Threat Intelligence & IOC

INDICE:

1. Obiettivo dell’analisi

L’obiettivo principale di questa analisi è identificare eventuali **Indicator of Compromise (IOC)** all'interno del file di cattura di rete `Cattura_U3_W1_L5.pcapng`, e determinare se siano presenti comportamenti anomali o malevoli. A tal fine, è stato utilizzato **Wireshark** come strumento di analisi, al fine di esaminare il traffico e individuare eventi sospetti.

2. Scenario della rete analizzata

L’intercettazione del traffico avviene in una rete interna, nella quale si osserva la comunicazione tra due host:

- **Host sorgente:** **192.168.200.100**
- **Host destinatario:** **192.168.200.150**

L’attività registrata è esclusivamente di tipo **TCP**. Le comunicazioni partono dall’host **`192.168.200.100`** verso una varietà di porte TCP dell’host **`192.168.200.150`**.

3. Indicator of Compromise (IOC)

Analizzando i pacchetti si evidenziano i seguenti indicatori:

- **Numerosi pacchetti SYN** provenienti da `192.168.200.100` verso porte TCP differenti su `192.168.200.150`, tra cui:
  - Porte comuni: 80 (HTTP)
  - Porte non standard: 4443, 63686, 52358, 56120, ecc.
- La maggior parte delle risposte ricevute da `192.168.200.150` sono pacchetti **RST, ACK**, che indicano che **le porte sono chiuse**.
- Il traffico non prosegue con handshakes completi o con lo scambio di dati applicativi, ma si limita alla fase iniziale della connessione TCP.

Questi comportamenti sono tipici di una **scansione delle porte TCP**, finalizzata a rilevare quali servizi siano in ascolto sull'host bersaglio.

4. Interpretazione e natura dell'attività osservata

Sulla base degli IOC rilevati, si può ragionevolmente affermare che l'host `192.168.200.100` stia eseguendo un'**attività di port scanning** nei confronti dell'host `192.168.200.150`.

Il port scanning è una tecnica di ricognizione impiegata comunemente in ambito sia offensivo (ricerca di vulnerabilità da parte di un attaccante) sia difensivo (mappatura della propria rete). In questo caso, la mancanza di traffico successivo al SYN e l'elevato numero di risposte RST, ACK confermano che l'intenzione era esclusivamente quella di verificare **la presenza di porte aperte**, senza avviare ulteriori attività malevole.

L'attività potrebbe essere stata effettuata con strumenti automatizzati come **Nmap**, configurato per effettuare uno **scan TCP SYN**, che è meno invasivo e più difficile da rilevare rispetto a uno scan completo.

5. Contromisure e raccomandazioni

Contromisure:

- **Monitorare l'attività dell'host 192.168.200.100**: accertarsi che l'attività di scanning sia stata autorizzata o eseguita in ambiente di test. In caso contrario, considerarla come una possibile attività malevola.
- **Bloccare o limitare il traffico verso porte non autorizzate** tramite firewall interni.
- **Isolare l'host sorgente** per effettuare ulteriori analisi forensi in caso di sospetto compromissione.

Misure preventive:

- **Implementare un sistema IDS/IPS** per rilevare attività di port scanning.
- **Segmentare la rete interna** tramite VLAN per limitare la visibilità tra host.
- **Effettuare controlli regolari sui log dei firewall e dei sistemi**.
- **Applicare una politica di accesso per porta**, limitando l'esposizione dei servizi solo agli host autorizzati.

---

6. Conclusione

L'analisi del file di cattura ha evidenziato una **scansione delle porte TCP** eseguita da un host interno verso un altro dispositivo della rete. Tale comportamento, pur non rappresentando una compromissione diretta, è una tecnica comunemente utilizzata durante la fase di ricognizione di un attacco informatico. Per questo motivo è essenziale monitorare, registrare e controllare sistematicamente queste attività, al fine di mantenere un buon livello di sicurezza e visibilità all'interno della rete.