Windows Kernel Exploitation Advanced

Section A – Personal Data

Name: Ashfaq Ansari
Handle: @HackSysTeam
Email: ashfaq@payatu.com
Company: Payatu Software Labs LLP.
Biography: Ashfaq Ansari is the founder of HackSys Team code named "Panthera". He has experience in various aspects of Information Security. He has authored "HackSys Extreme Vulnerable Driver" and "Shellcode of Death". He has also written and published various white papers on low level software exploitation. His core interest lies in Low Level Software Exploitation both in User and Kernel Mode, Vulnerability Research, Reverse Engineering, Program Analysis and Hybrid Fuzzing. He is a fan boy of Artificial Intelligence and Machine Learning. He is the chapter lead for null (Pune).

Section B – Training

Title: Windows Kernel Exploitation Advanced
Duration: 3 Days
Description: This training is the advanced version of Windows Kernel Exploitation course focused on exploitation of different Windows Kernel Mode vulnerabilities on latest patched version of Windows 10 version 1703. We will cover basics of Windows Kernel Internals and hands-on fuzzing of Windows Kernel Mode drivers.

We will dive deep into exploit development of various kernel mode vulnerabilities. We will also look into different vulnerabilities in terms of code and the mitigations applied to fix the respective vulnerabilities. We will take a look how we can defeat exploit mitigations like SMEP by performing data-only attacks.

This training assumes that the attendees have less or no prior experience with Windows Kernel Internals and Kernel land as well as User land exploitation techniques.

Upon completion of this training, participants will be able to:

- Learn basics of Windows Internals
- Understand how to fuzz Windows Kernel mode drivers to find vulnerabilities
- Learn the exploit development process in Kernel mode
- Understand how a vulnerability looks like in driver code
- Understand how a vulnerability can be mitigated in the code
- Understand how to groom Kernel Pool and Stack
- Get comfortable with Windows Kernel Debugging

Prerequisites

- Basics of User Mode Exploitation is good to have but not required
- Basics of x86 Assembly and C/Python is good to have but not required
- Familiarity with VMware/VirtualBox (only to run virtual machines)
- Patience

Day 1

- ❖ Windows Internals
  - Windows NT Architecture
  - Executive & Kernel
  - Hardware Abstraction Layer (HAL)
  - Privilege Rings
  - Key Data Structures

- ❖ Memory Management
  - Virtual Address Space
  - Memory Pool & Allocator

- ❖ Why to Attack Kernel?
  - User Mode vs Privileged Mode
  - User Mode Exploit Mitigations

- ❖ Windows Driver Basics
  - I/O Request Packet (IRP)
  - I/O Control Code (IOCTL)
  - Data Buffering (Buffered I/O, Direct I/O, Neither Buffered Nor Direct I/O)

- ❖ Fuzzing Windows Drivers (Hands-On)
  - Locating IOCTLs in Windows Drivers
  - Locating input entry points
  - Writing scripts to fuzz the discovered IOCTLs

Day 2

- ❖ Quick Revision
  - Windows Internals
  - Memory Management
  - Windows Drivers Basics
  - Fuzzing Windows Drivers

- ❖ Fuzzing Windows Drivers (Hands-On)
  - Playing with public fuzzers

- ❖ Exploitation (Hands-On)
  - Pool Feng Shui/Pool Grooming (Lookaside List & ListHeads List)
  - Pool Overflow Exploitation
  - Arbitrary Memory Overwrite (Data-only attack)

Day 3

- ❖ Quick Revision
  - Pool Feng Shui
  - Pool Overflow

- Arbitrary Memory Overwrite

❖ Exploitation (Hands-On)
- Insecure Kernel Resource Access (Logical Bug)

❖ Kernel Payload (Hands-On)
- Escalate Privilege of a Process from Kernel Debugger
- Considerations while writing Escalation of Privilege Payload
- Kernel Recovery (Fixating Kernel State after exploitation)

❖ Exploit Mitigations
- Kernel Address Space Layout Randomization (KASLR)
- Supervisor Mode Execution Prevention (SMEP)

❖ Miscellaneous
- Assignment to write a full blown Windows Kernel exploit
- Q/A and Feedback

Who should attend?

- Windows Kernel Exploitation – Foundation attendees
- Bug Hunters & Read Teamers
- User Mode Exploit Developers
- Windows Driver Developers & Testers
- Anyone with an interest in understanding Windows Kernel exploitation
- Ethical Hackers and Penetration Testers looking to upgrade their skill-set to the kernel level

Why attend?

Upon completion of this training, participants will be able to:

- Get comfortable with Windows Kernel Debugging
- Understand how Kernel and Kernel Mode driver works
- Understand exploitation techniques for different software vulnerabilities
- Understand how Windows Pool Allocator works in order to write reliable exploit for complex bugs like Pool Overflow(s) and Use after Free(s)
- Learn to write own exploits for the found vulnerabilities in Kernel or Kernel mode drivers
- Understand vulnerabilities in terms of code and mitigations applied to fix the vulnerabilities

Prerequisites

- Basics of User Mode Exploitation is good to have but not required
- Basics of x86 Assembly and C/Python is good to have but not required
- Familiarity with VMware/VirtualBox (only to run virtual machines)
- Patience

Hardware & Software Requirement

- 8 GB Flash drive
- A laptop capable of running two virtual machines simultaneously (8 GB of RAM)
- 40 GB free hard drive space
- Everyone should have Administrator privilege on their laptop

What to Expect?

- Complete Hands-on
- WinDbg-Fu
- Fast & Quick Overview of Windows Internals
- Windows Kernel Drivers Basics/IOCTL/IRP
- Techniques to exploit Windows Kernel/Driver vulnerabilities

What students will be provided with?

- Printed Lab Manual
- Training slides
- Scripts and code samples
- BSOD T-Shirt