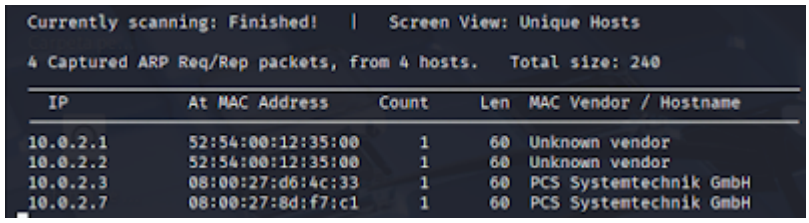
Máquina Basic (Vulnyx)

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:

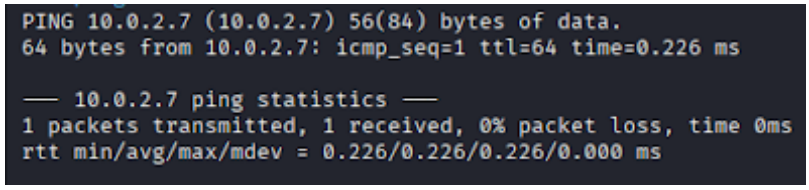
$ netdiscover -i eth1 -r 10.0.2.0/24



- **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:

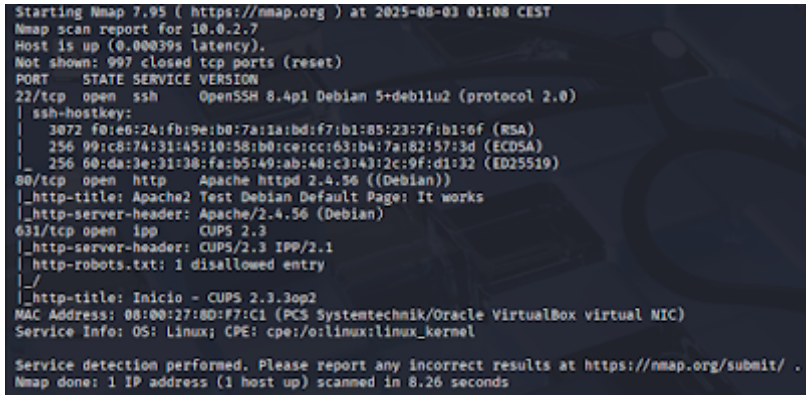
$ ping -c 1 10.0.2.7



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

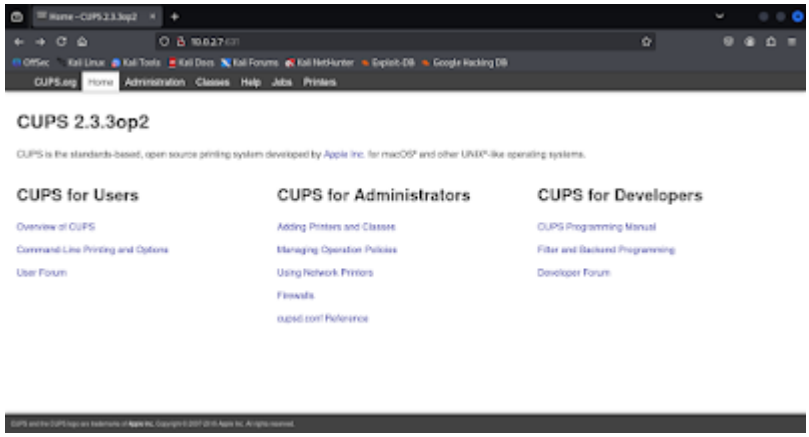
A continuación realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

$ nmap -PN 10.0.2.7 -sVC



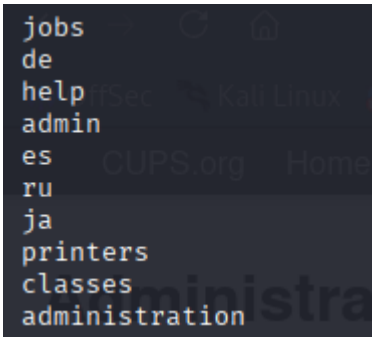
Como podemos comprobar la Máquina Víctima tiene abiertos los puertos **22**, **80** y **631**.

Comprobamos que es lo que corre en el puerto 631.



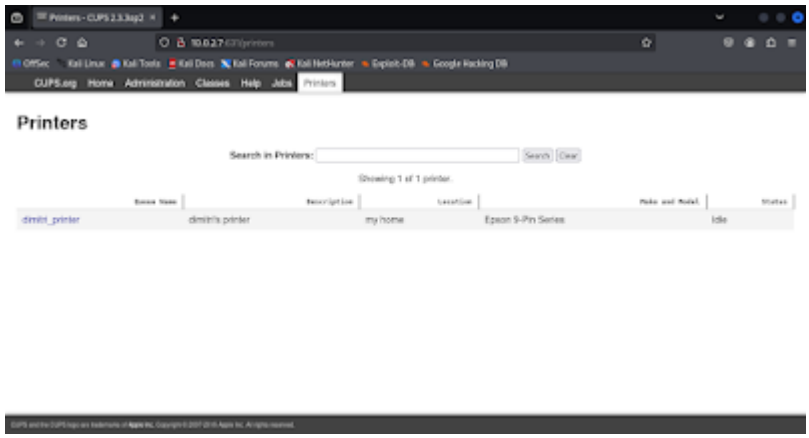
A continuación, realizamos con la herramienta **FFUF** un fuzzing web, para ello ejecutamos el siguiente comando:

$ 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**.

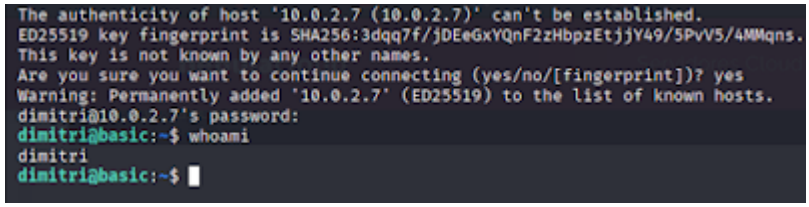


Con la herramienta **hydra** realizamos un ataque a ssh para intentar crackear la contraseña del usuario dimitri, para ello ejecutamos el siguiente comando:

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

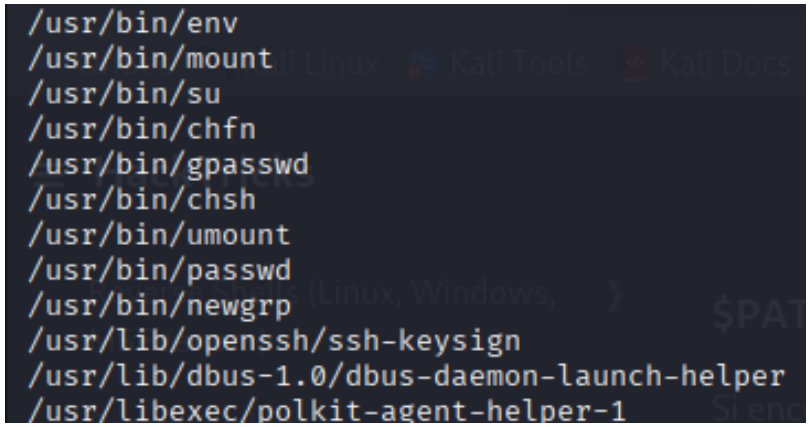
A continuación, nos conectamos por ssh, para ello ejecutamos el siguiente comando:

$ ssh dimitri@10.0.2.7

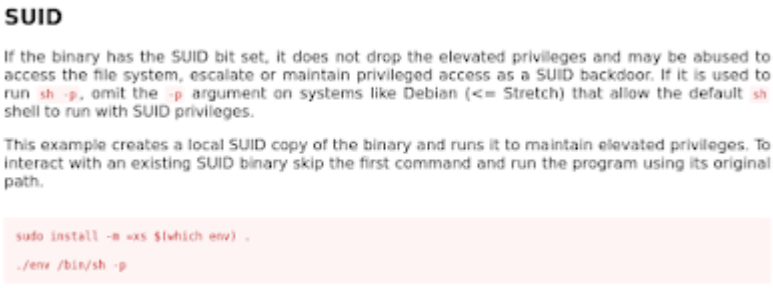


Buscamos todos los binarios **SUID**, para ello ejecutamos el siguiente comando:

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

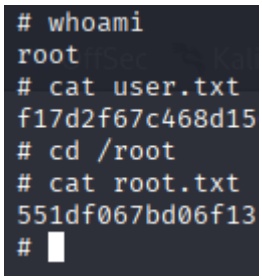


Como podemos comprobar el binario **env** tiene el bit **SUID** activado, no eliminando los privilegios elevados pudiendo utilizarse de forma abusiva para escalar privilegios como una puerta trasera **SUID**, por lo tanto nos vamos a la página gtfobins a mirar el payload.



Lo ejecutamos:

$ env /bin/sh -p



¡¡¡ Ya somos **root**!!!

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