Relazione sull'Analisi di Threat Intelligence & Indicatori di Compromissione (IOC)

Introduzione

L'analisi di Threat Intelligence ha l'obiettivo di identificare potenziali minacce alla sicurezza informatica attraverso lo studio degli Indicatori di Compromissione (IOC). Gli IOC sono evidenze di attacchi informatici in corso o già avvenuti, che permettono di individuare attività malevole e mitigare eventuali danni.

Questa relazione si basa sull'analisi di una cattura di rete ottenuta tramite Wireshark, al fine di identificare possibili compromissioni e fornire strategie di difesa efficaci.

Identificazione e Analisi degli IOC

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

- **Traffico sospetto sulle porte 80 (HTTP) e 443 (HTTPS)**: Si osservano numerosi pacchetti SYN inviati senza una corrispondente risposta ACK, suggerendo una possibile scansione delle porte o un tentativo di connessione illegittima.

- **Presenza di pacchetti TCP con flag RST (Reset)**: Un elevato numero di pacchetti RST può indicare un'attività di scansione aggressiva o un attacco di tipo Denial of Service (DoS).

- **Annuncio di rete da "Metasploitable"**: La presenza di Metasploitable nella rete suggerisce un ambiente di test vulnerabile, che potrebbe essere stato preso di mira per attività di exploit.

- **Comunicazioni ripetute tra lo stesso IP di origine e più porte di destinazione**: Questo comportamento è tipico di attacchi di port scanning effettuati con strumenti come Nmap.

Ipotesi sui Vettori di Attacco

Dall'analisi degli IOC possiamo ipotizzare che gli attacchi in corso siano riconducibili a:

1. **Scansione delle porte (Reconnaissance Phase)**: Un attaccante potrebbe essere alla ricerca di porte aperte e servizi vulnerabili tramite tecniche di SYN scan o ACK

scan.

2. **Tentativi di exploit su Metasploitable**: La macchina Metasploitable potrebbe essere il bersaglio di tentativi di sfruttamento di vulnerabilità note.

3. **Attacco DoS tramite pacchetti SYN**: L'alto numero di richieste SYN potrebbe indicare un tentativo di SYN Flooding, volto a esaurire le risorse del sistema bersaglio.

Contromisure per Mitigare l'Attacco

Per ridurre gli impatti dell'attacco attuale e prevenire attacchi futuri, si consiglia di implementare le seguenti contromisure:

- **Bloccare gli IP sospetti**: Configurare regole di firewall per bloccare indirizzi IP che generano traffico anomalo o riconducibile a scansioni.

- **Limitare il numero di richieste SYN per IP**: Utilizzare meccanismi di rate limiting per prevenire SYN Flooding.

- **Abilitare un sistema IDS/IPS**: Strumenti come Snort o Suricata possono rilevare e bloccare attività di scansione e tentativi di exploit.

- **Chiudere le porte non necessarie**: Limitare l'esposizione dei servizi e disabilitare quelli non indispensabili.

- **Monitorare i log di sistema e di rete**: Analizzare regolarmente i log di rete per individuare tempestivamente attività sospette.

Conclusione

L'analisi della cattura di rete ha permesso di identificare potenziali minacce, tra cui scansioni di rete e tentativi di attacco su una macchina vulnerabile. Implementando le contromisure sopra descritte, è possibile migliorare la postura di sicurezza della rete e mitigare futuri attacchi.

Questa esercitazione dimostra l'importanza della Threat Intelligence e dell'analisi degli IOC per proteggere le infrastrutture informatiche da minacce esterne.