Course 831 – EC-Council Certified Ethical Hacker v11 (CEH)

Duration: 5 days

What You Get:

- CEH v11 Certification exam voucher
- 5 days of high quality classroom training
- Access to ActiveLearning's Virtual Labs
- 18 comprehensive modules
- 40% of class hours dedicated to labs
- 270 attack techniques
- 1685 slides
- More than 2,200 tools
- Certified EC-Council Instructor
- Course Completion Certificate
- Access to EC-Council Student Portal

Course Benefits

The Certified Ethical Hacker (C|EH v11) program is a trusted and respected ethical hacking training Program that any information security professional will need.

Since its inception in 2003, the Certified Ethical Hacker has been the absolute choice of the industry globally. It is a respected certification in the industry and is listed as a baseline certification on the United States Department of Defense Directive 8570.The C|EH exam is ANSI 17024 compliant adding credibility and value to credential members.

This course in its 11th iteration, is updated to provide you with the tools and techniques used by hackers and information security professionals alike to break into any computer system. This course will immerse you into a "Hacker Mindset" in order to teach you how to think like a hacker and better defend against future attacks. It puts you in the driver's seat with a hands-on training environment employing a systematic ethical hacking process.

You Will Learn

- Key issues plaguing the information security world, incident management process, and penetration testing
- Various types of footprinting, footprinting tools, and countermeasures
- Network scanning techniques and scanning countermeasures
- Enumeration techniques and enumeration countermeasures
- System hacking methodology, steganography, steganalysis attacks, and covering tracks
- Different types of Trojans, Trojan analysis, and Trojan countermeasures
- Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures
- Packet sniffing techniques and how to defend against sniffing

- Social Engineering techniques, identify theft, and social engineering countermeasures
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures
- Session hijacking techniques and countermeasures
- Different types of webserver attacks, attack methodology, and countermeasures
- Different types of web application attacks, web application hacking methodology, and countermeasures
- SQL injection attacks and injection detection tools
- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and wi-fi security tools
- Mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools
- Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures
- Various cloud computing concepts, threats, attacks, and security techniques and tools
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools
- Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- Different threats to IoT platforms and learn how to defend IoT devices securely.

About the Exam

- 125 questions
- 4 hours
- Multiple choice
- 70% passing score

Who Should Attend

This course will benefit:

- security officers / auditors
- security professionals
- site administrators
- anyone who is concerned about the integrity of
  their network infrastructure

Prerequisites:

- Basic networking knowledge
- MCSE or CCNA certification beneficial, but not required

Course Content

Introduction to Ethical Hacking

- Information Security Overview
- Cyber Kill Chain Concepts
- Hacking Concepts
- Ethical Hacking Concepts
- Information Security Controls
- Information Security Laws and Standards

Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting through Search Engines
- Footprinting through Web Services
- Footprinting through Social Networking Sites
- Website Footprinting

- Email Footprinting
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures

Scanning Networks

- Network Scanning Concepts
- Scanning Tools
- Host Discovery
- Port and Service Discovery
- OS Discovery (Banner Grabbing/OS Fingerprinting)
- Scanning Beyond IDS and Firewall
- Draw Network Diagrams

Enumeration

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP and NFS Enumeration
- SMTP and DNS Enumeration
- Other Enumeration Techniques
- Enumeration Countermeasures

Vulnerability Analysis

- Vulnerability Assessment Concepts
- Vulnerability Classification and Assessment Types
- Vulnerability Assessment Solutions and Tools
- Vulnerability Assessment Reports

System Hacking

- System Hacking Concepts
- Gaining Access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

Malware Threats

- Malware Concepts
- APT Concepts
- Trojan Concepts
- Virus and Worms Concepts
- Fileless Malware Concepts
- Malware Analysis
- Countermeasures
- Anti-Malware Software

Sniffing

- Sniffing Concepts
- Sniffing Technique: MAC Attacks
- Sniffing Technique: DHCP Attacks
- Sniffing Technique: ARP Poisoning
- Sniffing Technique: Spoofing Attack
- Sniffing Technique: DNS Poisoning
- Sniffing Tools
- Counter measures
- Sniffing Detection Techniques

Social Engineering

- Social Engineering Concepts
- Social Engineering Techniques
- Insider Threats
- Impersonation on Social Networking Sites
- Identity Theft
- Countermeasures

Denial-of-Service

- DoS/DDoS Concepts
- DoS/DDoS Attack Techniques
- Botnets
- DDoS Case Study
- DoS/DDoS Attack Tools
- Countermeasures
- DoS/DDoS Protection Tools

Session Hijacking

- Session Hijacking Concepts
- Application Level Session Hijacking
- Network-level Session Hijacking
- Session Hijacking Tools
- Countermeasures

Evading IDS, Firewalls, and Honeypots

- IDS, IPS, Firewall and Honeypot Concepts
- IDS, IPS, Firewall and Honeypot Solutions
- Evading IDS
- Evading Firewalls
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Countermeasures

Hacking Web Servers

- Web Server Concepts
- Web Server Attacks
- Web Server Attack Methodology
- Web Server Attack Tools
- Countermeasures
- Patch Management
- Web Server Security Tools

Hacking Web Applications

- Web Application Concepts
- Web Application Threats
- Web Application Hacking Methodology
- Web API, Webhooks, and Web Shell
- Web Application Security

SQL Injection

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- Evasion Techniques
- Countermeasures

Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Countermeasures
- Wireless Security Tools

Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Mobile Device Management
- Mobile Security Guidelines and Tools

IoT and OT Hacking

- IoT Hacking
- IoT Concepts
- IoT Attacks
- IoT Hacking Methodology
- IoT Hacking Tools

- Countermeasures
- OT Hacking
- OT Concepts
- OT Attacks
- OT Hacking Methodology
- OT Hacking Tools
- Countermeasures

Cloud Computing

- Cloud Computing Concepts
- Container Technology
- Serverless Computing
- Cloud Computing Threats
- Cloud Hacking
- Cloud Security

Cryptography

- Cryptography Concepts
- Encryption Algorithms
- Cryptography Tools
- Public Key Infrastructure(PKI)
- Email Encryption
- Disk Encryption
- Cryptanalysis
- Countermeasures

About ActiveLearning, Inc.

ActiveLearning is the Philippines' leading provider of Information Technology and Project Management education, where thousands of students take courses from Application Development to Project Management to Network Security, and much more. Our courses are taught by expert instructors, and learning is enhanced through a blend of in-depth lectures, workshops, and hands-on exercises.