



CEH Version 7

Module 1: Introduction to Ethical Hacking

- Problem Definition -Why Security?
- Essential Terminologies
- Elements of Security
- The Security, Functionality and Ease of Use Triangle
- Effect on Business
- Case Study
- What does a Malicious Hacker do?
- Types of Hacker Attacks
- Hacktivism
- Hacker Classes
- Security News: Suicide Hacker
- Ethical Hacker Classes
- What do Ethical Hackers do
- Can Hacking be Ethical
- How to become an Ethical Hacker
- Skill Profile of an Ethical Hacker
- What is Vulnerability Research
- How to Conduct Ethical Hacking
- How Do They Go About It
- Approaches to Ethical Hacking
- Ethical Hacking Testing
- Ethical Hacking Deliverables
- Computer Crimes and Implications

Module 2: Footprinting and Reconnaissance

- Revisiting Reconnaissance
- Defining Footprinting
- Why is Footprinting Necessary
- Areas and Information which Attackers Seek
- Information Gathering Methodology
- Footprinting Tools
- E-Mail Spiders
- How to Create Fake Website
- Real and Fake Website
- Tool: Reamweaver
- Mirrored Fake Website
- Faking Websites using Man-in-the-Middle Phishing Kit
- Benefits to Fraudster
- Steps to Perform Footprinting

Module 3: Scanning Networks

- Scanning: Definition
- Types of Scanning
- Objectives of Scanning
- CEH Scanning Methodology
- War Dialer Technique
- Banner Grabbing
- Vulnerability Scanning
- Draw Network Diagrams of Vulnerable Hosts

- Preparing Proxies
- Scanning Countermeasures
- Tool: SentryPC

Module 4: Enumeration

- Overview of System Hacking Cycle
- What is Enumeration?
- Techniques for Enumeration
- NetBIOS Null Sessions
- PS Tools
- Simple Network Management Protocol(SNMP) Enumeration
- LDAP enumeration
- NTP enumeration
- SMTP enumeration
- Web enumeration
- Winfingerprint
- How To Enumerate Web Application Directories in IIS Using DirectoryServices
- IP Tools Scanner
- Enumerate Systems Using DefaultPassword
- Tools:
- Steps to Perform Enumeration

Module 5: System Hacking

- Part 1- Cracking Password
- Part 2-Escalating Privileges
- Part 3-Executing applications
- Part 4-Hiding files
- Part 5-Covering Tracks

Module 6: Trojans and Backdoors

- What is a Trojan?
- Indications of a Trojan Attack
- Ports Used by Trojans
- Classic Trojans
- Stealth Trojans
- Reverse Connecting Trojans
- Miscellaneous Trojans
- How to Detect Trojans?
- Anti-Trojan Software
- Evading Anti-Virus Techniques
- Sample Code for Trojan Client/Server
- Evading Anti-Trojan/Anti-Virus using Stealth Tools
- Backdoor Countermeasures
- Tripwire
- System File Verification
- MD5 Checksum.exe
- Microsoft Windows Defender
- How to Avoid a Trojan Infection

Module 7: Viruses and Worms

- Virus History
- Characteristics of Virus
- Working of Virus
- Why people create Computer Viruses
- Symptoms of a Virus-like Attack
- Virus Hoaxes
- Chain Letters
- Worms
- How is a Worm Different from a Virus
- Indications of a Virus Attack
- Virus Damage
- Stages of Virus Life
- Types of Virus
- Famous Viruses and Worms
- Latest Viruses
- Writing Virus Program
- Virus Detection Methods
- Anti-Virus Software
- Popular Anti-Virus Packages
- Virus Databases
- Snopes.com

Module 8: Sniffers

- Definition: Sniffing
- Types of Sniffing
- Protocols Vulnerable to Sniffing
- Passive Sniffing
- Active Sniffing
- Switched Port Analyzer (SPAN)
- SPAN Port
- Lawful Intercept
- Benefits of Lawful Intercept
- Network Components Used for Lawful Intercept
- Ready to Sniff?
- Tool: Network View – Scans the Network for Devices
- The Dude Sniffer
- Look@LAN
- Wireshark
- Display Filters in Wireshark
- Following the TCP Stream in Wireshark
- Pilot
- Tcpdump
- Tcpdump Commands
- Features of Sniffing Tools
- What is Address Resolution Protocol(ARP)
- ARP Spoofing Attack
- How Does ARP Spoofing Work
- ARP Poisoning
- Threats of ARP Poisoning
- MAC Flooding
- Mac Duplicating
- Mac Duplicating Attack
- Tools for ARP Spoofing
- DHCP Starvation Attack
- DNS Poisoning Techniques
- Tools for MAC Flooding
- Sniffing Tools
- Linux Sniffing Tools (dsniff package)

- Hardware Protocol Analyzers
- How to Detect Sniffing

Module 9: Social Engineering

- What is Social Engineering?
- Human Weakness
- “Rebecca” and “Jessica”
- Office Workers
- Types of Social Engineering
- Social Engineering Threats and Defenses
- Factors that make Companies Vulnerable
- Why is Social Engineering Effective
- Warning Signs of an Attack
- Tool: Netcraft Anti-Phishing Toolbar
- Behaviors Vulnerable to Attacks
- Impact on the Organization
- Countermeasures
- Policies and Procedures
- Security Policies – Checklist
- Impersonating Orkut, Facebook, MySpace
- Orkut
- Impersonating on Orkut
- MW.Orc worm
- Facebook
- Impersonating on Facebook
- MySpace
- Impersonating on MySpace
- How to Steal Identity
- Comparison
- Original
- Identity Theft
- <http://www.consumer.gov/idtheft/>

Module 10: Denial-of-Service

- Real World Scenario of DoS Attacks
- What are Denial-of-Service Attacks
- Goal of DoS
- Impact and the Modes of Attack
- Types of Attacks
- DoS Attack Classification
- Bot (Derived from the Word RoBOT)
- Botnets
- Uses of Botnets
- Types of Bots
- How Do They Infect? Analysis Of Agabot
- How Do They Infect
- Tool: Nuclear Bot
- What is DDoS Attack
- Characteristics of DDoS Attacks
- Is DDOS Unstoppable?
- Agent Handler Model
- DDoS IRC based Model
- DDoS Attack Taxonomy
- Amplification Attack
- Reflective DNS Attacks
- Reflective DNS Attacks Tool: ihateperl.pl
- DDoS Tools
- How to Conduct a DDoS Attack

- The Reflected DoS Attacks
- Reflection of the Exploit
- Countermeasures for Reflected DoS
- DDoS Countermeasures
- Taxonomy of DDoS Countermeasures
- Preventing Secondary Victims
- Detect and Neutralize Handlers
- Detect Potential Attacks
- DoSHTTP Tool
- Mitigate or Stop the Effects of DDoS Attacks
- Deflect Attacks
- Post-attack Forensics
- Packet Traceback

Module 11: Session Hijacking

- What is Session Hijacking?
- Understanding Session Hijacking
- Spoofing v Hijacking
- Steps in Session Hijacking
- Types of Session Hijacking
- Session Hijacking Levels
- Network Level Hijacking
- The 3-Way Handshake
- TCP Concepts 3-Way Handshake
- Sequence Numbers
- Sequence Number Prediction
- TCP/IP hijacking
- IP Spoofing: Source Routed Packets
- RST Hijacking
- Blind Hijacking
- Man in the Middle Attack using PacketSniffer
- UDP Hijacking
- Application Level Hijacking
- Programs that Performs Session Hacking
- Dangers Posed by Hijacking
- Protecting against Session Hijacking
- Countermeasure: IPSec

Module 12: Hacking Webservers

- How Web Servers Work
- How are Web Servers Compromised
- Web Server Defacement
- Apache Vulnerability
- Attacks against IIS
- Unicode
- Hacking Tool
- Tool: Metasploit Framework
- KARMA
- Tool: Immunity CANVAS Professional
- Tool: Core Impact
- Tool: MPack
- Tool: Neosploit
- Patch Management
- Vulnerability Scanners
- Countermeasures
- Increasing Web Server Security
- Web Server Protection Checklist

Module 13: Hacking Web Application

- Web Application
- Web application Hacking
- Anatomy of an Attack
- Web Application Threats
- Cross-Site Scripting/XSS Flaws
- SQL Injection
- Command Injection Flaws
- Cookie/Session Poisoning
- Parameter/Form Tampering
- Hidden Field at
- Buffer Overflow
- Directory Traversal/Forceful Browsing
- Cryptographic Interception
- Cookie Snooping
- Authentication Hijacking
- Log Tampering
- Error Message Interception
- Attack Obfuscation
- Platform Exploits
- DMZ Protocol Attacks
- Security Management Exploits
- TCP Fragmentation
- Hacking Tools

Module 14: SQL Injection

- SQL Injection: Introduction
- SQL Injection Tools
- Blind SQL Injection
- SQL Injection Countermeasures
- SQL Injection Blocking Tool: SQL Block
- Acunetix Web Vulnerability Scanner

Module 15: Hacking Wireless Networks

- Introduction to Wireless Networking
- Wireless Standards
- Wireless Concepts
- Wireless Devices
- WEP
- WPA
- TKIP and LEAP
- Hacking Methods
- Cracking WEP
- Rogue Access Point
- Scanning Tools
- Sniffing Tools
- Wireless Security Tools

Module 16: Evading IDS, Firewalls and Honeypots

- Introduction to Intrusion Detection System
- Terminologies
- Intrusion Detection System (IDS)
- Intrusion Prevention System
- What is a Firewall?
- Common Tool for Testing Firewall and IDS
- What is Honeypot?
- Tools to Detect Honeypots
- What to do when hacked



TRUNG TÂM ĐÀO TẠO AN NINH MẠNG FIREWALL

340A BẮC HẢI P6 QUẬN TÂN BÌNH

ĐT: (84.8) 22429682 -22426933

www.tuonglua.net- www.anninhmang.edu.vn

Module 17: Buffer Overflows

- Buffer Overflow Concepts
- Attacking a Real Program
- NOPs
- How to Mutate a Buffer Overflow Exploit
- Once the Stack is Smashed
- Examples of Buffer Overflow
- Tools
- How to Detect Buffer Overflows in a Program
- Defense Against Buffer Overflows

Module 18: Cryptography

- Public-key Cryptography
- Working of Encryption
- Digital Signature
- RSA (Rivest Shamir Adleman)
- RC4, RC5, RC6, Blowfish
- Algorithms and Security
- Brute-Force Attack
- RSA Attacks
- Message Digest Functions
- SHA (Secure Hash Algorithm)
- SSL (Secure Sockets Layer)
- What is SSH
- Government Access to Keys (GAK)
- RSA Challenge
- distributed.net
- Code Breaking: Methodologies
- Cryptography Attacks
- Disk Encryption
- Magic Lantern
- WEPCrack
- Cracking S/MIME Encryption Using Idle CPU Time
- Cryptography Tools

Module 19: Penetration Testing

- Overview of penetration testing methodologies
- Understand security assessments
- Understand vulnerability assessment and its limitation
- Understand types of penetration testing
- Understand risk management
- Outsourcing penetration testing service
- List the penetration testing steps
- Overview of the Pen-Test legal framework
- Overview of the Pen-Test deliverables
- List the automated penetration testing tools
- Best practices
- Phases of penetration testing