CWL
CyberWarFare Labs

Certified Cyber Security Engineer (CCSE)

@CyberWarFare Labs

I. Introduction to Penetration testing

1.1 What is Penetration testing?

1.2 Penetration Testing Market Overview

1.3 Why CCSE?

1.4 CCSE Modules:

- 1.4.1 Scripting / Programming
- 1.4.2 Open Source Intelligence (OSINT)
- 1.4.3 Phishing
- 1.4.4Web Application Exploitation
- 1.4.5 Network Exploitation
- 1.4.6 Operating System Exploitation

I. Introduction to Penetration testing

- 1.4.7 Exploit Development
- 1.4.8 Cloud Penetration Testing
- 1.4.9 Docker Container Penetration Testing
- 1.4.10 Mobile Application Security
- 1.4.11 Wi-Fi Security

1.5 Penetration Testing Prerequisite

1.6 Penetration Testing Life Cycle (Phases)

1.7 Technical Penetration Testing Report

II. Environment Setup for Lab Access

2.1 Virtualization platform

2.2 Pentesting OS

2.3 CCSE practise lab

III. Scripting / Programming

3.1 Bash, Python

- 3.1.1 IP Geo Tracking
- 3.1.2 Network Scanner
- 3.1.3 Mass Vulnerability Scanner
- 3.1.4 Practical exercise

3.2 C/C++

- 3.2.1 Wifi Credential Extraction

IV. Open-Source Intelligence

4.1 Google Dorking
4.2 Pillaging Credentials in Open-Source Repositories
4.3 Publicly Exposed Cloud Services
4.4 Social Media
4.5 Email Extraction
4.6 Metadata discovery
4.7 Domain recon
4.8 Advanced OSINT
4.9 OSINT Methodology

V. Phishing

5.1 Phishing tests

5.2 Phishing Infrastructure Setup

5.2.1 SMTP Setup

5.2.2 GoPhish

5.3 Landing pages & email templates

5.4 Executing Phishing Campaigns

5.5 Analysis & Reporting

VI. Web Application Exploitation

6.1 Introduction

6.2 Tools

6.3 Server Side Vulnerabilities

- 6.3.1 SSRF
- 6.3.2 XXE
- 6.3.3 SSTi
- 6.3.4 File Inclusion
- 6.3.5 SQLi / No SQLi
- 6.3.6 RCE
- 6.3.7 API Misconfigs
- 6.3.8 OAuth Misconfigs

VI. Web Application Exploitation

- 6.4 Client Side Vulnerabilities
  - 6.4.1 XSS
  - 6.4.2 CSRF
- 6.5 Case Study (Chained Vulnerabilities)
- 6.6 OAuth
  - 6.6.1 Introduction
  - 6.6.2 OAuth Mis-configurations
- 6.7 API
  - 6.7.1 Introduction
  - 6.7.2 API Mis-configurations

VII. Network Exploitation

- 7.1 Network Pentesting Methodology
- 7.2 Information Gathering
  - 7.2.1 Passive
    - 7.2.1.1 OWASP Amass
    - 7.2.1.2 FOCA
  - 7.2.2 Active
    - 7.2.2.1 Nmap Host Discovery & Reporting
    - 7.2.2.2 Nmap Vulnerability Discovery & Reporting

VII. Network Exploitation

7.3 Attacking Network Components

7.3.1 Services & it's exploitation:

7.3.1.1 SSH

7.3.1.2 SMB

7.3.1.3 SNMP

7.3.1.4 RDP

7.3.1.5 FTP / SFTP

7.3.1.6 SMTP

7.3.1.7 WinRM

7.3.1.8 LDAP

VII. Network Exploitation

7.4 Network Pivoting

7.4.1 Tunnelling

7.4.1.1 Forward

7.4.1.2 Reverse

7.5 Case Study

VIII. Operating System Exploitation

- 8.1 Windows Privilege Escalation
    - 8.1.1 Sensitive Information Discovery
        - 8.1.1.1 PowerShell History
        - 8.1.1.2 3rd Party Application Cache
    - 8.1.2 Methods
        - 8.1.2.1 Full Permission over a Service
        - 8.1.2.2 Full Permission over a Folder associated with a Service (DLL Hijacking)
        - 8.1.2.3 Unquoted Service Path
- 8.2 Windows Credential Dumping
    - 8.2.1 Privileges
    - 8.2.2 SAM
    - 8.2.3 LSA

VIII. Operating System Exploitation

8.3 Windows Credential Cracking

- 8.3.1 NT/LM Hash
- 8.3.2 Net-NTLM v2 Hash
- 8.3.3 MSV2 Hash

8.4 Windows Persistence

- 8.4.1 Exclusion
- 8.4.2 Disable
- 8.4.3 Startup
- 8.4.4 Schedule Tasks
- 8.4.5 Malicious Service
- 8.4.6 Always Install Elevated

VIII. Operating System Exploitation

8.5 Windows Data Exfiltration
- 8.5.1 Python pyftpdlib
- 8.5.2 SMB Server
- 8.5.3 Socat

8.6 Linux Privilege Escalation
- 8.6.1 Sensitive Information Discovery
  - 8.6.1.1 Application logs
  - 8.6.1.2 Bash history
  - 8.6.1.3 3rd party application cache
- 8.6.2 Methods
  - 8.6.2.1 SUID Bit
  - 8.6.2.2 Sudo Privileges
  - 8.6.2.3 Full permission over a service

VIII. Operating System Exploitation

- 8.7 Linux Credential Cracking
  - 8.7.1 Cracking Shadow File
- 8.8 Linux Persistence
  - 8.8.1 User Account Creation
  - 8.8.2 Profile Modification
  - 8.8.3 SSH Authorized_keys
  - 8.8.4 Malicious Cron Jobs
  - 8.8.5 Backdooring APT Package Managers
- 8.9 Linux Data Exfiltration
  - 8.9.1 Exfiltration using SSH reverse tunnels
  - 8.9.2 Languages (Python, PHP etc)

IX. Exploit Development

9.1 Introduction

9.2 Payload

9.3 CPU registers

9.4 Stack Overflow

9.5 Win32 SEH

9.6 Exploit Framework

9.7 Fixing & running exploit

9.8 Getting shell access

X. Cloud Penetration Testing

- 10.1 AWS
  - 10.1.1 Tools
  - 10.1.2 Storage & compute mis-configuration
  - 10.1.3 Exploitation
- 10.2 Azure
  - 10.2.1 Tools
  - 10.2.2 Storage & compute mis-configuration
  - 10.2.3 Exploitation
- 10.3 GCP
  - 10.3.1 Tools
  - 10.3.2 Storage & compute mis-configuration
  - 10.3.3 Exploitation
- 10.4 Cloud pentesting case study

XI. Docker Container Penetration Testing

11.1 Introduction

11.2 Basics

11.3 Docker in Depth

11.4 Container Orchestration

11.5 Lab Setup

11.6 Container Mis-Configurations & Exploitation (practical exercises)

- 11.6.1 Application Based
- 11.6.2 Configuration Based
- 11.6.3 Network Based
- 11.6.4 Image Based
- 11.6.5 Host Based

XI. Docker Container Penetration Testing

11.7 Case Studies

- 11.7.1 Backdoored Docker Image
- 11.7.2 CI/CD Attack (Gitlab Runner)

11.8 Docker Hardening

- 11.8.1 Docker Security Best Practises
- 11.8.2 Tools for Docker Security Assessment

XII. Mobile Application Penetration Testing

- 12.1 Introduction to Mobile Pentesting
- 12.2 Lab Setup
  - 12.2.1 Resource Allocation
  - 12.2.2 Installing Android Studio
- 12.3 Introduction to Android, its design & architecture
- 12.4 Android attack surface & attacks
  - 12.4.1 Tools
    - 12.4.1.1 Android Debug Bridge (ADB)
    - 12.4.1.2 APKTool
    - 12.4.1.3 Jadx
    - 12.4.1.4 Frida
    - 12.4.1.5 BurpSuite
    - 12.4.1.6 Wireshark

XII. Mobile Application Penetration Testing

- 12.4.2 APK File Structure
- 12.4.3 APK Analysis
  - 12.4.3.1 APKs Repositories
    - A. Online
    - B. Pre-Installed APKs
  - 12.4.3.2 Reverse Engineering APKs
  - 12.4.3.3 De-Compiling & Recompiling APKs
- 12.4.4 Android mis-configuration (exercise)

12.5 Mobile Penetration Testing Playbook

XIII. Active Directory Exploitation

- 13.1 AD & Kerberos 101
- 13.2 Recon & Initial Access
  - 13.2.1 Network Scan
  - 13.2.2 Password Spraying
  - 13.2.3 ASREPRoasting
  - 13.2.4 Credential Relaying
- 13.3 Domain Enumeration
  - 13.3.1 DNS
  - 13.3.2 Domain Computers
  - 13.3.3 Domain Users

XIII. Active Directory Exploitation

13.4 Lateral Movement

- 13.4.1 Bloodhound
- 13.4.2 Kerberoasting
- 13.4.3 Pass the Hash
- 13.4.4 Pass the Key
- 13.4.5 Pass the ticket / Pass the cache

13.5 Persistence

- 13.5.1 Silver Ticket
- 13.5.2 Golden Ticket

13.6 AD Pentesting Case Study

XIV. Wi-Fi Security

- 14.1 Introduction
  - 14.1.1 Wi-Fi 101
  - 14.2.2 Terminology
  - 14.2.3 Topology
  - 14.2.4 Wireless Encryption
- 14.2 Automated Framework
  - 14.2.1 Aircrack-ng Suite
- 14.3 Cracking Wi-Fi Encryption
  - 14.3.1 WEP
  - 14.3.2 WPA, WPA2, WPA3 & WPA Enterprise
- 14.4 Attacks
  - 14.4.1 MiTM Attacks
  - 14.4.2 Rogue Access Point

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live