ReadyBell
Software Services Pvt. Ltd.

Course Name	EC-Council curriculum - Ethical Hacker v13
About the Course	Gain Cybersecurity Mastery for Real-world, Success with Certified Ethical Hacker v13. Powered by AI Capabilities, Future Proof Your Cybersecurity Career with AI. Build Your Career with the Most In-Demand Ethical Hacking Certification
Key Skills You Will Learn	Certified Ethical Hackers, trained in the latest version of CEH v13, are equipped with AI-powered tools and techniques to identify, exploit, and secure vulnerabilities in systems and networks. You'll learn to leverage AI for automating threat detection, predicting security breaches, and responding swiftly to cyber incidents. Moreover, you'll also gain the skills needed to secure AI-driven technologies against potential threats. This combination of ethical hacking and AI capabilities will place you at the forefront of cybersecurity, ready to defend organizations across industries from advanced threats and adapt to evolving challenges
Course Pre-Requisite	No prerequisites however it is recommended that candidates possess a 2 years of experience in IT Security role
Target Audience	Anyone interested to learn Cybersecurity, Security infrastructure specialists, Network security consultants, Security analysts, Threat hunters
Job prospects with this role	Cybersecurity Analyst, Penetration Tester (Ethical Hacker), Security Consultant, Incident Responder, Security Engineer, Security Researcher, Information Security Manager, Network Security Engineer, Forensic Analyst and Security Architect
Course Duration	~ 50 Hrs
Course Customisation	Not applicable
Certification	READYBELL Ethical Hacker v13 Certificate
Mode of Training	Instructor-led 100% Online or 100% Classroom (Salt Lake, Kolkata - India) or hybrid mode (Online + Classroom) as suitable for the learner
Course Fees	Please contact us
Refund Policy	Get a 3-hours free trial during which you can cancel at no penalty. After that, we don't give refunds
Job Assistance	Will assist candidate in securing a suitable job
Contact	**READYBELL SOFTWARE SERVICES PVT. LIMITED** **AH 12, SALT LAKE SECTOR 2, KOLKATA (INDIA) - 700 091** **E-MAIL: contact@readybellsoftware.com** **PH: +91 - 9147708045/9674552097, +91 - 33-79642872**

ReadyBell
Software Services Pvt. Ltd.

CURRICULUM		
Topic	**Sub-Topic**	**Duration (Hrs)**
EC curriculum - Ethical Hacker v13	**Module 01: Introduction to Ethical Hacking**	50 Hrs
	Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.	
	Module 02: Footprinting and Reconnaissance	
	Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking	
	Module 03: Scanning Networks	
	Learn different network scanning techniques and countermeasures.	
	Module 04: Enumeration	
	Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures	
	Module 05: Vulnerability Analysis	
	Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included	
	Module 06: System Hacking	
	Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks	
	Module 07: Malware Threats	
	Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures	
	Module 08: Sniffing	
	Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks	
	Module 09: Social Engineering	
	Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures	
	Module 10: Denial-of-Service	
	Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections	
	Module 11: Session Hijacking	
	Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures	

	Module 12: Evading IDS, Firewalls, and Honeypots	
	Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures	
	Module 13: Hacking Web Servers	
	Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures	
	Module 14: Hacking Web Applications	
	Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures	
	Module 15: SQL Injection	
	Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures	
	Module 16: Hacking Wireless Networks	
	Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools and countermeasures for wireless networks	
	Module 17: Hacking Mobile Platforms	
	Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools	
	Module 18: IoT Hacking	
	Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures	
	Module 19: Cloud Computing	
	Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools	
	Module 20: Cryptography	
	Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools	
	Hands-On Learning Labs	
To register for this course please e-mail/call us		