

# NETWORK SCANNING CON NMAP

## TASK

1. Scansione TCP sulle porte well-known
2. Scansione SYN sulle porte well-known
3. Scansione con switch <<-A>> sulle porte well-known

Successivamente per ognuno degli scan effettuati riportare:

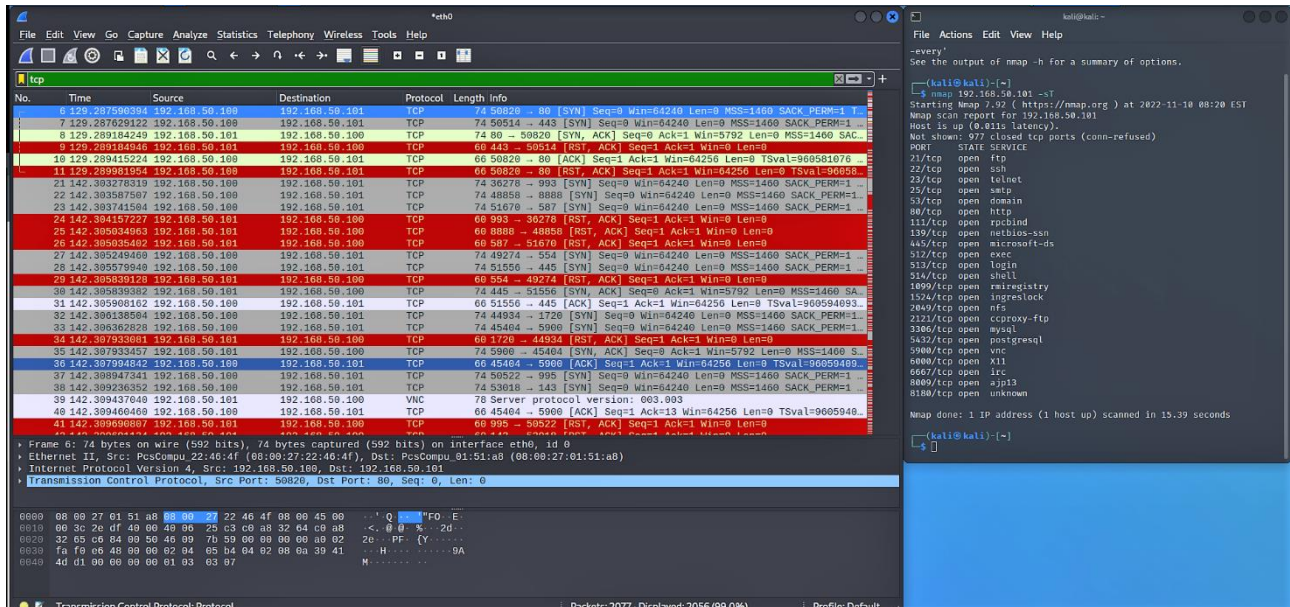
- La fonte dello scan
- Il target dello scan
- Il tipo di scan
- I risultati ottenuti

## ANALISI E VALUTAZIONI

Innanzitutto dobbiamo effettuare lo scan come richiesto, di fatti elenchiamo una tabella con le diverse caratteristiche:

FONT SCAN	TARGET SCAN	TYPE SCAN	RESULTS SCAN
192.168.50.100	192.168.50.101	nmap 192.168.50.101 - sT	12 porte well-known aperte trovate
192.168.50.100	192.168.50.101	nmap 192.168.50.101 - sS	12 porte well-known aperte trovate
192.168.50.100	192.168.50.101	nmap 192.168.50.101 - A	x porte well-known aperte trovate

1. **SCAN TCP:** Partiamo nello scansionare il protocollo TCP sulle porte well-known le quali sono le porte che vanno da 0 a 1023. Per riuscire a identificare quali sono le porte aperte del protocollo ci basterà effettuare uno scan su di un server target il quale sarà il nostro metasploitable. Di fatti il comando da utilizzare sarà `<<nmap 192.168.50.101 -sT>>`. L'indirizzo IP utilizzato è proprio quello di metasploitable, pertanto verranno fuori i servizi con i protocolli di tipo TCP di cui di seguito:



Poiché dobbiamo considerare solo le porte well-known allora saranno quest'ultime:

PORT	STATUS	SERVICE
21/tcp	Open	ftp
22/tcp	Open	Ssh
23/tcp	Open	telnet
25/tcp	Open	Smtpt
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	Logic
514/tcp	Open	shell

Ricordando che protocolli TCP sono quei protocolli che effettuano la connessione di tipo 3-way-handshake ovvero che attraverso 3 passaggi tra client-server si instaura la connessione. Di fatti andando a filtrare i risultati ottenuti su di una singola porta possiamo effettuare un analisi:

No.	Time	Source	Destination	Protocol	Length	Info
50	142.320308770	192.168.50.100	192.168.50.101	TCP	74	39418 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=...
52	142.321153659	192.168.50.101	192.168.50.100	TCP	74	22 → 39418 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER...
54	142.321225522	192.168.50.100	192.168.50.101	TCP	66	39418 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=960594108 TSecr...
97	142.330850366	192.168.50.100	192.168.50.101	TCP	66	39418 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=960594118 ...

Come si può notare i passaggi effettuati sono effettivamente “4” (l’ultimo per chiudere la connessione):

1. SYN da kali a metasploitable
2. SYN+ACK da metasploitable a kali
3. ACK da kali a metasploitable
4. RESET(RST) chiusura connessione da parte di metasploitable

**N.B.** E’ possibile andare ad analizzare proprio questi passaggi andando dal menù “Transmission control protocol” → “Conversation completeness” → “Complete”

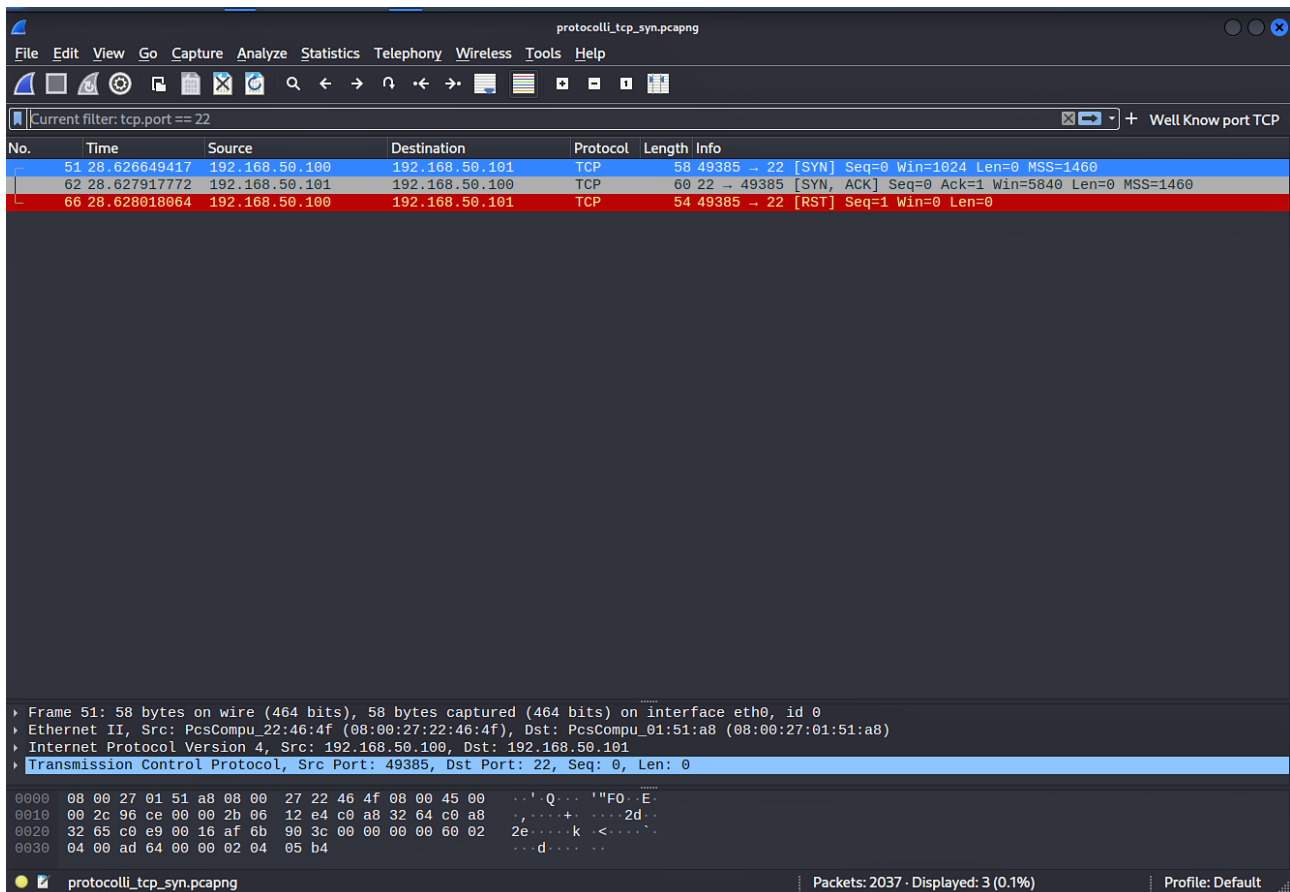
2. **SCAN SYN:** Successivamente andiamo a scansionare SYN, tramite il comando <<sudo nmap 192.168.50.101 -sS>> (Sudo perché richiede i permessi) e tra le porte well-known ritroviamo le seguenti:

PORT	STATUS	SERVICE
21/tcp	Open	ftp
22/tcp	Open	Ssh
23/tcp	Open	telnet
25/tcp	Open	Sntp
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	Logic
514/tcp	Open	Shell

In pratica avremo le stesse porte. Ora attraverso wireshark andiamo ad intercettare i pacchetti, e il risultato sarà il seguente:

The image shows a terminal window with the command `sudo nmap 192.168.50.101 -sS` and its output. The output lists 13 open ports with their corresponding services. On the left, the Wireshark interface displays a packet capture on the `eth0` interface, showing a SYN packet from 192.168.50.101 to 192.168.50.101 on port 445. The packet details show the TCP header with sequence number 49385 and window size 0.

Andando ora ad esaminare una delle porte (es.22 la stessa esaminata precedentemente) noteremo in effetti che in questo caso avremo “3” pacchetti, in quanto nella scansione SYN la connessione non viene conclusa, ma si ferma e si chiude dopo il primo ACK inviato, di fatti:



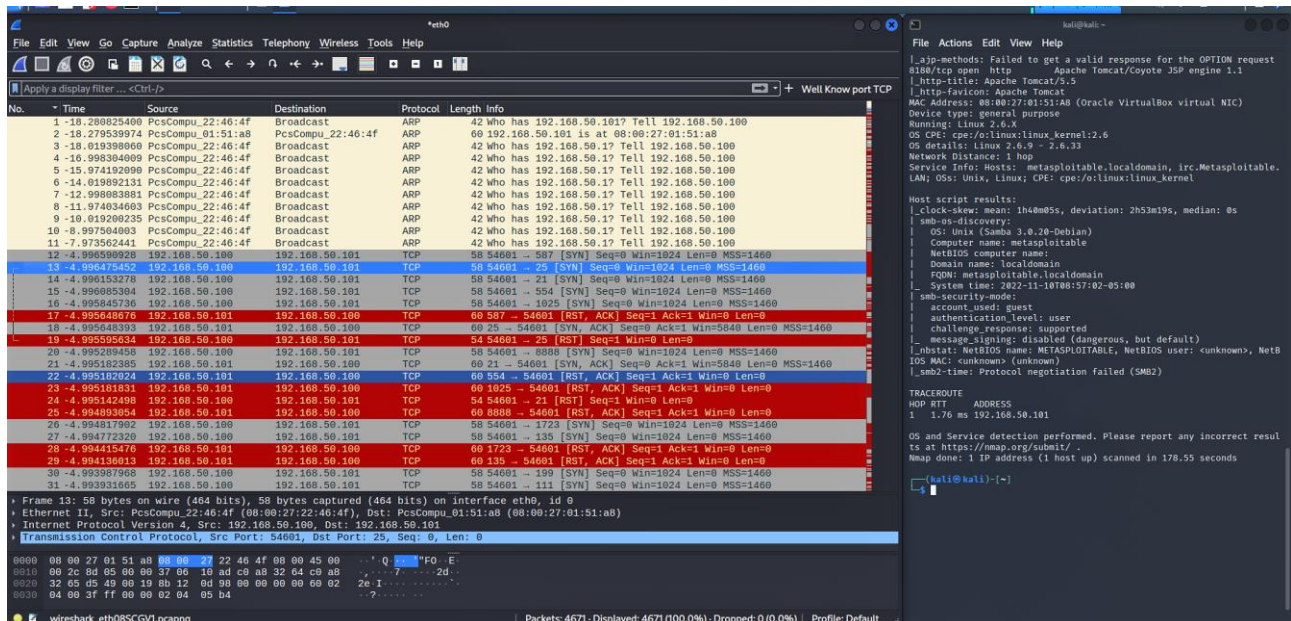
I passaggi sono:

1. SYN da parte di kali per metasploitable
2. SYN+ACK da parte di metasploitable per kali
3. RESET(RST) in questo caso kali termina la connessione con metasploitable

**N.B.** Anche in questo caso possiamo andare ad analizzare questi 3 semplici passaggi andando su  
 “Transmission control Protocol” → “Conversation completeness” → “Incomplete”

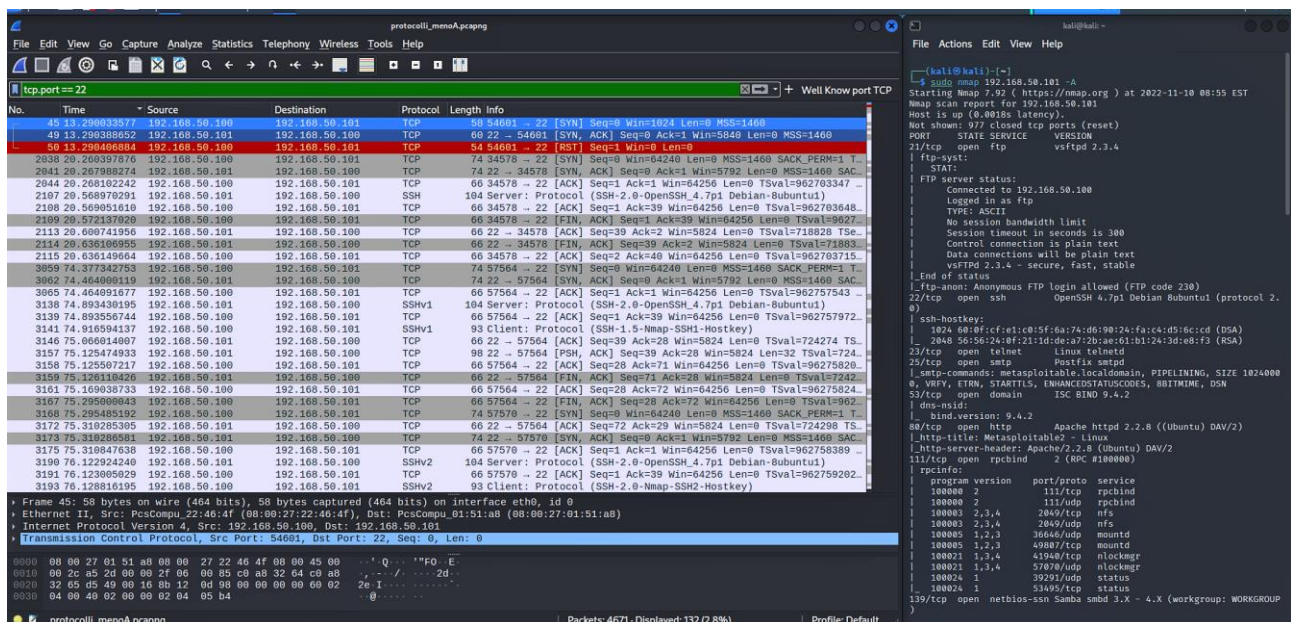


3. **SCAN -A:** Infine come ultimo passaggio andiamo ad effettuare la scansione, con target metasploitable, con il comando `<<nmap 192.168.50.101 -A>>`, in tal caso troveremo molti più pacchetti scambiati da protocolli diversi, non solo TCP, di fatti il risultato ottenuto sarà del tipo:



```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[Apply a display filter ...<Ctrl>] Well known port TCP
No. Time Source Destination Protocol Length Info
1 -18.280625408 PcsCompu_22:46:4f Broadcast ARP 42 Who has 192.168.50.101? Tell 192.168.50.100
2 -18.279539974 PcsCompu_01:51:a8 PcsCompu_22:46:4f ARP 60 192.168.50.101 is at 08:00:27:01:51:a8
3 -18.013998968 PcsCompu_22:46:4f Broadcast ARP 42 Who has 192.168.50.17? Tell 192.168.50.100
4 -18.998304069 PcsCompu_22:46:4f Broadcast ARP 42 Who has 192.168.50.17? Tell 192.168.50.100
5 -15.974192090 PcsCompu_22:46:4f Broadcast ARP 42 Who has 192.168.50.17? Tell 192.168.50.100
6 -14.018982131 PcsCompu_22:46:4f Broadcast ARP 42 Who has 192.168.50.17? Tell 192.168.50.100
7 -12.998038381 PcsCompu_22:46:4f Broadcast ARP 42 Who has 192.168.50.17? Tell 192.168.50.100
8 -11.974034693 PcsCompu_22:46:4f Broadcast ARP 42 Who has 192.168.50.17? Tell 192.168.50.100
9 -10.019206235 PcsCompu_22:46:4f Broadcast ARP 42 Who has 192.168.50.17? Tell 192.168.50.100
10 -8.997504093 PcsCompu_22:46:4f Broadcast ARP 42 Who has 192.168.50.17? Tell 192.168.50.100
11 -7.973562441 PcsCompu_22:46:4f Broadcast ARP 42 Who has 192.168.50.17? Tell 192.168.50.100
12 -4.998309978 192.168.50.100 192.168.50.101 TCP 60 54601 -> 54601 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13 -4.998475452 192.168.50.100 192.168.50.101 TCP 58 54601 -> 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14 -4.996153278 192.168.50.100 192.168.50.101 TCP 58 54601 -> 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15 -4.996885384 192.168.50.100 192.168.50.101 TCP 58 54601 -> 534 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16 -4.995845736 192.168.50.100 192.168.50.101 TCP 58 54601 -> 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17 -4.995648076 192.168.50.101 192.168.50.100 TCP 60 587 -> 54601 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18 -4.995648393 192.168.50.101 192.168.50.100 TCP 60 25 -> 54601 [SYN, ACK] Seq=0 Ack=1 Win=5848 Len=0 MSS=1460
19 -4.995555224 192.168.50.100 192.168.50.101 TCP 54 54601 -> 25 [RST] Seq=1 Win=0 Len=0
20 -4.995304538 192.168.50.100 192.168.50.101 TCP 58 54601 -> 6500 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21 -4.995182385 192.168.50.101 192.168.50.100 TCP 60 21 -> 54601 [SYN, ACK] Seq=0 Ack=1 Win=5848 Len=0 MSS=1460
22 -4.995182924 192.168.50.101 192.168.50.100 TCP 60 554 -> 54601 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 -4.995182924 192.168.50.101 192.168.50.100 TCP 60 1025 -> 54601 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 -4.995142486 192.168.50.100 192.168.50.101 TCP 54 54601 -> 21 [RST] Seq=1 Win=0 Len=0
25 -4.994893854 192.168.50.101 192.168.50.100 TCP 60 8888 -> 54601 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26 -4.994817992 192.168.50.100 192.168.50.101 TCP 58 54601 -> 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27 -4.994772320 192.168.50.101 192.168.50.101 TCP 58 54601 -> 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28 -4.994414576 192.168.50.100 192.168.50.100 TCP 60 1723 -> 54601 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29 -4.994136013 192.168.50.101 192.168.50.100 TCP 60 135 -> 54601 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30 -4.993987968 192.168.50.100 192.168.50.101 TCP 58 54601 -> 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31 -4.993931665 192.168.50.100 192.168.50.101 TCP 58 54601 -> 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
...
Frame 33: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_22:46:4f (08:00:27:22:46:4f), Dst: PcsCompu_01:51:a8 (08:00:27:01:51:a8)
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
Transmission Control Protocol, Src Port: 54601, Dst Port: 25, Seq: 0, Len: 0
...
Packets: 4671 - Displayed: 4671 (100.0%) - Dropped: 0 (0.0%) - Profile: Default
```

Dove se andassimo ad analizzare una sola porta in questione, ovvero la n.22 otterremo molti più pacchetti di questo risultato:



```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[Apply a display filter ...<Ctrl>] Well known port TCP
No. Time Source Destination Protocol Length Info
45 13.299033577 192.168.50.100 192.168.50.101 TCP 60 22 -> 54601 [SYN, ACK] Seq=0 Win=1024 Len=0 MSS=1460
49 13.298388652 192.168.50.101 192.168.50.100 TCP 60 22 -> 54601 [SYN, ACK] Seq=0 Win=1024 Len=0 MSS=1460
50 13.298406804 192.168.50.100 192.168.50.101 TCP 60 54601 -> 22 [RST] Seq=1 Win=0 Len=0
2038 20.260397076 192.168.50.100 192.168.50.101 TCP 74 34578 -> 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
2041 20.267988274 192.168.50.101 192.168.50.100 TCP 74 22 -> 34578 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC...
2044 20.268102242 192.168.50.100 192.168.50.101 TCP 66 34578 -> 22 [ACK] Seq=1 Ack=28 Win=64256 Len=0 TSval=962703347...
2107 20.569970291 192.168.50.101 192.168.50.100 SSH 104 Server: Protocol (SSH-2.0-OpenSSH_4.7p1 Debian-Rubuntu1)
2108 20.569951610 192.168.50.100 192.168.50.101 TCP 66 34578 -> 22 [ACK] Seq=1 Ack=39 Win=64256 Len=0 TSval=962703648...
2109 20.572137020 192.168.50.100 192.168.50.101 TCP 66 34578 -> 22 [FIN, ACK] Seq=1 Ack=39 Win=64256 Len=0 TSval=9627...
2113 20.609741956 192.168.50.101 192.168.50.100 TCP 66 22 -> 34578 [ACK] Seq=39 Ack=2 Win=5824 Len=0 TSval=718028 Tse...
2114 20.636169995 192.168.50.101 192.168.50.100 TCP 66 22 -> 34578 [FIN, ACK] Seq=39 Ack=2 Win=5824 Len=0 TSval=718088...
2115 20.636149664 192.168.50.100 192.168.50.101 TCP 66 34578 -> 22 [ACK] Seq=2 Ack=40 Win=64256 Len=0 TSval=962703715...
3059 74.377342553 192.168.50.100 192.168.50.101 TCP 74 57564 -> 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
3062 74.464809119 192.168.50.101 192.168.50.100 TCP 74 22 -> 57564 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC...
3065 74.464891677 192.168.50.100 192.168.50.101 TCP 66 57564 -> 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=962757543...
3138 74.893430195 192.168.50.101 192.168.50.100 SSHv1 104 Server: Protocol (SSH-2.0-OpenSSH_4.7p1 Debian-Rubuntu1)
3139 74.893556744 192.168.50.100 192.168.50.101 TCP 66 57564 -> 22 [ACK] Seq=1 Ack=39 Win=64256 Len=0 TSval=962757972...
3141 74.916594137 192.168.50.100 192.168.50.101 SSHv1 93 Client: Protocol (SSH-1.5-Nmap-SSH-Hostkey)
3146 75.060614097 192.168.50.101 192.168.50.100 TCP 66 22 -> 57564 [ACK] Seq=39 Ack=28 Win=5824 Len=0 TSval=724274 TS...
3157 75.125474933 192.168.50.101 192.168.50.100 TCP 98 22 -> 57564 [PSH, ACK] Seq=39 Ack=28 Win=5824 Len=32 TSval=724...
3158 75.125507217 192.168.50.100 192.168.50.101 TCP 66 57564 -> 22 [ACK] Seq=28 Ack=71 Win=64256 Len=0 TSval=962758020...
3159 75.126118426 192.168.50.101 192.168.50.100 TCP 66 22 -> 57564 [FIN, ACK] Seq=71 Ack=28 Win=5824 Len=0 TSval=724298 TS...
3161 75.169038733 192.168.50.100 192.168.50.101 TCP 66 57564 -> 22 [ACK] Seq=28 Ack=72 Win=64256 Len=0 TSval=96275824...
3167 75.295080943 192.168.50.100 192.168.50.101 TCP 66 57564 -> 22 [FIN, ACK] Seq=28 Ack=72 Win=64256 Len=0 TSval=962...
3168 75.295485192 192.168.50.100 192.168.50.101 TCP 74 57578 -> 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
3172 75.319285395 192.168.50.101 192.168.50.100 TCP 66 22 -> 57564 [ACK] Seq=72 Ack=29 Win=5824 Len=0 TSval=724298 TS...
3173 75.319285981 192.168.50.101 192.168.50.100 TCP 74 22 -> 57578 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC...
3175 75.319847638 192.168.50.100 192.168.50.101 TCP 66 57578 -> 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=962758389...
3190 76.122924240 192.168.50.101 192.168.50.100 SSHv2 104 Server: Protocol (SSH-2.0-OpenSSH_4.7p1 Debian-Rubuntu1)
3191 76.123069629 192.168.50.100 192.168.50.101 TCP 66 57578 -> 22 [ACK] Seq=1 Ack=39 Win=64256 Len=0 TSval=962759202...
3193 76.123016510 192.168.50.100 192.168.50.101 SSHv2 93 Client: Protocol (SSH-2.0-Nmap-SSH-Hostkey)
...
Frame 45: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_22:46:4f (08:00:27:22:46:4f), Dst: PcsCompu_01:51:a8 (08:00:27:01:51:a8)
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101
Transmission Control Protocol, Src Port: 54601, Dst Port: 22, Seq: 0, Len: 0
...
Packets: 4671 - Displayed: 132 (2.8%) - Profile: Default
```

Tale scansione è molto più approfondita di fatti essa ci fornisce molte più informazioni riguardo ai pacchetti trasmessi delle porte aperte, soprattutto dall'interfaccia del terminale.