Certified Ethical Hacker Certification

Description

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

Expectations and Goals

The Purpose of the CEH credential is to:

- Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.
- Inform the public that credentialed individuals meet or exceed the minimum standards.
- Reinforce ethical hacking as a unique and self-regulating profession.

Prerequisites

- Fundamental of Networking
- Fundamental of Linux

Course Schedule

Module	Topic
Module 1	Introduction to Ethical Hacking Information Security Overview Information Security Threats and Attack Vectors Hacking Concepts Ethical Hacking Concepts Information Security Controls Penetration Testing Concepts Information Security Laws and Standards
Module 2	Footprint & Reconnaissance Footprinting Concepts Footprinting through Search Engines Footprinting through Web Services Footprinting through Social Networking Sites Website Footprinting Email Footprinting Competitive Intelligence Whois Footprinting DNS Footprinting Network Footprinting Footprinting Through Social Engineering Footprinting Tools Footprinting Countermeasures Footprinting Penetration Testing
Module 3	Scanning Network Network Scanning Concepts Scanning Tools Scanning Techniques Scanning Beyond IDS and Firewall Banner Grabbing Draw Network Diagrams

	Scanning Pen Testing
Module 4	Enumeration Enumeration Concepts NetBIOS Enumeration SANP Enumeration LDP Enumeration SMTP and DNS Enumeration Other Enumeration Techniques Enumeration Countermeasures Enumeration Pen Testing
Module 5	Vulnerability Analysis Vulnerability Assessment Concepts Vulnerability Assessment Solutions Vulnerability Scoring Systems Vulnerability Assessment Tools Vulnerability Assessment Reports
Module 6	System Hacking System Hacking Concepts Cracking Passwords Escalating Privileges Executing Applications Hiding Files Covering Tracks Penetration Testing
Module 7	Malware Threats Malware Concepts Trojan Concepts Virus and Worm Concepts Malware Analysis Countermeasures Anti-Malware Software Malware Penetration testing
Module 8	Sniffing Sniffing Concepts Sniffing Technique: MAC Attacks Sniffing Technique: DHCP Attacks Sniffing Technique: ARP Poisoning Sniffing Technique: Spoofing Attacks Sniffing Technique: DNS Poisoning Sniffing Tools Countermeasures Sniffing Detection Techniques Sniffing Pen Testing
Module 9	Social Engineering Social Engineering Concepts Social Engineering Techniques Insider Threats Impersonation on Social Networking Sites Identity Theft Countermeasures Social Engineering Pen Testing

Module 10	Denial-Of-Service DoS/DDos Concepts DoS/DDos Attack Techniques Botnets DDoS Case Study DoS/DDos Attack Tools Countermeasures DoS/DDos Protection Tools DoS/DDos Penetration Testing
Module 11	Session Hijacking Session Hijacking Concepts Application Level Session Hijacking Network Level Session Hijacking Session Hijacking Tools Countermeasures Penetration Testing
Module 12	Evading IDS, Firewall & Honeypot IDS, Firewall and Honeypot Concepts IDS, Firewall and Honeypot Solutions Evading IDS Evading Firewalls IDS/Firewall Evading Tools Detecting Honeypots IDS/Firewall Evasion Countermeasures Penetration Testing
Module 13	Hacking Web Server Web Server Concepts Web Server Attacks Web Server Attacks Methodology Web Server Attack Tools Countermeasures Patch Management Web Server Security Tools Web Server Pen Testing
Module 14	Hacking Web Application Web App Concepts Web App Threats Hacking Methodology Web App Hacking Tools Countermeasures Web App Security Testing Tools Web App Pen Testing
Module 15	SQL Injection SQL Injection Concepts Types of SQL Injection SQL Injection Methodology SQL Injection Tools Evasion Techniques Countermeasures
Module 16	Hijacking Wireless Networks Wireless Concepts

	Wireless Encryption Wireless Threats Wireless Hacking Methodology Wireless Hacking Tools Bluetooth Hacking Countermeasures Wireless Security Tools Wireless Pen Testing
Module 17	Hacking Mobile Platforms Mobile Platform Attack Vectors Hacking Android OS Hacking iOS Mobile Spyware Mobile Device Management Mobile Security Guidelines and Tools Mobile Pen Testing
Module 18	Cloud Computing Cloud Computing Concepts Cloud Computing Threats Cloud Computing Attacks Cloud Security Cloud Security Tools Cloud Penetration Testing
Module 19	Cryptography Cryptography Concepts Encryption Algorithms Cryptography Tools Public Key Infrastructure (PKI) Email Encryption Disk Encryption Cryptanalysis Countermeasures
Module 20	Project work and documentation