

Esercitazione S5-L2 - Extra

- Differenza tra -sS ed -sT

Osservando i risultati forniti da questi due comandi sono arrivato alla conclusione che i risultati sono uguali. Tuttavia c'è una grande differenza tra le due istruzioni che è il modo in cui esse agiscono. Infatti, mentre il comando **-sT** apre una vera connessione TCP in 4 passaggi, il comando **-sS** non completa il threeway-handshake fermandosi a 3 passaggi. Questo porta il comando **-sS** ad avere meno latenza e quindi ad essere più veloce.

Ciò si può facilmente notare nelle immagini sottostanti, dove per analizzare le stesse porte, l'istruzione **-sT** ci impiega 15,94 secondi, mentre l'istruzione **-sS** ci impiega 15,40 secondi.

Ovviamente più operazioni verranno elaborate, più tale differenza diventerà tangibile.

```
(kali㉿kali)-[~]
└─$ sudo nmap -p- -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:07 CET
Nmap scan report for 192.168.50.101
Host is up (0.00033s latency).
Not shown: 65505 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
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
33616/tcp open  unknown
36821/tcp open  unknown
43988/tcp open  unknown
44731/tcp open  unknown
MAC Address: 08:00:27:CE:05:91 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.94 seconds
```

```

(kali@kali)-[~]
$ sudo nmap -p- -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:06 CET
Nmap scan report for 192.168.50.101
Host is up (0.00029s 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
33616/tcp open  unknown
36821/tcp open  unknown
43988/tcp open  unknown
44731/tcp open  unknown
MAC Address: 08:00:27:CE:05:91 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.40 seconds

```

- **Comando U:53,T:200**

Come richiesto, ho verificato se tale comando fosse utilizzabile con **nmap** per specificare, oltre al numero della porta da analizzare, anche il protocollo.

La risposta è sì, come si può notare dall'immagine sottostante, tuttavia è importante inserire anche delle istruzioni capaci di analizzare i protocolli specificati (in questo caso **-sU** e **-sT**):

```

(kali@kali)-[~]
$ nmap -p U:53,T:200 -sT -sU 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 16:48 CET
Nmap scan report for 192.168.50.101
Host is up (0.00036s latency).

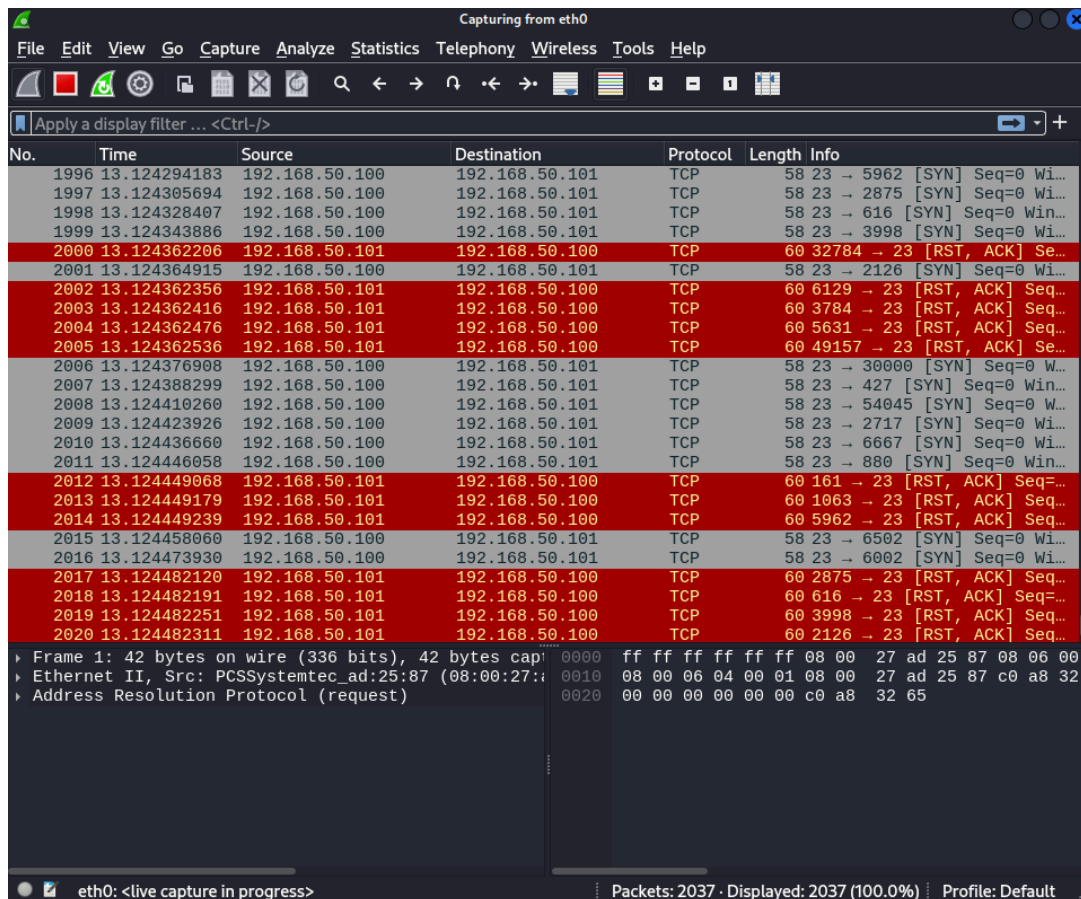
PORT      STATE SERVICE
200/tcp    closed src
53/udp     open  domain
MAC Address: 08:00:27:CE:05:91 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds

```

- **Comando -g**

Il comando **-g** in **nmap** è utilizzato per lo spoofing. In particolare, con tale comando, è possibile selezionare una porta sorgente da cui far partire la scansione del target. Nell'immagine sottostante si può notare il traffico catturato tramite **Wireshark** tra la sorgente 192.168.50.100:23 (dove la porta 23 è stata selezionata con il comando -g) e il target 192.168.50.101. Si può notare come tutte le comunicazioni partono dalla porta 23 e arrivano alla porta 23.



The image shows a Wireshark packet capture window titled "Capturing from eth0". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a display filter bar. The main packet list table is as follows:

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|----------------|----------------|----------|--------|------------------------------|
| 1996 | 13.124294183 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 5962 [SYN] Seq=0 Win... |
| 1997 | 13.124305694 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 2875 [SYN] Seq=0 Win... |
| 1998 | 13.124328407 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 616 [SYN] Seq=0 Win... |
| 1999 | 13.124343886 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 3998 [SYN] Seq=0 Wi... |
| 2000 | 13.124362206 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 32784 → 23 [RST, ACK] Se... |
| 2001 | 13.124364915 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 2126 [SYN] Seq=0 Wi... |
| 2002 | 13.124362356 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 6129 → 23 [RST, ACK] Seq... |
| 2003 | 13.124362416 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 3784 → 23 [RST, ACK] Seq... |
| 2004 | 13.124362476 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 5631 → 23 [RST, ACK] Seq... |
| 2005 | 13.124362536 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 49157 → 23 [RST, ACK] Se... |
| 2006 | 13.124376908 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 30000 [SYN] Seq=0 W... |
| 2007 | 13.124388299 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 427 [SYN] Seq=0 Win... |
| 2008 | 13.124410260 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 54045 [SYN] Seq=0 W... |
| 2009 | 13.124423926 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 2717 [SYN] Seq=0 Wi... |
| 2010 | 13.124436660 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 6667 [SYN] Seq=0 Wi... |
| 2011 | 13.124446058 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 880 [SYN] Seq=0 Win... |
| 2012 | 13.124449068 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 161 → 23 [RST, ACK] Seq=... |
| 2013 | 13.124449179 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 1063 → 23 [RST, ACK] Seq... |
| 2014 | 13.124449239 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 5962 → 23 [RST, ACK] Seq... |
| 2015 | 13.124458060 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 6502 [SYN] Seq=0 Wi... |
| 2016 | 13.124473930 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 23 → 6002 [SYN] Seq=0 Wi... |
| 2017 | 13.124482120 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 2875 → 23 [RST, ACK] Seq... |
| 2018 | 13.124482191 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 616 → 23 [RST, ACK] Seq=... |
| 2019 | 13.124482251 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 3998 → 23 [RST, ACK] Seq... |
| 2020 | 13.124482311 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 2126 → 23 [RST, ACK] Seq... |

Below the packet list, the details pane shows the structure of the selected packet (Frame 1):

- Frame 1: 42 bytes on wire (336 bits), 42 bytes captured on interface eth0
- Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:00:10:08), Dst: 192.168.50.101
- Address Resolution Protocol (request)

The status bar at the bottom indicates: eth0: <live capture in progress> | Packets: 2037 · Displayed: 2037 (100.0%) | Profile: Default

- **Comando -f**

Con il comando **-f** è possibile frammentare i pacchetti inviati per la scansione. Tale funzionalità è utilizzata per sfuggire a diversi sistemi di sicurezza. Questo si può notare grazie al traffico catturato tramite **Wireshark**.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|----------------|----------------|----------|--------|------------------------------|
| 3992 | 32.724063696 | 192.168.50.100 | 192.168.50.101 | TCP | 42 | 47348 → 2190 [SYN] Seq=0... |
| 3993 | 32.724077021 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 3994 | 32.724085237 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 6668 → 47348 [RST, ACK] ... |
| 3995 | 32.724086699 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 3996 | 32.724085347 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 3333 → 47348 [RST, ACK] ... |
| 3997 | 32.724085418 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 49154 → 47348 [RST, ACK] ... |
| 3998 | 32.724094835 | 192.168.50.100 | 192.168.50.101 | TCP | 42 | 47348 → 1216 [SYN] Seq=0... |
| 3999 | 32.724115413 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 4000 | 32.724123448 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 4001 | 32.724142053 | 192.168.50.100 | 192.168.50.101 | TCP | 42 | 47348 → 1641 [SYN] Seq=0... |
| 4002 | 32.724154567 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 4003 | 32.724160889 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 4004 | 32.724163714 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 2190 → 47348 [RST, ACK] ... |
| 4005 | 32.724167661 | 192.168.50.100 | 192.168.50.101 | TCP | 42 | 47348 → 1301 [SYN] Seq=0... |
| 4006 | 32.724176388 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 4007 | 32.724183491 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 4008 | 32.724196616 | 192.168.50.100 | 192.168.50.101 | TCP | 42 | 47348 → 1044 [SYN] Seq=0... |
| 4009 | 32.724211173 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 4010 | 32.724218106 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 4011 | 32.724217876 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 1216 → 47348 [RST, ACK] ... |
| 4012 | 32.724217986 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 1641 → 47348 [RST, ACK] ... |
| 4013 | 32.724218046 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 1301 → 47348 [RST, ACK] ... |
| 4014 | 32.724224608 | 192.168.50.100 | 192.168.50.101 | TCP | 42 | 47348 → 6389 [SYN] Seq=0... |
| 4015 | 32.724233254 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |
| 4016 | 32.724240097 | 192.168.50.100 | 192.168.50.101 | IPv4 | 42 | Fragmented IP protocol (...) |

▶ Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0
 ▶ Ethernet II, Src: PCSSystemtec_ad:05:91:08:00:27, Dst: 08:00:06:04:00:01
 ▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 192.168.50.100
 ▶ User Datagram Protocol, Src Port: 68, Dst Port: 47348
 ▶ Dynamic Host Configuration Protocol (Discover)

- Comando -D

Il comando -D è utilizzato per mascherare l'indirizzo IP sorgente, utilizzando un pool di indirizzi IP forniti. In particolare, è possibile utilizzare la funzione RND:10 interna per assegnare 10 indirizzi IP generati in maniera randomica.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|--------------|-----------------|----------------|----------|--------|-----------------------------|
| 12007 | 13.319429108 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 58101 → 2607 [SYN] Seq=0... |
| 12008 | 13.319436021 | 6.231.194.169 | 192.168.50.101 | TCP | 58 | 58101 → 2607 [SYN] Seq=0... |
| 12009 | 13.319459555 | 142.145.79.214 | 192.168.50.101 | TCP | 58 | 58101 → 2607 [SYN] Seq=0... |
| 12010 | 13.319529737 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 2607 → 58101 [RST, ACK] ... |
| 12011 | 13.319544073 | 39.192.62.152 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12012 | 13.319556026 | 138.102.147.223 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12013 | 13.319562558 | 217.20.47.199 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12014 | 13.319590130 | 123.180.166.177 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12015 | 13.319597454 | 103.181.20.59 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12016 | 13.319623502 | 41.92.3.148 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12017 | 13.319696169 | 33.81.10.221 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12018 | 13.319709574 | 181.74.223.145 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12019 | 13.319731725 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12020 | 13.319738839 | 6.231.194.169 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12021 | 13.319769286 | 142.145.79.214 | 192.168.50.101 | TCP | 58 | 58101 → 9040 [SYN] Seq=0... |
| 12022 | 13.319780397 | 39.192.62.152 | 192.168.50.101 | TCP | 58 | 58101 → 992 [SYN] Seq=0... |
| 12023 | 13.319786438 | 138.102.147.223 | 192.168.50.101 | TCP | 58 | 58101 → 992 [SYN] Seq=0... |
| 12024 | 13.319803730 | 192.168.50.101 | 192.168.50.100 | TCP | 60 | 9040 → 58101 [RST, ACK] ... |
| 12025 | 13.319814501 | 217.20.47.199 | 192.168.50.101 | TCP | 58 | 58101 → 992 [SYN] Seq=0... |
| 12026 | 13.319821223 | 123.180.166.177 | 192.168.50.101 | TCP | 58 | 58101 → 992 [SYN] Seq=0... |
| 12027 | 13.319827295 | 103.181.20.59 | 192.168.50.101 | TCP | 58 | 58101 → 992 [SYN] Seq=0... |
| 12028 | 13.319832815 | 41.92.3.148 | 192.168.50.101 | TCP | 58 | 58101 → 992 [SYN] Seq=0... |
| 12029 | 13.319865075 | 33.81.10.221 | 192.168.50.101 | TCP | 58 | 58101 → 992 [SYN] Seq=0... |
| 12030 | 13.319887938 | 181.74.223.145 | 192.168.50.101 | TCP | 58 | 58101 → 992 [SYN] Seq=0... |
| 12031 | 13.319895022 | 192.168.50.100 | 192.168.50.101 | TCP | 58 | 58101 → 992 [SYN] Seq=0... |

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0
 ▶ Ethernet II, Src: PCSSystemtec_ad:25:87:08:00:27, Dst: 08:00:06:04:00:01
 ▶ Address Resolution Protocol (request)

