AMATO SARA

S11L3

**Relazione sull’Analisi di Pacchetti TCP con Wireshark e Tcpdump**

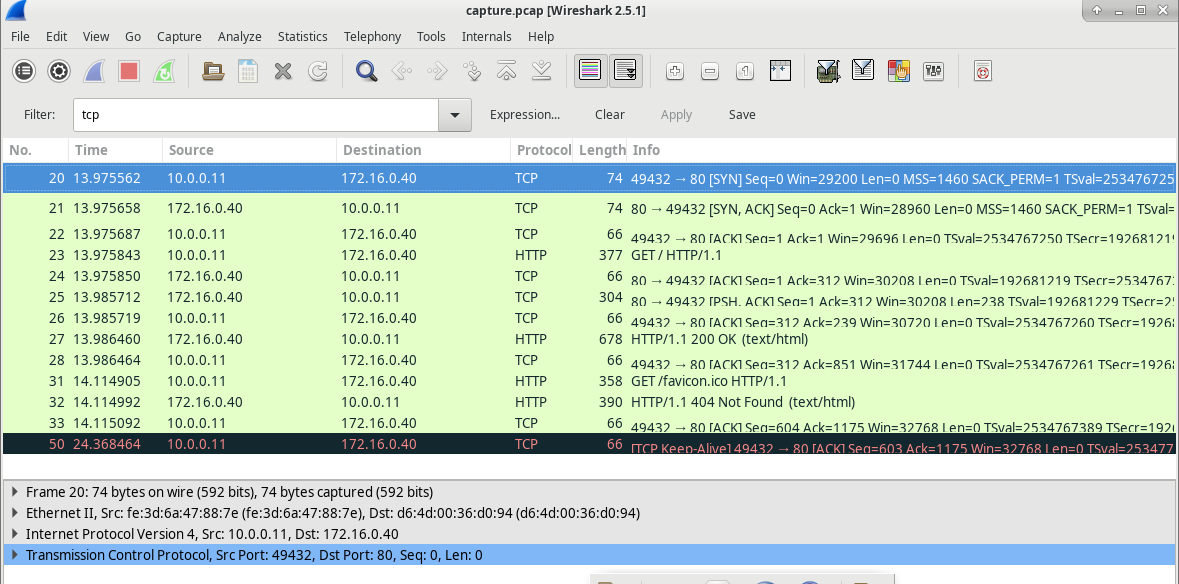
**Introduzione** L'analisi del traffico di rete è una competenza fondamentale per i professionisti della cybersecurity e della gestione di reti. In questa relazione esploreremo i concetti chiave relativi alla cattura e analisi di pacchetti TCP, utilizzando due strumenti principali: **Wireshark** e **Tcpdump**. Verrà illustrato il processo di analisi di una connessione TCP, evidenziando la comunicazione tra un client e un server tramite la procedura nota come "Three-Way Handshake".

**Obiettivi**

1. Comprendere la struttura di un pacchetto TCP e i relativi flag.
2. Analizzare una connessione TCP utilizzando Wireshark.
3. Esplorare le funzionalità di Tcpdump per analisi da terminale.

**Parte 1: Configurazione e Apertura di Wireshark** Wireshark è uno strumento grafico che consente di catturare e analizzare il traffico di rete in tempo reale o da file precedentemente salvati.

1. **Avvio di Wireshark**: Dopo aver aperto il programma, è necessario selezionare l'interfaccia di rete da monitorare.
2. **Cattura di traffico**: Si inizia la cattura cliccando sul pulsante “Start”.
3. **Filtraggio**: Per analizzare solo il traffico TCP, si utilizza il filtro tcp nella barra dei filtri in alto.
4. **Salvataggio**: Il traffico catturato viene salvato in un file .pcap per analisi successive.

****

**Parte 2: Analisi del "Three-Way Handshake" con Wireshark** La connessione TCP utilizza una procedura detta "Three-Way Handshake" per stabilire una connessione affidabile tra due dispositivi. Questo processo coinvolge tre pacchetti:

1. **Primo Pacchetto (SYN)**:
   * Rappresenta la richiesta iniziale di connessione da parte del client al server.
   * **Porta sorgente**: dinamica (ad esempio, 58716).
   * **Porta destinazione**: ben nota (ad esempio, 80 per HTTP).
   * **Flag impostato**: SYN.
   * **Numero di sequenza relativo**: 0.
2. **Secondo Pacchetto (SYN-ACK)**:
   * Il server risponde confermando la richiesta del client.
   * **Porta sorgente**: 80.
   * **Porta destinazione**: 58716.
   * **Flag impostati**: SYN e ACK.
   * **Numero di sequenza relativo**: 0.
   * **Numero di acknowledgment relativo**: 1.
3. **Terzo Pacchetto (ACK)**:
   * Il client conferma la ricezione del pacchetto del server.
   * **Flag impostato**: ACK.
   * **Numeri di sequenza e acknowledgment relativi**: entrambi a 1.

**Parte 3: Analisi con Tcpdump** Tcpdump è uno strumento a riga di comando per la cattura e analisi di traffico di rete. Consente di lavorare direttamente da terminale, ed è ideale per analisi rapide o in ambienti privi di interfaccia grafica.

1. **Lettura di un file .pcap**:
   * Il comando seguente legge un file .pcap e mostra i primi tre pacchetti TCP catturati:  
     tcpdump -r /home/analyst/capture.pcap tcp -c 3
   * L'output fornisce informazioni su:
     + Indirizzi IP sorgente e destinazione.
     + Porte utilizzate.
     + Flag impostati (ad esempio, [S] per SYN, [S.] per SYN-ACK).
2. **Ricerca nella documentazione**:
   * Il comando man tcpdump permette di accedere alla guida completa di Tcpdump, inclusa la descrizione delle opzioni.
   * Ad esempio, l'opzione -r serve per leggere un file .pcap salvato.

**Conclusione** L'analisi di pacchetti TCP è essenziale per comprendere il funzionamento della rete e per individuare eventuali anomalie o problemi. Wireshark è uno strumento grafico intuitivo, ideale per analisi dettagliate, mentre Tcpdump offre la flessibilità della riga di comando per utilizzi avanzati o in ambienti server.

**Domande Riflessive**

1. **Quali filtri sono utili in Wireshark?**
   * TCP, specifici indirizzi IP, e protocolli (es. HTTP).
2. **Come si usa Wireshark in un ambiente di produzione?**
   * Per analisi di sicurezza post-attacco.
   * Per monitoraggio delle prestazioni di rete.
   * Per configurazione e verifica di nuovi servizi o protocolli.

Questa esercitazione ha fornito una base pratica per esplorare la struttura e il comportamento dei protocolli di rete, arricchendo le competenze operative per gestire e proteggere le infrastrutture digitali.