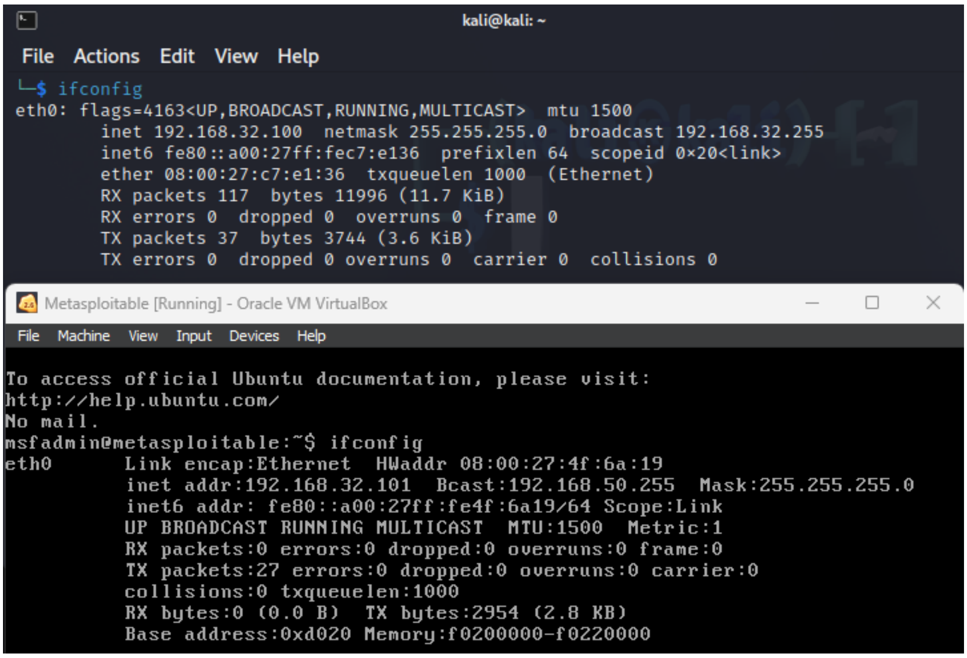
REPORT UNIT 1.3

MODULO 4

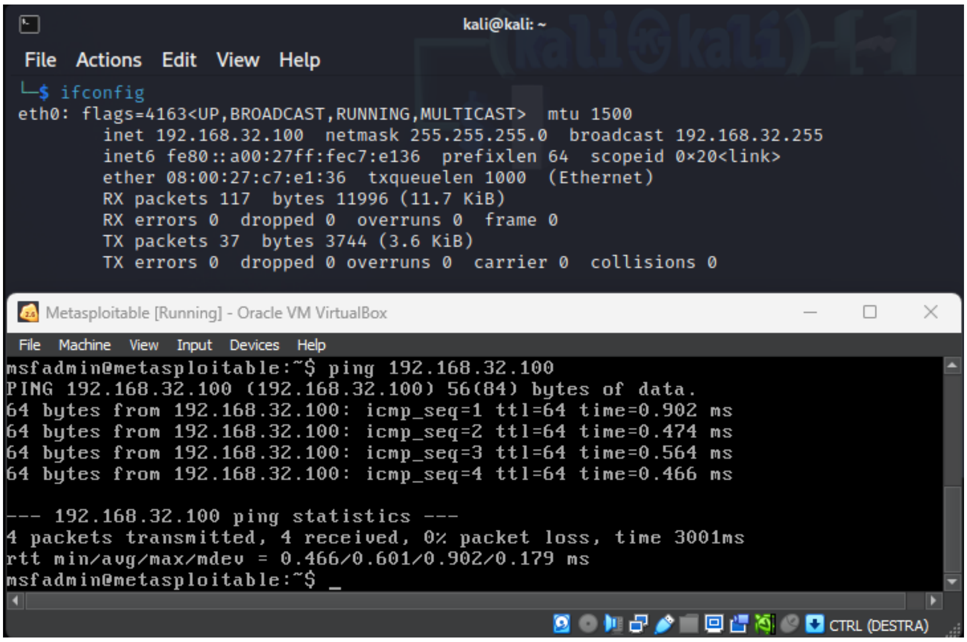
Configuro gli indirizzi IP su entrambe le VM, settandole su rete interna. Controllo che gli indirizzi combacino


kali@kali: ~
File Actions Edit View Help
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.100  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::a00:27ff:fec7:e136  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 117  bytes 11996 (11.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 3744 (3.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4f:6a:19
          inet addr:192.168.32.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4f:6a19/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:2954 (2.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

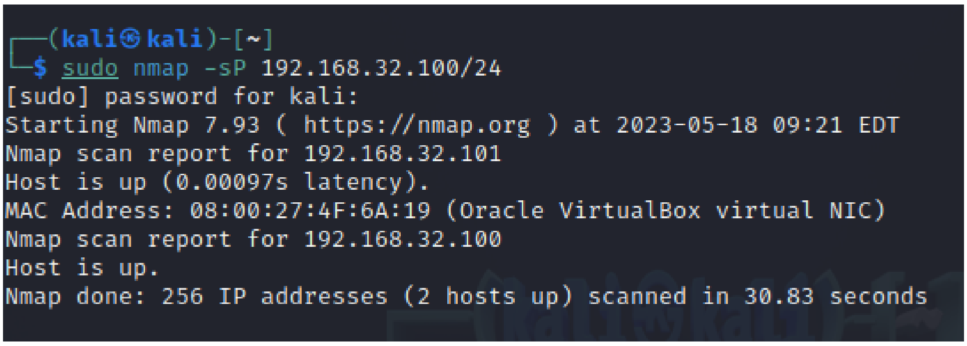
Controllo che le VM siano raggiungibili tra loro


kali@kali: ~
File Actions Edit View Help
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
CTRL (DESTRA)

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.100  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::a00:27ff:fec7:e136  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 117  bytes 11996 (11.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 3744 (3.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

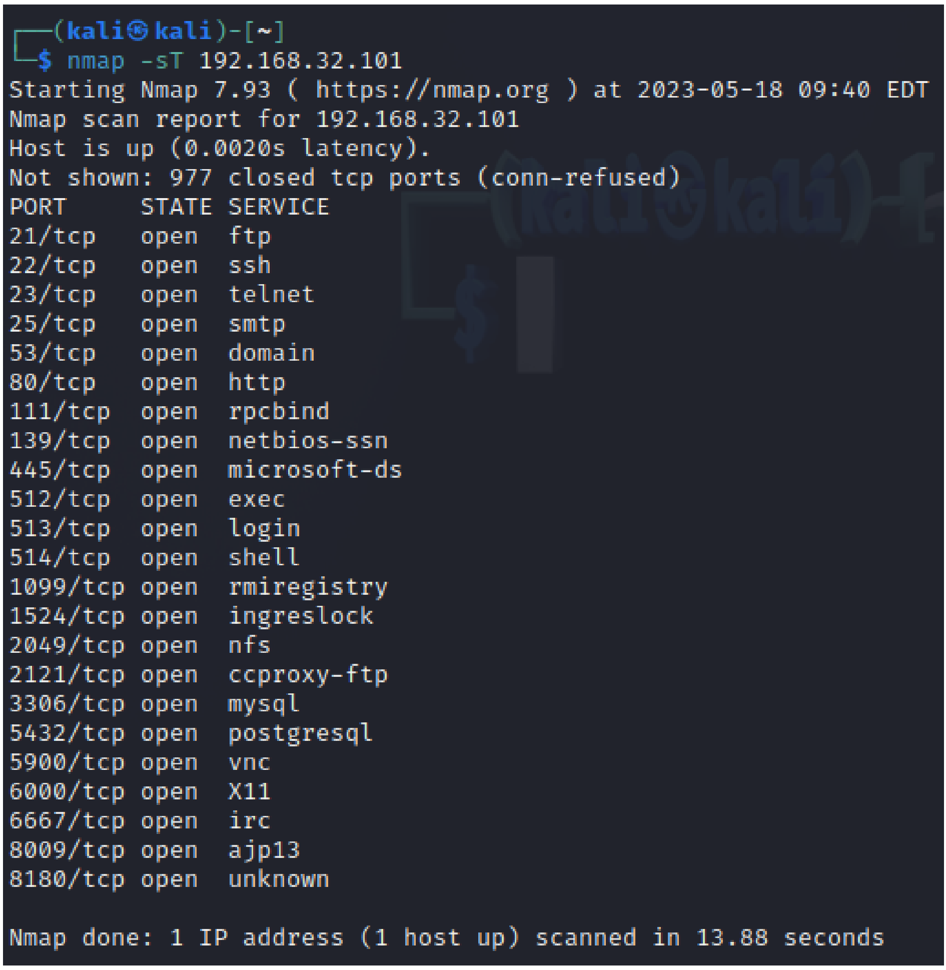
```
msfadmin@metasploitable:~$ ping 192.168.32.100
PING 192.168.32.100 (192.168.32.100) 56(84) bytes of data.
64 bytes from 192.168.32.100: icmp_seq=1 ttl=64 time=0.902 ms
64 bytes from 192.168.32.100: icmp_seq=2 ttl=64 time=0.474 ms
64 bytes from 192.168.32.100: icmp_seq=3 ttl=64 time=0.564 ms
64 bytes from 192.168.32.100: icmp_seq=4 ttl=64 time=0.466 ms

--- 192.168.32.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.466/0.601/0.902/0.179 ms
msfadmin@metasploitable:~$ _
```

Utilizzo il comando nmap –sP, esegue una ricerca rapida della rete di destinazione per vedere quali host sono in linea senza realmente fare una scansione per individuare le porte aperte



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.32.100/24
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:21 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00097s latency).
MAC Address: 08:00:27:4F:6A:19 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.32.100
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 30.83 seconds
```

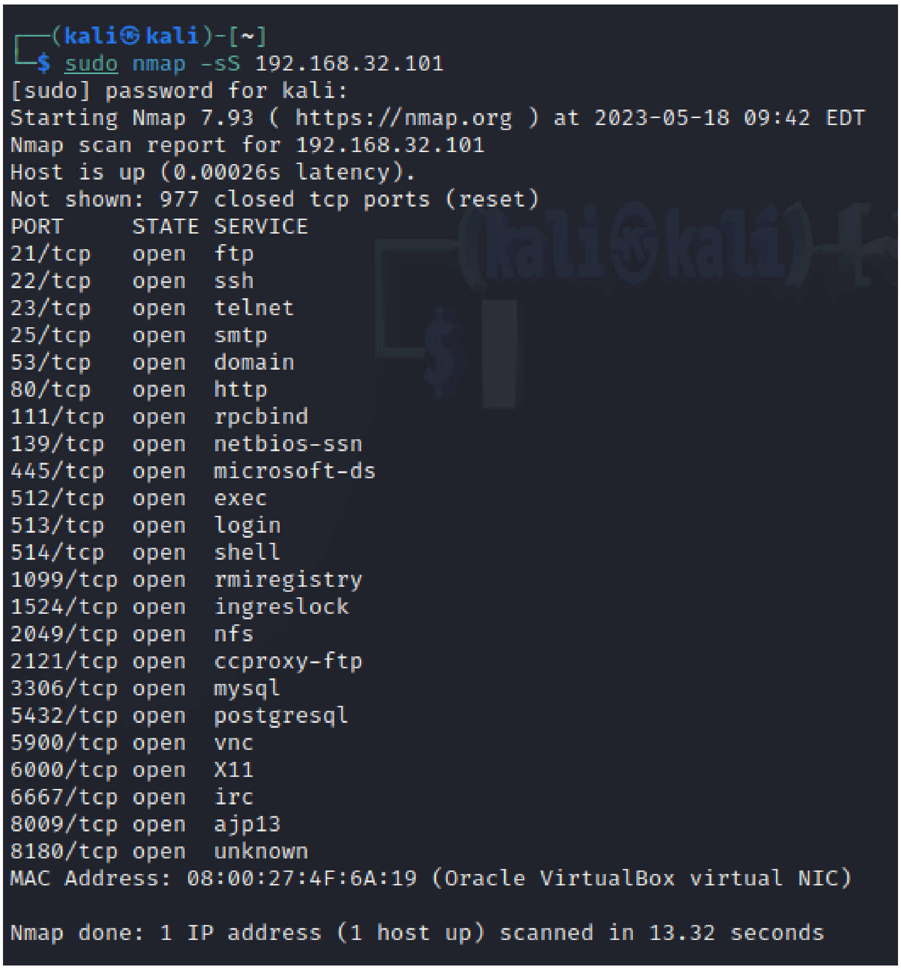
Scansione TCP su VM Meta (nmap –sT)



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.32.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:40 EDT
Nmap scan report for 192.168.32.101
Host is up (0.0020s 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 13.88 seconds
```

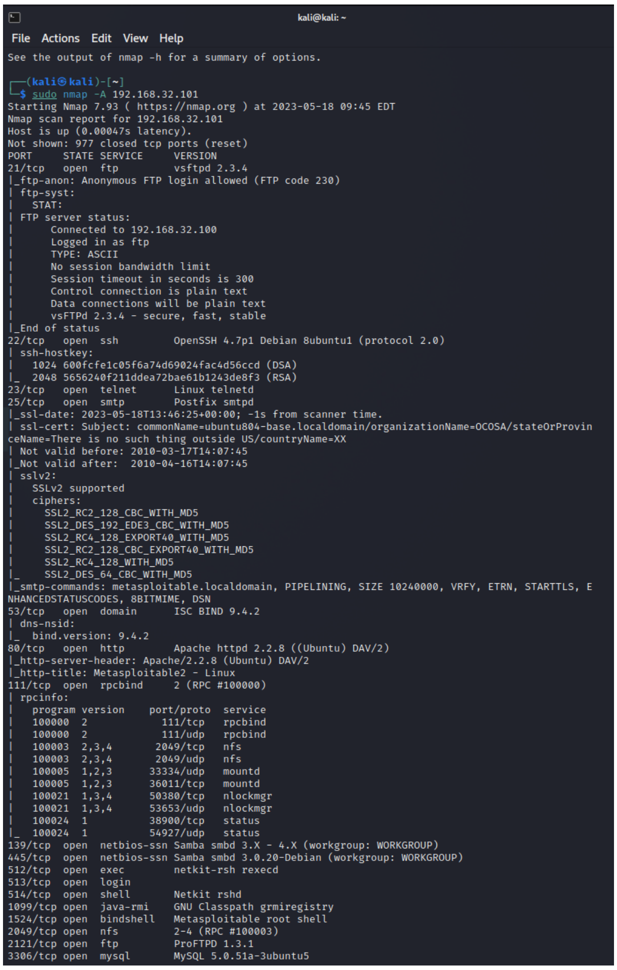
ù

Scansione SYN VM Meta (nmap –sS)

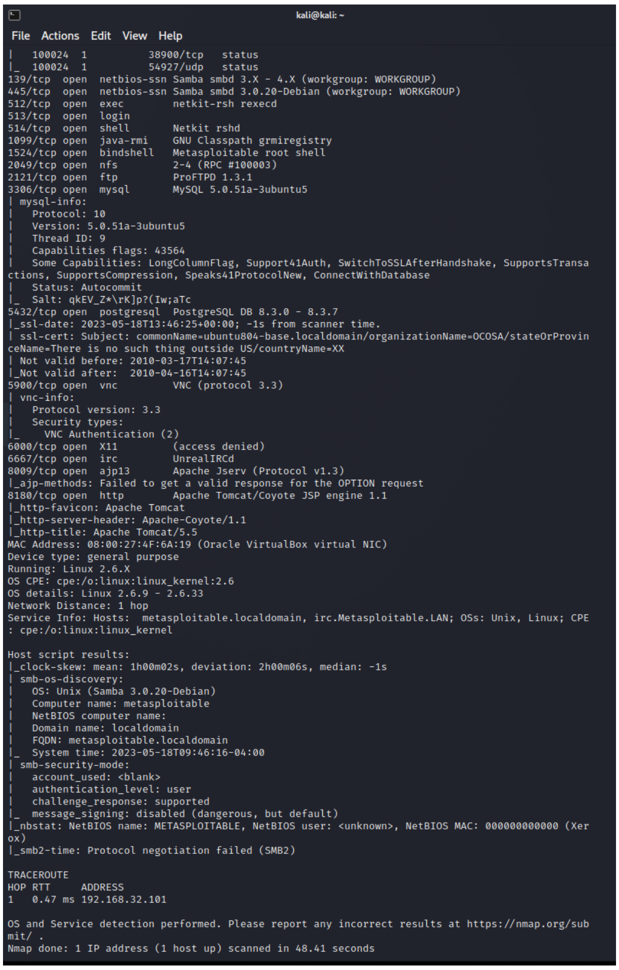


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.32.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:42 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00026s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   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: 08:00:27:4F:6A:19 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
```

Scansione switch a (nmap –A)

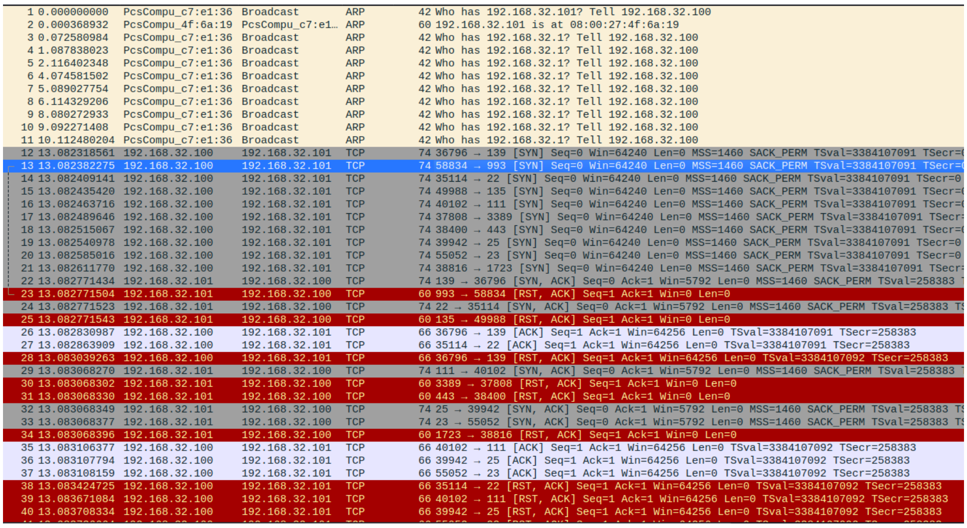


```
See the output of nmap -h for a summary of options.

┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.32.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 09:45 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00047s latency).
Not shown: 977 closed tcp ports (reset)
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
|_ssl-date: 2023-05-18T13:46:25+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvin
ceName=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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, E
NHANCEDSTATUSCODES, 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      33334/udp   mountd
|   100005  1,2,3      36011/tcp   mountd
|   100021  1,3,4      50380/tcp   nlockmgr
|   100021  1,3,4      53653/udp   nlockmgr
|   100024  1          38900/tcp   status
|_  100024  1          54927/udp   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
```

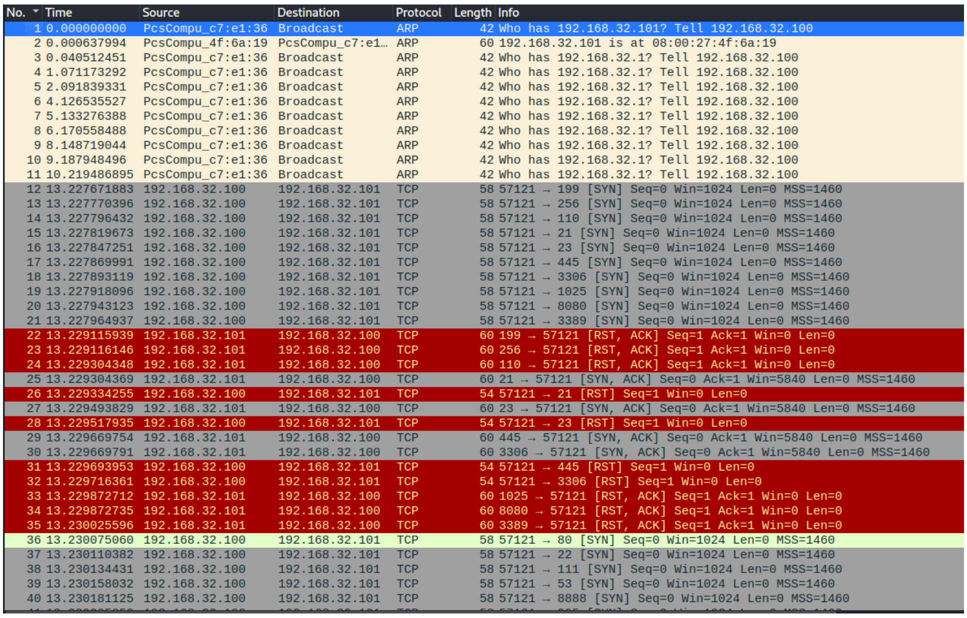


```
|   100024  1          38900/tcp   status
|_  100024  1          54927/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  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: 9
|   Capabilities flags: 43564
|   Some Capabilities: LongColumnFlag, Support41Auth, SwitchToSSLAfterHandshake, SupportsTransa
ctions, SupportsCompression, Speaks41ProtocolNew, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: qkEV_Z*\rK]p?(Iw;aTc
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-05-18T13:46:25+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvin
ceName=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-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:4F:6A:19 (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: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h00m02s, deviation: 2h00m06s, median: -1s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-05-18T09:46:16-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xer
ox)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.47 ms 192.168.32.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.41 seconds
```

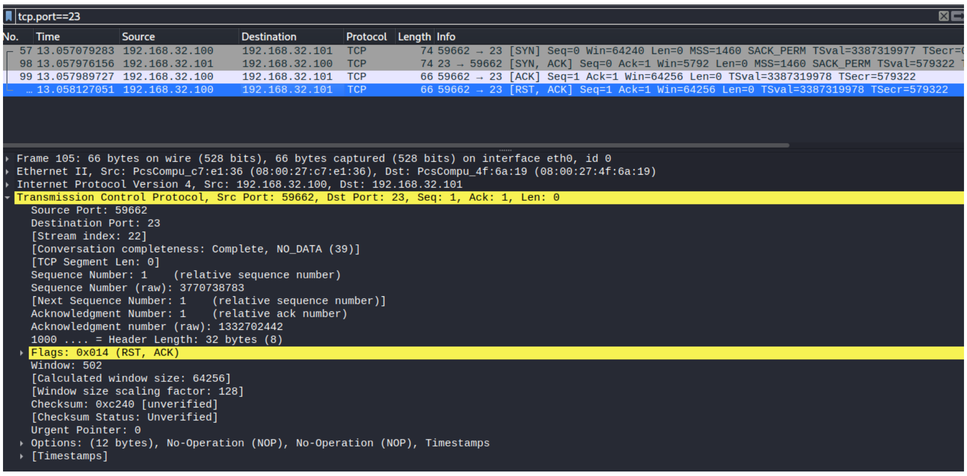
Nmap –sT con Wireshark



```
 1 0.000000000  PcsCompu_c7:e1:36 Broadcast         ARP   42 Who has 192.168.32.101? Tell 192.168.32.100
 2 0.000368932  PcsCompu_4f:6a:19 PcsCompu_c7:e1…   ARP   60 192.168.32.101 is at 08:00:27:4f:6a:19
 3 0.072580984  PcsCompu_c7:e1:36 Broadcast         ARP   42 Who has 192.168.32.1? Tell 192.168.32.100
 4 1.087838023  PcsCompu_c7:e1:36 Broadcast         ARP   42 Who has 192.168.32.1? Tell 192.168.32.100
 5 2.116402348  PcsCompu_c7:e1:36 Broadcast         ARP   42 Who has 192.168.32.1? Tell 192.168.32.100
 6 4.074581502  PcsCompu_c7:e1:36 Broadcast         ARP   42 Who has 192.168.32.1? Tell 192.168.32.100
 7 5.089027754  PcsCompu_c7:e1:36 Broadcast         ARP   42 Who has 192.168.32.1? Tell 192.168.32.100
 8 6.114329206  PcsCompu_c7:e1:36 Broadcast         ARP   42 Who has 192.168.32.1? Tell 192.168.32.100
 9 8.080272933  PcsCompu_c7:e1:36 Broadcast         ARP   42 Who has 192.168.32.1? Tell 192.168.32.100
10 9.092271408  PcsCompu_c7:e1:36 Broadcast         ARP   42 Who has 192.168.32.1? Tell 192.168.32.100
11 10.112480204 PcsCompu_c7:e1:36 Broadcast         ARP   42 Who has 192.168.32.1? Tell 192.168.32.100
12 13.082318561 192.168.32.100    192.168.32.101    TCP   74 36796 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3384107091 TSecr=
13 13.082382275 192.168.32.100    192.168.32.101    TCP   74 58834 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3384107091 TSecr=
14 13.082409141 192.168.32.100    192.168.32.101    TCP   74 35114 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3384107091 TSecr=0
15 13.082435420 192.168.32.100    192.168.32.101    TCP   74 49988 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3384107091 TSecr=
16 13.082463716 192.168.32.100    192.168.32.101    TCP   74 40102 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3384107091 TSecr=
17 13.082489646 192.168.32.100    192.168.32.101    TCP   74 37808 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3384107091 TSecr=
18 13.082515067 192.168.32.100    192.168.32.101    TCP   74 38400 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3384107091 TSecr=
19 13.082540978 192.168.32.100    192.168.32.101    TCP   74 39942 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3384107091 TSecr=0
20 13.082585016 192.168.32.100    192.168.32.101    TCP   74 55052 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3384107091 TSecr=0
21 13.082611770 192.168.32.100    192.168.32.101    TCP   74 38816 → 1723 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3384107091 TSecr=
22 13.082771434 192.168.32.101    192.168.32.100    TCP   74 139 → 36796 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=258383 T
23 13.082771504 192.168.32.101    192.168.32.100    TCP   60 993 → 58834 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 13.082771523 192.168.32.101    192.168.32.100    TCP   74 22 → 35114 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=258383 TS
25 13.082771543 192.168.32.101    192.168.32.100    TCP   60 135 → 49988 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26 13.082830987 192.168.32.100    192.168.32.101    TCP   66 36796 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3384107091 TSecr=258383
27 13.082863909 192.168.32.100    192.168.32.101    TCP   66 35114 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3384107091 TSecr=258383
28 13.083039263 192.168.32.100    192.168.32.101    TCP   66 36796 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3384107092 TSecr=258383
29 13.083068270 192.168.32.101    192.168.32.100    TCP   74 111 → 40102 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=258383 T
30 13.083068302 192.168.32.101    192.168.32.100    TCP   60 3389 → 37808 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31 13.083068330 192.168.32.101    192.168.32.100    TCP   60 443 → 38400 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32 13.083068349 192.168.32.101    192.168.32.100    TCP   74 25 → 39942 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=258383 TS
33 13.083068377 192.168.32.101    192.168.32.100    TCP   74 23 → 55052 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=258383 TS
34 13.083068396 192.168.32.101    192.168.32.100    TCP   60 1723 → 38816 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35 13.083106377 192.168.32.100    192.168.32.101    TCP   66 40102 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3384107092 TSecr=258383
36 13.083107794 192.168.32.100    192.168.32.101    TCP   66 39942 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3384107092 TSecr=258383
37 13.083108159 192.168.32.100    192.168.32.101    TCP   66 55052 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3384107092 TSecr=258383
38 13.083424725 192.168.32.100    192.168.32.101    TCP   66 35114 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3384107092 TSecr=258383
39 13.083671084 192.168.32.100    192.168.32.101    TCP   66 40102 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3384107092 TSecr=258383
40 13.083708334 192.168.32.100    192.168.32.101    TCP   66 39942 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3384107092 TSecr=258383
```

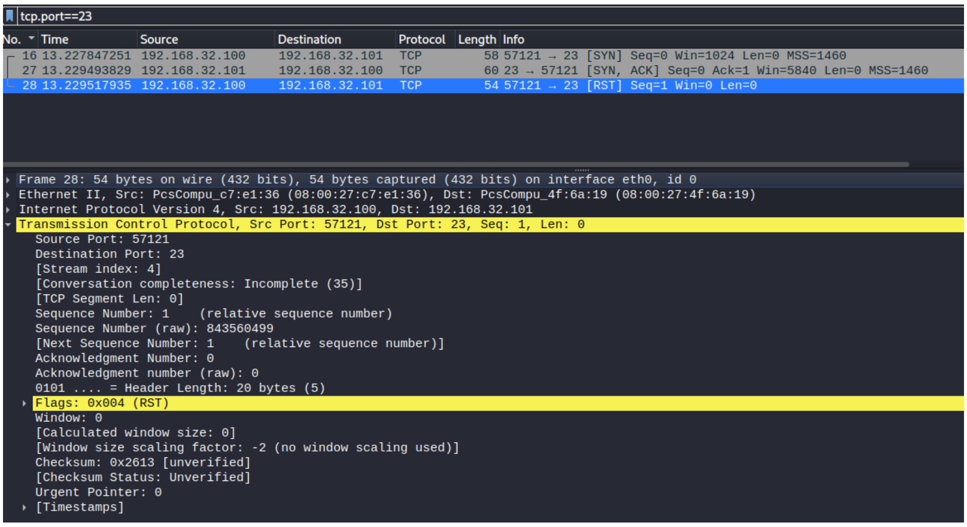


```
No. Time         Source            Destination       Protocol Length Info
  1 0.000000000  PcsCompu_c7:e1:36 Broadcast         ARP      42 Who has 192.168.32.101? Tell 192.168.32.100
  2 0.000637994  PcsCompu_4f:6a:19 PcsCompu_c7:e1…   ARP      60 192.168.32.101 is at 08:00:27:4f:6a:19
  3 0.040512451  PcsCompu_c7:e1:36 Broadcast         ARP      42 Who has 192.168.32.1? Tell 192.168.32.100
  4 1.071173292  PcsCompu_c7:e1:36 Broadcast         ARP      42 Who has 192.168.32.1? Tell 192.168.32.100
  5 2.091839331  PcsCompu_c7:e1:36 Broadcast         ARP      42 Who has 192.168.32.1? Tell 192.168.32.100
  6 4.126535527  PcsCompu_c7:e1:36 Broadcast         ARP      42 Who has 192.168.32.1? Tell 192.168.32.100
  7 5.133276388  PcsCompu_c7:e1:36 Broadcast         ARP      42 Who has 192.168.32.1? Tell 192.168.32.100
  8 6.170558488  PcsCompu_c7:e1:36 Broadcast         ARP      42 Who has 192.168.32.1? Tell 192.168.32.100
  9 8.148719044  PcsCompu_c7:e1:36 Broadcast         ARP      42 Who has 192.168.32.1? Tell 192.168.32.100
 10 9.187948496  PcsCompu_c7:e1:36 Broadcast         ARP      42 Who has 192.168.32.1? Tell 192.168.32.100
 11 10.219486895 PcsCompu_c7:e1:36 Broadcast         ARP      42 Who has 192.168.32.1? Tell 192.168.32.100
 12 13.227671883 192.168.32.100    192.168.32.101    TCP      58 57121 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 13 13.227770396 192.168.32.100    192.168.32.101    TCP      58 57121 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 14 13.227796432 192.168.32.100    192.168.32.101    TCP      58 57121 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 15 13.227819673 192.168.32.100    192.168.32.101    TCP      58 57121 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 16 13.227847251 192.168.32.100    192.168.32.101    TCP      58 57121 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 17 13.227869991 192.168.32.100    192.168.32.101    TCP      58 57121 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 18 13.227893119 192.168.32.100    192.168.32.101    TCP      58 57121 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 19 13.227918096 192.168.32.100    192.168.32.101    TCP      58 57121 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 20 13.227943123 192.168.32.100    192.168.32.101    TCP      58 57121 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 21 13.227964937 192.168.32.100    192.168.32.101    TCP      58 57121 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 22 13.229115939 192.168.32.101    192.168.32.100    TCP      60 199 → 57121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 23 13.229116146 192.168.32.101    192.168.32.100    TCP      60 256 → 57121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 24 13.229304348 192.168.32.101    192.168.32.100    TCP      60 110 → 57121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 25 13.229304369 192.168.32.101    192.168.32.100    TCP      60 21 → 57121 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 26 13.229334255 192.168.32.100    192.168.32.101    TCP      54 57121 → 21 [RST] Seq=1 Win=0 Len=0
 27 13.229493829 192.168.32.101    192.168.32.100    TCP      60 23 → 57121 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 28 13.229517935 192.168.32.100    192.168.32.101    TCP      54 57121 → 23 [RST] Seq=1 Win=0 Len=0
 29 13.229669754 192.168.32.101    192.168.32.100    TCP      60 445 → 57121 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 30 13.229669791 192.168.32.101    192.168.32.100    TCP      60 3306 → 57121 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 31 13.229693953 192.168.32.100    192.168.32.101    TCP      54 57121 → 445 [RST] Seq=1 Win=0 Len=0
 32 13.229716361 192.168.32.100    192.168.32.101    TCP      54 57121 → 3306 [RST] Seq=1 Win=0 Len=0
 33 13.229872712 192.168.32.101    192.168.32.100    TCP      60 1025 → 57121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 34 13.229872735 192.168.32.101    192.168.32.100    TCP      60 8080 → 57121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 35 13.230025596 192.168.32.101    192.168.32.100    TCP      60 3389 → 57121 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 36 13.230075060 192.168.32.100    192.168.32.101    TCP      58 57121 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 37 13.230110382 192.168.32.100    192.168.32.101    TCP      58 57121 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 38 13.230134431 192.168.32.100    192.168.32.101    TCP      58 57121 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 39 13.230158032 192.168.32.100    192.168.32.101    TCP      58 57121 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 40 13.230181125 192.168.32.100    192.168.32.101    TCP      58 57121 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```



```
tcp.port==23

No. Time         Source         Destination    Protocol Length Info
 57 13.057079283 192.168.32.100 192.168.32.101 TCP      74 59662 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3387319977 TSecr=
 98 13.057976156 192.168.32.101 192.168.32.100 TCP      74 23 → 59662 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=579322
 99 13.057989727 192.168.32.100 192.168.32.101 TCP      66 59662 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3387319978 TSecr=579322
  … 13.058127051 192.168.32.100 192.168.32.101 TCP      66 59662 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3387319978 TSecr=579322

› Frame 105: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
› Ethernet II, Src: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36), Dst: PcsCompu_4f:6a:19 (08:00:27:4f:6a:19)
› Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
⌄ Transmission Control Protocol, Src Port: 59662, Dst Port: 23, Seq: 1, Ack: 1, Len: 0
    Source Port: 59662
    Destination Port: 23
    [Stream index: 22]
    [Conversation completeness: Complete, NO_DATA (39)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3770738783
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1332702442
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x014 (RST, ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0xc240 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  › [Timestamps]
```

st



```
tcp.port==23

No. Time         Source         Destination    Protocol Length Info
 16 13.227847251 192.168.32.100 192.168.32.101 TCP      58 57121 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 27 13.229493829 192.168.32.101 192.168.32.100 TCP      60 23 → 57121 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
 28 13.229517935 192.168.32.100 192.168.32.101 TCP      54 57121 → 23 [RST] Seq=1 Win=0 Len=0

› Frame 28: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
› Ethernet II, Src: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36), Dst: PcsCompu_4f:6a:19 (08:00:27:4f:6a:19)
› Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
⌄ Transmission Control Protocol, Src Port: 57121, Dst Port: 23, Seq: 1, Len: 0
    Source Port: 57121
    Destination Port: 23
    [Stream index: 4]
    [Conversation completeness: Incomplete (35)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 843560499
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x004 (RST)
    Window: 0
    [Calculated window size: 0]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x2613 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › [Timestamps]
```

Ss

Prendo la porta telnet aperta e la metto come filtro, nella scansione st si può vedere come il 3way handshake venga completato, mentre nella scansione ss non viene completato ed invia un pacchetto reset rst