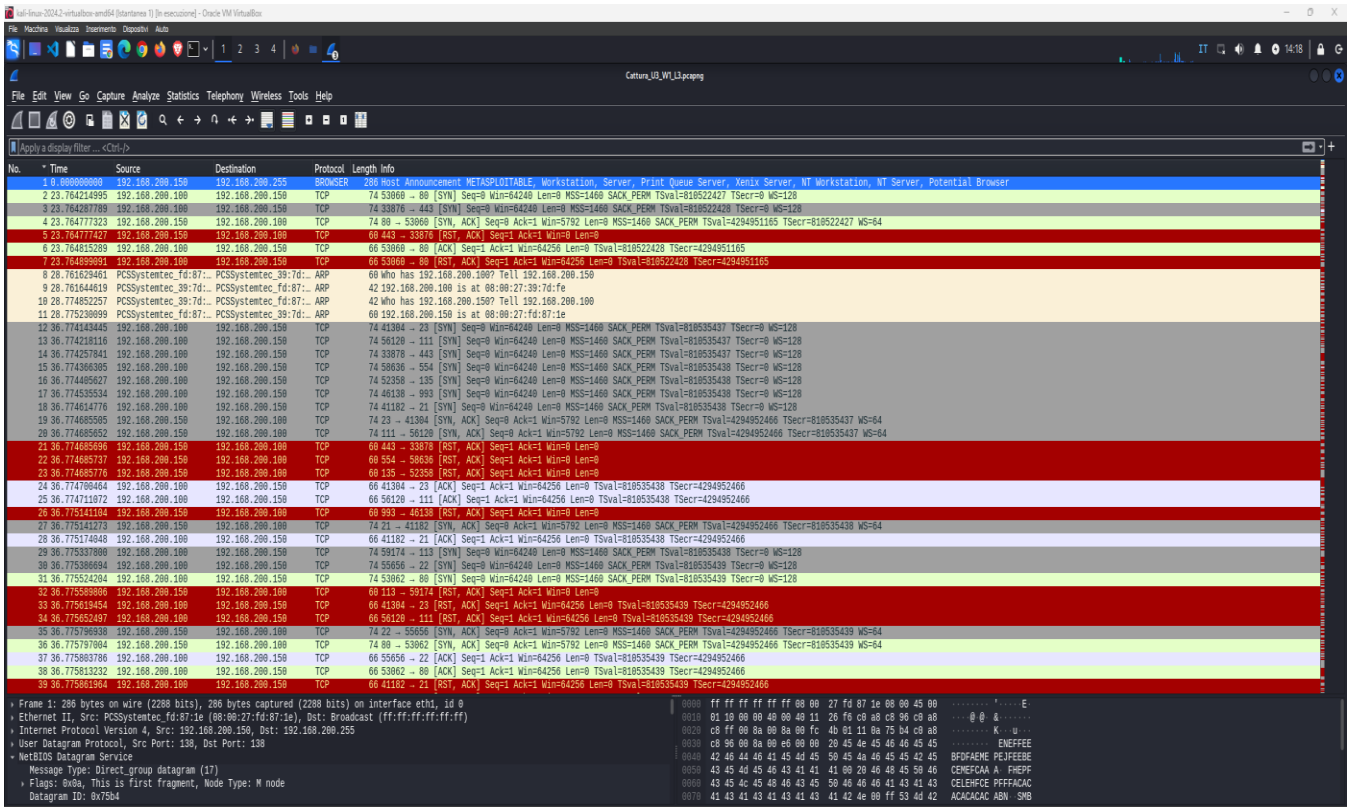
Relazione

Relazione sull'analisi del traffico di rete

1. Descrizione del traffico anomalo

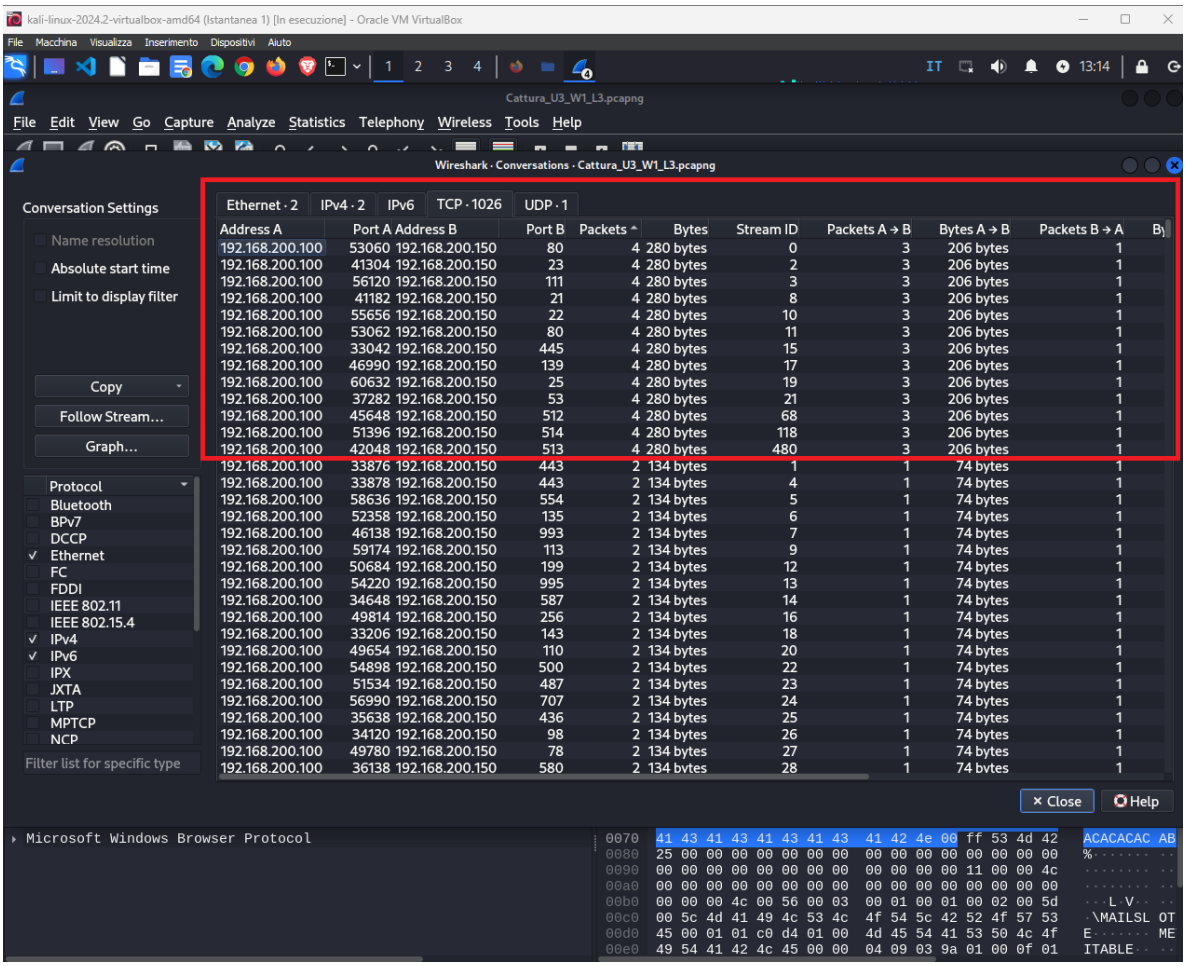
Durante l'analisi del file di cattura di rete con **Wireshark**, è stato individuato un traffico sospetto associato alla macchina con indirizzo IP **192.168.200.150**, che sembra essere una macchina **Metasploitable**,.Il traffico evidenziato in rosso, segnalato da **Wireshark** come pacchetti non andati a buon fine, potrebbe indicare tentativi di attacco o scansioni aggressive delle porte.



2. Porte coinvolte

Dall'analisi della cattura di rete, le seguenti porte sono risultate aperte sulla macchina **192.168.200.150**:

- **TCP**: 80 (HTTP), 23 (Telnet), 111 (RPC), 21 (FTP), 22 (SSH), 445 (SMB), 139 (NetBIOS), 25 (SMTP), 53 (DNS), 5125 (probabile servizio custom), 514 (Syslog)
- **UDP**: 138 (NetBIOS Datagram Service)



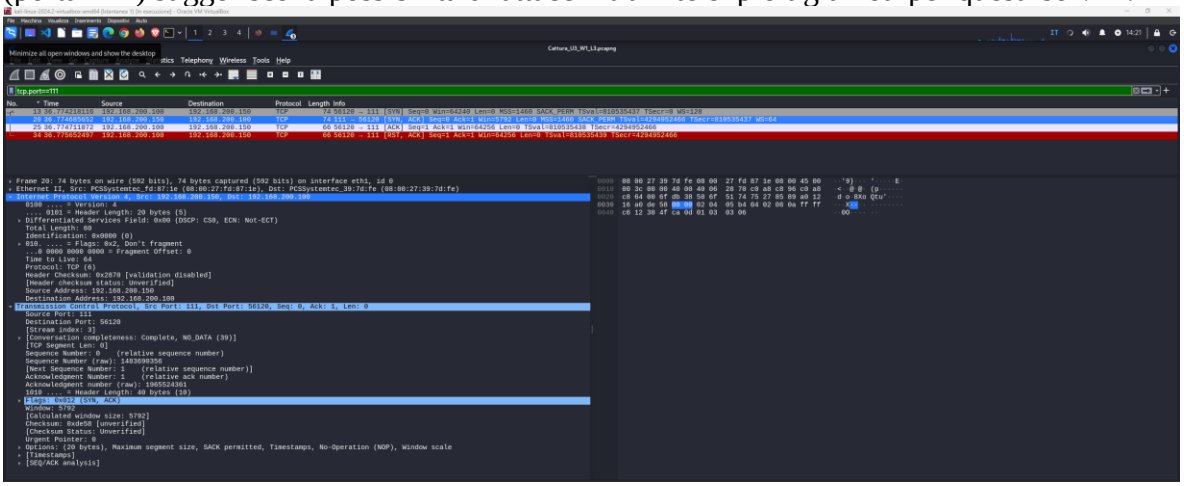
Questa configurazione lascia presumere che la macchina Metasploitable sia vulnerabile a diversi attacchi, in quanto espone un numero considerevole di servizi, molti dei quali notoriamente deboli dal punto di vista della sicurezza, come **Telnet** (porta 23) e **FTP** (porta 21), entrambi non criptati.

3. Indicatori di compromissione (IOC)

Durante l'analisi del traffico, i seguenti Indicatori di Compromissione (IOC) sono stati identificati:

- **Connessioni fallite**: Il traffico segnalato in rosso, evidenziando connessioni non completate, potrebbe rappresentare tentativi di ricognizione o attacco, come **scansioni di porte** o tentativi di brute force.

- **Porte vulnerabili aperte**: La presenza di porte vulnerabili come Telnet, FTP, SMB e RPC (porta 111) suggerisce la possibilità di attacchi tramite exploit già noti per questi servizi.



- **Traffico UDP sulla porta 138**: Il servizio NetBIOS Datagram sulla porta UDP 138 potrebbe essere usato per intercettare dati sensibili o facilitare un attacco **man-in-the-middle**.

4. Ipotesi sui vettori di attacco

Basandoci sugli IOC individuati, possiamo ipotizzare che i vettori di attacco più probabili siano:

- **Scansioni di porte**: L'alto numero di pacchetti inviati, in particolare su molteplici porte aperte, indica un possibile tentativo di scansione delle porte per identificare i servizi attivi e preparare un attacco mirato.
- **Tentativi di brute force** su servizi non sicuri come **Telnet** (porta 23) o **FTP** (porta 21), che non offrono cifratura e sono vulnerabili a questo tipo di attacchi.
- **Attacchi SMB**: Le porte 445 e 139, associate al protocollo SMB, sono note per essere vettori di attacchi quali **EternalBlue**, utilizzato da malware come **WannaCry**.
- **Possibile exploit su RPC (porta 111)**: Questa porta è comunemente associata a vulnerabilità come **RPC DCOM** che potrebbe consentire esecuzione di codice da remoto.

5. Azioni consigliate per mitigare l'attacco

Per ridurre gli impatti dell'attacco in corso e prevenire eventuali attacchi futuri, si consiglia di adottare le seguenti azioni:

- **Chiusura delle porte non necessarie**: Disattivare o filtrare le porte che non sono strettamente necessarie, in particolare servizi vulnerabili come **Telnet** (23), **FTP** (21), **RPC** (111) e **SMB** (445/139). L'uso di firewall per limitare l'accesso a queste porte potrebbe ridurre drasticamente la superficie di attacco.
- **Implementazione di protocolli sicuri**: Sostituire servizi non sicuri con alternative più sicure, ad esempio:
  - Usare **SSH** (22) al posto di Telnet per connessioni remote.
  - Usare **SFTP** o **FTPS** al posto di FTP per il trasferimento di file.
- **Aggiornamenti di sicurezza**: Assicurarsi che il sistema operativo e i servizi esposti siano aggiornati con le ultime patch di sicurezza per prevenire attacchi basati su vulnerabilità note come **EternalBlue**.

- **Monitoraggio del traffico di rete**: Utilizzare strumenti di **Intrusion Detection System (IDS)** per identificare tempestivamente traffico sospetto e bloccare gli IP da cui provengono le scansioni o i tentativi di attacco.
- **Abilitazione del logging**: Configurare il sistema per registrare tutti i tentativi di accesso falliti, in modo da poter effettuare un'analisi forense in caso di compromissione e correlare gli eventi.

6. Prevenzione di attacchi futuri

Per prevenire simili attacchi in futuro, si suggerisce di:

- **Applicare una difesa in profondità**: Oltre a chiudere le porte non necessarie, implementare misure come la segmentazione della rete e il monitoraggio continuo per rilevare comportamenti anomali.
- **Formazione del personale**: Assicurare che gli amministratori di sistema comprendano le implicazioni della sicurezza dei servizi esposti e l'importanza di protocolli sicuri.
- **Pianificazione della risposta agli incidenti**: Preparare e testare piani di risposta agli incidenti per ridurre il tempo di reazione in caso di attacco.

Conclusioni

L'analisi della cattura di rete ha rivelato che la macchina **192.168.200.150** è potenzialmente sotto attacco. Il traffico anomalo, le porte aperte e i servizi vulnerabili indicano tentativi di scansione e possibile sfruttamento delle vulnerabilità. È essenziale intervenire tempestivamente con l'adozione di misure di sicurezza come la chiusura delle porte vulnerabili e il rafforzamento della rete per prevenire attacchi futuri.