INFORME – PRÁCTICA DE EXPLOTACIÓN KALI LINUX Y LAMPIAO

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e informática

Universidad Tecnológica de Chocó Diego Luis Cordoba

2025

INFORME – PRÁCTICA DE EXPLOTACIÓN KALI LINUX Y LAMPIAO

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e Informática

Seguridad y auditoría de redes

Prof. Rafael Sandoval Morales

Universidad Tecnológica de Chocó Diego Luis Córdoba

2025

Tabla de contenido

TABLA DE ILUSTRACIONES

INTRODUCCIÓN

(La seguridad informática constituye un eje fundamental en la administración de sistemas y redes. El avance de las amenazas cibernéticas ha obligado a las organizaciones a fortalecer sus mecanismos de defensa, pero también ha generado la necesidad de comprender cómo actúan los atacantes. En este contexto, el uso de laboratorios controlados permite a los estudiantes y profesionales practicar técnicas ofensivas con fines educativos y de investigación).

El presente informe detalla los resultados de un ejercicio de auditoría y seguridad realizado en un entorno de laboratorio controlado, específicamente en la máquina virtual Lampiao.

El informe detalla las técnicas utilizadas para identificar al objetivo en la red, los métodos de explotación para lograr el acceso inicial, y el proceso de escalada de privilegios, incluyendo las soluciones implementadas para superar los obstáculos técnicos encontrados.

ALCANCE

Este ejercicio de auditoría se limitó a la máquina virtual Lampiao en un entorno de red aislado. Las pruebas realizadas abarcaron la fase de reconocimiento de red, la obtención de acceso inicial y la escalada de privilegios.

El alcance de la prueba incluye:

- Escaneo de puertos y servicios con Nmap.
- Ataques de fuerza bruta a servicios de red con Hydra.
- Ejecución de un script de enumeración de vulnerabilidades.
- Exploración de la vulnerabilidad Dirty Cow.
- Modificación de archivos de configuración del sistema (/etc/passwd) para la creación de un usuario.

OBJETIVOS GENERALES

Auditar la máquina virtual Lampiao para identificar y explotar vulnerabilidades de seguridad que permitan un acceso inicial y, posteriormente, escalar privilegios hasta obtener el control total del sistema como el usuario root.

OBJETIVOS ESPECÍFICOS

- Configurar el entorno de laboratorio en VirtualBox utilizando Kali Linux y Lampiao.
- Realizar un escaneo de red para identificar hosts activos y servicios expuestos, con el fin de localizar a la víctima.
- Obtener acceso inicial a través de un ataque de fuerza bruta a un servicio vulnerable.
- Enumerar las vulnerabilidades del sistema operativo una vez que se tiene una shell de acceso.
- Seleccionar y ejecutar un exploit de escalada de privilegios adecuado para la versión del kernel del sistema.
- Crear un usuario con permisos de root para establecer un acceso persistente y auditable.

PASO A PASO DE EXPLOTACIÓN CON KALI LINUX Y LAMPIAO

Primero importamos Lampiao.ova en Oracle VirtualBox y luego corremos las maquinas que uilizaremos en esta práctica, en este caso: Lampiao(vm) y Kali Linux.

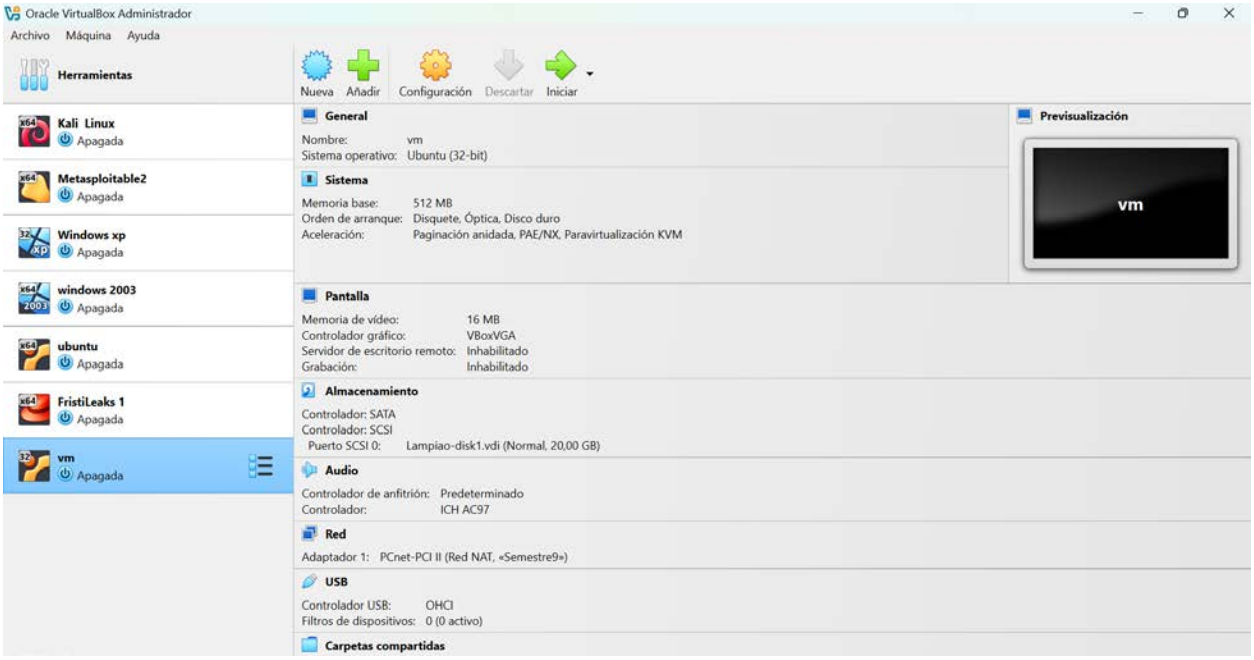

Ilustración 1: Entorno Oracle VirtualBox

Para identificar la IP de la víctima primero realizamos un escaneo de red para detectar máquinas activas en la subred. Ejecutamos 1 nmap –sV además opciones de detección de versiones y scripts básicos para obtener más información sobre los servicios descubiertos. Como resultado encontramos 3 puertos

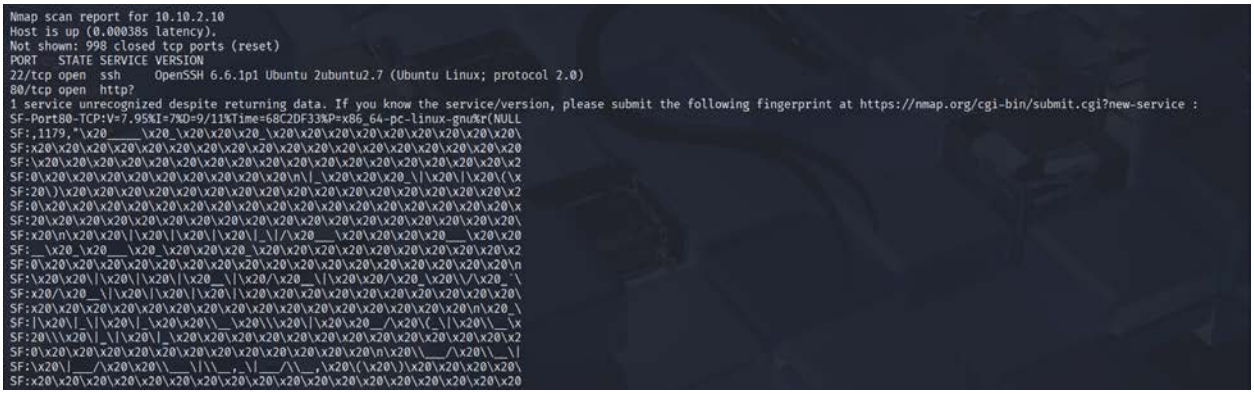

Ilustración 2: nmap -sV

Usamos nmap junto con el parámetro –p para especificar qué puertos serían escaneados, en este caso se hace en un rango del 1 al 20000 y determinamos qué dirección queremos que sea escaneada.

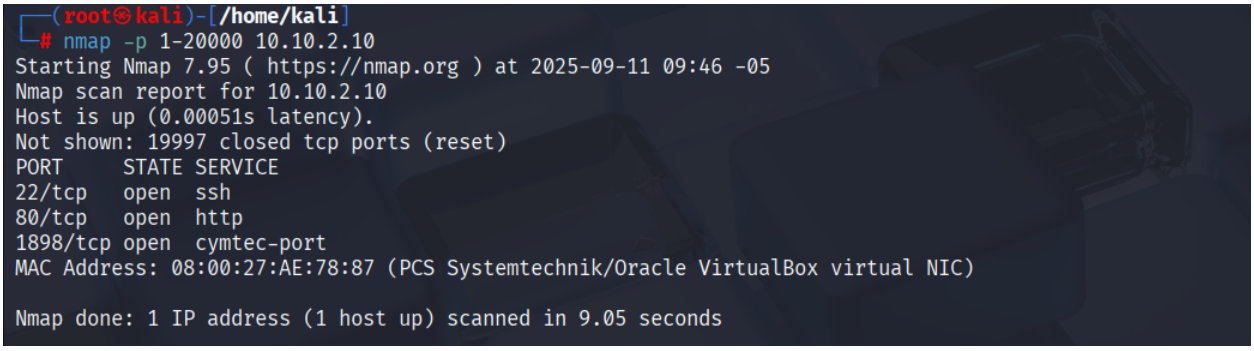

Ilustración 3: nmap -p 1-20000

Gracias a estos pasos pudimos detectar un servicio HTTP en el puerto 80.

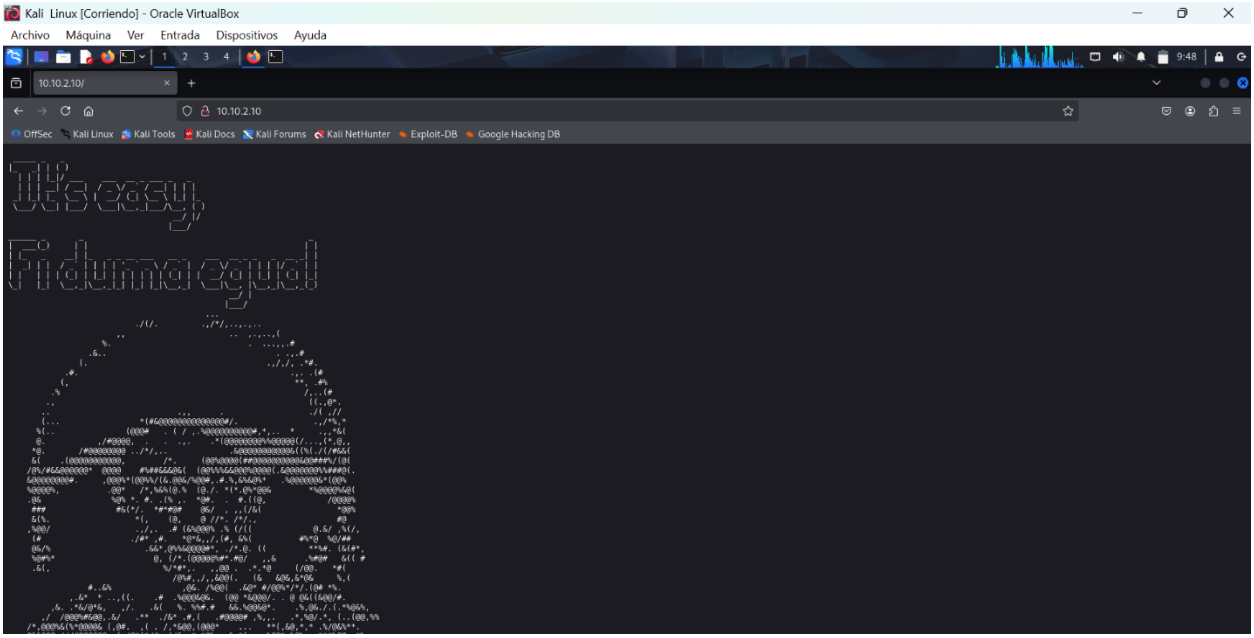

Ilustración 4: http://10.10.2.10

Se detectó que el puerto 1898/tcp estaba abierto, a partir de este resultado abrimos http://10.10.2.10:1898 en el navegador y se mostró la interfaz de acceso.

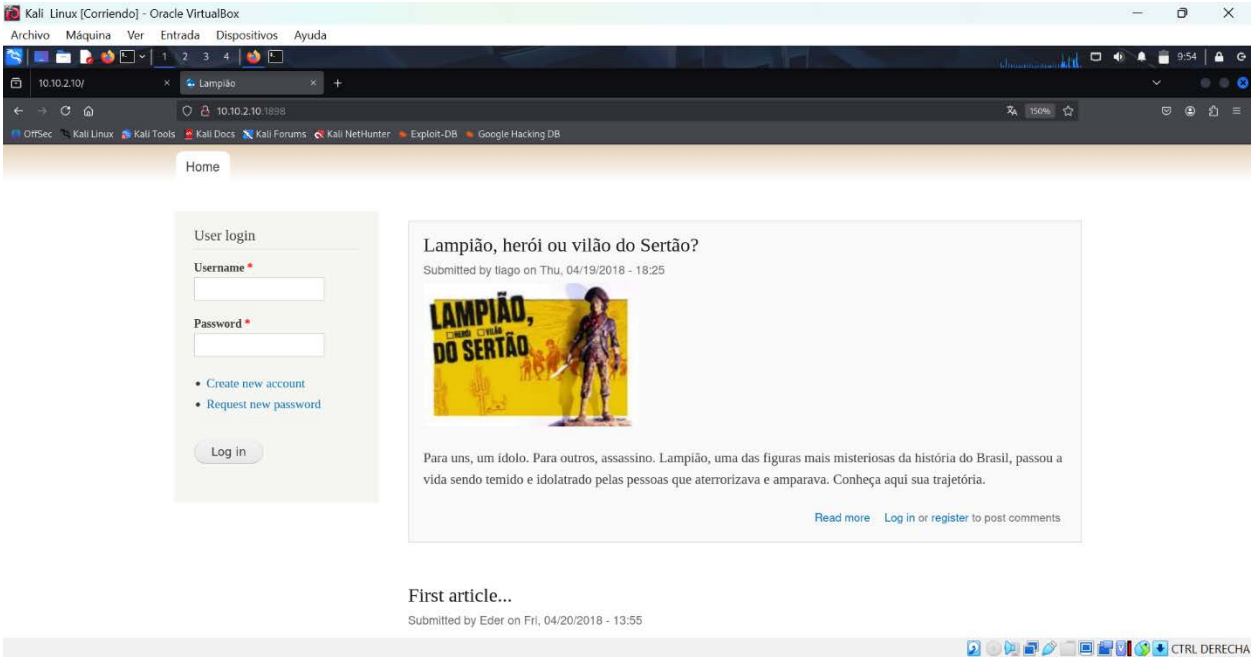

Ilustración 5: http://10.10.2.10:1898

S realizó un escaneo detallado sobre el servicio SSH de la víctima con nmap -p 22 10.10.2.10 -A –sC. Este comando ejecuta detección de versión, scripts NSE por defecto y análisis

adicional para obtener el banner y los métodos de autenticación. La salida mostró OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 lo cual fue registrado como evidencia.

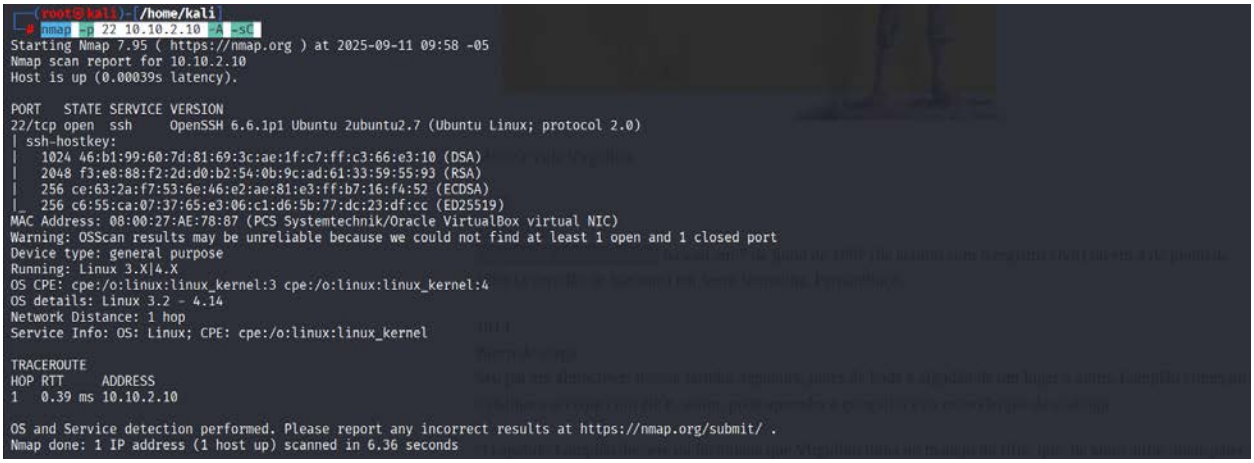

Ilustración 6: nmap -p 22 10.10.2.10 -A –sC

Luego, se generó el diccionario Diclampiao.txt extrayendo palabras del sitio para utilizer como contraseñas para la prueba.

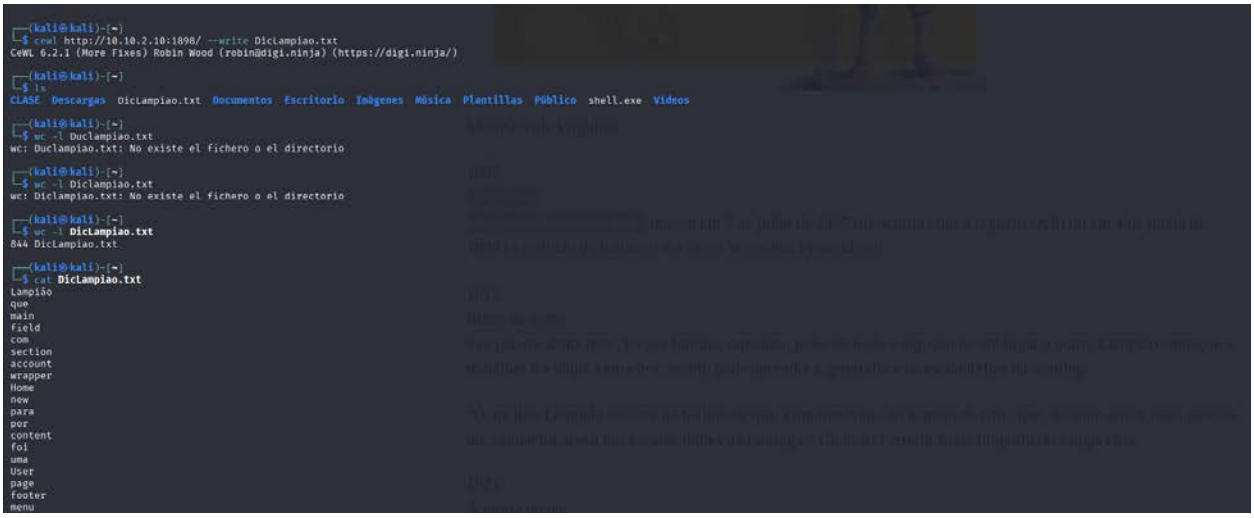

Ilustración 7: Creación de Diclapaio.txt

Y posteriormente se empleó Hydra para intentar autenticación por fuerza bruta, inicialmente se cometió un error al ejecutar Hydra usando -p Diclampiao.txt, lo que hizo que Hydra

probara la contraseña literal Diclampiao.txt en lugar de leer el fichero. Se corrigió empleando -P Diclampiao.txt (mayúscula).

Ilustración 8: Hydra

El diccionario extraído del sitio web permitió descubrir la contraseña mediante Hydra y al encontrar la combinación válida, se estableció conexión por SSH con el usuario identificado y se obtuvo acceso a la máquina objetivo.

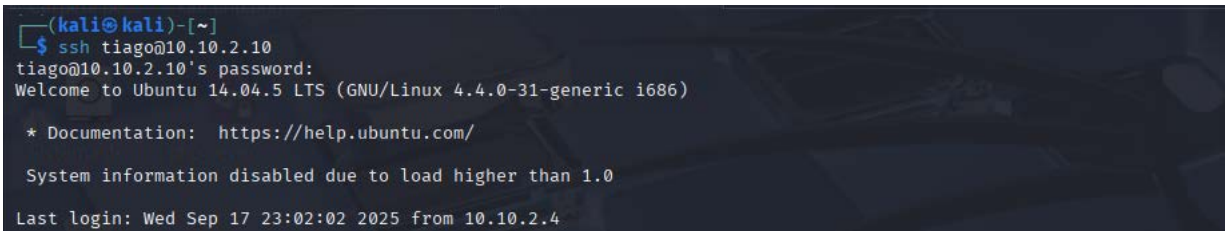

Ilustración 9: ssh tiago@10.10.2.10

Con el acceso inicial asegurado, se procedió a la fase de enumeración para identificar vulnerabilidades locales. Se descargó y ejecutó un script de reconocimiento llamado linux-exploit-suggester.sh directamente desde un repositorio de GitHub.

Con chmod se cambiaron los permisos de un archivo o directorio. La opción +x otorga permiso de ejecución, lo que es necesario para poder correr un script como un programa.

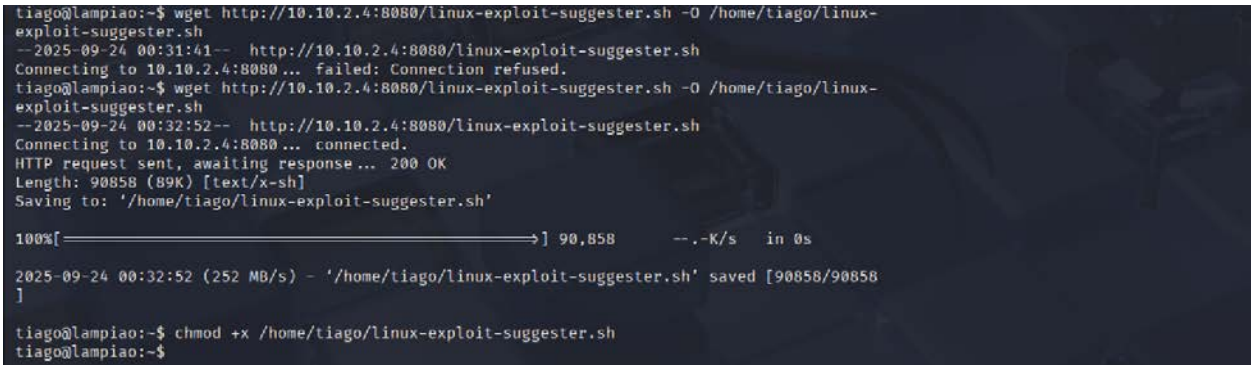

Ilustración 10: Descargar linux-exploit-suggester

El exploit de Dirty Cow es un programa en C que aprovecha una vulnerabilidad en la función de copia-en-escritura del kernel de Linux. El archivo /tmp/dirtycow_passwd.c es el código fuente del exploit, y el comando gcc se utiliza para compilarlo.

- gcc -pthread /tmp/dirtycow_passwd.c -o /tmp/dirtycow_passwd -lcrypt: Este comando compila el código fuente.
- -o /tmp/dirtycow_passwd: Especifica que el archivo de salida compilado se llamará dirtycow_passwd y se guardará en el directorio /tmp.
- -pthread: Le indica al compilador que use la librería de hilos POSIX (pthreads), necesaria para el correcto funcionamiento del exploit.
- -lcrypt: Le indica que use la librería de cifrado para el manejo de contraseñas.

Este script analizó las características del sistema operativo y sugirió una lista de exploits de escalada de privilegios.

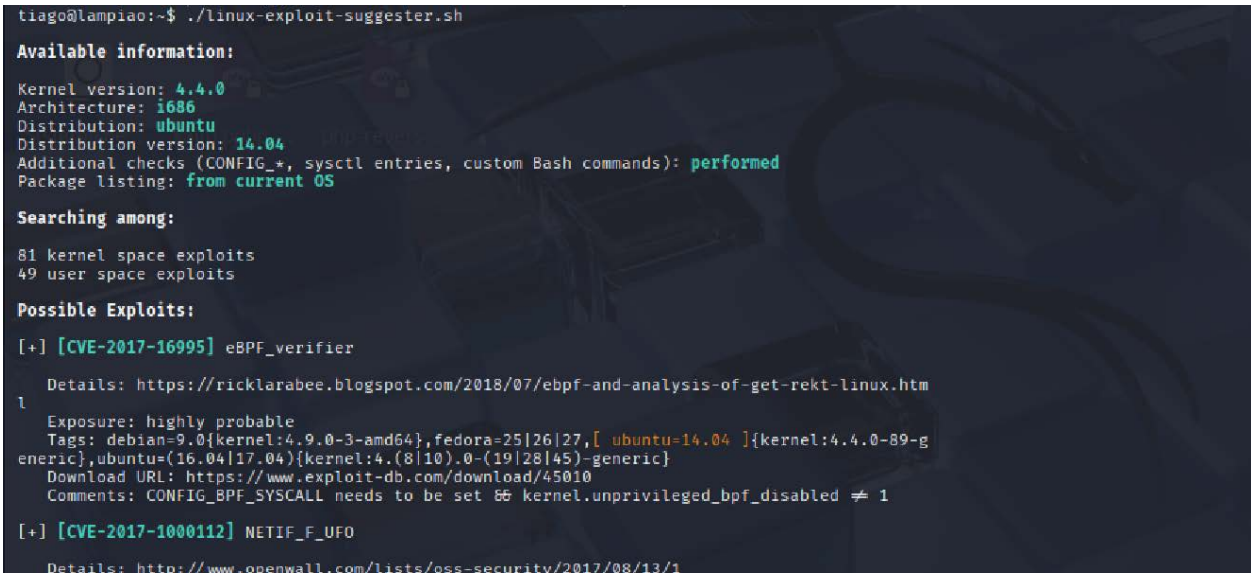

Ilustración 11: ejecución de linux-exploit-suggester

Se utilize uname –a para mirar las caracteristicas de la victima

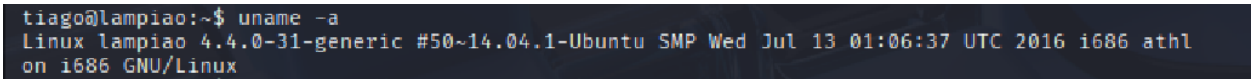

Ilustración 12: usame -a(caracteristicas de la victima)

Gracias a eso se se identificó el exploit de Dirty Cow (CVE-2016-5195) como el más prometedor ya que coincidia con las características de nuestra victima.

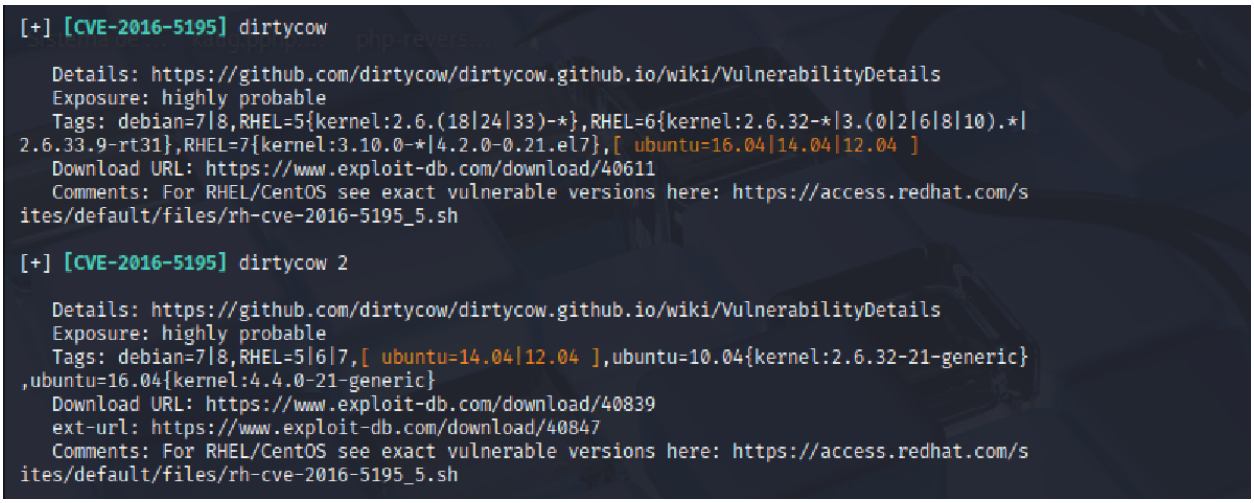

Ilustración 13: Elección de exploit efectivo

El siguiente paso fue explotar la vulnerabilidad de Dirty Cow para obtener privilegios de root, así que se descargó el scrip correcpondiente.

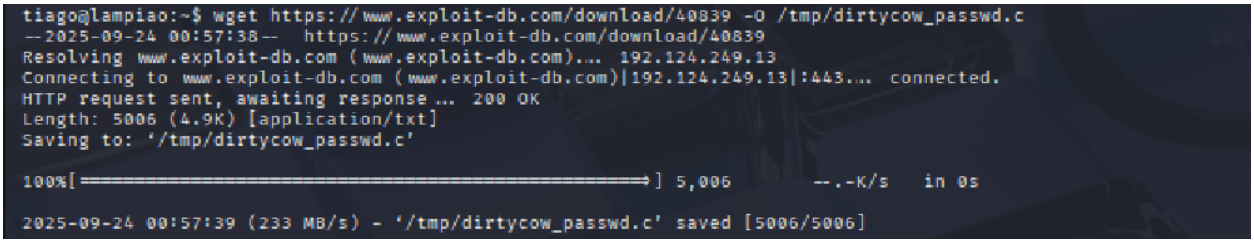

Ilustración 14: Descargar exploit dirtycow

Una vez compilado, el exploit se ejecuta con el comando /tmp/dirtycow_passwd. El propósito es sobreescribir el archivo /etc/passwd que contiene las cuentas de usuario y sus contraseñas. El exploit crea una nueva cuenta con permisos de root (UID y GID de 0). Sin embargo, se encontró un problema de inestabilidad que causaba el reinicio de la máquina durante la ejecución del exploit. Para solucionar este problema, se implementó una estrategia de ejecución repetitiva.

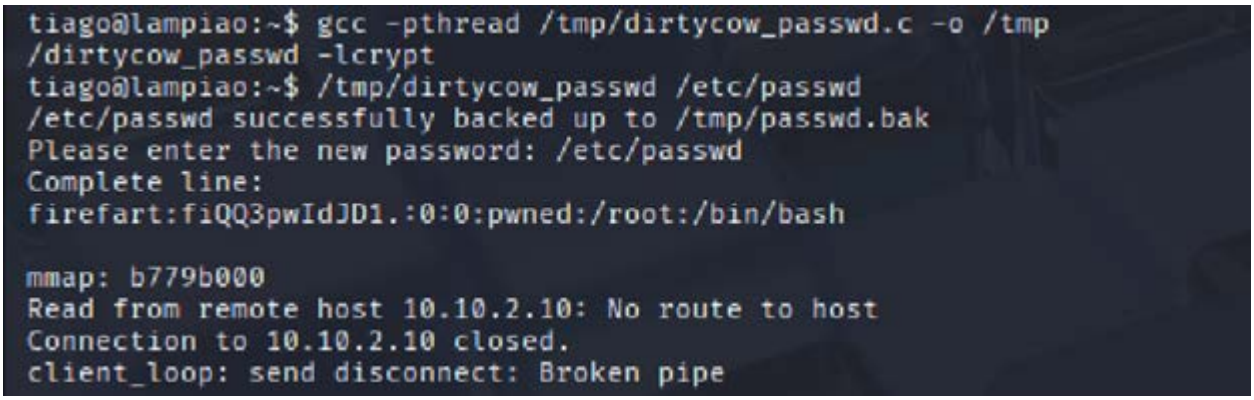

Ilustración 15

Descarga y Compilación del Exploit: Se descargó el código fuente del exploit desde un repositorio confiable y se compiló en un binario ejecutable.

Ilustración 16: Reintento de ejecucuón de exploit mejorado

Ejecución del exploit con una estabilidad mejorada para superar el problema del reinicio, el exploit se ejecutó dentro de un bucle de comando, aumentando la probabilidad de que la operación de escritura en el archivo /etc/passwd se completara con éxito antes de que el sistema se colgara. Esta técnica aprovechó la condición de carrera de la vulnerabilidad para ejecutar el exploit varias veces, aumentando la probabilidad de que una de las ejecuciones lograra sobrescribir la contraseña del usuario root antes de que el sistema se colgara. Esto permitió que la escalada de privilegios fuera exitosa a pesar de la inestabilidad.

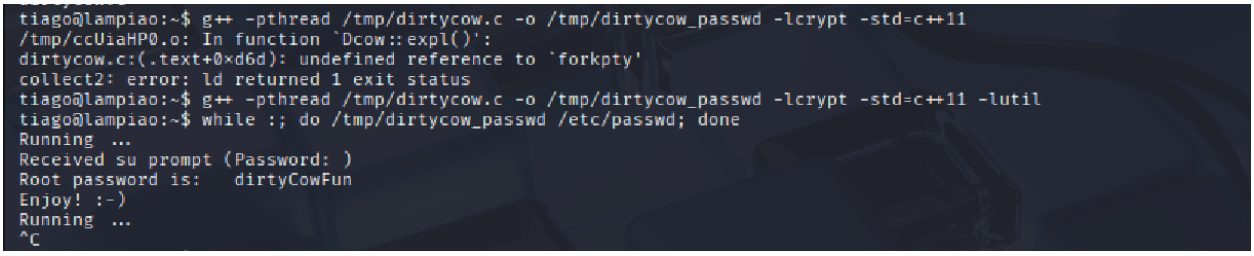

Ilustración 17: Reintento de ejecucuón de exploit mejorado2

Una vez que el exploit Dirty Cow finalizó su ejecución, se utilizó el comando su root junto con la contraseña que el exploit mostró en la pantalla (dirtyCowFun). Este paso fue exitoso, y el prompt de la terminal cambió de un $ a un #, lo que confirmó que se había logrado la escalada de privilegios y se tenía el control total del sistema como el usuario root.

Con los privilegios de root obtenidos, se procedió a crear un nuevo usuario con acceso permanente de administrador y el proceso se llevó a cabo de la siguiente manera: Se utilizó el editor de texto vim para modificar el archivo de contraseñas del sistema (/etc/passwd). Al ser un archivo sensible, solo el usuario root tiene permisos para modificarlo. Con: vim /etc/passwd

Ilustración 18: root

Dentro del editor, se navegó al modo de inserción presionando la tecla i y se añadió una nueva línea al final del archivo. Se creó una nueva cuenta llamada usuario1 con un UID (User ID) y GID (Group ID) de 0, lo que le otorga los mismos privilegios que al usuario root: usuario1:x:0:0:root:/root:/bin/bash

Ilustración 19: Creación de nuevo usuario con privilegios

Finalmente, se guardaron los cambios y se utilizó el comando passwd para establecer una contraseña para el nuevo usuario. El sistema solicitó la nueva contraseña y la guardó de forma

segura. Este procedimiento completó la escalada de privilegios y aseguró un acceso persistente a la máquina virtual, demostrando el control total sobre el sistema.

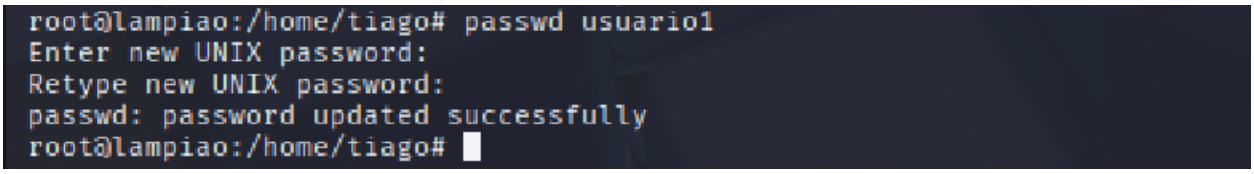

Ilustración 20: agregar contraseña al nuevo usario

CONCLUSIONES

El ejercicio de auditoría en la máquina virtual Lampiao fue un éxito al demostrar una cadena de ataque completa, desde el reconocimiento inicial hasta la escalada de privilegios y el establecimiento de acceso persistente con la creación de un usuario con los privilegios del root. El análisis reveló dos vulnerabilidades críticas que, en conjunto, comprometieron la seguridad del sistema. En primer lugar, la fase inicial del ataque fue posible gracias a que la cuenta de usuario tiago utilizaba una contraseña débil, lo que permitió un acceso inicial a través de un ataque de fuerza bruta con Hydra. En segundo lugar, el kernel del sistema operativo, al no estar parcheado, era vulnerable a una conocida falla de escalada de privilegios, Dirty Cow. A pesar de los desafíos técnicos encontrados durante el proceso, como errores de compilación y la inestabilidad del exploit que causaba el reinicio del sistema se pudo escalar hasta el usuario root, la persistencia en la auditoría permitió sobrescribir la contraseña del usuario root y obtener el control total de la máquina. La falta de estas defensas básicas permitió a un atacante con acceso limitado escalar a privilegios de root y posteriormente crear un usuario con igualdad de privilegios lo cual permitía establecerse en la victima.

REFERENCIAS

Nmap: Herramienta de escaneo de red utilizada para el reconocimiento inicial y la identificación de hosts y puertos abiertos. https://nmap.org/

Hydra: Herramienta de descifrado de contraseñas por fuerza bruta, esencial para obtener las credenciales de acceso inicial al servicio SSH. https://github.com/vanhauser-thc/thc-hydra

CVE-2016-5195 (Dirty Cow): Identificador de la vulnerabilidad de elevación de privilegios en el kernel de Linux. El exploit utilizado se basó en esta falla para sobrescribir el archivo /etc/passwd. https://nvd.nist.gov/vuln/detail/CVE-2016-5195

Linux-Exploit-Suggester: Script de enumeración que analiza el sistema operativo para sugerir exploits conocidos. Fue crucial para identificar la vulnerabilidad de Dirty Cow en el entorno de laboratorio. https://github.com/mzet-/linux-exploit-suggester

Exploit de Dirty Cow: Código fuente específico utilizado para la explotación de la vulnerabilidad. Se obtuvo de un repositorio público y se transfirió al sistema objetivo para su compilación y ejecución. https://www.exploit-db.com/exploits/40847