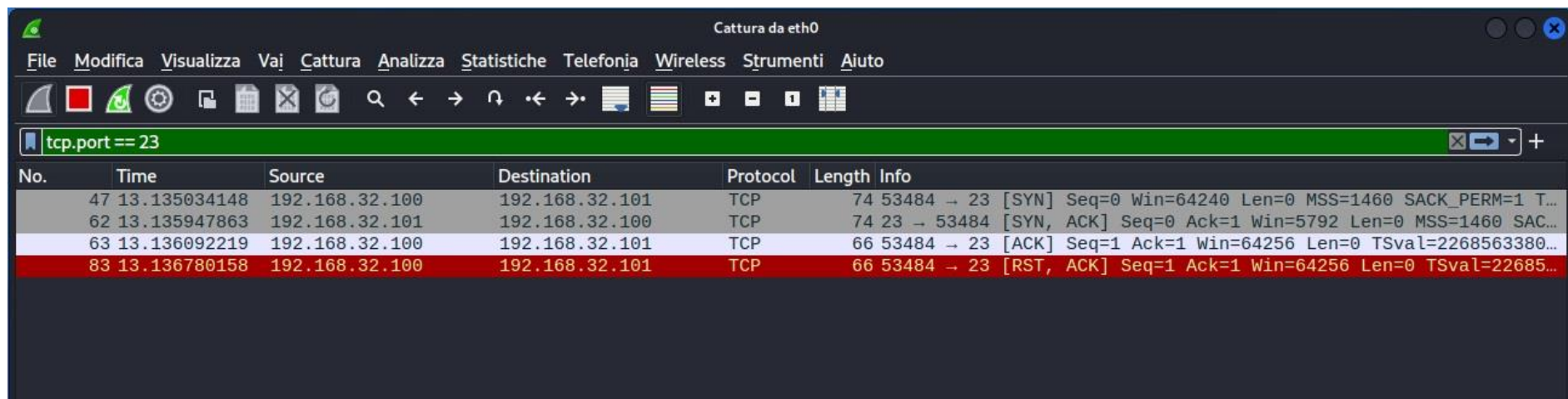


Network scanning e intercettazione richieste

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo nmap -sT 192.168.32.101  
[sudo] password di kali:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 18:43 CET  
Nmap scan report for 192.168.32.101  
Host is up (0.00076s 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  
MAC Address: 08:00:27:EE:87:2A (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds  
  
(kali@kali)-[~]  
$
```

Scansione TCP

Attraverso il port scanner Nmap, si esegue una scansione TCP sulle porte well-know alla VM Metasploitable, con IP: 192.168.32.101, con il comando da terminale: `sudo nmap -sT 192.168.32.101`. TCP scan è un metodo più invasivo rispetto a SYN, in quanto, Nmap, per controllare se una porta è aperta o meno e recuperare informazioni sul servizio in ascolto, conclude il 3-way-handshake (modo in cui TCP lavora per stabilire una connessione composta da tre step), effettuando: un SYN, un SYN/ACK e un ACK, significando solo che la porta è aperta, stabilendo, di fatto, un canale.



Cattura da eth0

File Modifica Visualizza Vaj Cattura Analizza Statistiche Telefonj Wireless Strumenti Aiuto

tcp.port == 23

No.	Time	Source	Destination	Protocol	Length	Info
47	13.135034148	192.168.32.100	192.168.32.101	TCP	74	53484 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
62	13.135947863	192.168.32.101	192.168.32.100	TCP	74	23 → 53484 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC...
63	13.136092219	192.168.32.100	192.168.32.101	TCP	66	53484 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2268563380...
83	13.136780158	192.168.32.100	192.168.32.101	TCP	66	53484 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=22685...

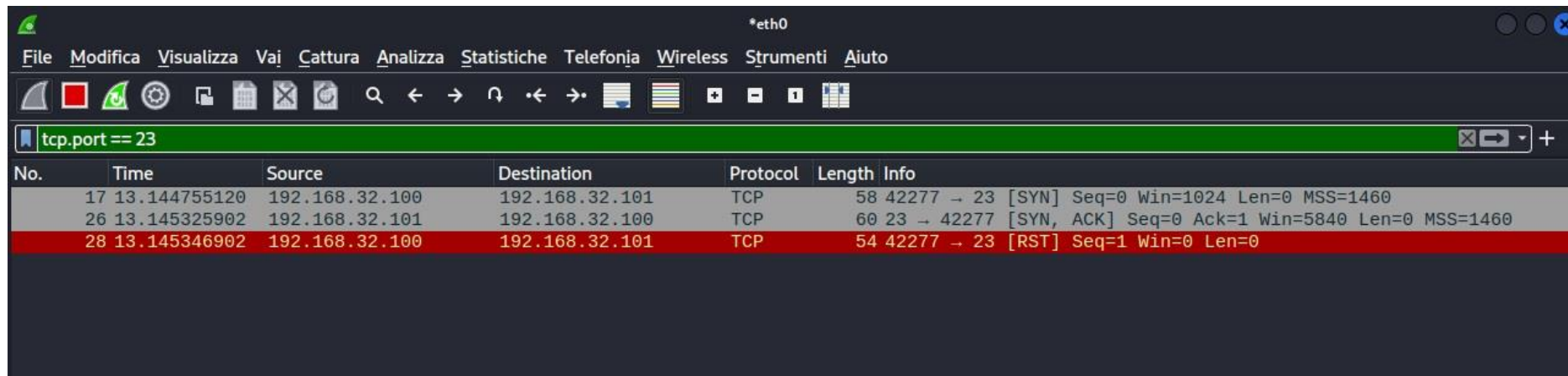
Intercettazione scansione TCP

Attraverso il packet sniffer Wireshark, si intercetta la scansione TCP sulle porte well-know alla VM Metasploitable, con IP: 192.168.32.101, nello specifico sulla Porta 23 del servizio Telnet (protocollo di rete che si basa sullo scambio di dati tramite connessioni TCP), dove si nota, nella sezione Info, che, il 3-way-handshake risulta completo.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo nmap -sS 192.168.32.101  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 16:17 CET  
Nmap scan report for 192.168.32.101  
Host is up (0.00021s 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:EE:87:2A (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.53 seconds  
  
(kali@kali)-[~]  
$
```

Scansione SYN

Attraverso il port scanner Nmap, si esegue una scansione SYN sulle porte well-know alla VM Metasploitable, con IP: 192.168.32.101, con il comando da terminale: `sudo nmap -sS 192.168.32.101`. SYN scan è un metodo meno invasivo rispetto a TCP, in quanto, Nmap, una volta ricevuto il pacchetto dalla macchina target, non conclude il 3-way-handshake, effettuando solo: un SYN e un SYN/ACK, appurando solo che la porta è aperta e chiude la comunicazione, evitando overload dato dalla creazione del canale.



*eth0

File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto

tcp.port == 23

No.	Time	Source	Destination	Protocol	Length	Info
17	13.144755120	192.168.32.100	192.168.32.101	TCP	58	42277 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	13.145325902	192.168.32.101	192.168.32.100	TCP	60	23 → 42277 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
28	13.145346902	192.168.32.100	192.168.32.101	TCP	54	42277 → 23 [RST] Seq=1 Win=0 Len=0

Intercettazione scansione SYN

Attraverso il packet sniffer Wireshark, si intercetta la scansione SYN sulle porte well-know alla VM Metasploitable, con IP: 192.168.32.101, nello specifico sulla Porta 23 del servizio Telnet, dove si nota, nella sezione Info, che, il 3-way-handshake risulta incompleto.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo nmap -A 192.168.32.101  
[sudo] password di kali:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-10 19:17 CET  
Nmap scan report for 192.168.32.101  
Host is up (0.00067s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
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: 1h40m07s, deviation: 2h53m19s, median: 2s  
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <  
unknown> (unknown)  
|_smb2-time: Protocol negotiation failed (SMB2)  
|_smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_smb-os-discovery:  
|   OS: Unix (Samba 3.0.20-Debian)  
|   Computer name: metasploitable  
|   NetBIOS computer name:  
|   Domain name: localdomain  
|   FQDN: metasploitable.localdomain  
|_ System time: 2022-11-10T13:18:49-05:00
```

Scansione con switch -A

Attraverso il port scanner Nmap, si esegue una scansione con switch -A sulle porte well-know alla VM Metasploitable, con IP: 192.168.32.101, con il comando da terminale: `sudo nmap -A 192.168.32.101`. La scansione con switch -A, risulta essere un metodo più invasivo rispetto a TCP, in quanto, Nmap, rivela tra molti dati: sistema operativo e versione, host script.

*eth0						
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonja Wireless Strumenti Aiuto						
tcp.port == 23						
No.	Time	Source	Destination	Protocol	Length	Info
55	6.998130253	192.168.32.100	192.168.32.101	TCP	58	38384 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
70	6.998672483	192.168.32.101	192.168.32.100	TCP	60	23 → 38384 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
75	6.998724927	192.168.32.100	192.168.32.101	TCP	54	38384 → 23 [RST] Seq=1 Win=0 Len=0
2030	7.480546729	192.168.32.100	192.168.32.101	TCP	74	57452 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
2038	7.480928390	192.168.32.101	192.168.32.100	TCP	74	23 → 57452 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC...
2041	7.480986164	192.168.32.100	192.168.32.101	TCP	66	57452 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2269609533...
2131	13.490675475	192.168.32.100	192.168.32.101	TELNET	70	Telnet Data ...
2145	13.491335024	192.168.32.101	192.168.32.100	TCP	66	23 → 57452 [ACK] Seq=1 Ack=5 Win=5824 Len=0 TSval=1183606 TSe...
2265	17.495253665	192.168.32.101	192.168.32.100	TELNET	78	Telnet Data ...
2266	17.495298231	192.168.32.100	192.168.32.101	TCP	66	57452 → 23 [ACK] Seq=5 Ack=13 Win=64256 Len=0 TSval=226961954...
2267	17.496407291	192.168.32.100	192.168.32.101	TCP	66	57452 → 23 [FIN, ACK] Seq=5 Ack=13 Win=64256 Len=0 TSval=2269...
2268	17.497248781	192.168.32.101	192.168.32.100	TCP	66	23 → 57452 [FIN, ACK] Seq=13 Ack=6 Win=5824 Len=0 TSval=11840...
2269	17.497274286	192.168.32.100	192.168.32.101	TCP	66	57452 → 23 [ACK] Seq=6 Ack=14 Win=64256 Len=0 TSval=226961954...
3448	59.491094360	192.168.32.100	192.168.32.101	TCP	74	45476 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
3451	59.491506868	192.168.32.101	192.168.32.100	TCP	74	23 → 45476 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC...
3452	59.491527609	192.168.32.100	192.168.32.101	TCP	66	45476 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2269661543...
3990	66.607571540	192.168.32.100	192.168.32.101	TELNET	115	Telnet Data ...
3991	66.608319708	192.168.32.101	192.168.32.100	TCP	66	23 → 45476 [ACK] Seq=1 Ack=50 Win=5824 Len=0 TSval=1188920 TS...
4029	69.487410150	192.168.32.101	192.168.32.100	TELNET	78	Telnet Data ...
4030	69.487454446	192.168.32.100	192.168.32.101	TCP	66	45476 → 23 [ACK] Seq=50 Ack=13 Win=64256 Len=0 TSval=22696715...
4033	69.568195008	192.168.32.100	192.168.32.101	TCP	66	45476 → 23 [FIN, ACK] Seq=50 Ack=13 Win=64256 Len=0 TSval=226...
4034	69.569305000	192.168.32.101	192.168.32.100	TCP	66	23 → 45476 [FIN, ACK] Seq=13 Ack=51 Win=5824 Len=0 TSval=1189...
4035	69.569339886	192.168.32.100	192.168.32.101	TCP	66	45476 → 23 [ACK] Seq=51 Ack=14 Win=64256 Len=0 TSval=22696716...

Intercettazione scansione -A

Attraverso il packet sniffer Wireshark, si intercetta la scansione con switch -A sulle porte well-know alla VM Metasploitable, con IP: 192.168.32.101, nello specifico sulla Porta 23 del servizio Telnet, dove si nota, nella sezione Info, che, il 3-way-handshake risulta completo.

Font Scan	Target Scan	Type Scan
192.168.32.100	192.168.32.101	sT
192.168.32.100	192.168.32.101	sS
192.168.32.100	192.168.32.101	-A

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

Report