



Cyber Security Essentials

Training Duration: 2 days

Cyber Security in the Real World

Introduction to Cyber Security
Hacking in the Real World

Fundamentals of Networking

OSI & TCP/IP Model
MAC Addressing
IPv4 & IPv6
Types of Network and Topologies
Understanding Network Services and Protocols
Understanding Network Devices
Introduction to Network Media
Understanding Ports
Network Troubleshooting Command

Introduction to Virtualization

What is Virtualization?
Benefits of Virtualization
Hypervisor
Common Security Issues with Virtual Machines

Fundamentals of Cloud Computing

What is Cloud Computing?
Benefits of Cloud Computing
Types & Services of Cloud Computing
Security Issues with Cloud Computing

Shodan Search Engine

Introduction to Shodan
How to Use Shodan
Explore Vulnerable Services and Servers

Google Hacking Database (GHDB)

Introduction to GHDB/Google Dorks



Finding Bugs
Information Gathering

Installing and Configuring Lab Setup

Installing Kali Linux
Installing Windows Desktop OS
Installing Vulnerable VM's

Essential Security Tools

Nmap
Zenmap
Wireshark

Essential Security Technologies

HTTP & HTTPS
SSL & TLS
Firewall and its Types
IPS & IDS
Antivirus
VPN
Proxy Servers
Endpoint Protection
Honeypot
DMZ
Sandbox

Important Hacking Concepts

What is Zero-day Attack or Vulnerability?
Exploit
Vulnerability
Payload

Introduction to Malwares

Virus
Worms
Adwares
Spywares
Rootkit
Trojan



Different Phases of Hacking

Reconnaissance
Scanning
Gaining Access.
Maintain Access
Clearing Tracks

System Hacking

Active Attack
Passive Attacks

Password Hacking

Default Passwords
Brute Force attack
Dictionary Attack

Website / Web Application Security

HTTP Vs HTTPS
XSS(Cross Site Scripting)
Command Execution
File Inclusion
Automated SQL Injection

Common Methods of Attack

DoS & DDoS Attacks
Network Attacks
Man in the Middle Attack
DNS Hijacking
Web Based Attacks

Wireless Hacking

Bypassing WEP
Bypassing WPA/WPA2
Create Fake Access Point



Sniffing Wireless Traffic

Overview on Information Security

Fundamentals of Information Security
Common Challenges in Information Security
Data Classification
Industrial Espionage
Non-repudiation

Understanding Risk Management

What is Risk?
Risk Assessment
Managing Risk
Asset Identification

Countermeasures

OWASP Top 10
Security Practices
Disaster Recovery & Planning

Hands-On and Discussion on Real Case Scenarios