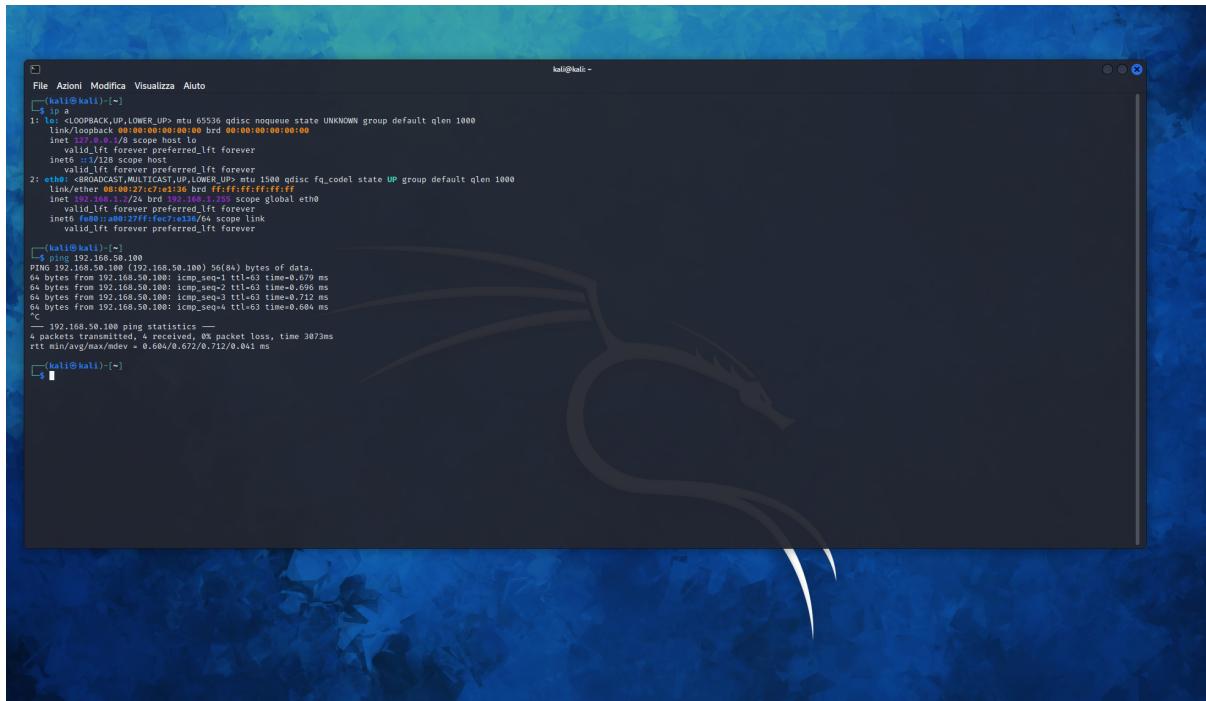


# Day 5:

## Esercizio 1

### Scansioni con Nmap

Oggi andremo ad analizzare due scansioni eseguite con il tool **Nmap** :  
Prima di tutto diamo un'occhiata alla configurazione.



```
kali㉿kali:~
```

```
File Azioni Modifica Visualizza Aiuto
[ kali㉿kali:~ ]$ 
[ kali㉿kali:~ ]$ ls
[ kali㉿kali:~ ]$ 
[ kali㉿kali:~ ]$ ifconfig
lo      Link encap:Local Loopback brd 0:0:0:0:0:0
        inet 127.0.0.1/8 brd 0:0:0:0:0:0
          brd 0:0:0:0:0:0
        inet6 ::1/128 scope host
          brd 0:0:0:0:0:0
[ kali㉿kali:~ ]$ 
[ kali㉿kali:~ ]$ cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
# Please consult /usr/share/doc/ifupdown/README.gz for usage details
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
    address 192.168.50.100
    netmask 255.255.255.0
    broadcast 192.168.50.255
    gateway 192.168.50.1
    dns-nameservers 8.8.8.8 8.8.4.4
    dns-search example.com
    up dhclient
[ kali㉿kali:~ ]$ 
[ kali㉿kali:~ ]$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=0.679 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=0.696 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=0.712 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=0.698 ms
[ kali㉿kali:~ ]$ 
[ kali㉿kali:~ ]$ ping -c 1 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=0.673 ms
[ kali㉿kali:~ ]$ 
```

La nostra macchina kali Linux ha un indirizzo IP **192.168.1.2** mentre la macchina metasploitable ha un ip **192.168.50.100**.

I due host si trovano quindi su due subnet differenti.

Dopo aver testato la raggiungibilità passiamo a fare le nostre analisi con Nmap.

Iniziamo con l'OS fingerprint, come possiamo leggere sul sito ufficiale di Nmap :

**Una delle più famose caratteristiche di Nmap è la possibilità di identificare da remoto il sistema operativo di un host attraverso il fingerprint dello stack TCP/IP. Nmap invia una serie di pacchetti TCP ed UDP all'host remoto ed esamina ogni bit ricevuto in risposta.**

```
[kali㉿kali:~]# nmap -sS 192.168.58.100 -r 1000
[sudo] password di kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2023-08-03 08:02 EDT
Nmap scan report for 192.168.58.100
Host is up, received arp-response (0.00026s latency).
The ports below were closed or filtered:
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 64
22/tcp    open  telnet       syn-ack ttl 64
23/tcp    open  telnet       syn-ack ttl 64
25/tcp    open  smtp         syn-ack ttl 64
53/tcp    open  domain      syn-ack ttl 64
80/tcp    open  http         syn-ack ttl 64
113/tcp   open  rpcbind     syn-ack ttl 64
139/tcp   open  netbios-ssn  syn-ack ttl 64
445/tcp   open  microsoft-ds syn-ack ttl 64
543/tcp   open  netbios-dgm  syn-ack ttl 64
513/tcp   open  login        syn-ack ttl 64
3128/tcp  open  http-proxy  syn-ack ttl 64
1900/tcp  open  rmiregistry  syn-ack ttl 64
32461/tcp open  unknown     syn-ack ttl 64
2327/tcp  open  cisco-ftp   syn-ack ttl 64
3128/tcp  open  http         syn-ack ttl 64
5423/tcp  open  postgresql  syn-ack ttl 64
5900/tcp  open  vnc          syn-ack ttl 64
6000/tcp  open  x11         syn-ack ttl 64
6001/tcp  open  x11          syn-ack ttl 64
6000/tcp  open  unknown     syn-ack ttl 64
8080/tcp  open  aJP13       syn-ack ttl 64
8111/tcp  open  http        syn-ack ttl 64
8888/tcp  open  http        syn-ack ttl 64
MAC Address: 00:0C:27:0E:C4:C2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
```

Come possiamo notare dopo aver scansionato le diverse porte, nmap ci indica il sistema operativo che ha rilevato : In questo caso un linux dal kernel 2.6

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
```

Una volta determinato il sistema operativo, passiamo a effettuare le altre scansioni. Partiamo con la SYN scan che consiste nell'andare a testare le porte mandando dei pacchetti SYN :

```
[kali㉿kali:~]# nmap -sS 192.168.58.100 -r 1000
[sudo] password di kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2023-08-03 07:58 EDT
Nmap scan report for 192.168.58.100
Host is up, received arp-response (0.0004us latency).
Not shown: 978 closed tcp ports (reset)
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

La SYN scan non completa il three way handshake, mentre la TCP scan lo fa.

Per questo motivo la SYN scan viene chiamata anche Stealth Scan.

Stealth infatti significa invisibile in inglese...

In poche parole la TCP scan completando il three way handshake genera molta più entropia nella rete del target e viene rilevata molto più facilmente rispetto alla SYN scan.

Notiamo però che a parte l'entropia generata le due scansioni riportano gli stessi risultati.

```
(kali㉿kali)-[~] nmap -sS -T4 -O 192.168.0.100 --reason
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-03 07:50 EDT
Nmap scan report for 192.168.0.100
Host is up, received echo-reply ttl 63 (0.00045s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack
22/tcp    open  ssh          syn-ack
23/tcp    open  telnet       syn-ack
25/tcp    open  smtp         syn-ack
3306/tcp  open  mysql        syn-ack
5432/tcp  open  postgresql   syn-ack
80/tcp    open  http         syn-ack
443/tcp   open  https        syn-ack
513/tcp   open  login        syn-ack
514/tcp   open  tftp         syn-ack
1090/tcp  open  rmiregistry  syn-ack
2049/tcp  open  nfs          syn-ack
2131/tcp  open  cvsserv-ftp  syn-ack
3389/tcp  open  mstsc        syn-ack
5632/tcp  open  postgresql   syn-ack
6000/tcp  open  x11          syn-ack
6008/tcp  open  irc          syn-ack
8009/tcp  open  ajp13        syn-ack
8180/tcp  open  unknown      syn-ack

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
(kali㉿kali)-[~]
```

Un'altra scansione molto utile che possiamo effettuare con Nmap è quella che ci permette di verificare la versione del servizio in uso sulla porta testata.

```
(kali㉿kali)-[~] nmap -sV -O 192.168.0.100 --reason
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-03 07:51 EDT
Nmap scan report for 192.168.0.100
Host is up, received echo-reply ttl 63 (0.00045s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 63 vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 63 OpenSSH 8.0p1 Debian Subuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 63 Linux telnetd
25/tcp    open  smtp         syn-ack ttl 63 Postfix smtpd
3306/tcp  open  mysql        syn-ack ttl 63 MySQL 5.7.33-0ubuntu0.20.04.1
513/tcp   open  login        syn-ack ttl 63 OpenBSD or Solaris rlogin
514/tcp   open  tftp         syn-ack ttl 63 GNU Classpath glibcrypt
139/tcp   open  netbios-ssn  syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp   open  netbios-ssn  syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5432/tcp  open  postgresql   syn-ack ttl 63 PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13        syn-ack ttl 63 Apache Jserv Protocol V.3
8080/tcp  open  http         syn-ack ttl 63 Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 32.19 seconds
(kali㉿kali)-[~]
```

### **Conclusioni :**

Abbiamo visto solo alcune delle possibili scansioni di Nmap, i risultati analizzati ci danno un'idea precisa sulle porte aperte rilevate, la versione dei demoni che le porte stanno utilizzando, il sistema operativo e a seconda della scansione scelta impostando un tempo per la scansione molto basso potremmo essere quasi invisibile agli occhi degli strumenti di difesa del nostro bersaglio.