S11L2

-Qual è il numero di porta TCP di origine?

58716

Come classificheresti la porta di origine?

È una **porta dinamica (o effimera)**, assegnata temporaneamente dal sistema operativo al browser.

-Qual è il numero di porta TCP di destinazione?

80

-Come classificheresti la porta di destinazione?

È una **porta well-known** associata al protocollo **HTTP**.

-Quale flag è impostato?

Il flag **SYN** (valore 1), questo indica un tentativo di sincronizzazione iniziale.

-A quale valore è impostato il numero di sequenza relativo?

È impostato a **0**

`-Quali sono i valori delle porte di origine e destinazione?`

Origine: **80**

Destinazione: **58716**

Sono invertite rispetto al primo pacchetto.

`-Quali flag sono impostati?`

Sono impostati **SYN** e **ACK**, il server ha ricevuto la richiesta e cerca di connettersi.

`-A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?`

Numero di sequenza: **0**

Numero di acknowledgment: **1**

`-Quale flag è impostato?`

Solamente il flag **ACK**.

`-Cosa fa l'opzione -r?`

L'opzione **-r** (read) permette di **leggere i pacchetti da un file salvato**, nel comando dell'esercizio, viene usato per riaprire il file **capture.pcap** creato precedentemente.

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.

ip.addr == x.x.x.x per vedere tutto il traffico (sia in entrata che in uscita) relativo a uno specifico dispositivo o server sospetto.

tcp.port == 80 || tcp.port == 443 per isolare solo il traffico web (HTTP e HTTPS).

http.request.method == "POST" utile per vedere quando vengono inviati dati ad un server.

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

Risoluzione problemi di performance (Troubleshooting): per capire perché un'applicazione è lenta (analizzando i ritardi tra i pacchetti o le ritrasmissioni TCP).

Analisi di sicurezza (Malware Analysis): per identificare traffico anomalo generato da virus o ransomware che tentano di comunicare con server di comando e controllo.

Analisi di protocolli sconosciuti: per capire come funziona un software legacy o proprietario che non ha documentazione.