Analisi di Scansione di Rete - Identificazione di IOC

1. Identificazione ed analisi degli IOC

Dalle immagini della cattura di rete effettuata con Wireshark, ho notato numerose connessioni TCP tra gli host 192.168.200.100 e 192.168.200.150; quindi ho potuto ipotizzare che gli indicatori di compromissione possano essere i seguenti:

- Un alto numero di pacchetti RST/ACK inviati, indicano potenzialmente un tentativo di terminare connessioni in modo anomalo.

- Ripetuti tentativi di connessione con pacchetti SYN, ma senza l'instaurazione di una vera e propria connessione tra i due host.

- Comunicazioni in ARP che potrebbero suggerire attività di scanning sulla rete locale.

2. Ipotesi sui potenziali vettori di attacco

Dati questi indicatori di compromissione, possiamo ipotizzare i possibili vettori di attacco, ovvero:

- Port scanning: un attaccante potrebbe essere alla ricerca di porte aperte sul sistema target.

- SYN flood attack: il volume di pacchetti SYN potrebbe essere il risultato di un attacco di tipo denial-of-service (DoS).

- ARP spoofing: le comunicazioni ARP anomale potrebbero indicare tentativi di intercettazione del traffico (Man-in-the-Middle).

3. Azioni consigliate

Queste le azioni consigliate, in base ai possibili vettori di attacco, per ridurre gli impatti dell’attacco attuale e dei potenziali futuri:

- Installare e configurare un Firewall

-Implementare IPS/IDS, questi infatti rileverebbero subito che si sta trattando di port scanning e bloccherebbero l’IP

- Monitorare attivamente il traffico ARP per identificare e bloccare attività di spoofing.

- Effettuare una scansione approfondita dei sistemi coinvolti per verificare l'assenza di compromissioni ulteriori. Quindi disabilitare possibili porte e servizi exploitabili da un attaccante.