

Nella scansione TCP delle porte well-known dalla macchina kali (192.168.1.248) verso la macchina metasploitable (192.168.1.9) notiamo come la maggior parte delle richieste di connessione si interrompono (RST, ACK) perché le porte sono chiuse; mentre le porte aperte rispondono con pacchetto SYN portando a termine la connessione

No.	Time	Source	Destination	Protocol	Length	Info
2067	89.265284169	192.168.1.248	192.168.1.9	TCP	74	57228 → 166 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379372 TSecr=0 WS=128
2068	89.265438445	192.168.1.9	192.168.1.248	TCP	60	680 → 55646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2069	89.265656814	192.168.1.9	192.168.1.248	TCP	60	166 → 57228 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2070	89.265724225	192.168.1.248	192.168.1.9	TCP	74	58118 → 456 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379372 TSecr=0 WS=128
2071	89.265913499	192.168.1.248	192.168.1.9	TCP	74	52594 → 977 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379372 TSecr=0 WS=128
2072	89.266066287	192.168.1.9	192.168.1.248	TCP	60	456 → 58118 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2073	89.266066377	192.168.1.9	192.168.1.248	TCP	60	977 → 52594 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2074	89.266311715	192.168.1.248	192.168.1.9	TCP	74	46328 → 979 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379373 TSecr=0 WS=128
2075	89.266504116	192.168.1.248	192.168.1.9	TCP	74	33594 → 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379373 TSecr=0 WS=128
2076	89.266657747	192.168.1.9	192.168.1.248	TCP	60	879 → 46328 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2077	89.266657813	192.168.1.9	192.168.1.248	TCP	60	884 → 33594 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2078	89.266979451	192.168.1.248	192.168.1.9	TCP	74	33426 → 164 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379373 TSecr=0 WS=128
2079	89.267117751	192.168.1.248	192.168.1.9	TCP	74	49522 → 43 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379374 TSecr=0 WS=128
2080	89.267469718	192.168.1.9	192.168.1.248	TCP	60	164 → 33426 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2081	89.267469833	192.168.1.9	192.168.1.248	TCP	60	43 → 49522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2082	89.267892850	192.168.1.248	192.168.1.9	TCP	74	47938 → 695 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379374 TSecr=0 WS=128
2083	89.268096671	192.168.1.248	192.168.1.9	TCP	74	56898 → 126 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379374 TSecr=0 WS=128
2084	89.268162376	192.168.1.9	192.168.1.248	TCP	60	695 → 47938 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2085	89.268162458	192.168.1.9	192.168.1.248	TCP	60	126 → 56898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2086	89.268559362	192.168.1.248	192.168.1.9	TCP	74	52496 → 197 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379375 TSecr=0 WS=128
2087	89.268748997	192.168.1.248	192.168.1.9	TCP	74	55202 → 426 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379375 TSecr=0 WS=128
2088	89.268906628	192.168.1.9	192.168.1.248	TCP	60	197 → 52496 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2089	89.268906116	192.168.1.9	192.168.1.248	TCP	60	426 → 55202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2090	89.269154287	192.168.1.248	192.168.1.9	TCP	74	56122 → 504 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379376 TSecr=0 WS=128
2091	89.269346272	192.168.1.248	192.168.1.9	TCP	74	57230 → 309 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1342379376 TSecr=0 WS=128
2092	89.269509033	192.168.1.9	192.168.1.248	TCP	60	504 → 56122 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2093	89.269509143	192.168.1.9	192.168.1.248	TCP	60	309 → 57230 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2094	94.063947610	fe80::9de0:e5a2:bfa...	fe80::a16:5ff:fe87:...	ICMPv6	86	Neighbor Solicitation for fe80::a16:5ff:fe87:47f0 from 08:00:27:08:06:a6
2095	94.068359705	fe80::a16:5ff:fe87:...	fe80::9de0:e5a2:bfa...	ICMPv6	78	Neighbor Advertisement fe80::a16:5ff:fe87:47f0 (rtr, sol)
2096	94.259411239	fe80::a16:5ff:fe87:...	fe80::9de0:e5a2:bfa...	ICMPv6	86	Neighbor Solicitation for fe80::9de0:e5a2:bfab:60ef from 08:16:05:87:47:f0
2097	94.259451104	fe80::9de0:e5a2:bfa...	fe80::a16:5ff:fe87:...	ICMPv6	78	Neighbor Advertisement fe80::9de0:e5a2:bfab:60ef (sol)

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0  
Ethernet II, Src: PAXCompu.d6:83:24 (00:17:0f:d6:83:24), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Address Resolution Protocol (request)

```
(kali㉿kali)-[~]
$ nmap -p 1-1024 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 12:51 EDT
Nmap scan report for kali.station (192.168.1.9)
Host is up (0.0017s latency).
Not shown: 1012 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

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Nella scansione SYN delle porte well-known con switch -sS le porte chiuse rispondono con il pacchetto RST ACK e quindi la richiesta di connessione non viene conclusa, invece quelle aperte rispondono con il pacchetto SYN

```
(kali㉿kali)-[~]
$ nmap -sS -p 1-1024 192.168.1.9
You requested a scan type which requires root privileges.
QUITTING!

(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(kali㉿kali)-[~/home/kali]
# nmap -sS -p 1-1024 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 12:53 EDT
Nmap scan report for kali.stasion (192.168.1.9)
Host is up (0.0011s latency).
Not shown: 1012 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
MAC Address: 08:00:27:5C:EF:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

(kali㉿kali)-[~/home/kali]
# _
```

No.	Time	Source	Destination	Protocol	Length	Info
2034	0.230466034	192.168.1.9	192.168.1.248	TCP	60	60 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2035	0.230466074	192.168.1.9	192.168.1.248	TCP	60	626 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2036	0.230715213	192.168.1.9	192.168.1.248	TCP	60	529 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2037	0.230715291	192.168.1.9	192.168.1.248	TCP	60	836 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2038	0.230715313	192.168.1.9	192.168.1.248	TCP	60	638 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2039	0.230715365	192.168.1.9	192.168.1.248	TCP	60	619 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2040	0.230715409	192.168.1.9	192.168.1.248	TCP	60	200 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2041	0.230965830	192.168.1.9	192.168.1.248	TCP	60	1003 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2042	0.230965914	192.168.1.9	192.168.1.248	TCP	60	351 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2043	0.230965959	192.168.1.9	192.168.1.248	TCP	60	644 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2044	0.231213234	192.168.1.9	192.168.1.248	TCP	60	557 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2045	0.231213309	192.168.1.9	192.168.1.248	TCP	60	833 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2046	0.231213344	192.168.1.9	192.168.1.248	TCP	60	206 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2047	0.231213376	192.168.1.9	192.168.1.248	TCP	60	905 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2048	0.231213407	192.168.1.9	192.168.1.248	TCP	60	112 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2049	0.231457620	192.168.1.9	192.168.1.248	TCP	60	330 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2050	0.231457705	192.168.1.9	192.168.1.248	TCP	60	257 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2051	0.231457729	192.168.1.9	192.168.1.248	TCP	60	756 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2052	0.231777785	192.168.1.9	192.168.1.248	TCP	60	341 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2053	0.231777862	192.168.1.9	192.168.1.248	TCP	60	967 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2054	0.231777885	192.168.1.9	192.168.1.248	TCP	60	1012 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2055	0.231777914	192.168.1.9	192.168.1.248	TCP	60	643 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2056	0.231777940	192.168.1.9	192.168.1.248	TCP	60	891 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2057	0.233130164	192.168.1.248	192.168.1.9	TCP	58	39829 → 712 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2058	0.233194713	192.168.1.248	192.168.1.9	TCP	58	39829 → 489 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2059	0.233233932	192.168.1.248	192.168.1.9	TCP	58	39829 → 869 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2060	0.233277850	192.168.1.248	192.168.1.9	TCP	58	39829 → 145 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2061	0.233697109	192.168.1.9	192.168.1.248	TCP	60	712 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2062	0.233697249	192.168.1.9	192.168.1.248	TCP	60	489 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2063	0.233697273	192.168.1.9	192.168.1.248	TCP	60	869 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2064	0.233982254	192.168.1.9	192.168.1.248	TCP	60	145 → 39829 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

▶ Frame 2058: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0

▶ Ethernet II, Src: PcsCompu\_08:06:a6 (08:00:27:08:06:a6), Dst: PcsCompu\_5c:ef:24 (08:00:27:5c:ef:24)

▶ Internet Protocol Version 4, Src: 192.168.1.248, Dst: 192.168.1.9

▶ Transmission Control Protocol, Src Port: 39829, Dst Port: 489, Seq: 0, Len: 0

La differenza fra la scansione SYN e TCP è che la TCP stabilisce delle connessioni complete, mentre la SYN inizia l'handshake a 3 vie senza completare la connessione infatti anche nelle porte aperte la connessione MISS viene interrotta, è quindi migliore poiché viene rilevata più difficilmente dalla macchina attaccata.

Lo switch -A fornisce una scansione più approfondita che include la versione dei servizi, il sistema operativo, ci da quindi più informazioni.

```
root@kali: /home/kali
File Actions Edit View Help
root@kali:~/home/kali
# nmap -A -p 1-1024 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 12:57 EDT
Nmap scan report for kali.station (192.168.1.9)
Host is up (0.0012s latency).
Not shown: 1012 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 192.168.1.248
|_   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
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkey:
|_   1024 600rfe1c05f6a74d69024fac4d56ccd (DSA)
|_   2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITIME, DSN
|_ ssl-date: 2023-07-19T16:59:09+00:00; +3s from scanner time.
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_   ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_ http-title: Metasploitable2 - Linux
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 35930/udp mountd
|_   100005 1,2,3 56812/tcp mountd
|_   100021 1,3,4 51491/udp nlockmgr
|_   100021 1,3,4 57404/tcp nlockmgr
|_   100024 1 44503/udp status
|_   100024 1 45654/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)
512/tcp   open  exec?
513/tcp   open  login        OpenBSD or Solaris rlogin
514/tcp   open  tcpwrapped
MAC Address: 08:00:27:5C:EF:24 (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
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ clock-skew: mean: 1h20m02s, deviation: 2h18m34s, median: 2s
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ smb-os-discovery:
|_   OS: Unix (Samba 3.0.20-Debian)
|_   Computer name: metasploitable
|_   NetBIOS computer name:
|_   Domain name: localdomain
|_   FQDN: metasploitable.localdomain
|_   System time: 2023-07-19T12:59:01-04:00
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_ smb-security-mode:
|_   account_used: <blank>
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT ADDRESS
1 1.22 ms kali.station (192.168.1.9)

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 75.24 seconds
```