Report Analisi Traffico TCP con Wireshark/tcpdump

Michele Storelli

10 Giugno 2025

Analisi Pacchetto 1 (SYN)

- **Porta TCP di origine:** 53078
- **Classificazione porta di origine:** Effimera/Dinamica/Privata
- **Porta TCP di destinazione:** 80
- **Classificazione porta di destinazione:** Ben nota (HTTP)
- **Flag impostato:** SYN
- **Numero di sequenza relativo:** 0

Analisi Pacchetto 2 (SYN-ACK)

- **Porte di origine e destinazione:** Origine: 80, Destinazione: 53078
- **Flag impostati:** SYN, ACK
- **Numero di sequenza relativo:** 0
- **Numero di acknowledgment relativo:** 1

Analisi Pacchetto 3 (ACK)

- **Flag impostato:** ACK

Opzione `-r` (in `tcpdump`)

L'opzione `-r` in `tcpdump` permette di **leggere pacchetti da un file di cattura** precedentemente salvato.

Domande di Riflessione

1. Tre filtri Wireshark utili a un amministratore di rete

- `ip.addr == X.X.X.X`: Isola il traffico da/verso un IP specifico.
- `tcp.flags.syn == 1 and tcp.flags.ack == 0`: Identifica pacchetti SYN iniziali (utile per troubleshooting connessioni, scansioni).
- `port XX` **(es.** `tcp.port == 80`**)**: Visualizza traffico relativo a una specifica porta/servizio.

2. Altri utilizzi di Wireshark in una rete di produzione

- **Diagnosi e Risoluzione dei Problemi**: Connettività, latenza, perdita pacchetti, errori configurazione.
- **Analisi delle Prestazioni**: Utilizzo banda, tempi risposta applicativi, colli di bottiglia TCP.
- **Sicurezza della Rete**: Rilevamento attacchi (scansioni, DoS), analisi forense, monitoraggio attività sospette.
- **Debugging Applicazioni**: Analisi interazioni client-server, problemi autenticazione, flussi protocollo.