Universidad Tecnológica del Chocó
Diego Luis Córdoba

Informe de la Explotación de la página de Lampiao desde Kali Linux.

Asignatura

Seguridad y Auditoría en Redes

Estudiante

Andrés Felipe Asprilla Córdoba

Universidad Tecnológica del Chocó “Diego Luis Córdoba”

Ingeniería de Telecomunicaciones e Informática

Quibdó/Chocó

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Informe de la Explotación de la página de Lampiao desde Kali Linux.

Docente

ING Rafael Sandoval Morales

Estudiante

Andrés Felipe Asprilla Córdoba

Asignatura

Seguridad y Auditoría en Redes

Universidad Tecnológica del Chocó “Diego Luis Córdoba”

Ingeniería de Telecomunicaciones e Informática

Quibdó/Chocó

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Tabla de contenido

Introducción 6

Planteamiento del Problema 7

Objetivo General 8

Objetivos Específicos 8

Instalación de Lampiao 9

Escaneo la red para saber que ip cogió Lampiao..... 10

Ip victima 10.10.10.15 11

Ip atacante 1010.10.5 12

Escaneo de 2000 puerto de lampiao ip 10.10.10.15 12

Vulnerar a página de Lampiao..... 13

Msfconsole..... 16

Crear diccionario 19

Ingreso por ssh tiago@10.10.10.15 22

Recomendaciones 30

Conclusión 31

Referencias Bibliográfica.....32

Tabla de Ilustraciones.

Ilustración 1Importando la máquina de Lampiao 9

Ilustración 2Importacion completada 10

Ilustración 3escaneo de red con Nmap 11

Ilustración 4Localizacion de la victima 11

Ilustración 5Ejecuté ifconfig 12

Ilustración 6Escaneo de 2000 puerto de Lampiao 13

Ilustración 7página de Lampiao 14

Ilustración 8página web que corre en el puerto 1898 14

Ilustración 9Login 15

Ilustración 10dirigido contra la IP objetivo 16

Ilustración 11msfconsole 17

Ilustración 12OpenSSH 17

Ilustración 13módulo auxiliar 18

Ilustración 14módulo de comprobación 18

Ilustración 15nombre de usuario como root 19

Ilustración 16archivo llamado DicLampiao.txt 19

Ilustración 17Verifiqué que DicLampiao.txt 20

Ilustración 18contenido del diccionario generado 20

Ilustración 19comprobé la ayuda de Hydra 21

Ilustración 20ataque de fuerza bruta con Hydra 22

Ilustración 21conecté por SSH 23

Ilustración 22enumeración local LinEnum 23

Ilustración 23README 24

Ilustración 24Cloné correctamente el repositorio LinEnum 25

Ilustración 25carpeta llamada LinEnum 25

Ilustración 26directorio del script 26

Ilustración 27/home utilizando el comando ls 27

Ilustración 28shell como /usr/sbin/nologin 27

Ilustración 29/etc/passwd 28

Ilustración 30comando find / -perm -4000 2>/dev/null 29

Introducción

El presente laboratorio se enmarca en el desarrollo de competencias prácticas dentro del área de Seguridad y Auditoría en Redes, abordando la simulación de escenarios reales de vulnerabilidad en sistemas informáticos. A través del uso de máquinas virtuales como Kali Linux y Lampião, se propone una experiencia técnica que permite al estudiante aplicar metodologías de análisis, reconocimiento y explotación de servicios inseguros, con el fin de comprender los riesgos que enfrentan los entornos digitales mal configurados o desactualizados.

El documento evidencia un proceso sistemático que inicia con la configuración de red entre las máquinas virtuales, seguido por el escaneo de puertos y servicios mediante herramientas como Nmap, y culmina con la ejecución de técnicas de fuerza bruta, enumeración local y escalada de privilegios.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Planteamiento del Problema

Proceda a realizar la explotación de la máquina virtual vulnerable utilizando Kali Linux como entorno atacante. Inicie con el reconocimiento de red para identificar la dirección IP del objetivo y los servicios activos mediante escaneo de puertos. Una vez detectados los servicios expuestos, como SSH y HTTP, utilice herramientas como Nmap y Hydra para ejecutar ataques de fuerza bruta y obtener credenciales válidas.

Acceda al sistema remoto y realice una enumeración local completa para identificar configuraciones débiles, archivos con permisos SUID y posibles vectores de escalada de privilegios. Aplique técnicas de auditoría para validar el nivel de exposición del sistema y documente cada hallazgo con evidencia técnica.

Objetivo General

Realizar un análisis técnico de la explotación de vulnerabilidades en una máquina virtual desde Kali Linux, aplicando técnicas de auditoría y penetración controlada para evaluar la seguridad del entorno.

Objetivos Específicos

- Configurar el entorno virtual con Kali Linux y la máquina vulnerable, asegurando la conectividad entre ambas.
- Ejecutar escaneos de red y puertos para identificar servicios activos y posibles vectores de ataque.
- Aplicar técnicas de fuerza bruta y enumeración local para obtener acceso al sistema y evaluar su configuración interna.
- Realizar el cambio de dirección MAC en Ubuntu y configurar el DHCP para validar la flexibilidad de red en entornos virtuales.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Instalación de Lampiao

Importé la máquina virtual **Lampião** a mi entorno de trabajo. Abrí la ventana de importación y seleccioné el archivo desde el sistema de archivos local; revisé las opciones básicas de configuración que ofrece el asistente y confirmé para que la máquina quedara registrada en el software de virtualización.

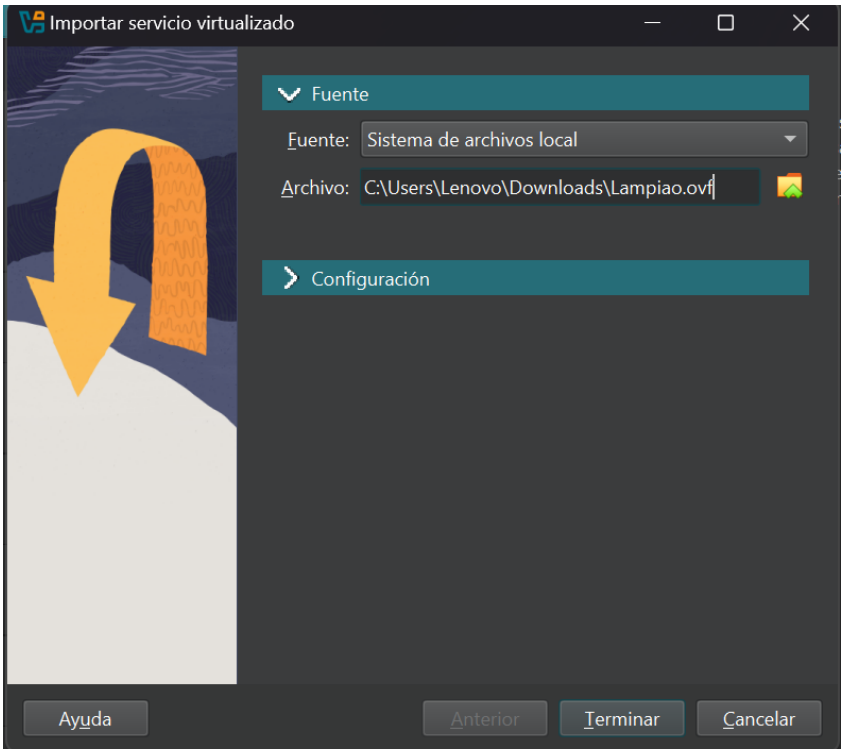

Ilustración 1Importando la máquina de Lampiao

Tras completar la importación, comprobé que la máquina aparece en la lista de máquinas disponibles y está lista para encenderse. Con esto dejé preparada la plataforma de laboratorio para iniciar la práctica: arrancar Lampião, verificar su conectividad y comenzar con el escaneo y las pruebas correspondientes.

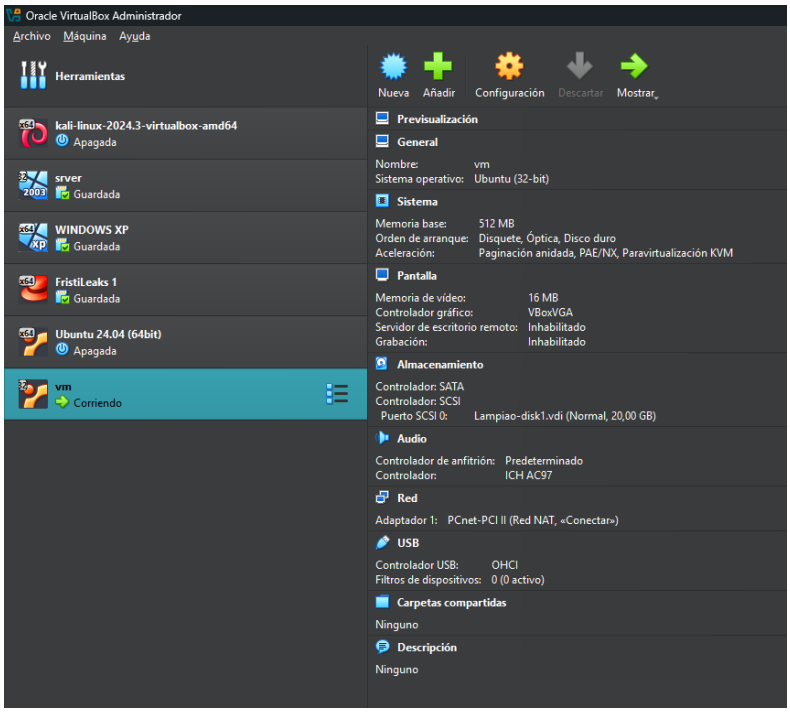

Ilustración 2Importacion completada

Escaneo la red para saber que ip cogió Lampiao

Primero arranqué la máquina Kali en mi entorno virtual y abrí una terminal. Desde allí realicé un **escaneo de red con Nmap** sobre el rango 10.10.10.0/24, con el fin de identificar qué direcciones IP estaban activas y qué servicios tenían abiertos. Con este barrido confirmé que la máquina objetivo, Lampião, se encontraba en la IP **10.10.10.15**.

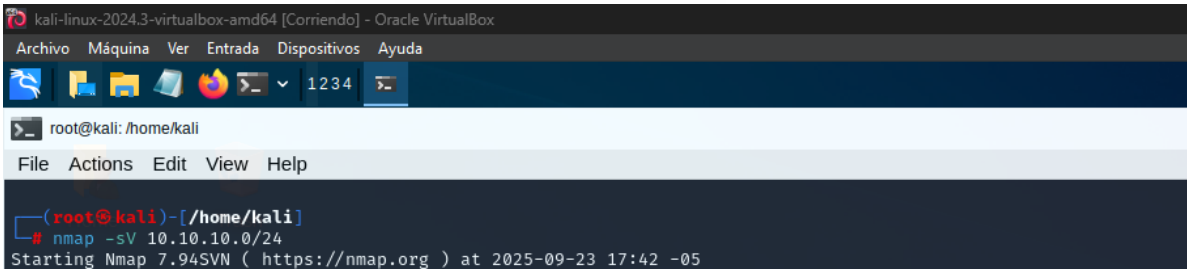

Ilustración 3escaneo de red con Nmap

Ip victima 10.10.10.15

Una vez localizada la máquina víctima, ejecuté un nuevo escaneo específico contra esa dirección IP. El resultado mostró que tenía abiertos los puertos **22 (SSH)** y **80 (HTTP)**. El servicio SSH estaba corriendo con **OpenSSH 6.6.1p1 sobre Ubuntu**, mientras que en el puerto 80 aparecía un servicio web activo que Nmap no logró identificar completamente, pero que confirmó que había algo escuchando.

Este reconocimiento inicial me permitió saber que la máquina estaba en línea, que respondía rápidamente y que disponía de dos servicios claves para las siguientes fases de la práctica: la conexión remota por SSH y el servicio web en el puerto 80.

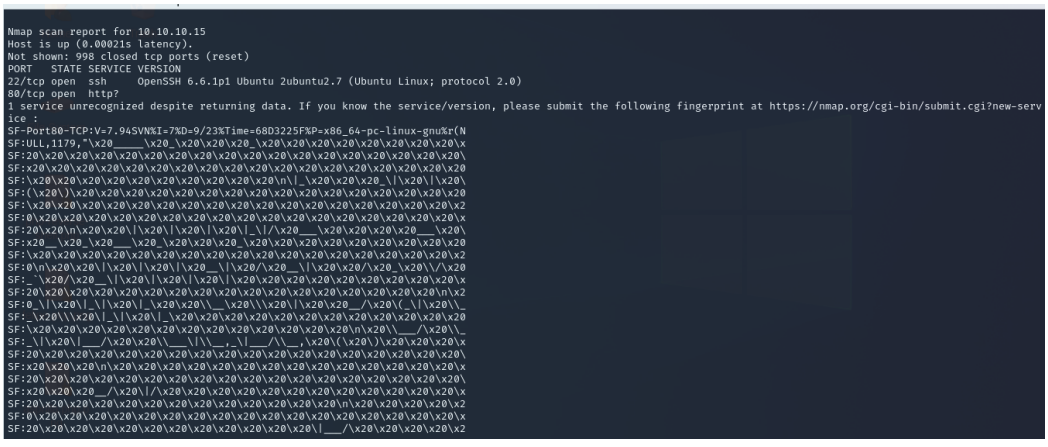

Ilustración 4Localizacion de la victima

Ip atacante 1010.10.5

Abrí una terminal en mi máquina atacante y verifiqué la configuración de red para asegurarme de la conectividad con el laboratorio. Ejecuté ifconfig y confirmé que mi interfaz eth0 tenía la dirección **10.10.10.5** con máscara 255.255.255.0 y broadcast 10.10.10.255; también comprobé que el loopback (lo) estaba activo con la dirección 127.0.0.1. Con esto confirmé que mi equipo está en la misma subred que la víctima (10.10.10.15) y listo para realizar las pruebas controladas que sigue el laboratorio.

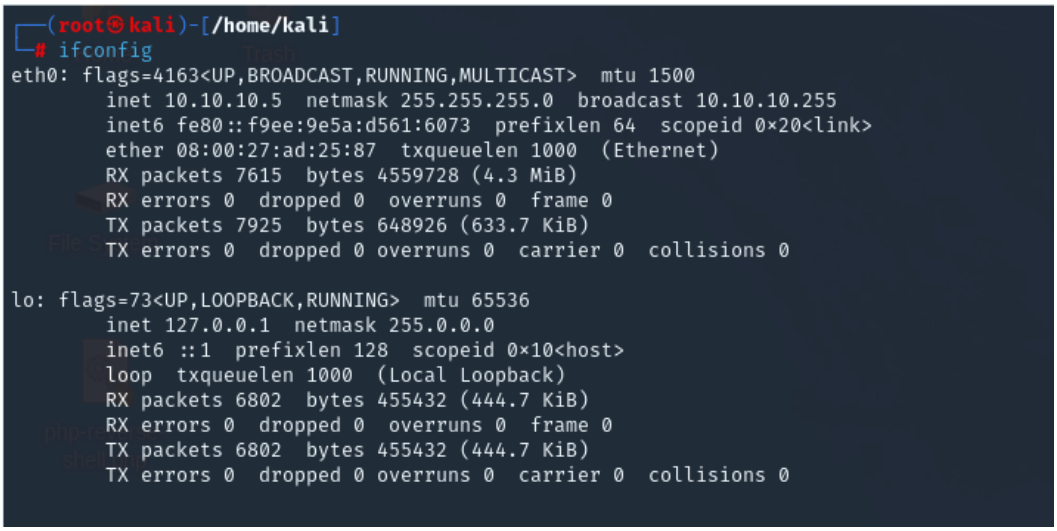

Ilustración 5Ejecuté ifconfig

Escaneo de 2000 puerto de lampiao ip 10.10.10.15

Ejecuté un escaneo dirigido contra la máquina objetivo para verificar qué servicios tenía activos. En la terminal lancé nmap -p- 10.10.10.15 y confirmé que el host respondía; el resultado mostró que estaban abiertos los puertos **22 (SSH)**, **80 (HTTP)** y **1898** (un puerto de servicio genérico identificado por VirtualBox). También pude ver la dirección MAC asociada a la tarjeta

de red virtual. Con esta información confirmé que la víctima está en línea y accesible desde mi equipo (que previamente comprobé que tiene la IP 10.10.10.5), y que los puntos más relevantes para continuar las pruebas son el acceso remoto por SSH y la interfaz web en el puerto 80.

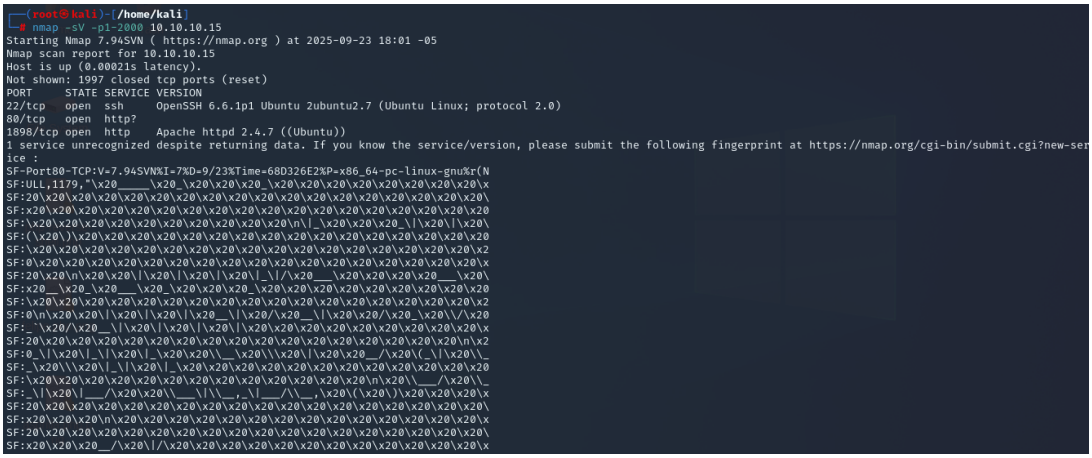

Ilustración 6Escaneo de 2000 puerto de Lampiao

Vulnerar a página de Lampiao

Abrí un navegador y navegué a http://10.10.10.15. Al cargar la página encontré una pantalla de bienvenida con arte ASCII grande (un “landing” muy simple), lo que confirmó de forma visual que el servicio web en el puerto 80 está activo y sirviendo contenido público. No vi formularios de registro ni opciones para crear usuarios en esa pantalla; simplemente era una página estática de presentación que sirve como punto de entrada al servicio.

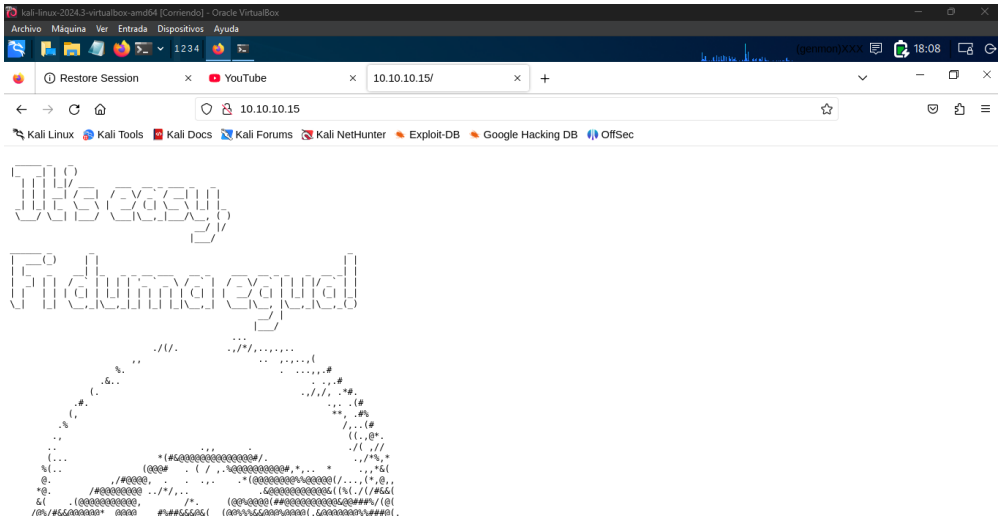

Ilustración 7página de Lampiao

Ingresé a una página web que corre en el puerto **1898** de la dirección IP **10.10.10.15**, a la cual accedí desde Kali Linux en una máquina virtual. En la parte izquierda aparece un panel de inicio de sesión donde se solicitan usuario y contraseña, además de enlaces para crear una nueva cuenta o recuperar la clave.

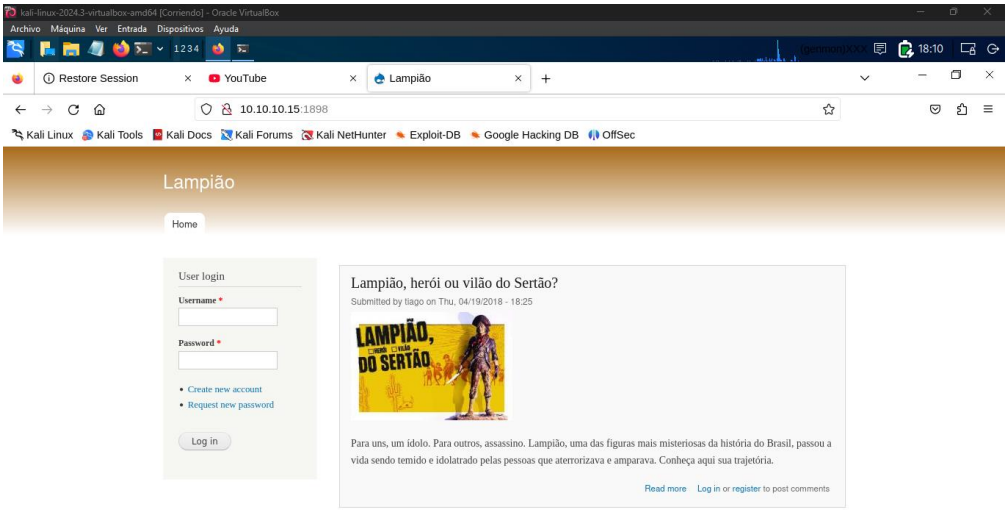

Ilustración 8página web que corre en el puerto 1898

Al pulsar “Login” el sistema respondió con un recuadro rojo que decía: *“Sorry, unrecognized username or password. Have you forgotten your password?”*. En la misma área del panel de login se ven también los enlaces **Create new account** y **Request new password**, lo que indica opciones para registrar una cuenta nueva o recuperar la contraseña si corresponde.

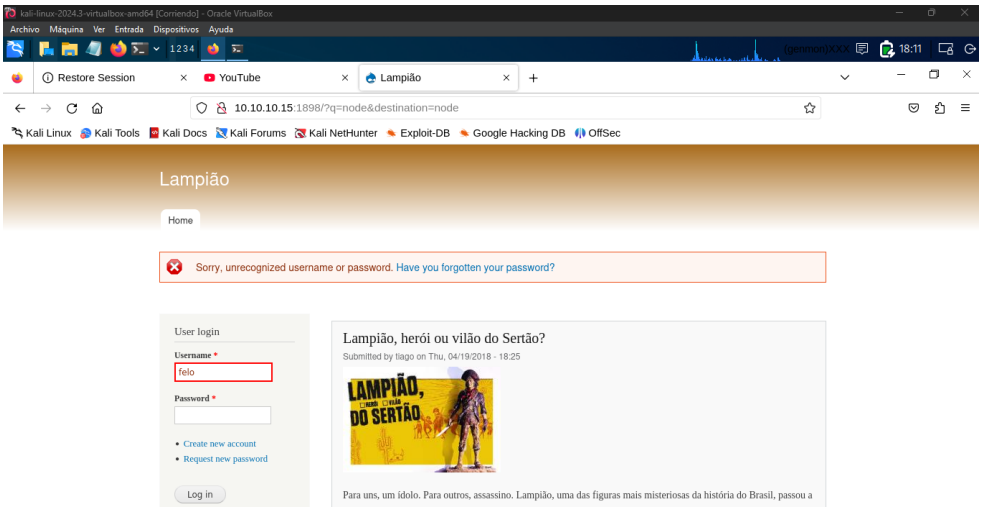

Ilustración 9Login

Abrí una terminal como root en mi máquina Kali y ejecuté un escaneo dirigido contra la IP objetivo. El comando que usé fue nmap -p 22 10.10.10.15 -A -sC, para probar específicamente el puerto SSH y obtener información adicional del servicio. El resultado mostró que el puerto **22** está abierto y responde con **OpenSSH 6.6.1p1** (típico de una instalación de Ubuntu), y además listó las claves host (DSA/RSA/ECDSA/ED25519) como parte de la huella del servidor.

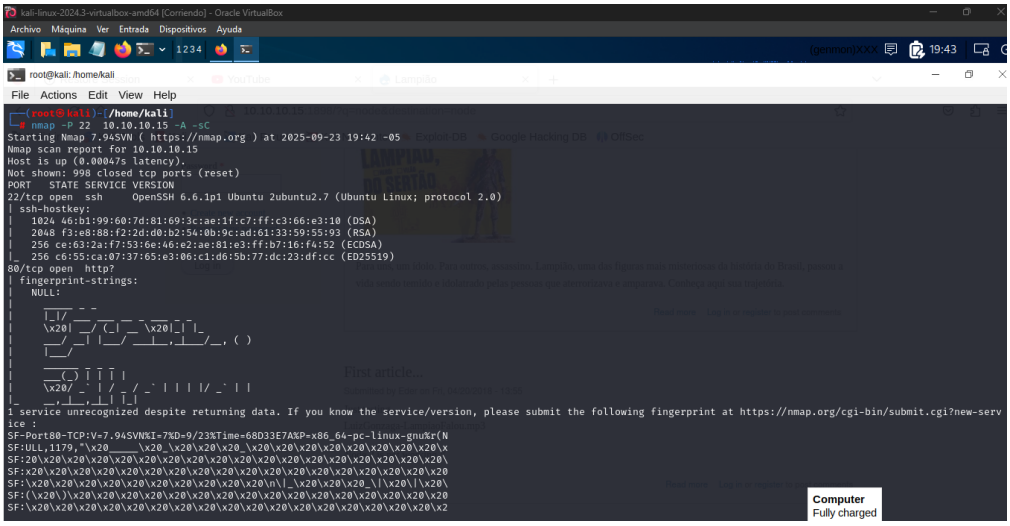

Ilustración 10dirigido contra la IP objetivo

Msfconsole

Abrí una terminal en Kali y lancé msfconsole para preparar las herramientas de pruebas; al iniciarlo aparecieron unos mensajes que bloqueaban accesos de prueba y una frase en rojo que decía “YOU DIDN’T SAY THE MAGIC WORD”, pero luego se mostró el banner de Metasploit indicando que la herramienta estaba lista y listando la cantidad de exploits, auxiliares y payloads disponibles; con eso dejé la consola preparada para las siguientes pruebas, documentando la salida como evidencia.

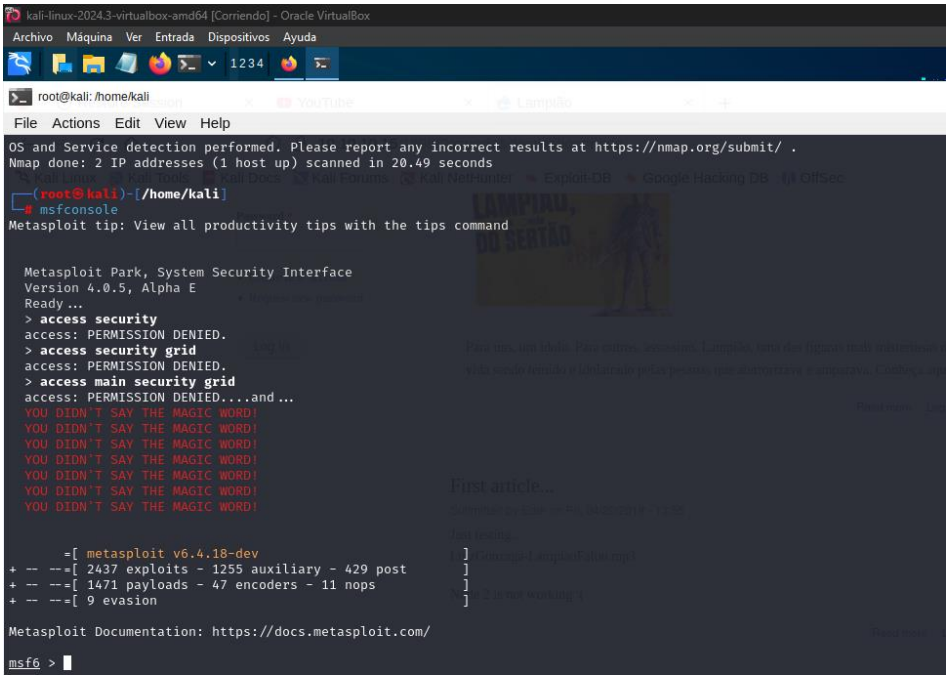

Ilustración 11msfconsole

busqué módulos relacionados con **OpenSSH** para ver qué herramientas tenía disponibles; la búsqueda me devolvió una lista de módulos y auxiliares (por ejemplo, para recopilar credenciales, enumerar usuarios SSH o probar autenticaciones) con su nombre y una breve descripción. Revisé esa lista para identificar qué módulos podrían ser útiles en la fase de reconocimiento y dejé registrada la salida en una captura como evidencia de la preparación de la herramienta antes de continuar con la práctica.

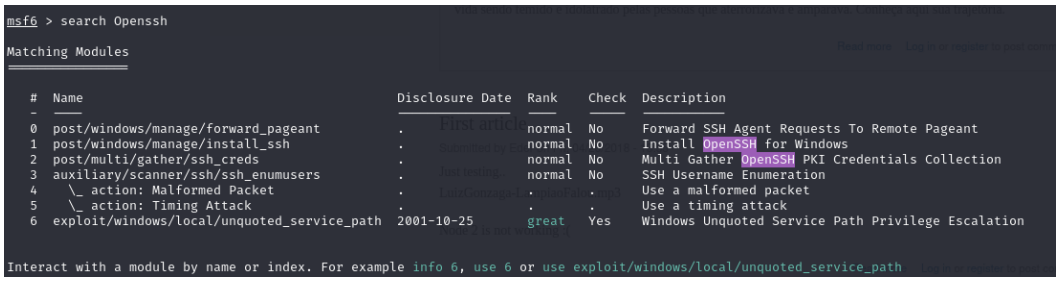

Ilustración 12OpenSSH

Seleccioné un módulo auxiliar para probar inicios de sesión por SSH contra la máquina 10.10.10.15; una vez cargado, revisé las opciones del módulo (qué archivos de usuarios o contraseñas puede usar, el puerto objetivo, la velocidad y el número de hilos, entre otros) para entender exactamente qué hace y qué parámetros admite. Dejé esa configuración documentada en la captura como parte de la preparación de la herramienta antes de tomar cualquier otra acción, asegurándome de no ejecutar nada sin la autorización correspondiente.

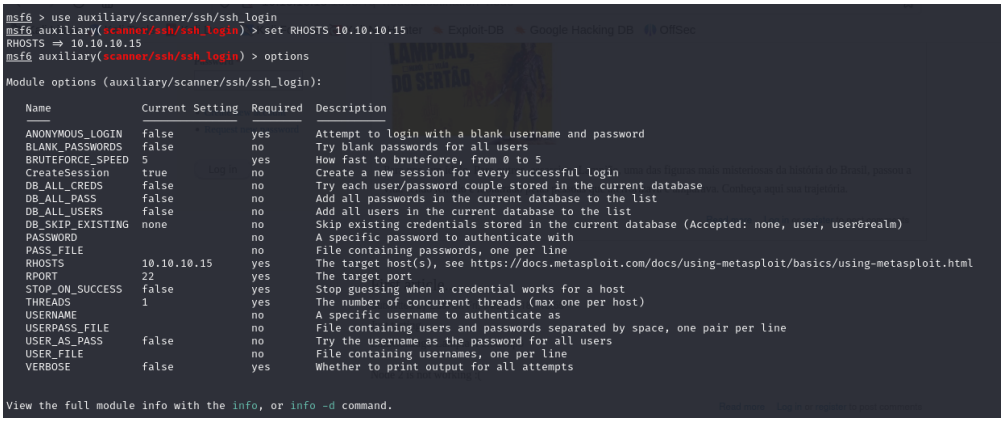

Ilustración 13módulo auxiliar

Cargué el módulo de comprobación de inicios de sesión por SSH en Metasploit y lo configuré para que intente acceder a la máquina objetivo usando el usuario **root**; además le indiqué que utilice la lista de contraseñas **rockyou.txt** como archivo de pruebas. Guardé esa configuración en la consola para tenerla lista en caso de que continúe con la prueba dentro del alcance del laboratorio.

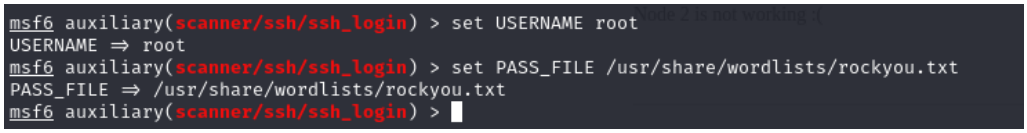

Ilustración 14módulo de comprobación

Primero se configuró el nombre de usuario como **root**, que suele ser la cuenta principal en muchos sistemas. Después se indicó un archivo de contraseñas llamado **rockyou.txt**, el cual es muy utilizado para pruebas de fuerza bruta porque contiene una gran cantidad de contraseñas comunes. Finalmente, se ejecutó el comando **run** para iniciar el proceso de intento de conexión.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME root
USERNAME ⇒ root
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE ⇒ /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

Ilustración 15nombre de usuario como root

Crear diccionario

Usé **CeWL** para generar una lista de palabras personalizada a partir del contenido publicado en el servicio web del objetivo. Ejecuté CeWL apuntando a la URL (http://10.10.10.15:1898/) y guardé el resultado en un archivo llamado **DicLampiao.txt**. Después verifiqué en el sistema que el archivo se había creado correctamente listando el directorio y comprobando la presencia de *DicLampiao.txt*.

```
┌──(root㉿kali)-[/home/kali]
└─# cewl http://10.10.10.15:1898/ --write DicLampiao.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop          Downloads            Laboratorio-felipe  Public
DicLampiao.txt   Escritorio           Music               Templates
Documents        Laboratorio-asprilla Pictures            Videos
```

Ilustración 16archivo llamado DicLampiao.txt

Verifiqué que **DicLampiao.txt** tiene **844** entradas. Recomendación: si la prueba fue autorizada, comprobar si alguna credencial funcionó y, de ser así, mitigar (deshabilitar root por SSH, usar claves y contraseñas fuertes). Si no está autorizada, detener la actividad.

Ilustración 17Verifiqué que DicLampiao.txt

Mostré el contenido del diccionario generado (**DicLampiao.txt**): es una lista de palabras extraídas del sitio objetivo —muchas en portugués— como *Lampião, bando, cangaceiros, morte*, además de términos comunes de página web (*password, account, footer, menu*).

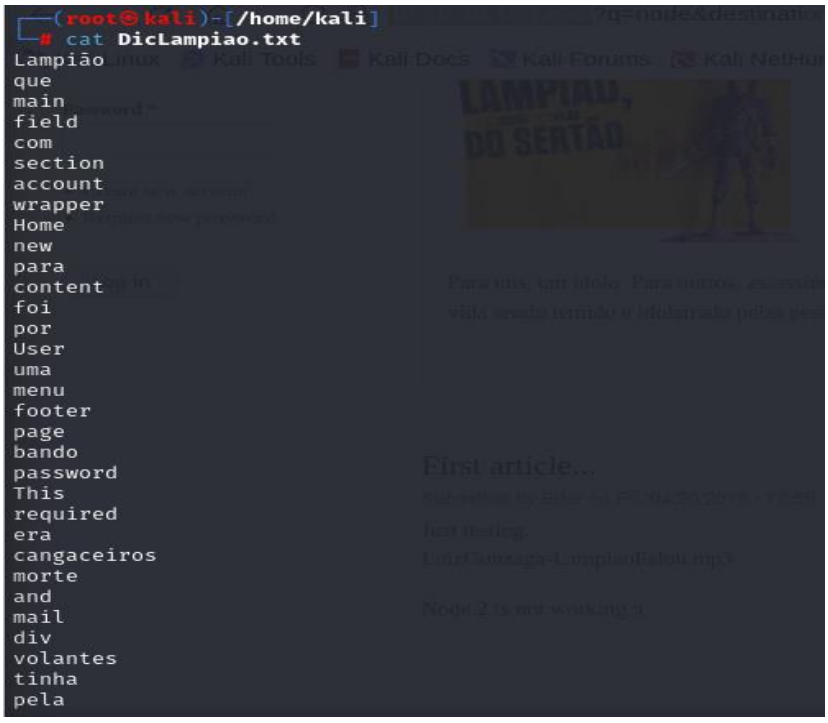

Ilustración 18contenido del diccionario generado

comprobé la ayuda de Hydra para entender qué parámetros puedo usar y qué servicios soporta, como paso previo a realizar pruebas controladas. Recomendación rápida: utiliza esta herramienta solo con autorización explícita, documenta cualquier intento (objetivo, listas usadas y resultados) y, si se encuentran accesos, propon medidas concretas como deshabilitar login root, exigir autenticación por clave y aplicar políticas de bloqueo/alerta ante intentos repetidos.

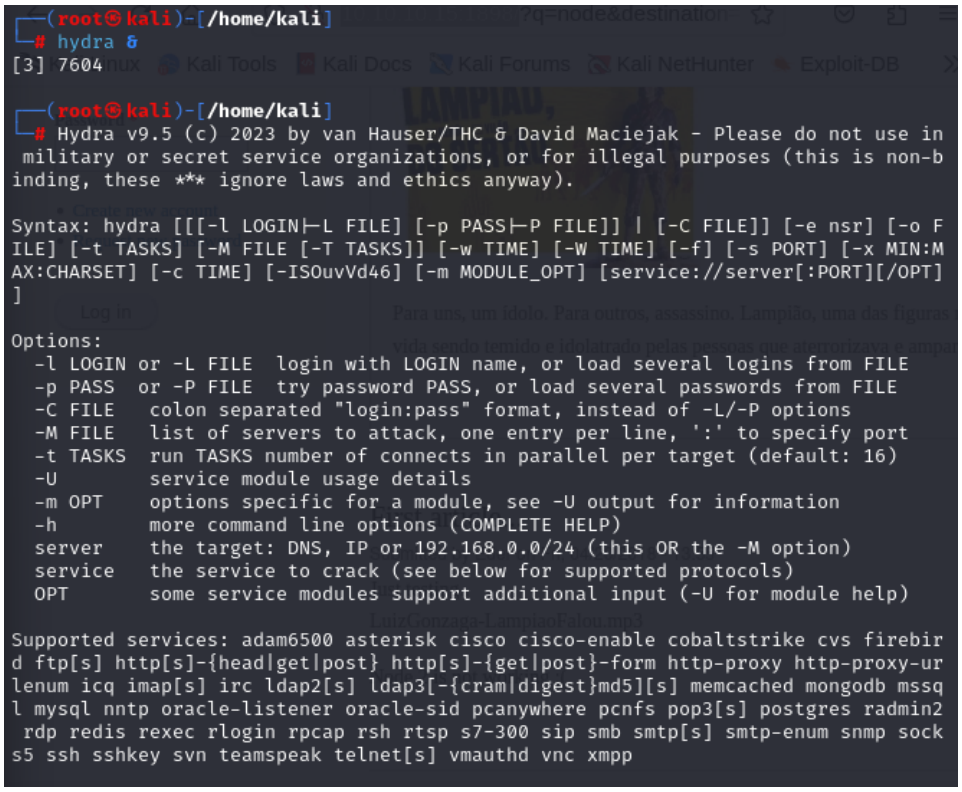

Ilustración 19comprobé la ayuda de Hydra

Ejecuté un ataque de fuerza bruta con **Hydra** usando el usuario **tiago** y el diccionario generado **DicLampiao.txt** contra el servicio SSH del objetivo (10.10.10.15). Hydra probó las ~844 entradas del archivo (con varios hilos en paralelo) y consiguió **una credencial válida**: usuario **tiago** con la contraseña **Virgulino**. La herramienta dejó además mensajes informando

sobre tareas en paralelo y un archivo de restauración porque algunos hilos no terminaron a tiempo.

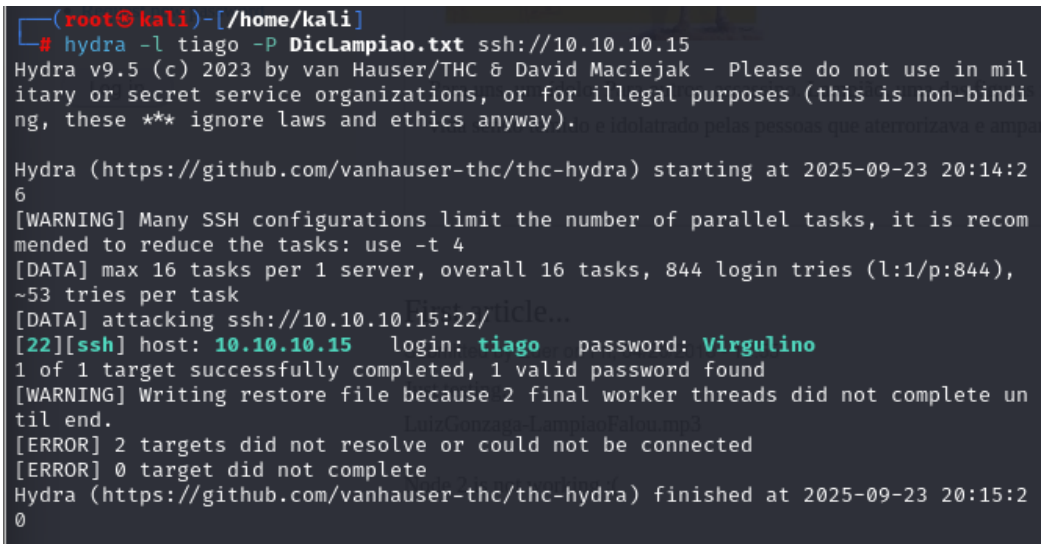

Ilustración 20ataque de fuerza bruta con Hydra

Ingreso por ssh tiago@10.10.10.15

Me conecté por SSH al objetivo usando la cuenta **tiago** y la contraseña encontrada (**Virgulino**), y obtuve acceso al sistema (se muestra el mensaje de bienvenida de Ubuntu y la información básica del equipo). En términos sencillos: tras descubrir la credencial válida, inicié sesión correctamente y quedé en un shell del usuario **tiago** en la máquina 10.10.10.15.

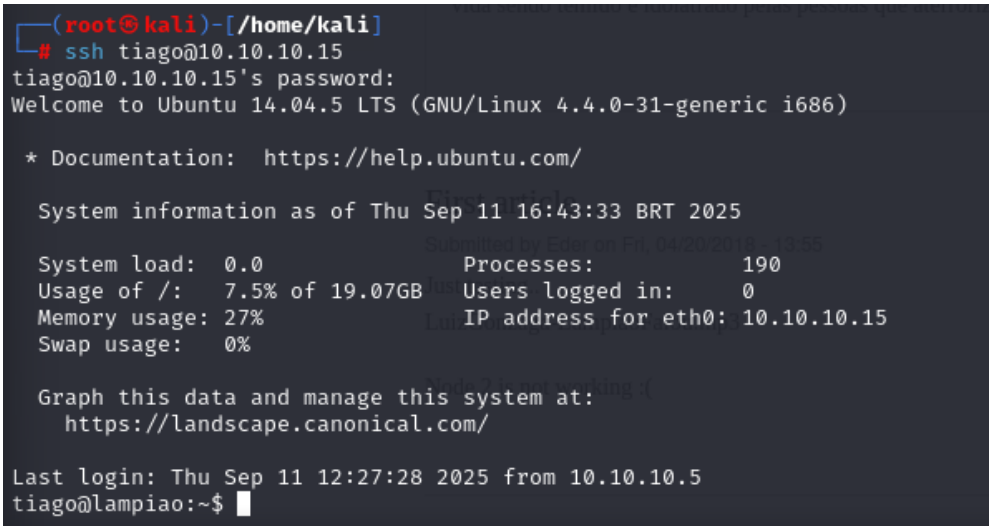

Ilustración 21conecté por SSH

Busqué en Google la herramienta de enumeración local **LinEnum** (repositorio de *rebootuser*) y abrí la página del proyecto en GitHub. Desde allí copié la URL para clonar el repositorio (o bien descargar el ZIP) para obtener el script **LinEnum.sh**. El objetivo de este paso fue conseguir una herramienta de enumeración local que me permita, una vez dentro del sistema, revisar configuraciones, servicios y posibles vectores de escalada de privilegios.

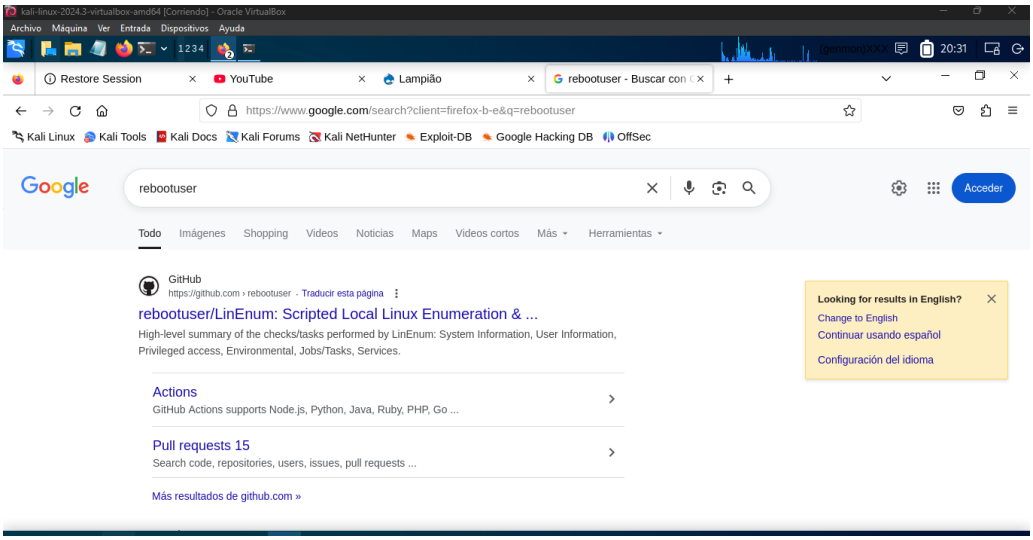

Ilustración 22enumeración local LinEnum

Revisé el README y el código para entender qué hace el script y evitar acciones indeseadas; luego transferiría el script al objetivo y lo ejecutaría con permisos adecuados solo si la prueba está autorizada.

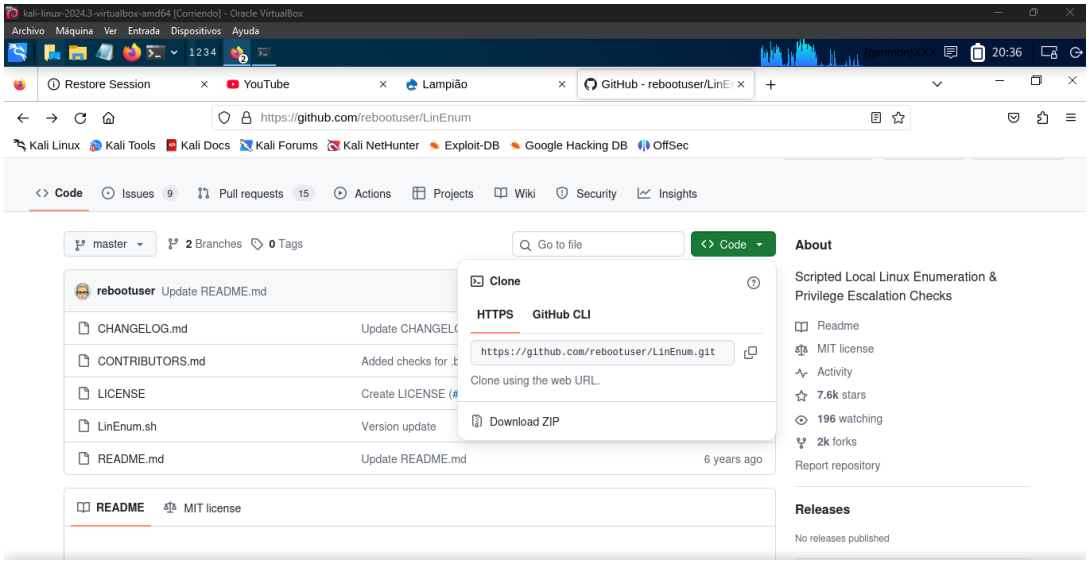

Ilustración 23README

Cloné correctamente el repositorio **LinEnum** desde GitHub (salida muestra que se descargaron y resolvieron los objetos: *Cloning into 'LinEnum'... Receiving objects: 100%*).

También revise el README y el contenido del script para entender qué hace; mover o transferir el script al sistema objetivo de forma segura; marcarlo ejecutable y lanzarlo para recopilar información local (salida, archivos y hallazgos) y luego analizar esos resultados en busca de posibles vectores de escalada.

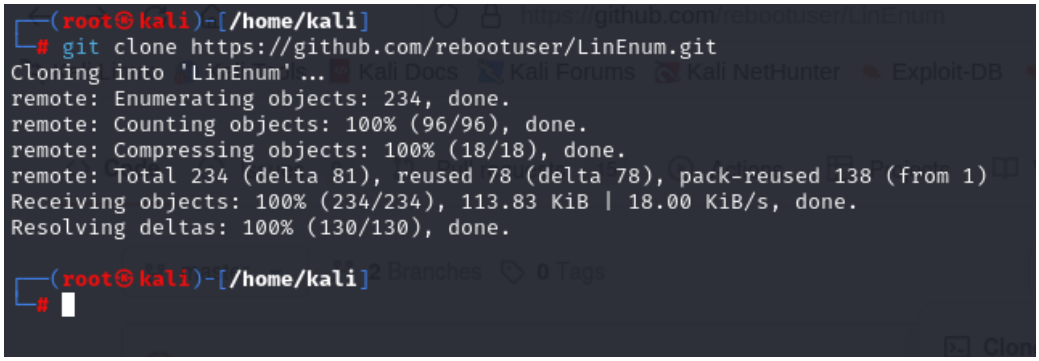

Ilustración 24Cloné correctamente el repositorio LinEnum

Intenté acceder a una carpeta llamada **LinEnum** usando el comando cd LinEnum, pero el sistema me devolvió un error indicando que no existía dicho directorio. Luego de verificar con el comando ls, noté que efectivamente el directorio no estaba en ese momento, por lo que asumí que podría haberme equivocado en la ubicación inicial.

Después cambié correctamente al directorio /home/kali/LinEnum, donde ya se encontraba el proyecto. Allí ejecuté ls y se listaron varios archivos, incluyendo documentación como CHANGELOG.md, CONTRIBUTORS.md, LICENSE, README.md, y el script principal LinEnum.sh, que es el que realmente me interesaba.

Ilustración 25carpeta llamada LinEnum

Después de ubicarme correctamente en el directorio del script (/home/kali/LinEnum), accedí al archivo principal **LinEnum.sh** usando el editor de texto nano. Al abrir el script, pude observar que está escrito en **Bash**, y su función principal es automatizar la enumeración de información del sistema desde un host Linux.

En las primeras líneas del código se muestra una sección de ayuda (#help function) en la que se describen los parámetros que se pueden usar al ejecutar el script.

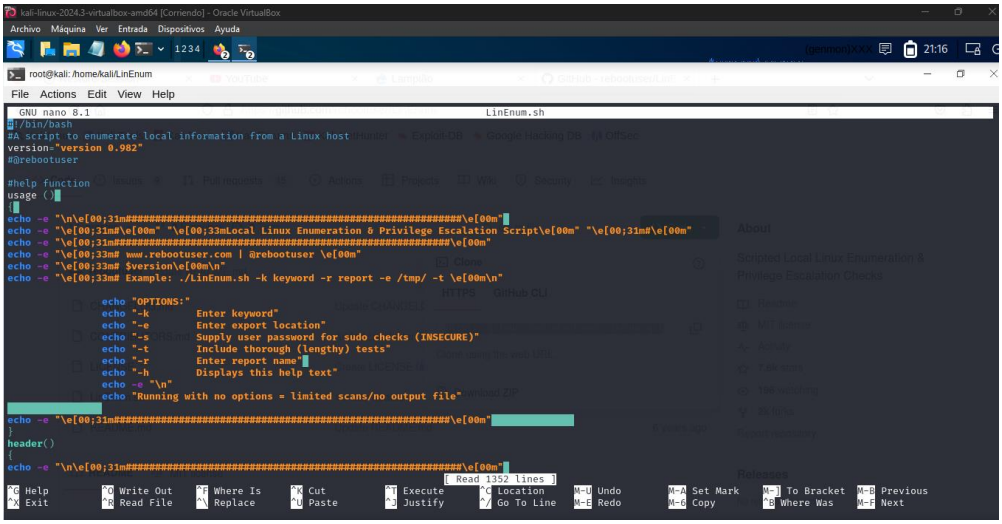

Ilustración 26directorio del script

Intenté listar el contenido de /home utilizando el comando ls, pero obtuve un error porque escribí mal el comando (ls /home en lugar de solo ls o cd /home). Luego, corregí el comando y accedí exitosamente al directorio /home, donde encontré un usuario llamado **tiago**.

Dentro del directorio /home/tiago, abrí un archivo con nombre **tiago** usando nano tiago, pero no se mostró el contenido en esta captura, por lo que probablemente era un archivo de texto sin información relevante. También utilicé ls -la para observar los permisos de los archivos y carpetas, confirmando que el propietario era el usuario **tiago**, y que las carpetas fueron creadas

en abril de 2018, lo cual indica que este sistema no es nuevo o ha sido restaurado desde una copia antigua.

Posteriormente, regresé al directorio raíz / y comencé a explorar el sistema de archivos, específicamente la carpeta **/var**, que comúnmente contiene archivos de logs, datos de servicios y carpetas temporales. Dentro de /var utilicé ls para listar su contenido y observé varias subcarpetas importantes como log, mail, spool, www, y tmp.

Ilustración 27/home utilizando el comando ls

Aquí, se observan varias líneas con diferentes usuarios y rutas asociadas, la mayoría de ellos tienen asignado un shell como /usr/sbin/nologin, lo que generalmente significa que no pueden iniciar sesión en el sistema.

Ilustración 28shell como /usr/sbin/nologin

Se muestra el contenido del archivo /etc/passwd visto desde una terminal de Linux, el cual contiene información sobre las cuentas de usuario del sistema. Se puede ver que el usuario principal es “tiago”, ya que tiene asignado el shell /bin/bash, lo que indica que puede iniciar sesión normalmente. El resto de las cuentas, como sshd, daemon, games, www-data, entre otras, están configuradas con el shell /usr/sbin/nologin o similares, lo cual significa que son cuentas de sistema o de servicio y no están destinadas para que alguien inicie sesión con ellas.

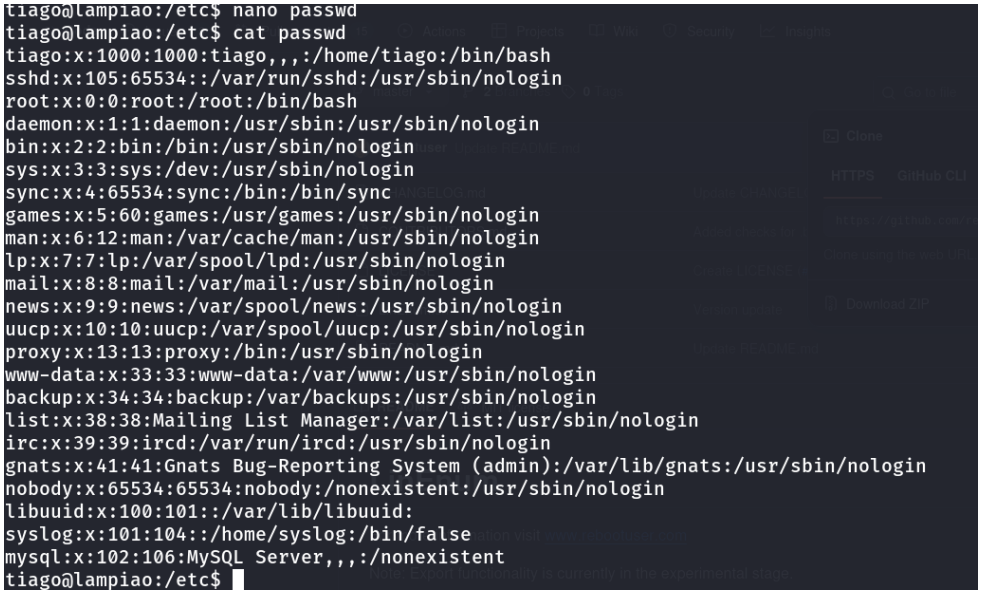

Ilustración 29/etc/passwd

Ejecute el comando find / -perm -4000 2>/dev/null, que sirve para buscar archivos con el **bit SUID** activado. Estos archivos se ejecutan con los permisos del dueño (usualmente el usuario root), lo que puede ser un riesgo de seguridad si alguno es explotable. Entre los resultados están comandos como /bin/su, /usr/bin/passwd, /usr/bin/sudo, /bin/ping, entre otros, los cuales son normales, pero también pueden ser aprovechados en ataques de escalada de privilegios si no están bien protegidos.

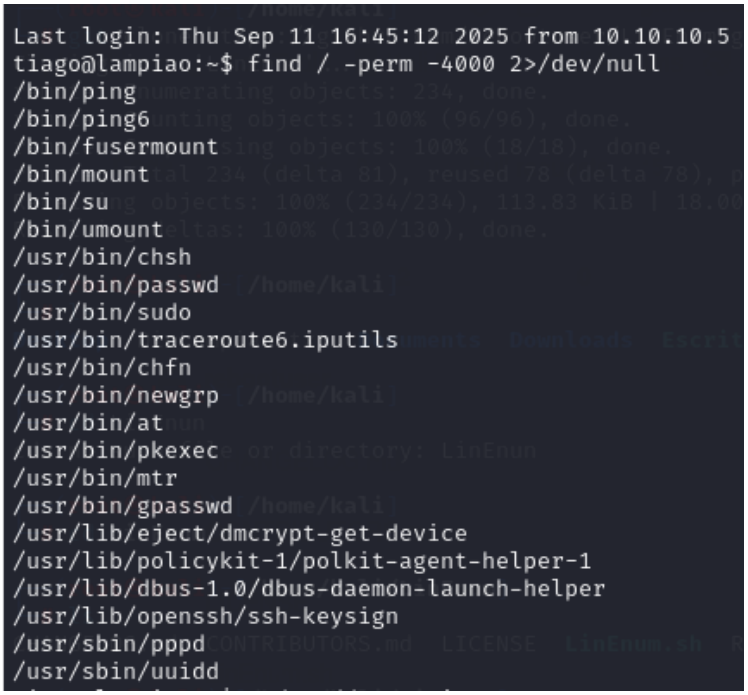

Ilustración 30comando find / -perm -4000 2>/dev/null

Recomendaciones

- Deshabilitar el acceso SSH para el usuario root y exigir autenticación por clave pública.
- Implementar políticas de bloqueo ante múltiples intentos fallidos de login.
- Mantener actualizados los servicios y sistemas operativos para evitar vulnerabilidades conocidas.
- Auditar periódicamente los archivos con permisos SUID y restringir su uso a lo estrictamente necesario.
- Utilizar contraseñas robustas y evitar el uso de credenciales comunes o predecibles.

Conclusión

El desarrollo del laboratorio permitió una inmersión profunda en el análisis de vulnerabilidades presentes en entornos virtuales, utilizando herramientas ampliamente reconocidas en el ámbito de la ciberseguridad ofensiva. A través de la interacción entre Kali Linux y la máquina vulnerable, se logró identificar servicios expuestos como SSH y HTTP, realizar escaneos detallados de red, ejecutar ataques de fuerza bruta y acceder al sistema mediante técnicas de enumeración y escalada de privilegios. Cada paso del proceso evidenció la fragilidad de sistemas que no cuentan con configuraciones seguras ni políticas de protección adecuadas.

El laboratorio representa una herramienta pedagógica valiosa para la formación de profesionales en telecomunicaciones e informática, capaces de identificar, evaluar y mitigar riesgos en sistemas reales.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Referencias Bibliográfica

Ingeniero Rafael Sandoval