Certified Ethical Hacker Certification (CEHv10) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. Visit https://cehv10.examzify.com

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **What is an XML External Entity attack?**
    - **A. An attack utilizing a buffer overflow vulnerability**
    - **B. An attack that leverages a poorly configured XML parser**
    - **C. An attack that installs malware through email attachments**
    - **D. An attack targeting server-side logic flaws**

2. **Which type of attack allows extraction of information by injecting true/false queries?**
    - **A. Blind SQL injection**
    - **B. Cross-site scripting**
    - **C. Command injection**
    - **D. Denial of service**

3. **What protocol does WPA2-Enterprise use for authentication?**
    - **A. RADIUS**
    - **B. LDAP**
    - **C. EAP**
    - **D. HTTPS**

4. **What is the aim of enumeration in network security?**
    - **A. To protect against viruses and malware**
    - **B. To extract information by creating active connections**
    - **C. To map out firewall rules**
    - **D. To monitor network traffic for anomalies**

5. **Which item is NOT typically covered under a security policy?**
    - **A. Authentication**
    - **B. Human resources policies**
    - **C. Encryption**
    - **D. Firewalls**

6. What defines an out-of-band SQL injection attack?

- **A. Using only one channel for attack**
- **B. Using multiple channels to inject queries**
- **C. Executing SQL queries in an isolated environment**
- **D. Restricting access to manipulation**

7. What does Thin Whois provide?

- **A. Extensive domain registration details**
- **B. Limited information about a specified set of data**
- **C. A comprehensive security audit**
- **D. Real-time traffic analysis**

8. Open System Authentication (OSA) is utilized in the context of which type of network access?

- **A. WPA wireless networks**
- **B. VPN connections**
- **C. WEP protocol Wi-Fi networks**
- **D. Ethernet wired networks**

9. What do technical security policies define?

- **A. The legal framework for cybersecurity operations**
- **B. The system configuration for security protocols**
- **C. The employee roles in security management**
- **D. The physical security measures for devices**

10. What is the primary objective of a Security Incident and Event Management (SIEM) system?

- **A. Data encryption during transmission**
- **B. Identifying and analyzing security incidents**
- **C. Optimizing network performance**
- **D. Backup and recovery of data**

Answers

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

Explanations

1. What is an XML External Entity attack?

A. An attack utilizing a buffer overflow vulnerability

B. An attack that leverages a poorly configured XML parser

C. An attack that installs malware through email attachments

D. An attack targeting server-side logic flaws

An XML External Entity (XXE) attack specifically targets weaknesses found in the parsing of XML data structures by applications. When an XML parser is misconfigured or poorly handled, it may allow an attacker to include external entities in their XML input. This can lead to unauthorized access to files on the server, expose sensitive information, or interact with internal services. In the context of XXE, well-formed XML can contain a reference to an external entity. If the XML parser is not set up to handle such entities securely, it may process them in a way that grants the attacker access to files or other resources on the server. This type of intrusion can result in data leaks, denial of service, or even a complete takeover of the application’s logic. Understanding this helps to emphasize the importance of properly configuring XML parsers and applying security controls to mitigate potential vulnerabilities associated with XML processing. Hence, the correct identification of a poorly configured XML parser as the avenue for an XXE attack is fundamental to grasping how these attacks can be executed and the necessary precautions to implement against them.

2. Which type of attack allows extraction of information by injecting true/false queries?

A. Blind SQL injection

B. Cross-site scripting

C. Command injection

D. Denial of service

Blind SQL injection is a type of attack where an attacker can send queries to a database, but the information returned is limited, typically only confirming whether the queries return true or false. Unlike standard SQL injection, where the attacker can directly see the output of their queries, blind SQL injection relies on evaluating the application's behavior based on the responses or delays. In a blind SQL injection attack, the attacker constructs queries to infer data based on the responses from the application. For instance, the attacker might ask if a particular value exists in the database and then check the application's response to determine if the answer is true or false. This method allows the extraction of sensitive information, such as usernames or passwords, albeit in a roundabout and less efficient manner. This form of attack is particularly dangerous because it can be conducted without the attacker needing to see direct database responses, making it harder to detect and mitigate. It showcases the importance of implementing secure coding practices and robust input validation to prevent unauthorized access to database systems.

3. What protocol does WPA2-Enterprise use for authentication?

A. RADIUS

B. LDAP

C. EAP

D. HTTPS

WPA2-Enterprise primarily utilizes the Extensible Authentication Protocol (EAP) for authentication. This protocol serves as a framework that supports various authentication methods, such as EAP-TLS, EAP-TTLS, PEAP, and others, allowing for secure and flexible authentication in wireless networks. In the context of a WPA2-Enterprise environment, EAP is crucial because it enables the use of other protocols, such as RADIUS, to facilitate authentication against a centralized server. This centralized authentication is essential for enterprise environments where multiple users and devices need to be authenticated in a scalable manner. While options like RADIUS are often used in conjunction with EAP for authenticating users by forwarding authentication requests to an authentication server, EAP itself is specifically recognized as the method that defines the procedures and policies for how authentication data is exchanged. This makes EAP the core component of the authentication process in WPA2-Enterprise setups.

4. What is the aim of enumeration in network security?

A. To protect against viruses and malware

B. To extract information by creating active connections

C. To map out firewall rules

D. To monitor network traffic for anomalies

The aim of enumeration in network security is to extract information by creating active connections. Enumeration is a process that involves gathering detailed information about a target network or system, which often requires connecting to various services and protocols to retrieve data such as user accounts, groups, and network shares. This information can be vital for an attacker to identify potential vulnerabilities and plan further attacks. By actively probing systems and collecting this information, an ethical hacker can pinpoint weak areas that could be exploited, thereby allowing organizations to take proactive measures to secure their networks. This phase typically follows scanning, where initial reconnaissance is performed to identify live hosts and services. The other aspects mentioned in the choices pertain to different facets of network security. Protecting against viruses and malware focuses on defensive measures rather than information gathering. Mapping out firewall rules involves analyzing and creating diagrams of network security policies but does not inherently involve active information extraction. Monitoring network traffic for anomalies is a crucial part of detection and response, aimed at identifying suspicious activity rather than the enumeration process itself.

5. Which item is NOT typically covered under a security policy?

A. Authentication

B. Human resources policies

C. Encryption

D. Firewalls

Human resources policies are generally not regarded as a direct component of a security policy. While security policies focus on the technical and procedural aspects of safeguarding information and systems—such as authentication, encryption, and firewalls—human resources policies relate more to the broader management of personnel and workplace guidelines. These might include hiring practices, employee conduct, and benefits, which are important but fall outside the typical scope of a technical security policy aimed specifically at protecting assets from threats. In contrast, authentication involves verifying the identity of individuals accessing systems, encryption secures data from unauthorized access, and firewalls are mechanisms to control incoming and outgoing network traffic based on predetermined security rules, all of which are integral components of a robust security framework.

6. What defines an out-of-band SQL injection attack?

A. Using only one channel for attack

B. Using multiple channels to inject queries

C. Executing SQL queries in an isolated environment

D. Restricting access to manipulation

An out-of-band SQL injection attack is characterized by using multiple channels to inject queries and retrieve data. This type of attack often involves the attacker sending a SQL injection payload in a way that relies on a different communication channel than the one being exploited. For example, the attacker might use HTTP requests to execute SQL commands and then extract data via DNS or another protocol. This approach is particularly valuable when the application's response is not sufficient to capture the needed information directly or when the attacker wants to avoid detection by traditional monitoring systems. In contrast, other options do not align with the definition of out-of-band attacks. Using only one channel limits the attack's effectiveness and prevents it from being classified as out-of-band. Executing SQL queries in an isolated environment pertains more to controlled testing rather than an attack method. Lastly, restricting access to manipulation does not represent the nature of how out-of-band SQL injections operate, as they typically seek to exploit and manipulate databases rather than limit access. The focus of out-of-band attacks is on leveraging multiple channels for data extraction and query execution.

7. What does Thin Whois provide?

A. Extensive domain registration details

B. Limited information about a specified set of data

C. A comprehensive security audit

D. Real-time traffic analysis

Thin Whois provides limited information about a specified set of data, typically offering only the bare minimum required to identify the registrant of a domain. This includes essential details like the domain name, registrar, registration dates, and sometimes basic contact information. Unlike a more comprehensive "thick" Whois database, which contains detailed registrant information, Thin Whois restricts data presentation, focusing on basic transparency while protecting more sensitive registrant details. This approach to domain information helps balance the need for public access to certain registration details with the privacy concerns of individuals and organizations. Therefore, when you think of Thin Whois, it's crucial to recognize its role in providing restricted access to domain registration details but generally lacking depth compared to its thicker counterpart. This understanding is particularly relevant for ethical hackers and cybersecurity professionals who may need to gather information on domains while considering privacy implications.

8. Open System Authentication (OSA) is utilized in the context of which type of network access?

A. WPA wireless networks

B. VPN connections

C. WEP protocol Wi-Fi networks

D. Ethernet wired networks

Open System Authentication (OSA) is a method used primarily in WEP (Wired Equivalent Privacy) protocol Wi-Fi networks to manage how devices gain access to the wireless network. In the context of OSA, the authentication process is relatively simple—any device that sends an authentication request will be granted access without any requirement for credentials or pre-shared keys, making it easy for devices to connect to the network. WEP networks implement OSA for their authentication processes, allowing clients to connect without the need for complex encryption or key management. This contrasts with more secure protocols, such as WPA (Wi-Fi Protected Access), which use more advanced forms of authentication that require mutual authentication between client and the access point, ensuring higher levels of security. On the other hand, VPN connections and Ethernet wired networks typically have their own specific authentication methods that are more secure and require user credentials or pre-established keys. Thus, they do not utilize OSA in their authentication processes.

9. What do technical security policies define?

A. The legal framework for cybersecurity operations

B. The system configuration for security protocols

C. The employee roles in security management

D. The physical security measures for devices

Technical security policies are critical documents that outline how an organization's IT resources should be secured and protected from various threats. The primary focus is on system configuration, which includes detailed guidelines about security protocols. This encompasses the standards, methodologies, and tools that should be employed to safeguard data and systems. These policies often specify configurations for firewalls, intrusion detection systems, encryption methodologies, and access controls. By defining these parameters, technical security policies ensure that technical controls are implemented effectively and consistently across the organization. This structured approach not only helps in maintaining a robust security posture but also facilitates compliance with relevant regulations and industry standards. Other aspects presented in the choices involve the legal framework, employee roles, and physical security. While these are essential components of an overall security strategy, they do not fall under the primary focus of technical security policies, which center distinctly on the technical configurations necessary for safeguarding information systems.

10. What is the primary objective of a Security Incident and Event Management (SIEM) system?

A. Data encryption during transmission

B. Identifying and analyzing security incidents

C. Optimizing network performance

D. Backup and recovery of data

A Security Incident and Event Management (SIEM) system is primarily designed to identify and analyze security incidents within an organization's network and IT environment. SIEM systems collect and aggregate log data from various sources, such as servers, network devices, and security appliances, allowing for real-time analysis of security alerts generated by applications and network hardware. The primary functions of a SIEM system include correlating events from different sources to detect patterns indicative of potential security threats, enabling security teams to respond to incidents swiftly and effectively. By continuously monitoring and assessing security-related data, a SIEM enhances an organization's ability to quickly identify breaches, anomalies, or policy violations, thereby improving its overall security posture. While data encryption during transmission, optimizing network performance, and backup and recovery of data are all important aspects of information security and IT management, they are not the core functions of a SIEM system. SIEM focuses specifically on security incident identification and analysis, which is why that choice accurately reflects its primary objective.