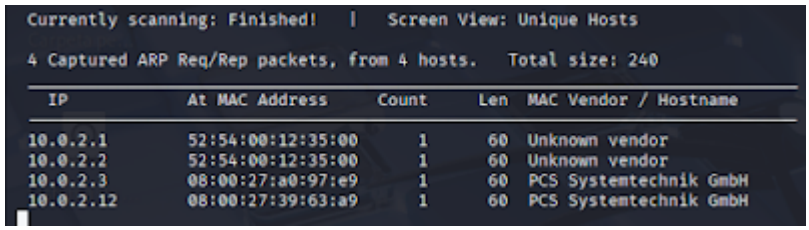
Máquina Wicca (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 29 agosto

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

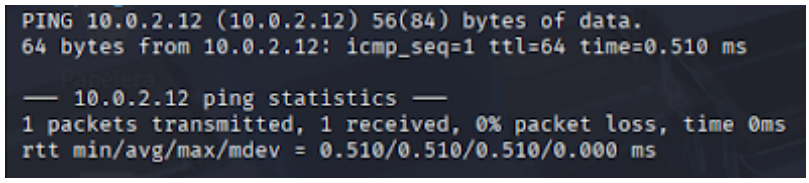
$ netdiscover -i eth1 -r 10.0.2.0/24



- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Victima:** 10.0.2.12

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

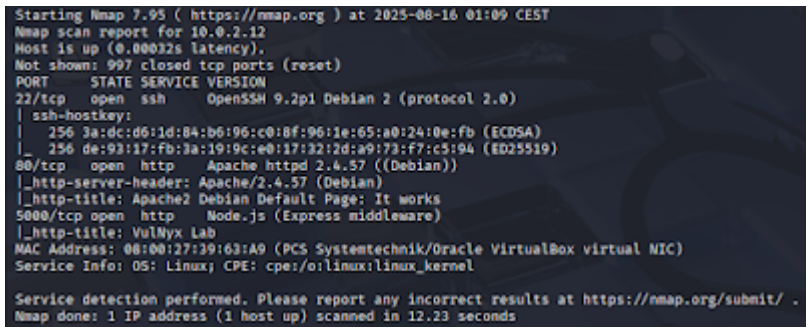
$ ping -c 1 10.0.2.12



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

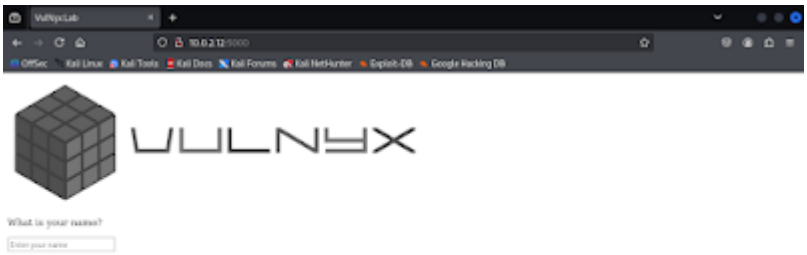
A continuación, realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

$ nmap -PN 10.0.2.12 -sVC

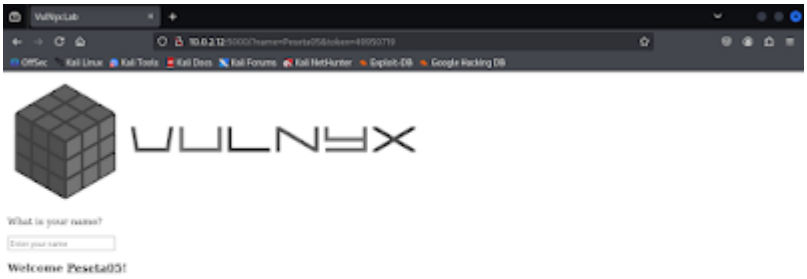


Como podemos comprobar la Máquina Victima tiene abiertos los puertos **22**, **80** y **5000**.

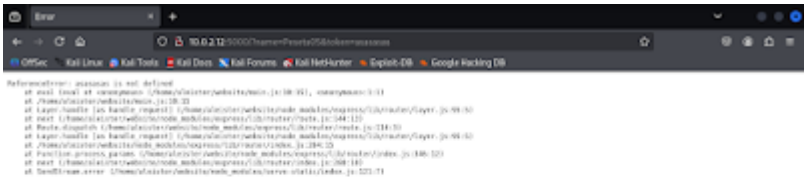
Comprobamos que es lo que corre en el puerto 5000.



Nos pide un texto, por lo tanto lo escribimos y pulsamos enter.

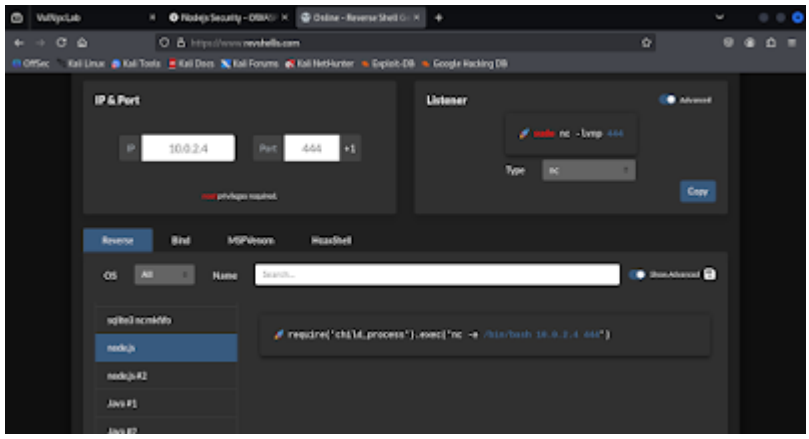


Nos damos cuenta que cambia la url añadiendo un nuevo parámetro "*token*", probamos cambiando esté parámetro por otro **numero** y no pasa nada, pero si lo cambiamos por **letras**, la web crashea.



Este error lo genera la función "*eval()*", investigando un poco nos damos cuenta de que esta función toma un argumento de cadena y lo ejecuta como cualquier otro código fuente de **Javascript**. Combinándolo con la entrada del usuario, este comportamiento conlleva una vulnerabilidad de **ejecución remota de codigo**.

Por lo tanto, nos generamos una reverse shell en **nodejs**.



En nuestra Máquina Atacante con la ayuda de la herramienta **netcat**(**nc**) nos ponemos a la escucha por el puerto **444** por donde vamos a recibir la conexión, para ello ejecutamos el siguiente comando:

$ nc -lvnp 444

```
listening on [any] 444 ...
```

Pegamos el **one-liner** creado anteriormente en el parámetro "*token*" y le damos enter.

Y obtenemos una shell como **aleister**.

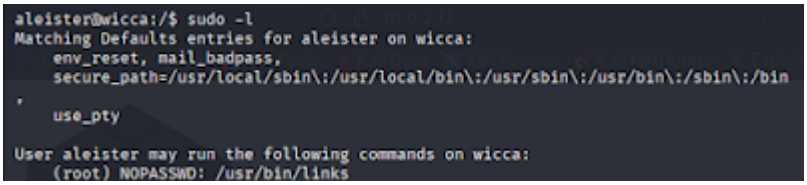
```
listening on [any] 444 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.12] 48406
whoami
aleister
```

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

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

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

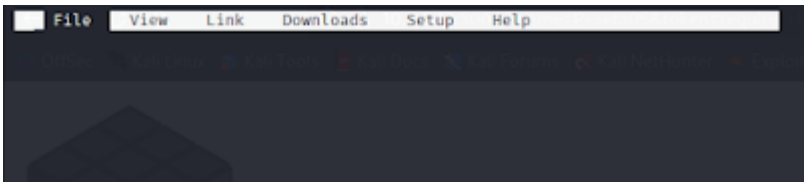
$ sudo -l



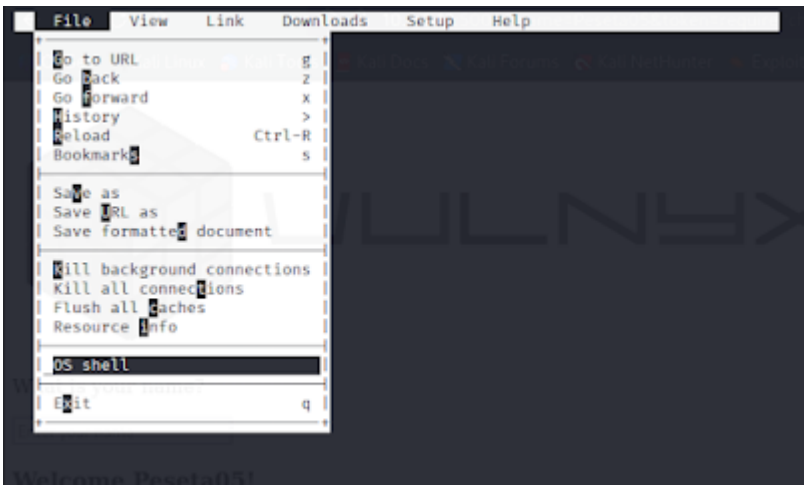
Nos encontramos con el binario **links** que lo podemos ejecutar como el usuario **root**, por lo tanto lo ejecutamos con el siguiente comando:

$ sudo /usr/bin/links

Pulsamos la tecla "*esc*" y nos aparece este menú.



Y con la flechas me desplazo por **File** > **OS shell**.



¡¡¡ Ya somos **root**!!!

```
root@wicca:/# whoami
root
```

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

```
root@wicca:/home/aleister# cat user.txt
VulNyx{d9f213df08ea2b3bf6cc90be28fa827f}
root@wicca:/home/aleister# cd /root/
root@wicca:~# cat root.txt
VulNyx{dab686b0ee76b5edf6fc317c51d6f102}
```