About Training

Objective

This training is to empower participants with comprehensive knowledge and practical skills in both defensive and offensive cybersecurity. This training aims to: equip learners with the ability to identify, assess, and mitigate security threats through proactive defense strategies. Develop expertise in offensive security techniques, including ethical hacking, penetration testing, and vulnerability exploitation, to strengthen system resilience. Provide hands-on experience with industry-standard tools and frameworks for securing networks, systems, and applications. Foster a deep understanding of cybersecurity principles, enabling participants to anticipate and counteract advanced cyber threats. Prepare professionals to excel in real-world scenarios, ensuring they can safeguard organizational assets while adhering to ethical and legal standards. This training bridges the gap between theory and practice, making participants proficient in both protecting and testing the security of digital environments.

Target Audience

This training is designed for:

IT Professionals: Network administrators, system administrators, and IT managers seeking to enhance their cybersecurity skills.

Cybersecurity Enthusiasts: Individuals passionate about learning defensive and offensive security techniques.

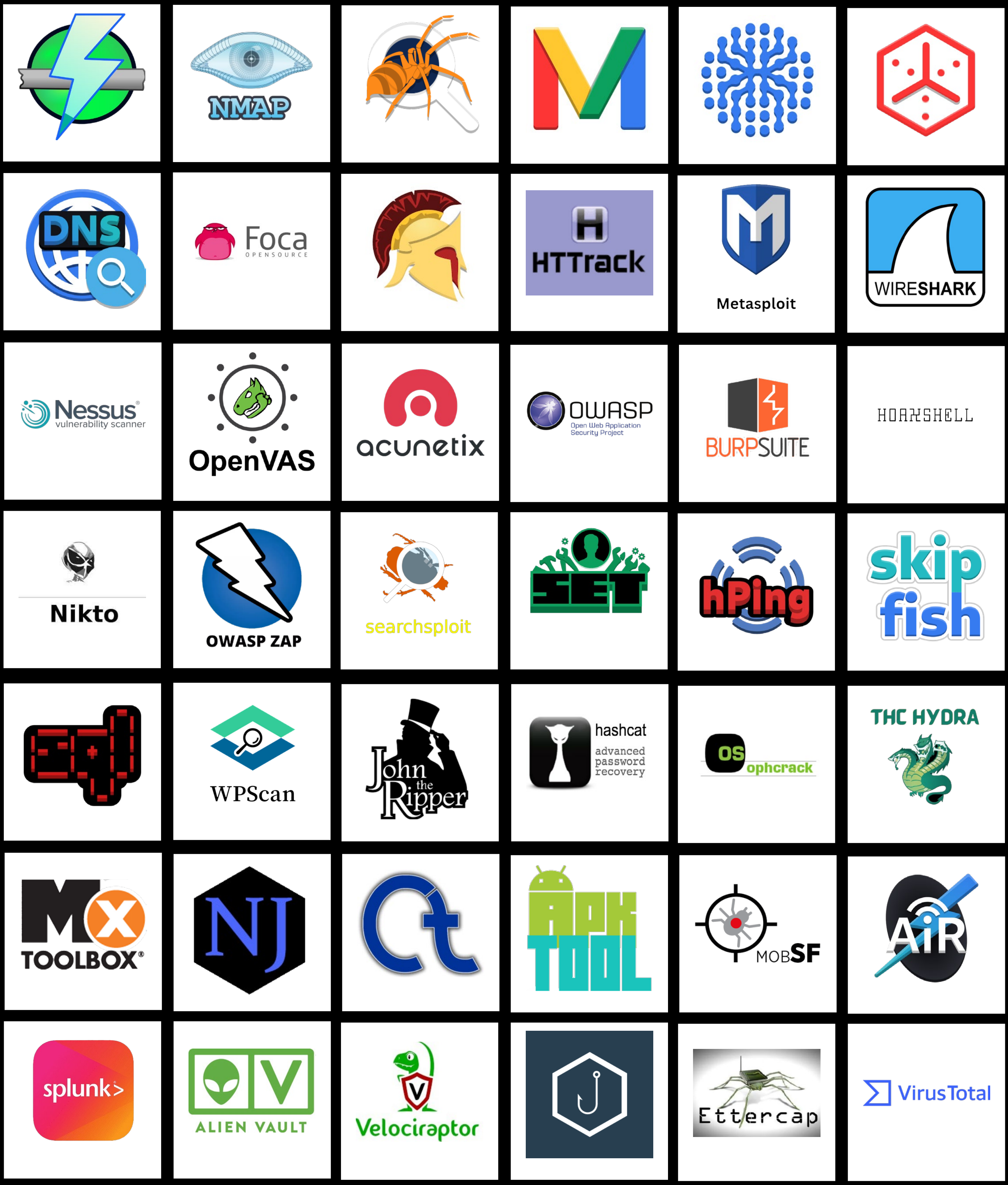
Students and Graduates: Aspiring cybersecurity professionals looking to kickstart their careers with hands-on training.

Business Owners and Decision Makers: Individuals responsible for securing organizational assets and ensuring compliance with cybersecurity standards.

Anyone Interested in Cybersecurity: From beginners to seasoned professionals, anyone eager to understand and implement effective cybersecurity strategies.

No matter your background, this training provides the tools and knowledge to thrive in the ever-evolving field of cybersecurity.

CYBERSECURITY TOOLS



TOOLS COVERING IN THIS COURSE

1. Information Gathering & Scanning

Gain hands-on experience with industry-leading tools for reconnaissance and scanning:

- **Nmap, Znmap, Masscan**: Network discovery and port scanning tools for mapping and assessing network vulnerabilities.
- **Hping3**: Advanced packet crafting and testing tool.
- **Wireshark**: Network protocol analyzer for real-time traffic inspection.
- **NetScanTool, Angry IP Scanner, Advanced IP Scanner**: Tools for fast and detailed network scanning.
- **Metasploit**: Comprehensive framework for penetration testing.
- **HTTrack**: Website copier for offline analysis.
- **Whois Lookup, Smart Whois**: Domain and IP ownership information.
- **DNS Recon, DNSEnum**: DNS enumeration tools.
- **SNMP-Check**: SNMP protocol scanner.
- **Legion Scanner, Metagoofil, FOCA, Spiderfoot, theHarvester**: OSINT tools for data extraction and analysis.
- **OSINT Framework**: A structured collection of online OSINT tools.

2. Vulnerability Scanning & Reporting

Learn to identify and document vulnerabilities effectively:

- **Nmap, Znmap**: For initial vulnerability detection.
- **SearchSploit**: Offline database of exploit codes.
- **Nessus, OpenVAS**: Advanced vulnerability scanning platforms.
- **Acunetix**: Web application vulnerability scanner.
- **Metasploit Pro**: For exploiting and verifying vulnerabilities.
- **OWASP Top 10**: Framework for addressing critical web application vulnerabilities.
- **Cherrytree, MS OneNote**: Tools for structured reporting and documentation.

3. Exploitation & Password Cracking

Master exploitation techniques and password recovery:

- **Hydra, Hashcat**: High-speed password-cracking tools.
- **John the Ripper**: Versatile password-cracking utility.
- **Metasploit**: Exploitation framework with built-in payloads.
- **PowerShell-Empire**: Post-exploitation framework.
- **Burp Suite**: Web vulnerability scanner and proxy tool.
- **OPHCrack, Pwdump7**: Tools for Windows password recovery.

4. Malware Threats & Analysis

Understand malware behavior and detection:

- **Msfvenom, Veil Framework**: Payload creation tools.
- **njRAT, 888 RAT**: Remote access trojans for testing.
- **VirusMaker, Crypters**: Malware creation and obfuscation tools.
- **HoaxShell**: Simulation of malicious behavior.
- **PE Explorer, Process Hacker, Process Monitor**: Tools for analyzing executable files and processes.
- **Autoruns Sysinternals, TCP View**: Advanced process and connection monitoring.
- **VirusTotal, FileScan**: Online malware scanning platforms.

---

5. Network Auditing & Sniffing Tools

Explore tools to audit and analyze network traffic:

- **Yersinia**: Testing network protocols for vulnerabilities.
- **MAC-Changer**: Spoofing MAC addresses.
- **Wireshark, Responder**: Capturing and analyzing network traffic.
- **Arpspoof, Ettercap, Bettercap**: Tools for ARP poisoning and packet interception.
- **WebSploit**: Network and web vulnerability testing.

---

6. DoS & DDoS Tools

Learn to simulate denial-of-service attacks responsibly:

- **LOIC, HOIC**: DoS testing tools.
- **Hping3**: Custom packet generation for network testing.
- **Metasploit**: Framework for launching DoS attacks.
- **Wireshark**: Analyzing the impact of DoS attacks.

---

7. Social Engineering Tools

Understand human-centric attack vectors:

- **SEToolkit**: Social engineering attack simulator.
- **Metasploit**: For phishing and payload delivery.
- **Find-Moiz, CamPhish, Zphisher**: Tools for phishing simulations.
- **GoPhish**: Phishing campaign management.

---

8. Web Auditing & Penetration Testing Tools

Test web applications for vulnerabilities:

- **Burp Suite**: Comprehensive web application security testing tool.
- **Metasploit, WebShells**: Tools for exploitation and access.
- **NetCat**: Networking utility for debugging and data transfer.
- **Acunetix, SQLMap, Nikto**: Scanners for web vulnerabilities.
- **WPScan**: WordPress vulnerability scanner.
- **Zap-Proxy**: OWASP tool for web application penetration testing.
- **Dirbuster, Gobuster**: Directory and file brute-forcing tools.
- **Commix**: Automated command injection tool.

9. WiFi & Bluetooth Auditing

Audit wireless networks and devices:

- **Aircrack-ng Suite (Airmon-ng, Airodump-ng, Aireplay-ng, Aircrack-ng)**: Wireless network auditing and cracking tools.
- **Kismet**: Wireless network detector and sniffer.
- **Wifiphisher, Fluxion**: Tools for WiFi phishing attacks.
- **Sparrow-WiFi**: GUI for WiFi and Bluetooth auditing.
- **HCI Tools, Spooftooth, L2ping, Bluesnarfer**: Bluetooth penetration testing tools.

10. Mobile Hacking & Penetration Testing Tools

Explore vulnerabilities in mobile platforms:

- **Metasploit, MobiHookRAT, SpyMaX RAT**: Tools for mobile exploitation.
- **PhoneSploitPro**: Android device penetration testing.
- **MobSF**: Mobile application security framework.
- **ApkTool, ApkStudio**: Tools for reverse engineering Android apps.

12. Cryptography & Steganography

Understand data protection and concealment:

- **AES Encryption Tools, Mcrypt, CrypTool**: Encryption and decryption utilities.
- **CyberChef**: Multi-purpose data transformation tool.
- **SNOW, Audacity**: Tools for hiding data in text and audio.
- **Stegosuite, OpenStego**: Image-based steganography tools.

COURESE OUTLINE

Module 01 – Introduction to Cybersecurity

Introduction to Cyberseuciry (Offensive & Defenseive)

Cybersecurity Framework (NIST, ISO 27001, MITRE ATT&CK)

Types of Hacker (BlackHat, WhiteHat, GrayHat, ScripKids,)

Introduction to Ethical Hacker (White Hat Hacker)

Phases of Ehtical Hacking (Recon, Vulnerability scanning, Exploitation, Post-Exploit)

Introduction to Penetration Testing (Network, Web, Android, Social-Engineering)

Introduction to Cybersecurity Team Strategies (Read, Blue, Purple)

Cyber Kill Chain Methodology

Threat Types and Actors

Attack Vectors and Methodologies (TTPs)

Case studies: Real-world Cyber Attacks

Module 02 – Linux, Windows and Networking Fundamentals

TCP/IP suite and OSI Model

Networking Types & Topologies

Networking ports and protocol (FTP, HTTP, HTTPS, SSH, RDP, SMB, SMTP, DNS, DHCPs)

Network Security Devices (IDS/IPS, Firewall, Router, Switch)

Network Secuiry Controls (Access, Identification, Authentication, Authorization, Accounting, Cryptography, Security Policy)ss

Linux Command Line, Windows PowerShell

Module 03 – Information Gathering & Scanning

Collecting Active and Pasive Information

Google Dorking & Hacking Techinques

OSINT (DNS, Traceroute, WhoisLookup, Sub-domains)

Network and Port Scanning

Service, Version and Operating System Detection (Enumeration)

Vulnerability Scanning, Reporting & Risk Management

Module 04 – System Exploiation & Malware Threat

Password Cracking Attacks (Dictionary & BruteForce)

Vulnerability Exploitation and Post-Exploitation

Lateral Movement and Pivoting

Hiding Tracks & Stegnographys

Malware and Malware Tpyes

Remote Access Trojan and Malware Hiding Techinques

Malware Analysis (Statics & Dynamic Analysis)

Module 05 – Networking Attaks & Social Engineering

ARP Spoofing, DNS Spoofing, MITM Attacks, Session Hijacking

IP Spoofing, MAC Spoofing and DHCP Spoofing

DoS, DDoS, Packet Flooding

Phishing and Social Media Attacks

Wireless Network Attacks and Types

Wireless Encryption Cracking and Evil-Twin Attacks

Wireless Rouge Access Point Attack

Detecting Deauth (DoS) Attack

Securing Wireless Networks

Module 06 – Web Server & Application

Scanning and Enumeration Web Servers

Exploitation Web Servers and Protocols

OWASP Top 10 Vulnerabilites

Fuzzing, Directory Finding

Web Vulnerabilies Scanning

Exploring the Power of Burpsuite

Exploiting SQL Injection, XSS and Command Injection

Exploiting Directory Traversal, File Upload

Module 07 – Mobile Exploitatio and Cryptography

Android Basics and History

Exploiting Android Mobiles Devices

Mobile OWASP Top 10 Vulnerabilities

Compiling and Decompling Android APK Files

Creating Undetectable Android Malware

Cryptography and Cryptography Attacks

Module 08 – Secrity Operation & SIEM

SOC roles and responsibilities

Security Information and Event Management (SIEM) basics

SIEM Tools Introduction (Wazuh, Splunk, IBM QRadar)

Windows & Linux Logs Analysis

IDS/IPS, Firewall, Router, Web Servers Log Analysis

Exploring the Power of Splunk

Splunk Use Cases

Module 09 – Nework and EndPoint Security

Network Traffic Analysis With Wireshark

Configuring IDS/IPS for Network Security

Configuring Snort IDS with Splunk to Enhance Network Security

Incident lifecycle and Playbooks

Incident Detection with SIEM

Incident Response of Cyber Attacks

Module 10 – Threat Intelligence

Threat Intelligence Platforms and Techinques

Indicator of Compromise and Incidator of Attacks

Online Threat Intelligence Tools