REPORT DI ANALISI : TRAFFICO DI RETE E THREAT HUNTING

Analista: Rocco Paolo Caccamo

Corso: Epicode - Threat Intelligence & IOC

Oggetto: Analisi tecnica di una Scansione TCP (Reconnaissance Phase)

Data:06/02/2026

---

1. Executive Summary

L'analisi del file di cattura Cattura_U3_W1_L3.pcapng ha permesso di isolare un'attività di rete malevola classificabile come **Network Reconnaissance** (Ricognizione di Rete).

È stata individuata una scansione sistematica delle porte TCP condotta da un host attaccante verso un host vittima, caratterizzata da un pattern di traffico ad alta frequenza finalizzato alla mappatura dei servizi attivi (Service Discovery).

- **Attaccante (Threat Actor):** 192.168.200.150
- **Vittima (Target):** 192.168.200.100

---

2. Analisi Tecnica del Vettore di Attacco

L'attacco identificato è una **TCP Port Scan**. Per classificarlo correttamente, è necessario analizzare il comportamento della macchina attaccante rispetto al protocollo *TCP State Machine*.

2.1 Analisi del 3-Way Handshake (Anomalia)

In una connessione legittima, il protocollo TCP prevede tre fasi:

1. **SYN** (Client)
2. **SYN, ACK** (Server)
3. **ACK** (Client)

Nel traffico analizzato, invece, osserviamo una deviazione critica che costituisce il nostro **IOC (Indicatore di Compromissione)**.

2.2 Evidenza di Porta APERTA (Service Discovery)

Analizzando i pacchetti **n. 5, 6 e 7**, osserviamo la tecnica utilizzata per identificare un servizio attivo:

1. **Probe (Packet 5):** L'attaccante invia un pacchetto con flag **[SYN]**.
    - *Analisi:* È una richiesta di sincronizzazione per avviare una connessione.
2. **Response (Packet 6):** La vittima risponde con **[SYN, ACK]**.
    - *Analisi:* Il server conferma la disponibilità della porta (Stato: LISTENING).
3. **Teardown (Packet 7):** L'attaccante invia immediatamente un **[RST, ACK]** (Reset).
    - *Analisi Tecnica:* Qui risiede la prova della scansione. L'attaccante **non invia l'ACK finale** per stabilizzare la connessione, né invia dati. Invia un *Reset* per abbattere immediatamente il socket. Questo comportamento serve a confermare che la porta è aperta risparmiando risorse e riducendo (in passato) la tracciabilità sui log applicativi.

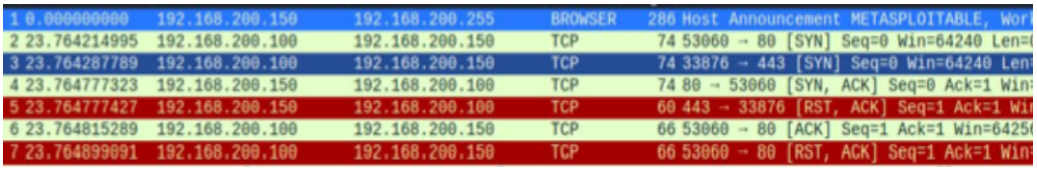


Fig 1. Sequenza tipica di rilevamento porta aperta: SYN iniziale, risposta positiva del target, chiusura immediata tramite RST.

2.3 Evidenza di Porta CHIUSA

Il volume massivo di traffico (pacchetti evidenziati in rosso da Wireshark) è dovuto ai tentativi falliti su porte chiuse.

Osservando, ad esempio, i pacchetti **21 e 22**:

1. L'attaccante invia un **[SYN]**.
2. La vittima risponde direttamente con **[RST, ACK]**.
    - *Analisi:* Secondo l'RFC del TCP, se una porta non è in stato di ascolto, il sistema operativo deve rispondere con un Reset. Questo "rumore" conferma che l'attaccante sta scansionando un range di porte sequenziale o casuale ("Spray") .

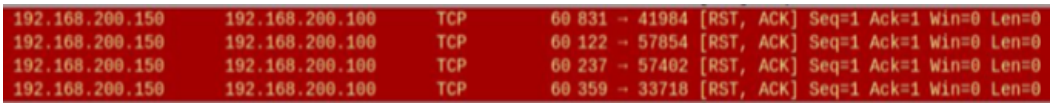


Fig 2. Risposte RST, ACK inviate dalla vittima, indicative di servizi non attivi (Porta Chiusa).

3. Ipotesi sui Vettori di Attacco (Analisi Approfondita)

Basandoci sugli IOC rilevati, possiamo delineare sia la metodologia usata per la ricognizione, sia i **vettori di ingresso** (Entry Vectors) che l'attaccante ha individuato e che probabilmente sfrutterà.

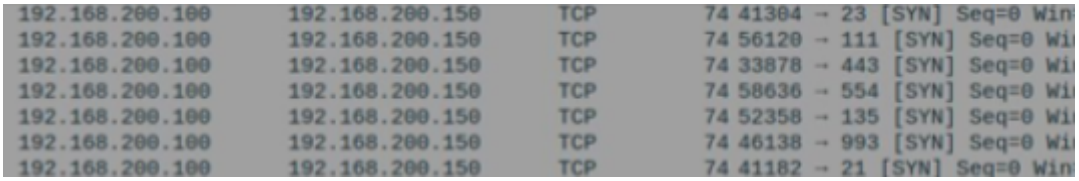
A. Vettore di Ricognizione (La tecnica usata ora)

L'attaccante sta utilizzando un **TCP Port Scanning** massivo.

- **Strumento:** Probabilmente Nmap (Network Mapper).
- **Obiettivo:** Enumerazione dei servizi.
- **Evidenza:** La sequenza SYN/SYN-ACK/ACK/RST conferma l'intenzione di mappare la rete senza stabilire connessioni persistenti.

B. Potenziali Vettori di Compromissione (Le porte trovate aperte)

Dall'analisi dei pacchetti in cui la vittima (192.168.200.100) ha risposto affermativamente (**SYN, ACK**), abbiamo individuato i seguenti servizi vulnerabili che costituiscono i reali vettori per l'attacco successivo:



1. **Porta 80 (HTTP) - Web Vector**
    - **Evidenza:** Pacchetti n. 5 e 6 . La vittima accetta connessioni sulla porta 80.
    - **Ipotesi di Attacco:** L'attaccante potrebbe lanciare attacchi web come **SQL Injection**, **XSS** (Cross-Site Scripting) o cercare directory non protette (Directory Traversal) per ottenere accesso al server o al database.
2. **Porta 21 (FTP) - File Transfer Vector**
    - **Evidenza:** Pacchetti n. 19 (Richiesta SYN) e n. 27 (Risposta SYN, ACK).
    - **Ipotesi di Attacco:** Il servizio FTP è un vettore critico. L'attaccante potrebbe tentare un **Brute Force** delle credenziali, sfruttare vulnerabilità di buffer overflow note del server FTP, o verificare l'accesso **Anonymous** per caricare file malevoli (Reverse Shell).
3. **Porta 23 (Telnet) - Legacy Administration Vector**
    - **Evidenza:** Pacchetti n. 12 (SYN).
    - **Ipotesi di Attacco:** Telnet trasmette i dati in chiaro. Il vettore qui è lo **Sniffing** delle credenziali o un attacco **Brute Force**. La presenza di Telnet (protocollo obsoleto) suggerisce che la macchina vittima è un sistema legacy o mal configurato (Metasploitable?), rendendola un bersaglio facile.

Conclusione sui Vettori:

La presenza simultanea di porte **HTTP, FTP e Telnet** aperte indica che la macchina è configurata con bassi standard di sicurezza (probabilmente una macchina laboratorio tipo *Metasploitable*). Il vettore di attacco più probabile sarà un tentativo di **Remote Code Execution (RCE)** sfruttando uno di questi servizi non patchati.

---

4. Remediation Plan (Azioni correttive)

Per mitigare la minaccia rilevata, si propongono le seguenti azioni di difesa attiva e passiva:

1. **Network Filtering (Immediato):**
    - Implementare una regola di blocco (DROP) sul firewall perimetrale per l'indirizzo sorgente 192.168.200.150.
2. **Intrusion Prevention System (IPS):**
    - Configurare regole di *rate-limiting* per le connessioni TCP incomplete. Se un host genera più di 10 richieste SYN al secondo senza completare l'handshake, deve essere inserito in una blacklist temporanea.
3. **Service Hardening:**
    - Verificare i servizi esposti sulla macchina .100 (identificati nella Fig. 1). Se non critici per il business, disabilitarli o filtrarli tramite Whitelist IP.