Report di Analisi del Traffico HTTP e HTTPS con Wireshark

Report di Analisi del Traffico HTTP e HTTPS con Wireshark

Obiettivo dell'esercitazione

L'obiettivo di questo laboratorio è utilizzare **Wireshark** per catturare e analizzare il traffico HTTP e HTTPS, comprendendo le differenze tra i due protocolli e come i dati vengono trasmessi in chiaro o cifrati.

Prerequisiti

- Un sistema con **Wireshark** installato.
- Un browser web per generare traffico HTTP e HTTPS.
- Connessione a Internet.

Passaggi dell'esercizio

Passo 1: Avviare Wireshark e selezionare l'interfaccia di rete

1. Aprire **Wireshark**.
2. Selezionare l'interfaccia di rete attiva (es. **Wi-Fi** o **Ethernet**).
3. Cliccare su **Start** per avviare la cattura dei pacchetti.

> **Nota:** L'interfaccia deve essere scelta in base al tipo di connessione utilizzata per la navigazione web.

Passo 2: Generare traffico HTTP

1. Aprire un browser web.
2. Digitare un indirizzo web che utilizza HTTP (es. `http://example.com`).
3. Premere **Invio** per caricare la pagina.

Analisi del traffico HTTP:

- Tornare su **Wireshark**.
- Nella barra dei filtri, digitare `http` e premere **Invio**.
- Analizzare i pacchetti catturati.

Osservazioni:

- I dati trasmessi sono in **chiaro**.
- È possibile vedere informazioni come **cookie**, **parametri GET e POST**, e il contenuto della richiesta e della risposta.

Passo 3: Generare traffico HTTPS

1. Aprire un browser web.
2. Digitare un indirizzo web che utilizza HTTPS (es. `https://example.com`).
3. Premere **Invio** per caricare la pagina.

Analisi del traffico HTTPS:

- Tornare su **Wireshark**.
- Nella barra dei filtri, digitare `tls` o `ssl` e premere **Invio**.
- Analizzare i pacchetti catturati.

Osservazioni:

- I dati sono **cifrati** e non visibili.
- Si possono osservare i pacchetti di handshake TLS/SSL.
- I dettagli della connessione (certificati, cifratura) sono visibili ma il contenuto della trasmissione no.

Passo 4: Confronto tra HTTP e HTTPS

Caratteristica	HTTP	HTTPS
Cifratura	No	Sì (TLS/SSL)
Sicurezza	Vulnerabile	Sicuro
Visibilità dati	In chiaro	Cifrato
Utilizzato per	Pagine non sensibili	Dati sensibili (login, pagamenti, ecc.)

Conclusioni

- **HTTP** trasmette i dati in chiaro, rendendoli visibili a chiunque intercetti il traffico.
- **HTTPS** protegge la trasmissione grazie alla cifratura TLS/SSL, garantendo riservatezza e sicurezza.
- Wireshark permette di analizzare le richieste e le risposte HTTP ma non i dati cifrati di HTTPS.

Questa analisi dimostra l'importanza di utilizzare HTTPS per proteggere i dati sensibili su Internet.