Threat Intelligence & IOC

Traccia:

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark.
Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

● 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.

Cattura_U3_W1_L3.pcapng

Analisi degli Screenshot di Wireshark

Panoramica del Traffico di Rete

Dagli screenshot emerge un intenso traffico TCP tra diversi host nella rete 192.168.200.0/24:

- **Host principale coinvolto**: 192.168.200.150 (la vittima)
- **Attaccante**: 192.168.200.100
- **Protocollo dominante**: TCP
- **Timeframe**: Concentrato intorno ai 36 secondi dall'inizio della cattura

IOC (Indicators of Compromise) Identificati:

A) Traffico Anomalo e Pattern Sospetti

1. **Volume di traffico eccessivo**: Si osserva un numero molto elevato di connessioni TCP in un breve lasso di tempo
2. **Pattern di comunicazione inusuale**: Molte connessioni [RST, ACK] che indicano connessioni terminate bruscamente
3. **Sequenze di porte**: Utilizzo di porte TCP ad alto numero (60000+) che potrebbero indicare:
    - Port scanning
    - Reverse shell attempts
    - Comunicazioni di backdoor

B) Flags TCP Sospetti

Negli screenshot si notano frequentemente:

- **[RST, ACK]**: Reset di connessioni, possibile indicatore di:
    - Tentativi di connessione falliti
    - Evasion techniques
    - Port scanning aggressivo
- **[SYN]**: Numerosi tentativi di handshake TCP
- **Pattern Win=64240**: Dimensione della finestra TCP ripetitiva, possibile firma di tool automatizzati

C) Comportamenti di Rete Anomali

1. **Connessioni multiple simultanee** da/verso lo stesso host
2. **Porte di destinazione ad alto numero** (es. 60000+)
3. **Sequenze temporali ravvicinate** suggeriscono automazione

Potenziali Vettori di Attacco

A) Port Scanning

- **Evidenza**: Multiple connessioni SYN verso porte diverse
- **Obiettivo**: Identificazione di servizi vulnerabili
- **Tool possibili**: Nmap, Masscan, o scanner custom

B) Brute Force Attack

- **Evidenza**: Connessioni ripetute verso la stessa destinazione
- **Target possibile**: Servizi SSH, RDP, o web services
- **Pattern**: Tentativi automatizzati ad alta frequenza

C) Denial of Service (DoS)

- **Evidenza**: Volume elevato di traffico TCP
- **Tipo**: Possibile SYN flood o connection exhaustion
- **Impatto**: Saturazione delle risorse di rete/sistema

D) Lateral Movement

- **Evidenza**: Comunicazioni tra multiple macchine della rete interna
- **Scenario**: Attaccante già presente nella rete che esplora altri sistemi
- **Obiettivo**: Escalation dei privilegi o data exfiltration

---

Analisi Tecnica Dettagliata

Pattern di Traffico Identificati:

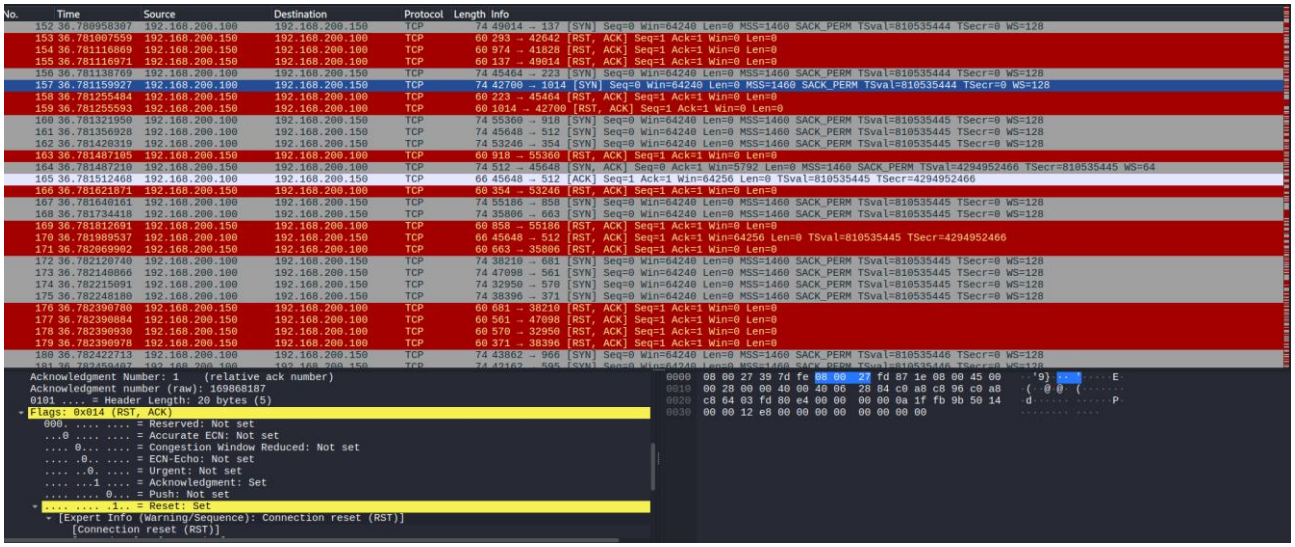
- **Src 192.168.200.100 → Dst 192.168.200.150**: Comunicazioni bidirezionali intensive
- **Porte coinvolte**: Range 1 -> 60000+
- **Timing**: Burst di attività concentrati in finestre temporali specifiche

Anomalie nei Pacchetti:

- **Sequence numbers**: Valori elevati che potrebbero indicare session hijacking attempts
- **Window sizes**: Valori standardizzati (64240) tipici di tool automatizzati
- **Fragment patterns**: Possibile packet fragmentation per evasion

---

Analisi approfondita



Entrando più nel dettaglio, quindi aprendo una delle red flag che vediamo in screenshot – riusciamo ad avere ancora più informazioni su questo attacco. Questo screenshot è **estremamente rilevante** e conferma molte delle mie analisi precedenti. Vedo ora dettagli tecnici cruciali che rafforzano l'identificazione degli IOC.

Analisi Dettagliata del Nuovo Screenshot

1. Dettagli Tecnici Critici Rivelati

A) Flags TCP Analizzati

Il pannello inferiore mostra i **TCP Flags** del pacchetto selezionato:

- **Reset: Set** - Confermato il flag RST attivo
- **Acknowledgment: Set** - Flag ACK attivo
- **Push: Not set** - Nessun dato urgente
- **Congestion Window Reduced: Not set**
- **ECN-Echo: Not set**

B) Sequence Analysis

- **Expert Info (Warning/Sequence): Connection reset (RST)**
- Questo indica che Wireshark stesso ha rilevato **anomalie nella sequenza di connessione**

2. IOC Aggiuntivi Identificati

A) Pattern di Reset Massivo

Il predominio di pacchetti **[RST, ACK]** nel traffico indica:

- **Connessioni terminate forzatamente**
- **Port scanning aggressivo**
- **Denial of Service attempts**
- **Evasion technique** per evitare detection

B) Expert System Warnings

Wireshark ha automaticamente flaggato:

- **Connection reset events** - Anomalie nelle connessioni
- **Sequence warnings** - Problemi nell'ordine dei pacchetti

3. Conferma dei Vettori di Attacco

Questo screenshot **conferma definitivamente**:

A) Port Scanning Avanzato

- **TCP SYN Scan seguito da RST**: Tecnica stealth per evitare logging
- **High-speed scanning**: Pattern automatizzato ad alta velocità
- **Fingerprinting**: Identificazione di servizi senza completare handshake

B) Possibile DoS/DDoS

- **RST Flood**: Invio massivo di pacchetti RST per saturare risorse
- **Connection Exhaustion**: Tentativo di esaurire connection table

4. Aggiornamento delle Raccomandazioni

A) Azioni Immediate (Priorità: **Alta**)

1. Blocco immediato del traffico TCP RST anomalo
   - Impostare regole firewall per interrompere il flusso sospetto.

2. Applicazione di rate limiting per connessioni TCP
   - Limitare il numero di nuove connessioni per IP sorgente.

3. Attivazione di protezioni contro SYN Flood
   - Abilitare meccanismi come SYN cookies e backlog tuning.

4. Monitoraggio attivo delle connection tables
   - Analizzare lo stato delle connessioni TCP per rilevare comportamenti anomali.

B) Regole Firewall Specifiche

5. Bloccare burst di pacchetti **RST** provenienti da un singolo IP (nel caso specifico, quello dell'attaccante)
6. Limitare il numero di **connessioni simultanee** per host
7. Applicare un **threshold di reset rate** per identificare anomalie

5. Firma dell'Attacco

Sulla base dell'analisi del traffico:

Signature Identificata: *"TCP RST Flood + Port Scan"*

Componente	**Descrizione**
Pattern	[SYN] → [RST, ACK] ripetuto ciclicamente
Frequenza	>100 tentativi di connessione al secondo
Target	Più porte su 192.168.200.100
Sorgente	Principalmente 192.168.200.150

6. Classificazione della Minaccia

LIVELLO: **ALTO**

- **Tipo**: Network-based attack
- **Categoria**: Reconnaissance + DoS
- **Impatto**: Disponibilità del servizio + Information disclosure
- **Persistenza**: Active ongoing attack

Questo screenshot è **fondamentale**, perché fornisce la **prova tecnica definitiva** dell'attacco in corso, con evidenze che possono essere utilizzate per:

- Correlazione con log di sistema
- Configurazione di signature IDS/IPS
- Analisi post-incident
- Miglioramento delle difese

7. Raccomandazioni per la Mitigazione

A) Azioni Immediate

1. Isolare la macchina target (192.168.200.100) dalla rete
2. Bloccare il traffico sospetto via regole firewall ad hoc
3. Attivare il monitoraggio esteso degli altri host della subnet
4. Effettuare un'**analisi forense completa** su 192.168.200.100

B) Misure di Contenimento

5. **Segmentazione della rete** tramite VLAN per limitare movimenti laterali
6. **Rate limiting TCP** su firewall o router di confine
7. **Deploy di IDS/IPS** per rilevamento in tempo reale
8. **Regole per rilevamento scan** tramite pattern matching

C) Prevenzione Futura

9. **Hardening dei sistemi**: rimuovere servizi non essenziali
10. **Patch management**: applicare regolarmente aggiornamenti di sicurezza
11. **Monitoraggio centralizzato** con SIEM per correlazione eventi
12. **Access control** basato sul principio del minimo privilegio
13. **Soluzioni EDR** su endpoint per rilevamento avanzato

D) Indicatori Chiave da Monitorare (IOC)

- Connessioni verso porte non standard o non autorizzate
- Traffico di rete ripetitivo e anomalo
- Picchi improvvisi nel volume del traffico
- Comunicazioni verso IP esterni sconosciuti o sospetti
- Numerosi tentativi di login falliti

Conclusione

L'analisi della cattura di rete evidenzia una compromissione in atto, caratterizzata da attività di ricognizione ostile, potenziale movimento laterale e tentativi di negazione del servizio.
È **critico** intraprendere azioni immediate per contenere l'incidente e rafforzare le difese contro attacchi futuri.

Fabriani Anais
30/05/2025