Ethical Hacking Essentials Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What is characterized by obtaining information from various victims to create a new identity?

A. Synthetic Identity Theft

B. Identity Cloning

C. Financial Identity Theft

D. Medical Identity Theft

2. What happens to a switch when it enters fail-open mode?

A. It routes packets intelligently

B. It starts acting as a hub

C. It blocks network traffic

D. It denies all new connections

3. What type of attack leads to system crashes and creates a denial of service?

A. Distributed Denial-of-Service (DDoS)

B. Phishing

C. SQL Injection

D. Man-in-the-browser attack

4. In a social engineering context, what is the main goal of impersonation attacks?

A. To access physical locations

B. To deceive and manipulate individuals

C. To gather intelligence on a company

D. To spread malware

5. Which is NOT a countermeasure against web server attacks?

A. Screen and filter incoming requests

B. Update server software regularly

C. Install IIS server on a domain controller

D. Use secure passwords

6. Which cloud computing model offers penetration testing and anti-malware services?

- **A. Infrastructure-as-a-Service**
- **B. Platform-as-a-Service**
- **C. Security-as-a-Service**
- **D. Function-as-a-Service**

7. How can employees prevent unauthorized access to their devices in a BYOD policy?

- **A. Use easily remembered passwords**
- **B. Connect to public Wi-Fi often**
- **C. Implement password protection and encryption**
- **D. Share devices among colleagues**

8. What method does a penetration tester employ to identify network and service vulnerabilities?

- **A. Data enrichment**
- **B. Network segmentation**
- **C. Scalability testing**
- **D. Information gathering techniques**

9. Which Google advanced search operator can be used to find websites similar to a specified URL?

- **A. related**
- **B. site:**
- **C. link:**
- **D. info:**

10. How can 'jailbreaking' a device affect data security?

- **A. Enhances security measures**
- **B. Bypasses encryption protections**
- **C. Restricts access to sensitive data**
- **D. Defaults all settings to secure**

Answers

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

Explanations

1. What is characterized by obtaining information from various victims to create a new identity?

A. Synthetic Identity Theft

B. Identity Cloning

C. Financial Identity Theft

D. Medical Identity Theft

Synthetic identity theft is characterized by the combination of real and fictitious information to create a new identity. This typically involves obtaining personal details from various victims, such as their social security numbers, names, or addresses, and then blending this information with fabricated data to create a credible new identity. This process allows the perpetrator to establish a false identity which can be used for various fraudulent activities, such as applying for loans or opening credit accounts, often without raising immediate suspicion. The distinction between synthetic identity theft and other forms of identity theft lies in its method: while traditional identity theft might focus on stealing the entire identity of a single individual, synthetic identity theft leverages information from multiple sources to craft something new and deceptive. This makes it particularly challenging to detect because it can make use of a combination of legitimate and invented information, thus obscuring the identity of the fraudster from authorities and financial institutions. In contrast, identity cloning involves fully taking over someone else's identity, financial identity theft focuses specifically on illegally obtaining someone's financial information for economic gain, and medical identity theft relates to the misuse of someone's identity specifically within the healthcare system for medical services or benefits. Each of these forms has different implications and methods of execution, but synthetic identity theft is unique in its composite

2. What happens to a switch when it enters fail-open mode?

A. It routes packets intelligently

B. It starts acting as a hub

C. It blocks network traffic

D. It denies all new connections

When a switch enters fail-open mode, it begins to function similarly to a hub. In this state, the device stops performing the intelligent packet switching typically associated with switches and instead broadcasts incoming packets to all ports. This behavior mimics that of a hub, which does not have the capability to filter or intelligently route packets based on their destination MAC addresses. The fail-open mode is a safety feature designed to ensure that network connectivity is maintained, albeit in a less efficient manner. While this mode allows for continued communication between devices on the network, it sacrifices the benefits of a switching infrastructure, such as bandwidth management and reduced collision domains—characteristics that are essential for optimizing network performance. Understanding this mode is crucial for network administrators, as it highlights the importance of redundant systems and failover strategies to maintain network performance and security. In contrast, the other options describe behaviors not associated with a switch in fail-open mode, which highlight how they operate under normal and malfunctioning conditions.

3. What type of attack leads to system crashes and creates a denial of service?

A. Distributed Denial-of-Service (DDoS)

B. Phishing

C. SQL Injection

D. Man-in-the-browser attack

A Distributed Denial-of-Service (DDoS) attack is designed specifically to overwhelm a target's resources, such as a server or network, by flooding it with a massive amount of traffic from multiple sources. This flood of traffic can incapacitate the target system, rendering it unable to respond to legitimate requests. As a result, users may experience delays or complete unavailability of services, leading to the denial of service. DDoS attacks commonly utilize botnets, which are networks of compromised computers, to carry out the attack on a large scale. In contrast, the other types of attacks listed, such as phishing, SQL injection, and man-in-the-browser attacks, focus on different goals like stealing sensitive information, exploiting database vulnerabilities, or intercepting user sessions. While these attacks can compromise system integrity and privacy, they do not primarily aim to cause system crashes or result in a denial of service in the same manner as a DDoS attack does.

4. In a social engineering context, what is the main goal of impersonation attacks?

A. To access physical locations

B. To deceive and manipulate individuals

C. To gather intelligence on a company

D. To spread malware

Impersonation attacks in the context of social engineering primarily aim to deceive and manipulate individuals into providing sensitive information or performing actions that would typically not occur under normal circumstances. This form of attack leverages trust by impersonating a familiar or authoritative figure, such as a coworker, a manager, or a service provider. The attacker's ultimate goal is to exploit the target's willingness to help or comply due to their perceived legitimacy, which can lead to unauthorized access to sensitive data or systems, or even financial loss. The effectiveness of such attacks hinges on the psychological manipulation of the target rather than technological vulnerabilities. By creating a false sense of security, the attacker guides the target into divulging confidential information or compromising security protocols. Understanding this tactic is essential for recognizing and defending against such approaches in an organization. While accessing physical locations, gathering intelligence, or spreading malware can also be components of an overall social engineering strategy, they are not the primary focus of impersonation attacks. The essence of impersonation attacks lies in the interpersonal manipulation and deception involved, making persuading the individual the main target.

5. Which is NOT a countermeasure against web server attacks?

A. Screen and filter incoming requests

B. Update server software regularly

C. Install IIS server on a domain controller

D. Use secure passwords

The selection of installing IIS server on a domain controller as the option that is not a countermeasure against web server attacks is based on understanding the risks associated with this practice. Using IIS (Internet Information Services) on a domain controller can expose the server to unnecessary risk because domain controllers already carry critical authentication functions for the network. By installing a web server, you increase its attack surface, making it more susceptible to vulnerabilities, exploits, and potential breaches. A compromised web server on a domain controller could lead to significant security issues, including unauthorized access to sensitive information or manipulation of user credentials. In contrast, the other measures—screening and filtering incoming requests, regularly updating server software, and using secure passwords—are focused on enhancing the security posture of the web server itself. Effective filtering can block malicious traffic, updates ensure known vulnerabilities are patched, and strong passwords protect against unauthorized access. All these are established best practices aimed at mitigating web server attacks.

6. Which cloud computing model offers penetration testing and anti-malware services?

A. Infrastructure-as-a-Service

B. Platform-as-a-Service

C. Security-as-a-Service

D. Function-as-a-Service

The correct choice, Security-as-a-Service, is an essential model in cloud computing that specifically provides security measures including penetration testing and anti-malware services. This model focuses on security solutions offered via the cloud, allowing organizations to leverage these services without the need for extensive in-house security infrastructure. Security-as-a-Service is beneficial for organizations looking to enhance their cybersecurity posture, as it enables them to access specialized security expertise and tools efficiently and effectively. It also provides scalability, allowing businesses to adjust their security services according to their needs without significant upfront investments. The other cloud models do not focus specifically on security services. Infrastructure-as-a-Service primarily offers computing resources like virtual machines and storage, while Platform-as-a-Service provides a platform allowing developers to build applications without dealing with the underlying infrastructure management. Function-as-a-Service allows developers to run individual pieces of code in the cloud but doesn't inherently include bundled security services. Therefore, Security-as-a-Service stands out as the clear solution for penetration testing and anti-malware needs.

7. How can employees prevent unauthorized access to their devices in a BYOD policy?

A. Use easily remembered passwords

B. Connect to public Wi-Fi often

C. Implement password protection and encryption

D. Share devices among colleagues

Implementing password protection and encryption is a fundamental step in safeguarding devices against unauthorized access in a Bring Your Own Device (BYOD) environment. This practice ensures that even if a device is lost or stolen, sensitive data remains protected from unauthorized users. Strong passwords serve as the first line of defense against access attempts, while encryption adds a layer of security by converting data into a format that can only be read by authorized users with the correct decryption key. This combination makes it considerably more difficult for malicious actors to gain access to confidential information. Other methods listed, such as using easily remembered passwords or frequently connecting to public Wi-Fi, do not provide the same level of security. Weak passwords can be easily guessed or cracked, while public Wi-Fi networks are often insecure, exposing devices to various attacks. Sharing devices among colleagues poses additional risks, as it increases the likelihood of someone unintentionally accessing sensitive information or compromising security protocols. Thus, implementing password protection and encryption is the most effective way to enhance device security in a BYOD setting.

8. What method does a penetration tester employ to identify network and service vulnerabilities?

A. Data enrichment

B. Network segmentation

C. Scalability testing

D. Information gathering techniques

A penetration tester employs information gathering techniques as a foundational step in identifying network and service vulnerabilities. This method encompasses various activities designed to collect as much relevant data as possible about the target system or network before attempting to exploit any weaknesses. Information gathering can include techniques such as reconnaissance, where tools and processes are used to map out the network topology, identify open ports, and determine the services running on those ports. This phase provides a wealth of information that can lead to the identification of potential vulnerabilities, such as outdated software, exposed services, and misconfigurations that could be exploited during an attack. By systematically gathering information, penetration testers can make informed decisions about which weaknesses to target, helping them to better simulate a real-world attack scenario. This comprehensive approach ensures that they have a clear understanding of the environment they are working with, allowing for more effective vulnerability identification and subsequent remediation recommendations. The other options do not serve the primary purpose of identifying vulnerabilities in the same direct way. Data enrichment refers to enhancing existing data, network segmentation is about dividing a network into segments for performance or security reasons, and scalability testing assesses how well a system can handle increased loads, thus not directly focusing on vulnerability identification.

9. Which Google advanced search operator can be used to find websites similar to a specified URL?

A. related

B. site:

C. link:

D. info:

The advanced search operator that can be used to find websites similar to a specified URL is "related." When you use this operator in a Google search, you can input a specific webpage URL, and Google will return a list of websites that it deems similar in content or context to the provided URL. This operator is particularly useful for researchers, marketers, and anyone interested in exploring a topic further by identifying other sites that offer comparable information or services. Understanding how this operator functions allows users to discover new sources or competitors in a particular niche, making it a valuable tool for competitive analysis or content research. In contrast, the other operators serve different purposes: - The "site:" operator restricts search results to a specific domain, showing only pages within that website. - The "link:" operator (though less effective in recent updates) used to show pages that link to a specified URL, focusing on backlink analysis rather than similarity. - The "info:" operator provides information about a specific webpage, such as its cache and links to it, but does not identify similar websites. Thus, "related" is the appropriate choice for finding similar websites effectively.

10. How can 'jailbreaking' a device affect data security?

A. Enhances security measures

B. Bypasses encryption protections

C. Restricts access to sensitive data

D. Defaults all settings to secure

Jailbreaking a device primarily affects data security by bypassing the inherent security measures that the device's operating system imposes. When a device is jailbroken, the user gains unauthorized root access, which allows them to install applications and tweaks that are not approved by the official app store. This can undermine the built-in encryption protections that safeguard user data. By bypassing these protections, malware can more easily be installed on the device, which in turn can lead to unauthorized access to sensitive information such as personal files, passwords, and financial data. Jailbreaking ultimately opens up potential vulnerabilities that can be exploited by malicious actors, thus significantly compromising data security. In comparison, enhancing security measures, restricting access to sensitive data, and defaulting settings to secure are contrary to the implications of jailbreaking, as they are associated with maintaining or improving security rather than undermining it.