

## Certified Ethical Hacking and Countermeasures v6.1

**Course Code:** CEH61PB

**Length:** 5 Days (10am-6pm)

**Course Description:** Computers around the world are systematically being victimized by rampant hacking. This hacking is not only widespread, but is being executed so flawlessly that the attackers compromise a system, steal everything of value and completely erase their tracks within 20 minutes. The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits. This philosophy stems from the proven practice of trying to catch a thief, by thinking like a thief. As technology advances and organization depend on technology increasingly, information assets have evolved into critical components of survival.

The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

### Prerequisites

Students are required to have taken EC Council's ENSA course, **or** have equivalent experience.

### Certification

The CEH 312-50 online Prometric exam needs to be passed by students following training to receive the CEH certification.

### Legal Agreement

Ethical Hacking and Countermeasures course mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only. 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.

### Outline

#### Lesson 1: Introduction to Ethical Hacking

- Topic 1A: Problem Definition - Why Security?
- Topic 1B: Essential Terminologies
- Topic 1C: Elements of Security
- Topic 1D: The Security, Functionality and Ease of Use Triangle
- Topic 1E: Case Study
- Topic 1F: What Does a Malicious Hacker Do?
- Topic 1G: Types of Hacker Attacks
- Topic 1H: Hactivism



- Topic 1I: Hacker Classes
- Topic 1J: Security News: Suicide Hacker
- Topic 1K: Ethical Hacker Classes
- Topic 1L: What Do Ethical Hackers Do?
- Topic 1M: Can Hacking be Ethical?
- Topic 1N: How to Become an Ethical Hacker
- Topic 1O: Skills of an Ethical Hacker
- Topic 1P: What is Vulnerability Research?
- Topic 1Q: How to Conduct Ethical Hacking
- Topic 1R: How Do They Go About It?
- Topic 1S: Approaches to Ethical Hacking
- Topic 1T: Ethical Hacking Testing
- Topic 1U: Ethical Hacking Deliverables
- Topic 1V: Computer Crimes and Implications

## Lesson 2: Hacking Laws

- Topic 2A: <http://www.usdoj.gov>
- Topic 2B: <http://www.gob.mx/>
- Topic 2C: <http://www.jf.gov.br/>
- Topic 2D: <http://canada.justice.gc.ca/en/>
- Topic 2E: <http://www.opsi.gov.uk>
- Topic 2F: <http://europa.eu/>
- Topic 2G: European Laws
- Topic 2H: Belgium Laws
- Topic 2I: Denmark Laws
- Topic 2J: France Laws
- Topic 2K: German Laws
- Topic 2L: Greece Laws
- Topic 2M: Italian Laws
- Topic 2N: Netherlands Laws
- Topic 2O: Norway
- Topic 2P: Switzerland
- Topic 2Q: <http://www.australia.gov.au/>
- Topic 2R: The Cybercrime Act 2001
- Topic 2S: The Information Technology Act
- Topic 2T: Japan's Cyber Laws
- Topic 2U: Singapore's Cyber Laws
- Topic 2V: Act on Promotion of Information and Communications Network Utilization and Information Protection
- Topic 2W: The Computer Crimes Act 1997
- Topic 2X: <http://www.legislation.gov.hk/>
- Topic 2Y: Telecommunication Law

## Lesson 3: Footprinting

- Topic 3A: Revisiting Reconnaissance
- Topic 3B: Defining Footprinting
- Topic 3C: Why is Footprinting Necessary?
- Topic 3D: Areas and Information which Attackers Seek
- Topic 3E: Information Gathering Methodology
- Topic 3F: Footprinting Tools
- Topic 3G: E-Mail Spiders
- Topic 3H: How to Create Fake Website
- Topic 3I: Real and Fake Website
- Topic 3J: Tool: Reamweaver
- Topic 3K: Mirrored Fake Website
- Topic 3L: Faking Websites using Man-in-the-Middle Phishing Kit
- Topic 3M: Benefits to Fraudster
- Topic 3N: Steps to Perform Footprinting

## Lesson 4: Google Hacking

- Topic 4A: What is Google Hacking?
- Topic 4B: What a Hacker Can do with Vulnerable Site
- Topic 4C: Anonymity with Caches
- Topic 4D: Using Google as a Proxy Server
- Topic 4E: Directory Listings
- Topic 4F: Going Out on a Limb: Traversal Techniques
- Topic 4G: Extension Walking
- Topic 4H: Site Operator
- Topic 4I: `intitle:index.of`
- Topic 4J: `error | warning`
- Topic 4K: `login | logon`
- Topic 4L: `username | userid | employee.ID | "your username is"`
- Topic 4M: `password | passcode | "your password is"`
- Topic 4N: `admin | administrator`
- Topic 4O: `-ext:html -ext:htm -ext:shtml -ext:asp -ext:php`
- Topic 4P: `inurl:temp | inurl:tmp | inurl:backup | inurl:bak`
- Topic 4Q: `intranet | help.desk`
- Topic 4R: Locating Public Exploit Sites
- Topic 4S: Locating Vulnerable Targets

## Overview



Advanced Infrastructure Solutions  
Networking Infrastructure Solutions  
Learning Solutions

- Topic 4T: Finding IIS 5.0 Servers
- Topic 4U: Web Server Software Error Messages
- Topic 4V: Application Software Error Messages
- Topic 4W: Default Pages
- Topic 4X: Searching for Passwords
- Topic 4Y: Google Hacking Database (GHDB)
- Topic 4Z: SiteDigger Tool
- Topic 4AA: Gooscan
- Topic 4AB: Goolink Scanner
- Topic 4AC: Goolag Scanner
- Topic 4AD: Tool: Google Hacks
- Topic 4AE: Google Hack HoneyPot
- Topic 4AF: Google Protocol
- Topic 4AG: Google Cartography

### Lesson 5: Scanning

- Topic 5A: Scanning: Definition
- Topic 5B: Types of Scanning
- Topic 5C: Objectives of Scanning
- Topic 5D: CEH Scanning Methodology
- Topic 5E: War Dialer Technique
- Topic 5F: Banner Grabbing
- Topic 5G: Vulnerability Scanning
- Topic 5H: Draw Network Diagrams of Vulnerable Hosts
- Topic 5I: Preparing Proxies
- Topic 5J: Scanning Countermeasures
- Topic 5K: Tool: SentryPC

### Lesson 6: Enumeration

- Topic 6A: Overview of System Hacking Cycle
- Topic 6B: What is Enumeration?
- Topic 6C: Techniques for Enumeration
- Topic 6D: NetBIOS Null Sessions
- Topic 6E: PS Tools
- Topic 6F: Network Management Protocol (SNMP) Enumeration
- Topic 6G: LDAP Enumeration
- Topic 6H: NTP Enumeration
- Topic 6I: SMTP Enumeration
- Topic 6J: Web Enumeration
- Topic 6K: Winfingerprint
- Topic 6L: How To Enumerate Web Application Directories in IIS Using DirectoryServices
- Topic 6M: IP Tools Scanner

- Topic 6N: Enumerate Systems Using Default Password
- Topic 6O: Tools
- Topic 6P: Steps to Perform Enumeration

### Lesson 7: System Hacking

- Topic 7A: Part 1- Cracking Password
- Topic 7B: Part 2 - Escalating Privileges
- Topic 7C: Part 3 - Executing Applications
- Topic 7D: Part 4 - Hiding Files
- Topic 7E: Part 5 - Covering Tracks

### Lesson 8: Trojans and Backdoors

- Topic 8A: Introduction
- Topic 8B: What is a Trojan?
- Topic 8C: Indications of a Trojan Attack
- Topic 8D: Ports Used by Trojans
- Topic 8E: Classic Trojans
- Topic 8F: Classic Trojans Found in the Wild
- Topic 8G: Stealth Trojans
- Topic 8H: Reverse Connecting Trojans
- Topic 8I: Miscellaneous Trojans
- Topic 8J: How to Detect Trojans
- Topic 8K: Anti-Trojan Software
- Topic 8L: Evading Anti-Virus Techniques
- Topic 8M: Sample Code for Trojan Client/Server
- Topic 8N: Evading Anti-Trojan/Anti-Virus using Stealth Tools
- Topic 8O: Backdoor Countermeasures
- Topic 8P: Tripwire
- Topic 8Q: System File Verification
- Topic 8R: MD5 Checksum.exe
- Topic 8S: Microsoft Windows Defender
- Topic 8T: How to Avoid a Trojan Infection

### Lesson 9: Viruses and Worms

- Topic 9A: Introduction to Virus
- Topic 9B: Virus History
- Topic 9C: Characteristics of Virus
- Topic 9D: Working of Virus
- Topic 9E: Why People Create Computer Viruses
- Topic 9F: Symptoms of a Virus-like Attack
- Topic 9G: Virus Hoaxes

## Overview



Advanced Infrastructure Solutions  
Networking Infrastructure Solutions  
Learning Solutions

- Topic 9H: Chain Letters
- Topic 9I: Worms
- Topic 9J: How is a Worm Different from a Virus?
- Topic 9K: Indications of a Virus Attack
- Topic 9L: Virus Damage
- Topic 9M: Stages of Virus Life
- Topic 9N: Types of Viruses
- Topic 9O: Famous Viruses and Worms
- Topic 9P: Latest Viruses
- Topic 9Q: Writing Virus Programs
- Topic 9R: Virus Detection Methods
- Topic 9S: Anti-Virus Software
- Topic 9T: Anti-Virus Software
- Topic 9U: Popular Anti-Virus Packages
- Topic 9V: Virus Databases
- Topic 9W: Snopes.com

- Topic 11G: Factors That Make Companies Vulnerable to Attacks
- Topic 11H: Why is Social Engineering Effective
- Topic 11I: Warning Signs of an Attack
- Topic 11J: Tool : Netcraft Anti-Phishing Toolbar
- Topic 11K: Phases in a Social Engineering Attack
- Topic 11L: Behaviors Vulnerable to Attacks
- Topic 11M: Impact on the Organization
- Topic 11N: Countermeasures
- Topic 11O: Policies and Procedures
- Topic 11P: Security Policies - Checklist
- Topic 11Q: Impersonating Orkut, Facebook, MySpace
- Topic 11R: How to Steal Identity
- Topic 11S: Comparison
- Topic 11T: Original
- Topic 11U: Identity Theft
- Topic 11V: <http://www.consumer.gov/idtheft/>

## Lesson 10: Sniffers

- Topic 10A: Definition - Sniffing
- Topic 10B: Types of Sniffing
- Topic 10C: IP-based Sniffing
- Topic 10D: Wiretap
- Topic 10E: Protocols Vulnerable to Sniffing
- Topic 10F: What is Address Resolution Protocol (ARP)?
- Topic 10G: Lawful Intercept
- Topic 10H: Types of Sniffing Attack
- Topic 10I: DNS Poisoning Techniques
- Topic 10J: Interactive TCP Relay
- Topic 10K: Interactive Replay Attacks
- Topic 10L: ARP Spoofing Tools
- Topic 10M: Tools for MAC Flooding
- Topic 10N: Sniffing Tools
- Topic 10O: Linux Sniffing Tools
- Topic 10P: Hardware Protocol Analyzers
- Topic 10Q: Detecting Sniffing

## Lesson 11: Social Engineering

- Topic 11A: What is Social Engineering?
- Topic 11B: Human Weakness
- Topic 11C: "Rebecca" and "Jessica"
- Topic 11D: Office Workers
- Topic 11E: Types of Social Engineering
- Topic 11F: Social Engineering Threats and Defenses

## Lesson 12: Phishing

- Topic 12A: Phishing
- Topic 12B: Introduction
- Topic 12C: Reasons for Successful Phishing
- Topic 12D: Phishing Methods
- Topic 12E: Process of Phishing
- Topic 12F: Types of Phishing Attacks
- Topic 12G: Phishing Statistics: March 2008
- Topic 12H: Anti-Phishing
- Topic 12I: Anti-Phishing Tools

## Lesson 13: Hacking Email Accounts

- Topic 13A: Introduction
- Topic 13B: Vulnerabilities
- Topic 13C: Email Hacking Tools
- Topic 13D: Securing Email Accounts

## Lesson 14: Denial-of-Service

- Topic 14A: Real World Scenario of DoS Attacks
- Topic 14B: What are Denial-of-Service Attacks
- Topic 14C: Goal of DoS
- Topic 14D: Impact and the Modes of Attack

## Overview



Advanced Infrastructure Solutions  
Networking Infrastructure Solutions  
Learning Solutions

- Topic 14E: Types of Attacks
- Topic 14F: DoS Attack Classification
- Topic 14G: Bot (Derived from the Word RoBOT)
- Topic 14H: What is DDoS Attack?
- Topic 14I: DDoS Tools
- Topic 14J: Countermeasures for Reflected DoS
- Topic 14K: DDoS Countermeasures
- Topic 14L: Taxonomy of DDoS Countermeasures
- Topic 14M: Preventing Secondary Victims
- Topic 14N: Detect and Neutralize Handlers
- Topic 14O: Detect Potential Attacks
- Topic 14P: DoSHTTP Tool
- Topic 14Q: Mitigate or Stop the Effects of DDoS Attacks
- Topic 14R: Deflect Attacks
- Topic 14S: Post-attack Forensics
- Topic 14T: Packet Traceback

## Lesson 15: Session Hijacking

- Topic 15A: What is Session Hijacking?
- Topic 15B: Understanding Session Hijacking
- Topic 15C: Spoofing vs. Hijacking
- Topic 15D: Steps in Session Hijacking
- Topic 15E: Types of Session Hijacking
- Topic 15F: Session Hijacking Levels
- Topic 15G: Network Level Hijacking
- Topic 15H: The 3-Way Handshake
- Topic 15I: TCP Concepts 3-Way Handshake
- Topic 15J: Sequence Numbers
- Topic 15K: TCP/IP Hijacking
- Topic 15L: IP Spoofing: Source Routed Packets
- Topic 15M: RST Hijacking
- Topic 15N: Blind Hijacking
- Topic 15O: Man in the Middle Attack Using Packet Sniffer
- Topic 15P: UDP Hijacking
- Topic 15Q: Application Level Hijacking
- Topic 15R: Programs that Performs Session Hacking
- Topic 15S: Dangers Posed by Hijacking
- Topic 15T: Protecting against Session Hijacking
- Topic 15U: Countermeasure: IPSec

## Lesson 16: Hacking Web Servers

- Topic 16A: How are Web Servers Compromised?

- Topic 16B: Web Server Defacement
- Topic 16C: Attacks Against IIS
- Topic 16D: Patch Management
- Topic 16E: Vulnerability Scanners
- Topic 16F: Countermeasures
- Topic 16G: File System Traversal Countermeasures
- Topic 16H: Increasing Web Server Security
- Topic 16I: Web Server Protection Checklist

## Lesson 17: Web Application Vulnerabilities

- Topic 17A: Web Application
- Topic 17B: Web Application Hacking
- Topic 17C: Anatomy of an Attack
- Topic 17D: Web Application Threats
- Topic 17E: Cross-Site Scripting/XSS Flaws
- Topic 17F: SQL Injection
- Topic 17G: Command Injection Flaws
- Topic 17H: Cookie/Session Poisoning
- Topic 17I: Parameter/Form Tampering
- Topic 17J: Hidden Field at JuggyBoy.com
- Topic 17K: Buffer Overflow
- Topic 17L: Directory Traversal/Forceful Browsing
- Topic 17M: Cryptographic Interception
- Topic 17N: Cookie Snooping
- Topic 17O: Authentication Hijacking
- Topic 17P: Log Tampering
- Topic 17Q: Error Message Interception
- Topic 17R: Attack Obfuscation
- Topic 17S: Platform Exploits
- Topic 17T: DMZ Protocol Attacks
- Topic 17U: DMZ
- Topic 17V: Security Management Exploits
- Topic 17W: TCP Fragmentation
- Topic 17X: Hacking Tools

## Lesson 18: Web-Based Password Cracking Techniques

- Topic 18A: Authentication
- Topic 18B: Password Cracking
- Topic 18C: Password Cracking Tools
- Topic 18D: Countermeasures

## Lesson 19: SQL Injection

- Topic 19A: SQL Injection: Introduction
- Topic 19B: SQL Injection Tools
- Topic 19C: Blind SQL Injection
- Topic 19D: SQL Injection Countermeasures
- Topic 19E: SQL Injection Blocking Tool: SQL Block
- Topic 19F: Acunetix Web Vulnerability Scanner

## Lesson 20: Hacking Wireless Networks

- Topic 20A: Introduction to Wireless Networking
- Topic 20B: Wireless Standards
- Topic 20C: Wireless Concepts
- Topic 20D: Wireless Devices
- Topic 20E: WEP
- Topic 20F: WPA
- Topic 20G: TKIP and LEAP
- Topic 20H: Hacking Methods
- Topic 20I: Cracking WEP
- Topic 20J: Rogue Access Point
- Topic 20K: Scanning Tools
- Topic 20L: Sniffing Tools
- Topic 20M: Wireless Security Tools

## Lesson 21: Physical Security

- Topic 21A: Security Facts
- Topic 21B: Understanding Physical Security
- Topic 21C: Physical Security
- Topic 21D: What Is the Need for Physical Security?
- Topic 21E: Who Is Accountable for Physical Security?
- Topic 21F: Factors Affecting Physical Security
- Topic 21G: Physical Security Checklist
- Topic 21H: Information Security
- Topic 21I: EPS (Electronic Physical Security)
- Topic 21J: Wireless Security
- Topic 21K: Laptop Theft Statistics for 2007
- Topic 21L: Statistics for Stolen and Recovered Laptops
- Topic 21M: Laptop Theft
- Topic 21N: Laptop Theft: Data Under Loss
- Topic 21O: Laptop Security Tools
- Topic 21P: Laptop Tracker - XTool Computer Tracker

- Topic 21Q: Tools to Locate Stolen Laptops
- Topic 21R: Stop's Unique, Tamper-proof Patented Plate
- Topic 21S: Tool: TrueCrypt
- Topic 21T: Laptop Security Countermeasures
- Topic 21U: Mantrap
- Topic 21V: TEMPEST
- Topic 21W: Challenges in Ensuring Physical Security
- Topic 21X: Spyware Technologies
- Topic 21Y: Spying Devices
- Topic 21Z: Physical Security: Lock Down USB Ports
- Topic 21AA: Tool: DeviceLock
- Topic 21AB: Blocking the Use of USB Storage Devices
- Topic 21AC: Track Stick GPS Tracking Device

## Lesson 22: Linux Hacking

- Topic 22A: Why Linux?
- Topic 22B: Linux Distributions
- Topic 22C: Linux – Basics
- Topic 22D: Linux Live CD-ROMs
- Topic 22E: Basic Commands of Linux: Files & Directories
- Topic 22F: Directories in Linux
- Topic 22G: Installing, Configuring, and Compiling Linux Kernel
- Topic 22H: How to Install a Kernel Patch
- Topic 22I: Compiling Programs in Linux
- Topic 22J: GCC Commands
- Topic 22K: Make Files
- Topic 22L: Make Install Command
- Topic 22M: Linux Vulnerabilities
- Topic 22N: Chrooting
- Topic 22O: Why is Linux Hacked?
- Topic 22P: How to Apply Patches to Vulnerable Programs
- Topic 22Q: Scanning Networks
- Topic 22R: Nmap in Linux
- Topic 22S: Scanning Tool: Nessus
- Topic 22T: Port Scan Detection Tools

## Overview



Advanced Infrastructure Solutions  
Networking Infrastructure Solutions  
Learning Solutions

- Topic 22U: Password Cracking in Linux: John the Ripper
- Topic 22V: Firewall in Linux: IPTables
- Topic 22W: IPTables Command
- Topic 22X: Basic Linux Operating System Defense
- Topic 22Y: SARA (Security Auditor's Research Assistant)
- Topic 22Z: Linux Tool: Netcat
- Topic 22AA: Linux Tool: tcpdump
- Topic 22AB: Linux Tool: Snort
- Topic 22AC: Linux Tool: SAINT
- Topic 22AD: Linux Tool: Wireshark
- Topic 22AE: Linux Tool: Abacus Port Sentry
- Topic 22AF: Linux Tool: DSNIFF Collection
- Topic 22AG: Linux Tool: Hping2
- Topic 22AH: Linux Tool: Sniffit
- Topic 22AI: Linux Tool: Nemesis
- Topic 22AJ: Linux Tool: LSOF
- Topic 22AK: Linux Tool: IPtraf
- Topic 22AL: Linux Tool: LIDS
- Topic 22AM: Hacking Tool: Hunt
- Topic 22AN: Tool: TCP Wrappers
- Topic 22AO: Linux Loadable Kernel Modules
- Topic 22AP: Hacking Tool: Linux Rootkits
- Topic 22AQ: Rootkits: Knark & Torn
- Topic 22AR: Rootkits: Tuxit, Adore, Ramen
- Topic 22AS: Rootkit: Beastkit
- Topic 22AT: Rootkit Countermeasures
- Topic 22AU: 'chkrootkit' detects the following Rootkits
- Topic 22AV: Linux Tools: Application Security
- Topic 22AW: Advanced Intrusion Detection Environment (AIDE)
- Topic 22AX: Linux Tools: Security Testing Tools
- Topic 22AY: Linux Tools: Encryption
- Topic 22AZ: Linux Tools: Log and Traffic Monitors
- Topic 22BA: Linux Security Auditing Tool (LSAT)
- Topic 22BB: Linux Security Countermeasures
- Topic 22BC: Steps for Hardening Linux

### Lesson 23: Evading IDS, Firewalls and Detecting Honey Pots

- Topic 23A: Introduction to Intrusion Detection System

- Topic 23B: Terminologies
- Topic 23C: Intrusion Detection System (IDS)
- Topic 23D: Intrusion Prevention System
- Topic 23E: What is a Firewall?
- Topic 23F: Common Tool for Testing Firewall and IDS
- Topic 23G: What is HoneyPot?
- Topic 23H: Tools to Detect HoneyPots
- Topic 23I: What to Do When Hacked

### Lesson 24: Buffer Overflows

- Topic 24A: Buffer Overflow Concepts
- Topic 24B: Attacking a Real Program
- Topic 24C: NOPS
- Topic 24D: How to Mutate a Buffer Overflow Exploit
- Topic 24E: Once the Stack is Smashed
- Topic 24F: Examples of Buffer Overflow
- Topic 24G: Tools
- Topic 24H: How to Detect Buffer Overflows in a Program
- Topic 24I: Defense Against Buffer Overflows

### Lesson 25: Cryptography

- Topic 25A: Public-key Cryptography
- Topic 25B: Working of Encryption
- Topic 25C: RSA (Rivest Shamir Adleman)
- Topic 25D: RC4, RC5, RC6, Blowfish
- Topic 25E: Algorithms and Security
- Topic 25F: Brute-Force Attack
- Topic 25G: RSA Attacks
- Topic 25H: Message Digest Functions
- Topic 25I: SHA (Secure Hash Algorithm)
- Topic 25J: SSL (Secure Sockets Layer)
- Topic 25K: What is SSH?
- Topic 25L: Government Access to Keys (GAK)
- Topic 25M: RSA Challenge
- Topic 25N: distributed.net
- Topic 25O: Code Breaking: Methodologies
- Topic 25P: Cryptography Attacks
- Topic 25Q: Disk Encryption
- Topic 25R: Magic Lantern

## Overview

- Topic 25S: WEPCrack
- Topic 25T: Cracking S/MIME Encryption Using Idle CPU Time
- Topic 25U: Cryptography Tools



Advanced Infrastructure Solutions  
Networking Infrastructure Solutions  
Learning Solutions

## Lesson 26: Penetration Testing

- Topic 26A: Introduction to Penetration Testing (PT)
- Topic 26B: Categories of Security Assessments
- Topic 26C: Vulnerability Assessment
- Topic 26D: Limitations of Vulnerability Assessment
- Topic 26E: Testing
- Topic 26F: Penetration Testing Tools
- Topic 26G: Threat
- Topic 26H: Other Tools Useful in Pen-Test
- Topic 26I: Phases of Penetration Testing
- Topic 26J: Pre-attack Phase
- Topic 26K: Best Practices
- Topic 26L: Results That Can be Expected
- Topic 26M: Passive Reconnaissance
- Topic 26N: Active Reconnaissance
- Topic 26O: Attack Phase
- Topic 26P: Post Attack Phase and Activities
- Topic 26Q: Penetration Testing Deliverables Templates

## Lesson 27: Macintosh Hacking

- Topic 27A: Introduction to MAC OS
- Topic 27B: Vulnerabilities in MAC
- Topic 27C: How a Malformed Installer Package Can Crack Mac OS X
- Topic 27D: Worm and Viruses in MAC
- Topic 27E: Anti-Viruses in MAC
- Topic 27F: Mac Security Tools
- Topic 27G: Countermeasures

## Lesson 28: Hacking Routers, cable Modems and Firewalls

- Topic 28A: Network Devices
- Topic 28B: Hacking Routers
- Topic 28C: Exploiting Vulnerabilities in Cisco IOS
- Topic 28D: Brute-Forcing Services
- Topic 28E: Attacking Router

- Topic 28F: Common Router, Switch, or Firewall Reconfigurations by Attackers
- Topic 28G: Pen-Testing Tools
- Topic 28H: Capturing Network Traffic
- Topic 28I: Cable Modem Hacking
- Topic 28J: [www.bypassfirewalls.net](http://www.bypassfirewalls.net)
- Topic 28K: Waldo Beta 0.7 (b)

## Lesson 29: Hacking Mobile Phones, PDA and Handheld Devices

- Topic 29A: Different OS in Mobile Phone
- Topic 29B: Different OS Structure in Mobile Phone
- Topic 29C: Evolution of Mobile Threat
- Topic 29D: Threats
- Topic 29E: What Can a Hacker Do?
- Topic 29F: Vulnerabilities in Different Mobile Phones
- Topic 29G: Malware
- Topic 29H: Spyware
- Topic 29I: Blackberry
- Topic 29J: PDA
- Topic 29K: iPod
- Topic 29L: Mobile: Is It a Breach to Enterprise Security?
- Topic 29M: Trojan and Viruses
- Topic 29N: Antivirus
- Topic 29O: Security Tools
- Topic 29P: Defending Cell Phones and PDAs Against Attack
- Topic 29Q: Mobile Phone Security Tips

## Lesson 30: Bluetooth Hacking

- Topic 30A: Bluetooth Introduction
- Topic 30B: Security Issues in Bluetooth
- Topic 30C: Attacks Against Bluetooth
- Topic 30D: Bluetooth Hacking Tools
- Topic 30E: Bluetooth Viruses and Worms
- Topic 30F: Bluetooth Security Tools
- Topic 30G: Countermeasures



## Lesson 31: VoIP Hacking

- Topic 31A: What is VoIP?
- Topic 31B: VoIP Hacking Steps
- Topic 31C: Footprinting
- Topic 31D: Scanning
- Topic 31E: Enumeration
- Topic 31F: Steps to Exploit the Network
- Topic 31G: Covering Tracks

- Topic 34B: Electrical Attack
- Topic 34C: Software Attack
- Topic 34D: USB Attack on Windows
- Topic 34E: Viruses and Worms
- Topic 34F: Hacking Tools
- Topic 34G: USB Security Tools
- Topic 34H: Countermeasures

## Lesson 32: RFID Hacking

- Topic 32A: RFID - Definition
- Topic 32B: Components of RFID Systems
- Topic 32C: RFID Collisions
- Topic 32D: RFID Risks
- Topic 32E: RFID and Privacy Issues
- Topic 32F: Countermeasures
- Topic 32G: RFID Security and Privacy Threats
- Topic 32H: Protection Against RFID Attacks
- Topic 32I: RFID Guardian
- Topic 32J: RFID Malware
- Topic 32K: RFID Exploits
- Topic 32L: Vulnerabilities in RFID-enabled Credit Cards
- Topic 32M: RFID Hacking Tool: RFDump
- Topic 32N: RFID Security Controls
- Topic 32O: RFID Security

## Lesson 35: Hacking Database Servers

- Topic 35A: Hacking Database Server: Introduction
- Topic 35B: Hacking Oracle Database Server
- Topic 35C: How SQL Server is Hacked
- Topic 35D: Security Tools
- Topic 35E: SQL Server Security Best Practices: Administrator Checklist
- Topic 35F: SQL Server Security Best Practices: Developer Checklist

## Lesson 33: Spamming

- Topic 33A: Introduction
- Topic 33B: Techniques Used by Spammers
- Topic 33C: How Spamming is Performed
- Topic 33D: Ways of Spamming
- Topic 33E: Spammer: Statistics
- Topic 33F: Worsen ISP: Statistics
- Topic 33G: Top Spam Affected Countries: Statistics
- Topic 33H: Types of Spam Attacks
- Topic 33I: Bulk Emailing Tools
- Topic 33J: Anti-Spam Techniques
- Topic 33K: Anti-Spamming Tools

## Lesson 36: Cyber Warfare - Hacking, Al-Qaida and Terrorism

- Topic 36A: Cyber Terrorism Over Internet
- Topic 36B: Cyber-Warfare Attacks
- Topic 36C: Muslim Doctors Planned US Terror Raids
- Topic 36D: Net Attack
- Topic 36E: Al-Qaeda
- Topic 36F: Why Terrorists Use Cyber Techniques
- Topic 36G: Cyber Support to Terrorist Operations
- Topic 36H: Planning
- Topic 36I: Recruitment
- Topic 36J: Research
- Topic 36K: Propaganda
- Topic 36L: Cyber Threat to the Military
- Topic 36M: Russia 'hired botnets' for Estonia Cyber-War
- Topic 36N: NATO Threatens War with Russia
- Topic 36O: Bush on Cyber War: 'a subject I can learn a lot about'
- Topic 36P: E.U. Urged to Launch Coordinated Effort Against Cybercrime
- Topic 36Q: Budget: Eye on Cyber-Terrorism Attacks

## Lesson 34: Hacking USB Devices

- Topic 34A: Introduction to USB Devices

## Overview



Advanced Infrastructure Solutions  
Networking Infrastructure Solutions  
Learning Solutions

- Topic 36R: Cyber Terror Threat is Growing, Says Reid
- Topic 36S: Terror Web 2.0
- Topic 36T: Table 1: How Websites Support Objectives of terrorist/Extremist Groups
- Topic 36U: Electronic Jihad
- Topic 36V: Electronic Jihad App Offers Cyber Terrorism for the Masses
- Topic 36W: <http://internet-haganah.com/haganah/>
- Topic 36X: Mujahedeen Secrets Encryption Program 2

### Lesson 37: Internet Content Filtering Techniques

- Topic 37A: Introduction to Internet Filter
- Topic 37B: Internet Content Filtering Tools

### Lesson 38: Privacy on the Internet

- Topic 38A: Internet Privacy
- Topic 38B: Proxy Privacy
- Topic 38C: Email Privacy
- Topic 38D: Cookies
- Topic 38E: Examining Information in Cookies
- Topic 38F: How Internet Cookies Work
- Topic 38G: How Google Stores Personal Information
- Topic 38H: Google Privacy Policy
- Topic 38I: Web Browsers
- Topic 38J: Web Bugs
- Topic 38K: Downloading Freeware
- Topic 38L: Internet Relay Chat
- Topic 38M: Pros and Cons of Internet Relay Chat
- Topic 38N: Electronic Commerce
- Topic 38O: Internet Privacy Tools: Anonymizers
- Topic 38P: Internet Privacy Tools: Firewall Tools
- Topic 38Q: Internet Privacy Tools: Others
- Topic 38R: Best Practices
- Topic 38S: Counter Measures

### Lesson 39: Securing Laptop Computers

- Topic 39A: Statistics for Stolen and Recovered Laptops
- Topic 39B: Statistics on Security
- Topic 39C: Percentage of Organizations Following the Security Measures

- Topic 39D: Laptop Threats
- Topic 39E: Laptop Theft
- Topic 39F: Fingerprint Reader
- Topic 39G: Protecting Laptops Through Face Recognition
- Topic 39H: Bluetooth in Laptops
- Topic 39I: Tools
- Topic 39J: Securing from Physical Laptop Thefts
- Topic 39K: Hardware Security for Laptops
- Topic 39L: Protecting the Sensitive Data
- Topic 39M: Preventing Laptop Communications from Wireless Threats
- Topic 39N: Protecting the Stolen Laptops from Being Used
- Topic 39O: Security Tips

### Lesson 40: Spying Technologies

- Topic 40A: Spying
- Topic 40B: Motives of Spying
- Topic 40C: Spying Devices
- Topic 40D: Vendors Hosting Spy Devices
- Topic 40E: Spying Tools
- Topic 40F: Anti-Spying Tools

### Lesson 41: Corporate Espionage- Hacking Using Insiders

- Topic 41A: Introduction To Corporate Espionage
- Topic 41B: Information Corporate Spies Seek
- Topic 41C: Insider Threat
- Topic 41D: Different Categories of Insider Threat
- Topic 41E: Privileged Access
- Topic 41F: Driving Force Behind Insider Attack
- Topic 41G: Common Attacks Carried Out by Insiders
- Topic 41H: Techniques Used for Corporate Espionage
- Topic 41I: Process of Hacking
- Topic 41J: Former Forbes Employee Pleads Guilty
- Topic 41K: Former Employees Abet Stealing Trade Secrets

## Overview

- Topic 41L: California Man Sentenced For Hacking
- Topic 41M: Federal Employee Sentenced for Hacking
- Topic 41N: Facts
- Topic 41O: Key Findings from U.S. Secret Service and CERT Coordination Center/SEI study on Insider Threat
- Topic 41P: Tools
- Topic 41Q: Countermeasures

### Lesson 42: Creating Security Policies

- Topic 42A: Security Policies
- Topic 42B: Key Elements of Security Policy
- Topic 42C: Defining the Purpose and Goals of Security Policy
- Topic 42D: Role of Security Policy
- Topic 42E: Classification of Security Policy
- Topic 42F: Design of Security Policy
- Topic 42G: Contents of Security Policy
- Topic 42H: Configurations of Security Policy
- Topic 42I: Implementing Security Policies
- Topic 42J: Types of Security Policies
- Topic 42K: Policy Statements
- Topic 42L: E-mail Security Policy
- Topic 42M: Software Security Policy
- Topic 42N: Software License Policy
- Topic 42O: Points to Remember While Writing a Security Policy
- Topic 42P: Sample Policies

### Lesson 43: Software Piracy and Warez

- Topic 43A: Software Activation: Introduction
- Topic 43B: Piracy
- Topic 43C: Software Copy Protection Backgrounders
- Topic 43D: Warez
- Topic 43E: Tool: Crypkey
- Topic 43F: Tool: EnTrial
- Topic 43G: EnTrial Tool: Distribution File
- Topic 43H: Tool: DF\_ProtectionKit
- Topic 43I: Tool: Crack Killer
- Topic 43J: Tool: Logic Protect
- Topic 43K: Tool: Software License Manager
- Topic 43L: Tool: Quick License Manager



Advanced Infrastructure Solutions  
Networking Infrastructure Solutions  
Learning Solutions

- Topic 43M: Tool: WTM CD Protect

### Lesson 44: Hacking and Cheating Online Games

- Topic 44A: Online Games
- Topic 44B: Basics of Game Hacking
- Topic 44C: Online Gaming Risks
- Topic 44D: Techniques used for Exploiting Online Games
- Topic 44E: Threats in Online Gaming
- Topic 44F: Stealing Online Games Passwords: Malwares
- Topic 44G: Social Engineering and Phishing
- Topic 44H: Example of Popular Game Exploits
- Topic 44I: Online Gaming Malware from 1997-2007
- Topic 44J: Best Practices for Secure Online Gaming
- Topic 44K: Tips for Secure Online Gaming

### Lesson 45: Hacking RSS and Atom

- Topic 45A: Introduction
- Topic 45B: Areas Where RSS and Atom is Used
- Topic 45C: Building a Feed Aggregator
- Topic 45D: Monitoring the Server with Feeds
- Topic 45E: Tracking Changes in Open Source Projects
- Topic 45F: Risks by Zone
- Topic 45G: Reader Specific Risks
- Topic 45H: Utilizing the Web Feeds Vulnerabilities
- Topic 45I: Example for Attacker to Attack the Feeds
- Topic 45J: Tools

### Lesson 46: Hacking Web Browsers

- Topic 46A: Introduction
- Topic 46B: How Web Browsers Work
- Topic 46C: How Web Browsers Access HTML Documents
- Topic 46D: Protocols for an URL
- Topic 46E: Hacking Firefox
- Topic 46F: Firefox Security

## Overview



Advanced Infrastructure Solutions  
Networking Infrastructure Solutions  
Learning Solutions

- Topic 46G: Hacking Internet Explorer
- Topic 46H: Internet Explorer Security
- Topic 46I: Hacking Opera
- Topic 46J: Security Features of Opera
- Topic 46K: Hacking Safari
- Topic 46L: Securing Safari
- Topic 46M: Hacking Netscape
- Topic 46N: Securing Netscape

- Topic 49H: Sources of GPS Signal Errors
- Topic 49I: Methods to Mitigate Signal Loss
- Topic 49J: GPS Secrets
- Topic 49K: Firmware Hacking
- Topic 49L: GPS Tools

### Lesson 47: Proxy Server Technologies

- Topic 47A: Introduction: Proxy Server
- Topic 47B: Working of Proxy Server
- Topic 47C: Types of Proxy Server
- Topic 47D: Socks Proxy
- Topic 47E: Free Proxy Servers
- Topic 47F: Use of Proxies for Attack
- Topic 47G: Tools
- Topic 47H: How Does MultiProxy Work
- Topic 47I: TOR Proxy Chaining Software
- Topic 47J: AnalogX Proxy
- Topic 47K: NetProxy
- Topic 47L: Proxy+
- Topic 47M: ProxySwitcher Lite
- Topic 47N: Tool: JAP
- Topic 47O: Proxomitron
- Topic 47P: SSL Proxy Tool
- Topic 47Q: How to Run SSL Proxy

### Lesson 50: Computer Forensics and Incident Handling

- Topic 50A: Computer Forensics
- Topic 50B: Incident Handling
- Topic 50C: Incident Management
- Topic 50D: Why Don't Organizations Report Computer Crimes?
- Topic 50E: Estimating Cost of an Incident
- Topic 50F: Whom to Report an Incident
- Topic 50G: Incident Reporting
- Topic 50H: Vulnerability Resources
- Topic 50I: What is CSIRT?
- Topic 50J: World CERTs  
<http://www.trustedintroducer.nl/teams/country.html>
- Topic 50K:  
<http://www.first.org/about/organization/teams/>
- Topic 50L: IRTs Around the World

### Lesson 48: Data Loss Prevention

- Topic 48A: Introduction: Data Loss
- Topic 48B: Causes of Data Loss
- Topic 48C: How to Prevent Data Loss
- Topic 48D: Impact Assessment for Data Loss Prevention
- Topic 48E: Tools

### Lesson 49: Hacking Global Positioning System (GPS)

- Topic 49A: Global Positioning System (GPS)
- Topic 49B: Terminologies
- Topic 49C: GPS Devices Manufacturers
- Topic 49D: Gpsd-GPS Service Daemon
- Topic 49E: Sharing Waypoints
- Topic 49F: Wardriving
- Topic 49G: Areas of Concern