Esercizio di Pratica S11L2 – Cisco CyberOps

Sergio Falcone

INTRODUZIONE

Obiettivi:

1. Parte 1 - Preparare gli Host per Catturare il Traffico
2. Parte 2 - Analizzare i Pacchetti usando Wireshark

Pacchetto 1:

- Qual è il numero di porta TCP di origine?
- Come classificheresti la porta di origine?
- Qual è il numero di porta TCP di destinazione?
- Come classificheresti la porta di destinazione?
- Quale flag è impostato?
- A quale valore è impostato il numero di sequenza relativo?

Pacchetto 2:

- Quali sono i valori delle porte di origine e destinazione?
- Quali flag sono impostati?
- A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?

Pacchetto 3

- Quale flag è impostato?

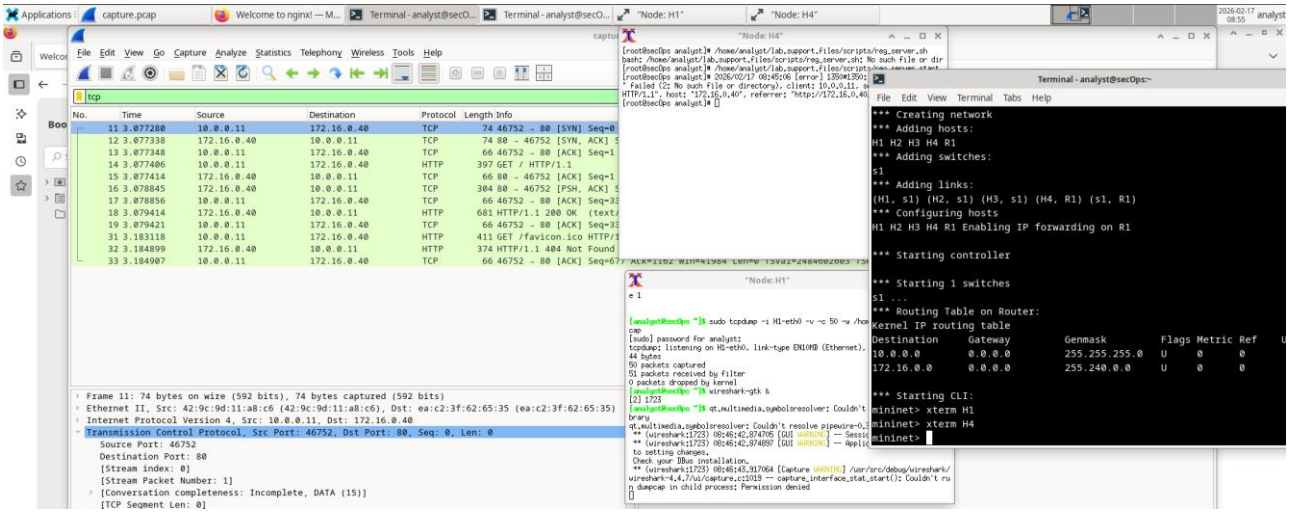
3. Parte 3 - Visualizzare i Pacchetti usando tcpdump
   - Cosa fa l'opzione -r?

4. Domande di Riflessione

   1. Ci sono centinaia di filtri disponibili in Wireshark. Una rete di grandi dimensioni potrebbe avere numerosi filtri e molti tipi diversi di traffico. Elenca tre filtri che potrebbero essere utili a un amministratore di rete.
   2. In quali altri modi Wireshark potrebbe essere utilizzato in una rete di produzione?

ESECUZIONE Parte 1

La traccia originale di questa esercitazione spiega la modalità di configurazione della Macchina Virtuale CyberOps Workstation.
Lo Screenshot seguente mostra il risultato della configurazione.



ESECUZIONE Parte 2

Analisi dei Pacchetti con Wireshark (Domande e Risposte)

Pacchetto 1:

- Qual è il numero di porta TCP di origine?

- Il numero della porta TCP di origine è 46752
  - Come classificheresti la porta di origine?
- La porta di origine è una porta Effimera (o Dinamica), poiché viene assegnata temporaneamente dal sistema operativo del client per una specifica sessione di comunicazione.
  - Qual è il numero di porta TCP di destinazione?
- Il numero di porta TCP di destinazione è la porta 80 (http)
  - Come classificheresti la porta di destinazione?
- La porta di destinazione viene classificata come Ben Nota, poiché è dei servizi di sistema
  - Quale flag è impostato?

- Il flag impostato è [SYN] Synchronize, la prima parte del Three-Way-Handshake
  - A quale valore è impostato il numero di sequenza relativo?
- Il valore di sequenza relativo impostato è 0, seq=0

Pacchetto 2:

- Quali sono i valori delle porte di origine e destinazione?
- I valori delle porte di origine è 80 (http) e destinazione 46752
- Quali flag sono impostati?
- I flag impostati sono [SYN, ACK], indicano la seconda fase del Three-Way-Handshake
- A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?
- Il valore del numero di sequenza è impostato su 0 mentre di aknowledgment su 1, seq=0 ack=1

Pacchetto 3

- Quale flag è impostato?
- Il flag impostato è [ACK], ultima fase del Three-Way-Handshake, indica che il Client ha ricevuto il pacchetto SYN-ACK del server e conferma la ricezione.

ESECUZIONE Parte 3

Visualizzare i Pacchetti usando tcpdump

- Cosa fa l'opzione -r?
- **-r file**, legge i pacchetti da un file (che è stato creato con l'opzione -w o da altri strumenti che scrivono file in formato pcap o pcapng).
  Se il file è " - ", viene utilizzato lo standard input.

DOMANDE DI RIFLESSIONE

1. Ci sono centinaia di filtri disponibili in Wireshark. Una rete di grandi dimensioni potrebbe avere numerosi filtri e molti tipi diversi di traffico. Elenca tre filtri che potrebbero essere utili a un amministratore di rete.

   - In una rete di grandi dimensioni i tre filtri di Wireshark che potrebbero essere utili ad un amministratore di rete sono:
     -ip.addr, per isolare il traffico di rete da o verso un host specifico.
     -dns, per consentire di isolare il traffico di risoluzione dei nomi di dominio, facilitando il troubleshooting dei servizi di rete e l'analisi di possibili attività malevole basate su DNS.
     -tcp.flags.reset == 1, mostra i pacchetti che sono stati interrotti con un reset le cui motivazioni dovrebbero essere oggetto di analisi

   2. In quali altri modi Wireshark potrebbe essere utilizzato in una rete di produzione?

   Oltre l'analisi dei pacchetti Wireshark potrebbe essere utilizzato per:

   - **Analisi delle Prestazioni (Latency Troubleshooting):** Gli amministratori lo usano per capire *dove* si perde tempo. Wireshark può calcolare il tempo che intercorre tra una richiesta e una risposta (Delta Time). Se il ritardo è nel pacchetto ACK del server, il problema è la rete; se il ritardo è tra l'ACK e la risposta dei dati, il problema è l'applicazione o il database lento.
   - **Audit di Sicurezza e Conformità:** Viene usato per verificare se i dati sensibili viaggiano in chiaro. Ad esempio, per assicurarsi che nessun servizio stia ancora usando protocolli insicuri come Telnet o FTP invece di SSH o SFTP, o per identificare traffico sospetto verso IP malevoli conosciuti.
   - **Debug di Telefonia VoIP:** Nelle reti che usano telefoni IP, Wireshark ha strumenti specifici per "ricostruire" le chiamate (analisi del protocollo SIP/RTP). Può misurare il *jitter* e la perdita di pacchetti che causano una cattiva qualità audio e persino riprodurre il flusso audio catturato per sentire cosa non è andato a buon fine.