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. ESCANEO NMAP – PUERTOS ABIERTOS DETECTADOS. 5
3. ANALISIS DE VULNERABILIDADES Y POSIBLES ATAQUES. 6
4. PUERTO 21 – VSFTPD 2.3.4 7
5. PUERTO 22 OPENSSH 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	postreSQL

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.

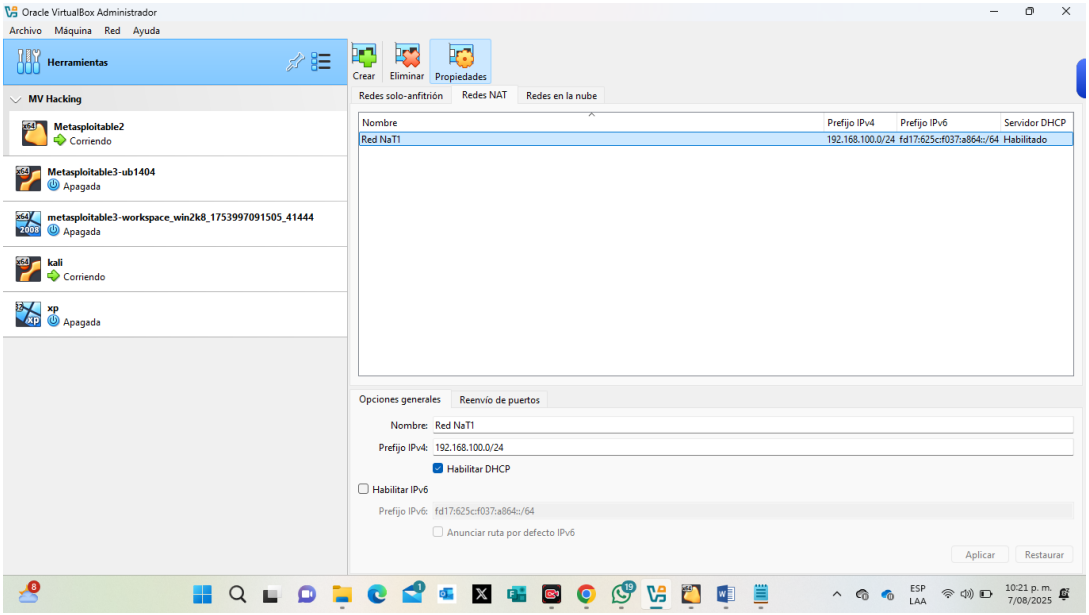

Ilustración 1 Creacion Red Nat

Como también en cada una de las máquinas virtuales.

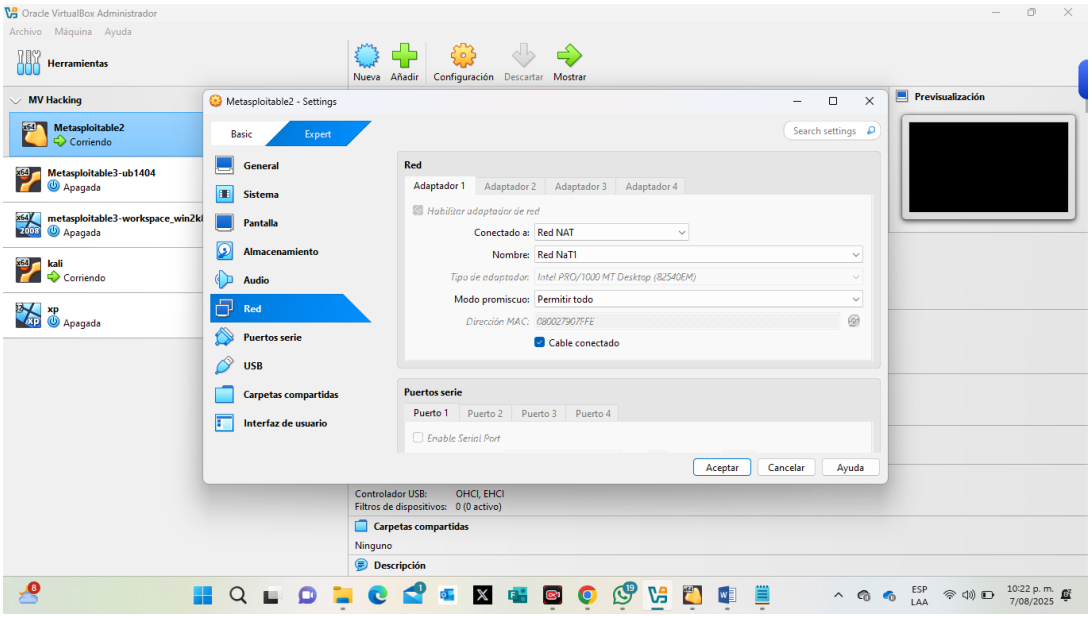

Ilustración 2 selecion de la red Nat en metasploitable2

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.

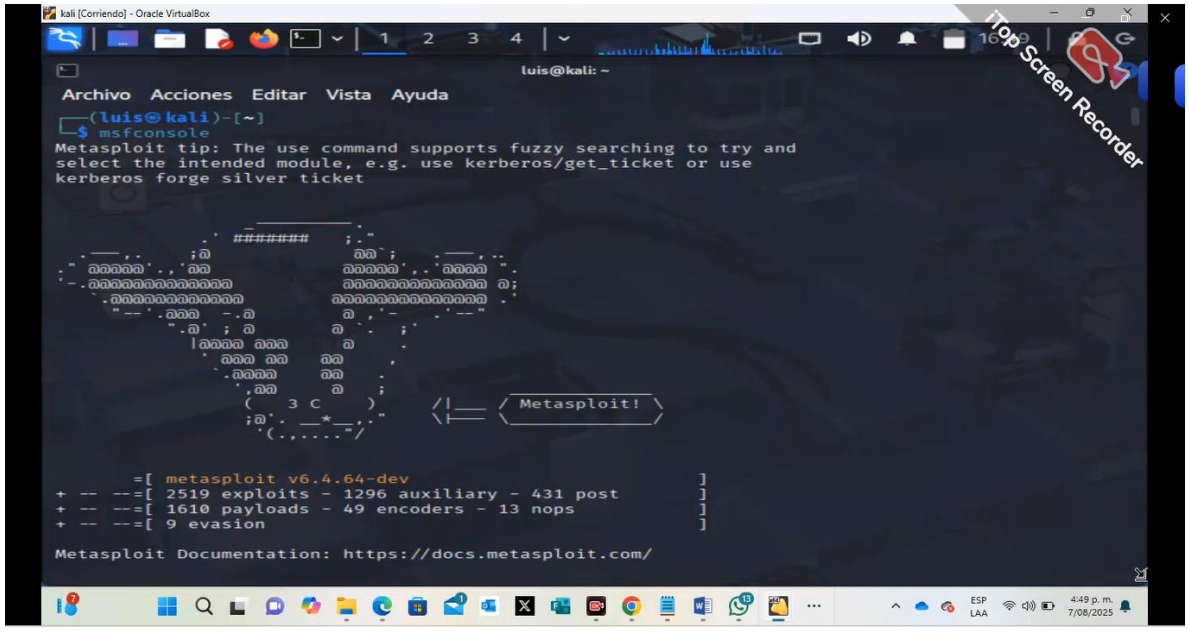

Ilustración 3 ataque PUERTO 21 – VSFTPD 2.3.4

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.

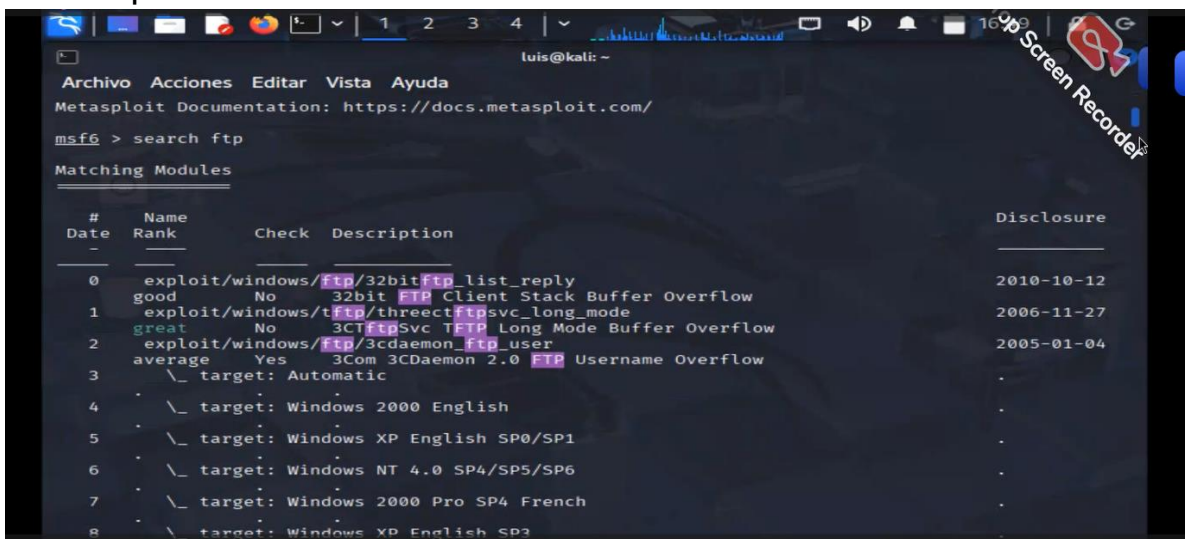

Ilustración 4 escaneo Search ftp

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

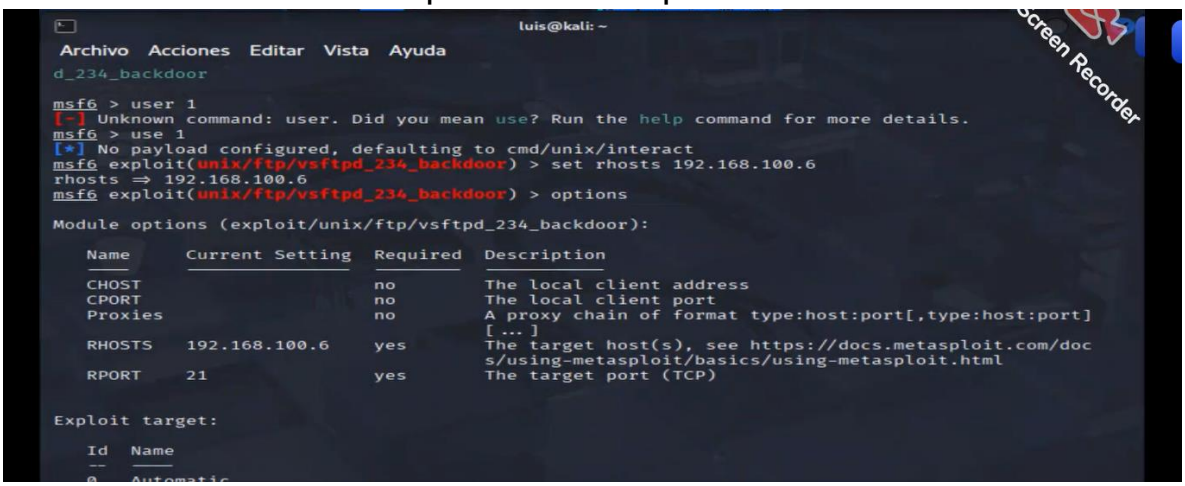

Ilustración 5 asignacion del RHOSTS

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.

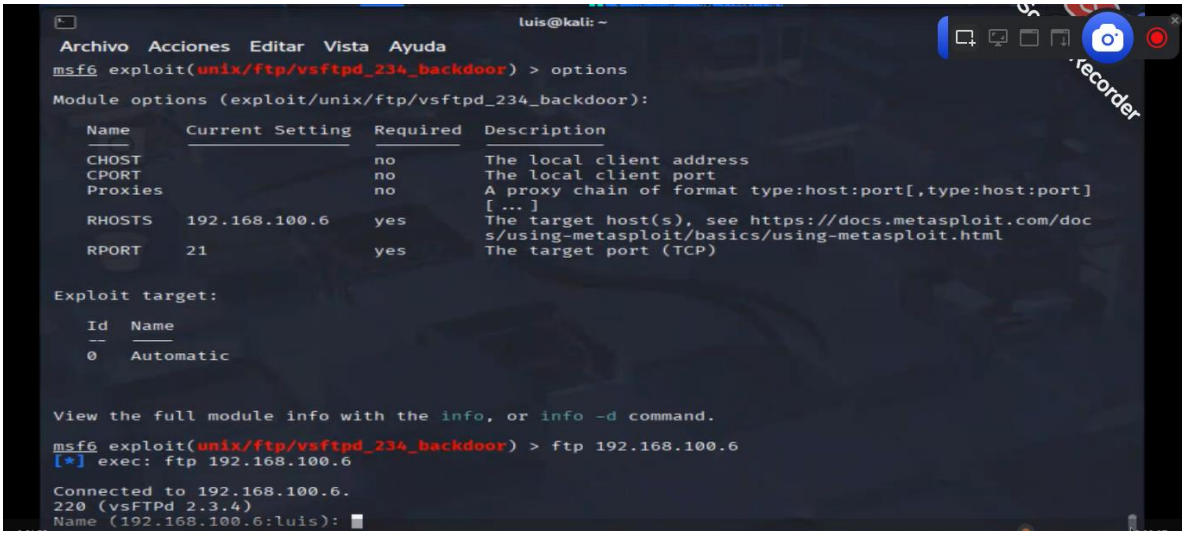

Ilustración 6 verificacion del RHOSTS y RPORT

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.

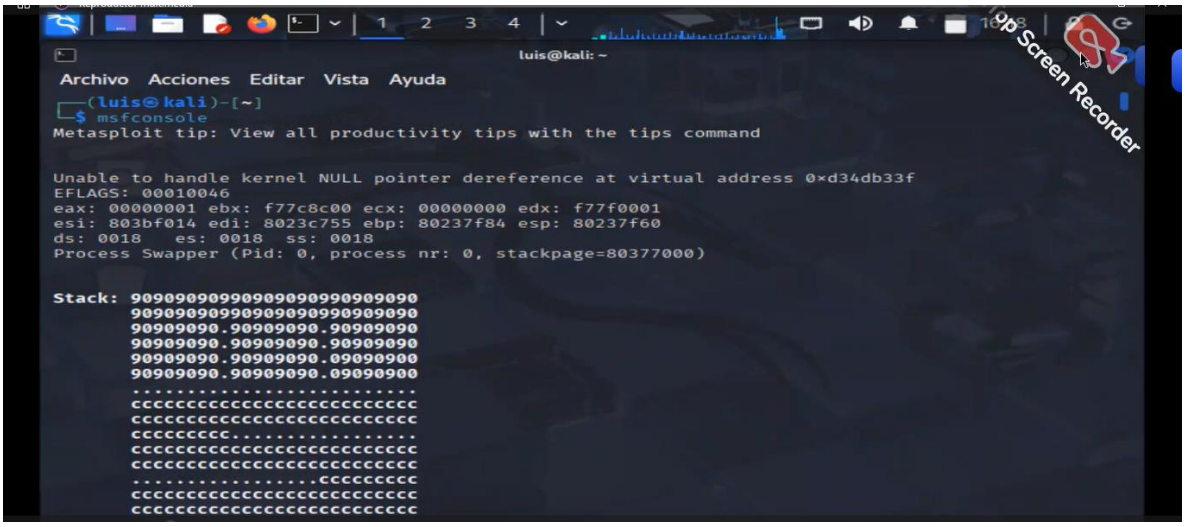

Ilustración 7 ATAQUE PUERTO 22 OPENSSH 4.7P1 DEBIAN

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.

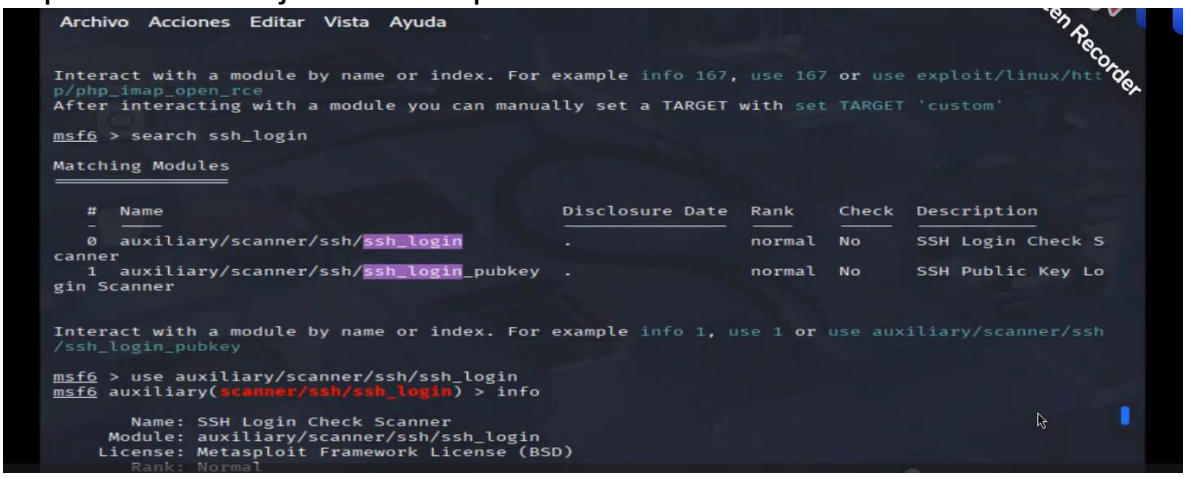

Ilustración 8 Escaneo Search SSH_LOGIN

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.

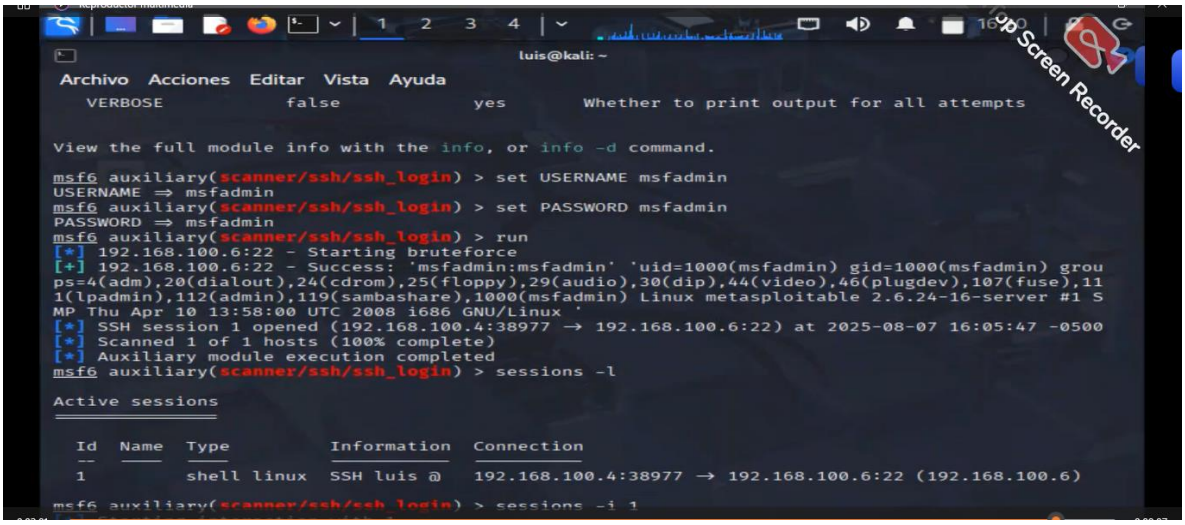

Ilustración 9 Asignacion de Usuario y Contraseña

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

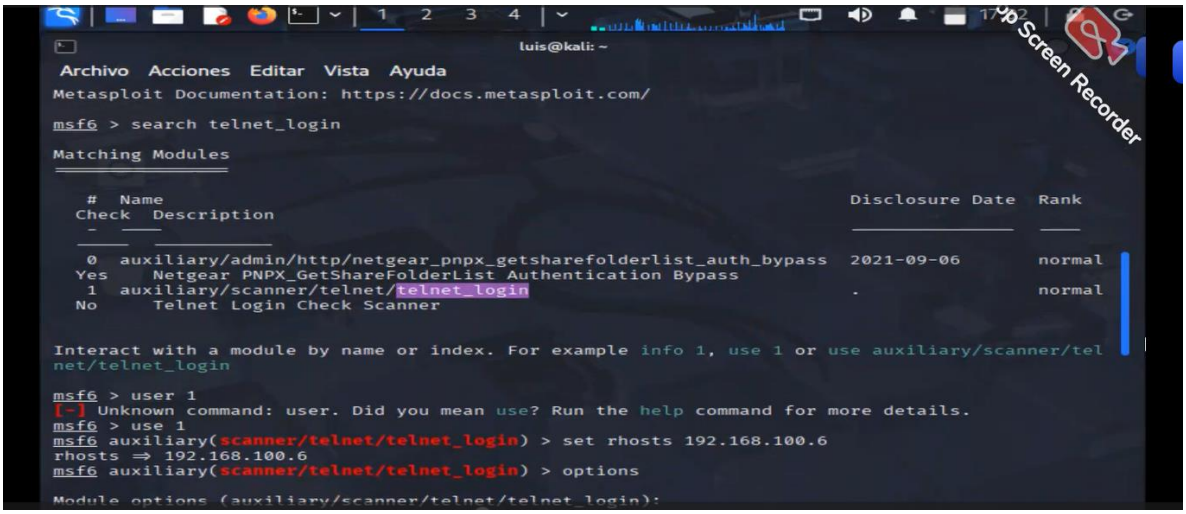

Ilustración 10 AtaquePUERTO 23 TELNET LINUX TELNETD

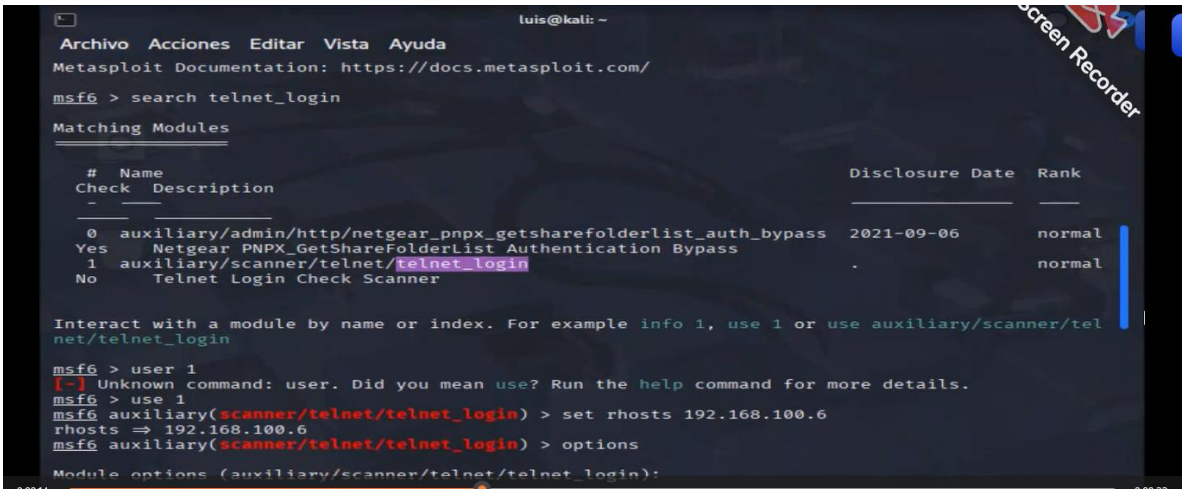

Ilustración 11 escaneo search telnet_login

7. PUERTO 25 SMTP POSTFIX SMTPD

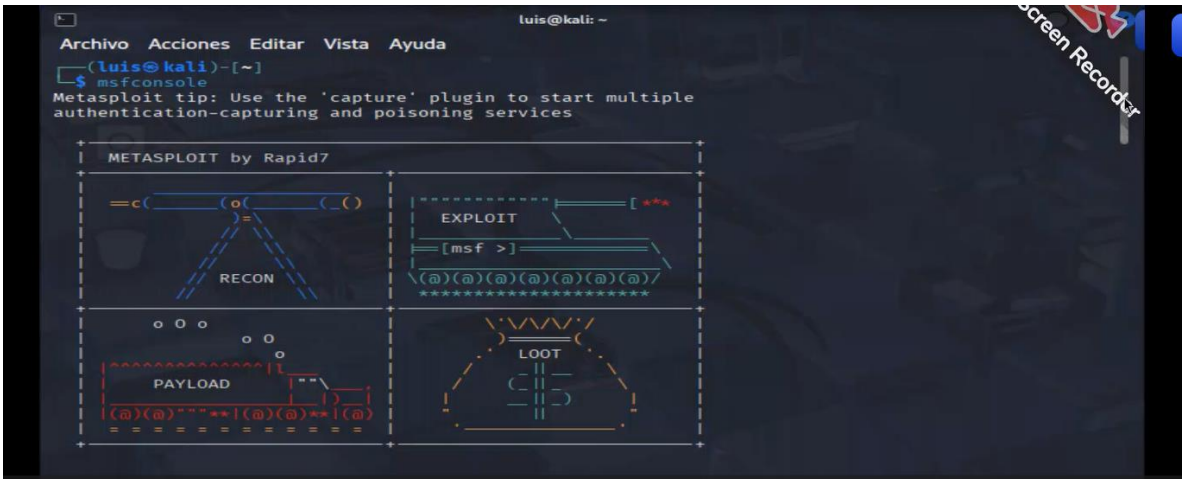

Ilustración 12 Ataque PUERTO 25 SMTP POSTFIX SMTPD

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

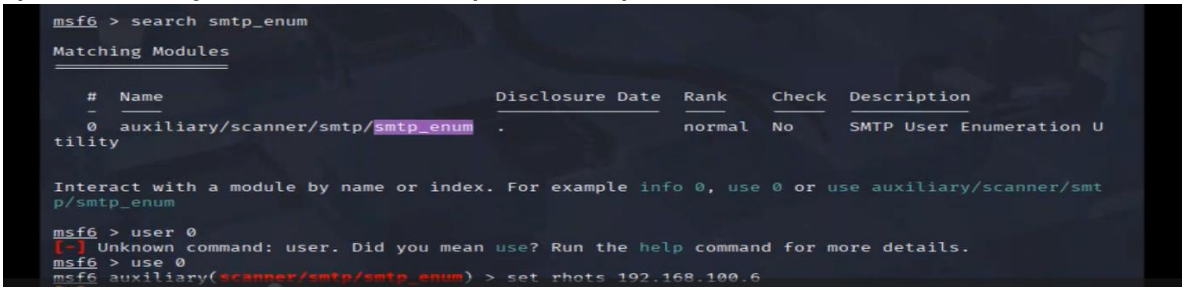

Ilustración 13 Escaneo smtp_enum

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.

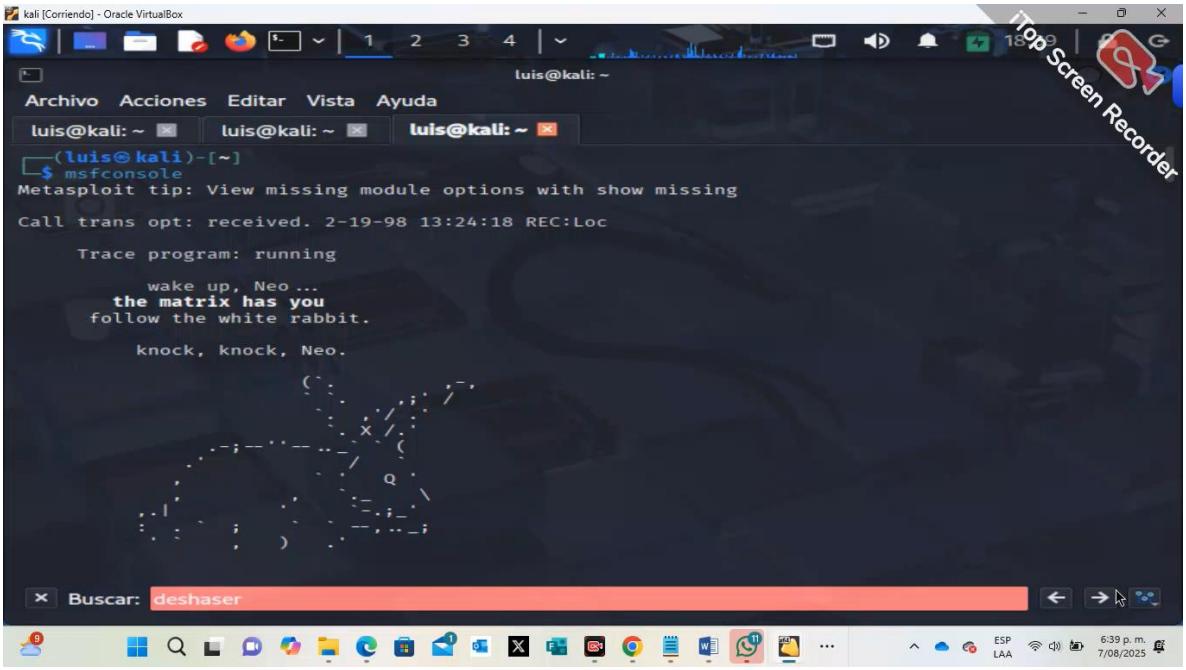

Ilustración 14 Ataque PUERTO 139 SAMBA SMB 3.x

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

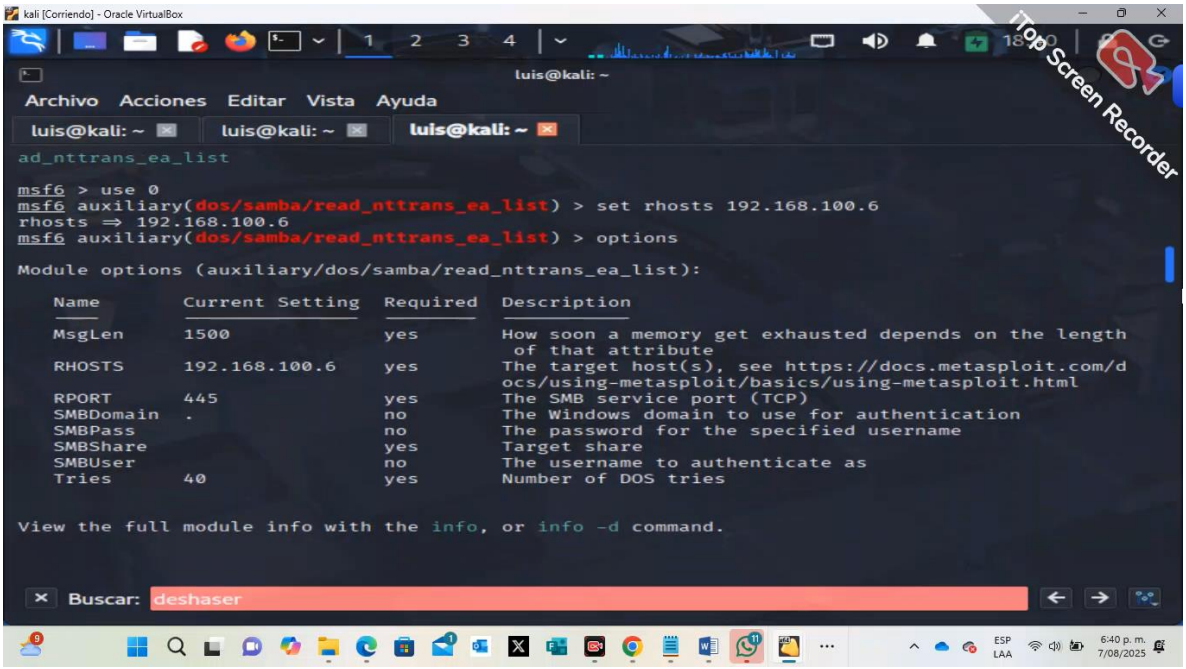

Ilustración 15 asignacion RHOSTS

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.**

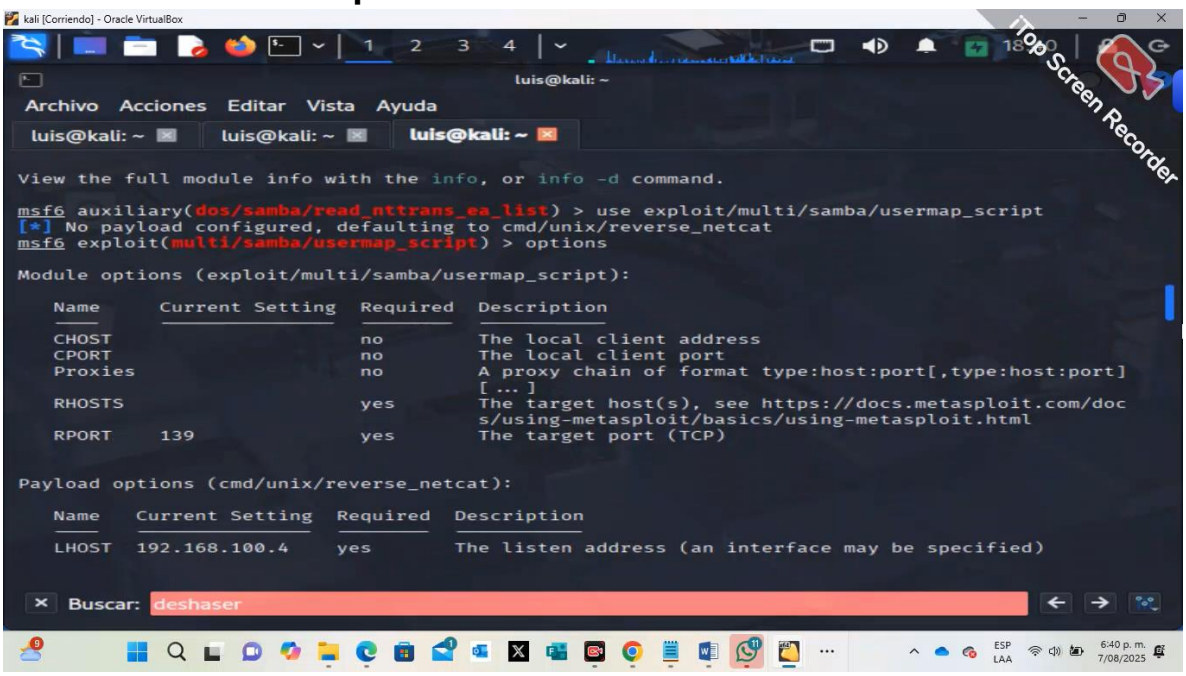

Ilustración 16 Verificacion despues de usar exploit

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

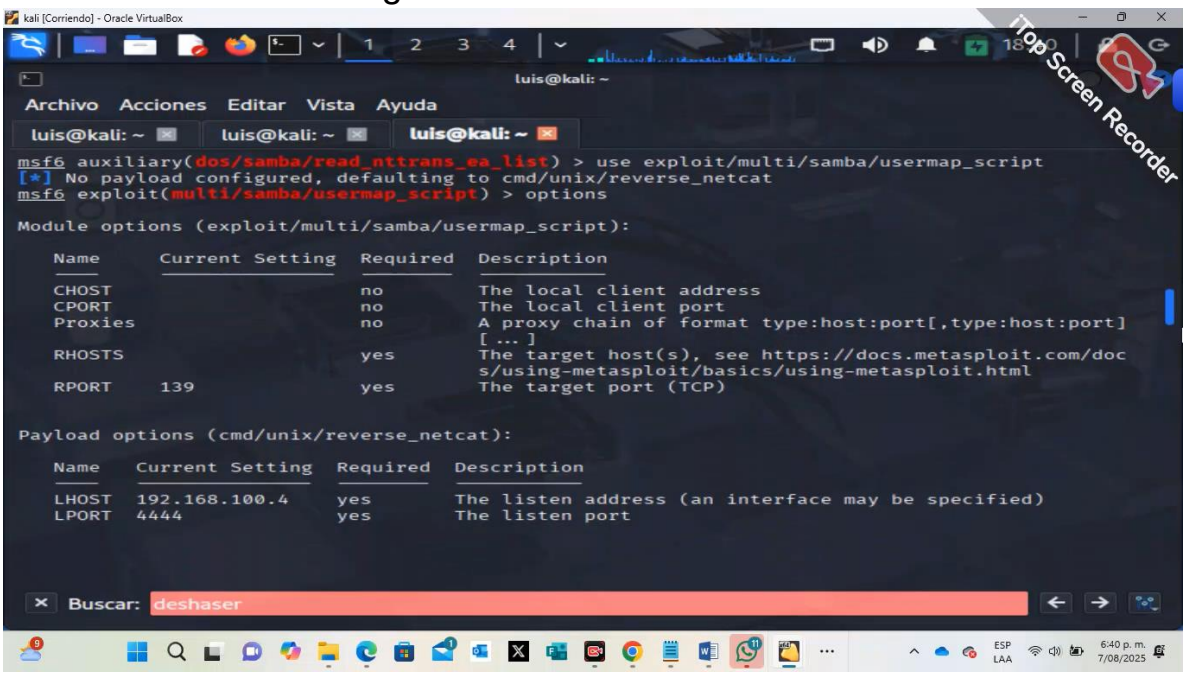

Ilustración 17 Verificacion de la ip local

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

9. PUERTO 445 SAMBA SMB SMBD 3.X

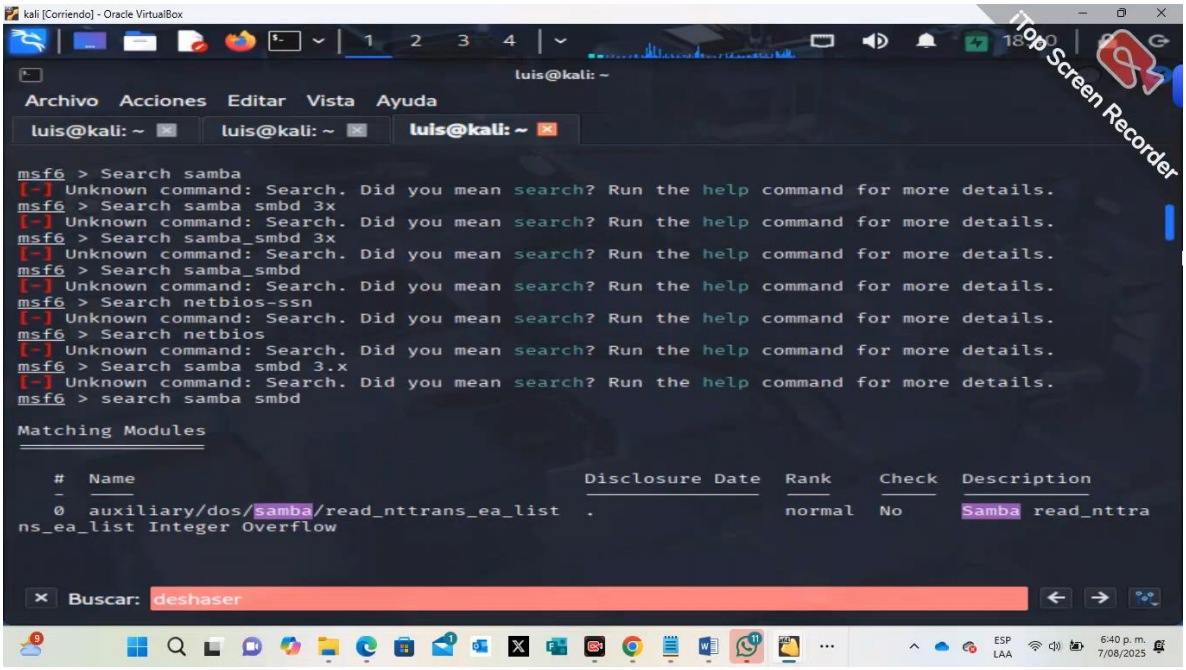

Ilustración 18 Ataque PUERTO 445 SAMBA SMB SMBD 3.X

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.

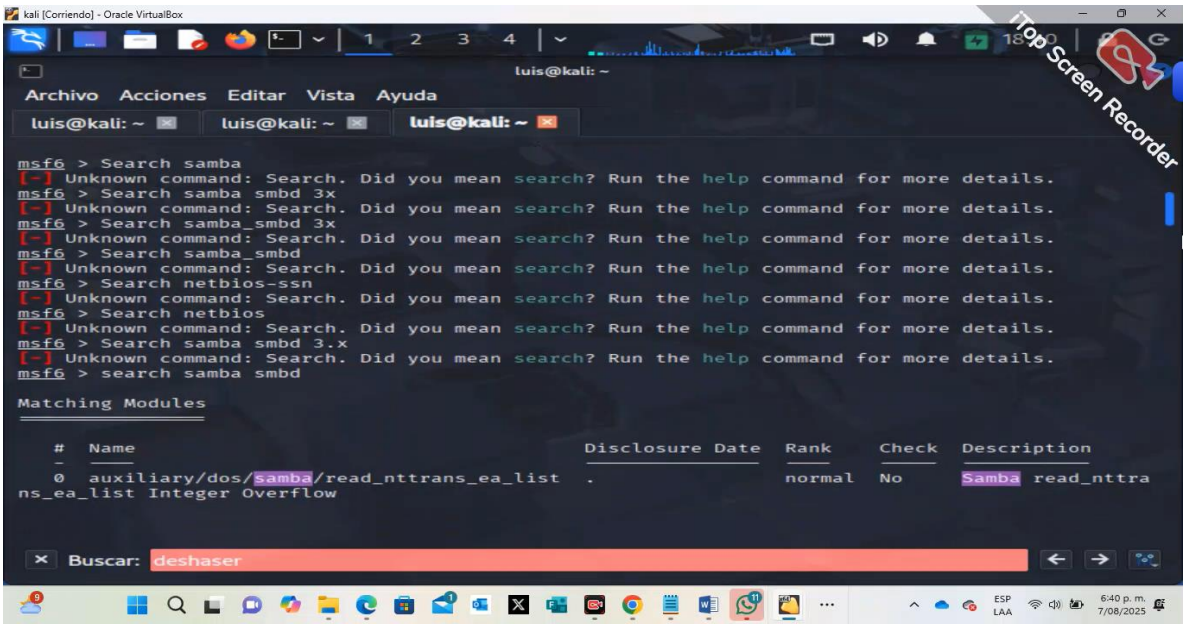

Ilustración 19 Escaneo Search samba

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

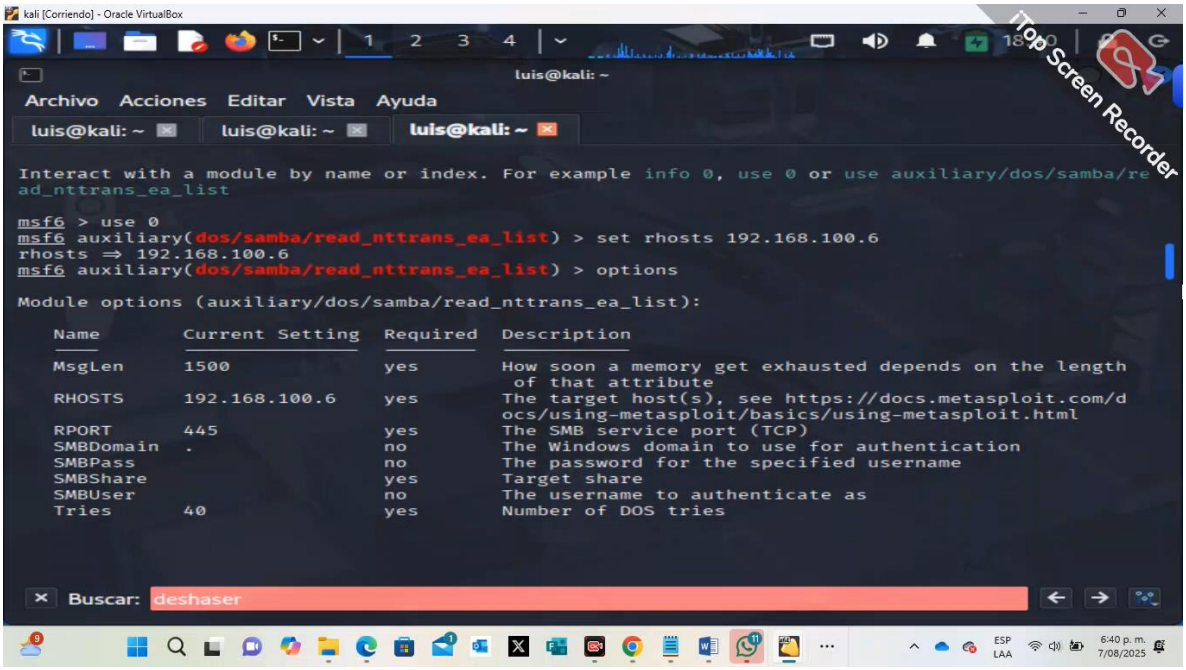

Ilustración 20 Asignacion Rhosts

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.

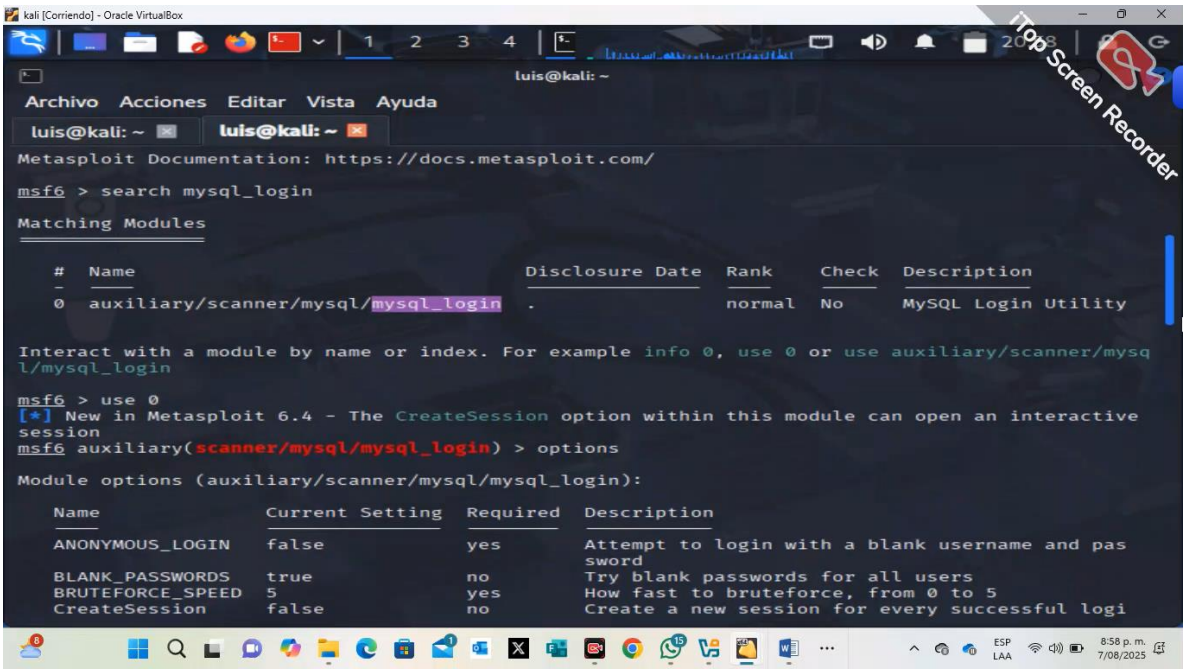

Ilustración 21 Ataque PUERTO 3306 MYSQL 5.0.51

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

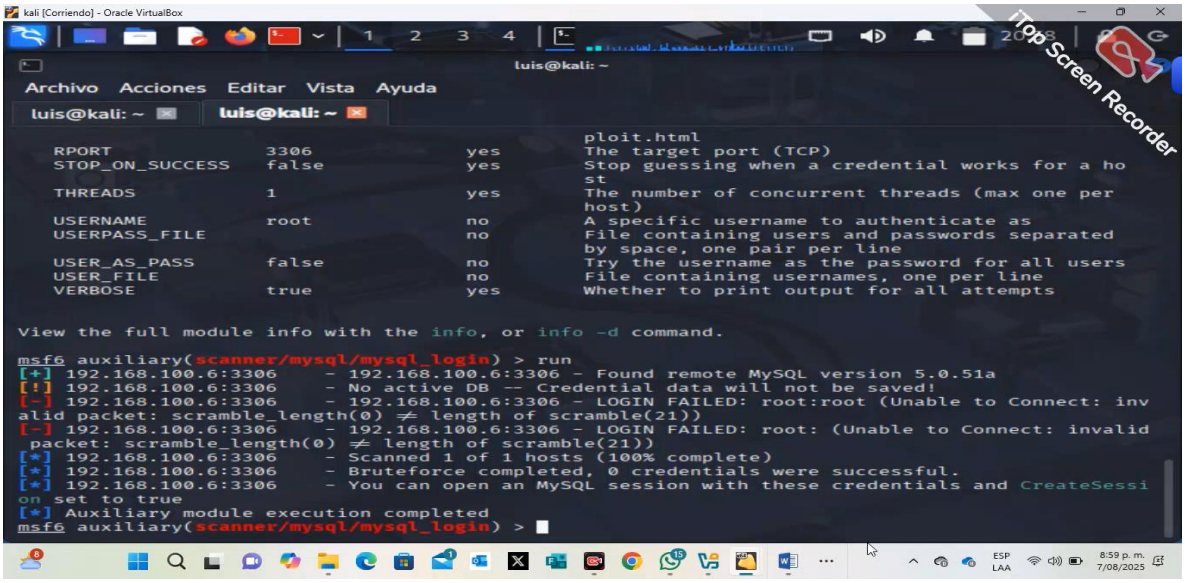

Ilustración 22 Ataque Con puerto 3306 no activo

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.