Process Injection Part II

Advanced Techniques & Modern Evasion

Module Overview

5 advanced injection techniques • Defense mechanisms • Practical exercises

THEORY & FUNDAMENTALS

01 Introduction

Module overview and prerequisites

02 Review: Process Injection Part I

Classic techniques from the first module

03 Evolution of Process Injection

From disk-based to modern memory-only techniques

04 Defense Mechanisms

How EDRs detect and prevent injection attempts

ADVANCED TECHNIQUES

05 APC Injection with NtTestAlert

Using Asynchronous Procedure Calls for stealth

Alertable states and queue-based execution

06 Early Cascade Injection

Timing-based injection before EDR hooks load

Hijacking LdrpInitShimEngine callback

07 Process Hypnosis

Debugger-assisted control flow hijacking

Using debug events to intercept execution

08 APC Injection with NtQueueApcThreadEx2

Modern Windows 11 APC injection with special flags

QUEUE_USER_APC_FLAGS_SPECIAL_USER_APC

09 Process Migration with Donut & Speck

Full process migration using memory-mapped sections

Donut shellcode + Speck encryption + Mutex control

PRACTICE & APPLICATION

10 Hands-on Exercise

Build your own APC injector with encryption

11 Conclusions & Future Trends

Summary and evolution of injection techniques