CEH Ethical Hacker Prep

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 1310 questions
+ unlimited timed mock exams + mistake book

Practice on the web: https://certs.theorypractice.app/ceh
$2.99 / week · $6.99 / month · cancel anytime

What you unlock: all 1310 questions • unlimited timed mock exams • mistake book • instant explanations

Also on iOS & Android — and watch the full Q&A walkthrough on YouTube @CertsQuizPrep

Practice Questions

Try all 30 first, then check the answer key at the back.

1. Which of the following is NOT a benefit of using cloud storage solutions in organizations?

A. It provides scalable storage
B. It offers cost efficiency
C. It supports disaster recovery
D. It is quick to deploy

2. Which of the following is a preventative measure to mitigate the risks associated with unsecured cloud access?

A. Performing regular security updates
B. Using encryption
C. Conducting penetration tests
D. Implementing access controls

3. Which type of hacker has the goal of causing widespread and irreversible damage to a targeted system or network?

A. Aggressive
B. Kiddie
C. Suicide
D. Extreme

4. What is the first step to securing a company's IT infrastructure in a structured and enforceable manner?

A. Antivirus installation
B. Network segmentation
C. User training
D. Security policy

5. An ethical hacker with expertise in social engineering but minimal experience with network penetration testing has been offered a job requiring extensive network penetration skills. What should the ethical hacker do?

A. Turn down the job and refer the client to someone who is more qualified, if possible.
B. Accept the job and learn as they go along.
C. Accept the job and notify management of their skill-set limitations when they hit a stumbling block.
D. Accept the job and consult with senior technicians to figure out the best processes.

6. Which of the following is essential during the initial phase of a security audit?

A. Continuous monitoring
B. Establishing a baseline
C. Incident response
D. Penetration testing

7. Which of the following is NOT TRUE about rootkits?

A. It is easily detectable by antivirus software.
B. It can mask processes to avoid detection.
C. It can modify kernel data structures.
D. It gains elevated privileges in the system.

8. Which of the following describes a situation where an attacker utilizes legitimate admin scripts found on a system to perform malicious tasks?

A. Living-off-the-Land Attacks
B. Service-Oriented Architecture
C. Spam Campaign
D. Privilege Escalation

9. During a security assessment, you need to exfiltrate data from a network. However, the firewall is configured to allow only DNS traffic through. Which evasion technique would you use in this scenario?

A. DNS tunneling
B. ICMP tunneling
C. SSH tunneling
D. DNS poisoning

10. Which factor most significantly increases a company's vulnerability to phishing attacks?

A. High employee turnover rate
B. Inadequate employee training on cybersecurity
C. Complex IT infrastructure
D. Outdated hardware equipment

11. Which of the following mechanisms can be used by employees to verify the authenticity of an internal company email to prevent phishing attacks?

A. Encrypted hash
B. Digital ID
C. Codeword
D. Steganographic message

12. Which of the following attacks involves intercepting Wi-Fi traffic to gather sensitive information?

A. Bluejacking
B. War Driving
C. Packet Sniffing
D. Evil Twin

13. What is the purpose of a honeypot in network security?

A. To secure internal data automatically
B. To lure and analyze potential attackers
C. To merge traffic flows for efficiency
D. To block all external threats

14. During a penetration test, which technique involves appending malicious SQL commands to the end of a URL query string?

A. Tunneling
B. Phishing
C. Piggybacking
D. Spoofing

15. An attacker is sniffing the network for communications operating over port 443. Which of the following services would they MOST LIKELY be attempting to obtain information about?

A. Compaq Insight Manager over SSL
B. Alternate WWW
C. SSL (HTTPS)
D. Kerberos

16. What is the MOST effective method to prevent SQL injection attacks in web applications?

A. Restrictive database permissions
B. Prepared statements
C. Fuzz testing
D. Input blacklisting

17. Which server component should a hacker target if they want to intercept and manipulate web application traffic between the client and the server?

A. Proxy server
B. Database server
C. File server
D. Mail server

18. In the context of modern web development, which feature of Single Page Applications (SPAs) increases their vulnerability to attacks?

A. Static content
B. Limited user interaction
C. Client-side scripts
D. Server-side rendering

19. Which of the following is a web security tool that enables you to intercept, inspect, and modify raw HTTP/HTTPS traffic between the client and the server?

A. OpenVAS
B. Burp Suite
C. Wireshark
D. Nmap

20. Which encryption tool does Apple provide to encrypt macOS data volumes?

A. Kryptos
B. FileVault
C. TrueCrypt
D. VeraCrypt

21. Which of the following is the essential requirement for a secure symmetric encryption algorithm?

A. Variable length keys
B. Fixed length input and output
C. High-speed performance
D. Strong key management

22. Your organization recently integrated a series of robotic systems into your manufacturing processes from ABB, a global leader in automation technologies. What industrial protocol is used that you need to put anti-hacking countermeasures in place for?

A. IRC5
B. Modbus
C. DNP3
D. IEC 61850

23. According to the EC-Council, which of the following is NOT considered a core component in the typical Operational Technology (OT) architecture?

A. Network Layer
B. Field Devices Layer
C. User Interface Layer
D. Control Layer

24. You plan to perform a Man-in-the-Middle (MitM) attack on an Android device. Which of the following tools would you use to accomplish this?

A. Nethunter
B. Intercepter-NG
C. dSploit
D. Zimperium

25. Which of the following is NOT a common security risk associated with jailbreaking a device?

A. Enhanced user experience
B. Increased malware exposure
C. Voided warranty
D. Device instability

26. Which of the following is NOT a recommended way to secure Operational Technology (OT) systems from cyber threats?

A. Utilize network segmentation to isolate OT systems from IT networks
B. Implement multi-factor authentication (MFA) for OT system access
C. Connect OT systems directly to the corporate network for seamless data flow
D. Disable unused user accounts and services on OT devices

27. Which tool is typically used for DNS zone transfers to gather domain information during footprinting?

A. Nmap
B. Wireshark
C. Nslookup
D. Dig

28. What type of network scanning method does not trigger IDS alerts and remains unnoticed?

A. Stealth
B. Intrusive
C. Active
D. Passive

29. Which protocol assists with translating domain names into IP addresses, facilitating communication between clients and servers on a network?

A. HTTP
B. DNS
C. FTP
D. SMTP

30. You need to find the active connections and their established states on your Debian server. What command would you use to achieve this?

A. ps aux
B. top
C. df -h
D. netstat -an

Answer Key & Explanations

1. D — It is quick to deploy
Answer: It is quick to deploy While cloud storage solutions offer many advantages, such as scalability, cost savings, and disaster recovery capabilities, they require careful planning and setup, which can make the implementation process time-consuming.

2. D — Implementing access controls
Answer: Implementing access controls One of the most effective ways to mitigate the risks associated with unsecured cloud access is to implement strict access controls, ensuring that only authorized users have access to sensitive data. Performing regular security updates and patching vulnerabilities is critical for maintaining cloud security but does not specifically address access control issues. Using encryption helps protect data in transit and at rest but doesn't manage who can access the data. Conducting penetration tests can identify security weaknesses but does not provide ongoing control over cloud access.

3. C — Suicide
Answer: Suicide A suicide hacker is one who is willing to go to great lengths, even facing jail time, to ensure the complete and absolute failure of their targeted system or network.

4. D — Security policy
The correct answer is Security policy. Establishing a comprehensive and enforceable security policy is the foundational step in any company's effort to secure its IT infrastructure. This policy sets the tone and guidelines for all subsequent security measures. While antivirus installation, network segmentation, and user training are important, they come after the policy has been established.

5. A — Turn down the job and refer the client to someone who is more qualified, if possible.
Answer: Turn down the job and refer the client to someone who is more qualified, if possible. All ethical hackers should be committed to providing service in their areas of competence while being honest and forthright about any limitations in their experience and education. Ensure that you are qualified for any project on which you work or propose to work by an appropriate combination of education, training, and experience.

6. B — Establishing a baseline
Answer: Establishing a baseline It is crucial to establish a baseline at the start of a security audit to: 1. Identify and understand business processes 2. Document applications, data, and critical services 3. Create an inventory of assets and prioritize them 4. Map the network infrastructure 5. Assess existing controls 6. Review policy implementations and compliance standards 7. Define the scope of the audit 8. Plan and coordinate the audit effectively

7. A — It is easily detectable by antivirus software.
Answer: It is easily detectable by antivirus software. Rootkits are designed to hide their presence from standard antivirus software, making them difficult to detect. They can mask processes, files, and system data to avoid detection. Rootkits typically gain elevated privileges in the system, allowing a malicious actor to control the system. They also can modify kernel data structures and APIs to conceal their operation and

presence.

8. A — Living-off-the-Land Attacks
Answer: Living-off-the-Land Attacks Living-off-the-Land (LotL) attacks involve the misuse of legitimate administrative tools and scripts within an operating system to achieve malicious objectives, making detection by security software more difficult. In contrast, Service-Oriented Architecture (SOA) facilitates communication between different software components over a network, Spam Campaigns aim to distribute unwanted emails, and Privilege Escalation refers to techniques used by attackers to gain elevated access to systems.

9. A — DNS tunneling
Answer: DNS tunneling DNS tunneling involves encapsulating data payloads within DNS queries to allow data transfer across a network that only permits DNS traffic. This method exploits the DNS protocol and can bypass certain firewall configurations.

10. B — Inadequate employee training on cybersecurity
Answer: Inadequate employee training on cybersecurity Phishing attacks are primarily successful due to the lack of adequate training among employees regarding cybersecurity measures. Employees should be trained to identify suspicious emails, attachments, or links, and to verify the identity of senders before providing any sensitive information.

11. C — Codeword
Answer: Codeword A codeword is a pre-agreed word or phrase that is used to authenticate the sender of an email within a company. This can help employees verify the legitimacy of the email and prevent falling victim to phishing attacks. A steganographic message is hidden within another medium, such as a photo or video, to conceal its presence. An encrypted hash is typically used for integrity verification rather than initial authentication. A digital ID is an electronic credential used to identify a user, often within PKI systems, but may not be easily verified by all employees in daily communications.

12. D — Evil Twin
Answer: Evil Twin An Evil Twin attack involves creating a rogue Wi-Fi access point that mimics a legitimate one to intercept and gather sensitive information from unsuspecting users. This is a type of sniffing attack because it captures data from the network traffic traversing the rogue access point.

13. B — To lure and analyze potential attackers
A honeypot is designed to attract potential attackers by simulating a target. It allows network administrators to observe, analyze, and understand malicious activities without risking valuable internal data.

14. C — Piggybacking
Piggybacking involves adding malicious SQL commands to a legitimate query, often appended to the URL. Spoofing impersonates another user or device, Tunneling encapsulates one protocol within another, and Phishing is a social engineering attack to steal sensitive information.

15. C — SSL (HTTPS)
Answer: SSL (HTTPS) HTTP services are often scanned during an attacker's reconnaissance phase on web applications. Of the typical services, SSL (HTTPS) operates on port 443. Other commonly used HTTP service ports include: Port Typical HTTP services 80 World Wide Web standard port 81 Alternate WWW 88 Kerberos 443 SSL (HTTPS) 900 IBM Websphere administration client 2301 Compaq Insight Manager 2381 Compaq Insight Manager over SSL 4242 Microsoft App. Center Remote Mgmt 7001 BEA Weblogic 7002 BEA

Weblogic over SSL 7070 Sun Java Web Server over SSL 8000 Alternate web server, or web cache 8001 Alternate web server or mgmt 8005 Apache Tomcat 9090 Sun Java Web Server admin module 10000 Netscape Administrator interface

16. B — Prepared statements
Answer: Prepared statements Prepared statements help to prevent SQL injection by parameterizing the SQL queries so that the input data is treated as data and not as part of the SQL code. This process avoids SQL injection by ensuring that input data cannot modify the intent of the query.

17. A — Proxy server
Correct answer: Proxy server. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. By targeting the proxy server, a hacker can intercept and manipulate traffic between the client and the web application, making it a critical point for compromising data integrity and security.

18. C — Client-side scripts
Answer: Client-side scripts Client-side scripts in SPAs increase vulnerability because they often run directly in the user's browser and can interact dynamically with server-side resources. This introduces the possibility for exploits like cross-site scripting (XSS) and increases the attack surface compared to static or server-rendered content.

19. B — Burp Suite
Answer: Burp Suite Burp Suite is a comprehensive toolset for web security testing that allows you to intercept, inspect, and modify raw HTTP/HTTPS traffic between the client and the server. It is widely used by security professionals for testing the security of web applications. Wireshark is a network protocol analyzer for network troubleshooting and analysis. Nmap is a network scanner used to discover hosts and services on a computer network. OpenVAS is a framework of several services and tools offering vulnerability scanning and vulnerability management.

20. B — FileVault
Answer: FileVault FileVault is an encryption utility included with MacOS. It provides encryption for all data on the drive to help protect against unauthorized access to the information on your startup disk.

21. D — Strong key management
The essential requirement for a secure symmetric encryption algorithm is strong key management. Efficiently managing keys ensures that unauthorized parties cannot easily decipher the encrypted information. Key management includes the generation, storage, distribution, and eventual destruction of keys.

22. A — IRC5
Answer: IRC5 IRC5 stands for the Industrial Robot Controller 5, which is ABB's proprietary communication protocol for their robotic systems. Hackers can target and compromise communications utilizing this protocol.

23. C — User Interface Layer
Answer: User Interface Layer The typical Operational Technology (OT) architecture generally includes the following layers: Layer Function Control Layer Manages and controls the operation of field devices Network Layer Facilitates communication between devices and systems Field Devices Layer Consists of the physical devices like sensors and actuators The User Interface Layer, while important for user interactions in many technologies, is not traditionally considered a core layer in OT architecture.

24. C — dSploit
Answer: dSploit dSploit is a powerful tool used to perform network security assessments, including Man-in-the-Middle attacks on Android devices.

25. A — Enhanced user experience
Answer: Enhanced user experience Jailbreaking a device involves bypassing manufacturer restrictions to gain root access, which can expose the device to various security risks such as malware, voided warranties, and instability. These risks undermine the device's security and reliability.

26. C — Connect OT systems directly to the corporate network for seamless data flow
Answer: Connect OT systems directly to the corporate network for seamless data flow. Operational Technology (OT) systems should be isolated from the IT network to enhance security. Directly connecting OT systems to the corporate network can expose them to additional vulnerabilities. It is recommended to implement strong controls, such as network segmentation, disabling unnecessary accounts, and using robust authentication mechanisms.

27. D — Dig
Answer: Dig Dig is a network administration command-line tool for querying DNS name servers. It is commonly used for DNS zone transfers, which can gather extensive information about a domain's DNS records.

28. D — Passive
Answer: Passive Passive network scanning involves the collection of data from network traffic without actively probing the network. It is less likely to be detected because it does not generate noticeable traffic.

29. B — DNS
Answer: DNS Domain Name System (DNS) is a protocol that translates domain names into IP addresses, enabling clients to locate servers on a network. Enumerating DNS records can help attackers identify internal structures and potential vulnerabilities within an organization's network.

30. D — netstat -an
Answer: netstat -an The `netstat` command is used for monitoring network connections (incoming and outgoing), as well as routing tables, interface statistics, masquerade connections, and multicast memberships. The `-an` parameter displays all connections and their established states. This information is invaluable for identifying active connections on the server, which can be crucial for troubleshooting and security audits.

Ready to pass?

Unlock the full CEH Ethical Hacker Prep bank, every explanation, and unlimited timed mock exams.

Scan to start practising
https://certs.theorypractice.app/ceh

Watch the full video walkthrough on YouTube @CertsQuizPrep