PENTESTING INFRASTRUCTURE

Infrastructure Penetration Testing **15 hours of content | 110 hours of practice | Final Project**

1. Setting Up Lab Environment

- Virtualization with VirtualBox
- Loading Kali Linux
- Loading Windows
- Loading Metasploitable2

2. Introduction to Penetration Testing

- Terminology in the Attack World
- Types of Infrastructure Tests
- Scanning and Vulnerability Identification Processes
- Gaining Control and Its Importance
- Persistence on a Compromised Machine

3. Fundamentals of Attacks

- Implementing Reverse Shell Communication
- Implementing Bind Shell Communication
- Listening on TCP/UDP Protocols
- File Transfer with Netcat
- Basic Scans with Netcat
- Introduction to Wireshark
- Filters in Wireshark
- Extracting Information from PCAP Files

4. Passive and Active Information Gathering

- Google Dorks
- Gathering and Identifying Email Addresses
- Passive Information Gathering (Open Source)
- DNS Enumeration
- Communication with DNS Servers
- Research Tools for DNS Servers
- DNS Forward Lookup
- DNS Reverse Lookup

5. Port Scanning

- Three-Way Handshake and TCP Communication
- UDP Scans
- Common Mistakes in Port Scanning
- Port Scanning with NMAP
- Advanced NMAP Scans (NMAP NSE)
- Firewall Evasion
- Operating System Detection
- Service Enumeration

6. Introduction to and Working with Metasploit

- Introduction to Metasploit
- Modules in Metasploit
- Introduction to Payloads
- Introduction to Auxiliaries
- Introduction to Exploits
- FTP Attack with RCE Vulnerability
- SMB Windows Brute Force
- Hydra Brute Force
- Password Profiles
- Enumeration Tactics
- Shellcode Injection
- Process Migration
- Attacks on WordPress & Drupal
- LFI/RFI (Local/Remote File Inclusion)
- Log Injections
- Environment & Fuzzing
- Remote Code Execution
- Command Injections
- Trojans with Msfvenom
- Control with Meterpreter
- Tomcat
- Backdooring
- Advanced Meterpreter
- Keylogging
- Download/Upload Functions
- SMTP Enumeration

7. File Transfer

- File Transfer using Python
- File Transfer in Windows via PowerShell
- File Transfer between Windows and Linux via FTP
- File Transfer using SMB Server
- Additional Methods for File Transfer

8. Windows Privilege Escalation

- UAC Bypass - User Interaction
- UAC Bypass - No User Interaction
- PE Suggester
- Patch enumeration
- Unquoted Path
- Insecure Service
- Zero Click PE

9. Linux Privilege Escalation

- Basic Enumerations
- Kernel Exploits
- suid Exploitation
- Sudo Abuse
- Word Writable
- CronTab PE
- Sensitive Files
- Http Methods

10. Vulnerability Research

- Introduction to x86
- Understanding Memory Processes
- Binary Memory
- CPU Registers
- Buffer Overflow Introduction
- OlyDBG Introduction
- Overflowing the Buffer
- Fuzzing
- Dealing with Crashes
- EIP Control
- Shellcode Space Locating
- Bad Characters
- Execution Flow Redirection
- Return Address
- Shellcoding with Metasploit
- Getting a Shell

11. Passwords

- Challenge-Response Authentication
- LM/NTLM Hashing
- SAM
- Password Flow
- Mimikatz
- Hash Extraction with SamDump
- Hash Extraction with SecretDump
- SecretDump Remoting
- Password Cracking with Hashcat/John
- Pass the Hash
- Responder & LLMNR Introduction
- Responder to Capture NTLMv2