REAL TIME CYBER SECURITY (Zero Coding)

Complete Practical Based-80% Hands-On

Introduction to Cyber Security:

- What is Cyber Security

- Importance of Cyber Security

- CIA Triad

Linux Essentials:

- History and Features of Linux

- Architecture of Linux OS

- Linux Distributions

- Linux Command Line

- Software Package installation

Linux Administration:

- File System

- Users and Groups

- File/folder Permissions

- Special Permissions

- Service and Process Management

Networking Fundamentals:

- What is Networking

- Network Components and Functions

- Types of Networks

- What is OSI Model
- What is IP address
- What is Subnetwork(Subnet)
- What is Super Network (Supernet)
- What is Network address translation
- What is DHCP, TCP, UDP, ICMP
- What is ARP
- What is Domain Name System
- Internet Group Management Protocol
- Routing
- Routing Protocol
- Packet Analysis using Wireshark

Scanning Network

- Network Scanning with Angry IP Scanner
- Network Scanning with netdiscover
- Ping Sweeping with nmap
- Port Scanning with nmap

Foot Printing and Reconnaissance:

- Finding domain registration details with Whois tool
- Extracting Emails and subdomains details using the harvester
- To find out targets IP address using IP tracking technique
- Footprinting domain using Recon-ng tool
- Google Dorks

Kali Linux:

- What is Kali Linux

- How Kali Linux is different from other Linux Dist

- What are the uses of Kali Linux

- What is Metasploit framework

- Tools for Footprinting, Scanning & Sniffing

- Using Metasploit framework to attack Windows

Hacking Environment :

- Steps to install VirtualBox on Windows Operating System

- Install Tor Browser in Kali Linux

- Install VPNBook in Kali Linux

- Install PIA VPN on Windows Platform

Vulnerability Management:

- Vulnerability Assessment

- Penetration Testing

- Installation of Vulnerability Assessment Tools (Nessus, OpenVAS)

- Penetration Testing Tools (Exploitation Tools)

- Interpreting and Calculating CVSS Score

- Reporting

- Qualys Tools and its functionality

Network Penetration Testing:

- Introduction to Penetration Testing

- Types of Penetration Testing

- Red Team activity

- Blue Team activity

- Hacking Linux OS using Metasploit Framework

- Hacking Linux operating system with Samba Vulnerability

- Steps to hack Linux OS using Metasploit framework

- Hacking Windows 7 Operating System with ms17_010 exploit

- Meterpreter Commands

- Hacking Windows machine with MS15_100 exploit.

- Hacking Windows 10 operating system

- Hacking Windows 11 operating system

Web Application Pentesting :
- Extracting Web Server details using whatweb

- Identifying web application firewall(WAF) using wafw00f

- Web Application Vulnerability Scanning using Vega

- Web application Scanning using OWASP-ZAP (Passive and Active)

- XSS(Cross Site Scripting) Attack

- Web Parameter tampering using Burp Suite

- Command Execution on vulnerable web application

- Directory Traversal or Path Traversal Attack

- Web Application Penetration Testing Checklist

- Session Management

- Tools: Burpsuite, SqlMap, Wafw00f, Nikto,Nmap,online tools, OSINT

Hacking Webserver:

• Hacking Webservers:

• Scanning Web Server using Nikto

• Hacking Webserver using Metasploit framework

• Hacking server with the help of vulnerability in PHP

• Hacking Tomcat Web Server with Metasploit

Cryptography:

• Introduction to Cryptography

• Symmetric Ciphers

• Asymmetric Ciphers

• Digital Certificates and Digital Signatures

• Disk Encryption

• Hashing

• Encoding

• Steganography
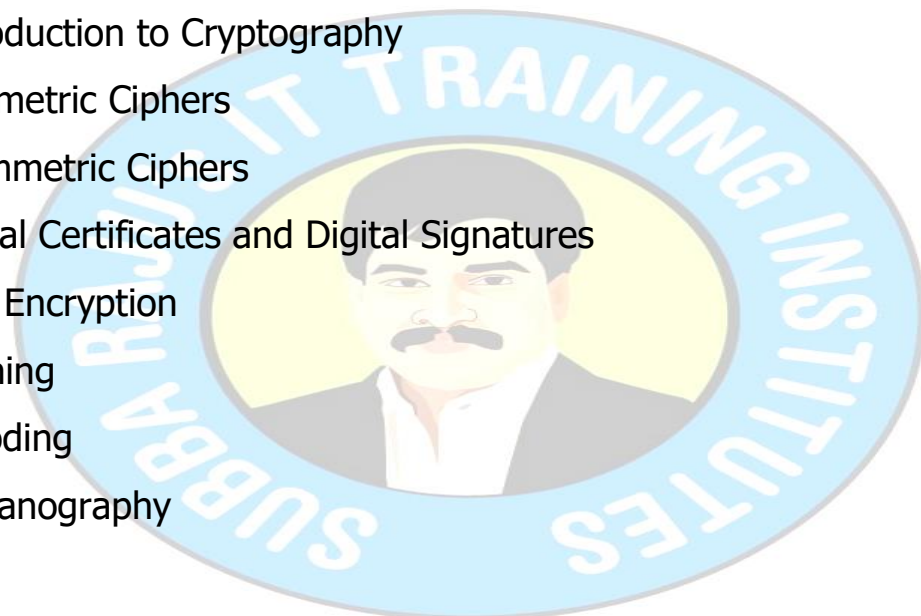
Cryptography Penetration Testing :

• Encrypting a backdoor with msfvenom encoding options

• Creating an encrypted virtual disk using VeraCrypt

• Identifying SSL details using SSLScan

• Identifying misconfigurations on the web server

• Evaluation Security of protocols running on a web server

• Identifying Hash algorithms for given has value

• Cracking encrypted password using John the ripper