Laboratori giorno 2 – Cisco CyberOps

Relazione: Analisi del Traffico di Rete con Wireshark e tcpdump

Introduzione

L'obiettivo di questo esercizio è comprendere il funzionamento del protocollo TCP (Transmission Control Protocol) e analizzare il traffico di rete utilizzando strumenti come tcpdump e Wireshark . Attraverso l'uso di una macchina virtuale (CyberOps Workstation) e la simulazione di una rete con Mininet, abbiamo catturato e analizzato i pacchetti scambiati tra un client (H1) e un server web (H4). Questo esercizio ci ha permesso di osservare il processo di handshake a tre vie (three-way handshake) e di esaminare i dettagli dei pacchetti TCP.

Obiettivi

1. Preparare gli host per catturare il traffico :
    - Configurare una rete simulata con Mininet.
    - Avviare un server web su H4 e un browser su H1.
    - Catturare il traffico di rete utilizzando tcpdump.
2. Analizzare i pacchetti con Wireshark :
    - Esaminare il three-way handshake TCP.
    - Identificare le porte sorgente e destinazione, i flag TCP e i numeri di sequenza/acknowledgment.
3. Visualizzare i pacchetti con tcpdump :
    - Leggere il file .pcap generato da tcpdump.
    - Filtrare e visualizzare i pacchetti TCP.

Ambiente di Lavoro

- Macchina Virtuale : CyberOps Workstation.
- Strumenti Utilizzati :
    - Mininet : Per simulare una rete con due nodi (H1 e H4).
    - tcpdump : Per catturare il traffico di rete.
    - Wireshark : Per analizzare i pacchetti catturati.
- Configurazione della Rete :
    - La VM è stata configurata in modalità NAT per consentire la connettività internet.
    - Mininet ha creato una rete interna con due host virtuali:
        - H1 : Simula un client con indirizzo IP 10.0.0.11.

- H4 : Simula un server web con indirizzo IP 172.16.0.40.

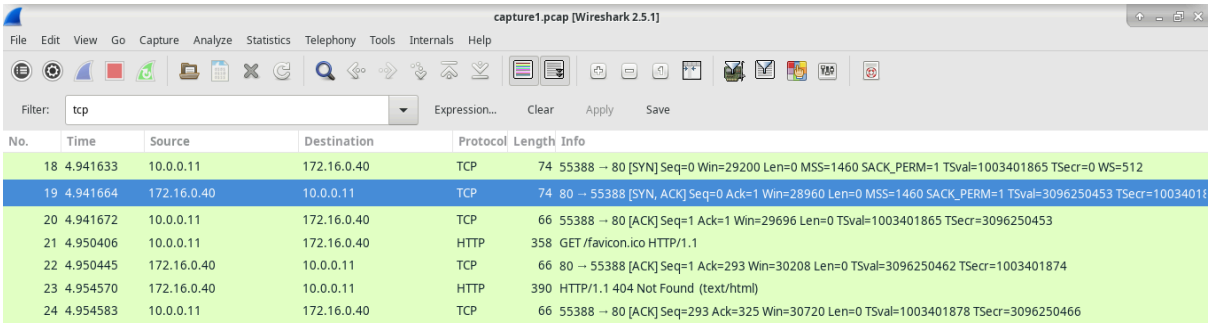
Procedura

Parte 1: Preparazione degli Host

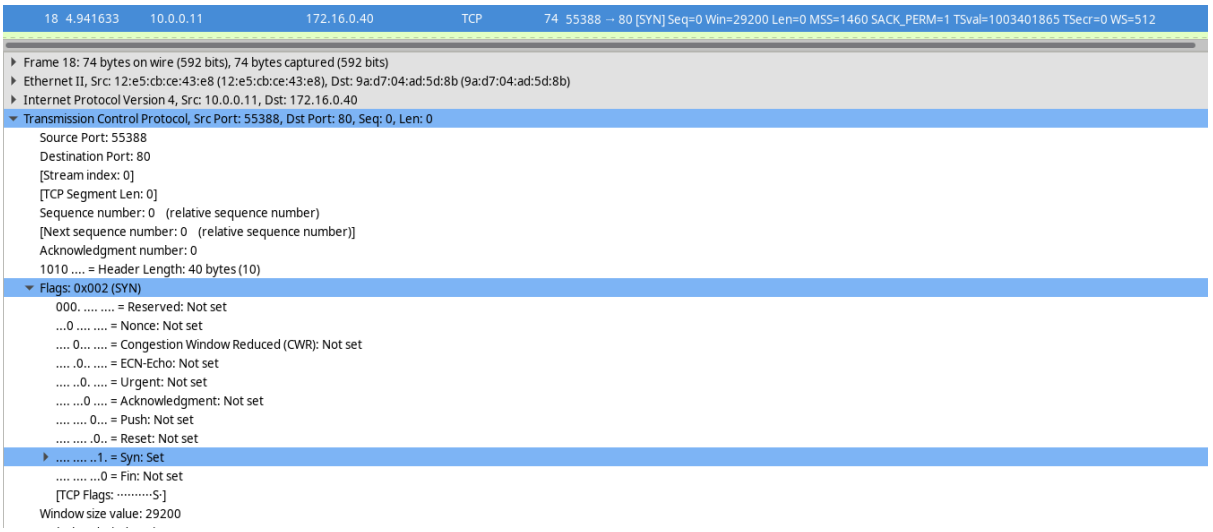
1. Avvio della VM :
    - La VM CyberOps Workstation è stata avviata e accesso effettuato con l'utente analyst.
2. Simulazione della Rete con Mininet :
    - È stato eseguito lo script cyberops_topo.py per creare una rete simulata con due nodi (H1 e H4).
3. Avvio del Server Web :
    - Su H4, è stato avviato uno script (reg_server_start.sh) per simulare un server web in ascolto sulla porta 80.
4. Navigazione sul Browser :
    - Su H1, è stato avviato Firefox e si è navigato verso l'indirizzo IP del server web (http://172.16.0.40).
5. Cattura del Traffico :
    - Utilizzando tcpdump, sono stati catturati 50 pacchetti di rete e salvati in un file chiamato capture1.pcap.

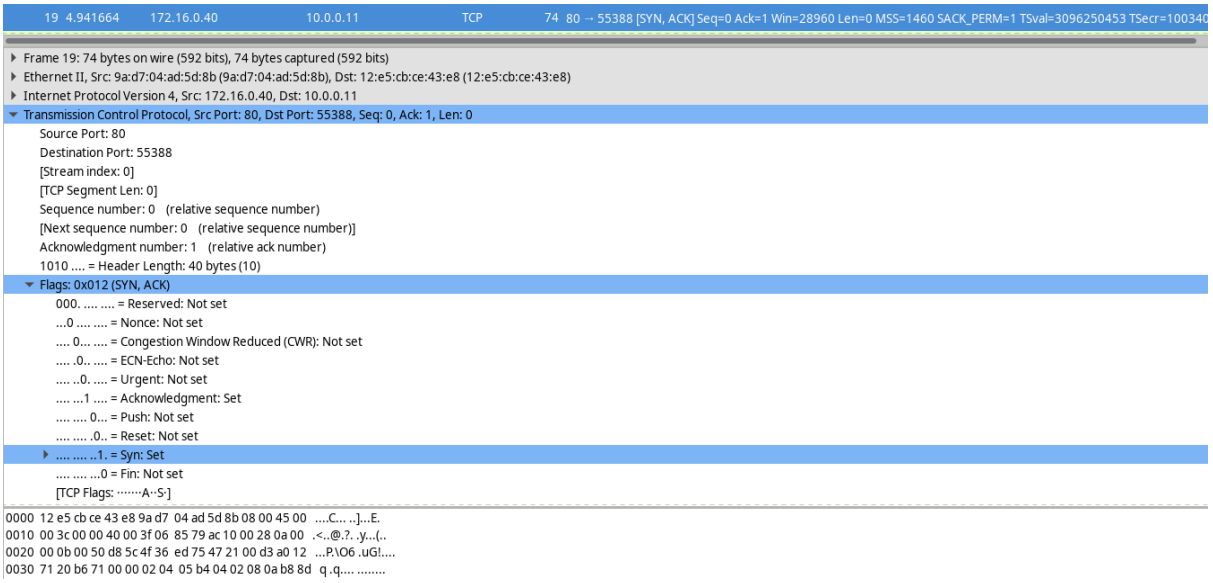
Parte 2: Analisi dei Pacchetti con Wireshark

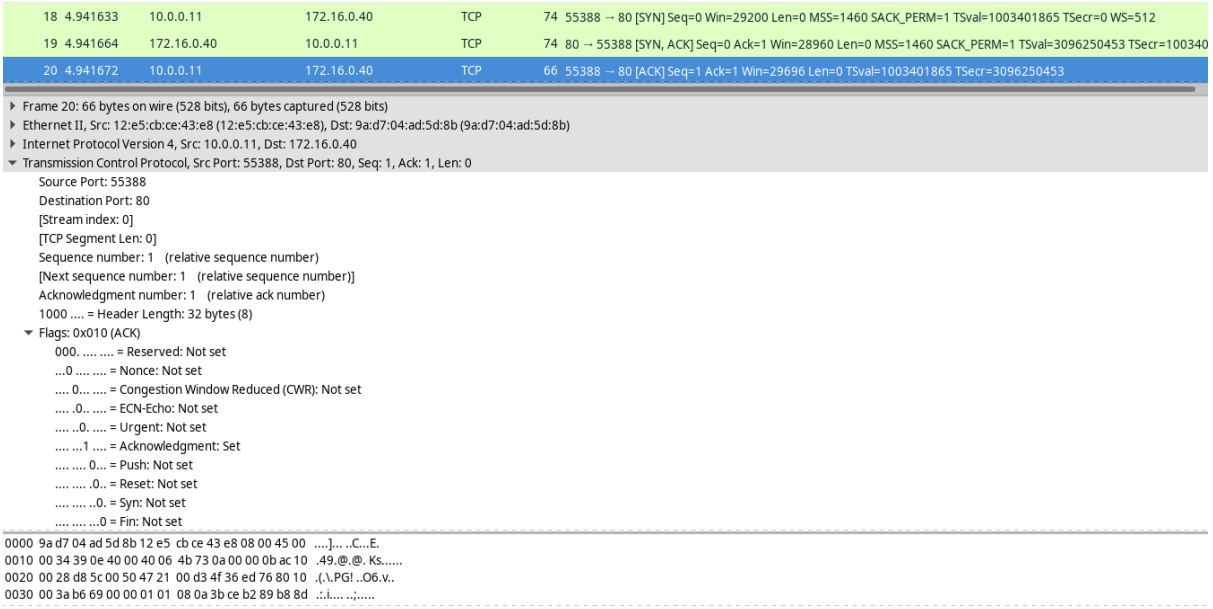
1. Apertura del File .pcap :
    - Il file capture.pcap è stato aperto in Wireshark per analizzare il traffico catturato.
2. Filtro TCP :
    - È stato applicato un filtro TCP (tcp) per visualizzare solo i pacchetti relativi al protocollo TCP.



3. Esame del Three-Way Handshake :
    - Pacchetto 1 : Richiesta di connessione dal client (flag SYN impostato).
        - Porta sorgente: Dinamica (55388).
        - Porta destinazione: 80 (HTTP).
    - Pacchetto 2 : Risposta del server (flag SYN e ACK impostati).
        - Porta sorgente: 80.
        - Porta destinazione: Dinamica (es. 55388).
    - Pacchetto 3 : Conferma del client (flag ACK impostato).
        - Numeri di sequenza e acknowledgment confermano l'inizio della comunicazione.

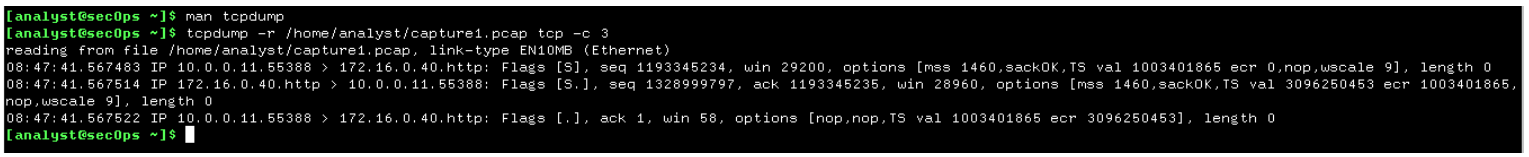






Parte 3: Visualizzazione dei Pacchetti con tcpdump

1. Lettura del File .pcap :
    - Il comando tcpdump -r /home/analyst/capture.pcap tcp -c 3 è stato utilizzato per visualizzare i primi 3 pacchetti TCP.
2. Verifica del Three-Way Handshake :
    - I pacchetti visualizzati corrispondono a quelli analizzati in Wireshark:
        - Primo pacchetto: Flag SYN.
        - Secondo pacchetto: Flag SYN e ACK.
        - Terzo pacchetto: Flag ACK.



Risultati

- Three-Way Handshake :
  - Il processo di handshake a tre vie è stato osservato chiaramente nei pacchetti catturati.
  - I numeri di sequenza e acknowledgment hanno confermato l'inizio della comunicazione tra il client e il server.
- Porte e Flag TCP :
  - La porta sorgente del client era dinamica, mentre la porta destinazione era 80 (HTTP).
  - I flag TCP (SYN, ACK) hanno dimostrato il corretto funzionamento del protocollo.

Conclusioni

Questo esercizio ha fornito una comprensione pratica del funzionamento del protocollo TCP e delle tecniche di cattura e analisi del traffico di rete. Gli strumenti utilizzati, tcpdump e Wireshark , sono essenziali per monitorare e diagnosticare problemi di rete, nonché per analizzare attacchi o anomalie. La simulazione della rete con Mininet ha reso possibile eseguire l'esercizio in un ambiente controllato e sicuro.