ISOEH
Indian School Of Ethical Hacking
www.isoeh.com

Network Penetration Testing Level I Syllabus

Module 1: Introduction to Network Penetration Testing *2 Hours - 4 Topics*

- Purpose and Scope of Penetration Testing *(Day 1)*
- Penetration Testing Methodologies *(Day 1)*
- Legal and Ethical Considerations *(Day 1)*
- Reporting and Documentation *(Day 1)*

Module 2: Lab Setup for Penetration Testing *2 Hours - 4 Topics*

- Setting Up Virtualization Environments (e.g., VMware, VirtualBox) *(Day 2)*
- Creating and Configuring Network Segments *(Day 2)*
- Deploying Target Machines (e.g., Windows, Linux) *(Day 2)*
- Tools Installation and Configuration *(Day 2)*

Module 3: SNMP Enumeration Techniques *2 Hours - 4 Topics*

- Understanding SNMP Versions (SNMPv1, SNMPv2c, SNMPv3) *(Day 3)*
- SNMP Walk and SNMP Get Methods *(Day 3)*
- Community String Guessing *(Day 3)*
- MIB (Management Information Base) Analysis *(Day 3)*

Module 4: SNMP Exploitation Methods *2 Hours - 2 Topics*

- SNMP Community String Attack (e.g., SNMP Dictionary Attack) *(Day 4)*
- Exploiting Vulnerable SNMP Services *(Day 4)*

Module 5: Network Protocol Brute Force Attacks *2 Hours - 4 Topics*

- Introduction to Brute Forcing *(Day 5)*
- Tools for Protocol Brute Forcing *(Day 5)*
- HTTP Basic/Digest Authentication Brute Forcing *(Day 5)*
- SSH/FTP/Telnet Brute Force Attacks *(Day 5)*

Module 6: HTTP Tunneling Techniques *2 Hours – 4 Topics*

- Understanding HTTP Tunneling Concepts *(Day 6)*
- Tools for HTTP Tunneling *(Day 6)*
- Using HTTP Tunneling for Data Exfiltration *(Day 6)*
- Evading Firewalls and IDS/IPS with HTTP Tunneling *(Day 6)*

Module 7: All Ports Attack Strategies *2 Hours - 4 Topics*

- Port Scanning Techniques (e.g., TCP Connect Scan, SYN Scan) *(Day 7)*
- Full Port Scanning vs. Top Ports Scanning *(Day 7)*
- Service Version Detection *(Day 7)*
- Firewall Evasion Techniques *(Day 7)*

Module 8: DLL Hijacking Exploitation *2 Hours - 4 Topics*

- Understanding DLL Search Order Hijacking *(Day 8)*
- Identifying DLL Hijacking Vulnerabilities *(Day 8)*
- Exploiting Applications with DLL Hijacking *(Day 8)*
- Mitigating DLL Hijacking Attacks *(Day 8)*

Module 9: NetBIOS and SMB Enumeration Methods *2 Hours - 4 Topics*

- Introduction to NetBIOS and SMB Protocols *(Day 9)*
- Enumerating NetBIOS Information (e.g., nbtstat, smbclient) *(Day 9)*
- SMB Version Detection and Enumeration *(Day 9)*
- Extracting User and Share Information *(Day 9)*

Module 10: SMB and NFS Enumeration Techniques *2 Hours - 4 Topics*

- Enumerating SMB Shares (e.g., smbclient, smbmap) *(Day 10)*
- NFS Enumeration (showmount, nfsstat) *(Day 10)*
- Finding Vulnerabilities in SMB and NFS Implementations *(Day 10)*
- Accessing and Interacting with Shared Resources *(Day 10)*

Module 11: Windows Privilege Escalation (Level 1) *2 Hours - 4 Topics*

- Basic Privilege Escalation Techniques *(Day 11)*
- Exploiting Unquoted Service Paths *(Day 11)*
- DLL Hijacking for Privilege Escalation *(Day 11)*
- Exploiting Weak Registry Permissions *(Day 11)*

Module 12: Post Exploitation Techniques *2 Hours - 3 Topics*

- Maintaining Access After Exploitation *(Day 12)*
- File System Navigation and Data Extraction *(Day 12)*
- Privilege Escalation Beyond Initial Access *(Day 12)*

Module 13: Linux Privilege Escalation (Level 1) *2 Hours - 4 Topics*

- Basic Linux Privilege Escalation Techniques *(Day 13)*
- Exploiting Weak File Permissions *(Day 13)*
- Exploiting Shell Escape Vulnerabilities *(Day 13)*
- Exploiting Cron Jobs and Weak File Permissions *(Day 13)*

Module 14: Continued Linux Privilege Escalation (Level 1) *2 Hours - 4 Topics*

- Advanced Linux Privilege Escalation Techniques *(Day 14)*
- Exploiting Capabilities and Kernel Vulnerabilities *(Day 14)*
- Exploiting Sudo Misconfigurations *(Day 14)*
- Exploiting SUID/GUID Binaries *(Day 14)*

Module 15: Covering Tracks after Penetration *2 Hours - 4 Topics*

- Removing Evidence of Compromise (EOC) *(Day 15)*
- Modifying Logs and Timestamps *(Day 15)*
- Deleting Backdoors and Persistence Mechanisms *(Day 15)*
- Techniques to Evade Forensic Analysis *(Day 15)*

Module 16: Pivoting Techniques (Level 1) *2 Hours - 4 Topics*

- Introduction to Pivoting in Penetration Testing *(Day 16)*
- Using Proxychains and SSH Tunnels for Pivoting *(Day 16)*
- Port Forwarding Techniques *(Day 16)*
- Exploiting Internal Network Vulnerabilities from Compromised Hosts *(Day 16)*

Module 17: Post Exploitation Techniques Cont.. *2 Hours - 4 Topics*

- Introduction to Mimikatz *(Day 17)*
- File Transfer *(Day 17)*
- Introduction to PowerShell *(Day 17)*
- WMIC *(Day 17)*

Module 18: Lab Solve 1 - Simple Pivoting *2 Hour*

Module 19: Lab Solve 2 – VULNIX *2 Hours*

Module 20: Lab Solve 3 - Network-Based Lab *2 Hours*