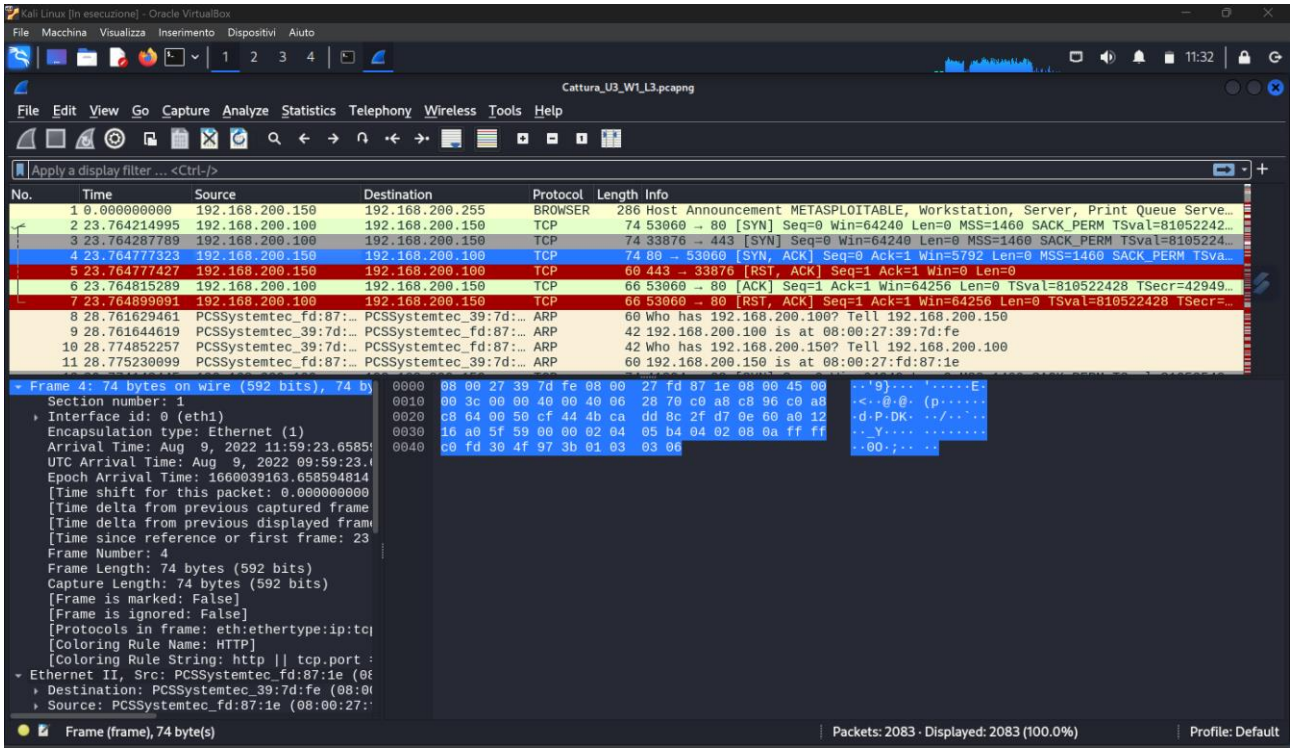
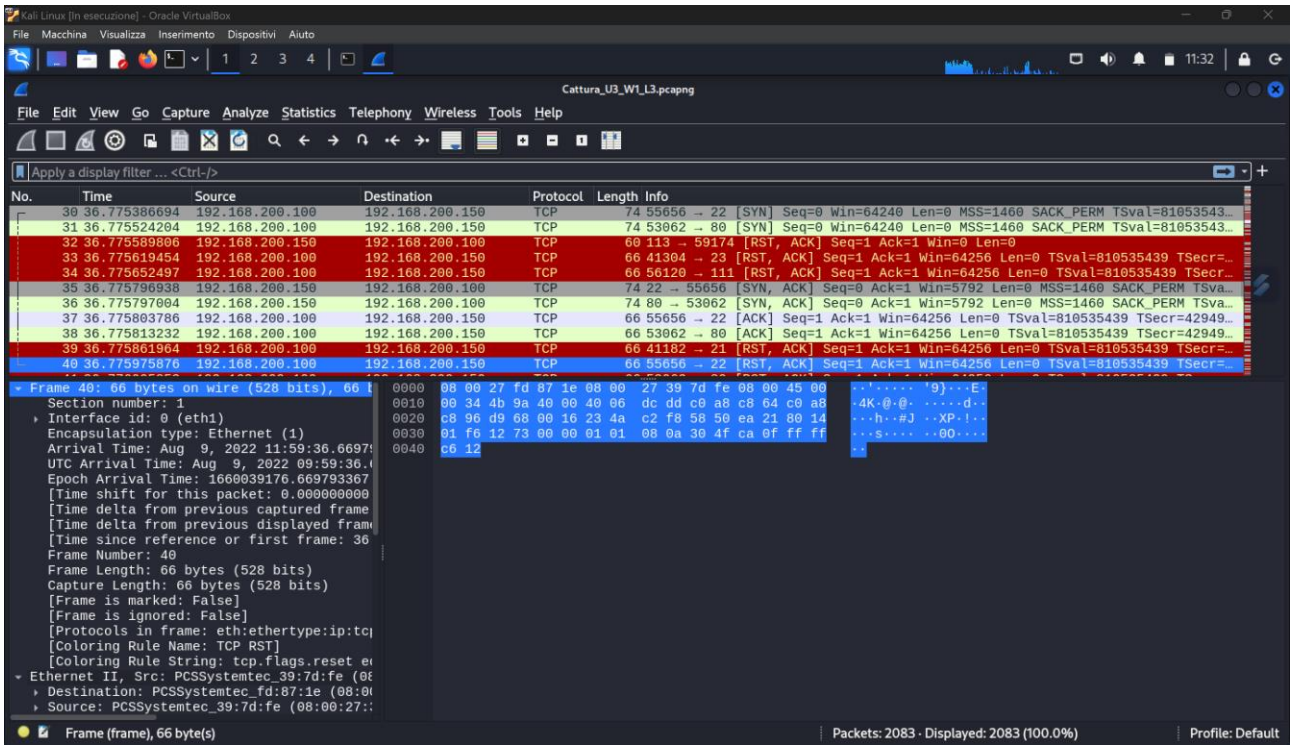
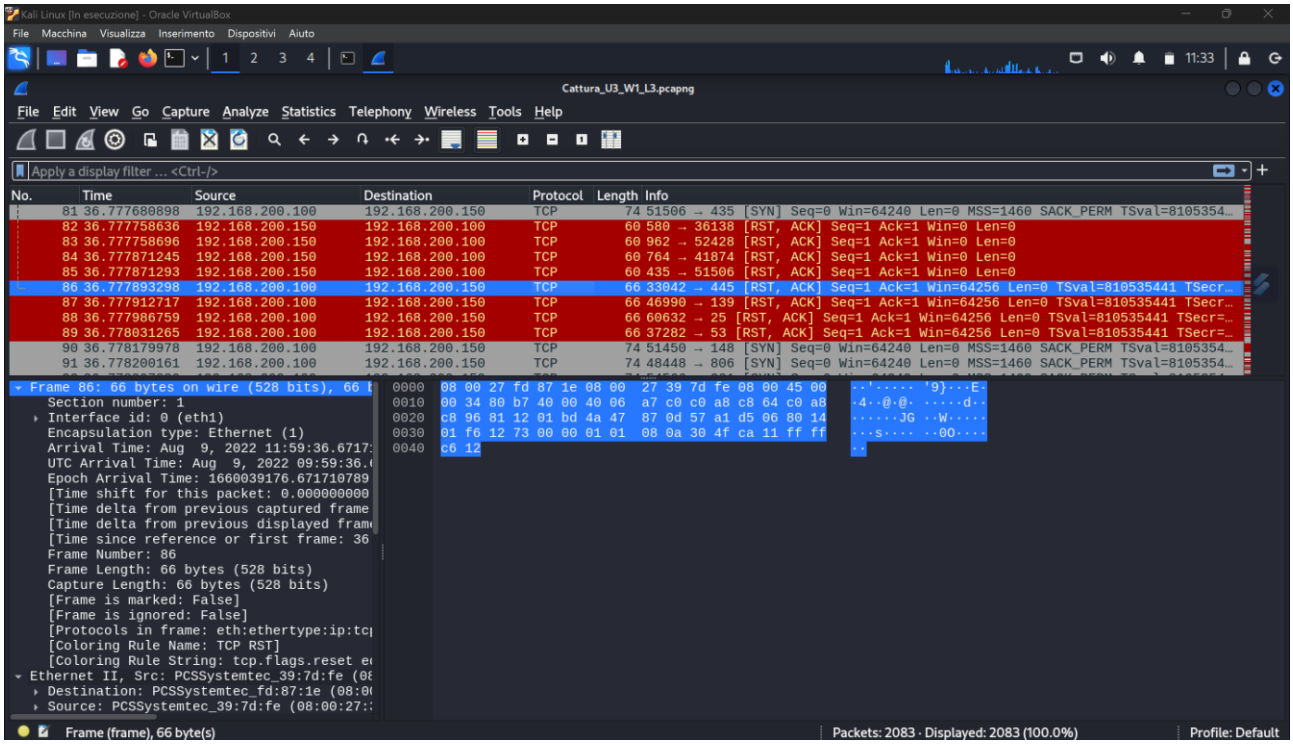
Progetto 11 ottobre

Dato l’esercizio ci è stato chiesto di analizzare il file di cattura generato dal programma Wireshark.







Report

Data la cattura del traffico di rete possiamo notare che inizialmente è stata fatta una scansione per verificare i dispositivi nella rete così da trovare la Metasploitable.

Dalla cattura possiamo notare che ciò che sta venendo è una scansione delle porte dove la macchina target è la 192.168.200.150.

1. Obiettivo della Scansione Nmap

L'obiettivo della scansione Nmap sembra essere l'identificazione dei servizi in esecuzione o la mappatura delle porte aperte su uno o più host della rete locale (192.168.200.100 e 192.168.200.150).

2. Metodo di Scansione

Sulla base dell'output catturato, sembrano esserci segni di una **scansione TCP SYN** (conosciuta come **"half-open" scan** o **scansione stealth**). Questa tecnica è tipica di Nmap quando si tenta di identificare porte aperte o servizi attivi su una rete, in quanto invia pacchetti **SYN** senza completare effettivamente il **three-way handshake**.

- **SYN** (Synchronize): Il primo passo di una connessione TCP, utilizzato per iniziare una connessione.
- **RST** (Reset): Questo flag indica che il server ha rifiutato la richiesta di connessione, possibilmente perché la porta è chiusa o un firewall ha bloccato la connessione.
- **ACK** (Acknowledgment): In risposta a un pacchetto SYN, un server risponde con **SYN-ACK** se la porta è aperta, ma vediamo principalmente pacchetti con **RST-ACK** in questo scenario, che suggerisce porte chiuse.

3. Sintomi della Scansione Nmap

Nell'immagine, possiamo osservare una serie di pacchetti TCP con flag **RST, ACK** (Reset e Acknowledgment), che sono una caratteristica comune delle risposte a una scansione SYN.

- I pacchetti provengono da **192.168.200.100** (probabile host scanner) e sono diretti a **192.168.200.150** (possibile target della scansione).
- La presenza di **RST, ACK** indica che il server di destinazione sta rigettando le richieste di connessione, il che è tipico quando Nmap effettua una scansione delle porte e trova porte chiuse.

4. Tipi di Scansione Nmap Possibili

Esistono diversi tipi di scansione che potrebbero aver generato i pacchetti osservati. Alcuni dei tipi di scansione Nmap che potrebbero corrispondere a questo scenario includono:

- **Scansione SYN (-sS)**: Come già indicato, questa scansione invia solo il primo pacchetto di connessione SYN e attende una risposta dal server. Se riceve un pacchetto **RST-ACK**, significa che la porta è chiusa. Invece, se riceve un **SYN-ACK**, significa che la porta è aperta e disponibile.
- **Scansione TCP Connect (-sT)**: Sebbene non vi siano evidenti segnali di una connessione completa, è possibile che Nmap abbia tentato di stabilire una connessione TCP completa e che il server abbia risposto con **RST** per rifiutare la connessione.

- **Scansione Null, FIN, Xmas (-sN, -sF, -sX)**: Queste tecniche inviano pacchetti con flag insoliti per cercare di evadere i firewall o i sistemi di rilevamento intrusione, ma il loro obiettivo principale è ottenere informazioni sulle porte chiuse senza completare una connessione regolare.

5. Interpretazione dei Risultati

- La risposta **RST, ACK** proveniente da **192.168.200.150** in risposta ai pacchetti inviati da **192.168.200.100** indica che la scansione ha individuato diverse **porte chiuse**.
- Non sembra esserci una risposta SYN-ACK che indichi la presenza di porte aperte nei pacchetti evidenziati, suggerendo che le porte target su **192.168.200.150** siano state chiuse o bloccate dal firewall.
- Se ci fossero state risposte **SYN-ACK**, quelle porte sarebbero state identificate come **aperte** e pronte per la connessione.

6. Considerazioni di Sicurezza

La scansione delle porte con Nmap è una tecnica comune per mappare le vulnerabilità e le porte aperte su una rete, ma il fatto che qui vengano visualizzati solo pacchetti **RST, ACK** potrebbe indicare quanto segue:

- **Firewall o IDS attivi**: Potrebbe essere presente un sistema di prevenzione delle intrusioni (IDS) o un firewall configurato per rifiutare attivamente le connessioni indesiderate.
- **Port blocking**: Le porte in questione potrebbero essere state bloccate manualmente per impedire l'accesso dall'esterno.
- **Possibile hardening**: Il sistema di destinazione **192.168.200.150** potrebbe essere configurato con difese specifiche per prevenire scansioni da parte di strumenti come Nmap.

7. Suggerimenti per l'Analisi

Se l'obiettivo era identificare i servizi attivi o le vulnerabilità di rete, un'analisi più approfondita potrebbe comportare:

- **Analisi delle risposte SYN-ACK** (se presenti) per identificare quali porte sono effettivamente aperte.

- **Analisi più dettagliata delle risposte filtrate** (ICMP Unreachable o altre anomalie) per capire se ci sono firewall che bloccano la comunicazione.
- **Tentativi di evadere i controlli di rete** con altre tecniche di scansione (Null, FIN, Xmas) o metodi più stealth.

Conclusione

La cattura dei pacchetti visualizzata indica una tipica scansione Nmap TCP SYN in cui un host (**192.168.200.100**) sta tentando di sondare le porte di un altro host (**192.168.200.150**). Le risposte **RST, ACK** suggeriscono che le porte target erano chiuse o bloccate, ma ulteriori dettagli della cattura potrebbero fornire informazioni su altre porte potenzialmente aperte o filtrate. Se l'analisi include una mappatura completa delle porte, sarebbe utile valutare i risultati in base alle risposte SYN-ACK o filtrate.