**Be Aware
Hackers will hit you from anywhere
at any time**

Certified Ethical Hacker version 8

Ethical Hacking & Counter Measures

5-days Instructor Led Training/Workshop

Overview

To beat a hacker, you need to think like one! This is exactly what this class will teach you. It is the pinnacle of the most desired information security training program any information security professional will ever want to be in. To master the hacking technologies, you will need to become one.

The Certified Ethical Hacker class will immerse the students into a hands-on environment where they will be shown how to conduct ethical hacking. They will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! They will scan, test, hack and secure their own systems.

The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this intensive 5 day class they will have hands on understanding and experience in Ethical Hacking.
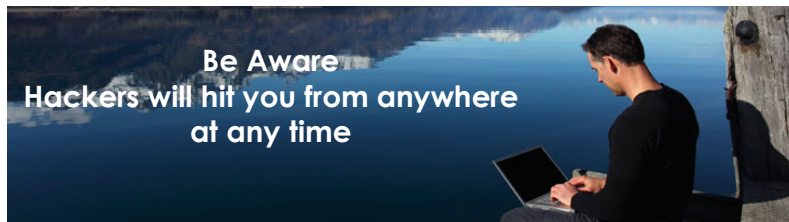
What you will learn.

Upon completion of this course, students will be able to:
- Understand how intruders escalate privileges
- Understand Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation
- Understand Ethical Hacking.

.

Target Audience

This course will significantly benefit:

- Security officers
- Auditors
- Security Professionals
- Police and other law enforcement personnel
- Defense and Military personnel
- e-Business Security professionals
- Site Administrators
- Systems administrators

- Legal professionals, Banking
- Insurance and other professionals
- IT managers.
- IT consultants who want to learn more about hacking tools and techniques will also benefit.
- And anyone who is concerned about the integrity of their network infrastructure.

BTCS

Be Aware
Hackers will hit you from anywhere
at any time

BTCS

Requirements

Trainees are typically experienced system, network or IT administrators, although interested persons from other backgrounds are welcome to contact the organizers to discuss the suitability of the course for them. They are expected to have an awareness of the security issues involved in connecting computers to the Internet, and must be committed to using their skills to improve the security of computers and networks. Familiarity with Internet protocols, addresses and port numbers is beneficial.

Certification

This course prepares you for EC-Council Certified Ethical Hacker exam 312-50. Students van take the CEH-exam at an Athorized Testing Center of Vue Pearson or Promteric. Students need to pass the 312-50 exam to complete the requirements for receiving 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.

N.B. *Not anyone can be a student — the Training organization will make sure the applicants work for legitimate companies.*

Be Aware
Hackers will hit you from anywhere
at any time

Outline: Certtified Ethical Hacker (CEH) version 8

Module 01: Introduction to Ethical Hacking
- Information Security Overview
  - Internet Crime Current Report: IC3
  - Data Breach Investigations Report
  - Essential Terminology
  - Elements of Information Security
  - The Security, Functionality, and Usability Triangle
- Information Security Threats and Attack Vectors
  - Top Information Security Attack Vectors
  - Motives, Goals, and Objectives of Information Security Attacks
  - Information Security Threats
  - Information Warfare
  - IPv6 Security Threats
- Hacking Concepts
  - Hacking vs. Ethical Hacking
  - Effects of Hacking on Business
  - Who Is a Hacker?
  - Hacker Classes
  - Hacktivism
- Hacking Phases
- Types of Attacks
  - Types of Attacks on a System
  - Operating System Attacks
  - Misconfiguration Attacks
  - Application-Level Attacks
  - Examples of Application-Level Attacks
  - Shrink Wrap Code Attacks
- Information Security Controls
  - Why Ethical Hacking is Necessary
  - Scope and Limitations of Ethical Hacking
  - Skills of an Ethical Hacker
  - Defense in Depth
  - Incident Management Process
  - Information Security Policies
  - Classification of Security Policies
  - Structure and Contents of Security Policies
  - Types of Security Policies
  - Steps to Create and Implement Security Policies
  - Examples of Security Policies
  - Vulnerability Research
  - Vulnerability Research Websites
  - What Is Penetration Testing?
  - Why Penetration Testing
  - Penetration Testing Methodology

Module 02: Footprinting and Reconnaissance
- Footprinting Concepts
  - Footprinting Terminology
  - What is Footprinting?
  - Why Footprinting?
  - Objectives of Footprinting
- Footprinting Threats
  - Footprinting Threats
- Footprinting Methodology
  - Footprinting through Search Engines
  - Finding Company's External and Internal URLs
  - Public and Restricted Websites
  - Collect Location Information
  - People Search
  - People Search Online Services
  - People Search on Social Networking Services
  - Gather Information from Financial Services
  - Footprinting through Job Sites
  - Monitoring Target Using Alerts
  - Website Footprinting
    - Mirroring Entire Website
    - Website Mirroring Tools
    - Extract Website Information from http://www.archive.org
    - Monitoring Web Updates Using Website Watcher
  - 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

Be Aware
Hackers will hit you from anywhere
at any time

BTCS   *BTCS*

Outline: Certtified Ethical Hacker (CEH) version 8

- o Footprinting using Google
  - 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
- o WHOIS Footprinting
  - WHOIS Lookup
  - WHOIS Lookup Result Analysis
  - WHOIS Lookup Tool: SmartWhois
  - WHOIS Lookup Tools
  - WHOIS Lookup Online Tools
- o DNS Footprinting
  - Extracting DNS Information
  - DNS Interrogation Tools
- o Network Footprinting
  - Locate the Network Range
  - Determine the Operating System
  - Traceroute
  - Traceroute Analysis
  - Traceroute Tools
- o Footprinting through Social Engineering
  - Footprinting through Social Engineering
  - Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving
- o Footprinting through
  - Collect Information through Social Engineering on Social Networking Sites
  - Information Available on Social Networking Sites
  - Collecting Facebook Information
  - Collecting Twitter Information
  - Collecting Linkedin Information
  - Collecting Youtube Information
  - Tracking Users on Social Networking Sites

- o Footprinting Tools
  - Footprinting Tool: Maltego
  - Footprinting Tool: Domain Name Analyzer Pro
  - Footprinting Tool: Web Data Extractor
  - Additional Footprinting Tools
- o Footprinting Countermeasures
- o Footprinting Penetration Testing
  - Footprinting Pen Testing
  - Footprinting Pen Testing Report Templates

Module 03: Scanning Networks
- Overview of Network Scanning
- CEH Scanning Methodology
  - o Check for Live Systems
    - Checking for Live Systems - ICMP Scanning
    - Ping Sweep
    - Ping Sweep Tools
  - o Check for Open Ports
    - Three-Way Handshake
    - TCP Communication Flags
    - Create Custom Packet Using TCP Flags
    - Create Custom Packet Using TCP Flags
    - Scanning IPv6 Network
    - Scanning Tool: Nmap
    - Hping2 / Hping3
    - Hping Commands
    - Scanning Techniques
    - TCP Connect / Full Open Scan
    - Stealth Scan (Half-open Scan)
    - Stealth Scan (Half-open Scan)
    - Xmas Scan
    - FIN Scan
    - NULL Scan
    - IDLE Scan
    - IDLE Scan: Step 1
    - IDLE Scan: Step 2 and 3
    - ICMP Echo Scanning/List Scan
    - UDP Scanning
    - Inverse TCP Flag Scanning
    - ACK Flag Scanning
    - Scanning Tool: NetScan Tools Pro
    - Scanning Tools
    - Do Not Scan These IP Addresses (Unless you want to get into trouble)
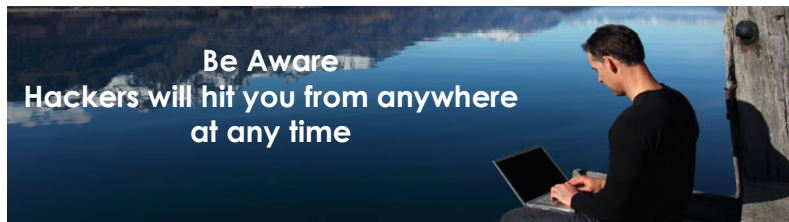   - Port Scanning Countermeasures

**Be Aware
Hackers will hit you from anywhere
at any time**

BTCS   *BTCS*
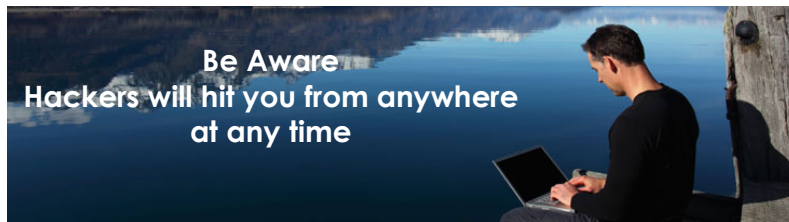
Outline: Certtified Ethical Hacker (CEH) version 8

- 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
  - Vulnerability Scanning Tool: GAFI LanGuard
  - Vulnerability Scanning Tool: SAINT
  - Network Vulnerability Scanners
- Draw Network Diagrams
  - Drawing Network Diagrams
  - Network Discovery Tool: LANsurveyor
  - Network Discovery Tool: OpManager
  - Network Discovery Tool: NetworkView
  - Network Discovery Tool: The Dude
  - Network Discovery and Mapping Tools
- Prepare Proxies
  - Proxy Servers
  - Why Attackers Use Proxy Servers?
  - Use of Proxies for Attack
  - Proxy Chaining
  - Proxy Tool: Proxy Workbench
  - Proxy Tool: Proxifier
  - Proxy Tool: Proxy Switcher
  - Proxy Tool: SocksChain
  - Proxy Tool: TOR (The Onion Routing)
  - Proxy Tools
  - Free Proxy Servers
  - HTTP Tunneling Techniques
  - Why do I Need HTTP Tunneling
  - HTTP Tunneling Tool: Super Network Tunnel
  - HTTP Tunneling Tool: HTTP-Tunnel
  - SSH Tunneling
  - SSH Tunneling Tool: Bitvise
  - Anonymizers
  - Case: Bloggers Write Text Backwards to Bypass Web Filters in China
  - Censorship Circumvention Tool: Psiphon
  - Censorship Circumvention Tool: Your-Freedom
  - How to Check if Your Website is Blocked in China or Not
  - G-Zapper
  - Anonymizers
  - Spoofing IP Address

- IP Spoofing Detection Techniques: Direct TTL Probes
- IP Spoofing Detection Techniques: IP Identification Number
- **H** IP Spoofing Detection Techniques: 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
  - NetBIOS Enumeration Tool: SuperScan
  - NetBIOS Enumeration Tool: Hyena
  - NetBIOS Enumeration Tool: Winfingerprint
  - NetBIOS Enumeration Tool: NetBIOS Enumerator
  - Enumerating User Accounts
  - Enumerate Systems Using Default Passwords
- SNMP Enumeration
  - SNMP (Simple Network Management Protocol) Enumeration
  - Working of SNMP
  - Management Information Base (MIB)
  - SNMP Enumeration Tool: OpUtils
  - SNMP Enumeration Tool: SolarWind's IP Network Browser
  - SNMP Enumeration Tools
- UNIX/Linux Enumeration
  - UNIX/Linux Enumeration Commands
  - Linux Enumeration Tool: Enum4linux
  - LDAP Enumeration
  - LDAP Enumeration Tool: Softerra LDAP Administrator
  - LDAP Enumeration Tools
- NTP Enumeration
  - NTP Enumeration
  - NTP Enumeration Commands
- SMTP Enumeration
  - SMTP Enumeration
  - SMTP Enumeration Tool: NetScanTools Pro
- DNS Enumeration
  - DNS Zone Transfer Enumeration Using NSLookup
- Enumeration Countermeasures
- SMB Enumeration Countermeasures
- Enumeration Pen Testing
- LDAP Enumeration

BTCS   **BTCS**

Be Aware
Hackers will hit you from anywhere
at any time

Outline: Certtified Ethical Hacker (CEH) version 8

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
    - Password Complexity
    - Password Cracking Techniques
    - Types of Password Attacks
    - Passive Online Attack: Wire Sniffing
    - Passive Online Attack: Eavesdropping
    - Passive Online Attacks: Man-in-the-Middle and Replay Attack
    - Active Online Attack: Password Guessing
    - Active Online Attack: Trojan/Spyware/Keylogger
    - Active Online Attack: Hash Injection Attack
    - Offline Attack: Rainbow Attacks
    - Tools to Create Rainbow Tables: Winrtgen and rtgen
    - 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
    - Stealing Passwords Using Keyloggers
    - 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
    - CEH System Hacking Steps

  - Escalating Privileges
    - Privilege Escalation
    - Privilege Escalation Tool: Active@ Password Changer
    - Privilege Escalation Tools
    - How to Defend Against Privilege Escalation

  - Executing Applications
    - Executing Applications: RemoteExec
    - Executing Applications: PDQ Deploy
    - Executing Applications: DameWare NT Utilities
  - Keylogger
    - Types of Keystroke Loggers
    - Methodology of Attacker in Using Remote Keylogger
    - Acoustic/CAM Keylogger
    - Keyloggers
    - Keylogger: Spytech SpyAgent
    - Keylogger: All In One Keylogger
    - Keyloggers for Windows
    - Keylogger for Mac: Amac Keylogger for Mac
    - Keyloggers for MAC
    - Hardware Keyloggers
    - Spyware
    - What Does the Spyware Do?
    - Types of Spywares
    - Desktop Spyware
    - Desktop Spyware: Activity Monitor
    - Desktop Spyware
    - Email and Internet Spyware
    - Email and Internet Spyware: Power Spy
    - Internet and Email Spyware
    - Child Monitoring Spyware
    - Child Monitoring Spyware: Net Nanny Home Suite
    - Child Monitoring Spyware
    - Screen Capturing Spyware
    - Screen Capturing Spyware: SoftActivity TS Monitor
    - Screen Capturing Spyware
  - USB Spyware
    - USB Spyware: USBSpy
    - USB Spyware
    - Audio Spyware
    - Audio Spyware: Spy Voice Recorder and Sound Snooper
    - Video Spyware
    - Video Spyware: WebCam Recorder
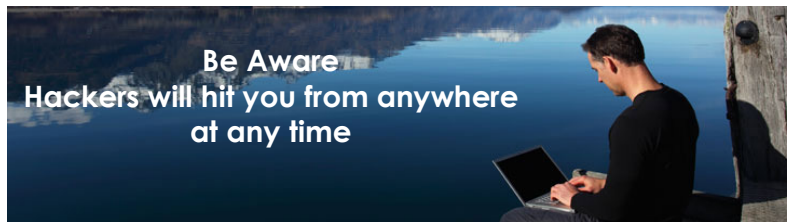   - Video Spyware

BTCS   Be Aware
Hackers will hit you from anywhere
at any time   **BTCS**
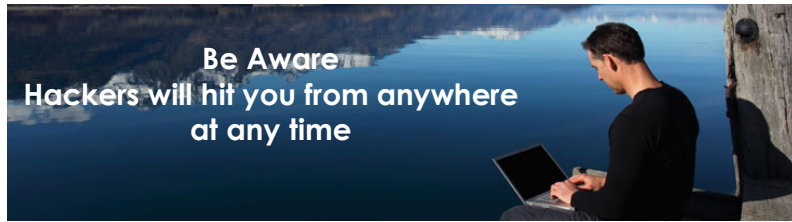
Outline: Certtified Ethical Hacker (CEH) version 8

- Print Spyware
- Print Spyware: Printer Activity Monitor
- Print Spyware
  - o Hiding Files
    - Rootkits
    - Types of Rootkits
    - How Rootkit Works
    - Rootkit: Fu
    - Rootkit: KBeast
    - Rootkit: Hacker Defender HxDef Rootkit
    - Detecting Rootkits
    - Steps for Detecting Rootkits
    - How to Defend against Rootkits
    - Anti-Rootkit: Stinger
    - Anti-Rootkit: 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?
    - Application of Steganography
    - Classification of Steganography
    - Technical Steganography
    - Linguistic Steganography
    - Steganography Techniques
    - How Steganography Works
    - Types of Steganography
    - 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
    - Video Steganography Tools
    - Audio Steganography
    - Audio Steganography Methods
    - Audio Steganography: DeepSound
    - Audio Steganography Tools
    - Folder Steganography: Invisible Secrets 4
    - Folder Steganography Tools
    - Spam/Email Steganography: Spam Mimic
    - Natural Text Steganography: Sams Big G Play Maker

- Issues in Information Hiding
- 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
  - o Covering Tracks
    - Why Cover Tracks?
    - Covering Tracks
    - Ways to Clear Online Tracks
    - Disabling Auditing: Auditpol
    - Covering Tracks Tool: CCleaner
    - Covering Tracks Tool: MRU-Blaster
    - Track Covering Tools
  - o Penetration Testing
    - Password Cracking
    - Privilege Escalation
    - Executing Applications
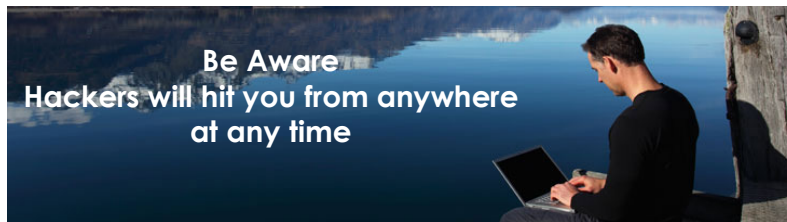   - Hiding Files
    - Covering Tracks

Module 06: Trojans and Backdoors
- Trojan Concepts
  - o What is a Trojan?
  - o Communication Paths: Overt and Covert Channels
  - o Purpose of Trojans
  - o What Do Trojan Creators Look For
  - o Indications of a Trojan Attack
  - o Common Ports used by Trojans
- Trojan Infection
  - o How to Infect Systems Using a Trojan
  - o Wrappers
  - o Wrapper Covert Programs
  - o Different Ways a Trojan can Get into a System
  - o How to Deploy a Trojan
  - o Evading Anti-Virus Techniques
- Types of Trojans
  - o Command Shell Trojans
  - o Command Shell Trojan: Netcat
  - o GUI Trojan: MoSucker
  - o GUI Trojan: Jumper and Biodox
  - o Document Trojans
  - o E-mail Trojans
  - o E-mail Trojans: RemoteByMail
  - o Defacement Trojans
  - o Defacement Trojans: Restorator

Be Aware
Hackers will hit you from anywhere
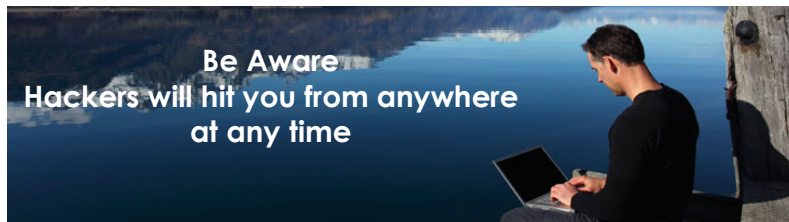**at any time**

BTCS

BTCS

Outline: Certtified Ethical Hacker (CEH) version 8

- o Botnet Trojans
- o Botnet Trojan: Illusion Bot and NetBot Attacker
- o Proxy Server Trojans
- o Proxy Server Trojan: W3bPrOxy Tr0j4nCr34t0r (Funny Name)
- o FTP Trojans
- o VNC Trojans
- o VNC Trojans: WinVNC and VNC Stealer
- o HTTP/HTTPS Trojans
- o HTTP Trojan: HTTP RAT
- o Shttpd Trojan - HTTPS (SSL)
- o ICMP Tunneling
- o Remote Access Trojans
- o Remote Access Trojan: RAT DarkComet and Apocalypse
- o Covert Channel Trojan: CCTT
- o E-banking Trojans
- o Banking Trojan Analysis
- o E-banking Trojan: ZeuS and SpyEye
- o Destructive Trojans: M4sT3r Trojan
- o Notification Trojans
- o Credit Card Trojans
- o Data Hiding Trojans (Encrypted Trojans)
- o OS X Trojan: Crisis
- o MAC OS X Trojan: DNSChanger
- o Mac OS X Trojan: Hell Raiser
- o Trojan Analysis: Flame
- o Flame C&C Server Analysis
- o Trojan Analysis: SpyEye
- o Trojan Analysis: ZeroAccess
- o Trojan Analysis: Duqu
- o Trojan Analysis: Duqu Framework
- o Trojan Analysis: Event Driven Framework
- Trojan Detection
  - o How to Detect Trojans
  - o Scanning for Suspicious Ports
  - o Port Monitoring Tools: TCPView and CurrPorts
  - o Scanning for Suspicious Processes
  - o Port Monitoring Tools: TCPView and CurrPorts
  - o Scanning for Suspicious Processes
  - o Process Monitoring Tool: What's Running
  - o Process Monitoring Tools
  - o Scanning for Suspicious Registry Entries
  - o Registry Entry Monitoring Tool: PC Tools Registry Mechanic
  - o Registry Entry Monitoring Tools
  - o Scanning for Suspicious Device Drivers
  - o Device Drivers Monitoring Tool: DriverView
  - o Device Drivers Monitoring Tools

- o Scanning for Suspicious Windows Services
- o Windows Services Monitoring Tool: Windows Service Manager (SrvMan)
- o Windows Services Monitoring Tools
- o Scanning for Suspicious Startup Programs
- o Windows8 Startup Registry Entries
- o Startup Programs Monitoring Tool: Starter
- o Startup Programs Monitoring Tool: Security AutoRun
- o Startup Programs Monitoring Tools
- o Scanning for Suspicious Files and Folders
- o Files and Folder Integrity Checker: FastSum and WinMD5
- o Files and Folder Integrity Checker
- o Scanning for Suspicious Network Activities
- o Detecting Trojans and Worms with Capsa Network Analyzer
- Countermeasures
  - o Trojan Countermeasures
  - o Backdoor Countermeasures
  - o Trojan Horse Construction Kit
- Anti-Trojan Software
  - o Anti-Trojan Software: TrojanHunter
  - o Anti-Trojan Software: Emsisoft Anti-Malware
  - o Anti-Trojan Softwares
- Pen Testing for Trojans and Backdoors

Module 07: Viruses and Worms
- Virus and Worms Concepts
  - o Introduction to Viruses
  - o Virus and Worm Statistics
  - o Stages of Virus Life
  - o Working of Viruses: Infection Phase
  - o Working of Viruses: Attack Phase
  - o Why Do People Create Computer Viruses
  - o Indications of Virus Attack
  - o How does a Computer Get Infected by Viruses
  - o Common Techniques Used to Distribute Malware on the Web
  - o Virus Hoaxes and Fake Antiviruses
  - o Virus Analysis: DNSChanger
- Types of Viruses
  - o System or Boot Sector Viruses
  - o o File and Multipartite Viruses
  - o o Macro Viruses
  - o Cluster Viruses
  - o Stealth/Tunneling Viruses
  - o o Encryption Viruses
  - o o Polymorphic Code
  - o o Metamorphic Viruses
  - o File Overwriting or Cavity Viruses
  - o Sparse Infector Viruses

Be Aware
Hackers will hit you from anywhere
at any time

BTCS   **B**TCS

Outline: Certtified Ethical Hacker (CEH) version 8

- 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 and DELmE's Batch Virus Maker

- Computer Worms
  - How Is a Worm Different from a Virus?
  - Worm Analysis: Stuxnet
  - Worm Maker: Internet Worm Maker Thing

- Malware Analysis
  - What is Sheep Dip Computer?
  - Anti-Virus Sensors Systems
  - Malware Analysis Procedure: Preparing Testbed
  - Malware Analysis Procedure
  - Virus Analysis Tool: IDA Pro
  - Online Malware Testing: VirusTotal
  - Online Malware Analysis Services

- Counter-measures
  - Virus Detection Methods
  - Virus and Worms Countermeasures
  - Companion Antivirus: Immunet
  - Anti-virus Tools

- Penetration Testing for Virus

Module 08: Sniffers
- Sniffing Concepts
  - Wiretapping
  - Lawful Interception
  - Packet Sniffing
  - Sniffing Threats
  - How a Sniffer Works
  - Types of Sniffing Attacks
  - Types of Sniffing: Passive Sniffing
  - Types of Sniffing: Active Sniffing
  - Protocols Vulnerable to Sniffing
  - Tie to Data Link Layer in OSI Model
  - IPv6 Addresses
  - IPv4 and IPv6 Header Comparison
  - Hardware Protocol Analyzers
  - SPAN Port

- MAC Attacks
  - 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
- 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 Techniques
  - ARP Spoofing Attack
  - How Does ARP Spoofing Work
  - Threats of ARP Poisoning
  - ARP Poisoning Tool: Cain & Abel
  - ARP Poisoning Tool: WinArpAttacker
  - ARP Poisoning Tool: Ufasoft Snif
  - How to Defend Against ARP Poisoning
  - Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches
  - ARP Spoofing Detection: XArp

- Spoofing Attack
  - Spoofing Attack Threats
  - 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: Cascade Pilot
  - Sniffing Tool: Tcpdump/Windump
  - Packet Sniffing Tool: Capsa Network Analyzer
  - Network Packet Analyzer: OmniPeek Network Analyzer
  - Network Packet Analyzer: Observer
  - Network Packet Analyzer: Sniff-O-Matic
  - Network Packet Analyzer: JitBit Network Sniffer

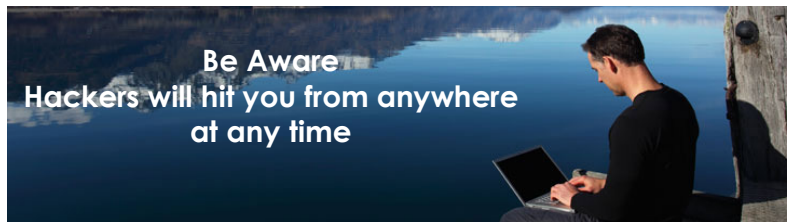## Outline: Certtified Ethical Hacker (CEH) version 8

- o Chat Message Sniffer: MSN Sniffer 2
- o TCP/IP Packet Crafter: Colasoft Packet Builder
- o Additional Sniffing Tools
- o How an Attacker Hacks the Network Using Sniffers
- ▪ Counter measures
  - o How to Defend Against Sniffing
  - o How to Detect Sniffing
  - o Sniffer Detection Technique: Ping Method
  - o Sniffer Detection Technique: ARP Method
  - o Sniffer Detection Technique: DNS Method
  - o Promiscuous Detection Tool: PromqryUI
- ▪ Sniffing Pen Testing

Module 09: Social Engineering
- ▪ Social Engineering Concepts
  - o What is Social Engineering?
  - o Behaviors Vulnerable to Attacks
  - o Factors that Make Companies Vulnerable to Attacks
  - o Why Is Social Engineering Effective?
  - o Warning Signs of an Attack
  - o Phases in a Social Engineering Attack
  - o Impact on the Organization
  - o "Rebecca" and "Jessica"
  - o Common Targets of Social Engineering
  - o Common Targets of Social Engineering: Office Workers
- ▪ Social Engineering Techniques
  - o Types of Social Engineering
  - o Human-based Social Engineering
  - o Technical Support Example
  - o Authority Support Example
  - o Human-based Social Engineering: Eavesdropping and Shoulder Surfing
  - o Human-based Social Engineering: Dumpster Diving
  - o Human-based Social Engineering
  - o Watch these Movies
  - o Watch this Movie
  - o Computer-based Social Engineering
  - o Computer-based Social Engineering: Pop-Ups
  - o Computer-based Social Engineering: Phishing
  - o Computer-based Social Engineering: Spear Phishing
  - o Mobile-based Social Engineering: Publishing Malicious Apps
  - o Mobile-based Social Engineering: Repackaging Legitimate Apps

- o Mobile-based Social Engineering: Fake Security Applications
- o Mobile-based Social Engineering: Using SMS
- o Insider Attack
- o Disgruntled Employee
- o Preventing Insider Threats
- o Common Social Engineering Targets and Defense Strategies
- ▪ Imperso-nation on Social Networking Sites
  - o Social Engineering Through Impersonation on Social Networking Sites
  - o Social Engineering on Facebook
  - o Social Engineering Example: LinkedIn Profile
  - o Social Engineering on Twitter
  - o Risks of Social Networking to Corporate Networks
- ▪ Identity Theft
  - o Identity Theft Statistics 2011
  - o Identify Theft
  - o How to Steal an Identity
    - ▪ STEP 1
    - ▪ STEP 2
    - ▪ Comparison
    - ▪ STEP 3
  - o Real Steven Gets Huge Credit Card Statement
  - o Identity Theft - Serious Problem
- ▪ Social Engineering Countermeasures
  - o How to Detect Phishing Emails
  - o Anti-Phishing Toolbar: Netcraft
  - o Anti-Phishing Toolbar: PhishTank
  - o Identity Theft Countermeasures
- ▪ Social Engineering Pen Testing
  - o Social Engineering Pen Testing: Using Emails
  - o Social Engineering Pen Testing: Using Phone
  - o Social Engineering Pen Testing: In Person
  - o Social Engineering Pen Testing: Social Engineering Toolkit (SET)

Module 10: Denial of Service
- ▪ DoS/DDoS Concepts
  - o What is a Denial of Service Attack?
  - o What Are Distributed Denial of Service Attacks?
  - o How Distributed Denial of Service Attacks Work
  - o Symptoms of a DoS Attack
  - o Cyber Criminals
  - o Organized Cyber Crime: Organizational Chart

BTCS

Be Aware
Hackers will hit you from anywhere
at any time

BTCS

Outline: Certtified Ethical Hacker (CEH) version 8

- 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
    - Botnet Trojans: Illusion Bot and NetBot Attacker
- DDoS Case Study
    - DDoS Attack
    - DDoS Attack Tool: LOIC
    - Hackers Advertise Links to Download Botnet
- DoS Attack Tools
- Counter-measures
    - 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 Appliances
- DoS/DDoS Protection Tools
    - DoS/DDoS Protection Tool: D-Guard Anti-DDoS Firewall
    - DoS/DDoS Protection Tools

- Denial-of-Service (DoS) Attack Penetration Testing
    - Botnet Trojans: Illusion Bot and NetBot Attacker
- DDoS Case Study
    - DDoS Attack
    - DDoS Attack Tool: LOIC
    - Hackers Advertise Links to Download Botnet
- DoS Attack Tools
- Counter-measures
    - 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 Appliances
- DoS/DDoS Protection Tools
    - DoS/DDoS Protection Tool: D-Guard Anti-DDoS Firewall
    - DoS/DDoS Protection Tools
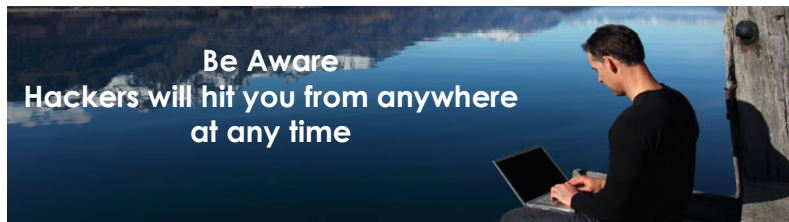- Denial-of-Service (DoS) Attack Penetration Testing

Module 11: Session Hijacking
- Session Hijacking Concepts
    - What is Session Hijacking?
    - Dangers Posed by Hijacking
    - Why Session Hijacking is Successful?
    - Key Session Hijacking Techniques
    - Brute Forcing Attack
    - Spoofing vs. Hijacking
    - Session Hijacking Process
    - Packet Analysis of a Local Session Hijack
    - Types of Session Hijacking
    - Session Hijacking in OSI Model
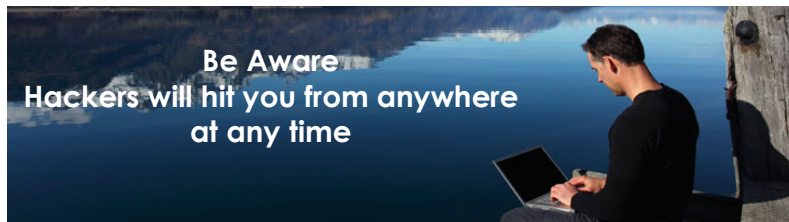   - Application Level Session Hijacking

Be Aware
Hackers will hit you from anywhere
at any time

BTCS   *BTCS*
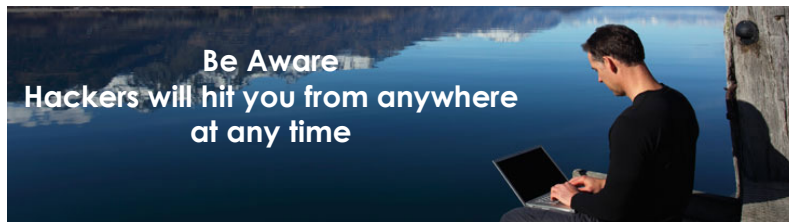
Outline: Certtified Ethical Hacker (CEH) version 8

- o Session Sniffing
- o Predictable Session Token
- o How to Predict a Session Token
- o Man-in-the-Middle Attack
- o Man-in-the-Browser Attack
- o Steps to Perform Man-in-the-Browser Attack
- o Client-side Attacks
- o Cross-site Script Attack
- o Session Fixation
- o Session Fixation Attack
- Network-level Session Hijacking
  - o The 3-Way Handshake
  - o Sequence Numbers
  - o Sequence Numbers Prediction
  - o TCP/IP Hijacking
  - o IP Spoofing: Source Routed Packets
  - o RST Hijacking
  - o Blind Hijacking
  - o Man-in-the-Middle Attack Using Packet Sniffer
  - o UDP Hijacking
- Session Hijacking Tools
  - o Session Hijacking Tool: Zaproxy
  - o Session Hijacking Tool: Burp Suite
  - o Session Hijacking Tool: JHijack
  - o Session Hijacking Tools
- Counter-measures
  - o Protecting against Session Hijacking
  - o Methods to Prevent Session Hijacking: To be Followed by Web Developers
  - o Methods to Prevent Session Hijacking: To be Followed by Web Users
  - o o IPSec
  - o o Modes of IPsec
  - o IPsec Architecture
  - o IPsec Authentication and Confidentiality
  - o Components of IPSec
  - o IPsec Implementation
- Session Hijacking Pen Testing

Module 12: Hacking Webservers
- Webserver Concepts
  - o Webserver Market Shares
  - o Open Source Webserver Architecture
  - o IIS Webserver Architecture
  - o Website Defacement
  - o Why Web Servers are compromised?
  - o Impact of Webserver Attacks
- Webserver Attacks
  - o Webserver Misconfiguration
  - o Webserver Misconfiguration Example
  - o Directory Traversal Attacks

- o HTTP Response Splitting Attack
- o Web Cache Poisoning Attack
- o HTTP Response Hijacking
- o SSH Bruteforce Attack
- o Man-in-the-Middle Attack
- o Webserver Password Cracking
- o Webserver Password Cracking Techniques
- o Web Application Attacks
- Attack Methodology
  - o Webserver Attack Methodology
  - o Webserver Attack Methodology: Information Gathering
  - o Webserver Attack Methodology: Webserver Footprinting
  - o Webserver Footprinting Tools
  - o Webserver Attack Methodology: Mirroring a Website
  - o Webserver Attack Methodology: Vulnerability Scanning
  - o Webserver Attack Methodology: Session Hijacking
  - o Webserver Attack Methodology: Hacking Web Passwords
- Webserver Attack Tools
  - o Webserver Attack Tools: Metasploit
  - o Metasploit Architecture
  - o Metasploit Exploit Module
  - o Metasploit Payload Module
  - o Metasploit Auxiliary Module
  - o Metasploit NOPS Module
  - o Webserver Attack Tools: Wfetch
  - o Web Password Cracking Tool: Brutus
  - o Web Password Cracking Tool: THC-Hydra
  - o Web Password Cracking Tool: Internet Password Recovery Toolbox
- Counter-measures
  - o Countermeasures: Patches and Updates
  - o Countermeasures: Protocols
  - o Countermeasures: Accounts
  - o Countermeasures: Files and Directories
  - o How to Defend Against Web Server Attacks
  - o How to Defend against HTTP Response Splitting and Web Cache Poisoning
- Patch Management
  - o Patches and Hotfixes
  - o What Is Patch Management?
  - o Identifying Appropriate Sources for Updates and Patches
  - o Installation of a Patch
  - o Implementation and Verification of a Security Patch or Upgrade
  - o Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)

Be Aware
Hackers will hit you from anywhere
at any time

BTCS

BTCS

Outline: Certtified Ethical Hacker (CEH) version 8

- o Patch Management Tools
- ▪ Webserver Security Tools
  - o Web Application Security Scanner: Syhunt Dynamic
  - o Web Application Security Scanner: N-Stalker Web Application Security Scanner
  - o Web Server Security Scanner: Wikto
  - o Web Server Security Scanner: Acunetix Web Vulnerability Scanner
  - o Web Server Malware Infection Monitoring Tool: HackAlert
  - o Web Server Malware Infection Monitoring Tool: QualysGuard Malware Detection
  - o Webserver Security Tools
- ▪ Webserver Pen Testing
  - o Web Server Pen Testing Tool: CORE Impact® Pro
  - o Web Server Pen Testing Tool: Immunity CANVAS
  - o Web Server Pen Testing
  - o Web Server Penetration Testing

Module 13: Hacking Web Applications
- ▪ Web App Concepts
  - o Web Application Security Statistics
  - o Introduction to Web Applications
  - o Web Application Components
  - o How Web Applications Work?
  - o Web Application Architecture
  - o Web 2.0 Applications
  - o Vulnerability Stack
  - o Web Attack Vectors
- ▪ Web App Threats
  - o Web Application Threats - 1
  - o Web Application Threats - 2
  - o Invalidated Input
  - o Parameter/Form Tampering
  - o Directory Traversal
  - o Security Misconfiguration
  - o Injection Flaws
  - o SQL Injection Attacks
  - o Command Injection Attacks
  - o Command Injection Attacks
  - o Command Injection Example
  - o File Injection Attack
  - o What is LDAP Injection?
  - o How LDAP Injection Works?
  - o Hidden Field Manipulation Attack
  - o Cross-Site Scripting (XSS) Attacks

- o How XSS Attacks Work?
- o Cross-Site Scripting Attack Scenario: Attack via Email
- o XSS Example: Attack via Email
- o XSS Example: Stealing Users' Cookies
- o XSS Example: Sending an Unauthorized Request
- o XSS Attack in Blog Posting
- o XSS Attack in Comment Field
- o XSS Cheat Sheet
- o Cross-Site Request Forgery (CSRF) Attack
- o How CSRF Attacks Work?
- o Web Application Denial-of-Service (DoS) Attack
- o Denial of Service (DoS) Examples
- o Buffer Overflow Attacks
- o Cookie/Session Poisoning
- o How Cookie Poisoning Works?
- o Session Fixation Attack
- o Insufficient Transport Layer Protection
- o Improper Error Handling
- o Insecure Cryptographic Storage
- o Broken Authentication and Session Management
- o Invalidated Redirects and Forwards
- o Web Services Architecture
- o Web Services Attack
- o Web Services Footprinting Attack
- o Web Services XML Poisoning
- ▪ Web App Hacking Methodology
  - o Footprint Web Infrastructure
    - ▪ Footprint Web Infrastructure: Server Discovery
    - ▪ Footprint Web Infrastructure: Service Discovery
    - ▪ Footprint Web Infrastructure: Server Identification/Banner Grabbing
    - ▪ Footprint Web Infrastructure: Hidden Content Discovery
    - ▪ Web Spidering Using Burp Suite
    - ▪ Web Spidering Using Mozenda Web Agent Builder
  - o Attack Web Servers
    - ▪ Hacking Web Servers
    - ▪ Web Server Hacking Tool: WebInspect
  - o Analyze Web Applications
    - ▪ Analyze Web Applications: Identify Entry Points for User Input
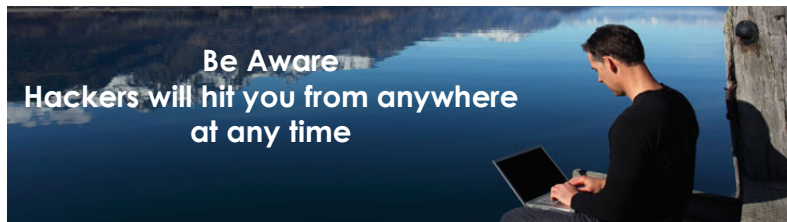   - ▪ Analyze Web Applications: Identify Server-Side Technologies

Be Aware
Hackers will hit you from anywhere
at any time

BTCS   BTCS

Outline: Certtified Ethical Hacker (CEH) version 8

- o Attack Authentication Mechanism
    - ▪ Password Attacks: Password Guessing
    - ▪ Password Attacks: Brute-forcing
    - ▪ Session Attacks: Session ID Prediction/ Brute-forcing
    - ▪ Cookie Exploitation: Cookie Poisoning
- o Authorization Attack Schemes
    - ▪ Authorization Attack
    - ▪ HTTP Request Tampering
    - ▪ Authorization Attack: Cookie Parameter Tampering
- o Attack Session Management Mechanism
    - ▪ Session Management Attack
    - ▪ Attacking Session Token Generation Mechanism
    - ▪ Attacking Session Tokens Handling Mechanism: Session Token Sniffing
- o Perform Injection Attacks
    - ▪ Injection Attacks
- o Attack Data Connectivity
    - ▪ Connection String Injection
    - ▪ Connection String Parameter Pollution (CSPP) Attacks
    - ▪ Connection Pool DoS
- o Attack Web App Client
- o 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 Tools
    - o Web Application Hacking Tool: Burp Suite Professional
    - o Web Application Hacking Tools: CookieDigger
    - o Web Application Hacking Tools: WebScarab
    - o Web Application Hacking Tools
- ▪ Countermeasures
    - o Encoding Schemes
    - o How to Defend Against SQL Injection Attacks?
    - o How to Defend Against Command Injection Flaws?
    - o How to Defend Against XSS Attacks?
    - o How to Defend Against DoS Attack?
    - o How to Defend Against Web Services

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

Module 14: SQL Injection
- ▪ SQL Injection Concepts
    - o SQL Injection
    - o Scenario
    - o SQL Injection is the Most Prevalent Vulnerability in 2012
    - o SQL Injection Threats
    - o What is SQL Injection?
    - o SQL Injection Attacks
    - o How Web Applications Work?
    - o Server Side Technologies
    - o HTTP Post Request
    - o Example 1: Normal SQL Query
    - o Example 1: SQL Injection Query
    - o Example 1: Code Analysis
    - o Example 2: BadProductList.aspx
    - o Example 2: Attack Analysis
    - o Example 3: Updating Table
    - o Example 4: Adding New Records

Outline: Certtified Ethical Hacker (CEH) version 8

- o Example 6: Deleting a Table
- Testing for SQL Injection
  - o SQL Injection Detection
  - o SQL Injection Error Messages
  - o SQL Injection Attack Characters
  - o Additional Methods to Detect SQL Injection
  - o SQL Injection Black Box Pen Testing
  - o Testing for SQL Injection
- Types of SQL Injection
  - o Simple SQL Injection Attack
  - o Union SQL Injection Example
  - o SQL Injection Error Based
- Blind SQL Injection
  - o What is Blind SQL Injection?
  - o No Error Messages Returned
  - o Blind SQL Injection: WAITFOR DELAY YES or NO Response
  - o Blind SQL Injection – Exploitation (MySQL)
  - o Blind SQL Injection - Extract Database User
  - o Blind SQL Injection - Extract Database Name
  - o Blind SQL Injection - Extract Column Name
  - o Blind SQL Injection - Extract Data from ROWS
- SQL Injection Methodology
- Advanced SQL Injection
  - o Information Gathering
  - o Extracting Information through Error Messages
  - o Understanding SQL Query
  - o Bypass Website Logins Using SQL Injection
  - o Database, Table, and Column Enumeration
  - o Advanced Enumeration
  - o Features of Different DBMSs
  - o Creating Database Accounts
  - o Password Grabbing
  - o Grabbing SQL Server Hashes
  - o Extracting SQL Hashes (In a Single Statement)
  - o Transfer Database to Attacker's Machine
  - o Interacting with the Operating System
  - o Interacting with the FileSystem
  - o Network Reconnaissance Using SQL Injection
  - o Network Reconnaissance Full Query

- o Example 5: Identifying the Table Name
- SQL Injection Tools
  - o SQL Injection Tools: BSQLHacker
  - o SQL Injection Tools: Marathon Tool
  - o SQL Injection Tools: SQL Power Injector
  - o SQL Injection Tools: Havij
  - o SQL Injection Tools
- Evasion Techniques
  - o Evading IDS
  - o Types of Signature Evasion Techniques
  - o Evasion Technique: Sophisticated Matches
  - o Evasion Technique: Hex Encoding
  - o Evasion Technique: Manipulating White Spaces
  - o Evasion Technique: In-line Comment
  - o Evasion Technique: Char Encoding
  - o Evasion Technique: String Concatenation
  - o Evasion Technique: Obfuscated Codes
- Counter-measures
  - o How to Defend Against SQL Injection Attacks?
  - o How to Defend Against SQL Injection Attacks: Use Type-Safe SQL Parameters
  - o How to Defend Against SQL Injection Attacks
  - o SQL Injection Detection Tool: Microsoft Source Code Analyzer
  - o SQL Injection Detection Tool: Microsoft UrlScan Filter
  - o SQL Injection Detection Tool: dotDefender
  - o SQL Injection Detection Tool: IBM Security AppScan
  - o SQL Injection Detection Tool: WebCruiser
  - o Snort Rule to Detect SQL Injection Attacks
  - o SQL Injection Detection Tools

Module 15: Hacking Wireless Networks
- Wireless Concepts
  - o Wireless Networks
  - o 2010 vs. 2011 Wi-Fi Device Type Comparison
  - o Wi-Fi Networks at Home and Public Places
  - o Types of Wireless Networks
  - o Wireless Standards
  - o Service Set Identifier (SSID)
  - o Wi-Fi Authentication Modes
  - o Wi-Fi Authentication Process Using a Centralized Authentication Server
  - o Wireless Terminologies
  - o Wi-Fi Chalking
  - o Wi-Fi Chalking Symbols
  - o Types of Wireless Antenna
  - o Parabolic Grid Antenna

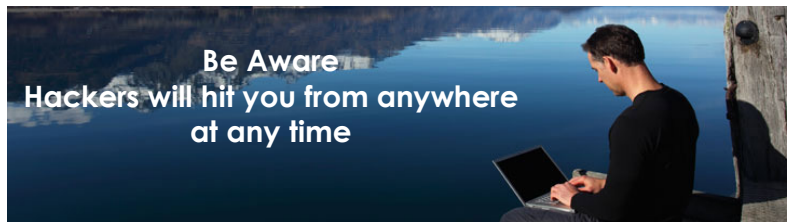## Outline: Certtified Ethical Hacker (CEH) version 8

- 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/WPA2 Encryption?
  - How to Defend Against WPA Cracking?
- Wireless Threats
  - 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
  - Wi-Fi Discovery
    - Footprint the Wireless Network
    - Attackers Scanning for Wi-Fi Networks
    - Find Wi-Fi Networks to Attack
    - 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
    - Mobile-based Wi-Fi Discovery Tool
    - Wi-Fi Discovery Tools
  - GPS Mapping
    - GPS Mapping Tool: WIGLE
    - GPS Mapping Tool: Skyhook
    - Wi-Fi Hotspot Finder: jiWire
    - Wi-Fi Hotspot Finder: WeFi
    - How to Discover Wi-Fi Network Using Wardriving?
  - Wireless Traffic Analysis

- Wireless Cards and Chipsets
- Wi-Fi USB Dongle: AirPcap
- 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
- 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
- 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
  - 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
- 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
    - Wi-Fi Packet Sniffer: Wireshark with AirPcap
    - Wi-Fi Packet Sniffer: Cascade Pilot
    - Wi-Fi Packet Sniffer: OmniPeek
    - Wi-Fi Packet Sniffer: CommView for Wi-Fi
    - What is Spectrum Analysis?
    - Wi-Fi Packet Sniffers

BTCS

BTCS

**Be Aware
Hackers will hit you from anywhere
at any time**

Outline: Certtified Ethical Hacker (CEH) version 8

- o 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)?
- o Crack Wi-Fi Encryption
  - 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
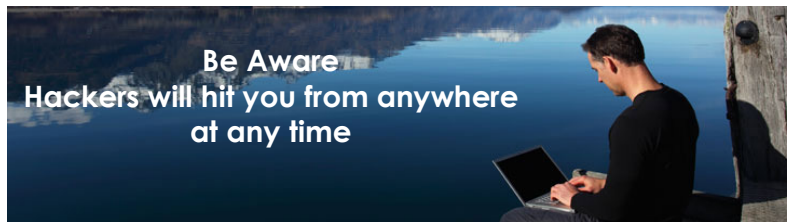 - WEP/WPA Cracking Tools

Module 16: Hacking Mobile Platforms
- Mobile Platform Attack Vectors
  - o Mobile Threat Report Q2 2012
  - o Terminology
  - o Mobile Attack Vectors
  - o Mobile Platform Vulnerabilities and Risks
  - o Security Issues Arising from App Stores
  - o Threats of Mobile Malware
  - o App Sandboxing Issues
- Hacking Android OS
  - o Android OS
  - o Android OS Architecture
  - o Android Device Administration API
  - o Android Vulnerabilities

- o Android Rooting
- o Rooting Android Phones using SuperOneClick
- o Rooting Android Phones Using Superboot
- o Android Rooting Tools
- o Session Hijacking Using DroidSheep
- o Android-based Sniffer: FaceNiff
- o Android Trojan: ZitMo (ZeuS-in-the-Mobile)
- o Android Trojan: GingerBreak
- o Android Trojan: AcnetSteal and Cawitt
- o Android Trojan: Frogonal and Gamex
- o Android Trojan: KabStamper and Mania
- o Android Trojan: PremiumSMS and SmsSpy
- o Android Trojan: DroidLive SMS and UpdtKiller
- o Android Trojan: FakeToken
- o Securing Android Devices
- o Google Apps Device Policy
- o Remote Wipe Service: Remote Wipe
- o Android Security Tool: DroidSheep Guard
- o Android Vulnerability Scanner: X-Ray
- o Android Penetration Testing Tool: Android Network Toolkit - Anti
- o Android Device Tracking Tools
- Hacking iOS
  - o Security News
  - o Apple iOS
  - o Jailbreaking iOS
  - o Types of Jailbreaking
  - o Jailbreaking Techniques
  - o App Platform for Jailbroken Devices: Cydia
  - o Jailbreaking Tools: Redsn0w and Absinthe
  - o Tethered Jailbreaking of iOS 6 Using RedSn0w
  - o Jailbreaking Tools: Sn0wbreeze and PwnageTool
  - o Jailbreaking Tools: LimeRa1n and Jailbreakme.com
  - o Jailbreaking Tools: Blackra1n and Spirit
  - o Guidelines for Securing iOS Devices
  - o iOS Device Tracking Tools
- Hacking Windows Phone OS
  - o Windows Phone 8
  - o Windows Phone 8 Architecture
  - o Secure Boot Process
  - o Windows Phone 8 Vulnerabilities
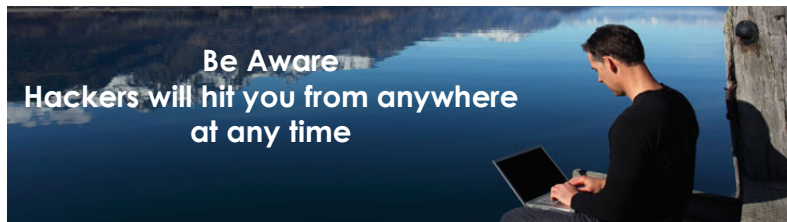 - o o Guidelines for Securing Windows OS Devices

Outline: Certtified Ethical Hacker (CEH) version 8

- o Hacking BlackBerry
- o BlackBerry Operating System
- o BlackBerry Enterprise Solution Architecture
- o Blackberry Attack Vectors
- o JAD File Exploits and Memory/ Processes Manipulations
- o Short Message Service (SMS) Exploits
- o Email Exploits
- o PIM Data Attacks and TCP/IP Connections Vulnerabilities
- o Telephony Attacks
- o Blackberry Spyware: FinSpy Mobile
- o BlackBerry Router Protocol
- o Guidelines for Securing BlackBerry Devices
- ▪ Mobile Device Management (MDM)
  - o MDM Logical Architecture
  - o MDM Solution: MaaS360 Mobile Device Management (MDM)
  - o MDM Solutions
- ▪ Mobile Security Guidelines and Tools
  - o General Guidelines for Mobile Platform Security
  - o Mobile Device Security Guidelines for Administrator
  - o Mobile Protection Tool: BullGuard Mobile Security
  - o Mobile Protection Tool: Lookout
  - o Mobile Protection Tool: WISeID
  - o Mobile Protection Tools
- ▪ Mobile Pen Testing
  - o Android Phone Pen Testing
  - o iPhone Pen Testing
  - o Windows Phone Pen Testing
  - o BlackBerry Pen Testing

Module 17: Evading IDS, Firewalls, and Honeypots
- ▪ IDS, Firewall and Honeypot Concepts
  - o Intrusion Detection Systems (IDS) and their Placement
  - o How IDS Works?
  - o Ways to Detect an Intrusion
  - o Types of Intrusion Detection Systems
  - o System Integrity Verifiers (SIV)
  - o General Indications of Intrusions
  - o General Indications of System Intrusions
  - o Firewall
  - o Firewall Architecture
  - o DeMilitarized Zone (DMZ)
  - o Types of Firewall
  - o Packet Filtering Firewall
  - o Circuit-Level Gateway Firewall
- o Application-Level Firewall
  - o Application-Level Firewall
  - o Stateful Multilayer Inspection Firewall
  - o Firewall Identification: Port Scanning
  - o Firewall Identification: Firewalking
  - o Firewall Identification: Banner Grabbing
  - o Honeypot
  - o Types of Honeypots
  - o How to Set Up a Honeypot
- ▪ IDS, Firewall and Honeypot System
  - o Intrusion Detection Tool: Snort
  - o How Snort Works
  - o Snort Rules
  - o Snort Rules : Rule Actions and IP Protocols
  - o Snort Rules : The Direction Operator and IP Addresses
  - o Snort Rules : Port Numbers
  - o Intrusion Detection Systems: Tipping Point
  - o Intrusion Detection Tools
  - o Firewall: ZoneAlarm PRO Firewall
  - o Firewalls
  - o Honeypot Tool: KFSensor
  - o Honeypot Tool: SPECTER
  - o Honeypot Tools
- ▪ Evading IDS
  - o Insertion Attack
  - o Evasion
  - o Denial-of-Service Attack (DoS)
  - o Obfuscating
  - o False Positive Generation
  - o Session Splicing
  - o Unicode Evasion Technique
  - o Fragmentation Attack
  - o Overlapping Fragments
  - o Time-To-Live Attacks
  - o Invalid RST Packets
  - o Urgency Flag
  - o Polymorphic Shellcode
  - o ASCII Shellcode
  - o Application-Layer Attacks
  - o Desynchronization - Pre Connection SYN
  - o Desynchronization - Post Connection SYN
  - o Other Types of Evasion
- ▪ Evading Firewalls
  - o IP Address Spoofing
  - o Source Routing
  - o Tiny Fragments
  - o Bypass Blocked Sites Using IP Address in Place of URL
  - o Bypass Blocked Sites Using Anonymous Website Surfing Sites
  - o Bypass a Firewall using Proxy Server

BUSINESS
TRAINING, CONSULTING & SOLUTIONS
Empowering People & Business
Page 18 of 20

BTCS

Be Aware
Hackers will hit you from anywhere
at any time

BTCS

Outline: Certtified Ethical Hacker (CEH) version 8

- o Bypassing Firewall through ICMP Tunneling Method
- o Malicious Code Signing
- o Types of Honeypots
- o How to Set Up a Honeypot?
- o Bypassing Firewall through ACK Tunneling Method
- o Bypassing Firewall through HTTP Tunneling Method
- o Bypassing Firewall through External Systems
- o o Bypassing Firewall through MITM Attack
- ▪ Detecting Honeypots
  - o Detecting Honeypots
  - o Honeypot Detecting Tool: Send-Safe Honeypot Hunter
- ▪ Firewall Evading Tools
  - o Firewall Evasion Tool: Traffic IQ Professional
  - o Firewall Evasion Tool: tcp-over-dns
  - o Firewall Evasion Tools
  - o Packet Fragment Generators
- ▪ Countermeasures
- ▪ Penetration Testing
  - o Firewall/IDS Penetration Testing
  - o Firewall Penetration Testing
  - o IDS Penetration Testing

Module 18: Buffer Overflow
- ▪ Buffer Overflow Concepts
  - o Buffer Overflows
  - o Why Are Programs and Applications Vulnerable to Buffer Overflows?
  - o Understanding Stacks
  - o Stack-Based Buffer Overflow
  - o Understanding Heap
  - o Heap-Based Buffer Overflow
  - o Stack Operations
  - o Shellcode
  - o No Operations (NOPs)
- ▪ Buffer Overflow Methodology
  - o Knowledge Required to Program Buffer Overflow Exploits
  - o Buffer Overflow Steps
  - o Attacking a Real Program
  - o Format String Problem
  - o Overflow using Format String
  - o Smashing the Stack
  - o Once the Stack is smashed...
- ▪ Buffer Overflow Examples
  - o Simple Uncontrolled Overflow

- o Simple Buffer Overflow in C: Code Analysis
- o Exploiting Semantic Comments in C (Annotations)
- o How to Mutate a Buffer Overflow Exploit?
- ▪ Buffer Overflow Detection
  - o Identifying Buffer Overflows
  - o How to Detect Buffer Overflows in a Program?
  - o Testing for Heap Overflow Conditions: heap.exe
  - o Steps for Testing for Stack Overflow in OllyDbg Debugger
  - o Testing for Stack Overflow in OllyDbg Debugger
  - o Testing for Format String Conditions using IDA Pro
  - o BoF Detection Tool: Immunity CANVAS
  - o BoF Detection Tools
- ▪ Buffer Overflow Counter-measures
  - o Defense Against Buffer Overflows
  - o Preventing BoF Attacks
  - o Programming Countermeasures
  - o Data Execution Prevention (DEP)
  - o Enhanced Mitigation Experience Toolkit (EMET)
  - o EMET System Configuration Settings
  - o EMET Application Configuration Settings
- ▪ Buffer Overflow Security Tools
  - o /GS http://microsoft.com
    o BoF Security Tool: BufferShield
  - o BoF Security Tools
- ▪ Buffer Overflow Penetration Testing

Module 19: Cryptography
- ▪ Cryptography Concepts
  - o Cryptography
  - o Types of Cryptography
  - o Government Access to Keys (GAK)
- ▪ Encryption Algorithms
  - o Ciphers
  - o Advanced Encryption Standard (AES)
  - o Data Encryption Standard (DES)
  - o RC4, RC5, RC6 Algorithms
  - o The DSA and Related Signature Schemes
  - o RSA (Rivest Shamir Adleman)
  - o Example of RSA Algorithm
  - o The RSA Signature Scheme
  - o Message Digest (One-way Hash) Functions
  - o Message Digest Function: MD5
  - o Secure Hashing Algorithm (SHA)
  - o What is SSH (Secure Shell)?

Be Aware
Hackers will hit you from anywhere
at any time

BTCS

BTCS

Outline: Certtified Ethical Hacker (CEH) version 8

- Cryptography Tools
    - MD5 Hash Calculators: HashCalc, MD5 Calculator and HashMyFiles
    - Cryptography Tool: Advanced Encryption Package
    - Cryptography Tool: BCTextEncoder
    - Cryptography Tools
- Public Key Infrastructure(PKI)
    - Public Key Infrastructure (PKI)
    - Certification Authorities
- Email Encryption
    - Digital Signature
    - SSL (Secure Sockets Layer)
    - Transport Layer Security (TLS)
- Disk Encryption
    - Disk Encryption Tool: TrueCrypt
    - Disk Encryption Tool: GiliSoft Full Disk Encryption
    - Disk Encryption Tools
- Cryptography Attacks
    - Code Breaking Methodologies
    - Brute-Force Attack
    - Meet-in-the-Middle Attack on Digital Signature Schemes
- Cryptanalysis Tools
    - Cryptanalysis Tool: CrypTool
    - Cryptanalysis Tools
    - Online MD5 Decryption Tool

Module 20: Penetration Testing
- Pen Testing Concepts
    - Security Assessments
    - Security Audit
    - Vulnerability Assessment
    - Limitations of Vulnerability Assessment
    - Introduction to Penetration Testing
    - Penetration Testing
    - Comparing Security Audit, Vulnerability Assessment, and Penetration Testing
    - What should be tested?
    - What Makes a Good Penetration Test?
    - ROI on Penetration Testing
    - Testing Points
    - Testing Locations
- Types of Pen Testing
    - 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
- Pen Testing Techniques
    - Common Penetration Testing Techniques
    - Using DNS Domain Name and IP Address Information
    - Enumerating Information about Hosts on Publicly-Available Networks
- Pen Testing Phases
    - Phases of Penetration Testing
    - Pre-Attack Phase: Define Rules of Engagement (ROE)
    - Pre-Attack Phase: Understand Customer Requirements
    - Pre-Attack Phase: Create a Checklist of the Testing Requirements
    - Pre-Attack Phase: Define the Pen-Testing Scope
    - Why Penetration Testing?
    - Pre-Attack Phase: Sign Penetration Testing Contract
    - Pre-Attack Phase: Sign Confidentiality and Non-Disclosure (NDA) Agreements
    - Pre-Attack Phase: Information Gathering
    - 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
- Pen Testing Roadmap
    - 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 Pen Testing Services
    - Outsourcing Penetration Testing Services
    - Terms of Engagement
    - Project Scope
    - Pentest Service Level Agreements
    - Penetration Testing Consultants