New Horizons Computer Learning Centers

UPGRADING PEOPLE EVERY DAY

EC-Council Certified Ethical Hacker (CEH) v10.0

Length Days: 5
Length Hours: 40
Language: Bulgarian or English

COURSE OUTLINE

1 - INTRODUCTION TO ETHICAL HACKING

- Overview of Current Security Trends
- Understanding Elements of Information Security
- Understanding Information Security Threats and Attack Vectors
- Overview of hacking concepts, types, and phases
- Understanding ethical hacking concepts and scope
- Overview of information security management and defense-in-depth
- Overview of policies, procedures, and awareness
- Overview of physical security and controls
- Understanding incidence management process
- Overview of vulnerability assessment and penetration testing
- Overview of information security acts and laws

2 - FOOTPRINTING AND RECONNAISSANCE

- Understanding footprinting concepts
- Footprinting through search engines
- Footprint using advance google hacking techniques
- Footprint through social networking sites
- Understanding different techniques for website footprinting
- Understanding different techniques for email footprinting
- Understanding different techniques of competitive intelligence
- Understanding different techniques for WHO IS footprinting
- Understanding different techniques for network footprinting
- Understanding different techniques of footprinting through social engineering
- Footprinting tools
- Footprinting countermeasures
- Overview of footprinting Pen Testing

3 - SCANNING NETWORKS

- Overview of networking scanning
- Understanding different techniques to check for Live Systems
- Understanding different techniques to check for Open Ports
- Understanding various scanning techniques
- Understanding various IDS Evasion Techniques
- Understanding banner grabbing
- Overview of Vulnerability scanning
- Drawing network diagrams

- Using Proxies and Anonymizer for attack
- Understanding IP Spoofing and various detection techniques
- Overview of scanning and Pen Testing

4 - ENUMERATION

- Understanding Enumeration Concepts
- Understanding different techniques for NetBIOS Enumeration
- Understanding different techniques for SNMP enumeration
- Understanding different techniques for LDAP enumeration
- Understanding different techniques for NTP enumeration
- Understanding different techniques for SMTP and DNS enumeration countermeasures
- Overview of enumeration pen testing

5 - VULNERABILITY ANALYSIS

- Vulnerability of the management life cycle
- Understanding various approaches to vulnerability analysis
- Tools used to perform the vulnerability assessments
- Vulnerability analysis tools and techniques

6 - SYSTEM HACKING

- Overview of CEH Hacking Methodology
- Understanding different techniques to gain access to the system
- Understanding privilege escalation techniques
- Understanding different techniques to create and maintain remote access to the system
- Overview of different types of Rootkits
- Overview of Steganograpy and Steganalysis
- Understanding techniques to hide the evidence of compromise
- Overview of system hacking penetration testing

7 - MALWARE THREATS

- Introduction to malware and malware propagation techniques
- Overview of Trojans, their types, and how to infect systems
- Overview of viruses, their types, and how they infect files
- Introduction to computer worm
- Understanding the Malware Analysis Process
- Understanding different techniques to detect malware
- Malware countermeasures
- Overview of Malware penetration testing

8 - SNIFFING

- Overview of sniffing concepts
- Understanding MAC attacks
- Understanding DHCP attacks
- Understanding ARP Poisoning
- Understanding MAC Spoofing attacks
- Understanding DNS poisoning

- Sniffing tools
- Sniffing countermeasures
- Understanding various techniques to detect sniffing
- Overview of sniffing Pen Testing

9 - SOCIAL ENGINEERING

- Overview of social engineering
- Understanding various social engineering techniques
- Understanding insider threats
- Understanding impersonation on social networking sites
- Understanding identity theft
- Social engineering countermeasures
- Identify theft countermeasures
- Overview of Social Engineering Pen Testing

10 - DENIAL-OF-SERVICE

- Overview of Denial of Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- Overview different DoS/DDoS) attack techniques
- Understanding the botnet network
- Understanding various DoS and DDoS Attack Tools
- DoS/DDoS Countermeasures
- Overview of DoS Attack Penetration Testing

11 - SESSION HIJACKING

- Understanding session hijacking concepts
- Understanding application level session hijacking
- Understanding network level session hijacking
- Session hijacking tools
- Session hijacking countermeasures
- Overview of session hijacking penetration testing

12 - EVADING IDS, FIREWALLS, AND HONEYPOTS

- Understanding IDS, Firewall, and honeypot concepts
- IDS, Firewall and honeypot solutions
- Understanding different techniques to bypass IDS
- Understanding different techniques to bypass firewalls
- IDS/Firewall evading tools
- Understanding different techniques to detect honeypots
- IDS/Firewall evasion countermeasures
- Overview of IDS and firewall Penetration Testing

13 - HACKING WEB SERVERS

- Understanding webserver concepts
- Understanding webserver attacks
- Understanding webserver attack methodology
- Webserver attack tools

- Countermeasures against webserver attacks
- Overview of Patch Management
- Webserver security tools
- Overview of Webserver penetration testing

14 - HACKING WEB APPLICATIONS

- Understanding web application concepts
- Understanding web application threats
- Understanding web application hacking methodology
- Web application hacking tools
- Understanding web application countermeasures
- Web application security tools
- Overview of web application penetration testing

15 - SQL INJECTION

- Understanding SQL injection concepts
- Understanding various types of SQL injection attacks
- Understanding SQL injection methodology
- SQL injection tools
- Understanding different IDS evasion techniques
- SQL injection countermeasures
- SQL injection detection tools

16 - HACKING WIRELESS NETWORKS

- Understanding wireless concepts
- Understanding wireless encryption algorithms
- Understanding wireless threats
- Understanding wireless hacking methodology
- Wireless hacking tools
- Understanding Bluetooth hacking techniques
- Understanding wireless hacking countermeasures

Wireless security tools
Overview of wireless penetration testing

17 - HACKING MOBILE PLATFORMS

- Understanding mobile attack platform vectors
- Understanding various android threat and attacks
- Understanding various iOS threats and attacks
- Understanding various Windows Phone OS threats and attacks
- Understanding various blackberry threats and attacks
- Understanding mobile device management (MDM)
- Mobile Security Guidelines and security tools
- Overview of Mobile Penetration Testing

18 - IOT HACKING

- Understanding IoT concepts

- Cryptography tools
- Understanding various IoT threats and attacks
- Understanding IoT Hacking
- Understanding IoT attacks
- IoT security Tools

19 - CLOUD COMPUTING

- Understanding Cloud Computing Concepts
- Understanding Cloud Computing Threats
- Understanding Cloud Computing Attacks
- Understanding Cloud Computing Security
- Cloud computing Security tools
- Overview of Cloud Penetration testing

20 - CRYPTOGRAPHY

- Understanding Cryptography concepts
- Overview of encryption algorithms
- Cryptography tools
- Understanding Public Key Infrastructure (PKI)
- Understanding email encryption
- Understanding disk encryption
- Understanding Cryptography attacks
- Cryptanalysis Tools