REPORT LABORATORIO: Analisi del Traffico TCP e Handshake a 3 Vie

Parte 1: Analisi Wireshark dell'Handshake TCP

In questa sezione, dissezioniamo i primi tre pacchetti catturati da Wireshark per vedere come viene stabilita la connessione tra il client (PC) e il server web.

1. Analisi del Primo Pacchetto (Il SYN)

Il primo pacchetto rappresenta la richiesta di inizio connessione inviata dal Client al Server.

- **Qual è il numero di porta TCP di origine?**
  - **58716**
- **Come classificheresti la porta di origine?**
  - Questa è una **Porta Dinamica o Privata** (Ephemeral Port).
  - *Il commento dell'esperto:* Le porte da 49152 a 65535 sono porte effimere assegnate dinamicamente dal sistema operativo al browser per gestire la sessione temporanea.
- **Qual è il numero di porta TCP di destinazione?**
  - **80**
- **Come classificheresti la porta di destinazione?**
  - Questa è una **Porta Ben Nota** (Well-Known Port).
  - *Il commento dell'esperto:* La porta 80 è standard per il traffico HTTP non crittografato. Il server rimane in ascolto su questa porta attendendo connessioni.
- **Quale flag è impostato?**
  - Il flag impostato è **SYN** (0x002).
  - *Significato:* Indica "Synchronize". Il client vuole sincronizzare i numeri di sequenza per avviare la comunicazione.
- **A quale valore è impostato il numero di sequenza relativo?**
  - **0**. (Wireshark mostra 0 come numero relativo per facilitare la lettura; il numero reale è un valore casuale a 32 bit).

---

2. Analisi del Secondo Pacchetto (Il SYN-ACK)

Il secondo pacchetto è la risposta del Server, che accetta la connessione e propone la sua sincronizzazione.

- **Quali sono i valori delle porte di origine e destinazione?**
  - **Porta di Origine:** 80 (Il Server Web).
  - **Porta di Destinazione:** 58716 (Il Client).

    - *Nota:* I ruoli si sono invertiti rispetto al primo pacchetto.
- **Quali flag sono impostati?**
    - I flag impostati sono **SYN, ACK** (0x012).
    - *Significato:* Il server dice "Ho ricevuto la tua richiesta (ACK)" e "Voglio sincronizzarmi anch'io (SYN)".
- **A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?**
    - **Sequence Number:** 0.
    - **Acknowledgment Number:** 1.
    - *Il commento dell'esperto:* L'ACK è 1 perché il server si aspetta il *prossimo* byte di dati dal client (Seq 0 + 1).

---

3. Analisi del Terzo Pacchetto (L'ACK finale)

Il terzo pacchetto conclude l'handshake. La connessione è ora stabilita.

- **Quale flag è impostato?**
    - Il flag impostato è **ACK** (0x010).
    - *Significato:* Il client conferma di aver ricevuto il SYN del server. La connessione è "ESTABLISHED".
- **Numeri relativi di sequenza e acknowledgment:**
    - Entrambi sono impostati a **1**. Da questo momento in poi, può iniziare lo scambio di dati HTTP (come la richiesta `GET /favicon.ico` visibile nel pacchetto 4).
      +2

Parte 2: Utilizzo di Tcpdump

Tcpdump è uno strumento da riga di comando essenziale per un analista di sicurezza, specialmente quando non si dispone di un'interfaccia grafica.

- **Cosa fa l'opzione `-r`?**
    - L'opzione `-r` (read) permette di **leggere ed elaborare i pacchetti da un file salvato** (come un file `.pcap`) invece di catturarli in tempo reale dall'interfaccia di rete.
      +1
    - *Esempio dal laboratorio:* `tcpdump -r /home/analyst/capture.pcap`.

Parte 3: Domande di Riflessione per l'Amministratore di Rete

Come esperto, ti invito a riflettere su come questi strumenti si applicano nel mondo reale, oltre il laboratorio.

1. Filtri Wireshark utili per un Amministratore

In una rete reale con traffico intenso, i filtri sono vitali. Ecco tre esempi cruciali:

1. **`ip.addr == x.x.x.x`**:
    - *Utilità:* Isola tutto il traffico (in entrata e uscita) relativo a uno specifico host o server sospetto. Fondamentale per l'Incident Response.
2. **`tcp.port == xx`** (es. `tcp.port == 443`):
    - *Utilità:* Permette di focalizzarsi su uno specifico servizio (come il traffico web HTTPS), escludendo il "rumore" di fondo di altri protocolli.
3. **`tcp.analysis.flags`**:
    - *Utilità:* Wireshark evidenzia automaticamente anomalie come ritrasmissioni, pacchetti persi o finestre zero. È essenziale per diagnosticare problemi di instabilità della rete.

2. Altri utilizzi di Wireshark in produzione

Oltre all'analisi didattica, Wireshark è uno strumento professionale usato per:

+1

- **Network Troubleshooting (Risoluzione problemi di performance):**
    - Analizzando i tempi di risposta (delta time) tra un pacchetto e l'altro, si può capire se la lentezza è causata dalla rete (latenza) o dall'applicazione server che è lenta a elaborare la richiesta.
- **Security Forensics & Threat Hunting:**
    - Dopo un attacco, si analizzano i file `.pcap` per ricostruire l'accaduto: quali dati sono stati esfiltrati? Sono state passate password in chiaro (es. Telnet o HTTP)? C'è stato un tentativo di scansione delle porte (SYN scan)?.