

# Nmap

Scansione della macchina Metasploitable (ip 192.168.32.101) da Kali Linux (ip 192.168.32.100).

## SCANSIONE TCP DELLE PORTE

### **nmap -sT**

Questo switch conclude il three-way-handshake ed esegue una scansione TCP di tutte le porte.

In evidenza le porte non scansionate nella scansione SYN con lo switch -F.

```
(kali㉿kali)-[~]
└─$ nmap -sT 192.168.32.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 18:21 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dn
s-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or sp
ecify valid servers with --dns-servers
Nmap scan report for 192.168.32.101
Host is up (0.0026s 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
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

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

## nmap -F

Questo switch esegue una scansione SYN, che significa che NON conclude il three-way-handshake e scansiona solo le porte well-known.

```
(kali@kali)-[~]
$ nmap -F 192.168.32.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 18:23 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.32.101
Host is up (0.00030s 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
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

## nmap -sS

Questo switch richiede di essere eseguito da utente admin.

Esegue una scansione SYN, che significa che NON conclude il three-way-handshake, ma scansiona tutte le porte. In evidenza le porte non scansionate nella scansione SYN con lo switch -F, possiamo notare che sono le stesse porte scansionate utilizzando lo switch -sT.

```
(kali@kali)-[~]
$ nmap -sS 192.168.32.101
You requested a scan type which requires root privileges.
QUITTING!

(kali@kali)-[~]
$ sudo nmap -sS 192.168.32.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 18:35 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.32.101
Host is up (0.000066s 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: 08:00:27:11:6C:88 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

## nmap -A

Scansione aggressiva, restituisce ulteriori informazioni, come il tempo di esecuzione della scansione, informazioni sull'host e sullo stato dei servizi attivi su ciascuna porta.

```
nmap -A 192.168.32.101

Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-19 18:56 EDT

mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers: No such file or directory (2)

mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 18:56 (0:00:02 remaining)
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 18:56 (0:00:01 remaining)
Nmap scan report for 192.168.32.101
Host is up (0.00024s latency).
Not shown: 977 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 192.168.32.100
|   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 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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            41410/tcp   mountd
|   100005   1,2,3            48914/udp   mountd
|   100021   1,3,4            42863/tcp   nlockmgr
|   100021   1,3,4            45225/udp   nlockmgr
|   100024   1                43466/udp   status
|_  100024   1                59242/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        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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 11
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, Support41Auth, SupportsTransactions,
SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsCompression
|   Status: Autocommit
|_  Salt: f=:lQ3GL'~fb;?is)nph
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-07-19T22:57:19+00:00; -2s from scanner time.
| 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
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_  VNC Authentication (2)

```

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|\_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|\_http-title: Apache Tomcat/5.5

|\_http-favicon: Apache Tomcat

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_clock-skew: mean: 1h19m58s, deviation: 2h18m34s, median: -2s

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|\_ System time: 2023-07-19T18:56:41-04:00

|\_smb2-time: Protocol negotiation failed (SMB2)

|\_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

| smb-security-mode:

| account\_used: <blank>

| authentication\_level: user

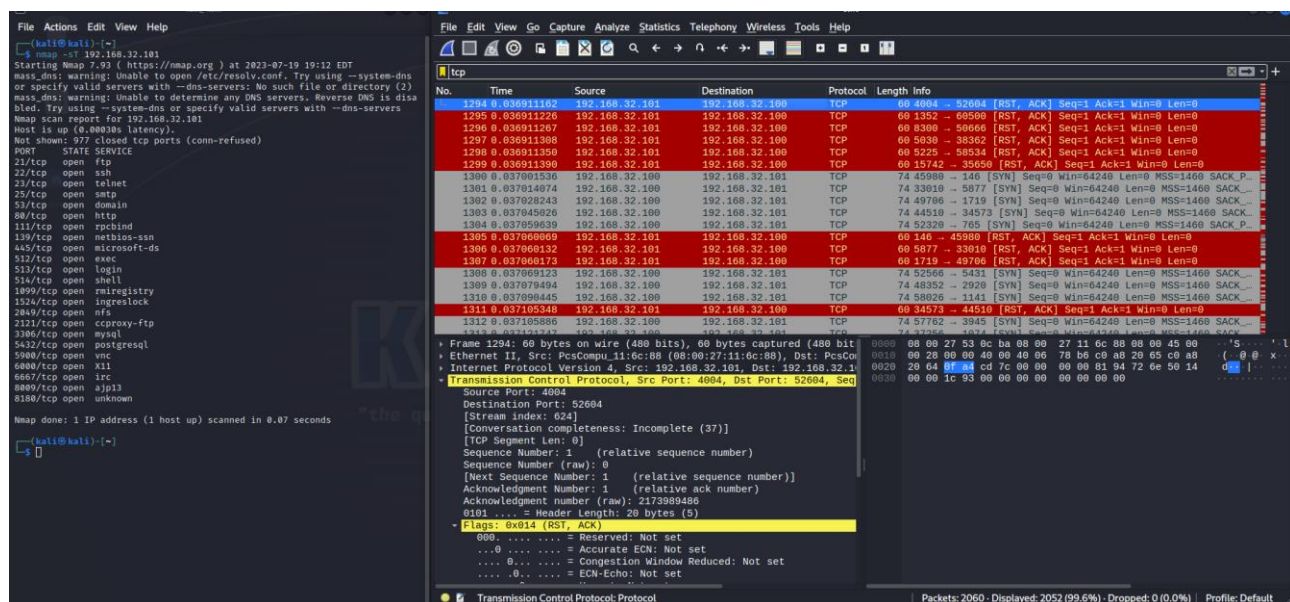
| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

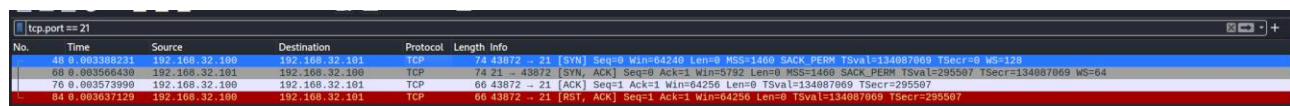
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 128.77 seconds

## Scansione TCP completa con switch -sT e cattura dei pacchetti con Wireshark



Vediamo i pacchetti su una porta aperta, la porta 21:



Step 1:

da Kali a Metasploitable

192.168.32.100 192.168.32.101

SYN Seq=0

21 [SYN] Seq=0

Step 2:

da Metasploitable a Kali

192.168.32.101 192.168.32.100

SYN, ACK Seq=0, Ack=1

[SYN, ACK] Seq=0 Ack=1

Step 3:

da Kali a Metasploitable

192.168.32.100 192.168.32.101

ACK Seq=1, Ack=1

21 [ACK] Seq=1 Ack=1

Step 4 (chiusura connessione con flag RST a three-way handshake concluso):

da Kali a Metasploitable

192.168.32.100 192.168.32.101

RST, ACK Seq=1, Ack=1

21 [RST, ACK] Seq=1 Ack=1



In caso di porta chiusa, come la 70, vediamo che il target chiude la comunicazione inviando il flag ACK, RST:

tcp.port == 70					
No.	Time	Source	Destination	Protocol	Length Info
532	0.007923612	192.168.32.100	192.168.32.101	TCP	74 44848 → 70 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=134087074 TSecr=0 WS=128
584	0.008268616	192.168.32.101	192.168.32.100	TCP	60 70 → 44848 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

## Scansione TCP SYN con switch -sS e cattura dei pacchetti con Wireshark

The image shows a Kali Linux terminal window on the left and a Wireshark network capture window on the right. The terminal window displays the output of an nmap -sS scan of 192.168.32.101. The scan results show 21 open ports: 21/tcp, 22/tcp, 23/tcp, 25/tcp, 53/tcp, 80/tcp, 111/tcp, 135/tcp, 445/tcp, 512/tcp, 513/tcp, 514/tcp, 515/tcp, 516/tcp, 517/tcp, 518/tcp, 519/tcp, 520/tcp, 521/tcp, 522/tcp, 523/tcp, 524/tcp, 525/tcp, 526/tcp, 527/tcp, 528/tcp, 529/tcp, 530/tcp, 531/tcp, 532/tcp, 533/tcp, 534/tcp, 535/tcp, 536/tcp, 537/tcp, 538/tcp, 539/tcp, 540/tcp, 541/tcp, 542/tcp, 543/tcp, 544/tcp, 545/tcp, 546/tcp, 547/tcp, 548/tcp, 549/tcp, 550/tcp, 551/tcp, 552/tcp, 553/tcp, 554/tcp, 555/tcp, 556/tcp, 557/tcp, 558/tcp, 559/tcp, 560/tcp, 561/tcp, 562/tcp, 563/tcp, 564/tcp, 565/tcp, 566/tcp, 567/tcp, 568/tcp, 569/tcp, 570/tcp, 571/tcp, 572/tcp, 573/tcp, 574/tcp, 575/tcp, 576/tcp, 577/tcp, 578/tcp, 579/tcp, 580/tcp, 581/tcp, 582/tcp, 583/tcp, 584/tcp, 585/tcp, 586/tcp, 587/tcp, 588/tcp, 589/tcp, 590/tcp, 591/tcp, 592/tcp, 593/tcp, 594/tcp, 595/tcp, 596/tcp, 597/tcp, 598/tcp, 599/tcp, 600/tcp, 601/tcp, 602/tcp, 603/tcp, 604/tcp, 605/tcp, 606/tcp, 607/tcp, 608/tcp, 609/tcp, 610/tcp, 611/tcp, 612/tcp, 613/tcp, 614/tcp, 615/tcp, 616/tcp, 617/tcp, 618/tcp, 619/tcp, 620/tcp, 621/tcp, 622/tcp, 623/tcp, 624/tcp, 625/tcp, 626/tcp, 627/tcp, 628/tcp, 629/tcp, 630/tcp, 631/tcp, 632/tcp, 633/tcp, 634/tcp, 635/tcp, 636/tcp, 637/tcp, 638/tcp, 639/tcp, 640/tcp, 641/tcp, 642/tcp, 643/tcp, 644/tcp, 645/tcp, 646/tcp, 647/tcp, 648/tcp, 649/tcp, 650/tcp, 651/tcp, 652/tcp, 653/tcp, 654/tcp, 655/tcp, 656/tcp, 657/tcp, 658/tcp, 659/tcp, 660/tcp, 661/tcp, 662/tcp, 663/tcp, 664/tcp, 665/tcp, 666/tcp, 667/tcp, 668/tcp, 669/tcp, 670/tcp, 671/tcp, 672/tcp, 673/tcp, 674/tcp, 675/tcp, 676/tcp, 677/tcp, 678/tcp, 679/tcp, 680/tcp, 681/tcp, 682/tcp, 683/tcp, 684/tcp, 685/tcp, 686/tcp, 687/tcp, 688/tcp, 689/tcp, 690/tcp, 691/tcp, 692/tcp, 693/tcp, 694/tcp, 695/tcp, 696/tcp, 697/tcp, 698/tcp, 699/tcp, 700/tcp, 701/tcp, 702/tcp, 703/tcp, 704/tcp, 705/tcp, 706/tcp, 707/tcp, 708/tcp, 709/tcp, 710/tcp, 711/tcp, 712/tcp, 713/tcp, 714/tcp, 715/tcp, 716/tcp, 717/tcp, 718/tcp, 719/tcp, 720/tcp, 721/tcp, 722/tcp, 723/tcp, 724/tcp, 725/tcp, 726/tcp, 727/tcp, 728/tcp, 729/tcp, 730/tcp, 731/tcp, 732/tcp, 733/tcp, 734/tcp, 735/tcp, 736/tcp, 737/tcp, 738/tcp, 739/tcp, 740/tcp, 741/tcp, 742/tcp, 743/tcp, 744/tcp, 745/tcp, 746/tcp, 747/tcp, 748/tcp, 749/tcp, 750/tcp, 751/tcp, 752/tcp, 753/tcp, 754/tcp, 755/tcp, 756/tcp, 757/tcp, 758/tcp, 759/tcp, 760/tcp, 761/tcp, 762/tcp, 763/tcp, 764/tcp, 765/tcp, 766/tcp, 767/tcp, 768/tcp, 769/tcp, 770/tcp, 771/tcp, 772/tcp, 773/tcp, 774/tcp, 775/tcp, 776/tcp, 777/tcp, 778/tcp, 779/tcp, 780/tcp, 781/tcp, 782/tcp, 783/tcp, 784/tcp, 785/tcp, 786/tcp, 787/tcp, 788/tcp, 789/tcp, 790/tcp, 791/tcp, 792/tcp, 793/tcp, 794/tcp, 795/tcp, 796/tcp, 797/tcp, 798/tcp, 799/tcp, 800/tcp, 801/tcp, 802/tcp, 803/tcp, 804/tcp, 805/tcp, 806/tcp, 807/tcp, 808/tcp, 809/tcp, 810/tcp, 811/tcp, 812/tcp, 813/tcp, 814/tcp, 815/tcp, 816/tcp, 817/tcp, 818/tcp, 819/tcp, 820/tcp, 821/tcp, 822/tcp, 823/tcp, 824/tcp, 825/tcp, 826/tcp, 827/tcp, 828/tcp, 829/tcp, 830/tcp, 831/tcp, 832/tcp, 833/tcp, 834/tcp, 835/tcp, 836/tcp, 837/tcp, 838/tcp, 839/tcp, 840/tcp, 841/tcp, 842/tcp, 843/tcp, 844/tcp, 845/tcp, 846/tcp, 847/tcp, 848/tcp, 849/tcp, 850/tcp, 851/tcp, 852/tcp, 853/tcp, 854/tcp, 855/tcp, 856/tcp, 857/tcp, 858/tcp, 859/tcp, 860/tcp, 861/tcp, 862/tcp, 863/tcp, 864/tcp, 865/tcp, 866/tcp, 867/tcp, 868/tcp, 869/tcp, 870/tcp, 871/tcp, 872/tcp, 873/tcp, 874/tcp, 875/tcp, 876/tcp, 877/tcp, 878/tcp, 879/tcp, 880/tcp, 881/tcp, 882/tcp, 883/tcp, 884/tcp, 885/tcp, 886/tcp, 887/tcp, 888/tcp, 889/tcp, 890/tcp, 891/tcp, 892/tcp, 893/tcp, 894/tcp, 895/tcp, 896/tcp, 897/tcp, 898/tcp, 899/tcp, 900/tcp, 901/tcp, 902/tcp, 903/tcp, 904/tcp, 905/tcp, 906/tcp, 907/tcp, 908/tcp, 909/tcp, 910/tcp, 911/tcp, 912/tcp, 913/tcp, 914/tcp, 915/tcp, 916/tcp, 917/tcp, 918/tcp, 919/tcp, 920/tcp, 921/tcp, 922/tcp, 923/tcp, 924/tcp, 925/tcp, 926/tcp, 927/tcp, 928/tcp, 929/tcp, 930/tcp, 931/tcp, 932/tcp, 933/tcp, 934/tcp, 935/tcp, 936/tcp, 937/tcp, 938/tcp, 939/tcp, 940/tcp, 941/tcp, 942/tcp, 943/tcp, 944/tcp, 945/tcp, 946/tcp, 947/tcp, 948/tcp, 949/tcp, 950/tcp, 951/tcp, 952/tcp, 953/tcp, 954/tcp, 955/tcp, 956/tcp, 957/tcp, 958/tcp, 959/tcp, 960/tcp, 961/tcp, 962/tcp, 963/tcp, 964/tcp, 965/tcp, 966/tcp, 967/tcp, 968/tcp, 969/tcp, 970/tcp, 971/tcp, 972/tcp, 973/tcp, 974/tcp, 975/tcp, 976/tcp, 977/tcp, 978/tcp, 979/tcp, 980/tcp, 981/tcp, 982/tcp, 983/tcp, 984/tcp, 985/tcp, 986/tcp, 987/tcp, 988/tcp, 989/tcp, 990/tcp, 991/tcp, 992/tcp, 993/tcp, 994/tcp, 995/tcp, 996/tcp, 997/tcp, 998/tcp, 999/tcp, 1000/tcp.

The Wireshark window shows a network capture of the scan. The first packet is a SYN packet from 192.168.32.100 to 192.168.32.101 on port 70. The second packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The third packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fourth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventh packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The tenth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eleventh packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twelfth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirteenth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fourteenth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifteenth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixteenth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventeenth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighteenth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The nineteenth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twentieth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twenty-first packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twenty-second packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twenty-third packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twenty-fourth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twenty-fifth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twenty-sixth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twenty-seventh packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twenty-eighth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The twenty-ninth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirtieth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirty-first packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirty-second packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirty-third packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirty-fourth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirty-fifth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirty-sixth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirty-seventh packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirty-eighth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The thirty-ninth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fortieth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The forty-first packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The forty-second packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The forty-third packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The forty-fourth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The forty-fifth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The forty-sixth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The forty-seventh packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The forty-eighth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The forty-ninth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fiftieth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifty-first packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifty-second packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifty-third packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifty-fourth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifty-fifth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifty-sixth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifty-seventh packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifty-eighth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The fifty-ninth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixtieth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixty-first packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixty-second packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixty-third packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixty-fourth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixty-fifth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixty-sixth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixty-seventh packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixty-eighth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The sixty-ninth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventieth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventy-first packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventy-second packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventy-third packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventy-fourth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventy-fifth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventy-sixth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventy-seventh packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventy-eighth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The seventy-ninth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eightieth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighty-first packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighty-second packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighty-third packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighty-fourth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighty-fifth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighty-sixth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighty-seventh packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighty-eighth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The eighty-ninth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninetieth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninety-first packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninety-second packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninety-third packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninety-fourth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninety-fifth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninety-sixth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninety-seventh packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninety-eighth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The ninety-ninth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70. The hundredth packet is a RST packet from 192.168.32.101 to 192.168.32.100 on port 70.

Prendendo sempre in esame la porta 21, notiamo che rispetto all'altra comunicazione, qui manca lo step in cui l'host (Kali) invia il flag ACK per chiudere il three-way handshake. In questo caso, dopo lo step SYN, ACK la comunicazione viene chiusa direttamente dall'host con il flag RST.

tcp.port == 21					
No.	Time	Source	Destination	Protocol	Length Info
5	0.064544328	192.168.32.100	192.168.32.101	TCP	58 60259 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.065083384	192.168.32.101	192.168.32.100	TCP	60 21 → 60259 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
22	0.065125702	192.168.32.100	192.168.32.101	TCP	54 60259 → 21 [RST] Seq=1 Win=0 Len=0

In caso di porta chiusa, anche qui la 70, non c'è differenza rispetto allo switch -sT. Anche qui è il target a chiudere la comunicazione con lo step RST, ACK:

tcp.port == 70					
No.	Time	Source	Destination	Protocol	Length Info
482	0.068470194	192.168.32.100	192.168.32.101	TCP	58 60259 → 70 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
512	0.068591044	192.168.32.101	192.168.32.100	TCP	60 70 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0