S11L3 **Luca Calvigioni**

Relazione sulle Attività di Analisi del Traffico di Rete con Mininet, tcpdump e Wireshark

Preparare gli Host per Catturare il Traffico

Avvio del sistema CyberOps

Il sistema CyberOps VM viene avviato utilizzando le credenziali:

Username: analyst

Password: cyberops

Configurazione di Mininet

Mininet viene avviato eseguendo il comando:

sudo lab.support.files/scripts/cyberops_topo.py

Apertura delle console per H1 e H4

Si accede alle console degli host H1 e H4 tramite i comandi:

mininet> xterm H1

mininet> xterm H4

Avvio del server web su H4

Il server web viene avviato con il comando:

/home/analyst/lab.support.files/scripts/reg_server_start.sh

Passaggio all'utente analyst su H1

Poiché il browser Firefox non può essere avviato con l'utente root, si esegue il comando per passare all'utente analyst:

su analyst

Passaggio 6: Avvio di Firefox su H1

Firefox viene avviato utilizzando:

firefox &

Passaggio 7: Avvio della cattura con tcpdump

Si avvia una sessione tcpdump per catturare i primi 50 pacchetti di traffico sull'interfaccia **H1-eth0**, salvandoli in un file **capture.pcap**:

sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap

Subito dopo, nel browser Firefox si accede all'indirizzo IP del server web: `172.16.0.40`.

Analisi dei Pacchetti con Wireshark

Passaggio 1: Apertura del file di cattura

Wireshark viene avviato con:

wireshark &

Si apre il file di cattura salvato:
Percorso del file: `/home/analyst/capture.pcap`

Passaggio 2: Filtraggio e analisi del traffico TCP

- Si applica un filtro **tcp** per visualizzare i pacchetti relativi al traffico TCP.
- Analisi del **three-way handshake**:

Primo pacchetto:
Porta di origine: 58716 (dinamica/privata).

Porta di destinazione: 80 (nota e registrata, HTTP).

Flag impostati: SYN

Numero di sequenza relativo: 0

Secondo pacchetto:
Porta di origine: 80

Porta di destinazione: 58716

Flag impostati: SYN, ACK

Numero di sequenza relativo: 0

Numero di riconoscimento relativo: 1

Terzo pacchetto:
Flag impostati: ACK

Numero di sequenza relativo e numero di riconoscimento: 1

Visualizzazione dei Pacchetti con tcpdump

Passaggio 1: Lettura del file pcap

Si usa il comando *man tcpdump* per studiare le opzioni disponibili.

L'opzione `-r` consente di leggere un file pcap salvato:

tcpdump -r /home/analyst/capture.pcap tcp -c 3

L’output mostra i primi 3 pacchetti:

Pacchetto con **Flag [S]**, che rappresenta la richiesta di sincronizzazione.

Pacchetto con **Flag [S.]**, che include il riconoscimento della richiesta iniziale.

Pacchetto con **Flag [.]**, che completa il three-way handshake.

Passaggio 2: Pulizia e chiusura di Mininet

Mininet viene chiuso con il comando:

mininet> quit

Si esegue una pulizia finale dei processi di Mininet:

sudo mn -c

Conclusioni

Questa esercitazione dimostra come utilizzare strumenti di analisi del traffico di rete come tcpdump e Wireshark per catturare e analizzare pacchetti. Si è esaminato in dettaglio il processo di handshake TCP, mostrando come i dati relativi a porte, numeri di sequenza e flag siano cruciali per comprendere le connessioni di rete.