

Table of Contents

Table of Contents	2
Introduction	4
Process Injection Techniques	6
Classic	10
DLL Injection	11
DLL Multi-Process Injector	21
Native API Injection	26
Function Pointer Declarations	31
EarlyBird	39
What is the APC Queue?	39
How APC Queue Works	39
Key Features of APCs	40
FindWindow	47
Thread Hijacking	50
FreeLoaderInjector	58
NinjaInjector	77
Exercise	89
Encrypt the shellcode	90
Conclusions	90