Windows Kernel Exploitation Foundation & Advanced

Section A – Personal Data

Name: Ashfaq Ansari
Handle: @HackSysTeam
Email: ashfaq@payatu.com
Company: Payatu Software Labs LLP.
Biography: Ashfaq Ansari a.k.a "HackSysTeam", is a vulnerability researcher and specializes in software exploitation. He has authored "HackSys Extreme Vulnerable Driver (HEVD)" which has helped many folks to get started with Windows kernel exploitation. He holds numerous CVEs under his belt and is the instructor of "Windows Kernel Exploitation" course. His core interest lies in Low-Level Software Exploitation both in User and Kernel Mode, Vulnerability Research, Reverse Engineering, Hybrid Fuzzing, and Program Analysis.

Section B – Training

Title: Windows Kernel Exploitation Foundation & Advanced
Duration: 3 days
Description: This is the combined version of the **Windows Kernel Exploitation Foundation & Advanced** course. In this course, we will use **Windows 7 SP1 x86 & Windows 10 RS6 x64** for all the labs and has a **CTF** that runs throughout the training.

This course starts with the **Foundation** course and builds the mindset required for the **Advanced** course. During this course, students will learn the basics of Windows & driver internals, different memory corruption classes, and fuzzing of kernel mode drivers. We will understand **pool manager** internals in order to groom kernel pool memory for reliable exploitation of pool-based vulnerabilities.

We will also look into how we can bypass **kASLR, kLFH,** and do hands-on exploitation using **Data-Only** attack, which effectively bypasses **SMEP** and other exploit mitigation.

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

- Basics of Windows and driver internals
- Different memory corruption classes
- Fuzz kernel mode drivers to find vulnerabilities
- Exploit development process in kernel mode
- Mitigation bypasses
- Pool internals & Feng-Shui
- Kernel debugging

Day 1 (Foundation)

- Windows Internals
  - Architecture
  - Executive & Kernel
  - Hardware Abstraction Layer (HAL)
  - Privilege Rings

- Memory Management
  - Virtual Address Space
  - Memory Pool

- Driver Internals
  - I/O Request Packet (IRP)
  - I/O Control Code (IOCTL)
  - Data Buffering

- Fuzzing Windows Drivers
  - Locating IOCTLs in Windows drivers
  - Sanitizers
    - Special Pool
  - Fuzzing the discovered IOCTLs

- Exploitation
  - Stack Buffer Overflow
    - Understand the vulnerability
    - Achieving code execution

- Escalation of Privilege Payload
- Kernel Recovery

Day 2 (Advanced)

- Quick Revision
  - Internals
  - Fuzzing
  - Stack Buffer Overflow
  - EoP Payload

- Windows 10
  - Architecture

- Exploit Mitigations
  - Kernel Address Space Layout Randomization (kASLR)
    - Understanding kASLR
    - Breaking kASLR using kernel pointer leaks
  - Supervisor Mode Execution Prevention (SMEP)

        - SMEP concepts
        - Breaking/bypassing SMEP

- Exploitation
    - Arbitrary Memory Overwrite
        - Understand the vulnerability
        - Achieving privilege escalation

- Pool Manager
    - Internals (kLFH)
    - Feng-Shui

- Exploitation
    - Memory Disclosure
        - Understand the vulnerability
        - Leak function pointer
        - Calculate driver base address

Day 3 (Advanced)

- Quick Revision
    - kASLR
    - SMEP
    - Feng-Shui
    - Memory Disclosure

- Exploitation
    - Pool Overflow
        - Understand the vulnerability
        - Finding corruption target
        - Grooming target pool
        - Achieving arbitrary read/write primitive (data-only attack)
        - Gaining local privilege escalation
            - Different places to corrupt

- Capture The Flag
    - Time to finish the CTF
    - Discuss any other vulnerability class if the students want and time permits

- Miscellaneous
    - Assignment to write a blog post about the vulnerability exploited during CTF
    - Q/A and Feedback

Who should attend?

- Windows Kernel Exploitation Foundation attendees
- Bug hunters & Red teamers
- User-mode exploit developers
- Windows driver developers & testers
- Anyone with 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:

- Understand exploitation techniques to defeat mitigation like SMEP and kASLR
- Understand how Windows Pool allocator works in order to write a reliable exploit for complex bugs like pool buffer overflow and use after free
- Learn to write exploits for the found vulnerabilities in the kernel or kernel mode components

Prerequisites

- Basic operating system concepts
- Good understanding of user-mode exploitation
- Basics of x86/x64 assembly and C/python
- 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
- Vmware Workstation/Player and VirtualBox installed
- Everyone should have Administrator privilege on their laptop

What to expect?

- Hands-on
- WinDbg-Fu
- Fast & quick overview of Windows internals
- Techniques to exploit Windows kernel/driver vulnerabilities

What students will be provided with?

- Training slides

- Scripts and code samples
- BSOD T-Shirt