Progetto S9L5

Obbiettivo:

- 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

Analizzando le catture di rete effettuate con Wireshark emergono numerosi Indicatori di Compromissione (IOC). Si può risalire ad un’attività sospetta e persistente che indica una fase di ricognizione, ovvero una scansione delle porte.

Panoramica del Traffico

Attori principali:

- **192.168.200.100** (computer/client)
- **192.168.200.150** (server/target)

Pattern di Comunicazione Osservato (IPOTESI)

1. Handshake TCP Iniziale

Nei primi pacchetti vedo il classico three-way handshake:

- **SYN** dal client (.100) al server (.150)
- **SYN, ACK** di risposta dal server
- **ACK** finale per completare la connessione

2. Trasferimento Dati Intensivo

Il traffico mostra:

- **Pacchetti di grandi dimensioni** (molti sono 74+ KB)
- **Sequenze continue** di [SYN], [ACK], [RST]
- **TSval (Timestamp Values)** progressivi che indicano una sessione continua
- **Window scaling** attivo (WS=128, WS=64)

3. Anomalie Interessanti

A) Reset Connection Frequenti: Vedo molti pacchetti **[RST, ACK]** che indicano connessioni terminate bruscamente. Questo potrebbe suggerire:

- Timeout di connessione
- Rifiuto di connessioni
- Possibile attacco o scansione

B) Pattern Ripetitivo: Le connessioni sembrano seguire un pattern ciclico, tipico di:

- **Brute force attack**
- **Port scanning**
- **DoS/DDoS attempt**
- **Automated tool** in azione

Possibili Scenari

Scenario 1: Attacco Brute Force

Il pattern di connessioni multiple rapide con reset potrebbe indicare un tentativo di brute force su un servizio.

Scenario 2: Port Scanning

Le connessioni rapide e i reset potrebbero essere un port scan avanzato.

Scenario 3: Trasferimento File

I pacchetti di grandi dimensioni potrebbero indicare un trasferimento file o un tentativo di DOS.

Possibile Scenario

Tra le varie ipotesi, la più probabile è l'attacco DoS. Questo sospetto si manifesta nel tentativo ripetuto e continuativo di richieste di comunicazione che si concretizzano nell'invio di pacchetti di grandi dimensioni, secondo un principio di flooding.

Azioni Raccomandate

Se l'ipotesi, con ulteriori analisi, si dovesse dimostrare corretta, consiglierei:

Azioni immediate:

- Implementare rate limiting per limitare il numero di richieste per IP/sorgente
- Configurare filtri di traffico per bloccare pacchetti anomali o di dimensioni eccessive
- Attivare sistemi di monitoraggio del traffico in tempo reale
- Implementare blacklisting automatico degli IP sospetti

Analisi approfondita:

- Analizzare i log per identificare pattern ricorrenti e sorgenti dell'attacco
- Verificare la distribuzione geografica del traffico anomalo
- Controllare se si tratta di attacco coordinato (botnet) o sorgente singola

Misure di mitigazione:

- Utilizzare servizi CDN con protezione DDoS
- Configurare firewall con regole specifiche anti-flooding
- Implementare sistemi di load balancing per distribuire il carico
- Considerare l'uso di servizi cloud con protezione DDoS integrata

finale

Queste conclusioni sono dipendenti dall'esperienza e dai casi, nel senso che la mia esperienza non può definiri sufficiente (per ora) e che questo caso non è realistico ma simulato; per consigliare soluzioni efficaci dovrei tenere conto di un ipotetico caso reale.