Cisco CyberOps

Laboratorio:

Utilizzo di Wireshark per Osservare la Stretta di Mano TCP a 3 Vie.

In questo laboratorio, completa i seguenti obiettivi:

- Preparare gli host per catturare il traffico
- Analizzare i pacchetti utilizzando Wireshark
- 3Visualizzare i pacchetti utilizzando tcpdump

https://itexamanswers.net/9-2-6-lab-using-wireshark-to-observe-the-tcp-3-way-handshake-answers.html

Relazione

Durante l'esecuzione dell'attività sulla CyberOps Workstation, ho seguito i passaggi necessari per configurare e analizzare la rete. Innanzitutto, ho avviato Mininet per simulare una rete con due host, H1 e H4, in modo da generare il traffico necessario per eseguire l'analisi del processo di handshake TCP. Successivamente, ho utilizzato xterm per aprire le console di H1 e H4.
Per avviare la comunicazione tra H1 e H4, ho dovuto eseguire una serie di operazioni specifiche. In particolare, su H1, ho iniziato con il login come root@secops, ma per avviare Firefox, che è stato utilizzato per generare traffico HTTP, ho dovuto passare all'utente analyst@secops. Questo passaggio è stato necessario poiché l'utente root non aveva i permessi per avviare applicazioni grafiche come Firefox. Una volta effettuato il passaggio a analyst@secops, sono riuscito ad aprire Firefox e avviare una sessione web, permettendo così la generazione del traffico TCP tra i due host.
Con il traffico generato, ho utilizzato Wireshark per catturare e analizzare i pacchetti. Ho applicato il filtro per il traffico TCP e ho osservato i pacchetti legati all'handshake a tre vie: il pacchetto SYN inviato da H1, il SYN-ACK ricevuto da H4, e infine il pacchetto ACK inviato da H1 per completare la connessione.
Successivamente, ho utilizzato tcpdump per eseguire un'ulteriore analisi del traffico, leggendo i pacchetti dal file .pcap creato con Wireshark. Questo mi ha permesso di confermare i dati già osservati con Wireshark, visualizzando in modo sintetico le informazioni sui pacchetti TCP.
In sintesi, l'intero processo mi ha permesso di comprendere meglio come funziona il protocollo TCP e di acquisire familiarità con gli strumenti di analisi come Wireshark e tcpdump, in un ambiente simulato con Mininet e CyberOps Workstation.

Daniel_Gabriel_Costeanu