**Analisi della Cattura di Rete: Indicatori di Compromissione (IOC)**

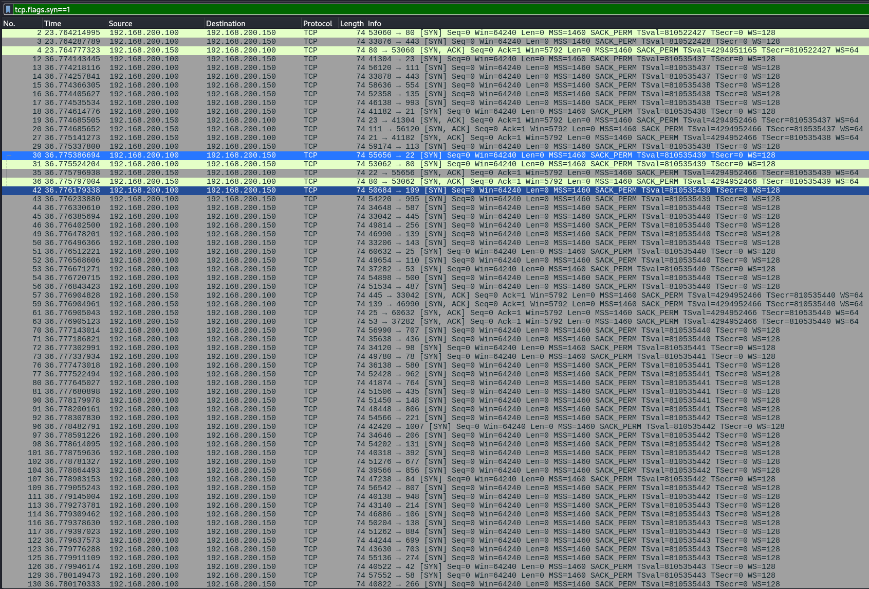
**1. Introduzione**

Questa analisi si concentra sulla cattura di rete per identificare indicatori di compromissione (IOC), ipotizzare i possibili vettori di attacco e suggerire azioni di mitigazione per ridurre l'impatto e prevenire futuri attacchi.  
I dati sono stati analizzati utilizzando uno **script in Python**.

**2. Indicatori di Compromissione (IOC)**

* Numerosi pacchetti **SYN** senza **ACK** di risposta.
* Traffico su **porte diverse** (21, 23, 111) suggerisce uno **scan aggressivo**.
* Pacchetti **ARP sospetti** che indicano possibili tentativi di **ARP Spoofing**.
* Comunicazioni bilanciate tra **192.168.200.100** e **192.168.200.150**.

**3. Vettori di Attacco Possibili**

* **Aggressive Port Scanning:** Invio massiccio di pacchetti **SYN** a porte diverse per identificare servizi attivi. Ipotesi più accreditata, le risposte mancate risposte ACK sono tipiche degli scan di porte che utilizzano i pacchetti SYN come il comando nmap -sS
* **SYN Flood:** Invio continuo di pacchetti **SYN** senza completare la connessione TCP, causando saturazione delle risorse. Meno probabile, poiché le porte di destinazione variano molto, un SYN Flood atto a limitare l’uso di un singolo servizio è quindi meno probabile

**4. Mitigazione dell'Attacco in Corso**

* **Implementare firewall** per limitare i pacchetti **SYN** da IP sospetti.
* **Disabilitare servizi insicuri** (Telnet, FTP) e utilizzare **SSH/SFTP**.
* **Isolare** i dispositivi coinvolti nella rete per limitare la propagazione.
* **Monitorare i log di rete** per identificare eventuali anomalie.

**5. Prevenzione di Attacchi Futuri**

* **Configurare firewall** per bloccare scansioni di porte aggressive.
* **Abilitare SYN Cookies** per difendersi dal **SYN Flood**.
* Utilizzare **IDS/IPS** (es. **Snort**, **Suricata**) per rilevare comportamenti sospetti.
* **Segmentare la rete** e limitare i permessi di accesso ai servizi critici.
* **Aggiornare regolarmente** software e sistemi con le ultime patch di sicurezza.

**6. Strumenti Utilizzati**

Per l'analisi dei dati della cattura di rete è stato utilizzato uno **script in Python** che ha permesso di:

* Identificare pattern sospetti nei pacchetti di rete.
* Analizzare i protocolli e le porte coinvolte.

