Fonte	Target	Tipo di scan	Servizi attivi
192.168.50.100	192.169.50.101	TCP	**PORT SERVICE** 21/tcp ftp 22/tcp ssh 23/tcp telnet 25/tcp smtp 53/tcp domain 80/tcp http 111/tcp rpcbind 139/tcp netbios-ssn 445/tcp microsoft-ds 512/tcp exec 513/tcp login 514/tcp shell 1099/tcp rmiregistry 1524/tcp ingreslock 2049/tcp nfs 2121/tcp ccproxy-ftp 3306/tcp mysql 5432/tcp postgresql 5900/tcp vnc 6000/tcp X11 6667/tcp irc 8009/tcp ajp13 8180/tcp unknown
Comando:	nmap -sT 192.168.50.101		
192.168.50.100	192.169.50.101	SYN	**PORT SERVICE** 21/tcp ftp 22/tcp ssh 23/tcp telnet 25/tcp smtp 53/tcp domain 80/tcp http 111/tcp rpcbind 139/tcp netbios-ssn 445/tcp microsoft-ds 512/tcp exec 513/tcp login 514/tcp shell

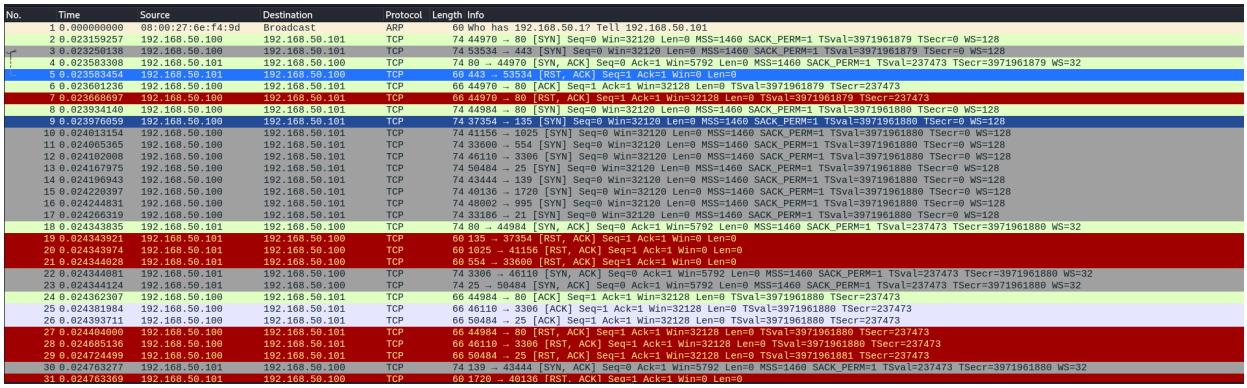
			1099/tcp rmiregistry 1524/tcp ingreslock 2049/tcp nfs 2121/tcp ccproxy-ftp 3306/tcp mysql 5432/tcp postgresql 5900/tcp vnc 6000/tcp X11 6667/tcp irc 8009/tcp ajp13 8180/tcp unknown
Comando:	sudo nmap -sS 192.168.50.101		
192.168.50.100	192.169.50.101	switch -A	**PORT SERVICE VERSION** 21/tcp ftp vsftpd 2.3.4 22/tcp ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) 23/tcp telnet? 25/tcp smtp? 53/tcp domain ISC BIND 9.4.2 80/tcp http Apache httpd 2.2.8 ((Ubuntu) DAV/2) 111/tcp rpcbind 2 (RPC #100000) 139/tcp netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 445/tcp netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP) 512/tcp exec? 513/tcp login? 514/tcp shell? 1099/tcp java-rmi GNU Classpath grmiregistry 1524/tcp bindshell Metasploitable root shell 2049/tcp nfs 2-4 (RPC #100003) 2121/tcp ccproxy-ftp? 3306/tcp mysql? 5432/tcp postgresql PostgreSQL DB 8.3.0 - 8.3.7 5900/tcp vnc VNC (protocol 3.3) 6000/tcp X11 6667/tcp irc UnrealIRCd 8009/tcp ajp13 Apache Jserv (Protocol v1.3) 8180/tcp http Apache Tomcat/Coyote JSP engine 1.1
Comando:	nmap 192.168.50.101 -A		

Wireshark - scansione completa TCP

Comando nmap -sT 192.168.50.101

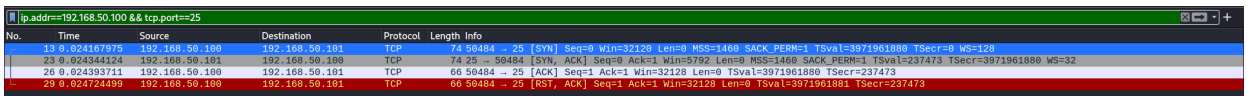
Lo screen di Wireshark per la scansione completa TCP mostra che Nmapinvia pacchetti TCP con la SYN flag attiva a varie porte (80, 443, etc.). Le porte chiuse rispondono con le flag RST e ACK attive, come mostrato ad esempio dalla riga 19 alla 21. Lo stesso viene ripetuto per tutte le porte chiuse.

Alla riga 23 notiamo che la porta 25 ad esempio è aperta, quindi risponde all'iniziale SYN con un SYN-ACK. Alla riga 26 il three-way-handshake si completa con un ACK finale.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	08:00:27:6e:f4:9d	Broadcast	ARP	60	Who has 192.168.50.1? Tell 192.168.50.101
2	0.023159257	192.168.50.100	192.168.50.101	TCP	74	44970 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961879 TSecr=0 WS=128
3	0.023250138	192.168.50.100	192.168.50.101	TCP	74	53534 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961879 TSecr=0 WS=128
4	0.023583308	192.168.50.101	192.168.50.100	TCP	74	80 → 44970 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=237473 TSecr=3971961879 WS=32
5	0.023583454	192.168.50.101	192.168.50.100	TCP	60	443 → 53534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	0.023601236	192.168.50.100	192.168.50.101	TCP	66	44970 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3971961879 TSecr=237473
7	0.023668697	192.168.50.100	192.168.50.101	TCP	66	44970 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3971961879 TSecr=237473
8	0.023934140	192.168.50.100	192.168.50.101	TCP	74	44984 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
9	0.023976059	192.168.50.100	192.168.50.101	TCP	74	37354 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
10	0.024013154	192.168.50.100	192.168.50.101	TCP	74	41156 → 1025 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
11	0.024065365	192.168.50.100	192.168.50.101	TCP	74	33600 → 554 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
12	0.024102008	192.168.50.100	192.168.50.101	TCP	74	46110 → 3306 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
13	0.024167975	192.168.50.100	192.168.50.101	TCP	74	50484 → 25 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
14	0.024196943	192.168.50.100	192.168.50.101	TCP	74	43444 → 139 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
15	0.024220397	192.168.50.100	192.168.50.101	TCP	74	40136 → 1720 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
16	0.024244831	192.168.50.100	192.168.50.101	TCP	74	48002 → 995 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
17	0.024266319	192.168.50.100	192.168.50.101	TCP	74	33186 → 21 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
18	0.024343835	192.168.50.101	192.168.50.100	TCP	74	80 → 44984 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=237473 TSecr=3971961880 WS=32
19	0.024343921	192.168.50.101	192.168.50.100	TCP	60	135 → 37354 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	0.024343974	192.168.50.101	192.168.50.100	TCP	60	1025 → 41156 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	0.024344028	192.168.50.101	192.168.50.100	TCP	60	554 → 33600 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	0.024344081	192.168.50.101	192.168.50.100	TCP	74	3306 → 46110 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=237473 TSecr=3971961880 WS=32
23	0.024344124	192.168.50.101	192.168.50.100	TCP	74	25 → 50484 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=237473 TSecr=3971961880 WS=32
24	0.024362307	192.168.50.100	192.168.50.101	TCP	66	44984 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3971961880 TSecr=237473
25	0.024381984	192.168.50.100	192.168.50.101	TCP	66	46110 → 3306 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3971961880 TSecr=237473
26	0.024393711	192.168.50.100	192.168.50.101	TCP	66	50484 → 25 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3971961880 TSecr=237473
27	0.024404000	192.168.50.100	192.168.50.101	TCP	66	44984 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3971961880 TSecr=237473
28	0.024685136	192.168.50.100	192.168.50.101	TCP	66	46110 → 3306 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3971961880 TSecr=237473
29	0.024724499	192.168.50.100	192.168.50.101	TCP	66	50484 → 25 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3971961881 TSecr=237473
30	0.024763277	192.168.50.101	192.168.50.100	TCP	74	139 → 43444 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=237473 TSecr=3971961880 WS=32
31	0.024763369	192.168.50.101	192.168.50.100	TCP	60	1720 → 40136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Lo screenshot di seguito mostra tutti i pacchetti inviati da nmap sulla macchina sorgente alla porta 25 della macchina target. I primi tre pacchetti mostrano la stretta di mano in tre fasi, mentre l'ultimo mostra le flag RST/ACK che denotano il reset della connessione.



ip.addr==192.168.50.100 && tcp.port==25

No.	Time	Source	Destination	Protocol	Length	Info
13	0.024167975	192.168.50.100	192.168.50.101	TCP	74	50484 → 25 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM=1 TSval=3971961880 TSecr=0 WS=128
23	0.024344124	192.168.50.101	192.168.50.100	TCP	74	25 → 50484 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=237473 TSecr=3971961880 WS=32
26	0.024393711	192.168.50.100	192.168.50.101	TCP	66	50484 → 25 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3971961880 TSecr=237473
29	0.024724499	192.168.50.100	192.168.50.101	TCP	66	50484 → 25 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3971961881 TSecr=237473

Wireshark - scansione SYN

Comando sudo nmap -sS 192.168.50.101

Impostando come filtro la stessa porta analizzata in dettaglio sopra per il TCP scan, possiamo osservare la differenza principale tra i due. Mentre nello screen di Wireshark sopra osserviamo che si completa il three-way-handshake prima di resettare la connessione, nel SYNscan vediamo che manca la ACK finale dopo la SYN/ACK.