Figure 1-2 to help explain the relationship between security and convenience. Point out that as security is increased, convenience is often decreased.

Defining Information Security

1. Define information security as the tasks of guarding information that is in a digital format. It ensures that protective measures are properly implemented. Information security cannot completely prevent attacks or guarantee that a system is totally secure.

2. Explain that information security is intended to protect information that has value to people and organizations. That value comes from the characteristics of the information:
   a. Confidentiality
   b. Integrity
   c. Availability

Teaching Tip	The confidentiality, integrity, and availability of information is known as CIA.

3. Explain that information security is achieved through a combination of three protections. Use Figure 1-3 and Table 1-3 to illustrate your explanation.

4. Emphasize that information security is that which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures.

Information Security Terminology

1. Define the following information security terms:
   a. Asset
   b. Threat
   c. Threat actor
   d. Vulnerability
   e. Attack vector
   f. Attack surface
   g. Risk

2. Use Figure 1-4 and Table 1-5 to illustrate the terminology above.

3. Discuss and define the different options available when dealing with risks.
    a. Acceptance
    b. Transference
    c. Risk avoidance
    d. Mitigation

Quick Quiz 1

1. Which protection ensures that only authorized parties can view the information?
   a. Confidentiality
   b. Integrity
   c. Accounting
   d. Availability
   Answer: A

2. Which of the following terms best describes ensuring that data is accessible to authorized users?
   a. Integrity
   b. Accounting
   c. Availability
   d. BYOD
   Answer: C

3. A(n) _____ is defined as something that has a value.
   Answer: asset

4. A situation that involves exposure to some type of danger is known as which of the following?
   a. vector
   b. risk
   c. threat
   d. asset
   Answer: B

5. Addressing a risk by making it less serious is known as which of the following?
   a. acceptance
   b. transference
   c. avoidance
   d. mitigation
   Answer: D

Understanding the Importance of Information Security

1. Mention that the main goals of information security are to prevent data theft, thwart identity theft, avoid the legal consequences of not securing information, maintain productivity, and foil cyberterrorism.

2. Explain that security is often associated with theft prevention. The theft of data is one of the largest causes of financial loss due to an attack. Individuals are often victims of data thievery.

3. Mention that identity theft involves using someone's personal information to establish bank or credit card accounts that are then left unpaid, leaving the victim with the debts and ruining their credit rating.

4. Explain that a number of federal and state laws have been enacted to protect the privacy of electronic data, including the following:
    a. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    b. The Sarbanes-Oxley Act of 2002 (Sarbox)
    c. The Gramm-Leach-Bliley Act (GLBA)
    d. Payment Card Industry Data Security Standard (PCI DSS)
    e. State notification and security laws

Teaching Tip	In 2008, California extended its data breach notification law to encompass incidents including electronic medical and health insurance information.

5. Explain that cleaning up after an attack diverts resources such as time and money away from normal activities. Use Table 1-6 to illustrate your explanation.

6. Define cyberterrorism as attacks by terrorist groups using computer technology and the Internet. Utility, telecommunications, and financial services companies are considered prime targets of cyberterrorists.

Who Are the Threat Actors?

1. Explain that the term threat actor, in a generic sense, is used to describe individuals who launch attacks against other users and their computers.

2. Explain that threat actors of today have a more focused goal of financial gain: to exploit vulnerabilities that can generate income.

3. Point out that the characteristic features of different groups of threat actors can vary widely:
   a. Sophisticated
   b. Funding and resources
   c. External or internal to the enterprise
   d. Intent and motivation

4. Today threat actors are recognized in more distinct categories, such as script kiddies, hactivists, nation state actors, insiders, and others.

Teaching Tip	Security vulnerabilities, however, can be exposed in ways other than attacking another computer without the owner's consent, and most security professionals would not refer to themselves as hackers.

Script Kiddies

1. Define script kiddies as individuals that want to break into computers to create damage. They download automated hacking software (scripts) from Web sites and use it to break into computers.

2. Point out that script kiddies can acquire entire exploit kits from other attackers. It takes little skill to be a script kiddie.

Hactivists

1. Mention that hactivists are a group strongly motivated by ideology. They are likely to break into a website and change the contents as a means of making a political statement.

2. Point out that it is estimated that there are thousands of hacktivist groups worldwide supporting a wide variety of causes.

Nation State Actors

1. Define nation state actors as individuals hired by governments to launch computer attacks against the country's foes.

2. Mention that a new class of attacks called Advanced Persistent Threat (APT) have been created. Further explain that these attacks uses innovative attack tools and once a system is infected it silently extracts data over an extended period.

Insiders

1. Mention that one of the largest information security threats to a business actually comes from an unlikely source: its employees, contractors and business partners.

2. Describe some of the reasons an employee would break into their company's computer, including:
    a. Disgruntled employees may be intent on retaliating against the company
    b. Industrial espionage
    c. Blackmailing

Other Threat Actors

1. Use Table 1-7 to discuss the characteristics of the different types of attackers mentioned in this section of the text.

Defending Against Attacks

1. Mention that although multiple defenses may be necessary to withstand an attack, these defenses should be based on five fundamental security principles: layering, limiting, diversity, obscurity, and simplicity.

Layering

1. Mention that information security must be created in layers.

2. Explain that one defense mechanism may be relatively easy for an attacker to circumvent. Instead, a security system must have layers, making it unlikely that an attacker has the tools and skills to break through all the layers of defenses.

3. Explain that a layered approach (also called defense-in-depth) can also be useful in resisting a variety of attacks. Layered security provides the most comprehensive protection.

Limiting

1. Mention that limiting access to information reduces the threat against it.

2. Explain that only those who must use data should have access to it. In addition, the amount of access granted to someone should be limited to what that person needs to know.

3. Mention that some ways to limit access are technology-based, while others are procedural.

Teaching Tip	What level of access should users have? The best answer is the least amount necessary to do their jobs, and no more.

Diversity

1. Explain that layers must be different (diverse) so that if attackers penetrate one layer, they cannot use the same techniques to break through all other layers.

2. Using diverse layers of defense means that breaching one security layer does not compromise the whole system.

Obscurity

1. Explain that an example of obscurity is not revealing the type of computer, operating system, software, and network connection that a computer uses. An attacker who knows that information can more easily determine the weaknesses of the system.

2. Mention that obscuring information can be an important way to protect information.

Simplicity

1. Explain that information security is by its very nature complex. Complex security systems can be hard to understand, troubleshoot, and feel secure about.

2. Mention that as much as possible, a secure system should be simple for those on the inside to understand and use. Complex security schemes are often compromised to make them easier for trusted users to work with. Keeping a system simple from the inside but complex on the outside can sometimes be difficult but reaps a major benefit.

Frameworks and Reference Architectures

1. Explain that industry-standard frameworks and reference architectures provide a resource of how to create a secure IT environment.

2. Point out to students that various frameworks/architectures are specific to a particular sector (industry-specific frameworks) such as the financial industry.

3. Discuss how some of the framework/architectures are domestic while others are worldwide (national vs. international).

Quick Quiz 2

1. _______ is a generic term used to describe individuals who launch attacks against other users and their computers.
   Answer: Threat actors

2. The motivation of which type of threat actor may be defined as ideology, or attacking for the sake of their principles or beliefs?
   a. script kiddies
   b. hactivists
   c. nation state actors
   d. insiders
   Answer: B

3. Attackers who do their work by downloading automated attack software from websites and use it to perform malicious acts are known as which of the following?
   a. script kiddies
   b. hactivists
   c. nation state actors
   d. insiders
   e. Answer: A

4. In which fundamental security principle would only those personnel who must use data have access to it?
   a. layering
   b. limiting
   c. diversity
   d. obscurity
   Answer: B

5. Which fundamental security principle involves not revealing the type of computer, version of operating system, or brand of software that is used?
   e. layering
   f. limiting
   g. diversity
   h. obscurity
   Answer: D

Class Discussion Topics

1. What are the differences between hactivists and state-sponsored attackers?

2. Ask students to explain why creating a defense-in-depth is a good strategy when creating a secure IT environment.

Additional Projects

1. Ask your students to read more about phishing scams and write a report with a series of guidelines to recognize them and other fraudulent e-mails.

2. Nessus is a widely used free vulnerability scanner tool used by many security experts. Ask your students to read more about Nessus and write a report summarizing its more important features.

Additional Resources

1. FTC – Computer Security
   http://www.consumer.ftc.gov/topics/computer-security

2. Fight Spam on the Internet!
   http://spam.abuse.net/

3. How to recognize phishing e-mail messages, links, or phone calls
   http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

4. Anti-Phishing Working Group
   http://www.antiphishing.org/

5. SANS' Information Security Reading Room
   http://www.sans.org/reading_room/

6. Zero day initiative
   http://www.zerodayinitiative.com/

Key Terms

- **accept**
- **administrative controls**
- **Advanced Persistent**
- **Threat (APT)**
- **architecture/design**
- **weaknesses**
- **asset**
- **attributes**
- **availability**
- **avoid**
- **competitors**
- **confidentiality**

- **control diversity**
- **default configurations**
- **defense-in-depth**
- **end-of-life system**
- **external**
- **funding and resources**
- **hactivists**
- **improper error**
- **handling**
- **improper input handling**
- **improperly configured**
- **accounts**
- **industry-specific**
- **frameworks**
- **industry-standard**
- **frameworks**
- **insiders**
- **integrity**
- **intent and motivation**
- **internal**
- **international**
- **lack of vendor support**
- **layered security**
- **misconfiguration**
- **mitigate**
- **nation state actors**
- **national**
- **new threat**
- **non-regulatory**
- **open-source intelligence**
- **organized crime**
- **race condition**
- **reference architectures**
- **regulatory**
- **resource exhaustion**
- **risk**
- **risk response**
- **techniques**
- **script kiddies**
- **sophisticated**
- **system sprawl**
- **technical controls**
- **threat**
- **threat actor**
- **transfer**
- **undocumented assets**

- **untrained users**
- **user training**
- **vendor diversity**
- **vulnerability**
- **vulnerable business**
- **processes**
- **weak configuration**
- **zero day**