Pablo García Morales A01745530

# **Ciberseguridad**

Dentro de la cibernética existen tres pilares de la seguridad estos son **confidencialidad** en el que se asegura de que la información, equipos y otros activos solo sean accedidos por entes de autorización. Después tenemos a la **integridad** que se asegura de que no hayan cambios no autorizados, que la información, equipos y activos permanezcan en un estado correcto y que las modificaciones intencionales sean realizadas con autorización. Y por último tenemos a la **disponibilidad** que se asegura que los recursos, información, y activos estén disponibles para quienes lo necesiten cuando los necesiten. En mi opinión estos son base para mantener protegidos tus dispositivos el problema es que todo nuestro sistema no fue creado para que sea seguro sino funcional y por eso se tuvo que crear esto para poder defendernos de aquellos que nos quieren atacar.

Asimismo el sistema tuvo que irse adaptando a ciertas condiciones por las vulnerabilidades que presentaba y por eso ahora está encargado de separar los espacios de **memoria** de cada proceso y permitiendo preservar la confidencialidad e integridad. Un ejemplo de estas vulnerabilidades se presentó con el exploit de **Dirty Cow** que aprovecha una condición de carrera en el proceso de Copy On Write. Este permite cambiar páginas de memoria de solo lectura a lectura/escritura.

Además existen existen estructuras dentro del sistema que pueden ser una debilidad como es el Buffer que es un espacio de almacenamiento temporal de datos donde hay lectura de strings desde la consola, introducción de datos y escritura de archivos. Los buffer son de tamaño limitado y muchas veces los programadores no verifican que los datos sean de tamaño correcto. Pueden permitir la ejecución de código arbitrario o crear problemas con las aplicaciones. Si no tenemos un uso adecuado de nuestros dispositivos este tipo de estructuras pueden ser atacadas.

Dentro del sistema operativo está el control de acceso y autenticación donde seguardan las identidades de los usuarios. Por cada usuario/archivo tiene una lista de que se puede realizar un ejemplo son los “Permisos \*Nix” en este Unix separa en 3 tipos:

Dueño: Creador del archivo

Grupo: Usuarios que tienen ciertos privilegios en conjunto.

Público: todos los demás.

Para mi la sección de “Cómo nos defendemos con configuración” es importante de conocer ya que existenmuchos ataques por una configuración incorrecta. Se recomienda, desactivar servicios, eliminar cuentas de invitados, revisar privilegios, Hardening, tener antivirus/firewall y eliminar aplicaciones innecesarias.

Si estudias algo relacionado con ciberseguridad es necesario tener claro qué es lo que quieres hacer y tener ética para hacer el bien a las personas y no hacer cosas malas.

Es bastante interesante los payouts de ZERODIUM porque son atractivas las ofertas por descubrir errores y ayudas a las compañías a ser más seguras.

En conclusión, es necesario tener una educación de seguridad informática para protegerte de atacantes, y también ayudar a las personas que no conocen mucho sobre el tema. Se pueden utilizar las herramientas y consejos que nos mostró el experto Jorge defendiendonos con la configuración de sus dispositivos.