CEH Eğitimi İçeriği

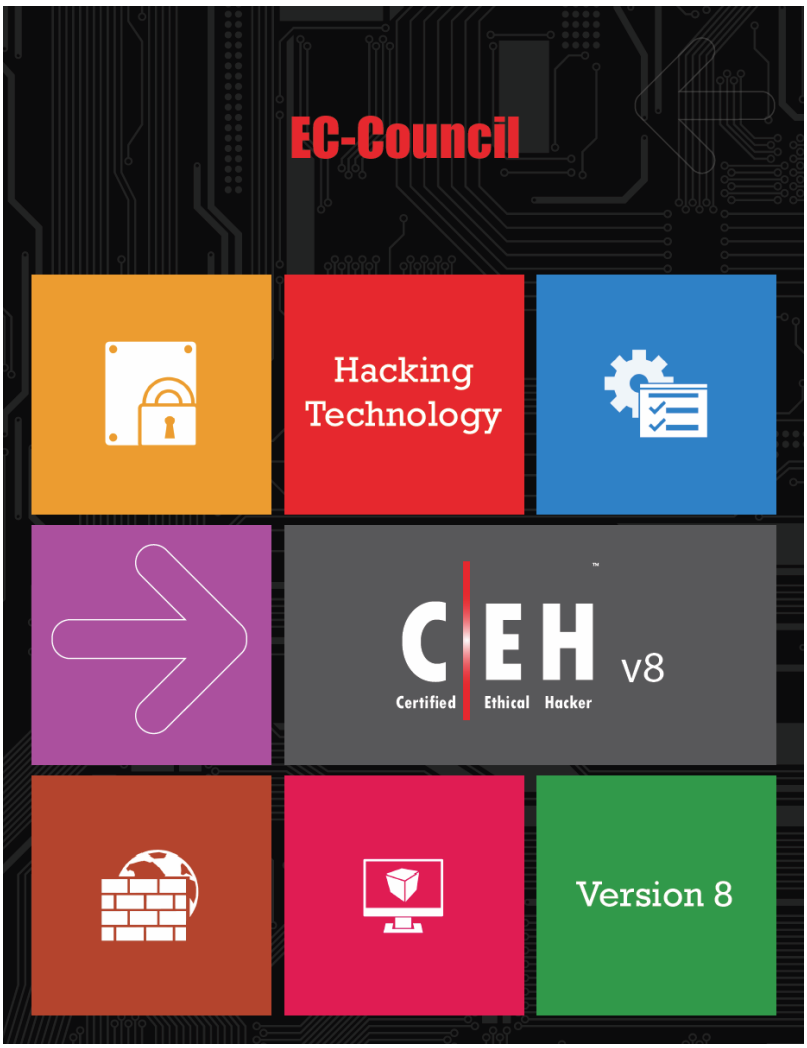
Öngereksinimler: Microsoft ve Linux Sistemleri hakkında bilgi, giriş seviye network bilgisi.

Kurs Tanımı:

CEH katılımcıları deneyimli güvenlik uzmanlarının seviyesine yükseltmek için detaylı bir Ethical Hacking ve network güvenliği eğitimi programıdır.

Kurs İçeriği:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- System Hacking
- Trojans and Backdoors
- Viruses and Worms
- Sniffers
- Social Engineering
- Denial of Service
- Session Hijacking
- Hacking Webservers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Evading IDS, Firewalls and Honeypots
- Buffer Overflows
- Cryptography
- Penetration Testing



Meşrutiyet Caddesi 12/10 Kızılay/ANKARA
0312 417 0 CLI info@cliguru.com
0312 417 0 254 www.cliguru.com

Ayrıntılı İçerik:

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
  - Effects of Hacking on Business
- Who is a Hacker?
- Hacker Classes
- Hacktivism
- What Does a Hacker Do?
- Phase 1 - Reconnaissance
  - Reconnaissance Types
- Phase 2 - Scanning
- Phase 3 - Gaining Access
- Phase 4 - Maintaining Access
- Phase 5 - Covering Tracks
- Types of Attacks on a System
  - Operating System Attacks
  - Application-Level Attacks
  - Shrink Wrap Code Attacks
  - Misconfiguration Attacks
- Why Ethical Hacking is Necessary?
- Defense in Depth
- Scope and Limitations of Ethical Hacking
- What Do Ethical Hackers Do?
- Skills of an Ethical Hacker
- Vulnerability Research
- Vulnerability Research Websites
- What is Penetration Testing?
- Why Penetration Testing?
- Penetration Testing Methodology

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
  - Tools to Extract Company's Data
- Footprinting Through Search Engines
- Collect Location Information
  - Satellite Picture of a Residence
- People Search
  - People Search Using http://pipl.com
  - People Search Online Services
  - People Search on Social Networking Services
- Gather Information from Financial Services
- Footprinting Through Job Sites
- Monitoring Target Using Alerts
- Competitive Intelligence Gathering
- Competitive Intelligence-When Did this Company Begin? How Did it Develop?
- Competitive Intelligence-What are the Company's Plans?
- Competitive Intelligence-What Expert Opinion Say About the Company?
- Competitive Intelligence Tools
- Competitive Intelligence Consulting Companies

- WHOIS Lookup
  - WHOIS Lookup
  - WHOIS Lookup Tools: SmartWhois
  - WHOIS Lookup Tools
  - WHOIS Lookup Online Tools
- Extracting DNS Information
  - DNS Interrogation Tools
  - DNS Interrogation Online Tools
- Locate the Network Range
- Traceroute
  - Traceroute Analysis
  - Traceroute Tool: 3D Traceroute
  - Traceroute Tool: LoriotPro
  - Traceroute Tool: Path Analyzer Pro
  - Traceroute Tools
- Mirroring Entire Website
  - Website Mirroring Tools
  - Mirroring Entire Website Tools
- Extract Website Information from http://www.archive.org
- Monitoring Web Updates Using Website Watcher
- Tracking Email Communications

  - Email Tracking Tools
- Footprint Using Google Hacking Techniques
- What a Hacker Can Do With Google Hacking?
- Google Advance Search Operators
  - Finding Resources using Google Advance Operator
- Google Hacking Tool: Google Hacking Database (GHDB)
- Google Hacking Tools
- Additional Footprinting Tools
- Additional Footprinting Tools
- Footprinting Pen Testing

Scanning Networks

- Network Scanning
- Types of Scanning
- Checking for Live Systems - ICMP Scanning
- Ping Sweep
  - Ping Sweep Tools
- Three-Way Handshake
- TCP Communication Flags
  - Create Custom Packet using TCP Flags
- Create Custom Packet using TCP Flags
- Hping Commands
- Scanning Techniques
  - TCP Connect / Full Open Scan
  - Stealth Scan (Half-open Scan)
  - Xmas Scan
  - FIN Scan
  - NULL Scan
  - IDLE Scan
    - IDLE Scan: Step 1
    - IDLE Scan: Step 2.1 (Open Port)
    - IDLE Scan: Step 2.1 (Open Port)
    - IDLE Scan: Step 3
  - ICMP Echo Scanning/List Scan
  - SYN/FIN Scanning Using IP Fragments
  - UDP Scanning
  - Inverse TCP Flag Scanning
  - ACK Flag Scanning
- 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)
- Scanning Countermeasures
- War Dialing
- Why War Dialing?
- War Dialing Tools
- War Dialing Countermeasures
  - War Dialing Countermeasures: SandTrap Tool
- OS Fingerprinting
  - Active Banner Grabbing Using Telnet
- Banner Grabbing Tool: ID Serve
- GET REQUESTS
- Banner Grabbing Tool: Netcraft
- Banner Grabbing Tools
- Banner Grabbing Countermeasures: Disabling or Changing Banner
- Hiding File Extensions

- Hiding File Extensions from Webpages
- Vulnerability Scanning
  - Vulnerability Scanning Tool: Nessus
  - Vulnerability Scanning Tool: SAINT
  - Active Banner Grabbing Using Telnet
- Network Vulnerability Scanners
- LANsurveyor
- Network Mappers
- Proxy Servers
- Why Attackers Use Proxy Servers?
- Use of Proxies for Attack
- How Does MultiProxy Work?
- Free Proxy Servers
- Proxy Workbench
- Proxifier Tool: Create Chain of Proxy Servers
- SocksChain
- TOR (The Onion Routing)
- TOR Proxy Chaining Software
- HTTP Tunneling Techniques
- Why do I Need HTTP Tunneling?
- Super Network Tunnel Tool
- Httptunnel for Windows
- Additional HTTP Tunneling Tools
- SSH Tunneling
- SSL Proxy Tool
- How to Run SSL Proxy?
- Proxy Tools
- Anonymizers
- Types of Anonymizers
- Case: Bloggers Write Text Backwards to Bypass Web Filters in China
- Text Conversion to Avoid Filters
- Censorship Circumvention Tool: Psiphon
- How Psiphon Works?
- How to Check if Your Website is Blocked in China or Not?
- How to Check if Your Website is Blocked in China or Not?
- Anonymizer Tools
- Spoofing IP Address
- IP Spoofing Detection Techniques: Direct TTL Probes
- IP Spoofing Detection Techniques: IP Identification Number
- IP Spoofing Detection Techniques: TCP Flow Control Method
- IP Spoofing Countermeasures
- Scanning Pen Testing

Enumeration

- What is Enumeration?
- Techniques for Enumeration
- Netbios Enumeration
  - NetBIOS Enumeration Tool: SuperScan
  - NetBIOS Enumeration Tool: NetBIOS Enumerator
- Enumerating User Accounts
- Enumerate Systems Using Default Passwords
- SNMP (Simple Network Management Protocol) Enumeration
  - Management Information Base (MIB)
  - SNMP Enumeration Tool: OpUtils Network Monitoring Toolset
  - SNMP Enumeration Tool: SolarWinds
  - SNMP Enumeration Tools
- UNIX/Linux Enumeration
  - Linux Enumeration Tool: Enum4linux
- LDAP Enumeration
  - LDAP Enumeration Tool: JXplorer
  - LDAP Enumeration Tool
- NTP Enumeration
  - NTP Server Discovery Tool: NTP Server Scanner
  - NTP Server: PresenTense Time Server
  - NTP Enumeration Tools
- SMTP Enumeration
  - SMTP Enumeration Tool: NetScanTools Pro
- DNS Zone Transfer Enumeration Using nslookup
  - DNS Analyzing and Enumeration Tool: The Men & Mice Suite
- Enumeration Countermeasures
  - SMB Enumeration Countermeasures
  - Enumeration Pen Testing

System Hacking

- Information at Hand Before System Hacking Stage
- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- Password Cracking
  - Password Complexity
  - Password Cracking Techniques
  - Types of Password Attacks
    - Passive Online Attacks: Wire Sniffing
    - Password Sniffing
    - Passive Online Attack: Man-in-the-Middle and Replay Attack
    - Active Online Attack: Password Guessing
      - Active Online Attack: Trojan/Spyware/Keylogger
      - Active Online Attack: Hash Injection Attack
    - Rainbow Attacks: Pre-Computed Hash
    - Distributed Network Attack
      - Elcomsoft Distributed Password Recovery
    - Non-Electronic Attacks
      - Default Passwords
    - Manual Password Cracking (Guessing)
    - Automatic Password Cracking Algorithm
    - Stealing Passwords Using USB Drive
- Microsoft Authentication
- How Hash Passwords are Stored in Windows SAM?
- What is LAN Manager Hash?
  - LM "Hash" Generation
  - LM, NTLMv1, and NTLMv2
  - NTLM Authentication Process
- Kerberos Authentication
- Salting
- PWdump7 and Fgdump
- L0phtCrack
- Ophcrack
- Cain & Abel
- RainbowCrack
- Password Cracking Tools
- LM Hash Backward Compatibility
  - How to Disable LM HASH?
- How to Defend against Password Cracking?
  - Implement and Enforce Strong Security Policy
- Privilege Escalation
  - Escalation of Privileges
- 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
  - Keylogger: Advanced Keylogger
  - Keylogger: Spytech SpyAgent
  - Keylogger: Perfect Keylogger
  - Keylogger: Powered Keylogger
  - Keylogger for Mac: Aobo Mac OS X KeyLogger
  - Keylogger for Mac: Perfect Keylogger for Mac
  - Hardware Keylogger: KeyGhost
- Keyloggers
- Spyware
  - What Does the Spyware Do?
  - Types of Spywares
    - Desktop Spyware
      - Desktop Spyware: Activity Monitor
    - Email and Internet Spyware
      - Email and Internet Spyware: eBLASTER
    - Internet and E-mail Spyware
    - Child Monitoring Spyware
      - Child Monitoring Spyware: Advanced Parental Control
    - Screen Capturing Spyware
      - Screen Capturing Spyware: Spector Pro
    - USB Spyware
      - USB Spyware: USBDumper
    - Audio Spyware
      - Audio Spyware: RoboNanny, Stealth Recorder Pro and Spy Voice Recorder
    - Video Spyware /li>
      - Video Spyware: Net Video Spy
    - Print Spyware
      - Print Spyware: Printer Activity Monitor
    - Telephone/Cellphone Spyware
    - Cellphone Spyware: Mobile Spy
    - GPS Spyware
      - GPS Spyware: GPS TrackMaker
- How to Defend against Keyloggers?
  - Anti-Keylogger
  - Anti-Keylogger: Zemana AntiLogger
  - Anti-Keyloggers
- How to Defend against Spyware?
  - Anti-Spyware: Spyware Doctor
- Rootkits
- Types of Rootkits
- How Rootkit Works?
- Rootkit: Fu
- Detecting Rootkits

- Steps for Detecting Rootkits
- How to Defend against Rootkits?
- Anti-Rootkit: RootkitRevealer and McAfee Rootkit Detective
- NTFS Data Stream
  - How to Create NTFS Streams?
  - NTFS Stream Manipulation
  - How to Defend against NTFS Streams?
  - NTFS Stream Detector: ADS Scan Engine
  - NTFS Stream Detectors
- What is Steganography?
  - Steganography Techniques
  - How Steganography Works?
- Types of Steganography
  - Whitespace Steganography Tool: SNOW
- Image Steganography
  - Image Steganography: Hermetic Stego
  - Image Steganography Tools
- Document Steganography: wbStego
  - Document Steganography Tools
- Video Steganography: Our Secret
  - Video Steganography Tools
- Audio Steganography: Mp3stegz
  - Audio Steganography Tools
- Folder Steganography: Invisible Secrets 4
  - Folder Steganography Tools
- Spam/Email Steganography: Spam Mimic
- Natural Text Steganography: Sams Big G Play Maker
- Steganalysis
  - Steganalysis Methods/Attacks on Steganography
- Steganography Detection Tool: Stegdetect
  - Steganography Detection Tools
- Why Cover Tracks?
  - Covering Tracks
- Ways to Clear Online Tracks
- Disabling Auditing: Auditpol
- Covering Tracks Tool: Window Washer
- Covering Tracks Tool: Tracks Eraser Pro
  - Track Covering Tools
- System Hacking Penetration Testing

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
  - Wrapper Covert Programs
- Different Ways a Trojan can Get into a System
- How to Deploy a Trojan?
- Evading Anti-Virus Techniques
- Types of Trojans
  - Command Shell Trojans
    - Command Shell Trojan: Netcat
  - GUI Trojan: MoSucker
    - GUI Trojan: Jumper and Biodox
  - Document Trojans
  - E-mail Trojans
    - E-mail Trojans: RemoteByMail
  - Defacement Trojans
    - Defacement Trojans: Restorator
  - Botnet Trojans
    - Botnet Trojan: Illusion Bot
    - Botnet Trojan: NetBot Attacker
  - Proxy Server Trojans
    - Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)
  - FTP Trojans
    - FTP Trojan: TinyFTPD
  - VNC Trojans
  - HTTP/HTTPS Trojans
    - HTTP Trojan: HTTP RAT
  - Shttpd Trojan - HTTPS (SSL)
  - ICMP Tunneling
    - ICMP Trojan: icmpsend
  - Remote Access Trojans
    - Remote Access Trojan: RAT DarkComet
    - Remote Access Trojan: Apocalypse
  - Covert Channel Trojan: CCTT
  - E-banking Trojans
  - Banking Trojan Analysis
    - E-banking Trojan: ZeuS
- 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?
  - Scanning for Suspicious Ports
  - Port Monitoring Tool: IceSword
  - Port Monitoring Tools: CurrPorts and TCPView
  - Scanning for Suspicious Processes
- Process Monitoring Tool: What's Running
  - Process Monitoring Tools
- Scanning for Suspicious Registry Entries
- Registry Entry Monitoring Tools
- Scanning for Suspicious Device Drivers
  - Device Drivers Monitoring Tools: DriverView
  - Device Drivers Monitoring Tool
- Scanning for Suspicious Windows Services
  - Windows Services Monitoring Tools: Windows Service Manager (SrvMan)
  - Windows Services Monitoring Tools
- Scanning for Suspicious Startup Programs
  - Windows7 Startup Registry Entries
  - Startup Programs Monitoring Tools: Starter
  - Startup Programs Monitoring Tools: Security AutoRun
  - Startup Programs Monitoring Tools
- Scanning for Suspicious Files and Folders
  - Files and Folder Integrity Checker: FastSum and WinMD5
  - Files and Folder Integrity Checker
- Scanning for Suspicious Network Activities
  - Detecting Trojans and Worms with Capsa Network Analyzer
- Trojan Countermeasures
- Backdoor Countermeasures
- Trojan Horse Construction Kit
- Anti-Trojan Software: TrojanHunter
- Anti-Trojan Software: Emsisoft Anti-Malware
- Anti-Trojan Softwares
- Pen Testing for Trojans and Backdoors

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:
  - W32/Sality AA
  - W32/Toal-A
  - W32/Virut
  - Klez
- Types of Viruses
  - System or Boot Sector Viruses
  - File and Multipartite Viruses
  - Macro Viruses
  - Cluster Viruses
  - Stealth/Tunneling Viruses
  - Encryption Viruses
  - Polymorphic Code
  - Metamorphic Viruses
  - File Overwriting or Cavity Viruses
  - Sparse Infector Viruses
  - Companion/Camouflage Viruses
  - Shell Viruses
  - File Extension Viruses
  - Add-on and Intrusive Viruses
- Transient and Terminate and Stay Resident Viruses
- Writing a Simple Virus Program
  - Terabit Virus Maker
  - JPS Virus Maker
  - DELmE's Batch Virus Maker
- Computer Worms
- How is a Worm Different from a Virus?
- Example of Worm Infection: Conficker Worm
  - What does the Conficker Worm do?
  - How does the Conficker Worm Work?
- Worm Analysis:
  - W32/Netsky
  - W32/Bagle.GE
- Worm Maker: Internet Worm Maker Thing
- 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:
  - Sunbelt CWSandbo
  - VirusTotal
- Online Malware Analysis Services
- Virus Detection Methods
- Virus and Worms Countermeasures
- Companion Antivirus: Immunet Protect
- Anti-virus Tools
- Penetration Testing for Virus

Sniffers

- Lawful Intercept
  - Benefits of Lawful Intercept
  - Network Components Used for Lawful Intercept
- Wiretapping
- Sniffing Threats
- How a Sniffer Works?
- Hacker Attacking a Switch
- Types of Sniffing: Passive Sniffing
- Types of Sniffing: Active Sniffing
- Protocols Vulnerable to Sniffing
- Tie to Data Link Layer in OSI Model
- Hardware Protocol Analyzers
- SPAN Port
- MAC Flooding
  - MAC Address/CAM Table
  - How CAM Works?
  - What Happens When CAM Table is Full?
  - Mac Flooding Switches with macof
  - MAC Flooding Tool: Yersinia
  - How to Defend against MAC Attacks?
- How DHCP Works?
  - DHCP Request/Reply Messages
  - IPv4 DHCP Packet Format
  - DHCP Starvation Attack
  - Rogue DHCP Server Attack
  - DHCP Starvation Attack Tool: Gobbler
  - How to Defend Against DHCP Starvation and Rogue Server Attack?
- What is Address Resolution Protocol (ARP)?
  - ARP Spoofing Attack
  - How Does ARP Spoofing Work?
  - Threats of ARP Poisoning
  - ARP Poisoning Tool: Cain and Abel
  - ARP Poisoning Tool: WinArpAttacker
  - ARP Poisoning Tool: Ufasoft Snif
  - How to Defend Against ARP Poisoning? Use DHCP Snooping Binding Table and Dynamic ARP Inspection
- Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
- MAC Spoofing/Duplicating
  - Spoofing Attack Threats
  - MAC Spoofing Tool: SMAC
  - How to Defend Against MAC Spoofing? Use DHCP Snooping Binding Table, Dynamic ARP Inspection and IP Source Guard
- DNS Poisoning Techniques
  - Intranet DNS Spoofing
  - Internet DNS Spoofing
  - Proxy Server DNS Poisoning

- DNS Cache Poisoning
- How to Defend Against DNS Spoofing?

- Sniffing Tool: Wireshark
  - Follow TCP Stream in Wireshark
  - Display Filters in Wireshark
  - Additional Wireshark Filters
- Sniffing Tool: CACE Pilot
- Sniffing Tool: Tcpdump/Windump
- 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
- 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: PromqryUI
- Promiscuous Detection Tool: PromiScan

Social Engineering

- What is Social Engineering?
- Behaviors Vulnerable to Attacks
  - Factors that Make Companies 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
  - Common Targets of Social Engineering: Office Workers
- Types of Social Engineering
  - Human-Based Social Engineering
- Types of Social Engineering
  - Human-Based Social Engineering
    - Technical Support Example
    - Authority Support Example
    - Human-based Social Engineering: Dumpster Diving
  - Computer-Based Social Engineering
    - Computer-Based Social Engineering: Pop-Ups
    - Computer-Based Social Engineering: Phishing
  - Social Engineering Using SMS
  - Social Engineering by a "Fake SMS Spying Tool"
- Insider Attack
  - Disgruntled Employee
  - Preventing Insider Threats
- Common Intrusion Tactics and Strategies for Prevention
- Social Engineering Through Impersonation on Social Networking Sites
  - Social Engineering Example: LinkedIn Profile
  - Social Engineering on Facebook
  - Social Engineering on Twitter
  - Social Engineering on Orkut
  - Social Engineering on MySpace
- Risks of Social Networking to Corporate Networks
- Identity Theft Statistics 2010
  - Identify Theft
  - How to Steal an Identity?
  - STEP 1
  - STEP 2
  - STEP 3
- Real Steven Gets Huge Credit Card Statement
- Identity Theft - Serious Problem
- Social Engineering Countermeasures: Policies
  - Social Engineering Countermeasures
- How to Detect Phishing Emails?
  - Anti-Phishing Toolbar: Netcraft
  - Anti-Phishing Toolbar: PhishTank

- Identity Theft Countermeasures
- Social Engineering Pen Testing
  - Social Engineering Pen Testing: Using Emails
  - Social Engineering Pen Testing: Using Phone
  - Social Engineering Pen Testing: In Person

Denial of Service

- What is a Denial of Service Attack?
- What is Distributed Denial of Service Attacks?
  - How Distributed Denial of Service Attacks Work?
- Symptoms of a DoS Attack
- Cyber Criminals
  - Organized Cyber Crime: Organizational Chart
- Internet Chat Query (ICQ)
- Internet Relay Chat (IRC)
- DoS Attack Techniques
  - Bandwidth Attacks
  - Service Request Floods
  - SYN Attack
  - SYN Flooding
  - ICMP Flood Attack
  - Peer-to-Peer Attacks
  - Permanent Denial-of-Service Attack
  - Application Level Flood Attacks
- Botnet
  - Botnet Propagation Technique
  - Botnet Ecosystem
  - Botnet Trojan: Shark
  - Poison Ivy: Botnet Command Control Center
  - Botnet Trojan: PlugBot
- WikiLeak Operation Payback
  - DDoS Attack
  - DDoS Attack Tool: LOIC
  - Denial of Service Attack Against MasterCard, Visa, and Swiss Banks
  - Hackers Advertise Links to Download Botnet
- DoS Attack Tools
- Detection Techniques
  - Activity Profiling
  - Wavelet Analysis
  - Sequential Change-Point Detection
- DoS/DDoS Countermeasure Strategies
- DDoS Attack Countermeasures
  - DoS/DDoS Countermeasures: Protect Secondary Victims
  - DoS/DDoS Countermeasures: Detect and Neutralize Handlers
  - DoS/DDoS Countermeasures: Detect Potential Attacks
  - DoS/DDoS Countermeasures: Deflect Attacks
  - DoS/DDoS Countermeasures: Mitigate Attacks
- 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

Session Hijacking

- What is Session Hijacking?
- Dangers Posed by Hijacking
- Why Session Hijacking is Successful?
- Key Session Hijacking Techniques
- Brute Forcing
  - Brute Forcing Attack
- HTTP Referrer Attack
- Spoofing vs. Hijacking
- Session Hijacking Process
- Packet Analysis of a Local Session Hijack
- Types of Session Hijacking
  - Session Hijacking in OSI Model
  - Application Level Session Hijacking
  - Session Sniffing
- Predictable Session Token
  - How to Predict a Session Token?
- Man-in-the-Middle Attack
- Man-in-the-Browser Attack
  - Steps to Perform Man-in-the-Browser Attack
- Client-side Attacks
- Cross-site Script Attack
- Session Fixation
  - Session Fixation Attack
- Network Level Session Hijacking
- The 3-Way Handshake
- Sequence Numbers
  - Sequence Number Prediction
- 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
  - Paros
  - Burp Suite
  - Firesheep
- 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
  - Modes of IPSec
  - IPSec Architecture

- IPSec Authentication and Confidentiality
- Components of IPSec
- IPSec Implementation
- Session Hijacking Pen Testing

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
  - Example
- 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
  - Webserver Password Cracking Techniques
- Web Application Attacks
- Webserver Attack Methodology
  - Information Gathering
  - Webserver Footprinting
    - Webserver Footprinting Tools
  - Mirroring a Website
  - Vulnerability Scanning
  - Session Hijacking
  - Hacking Web Passwords
- Webserver Attack Tools
  - Metasploit
    - Metasploit Architecture
    - Metasploit Exploit Module
    - Metasploit Payload Module
    - Metasploit Auxiliary Module
    - Metasploit NOPS Module
  - Wfetch
- Web Password Cracking Tool
  - Brutus
  - THC-Hydra
- Countermeasures
  - Patches and Updates
  - Protocols
  - Accounts
  - Files and Directories
- 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)
    - Patch Management Tools
- Web Application Security Scanner: Sandcat
- Web Server Security Scanner: Wikto
- Webserver Malware Infection Monitoring Tool: HackAlert
- Webserver Security Tools
- Web Server Penetration Testing

Hijacking 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
  - SQL Injection Attacks
  - Command Injection Attacks
  - Command Injection Example
  - File Injection Attack
- What is LDAP Injection?
- How LDAP Injection Works?
- Hidden Field Manipulation Attack
- Cross-Site Scripting (XSS) Attacks
  - How XSS Attacks Work?
  - Cross-Site Scripting Attack Scenario: Attack via Email
  - XSS Example: Attack via Email
  - XSS Example: Stealing Users' Cookies
  - XSS Example: Sending an Unauthorized Request
  - XSS Attack in Blog Posting
  - XSS Attack in Comment Field
  - XSS Cheat Sheet
  - Cross-Site Request Forgery (CSRF) Attack
  - How CSRF Attacks Work?
- Web Application Denial-of-Service (DoS) Attack
  - Denial of Service (DoS) Examples
- Buffer Overflow Attacks
- Cookie/Session Poisoning
  - How Cookie Poisoning Works?
- 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
  - Web Services Attack

- Web Services Footprinting Attack
- Web Services XML Poisoning

- Footprint Web Infrastructure
  - Footprint Web Infrastructure: Server Discovery
  - Footprint Web Infrastructure: Server Identification/Banner Grabbing
  - Footprint Web Infrastructure: Hidden Content Discovery
- Web Spidering Using Burp Suite
- Hacking Web Servers
  - Web Server Hacking Tool: WebInspect
- Analyze Web Applications
  - Analyze Web Applications: Identify Entry Points for User Input
  - Analyze Web Applications: Identify Server-Side Technologies
  - Analyze Web Applications: Identify Server-Side Functionality
  - Analyze Web Applications: Map the Attack Surface
- Attack Authentication Mechanism
- Username Enumeration
- Password Attacks: Password Guessing
- Password Attacks: Brute-forcing
- Session Attacks: Session ID Prediction/ Brute-forcing
- Cookie Exploitation: Cookie Poisoning
- Authorization Attack
  - HTTP Request Tampering
  - Authorization Attack: Cookie Parameter Tampering
- Session Management Attack
  - Attacking Session Token Generation Mechanism
  - Attacking Session Tokens Handling Mechanism: Session Token Sniffing
- Injection Attacks
- Attack Data Connectivity
  - Connection String Injection
  - Connection String Parameter Pollution (CSPP) Attacks
  - Connection Pool DoS
- Attack Web App Client
- Attack Web Services
- Web Services Probing Attacks
  - Web Service Attacks: SOAP Injection
  - Web Service Attacks: XML Injection
  - Web Services Parsing 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
  - Web Application Hacking Tools
- Encoding Schemes
  - How to Defend Against SQL Injection Attacks?
  - How to Defend Against Command Injection Flaws?
  - How to Defend Against XSS Attacks?
  - How to Defend Against DoS Attack?
  - How to Defend Against Web Services Attack?

- Web Application Countermeasures
  - How to Defend Against Web Application Attacks?
  - Web Application Security Tool: Acunetix Web Vulnerability Scanner
  - Web Application Security Tool: Falcove Web Vulnerability Scanner
  - Web Application Security Scanner: Netsparker
  - Web Application Security Tool: N-Stalker Web Application Security Scanner
  - Web Application Security Tools
- Web Application Firewall: dotDefender
- Web Application Firewall: IBM AppScan
- Web Application Firewall: ServerDefender VP
  - Web Application Firewall
- Web Application Pen Testing
  - Information Gathering
  - Configuration Management Testing
  - Authentication Testing
  - Session Management Testing
  - Authorization Testing
  - Data Validation Testing
  - Denial of Service Testing
  - Web Services Testing
  - AJAX Testing

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
  - Example 1: Normal SQL Query
  - Example 1: SQL Injection Query
  - Example 1: Code Analysis
  - Example 2: BadProductList.aspx
  - Example 2: Attack Analysis
  - Example 3: Updating Table
  - Example 4: Adding New Records
  - Example 5: Identifying the Table Name
  - Example 6: Deleting a Table
- SQL Injection Detection
  - SQL Injection Error Messages
  - SQL Injection Attack Characters
  - Additional Methods to Detect SQL Injection
- SQL Injection Black Box Pen Testing
  - Testing for SQL Injection
- Types of SQL Injection
  - Simple SQL Injection Attack
  - Union SQL Injection Example
  - SQL Injection Error Based
- What is Blind SQL Injection?
  - No Error Messages Returned
  - Blind SQL Injection: WAITFOR DELAY YES or NO Response
  - Blind SQL Injection - Exploitation (MySQL)
  - Blind SQL Injection - Extract Database User
  - Blind SQL Injection - Extract Database Name
  - Blind SQL Injection - Extract Column Name
  - Blind SQL Injection - Extract Data from ROWS
- SQL Injection Methodology
- Information Gathering
  - Extracting Information through Error Messages
  - Understanding SQL Query
  - Bypass Website Logins Using SQL Injection
- Database, Table, and Column Enumeration
  - Advanced Enumeration
- Features of Different DBMSs
  - Creating Database Accounts
- Password Grabbing
  - Grabbing SQL Server Hashes
  - Extracting SQL Hashes (In a Single Statement)

- Transfer Database to Attacker's Machine
- Interacting with the Operating System
- Interacting with the FileSystem
- Network Reconnaissance Full Query
- SQL Injection Tools
  - SQL Injection Tools: BSQLHacker
  - SQL Injection Tools: Marathon Tool
  - SQL Injection Tools: SQL Power Injector
  - SQL Injection Tools: Havij
- Evading IDS
  - Types of Signature Evasion Techniques
  - Evasion Technique: Sophisticated Matches
  - Evasion Technique: Hex Encoding
  - Evasion Technique: Manipulating White Spaces
  - Evasion Technique: In-line Comment
  - Evasion Technique: Char Encoding
  - Evasion Technique: String Concatenation
  - Evasion Technique: Obfuscated Codes
- How to Defend Against SQL Injection Attacks?
  - How to Defend Against SQL Injection Attacks: Use Type-Safe SQL Parameters
- SQL Injection Detection Tools
  - SQL Injection Detection Tool: Microsoft Source Code Analyzer
  - SQL Injection Detection Tool: Microsoft UrlScan
  - SQL Injection Detection Tool: dotDefender
  - SQL Injection Detection Tool: IBM AppScan
  - Snort Rule to Detect SQL Injection Attacks

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
  - Wi-Fi Authentication Process Using a Centralized Authentication Server
  - Wi-Fi Authentication Process
- Wireless Terminologies
- Wi-Fi Chalking
  - Wi-Fi Chalking Symbols
- Wi-Fi Hotspot Finder: jiwire.com
- Wi-Fi Hotspot Finder: WeFi.com
- Types of Wireless Antenna
- Parabolic Grid Antenna
- Types of Wireless Encryption
- WEP Encryption
  - How WEP Works?
- What is WPA?
  - How WPA Works?
- Temporal Keys
- What is WPA2?
  - How WPA2 Works?
- 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
  - GPS Mapping Tool: WIGLE
  - GPS Mapping Tool: Skyhook
- 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 Set Up a Fake Hotspot (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
  - Bluetooth Stack
  - Bluetooth Threats
- How to BlueJack a Victim?
- Bluetooth Hacking Tool: Super Bluetooth Hack
- Bluetooth Hacking Tool: PhoneSnoop
- Bluetooth Hacking Tool: BlueScanner
  - Bluetooth Hacking Tools
- 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 RFProtect WIPS
- Wi-Fi Intrusion Prevention System
- Wi-Fi Predictive Planning Tools
- Wi-Fi Vulnerability Scanning Tools
- Wireless Penetration Testing
  - Wireless Penetration Testing Framework
  - Wi-Fi Pen Testing Framework
  - Pen Testing LEAP Encrypted WLAN
  - Pen Testing WPA/WPA2 Encrypted WLAN
  - Pen Testing WEP Encrypted WLAN
  - Pen Testing Unencrypted WLAN

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
  - Firewall Architecture
- DeMilitarized Zone (DMZ)
- Types of Firewall
  - Packet Filtering Firewall
  - Circuit-Level Gateway Firewall
  - Application-Level Firewall
  - Stateful Multilayer Inspection Firewall
- Firewall Identification
  - Port Scanning
  - Firewalking
  - Banner Grabbing
- Honeypot
  - Types of Honeypots
- How to Set Up a Honeypot?
- Intrusion Detection Tool
  - Snort
  - Snort Rules
  - Rule Actions and IP Protocols
  - The Direction Operator and IP Addresses
  - Port Numbers
- Intrusion Detection Systems: Tipping Point
  - Intrusion Detection Tools
- Firewall: Sunbelt Personal Firewall
  - Firewalls
- Honeypot Tools
  - KFSensor
  - SPECTER
- 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
  - IP Address Spoofing
  - Attacking Session Token Generation Mechanism
  - Tiny Fragments
- Bypass Blocked Sites Using IP Address in Place of URL
  - Bypass Blocked Sites Using Anonymous Website Surfing Sites
- Bypass a Firewall using Proxy Server
  - Bypassing Firewall through ICMP Tunneling Method
  - Bypassing Firewall through ACK Tunneling Method
  - Bypassing Firewall through HTTP Tunneling Method
  - Bypassing Firewall through External Systems
  - Bypassing Firewall through MITM Attack
- Detecting Honeypots
- Honeypot Detecting Tool: Send-Safe Honeypot Hunter
- Firewall Evasion Tools
  - Traffic IQ Professional
  - tcp-over-dns
  -
- Packet Fragment Generators
- Countermeasures
- Firewall/IDS Penetration Testing
  - Firewall Penetration Testing
  - IDS Penetration Testing

Buffer Overflow

- Buffer Overflows
- Why are Programs And Applications Vulnerable?
- Understanding Stacks
- Stack-Based Buffer Overflow
- Understanding Heap
  - Heap-Based Buffer Overflow
- Stack Operations
  - Shellcode
  - No Operations (NOPs)
- Knowledge Required to Program Buffer Overflow Exploits
- Buffer Overflow Steps
  - Attacking a Real Program
  - Format String Problem
  - Overflow using Format String
  - Smashing the Stack
  - Once the Stack is Smashed...
- 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 Stack Overflow in OllyDbg Debugger
- Testing for Format String Conditions using IDA Pro
- BoF Detection Tools
- Defense Against Buffer Overflows
  - Preventing BoF Attacks
  - Programming Countermeasures
- Data Execution Prevention (DEP)
- Enhanced Mitigation Experience Toolkit (EMET)
  - EMET System Configuration Settings
  - EMET Application Configuration Window
- /GS http://microsoft.com
- BoF Security Tools
  - BufferShield
  - Buffer Overflow Penetration Testing

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)
    - Example of RSA Algorithm
    - The RSA Signature Scheme
- Message Digest (One-way Bash) Functions
    - Message Digest Function: MD5
- 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
    - Disk Encryption Tool: TrueCrypt
    - Disk Encryption Tools
- Cryptography Attacks
- Code Breaking Methodologies
    - Brute-Force Attack
- Meet-in-the-Middle Attack on Digital Signature Schemes
- Cryptanalysis Tool: CrypTool
- Cryptanalysis Tools
- Online MD5 Decryption Tool

Penetration Testing

- Introduction to Penetration Testing
- Security Assessments
- Vulnerability Assessment
    - Limitations of 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
    - External Penetration Testing
    - Internal Security Assessment
    - Black-box Penetration Testing
    - Grey-box Penetration Testing
    - White-box Penetration Testing
    - Announced / Unannounced Testing
    - Automated Testing
    - Manual 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
    - Pre-Attack Phase
    - Attack Phase
        - Activity: Perimeter Testing
        - Enumerating Devices
        - Activity: Acquiring Target
        - Activity: Escalating Privileges
        - Activity: Execute, Implant, and Retract
    - Post-Attack Phase and Activities
        - Penetration Testing Deliverable Templates
- Penetration Testing Methodology
    - Application Security Assessment
        - Web Application Testing - I
        - Web Application Testing - II
        - Web Application Testing - III
    - Network Security Assessment
    - Wireless/Remote Access Assessment
        - Wireless Testing
    - Telephony Security Assessment
    - Social Engineering
    - Testing Network-Filtering Devices
    - Denial of Service Emulation
- Outsourcing Penetration Testing Services

    - Terms of Engagement
    - Project Scope
    - Project Scope
    - Penetration Testing Consultants
    - Denial of Service Emulation
- Evaluating Different Types of Pentest Tools
- Application Security Assessment Tool
    - Webscarab
- Network Security Assessment Tool
    - Angry IP scanner
    - GFI LANguard
- Wireless/Remote Access Assessment Tool
    - Kismet
- Telephony Security Assessment Tool
    - Omnipee
- Testing Network-Filtering Device Tool
- Traffic IQ Professional