Network Penetration Testing

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: Information Gathering

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

2.1. Active Information Gathering

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

2.2. 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.

3. 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.

4. 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

5. Module: Metasploit Framework

- Introduction of Metasploit Framework
- Exploring Metasploit Framework
- The CLI Interface
- Meterpreter shell
- Searching exploits
- Exploiting vulnerabilities
- Auxiliary Modules, Payloads, Scripts
- Use for Post-exploitation

6. 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
- Acunetix, Nessus
- Qualys, Crashtest, Nikto, MSF-Pro, NSE Script, Pentest toolbox etc.
- Exploring Exploit Database
- Vulnerability Assessment Reports

7. Module: Sniffing & MITM Attack

- Introduction of Sniffing
- Type of Sniffing
- Sniffing Tools
- DNS Spoofing
- SSL Pinging
- DHCP and MAC Flooding Attacks
- MAC and ARP Attacks
- Sniffing Tools
- Ettercap ,Better cap and Wireshark
- Sniffing Detection Techniques

8. Module: Buffer Overflows Attack

- Introduction of Buffer Overflow
- Concept of Buffer Overflow
- Types of Buffer Overflow
- Shellcode
- Identify a vulnerable program
- Fuzz input to crash the program
- Control EIP/RIP
- Inject shellcode or ROP chain
- Gain shell or desired control
- Windows buffer overflow exploits
- Debugging and stack inspection
- Shellcode generation through Msfvenom
- Tool :- GDB, Immunity Debugger, Pattern create/offset, msfvenom, Objdump

9. 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

10. Module: Fixing Exploits

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

11. Module: Locating Public Exploits

- Online Exploits Method
- Manual Exploits Method

12. Module: Firewall and IDS Evasion Techniques

- Introduction of Firewall
- Types of Firewall
- Working Process of Firewall
- IDS and IPS
- Working Process of IDS and IPS
- Set Firewall Rules in windows
- Set Firewall Rules in Linux
- Firewall Fragmentation
- ICMP and HTTP Tunneling
- Tool :- Nmap, hping3, fragroute, Scapy , Veil, obfuscation.io , iodine, dnscat2, ptunnel, etc.

13. 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

14. Module: Power Shell Empire

- Introduction of Power Shell Empire
- Setup and Installation in Linux
- Creating a Listener and set Target IP Address
- File Transfer in Empire
- Privilege access through Power Shell Empire

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 (Remote Code Execution)
- 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 Tunneling Exploits

- Introduction of Port forwarding
- Types of Port Forwarding
- Used Port Forwarding Tool
- DNS Tunneling
- ICMP Tunneling
- SSH Tunneling
- HTTP Tunneling
- Tunneling Through Deep Packet Analysis
- VPN Configurations
- Bind port 22 on port 80 and then used tool like MobaXterm, Putty, Chisel etc.

19. Module: AI and ML

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

20. 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 , NPT (Optional)
- Linux Playground (Optional)
- Windows Playground (Optional)
- Wireless Penetration Testing (Optional)