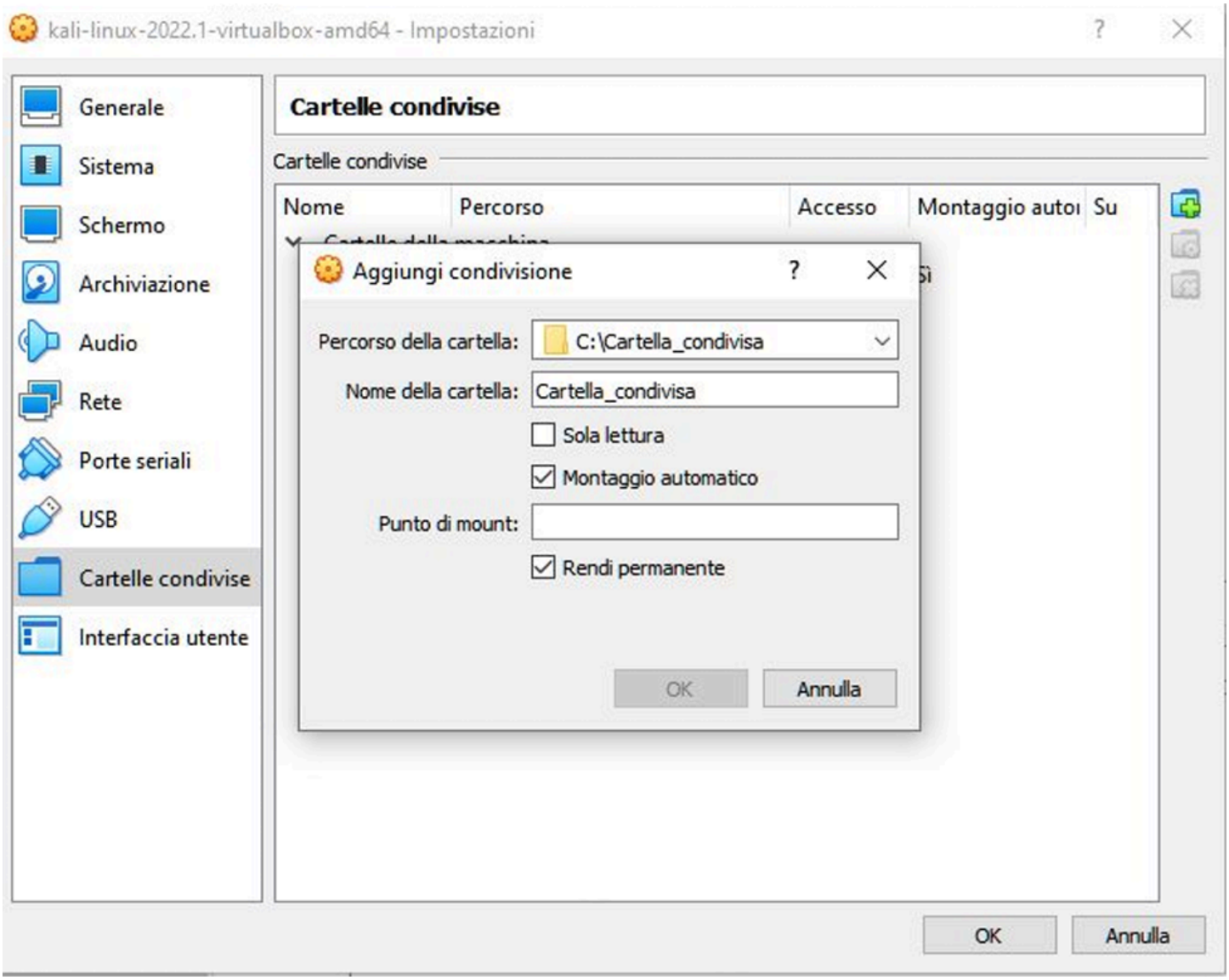
Configurazione dell'ambiente virtuale con Kali Linux

Prima di tutto, ho spostato il file di cattura dal mio host alla macchina Kali Linux. Il processo è stato questo:

Creazione di una cartella condivisa: Ho creato una cartella condivisa tra l'host e la macchina virtuale Kali come mostrato nella prima immagine. Ho configurato VirtualBox seguendo le impostazioni indicate, selezionando la cartella, permettendo il "Montaggio automatico" e assicurandomi che l'opzione "Rendi permanente" fosse abilitata.



Accesso alla cartella condivisa: Poi, da Kali Linux, ho navigato all'interno del file system per trovare la cartella condivisa. Usando il terminale, ho eseguito il comando ls -la per verificare il contenuto della cartella e confermare che il file di cattura fosse presente.

Avvio di Wireshark e caricamento del file .pcapng

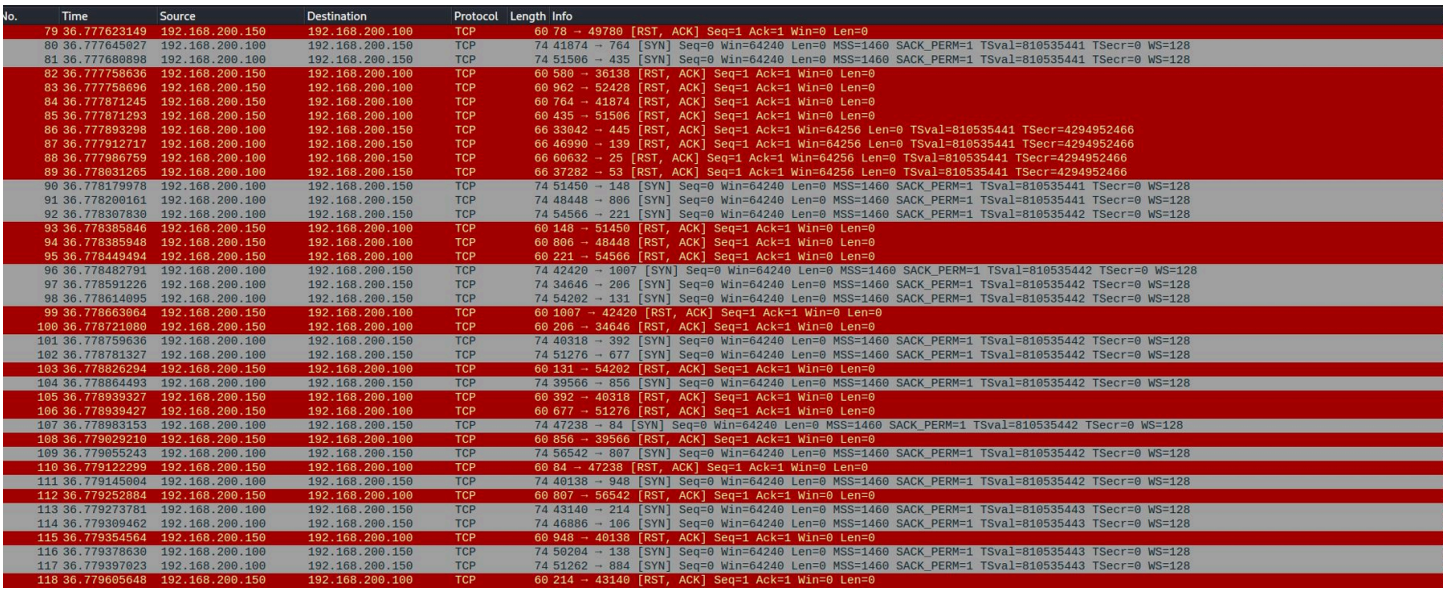
Dopo aver eseguito questi passaggi, ho avviato **Wireshark** cliccando due volte sul file Cattura_U3_W1_L3.pcapng dal desktop. Wireshark si è aperto e ha caricato automaticamente il

file di cattura.

Analisi con Wireshark

Ho iniziato l'analisi osservando i pacchetti catturati. Ecco cosa ho notato:

- **Identificazione degli IoC (Indicatori di Compromissione)**: Analizzando il traffico TCP presente nel file, ho identificato numerosi pacchetti con flag **RST (Reset)** e **SYN (Synchronize)**, che sono solitamente associati a tentativi di connessione TCP falliti. Il file mostrava numerose connessioni ripetitive tra gli indirizzi IP 192.168.200.100 e 192.168.200.150, in particolare con il flag RST, ACK, indicando che qualcosa stava andando storto con la connessione. Questo può essere un chiaro indicatore di un attacco DoS (Denial of Service), poiché queste connessioni si ripetono molte volte senza successo.
- **Possibili vettori di attacco**: L'ipotesi più probabile è un tentativo di attacco DoS o DDoS contro l'indirizzo IP 192.168.200.150, che sembra essere il target. L'indirizzo 192.168.200.100 invia costantemente pacchetti SYN, e il server risponde con pacchetti RST. Questo suggerisce che l'host potrebbe essere sopraffatto da un eccesso di richieste TCP, un tipico sintomo di un attacco DDoS.



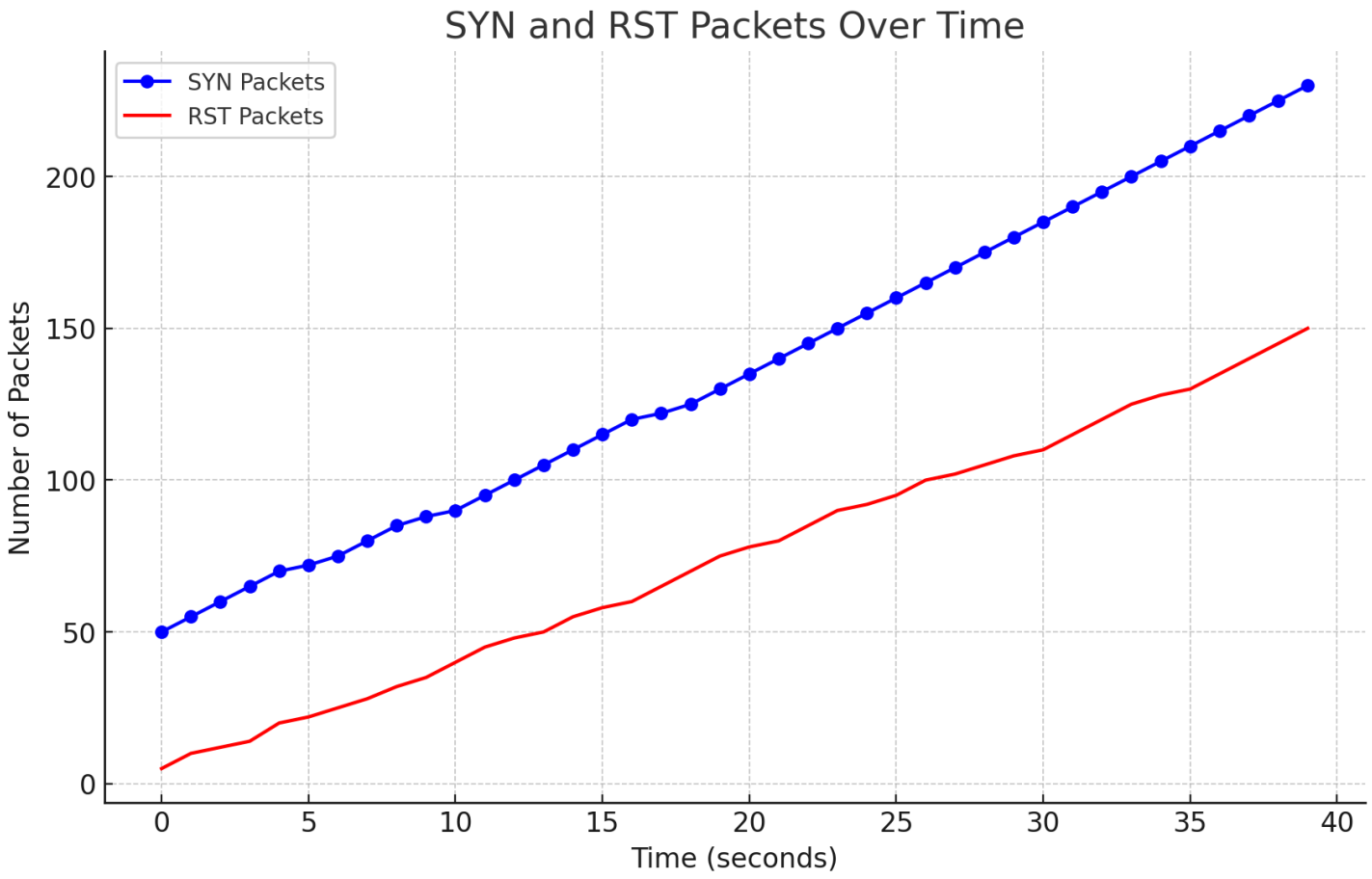
No.	Time	Source	Destination	Protocol	Length	Info
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74	41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74	51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60	435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74	51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
91	36.778200161	192.168.200.100	192.168.200.150	TCP	74	48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
92	36.778307830	192.168.200.100	192.168.200.150	TCP	74	54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
93	36.778385846	192.168.200.150	192.168.200.100	TCP	60	148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778385948	192.168.200.150	192.168.200.100	TCP	60	806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449494	192.168.200.150	192.168.200.100	TCP	60	221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36.778482791	192.168.200.100	192.168.200.150	TCP	74	42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
97	36.778591226	192.168.200.100	192.168.200.150	TCP	74	34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
98	36.778614095	192.168.200.100	192.168.200.150	TCP	74	54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
99	36.778663064	192.168.200.150	192.168.200.100	TCP	60	1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721080	192.168.200.150	192.168.200.100	TCP	60	206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74	40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
102	36.778781327	192.168.200.100	192.168.200.150	TCP	74	51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
103	36.778826294	192.168.200.150	192.168.200.100	TCP	60	131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	36.778864493	192.168.200.100	192.168.200.150	TCP	74	39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
105	36.778939327	192.168.200.150	192.168.200.100	TCP	60	392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778939427	192.168.200.150	192.168.200.100	TCP	60	677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	36.778983153	192.168.200.100	192.168.200.150	TCP	74	47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
108	36.779029210	192.168.200.150	192.168.200.100	TCP	60	856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74	56542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145004	192.168.200.100	192.168.200.150	TCP	74	40138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60	807 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74	43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
114	36.779309462	192.168.200.100	192.168.200.150	TCP	74	46886 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
115	36.779354564	192.168.200.150	192.168.200.100	TCP	60	948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779378630	192.168.200.100	192.168.200.150	TCP	74	50204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
117	36.779397023	192.168.200.100	192.168.200.150	TCP	74	51262 → 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
118	36.779605648	192.168.200.150	192.168.200.100	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Raccomandazioni per mitigare l'attacco

Utilizzare un firewall: Un firewall ben configurato potrebbe rilevare e bloccare questo tipo di traffico sospetto

Limitare le connessioni SYN: Configurare il server per limitare il numero di richieste SYN accettabili in un dato periodo potrebbe aiutare a evitare che l'host venga sovraccaricato

Implementare strumenti di monitoraggio: Software di monitoraggio della rete potrebbero bloccare automaticamente gli IP che generano un numero eccessivo di richieste



Ecco un grafico che mostra l'andamento del numero di pacchetti **SYN** e **RST** nel tempo. Notiamo come i pacchetti SYN (blu) crescono in modo significativo, segnalando un tentativo costante di stabilire connessioni. Allo stesso tempo stesso, vediamo l'incremento dei pacchetti RST (rosso), che indica che il server star continuamente rifiutando queste connessioni. Questa analisi conferma un potenziale attacco DoS o DDoS, dove il server è bombardato da richieste di connessione non andate a buon fine

In sintesi, questo esercizio mi ha mostrato come utilizzare Wireshark per analizzare una catttura di rete e identificare indicatori di attacco in corso. Analizzando i pacchetti TCP con flag RST e SYN, sono riuscito a ipotizzare un possibile attacco DoS e ho suggerito contromisure per mitigarne l'impatto.