CISCO Certified Ethical Hacker (CEH)
(Self-paced Online)

Course Name	**Cisco Certified Ethical Hacker (CEH)**
Instructor	**Cisco Instructor LIVE Chat – (24/7 Discord, Teams and WhatsApp)**
Course Delivery	**Self-paced Online**

The digital landscape is evolving at an unprecedented rate and cyber threats lurk around every corner. Cybersecurity resilience in the modern world cannot be just an add-on - it's a necessity. Offensive security professionals like ethical hackers and penetration testers can help proactively discover unknown threats and address them before the cyber criminals do.

With our 100% Self-paced training with month Tutor Drop In Sessions, Recorded Videos and excellent Discord/Webex Tutor Forums, this course is designed to prepare you with an Ethical Hacker skillset and give you a solid understanding of offensive security. You will become proficient in the art of scoping, executing, and reporting on vulnerability assessments, while recommending mitigation strategies. Follow an engaging gamified narrative throughout the course and get lots of practice with hands-on labs inspired by real-world scenarios.

After completing this course, continue your cybersecurity career in offensive security as an ethical hacker or penetration tester. Or use this course to strengthen your defensive security knowledge. By understanding the mindset of threat actors, you will be able to more effectively implement security controls and monitor, analyze, and respond to current security threats.

Course Schedule (70 Hours Learning) – FIRST THREE (2) MODULES ARE FREE

Module	Topics Covered	Labs/Practical
Introduction to Ethical Hacking & Penetration Testing	Ethical hacking vs. penetration testing, Common frameworks and methodologies, Setting up a virtual lab environment.	Configuring a virtual lab (e.g., deploying Kali VM)
Planning & Scoping a Penetration Testing Assessment	Governance, risk management, and compliance (GRC), Scoping tests & client requirements, Ethical conduct and pen-tester code of ethics	Creating test planning documents and code of conduct drafts
Information Gathering & Vulnerability Scanning	Passive and active reconnaissance techniques, Vulnerability scanning methodologies and analysis	Using tools like Nmap and vulnerability scanners in lab environments
Social Engineering Attacks	Pretexting, impersonation, phishing, baiting, Offline attacks and physical security considerations	Setting up and simulating phishing or social-engineering scenarios
Exploiting Wired & Wireless Networks	ARP spoofing, man-in-the-middle (MiTM) attacks, Wireless network vulnerabilities (e.g., WPA/WPA2 exploits)	Network sniffing, MiTM, and Wi-Fi cracking exercises
Exploiting Application-Based Vulnerabilities	Web vulnerabilities: SQL injection, XSS, CSRF, insecure deserialisation	Exploiting a simulated web app to identify vulnerabilities
Cloud, Mobile & IoT Security	Cloud security fundamentals and attacks Mobile OS penetration (e.g., Android/iOS) IoT device vulnerabilities and testing methods	Exercises targeting cloud consoles, IoT devices, and mobile environments
Performing Post-Exploitation Techniques	Privilege escalation methods, Persistence mechanisms and data exfiltration	Achieving elevated access and maintaining control on compromised hosts
Reporting & Communication	Structuring reports and communicating technical findings, Crafting remediation	Drafting executive & technical reports based on simulated engagements

Module	Topics Covered	Labs/Practical
	recommendations and stakeholder presentation	
Tools & Code Analysis	In-depth usage of tools like Metasploit, Wireshark, Burp Suite, John the Ripper, Reviewing exploit scripts and automating tasks	Tool-focused labs, exploit execution, and simple scripting.

Exam schedule

Mid module	10 module-end quizzes/exams
End of Course	1 final comprehensive course exam
End of Course	1 hands-on skills-based assessment (typically a Capture-the-Flag challenge

Course Badge(s) Included

Contact Us for Registration

- **Phone: +441416286918 (WhatsApp Call/Text)**
- **E:** info@csmentors.uk **| support@computersciencementors.co.uk**
- **URL: https://www.csmentors.uk**

Any Questions?

- **P: WhatsApp Call/Text:** +44 141 628 6918 – (for faster communication)
- **E:** info@csmentors.uk || support@computersciencementors.co.uk