Ethical Hacking

Introduction To Ethical Hacking

- ▶ Information Security Overview
- ▶ Information Security Threats and Attack Vectors
- ▶ Penetration Testing Concepts
- ▶ Hacking Concepts
- ▶ Ethical Hacking Concepts
- ▶ Information Security Controls
- ▶ Information Security Laws and Standards

Footprinting & 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
- ▶ Countermeasures
- ▶ Footprinting Pen Testing

Scanning Networks

- Network Scanning Concepts
- Scanning Tools
- Scanning Techniques
- Scanning Beyond IDS and Firewall
- Banner Grabbing
- Draw Network Diagrams
- Scanning Pen Testing

Enumeration

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

Vulnerability Analysis

- Vulnerability Assessment Concepts
- Vulnerability Assessment Solutions
- Vulnerability Scoring Systems
- Vulnerability Assessment Tools
- Vulnerability Assessment Reports

System Hacking

- System Hacking Concepts
- Cracking Passwords
- Escalating Privileges
- Executing Applications
- Hiding Files
- Covering Tracks
- Penetration Testing

Malware Threats

- Malware Concepts
- Trojan Concepts
- Virus and Worm Concepts
- Malware Analysis
- Countermeasures
- Anti-Malware Software
- Malware Penetration Testing

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
- 10- Sniffing Pen Testing

Social Engineering

- Malware Concepts
- Trojan Concepts
- Virus and Worm Concepts
- Malware Analysis
- Countermeasures
- Anti-Malware Software
- Malware Penetration Testing

Denial-of-Service

Session Hijacking

Evading IDS, Firewalls, & Honeypots

- 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

Hacking Web Servers

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

Hacking Web Applications

- Web App Concepts
- Web App Threats
- Hacking Methodology
- Web Application Hacking Tools
- Countermeasures
- Web App Security Testing Tools
- Web App Pen Testing

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
- Wi-Fi Pen Testing

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

IoT Hacking

- IoT Concepts
- IoT Attacks
- IoT Hacking Methodology
- IoT Hacking Tools
- Countermeasures
- IoT Pen Testing

Cloud Computing

- Cloud Computing Concepts
- Cloud Computing Threats
- Cloud Computing Attacks
- Cloud Security
- Cloud Security Tools
- Cloud Penetration Testing

Cryptography

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