



Penetration Testing

Table of content:

Introduction to Penetration

- Testing Requirements
- What is penetration testing?
- Stages of a penetration test
- Getting started with your lab
- Creating virtual machines in VMware, Hyper-V, and VirtualBox

Getting Started with Kali Linux

- An introduction to Kali Linux
- Installing and configuring Kali Linux
- Basic commands in Kali Linux
- Scripting in Kali Linux
- The essential tools of Kali Linux

Performing Information Gathering

- Passive information gathering
- Active information gathering
- Vulnerability scanning
- Capturing traffic

Mastering Social Engineering

- What is social engineering?
- Social engineering tools
- Creating a social engineering campaign

Diving into the Metasploit Framework

- Introducing Metasploit
- Finding modules
- Adding modules
- Metasploit options, shells, and payloads
- Working with MSFvenom

Understanding Password Attacks

- Introduction to password attacks
- Working with wordlists
- Offline password attacks
- Online password attacks
- Dumping passwords from memory

- Working with Burp Suite

- Understanding Burp Suite
- Preparing your environment
- Exploring and configuring Burp Suite components

Attacking Web Applications

- Preparing your environment
- Types of web application security testing
- The components of a web application
- Understanding the HTTP protocol
- Common web application attacks
- Attacking web applications

Getting Started with Wireless Attacks

- Exploring wireless attacks
- Compatible hardware
- Wireless attack tools
- Cracking WEP, WPA, and WPA2

Moving Laterally and Escalating Your Privileges

- Discovering post-exploitation techniques
- Preparing your environment
- Performing post-exploitation attacks

Antivirus Evasion

- The evolution of antivirus technologies
- Concepts of antivirus evasion
- Getting started with antivirus evasion
- Testing evasion techniques

Maintaining Control within the Environment

- The importance of maintaining access
- Techniques used to maintain access
- Using tools for persistence

Reporting and Acting on Your Findings

- The importance of a penetration testing report
- What goes into a penetration test report?
- Tools for report writing
- Recommending remediation options