Introduction

Are you ready to delve into the world of advanced Windows malware development? In this comprehensive course, we will take you on a journey through the intricate art of crafting malware for Windows systems. Whether you're an aspiring red teamer, a seasoned malware developer, or simply curious about the dark side of cybersecurity, this course is designed to equip you with the knowledge and skills needed to understand, create, and defend against malicious software.

Course Contents:

Module 1: Shellcode Mastery

- **Shellcode Creator:** Explore the power of MSFVenom for crafting versatile shellcode.
- **Shellcode Execution:** Learn about callbacks and timers to execute your shellcode discreetly.

Module 2: Evading Detection

- **Shellcode Encryption:** Dive into encryption techniques using AES and XOR to obfuscate your code.
- **Process Injection:** Master classic, APC, threat hijacking, FindWindow, and DLL injection to infiltrate processes.

Module 3: Controlling Payload

- **Payload Control IPC:** Discover communication through pipes, mutex, and the Windows Registry.
- **Persistence:** Establish a lasting presence with Registry Keys and Image File Execution Options.

Module 4: Advanced Techniques

- **API Hooking:** Implement API hooking techniques with RDPCredStealer.
- **Token Manipulation:** Gain elevated privileges through impersonation and token duplication.
- **Privilege Escalation Techniques:** Explore Fodhelper, token manipulation, and PrivEsc Class.

Module 5: Adapting to the Environment

- **Multiplatform:** Develop malware for both 32 and 64-bit Windows systems.
- **Botnet Infrastructure:** Understand the server and victim-side components of a botnet.

Module 6: Beyond the Basics

- **Additional Techniques:** Study SigThief, IAT bypass, string encryption with SkCrypter, malware as a service, downloader malware, and techniques to evade VMs and sandboxes.
- **Exploiting Windows:** Master keyloggers, PPID spoofing, Windows Defender evasion, reverse shells, and the art of dumping lsass.exe.