CertiProf CEHPC Practice Questions

Shared by Shelton on 03-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

vectors]

What is masquerading?

Options:

A- A method for masking network traffic only.
B- A web authentication method.
C- Impersonating the identity of a legitimate user or system to gain unauthorized access.

Answer:

C

Explanation:

Masquerading is an attack technique in which an attacker impersonates a legitimate user, device, or system to gain unauthorized access, making option C the correct answer. This can involve stolen credentials, forged identities, or spoofed system information.

Masquerading attacks are commonly associated with credential theft, session hijacking, and privilege abuse. Ethical hackers test for masquerading risks by assessing authentication mechanisms, access controls, and identity management systems.

Option A is incorrect because masking traffic alone does not define masquerading. Option B is incorrect because masquerading is not a legitimate authentication method.

Understanding masquerading is essential for mitigating identity-based attacks. Defenses include strong authentication, multi-factor authentication, logging, and anomaly detection.

Ethical hackers help organizations identify weaknesses that allow masquerading and implement controls to prevent impersonation-based attacks.

Here are the 100% verified answers for the first batch of questions, aligned with the provided documentation and standard ethical hacking principles.

Question 2

Question Type: MultipleChoice

Is it possible to perform geolocation phishing?

Options:

A- Yes, but with paid tools.
B- YES, it can be done with a seeker.
C- NO, it is a very complicated technique.

Answer:

B

Explanation:

Comprehensive and Detailed 250 to 300 words of Explanation From Ethical Hacking documents: Geolocation phishing is an advanced social engineering technique used to trick a victim into revealing their precise physical location. This is typically achieved by sending the target a link to a deceptive web page that appears to offer a legitimate service or interesting content. When the user clicks the link, the page requests permission to access the device's location services (GPS). If the user clicks 'Allow,' the exact coordinates are transmitted back to the attacker.

One of the most prominent tools used in the ethical hacking course for this purpose is Seeker. Seeker is an open-source tool that creates a fake website---often mimicking a 'Near Me' service or a weather app---to entice the user into sharing their location. Unlike standard IP-based geolocation, which only provides a general area based on the Internet Service Provider's location, Seeker uses the device's actual GPS data to provide accuracy within meters.

This technique is a powerful example of how attackers can combine technical vulnerabilities with human psychology. In a professional penetration test, geolocation phishing might be used to demonstrate how an executive could be tracked or how a remote worker's location could be compromised. Defending against this threat requires high user awareness: individuals should never grant location permissions to unfamiliar websites or links received via unsolicited emails or messages. It highlights that sensitive data isn't just limited to passwords; it also includes the physical whereabouts of individuals.

Question 3

Question Type: MultipleChoice

Do Google Dorks show hacked computers or systems?

Options:

A- No, Google Dorks are used to search for specific information indexed by search engines.
B- Yes, Google Dorks work as a backdoor to all web pages.
C- Yes, Google Dorks hack pages automatically to access data.

Answer:

A

Explanation:

Google Dorks, also known as Google hacking, are advanced search queries that use specific operators to locate publicly accessible information indexed by search engines. Therefore, option A is the correct answer.

Google Dorks do not hack systems, compromise computers, or act as backdoors. Instead, they reveal information that is already publicly available but may be unintentionally exposed due to poor configuration. Examples include exposed login pages, backup files, configuration files, error messages, or sensitive documents that should not be indexed.

Option B is incorrect because Google Dorks do not provide unauthorized access to web pages. Option C is also incorrect because Google Dorks do not exploit vulnerabilities or bypass authentication mechanisms.

From an ethical hacking perspective, Google Dorks are commonly used during the passive reconnaissance phase to identify information leakage without directly interacting with the target system. This makes them low-impact but highly effective for discovering misconfigurations.

Understanding Google Dorks is important for managing information exposure risks. Ethical hackers use them to demonstrate how attackers can gather intelligence without triggering security alerts. Defenders can mitigate these risks by properly configuring robots.txt files, access controls, and removing sensitive content from public indexing.

Question 4

Question Type: MultipleChoice

What is a private IP?

Options:

A- It is the IP address assigned by the service provider.
B- It is an IP that no one can use.
C- Private IP addresses are used to enable communication between devices within a local network.

Answer:

C

Explanation:

Comprehensive and Detailed 250 to 300 words of Explanation From Ethical Hacking documents:
A private IP address is a fundamental element of network architecture used to enable communication between devices within a local network, such as a home, office, or enterprise environment. Unlike public IP addresses, which are globally unique and assigned by Internet Service Providers (ISPs) to identify a specific gateway to the internet, private IP addresses are reserved for internal use only. They are not routable on the public internet, which means a device with a private IP cannot be directly accessed by an outside computer without passing through a router or firewall.

The use of private IPs is governed by standards like RFC 1918, which defines specific ranges of addresses for private use, such as 192.168.x.x, 10.x.x.x, and 172.16.x.x through 172.31.x.x. This system allows thousands of devices on a local network to share a single public IP address through a process called Network Address Translation (NAT). This not only conserves the limited supply of IPv4 addresses but also provides a basic layer of security, as internal devices are effectively 'hidden' from the public web.

For an ethical hacker, understanding the distinction between public and private IPs is crucial during the reconnaissance and scanning phases of a penetration test. During an internal pentest, the researcher will be working almost exclusively with private IPs to map out the organization's servers, workstations, and printers. In contrast, an external pentest focuses on the public IP of the organization's perimeter. Identifying a device's private IP can reveal its role in the network and help a tester understand the internal topology. Because private IPs are the 'language' of local communication, securing the internal network involves ensuring that these private addresses are not being leaked or 'spoofed' to gain unauthorized access to sensitive internal resources.

Question 5

Question Type: MultipleChoice

What is active recognition?

Options:

A- We only see the target without performing actions.
B- Gathers information by interacting with the target.
C- Recognizes the target but does nothing.

Answer:

B

Explanation:

Comprehensive and Detailed 250 to 300 words of Explanation From Ethical Hacking documents: Active recognition, also known as 'Active Reconnaissance,' is a critical phase of penetration testing where the tester gathers detailed information by directly interacting with the target system or network. Unlike 'Passive Reconnaissance,' which involves collecting publicly available information from search engines (like Google Dorking) or social media without the target's knowledge, active recognition involves sending data packets to the target's infrastructure to elicit a response.

Common activities during the active recognition phase include port scanning, service version detection, and vulnerability scanning. For example, using a tool like Nmap to scan a server's open ports is a form of active recognition. The scanner sends 'probes' to the server, and based on the server's reply (or lack thereof), the tester can determine which services are running (e.g., a web server on port 80 or a database on port 3306). This phase is essential because it provides the technical 'blueprint' of the target that the tester will use to plan an exploit.

However, active recognition carries a significant risk: it is much more likely to be detected by security systems like Intrusion Detection Systems (IDS) or firewalls. Because the tester is directly 'knocking on the doors' of the target, their IP address and activity may be logged. In a professional pentest, the degree of 'stealth' used during active recognition is a key consideration. Testers may slow down their scans or use techniques to blend in with normal network traffic to avoid detection. For the organization, being able to detect active reconnaissance is a vital part of threat management, as it often serves as the 'early warning sign' that a more sophisticated attack is being prepared. Mastering this phase allows a pentester to efficiently map the attack surface while understanding the operational limits of the target's defensive controls.

Question 6

Question Type: MultipleChoice

What is a security breach?

Options:

A- A cybersecurity incident that results in unauthorized access to personal or corporate data.
B- The hacking of the entire internet.
C- An internet shutdown or breakup.

Answer:

A

Explanation:

A security breach is a cybersecurity incident in which unauthorized individuals gain access to sensitive personal or organizational data, making option A the correct answer. Security breaches can involve data theft, data exposure, system compromise, or loss of confidentiality, integrity, or availability.

Breaches may occur due to malware infections, phishing attacks, weak credentials, unpatched vulnerabilities, insider threats, or misconfigured systems. Ethical hackers analyze breach scenarios to understand how attackers bypass defenses and what impact the breach can have on business operations.

Option B is incorrect because hacking the entire internet is unrealistic and not a valid definition. Option C is incorrect because internet outages are infrastructure issues, not necessarily security breaches.

From a defensive standpoint, understanding security breaches helps organizations improve detection, response, and recovery capabilities. Ethical hackers help simulate breach scenarios to identify gaps in monitoring and incident response plans.

Preventing breaches requires layered security controls, user awareness, continuous monitoring, and regular testing. Ethical hacking plays a critical role in reducing breach likelihood and impact.

Question 7

Question Type: MultipleChoice

What is ZAP?

Options:

A- ZAP is a closed source penetration testing tool used to evaluate online servers.

B- It is a term used to describe the collection and analysis of information from publicly available sources, such as websites, social networks, government databases, news articles, among other resources freely available on the web.
C- It is an open-source penetration testing tool used to evaluate the security of web applications.

Answer:

C

Explanation:

Comprehensive and Detailed 250 to 300 words of Explanation From Ethical Hacking documents: The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free, open-source security tools for finding vulnerabilities in web applications. It is actively maintained by a global community of volunteers under the Open Web Application Security Project (OWASP). ZAP acts as a 'man-in-the-middle proxy,' meaning it sits between the tester's web browser and the web application being tested. This allows the tester to intercept, inspect, and even modify the requests and responses traveling between the two.

ZAP provides a wide array of functionalities essential for the Web Application Pentesting process:

Automated Scanner: It can automatically crawl a website to find vulnerabilities like SQL injection, Cross-Site Scripting (XSS), and insecure headers.

Spidering: It maps out the structure of a website by following every link it finds.

Fuzzing: It can send many variations of malicious input to a specific field to see if it can break the application or trigger an error.

Active and Passive Scanning: It can passively watch traffic to find easy-to-spot issues or actively probe the server for deeper flaws.

For ethical hackers, ZAP is often compared to the commercial tool Burp Suite. While both perform similar tasks, ZAP's open-source nature and robust API make it a favorite for integrating into 'DevSecOps' pipelines, where it can automatically test new code for vulnerabilities before it is deployed. Mastering ZAP is a core skill for any professional focused on securing the web-facing assets of an organization.

Question 8

Question Type: MultipleChoice

vectors]

What is Google Hacking?

Options:

A- Refers to the use of advanced search techniques in the Google engine to find public information without vulnerabilities in websites and systems.
B- It is a special browser for ethical hackers seeking to protect systems.
C- It refers to the use of certain advanced search techniques in Google's search engine to find sensitive information or vulnerabilities in websites and systems.

Answer:

C

Explanation:

Comprehensive and Detailed 250 to 300 words of Explanation From Ethical Hacking documents: Google Hacking, also known as Google Dorking, is a powerful reconnaissance strategy that involves using advanced search operators within the Google search engine to identify sensitive information or vulnerabilities that are inadvertently exposed on the public internet. By utilizing specific syntax---such as site:, filetype:, intitle:, and inurl:---an attacker or an ethical hacker can filter search results to find 'low-hanging fruit' that would be impossible to locate with a standard query.

Common targets of Google Hacking include exposed database configuration files (which might contain passwords), server logs that reveal internal IP addresses, and 'Index of' directories that provide a raw view of a server's file structure. For example, a search like filetype:env 'DB_PASSWORD' could potentially reveal environment variables for web applications. This is an essential attack vector to mitigate because it requires no specialized hacking software; it simply exploits the fact that Google's crawlers have indexed files that administrators forgot to protect or hide via robots.txt.

Managing this vector involves 'Self-Dorking'---regularly searching one's own domain using these advanced techniques to see what information is visible to the public. Mitigation strategies include proper server configuration, ensuring that sensitive files are not stored in the webroot, and using authentication for all administrative interfaces. From a penetration testing perspective, Google Hacking is part of the 'Passive Reconnaissance' phase, allowing a tester to gather intelligence about a target's infrastructure without ever sending a single packet directly to the target's servers. This highlights how easily information leakage can lead to a full system compromise if not actively monitored.

Question 9

Question Type: MultipleChoice

What is a backdoor in terms of computer security?

Options:

A- A hidden access mechanism in a system that allows bypassing normal authentication or security controls.
B- A type of malware that spreads through instant messaging applications.
C- A main or official entry point used to access a system.

Answer:

A

Explanation:

In computer security, a backdoor refers to a hidden method of accessing a system that bypasses normal authentication and security mechanisms, making option A the correct answer. Backdoors can be intentionally created by developers for maintenance purposes or maliciously installed by attackers after compromising a system.

From an ethical hacking perspective, backdoors are commonly discovered during post-exploitation activities. Attackers use them to maintain persistent access, even if passwords are changed or vulnerabilities are patched. Backdoors may take the form of hidden user accounts, modified services, malicious scripts, or hardcoded credentials.

Option B is incorrect because malware that spreads through instant messaging is typically classified as a worm or trojan, not specifically a backdoor. Option C is incorrect because a backdoor is not a legitimate or documented access point.

Understanding backdoors is essential for managing information security threats. Ethical hackers identify backdoors to demonstrate long-term risks and highlight weaknesses in system monitoring and access controls. Defenders can mitigate backdoor threats by implementing integrity monitoring, endpoint detection and response (EDR), regular audits, and strict access management.

Backdoors pose significant risks because they undermine trust in system security. Identifying and removing them is critical for restoring system integrity and preventing repeated compromise.

To Get Premium Files for CEHPC Visit

https://www.p2pexams.com/products/cehpc

For More Free Questions Visit

https://www.p2pexams.com/certiprof/pdf/cehpc

