PE304: Post Exploitation

Course 71579 – 40 Hours

Overview

The goal of Post Exploitation is to determine the value of the machine by collecting the data that stored in, the value of the machine determined by the sensitivity of this data. We will learn how to identify and document this data, configuration settings and communication channels with other devices.

Objectives

- Gathering information from different operating systems
- Inject files to remote operating systems
- Privilege Escalation
- Creating backdoors
- Gathering information from networks
- Infect users and servers
- Retrieve sensitive data
- Covering tracks

Who Should Attend

- Security practitioners
- Penetration testers
- Ethical hackers
- Private companies
- Individuals with previous background

Prerequisites

- Previous knowledge in penetration testing

Course Contents

Module 1: Information Gathering

In this module we will learn how to gather information from different operating systems, we will see techniques that help us cover our track, we will use commands and systems that help us to maintain our access to the target machine and make use in related tools. Also, we learn how to use scripts to manipulate the target operating system.

- Network Recon
  - ARP table
  - Broadcast
  - Nmap
  - Ports Scans
  - Host Scans
  - Nessus
- Windows
  - Blind File Systems

- Networking
- User Accounts (Users & Groups)
- Finding Important Files
- Remote System Access
- Auto-Start Directories
- WMI
- Reg Command
- Deleting Logs
- Uninstalling Software's (Anti-Virus & more)
- Invasion or Alerting Commands
- Meterpreter Commands
- Meterpreter Scripts
- PowerShell Scrips (Powerpreter)

- Linux/Unix
  - Blind Files
  - System
  - Networking
  - User Accounts (Users & Groups)
  - Credentials
  - Installed Packages
  - Package Sources
  - Finding Important Files
  - Deleting Logs

Module 2: Working with files and permissions

In this module we will learn how deal with files that exists in the target device, how to evade an Anti-Virus when we upload files. We will learn how to extract information and sensitive data from the target machine. Students will learn how to exploit the target machine in order to get permissions using privilege escalation techniques.

- File Transferring (Tools & Payloads)
  - Download from CMD
  - Download from PowerShell
  - Download from Terminal
  - Extracting from CMD
  - Extracting from PowerShell
  - Extracting from Terminal
  - Anti-Virus Evasion
- Privilege Escalation
  - Finding Vulnerabilities
  - Executing a Script
  - Local Exploits
  - Hash (SAM File) & Tokens
  - Process Injection
  - Sensitive Files in Sharing Folder
  - DLL Injection
  - Bypassing UAC

Module 3: Creating Backdoors

This module discusses on tools and knowledge that enable us to create backdoors for different operating systems so that we can return to the target machine later. We will learn how to move inside the network and get relevant information about the network and the devices inside.

- Backdoor
  - Windows
  - Windows API
  - Linux/Unix
  - Metasploit
  - Trojans
- Persistence
  - Meterpreter
  - Netcat
  - Handler

Module 4: Pivoting and Stealthy

In this module we will upgrade our capabilities in the network area and pivot our attack to other targets on the network. We will learn about tunneling and learn techniques to cover our tracks.

- Pivot & MiTM
  - Local Port Forwarding
  - Remote Port Forwarding
  - Dynamic Port Forwarding
  - LLMNR Poising
  - Arp Spoof
  - SSL strip
  - Encryption and Decrypting Files
- Anti-Forensic
  - Thinking Anonymous
  - Secure Log & Data Deletion
  - Overwriting Metadata
  - Preventing Data Creation