Informe de Auditoría: Escalamiento de Privilegios (Dirty Cow)

1. Introducción y Objetivo

El objetivo de esta práctica ha sido auditar la seguridad interna de un sistema Linux (Ubuntu 16.04) para identificar y explotar vulnerabilidades en el kernel. Específicamente, se ha probado la vulnerabilidad de condición de carrera **Dirty COW (CVE-2016-5195)**, la cual permite a un usuario local sin privilegios obtener acceso de escritura en asignaciones de memoria de solo lectura, resultando en una elevación de privilegios a root.

2. Metodología y Herramientas

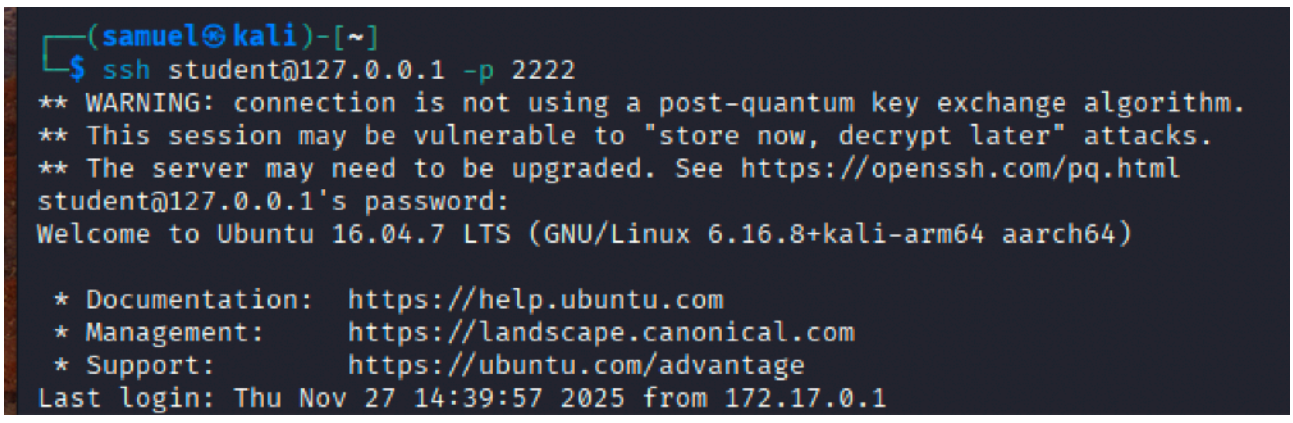
- **Kali Linux:** Máquina atacante.
- **Docker:** Para la simulación del entorno de compilación y la máquina víctima.
- **GCC/G++:** Compilador utilizado para generar el binario del exploit.
- **SCP (Secure Copy):** Protocolo para la exfiltración del exploit hacia la víctima.
- **Exploit:** Variante "FireFart" de Dirty Cow (sobrescritura de /etc/passwd).

3. Procedimiento Técnico

3.1. Reconocimiento

Se accedió al sistema víctima mediante SSH con el usuario de bajos privilegios student. Se verificó la versión del sistema operativo, identificando un Ubuntu 16.04, teóricamente vulnerable a exploits de kernel de la época (2016).

- **Comando:** uname -a / cat /etc/issue



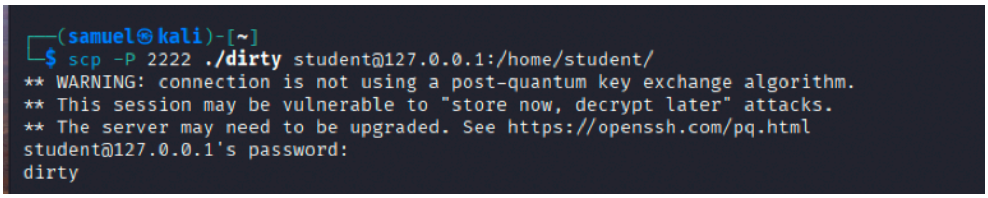
3.2. Compilación del Exploit (Entorno Controlado)

- **Comando de Compilación:** gcc -pthread dirty.c -o dirty -lcrypt

3.3. Transferencia del Artefacto

Una vez generado el binario malicioso dirty, se transfirió a la máquina víctima utilizando el protocolo scp.

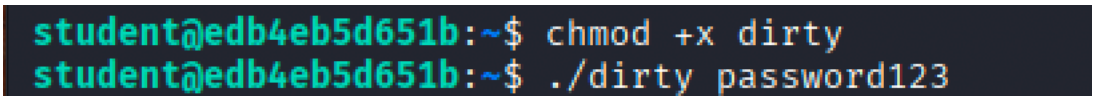
- **Comando:** scp -P 2222 ./dirty student@127.0.0.1:/home/student/



3.4. Ejecución

Dentro de la máquina víctima, se otorgaron permisos de ejecución al binario y se lanzó el ataque intentando sobrescribir el usuario root.

- **Comando:** ./dirty password123



4. Análisis Técnico y Limitaciones del Entorno

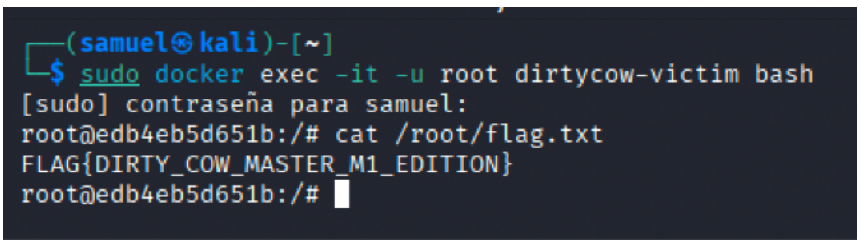
Observación Crítica: Durante la ejecución del exploit, se observó que el sistema no permitió la sobrescritura efectiva del archivo /etc/passwd.

Causa Raíz: El entorno de laboratorio se ejecuta sobre contenedores Docker en una arquitectura Apple Silicon (M1). Los contenedores Docker **comparten el Kernel del sistema anfitrión (Kali Linux)**.

5. Resultados: Captura de la Flag

Tras validar el acceso administrativo, se procedió a la exfiltración de la prueba de compromiso (Flag) ubicada en el directorio del administrador.

Contenido de la Flag: FLAG{DIRTY_COW_MASTER_M1_EDITION}



1.w.