OFFENSIVE TOOL DEVELOPMENT

A Windows API Exploitation Training Program in C/C++

Dark Vortex LLP

Table of Contents

Day 1

Day 2

- Replacing Windows API with NTAPI
- NTAPI and Syscalls
- Remote Service Authentication
- Named Pipes and Token Impersonation
- Custom PsExec Service
- Share Enumeration and Evasion Techniques
- Tooling for Domain Environment
    - LDAP Enumeration
        - Domain Admin Enumeration
        - ACL Enumeration
        - User Enumeration
        - Enumerating Domain Services
    - SPN Enumeration
    - SPN Ticket Extraction
    - Kerberoasting

Day 3

- Reflective Modules
  - Credential Harvesting with MiniDump Reroutes
  - Service Payloads - Local and Remote
  - Registry Persistence/Query – Local and Remote
- Building Object File Loaders
  - Understanding PE/DLLs
  - Position Independent Shellcode
  - COFF In-memory Executions
- Side Loading DLLs
- EDR Unhooking and Evasion
  - Patching EDR Hooks in Memory
  - Blocking Non-Microsoft DLLs From Loading Into Memory
- AMSI Evasion
  - Modifying Existing Toolset
  - Patching AMSI In-memory
- ETW Evasion

Target Audience

- Red Team members
- Offsec Developers

Offensive Tool Development is a highly technical course. Every aspect of the course will contain heavy coding in C/C++ for the payload/modules and a handler/server for some tools in Python3 or Golang. All the tools mentioned in the above TOC will be handcrafted by the trainee during the tenure of the course. This course is highly recommended for people who do Red Teams on a day-to-day basis but want to gain an extra advantage by understanding the tools on a lower level and building your own detection-free tools.

Requirements

- A laptop with 16GB RAM to support 2 VMs running at the same time.
- Experience with programming languages, especially C/C++. Knowing Python3 or Golang is an added advantage.
- Good knowledge of pointers and data structures.
- Basic Knowledge of Windows API
- Strong will to learn and creative mindset.

What all do you get in the end

- 3 days of rigorous training program
- Course PDF and content materials

For any queries, contact paranoidninja@0xdarkvortex.dev