Osservare l'Handshake a 3 Vie TCP

profilo studente

- **Gabriel Giustinelli**
- **Epicode Cyber Security**
- **classe** CS0525
- **data** 12/02/2026

Contesto / Scenario

In questo laboratorio, si usa Wireshark per catturare ed esaminare i pacchetti generati tra il browser del PC che utilizza il protocollo HTTP (HyperText Transfer Protocol) e un server web, come www.google.com.
Quando un'applicazione, come HTTP o FTP (File Transfer Protocol), si avvia per la prima volta su un host, TCP utilizza l'handshake a tre vie per stabilire una sessione TCP affidabile tra i due host.
Ad esempio, quando un PC utilizza un browser web per navigare in internet, viene avviato un handshake a tre vie e viene stabilita una sessione tra l'host del PC e il server web.
Un PC può avere più sessioni TCP attive simultaneamente con vari siti web.

analisi con wireshark

Quali sono gli indirizzi IP di H1 e H4?

- **H1 (il Client):** `10.0.0.11`
- **H4 (il Server):** `172.16.0.40`

Quali sono i numeri di porta utilizzati per la connessione?

- Il numero di porta TCP di origine è **un numero casuale elevato** `58716` (porta effimera)
- **Porta Destinazione (H4):** È la porta `80` del servizio HTTP

Quali sono i flag TCP impostati nel primo pacchetto?

- Il flag impostato è solo il flag **SYN** (Synchronize) espandendo la sezione "Flags" nel dettaglio del pacchetto: **`Flags: 0x002 (SYN)`**.

Qual è il numero di sequenza (Sequence Number) relativo?

- Il numero di sequenza relativo è **0**.

pacchetto successivo nella handshake a tre vie.

Quali sono i valori delle porte di origine e destinazione?

- **Porta di Origine (Source Port):** È la porta **80** (il server risponde dalla sua porta di servizio).
- **Porta di Destinazione (Destination Port):** È la porta **58716** (il server risponde esattamente alla porta che H1 aveva aperto).

Quali flag sono impostati?

I flag impostati sono due: **SYN** e **ACK** (Acknowledgment).
entrambi i flag sono impostati (Set/1).

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

Il numero di sequenza relativo è 0 e il numero di riconoscimento relativo è 1.

terzo pacchetto nell'handshake a tre vie.

Quale flag è impostato?

ACK

Il numero di sequenza relativo è 1 e il numero di riconoscimento relativo è 1

Visualizzare i pacchetti usando tcpdump

cosa fa l'opzione -r?

leggere i dati dei pacchetti da un file di cattura precedentemente salvato

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.

1. **`tcp.flags.syn == 1 and tcp.flags.ack == 0`**: Questo filtro mostra solo i pacchetti di richiesta di connessione iniziale (SYN). È utile per individuare tentativi di connessione o potenziali attacchi di tipo "SYN Scan" (port scanning).

2. **`ip.addr == [indirizzo_IP]`**: Sostituendo **`[indirizzo_IP]`** con un IP specifico (es. **`10.0.0.11`**), l'amministratore può isolare tutto il traffico (sia in entrata che in uscita) relativo a un singolo host sospetto o a un server specifico.

3. **`http.request.method == "POST"`**: Questo filtro isola i pacchetti HTTP in cui vengono inviati dati a un server (come credenziali di login o caricamento di file). È fondamentale per monitorare quali informazioni vengono trasmesse verso l'esterno.

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

Wireshark è uno strumento estremamente versatile che può essere utilizzato per:

1. **Risoluzione dei problemi di prestazioni (Troubleshooting):**

   Identificare colli di bottiglia, latenze anomale o pacchetti persi che rallentano le applicazioni aziendali.

2. **Analisi di sicurezza (Network Forensics):**

   Investigare un sospetto attacco informatico analizzando il traffico per trovare malware, esfiltrazione di dati o tentativi di intrusione.

3. **Verifica della conformità e debugging:**

   Aiutare gli sviluppatori di software a verificare che i nuovi protocolli o le applicazioni comunichino correttamente secondo gli standard stabiliti.

4. **Rilevamento di software non autorizzato:**

   Identificare applicazioni o dispositivi "ombra" (Shadow IT) che comunicano sulla rete senza il permesso dell'amministratore.