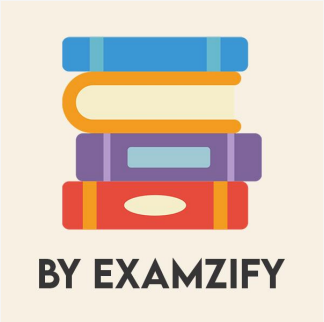
University of Central Florida (UCF) CIS3360 Security in Computing Final Practice Exam (Sample)

Study Guide



Everything you need from our exam experts!

Questions

1. What type of packet does the server send in response to a client's connection request?

   A. ACK packet

   B. SYN/ACK packet

   C. Connection packet

   D. Data packet

2. Where is NAT usually implemented in a network setup?

   A. Between two private networks

   B. On the public internet

   C. Between the private network and the public network

   D. On user devices directly

3. What is the main risk associated with session hijacking?

   A. Increased latency

   B. Data integrity loss

   C. Unauthorized user access to active sessions

   D. Reduced network performance

4. What is a common form of cyber attack that uses a network of compromised systems?

   A. Social engineering

   B. Phishing

   C. DDoS attack

   D. Malware infection

5. What is the primary focus of NAT technology?

   A. Enhancing security

   B. Increasing bandwidth

   C. Conserving IP address space

   D. Improving latency

6. What is one of the functions of a rogue access point (AP)?

A. To Secure Network Connections

B. To Enhance Wireless Coverage

C. To Intercept Contained Data

D. To Improve Signal Strength

7. What is paid to a patent holder for lost profits due to infringement?

A. Compensation funds

B. Legal compensation

C. License fees

D. Royalty payments

8. What does "security by obscurity" refer to?

A. A strong security measure using encryption

B. A misguided strategy relying on system secrecy

C. A practice of regularly updating security policies

D. A method for educating users about security

9. What does public key infrastructure (PKI) manage?

A. Digital certificates and public-key encryption

B. Firewall configurations and settings

C. Network security protocols

D. User authentication processes

10. What is a potential outcome of effective penetration testing?

A. Increased network speed

B. Identification of security gaps before exploitation

C. Reduction of employee turnover

D. Improved software redundancy

Answers

1. B
2. C
3. C
4. C
5. C
6. C
7. B
8. B
9. A
10. B

Explanations

1. What type of packet does the server send in response to a client's connection request?

A. ACK packet

B. SYN/ACK packet

C. Connection packet

D. Data packet

When a client initiates a connection request to a server in the context of the Transmission Control Protocol (TCP), the server's response is a SYN/ACK packet. This is part of the three-way handshake process that establishes a TCP connection. Initially, the client sends a SYN packet to indicate a desire to establish a connection. Upon receiving this SYN packet, the server responds not only to acknowledge the receipt of the SYN but also to indicate that it is ready to establish a connection. Therefore, it sends a SYN/ACK packet, combining both the synchronization (SYN) to request a connection and acknowledgment (ACK) to confirm the receipt of the client's request. The SYN/ACK packet signifies that the server is actively participating in the connection establishment process and is prepared to communicate further. Following this, the client will send an ACK packet back to the server to complete the handshake, resulting in a fully established connection. The other types of packets listed are not relevant in this context: an ACK packet is simply an acknowledgment of received data but does not initiate a connection; a connection packet is not a formally defined packet type in the TCP/IP suite; and a data packet pertains to the actual data transfer after the connection has been established, not the initial handshake process

2. Where is NAT usually implemented in a network setup?

A. Between two private networks

B. On the public internet

C. Between the private network and the public network

D. On user devices directly

Network Address Translation (NAT) is primarily implemented in a network setup at the boundary where a private network connects to a public network, typically the internet. The main function of NAT is to allow multiple devices on a private network to share a single public IP address when accessing external networks. When devices on a private network (like a home or office network) make requests to the internet, their private IP addresses are not routable on the public internet. The NAT device, often a router, translates these private addresses to the public IP address assigned to the network. This process helps to conserve the number of public IP addresses used and provides an additional layer of security by keeping the internal IP addresses hidden from external entities. Additionally, implementing NAT between private networks or solely on user devices does not fulfill its designed purpose of facilitating communication with external networks. Similarly, while NAT interacts with the public internet, it is not usually set up *on* the internet, but rather in the infrastructure that connects private networks to it.

3. What is the main risk associated with session hijacking?

A. Increased latency

B. Data integrity loss

C. Unauthorized user access to active sessions

D. Reduced network performance

The primary risk linked to session hijacking is unauthorized user access to active sessions. Session hijacking occurs when an attacker takes over a user's active session, which can happen through various methods such as stealing session cookies or exploiting vulnerabilities in the application that manages sessions. Once an attacker gains control of a session, they can perform any actions that the legitimate user can, often without any additional authentication. This can lead to severe security breaches, as sensitive information may be accessed, modified, or even deleted without the user's consent or knowledge. Other options relate to concerns that might arise in different contexts but do not capture the core issue with session hijacking as effectively as the risk of unauthorized access does. For example, increased latency and reduced network performance are performance-related issues, while data integrity loss refers more to the corruption or unauthorized alteration of data rather than the unauthorized access aspect of session hijacking. Thus, the focus on unauthorized access encapsulates the most significant risk associated with this attack vector.

4. What is a common form of cyber attack that uses a network of compromised systems?

A. Social engineering

B. Phishing

C. DDoS attack

D. Malware infection

A Distributed Denial of Service (DDoS) attack is a prevalent form of cyber attack that utilizes a network of compromised systems, commonly referred to as a botnet. In a DDoS attack, the attacker orchestrates a large volume of traffic from multiple sources to overwhelm a targeted system, such as a web server, causing it to become slow or completely inaccessible to legitimate users. This massive influx of traffic is made possible because the compromised systems, or bots, act in unison to bombard the target with requests, effectively disrupting its ability to function correctly. Understanding DDoS attacks is crucial in cybersecurity, as they can lead to significant downtime for organizations, financial losses, and damage to reputation. Recognizing that DDoS attacks are distinct in their method—leveraging a distributed set of compromised devices—is important, especially when differentiating them from approaches that involve single points of attack or social manipulation tactics, such as social engineering or phishing, which do not require a network of compromised systems.

5. What is the primary focus of NAT technology?

A. Enhancing security

B. Increasing bandwidth

C. Conserving IP address space

D. Improving latency

The primary focus of NAT (Network Address Translation) technology is conserving IP address space. NAT allows multiple devices on a local network to be mapped to a single public IP address, which effectively reduces the number of public IP addresses required for a network. This is especially significant given the limited availability of IPv4 addresses. By using private IP addresses internally and translating them to a single public address for external communication, NAT enables better utilization of the finite pool of available IP addresses. In addition to conserving IP address space, NAT provides other benefits, such as moderate increases in security by obscuring internal network structures from external view and simplifying network management. However, these secondary benefits stem from its primary function of address conservation, not the other aspects, such as bandwidth enhancement or latency improvement, which are not directly related to the core purpose of NAT technology.

6. What is one of the functions of a rogue access point (AP)?

A. To Secure Network Connections

B. To Enhance Wireless Coverage

C. To Intercept Contained Data

D. To Improve Signal Strength

A rogue access point functions primarily to intercept contained data. This type of access point is typically set up without proper authorization and can mimic a legitimate access point in order to deceive unsuspecting users into connecting to it. Once users connect, the rogue access point can capture sensitive information such as login credentials, personal data, and other sensitive communications transmitted over the network. This capability highlights the significant security threat posed by rogue access points, as they can facilitate various types of attacks, including man-in-the-middle attacks, leading to data breaches and loss of confidentiality. Therefore, understanding the risks associated with rogue access points is crucial for maintaining secure wireless networks.

7. What is paid to a patent holder for lost profits due to infringement?

A. Compensation funds

B. Legal compensation

C. License fees

D. Royalty payments

The compensation paid to a patent holder for lost profits due to infringement is known as legal compensation. This refers specifically to the financial restitution that a patent holder seeks in a legal context when they can demonstrate that their profits have been adversely affected by another party's unauthorized use of their patented invention. Such legal compensation can include not only the lost profits that the patent holder would have made had the infringement not occurred but also any additional damages that the court deems appropriate. This concept is important in intellectual property law, as it provides a means for patent holders to seek justice and recovery for economic harm caused by infringement. While license fees and royalty payments may involve compensation for use of a patent, these terms are generally associated with authorized agreements where the patent holder is willingly allowing use of their invention in exchange for payment. Legal compensation, in this instance, specifically addresses the harm and losses that arise from infringement actions without permission.

8. What does "security by obscurity" refer to?

A. A strong security measure using encryption

B. A misguided strategy relying on system secrecy

C. A practice of regularly updating security policies

D. A method for educating users about security

"Security by obscurity" refers to a misguided strategy that relies on the assumption that keeping the details of a system's security measures secret will protect it from threats and vulnerabilities. This approach often involves hiding the inner workings of a security mechanism, such as proprietary algorithms or unique configurations, with the belief that if potential attackers do not know how a system works, they cannot compromise it. This strategy is often criticized because security should not solely depend on secrecy; rather, it should involve robust safeguards that remain effective even when the system's details are publicly known. A well-designed security system should utilize best practices that include strong encryption, regular updates, user education, and especially defense mechanisms that are resilient to potential attacks, regardless of whether an attacker knows the system's specifics. In contrast, the other choices represent different aspects of security practices. Strong security measures that utilize encryption stand on sound principles of cryptography that maintain secure data regardless of transparency about the algorithm. Regularly updating security policies is a critical part of maintaining a secure environment rather than relying on obscurity. Educating users about security helps build overall awareness and reinforces security measures, which is essential in preventing human error that can lead to breaches.

9. What does public key infrastructure (PKI) manage?

A. Digital certificates and public-key encryption

B. Firewall configurations and settings

C. Network security protocols

D. User authentication processes

Public Key Infrastructure (PKI) is fundamentally designed to manage digital certificates and public-key encryption. This technology forms the backbone of secure communications and transactions over the internet. By utilizing asymmetrical cryptography, PKI enables users to securely exchange information and authenticate identities. Digital certificates serve to confirm that a public key belongs to a specific individual or entity, effectively binding the public key to the identity of the certificate holder. This ensures that users can trust the origin of the public key, which is crucial when establishing secure channels for data transmission. The role of PKI extends to managing the lifecycle of digital certificates, which includes their issuance, renewal, suspension, and revocation. This lifecycle management is essential to ensure that any user's keys remain valid and trustworthy, especially in environments where security is paramount. While options related to firewall configurations, network security protocols, and user authentication processes play significant roles in an organization's overall security posture, they do not encapsulate the primary functions of PKI as directly as digital certificates and public-key encryption do. Therefore, the emphasis on managing these specific elements marks option A as the most accurate and relevant choice regarding PKI.

10. What is a potential outcome of effective penetration testing?

A. Increased network speed

B. Identification of security gaps before exploitation

C. Reduction of employee turnover

D. Improved software redundancy

Effective penetration testing serves as a proactive security measure designed to identify vulnerabilities and security gaps within a system or network before they can be exploited by malicious actors. By simulating attacks, penetration testers can uncover weaknesses related to security configurations, outdated software, and potential entry points for attackers. This process allows organizations to address and remediate these vulnerabilities, thereby strengthening their overall security posture and preventing breaches that could lead to data loss or financial damage. While increased network speed, reduction of employee turnover, and improved software redundancy might be beneficial aspects of an organization's operation, they are not direct outcomes derived from the effective implementation of penetration testing. The primary purpose of this testing is to enhance security by identifying and addressing gaps, making the identification of security gaps before exploitation the most relevant and significant outcome in this context.