



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

## Course Content

### Course Description:

The Certified Ethical Hacker (CEH) program is the core of the most desired information security training system any information security professional will ever want to be in. The CEH, is the first part of a 3 part EC-Council Information Security Track which helps you master hacking technologies. You will become a hacker, but an ethical one!

As the security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment.

This course was designed to provide you with the tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, "To beat a hacker, you need to think like a hacker". This course will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. It puts you in the driver's seat of a hands-on environment with a systematic ethical hacking process.

Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be thought the Five Phases of Ethical Hacking and thought how you can approach your target and succeed at breaking in every time! The ve phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

The tools and techniques in each of these five phases are provided in detail in an encyclopedic approach to help you identify when an attack has been used against your own targets. Why then is this training called the Certified Ethical Hacker Course? This is because by using the same techniques as the bad guys, you can assess the security posture of an organization with the same approach these malicious hackers use, identify weaknesses and x the problems before they are identified by the enemy, causing what could potentially be a catastrophic damage to your respective organization.

Throughout the CEH course, you will be immersed in a hacker's mindset, evaluating not just logical, but physical security.



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

## Target Student:

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

## Prerequisites:

N/A

## Topics:

### Module 1: Introduction to Ethical Hacking

- Internet is Integral Part of Business and Personal Life - What Happens Online in 60 Seconds
  - Information Security Overview
    - Case Study
      - eBay Data Breach
      - Google Play Hack
      - The Home Depot Data Breach
    - Year of the Mega Breach
    - Data Breach Statistics
    - Malware Trends in 2014
    - Essential Terminology
    - Elements of Information Security
    - The Security, Functionality, and Usability Triangle
  - Information Security Threats and Attack Vectors
    - Motives, Goals, and Objectives of Information Security Attacks
    - Top Information Security Attack Vectors
    - Information Security Threat Categories
    - Types of Attacks on a System
      - Operating System Attacks
        - Examples of OS Vulnerabilities
      - Misconfiguration Attacks
    - Application-Level Attacks
      - Examples of Application-Level Attacks
    - Shrink Wrap Code Attacks
  - Information Warfare
- Hacking Concepts, Types, and Phases
  - What is Hacking
  - Who is a Hacker?
  - Hacker Classes
  - Hacking Phases
    - Reconnaissance
    - Scanning
    - Gaining Access
    - Maintaining Access
    - Clearing Tracks
- Ethical Hacking Concepts and Scope
  - What is Ethical Hacking?
  - Why Ethical Hacking is Necessary
  - Scope and Limitations of Ethical Hacking
  - Skills of an Ethical Hacker
- Information Security Controls
  - Information Assurance (IA)
  - Information Security Management Program
  - Threat Modeling
  - Enterprise Information Security Architecture (EISA)
  - Network Security Zoning



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Defense in Depth
  - Information Security Policies
    - Types of Security Policies
    - Examples of Security Policies
    - Privacy Policies at Workplace
    - Steps to Create and Implement Security Policies
    - HR/Legal Implications of Security Policy Enforcement
  - Physical Security
    - Physical Security Controls
  - Incident Management
    - Incident Management Process
    - Responsibilities of an Incident Response Team
  - What is Vulnerability Assessment?
    - Types of Vulnerability Assessment
    - Network Vulnerability Assessment Methodology
    - Vulnerability Research
    - Vulnerability Research Websites
  - Penetration Testing
    - Why Penetration Testing
    - Comparing Security Audit, Vulnerability Assessment, and Penetration Testing
    - Blue Teaming/Red Teaming
    - Types of Penetration Testing
    - Phases of Penetration Testing
    - Security Testing Methodology
    - Penetration Testing Methodology
  - Information Security Laws and Standards
    - Payment Card Industry Data Security Standard (PCI-DSS)
    - ISO/IEC 27001:2013
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Sarbanes Oxley Act (SOX)
    - The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)
    - Cyber Law in Different Countries
- 
- **Module 02: Footprinting and Reconnaissance**
    - Footprinting Concepts
      - What is Footprinting?
      - Objectives of Footprinting
    - Footprinting Methodology
      - Footprinting through Search Engines
        - Finding Company's Public and Restricted Websites
        - Determining the Operating System
        - Collect Location Information
        - People Search: Social Networking Services
        - People Search Online Services
        - Gather Information from Financial Services
        - Footprinting through Job Sites
        - Monitoring Target Using Alerts
        - Information Gathering Using Groups, Forums, and Blogs
      - Footprinting using Advanced Google Hacking Techniques
        - Google Advance Search Operators
        - Finding Resources Using Google Advance Operator



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Google Hacking Database (GHDB)
- Information Gathering Using Google Advanced Search
- Footprinting through Social Networking Sites
  - Collect Information through Social Engineering on Social Networking Sites
  - Information Available on Social Networking Sites
- Website Footprinting
  - Website Footprinting using Web Spiders
  - Mirroring Entire Website
    - Website Mirroring Tools
  - Extract Website Information from <http://www.archive.org>
  - Monitoring Web Updates Using Website Watcher
    - Web Updates Monitoring Tools
- Email Footprinting
  - Tracking Email Communications
    - Collecting Information from Email Header
    - Email Tracking Tools
- Competitive Intelligence
  - 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 Opinions Say About the Company
- Monitoring Website Traffic of Target Company
- Tracking Online Reputation of the Target
  - Tools for Tracking Online Reputation of the Target
- WHOIS Footprinting
  - WHOIS Lookup
  - WHOIS Lookup Result Analysis
  - WHOIS Lookup Tools
  - WHOIS Lookup Tools for Mobile
- DNS Footprinting
  - Extracting DNS Information
  - DNS Interrogation Tools
- Network Footprinting
  - Locate the Network Range
  - Traceroute
  - Traceroute Analysis
  - Traceroute Tools
- Footprinting through Social Engineering
  - Footprinting through Social Engineering
  - Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving
- Footprinting Tools
  - Footprinting Tool
    - Maltego
    - Recon-ng
  - Additional Footprinting Tools



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Footprinting Countermeasures
- Footprinting Penetration Testing
  - Footprinting Pen Testing
  - Footprinting Pen Testing Report Templates

## Module 03: Scanning Networks

- Overview of Network Scanning
  - TCP Communication Flags
  - TCP/IP Communication
  - Creating Custom Packet Using TCP Flags
- CEH Scanning Methodology
  - Check for Live Systems
    - Checking for Live Systems - ICMP Scanning
    - Ping Sweep
      - Ping Sweep Tools
  - Check for Open Ports
    - SSDP Scanning
    - Scanning IPv6 Network
    - Scanning Tool
      - Nmap
      - Hping2 / Hping3
      - Hping Commands
    - Scanning Techniques
      - TCP Connect / Full Open Scan
      - Stealth Scan (Half-open Scan)
      - Inverse TCP Flag Scanning
      - Xmas Scan
      - ACK Flag Probe Scanning

- IDLE/IPID Header Scan
  - ✓ IDLE Scan: Step 1

- ✓ IDLE Scan: Step 2 and 3

- UDP Scanning
- ICMP Echo Scanning/List Scan

- Scanning Tool: NetScan Tools Pro
- Scanning Tools
- Scanning Tools for Mobile
- Port Scanning Countermeasures

- Scanning Beyond IDS
  - IDS Evasion Techniques
  - SYN/FIN Scanning Using IP Fragments

- Banner Grabbing
  - Banner Grabbing Tools
  - Banner Grabbing Countermeasures
    - Disabling or Changing Banner
    - Hiding File Extensions from Web Pages

- Scan for Vulnerability
  - Vulnerability Scanning
  - Vulnerability Scanning Tool
    - Nessus
    - GAFI LanGuard
    - Qualys FreeScan
  - Network Vulnerability Scanners
  - Vulnerability Scanning Tools for Mobile



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Draw Network Diagrams
  - Drawing Network Diagrams
  - Network Discovery Tool
    - Network Topology Mapper
    - OpManager and NetworkView
  - Network Discovery and Mapping Tools
  - Network Discovery Tools for Mobile
- Prepare Proxies
  - Proxy Servers
  - Proxy Chaining
  - Proxy Tool
    - Proxy Switcher
    - Proxy Workbench
    - TOR and CyberGhost
  - Proxy Tools
  - Proxy Tools for Mobile
  - Free Proxy Servers
  - Introduction to Anonymizers
    - Censorship Circumvention Tool: Tails
    - G-Zapper
    - Anonymizers
    - Anonymizers for Mobile
  - Spoofing IP Address
  - IP Spoofing Detection Techniques
    - Direct TTL Probes
    - IP Identification Number
  - TCP Flow Control Method
  - IP Spoofing Countermeasures
- Scanning Pen Testing

## Module 04: Enumeration

- Enumeration Concepts
  - What is Enumeration?
  - Techniques for Enumeration
  - Services and Ports to Enumerate
- NetBIOS Enumeration
  - NetBIOS Enumeration Tool
    - SuperScan
    - Hyena
    - Winfingerprint
    - NetBIOS Enumerator and Nsauditor Network Security Auditor
  - Enumerating User Accounts
  - Enumerating Shared Resources Using Net View
- SNMP Enumeration
  - Working of SNMP
  - Management Information Base (MIB)
  - SNMP Enumeration Tool
    - OpUtils
    - Engineer's Toolset
  - SNMP Enumeration Tools
- LDAP Enumeration
  - LDAP Enumeration Tool: Softerra LDAP Administrator
  - LDAP Enumeration Tools
- NTP Enumeration
  - NTP Enumeration Commands
  - NTP Enumeration Tools
- SMTP Enumeration
  - SMTP Enumeration Tool: NetScanTools Pro
  - Telnet Enumeration
  - DNS Zone Transfer Enumeration Using NSLookup
- Enumeration Countermeasures
- SMB Enumeration Countermeasures
- Enumeration Pen Testing



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

## Module 05: System Hacking

- Information at Hand Before System Hacking Stage
- System Hacking: Goals
- CEH Hacking Methodology (CHM)
- CEH System Hacking Steps
  - Cracking Passwords
    - Password Cracking
    - Types of Password Attacks
    - Non-Electronic Attacks
    - Active Online Attack
      - Dictionary, Brute Forcing and Rule-based Attack
      - Password Guessing
    - Default Passwords
    - Active Online Attack:
      - Trojan/Spyware/Keylogger
      - Example of Active Online Attack Using USB Drive
      - Hash Injection Attack
      - Passive Online Attack
      - Wire Sniffing
      - Man-in-the-Middle and Replay Attack
    - Offline Attack
      - Rainbow Attacks
        - ✓ Tools to Create Rainbow Tables: rtgen and Winrtgen
      - Distributed Network Attack
    - Elcomsoft Distributed Password Recovery
    - Microsoft Authentication
    - How Hash Passwords Are Stored in Windows SAM?
      - NTLM Authentication Process
      - Kerberos Authentication
    - Password Salting
    - pwdump7 and fgdump
    - Password Cracking Tools
      - L0phtCrack and Ophcrack
      - Cain & Abel and RainbowCrack
    - Password Cracking Tools
    - Password Cracking Tool for Mobile: FlexiSPY Password Grabber
    - How to Defend against Password Cracking
    - Implement and Enforce Strong Security Policy
    - CEH System Hacking Steps
  - Escalating Privileges
    - Privilege Escalation
    - Privilege Escalation Using DLL Hijacking
    - Privilege Escalation Tool: Active@ Password Changer
    - Privilege Escalation Tools
    - How to Defend Against Privilege Escalation
  - Executing Applications
    - RemoteExec
    - PDQ Deploy
    - DameWare Remote Support



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Keylogger
  - Types of Keystroke Loggers
  - Hardware Keyloggers
  - Keylogger: All In One Keylogger
  - Keyloggers for Windows
  - Keylogger for Mac: Amac Keylogger for Mac
  - Keyloggers for MAC
- Spyware
  - Spyware: Spytech SpyAgent
  - Spyware: Power Spy 2014
  - What Does the Spyware Do?
  - Spyware
  - USB Spyware: USBSpy
  - Audio Spyware: Spy Voice Recorder and Sound Snooper
  - Video Spyware: WebCam Recorder
  - Cellphone Spyware: Mobile Spy
  - Telephone/Cellphone Spyware
  - GPS Spyware: SPYPhone
  - GPS Spyware
- How to Defend Against Keyloggers
  - Anti-Keylogger: Zemana AntiLogger
  - Anti-Keylogger
- How to Defend Against Spyware
  - Anti-Spyware: SUPERAntiSpyware
  - Anti-Spyware
- Hiding Files
  - Rootkits
    - Types of Rootkits
    - How Rootkit Works
    - Rootkit
      - ✓ Avatar
      - ✓ Necurs
      - ✓ Azazel
      - ✓ ZeroAccess
  - Detecting Rootkits
    - Steps for Detecting Rootkits
    - How to Defend against Rootkits
    - Anti-Rootkit: Stinger and UnHackMe
    - Anti-Rootkits
  - NTFS Data Stream
    - How to Create NTFS Streams
    - NTFS Stream Manipulation
    - How to Defend against NTFS Streams
    - NTFS Stream Detector: StreamArmor
    - NTFS Stream Detectors
- What Is Steganography?
  - Classification of Steganography
  - Types of Steganography based on Cover Medium





# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- ✓ Whitespace
- Steganography Tool: SNOW
  - ✓ Image
- Steganography
  - ✓ Least Significant
- Bit Insertion
  - ✓ Masking and Filtering
  - ✓ Algorithms and Transformation
  - ✓ Image
- Steganography: QuickStego
  - ✓ Image
- Steganography Tools
  - ✓ Document
- Steganography: wbStego
  - ✓ Document
- Steganography Tools
  - ✓ Video
- Steganography
  - ✓ Video
- Steganography: OmniHide PRO and Masker
  - ✓ Video
- Steganography Tools
  - ✓ Audio
- Steganography
  - ✓ Audio
- Steganography: DeepSound
  - ✓ Audio
- Steganography Tools
  - ✓ Folder
- Steganography: Invisible Secrets 4
  - ✓ Folder
- Steganography Tools
  - ✓ Spam/Email
- Steganography: Spam Mimic
  - Steganography Tools for Mobile Phones
- Steganalysis
  - Steganalysis Methods/Attacks on Steganography
  - Detecting Text and Image Steganography
  - Detecting Audio and Video Steganography
  - Steganography Detection Tool: Gargoyle Investigator™ Forensic Pro
  - Steganography Detection Tools
- Covering Tracks
  - Covering Tracks
  - Disabling Auditing: Auditpol
  - Clearing Logs
  - Manually Clearing Event Logs
  - Ways to Clear Online Tracks
  - Covering Tracks Tool: CCleaner
  - Covering Tracks Tool: MRU-Blaster
  - Track Covering Tools
- Penetration Testing
  - Password Cracking
  - Privilege Escalation
  - Executing Applications
  - Hiding Files
  - Covering Tracks



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

## Module 06: Malware Threats

- Introduction to Malware
  - Different Ways a Malware can Get into a System
  - Common Techniques Attackers Use to Distribute Malware on the Web
- Trojan Concepts
  - Financial Loss Due to Trojans
  - What is a Trojan?
  - How Hackers Use Trojans
  - Common Ports used by Trojans
  - How to Infect Systems Using a Trojan
  - Wrappers
  - Dark Horse Trojan Virus Maker
  - Trojan Horse Construction Kit
  - Crypters: AIO FUD Crypter, Hidden Sight Crypter, and Galaxy Crypter
  - Crypters: Criogenic Crypter, Heaven Crypter, and SwayzCryptor
  - How Attackers Deploy a Trojan
  - Exploit Kit
    - Exploit Kit: Infinity
    - Exploit Kits: Phoenix Exploit Kit and Blackhole Exploit Kit
    - Exploit Kits: Bleedinglife and Crimepack
  - Evading Anti-Virus Techniques
- Types of Trojans
  - Command Shell Trojans
  - Defacement Trojans
  - Defacement Trojans: Restorator
  - Botnet Trojans
    - Tor-based Botnet Trojans: ChewBacca
    - Botnet Trojans: Skynet and CyberGate
  - Proxy Server Trojans
    - Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)
  - FTP Trojans
  - VNC Trojans
    - VNC Trojans: WinVNC and VNC Stealer
  - HTTP/HTTPS Trojans
    - HTTP Trojan: HTTP RAT
  - Shttpd Trojan - HTTPS (SSL)
  - ICMP Tunneling
  - Remote Access Trojans
    - Optix Pro and MoSucker
    - BlackHole RAT and SSH - R.A.T
    - njRAT and Xtreme RAT
    - SpyGate – RAT and Punisher RAT
    - DarkComet RAT, Pandora RAT, and HellSpy RAT
    - ProRat and Theef
    - Hell Raiser
    - Atelier Web Remote Commander
  - Covert Channel Trojan: CCTT
  - E-banking Trojans
    - Working of E-banking Trojans
    - E-banking Trojan
      - ZeuS and SpyEye
      - Citadel Builder and Ice IX
  - Destructive Trojans: M4sT3r Trojan
  - Notification Trojans
  - Data Hiding Trojans (Encrypted Trojans)



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Virus and Worms Concepts
  - Introduction to Viruses
  - Stages of Virus Life
  - Working of Viruses:
    - Infection Phase
    - Attack Phase
  - Why Do People Create Computer Viruses
  - Indications of Virus Attack
  - Virus Hoaxes and Fake Antiviruses
  - Ransomware
  - 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
    - Sam's Virus Generator and JPS Virus Maker
    - Andreinick05's Batch Virus Maker and DeadLine's Virus Maker
    - Sonic Bat - Batch File Virus Creator and Poison Virus Maker
- Computer Worms
  - How Is a Worm Different from a Virus?
  - Computer Worms: Ghost Eye Worm
  - Worm Maker: Internet Worm Maker Thing
- Malware Reverse Engineering
  - What is Sheep Dip Computer?
  - Anti-Virus Sensor Systems
  - Malware Analysis Procedure: Preparing Testbed
  - Malware Analysis Procedure
  - Malware Analysis Tool: IDA Pro
  - Online Malware Testing: VirusTotal
  - Online Malware Analysis Services
  - Trojan Analysis: Neverquest
  - Virus Analysis: Ransom Cryptolocker
  - Worm Analysis: Darlloz (Internet of Things (IoT) Worm)
- Malware Detection
  - How to Detect Trojans
    - Scanning for Suspicious Ports
      - Tools: TCPView and CurrPorts
    - Scanning for Suspicious Processes
      - Process Monitoring Tool: What's Running
      - Process Monitoring Tools



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Scanning for Suspicious Registry Entries
    - Registry Entry Monitoring Tool: RegScanner
    - Registry Entry Monitoring Tools
  - Scanning for Suspicious Device Drivers
    - Device Drivers Monitoring Tool: DriverView
    - Device Drivers Monitoring Tools
  - Scanning for Suspicious Windows Services
    - Windows Services Monitoring Tool: Windows Service Manager (SrvMan)
    - Windows Services Monitoring Tools
  - Scanning for Suspicious Startup Programs
    - Windows 8 Startup Registry Entries
    - Startup Programs Monitoring Tool: 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
    - Virus Detection Methods
  - Countermeasures
    - Trojan Countermeasures
    - Backdoor Countermeasures
    - Virus and Worms Countermeasures
  - Anti-Malware Software
    - Anti-Trojan Software
      - TrojanHunter
      - Emsisoft Anti-Malware
    - Anti-Trojan Software
    - Companion Antivirus: Immundet
    - Anti-virus Tools
  - Penetration Testing
    - Pen Testing for Trojans and Backdoors
    - Penetration Testing for Virus
- Module 07: Sniffing**
- Sniffing Concepts
    - Network Sniffing and Threats
    - How a Sniffer Works
    - Types of Sniffing
      - Passive Sniffing
      - Active Sniffing
    - How an Attacker Hacks the Network Using Sniffers
    - Protocols Vulnerable to Sniffing
    - Sniffing in the Data Link Layer of the OSI Model
    - Hardware Protocol Analyzer
    - Hardware Protocol Analyzers
    - SPAN Port
    - Wiretapping
    - Lawful Interception
    - Wiretapping Case Study: PRISM



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- MAC Attacks
  - MAC Address/CAM Table
  - How CAM Works
  - What Happens When CAM Table Is Full?
  - MAC Flooding
  - Mac Flooding Switches with macof
  - Switch Port Stealing
  - How to Defend against MAC Attacks
- DHCP Attacks
  - How DHCP Works
  - DHCP Request/Reply Messages
  - IPv4 DHCP Packet Format
  - DHCP Starvation Attack
  - DHCP Starvation Attack Tools
  - Rogue DHCP Server Attack
  - How to Defend Against DHCP Starvation and Rogue Server Attack
- ARP Poisoning
  - What Is Address Resolution Protocol (ARP)?
  - ARP Spoofing Attack
  - How Does ARP Spoofing Work
  - Threats of ARP Poisoning
  - ARP Poisoning Tool
    - Cain & Abel and WinArpAttacker
    - Ufasoft Snif
  - How to Defend Against ARP Poisoning
  - Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
  - ARP Spoofing Detection: XArp
- Spoofing Attack
  - MAC Spoofing/Duplicating
  - MAC Spoofing Technique: Windows
  - MAC Spoofing Tool: SMAC
  - IRDP Spoofing
  - How to Defend Against MAC Spoofing
- DNS Poisoning
  - DNS Poisoning Techniques
  - Intranet DNS Spoofing
  - Internet DNS Spoofing
  - Proxy Server DNS Poisoning
  - DNS Cache Poisoning
  - How to Defend Against DNS Spoofing
- Sniffing Tools
  - Sniffing Tool: Wireshark
  - Follow TCP Stream in Wireshark
  - Display Filters in Wireshark
  - Additional Wireshark Filters
  - Sniffing Tool
    - SteelCentral Packet Analyzer
    - Tcpdump/Windump
  - Packet Sniffing Tool: Capsa Network Analyzer
  - Network Packet Analyzer
    - OmniPeek Network Analyzer
    - Observer
    - Sniff-O-Matic
  - TCP/IP Packet Crafter: Colasoft Packet Builder
  - Network Packet Analyzer: RSA NetWitness Investigator
  - Additional Sniffing Tools
  - Packet Sniffing Tools for Mobile: Wi.cap. Network Sniffer Pro and FaceNiff



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Counter measures
  - How to Defend Against Sniffing
- Sniffing Detection Techniques
  - How to Detect Sniffing
  - Sniffer Detection Technique
    - Ping Method
    - ARP Method
    - DNS Method
  - Promiscuous Detection Tool
    - PromqryUI
    - Nmap
- Sniffing Pen Testing
  - Eavesdropping and Shoulder Surfing
  - Dumpster Diving
  - Reverse Social Engineering, Piggybacking, and Tailgating

## Module 08: Social Engineering

- Social Engineering Concepts
    - 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
  - Social Engineering Techniques
    - Types of Social Engineering
      - Human-based Social Engineering
      - Impersonation
        - Impersonation Scenario
          - ✓ Over-Helpfulness of Help Desk
          - ✓ Third-party Authorization
          - ✓ Tech Support
          - ✓ Internal Employee/Client/Vendor
          - ✓ Repairman
          - ✓ Trusted Authority Figure
  - Insider Attack
  - Disgruntled Employee
  - Preventing Insider Threats
  - Common Social Engineering Targets and Defense Strategies
- Impersonation on Social Networking Sites
  - Social Engineering Through Impersonation on Social Networking Sites
  - Social Engineering on Facebook
  - Social Engineering on LinkedIn and Twitter
  - Risks of Social Networking to Corporate Networks
- Identity Theft
  - Identity Theft Statistics
  - Identify Theft
  - How to Steal an Identity
    - STEP 1
    - STEP 2
    - Comparison
    - STEP 3
  - Real Steven Gets Huge Credit Card Statement



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Identity Theft - Serious Problem
  - Social Engineering Countermeasures
    - How to Detect Phishing Emails
    - Anti-Phishing Toolbar
      - Netcraft
      - PhishTank
    - Identity Theft Countermeasures
  - Penetration Testing
    - Social Engineering Pen Testing
      - Using Emails
      - Using Phone
      - In Person
      - Social Engineering Toolkit (SET)
  - Organized Cyber Crime: Organizational Chart
  - Botnet
  - A Typical Botnet Setup
  - Botnet Ecosystem
  - Scanning Methods for Finding Vulnerable Machines
  - How Malicious Code Propagates?
  - Botnet Trojan
    - Blackshades NET
    - Cythosia Botnet and Andromeda Bot
    - PlugBot
  - DDoS Case Study
    - DDoS Attack
    - Hackers Advertise Links to Download Botnet
  - DoS/DDoS Attack Tools
    - Pandora DDoS Bot Toolkit
    - Dereil and HOIC
    - DoS HTTP and BanglaDos
    - DoS and DDoS Attack Tools
    - DoS and DDoS Attack Tool for Mobile
      - AnDOSid
      - Low Orbit Ion Cannon (LOIC)
  - Counter-measures
    - Detection Techniques
    - Activity Profiling
    - Wavelet Analysis
    - Sequential Change-Point Detection
    - DoS/DDoS Countermeasure Strategies
    - DDoS Attack Countermeasures
      - Protect Secondary Victims
      - Detect and Neutralize Handlers
      - Detect Potential Attacks
      - Deflect Attacks
- Module 09: Denial-of-Service**
- DoS/DDoS Concepts
    - DDoS Attack Trends
    - What is a Denial of Service Attack?
    - What Are Distributed Denial of Service Attacks?
    - How Distributed Denial of Service Attacks Work
  - DoS/DDoS Attack Techniques
    - Basic Categories of DoS/DDoS Attack Vectors
    - DoS/DDoS 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
      - Distributed Reflection Denial of Service (DRDoS)
  - Botnets



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- 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 Appliances
  - DoS/DDoS Protection Tools
    - DoS/DDoS Protection Tool: FortGuard Anti-DDoS Firewall 2014
    - DoS/DDoS Protection Tools
  - DoS/DDoS Attack Penetration Testing
- Module 10: Session Hijacking**
- Session Hijacking Concepts
    - What is Session Hijacking?
    - Why Session Hijacking is Successful?
    - Session Hijacking Process
    - Packet Analysis of a Local Session Hijack
    - Types of Session Hijacking
    - Session Hijacking in OSI Model
    - Spoofing vs. Hijacking
  - Application Level Session Hijacking
    - Compromising Session IDs using Sniffing
    - Compromising Session IDs by Predicting Session Token
    - How to Predict a Session Token
    - Compromising Session IDs Using Man-in-the-Middle Attack
    - Compromising Session IDs Using Man-in-the-Browser Attack
    - Steps to Perform Man-in-the-Browser Attack
  - Compromising Session IDs Using Client-side Attacks
  - Compromising Session IDs Using Client-side Attacks: Cross-site Script Attack
  - Compromising Session IDs Using Client-side Attacks: Cross-site Request Forgery Attack
  - Compromising Session IDs Using Session Replay Attack
  - Compromising Session IDs Using Session Fixation
  - Session Fixation Attack
  - Session Hijacking Using Proxy Servers
- Network-level Session Hijacking
    - The 3-Way Handshake
    - TCP/IP Hijacking
    - TCP/IP Hijacking Process
    - IP Spoofing: Source Routed Packets
    - RST Hijacking
    - Blind Hijacking
    - MiTM Attack Using Forged ICMP and ARP Spoofing
    - UDP Hijacking
  - Session Hijacking Tools
    - Session Hijacking Tool
      - Zaproxy
      - Burp Suite and Hijack
    - Session Hijacking Tools
    - Session Hijacking Tools for Mobile: DroidSheep and DroidSniff
  - Counter-measures
    - Session Hijacking Detection Methods
    - Protecting against Session Hijacking





# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Methods to Prevent Session Hijacking
  - To be Followed by Web Developers
  - To be Followed by Web Users
- Approaches Vulnerable to Session Hijacking and their Preventative Solutions
- IPSec
- Modes of IPsec
- IPsec Architecture
- IPsec Authentication and Confidentiality
- Components of IPsec
- Session Hijacking Pen Testing
- Module 11: Hacking Webservers**
- Webservice Concepts
  - Web Server Security Issue
  - Why Web Servers Are Compromised
  - Impact of Webservice Attacks
  - Open Source Webservice Architecture
  - IIS Webservice Architecture
- Webservice Attacks
  - DoS/DDoS Attacks
  - DNS Server Hijacking
  - DNS Amplification Attack
  - Directory Traversal Attacks
  - Man-in-the-Middle/Sniffing Attack
  - Phishing Attacks
  - Website Defacement
  - Webservice Misconfiguration
    - Webservice Misconfiguration Example
  - HTTP Response Splitting Attack
  - Web Cache Poisoning Attack
  - SSH Brute-force Attack
- Webservice Password Cracking
  - Webservice Password Cracking Techniques
- Web Application Attacks
- Attack Methodology
  - Webservice Attack Methodology
    - Information Gathering
    - Information Gathering from Robots.txt File
    - Webservice Footprinting
  - Webservice Footprinting Tools
  - Enumerating Webservice Information Using Nmap
  - Webservice Attack Methodology
    - Mirroring a Website
    - Vulnerability Scanning
    - Session Hijacking
    - Hacking Web Passwords
- Webservice Attack Tools
  - Metasploit
    - Metasploit Architecture
    - Metasploit Exploit Module
    - Metasploit Payload Module
    - Metasploit Auxiliary Module
    - Metasploit NOPS Module
  - Webservice Attack Tools: Wfetch
  - Web Password Cracking Tool: THC-Hydra and Brutus
- Counter-measures
  - Place Web Servers in Separate Secure Server Security Segment on Network
  - Countermeasures
    - Patches and Updates
    - Protocols
    - Accounts
    - Files and Directories
  - Detecting Web Server Hacking Attempts



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- How to Defend Against Web Server Attacks
- How to Defend against HTTP Response Splitting and Web Cache Poisoning
- How to Defend against DNS Hijacking
- Patch Management
  - Patches and Hotfixes
  - What Is Patch Management?
  - Identifying Appropriate Sources for Updates and Patches
  - Installation of a Patch
  - Implementation and Verification of a Security Patch or Upgrade
  - Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)
  - Patch Management Tools
- Webservers Security Tools
  - Web Application Security Scanner: Syhunt Dynamic and N-Stalker Web Application Security Scanner
  - Web Server Security Scanner: Wikto and Acunetix Web Vulnerability Scanner
  - Web Server Malware Infection Monitoring Tool
    - HackAlert
    - QualysGuard Malware Detection
  - Webservers Security Tools
- Webservers Pen Testing
  - Web Server Pen Testing Tool
    - CORE Impact® Pro
    - Immunity CANVAS
    - Arachni

## Module 12: Hacking Web Applications

- Web App Concepts
  - Introduction to Web Applications
  - How Web Applications Work?
  - Web Application Architecture
  - Web 2.0 Applications
  - Vulnerability Stack
- Web App Threats
  - 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
    - Websites Vulnerable to XSS Attack
  - Cross-Site Request Forgery (CSRF) Attack
    - How CSRF Attacks Work?



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- 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
- CAPTCHA Attacks
- 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
- Web App Hacking Methodology
  - Footprint Web Infrastructure
    - Server Discovery
    - Service Discovery
    - Server Identification/Banner Grabbing
      - Detecting Web App Firewalls and Proxies on Target Site
    - Hidden Content Discovery
    - Web Spidering Using Burp Suite
    - Web Crawling Using Mozenda Web Agent Builder
  - Attack Web Servers
    - Hacking Web Servers
    - Web Server Hacking Tool: WebInspect
  - Analyze Web Applications
    - Identify Entry Points for User Input
    - Identify Server-Side Technologies
    - Identify Server-Side Functionality
    - Map the Attack Surface
  - Attack Authentication Mechanism
    - Username Enumeration
    - Password Attacks
      - Password Functionality Exploits
      - Password Guessing
      - Brute-forcing
    - Session Attacks: Session ID Prediction/ Brute-forcing
    - Cookie Exploitation: Cookie Poisoning
  - Authorization Attack Schemes
    - Authorization Attack
    - HTTP Request Tampering
    - Authorization Attack: Cookie Parameter Tampering
  - Attack Session Management Mechanism
    - Session Management Attack
    - Attacking Session Token Generation Mechanism
    - Attacking Session Tokens Handling Mechanism: Session Token Sniffing
  - Perform Injection Attacks
    - Injection Attacks/Input Validation Attacks
  - Attack Data Connectivity
    - Connection String Injection
    - Connection String Parameter Pollution (CSPP) Attacks
    - Connection Pool DoS



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Attack Web App Client
- Attack Web Services
  - Web Services Probing Attacks
  - Web Service Attacks
    - SOAP Injection
    - XML Injection
  - Web Services Parsing Attacks
  - Web Service Attack Tool: soapUI and XMLSpy
- Web Application Hacking Tools
  - Web Application Hacking Tools
    - Burp Suite Professional
    - CookieDigger
    - WebScarab
  - Web Application Hacking Tools
- Countermeasures
  - 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?
  - Guidelines for Secure CAPTCHA Implementation
  - Web Application Countermeasures
  - How to Defend Against Web Application Attacks?
- Security Tools
  - Web Application Security Tool
    - Acunetix Web Vulnerability Scanner
    - Watcher Web Security Tool
    - Netsparker
    - N-Stalker Web Application Security Scanner
  - VampireScan
  - Web Application Security Tools
  - Web Application Firewall
    - dotDefender
    - ServerDefender VP
  - Web Application Firewall
  - Web App Pen Testing
    - 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
    - Web Application Pen Testing Framework
      - Kali Linux
      - Metasploit
      - Browser Exploitation Framework (BeEF)
      - PowerSploit

## Module 13: SQL Injection

- SQL Injection Concepts
  - What is SQL Injection?
  - Why Bother about SQL Injection?
  - How Web Applications Work?
  - SQL Injection and Server-side Technologies
  - Understanding HTTP Post Request
  - Example: Normal SQL Query
  - Understanding an SQL Injection Query
    - Code Analysis



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Example of a Web App Vulnerable to SQL Injection
  - BadProductList.aspx
  - Attack Analysis
- Example of SQL Injection
  - Updating Table
  - Adding New Records
  - Identifying the Table Name
  - Deleting a Table
- Types of SQL Injection
  - Error Based SQL Injection
  - Union SQL Injection
  - Blind SQL Injection
  - No Error Messages Returned
  - Blind SQL Injection: WAITFOR DELAY (YES or NO Response)
  - Boolean Exploitation Technique
- SQL Injection Methodology
  - Information Gathering and SQL Injection Vulnerability Detection
    - Information Gathering
    - Identifying Data Entry Paths
    - Extracting Information through Error Messages
    - Testing for SQL Injection
    - Additional Methods to Detect SQL Injection
    - SQL Injection Black Box Pen Testing
    - Source Code Review to Detect SQL Injection Vulnerabilities
  - Launch SQL Injection Attacks
    - Perform Union SQL Injection
    - Perform Error Based SQL Injection
    - Perform Error Based SQL Injection: Using Stored Procedure Injection
- Bypass Website Logins Using SQL Injection
- Perform Blind SQL Injection – Exploitation (MySQL)
- Blind SQL Injection
  - Extract Database User
  - Extract Database Name
  - Extract Column Name
  - Extract Data from ROWS
- Perform Double Blind SQL Injection - Classical Exploitation (MySQL)
  - Perform Blind SQL Injection Using Out of Band Exploitation Technique
- Exploiting Second-Order SQL Injection
- Advanced 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 File System
  - Network Reconnaissance Using SQL Injection



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Network Reconnaissance Full Query
- SQL Injection Tools
  - BSQLHacker
  - Marathon Tool
  - SQL Power Injector
  - Havij
  - SQL Injection Tools
  - SQL Injection Tool for Mobile
    - DroidSQLi
    - sqlmapchik
- Evasion Techniques
  - Evading IDS
  - Types of Signature Evasion Techniques
  - Evasion Technique
    - Sophisticated Matches
    - Hex Encoding
    - Manipulating White Spaces
    - In-line Comment
    - Char Encoding
    - String Concatenation
    - Obfuscated Codes
- Counter-measures
  - How to Defend Against SQL Injection Attacks?
  - How to Defend Against SQL Injection Attacks: Use Type-Safe SQL Parameters
  - How to Defend Against SQL Injection Attacks
  - SQL Injection Detection Tool
    - dotDefender
    - IBM Security AppScan
    - WebCruiser
  - Snort Rule to Detect SQL Injection Attacks
  - SQL Injection Detection Tools

## Module 14: Hacking Wireless Networks

- Wireless Concepts
  - Wireless Terminologies
  - Wireless Networks
  - Wi-Fi Networks at Home and Public Places
  - Wireless Technology Statistics
  - 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 Chalking
    - Wi-Fi Chalking Symbols
  - Types of Wireless Antenna
    - Parabolic Grid Antenna
- Wireless Encryption
  - 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 Encryption?
  - How to Defend Against WPA Cracking?
- Wireless Threats
  - Access Control Attacks
  - Integrity Attacks
  - Confidentiality Attacks
  - Availability Attacks
  - Authentication Attacks
  - Rogue Access Point Attack



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- 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
  - Wi-Fi Discovery
    - Footprint the Wireless Network
    - Find Wi-Fi Networks to Attack
    - Wi-Fi Discovery Tool
      - inSSIDer and NetSurveyor
      - Vistumbler and NetStumbler
    - Wi-Fi Discovery Tools
    - Mobile-based Wi-Fi Discovery Tool
  - GPS Mapping
    - GPS Mapping Tool
      - WIGLE
      - Skyhook
    - Wi-Fi Hotspot Finder
      - Wi-Fi Finder
      - WeFi
    - 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
      - SteelCentral Packet Analyzer
    - OmniPeek Network Analyzer
    - CommView for Wi-Fi
      - What is Spectrum Analysis?
      - Wi-Fi Packet Sniffers
  - Launch Wireless Attacks
    - 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)?
  - Crack Wi-Fi Encryption
    - How to Crack WEP Using Aircrack
    - 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



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- WEP/WPA Cracking Tool for Mobile: Penetrate Pro
  - Wireless Hacking Tools
    - Wi-Fi Sniffer: Kismet
    - Wardriving Tools
    - RF Monitoring Tools
    - Wi-Fi Traffic Analyzer Tools
    - Wi-Fi Raw Packet Capturing and Spectrum Analyzing Tools
    - Wireless Hacking Tools for Mobile: HackWifi and Backtrack Simulator
  - Bluetooth Hacking
    - Bluetooth Stack
    - Bluetooth Threats
    - How to BlueJack a Victim?
    - Bluetooth Hacking Tool
      - Super Bluetooth Hack
      - PhoneSnoop
      - BlueScanner
    - Bluetooth Hacking Tools
  - Counter-measures
    - How to Defend Against Bluetooth Hacking?
    - How to Detect and Block Rogue AP?
    - Wireless Security Layers
    - How to Defend Against Wireless Attacks?
  - Wireless Security Tools
    - Wireless Intrusion Prevention Systems
    - Wireless IPS Deployment
    - Wi-Fi Security Auditing Tool
      - AirMagnet WiFi Analyzer
      - Motorola's AirDefense Services Platform (ADSP)
      - Adaptive Wireless IPS
      - Aruba RFProtect
    - Wi-Fi Intrusion Prevention System
    - Wi-Fi Predictive Planning Tools
    - Wi-Fi Vulnerability Scanning Tools
  - Bluetooth Security Tool: Bluetooth Firewall
  - Wi-Fi Security Tools for Mobile: Wifi Protector, WiFiGuard, and Wifi Inspector
  - Wi-Fi Pen Testing
    - 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
- ## Module 15: Hacking Mobile Platforms
- Mobile Platform Attack Vectors
    - Vulnerable Areas in Mobile Business Environment
    - OWASP Mobile Top 10 Risks
    - Anatomy of a Mobile Attack
    - How a Hacker can Profit from Mobile when Successfully Compromised
    - Mobile Attack Vectors
    - Mobile Platform Vulnerabilities and Risks
    - Security Issues Arising from App Stores
    - App Sandboxing Issues
    - Mobile Spam
    - SMS Phishing Attack (SMiShing) (Targeted Attack Scan)
      - Why SMS Phishing is Effective?
      - SMS Phishing Attack Examples





# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections
- Hacking Android OS
  - Android OS
  - Android OS Architecture
  - Android Device Administration API
  - Android Vulnerabilities
  - Android Rooting
    - Rooting Android Phones using SuperOneClick
    - Rooting Android Phones Using Superboot
    - Android Rooting Tools
  - Hacking Networks Using Network Spoofer
  - Session Hijacking Using DroidSheep
  - Android-based Sniffer
    - FaceNiff
    - Packet Sniffer, tPacketCapture, and Android PCAP
  - Android Trojan
    - ZitMo (ZeuS-in-the-Mobile)
    - FakeToken and TRAMP.A
    - Fakedefender and Obad
    - FakeInst and OpFake
    - AndroRAT and Dendroid
  - Securing Android Devices
  - Google Apps Device Policy
  - Remote Wipe Service: Remote Wipe
  - Android Security Tool
    - DroidSheep Guard
    - TrustGo Mobile Security and Sophos Mobile Security
    - 360 Security, AVL, and Avira Antivirus Security
  - Android Vulnerability Scanner: X-Ray
  - Android Device Tracking Tools
- Hacking iOS
  - Apple iOS
  - Jailbreaking iOS
    - Types of Jailbreaking
    - Jailbreaking Techniques
    - App Platform for Jailbroken Devices: Cydia
    - Jailbreaking Tool: Pangu
    - Untethered Jailbreaking of iOS 7.1.1/7.1.2 Using Pangu for Mac
    - Jailbreaking Tools
      - Redsn0w and Absinthe
      - evasi0n7 and GeekSn0w
      - Sn0wbreeze and PwnageTool
      - LimeRa1n and Blackra1n
  - Guidelines for Securing iOS Devices
  - iOS Device Tracking Tools
- Hacking Windows Phone OS
  - Windows Phone 8 Architecture
  - Secure Boot Process
  - Guidelines for Securing Windows OS Devices
  - Windows OS Device Tracking Tool: FollowMee GPS Tracker
- Hacking BlackBerry
  - BlackBerry Operating System
  - BlackBerry Enterprise Solution Architecture
  - Blackberry Attack Vectors
    - Malicious Code Signing
    - JAD File Exploits and Memory/ Processes Manipulations
    - Short Message Service (SMS) Exploits



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Email Exploits
- PIM Data Attacks and TCP/IP Connections Vulnerabilities
- Guidelines for Securing BlackBerry Devices
- BlackBerry Device Tracking Tools: MobileTracker and Position Logic Blackberry Tracker
- Mobile Spyware: mSpy and StealthGenie
- Mobile Spyware
- Mobile Device Management (MDM)
  - MDM Solution: MaaS360 Mobile Device Management (MDM)
  - MDM Solutions
  - Bring Your Own Device (BYOD)
    - BYOD Risks
    - BYOD Policy Implementation
    - BYOD Security Guidelines for Administrator
    - BYOD Security Guidelines for Employee
- Mobile Security Guidelines and Tools
  - General Guidelines for Mobile Platform Security
  - Mobile Device Security Guidelines for Administrator
  - SMS Phishing Countermeasures
  - Mobile Protection Tool
    - BullGuard Mobile Security
    - Lookout
    - WISEID
    - zIPS
  - Mobile Protection Tools
  - Mobile Anti-Spyware

- Mobile Pen Testing
  - Android Phone Pen Testing
  - iPhone Pen Testing
  - Windows Phone Pen Testing
  - BlackBerry Pen Testing
  - Mobile Pen Testing Toolkit
    - zANTI
    - dSploit
    - Hackode (The Hacker's Toolbox)

## Module 16: Evading IDS, Firewalls, and Honeypots

- IDS, Firewall and Honeypot Concepts
  - Intrusion Detection Systems (IDS) and their Placement
    - How IDS Works?
    - Ways to Detect an Intrusion
    - General Indications of Intrusions
    - General Indications of System Intrusions
    - Types of Intrusion Detection Systems
    - System Integrity Verifiers (SIV)
  - Firewall
    - Firewall Architecture
    - DeMilitarized Zone (DMZ)
    - Types of Firewall
      - Packet Filtering Firewall
      - Circuit-Level Gateway Firewall
      - Application-Level Firewall
      - Stateful Multilayer Inspection Firewall



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- Honeypot
  - Types of Honeypots
- IDS, Firewall and Honeypot System
  - 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
  - Intrusion Detection Tools for Mobile
  - Firewall
    - ZoneAlarm PRO Firewall 2015
    - Comodo Firewall
  - Firewalls
  - Firewalls for Mobile: Android Firewall and Firewall iP
  - Firewalls for Mobile
  - Honeypot Tool: KFSensor and SPECTER
  - Honeypot Tools
  - Honeypot Tool for Mobile: HosTaGe
- Evading IDS
  - 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
- Desynchronization - Post Connection SYN
- Other Types of Evasion
- Evading Firewalls
  - Firewall Identification
    - Port Scanning
    - Firewalking
    - Banner Grabbing
  - IP Address Spoofing
  - Source Routing
  - 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
  - Why do I Need HTTP Tunneling
  - HTTP Tunneling Tools
    - HTTPPort and HTTPHost
    - Super Network Tunnel
    - HTTP-Tunnel
  - Bypassing Firewall through SSH Tunneling Method
  - SSH Tunneling Tool: Bitwise
  - Bypassing Firewall through External Systems
  - Bypassing Firewall through MITM Attack
  - Bypassing Firewall through Content



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

- IDS/Firewall Evading Tools
  - IDS/Firewall Evasion Tool
    - Traffic IQ Professional
    - tcp-over-dns
  - IDS/Firewall Evasion Tools
  - Packet Fragment Generator: Colasoft Packet Builder
  - Packet Fragment Generators
- Detecting Honeypots
  - Detecting Honeypots
  - Honeypot Detecting Tool: Send-Safe Honeypot Hunter
- IDS/Firewall Evasion Counter-measures
  - Countermeasures
- Penetration Testing
  - Firewall/IDS Penetration Testing
  - Firewall Penetration Testing
  - IDS Penetration Testing
- Domain Name System (DNS) Attacks
- Side Channel Attacks or Cross-guest VM Breaches
  - Side Channel Attack Countermeasures
  - SQL Injection Attacks
- Cryptanalysis Attacks
  - Cryptanalysis Attack Countermeasures
- Wrapping Attack
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

## Module 17: Cloud Computing

- Introduction to Cloud Computing
  - Types of Cloud Computing Services
  - Separation of Responsibilities in Cloud
  - Cloud Deployment Models
  - NIST Cloud Computing Reference Architecture
  - Cloud Computing Benefits
  - Understanding Virtualization
  - Benefits of Virtualization in Cloud
- Cloud Computing Threats
- Cloud Computing Attacks
  - Service Hijacking using Social Engineering Attacks
  - Service Hijacking using Network Sniffing
  - Session Hijacking using XSS Attack
  - Session Hijacking using Session Riding
- Cloud Security
  - Cloud Security Control Layers
  - Cloud Security is the Responsibility of both Cloud Provider and Consumer
  - Cloud Computing Security Considerations
  - Placement of Security Controls in the Cloud
  - Best Practices for Securing Cloud
  - NIST Recommendations for Cloud Security
  - Organization/Provider Cloud Security Compliance Checklist
- Cloud Security Tools
  - Core CloudInspect
  - CloudPassage Halo
  - Cloud Security Tools
- Cloud Penetration Testing
  - What is Cloud Pen Testing?
  - Key Considerations for Pen Testing in the Cloud
  - Scope of Cloud Pen Testing
  - Cloud Penetration Testing
  - Recommendations for Cloud Testing



# CEH: Certified Ethical Hacker

Course ID #: 1275-100-ZZ-W

Hours: 35

## Module 18: Cryptography

- Market Survey 2014: The Year of Encryption
- Case Study: Heartbleed
- Case Study: Poodlebleed
- Cryptography Concepts
  - Cryptography
  - Types of Cryptography
  - Government Access to Keys (GAK)
- Encryption Algorithms
  - Ciphers
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
  - RC4, RC5, RC6 Algorithms
  - The DSA and Related Signature Schemes
  - RSA (Rivest Shamir Adleman)
    - The RSA Signature Scheme
    - Example of RSA Algorithm
  - Message Digest (One-way Hash) Functions
    - Message Digest Function: MD5
  - Secure Hashing Algorithm (SHA)
  - What is SSH (Secure Shell)?
- Cryptography Tools
  - MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles
  - Hash Calculators for Mobile: MD5 Hash Calculator, Hash Droid, and Hash Calculator
  - Cryptography Tool
    - Advanced Encryption Package 2014
    - BCTextEncoder
  - Cryptography Tools
  - Cryptography Tools for Mobile: Secret Space Encryptor, CryptoSymm, and Cipher Sender
- Public Key Infrastructure(PKI)
  - Certification Authorities
  - Signed Certificate (CA) Vs. Self Signed Certificate
- Email Encryption
  - Digital Signature
  - SSL (Secure Sockets Layer)
  - Transport Layer Security (TLS)
  - Cryptography Toolkit
    - OpenSSL
    - Keyczar
  - Pretty Good Privacy (PGP)
- Disk Encryption
  - Disk Encryption Tools: Symantec Drive Encryption and GiliSoft Full Disk Encryption
  - Disk Encryption Tools
- Cryptography Attacks
  - Code Breaking Methodologies
  - Brute-Force Attack
  - Meet-in-the-Middle Attack on Digital Signature Schemes
  - Side Channel Attack
    - Side Channel Attack - Scenario
- Cryptanalysis Tools
  - Cryptanalysis Tool: CrypTool
  - Cryptanalysis Tools
  - Online MD5 Decryption Tool