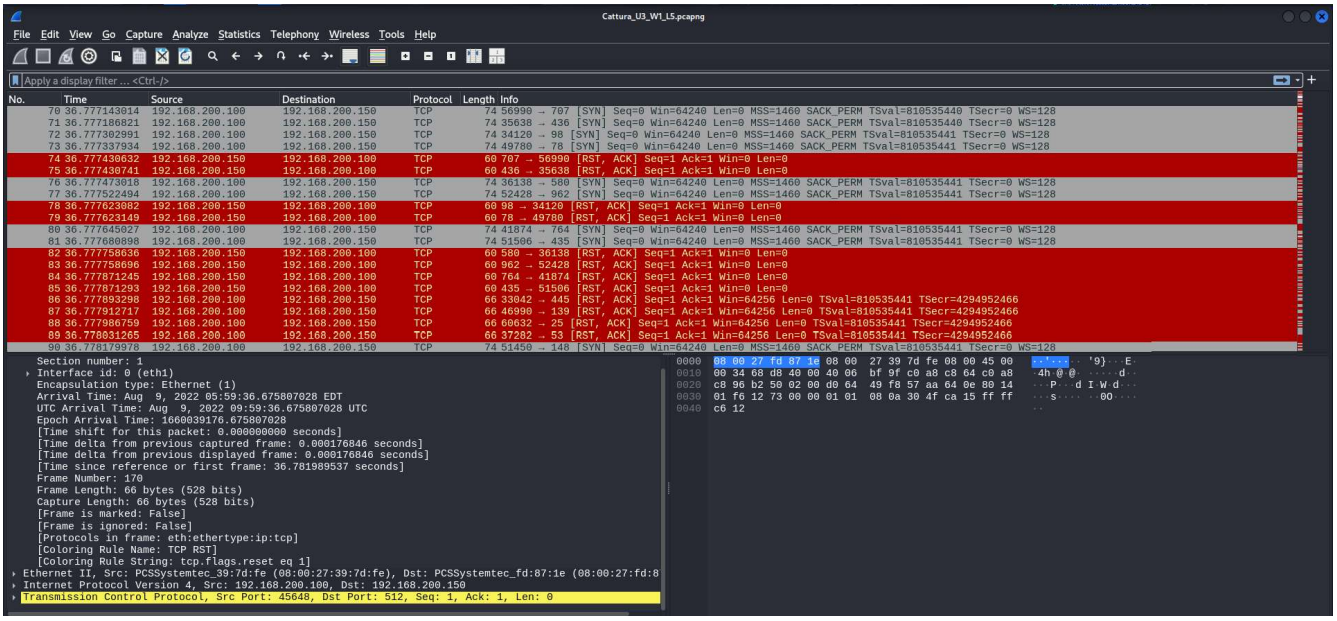
Analisi di Minacce Nascoste nella Rete: Identificazione di IOC e Strategie per Prevenire Futuri Attacchi

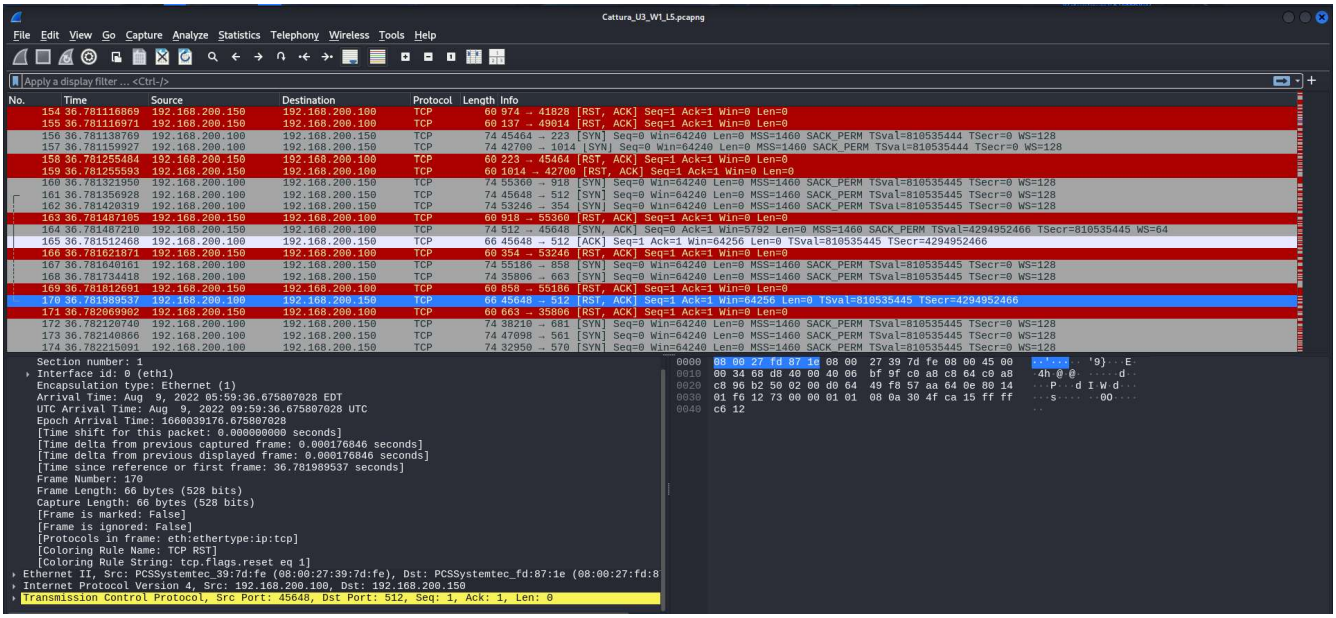
L’analisi della cattura di rete effettuata con Wireshark mette in evidenza chiari indicatori di compromissione (IOC) relativi all’host 192.168.200.150. In particolare, si osservano numerosi tentativi di connessione provenienti dall’indirizzo 192.168.200.100, che invia pacchetti SYN verso un’ampia gamma di porte TCP dell’host bersaglio, con una frequenza elevata e ravvicinata.



Le risposte ricevute da 192.168.200.150 consistono in pacchetti [RST, ACK], dove RST (Reset) indica la volontà di terminare immediatamente la comunicazione, mentre ACK (Acknowledgment) conferma la ricezione del SYN. Questo comportamento è tipico di una scansione delle porte: l’host mittente sta cercando di individuare porte aperte sul sistema di destinazione.

Proseguendo con l’analisi dei pacchetti, emerge un dettaglio significativo: al pacchetto 164, l’host 192.168.200.150 risponde con [SYN, ACK] a una richiesta di connessione TCP sulla porta 512. La sequenza si completa con un [ACK] da parte dell’host 192.168.200.100 (pacchetto 165), confermando l’avvenuto handshake TCP. Questo indica che la porta 512 è effettivamente aperta e potenzialmente vulnerabile. Tuttavia, dopo poco (pacchetto 170), l’host mittente termina volontariamente la connessione.

Questo comportamento suggerisce che l’attività in corso sia di ricognizione: l’host 192.168.200.100 sta mappando il sistema 192.168.200.150 alla ricerca di porte aperte o servizi vulnerabili. Sebbene abbia identificato una porta accessibile, ha scelto di non sfruttarla subito, probabilmente raccogliendo informazioni per un possibile attacco futuro.



È importante notare che, in tutto il traffico analizzato, non si osservano richieste DNS o HTTP, il che indica che l’indirizzo IP dell’host bersaglio era già noto al mittente. Questo rafforza l’ipotesi di un attaccante interno alla rete, o comunque di una macchina già compromessa che opera dall’interno. Inoltre, la rapidità e la sistematicità dei pacchetti suggeriscono l’uso di strumenti automatizzati di scansione, come Nmap in modalità SYN scan, frequentemente utilizzati per identificare servizi attivi senza completare del tutto la connessione TCP.

Azioni correttive e misure di prevenzione

Per ridurre l’impatto dell’attacco in corso e prevenire attacchi simili in futuro, è consigliabile adottare le seguenti misure:

1. **Isolare immediatamente l’host 192.168.200.100**, qualora non sia autorizzato alla scansione, per limitare ulteriori attività dannose.
2. **Chiudere la porta 512** sull’host 192.168.200.150 se non strettamente necessaria, e verificare che i servizi attivi siano effettivamente richiesti.
3. **Analizzare i log di sistema** per rilevare eventuali tentativi di exploit, accessi anomali o connessioni sospette.

4. **Eseguire una scansione approfondita antivirus e antimalware** sull’host target per rilevare eventuali compromissioni.
5. **Implementare una suddivisione della rete** per limitare la visibilità tra le diverse parti e ridurre la superficie di attacco .
6. **Installare un sistema IDS/IPS**, utile per individuare e bloccare scansioni sospette in tempo reale.
7. **Disabilitare i servizi non utilizzati**, e **configurare correttamente firewall interni ed esterni** per limitare il traffico solo alle porte e ai protocolli indispensabili.