S9/L3

THREAT INTELLIGENCE & IOC

Presentato da
Noemi de Martino

TRACCIA

Durante la lezione teorica, abbiamo visto la **Threat Intelligence** e gli indicatori di compromissione.
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 rispondere ai seguenti quesiti:

- Identificare eventuali **IOC**, ovvero evidenze di attacchi in corso In base agli **IOC** trovati,
- Fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

INTRODUZIONE A THREAT INTELLIGENCE E IOC

La **Threat Intelligence** è un settore della sicurezza informatica che si occupa di raccogliere, analizzare e interpretare informazioni relative alle minacce cibernetiche. Gli **Indicatori di Compromissione (IOC)** sono evidenze di attività malevole o di attacchi informatici in corso o già avvenuti.

Gli **IOC** possono includere file sospetti, hash, indirizzi IP, URL e altre tracce lasciate da attività malevole. In questo esercizio pratico, analizzeremo una cattura di rete con Wireshark per identificare eventuali IOC e formulare ipotesi sui possibili vettori di attacco. Infine, proporremo azioni per mitigare l'impatto dell'attacco.

ANALISI DEL TRAFFICO DI RETE

Dall'analisi della cattura di rete con Wireshark, emergono i seguenti Indicatori di Compromissione:

- **Richieste TCP ripetute:** Abbiamo osservato un numero elevato di richieste **TCP (SYN)** su porte diverse in destinazione.
- **Pattern di Scansione:** Le richieste **SYN** provengono dall'host **192.168.200.100** e sono dirette all'host target **192.168.200.150** su diverse porte.
- **Risposte Differenziate**:
  - Per alcune richieste, il target risponde con **[SYN+ACK]**, indicando che la porta è aperta.
  -Per altre richieste, il target risponde con **[RST+ACK]**, indicando che la porta è chiusa.
- **Scansione delle Porte**: Un numero elevato di richieste **TCP (SYN)** provenienti dall'host **192.168.200.100** verso l'host **192.168.200.150** su diverse porte indica una possibile scansione delle porte.
- **Mappe dei Servizi**: La presenza di risposte **SYN+ACK** e **RST+ACK** indica che l'attaccante sta cercando di mappare i servizi attivi e le porte aperte sull'host target.

AZIONI CONSIGLIATE PER RIDURRE GLI IMPATTI DELL'ATTACCO

Per mitigare l'impatto dell'attacco, possiamo:

01 **Configurazione del Firewall:**

Bloccare l'accesso alle porte dell'host attaccante (192.168.200.100) tramite regole firewall.

02 **Monitoraggio Attivo**

Implementare sistemi di Intrusion Detection System (IDS) per rilevare tentativi di scansione e altre attività sospette.

03 **Aggiornamenti e Patch**

Assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza.

04 **Segmentazione della Rete**

Implementare la segmentazione della rete per limitare l'accesso alle risorse critiche.