INTRODUCTION TO WINDOWS KERNEL EXPLOITATION: RELOADED

Trainers: Lucas Dominikow & Josué Rojas

Descripción general:

"Introduction to Windows Kernel Exploitation: Reloaded" es la continuación del curso "Introduction to software vulnerabilities exploitation".

La primera versión de este curso fue creada en 2019 con el fin de introducir conceptos más avanzados relacionados a la explotación de vulnerabilidades a nivel kernel.

Luego en 2021 se actualizó el contenido para abarcar también las últimas versiones de Windows 10 y, con el fin de mostrar el día a día de un exploit writer, se agregaron ejemplos reales de explotación de CVEs en el kernel de Windows.

En esta nueva edición se agregaron ejemplos reales de RCE + LPE para escapar la sandbox. Se verán algunos ejemplos reales orquestados supuestamente por "APT 28/Fancy Bear/Sednit/STRONTIUM" señalados como parte de GRU.

Por último, se agregó la categoría de race condition que hoy en día están saliendo varias vulnerabilidades en el kernel que tienen esto como principio. Normalmente race condition que genera un UAF.

La dinámica del curso es concepto-ejercicio: se introduce un nuevo concepto y se resuelven ejercicios relacionados a dicho concepto.

El alumno aprenderá técnicas para explotar vulnerabilidades que se puede encontrar en ring0 tanto en Windows 7 como en las últimas versiones de Windows 10.

Requisitos

- Conocimientos de exploiting básico
- Interpretación de las instrucciones assembly x86-64
- C/C++
- Python

Temario:

-Herramientas, configuración y armado del entorno

-Debuggeando en Kernel

-Arquitectura de Windows

-Estructura de un driver WDM

-Payloads para elevar a SYSTEM

-Explotación en Windows 7
>Null Pointer Dereference
> Integer overflow

> Stack buffer overflow
> Arbitrary Write
> Race condition

-Ejercicios en Windows 7

- Mitigaciones

-Explotación en Windows 10
>Stack Buffer overflow
>Integer overflow
>Arbitrary Write
>Race condition

-Ejercicios en Windows 10

-Ejemplos de explotación de CVEs

-Ejemplos de combinación de RCE + LPE para sandbox escape utilizado por malware

Reservá tu lugar

Costo:

USD 1.000

ARS 291.000

Reservá tu lugar

CONSULTAS

Para realizar consultas sobre el training o alguno de sus beneficios, escribir a: capacitacion@ekoparty.org

Trainers:

Lucas Dominikow

Trabaja como Exploit Writer en Core Security (una empresa de HelpSystems). Si bien se especializa en Windows, ha desarrollado exploits para otras plataformas como: GNU/Linux, FreeBSD, QNX, iOS y Android, tanto en userland como kernel. Ocasionalmente, tambien desarrolla exploits a nivel web. Dentro de la seguridad informática, sus intereses son el pentesting, la ingeniería inversa, la búsqueda y explotación de vulnerabilidades a nivel kernel (especialmente windows) y el análisis de malware.

Posee múltiples CVEs en varios productos de renombre. Ha publicado tecnicas de explotacion en revistas internacionales. Ha participado de varios CTFs presenciales e individuales a nivel nacional e internacional previa clasificación online.

Fue co-autor e instructor de los cursos "Introduction to Windows Kernel Exploitation" en 2019-2021 e "Introduction to software vulnerabilities" en 2021. Ha escrito varios blogposts analizando vulnerabilidades y sus respectivas explotaciones.

Twitter: ltdominikow

Josué Rojas

Josué Rojas aka Nox, hace ingeniería inversa desde hace 15 años en diferentes áreas, entre ellos, creación de cheats en un juego en línea MMORPG, análisis de malware, búsqueda de vulnerabilidades y desarrollo de exploits. Ha sido orador en conferencias como, LimaHack, OWASP, Ekoparty y DragonJAR. Trabajó previamente en Core Security e Immunity Inc. creando exploits en diferentes tecnologías como, Meltdown ataque de canal lateral, escapar del hipervisor en VBox, exploits de kernel sobre Windows, entre otros y actualmente es Security Independent Researcher.

Twitter: MrNox_

Resources

- ARCHIVE: PAST EDITIONS
- CODE OF CONDUCT
- NEWSLETTER
- EKOMAGAZINE

About Ekoparty

- OVERVIEW
- CTFs & CHALLENGES
- HACKTIVITIES
- SPONSORS

organizacion@ekoparty.org