Ethical Hacking Essentials Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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

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

Questions

1. **What attack is characterized by sending a malicious text message to collect sensitive information from mobile devices?**

   A. Phishing

   B. SMiShing

   C. Vishing

   D. Malware injection

2. **What phase of hacking was Lopez performing if she finds vulnerabilities such as password cracking and denial of service?**

   A. Maintaining Access

   B. Gaining Access

   C. Reconnaissance

   D. Clearing Tracks

3. **Which protocol is utilized for accessing and manipulating electronic mail messages on a server?**

   A. Internet Message Access Protocol (IMAP)

   B. Network File System (NFS)

   C. Hypertext Transfer Protocol (HTTP)

   D. Secure Copy Protocol (SCP)

4. **Who is identified as a malicious insider likely to damage network security intentionally?**

   A. Disgruntled employee

   B. Negligent insider

   C. Compromised insider

   D. Professional insider

5. **During which phase of a social engineering attack do hackers typically research their target to identify vulnerabilities?**

   A. Exploit the relationship

   B. Select a target

   C. Research the target company

   D. Develop a relationship

6. What method can be used to mitigate side-channel attacks in cloud environments?

A. Only allow local memory access

B. Check for repeated access attempts to local memory

C. Implement strict user authentication

D. Activate firewall on all servers

7. 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

8. What type of attack did Alice launch against the manufacturing plant?

A. Ransomware

B. Spear Phishing

C. Malware attack

D. SQL Injection

9. What vulnerability arises from insecure data storage on mobile devices?

A. Dependence on user awareness of security

B. Assumptions about malware access to file systems

C. Overreliance on physical device security

D. Encryption of sensitive data only

10. In which hacking phase is Peter, who manages to gain control and uses techniques to stay undetected?

A. Scanning

B. Clearing Tracks

C. Gaining Access

D. Reconnaissance

Answers

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

Explanations

1. What attack is characterized by sending a malicious text message to collect sensitive information from mobile devices?

A. Phishing

B. SMiShing

C. Vishing

D. Malware injection

The focus of this question centers around the specific type of attack that involves sending malicious text messages to target individuals and gather sensitive information from their mobile devices. SMiShing is a term specifically coined to describe SMS phishing, where cybercriminals send text messages that appear legitimate but are designed to provoke recipients into providing personal details, such as passwords or financial information. These messages often contain links to fake websites or instruct the user to reply with sensitive information, exploiting the trust associated with text communications on mobile devices. By understanding that SMiShing is a targeted approach leveraging SMS technology, it is clear why this answer accurately aligns with the characteristics described in the question. The other options represent different forms of social engineering attacks: phishing generally refers to similar tactics using email instead of text messages, vishing uses voice communication via phone calls, and malware injection pertains to compromising systems through malicious software, none of which involve the specific use of SMS to bait victims.

2. What phase of hacking was Lopez performing if she finds vulnerabilities such as password cracking and denial of service?

A. Maintaining Access

B. Gaining Access

C. Reconnaissance

D. Clearing Tracks

In the context of ethical hacking, finding vulnerabilities such as password cracking and denial of service attacks falls under the phase known as Gaining Access. This phase is crucial because it involves exploiting the identified vulnerabilities to gain unauthorized access to systems or data. During the Gaining Access phase, hackers utilize the information gathered during earlier phases, like Reconnaissance, to execute attacks that compromise the integrity of a system. This can involve techniques such as exploiting weak passwords (password cracking) or overwhelming a server with traffic to disrupt legitimate services (denial of service). In this phase, the focus is on actively engaging with the target systems through exploitation methods, contrasting with other phases, such as Maintaining Access, which is concerned with establishing a foothold after access has been gained, or Clearing Tracks, which involves erasing any evidence of intrusion. Each of these phases has distinct objectives and techniques associated with them, but the activities highlighted in this case align closely with the act of gaining initial access through exploitative tactics.

3. Which protocol is utilized for accessing and manipulating electronic mail messages on a server?

A. Internet Message Access Protocol (IMAP)

B. Network File System (NFS)

C. Hypertext Transfer Protocol (HTTP)

D. Secure Copy Protocol (SCP)

The Internet Message Access Protocol (IMAP) is specifically designed for accessing and managing email messages on a mail server. With IMAP, users can retrieve, read, and organize their emails while leaving the messages stored on the server. This allows users to maintain access to their email from multiple devices without having to download the messages each time. IMAP also supports folder manipulation, message searching, and synchronization between the server and the email client, ensuring that actions taken in one client are reflected across all clients. This makes it an ideal protocol for modern email usage, where users often check their email on various devices. In contrast, other protocols like the Network File System (NFS) are used for file sharing between systems, and the Hypertext Transfer Protocol (HTTP) is designed for transferring hypertext and web content rather than email. The Secure Copy Protocol (SCP) is utilized for securely transferring files over a network but is not related to email access or manipulation. This distinction highlights IMAP's unique role in email management.

4. Who is identified as a malicious insider likely to damage network security intentionally?

A. Disgruntled employee

B. Negligent insider

C. Compromised insider

D. Professional insider

The identification of a malicious insider as a disgruntled employee is grounded in the understanding of motivations behind insider threats. Disgruntled employees often feel a sense of injustice, dissatisfaction with their job, or personal grievances against the organization. This discontent can drive them to intentionally engage in harmful activities, such as compromising sensitive data or undermining network security, because they believe it will retaliate against the organization or cause harm. In contrast, negligent insiders may cause security issues due to carelessness or lack of awareness, rather than with any malicious intent. Compromised insiders usually don't initiate harm themselves but may act under duress or influence from external threats, such as being coerced or manipulated by cybercriminals. Professional insiders, while knowledgeable about the system, are not inherently malicious unless they decide to exploit their expertise for nefarious purposes. Understanding these distinctions helps to clarify why a disgruntled employee is recognized as a malicious insider more clearly than the other types, who do not have a primary intent to cause intentional damage.

5. During which phase of a social engineering attack do hackers typically research their target to identify vulnerabilities?

A. Exploit the relationship

B. Select a target

C. Research the target company

D. Develop a relationship

The phase of a social engineering attack where hackers research their target to identify vulnerabilities is characterized by the in-depth gathering of information about the target. This involves analyzing various aspects such as the target company's structure, personnel, technology in use, and security measures. During this research phase, hackers aim to collect pertinent data that can be exploited later in the attack. This could include details about employees' roles, access privileges, or weaknesses in security protocols. By understanding the target's environment, attackers can devise more tailored and effective approaches to their subsequent actions. The focus on researching the target company is crucial because the insights gained during this phase allow attackers to plan and execute their strategies with more precision, increasing the likelihood of a successful social engineering attack.

6. What method can be used to mitigate side-channel attacks in cloud environments?

A. Only allow local memory access

B. Check for repeated access attempts to local memory

C. Implement strict user authentication

D. Activate firewall on all servers

The method of checking for repeated access attempts to local memory is effective in mitigating side-channel attacks in cloud environments because it helps detect potential malicious behavior that could indicate an ongoing attack. Side-channel attacks often exploit timing information, power consumption, electromagnetic leaks, or other unintentional information that can be gathered during the execution of a program. By monitoring and logging access attempts to local memory, systems can identify unusual patterns or excessive requests, which may be signals of an attacker trying to glean sensitive information through side-channel observations. In a cloud environment, where resources are shared among different users and applications, such monitoring is critical to ensure the integrity and security of the system. This proactive approach makes it harder for an attacker to conduct reconnaissance without being noticed, thus reducing the risk of successful side-channel attacks. The other methods, while important for general security, do not directly target the unique aspects of side-channel attacks. Limiting local memory access addresses broader security concerns but may not specifically prevent side-channel attacks since they can still occur if an attacker is already gaining data from shared resources. Implementing strict user authentication, while a strong security practice, focuses primarily on ensuring that users are verified rather than preventing access to system vulnerabilities. Activating firewalls helps control incoming and outgoing network

7. 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.

8. What type of attack did Alice launch against the manufacturing plant?

A. Ransomware

B. Spear Phishing

C. Malware attack

D. SQL Injection

Spear phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific individual, often for malicious reasons, using social engineering techniques. In this context, if Alice launched a spear phishing attack against the manufacturing plant, it indicates that she crafted a personalized communication designed to deceive a particular employee or group of employees within the organization. This method usually involves research and knowledge about the target, allowing the attacker to create a convincing scenario that prompts the recipient to take an action, such as clicking a link or providing personal information. Spear phishing exploits the trust and credibility of the individual being impersonated, making it an effective and dangerous form of attack. The other types of attacks mentioned carry different characteristics and methods. Ransomware focuses on encrypting data to extort money from the victim, while a general malware attack can refer to a broader category of malicious software that affects systems without a specific target. SQL Injection is a code injection technique that exploits vulnerabilities in database-driven applications, typically aiming to manipulate or access database data directly, rather than targeting individuals through deceitful communications. Thus, the identification of the attack type as spear phishing correctly reflects the nature of a focused and personalized attack on individuals within the manufacturing plant.

9. What vulnerability arises from insecure data storage on mobile devices?

A. Dependence on user awareness of security

B. Assumptions about malware access to file systems

C. Overreliance on physical device security

D. Encryption of sensitive data only

Insecure data storage on mobile devices can lead to various vulnerabilities, with one significant concern being the assumption about malware access to file systems. When developers or users of mobile devices believe that the file system is inherently secure, they might overlook implementing the necessary security measures. This complacency allows malware to gain access to sensitive data stored within the device’s file system, leading to data leaks or unauthorized data manipulation. Relying solely on presumed security exposes the device's data to attacks, especially if proper sanitization and access controls are not enforced. Therefore, the correct answer highlights the vulnerability that arises from underestimating the capabilities of malicious software, which can exploit weak security implementations, particularly in the context of mobile device storage.

10. In which hacking phase is Peter, who manages to gain control and uses techniques to stay undetected?

A. Scanning

B. Clearing Tracks

C. Gaining Access

D. Reconnaissance

In the context of ethical hacking, the phase where Peter gains control and applies techniques to remain undetected aligns with the concept of clearing tracks. This phase is crucial because once a hacker (or an ethical hacker, in the case of penetration testing) successfully gains access to a system, they often need to ensure that their presence is not detected. This involves deleting log entries, erasing traces of their activities, and employing other methods to obfuscate any indicators that could lead to their detection. The clearing tracks phase is about maintaining secrecy and safeguarding access to the compromised system. Employing such techniques allows the hacker to continue operating without raising alarms that could lead to their discovery or the remediation of the security vulnerabilities they exploited. The other options—scanning, gaining access, and reconnaissance—represent different stages in the hacking process. Reconnaissance involves gathering information about the target, scanning focuses on identifying vulnerabilities in the system, and gaining access is centered around exploiting identified vulnerabilities to enter the system. While all these phases are vital steps in the overall hacking process, they do not specifically pertain to the actions taken to conceal one's presence after gaining control, which is the essence of clearing tracks.