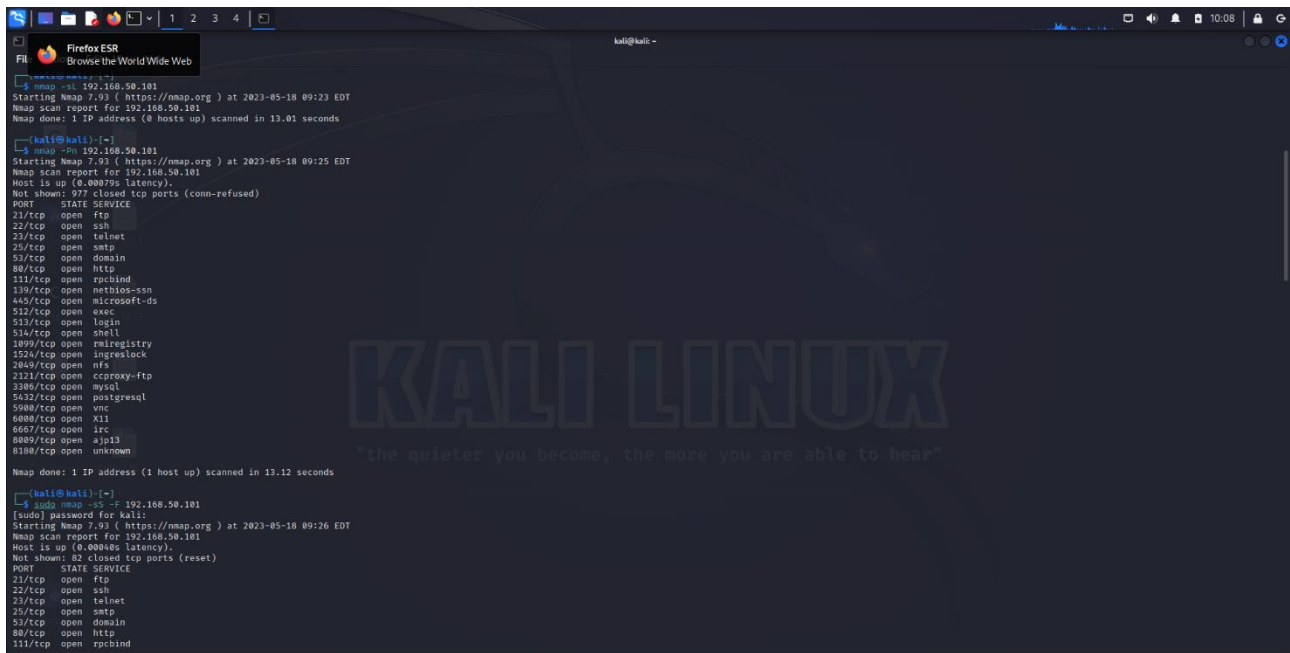


1. Host discovery con comandi -sL e -Pn



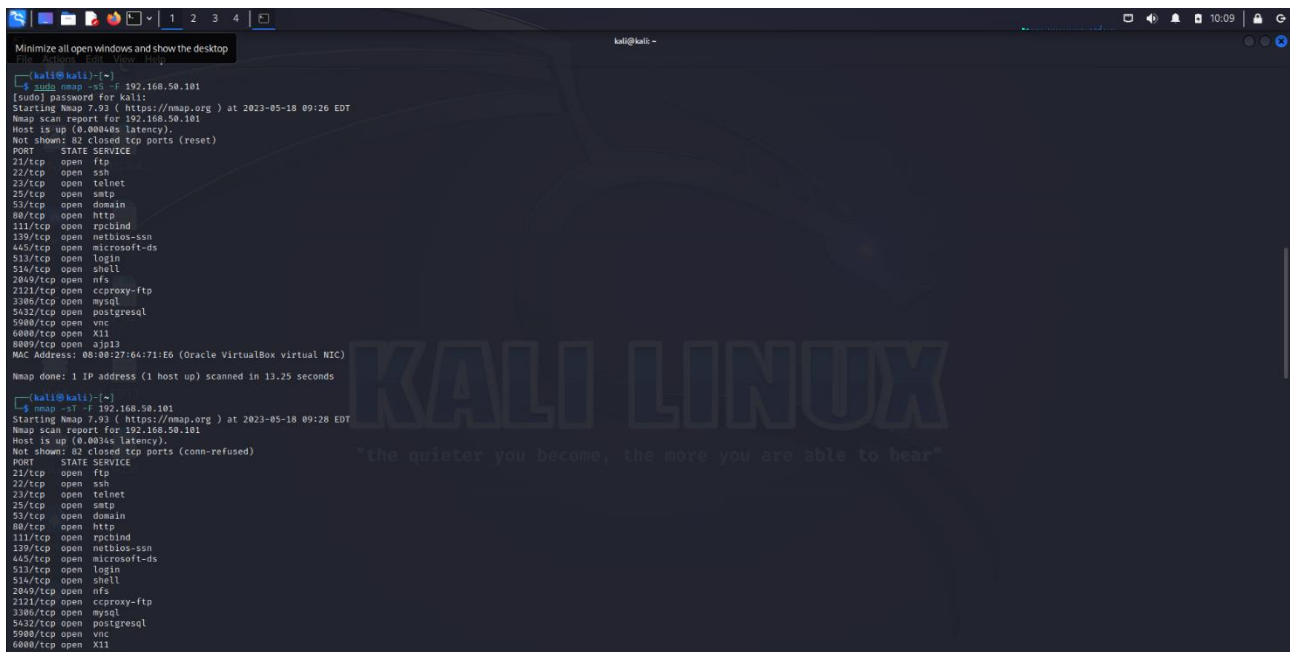
```
kali@kali:~$ nmap -sL 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:23 EDT
Nmap scan report for 192.168.50.101
Nmap done: 1 IP address (0 hosts up) scanned in 13.01 seconds

kali@kali:~$ nmap -Pn 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:25 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00079s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
2380/tcp  open  mysql
2432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6080/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds

kali@kali:~$ sudo nmap -sS -F 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:26 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00048s 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
2380/tcp  open  mysql
2432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6080/tcp  open  ajp13
MAC Address: 08:00:27:64:71:E6 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds

kali@kali:~$ nmap -sT -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:28 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0003s latency).
Not shown: 82 closed tcp ports (conn-refused)
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
2380/tcp  open  mysql
2432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
```

2. Scansione SYN su porte well-known



```
kali@kali:~$ sudo nmap -sS -F 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:26 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00048s 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
2380/tcp  open  mysql
2432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
MAC Address: 08:00:27:64:71:E6 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds

kali@kali:~$ nmap -sT -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:28 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0003s latency).
Not shown: 82 closed tcp ports (conn-refused)
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
2380/tcp  open  mysql
2432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
```

3. Scansione TCP su porte well-known

```
kali@kali:~$ nmap -sT -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:28 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0031s latency).
Not shown: 82 closed tcp ports (conn-refused)
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  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
8000/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds

kali@kali:~$ nmap -sA -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:29 EDT

kali@kali:~$ nmap -sA -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:33 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0026s latency).
Not shown: 82 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.50.100
|_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
vsftpd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_1024 6081fc1e1856a74d69024fec4d56cccd (DSA)
|_2048 5656240f21ddea72bae61b1243debf3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-command: VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sasl2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_DES_192_CBC1_CBC_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #1000000)
|_rpcinfo:
|_program version port/proto service
|_100000 2 111/tcp rpcbind
|_100000 2 111/udp rpcbind
|_100003 2,3,4 2049/tcp nfs
|_100003 2,3,4 2049/udp nfs
|_100005 1,2,3 39256/udp mountd
|_100005 1,2,3 5617/tcp mountd
|_100021 1,3,4 38796/udp nlockmgr
|_100021 1,3,4 56557/tcp nlockmgr
```

4. Scansione con switch -A sulle porte well-known

```
kali@kali:~$ nmap -sA -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:33 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0026s latency).
Not shown: 82 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.50.100
|_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
vsftpd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_1024 6081fc1e1856a74d69024fec4d56cccd (DSA)
|_2048 5656240f21ddea72bae61b1243debf3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-command: VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sasl2:
|_SSLv2 supported
|_ciphers:
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_SSL2_DES_192_CBC1_CBC_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #1000000)
|_rpcinfo:
|_program version port/proto service
|_100000 2 111/tcp rpcbind
|_100000 2 111/udp rpcbind
|_100003 2,3,4 2049/tcp nfs
|_100003 2,3,4 2049/udp nfs
|_100005 1,2,3 39256/udp mountd
|_100005 1,2,3 5617/tcp mountd
|_100021 1,3,4 38796/udp nlockmgr
|_100021 1,3,4 56557/tcp nlockmgr
```

```
kali@kali: ~  
111/tcp open  rpcbind 2 (RPC #100000)  
|  
|_ rpcinfo:  
|_ program version port/proto service  
|_ 100000 2 111/tcp rpcbind  
|_ 100000 2 111/udp rpcbind  
|_ 100003 2,3,4 2049/tcp nfs  
|_ 100003 2,3,4 2049/udp nfs  
|_ 100005 1,2,3 39258/udp mountd  
|_ 100005 1,2,3 56417/tcp mountd  
|_ 100021 1,3,4 38796/udp nlockmgr  
|_ 100021 1,3,4 50557/tcp nlockmgr  
|_ 100024 1 34366/udp status  
|_ 100024 1 45913/tcp status  
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)  
513/tcp open  login?  
514/tcp open  shell Netkit rshd  
2049/tcp open nfs 2+ (RPC #100003)  
2121/tcp open ftp ProFTPD 1.3.1  
3306/tcp open mysql?  
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7  
|_ ssl-date: 2023-05-18T13:55:05+00:00; +17m54s from scanner time.  
|_ ssl-cert: Subject: commonName=ubuntu004-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX  
|_ Not valid before: 2018-04-16T14:07:45  
|_ Not valid after: 2018-04-16T14:07:45  
5980/tcp open vnc VNC (protocol 3.3)  
|_ vnc-info:  
|_ Protocol version: 3.3  
|_ Security types:  
|_ VNC Authentication (2)  
6000/tcp open x11 (access denied)  
8080/tcp open ajp13 Apache Jserv (Protocol v1.3)  
|_ _ajp-methods: failed to get a valid response for the OPTIONS request  
Service Info: Host: metasploitable.localdomain; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Host script results:  
|_ clock-skew: mean: 1h37m58s, deviation: 2h18m41s, median: 17m33s  
|_ smb-security-mode:  
|_ account-used: blank  
|_ authentication_level: user  
|_ challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_ smb-os-discovery:  
|_ OS: Unix (Samba 3.0.20-Debian)  
|_ Computer name: metasploitable  
|_ NetBIOS computer name:  
|_ Domain name: localdomain  
|_ FQDN: metasploitable.localdomain  
|_ System time: 2023-05-18T09:54:11-04:00  
|_ smb2-time: Protocol negotiation failed (SMB2)  
|_ _nbtstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 275.04 seconds
```

5. Scansione SYN su Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
49	13.088131582	192.168.50.101	192.168.50.100	TCP	60	111 → 62723 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
50	13.088138450	192.168.50.100	192.168.50.101	TCP	54	62723 → 111 [RST] Seq=1 Win=0 Len=0
51	13.088527013	192.168.50.101	192.168.50.100	TCP	60	23 → 62723 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
52	13.088534810	192.168.50.100	192.168.50.101	TCP	54	62723 → 23 [RST] Seq=1 Win=0 Len=0
53	13.088831773	192.168.50.100	192.168.50.101	TCP	58	62723 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
54	13.089645168	192.168.50.100	192.168.50.101	TCP	58	62723 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55	13.089215294	192.168.50.101	192.168.50.100	TCP	60	1723 → 62723 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	13.089448493	192.168.50.101	192.168.50.100	TCP	60	5900 → 62723 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
57	13.089448643	192.168.50.100	192.168.50.101	TCP	54	62723 → 5900 [RST] Seq=1 Win=0 Len=0
58	13.089737570	192.168.50.100	192.168.50.101	TCP	58	62723 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
59	13.089860671	192.168.50.100	192.168.50.101	TCP	58	62723 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
60	13.090182807	192.168.50.101	192.168.50.100	TCP	60	8888 → 62723 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	13.090247681	192.168.50.100	192.168.50.101	TCP	58	62723 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
62	13.090416343	192.168.50.101	192.168.50.100	TCP	60	1720 → 62723 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	13.090602029	192.168.50.101	192.168.50.100	TCP	60	139 → 62723 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
64	13.090642892	192.168.50.100	192.168.50.101	TCP	54	62723 → 139 [RST] Seq=1 Win=0 Len=0
65	13.090978184	192.168.50.100	192.168.50.101	TCP	58	62723 → 1825 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
66	13.091172682	192.168.50.100	192.168.50.101	TCP	58	62723 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
67	13.091311434	192.168.50.101	192.168.50.100	TCP	60	1825 → 62723 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
68	13.091341537	192.168.50.101	192.168.50.100	TCP	60	993 → 62723 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
• Ethernet II, Src: PcsCompu, c7:e1:36 (08:00:27:c7:e1:36), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
• Address Resolution Protocol (request)

La differenza tra SYN e TCP è che con SYN vi è la chiusura della comunicazione inviando un pacchetto RST (reset), i firewall non interferiscono ed è quindi più stealth.