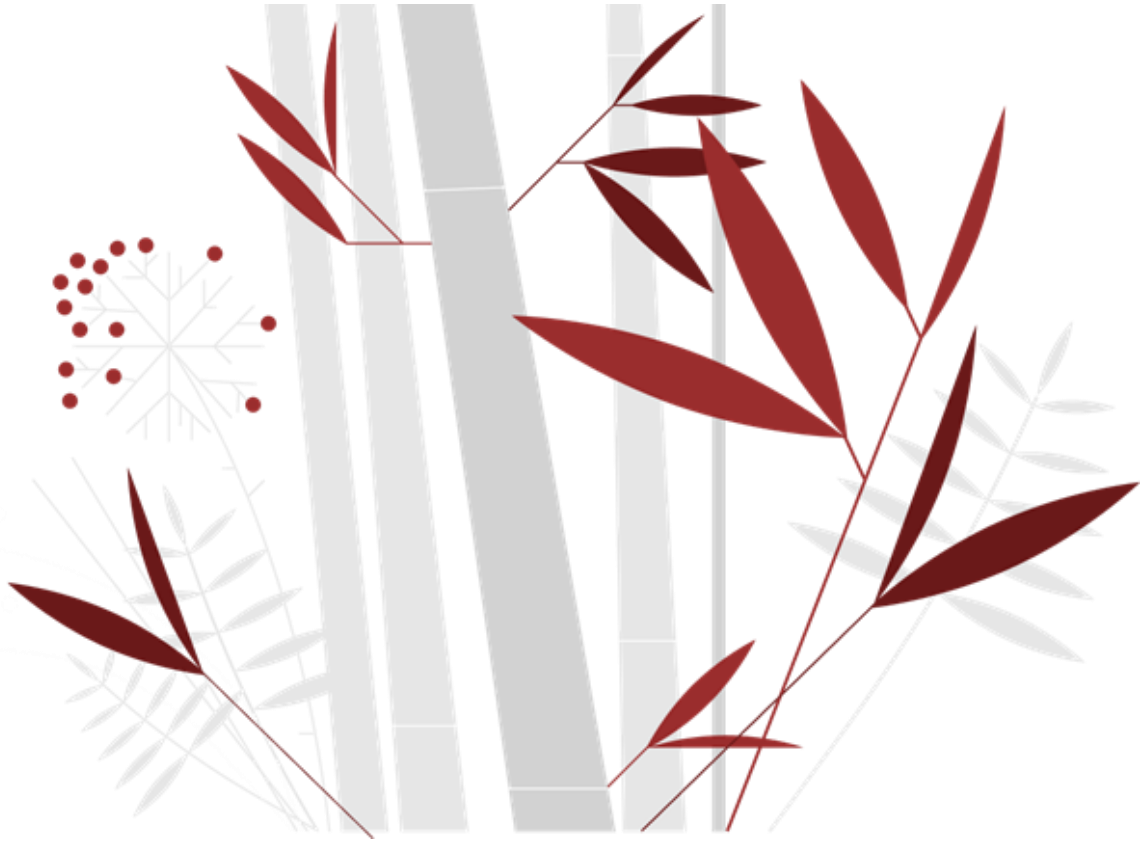
CYBER SECURITY

Cisco CyberOps

sara maimone

S11.L3

11/12/2024



Relazione del Laboratorio: Osservazione della Stretta di Mano TCP a 3 Vie

Obiettivo

L'obiettivo di questo laboratorio è utilizzare strumenti come Wireshark e `tcpdump` per catturare e analizzare il traffico di rete, con particolare attenzione alla stretta di mano TCP a tre vie. La stretta di mano a tre vie è un processo fondamentale che avviene quando due host stabiliscono una connessione TCP.

Parte 1: Preparazione degli Host per la Cattura del Traffico

1. **Configurazione della rete**

2. Gli host sono stati configurati in una rete locale. Sono stati assegnati indirizzi IP specifici agli host per semplificare l'identificazione del traffico.

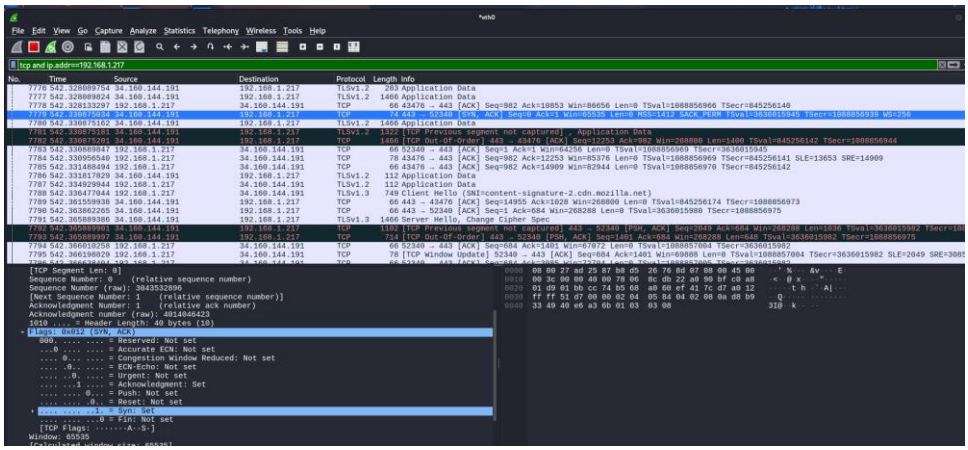
3. In questo esempio, l'host con indirizzo IP **192.168.1.217** comunica con il server remoto **34.160.144.191**.

4. **Strumenti utilizzati**
    a. **Wireshark:** Per catturare e analizzare i pacchetti con un'interfaccia grafica.
    b. **tcpdump:** Per osservare il traffico da terminale con comandi mirati.
5. **Configurazione iniziale**

Prima di iniziare la cattura, è stata scelta l'interfaccia di rete corretta e configurati i filtri TCP (`tcp and ip.addr==192.168.1.217`) per concentrare l'attenzione solo sul traffico rilevante.

Parte 2: Analisi dei Pacchetti con Wireshark

Dallo screenshot allegato si può osservare il seguente processo di stretta di mano TCP:



1. **Primo passaggio - SYN:**

L'host 192.168.1.217 invia un pacchetto SYN al server 34.160.144.191, indicando che desidera stabilire una connessione.

   a. **Flags TCP:** Solo il flag SYN è impostato.
   b. **Numero di Sequenza:** Inizializzato dall'host (ad esempio, Seq=0).

2. **Secondo passaggio - SYN, ACK:**

Il server risponde con un pacchetto contenente i flag SYN e ACK, confermando la ricezione del pacchetto iniziale e indicando che è pronto per stabilire la connessione.

   a. **Flags TCP:** SYN, ACK.
   b. **Numero di Sequenza:** Il server invia il proprio numero di sequenza iniziale e conferma il numero di sequenza dell'host incrementato di 1.

3. **Terzo passaggio - ACK:**

L'host completa la stretta di mano inviando un pacchetto con il flag ACK, confermando la ricezione del pacchetto SYN, ACK del server.

   a. **Flags TCP:** Solo ACK è impostato.

Con questa sequenza, la connessione TCP è stabilita e pronta per il trasferimento dati.

Parte 3: Visualizzazione dei Pacchetti con tcpdump

Per replicare l'analisi effettuata con Wireshark utilizzando `tcpdump`, sono stati utilizzati comandi specifici come: `sudo tcpdump -i eth0 'tcp and host 192.168.1.217'`

Questo comando cattura tutti i pacchetti TCP tra l'host locale e l'indirizzo IP remoto. Il risultato può essere analizzato direttamente in terminale oppure salvato in un file (`tcpdump -w capture.pcap`) per analisi successiva in Wireshark.

Conclusioni

Lo screenshot conferma che la stretta di mano TCP a tre vie è avvenuta correttamente tra i due host. Questo processo è un aspetto fondamentale delle comunicazioni TCP/IP, garantendo che entrambi gli endpoint siano sincronizzati e pronti a scambiarsi dati.