Windows Privilege Escalation | 2 hours of content | 20 hours of practice | Final project

1. Introduction & Lab Setup

- Windows 10
- Kali Linux
- Groups & Members in Windows
- ACL's, Services, Registry, Directories

2. Must Known Tools

- PowerUP
- SharpUP
- SeatBelt
- winPEAS
- Accesschk
- JuicyPotato
- Procmon

3. Spawn a shell & Kernel Exploits

- Reverse Shell Over MSFvenom
- Netcat
- Psexec to System
- Manual Kernel Enumeration
- Automatic Kernel Enumeration

4. Service Exploits

- Insecure Properties - Enumeration & Exploitation
- Unquoted Path - Enumeration & Exploitation
- Weak Registry Permissions - Enumeration & Exploitation
- Insecure Service Executables - Enumeration & Exploitation
- DLL Hijacking

5. Registry Exploits

- Manual Registry Enumeration
- Automatic Registry Enumeration
- Registry Exploitation
- Query Registry Services
- Manual AIE Enumeration
- Automatic AIE Enumeration
- AIE Exploitation

6. Passwords

- Manual Password Enumeration
- Automatic Password Enumeration
- Query Registry Passwords Store
- Saved Creds Manual & Auto Enumeration
- Configurations Files
- Recursive Configuration Files
- SAM & System Locations
- SAM & System Hash Dump
- SAM & System Hash Crack
- PTH-Wineex

7. Scheduled Tasks

- Manual Scheduled Tasks Enumeration
- Scheduled Tasks Exploitation

8. Insecure GUI Apps

- Insecure GUI Apps Enumeration
- Insecure GUI Apps Exploitation
- Startup Apps Enumeration
- Startup Apps Exploitation

9. Insecure GUI Apps

- Insecure GUI Apps Enumeration
- Insecure GUI Apps Exploitation
- Startup Apps Enumeration
- Startup Apps Exploitation
- Vulnerability Research WAN
- Vulnerability Research winPEAS