Offensive Hacking Cookbook Curriculum

1. Course Introduction

- Intro
- Whoami
- Why this course ?
- What you will learn here ?
- Pre-requisites & requirement

---

2. Note taking and Learning

- Notetaking process (including Screenshots)
- Reading vs Visual learning
- Learn in Public
- Assignment, Quizzes & Labs
- Course Discord

---

3. Networking Refresher

- IP addresses
- MAC addresses
- Client-Server Model
- DNS
- TCP VS UDP and Three-way handshake
- Common Ports & Protocols
- OSI Model and TCP/IP Model
- How Web Works ?
- Subnetting

---

4. Linux Refresher

- Installing Kali Linux on Vmware & Virtual Box.
- Kali Linux Overview
- Sudo Overview
- Navigating the File System
- File & Directory permissions
- Users & privileges
- Viewing, Creating and Editing Files
- grep and piping
- Finding files in Linux
- Enumerating Distribution & Kernel Information
- Shells & Bash configuration
- Disk Usage
- Networking
- File compression in linux
- Service & Process Management
- Installing software & tools
- Useful Keyboard Shortcuts
- Using TOR & Proxychains

---

5. Cybersecurity Principles

- Understanding Threats & Threat Actors
- The CIA Triad
- The Cyber Kill Chain
- Security Principles
- Threat Modelling and Threat Intelligence
- Information Security Laws & Standards
- The Ethical Hacking Methodology

---

6. Information Gathering (Reconnaissance)

L1 Recon

- Introduction to Reconnaissance
- Identifying our Target

- Whois Records
- Google Dorking
- Company OSINT
- Web Archives
- Identifying Website Technologies
- Discovering Email addresses -
- Hunting breached credentials
- Hunting for subdomains
- Open Source code reconnaissance
- Security Headers and SSL/TLS testing
- Banner grabbing and Firewall Detection
- Finding IP address behind Cloudfare
- Shodan, Zoomeye and Censys
- Enumeration with Carbon Dating
- Android Apps Enumeration
- Utilizing Social Media
- Information Gathering with black widow

L2 Recon

- DNS recon using host, nslookup and dig
- DNS Zone Transfer
- Historical DNS records
- DNS Brute forcing and subdomain enumeration
- Finding and enumerating ASN

L3 Recon

- Finding Cloud resources
- Filtering live hosts and domains
- Finding Hidden parameters and endpoints
- Automating the Reconnaissance

---

7. Active Reconnaissance

- Introduction to Active Reconnaissance
- Installing Metasploitable

- Host discovery with netdiscover
- Host discovery with nmap
- Port scanning with nmap
- Service Fingerpriting
- OS Fingerprinting
- Scanning beyond Firewall & IDS
- Optimizing your scans
- Port Scanning in Windows
- Scanning with masscan
- Scanning with Rustscan
- Directory Bruteforcing

---

8. Enumeration

- Introduction to Enumeration
- FTP Enumeration
- Telnet Enumeration
- SSH Enumeration
- NetBIOS Enumeration
- SMB Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP Enumeration
- NFS Enumeration
- SMTP Enumeration
- IMAP Enumeration
- POP Enumeration
- MYSQL Enumeration
- TFTP Enumeration
- IPSec Enumeration

---

9. Vulnerability Scanning

- Introduction to Vulnerability Scanning

- Vulnerability Classification
- Vulnerability assessments
- Vulnerability Scanning with nikto
- Vulnerability Scanning with nmap
- Vulnerability Scanning with Nessus
- Vulnerability Scanning with OpenVAS
- The Zero days

---

10. Exploitation (Popping Shellz)

- Introduction to Exploitation
- Reverse Shells vs Bind Shells
- Staged vs Non-staged payloads
- All about Malwares
- Default Passwords attacks
- Bruteforce Attacks
- Credential Stuffing & Password Spraying
- Gaining Access with Metasploit
- Locating Public Exploits
- Fixing Public Exploits
- Manual Exploitation

---

11. The Metasploit Framework

- Metasploit Framework Overview
- Setting up the working environment
- Auxiliary Modules
- Exploit Modules
- Post, Nops and encoders Modules
- Meterpreter Payloads
- Creating payloads with msfvenom
- Hacking Windows XP with Metasploit
- Hacking Windows 7 with Metasploit
- Hacking Windows 10 with Metasploit

- Hacking Windows remotely over WAN
- Adding a new exploit
- Resource scripts

---

12. Client Side Attacks

- Introduction to Client Side Attacks
- Performing Target Recon
- Exploitation with Office Macros
- Exploitation with HTA attack
- The Browser Exploitation Framework (BeEF)

---

13. Antivirus & EDR Evasion

- Introduction to Antivirus & EDR Evasion
- How AV Detection Works ?
- AV Evasion Concepts
- AV Evasion with Shellter
- AV Evasion with Scarecrow

---

14. Getting hands dirty

- THM - Agent T Walkthrough
- THM - Bolt CMS Walkthrough
- THM - Blue Walkthrough
- THM - Blueprint Walkthrough
- PG - Stapler Walkthrough
- PG - Monitoring Walkthrough
- HTB - Crocodile Walkthrough
- Vulnhub - Kioptrix Walkthrough
