Certified Ethical Hacking (CEH V13 AI) Training Brochure

Karol Bagh Address: 16/8 3rd Floor Karol Bagh New Delhi 110005

For queries on Training, please contact the undersigned:-

Nikita Bhasin 9310719612

Silicon Univ EC-Council Accredited Training Centre- Training Arm of Silicon Comnet Pvt. Ltd.

CEH Training Details:-

- **Duration: 70 Hours**
- **Mode: Hybrid (Online/Classroom)**
- **Classes: Weekdays/Weekends/ Evening**

Pre-Requisite:-
Knowledge of Networking is required

COURSE CONTENTS

CERTIFIED ETHICAL HACKING (CEH V13 AI)

Modules	Topics
Module 1	**Introduction to Ethical Hacking**
	Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.
Module 2	**Foot Printing and Reconnaissance**
	Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking.
Module 3	**Scanning Networks**
	Learn different network scanning techniques and countermeasures.
Module 4	**Enumeration**
	Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures.
Module 5	**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 6	**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 7	**Malware Threats**
	Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.
Module 8	**Sniffing**
	Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.
Module 9	**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 and OT 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 server less 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.

Additional Topics:-

S. No	Topic
1	Vulnerability Introduction
2	Vulnerability
3	Threat
4	Risk
5	Vulnerability Assessment
6	Vulnerability Management
7	Vulnerability Assessment Vs Vulnerability Management
8	Risk Assessment
9	Trends In Cyber Security
10	Attack Surfaces
11	High Profile Breaches
12	Learn From Other's Failure
13	Cve
14	Cvss
15	Vulnerability Management & Periodicity
16	Core Element Of Vulnerability Management Strategy
17	Seven Habits Highly Effective VM Program
18	Some Vulnerability Management Solutions
19	Lab Architecture Discussion
20	Questions Before Start VAPT
21	Tenable Introduction
22	Architecture
23	Scanner And Senson Installation
24	Capabilities
25	Key Features
26	Predictive Prioritization

27	Partnering And 3 Party Integration
28	How Integration Works
29	User Roles Defination
30	Challenging Questions
31	Stages Of Vulnerability Managemnet
32	Industry Accepted Approaches
33	Types Of Scanning
34	Active Scanning
35	Passive Scanning
36	Agent Scanning
37	Detection Methods Of Scanning
38	Low Hanging Threat Vector
39	Challenging Questions
40	Stage Discovery
41	True Cost Of Rogue Device
42	Best Practice Zero Trust
43	How Scanner And / Sensor Works
44	Challenging Questions