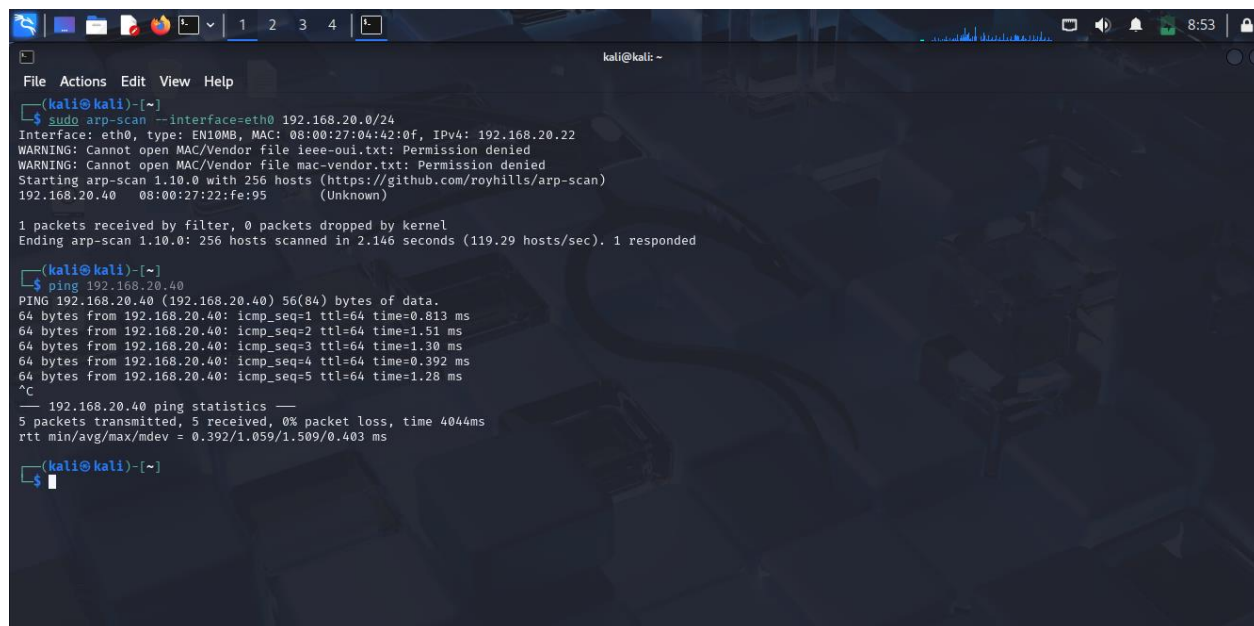


Esercizio Extra: Analisi macchina bsidesvancouver2018

Rete e configurazione iniziale

- IP Kali: 192.168.20.22
- Rete interna: kalinet
- DHCP server configurato su Kali per assegnazione IP alla macchina target



```
(kali@kali)-[~]
$ sudo arp-scan --interface=eth0 192.168.20.0/24
Interface: eth0, type: EN10MB, MAC: 08:00:27:04:42:0f, IPv4: 192.168.20.22
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.20.40 08:00:27:22:fe:95 (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.146 seconds (119.29 hosts/sec). 1 responded

(kali@kali)-[~]
$ ping 192.168.20.40
PING 192.168.20.40 (192.168.20.40) 56(84) bytes of data:
64 bytes from 192.168.20.40: icmp_seq=1 ttl=64 time=0.813 ms
64 bytes from 192.168.20.40: icmp_seq=2 ttl=64 time=1.51 ms
64 bytes from 192.168.20.40: icmp_seq=3 ttl=64 time=1.30 ms
64 bytes from 192.168.20.40: icmp_seq=4 ttl=64 time=0.392 ms
64 bytes from 192.168.20.40: icmp_seq=5 ttl=64 time=1.28 ms
^C
--- 192.168.20.40 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4044ms
rtt min/avg/max/mdev = 0.392/1.059/1.509/0.403 ms

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

Scansione di rete

- Scoperta IP target: 192.168.20.40
- nmap ha rivelato porte aperte: 21 (FTP), 22 (SSH), 80 (HTTP)

```
kali@kali: ~  
File Actions Edit View Help  
- (kali@kali) - [~]  
$ sudo nmap -sS -Pn -T4 192.168.20.40  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 08:56 CEST  
Nmap scan report for 192.168.20.40  
Host is up (0.00030s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 08:00:27:22:FE:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds  
  
- (kali@kali) - [~]  
$ sudo nmap -sV -O 192.168.20.40  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 08:57 CEST  
Nmap scan report for 192.168.20.40  
Host is up (0.00089s 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 Subuntu1.10 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))  
MAC Address: 08:00:27:22:FE:95 (PCS Systemtechnik/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 - 4.14, Linux 3.8 - 3.16  
Network Distance: 1 hop  
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 22.47 seconds
```

Prova con FTP

- Accesso anonimo disponibile
- Scaricato file users.txt.bk contenente 5 utenti:
 - abatchy, john, mai, anne, doomguy

```
kali@kali: ~  
File Actions Edit View Help  
- (kali@kali) - [~]  
$ GET / HTTP/1.1  
Host: 192.168.20.40  
<HTML>  
<HEAD>  
<TITLE>Directory /</TITLE>  
<BASE HREF="file:/">  
</HEAD>  
<BODY>  
<H1>Directory listing of /</H1>  
<UL>  
<LI><A HREF=".">.</A>  
<LI><A HREF="..">..</A>  
<LI><A HREF=".autorelabel">.autorelabel</A>  
<LI><A HREF="bin/">bin/</A>  
<LI><A HREF="boot/">boot/</A>  
<LI><A HREF="dev/">dev/</A>  
<LI><A HREF="etc/">etc/</A>  
<LI><A HREF="home/">home/</A>  
<LI><A HREF="initrd.img">initrd.img</A>  
<LI><A HREF="initrd.img.old">initrd.img.old</A>  
<LI><A HREF="lib/">lib/</A>  
<LI><A HREF="lib32/">lib32/</A>  
<LI><A HREF="lib64/">lib64/</A>  
<LI><A HREF="lost%2Bfound/">lost+found/</A>  
<LI><A HREF="media/">media/</A>  
<LI><A HREF="mnt/">mnt/</A>  
<LI><A HREF="opt/">opt/</A>  
<LI><A HREF="proc/">proc/</A>  
<LI><A HREF="root/">root/</A>  
<LI><A HREF="run/">run/</A>  
<LI><A HREF="sbin/">sbin/</A>  
<LI><A HREF="srv/">srv/</A>
```

```
kali@kali: ~  
File Actions Edit View Help  
<LI><A HREF="/opt/">opt/</A>  
<LI><A HREF="/proc/">proc/</A>  
<LI><A HREF="/root/">root/</A>  
<LI><A HREF="/run/">run/</A>  
<LI><A HREF="/sbin/">sbin/</A>  
<LI><A HREF="/srv/">srv/</A>  
<LI><A HREF="/swapfile">swapfile</A>  
<LI><A HREF="/sys/">sys/</A>  
<LI><A HREF="/tmp/">tmp/</A>  
<LI><A HREF="/usr/">usr/</A>  
<LI><A HREF="/var/">var/</A>  
<LI><A HREF="/vmlinuz">vmlinuz</A>  
<LI><A HREF="/vmlinuz.old">vmlinuz.old</A>  
</UL>  
</BODY>  
</HTML>  
  
Can't connect to HTTP:80 (Temporary failure in name resolution)  
  
Temporary failure in name resolution at /usr/share/perl5/LWP/Protocol/http.pm line 49.  
Host:: command not found  
  
(kali@kali)-[~]  
$  
  
(kali@kali)-[~]  
$ ftp 192.168.20.40  
Connected to 192.168.20.40.  
220 (vsFTPD 2.3.5)  
Name (192.168.20.40:kali): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

Prova con SSH

- Servizio attivo, ma non accetta login via password
- Tentato bruteforce con hydra: fallito → solo chiavi SSH accettate

```
kali@kali: ~  
File Actions Edit View Help  
$ cat users.txt  
abatchy  
john  
mai  
anne  
doomguy  
  
(kali@kali)-[~]  
$ ls /usr/share/wordlists/rockyou.txt  
ls: cannot access '/usr/share/wordlists/rockyou.txt': No such file or directory  
  
(kali@kali)-[~]  
$ gunzip /usr/share/wordlists/rockyou.txt.gz  
gzip: /usr/share/wordlists/rockyou.txt: Permission denied  
  
(kali@kali)-[~]  
$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz  
[sudo] password for kali:  
  
(kali@kali)-[~]  
$ hydra -L users.txt -P /usr/share/wordlists/rockyou.txt ssh://192.168.20.40  
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 2025-05-12 09:25:43  
[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, 86066394 login tries (l:/p:14344399), ~5379150 tries per task  
[DATA] attacking ssh://192.168.20.40:22/  
[ERROR] target ssh://192.168.20.40:22/ does not support password authentication (method reply 4).  
  
(kali@kali)-[~]  
$ ftp 192.168.20.40
```

Ho cercato di trovare la soluzione in solitaria anche non completando l'esercizio. Recupererò la lezione il prima possibile per scoprire la soluzione. grazie!