Offensive C#

Introduction

- Introduction

C# Basics

- Environment Setup and Hello World
- Variables and Operators
- Reading User Input
- Loops
- Arrays
- Functions

Python C2 Server

- Sockets and Multithreading
- Flask basics
- Linking Sockets and web interface
- Bidirectional File Transfer
- Multithreaded keylogger

C # Reverse Shell

- Coding a reverse shell in C#

LDAP Enumeration with Idapsearch

- Privilege Escalation
- Finding Unquoted Service paths
- Finding Writable Files

Automating Active Directory Enumeration

- Finding ASREP Roastable users
- Finding Nested groups
- Finding DCSync capable users
- Finding Unconstrained Delegation users
- Kerberos Constrained Delegation Attack
- Resource based Constrained Delegation

.Net Loader

- Simple .NET Loader

Persistence

- AdminSDHolder Persistence via C#

WinAPI with C#

- MessageBoxW and GetUserNameW
- Structures and Unions
- NetShareEnumW - Enumerating network shares
- GetTokenInformation - Checking our elevation privilege
- Listing All token privileges
- Enabling all assigned token privileges – AdjustTokenPrivilege
- Simple Shellcode runner
- Shellcode Injection in remote process
- Storing shellcode in .rsrc resources section
- DLL Injection
- Finding DLLs and their Base addresses in a process
- Checking if Process is attached to debugger or not
- Detaching the debugger from process using NtRemoveProcessDebug
- Backdooring PE Files
- Getting Screenshots
- Obfuscating Function names using Delegates

LSA API

- Enumerating Logon Sessions
- PE file format
- DOS Header, DOS Stub, Signature, File Header
- Optional Header
- Section Headers
- Import Name Table and Import Address Table
- Parsing Exports in a DLL

Reflective PE64 Injection

- Parsing Headers
- Mapping sections into memory
- Fixing Import Address Table
- Fixing Base Relocations
- Testing Metasploit payloads
- Adding a New Section via C#

Process Hollowing

- Process Hollowing

DLL Injection via SetWindowsHookExa

- SetWindowsHookExA DLL Injection

Shellcode Injection via Mapping Sections

- Shellcode Injection via NtMapViewofSection
- DLL Hollowing
- Thread QueueAPC Code Injection

Evasion Techniques

- Obfuscating Imports

AMSI Bypassing techniques

- Patching AmsiScanBuffer in memory

API Hooking

- Simple Function Hooking
- Local Function Hooking with EasyHook

API Hashing

- Hashing the function names to avoid static analysis
- Walkthrough
- Hackthebox - SAUNA