OSCP AND OSCP+

1. Module: Introduction to Ethical Hacking

- Information security
- CIA Triad, Security Standards
- IT laws and Rules
- Deep web and Dark web
- Deep fake Threat
- Penetration Testing Methodology

2. Module: Getting Comfortable with kali Linux

- Introduction to Kali Linux
- Setting up the Virtualization environment
- Kali Linux Installation
- Linux special commands for Penetration Testing

3. Module: Information Gathering

- Collect information on target URL
- Making and Analysis of OSIENT report on target URL
- Gathering information on Websites and IP addresses

3.1. Active Information Gathering

- Collect information using Automated Tools
- Foot printing through Social Engineering
- Network Foot printing

3.2. Passive Information Gathering

- Collect information through Automated Tools
- Collect information through Automated Tools
- Domain Recon Technique
- Email Recon Technique
- Whois Foot printing
- Google Hacking dB
- Netcraft, Shodan, Censys.io, crt.sh, fullhunt.io etc.

4. Module: In-Depth Scanning

- Introduction to Scanning
- Network Scanning Concepts
- Host Discovery
- Scanning for Open Ports and Services
- Scanning Tools (Windows based tool and Linux based tool)
- Performing Port Scanning - Nmap
- Collect information about Network like, active machines, active services, Operating Systems, and we cover tools like Nmap, Hping3, angryip-scanner, MSF, Recon-ng, and Katana etc.

5. Module: Exploitation and Enumeration

- Collecting information about Active Machines and target
- Searching for exploits online and offline
- SNMP Enumeration
- SMTP Enumeration
- LDAP Enumeration
- FTP Enumeration
- SSH Enumeration
- Telnet Enumeration
- HTTP Enumeration
- VNC Enumeration
- SNMP Enumeration
- MYSQL Enumeration
- Load Balancer Detector

6. Module: Metasploit Framework

- Introduction of Metasploit Framework
- Exploring Metasploit Framework
- The CLI Interface
- Meterpreter shell
- Searching exploits
- Exploiting vulnerabilities
- In this module, we use auxiliary modules, payloads, scripts and post-exploitation module etc.

7. Module: Vulnerability Scanning

- Introduction of Metasploit Framework
- Introduction of Vulnerability
- Bug and Payload
- Vulnerability Assessment Concepts
- Vulnerability Classification and Assessment
- Vulnerability Scoring System
- Tool for Vulnerability Scanning
- WPScan , Acunetix, Nessus
- Qualys, Crashtest, Nikto, MSF-Pro, NSE Script, Pentest toolbox etc.
- Exploring Exploit Database
- Vulnerability Assessment Reports

8. Module: Web Application Vulnerabilities

- Introduction of Web Architecture
- Reconnaissance of web Application and server with tools
- Technology Analyses with Wappalyzer , Netcraft etc.
- Directory Busting with Gobuster, Dirbuster etc.
- Directory Traversal
- Exploiting Absolute Path and Relative Path
- File Inclusion
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- File Upload Vulnerabilities
- Command Injection
- Broken Authentication
- Broken Access Control
- Cross-Site Scripting (XSS)
- Basic XSS
- Stored and Reflected XSS
- IDOR- Insecure Direct Object Reference
- Testing on live website
- Solving Web Based CTFs

9. Module: SQL Injection Attack

- Introduction of SQL and Database
- Understand SQL queries
- Authentication Bypass using SQLi
- Manual Testing on live website
- Types 0f SQL Injection
- Error-based SQL injection
- UNION-based SQL Injection
- Blind SQL Injection
- Time-based SQL Injection

10. Module: Client Side Attack

- Introduction of Client Side Attack
- Social Engineering
- Exploring techniques different type of attack like
  Phishing web-pages, Mirroring websites, Client Fingerprinting .etc.

11. Module: Password Attacks

- Encryption, Hashing and Encoding
- Cracking and Passing NTLM Password,
- Attack on SSH and RDP port
- Using Encryption, Calculate Hashes and Cracking.
- Exploring tools like John The Ripper, Hashcat, Hydra, NCrack & Medusa

12. Module: Fixing Exploits

- Fixing Memory Corruption Exploits
- Troubleshooting the “index out of range” Error
- Fixing Web Exploits

13. Module: Locating Public Exploits

- Online Exploits Method
- Manual Exploits Method

14. Module: Antivirus Evasion and Anti-Virus Bypass

- Introduction of Antivirus
- Antivirus Working Process
- Antivirus key Components
- Antivirus Thread Injection
- Bypass Antivirus and Hack Remote Windows PC.
- Exploring tool Nim

15. Module: Windows Privilege Escalation

- Introduction of Windows Privilege Escalation
- Enumerating Windows
- Understanding of Kernel
- Windows Kernel Exploitation
- Enumerating Kernel details
- User Account Privilege
- Enumerating Windows using Automated Scripts
- RCE
- Tool: - BeRoot, Seatbelt, WindowsEnum etc.

16. Module: Linux Privilege Escalation

- Introduction of Linux Privilege Escalation
- Enumerating Linux
- Exposed Confidential Information
- Exploit Password Authentication
- Enumerating Linux OS using Automated Scripts
- Root Account Privilege
- User Account Privilege
- Exploiting RCE

17. Module: Active Directory Attacks

- Introduction of Active Directory concept
- Lab setup for AD
- Enumerate Active Directory
- Analyze domain data using Bloodhound
- Kerberos attack

- Pass the Hash using Mimi Katz
- NTLM Attack etc.

18. Module: Port Redirection and SSH Tunneling

- Introduction of Port forwarding
- SSH Tunneling
- HTTP Tunneling
- Tunneling Through Deep Packet Analysis
- Bind port 22 on port 80 and then used tool like MobaXterm, Putty, Chisel etc.

19. Module: Assembling the Pieces

- Enumerating the Public Network
- Exploit Internal Network
- Attacking on Internal Application
- Relay attack on web Plugin
- Privilege access of the Domain Controller

20. Module: AI and ML

- Introduction of AI and ML
- Types of AI
- Types of ML
- Area of AI
- AI and ML Concepts

21. Module: AI and ML in Cyber Security

- Role of AI and ML in Cyber Security
- AI and ML Prevent Cyber Attack
- AI-based Security
- 30+ AI tool used in Cyber Security
- AI for Defensive and Offensive Mode

Note: -

- CTF Practice on TryHackMe, HackTheBox and Vulnhub.
- Report Making: - VAPT, OSIENT (Optional)

- Linux Playground (Optional)
- Windows Playground (Optional)