

ESERCIZIO FACOLTATIVO M3 W9D1

SCANSIONE SYN

```
(kali@kali)-[~]
$ nmap -sT -p 21 192.168.32.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 09:09 EST
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 (0.0023s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:83:88:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Questa sezione documenta l’esecuzione di una scansione SYN diretta verso la porta 21 della macchina di destinazione. L’analisi ha lo scopo di verificare in modo mirato la risposta del servizio FTP senza instaurare una connessione completa. La procedura prevede l’invio di un pacchetto iniziale SYN e la valutazione del comportamento successivo del sistema remoto, al fine di confermare l’effettiva apertura della porta monitorata.

tcp											
No.	Time	Source	Destination	Protocol	Length	Info		src MAC	dst MAC		
30	197.938463547	192.168.32.100	192.168.32.101	TCP	74	36710 -> 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1926256608 TSecr=0 W...		PCSSystemtec_1f:b7:23	PCSSystemtec_83:88:d0		
33	197.947029086	192.168.32.101	192.168.32.100	TCP	74	23 -> 36710 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=5695 TSecr...		PCSSystemtec_83:88:d0	PCSSystemtec_1f:b7:23		
34	197.947053684	192.168.32.100	192.168.32.101	TCP	66	36710 -> 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1926256617 TSecr=5695		PCSSystemtec_1f:b7:23	PCSSystemtec_83:88:d0		
35	197.947508662	192.168.32.100	192.168.32.101	TCP	66	36710 -> 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1926256617 TSecr=5695		PCSSystemtec_1f:b7:23	PCSSystemtec_83:88:d0		

La cattura del traffico mostra il classico scambio ridotto tipico di una scansione SYN, evidenziando la ricezione del pacchetto SYN/ACK da parte del server, seguita dall’invio del pacchetto RST da parte della macchina sorgente. Questa dinamica conferma sia la disponibilità del servizio in ascolto, sia la natura non intrusiva della metodologia utilizzata, che permette di ottenere informazioni senza completare il processo di connessione.

CONNESSIONE TCP

```
(kali@kali)-[~]
$ nmap -ss -p 21 192.168.32.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 09:10 EST
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 (0.0017s latency).

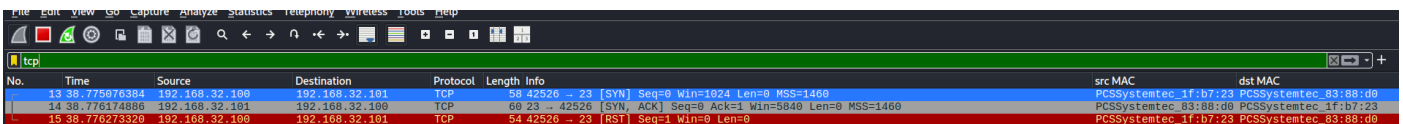
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:83:88:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

(kali@kali)-[~]
$
```

La procedura mostra il comportamento della porta 21 del sistema di destinazione quando viene effettuata una scansione TCP SYN verso l'host 192.168.32.101.

Nmap segnala la porta come **open**, indicando che il servizio FTP accetta la connessione sulla porta 21.



The image shows a Wireshark packet capture of a TCP connection. The packet list on the left shows three packets: a SYN packet (No. 13), a SYN/ACK packet (No. 14), and a RST packet (No. 15). The packet details pane on the right shows the selected packet (No. 14) with its TCP header fields: Seq=0, Win=5840, Len=0, MSS=1460. The packet bytes pane on the right shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info	src MAC	dst MAC
13	38.775976384	192.168.32.100	192.168.32.101	TCP	58	42526 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	PCSSystemtec_1f:b7:23	PCSSystemtec_83:88:d0
14	38.776174886	192.168.32.101	192.168.32.100	TCP	60	23 → 42526 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460	PCSSystemtec_83:88:d0	PCSSystemtec_1f:b7:23
15	38.776273320	192.168.32.100	192.168.32.101	TCP	54	42526 → 23 [RST] Seq=1 Win=0 Len=0	PCSSystemtec_1f:b7:23	PCSSystemtec_83:88:d0

La cattura in Wireshark conferma che il sistema sorgente invia il pacchetto **SYN**, la destinazione risponde con **SYN/ACK**, e il client completa la sequenza con **ACK**.

L'analisi congiunta di Nmap e Wireshark consente quindi di verificare in modo chiaro che la porta 21 è attiva e che la comunicazione TCP avviene correttamente fino alla chiusura volontaria del client.