# 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 Foundation** course. In this course we will use **Windows 10 RS2 x64** for all the labs. This course starts with the changes in Windows 10 RS2, Internals, hands-on fuzzing of Windows kernel mode drivers.

We will understand Pool Internals in order to groom pool memory from user mode for reliable exploitation of pool based vulnerabilities.

We will look into how we can bypass **KASLR** using **kernel pointer leaks**. We will do hands-on exploitation using **Data-Only** attack which effectively bypasses **SMEP** and other exploit mitigation.

**At the last day of the training, we will have a full day CTF to write an exploit for the known kernel vulnerability in Windows 10 RS2 x64.**

**This training assumes that the attendees have either taken "Foundation course" or have basic understanding of operating system concepts, familiar with software debugging, and knowledge about exploitation of vulnerabilities in user mode.**

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 to groom kernel pool from user land
- Get comfortable with Windows kernel debugging

## Day 1

❖ Windows 10

    - Architecture

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

- 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

- Pool
    - Internals
    - Tracing object allocations
    - Feng-Shui (Lookaside List & ListHeads List)

- Exploitation (Hands-On)
    - Pool Overflow

## Day 2

- Quick Revision
    - kASLR
    - SMEP
    - Feng Shui

- Exploitation
    - Pool Overflow (continued)
        - Achieving arbitrary read/write primitive (Data-only attack)
        - Gaining local privilege escalation
            - Different places to corrupt
    - Arbitrary Memory Overwrite
        - Achieving arbitrary read/write primitive (Data-only attack)
        - Gaining local privilege escalation

## Day 3

- Quick Revision
    - Pool Overflow
    - Data-only attacks

- ❖ Exploitation CTF
    - Write exploit for a known Windows 10 kernel vulnerability (CVE)

- ❖ 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 & 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:

- Understand exploitation techniques to defeat mitigation like SMEP
- 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

## Prerequisites

- Basic operating system concepts
- Good understanding of user mode exploitation
- Basics of x86 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
- Everyone should have Administrator privilege on their laptop

## What to Expect?

- 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