INTRODUCTION TO SOFTWARE VULNERABILITIES EXPLOITATION: RELOADED

Trainers: Lucas Dominikow & Josué Rojas

Descripción general:

Muchas personas saben qué es una vulnerabilidad en un sistema o, por lo menos, tienen una idea aproximada. Pero, ¿por qué eso representa un peligro para nosotros? ¿Qué se puede hacer con una vulnerabilidad? Y, aún más importante: ¿cómo se hace?

Tanto para una empresa, como para un consultor, como para un curioso informático, conocer cómo abusar de una vulnerabilidad es muy importante y muy desafiante.

En este curso se enseñará a desarrollar programas que aprovechan una vulnerabilidad (un “exploit”) para ganar control de un sistema.

Se trata de un curso teórico-práctico, con muchas actividades para que los participantes tengan contacto con ejemplos creados especialmente para desafiar el ingenio y sentir la satisfacción de estar realmente explotando una aplicación.

Se cubrirán temas de explotación de vulnerabilidades en binarios. Trataremos también temas como las mitigaciones implementadas por los sistemas operativos y como saltearlas.

Este curso es una actualización/expansión del anterior curso "Introduction to software vulnerabilities exploitation". A diferencia del anterior, también hablaremos como las vulnerabilidades lógicas pueden ser explotadas de manera fácil, segura, y confiable para la escalación de privilegios.

Todo se verá en las últimas versiones de Windows 10.

Contaremos las nuevas mitigaciones que salieron desde la primera versión del curso.

Se harán ejercicios de identificación de vulnerabilidades en software real y, por último, hablaremos sobre heap internals.

Requisitos

Software: s e le otorgará a cada alumno una máquina virtual con todos los ejercicios y el material del curso. Por este motivo, es necesario contar con VMWare 16 (Workstation o Player).

Conocimientos

Si bien en el curso se repasará assembly x86-64, este está enfocado en la explotación de vulnerabilidades. Por lo tanto, es mejor tener una base para poder concentrarse en los conceptos relacionados a la explotación de vulnerabilidades.

Dicho lo anterior, sugerimos:

*Conocimientos de reversing
*C/C++
*Python
*Assembly x86-64

Temario:

-Repaso del ISA x86-64

-Entendiendo y explotando vulnerabilidades (Locales/Remotas)

> Stack buffer overflow
> Heap buffer overflow**
> Integer overflow
> OOB read/write
> Use after free
> Logical Vulnerabilities

-Vulnerabilidades en aplicaciones reales: Identificando la vulnerabilidad

-Mitigaciones

-Bypasses de mitigaciones

-Ejercicios

***Dependiendo del tiempo y el nivel de los alumnos, se ahondará en heap internals (Win 10)*

Reservá tu lugar

Costo:

USD 1.000

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

Josue 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

 English