Exam Essentials

**Describe the CIA triad.** :Every security measure you implement should contribute to the achievement of one of three goals. The three fundamentals of security are confidentiality, integrity, and availability (CIA), often referred to as the CIA triad.

**Define important security terms**. :Security professionals should become familiar with terms such as assets, vulnerabilities, threats, threat agent, risk, exposure, and countermeasures.

**Identify common security zones.:** Describe intranet, extranet, DMZ, and the Internet. Explain their proper use.

**Describe common network topologies.:** Explain various topologies as seen from the perspective of the Cisco campus area network such as the enterprise core, enterprise campus, intranet data center, WAN edge, and intranet edge. Describe the common security issues found in each.

Review Questions

1. Which of the following is not one of the CIA triad? A. Confidentiality B. Integrity C. Availability D. Accountability
2. Which of the following requires that a user or process is given only the minimum access privilege needed to perform a particular task? A. Least privilege B. Separation of duties C. Job rotation D. Mandatory vacation
3. Which of the following occurs when a vulnerability is identified or exploited? A. Risk B. Threat C. Exposure D. Countermeasure
4. According to NIST SP 800-30, what is the first step in the risk management process? A. Identify threats B. Identify impact C. Identify vulnerabilities D. Identify the assets and their value
5. Which of the following is a measure of how freely data can be handled? A. Criticality B. Sensitivity C. Integrity D. Value
6. Which of the following is not a typical commercial data classification level? A. Sensitive B. Confidential C. Secret D. Public
7. Which of the following represents data shared only within a meeting in the TLP system? A. Amber B. White C. Red D. Green
8. Which of the following is a standard used by the security automation community used to enumerate software flaws and configuration issues? A. TLP B. CIA C. SCAP D. CAN
9. Which of the following is not a metric group in the Common Vulnerability Scoring System? A. Base B. Access vector C. Temporal D. Environmental
10. Which of the following is the monetary impact of each threat occurrence? A. ALE B. AV C. ARO D. SLE
11. Which method of handling risk involves defining the acceptable risk level the organization can tolerate and reducing the risk to that level? A. Avoidance B. Mitigation C. Acceptance D. Transfer
12. What part of the campus area network includes the end devices and provides them with access to the outside world and to the Intranet data center through the enterprise core? A. Intranet data center B. Enterprise campus C. Enterprise core D. Enterprise WAN edge
13. Which of the following is an area where you can place a public server for access by anyone? A. Intranet B. DMZ C. Internet D. Extranet
14. Which of the following is a logical subdivision of a switch that segregates ports from one another? A. VLAN B. VPN C. DMZ D. STP
15. Which of the following refers to the data being unaltered by unauthorized individuals? A. Confidentiality B. Integrity C. Availability D. Accountability
16. Which of the following refers to the practice of using multiple layers of security between data and the resources on which it resides and possible attackers? A. Default to no access B. Defense in depth C. Separation of duties D. Job rotation
17. Which of the following is the probability that a threat agent will exploit a vulnerability and the impact if the threat is carried out? A. Risk B. Threat C. Exposure D. Countermeasure
18. Which of the following is a system that uses traffic light colors to classify information assets? A. DLP B. VLAN C. TLP D. VTP
19. Which component of SCAP refers to vulnerabilities in published operating systems and applications software? A. CWE B. CVE C. CCE D. CPE
20. Which of the following is the percent value or functionality of an asset that will be lost when a threat event occurs? A. SLE B. AV C. EF D. ALE

Exam Essentials

**Describe attack motivations.** :These include financial gain, disruption, geopolitical change, and notoriety. They may be attempted by organized crime groups, state sponsors, terrorist groups, hacktivists, and thrill hackers.

**Identify common network attacks.:** These include but are not limited to IP address spoofing, MAC address spoofing, and email spoofing. They also include password attacks such as dictionary and brute-force attacks. Finally, explain reconnaissance attacks such as ping scans, port scans, and SYN scans.

**Explain social engineering attacks:.** Describe phishing and pharming attacks and how these attacks can lead to malware such as viruses, worms, and Trojan horses.

**Define the types of information most susceptible to data exfiltration**:. These include personally identifiable information (PII), intellectual property, and credit card information. Provide examples for each type of data.

Review Questions

1. What is the typical motivation of a hacktivist? A. Financial gain B. Disruption C. Geopolitical change D. Notoriety

2. Which of the following attacks has as its goal to get through an ACLon a router? A. IP address spoofing B. MAC address spoofing C. Email spoofing D. Buffer overflow

3. Which of the following is not a form of password attack? A. Brute force B. Dictionary C. Port scan D. Social engineering

4. When executing a NULLscan, which response indicates the port is closed on the target? A. No response B. Destination unreachable C. RST D. ACK

5. Which of the following is a measure used to prevent buffer overflows? A. Input validation B. Multifactor authentication C. Complex passwords D. Sensitivity labels

6. Which of the following is not a DDoS attack? A. SYN flood B. Ping of death C. Smurf attack D. Man-in-the-middle

7. Which of the following is typically used to set up a man-in-the-middle attack? A. ARP poisoning B. Dynamic ARP inspection C. Rogue switches D. MAC overflow

8. Which of the following is mitigation for ARP poisoning? A. Input validation B. DAI C. Multifactor authentication D. Rootguard

9. Which of the following must be implemented to use DAI? A. DTP B. Authenticated ARP C. DHCP snooping D. NAT

10. Which of the following attaches itself to another application to replicate or distribute itself? A. Worm B. Rootkit C. Spyware D. Virus

11. Which of the following is considered to be a unique creation of the mind? A. PII B. IP C. PHI D. IPS

12. Which of the following provides recommendations for securely handling credit card data? A. HIPAA B. SOX C. PCI-DSS D. GLBA

13. At what OSI layer does MAC address spoofing occur? A. 1 B. 2 C. 3 D. 4

14. Which of the following is mitigation for email spoofing? A. SPF B. DAI C. DNSSec D. DHCP snooping

15. Which of the following is a common tool used for ping and port scans? A. Metasploit B. Nmap C. Netstat D. Snort

16. Which of the following is not a flag set in an XMAS scan? A. FIN B. PSH C. SYN D. URG

17. Which of the following attacks uses an oversized ICMP packet? A. Ping of death B. Smurf C. Fraggle D. SYN flood

18. Which of the following is a reflected DDoS attack? A. Ping of death B. Smurf C. Buffer overflow D. XXS

19. Which attack type does DAI address? A. IP spoofing B. MAC overflow C. ARP poisoning D. Ping of death

20. Which of the following pollutes the contents of a computer’s DNS cache so that requests to a legitimate site are actually routed to an alternate site? A. Phishing B. Pharming C. Vishing D. Whaling

Exam Essentials

**Differentiate between symmetric and asymmetric key cryptography**. This includes the types of keys used, the scenarios in which they are used, and the disadvantages and advantages of each.

**Describe the hashing process**. This includes how hashing algorithms work, examples of hashing algorithms, and the role of hashing in digital signatures.

**Explain the role of a PKI**. Describe the components of a PKI, the certificate enrollment process, and the use of public and private keys in the process.

**Define cryptanalytic attacks.** These include ciphertext-only attack, chosen plaintext, chosen ciphertext, brute force, birthday, and meet-in-the-middle.

Review Questions

1. Which of the following is not true of symmetric algorithms? A. They use a public key. B. They are faster than asymmetric algorithms. C. They present key exchange issues. D. They are typically used for data at rest.

2. Which of the following is not true of asymmetric algorithms? A. They provide automatic key exchange. B. They are typically used for data at rest. C. They use a private and public key. D. They are slower than symmetric algorithms.

3. Which of the following is not an advantage of block ciphers? A. The implementation is easier than stream-based cipher implementation. B. Generally they are less susceptible to security issues. C. Generally they are used more in software implementations. D. They employ only substitution.

4. Which of the following ciphers perform encryption on a bit-by-bit basis? A. Block B. Stream C. Asymmetric D. Polyalphabetic

5. Which of the following is used to ensure that patterns are not produced during encryption? A. IVs B. HMAC C. RC4 D. Salting

6. In which of the following modes of DES is every 64-bit block encrypted with the same key? A. CBC B. ECB C. ECC D. CFB

7. Which of the following is the replacement algorithm for 3DES? A. Blowfish B. AES C. IDEA D. RC4

8. Which of the following is the most popular asymmetric algorithm? A. RSA B. El Gamal C. DSA D. ECC

9. Which of the following occurs when a hash function produces the same hash value on different messages? A. Birthday attack B. Key exposure C. Collision D. Substitution

10. Which of the following hashing algorithms is required by the U.S. government? A. MD4 B. MD5 C. SHA1 D. SHA

11. Which of the following can help to reduce the collision rate of the hash function? A. MAC B. HMAC C. Digital signatures D. Substitution

12. Which of the following is a hash value encrypted with the sender’s private key? A. Salt B. Nonce C. Digital signature D. HMAC

13. Which of the following is true of a hybrid cryptosystem? A. Asymmetric algorithms are used for the key exchange. B. Symmetric keys are used for the key exchange. C. Asymmetric keys are used for the data encryption. D. Asymmetric keys are exchange automatically.

14. Which of the following is a digital document binding a key pair to an entity? A. Certificate B. Nonce C. Salt D. IV

15. Which of the following is the standard for digital certificates? A. X.500 B. X.509 C. IEEE 509 D. RFC 500

16. Which of the following is a list of digital certificates that a CA has revoked? A. OSCP B. CRL C. SCEP D. REVC

17. Which of the following certificate classes is for individuals intended for email? A. 1 B. 2 C. 3 D. 4

18. Which of the following PKI components verifies the requestor’s identity? A. CA B. RA C. DN D. CN

19. Which of the following can be used to allow one root CA to trust another root CA’s certificates? A. Subordination B. Cross certification C. Certlink D. Trust

20. What type of certificate does the ASA use out of the box? A. Public B. Self-signed C. Globally trusted D. Locally trusted

Exam Essentials

Identify the security services provided by IPsec. They include confidentiality, integrity, origin authentication, anti-replay, and key management.

List the components and delivery modes of IPsec. These include ISAKMP, IKE, AH, and ESP. Delivery modes include transport and tunnel mode.

Describe the operation of hairpinning. Hairpinning can be used to allow traffic between two hosts to connect to the same VPN interface. It is required because of the default rule that an ASA will not forward packets back out the same interface in which they were received.

Describe the operation of split tunneling. When enabled, it allows a user to have the tunnel up and use the same interface to access the Internet without traversing the tunnel. Review Questions

1. Which IPsec component provides confidentiality? A. AH B. IKE C. ESP D. ISAKMP

2. Which IPsec component provides integrity? A. HMAC B. IKE C. ESP D. ISAKMP

3. Which IPsec component provides only data integrity, origin authentication, and anti-replay protection? A. HMAC B. AH C. ESP D. ISAKMP

4. Which IPsec component provides key exchange? A. HMAC B. AH C. Diffie-Hellman D. ISAKMP

5. What is the minimum key length for Suite B algorithms? A. 64-bit B. 80-bit C. 128-bit D. 160-bit

6. What hashing algorithm is required by the Suite B standard? A. MD5 B. SHA-1 C. SHA-2 D. AES

7. Which of the following is not a function of IKE? A. Automatic key generation B. Automatic key refresh C. key exchange D. Negotiation of the security association (SA)

8. Which of the following does not occur in phase 1 of IKE? A. Negotiates the policy sets. B. Sets up a secure channel. C. Authenticates the peer devices to one another. D. The IPsec transform set is negotiated.

9. Which of the following is true of the Main and Aggressive IKE modes? A. Main mode uses two messages, and Aggressive mode uses three. B. Main mode uses three messages, and Aggressive mode uses two. C. Both modes use three messages. D. Both modes use two messages.

10. Which of the following is not performed during IKE phase 2? A. Periodic renegotiation of the SA. B. The SA is established. C. The IPsec transform set is negotiated. D. The Diffie-Hellman protocol is used to generate a shared symmetric key.

11. Which of the following is not true of IKEv2 when compared with IKEv1? A. More transactions that result in decreased speed B. Stronger security through denial-of-service protection C. Supports EAP as an authentication method D. Incorporates extensions such as NAT traversal and dead peer detection

12. When using AH in transport mode, which parts of the packet are authenticated? A. Only the header B. Only the payload C. Header and payload D. None

13. When using ESP in tunnel mode, which parts of the packet are encrypted? A. Only the header B. Only the payload C. Header and payload D. None

14. Which if the following is not true of IPsec in IPv6 and IPv4? A. IPsec is required in IPv6. B. In IPv4, AH and ESP are implemented as IP protocol headers. C. In IPv6, extension headers are used to implement IPsec. D. In IPv6, the extension header lies between the IPv6 header and the payload.

15. Which of the following is true? A. By default, an ASA will not forward packets back out the same interface in which it was received. B. By default, an ASA will forward packets back out the same interface in which it was received. C. Once a tunnel is operational, all traffic leaving the VPN client need not pass through the tunnel. D. In IPv4, AH and ESP are implemented as IP protocol headers.

16. Which of the following features can be used to allow traffic to re-enter the end of an IPsec tunnel? A. Split horizon B. Hairpinning C. Split tunnel D. Poison reverse

17. Which feature, when enabled, allows a user to have the tunnel up and use the same interface to access the Internet without traversing the tunnel? A. Split horizon B. Hairpinning C. Split tunnel D. Poison reverse

18. Which additional feature must be enabled to use Always-on VPN? A. MDM B. Trusted network detection C. Hairpinning D. STP

19. What feature encapsulates IPsec within UDP? A. NAT-T B. DNSSec C. Split tunnel D. Trusted network detection

20. What protocol number is used for ESP? A. 48 B. 49 C. 50 D. 51