



Ethical Hacking

COURSE CURRICULUM

Course Description

- ▶ FORBIDDEN- Ethical Hacking Workshop
- ▶ Course Type: Workshop
- ▶ Total Time: 15 hours
- ▶ Security Competition: 1 hour
- ▶ Days: 2 Days

Module 1- Concepts Of Hacking

Elements of Information Security

- Information Security Supports the Mission of the Organization
- Information Security Should Be Cost-Effective
- Responsibilities and Accountability Should Be Made Explicit
- Owners Have Security Responsibilities Outside Organizations

Roles and Responsibilities

- Senior Management
- Program and Functional Managers/Application Owners
- Users

Common Threats: A Brief Overview

- Fraud and Theft
- Employee Sabotage
- Loss of Physical and Infrastructure Support
- Threats to Personal Privacy

Core Pillar Of Information Security

- Confidentiality
- Integrity
- Availability

General steps of Malicious Attack

- Footprinting
- Scanning
- Gaining Access
- Maintaining Access

Module 2- Concepts Of Virtualization

Introduction to Virtual Machines and Virtualization

- Concept of Virtualization
- Need and Advantages of Virtualization

Installation and Configuration

- Hardware and Software Requirements
- Installation and Configuration
- Performance Optimization
 - CPU & Memory Performance
 - Network Performance Optimization
 - ❑ Host to Host Networking
 - ❑ Host to LAN Networking
- Storage Performance

Module 3- Windows Hacking

Introduction to Windows Security

- Overview of Windows OS
- Windows File System
- Security Architecture in Windows
 - Local Security Authority
 - Security Account Manager
 - Security Reference Monitor

User Account Security

- Password Attacks in Windows
 - Bruteforcing, Dictionary and Rainbow Table Attacks
- Account Security Strengthening
 - Strong Password Policy
 - Additional Security: Syskey Encryption
 - User Account Control : Parental Controls
 - Restricting BIOS Setup

Services, Port and Protocol Security

- Auditing and Monitoring Network Connections
- Restricting Ports, Protocols and Services
- Windows Firewall with Advance Restrictions

Security Applications in Windows

- Auditing and Monitoring Windows Auto Startup
- Defending Windows via Windows Defender
- Policy Management with MBSA
- File and Folder Scanning with MSSE

Module 4- Attacks on Social Media

Cyber Social Media Threats

- Social Engineering
 - Human Based Social Engineering
 - Computer Based Social Engineering
- Fake Emails
- Keystroke Loggers
- Phishing
- Identity Theft

Securing Your Cyber Social Life

- Awareness is the Key
- Email Security
 - Detecting Fake Emails
 - Creating Account Filters
- Online Account Security
 - Strong Password Setup
 - Designing Account Recovery Mechanism
- Secure Logout
- Browser Remember Password
 - Recognizing Phishing Websites

Module 5- Web server Attacks

Introduction to Penetration Testing

- Legal and Ethical Implications
- Types of Penetration Testing
 - White Box Penetration Testing
 - Black Box Penetration Testing
 - Grey Box Penetration Testing

Setting Up Web Application Penetration Testing Lab

- Collecting and Installing PenTest Tools
- Flexible Browser with Security Add-ons
- Setting up Browser Proxies

Beginning Application Penetration Testing

- Identification of Application Entry Points
 - Get and Post Parameters
- Testing for Security Vulnerabilities
 - SQL Injection
 - Cross Site Scripting
 - Session Hijacking
 - Local and Remote File Inclusion Attacks
 - Parameter Tampering

Module 6- Google Digging

Working of Google and its methodology

- Introduction to Crawlers, Bots
- Caching Process of Crawlers

Various Attacks with the help of Google

- Password Harvesting
- Controlling CCTV Camera

Various Roles of Google as a Friend of Hacker

- Advance Google Search Operators
- Directory Traversal Tool
 - Finding Directory Listings
 - Locating Specific Directories
- Vulnerable Website Locator
 - Locating via Company Tags
 - Locating via Web Applications
 - Locating via Common Names

Module 7- Trojans and Viruses

Introduction to Computer Malware

- Overview Malware: Malicious Software
- Proliferation and Purposes
- Types of Malware
- Virus: Vital Information Resources Under Seize
- Worm: Write Once Read Multiple
- Trojan Horse, Rootkit
- Spyware, Keystroke Logger

Virus and Worm: Infectious Malware

- Significance of Virus and Worm
- Behavioral Activity of Virus and Worm
- Virus and Worm Development
 - By Automated Tools
 - Coding own Viruses and Worms

Trojan Horse: Concealment

- Overview of Trojan
- Trojan Attack
 - Direct Connection
 - Reverse Connection
- Injection in System Files

Detection and Removal

- Anti Malware Tools
- Manual Removal of Malwares

Module 8- Reverse Engineering

Introduction to Assembly Language

- Role of Assembly Language in Reverse Engineering
- Concept of Debuggers and Dis-assemblers

Understanding Data Flow

- “Step Over” view of Data flow
- “Step Into” view of Data flow

Principles of Software Security

- Encryption
- Online Key Checking
- Fake Checking Points
- DLL Breakpoints

Module 9- Indian Cyber Law

Information Technology Act 2000-2008

- Introduction to IT Act 2000
- Amendment 2008
- Under Umbrella of IT Act 2000
 - Cyber Crimes
 - Intellectual Property
 - Data Protection and Property
- Limitations of Indian IT Act