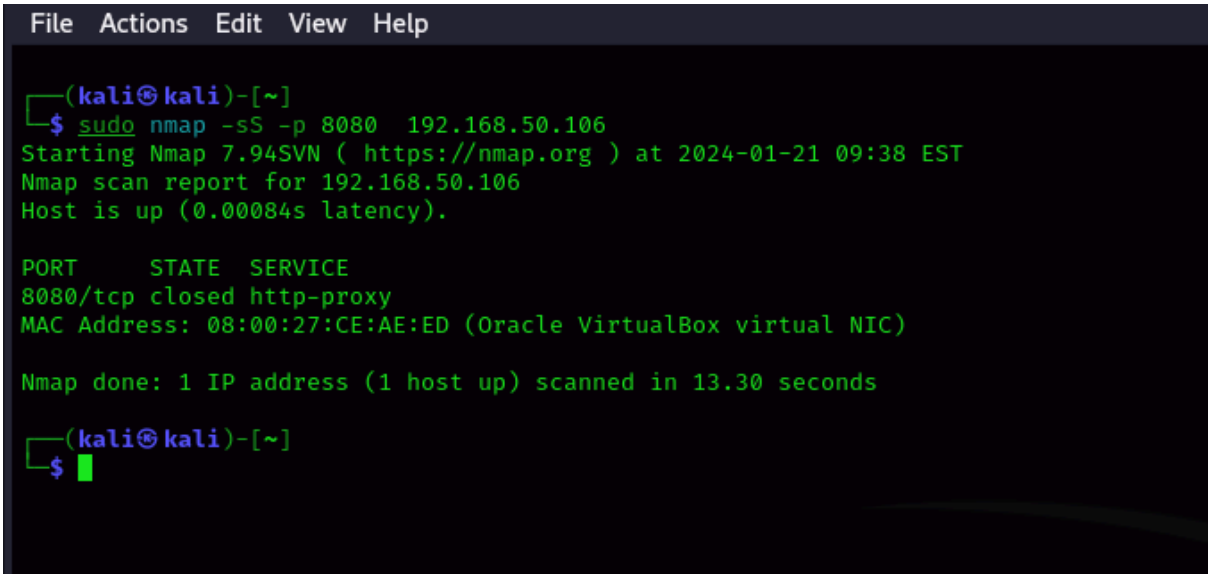
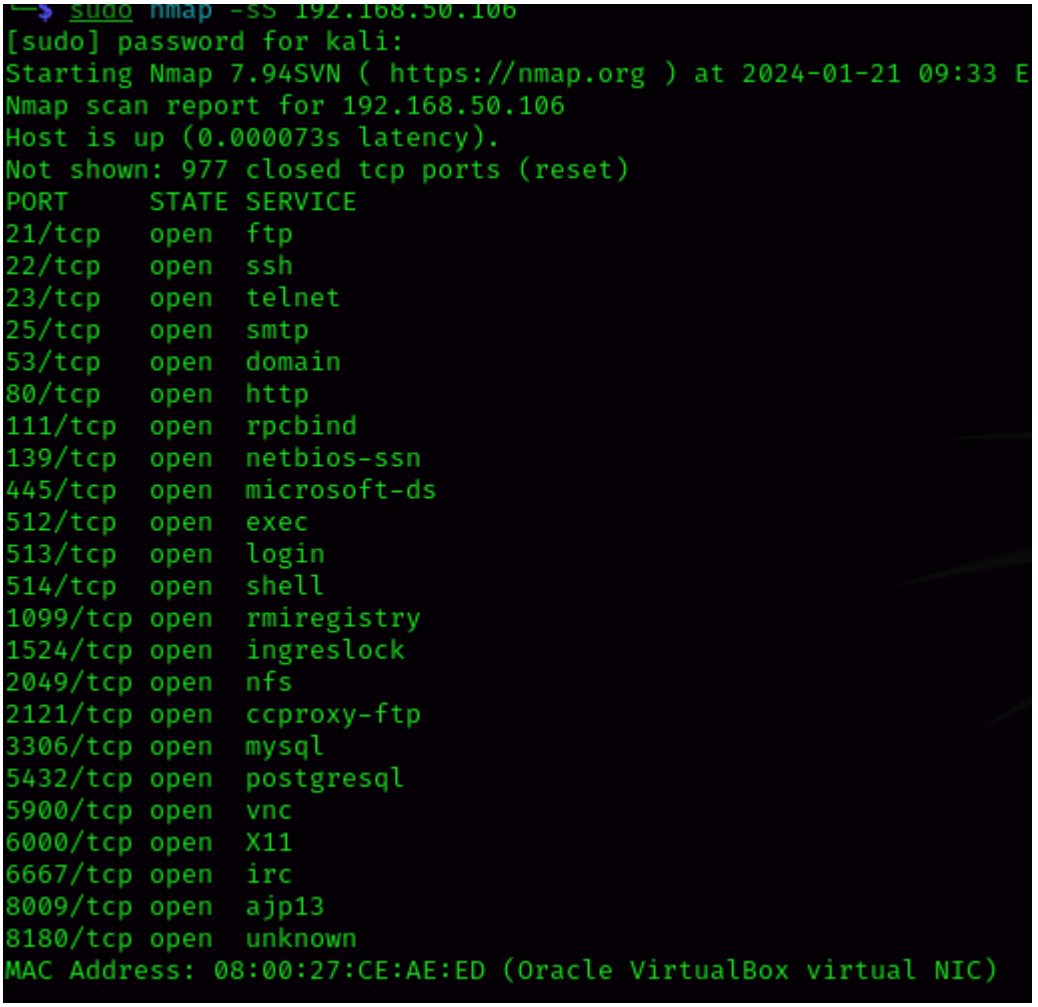
Gelosa Matteo Esercizio D11W4

In questo esercizio vengono mostrate alcune scansioni del tool nmap.
I test sono stati eseguiti da una macchina Kali Linux ad una macchina metasploitable.





```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.50.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 11:17 EST
Nmap scan report for 192.168.50.106
Host is up (0.00014s latency).
MAC Address: 08:00:27:CE:AE:ED (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 09:34 EST
Nmap scan report for 192.168.50.106
Host is up (0.000067s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CE:AE:ED (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;
```

```
└─$ sudo nmap -sV 192.168.50.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 09:34 EST
Nmap scan report for 192.168.50.106
Host is up (0.000067s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CE:AE:ED (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -oN scan.txt  192.168.50.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 09:36 EST
Nmap scan report for 192.168.50.106
Host is up (0.00012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CE:AE:ED (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS

Service detection performed. Please report any incorrect results at https://
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p-    192.168.50.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 09:39 EST
Nmap scan report for 192.168.50.106
Host is up (0.00011s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35267/tcp open  unknown
39983/tcp open  unknown
41384/tcp open  unknown
46424/tcp open  unknown
MAC Address: 08:00:27:CE:AE:ED (Oracle VirtualBox virtual NIC)
```

```
File  Actions  Edit  View  Help
Discovered open port 53/udp on 192.168.50.106
Increasing send delay for 192.168.50.106 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.50.106 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.50.106 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.50.106 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.50.106 from 400 to 800 due to 11 out of 12 dropped probes since last increase.
Discovered open port 137/udp on 192.168.50.106
UDP Scan Timing: About 3.66% done; ETC: 09:54 (0:13:37 remaining)
UDP Scan Timing: About 20.98% done; ETC: 09:56 (0:12:52 remaining)
Discovered open port 2049/udp on 192.168.50.106
UDP Scan Timing: About 27.80% done; ETC: 09:56 (0:12:02 remaining)
UDP Scan Timing: About 33.96% done; ETC: 09:57 (0:11:09 remaining)
UDP Scan Timing: About 39.71% done; ETC: 09:57 (0:10:18 remaining)
UDP Scan Timing: About 45.06% done; ETC: 09:57 (0:09:26 remaining)
UDP Scan Timing: About 50.19% done; ETC: 09:57 (0:08:34 remaining)
UDP Scan Timing: About 55.52% done; ETC: 09:57 (0:07:41 remaining)
UDP Scan Timing: About 60.66% done; ETC: 09:57 (0:06:48 remaining)
UDP Scan Timing: About 66.01% done; ETC: 09:57 (0:05:53 remaining)
UDP Scan Timing: About 71.17% done; ETC: 09:57 (0:05:01 remaining)
UDP Scan Timing: About 76.14% done; ETC: 09:57 (0:04:08 remaining)
UDP Scan Timing: About 81.18% done; ETC: 09:57 (0:03:16 remaining)
UDP Scan Timing: About 86.50% done; ETC: 09:57 (0:02:21 remaining)
UDP Scan Timing: About 91.50% done; ETC: 09:57 (0:01:29 remaining)
UDP Scan Timing: About 96.63% done; ETC: 09:57 (0:00:35 remaining)
Completed UDP Scan at 09:58, 1076.97s elapsed (1000 total ports)
Nmap scan report for 192.168.50.106
Host is up (0.00016s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 08:00:27:CE:AE:ED (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1090.12 seconds
           Raw packets sent: 1437 (65.419KB) | Rcvd: 1100 (80.093KB)
```

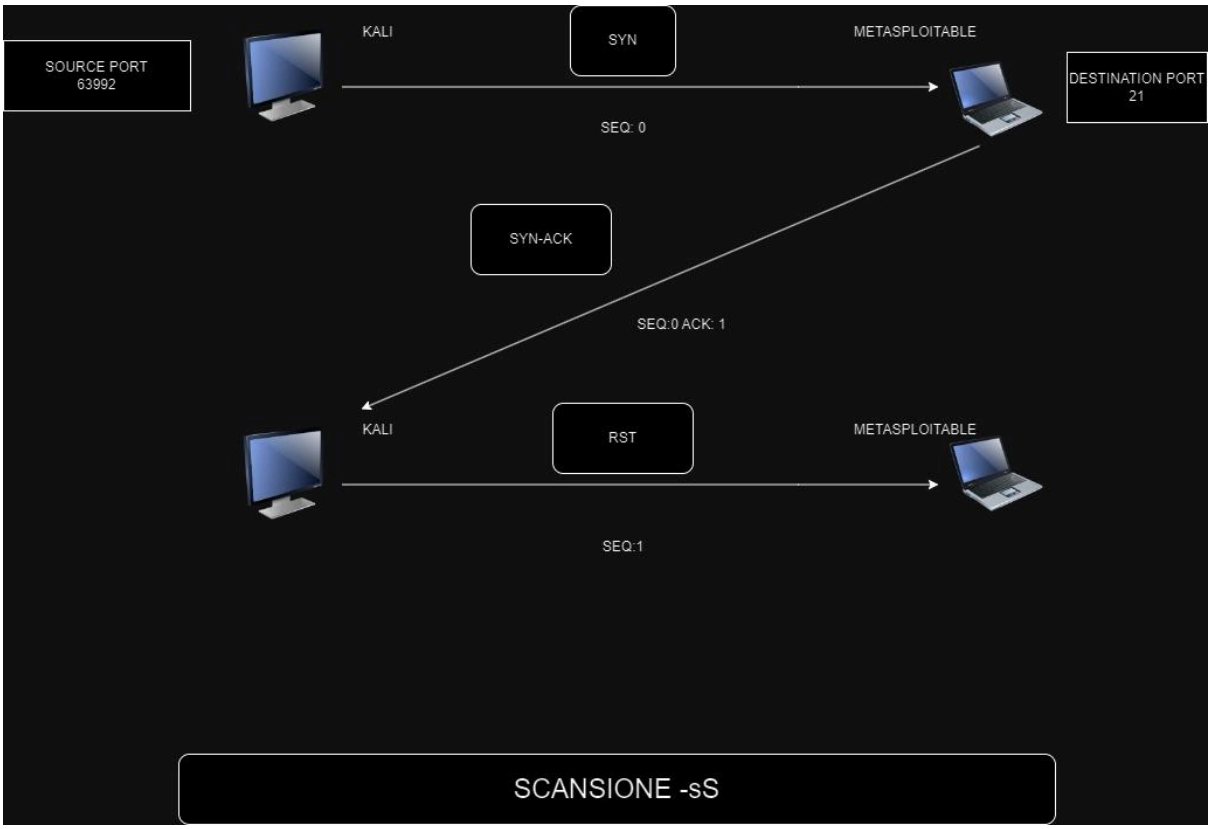
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.106
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 11:10 EST
Nmap scan report for 192.168.50.106
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:CE:AE:ED (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 14.51 seconds

┌──(kali㉿kali)-[~]
└─$
```

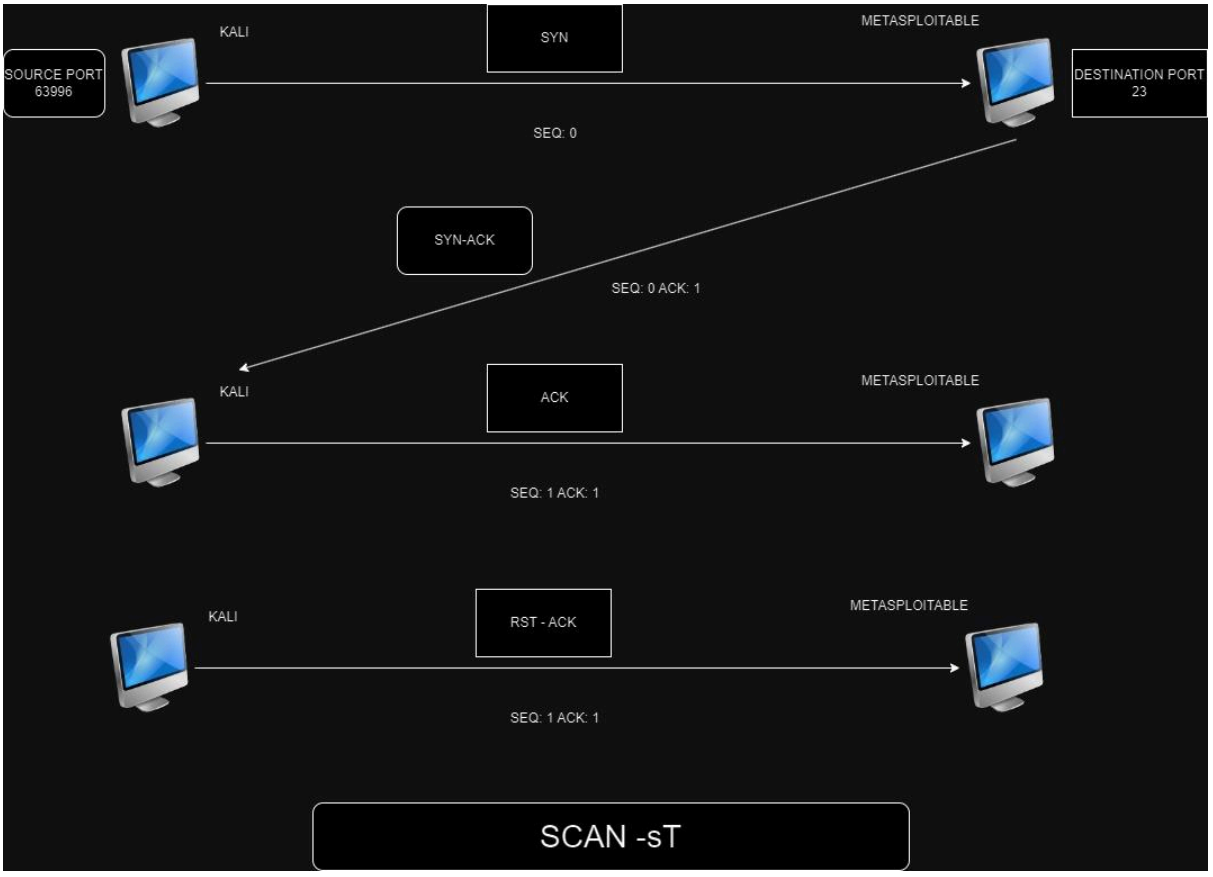
```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo nmap -F 192.168.50.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 11:16 EST
Nmap scan report for 192.168.50.106
Host is up (0.00011s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 08:00:27:CE:AE:ED (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds

┌──(kali㉿kali)-[~]
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PR 192.168.50.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 11:17 EST
Nmap scan report for 192.168.50.106
Host is up (0.000048s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:CE:AE:ED (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

┌──(kali㉿kali)-[~]
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PN 192.168.50.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 11:18 EST
Nmap scan report for 192.168.50.106
Host is up (0.000051s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:CE:AE:ED (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
```

Infine per la scansione sS e sT ho creato un grafico in cui spiego come avviene lo scambio di pacchetti per ver verificare se una porta è aperta.


SOURCE PORT
63992
KALI
SYN
METASPLOITABLE
DESTINATION PORT
21
SEQ: 0
SYN-ACK
SEQ:0 ACK: 1
KALI
RST
METASPLOITABLE
SEQ:1
SCANSIONE -sS


SOURCE PORT
63996
KALI
SYN
METASPLOITABLE
DESTINATION PORT
23
SEQ: 0
SYN-ACK
SEQ: 0 ACK: 1
KALI
ACK
METASPLOITABLE
SEQ: 1 ACK: 1
KALI
RST - ACK
METASPLOITABLE
SEQ: 1 ACK: 1
SCAN -sT