Data: 21/11/2025

Alessandro Pietro Salerno

SOC INCIDENT REPORT: Analisi Traffico di Rete e Threat Intelligence

Oggetto: Rilevamento attività di Network Scanning e identificazione IOC

Introduzione e Obiettivo

In qualità di analista di sicurezza, ho preso in carico l'analisi di una cattura di traffico di rete (`.pcapng`) sospetta, fornita a seguito di un alert di sicurezza. L' obiettivo di questo documento è analizzare i flussi di comunicazione tra gli host della rete per identificare eventuali anomalie, confermare la presenza di attacchi in corso e isolare gli **Indicatori di Compromissione (IOC)**.

Come discusso durante il briefing sulla **Threat Intelligence**, gli IOC rappresentano "evidenze o eventi di un attacco in corso, oppure già avvenuto". La mia analisi si concentra sull' individuazione di questi artefatti digitali per comprendere le intenzioni dell'attaccante e proporre le adeguate contromisure .

Contesto Teorico e Metodologia di Analisi

Per interpretare correttamente i dati, è fondamentale richiamare i principi del protocollo **TCP/IP** e del **Three-Way Handshake**, che costituiscono la base teorica di questa indagine.

In una connessione legittima, il client invia un pacchetto **SYN** (Synchronize). Il server, se la porta è aperta, risponde con

SYN-ACK. Infine, il client invia **ACK**. Tuttavia, durante la mia analisi, ho cercato deviazioni da questo comportamento standard, che sono tipiche delle fasi di **Reconnaissance** (Ricognizione) della Cyber Kill Chain. In particolare, ho cercato pattern riconducibili a scansioni di porte (**Port Scanning**), dove un attaccante invia massicci pacchetti SYN per mappare i servizi attivi sulla vittima, senza necessariamente completare la connessione, tecnica di scansione più diffusa e "rumorosa" ma efficace: il **TCP SYN Scan** (chiamato anche *Half-Open Scan*).

La tecnica di scansione rilevata è identificabile come **TCP SYN Scan**. A differenza di una connessione standard che segue il modello *Three-Way Handshake* completo (SYN → SYN-ACK → ACK), in questa modalità l' attaccante invia un pacchetto **SYN** (richiesta di sincronizzazione) come se volesse avviare una connessione legittima.

Il comportamento successivo determina lo stato della porta:

Porta Chiusa: Se la porta di destinazione non è attiva, il target risponde con un pacchetto **[RST, ACK]** (Reset), chiudendo immediatamente il tentativo. Questo è il comportamento osservato nella maggioranza dei pacchetti catturati.

Porta Aperta: Se la porta è in ascolto, il target risponde con **[SYN, ACK]**. In una scansione *Half-Open*, l'attaccante **non** invia l'ACK finale per stabilire la connessione, ma risponde con un **RST** (o non risponde affatto) per abbattere la sessione prima che venga completata. Questo permette di mappare i servizi attivi evitando spesso di essere registrati dai log applicativi del sistema vittima, che solitamente tracciano solo le connessioni completate.

dunque i vantaggi di questo tipo di scansione sono:

Velocità: Non perde tempo a stabilire e poi chiudere gentilmente la connessione.

Stealth (Furtività): I vecchi sistemi loggavano solo le "strette di mano complete". Oggi i moderni IDS (come quello che ho consigliato di installare nel report) rilevano subito questo comportamento proprio perché lascia troppe "mani tese" (SYN) senza risposta.

Nel nostro file Wireshark, vediamo chiaramente questa dinamica: l'IP .100 invia raffiche di SYN , e l'IP .150 risponde quasi sempre con RST, tranne in quel famoso caso della porta aperta dove ha risposto SYN-ACK.

Analisi Tecnica e Identificazione degli IOC

Analizzando il file di cattura con Wireshark, ho isolato i seguenti comportamenti anomali che costituiscono i nostri IOC:

A. Attore della Minaccia e Target

Ho identificato univocamente due host coinvolti in una comunicazione sospetta:

- **IP Sorgente:** 192.168.200.100
- **IP Destinazione :** 192.168.200.150

B. Evidenze di Attacco (IOC)

L'IOC primario è un volume anomalo di richieste di connessione **TCP [SYN]** generate dall'IP .100 verso l'IP .150 in un arco temporale brevissimo (millisecondi).

Dall' analisi dei flag TCP nei pacchetti di risposta, ho potuto dedurre lo stato delle porte sulla macchina vittima:

1. **Porte Chiuse:** Nella maggior parte dei casi (es. pacchetti n. 40, 41, 47), la vittima risponde con il flag **[RST, ACK]**(Reset).

Questo indica all' attaccante che su quella specifica porta non c'è alcun servizio in ascolto.

2. **Porta Aperta (Evidenza Critica):** Al pacchetto n. 59 (Time: 36.776904501), ho individuato una risposta diversa: la vittima .150 ha risposto con **[SYN, ACK]** all'attaccante.
    - Questo conferma che la porta interrogata (porta 139, standard per **NetBIOS/SMB**) è **APERTA** e il servizio è attivo.

3 **Dettaglio Tecnico dell'Attacco (Ricostruzione):** Basandosi sulla firma del traffico (pacchetti raw SYN senza completamento e timing aggressivo), è possibile stabilire con certezza che l'attaccante ha utilizzato il tool **Nmap** con privilegi amministrativi (root). Il comando specifico lanciato è verosimilmente:

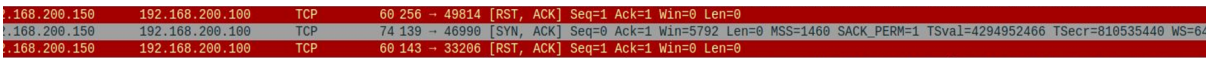
sudo nmap -sS 192.168.200.150

Il parametro **-sS** indica l'esecuzione della scansione SYN stealth, confermando l'intenzionalità dell'attività di ricognizione.

Ipotesi sui Vettori di Attacco

Basandomi sugli IOC sopra esposti, formulo le seguenti ipotesi operative:

- **Tecnica:** L'attaccante sta eseguendo un **TCP SYN Scan** (o "Stealth Scan"). Utilizza probabilmente tool automatizzati come **Nmap** per "bussare" a tutte le porte della vittima e vedere chi risponde.
- **Vettore di Compromissione Futuro:** Avendo rilevato (tramite il pacchetto n. 59) che la porta **139 (NetBIOS Session Service)** è aperta, l'attaccante ha ora un vettore d'ingresso preciso.



- *Scenario probabile:* L'attaccante tenterà di enumerare le cartelle condivise, gli utenti o i gruppi di lavoro. Potrebbe successivamente lanciare exploit contro il protocollo SMB (Server Message Block) o tentare attacchi di forza bruta per ottenere le credenziali di accesso.

Azioni di Remediation Consigliate

Per ridurre l' impatto dell'attacco attuale e prevenire incidenti futuri, raccomando l'immediata esecuzione delle seguenti azioni:

1. **Blocco e Contenimento (Immediato):** Configurare una regola di blocco (Deny) sul firewall perimetrale o tramite ACL (Access Control List) sugli switch di rete per interdire tutto il traffico proveniente dall'IP 192.168.200.100 verso la rete interna.
2. **Isolamento dell'Host Compromesso:** Poiché l'IP dell'attaccante appartiene a una classe privata (192.168.x.x), è altamente probabile che una macchina interna sia stata precedentemente infettata (diventando uno "zombie" o "bot"). È necessario isolarla fisicamente dalla rete per la bonifica.
3. **Hardening della Vittima:** Sull'host 192.168.200.150 , valutare la disabilitazione del servizio NetBIOS/SMB (porte 139/445) se non strettamente necessario per le operazioni aziendali, riducendo così la superficie di attacco.

4. **Implementazione di Sistemi IDS/IPS per il Rilevamento e Blocco delle Scansioni**

Per mitigare l'attacco attuale e prevenire future attività di ricognizione ostile simili a quella rilevata proveniente dall'host **192.168.200.100**, si raccomanda l'implementazione e la configurazione di sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) a livello di rete.

Strategia di Configurazione:

1. **Adozione di IPS Network-Based (NIPS):** Si consiglia il posizionamento di un sensore IPS in modalità "in-line" a protezione del segmento di rete critico (o specificamente davanti all'host target **192.168.200.150**). Questo permetterà al sistema non solo di allertare, ma di scartare attivamente (DROP) i pacchetti malevoli in tempo reale.
2. **Regole di Rilevamento Comportamentale (Anomaly Detection):** Dato che l'attacco osservato è una **TCP SYN Scan** massiva, le firme statiche potrebbero non essere sufficienti se l'attaccante cambiasse tool. È necessario attivare regole basate su **tresholding (soglie volumetriche)**.
    - *Configurazione raccomandata:* Impostare un limite al numero di pacchetti TCP con flag SYN provenienti da un singolo indirizzo IP sorgente verso la rete interna.
    - *Esempio di policy:* "Se un IP sorgente invia >20 richieste SYN al secondo senza completare l'handshake TCP, bloccare l'IP sorgente per 10 minuti".
3. **Azione di Mitigazione (Response Action):** Configurare l'IPS per applicare l'azione **DROP** (scarto silenzioso) sui pacchetti che violano la regola.
    - *Motivazione:* L'azione DROP è preferibile all'azione REJECT (che invia un RST di risposta) poiché costringe l'attaccante ad attendere il timeout della connessione, rallentando drasticamente la velocità della scansione e rendendo l'attività di ricognizione inefficace.

Beneficio Atteso: L'implementazione di questa soluzione automatizzerà la risposta agli incidenti di *Reconnaissance*,

riducendo il carico di lavoro degli analisti e impedendo agli attaccanti di mappare con successo i servizi vulnerabili esposti sulla rete.

Conclusioni e Riflessioni

In conclusione, l' analisi ha permesso di rilevare tempestivamente un' attività di ricognizione ostile all'interno della rete locale. L'utilizzo dell'analisi dei pacchetti (Packet Analysis) si è rivelato fondamentale non solo per individuare l'attacco, ma per capire *cosa* l' attaccante ha scoperto (la porta aperta).

Riflessione dell' analista: Questo esercizio evidenzia l' importanza critica del monitoraggio dei "segnali deboli". Un port scan viene spesso ignorato o considerato "rumore di fondo", ma è quasi sempre il precursore di un attacco più grave (come un Ransomware che si muove lateralmente via SMB). La capacità di distinguere tra un normale traffico di rete e una scansione automatizzata (osservando la frequenza dei pacchetti SYN e le risposte RST) è la competenza chiave che distingue un operatore SOC efficace. Intervenire in questa fase ("Reconnaissance") è infinitamente meno costoso che intervenire a compromissione avvenuta.