

Course Description:

This class will immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this intensive 5--day class they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

Who Should Attend:

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Prerequisites:

Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent. Not anyone can be a student - the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.

Benefits of Attendance:

Upon completion of this course, students will be able to:

- Understand how intruders escalate privileges.
- Understand Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.
- Understand Ethical Hacking.

Course Outline:

Module 01: Introduction to Ethical Hacking

Internet Crime Current Report: IC3
Data Breach Investigations Report
Types of Data Stolen From the Organizations
Essential Terminologies
Elements of Information Security
Authenticity and Non-Repudiation
The Security, Functionality, and Usability Triangle
Security Challenges
Effects of Hacking
Who is a Hacker?
Hacker Classes
Hacktivism
What Does a Hacker Do?
Phase 1 - Reconnaissance
Phase 2 - Scanning
Phase 3 - Gaining Access
Phase 4 - Maintaining Access
Phase 5 - Covering Tracks
Types of Attacks on a System
Why Ethical Hacking is Necessary?
Defense in Depth
Scope and Limitations of Ethical Hacking
Who Do Ethical Hackers Do?
Skills of an Ethical Hacker
Vulnerability Research
Vulnerability Research Websites
What is Penetration Testing?
Why Penetration Testing?
Penetration Testing Methodology

Module 02: Footprinting and Reconnaissance

Footprinting Terminologies
What is Footprinting?
Objectives of Footprinting
Footprinting Threats
Finding a Company's URL
Locate Internal URLs
Public and Restricted Websites
Search for Company's Information
Footprinting Through Search Engines
Collect Location Information
People Search
Gather Information from Financial Services
Footprinting Through Job Sites
Monitoring Target Using Alerts
Competitive Intelligence Gathering
WHOIS Lookup
Extracting DNS Information
Locate the Network Range
Traceroute
Mirroring Entire Website
Extract Website Information from http://www.archive.org
Monitoring Web Updates Using Website Watcher

Tracking Email Communications
Footprint Using Google Hacking Techniques
What a Hacker Can Do With Google Hacking?
Google Advance Search Operators
Google Hacking Tool: Google Hacking Database (GHD)
Google Hacking Tools
Additional Footprinting Tools
Footprinting Countermeasures
Footprinting Pen Testing

Module 03: Scanning Networks

Network Scanning
Types of Scanning
Checking for Live Systems - ICMP Scanning
Ping Sweep
Three-Way Handshake
TCP Conversation Flags
Hping2 / Hping3
Hping Commands
Scanning Techniques
Scanning: IDS Evasion Techniques
IP Fragmentation Tools
Scanning Tool: Nmap
Scanning Tool: NetScan Tools Pro
Scanning Tools
Do Not Scan These IP Addresses (Unless you want to get into trouble)

Module 04: Enumeration

What is Enumeration?
Techniques for Enumeration
Netbios Enumeration
Enumerating User Accounts
Enumerate Systems Using Default Passwords
SNMP (Simple Network Management Protocol) Enumeration
UNIX/Linux Enumeration
LDAP Enumeration
NTP Enumeration
SMTP Enumeration
DNS Zone Transfer Enumeration
Using nsllookup
Enumeration Countermeasures
Enumeration Pen Testing

Module 05: System Hacking

Information at Hand Before System Hacking Stage
System Hacking: Goals
CEH Hacking Methodology (CHM)
Password Cracking
Microsoft Authentication
How Hash Passwords are Stored in Windows SAM?
What is LAN Manager Hash?
Kerberos Authentication

Salting
PWdump7 and Fgdump
L0phtCrack
Optcrack
Cain & Abel
RainbowCrack
Password Cracking Tools
LM Hash Backward Compatibility
How to Defend against Password Cracking?

Privilege Escalation
Active@ Password Changer
Privilege Escalation Tools
How to Defend against Privilege Escalation?
Executing Applications
Alchemy Remote Executor
RemoteExec
Execute This!
Keylogger
Types of Keystroke Loggers
Acoustic/CAM Keylogger
Keyloggers
Spyware
How to Defend against Keyloggers?
How to Defend against Spyware?
Rootkits
Types of Rootkits
How Rootkit Works?
Rootkit: F
Detecting Rootkits
How to Defend against Rootkits?
Anti-Rootkit: RootkitRevealer and McAfee Rootkit Detective
NTFS Data Stream
What is Steganography?
Types of Steganography
Image Steganography
Document Steganography: wbStego
Video Steganography: Our Secret
Audio Steganography: Mp3stegz
Folder Steganography: Invisible Secrets 4
Spam/Email Steganography: Spam Mirror
Natural Text Steganography: Sams Big G Play Maker
Steganalysis
Steganography Detection Tool: Stegdetect

Why Cover Tracks?
Ways to Clean Online Tracks
Disabling Auditing: Auditpol
Covering Tracks Tool: Window Washer
Covering Tracks Tool: Tracks Eraser Pro
System Hacking Penetration Testing

Module 06: Trojans and Backdoors

What is a Trojan?
Overt and Covert Channels
Purpose of Trojans
What Do Trojan Creators Look For?
Indications of a Trojan Attack
Common Ports used by Trojans
How to Infect Systems Using a Trojan?
Wrappers
Different Ways a Trojan can Get into a System
How to Deploy a Trojan?
Evading Anti-Virus Techniques
Types of Trojans
Destructive Trojans
Notification Trojans
Credit Card Trojans
Data Hiding Trojans (Encrypted Trojans)
BlackBerry Trojan: PhoneSnoop
MAC OS X Trojan: DNSChanger
MAC OS X Trojan: DNSChanger
Mac OS X Trojan: Hell Raiser
How to Detect Trojans?
Process Monitoring Tool: What's Running
Scanning for Suspicious Registry Entries
Registry Entry Monitoring Tools
Scanning for Suspicious Device Drivers
Scanning for Suspicious Windows Services
Scanning for Suspicious Startup Programs
Scanning for Suspicious Files and Folders
Scanning for Suspicious Network Activities
Trojan Countermeasures
Backdoor Countermeasures
Trojan Horse Construction Kit
Anti-Trojan Software: TrojanHunter
Anti-Trojan Software: Emissoft Anti-Malware
Anti-Trojan Softwares
Pen Testing for Trojans and Backdoors

Types of Viruses
Transient and Terminate and Stay Resident Viruses
Writing a Simple Virus Program
Computer Worms
How is a Worm Different from a Virus?
Example of Worm Infection: Conficker Worm
Worm Analysis:
What is Sheep Dip Computer?
Anti-Virus Sensors Systems
Malware Analysis Procedure
String Extracting Tool: Bintext
Compression and Decompression Tool: UPX
Process Monitoring Tools: Process Monitor
Log Packet Content Monitoring Tools: NetResident
Debugging Tool: Ollydbg
Virus Analysis Tool: IDA Pro
Online Malware Testing:
Online Malware Analysis Services
Virus Detection Methods
Virus and Worms Countermeasures
Compensation Antivirus: Immunet Protect
Anti-virus Tools
Penetration Testing for Virus

Module 07: Viruses and Worms

Introduction to Viruses
Virus and Worm Statistics 2010
Stages of Virus Life
Working of Viruses: Infection Phase
Working of Viruses: Attack Phase
Why Do People Create Computer Viruses?
Indications of Virus Attack
How does a Computer get Infected by Viruses?
Virus Hoaxes
Virus Analysis:

Types of Viruses
Transient and Terminate and Stay Resident Viruses
Writing a Simple Virus Program
Computer Worms
How is a Worm Different from a Virus?
Example of Worm Infection: Conficker Worm
Worm Analysis:
What is Sheep Dip Computer?
Anti-Virus Sensors Systems
Malware Analysis Procedure
String Extracting Tool: Bintext
Compression and Decompression Tool: UPX
Process Monitoring Tools: Process Monitor
Log Packet Content Monitoring Tools: NetResident
Debugging Tool: Ollydbg
Virus Analysis Tool: IDA Pro
Online Malware Testing:
Online Malware Analysis Services
Virus Detection Methods
Virus and Worms Countermeasures
Compensation Antivirus: Immunet Protect
Anti-virus Tools
Penetration Testing for Virus

Module 08: Sniffers

Lawful Intercept
Wiretapping
Sniffing Threats
How a Sniffer Works?
Hacker Attacking a Switch
Types of Sniffing: Active Sniffing
Protocols Vulnerable to Sniffing
Tie to Data Link Layer in OSI Model
Hardware Protocol Analyzers
SPAN Port
MAC Flooding
How DHCP Works?
What is Address Resolution Protocol (ARP)?
Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
MAC Spoofing/Duplicating
DNS Poisoning Techniques
Sniffing Tool: WireShark
Sniffing Tool: CACE Pilot
Sniffing Tool: Tcplump/Windowump
Discovery Tool: NetworkView
Discovery Tool: The Dude Sniffer
Password Sniffing Tool: Ace Packet Sniffing Tool: Capsa Network Analyzer
OmniPeek Network Analyzer
Network Packet Analyzer: Observer

Certified Ethical Hacker

Session Capture Sniffer: NetWitness
Email Message Sniffer: Big-Mother
TCP/IP Packet Crafter: Packet Builder
Additional Sniffing Tools
How an Attacker Hacks the Network
Using Sniffers?
How to Defend Against Sniffing?
Sniffing Prevention Techniques
How to Detect Sniffing?
Promiscuous Detection Tool:
PromyUI
Promiscuous Detection Tool:
PromiScan

Module 09: Social Engineering

What is Social Engineering?
Behaviors Vulnerable to Attacks
Why is Social Engineering Effective?
Warning Signs of an Attack
Phases in a Social Engineering Attack
Impact on the Organization
Command Injection Attacks
Common Targets of Social Engineering
Types of Social Engineering
Insider Attack
Common Intrusion Tactics and Strategies for Prevention
Social Engineering Through Impersonation on Social Networking Sites
Risks of Social Networking to Corporate Networks
Identity Theft Statistics 2010
Real Steven Gets Huge Credit Card Statement
Identity Theft - Serious Problem
Social Engineering Countermeasures: Policies
How to Detect Phishing Emails?
Identity Theft Countermeasures
Social Engineering Pen Testing

Module 10: Denial of Service

What is a Denial of Service Attack?
What is Distributed Denial of Service Attacks?
Symptoms of a DoS Attack
Cyber Criminals
Internet Chat Query (ICQ)
Internet Relay Chat (IRC)
DoS Attack Techniques
Botnet
WikiLeak Operation Payback
DoS Attack Tools
Detection Techniques
DoS/DDoS Countermeasure Strategies
DDoS Attack Countermeasures
Post-attack Forensics
Techniques to Defend against Botnets
DoS/DDoS Countermeasures
DoS/DDoS Protection at ISP Level
Enabling TCP Intercept on Cisco IOS Software
Advanced DDoS Protection:
IntelliGuard DDoS Protection System (DPS)
DoS/DDoS Protection Tool
Denial of Service (DoS) Attack Penetration Testing

Module 11: Session Hijacking

What is Session Hijacking?
Dangers Posed by Hijacking
Why Session Hijacking is Successful?
Key Session Hijacking Techniques
Brute Forcing
HTTP Referrer Attack
Spoofing vs. Hijacking
Session Hijacking Process
Packet Analysis of a Local Session Hijack
Types of Session Hijacking
Predictable Session Token
Man-in-the-Middle Attack
Man-in-the-Browser Attack
Client-side Attacks
Cross-site Script Attack
Session Fixation
Network Level Session Hijacking
The 3-Way Handshake
Sequence Numbers
TCP/IP Hijacking
IP Spoofing: Source Routed Packets
RST Hijacking
Blind Hijacking
Man-in-the-Middle Attack using Packet Sniffer
UDP Hijacking
Session Hijacking Tools
Countermeasures
Protecting against Session Hijacking
Methods to Prevent Session

Hijacking: To be Followed by Web Developers
Methods to Prevent Session Hijacking: To be Followed by Web Users
Defending against Session Hijack Attacks
Session Hijacking Remediation
IPSec
Session Hijacking Pen Testing

Module 12: Hijacking Webservers

Webserver Market Shares
Open Source Webserver Architecture
IIS Webserver Architecture
Website Defacement
Case Study
Why Web Servers are Compromised?
Impact of Webserver Attacks
Webserver Misconfiguration
Directory Traversal Attacks
HTTP Response Splitting Attack
Web Cache Poisoning Attack
HTTP Response Hijacking
SSH BruteForce Attack
Man-in-the-Middle Attack
Webserver Password Cracking
Web Application Attacks
Webserver Attack Methodology
Webserver Attack Tools
Web Password Cracking Tool
Countermeasures
How to Defend Against Web Server Attacks?
How to Defend against HTTP Response Splitting and Web Cache Poisoning?
Patches and Hotfixes
What is Patch Management?
Identifying Appropriate Sources for Updates and Patches
Installation of a Patch
Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)
Web Application Security Scanner: Sandcat
Web Server Security Scanner: Wiktow
Webserver Malware Infection Monitoring Tool: HackAlert
Webserver Security Tools
Web Server Penetration Testing

Module 13: Hacking Web Applications

Web Application Security Statistics
Introduction to Web Applications
Web Application Components
How Web Applications Work?
Web Application Architecture
Web 2.0 Applications
Vulnerability Stack
Web Attack Vectors
Web Application Threats - 1
Web Application Threats - 2
Unvalidated Input
Parameter/Form Tampering
Directory Traversal
Security Misconfiguration
Injection Flaws
What is LDAP Injection?
How LDAP Injection Works?
Hidden Field Manipulation Attack
Cross-Site Scripting (XSS) Attacks
Web Application Denial-of-Service (DoS) Attack
Buffer Overflow Attacks
Cookie/Session Poisoning
Session Fixation Attack
Insufficient Transport Layer Protection
Improper Error Handling
Insecure Cryptographic Storage
Broken Authentication and Session Management
Unvalidated Redirects and Forwards
Web Services Architecture
Footprint Web Infrastructure
Web Spidering Using Burp Suite
Hacking Web Servers
Analyze Web Applications
Attack Authentication Mechanism
Username Enumeration
Password Attacks: Password Functionality Exploits
Password Attacks: Password Guessing
Password Attacks: Brute-forcing
Session Attacks: Session ID Prediction/Brute-forcing
Cookie Exploitation: Cookie Poisoning
Authorization Attack
Session Management Attack
Injection Attacks
Attack Data Connectivity
Attack Web App Client
Attack Web Services

Web Services Probing Attacks
Web Service Attack Tool: soapUI
Web Service Attack Tool: XMLSpy
Web Application Hacking Tool: Burp Suite Professional
Web Application Hacking Tools: CookieDigger
Web Application Hacking Tools: WebScarab
Encoding Schemes
Web Application Countermeasures
Web Application Firewall: dotDefender
Web Application Firewall: IBM AppScan
Web Application Firewall: ServerDefender VP
Web Application Pen Testing

Module 14: SQL Injection

SQL Injection is the Most Prevalent Vulnerability in 2010
SQL Injection Threats
What is SQL Injection?
SQL Injection Attacks
How Web Applications Work?
Server Side Technologies
HTTP Post Request
SQL Injection Detection
SQL Injection Black Box Pen Testing
Types of SQL Injection
What is Blind SQL Injection?
SQL Injection Methodology
Information Gathering
Database, Table, and Column Enumeration
Features of Different DBMSs
Password Grabbing
Transfer Database to Attacker's Machine
Interacting with the Operating System
Interacting with the File System
Network Reconnaissance Full Query
SQL Injection Tools
Evading IDS
How to Defend Against SQL Injection Attacks?
SQL Injection Detection Tools
Short Rule to Detect SQL Injection Attacks

Module 15: Hacking Wireless Networks

Wireless Networks
Wi-Fi Usage Statistics in the US
Wi-Fi Hotspots at Public Places
Wi-Fi Networks at Home
Types of Wireless Networks
Wireless Standards
Service Set Identifier (SSID)
Wi-Fi Authentication Modes
Wireless Terminologies
Wi-Fi Chalking
Wi-Fi Hotspot Finder: jwire.com
Wi-Fi Hotspot Finder: WeFi.com
Types of Wireless Antenna
Parabolic Grid Antenna
Types of Wireless Encryption
WEP Encryption
What is WPA?
Temporal Keys
What is WPA2?
WEP vs. WPA vs. WPA2
WEP Issues
Weak Initialization Vectors (IV)
How to Break WEP Encryption?
How to Break WPA/WPA2 Encryption?
How to Defend Against WPA Cracking?
Wireless Threats: Access Control Attacks
Wireless Threats: Integrity Attacks
Wireless Threats: Confidentiality Attacks
Wireless Threats: Availability Attacks
Wireless Threats: Authentication Attacks
Rogue Access Point Attack
Client Mis-association
Misconfigured Access Point Attack
Unauthorized Association
Ad Hoc Connection Attack
HoneySpot Access Point Attack
AP MAC Spoofing
Denial-of-Service Attack
Jamming Signal Attack
Wi-Fi Jamming Devices
Wireless Hacking Methodology
Find Wi-Fi Networks to Attack
Attackers Scanning for Wi-Fi Networks
Footprint the Wireless Network
Wi-Fi Discovery Tool: inSSIDer
Wi-Fi Discovery Tool: NetSurveyor
Wi-Fi Discovery Tool: NetStumbler
Wi-Fi Discovery Tool: Vistumbler

Wi-Fi Discovery Tool: WirelessMon
Wi-Fi Discovery Tools
GPS Mapping
How to Discover Wi-Fi Network Using Wardriving?
Wireless Traffic Analysis
Wireless Cards and Chipsets
Wi-Fi USB Dongle: AirPcap
Wi-Fi Packet Sniffer: Wireshark with AirPcap
Wi-Fi Packet Sniffer: Wi-Fi Pilot
Wi-Fi Packet Sniffer: OmniPeek
Wi-Fi Packet Sniffer: CommView for Wi-Fi
What is Spectrum Analysis?
Wireless Sniffers
Aircrack-ng Suite
How to Reveal Hidden SSIDs
Fragmentation Attack
How to Launch MAC Spoofing Attack?
Denial of Service: Deauthentication and Disassociation Attacks
Man-in-the-Middle Attack
MITM Attack Using Aircrack-ng
Wireless ARP Poisoning Attack
Rogue Access Point
Evil Twin
How to Crack WEP Using Aircrack?
How to Crack WEP Using Aircrack? Screenshot 1/2
How to Crack WEP Using Aircrack? Screenshot 2/2
How to Crack WPA-PSK Using Aircrack?
WPA Cracking Tool: KisMAC
WEP Cracking Using Cain & Abel
WPA Brute Forcing Using Cain & Abel
WPA Cracking Tool: Elcomsoft Wireless Security Auditor
WEP/WPA Cracking Tools
Wi-Fi Sniffer: Kismet
Wardriving Tools
RF Monitoring Tools
Wi-Fi Connection Manager Tools
Wi-Fi Traffic Analyzer Tools
Wi-Fi Raw Packet Capturing Tools
Wi-Fi Spectrum Analyzing Tools
Bluetooth Hacking
How to BlueJack a Victim?
Bluetooth Hacking Tool: Super Bluetooth Hack
Bluetooth Hacking Tool: PhoneSnoop
Bluetooth Hacking Tool: BlueScanner
How to Defend Against Bluetooth Hacking?
How to Detect and Block Rogue AP?
Wireless Security Layers
How to Defend Against Wireless Attacks?

Wireless Intrusion Prevention Systems
Wireless IPS Deployment
Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer
Wi-Fi Security Auditing Tool: AirDefense
Wi-Fi Security Auditing Tool: Adaptive Wireless IPS
Wi-Fi Security Auditing Tool: Aruba RFPProtect WIPS
Wi-Fi Intrusion Prevention System
Wi-Fi Predictive Planning Tools
Wi-Fi Vulnerability Scanning Tools
Wireless Penetration Testing

Module 16: Evading IDS, Firewalls, and Honeypots

Intrusion Detection Systems (IDS) and its Placement
How IDS Works?
Ways to Detect an Intrusion
Types of Intrusion Detection Systems
System Integrity Verifiers (SIV)
General Indications of Intrusions
General Indications of System Intrusions
Firewall
DeMilitarized Zone (DMZ)
Types of Firewall
Firewall Identification
Honeypot
How to Set Up a Honeypot?
Intrusion Detection Tool
Intrusion Detection Systems: Tipping Point
Firewall: Sunbelt Personal Firewall
Honeypot Tools
Insertion Attack
Evasion
Denial-of-Service Attack (DoS)
Obfuscating
False Positive Generation
Session Splicing
Unicode Evasion Technique
Fragmentation Attack
Overlapping Fragments

Time-To-Live Attacks
Invalid RST Packets
Urgency Flag
Polymorphic Shellcode
ASCII Shellcode
Application-Layer Attacks
Desynchronization
Pre Connection SYN
Post Connection SYN
Other Types of Evasion
Bypass Blocked Sites Using IP Address in Place of URL
Bypass a Firewall using Proxy Server
Detecting Honeypots
HoneyPot Detecting Tool: Send-Safe
HoneyPot Hunter
Firewall Evasion Tools
Packet Fragment Generators
Countermeasures
Firewall/IDS Penetration Testing

Module 17: Buffer Overflow

Buffer Overflows
Why are Programs And Applications Vulnerable?
Understanding Stacks
Stack-Based Buffer Overflow
Understanding Heap
Stack Operations
Knowledge Required to Program Buffer Overflow Exploits
Buffer Overflow Steps
Simple Uncontrolled Overflow
Simple Buffer Overflow in C
Code Analysis
Exploiting Semantic Comments in C (Annotations)
How to Mutate a Buffer Overflow Exploit?
Identifying Buffer Overflows
How to Detect Buffer Overflows in a Program?
BOU (Buffer Overflow Utility)
Testing for Heap Overflow Conditions: heap.exe
Steps for Testing for Stack Overflow in OllyDbg Debugger
Testing for Format String Conditions using IDA Pro
BoF Detection Tools
Defense Against Buffer Overflows
Data Execution Prevention (DEP)
Enhanced Mitigation Experience Toolkit (EMET)
/GS http://microsoft.com
BoF Security Tools
Buffer Overflow Penetration Testing

Module 18: Cryptography

Cryptography
Types of Cryptography
Government Access to Keys (GAK)
Ciphers
Advanced Encryption Standard (AES)
Data Encryption Standard (DES)
RC4, RC5, RC6 Algorithms
The DSA and Related Signature Schemes
RSA (Rivest Shamir Adleman)
Message Digest (One-way Bash) Functions
Secure Hashing Algorithm (SHA)
What is SSH (Secure Shell)?
MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles
Cryptography Tool: Advanced Encryption Package
Cryptography Tools
Public Key Infrastructure (PKI)
Certification Authorities
Digital Signature
SSL (Secure Sockets Layer)
Transport Layer Security (TLS)
Disk Encryption
Cryptography Attacks
Code Breaking Methodologies
Meet-in-the-Middle Attack on Digital Signature Schemes
Cryptanalysis Tool: CrypTool
Cryptanalysis Tools
Online MD5 Decryption Tool

Module 19: Penetration Testing

Introduction to Penetration Testing
Security Assessments
Vulnerability Assessment
Penetration Testing
Why Penetration Testing?
What Should be Tested?
What Makes a Good Penetration Test?
ROI on Penetration Testing
Testing Points
Testing Locations
Types of Penetration Testing

Common Penetration Testing Techniques
Using DNS Domain Name and IP Address Information
Enumerating Information about Hosts on Publicly-Available Networks
Phases of Penetration Testing
Penetration Testing Methodology
Outsourcing Penetration Testing Services
Evaluating Different Types of Pentest Tools
Application Security Assessment Tool
Network Security Assessment Tool
Wireless/Remote Access Assessment Tool
Telephony Security Assessment Tool
Testing Network-Filtering Device Tool