EC-Council Advanced Penetration Testing: LPT (Master)

Course Details

Course Outline

1. **Introduction to Vulnerability Assessment and Penetration Testing**
    - Review of vulnerability assessment
    - Types of vulnerability scanners
    - Challenges faced by vulnerability scanners
    - Creating a Security Testing Plan
    - Explaining the Hacking Methodology
    - Concepts of Evasion
2. **Information Gathering Methodology**
    - Information Gathering with NSLOOKUP and Dig
    - DNS Enumeration with dnsenum and dnsrecon
    - Enumeration with fierce
    - Creating a Security Testing Plan
    - Registrars and Whois
    - Google Hacking Database
    - Enumeration with Metagoofil
    - Cloud Scanning with Shodan
3. **Scanning and Enumeration**
    - Scanning with Nmap
    - Scanning with the Tool Dmitry
    - Scanning with the Tool Netdiscover
    - Scanning with the Tool sslscan
    - Scanning and Scripting with the Tool hping3
    - Scanning the Internet
    - Using Metasploit Databases and Workspaces
    - Enumeration of Targets
    - Mastering the Nmap Scripting Engine

4. **Identify Vulnerabilities**
    - Vulnerability Sites
    - Vulnerability Analysis with OpenVAS
    - Web Application Vulnerability Scanners
    - Customizing and Optimizing Scan Policies
    - Web Vulnerability Scanning within Metasploit
    - Analysis of Vulnerability Findings
    - Custom Script Design
5. **Exploitation**
    - Exploit Sites
    - Manual Exploitation
    - Exploitation with Metasploit
    - Searching for Exploits
    - Remote Exploitations with SMB, RDP and SSH
    - Web Application Exploitation
    - Customization of Shells
    - Staged and Stageless Payloads
    - Custom Exploits
6. **Post Exploitation**
    - Disabling protections
    - Local Assessment
    - Harvesting Information
    - Scripts for pilfering
    - Leveraging backdoors
    - Mangling log files
    - Escalation of privileges
    - Data search and extraction techniques
    - Achieving an advanced shell
    - File transfers
7. **Advanced Tips and Techniques**
    - Scanning with Nmap against Defenses
    - Session routing

- Performing pivoting
- Executing a double pivot
- Custom payloads for network traversal
- Using proxies
- Leveraging web shells
- Custom web shells to avoid detection

8. Preparing a Report

- Importance of a report
- Avoiding the common mistakes
- Compiling data in Magic Tree
- Designing the report structure
- Essential report components