

Kyriion Ethical Hacking and Information Security

Summer Training Module

Duration: 6 Weeks

Making of a Hacker

- Hacking Dictionary – Major Terms
- What is a Computer - From the eyes of a Hacker
- Concept of Computer
 - Descriptions of the Devices
 - OS Installation – Windows & Linux
 - Boot Process
 - Types of OS
 - Live OS
 - File System
 - Kernel & Library
 - Drivers
 - Software Apps
 - Registry Database
- What is a Network?
- Concept of Networking
 - IP Address
 - Static v/s Dynamic
 - Public v/s Private
 - LAN/WAN
 - IPv4/IPv6
 - Classes of IP
 - MAC Address
 - Client & Server
 - Web Server
 - DNS Server
 - Network Devices
 - Switch
 - Router
 - Wire
 - Protocols
 - Ports & Services
 - DNS
 - FTP
 - HTTP
 - SMTP
 - DHCP
 - UDP
 - Telnet
 - TCP
 - ARP

1. Concept of Hacking

- What is Hacking?
- Who is a Hacker?
- Who is not a Hacker?
- What is Cracking?
- Who is a Cracker?
- How to become a Hacker?
- Types of Hackers?
- Types of Hacking?
- Let Us Become a Hacker
 - Software Requirement
 - Hardware
 - Intellectual
 - Appearance & Interaction
 - Communication Skills
 - Time Management
- Start with Hacking
 - Foot Printing
 - Scanning
 - Port Scanning
 - Finger Printing
 - Fire walking
 - Gaining Access
 - Password Attacks
 - Social Engineering
 - Viruses
 - Keyloggers
 - Maintaining Access
 - OS Backdoors
 - Trojans
 - PHP Injection
 - Clearing Tracks
 - Deleting Log Files
 - Remove Traces
 - Delete Event Logs
- Foot Printing
 - What is Foot Printing
 - Why is it Necessary
 - Whois Lookup
 - NS Lookup
 - IP lookup
 - Target Information gathering
 - Website
 - Social Profiles

- Contact Info
 - Fake Calling
 - Fake Mails
- Google Digging
- Make a Report
- Scanning:
 - What is Scanning
 - Why is it Necessary
 - Port Scanning
 - Types of Port Scanning
 - Finger Printing
 - Active Finger Printing
 - Passive Finger Printing
 - Fire Walking
 - Network enumeration
 - Make a Report

2. Attacks on Email

- What is an Email
- What is an Email Server?
- Working of an Email Server?
 - How to setup an Email Server
- What is the Login Process?
- What is Email Hacking?
- Different kind of Attacks on Email
 - Sending Fake Mails
 - Phishing
 - Stealing Cookies
 - Keyloggers
- Fake Mails
 - Introduction to Email
 - What is a Fake Mail
 - Why Fake Mail goes?
 - Sending a Fake Mail
 - Using Scripts
 - What is the working of the Script
 - How to use the Script
 - Topic Hierarchy
 - From Open Relay Servers
 - What is a Open Relay Server
 - How to Send Email
 - Topic Hierarchy
 - Detecting a Fake Mail
 - Understanding the Travelling Path of an email
 - Reading Headers

- What is a Header
 - How to Access the Header in different Email Accounts
 - Checking outgoing server address from Header
 - Tracing an Original Email
 - Reading Headers
 - Checking the Sender's IP Address
 - Tracing the IP Address
 - Tools
 - Websites
- Phishing
 - Introduction to the Topic
 - Why Phishing is successful
 - Steps in Phishing
 - Making a look alike website, as the Original one
 - Changing the code of the Webpage
 - Sending the link of the webpage to several users to get the Personal Data
 - Working of Phishing
 - Introduction to Phishing Script
 - Ways to do Phishing
 - Protection from Phishing
 - Anti-Phishing Tools
 - Awareness about Phishing techniques
- Stealing Cookies
 - Introduction to Cookies
 - Information stored in Cookies
 - Ways to get Cookies from a computer
 - Physically accessing the computer
 - Remote Attacks
 - Getting Information from Cookies
 - Using Cookie to impersonate as a different user
 - Protection from Cookie Attacks
 - Deleting Cookies
- Keyloggers
 - Introduction to Keyloggers
 - Using a Keylogger
 - Types of Keylogger
 - Local Keylogger
 - Remote Keylogger
 - Detecting a Keylogger
 - Using Anti-Virus
 - Using Process Explorer
- Securing an Email Account
 - Configure Strong Passwords
 - Configure a Secure Account
 - Follow Counter-measures of Phishing

3. Windows Systems Hacking

- Introduction to Windows OS
 - Windows Architecture
 - Windows File system
 - NT File System
 - FAT File System
 - Windows Security
 - Local Security Authority
 - Security Account Manager
 - Security Reference Monitor
 - Windows Login Process
- Cracking Login Password
 - Security Account Manager (SAM)
 - Introduction to SAM File
 - Location of SAM File
 - Importance of SAM File
 - Introduction to Hashes
 - Introduction to Live OS Disks
 - Using a Live CD
 - Advantages of a Live CD
 - Ways to Crack Login Password
 - Shoulder Surfing
 - Password Guessing
 - Dictionary Attack
 - Rainbow Table Attack
 - Brute-force Attack
 - Using Command Prompt
 - Cracking Password from Hashes
 - Using Ophcrack Live CD
 - Using NT Offline Password Cracker
 - Using Cain & Abel
- Privilege Escalation
 - Using Live CD
 - Using Command Prompt
 - Using GPEdit
- Creating Backdoors
 - Creating Hidden Account
 - Getting Command Prompt on Login Screen(Sticky Keys Attack)
- Clearing Tracks
 - Introduction to Event Viewer
 - Deleting Event Logs
 - Deleting Windows Logs
- Securing Windows Systems
 - Configuring Strong Login Passwords
 - Using Syskey
 - Introduction to Syskey

- Configuring the Syskey Password
 - BIOS Password
 - Introduction to BIOS
 - Configuring BIOS
 - Changing Boot Sequence
 - Checking for Backdoors
 - Checking Hidden Accounts
 - Checking Sticky Keys Attack
 - Checking the Event Logs
- Hiding Files in Windows
 - CACLS
 - Introduction to ACL
 - Changing ACL
 - ADS
 - Performing ADS
 - Retrieving Data from ADS files
 - Detecting ADS Files
 - Introduction to Streams
 - Steganography
 - Introduction to Steganography
 - Ways to perform Steganography
 - Using Command Prompt
 - Using Tools
 - Winrar

4. Website Hacking

- Introduction to Web Server
 - What is a Web Server
 - Working of a Web Server
 - Request-response Cycle
 - Setup a Web Server
 - Tools
- Introduction to Database Server
 - What is a Database Server
 - Working of a Database Server
 - Setup a Database Server
 - Tools Required
- Login Process on a Website
 - Connection between Web Server & Database Server
- Attacking a Web Server
 - SQL Injection
 - Remote Code Execution
 - Cross Side Scripting
 - Directory Traversal Attack
- SQL Injection
 - Introduction to SQL

- Working of SQL Database
 - Introduction to SELECT Query
 - Working of SELECT Query in Login Process
- Introduction to SQL Injection
 - The SQL Injection Query
 - Understanding the Working of the Query
- Using the SQL Injection to Get Login
 - Live Demonstrations
- Counter-measures of SQL Injection Attack
 - Validating the Input on the Web Server
 - Encrypting the Input on the Web Server
- Remote Code Execution
 - Introduction to the Topic
 - Introduction to PHP eval() function
 - Working of the eval() function
 - Hacking using the eval() function
 - Executing commands on the Web Server
 - Live Demonstrations
 - Getting information on the Web Server
 - Live Demonstrations
 - Counter-measures
- Cross-side Scripting
 - Introduction to the XSS
 - Working of XSS
 - Flaw in XSS implemented websites
 - Hacking using XSS
 - Counter-measures
- Directory Traversal Attack
 - Introduction to the Topic
 - Structure of a Website
 - Performing the Attack
 - Live Demonstrations
 - Counter-measures
- Alternative way to Attack websites
 - Getting all the files of a Website
 - Using Tools
 - Black Widow
 - Wget
 - WebSleuth

5. Linux & Macintosh Hacking

- History of Unix
- Introduction to Linux
- Advantages to Linux
- Different Versions of Linux
- Difference between Linux & Windows
- Basics of Linux
 - Commands
 - File System
 - Kernels
 - Installation
 - Configuration
 - Compilation
 - Files & Directories
 - File Structure
- Compiling Programs in Linux
 - Introduction to GCC Compiler
- Linux Vulnerabilities
 - Concept of Open Source Code
 - Optimizing Linux
- Hacking Linux
 - Introduction to /etc/shadow file
 - Cracking Passwords
 - Modifying the Grub
 - Using Live CD
 - Using Tools
 - Hacking Linux Networks
 - Tools Used
 - Maintaining Access
 - Installing Rootkits
- Firewalls in Linux
 - Introduction to IP Tables
- Clearing Tracks
 - Deleting System Logs
- Securing Linux
 - Improve Login & User Security
 - Protect GRUB
 - Set Boot Security Controls
 - Secure Network
 - Secure via daemons
 - Increase Logging & Audit Information
 - Auditing Tools
 - Patch System
 - Download Updates
- Introduction to MAC OS

- History of MAC
- Basics of MAC OS
- Vulnerability in MAC OS
 - Crafted URL
 - CoreText Pointer
 - Image IO Integer Overflow
 - Image IO Memory Corruption
 - UFS File System Overflow
 - User Privilege Escalation
- Cracking MAC OS
 - Malformed Installer Package Crack
- Worms & Viruses In MAC OS
 - Working of Worms & Viruses
 - Removal of Worms & Viruses
 - Anti-Viruses in MAC
- Security Tools in MAC
- Counter-measures

6. Network and Networking Security Measures and Attacks

- Networking Devices
 - Switches
 - Router
- Types of Network
 - Local Area Network
 - Wide Area Network
- Three Way Handshake
- Compromising a Network
 - Network Enumeration
 - Ping Sweep
 - OS Fingerprinting
 - Sniffing
 - Host Scanning
 - Active Sniffing
 - Passive Sniffing
 - ARP Poisoning - Man in the Middle Attack
 - DNS Spoofing
 - Pharming
 - Denial of Service Attack
- Tools Used in Network Attack
 - Ethereal
 - Ettercap
 - Wireshark
- Detecting Network Attacks
- Securing Network Perimeter
 - Concept of Firewalls

- Intrusion Detection Systems
- Configuring Firewall on Windows Operating System

7. Wireless Hacking

- Introduction to Wireless Technology
- History of Wireless Technology
- Concept of Wireless Networks
- Wired Network vs. Wireless Network
- Types of Wireless Network
- Types of Wireless Standards
 - 802.11
 - 802.11a
 - 802.11b
 - 802.11g
 - 802.11i
 - 802.11n
- Terminology in Wireless Networks
 - MAC Address
 - WAP
 - SSID
 - Beacon Frames
 - ESSID
 - Channel
 - Association & Authentication
- Setting up a WLAN
 - Ad-Hoc Mode
 - Infrastructure Mode
- Security Options in WLAN
 - MAC Filtering
 - WEP Key
 - WPA & WPA2 Keys
- Hacking a WLAN
 - Terminologies
 - War Walking
 - War Driving
 - War Flying
 - MAC Spoofing
 - WEP Cracking
 - WEP Flaws
 - Passive Attacks
 - Active Attacks
 - Steps to Hack a WLAN
 - Finding Networks
 - Analyzing the Target Network
 - Sniffing the Network
 - Cracking the WEP Key

- Authentication & Disassociation Attack
 - Live Demonstration using Aircrack
 - Rogue Access Point
 - Creating a Rogue Access Point
 - WPA Cracking
 - Live Demonstration
- Some More Attacks on WLAN
 - Man in the Middle Attack (MITM)
 - Eavesdropping
 - Manipulation (ARP Poisoning)
 - Denial of Service Attack
- Wireless Sniffing Tools
 - Introduction to the Tools
- Securing a Wireless Network
 - MAC Filtering
 - Disable Broadcasting of SSID
 - Correct selection of Encryption Method
 - WLAN Security Passphrase
 - Configure Firewall

8. Reverse Engineering

- Introduction to the Topic
- Why to Reverse Engineer
 - Advantages
 - Disadvantages
- What is a Software
- Concept of Languages
 - Programming Language
 - Machine Language
 - Assembly Language
- What is a Disassembler
 - Why to Disassemble a Software
 - Working of a Disassembler
 - Tools to Disassemble
- What is a Decompiler
 - Why Decompile a Software
 - Working of a Decompiler
 - Tools to Decompiler
- What is a Debugger
 - Why to Debug a Software
 - Working of a Debugger
 - Tools to Debug a Software
- Difference between Disassembler & Debugger
- Serial Key Phishing
 - Introduction to the Topic

- Steps in Serial Key Phishing
 - Analyzing Assembly Code of Software
 - Tracing the Error Message
 - Setting Break Point
 - Stepping the Assembly Code
 - Checking the Registers for the Key
- Manipulating the Software
 - Introduction to the Topic
 - Steps to Manipulate
 - Analyzing Assembly Code
 - Error Tracing
 - Setting Break Point
 - Stepping the Assembly Code
 - Tracing Conditional Jumps
 - Injecting the Code
 - Generating Patched Exe File
- Software Patching
 - Concept of Patching
 - Steps in Patching
 - Disassembling a Software
 - Tool
 - Error Tracing
 - Decoding the Instructions
 - Generating Patch to Inject the instruction
 - Introduction to Patching Tool
 - Using Code Fusion
 - Running the Patch
- Counter-measures
 - Securing a Software
 - Encryption
 - Program Obfuscation

9. Trojans & Viruses

- Introduction to the Topic
- Different Applications
 - Trojans
 - Viruses
 - Worms
 - Spywares
- What is a Trojan
- Types of Trojans
 - Remote Access Trojans
 - Service Denying or Destructive Trojans
 - FTP Trojans
- Trojan Attack Methods

- Emails & Attachments
- Deception & Social Engineering
- Website Bugs & Downloads
- Physical Access
- Fake Executables
 - Concept of Wrappers
 - Working of Wrappers
- Live Demonstration of Known Trojans
 - Beast
 - Back Orifice
 - Donald Dick
 - Netbus
- Detecting a Trojan
 - Using Anti-Trojan Software
 - Manual Detection
 - TCPView
 - Process Viewer
 - Process Explorer
- What is a Virus
- Working of a Virus
- Types of Viruses
- Developing a Virus
 - Introduction to Batch Programming
- Removal of Virus
 - Using Anti-Virus Software
 - Manual Removal
 - Process Explorer
 - TCPView

10. Penetration Testing

- Concept of Penetration Testing
- Difference between Ethical Hacking and Penetration Testing
- Manuals of Penetration Testing
 - OWASP
 - OSSTM
- Types of Penetration Testing
 - White Box Testing
 - Black Box Testing
 - Grey Box Testing
- Steps in Penetration Testing
 - Preparation
 - Conduct
 - Conclusion
- Tools Used in Penetration Testing
 - Backtrack - Linux Based Live OS

- Nessus - Network Vulnerability Scanner
- Nmap - Port Scanner
- Accunetix - Web Scanner

11. Buffer Overflow Attacks

- Concept of Buffer, Stack and Heap
- What is Buffer Overflow?
- Exploiting an Overflow in Buffer
- Types of Buffer Overflow Attacks
 - Heap Based Buffer Overflow
 - Stack Based Buffer Overflow
- NOPS (No-Operation instructions)
- Tools Used in Buffer Overflow Attacks
 - Meta-Sploit in Windows
 - Backtrack Meta-Sploit Framework
- Live Demonstrations
 - Exploiting Internet Explorer
 - Take Control of Victim's Command Prompt
 - Take Over Victim's Computer
 - Exploiting Adobe Reader
 - Tracking the location of the Victim
- Protective countermeasures
 - Choice of programming language
 - Use of safe libraries
 - Pointer protection

12. Cryptography

- Introduction to Symmetric Key Cryptography
 - Symmetric Key Encipherment
 - Substitution Cipher
 - Vernam Cipher (One-Time Pad)
 - Transposition (Permutation) Cipher
 - Symmetric Key Cryptography Characteristics
 - Data Encryption Standard (DES)
 - Triple DES
 - The Advanced Encryption Standard (AES)
 - The Blowfish Algorithm
 - The Twofish Algorithm
 - The IDEA Cipher
 - RC5/RC6
- Public Key Cryptosystems
 - One-Way Functions
 - Public Key Algorithms
 - RSA

- El Gamal
- Summaries of Public Key Cryptosystem Approaches
- Digital Signatures
 - Hash Function
 - Developing the Digital Signature
 - MD5
- Public Key Certificates
 - Digital Certificates
 - Public Key Infrastructure (PKI)
- Cryptanalysis
- Email Security
- Wireless Security
- Disk Encryption

13. Cyber Forensics and Investigation

- Introduction
- The History of Forensics
- The Objectives of Computer Forensics
- Reasons for Cyber Attacks
- Computer Forensics
 - Rules
 - Procedures
 - Legal Issues
- Digital Forensics
 - Assessing the Case
 - Detecting
 - Identifying the Event
 - Crime
 - Preservation of Evidence
 - Chain of Custody
 - Collection
 - Data Recovery
 - Evidence Collection
 - Examination:
 - Tracing
 - Filtering
 - Extracting Hidden Data
 - Analysis
 - Where and When to Use Computer Forensics?
- Investigating Computer Crime
 - How an Investigation Starts
 - The Role of Evidence
 - Investigation Methodology
 - Securing Evidence
 - Chain of Evidence Form

- Before Investigating
- Professional Conduct
- Acquiring Data, Duplicating Data, and Recovering Deleted Files
 - Recovering Deleted Files and Deleted Partitions
 - Data Recovery in Linux
 - Deleted File Recovery Tools
 - Recovering Deleted Partitions
 - Deleted Partition Recovery Tools
 - Data Acquisition and Duplication
 - Data Acquisition Tools
 - Backing Up and Duplicating Data
 - Acquiring Data in Linux

