Threat intelligence & IOC
S9L5

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 ed analizzare 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 attuale ed eventualmente un simile attacco futuro

Fase 1: identificazione e analisi degli IOC (indicatori di compromissione)

Dall'analisi del traffico di rete fornito, sono stati isolati i seguenti indicatori tecnici che evidenziano un'attività sospetta in corso:

- **Traffico TCP anomalo:** si registra un volume elevato di richieste di connessione inviate in un arco temporale estremamente ridotto.
- **Indirizzo IP attaccante:** `192.168.200.150`, questo host è l'origine univoca di tutte le richieste sospette.
- **Indirizzo IP vittima:** `192.168.200.100`, questo host è il bersaglio delle richieste.
- **Pattern di scansione:** l'attaccante invia pacchetti con flag **SYN** (richiesta di sincronizzazione) verso una molteplicità di porte di destinazione sequenziali o casuali sulla vittima.
- **Risposta della vittima:** l'host destinazione risponde prevalentemente con pacchetti **RST, ACK** (Reset), indicando che le porte contattate sono chiuse e il servizio non è attivo.

Fase 2: ipotesi sui potenziali vettori di attacco

Basandosi sugli IOC identificati, si formulano le seguenti ipotesi:

Tipologia di attacco: l'evidenza suggerisce un attacco di tipo **port scanning** (scansione delle porte), non si tratta ancora di una compromissione attiva del sistema, ma di una fase preliminare.

Fase della kill chain: l'attacco si colloca nella fase di **reconnaissance (ricognizione) ed Enumerazione**, l'attaccante sta mappando la superficie di attacco per identificare servizi attivi (porte aperte) e potenzialmente vulnerabili.

Vettori successivi: una volta identificate le porte aperte (es. SSH, HTTP, SMB), è probabile che l'attaccante tenterà di sfruttare vulnerabilità specifiche dei servizi (exploitation) o tenterà attacchi di tipo **brute force** per ottenere credenziali di accesso validi.

Fase 3: azioni di mitigazione e prevenzione

Per ridurre l'impatto dell'attacco attuale e prevenire incidenti futuri, si consigliano le seguenti azioni:

- **Contenimento immediato:** implementare una regola di blocco sul Firewall perimetrale o sull'host stesso per l'indirizzo IP sorgente `192.168.200.150`, interrompendo immediatamente la scansione.
- **Hardening del sistema:** applicare il principio del "minimo privilegio" a livello di rete, chiudendo tutte le porte non strettamente necessarie ai servizi di business.
- **Monitoraggio attivo (IDS/IPS):** implementare e configurare sistemi di rilevamento e prevenzione delle intrusioni (come Snort o Suricata), questi sistemi sono in grado di riconoscere automaticamente la firma di un "port scan" e bloccare l'indirizzo IP malevolo in tempo reale senza intervento umano.

Su sistemi Linux è possibile bloccare l'IP attaccante tramite iptables con il comando:
`iptables -A INPUT -s 192.168.200.150 -j DROP`

Conclusioni:

L'analisi dell'incidente dimostra l'importanza critica del monitoraggio continuo del traffico di rete, sebbene un **port scan** possa apparire come un evento a basso impatto, rappresenta quasi sempre il preludio a un attacco mirato più sofisticato.

L'identificazione tempestiva di questo **IOC** ha permesso di comprendere le intenzioni dell'attaccante (fase di ricognizione) e di definire strategie difensive proattive.

Questo esercizio conferma come una corretta **threat intelligence** non serva solo a rispondere agli attacchi avvenuti, ma a prevenire compromissioni future riducendo la finestra di opportunità per l'attaccante.