



Emanuele Di Stefano

S9-L3



Passaggi eseguiti nel terminale:

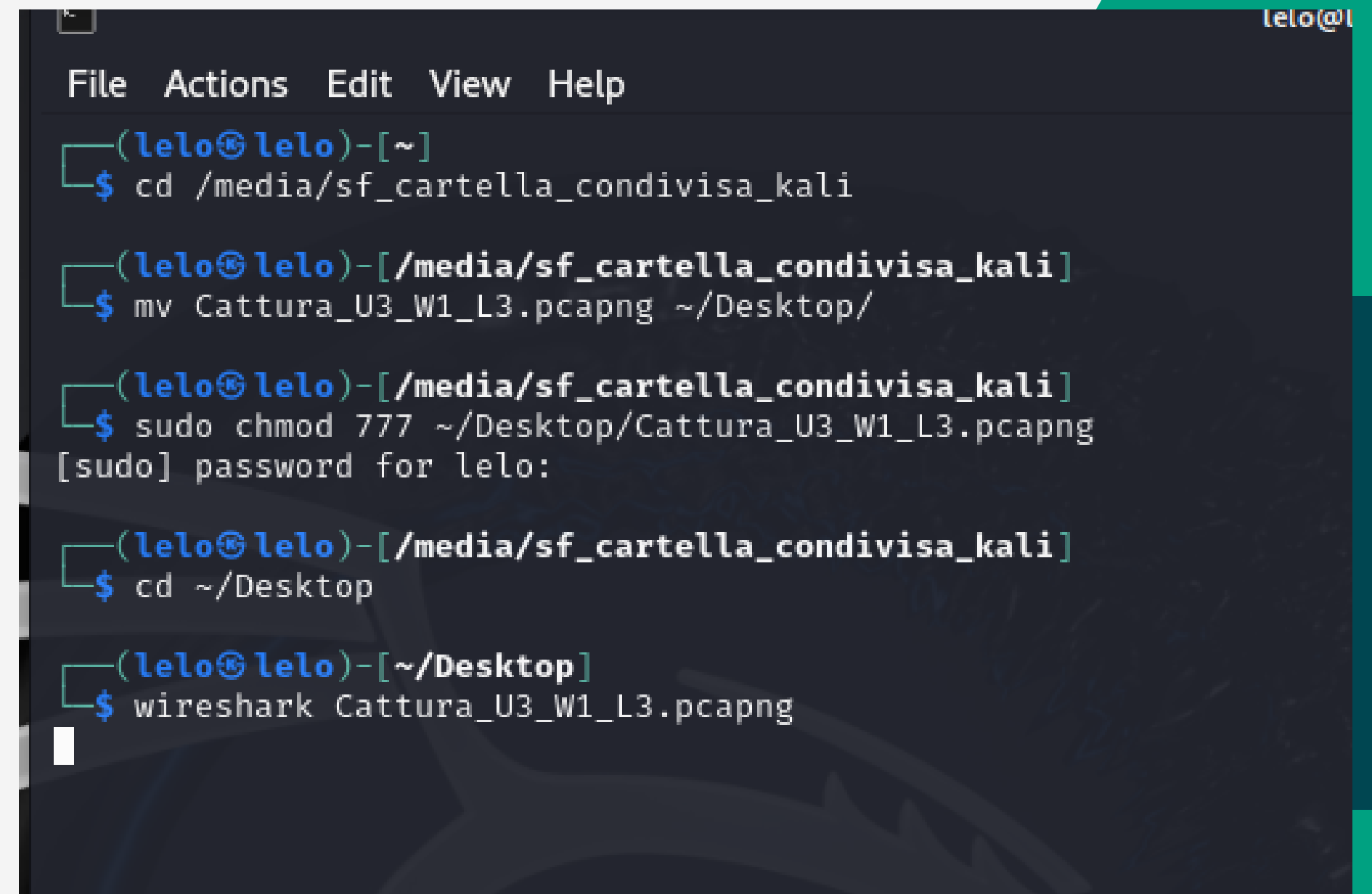
-Ho cambiato la directory di lavoro nel terminale per accedere alla cartella condivisa tra il tuo host e Kali Linux.

-Ho spostato il file di cattura Cattura_U3_W1_L3.pcapng dalla cartella condivisa alla directory Desktop del tuo utente in Kali Linux.

-Ho modificato i permessi del file Cattura_U3_W1_L3.pcapng per assicurarti di avere i permessi necessari per aprirlo e modificarlo.

-Ho cambiato la directory di lavoro nel terminale per accedere al tuo Desktop, dove hai spostato il file di cattura.

-Ho avviato Wireshark e aperto il file di cattura Cattura_U3_W1_L3.pcapng per analizzarlo.

A screenshot of a terminal window with a dark background. The window title is 'lelo@l'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the following commands and their outputs:
1. Prompt: (lelo@lelo)-[~]
Command: \$ cd /media/sf_cartella_condivisa_kali
2. Prompt: (lelo@lelo)-[/media/sf_cartella_condivisa_kali]
Command: \$ mv Cattura_U3_W1_L3.pcapng ~/Desktop/
3. Prompt: (lelo@lelo)-[/media/sf_cartella_condivisa_kali]
Command: \$ sudo chmod 777 ~/Desktop/Cattura_U3_W1_L3.pcapng
Output: [sudo] password for lelo:
4. Prompt: (lelo@lelo)-[/media/sf_cartella_condivisa_kali]
Command: \$ cd ~/Desktop
5. Prompt: (lelo@lelo)-[~/Desktop]
Command: \$ wireshark Cattura_U3_W1_L3.pcapng
The cursor is at the end of the last command.

```
(lelo@lelo)-[~]  
$ cd /media/sf_cartella_condivisa_kali  
  
(lelo@lelo)-[/media/sf_cartella_condivisa_kali]  
$ mv Cattura_U3_W1_L3.pcapng ~/Desktop/  
  
(lelo@lelo)-[/media/sf_cartella_condivisa_kali]  
$ sudo chmod 777 ~/Desktop/Cattura_U3_W1_L3.pcapng  
[sudo] password for lelo:  
  
(lelo@lelo)-[/media/sf_cartella_condivisa_kali]  
$ cd ~/Desktop  
  
(lelo@lelo)-[~/Desktop]  
$ wireshark Cattura_U3_W1_L3.pcapng
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
tcp.flags.syn == 1 && tcp.flags.ack == 1									
No.	Time	Source	Destination	Protocol	Length	Info			
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64	
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64	
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64	
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64	
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64	
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64	
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33042	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64	
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64	
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64	
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535440 WS=64	
164	36.781487210	192.168.200.150	192.168.200.100	TCP	74	512 → 45648	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535445 WS=64	
267	36.788805940	192.168.200.150	192.168.200.100	TCP	74	514 → 51396	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952467 TSecr=810535452 WS=64	
994	36.825722553	192.168.200.150	192.168.200.100	TCP	74	513 → 42048	[SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952471 TSecr=810535489 WS=64	

Questo filtro mostra solo i pacchetti TCP che hanno entrambi i flag SYN e ACK impostati. Nello screenshot, vediamo vari pacchetti che soddisfano questo criterio, indicando connessioni che sono state richieste e riconosciute.

No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165

Questo filtro isola il primo stream TCP nel file di cattura, permettendo di analizzare l'intera conversazione tra due endpoint specifici. Lo screenshot mostra la sequenza di pacchetti per questo stream, inclusi SYN, SYN-ACK, ACK e RST.

Interpretazione dei dati

Pacchetti SYN-ACK: Sono presenti numerosi pacchetti SYN-ACK, che indicano richieste di connessione riconosciute. Questo è normale per le connessioni iniziate.

Pacchetti RST: Alcuni pacchetti contengono il flag RST (Reset), che interrompe la connessione. Questo potrebbe indicare tentativi di interrompere comunicazioni legittime o di scansione delle porte.