EPICODE

Laboratorio giorno 2 - Cisco CyberOps

By Xian Long Qiu

EPICODE

Wireshark handshake tcp

1. La porta TCP di origine è 51344.
2. La porta è classificata come porta non assegnata/riservata, ma utilizzata per applicazioni temporanee o personalizzate.
3. La porta di destinazione è 80.
4. La porta è classificata come porta nota e standard per il protocollo HTTP.
5. Flag SYN = 0x002.
6. Il numero di sequenza SYN è 0.
7. La porta di origine e quella di destinazione sono rispettivamente 80 e 51344.
8. Flag SYN-ACK = 0x012.
9. Il numero di sequenza del pacchetto SYN-ACK è 0, mentre il valore di acknowledgement è 1, indicando che la connessione è stabilita.
10. Flag ACK = 0x010.

Questi dettagli descrivono una tipica sequenza di handshake TCP tra una porta temporanea di origine e la porta HTTP standard di destinazione.

EPICODE

TcpDump

L’opzione -r di tcpdump serve a leggere un file di cattura e visualizzarne il contenuto direttamente nel terminale.

Riflessioni

Ecco tre filtri Wireshark molto utili per un amministratore di rete nell’analisi del traffico in reti di grandi dimensioni:

- Filtro per protocollo specifico:

-Utilità: Consente di isolare il traffico di un protocollo specifico, facilitando l’analisi di problemi relativi a servizi particolari.

- Filtro per indirizzo IP (sorgente o destinazione):

-Utilità: Permette di monitorare il traffico proveniente o diretto verso un dispositivo specifico, utile per identificare attacchi o dispositivi problematici.

- Filtro per porte (utile nel troubleshooting di servizi):

-Utilità: Consente di analizzare il traffico su porte critiche, rilevando connessioni non autorizzate o errori nei servizi di rete.

Gli utilizzi di Wireshark in una rete di produzione

Gli utilizzi di Wireshark in una rete di produzione:

- Troubleshooting di problemi di rete

Analisi di ritardi, perdite di pacchetti e malfunzionamenti DHCP/DNS.

- Sicurezza e rilevamento di attacchi

Individuazione di scansioni SYN, traffico sospetto e ARP spoofing.

- Ottimizzazione delle prestazioni

Identificazione di broadcast eccessivi e analisi del throughput tramite grafici.