

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 well-known.

In evidenza le porte non scansionate nella scansione fast 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 fast su un numero inferiore di porte rispetto allo switch -sT.
Come nel caso dello switch -sT, anche qua viene concluso il three-way handshake.

```
(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, e scansiona tutte le porte well-known come lo switch -sT. In evidenza le porte non scansionate nella scansione fast 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 600fcfc1c05f6a74d69024fac4d56ccd (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

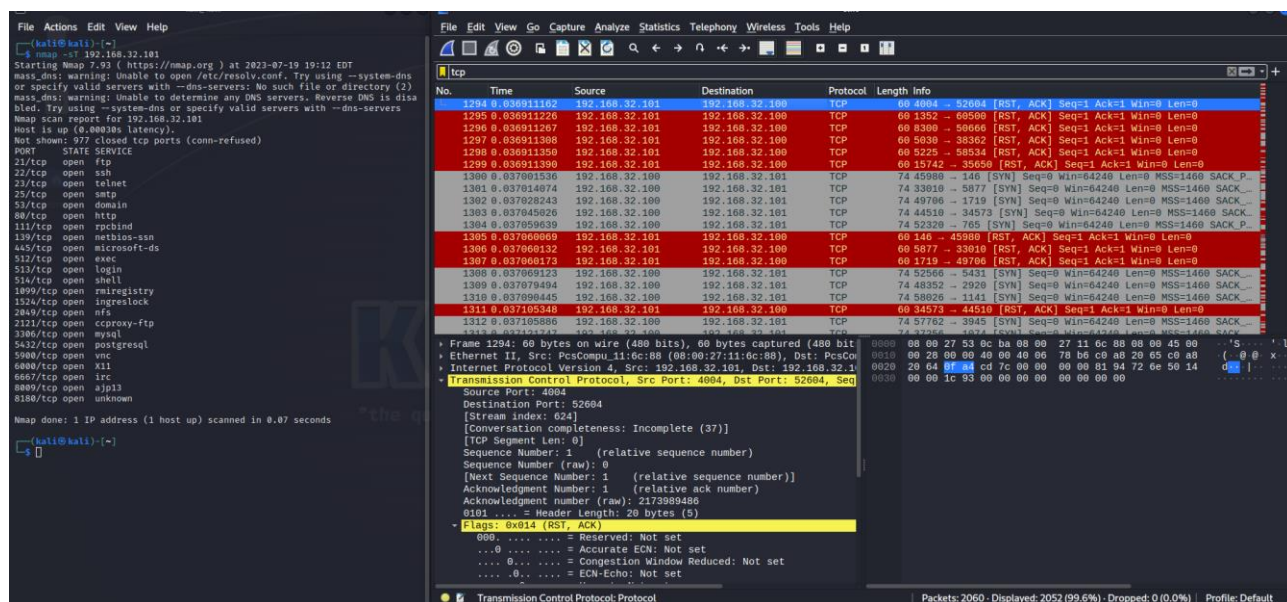
| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

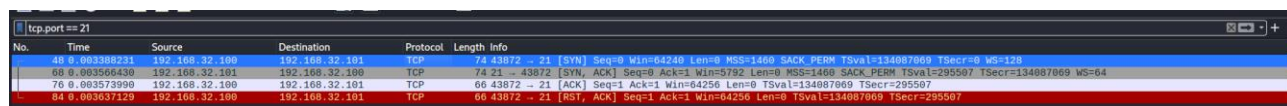
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

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 terminal window shows the following commands and output:

```
kali@kali:~$ nmap -sS 192.168.32.101
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

kali@kali:~$ sudo nmap -sS 192.168.32.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-19 19:46 EDT
nmap_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)
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disa
bled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.32.101
Host is up (0.000097s 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
32/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  raiquery
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3380/tcp  open  mysql
5432/tcp  open  postgresql
5980/tcp  open  vnc
6080/tcp  open  iis
6667/tcp  open  irc
8080/tcp  open  xjpi3
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 0.18 seconds

kali@kali:~$
```

The Wireshark capture shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
1992	0.078454447	192.168.32.101	192.168.32.100	TCP	60	16113 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1993	0.078454513	192.168.32.101	192.168.32.100	TCP	60	84 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1994	0.078454579	192.168.32.101	192.168.32.100	TCP	60	0259 → 5107 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1995	0.078454561	192.168.32.101	192.168.32.100	TCP	60	211 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1996	0.078454605	192.168.32.101	192.168.32.100	TCP	60	44442 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1997	0.078454652	192.168.32.101	192.168.32.100	TCP	60	54645 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1998	0.078454700	192.168.32.101	192.168.32.100	TCP	60	89 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1999	0.078454744	192.168.32.101	192.168.32.100	TCP	60	2843 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2000	0.078454788	192.168.32.101	192.168.32.100	TCP	60	49152 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2001	0.078460186	192.168.32.100	192.168.32.101	TCP	58	60259 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2002	0.078460976	192.168.32.101	192.168.32.100	TCP	60	8080 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2003	0.078471968	192.168.32.101	192.168.32.100	TCP	60	26 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2004	0.078471113	192.168.32.101	192.168.32.100	TCP	60	801 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2005	0.078475963	192.168.32.100	192.168.32.101	TCP	58	60259 → 1580 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2006	0.078505295	192.168.32.100	192.168.32.101	TCP	58	60259 → 60820 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2007	0.078514679	192.168.32.100	192.168.32.101	TCP	58	60259 → 6567 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2008	0.078514664	192.168.32.101	192.168.32.100	TCP	60	2522 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2009	0.078514730	192.168.32.101	192.168.32.100	TCP	60	0 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2010	0.078514763	192.168.32.101	192.168.32.100	TCP	60	5988 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2011	0.078514829	192.168.32.101	192.168.32.100	TCP	60	9877 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2012	0.078514876	192.168.32.101	192.168.32.100	TCP	60	1044 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2013	0.078514925	192.168.32.101	192.168.32.100	TCP	60	6839 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2014	0.078550271	192.168.32.101	192.168.32.100	TCP	58	60259 → 100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2015	0.078550816	192.168.32.101	192.168.32.100	TCP	60	3268 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2016	0.078550876	192.168.32.101	192.168.32.100	TCP	60	6881 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2017	0.078550920	192.168.32.101	192.168.32.100	TCP	60	1066 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2018	0.078550966	192.168.32.101	192.168.32.100	TCP	60	2288 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2019	0.078551008	192.168.32.101	192.168.32.100	TCP	60	1038 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2020	0.078551053	192.168.32.101	192.168.32.100	TCP	60	5862 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2021	0.078551101	192.168.32.101	192.168.32.100	TCP	60	8080 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2022	0.078550804	192.168.32.101	192.168.32.100	TCP	60	1580 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2023	0.078550946	192.168.32.101	192.168.32.100	TCP	60	60820 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2024	0.078550907	192.168.32.101	192.168.32.100	TCP	60	6567 → 60259 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

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