Analisi di Threat Intelligence e Identificazione IOC da Cattura di Rete: Rilevamento di Scansione Porte Interna

Michele Storelli

Indice

1 Introduzione

Il presente documento ha lo scopo di analizzare una cattura di traffico di rete, precedentemente effettuata tramite Wireshark, al fine di identificare potenziali Indicatori di Compromissione (IOC), vettori di attacco e proporre strategie di mitigazione e risposta. L'analisi si concentra su un'attività anomala rilevata tra due host interni alla medesima rete, suggerendo la necessità di una valutazione approfondita della sicurezza perimetrale e interna.

2 Analisi del Traffico di Rete e Identificazione degli IOC

Dall'esame preliminare della cattura di rete, emerge un volume significativo di traffico sospetto originato dall'indirizzo IP **192.168.200.100** e diretto verso l'IP di destinazione **192.168.200.150**. Entrambi gli host appartengono alla subnet `192.168.200.0/24`, indicando un'attività interna.

Gli Indicatori di Compromissione (IOC) principali identificati sono:

- **Elevato numero di pacchetti TCP SYN:** L'host `192.168.200.100` invia una sequenza rapida di pacchetti `SYN` verso molteplici porte dell'host `192.168.200.150`.
- **Mancato completamento dell'handshake a tre vie:** Per la maggior parte di queste richieste `SYN`, non segue un `SYN, ACK` dall'iniziatore per completare la connessione, oppure l'host target risponde direttamente con `RST, ACK`.
- **Risposte TCP RST, ACK:** L'host `192.168.200.150` risponde a molte delle richieste `SYN` con pacchetti `RST, ACK`, tipico comportamento quando una porta è chiusa o il servizio non è in ascolto.
- **Dimensione specifica dei pacchetti SYN:** Molti pacchetti `SYN` presentano una dimensione di **74 byte**. Questa dimensione suggerisce la presenza di opzioni TCP aggiuntive (come MSS, Window Scaling, Timestamp) spesso utilizzate da tool di scansione per ottenere maggiori informazioni sui servizi o per fingerprinting del sistema operativo.
- **Rapidità dell'attività:** L'intera sequenza di invio dei pacchetti e delle relative risposte si svolge in un lasso di tempo estremamente breve (pochi istanti o secondi), indicativo di un processo automatizzato e aggressivo.
- **Utilizzo di filtri Wireshark:** Per isolare e confermare queste osservazioni, sono stati applicati filtri specifici.

3 Identificazione della Minaccia e Vettore d'Attacco

Sulla base degli IOC raccolti, l'attività osservata è riconducibile con alta probabilità a una **scansione di porte (Port Scan)**. Questo tipo di attacco è comunemente utilizzato nella fase di ricognizione per identificare porte aperte, servizi attivi e loro versioni, ed eventuali vulnerabilità sfruttabili sull'host target.

Il tool sospettato di essere stato utilizzato è **Nmap**, uno strumento molto diffuso per l'auditing di rete e le scansioni di sicurezza. Le caratteristiche del traffico, come l'uso di opzioni TCP avanzate e la velocità, sono compatibili con comandi Nmap quali:

- `nmap -sS 192.168.200.150`: SYN Scan (o "half-open scan"), che invia pacchetti SYN e analizza le risposte senza completare la connessione, rendendolo più furtivo.
- L'opzione `-sV` (version detection) potrebbe essere stata usata per tentare di identificare le versioni dei servizi, spiegando le opzioni TCP aggiuntive.
- L'aggressività della scansione suggerisce l'uso di opzioni di timing come `-T4` o `-T5`.

Considerazione critica: Il fatto che l'attacco provenga da un IP interno (`192.168.200.100`) è di particolare rilevanza. Ciò implica due scenari principali:

1. **Minaccia Interna:** Un utente malintenzionato con accesso legittimo alla rete sta conducendo la scansione.
2. **Host Interno Compromesso:** Una macchina all'interno della rete è stata compromessa da un malware o da un attaccante esterno, che la sta utilizzando come testa di ponte per attività di ricognizione interna.

Questa scansione ha lo scopo di raccogliere informazioni sullo stato delle porte del sistema `192.168.200.150`.

4 Azioni di Mitigazione e Risposta Consigliate

Si raccomanda un approccio multifasico per gestire questa minaccia:

4.1 Fase 1: Contenimento Immediato

- **Isolamento dell'Host Sorgente:** Se l'attività è chiaramente dannosa e in corso, considerare l'isolamento temporaneo dell'host `192.168.200.100` dalla rete per prevenire ulteriori danni, previa valutazione dell'impatto operativo.
- **Regole Firewall:** Implementare o rafforzare regole firewall sull'host target (`192.168.200.150`) per bloccare connessioni anomale e tentativi di scansione provenienti da `192.168.200.100` o pattern di scansione generici. È possibile configurare il firewall per limitare il numero di connessioni incomplete da una singola sorgente in un breve periodo.

4.2 Fase 2: Indagine Approfondita

- **Analisi dell'Host Sorgente (`192.168.200.100`):** È fondamentale investigare questo host per determinare la causa della scansione:
  - Verificare la presenza di malware o tool di scansione non autorizzati.
  - Analizzare i log di sistema e di sicurezza.
  - Intervistare l'utente abituale della macchina, se applicabile, per capire se l'attività è stata intenzionale o accidentale.
- **Analisi dell'Host Target (`192.168.200.150`):** Verificare i log per confermare i tentativi di connessione e identificare eventuali porte aperte che potrebbero essere state scoperte.

4.3 Fase 3: Misure Correttive e Preventive a Lungo Termine

- **Configurazione di Sistemi IDS/IPS (Intrusion Detection/Prevention System):** Implementare o aggiornare firme sui sistemi per rilevare e potenzialmente bloccare automaticamente pattern di traffico riconducibili a scansioni di porte (es. rilevamento di Nmap basato su opzioni TCP, frequenza delle connessioni, ecc.).
- **Rate Limiting:** Implementare meccanismi di rate limiting a livello di firewall o host per limitare la velocità delle connessioni da una singola sorgente, rendendo le scansioni aggressive meno efficaci e più facili da rilevare.
- **Hardening dei Sistemi:**
  - Mantenere tutti i sistemi e i servizi aggiornati con le ultime patch di sicurezza.
  - Disabilitare o disinstallare servizi e porte non necessari per ridurre la superficie d'attacco.
  - Configurare i servizi in ascolto solo sulle interfacce di rete strettamente necessarie.
- **Implementazione di Honeypots:** Considerare l'uso di honeypot per attirare e analizzare tentativi di scansione e altre attività malevole, fornendo early warning e intelligence.
- **Segmentazione della Rete:** Rafforzare la segmentazione della rete per limitare la capacità di un host compromesso di muoversi lateralmente e scansionare altre porzioni della rete.
- **Formazione e Sensibilizzazione del Personale:** Educare gli utenti sulle policy di sicurezza, sull'uso corretto degli strumenti di rete e sui rischi associati a software non autorizzato o comportamenti negligenti.
- **Monitoraggio Continuo:** Monitorare regolarmente i log di firewall, IDS/IPS e dei sistemi per identificare tempestivamente attività sospette.

5 Conclusioni

L'analisi del traffico di rete ha rivelato una chiara attività di scansione di porte originata dall'interno della rete, probabilmente effettuata tramite Nmap. Questo evento sottolinea l'importanza non solo della sicurezza perimetrale, ma anche della vigilanza contro minacce interne o host compromessi. L'adozione di un approccio difensivo stratificato, che includa controlli tecnici, procedure di risposta agli incidenti e formazione del personale, è cruciale per ridurre l'impatto di tali attacchi e migliorare la postura di sicurezza complessiva dell'organizzazione. L'indagine sull'host sorgente è il passo successivo più critico per determinare la natura esatta della minaccia.