ISOEH
Indian School Of Ethical Hacking
www.isoeh.com

Network Penetration Testing Level II Syllabus

Module 1: Active Directory Basics *2 Hours - 5 Topics*

- Introduction to Active Directory (AD) *(Day 1)*
- AD Architecture and Components *(Day 1)*
- AD Access control lists and types of authentications used *(Day 1)*
- Understanding Kerberos Ticketing System *(Day 1)*
- User and Group Management in AD *(Day 1)*

Module 2: Introduction to Powershell *2 Hours*

Module 3: Practical Setup of Active Directory *2 Hours - 4 Topics*

- Installing and Configuring Windows Server for AD *(Day 3)*
- Setting up Domain Controllers *(Day 3)*
- Creating and Managing Domains and Trusts *(Day 3)*
- Group Policy Objects (GPOs) in AD *(Day 3)*

Module 4: AD Enumeration pre-attack *2 Hours - 4 Topics*

- Introduction to LDAP (Lightweight Directory Access Protocol) *(Day 4)*
- LDAP Data Interchange Format (LDIF) *(Day 4)*
- Enumerating AD Using enum4linux, crackmapexec *(Day 4)*
- Enumerating AD users pre-attack *(Day 4)*

Module 5: Responder and Hash Capture *2 Hours - 5 Topics*

- Introduction to Responder for Capturing Hashes *(Day 5)*
- Setting Up and Using Responder in Penetration Tests *(Day 5)*
- Exploiting NetBIOS and LLMNR to Capture Hashes *(Day 5)*
- Pass-the-Hash Attacks and Defense Mechanisms *(Day 5)*
- Exploiting AD Misconfigurations for initial access *(Day 5)*

Module 6: AD Enumeration post-attack *2 Hours – 2 Topics*

- Reconnaissance Techniques for AD *(Day 6)*
- AD Enumeration (Users, Computers, Domain, Forests, DC, ACL, SPN, Special Permissions) using PowerView and Bloodhound *(Day 6)*

Module 7: Post-Initial Access exploitation and Privilege Escalation Techniques-1 *2 Hours - 4 Topics*

- Privilege Escalation Techniques in AD Environments *(Day 7)*
- Data Exfiltration Techniques and Credential Dumping techniques *(Day 7)*
- Password spray, Overpass the hash attacks *(Day 7)*
- DCSync, Kerberoasting, ASREPRoasting *(Day 7)*

Module 8: Post-Initial Access exploitation and Privilege Escalation Techniques-2 *2 Hours - 1 Topic*

- DCSync, Kerberoasting, ASREPRoasting *(Day 8)*

Module 9: Persistence and Maintaining *2 Hours - 3 Topics*

- Generating and Using Golden Tickets post exploitation *(Day 9)*
- Creating and Using Silver Tickets post exploitation *(Day 9)*
- Mitigating Golden/Silver Ticket Attacks *(Day 9)*

Module 10: Advanced Pivoting through Tunnelling *2 Hours - 3 Topics*

- Using SSH Tunnels for Pivoting *(Day 10)*
- Proxy Chains and Multi-Hop Tunnelling *(Day 10)*
- Advanced Local Port Forwarding, Remote Port Forwarding *(Day 10)*

Module 11: Windows Privilege Escalation *2 Hours - 4 Topics*

- Local Privilege Escalation Techniques *(Day 11)*
- Exploiting Service Permissions and Weaknesses *(Day 11)*
- Kernel Exploits and DLL Hijacking *(Day 11)*
- Hunting for Credentials in Memory *(Day 11)*

Module 12: Buffer Overflow Concepts and Fuzzing *2 Hours - 4 Topics*

- Understanding Buffer Overflows *(Day 12)*
- Fuzzing Techniques for Vulnerability Discovery *(Day 12)*
- Crafting Exploits for Buffer Overflows *(Day 12)*
- Mitigations and Countermeasures *(Day 12)*

Module 13: Practical Buffer Overflow *2 Hours - 4 Topics*

- Setting up a Lab Environment for Buffer Overflow Exploitation *(Day 13)*
- Exploiting Buffer Overflow in Real-world Applications *(Day 13)*
- Shellcode Development and Execution *(Day 13)*
- Exploit Payload Customization *(Day 13)*

Module 14: Introduction to Docker Penetration Testing *2 Hours - 4 Topics*

- Setup of Docker Penetration Testing Lab *(Day 14)*

- Container Enumeration *(Day 14)*
- Exploiting Docker container for Initial Access *(Day 14)*
- Linux Capability Exploitation *(Day 14)*

Module 15: Red Team Exercises and Simulation *2 Hours - 4 Topics*

- Planning and Executing Red Team Engagements (MITRE framework) *(Day 15)*
- Advanced TTPs (Tactics, Techniques, and Procedures) *(Day 15)*
- Collaborative Red Team Tools: Empire *(Day 15)*
- Adversary Simulation and Threat Intelligence Integration *(Day 15)*

Module 16: Capture The Flag (CTF) PART 1 *2 Hours - 2 Topics*

- Practical Challenges in Exploitation and Defences *(Day 16)*
- Real-world Scenarios and Hands-on Exercises *(Day 16)*

Module 17: Capture The Flag (CTF) PART 2 *2 Hours*

Module 18: Report Writing *2 Hour - 4 Topics*

- Writing Comprehensive Penetration Testing Reports *(Day 18)*
- CVE and Risk Assessment *(Day 18)*
- Executive Summary and Technical Details *(Day 18)*
- Mitigation Recommendations and Roadmap *(Day 18)*

Module 19: Final CTF Challenge *2 Hours*

Module 20: Assignment *2 Hours - 2 Topics*

- Individual or Group Assignment on Advanced Topics in Network Penetration Testing *(Day 20)*
- Project Presentation *(Day 20)*