

CEH (Certified Ethical Hacker)

Exam Practice Questions and Answers

Part 2



Introduction

Think you have what it takes to become an Ethical Hacker? Think again! The **Certified Ethical Hacker (CEH)** exam is not just another cybersecurity certification; it's a rigorous test that challenges even the most seasoned professionals. With 125 complex multiple-choice questions covering 20 in-depth modules, this exam is designed to push your limits in ethical hacking techniques, reconnaissance, vulnerability exploitation, cloud computing, and more.

But here's the real challenge: not all topics carry the same weightage. Some modules, like System Hacking and Reconnaissance, demand in-depth knowledge. However, others focus on cloud security, IoT vulnerabilities, and mobile threats, making it crucial to strategize your study plan wisely. That's exactly why we've compiled this guide, a handpicked selection of the top **CEH exam practice questions** crafted to reinforce key concepts and enhance your exam readiness. Each question is designed to mimic real exam scenarios, providing detailed explanations and quick memory hacks to reinforce your learning.

So, are you ready to test your skills and see if you can think like a hacker? Let's dive into part 2.

CEH (Certified Ethical Hacker)

Exam Practice Questions and Answers

Q.1. A hacker uses the following Google search operator: `intitle:index of passwd` to find sensitive files online. What type of attack is this?

- A** Phishing
- B** SQL injection
- C** Google hacking
- D** Cross-site scripting (XSS)

Answer: C. Google hacking

Explanation: Google hacking (also called Google dorking) leverages advanced search operators to find exposed directories, passwords, and sensitive data on public websites.

STUDY TIP

"Google = Open Book"—Hackers use search engines to find weak points. Prevent exposure by disabling directory indexing and using `robots.txt` files.

Q.2. A tester successfully exploits a web application vulnerability and gains access to the backend database. What should they do next according to ethical hacking guidelines?

- A** Download all records for analysis
- B** Report the vulnerability immediately
- C** Modify database entries for testing
- D** Leave a backdoor for future testing

Answer: B. Report the vulnerability immediately

Explanation: Ethical hacking is about responsible security testing. After discovering a flaw, the Ethical Hacker must document the issue and report it to the organization without causing damage.

STUDY TIP

"Find It, Report It"—Following proper responsible disclosure protects both the hacker and the organization. Always act ethically!



Q.3. A company's security team detects repeated failed login attempts from multiple IPs on their SSH server. What type of attack is likely happening?

- A** SQL injection
- B** Brute-force attack
- C** Cross-site request forgery (CSRF)
- D** DNS spoofing

Answer: B. Brute-force attack

Explanation: A brute-force attack attempts to guess passwords by systematically trying different combinations until access is granted.

STUDY TIP

"Slow It Down"—Implement account lockouts, CAPTCHA, and Multi-factor Authentication (MFA) to defend against brute-force attacks.



Q.4. What is the most effective way to prevent privilege escalation attacks?

- A** Using strong passwords
- B** Implementing least privilege access control
- C** Disabling unused ports
- D** Encrypting all stored data

Answer: B. Implementing least privilege access control

Explanation: Least privilege access control ensures users and applications only have the permissions they need, reducing the risk of privilege escalation.

STUDY TIP

"Less is More"—The fewer privileges an account has, the less damage an attacker can do!



Q.5. Which of the following methods is most effective for detecting and stopping ransomware attacks?

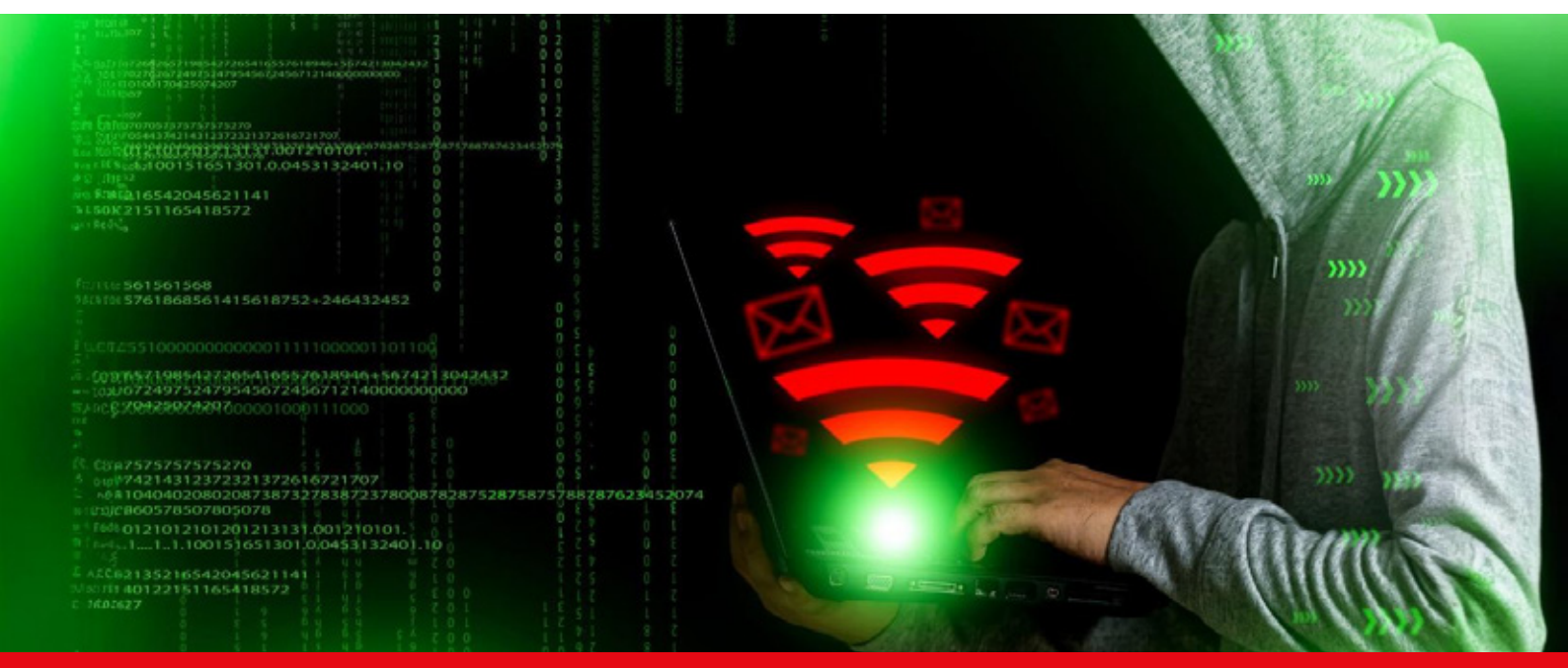
- A** Antivirus software
- B** Regular data backups and endpoint detection
- C** Disabling macros in Microsoft Office
- D** Changing user passwords frequently

Answer: B. Regular data backups and endpoint detection

Explanation: Ransomware protection relies on secure backups and real-time endpoint detection to mitigate the impact of an attack.

STUDY TIP

"Backup, Detect, Protect"—Regular backups and ransomware-specific defenses can prevent costly data loss.



Q.6. Jane, an Ethical Hacker, is testing an organization's web server and website for security vulnerabilities. She copied the entire website onto her local drive to analyze its directory structure, file structure, external links, images, and web pages. This information helps her map the website's directories and gather valuable insights. What attack technique did Jane use?

- A** Web cache poisoning
- B** Session hijacking
- C** Website mirroring
- D** Website defacement
- E** Directory traversal

Answer: C. Website mirroring

Explanation: Website mirroring is the process of copying an entire website, including its content, structure, and resources, for analysis. Ethical Hackers use this technique to identify security flaws in web applications, while malicious actors may use it for phishing attacks or reconnaissance.

STUDY TIP

- ✓ **Web cache poisoning:** Injects malicious content into cached responses.
- ✓ **Session hijacking:** Steals session cookies to impersonate users.
- ✓ **Website mirroring:** Clones a site for analysis or phishing.
- ✓ **Website defacement:** Modifies a website's content maliciously.
- ✓ **Directory traversal:** Accesses restricted directories on a web server.

Q.7. Clark, a professional hacker, created and configured multiple domains pointing to the same host, allowing him to switch quickly between domains to evade detection. What adversary behavior does this represent?

- A** Unspecified proxy activities
- B** Use of command-line interface
- C** Data staging
- D** Use of DNS tunneling
- E** Fast flux technique

Answer: E. Fast flux technique

Explanation: Fast flux is a technique where attackers rapidly change IP addresses and domain associations to evade detection. By using multiple domains pointing to the same host, attackers make it difficult for security systems to block their malicious infrastructure. This technique is commonly used in botnets, phishing, and malware distribution.

STUDY TIP

- ✓ **Unspecified proxy activities:** Uses proxy servers to mask identity.
- ✓ **Use of command-line interface:** Executes attacks via CLI tools.
- ✓ **Data staging:** Prepares data before exfiltrating it.
- ✓ **Use of DNS tunneling:** Hides malicious traffic within DNS queries.
- ✓ **Fast flux technique:** Rapidly switches domains/IPs to evade detection.

Q.8. Sam, a Penetration Tester at InfosecTrain, was assigned to perform port scanning on a target host. He sent FIN/ACK probes, and the target host responded with an RST packet, indicating that the port is closed. Which port scanning technique did Sam use?

- A** IDLE/IPID header scan
- B** Xmas scan
- C** ACK flag probe scan
- D** TCP Maimon scan
- E** FIN scan

Answer: C. ACK flag probe scan

Explanation: The ACK flag probe scan is used to determine the state of firewall rules and identify whether ports are filtered or unfiltered. When an ACK probe is sent:

If an RST packet is received, the port is unfiltered (closed).

If no response or an ICMP unreachable message is received, the port is filtered (likely blocked by a firewall).

STUDY TIP

- ✓ **IDLE/IPID header scan:** Uses a “zombie” host to perform stealth scanning.
- ✓ **Xmas scan:** Sends FIN, PSH, and URG flags; works on UNIX-based systems.
- ✓ **ACK flag probe scan:** Identifies filtered vs. unfiltered ports.
- ✓ **TCP Maimon scan:** Similar to FIN scan, but bypasses some firewalls.
- ✓ **FIN scan:** Uses FIN flag to check if ports are open on UNIX systems.

Q.9. Judy created a forum where users can post comments and images. One day, she noticed that a user was posting strange images without any comments. Concerned, she contacts a security expert, who discovers the following hidden code behind those images:

```
<script>
document.write('');
</script>
```

- A** The code redirects the user to another site.
- B** The code injects a new cookie into the browser.
- C** The code is a virus that attempts to gather the user's username and password.
- D** The PHP file silently executes the code and grabs the user's session cookie and session ID.
- E** The code modifies the forum database to create a backdoor.

Answer: D. The PHP file silently executes the code and grabs the user's session cookie and session ID.

Explanation: The code is an example of Cross-Site Scripting (XSS). It steals the user's session cookies by sending them to an attacker's server (submitcookie.php). With a stolen session cookie, an attacker can hijack the user's session, gaining unauthorized access to their account.

STUDY TIP

- ✓ **XSS Attack:** Injects malicious scripts into web pages.
- ✓ **Session Hijacking:** Steals session cookies for unauthorized access.
- ✓ **Mitigation:** Use HTTPOnly and Secure cookie attributes, input validation, and Content Security Policy (CSP).
- ✓ **Stored XSS:** Malicious code is permanently stored on the site.
- ✓ **Reflected XSS:** Malicious code is executed only when a user clicks a crafted link.

Q.10. A hacker sends a malicious script disguised as an image file to a victim. When the victim opens the file, their browser executes the script, stealing their session tokens. What type of attack is this?

- A** SQL injection
- B** Cross-site Scripting (XSS)
- C** Command injection
- D** XML External Entity (XXE) attack

Answer: B. Cross-site Scripting (XSS)

Explanation: XSS attacks inject malicious scripts into web pages that execute in the victim's browser, allowing attackers to steal session cookies and sensitive data.

STUDY TIP

"Never Trust User Input"—Always validate, sanitize, and encode user input to prevent XSS attacks!

Q.11. Which type of wireless attack involves capturing authentication handshakes to crack Wi-Fi passwords?

- A** Rogue access point attack
- B** Evil twin attack
- C** WPA2 handshake capture attack
- D** Bluetooth sniffing

Answer: C. WPA2 handshake capture attack

Explanation: Attackers capture WPA2 handshake packets using tools like Aircrack-ng and attempt to crack the Wi-Fi password through brute force.

STUDY TIP

"Strong Passwords Win"—Use long, complex Wi-Fi passwords and enable WPA3 if possible!



Q.12. Susan, a Software Developer, wants her web API to update other applications with the latest information. She uses a user-defined HTTP callback or push API that triggers events to supply data in real-time, allowing users to receive instant updates. What technique is she using?

- A** Webhooks
- B** REST API
- C** SOAP API
- D** Web shells
- E** Server-Sent Events (SSE)

Answer: A. Webhooks

Explanation: Webhooks are event-driven HTTP callbacks that automatically send data to other applications when a trigger event occurs. Unlike REST APIs that require polling, webhooks push real-time updates, improving efficiency and reducing server load.

STUDY TIP

- ✓ **Webhooks:** Push-based, triggered by events.
- ✓ **REST API:** Pull-based, requires periodic requests.
- ✓ **SOAP API:** Uses XML, a more complex and strict structure.
- ✓ **Web shells:** Malicious scripts used for remote control.
- ✓ **Server-Sent Events (SSE):** One-way connection from server to client.

Q.13. A Red Team Tester wants to remain undetected while scanning an internal network. Which Nmap option should they use?

- A** -T5
- B** -A
- C** -sS
- D** -sT

Answer: C. -sS

Explanation: The SYN scan (-sS) is stealthier than a full TCP connect scan because it does not complete the three-way handshake, making it harder for IDS/IPS systems to detect.

STUDY TIP

"Stealth is Key"—Use SYN scans for quiet reconnaissance and avoid detection.

- ✓ **-T5:** Too fast, easily detected. Trick: "Turbo = Trouble."
- ✓ **-A:** Aggressive mode, loud scan. Trick: "A for Alert."
- ✓ **-sS:** Stealthy, avoids full handshake. Trick: "Silent SYN."
- ✓ **-sT:** Full handshake, easily logged. Trick: "T for Tracked."

Q.14. During the enumeration phase, Lawrence performs banner grabbing to gather information such as OS details and service versions. He targets a service running on TCP port 445. Which service did Lawrence enumerate?

- A** Remote Procedure Call (RPC)
- B** Telnet
- C** Network File System (NFS)
- D** Server Message Block (SMB)
- E** Secure Shell (SSH)

Answer: D. Server Message Block (SMB)

Explanation: Server Message Block (SMB) operates on TCP port 445 and is used for file sharing, printer access, and network communication in Windows environments. Attackers often enumerate SMBs to extract user accounts and shared resources as well as exploit vulnerabilities like EternalBlue.

STUDY TIP

- ✓ **RPC (Remote Procedure Call):** Runs on port 135, used for inter-process communication.
- ✓ **Telnet:** Runs on port 23 and provides remote command-line access.
- ✓ **NFS (Network File System):** Runs on port 2049, and allows file sharing in UNIX/Linux.
- ✓ **SMB (Server Message Block):** Runs on port 445, used for Windows file sharing.
- ✓ **SSH (Secure Shell):** Runs on port 22 and encrypts remote administration sessions.

Q.15. An attacker sets up a fake Wi-Fi hotspot with a name similar to a nearby legitimate network to trick users into connecting. What is this attack called?

- A** DNS Spoofing
- B** Evil Twin Attack
- C** Rogue DHCP Attack
- D** SSID Flooding

Answer: B. Evil Twin Attack

Explanation: Evil Twin attacks involve setting up a rogue wireless access point that mimics a legitimate one, tricking users into connecting and exposing their credentials.

STUDY TIP

"Always Verify Wi-Fi"—Before connecting, verify the Wi-Fi network name and ask IT for confirmation!

Q.16. An attacker successfully installs a keylogger on a victim's machine to capture sensitive credentials. What type of attack is this?

- A** Spyware attack
- B** Phishing attack
- C** Rootkit attack
- D** Denial-of-Service (DoS) attack

Answer: A. Spyware attack

Explanation: Spyware is malicious software designed to secretly record user activity, such as keystrokes, and send it to attackers.

STUDY TIP

"KEY = Keep Examining Your system"—Run frequent malware scans and avoid unknown software!

Q.17. What is the most effective way to mitigate a brute-force attack on a login portal?

- A** Increasing password complexity
- B** Implementing account lockout policies
- C** Encrypting all stored passwords
- D** Using a VPN

Answer: B. Implementing account lockout policies

Explanation: Account lockout policies help prevent brute-force attacks by locking accounts after a set number of failed login attempts.

STUDY TIP

"BLOCK = Brute-force Lockout On Count"—Set up MFA and lockout policies to prevent brute-force attacks!



Q.18. Which Google advanced search operator helps an attacker find websites similar to a specified target URL?

- A** site:
- B** related:
- C** info:
- D** inurl:
- E** cache:

Answer: B. related:

Explanation: The related: operator helps find websites similar to a specified domain. Attackers use it for competitive analysis, reconnaissance, and expanding target scope during OSINT (Open-Source Intelligence) gathering.

STUDY TIP

- ✓ **site:** --> Searches within a specific domain (**site:example.com**).
- ✓ **related:** --> Finds similar websites (**related:example.com**).
- ✓ **info:** --> Displays cached pages and link details (**info:example.com**).
- ✓ **inurl:** --> Finds URLs containing specific keywords (**inurl:admin**).
- ✓ **cache:** --> Shows Google's last cached version of a page (**cache:example.com**).

Q.19. An attacker installs a rootkit that remains undetected in the core components of the operating system, allowing them to maintain access to a machine invisibly. What type of rootkit is this?

- A** Firmware rootkit
- B** Hypervisor rootkit
- C** Kernel rootkit
- D** Hardware rootkit
- E** User-mode rootkit

Answer: C. Kernel rootkit

Explanation: A kernel rootkit operates at the operating system's core (kernel level), making it extremely difficult to detect and remove. It intercepts system calls, hides processes, and provides persistent backdoor access while remaining invisible to antivirus software.

STUDY TIP

- ✓ **Firmware rootkit:** Embedded in hardware firmware (BIOS, UEFI).
- ✓ **Hypervisor rootkit:** Runs beneath the OS, controlling it.
- ✓ **Kernel rootkit:** Hides in the OS kernel, most stealthy.
- ✓ **Hardware rootkit:** Resides in system hardware (chipsets).
- ✓ **User-mode rootkit:** Runs in user space, easier to detect.

Q.20. While performing a web application scan, you want to determine the web server version hosting the application. Using the **-sV** flag with Nmap, you receive this response:

80/tcp open http-proxy Apache Server 7.1.6. What information-gathering technique does this describe?

- A** Dictionary attack
- B** Brute forcing
- C** Banner grabbing
- D** WHOIS lookup
- E** Passive reconnaissance

Answer: C. Banner grabbing

Explanation: Banner grabbing is a technique used to gather information about a service by retrieving its version, operating system, and other metadata. The **-sV** flag in Nmap is specifically used for service version detection, helping security professionals assess potential vulnerabilities.

STUDY TIP

- ✓ **Dictionary attack:** Uses a pre-compiled list of passwords for cracking.
- ✓ **Brute forcing:** Tries all possible password combinations.
- ✓ **Banner grabbing:** Extracts server details from response headers.
- ✓ **WHOIS lookup:** Retrieves domain registration info.
- ✓ **Passive reconnaissance:** Collects data without direct interaction.

Q.21. John is investigating web application firewall logs and notices an attempt to inject the following code:

```
char buff[10];
```

```
buff[10] = 'a';
```

What type of attack is this?

- A** SQL injection
- B** CSRF
- C** Buffer overflow
- D** XSS
- E** Directory traversal

Answer: C. Buffer overflow

Explanation: A buffer overflow attack occurs when a program writes data beyond the allocated memory buffer. In this case, `buff[10] = 'a';` attempts to write outside the bounds of the buffer, which can cause memory corruption, crashes, or remote code execution.

STUDY TIP

- ✓ **SQL Injection:** Injects malicious SQL queries into a database.
- ✓ **CSRF (Cross-Site Request Forgery):** Tricks users into executing unwanted actions.
- ✓ **Buffer Overflow:** Overwrites memory, leading to crashes or exploits.
- ✓ **XSS (Cross-Site Scripting):** Injects malicious JavaScript into web pages.
- ✓ **Directory Traversal:** Gains unauthorized access to system files.

Q.22. Which common files on a web server, if misconfigured, could expose useful information such as verbose error messages to hackers?

- A** administration.config
- B** php.ini
- C** httpd.conf
- D** idq.dll
- E** web.config

Answer: B. php.ini

Explanation: The php.ini file controls PHP settings, including error reporting and logging. If misconfigured, it may expose verbose error messages, file paths, and database credentials, helping attackers exploit vulnerabilities.

STUDY TIP

- ✓ **administration.config:** Not a common web server config file.
- ✓ **php.ini:** Manages PHP settings, crucial for security.
- ✓ **httpd.conf:** Configures Apache web server settings.
- ✓ **idq.dll:** Old IIS indexing service component.
- ✓ **web.config:** ASP.NET configuration file, contains sensitive settings.

Q.23. If you suspect an IoT device has been compromised, which port should you block first?

- A** 48101
- B** 443
- C** 80
- D** 22
- E** 23

Answer: A. 48101

Explanation: Port 48101 is commonly used by IoT devices for remote access and botnet communication. Attackers often target IoT devices for DDoS attacks, unauthorized control, and data theft. Blocking this port can limit attacker access.

STUDY TIP

- ✓ **Port 48101:** Used by compromised IoT devices for C2 (Command & Control).
- ✓ **Port 443 (HTTPS):** Encrypts web traffic, usually safe.
- ✓ **Port 80 (HTTP):** Handles unencrypted web traffic.
- ✓ **Port 22 (SSH):** Used for remote access, often targeted.
- ✓ **Port 23 (Telnet):** Unsecured remote login, commonly exploited.

Q.24. Heather's company is adopting a new cloud-hosted customer relationship management (CRM) tool. The provider will handle hardware, OS, software administration, patching, and monitoring, while Heather's only task is user account management. What type of cloud solution is this?

- A** SaaS
- B** CaaS
- C** PaaS
- D** IaaS
- E** FaaS

Answer: A. SaaS (Software as a Service)

Explanation: SaaS is a fully managed cloud solution where users access applications over the internet without managing infrastructure, OS, or software updates. Examples include CRM tools (e.g., Salesforce), email services (e.g., Gmail), and collaboration platforms (e.g., Microsoft 365).

STUDY TIP

- ✓ **SaaS (Software as a Service):** Fully managed software, just use it.
- ✓ **CaaS (Container as a Service):** Manages containers in the cloud.
- ✓ **PaaS (Platform as a Service):** Provides a development environment.
- ✓ **IaaS (Infrastructure as a Service):** Gives virtual machines & storage.
- ✓ **FaaS (Function as a Service):** Runs serverless functions on demand.

Q.25. During a penetration test, you gained access to a user account. You connected to your own machine via the SMB service and entered your login and password in plaintext. Which file must you clean to remove the password?

- A** `.bash_history`
- B** `.xsession-log`
- C** `.bashrc`
- D** `.profile`
- E** `syslog`

Answer: A. `.bash_history`

Explanation: The `.bash_history` file logs previously executed commands, including credentials entered in plaintext. Clearing or securely deleting this file prevents password recovery by an attacker or forensic investigator.

STUDY TIP

- ✓ **.bash_history:** Stores command history, including passwords.
- ✓ **.xsession-log:** Logs X session events, not commands.
- ✓ **.bashrc:** Configures bash shell settings, no history.
- ✓ **.profile:** Loads user environment variables, no history.
- ✓ **syslog:** Stores system logs, but not user commands.

Summary

Mastering ethical hacking requires more than theoretical knowledge—it demands hands-on experience, real-world scenarios, and continuous learning. This guide covered top essential CEH questions, helping you understand key security concepts such as penetration testing, malware analysis, and cryptographic attacks.

While self-study is valuable, a structured learning approach accelerates success. InfosecTrain's CEH Training Course provides:

- ✔ **Expert-Led Training:** Learn from certified CEH professionals with industry experience.
- ✔ **Hands-On Labs:** Gain practical skills through real-world hacking scenarios.
- ✔ **Exam-Focused Content:** Covers the latest CEH v13 curriculum, including updated cyber threats and ethical hacking techniques.
- ✔ **Flexible Learning Options:** Choose from self-paced, instructor-led, or corporate training tailored to your schedule.

Ready to take the next step? Elevate your CEH preparation with InfosecTrain's CEH Training Course and become a Certified Ethical Hacker with confidence!

Enroll now! Visit **www.InfosecTrain.com** to learn more.



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on

