Analisi di una Cattura di Rete con Wireshark

Traccia

Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione (IOC). Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark.

Analizzate la cattura attentamente e rispondete ai seguenti quesiti:

1. Identificare eventuali IOC, ovvero evidenze di attacchi in corso

2. In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati

3. Consigliate un'azione per ridurre gli impatti dell'attacco

Identificazione di eventuali IOC

Gli **Indicatori di Compromissione** (IOC) sono segni o artefatti osservabili che indicano che una rete o un sistema è stato compromesso.

Possono includere indirizzi IP sospetti, file con hash specifici,

URL malevoli, ecc.

Analizzando gli screenshot di Wireshark, sono stati identificati i seguenti possibili IOC:

- Numerosi pacchetti TCP con flag [RST, ACK]: Un numero elevato di pacchetti con flag di reset e acknowledgment può indicare un tentativo di interruzione di connessioni attive o una risposta a connessioni non riconosciute.

- Ripetute connessioni da indirizzi IP specifici: Gli indirizzi IP come 192.168.200.150 e 192.168.200.100 appaiono frequentemente come sorgenti o destinazioni, suggerendo che potrebbero essere coinvolti in attività sospette.

Ipotesi sui potenziali vettori di attacco

In base agli IOC trovati, possiamo formulare le seguenti ipotesi sui potenziali vettori di attacco:

- DoS (Denial of Service): L'alto numero di pacchetti RST, ACK potrebbe essere un segnale di attacco DoS, volto a interrompere il normale funzionamento dei servizi di rete.
- Scansione delle porte: Le connessioni ripetitive possono indicare un tentativo di scansione delle porte per identificare servizi vulnerabili. (ipotesi più probabile data la quantità di richieste)

Consigli per ridurre gli impatti dell'attacco

Per ridurre gli impatti dell'attacco, si consiglia di adottare le seguenti misure:

- Implementare firewall e IDS/IPS: Utilizzare sistemi di rilevamento e prevenzione delle intrusioni per monitorare e bloccare il traffico sospetto.

- Bloccare gli IP sospetti: Se confermato che gli IP 192.168.200.150 e 192.168.200.100 sono malevoli, bloccarli tramite il firewall.

- Analizzare i log di sistema: Controllare i log dei server e dei dispositivi di rete per ulteriori segni di compromissione.

- Aggiornare e patchare: Assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza per ridurre le vulnerabilità sfruttabili.