CyberCure Technologies Pvt. Ltd.

Leading the way in IT Securities (Training, Services and Consultancy)

Ethical Hacking and Cyber Security

Duration & Fees

Lecture with Hands on Session: 40 Hours

Fees: INR 18000/- Per Candidate

Introduction

As technology advances, organizations increasingly depend on technology and information assets have evolved into critical components of survival.

Ethical hackers are individuals who are generally hired in organizations to perform a trusted and controlled attempt to penetrate into the digital resources of the organization which includes systems, network and applications, using the same tools, thoughts and methodology adopted by malicious attackers.

The goal of ethical hackers is to help organizations being proactive and take necessary measures against malicious attacks by attacking system themselves, most importantly staying within the legal limits. This activity comes from a proven practice of trying to catch a thief by thinking like a thief.

Module Structure

This training module introduces you to Ethical Hacking and Information Security. It presents today's most critical cyber security vulnerabilities and solutions for fixing such vulnerabilities.

What Will You Learn?

Introduction to Ethical Hacking

- ✓ What is hacking?
- ✓ Definition of Hacking
- ✓ Future scope and Job Opportunities
- ✓ How to become a hacker?
- ✓ Why do we need a hacker?
- ✓ Case Studies
- ✓ Types of Hackers
  - As per Working
  - As per Knowledge
- ✓ Hacking Methodology
  - Reconnaissance
  - Scanning
  - Gaining Access
  - Maintaining Access
  - Clearing Tracks
- ✓ Indian Cyber Laws
- ✓ IT Security Compliance
- ✓ VA vs PT

- ✓ CIA TRIAD

Methodology and Concepts of Hacking

- ✓ Reconnaissance
  - Banner Grabbing(Practical)
  - Web Ripping (Practical)
  - Website at Offline Mode(Practical)
  - Foot Printing (Practical)
  - Name Space Lookup (Practical)
  - Trace Routing Techniques (Practical)
  - Whois Lookup Query (Practical)
  - Fingerprinting (Practical)
- ✓ Scanning
  - IP Scanners (Practical)
  - Port Scanners (Practical)
  - Web Scanners (Practical)
- ✓ Gaining Access
  - Attacks on Networks
  - Attacks on Web Servers
  - Attacks on Wireless Technologies
  - Attacks on Emails
  - Attacks on Bluetooth
  - Maintaining Access (Back Doors)
  - Operating System Backdoors
  - Rootkits
  - Shell Injections
  - Network Backdoors
- ✓ Clearing Tracks

Operating System Hacking & Security

- ✓ Introduction to Operating System
  - Windows Hacking
    - Introduction to Windows Security
    - Architecture
    - Attacks on Windows Login Password (Practical)
    - Introduction to Registry (Practical)
- ✓ Linux Hacking
  - Introduction to Linux
    - Cracking Linux Passwords(Practical)
- ✓ Steganography
  - Hiding Data Behind Images(Practical)
- ✓ Cryptography
  - Symmetric Cryptography(Practical)
  - Asymmetric Cryptography
- ✓ Alternate Data Streaming
  - Injecting Data inside a File(Practical)
  - Detecting ADS Files(Practical)
- ✓ Windows Server Hacking(Practical)
- ✓ Windows Server Hardening

Internet: Vulnerability & Security

- ✓ Identity Masking: Proxies
  - Introduction to proxies
  - Types of Proxies
    - Web Proxies (Practical)
    - Anonymous Proxy Servers(Practical)
    - Sock Chain Techniques (Practical)
    - HTTP Tunnelling (Practical)
  - Un-Intentional Proxies
    - Google as a Proxy Server (Practical)
- ✓ RFI Attacks (Introduction) (Practical)

- ✓ E-mails: Attacks and Security
  - What is E-Mail and its working?
    - What is email server?
    - E-Mail Forgery (Practical)
    - E-Mail Spammers
    - E-Mail Bombers (Practical)
    - Security to Anonymous Mailing (Practical)
    - Attacks on E-Mail Password (Practical)
    - Securing the E-Mail Passwords (Practical)
    - Tracing E-Mail Sender (Practical)
- ✓ Web Servers
  - OWASP TOP 10
  - XSS- Cross Site Scripting (Introduction) (Practical)
  - Directory Traversal Attack (Introduction) (Practical)
  - Website Scanners (Practical)
  - Database Servers
  - Attacks on Database Servers
    - SQL Injection (Practical)
      - Advance SQL Injection
      - Blind SQL Injection
      - URL Based SQL Injection
  - Non-Technical Attacks
    - Social Engineering (Practical)
    - Shoulder Surfing
    - Dumpster Diving
    - Counter-Measures

Network & Security

- ✓ Introduction to Networking
  - Devices and Terminologies in Networking
  - Attacks on Networks
    - Sniffing (Practical)
    - ARP Poisoning (Practical)
  - DNS Spoofing (Practical)
  - Buffer Overflow Attacks (Introduction) (Practical)
    - Metasploit Framework (Introduction)
      - Denial of Service (Introduction) (Practical)
      - Remote Code Execution (Practical)
  - Distributed Denial of Service (Introduction)
  - MAC Flooders (Practical)
  - Wireless Networks (Wi-Fi)
- ✓ Introduction to Wireless Fidelity
  - Advantages/Disadvantages of Wireless Networks
  - Wireless Encryption Keys:
  - Cracking WEP / WPA(Practical)
  - WAP
- ✓ Modes of Wireless Network Cards
  - Managed Mode (Practical)
  - Monitor Mode (Practical)
  - Ad-Hoc Mode (Practical)
- ✓ Working on Ad-Hocs
- ✓ Working on Cloud (Practical)
- ✓ VA of Cloud (Practical)
- ✓ Working on IOT Networks (Practical)
- ✓ IOT Search Engines (Practical)

Viruses & Malwares

- ✓ Trojans
  - Introduction to Trojans
  - Usage of Trojan (Practical)
  - Developing a Server File (Practical)
- ✓ Viruses
  - Introduction to Viruses
  - Batch Programming (Practical)
  - Using Batch Compilers (Practical)
  - Virus Writing (Practical)

- ✓ Introduction to other Malwares
- ✓ Keyloggers (Practical)
- ✓ Introduction to Anti-Viruses Removal of Malwares
  - Working of Anti-Virus
  - Manual Removal of Viruses and Trojans (Practical)

Mobile Hacking

- ✓ Introduction to Mobile Technology
  - VOIP – Definition and Usage
  - Introduction to SIP Lines
- ✓ Call Forgery
  - Anonymous Calling (Practical)
  - Caller ID Spoofing (Demo Only)
- ✓ SMS Forgery
- ✓ Mobile Spywares (Demo Only)

Software Reverse Engineering

- ✓ What is Reverse Engineering?
  - Disassembling the Software (Practical)
  - Debugging the Software (Practical)
- ✓ Software Cracking & Serial Key Phishing (Practical)
- ✓ Software Patch Development (Practical)

Computer Forensics & Cyber Crime Investigation

- ✓ Introduction to Computer Forensics
- ✓ Reasons for Cyber Attacks
- ✓ Computer Forensics
- ✓ Introduction to Data Storage
- ✓ Data Recovery
  - Recovering Deleted Files(Practical)

Bug Bounty Hunting and Catch the flag

- ✓ PWNLABS (Practical)
- ✓ VULNUNI(Practical)
- ✓ NODE(Practical)
- ✓ ZICO(Practical)
- ✓ Custom(Practical)

Cyber Security Compliance

- ✓ Introduction to ISO 27001:2013
- ✓ Introduction to GDPR
- ✓ Introduction to PCI-DSS