Analisi dei Pacchetti TCP con Wireshark

Obiettivo del Laboratorio Il laboratorio mira a catturare e analizzare pacchetti di rete generati durante una sessione HTTP tra un browser web su un host e un server web remoto. L'attività prevede l'uso di strumenti come Mininet per simulare la rete, tcpdump per catturare i pacchetti e Wireshark per analizzarli.

Cattura dei Pacchetti

Preparazione dell'Ambiente

- È stata avviata la macchina virtuale (VM) CyberOps, effettuando l'accesso con le credenziali:
 - Nome utente: analyst
 - Password: **cyberops**
- Successivamente, è stato avviato Mininet tramite il comando:
- sudo lab.support.files/scripts/cyberops_topo.py

Configurazione degli Host

- Nel terminale Mininet, sono stati avviati gli host H1 e H4 utilizzando:
- xterm H1
- xterm H4
- Sul nodo H4, è stato avviato il server web tramite il comando:
- /home/analyst/lab.support.files/scripts/reg_server_start.sh

Accesso e Avvio del Browser Web

- Sul nodo H1, è stato effettuato lo switch all'account utente analyst con:
- su analyst
- Successivamente, è stato avviato Firefox tramite il comando:
- firefox &

Cattura dei Pacchetti

- Sul nodo H1, è stato avviato il comando tcpdump per catturare 50 pacchetti, salvando l'output in un file denominato capture.pcap:
- sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analista/capture.pcap
- Mentre tcpdump era attivo, è stato effettuato l'accesso all'indirizzo IP del server web (172.16.0.40) utilizzando il browser Firefox.

Analisi dei Pacchetti con Wireshark

Avvio di Wireshark

- Sul nodo H1, è stato avviato Wireshark tramite il comando:
- wireshark &
- All'avvio, è stato aperto il file di cattura (capture.pcap) tramite il percorso: File > Apri.

Applicazione del Filtro TCP

- In Wireshark, è stato applicato un filtro per visualizzare esclusivamente il traffico TCP. Questo filtro ha permesso di identificare i pacchetti relativi all'handshake a tre vie e alla sessione HTTP stabilita tra H1 e il server web H4.
- Sono stati osservati i seguenti elementi chiave nei primi 3 frame:
 - **SYN:** Richiesta di sincronizzazione inviata dall'host H1 al server H4.
 - **SYN-ACK:** Risposta del server H4 per confermare la richiesta.
 - **ACK:** Conferma finale dell'host H1 per completare l'handshake.

Dettagli dell'Analisi dei Pacchetti

- Fai clic sulla freccia a sinistra di Flags. Un valore di 1 significa che il flag è impostato.
 Individua il flag impostato in questo pacchetto.
 - Numero della porta sorgente TCP: 58716 (esempio). Classificazione: dinamico o privato.
 - Numero della porta di destinazione TCP: 80. Classificazione: noto, registrato (protocollo HTTP o web).
 - Flag impostato: Bandiera SYN.
 - Numero di sequenza relativo: 0.
- Seleziona il pacchetto successivo nell'handshake a tre vie (esempio: frame 2). Questo è il server web che risponde alla richiesta iniziale di avviare una sessione.
 - Porta di origine: 80.
 - Porta di destinazione: 58716.
 - Flag impostati: Flag di riconoscimento (ACK) e Syn (SYN).
 - Numeri di sequenza e di conferma relativi: Numero di sequenza relativo: 0. Numero di conferma relativo: 1.
- Infine, seleziona il terzo pacchetto nell'handshake a tre vie.
 - Flag impostato: Flag di conferma (ACK).
 - Numeri di sequenza e di conferma relativi: Entrambi impostati su 1 come punto di partenza.
- La connessione TCP è stata stabilita e la comunicazione tra il computer sorgente e il server Web può iniziare.

Visualizza i Pacchetti Utilizzando tcpdump

È anche possibile visualizzare il file pcap e filtrare le informazioni desiderate.

Visualizzare il Manuale di tcpdump

- Apri una nuova finestra del terminale e digita:
- man tcpdump
- Nota: potrebbe essere necessario premere INVIO per visualizzare il prompt.
- Utilizzando le pagine del manuale disponibili con il sistema operativo Linux, è possibile leggere o cercare al loro interno le opzioni per selezionare le informazioni desiderate dal file pcap. Per cercare nelle pagine man, puoi usare / (ricerca in avanti) o ? (ricerca all'indietro) per trovare termini specifici, e n per andare avanti alla corrispondenza successiva e q per uscire.
 - A cosa serve l'opzione -r? L'opzione -r consente di leggere il pacchetto dal file salvato utilizzando l'opzione -w con tcpdump o altri strumenti che scrivono file pcap o pcapng, come Wireshark.

Visualizzazione dei Pacchetti Acquisiti

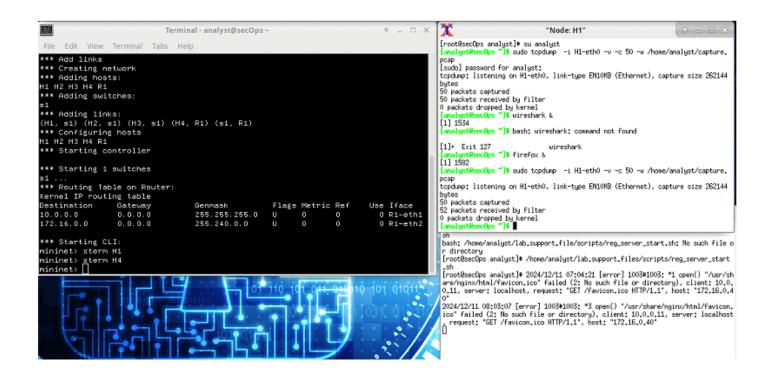
- Nel terminale, apri il file di acquisizione per visualizzare i primi 3 pacchetti TCP acquisiti:
- tcpdump -r /home/analista/capture.pcap -c 3
- Per visualizzare l'handshake a 3 vie, potrebbe essere necessario aumentare il numero di righe dopo l'opzione -c.

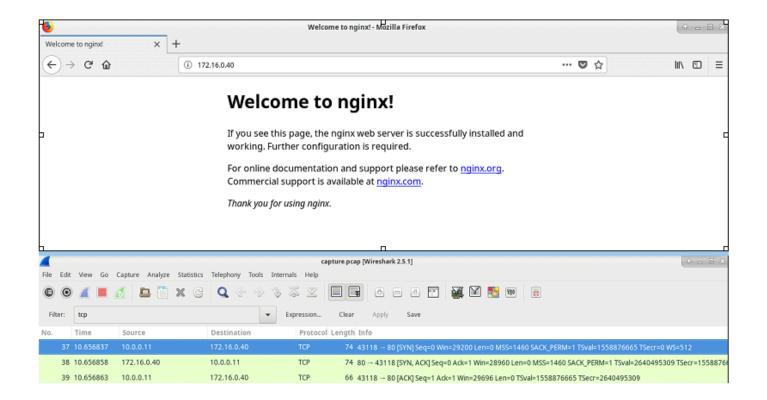
Pulizia e Chiusura di Mininet

- Vai al terminale utilizzato per avviare Mininet. Termina Mininet immettendo:
- quit
- nella finestra principale del terminale CyberOps VM.
- Dopo aver chiuso Mininet, esegui:
- sudo mn -c
- per ripulire i processi avviati da Mininet. Inserisci la password cyberops quando richiesto.

Conclusioni Il laboratorio ha permesso di:

- Comprendere il processo di handshake a tre vie utilizzato da TCP per stabilire una connessione affidabile.
- Utilizzare tcpdump per catturare pacchetti di rete e salvare i dati in formato pcap.
- Analizzare il traffico di rete catturato utilizzando Wireshark, applicando filtri per isolare pacchetti specifici.
- Visualizzare e analizzare i file pcap direttamente dal terminale con tcpdump, utilizzando le opzioni disponibili nel manuale del comando.





```
analyst@secOps ~]$ sudo mn =c
sudo] password for analyst:

*** Removing excess controllers/ofprotocols/ofdatapaths/pings/noxes
silall controller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udpbwtest mnexec ivs 2> /dev/null
silall =9 sontroller ofprotocol ofdatapath ping nox_core lt-nox_core ovs-openflowd ovs-controller udpbwtest mnexec ivs 2> /dev/null
skill =9 =f "sudo mnexec"

*** Removing junk from /trp

m =f /trp/vconn* /trp/vlogs* /tmp/*.out /tmp/*.log

*** Removing old X11 tunnels

*** Removing ovs datapaths

se ax | egrep =0 'dp[0-9]*' | sed 's/dp/nl:/'

*** Removing ovs datapaths

se-vsctl =-timeout=1 list=br

se-vsct
```