

Ethical Hacking and Countermeasures v5

Length: 5 Days

Summary: You will understand and know how to look for weaknesses and vulnerabilities in targeted systems, and use the same knowledge and tools as a malicious hacker. If you're concerned about the integrity of your network's infrastructure, you need the ethical hacking tools and techniques you will learn in Certified Ethical Hacker (CEH) v7 to enhance your network's defenses. You'll begin by learning how perimeter defenses work. Then, by scanning and attacking your own network (no real networks will be harmed), you'll learn how intruders operate and the steps you can take to secure a system.

In the interactive, lab-filled environment of this ethical hacking course, you will gain in-depth knowledge and practical experience with current, essential security systems. You will explore common ethical hacking topics, such as intrusion detection, policy creation, social engineering, DDoS attacks, buffer overflows, and virus creation.

In addition to learning how to scan, test, hack, and secure a system, you'll prepare for the latest Certified Ethical Hacker exam from EC-Council.

COURSE CONTENT

Module 1: Introduction to Ethical Hacking

Module 2: Footprinting

Module 3: Scanning

Module 4: Enumeration

Module 5: System Hacking

Module 6: Trojans and Backdoors

NDA: Non-Disclosure Agreement

Module 7: Sniffers

Module 8: Denial of Service

Module 9: Social Engineering

Module 10: Session Hijacking

Module 11: Hacking Web Servers

Module 12: Web Application Vulnerabilities

Module 13: Web-Based Password Cracking Techniques

Module 14: SQL Injection

Module 15: Hacking Wireless Networks

Module 16: Virus

Module 17: Physical Security

Module 18: Linux Hacking

Module 19: Evading IDS, Firewalls and Detecting Honey Pots

Module 20: Buffer Overflows

Module 21: Cryptography

Module 22: Penetration Testing

Modules 23-26: Advanced Modules

Lab Manual: Ethical Hacking and Countermeasures CEHv5

Lab 1.1 Visits The Securiteam Website And Analyzes Vulnerabilities

Lab 1.2 Visit the U.S. Cybercrime Website

Lab 1.3 Visit Various Hacker Websites

Lab 1.4 Read Ethical Hacking Agreement

Lab 2.1 Use SamSpade

Lab 2.2 Use Web Data Extractor to Footprint a Website

Lab 2.3 Use GEO spider to Footprint a Website

Lab 2.4 Use NEOTRACE to Footprint a Website

- Lab 2.5 Use Which ISP Owns IP to Footprint a Network Address
- Lab 2.6 Use WhereIsIP to Footprint a Network Address
- Lab 2.7 Use My IP Suite to Footprint a Network Address
- Lab 2.8 Use Way Back Machine to View Web History
- Lab 2.9 Use Public Websites for Footprinting
- Lab 2.10 Use Kartoo Visual Browser for Footprinting a Company's Network
- Lab 2.11 Use Yahoo People for Footprinting an Individual
- Lab 2.12 Use Intellius for Footprinting an Individual
- Lab 2.13 Use Google Earth
- Lab 2.14 Mirror a Website
- Lab 2.15 Email Tracking
- Lab 2.16 Search the Internet for Email Addresses
- Lab 2.17 GeoWhere – Query multiple search engines at once, find and test proxies, get daily topnews
- Lab 2.18 Web The Ripper
- Lab 2.19 Website Watcher
- Lab 2.20 Whois
- Lab 3.1 Use NMAP to Portscan a Website
- Lab 3.2 Use Angry IP to Check for Live Hosts
- Lab 3.3 Scan the Network Using Hping2 for Windows
- Lab 3.4 Scan the Network Using NetScan Tools Pro
- Lab 3.5 Scan the Network Using SuperScan 4
- Lab 3.6 Scan the Network Using Floppyscan
- Lab 3.7 Banner Grabbing Using Telnet
- Lab 3.8 Banner Grabbing Using Netcraft
- Lab 3.9 HTTP Tunneling
- Lab 3.10 Block and restore Cookies G-Zapper
- Lab 3.11 Global Network Inventory
- Lab 3.12 Mega Ping
- Lab 4.1 Connect via a Null Session
- Lab 4.2 Use GetAcct to Enumerate Users
- Lab 4.3 Use SuperScan 4 to Enumerate Users
- Lab 4.4 Use SNMP Scanner
- Lab 4.5 Use Winfingerprint to Enumerate Services
- Lab 5.1 Use L0phtack to Bruteforce SAM Passwords
- Lab 5.2 Extract SAM Hashes Using Pwdump
- Lab 5.3 Privilege Escalation Using X.EXE
- Lab 5.4 Execute Commands on a Remote Computer
- Lab 5.5 Email Keylogger
- Lab 5.6 Use the "Klogger" Keylogger
- Lab 5.7 Use Desktop Spy to Capture Screen Images
- Lab 5.8 NTFS Streams
- Lab 5.9 Use Fu Rootkit to Hide Files and Processes
- Lab 5.10 Use Camera/Shy to View Hidden Files
- Lab 5.11 Use Spammimic to Hide Messages
- Lab 5.12 Use Snow to Hide Information
- Lab 5.13 Use Auditpol to Enable/Disable Auditing
- Lab 5.14 ADS Spy
- Lab 5.15 Brute Force Password Estimation Tool
- Lab 5.16 Masker Stenography Tool
- Lab 5.17 Max File Encryption
- Lab 5.18 Merge Streams
- Lab 5.19 Rootkit Revealer – Rootkit Detection Utility
- Lab 5.20 Traceless
- Lab 5.21 Rainbowcrack
- Lab 5.22 Invisible Secrets 4
- Lab 6.1 Tini Trojan
- Lab 6.2 NetBus Trojan
- Lab 6.3 Netcat Trojan
- Lab 6.4 Beast Trojan
- Lab 6.5 Use Wrappers
- Lab 6.6 Proxy Trojan
- Lab 6.7 Atelier Web Commander
- Lab 6.8 Use TCPVIEW to Monitor the Network Connections
- Lab 6.9 What's on My Computer
- Lab 6.10 Use Process Viewer to View the Running Processes
- Lab 6.11 Use MSCONFIG to View the Startup Programs
- Lab 6.12 Use MD5SUM to Create Digital File Signatures
- Lab 6.13 Check the Registry for Trojan Startup Entries
- Lab 6.14 CurrPorts
- Lab 6.15 Fast Sum – Using MD5 Checksum
- Lab 6.16 Netstat
- Lab 6.17 Additional Labs
- Lab 7.1 Use Ethereal to Sniff the Network
- Lab 7.2 Use Windump to Sniff the Network
- Lab 7.3 Network View
- Lab 7.4 Ettercap
- Lab 7.5 Ettercap-NG (Next Generation)
- Lab 7.6 Mac Flooding
- Lab 7.7 DNS Poisoning
- Lab 7.8 EffeTech Sniffer
- Lab 7.9 Password Sniffer
- Lab 7.10 Cain and Abel
- Lab 7.11 Packet Crafter
- Lab 7.12 SMAC – Spoofing MAC Address
- Lab 8.1 Freak88 – Distributed Denial-of-Service
- Lab 8.2 Ping of Death
- Lab 8.3 ImageWolf Bot
- Lab 8.4 DoS Attack Using Nemesys
- Lab 8.5 DoS Attack Using Panther
- Lab 8.6 DDOS Ping Attack
- Lab 9.1 Read Social Engineering Story
- Lab 9.2 Phishing Attack – Fake Address Bar
- Lab 9.3 Phishing Attack – Fake Status Bar

Lab 9.4 Phishing Attack – Fake Toolbar
Lab 9.5 IP Address Conversion
Lab 9.6 NETCRAFT Anti-Phishing Toolbar
Lab 10.1 Session Hijacking Analysis
Lab 10.2 Session Hijacking Using Paros
Lab 11.1 Exploit Windows 2000
Lab 11.2 RPC Exploit
Lab 11.3 Metasploit Exploit
Lab 11.4 Vulnerability Assessment Using Shadow Security Scanner
Lab 11.5 Nessus for Windows
Lab 11.6 Microsoft Baseline Security Analyzer
Lab 11.7 Qfecheck
Lab 12.1 E-Shopping Using Hidden Values
Lab 12.2 Footprint a Website Using BlackWidow
Lab 12.3 Footprint a Website Using Wget
Lab 12.4 Footprint a Website Using an Access Diver
Lab 12.4 Unicode Strings
Lab 12.5 Acunetix Web Vulnerability Scanner
Lab 13.1 ObiWan Password Cracking Tool
Lab 13.2 Brutus Password Cracking Tool
Lab 13.3 Dictionary Maker
Lab 13.4 SnadBoy – Password Revelation
Lab 13.5 Cookie Spy
Lab 13.6 Password Recovery Time Simulator
Lab 13.7 RockXP
Lab 14.1 Juggybank SQL Interjection
Lab 14.2 SQL Interjection Whitepaper
Lab 15.1 AiroPeek
Lab 16.1 Write a Simple Virus
Lab 16.2 Use Virus Construction Kits
Lab 16.3 Virus Analysis Using IDA Pro
Lab 16.4 A2 Scanner
Lab 16.5 AVG Scanner
Lab 16.6 McAfee
Lab 16.7 Norton Internet Security
Lab 17.1 MIT Document
Lab 18.1
Lab 19.1 Install and Run Snort
Lab 19.2 Install and TrapServer
Lab 20.1 Compile and Execute a Simple Buffer Overflow Program
Lab 22.1 Azure Web Log
Lab 22.2 Inventory
Lab 22.3 Link Utility
Lab 22.4 MaxCrypt
Lab 22.5 Sniff'em
Lab 22.6 SQL Stripes
Lab 22.7 Trace Route
Lab 22.8 Windows Security Officer

