Axpino Technologies

Ethical Hacking

COURSE CURRICULUM

Course Description

- Ethical Hacking Boot Camp

- Course Type: Boot Camp
- Total Time: 60 hours
- Days: 15 Days
- Daily Classes: 4 hours

Module 1- Basics Of Hacking

Basic Concept of Hacking

- What is Ethical Hacking?
- Understanding the Hacking Psychology and Methodology
- Real Meaning of Hacking v/s Public Perspective
- Reading the Hacker's mind
- Difference between Hacker and Cracker
- Categories of Hackers: Based on Knowledge
- Categories of Hackers: Based on Actions
- Hactivism and Cyber Terrorism
- Why Hackers Hack?
- Steps performed by Hackers
  - FootPrinting
  - Scanning
  - Gaining Access
  - Maintaining Access
  - Clearing Tracks

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
- Virtual Machine Performance
- Application Performance

Module 3 - Basics Of Networking

Introduction to Computer Networks

- Introduction of Network and Networking
- Network Devices
- Networking Ports and Protocols
  - Well Known TCP and UDP Ports

Various Networking Aspects

- Routing Technology
  - Networking Topology
- IP Addressing and Subnetting
- Machine Identification: MAC Addresses

Internet Connection Sharing

- Setting up ICS
- Restricting and Limiting Network Users

Module 4 - Google Digging

Working of Google and its methodology

- Introduction to Crawlers, Bots
- Caching Process of Crawlers
- Significance of Google Hacking

Various Roles of Google as a Friend of Hacker

- Google Advance Search Operators
- Hacking Tool
  - Anonymity with Google
  - Using Google as a Proxy Server
- Directory Traversal Tool
- Vulnerable Website Locator
- Locating via Company Tags
- Locating via Web Applications
- Locating via Common Names
- Google Hacking Database

Various Attacks with the help of Google

- Password Harvesting
- Controlling CCTV Camera

Module 5 - 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 6 – Linux Hacking

Basics of Attacks in Linux

- Single User Mode
- Bruteforcing Attack
- Kernel Bypassing

Password Hacking In Linux

- Hacking Linux password through recover mode
- Hacking Linux password through generic mode
- Hacking password of (Red Hat)

Module 7 - Social Media Threats

Email Server

- What is an Email Server?
  - Introduction
  - Types
  - Working
- How to Setup an Email Server?

Email Forgery

- Introduction to Email Forgery
- Ways of Email Forgery
- PHP Fake Mail Scripts
- Fake mail sending websites
- Email Spamming and Email Bombing

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

Module 8 - 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 9 - Web server Attacks

Injection Based Attacks

- SQL Injection
- Types of SQL Injection
  - Form Based
  - URL Based SQL Injection
  - Union Based SQL Injection
- HTML Injection (Cross Site Scripting) – XSS
- Types of XSS Attacks
  - Stored XSS or Persistent XSS
  - Reflected XSS or Non-Persistent XSS
  - DOM Based XSS
- Code Injection
  - Remote Code Execution

Setting Up Web Application Penetration Testing Lab

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

Introduction to other Miscellaneous Web Based Attacks

- Web Based Brute Forcing
- Insecure Cryptographic Storage
- Broken Authentication and Session Management
- Basics of Cookies Stealing/Session Hijacking
  - What is Cookies Stealing/Session Hijacking
  - Session Hijacking: Threats
  - Attack the Victim
- HTTP Referrer Attack
- MITM Attack
- Man-in-the-Browser Attack
- Remote File Inclusion
- Local File Inclusion
- Directory Traversal
- Parameter Tampering
- Shell Injection

Module 10 – Buffer Overflow

Introduction to Computer Memory Architecture

- Concept of Buffer, Heap and Stack
- Introduction to Memory Exploitation/Buffer Overflow
- Categories of Error Conditions
  - Heap Based Overflow
  - Stack Based Overflow
  - Integer Based Overflow
- NOPS (No-Operation instructions)

Introduction to Attack Hierarchy

- Logics of Payloads, Exploits
- Information Gathering and Identification
- Client Side Services Identification
- Setting up Arrow and Bow
- Exploitation

MetaSploit Framework

- Introduction to MSF: MetaSploit framework
- Working of MSF
- Exploitation with MSF
  - Using WebGUI
  - Using Console

Module 11 – Wireless Hacking

Introduction to Wireless LAN Security

- Wireless LAN Technology
- General security threats
- Overview of Wireless LAN Security

De-authentication Phase

- MAC Address Spoofing

Getting Access of Wireless LAN

- WEP Key Cracking
- WPA De-authentication Attacks

Module 12 - 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 13 - Recovery and Backup

Introduction to Data Recovery and Backup

- Types of Backup
  - Full Backup
  - Differential
  - Incremental
- Daily Backup

Planning a Backup

- Data Severity Checking
- Choices of Backup Solutions
- Trigger Backup
- Data Integrity Checking

Module 14 - 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