W4D4 - Alfonso Scoppetta

Requisiti e servizi:

1. Kali Linux - IP 192.168.32.100
2. Windows 7 - IP 192.168.32.101
3. HTTPS server: Attivo
4. Servizio DNS per risoluzione nomi di dominio: Attivo

Traccia:

Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (Kali).

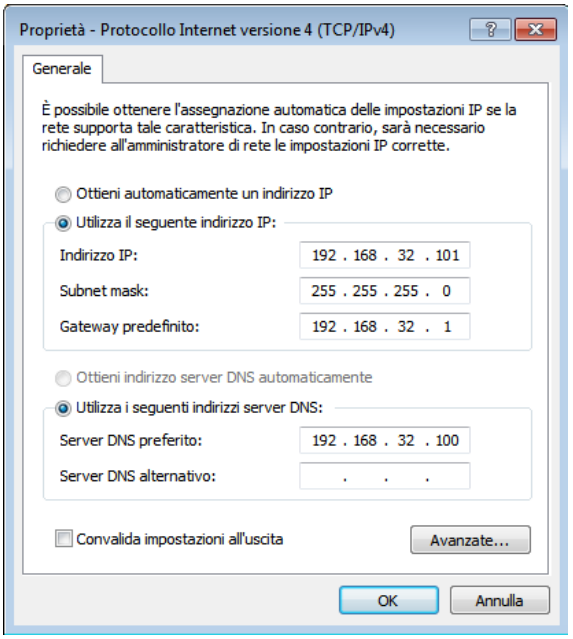
Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

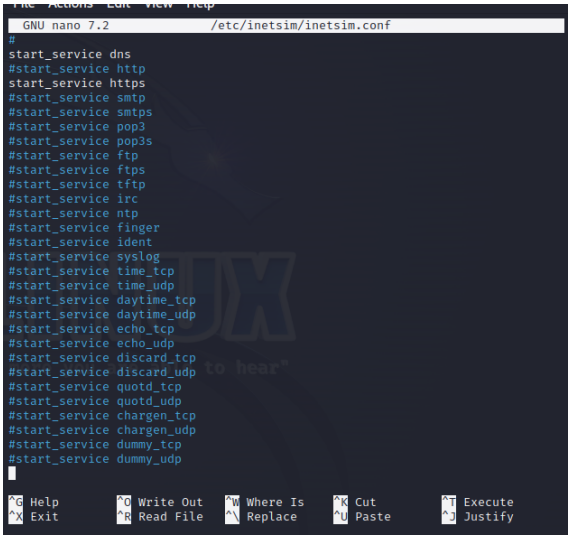
Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

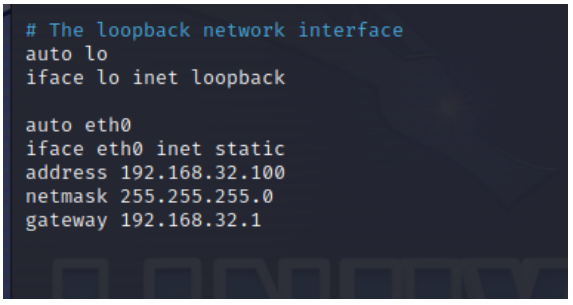
Esecuzione:

1. Configurazione IP Kali Linux e Window:

- Kali Linux: IP 192.168.32.100
- Windows 7: IP 192.168.32.101
- Inserimento dell'IP DNS su Windows 7: IP 192.168.32.100
- HTTPS server: Attivo
- Servizio DNS: Attivo
- Altri servizi spenti







2. Fase 1: Comunicazione tramite HTTPS

1. Configurazione Iniziale:

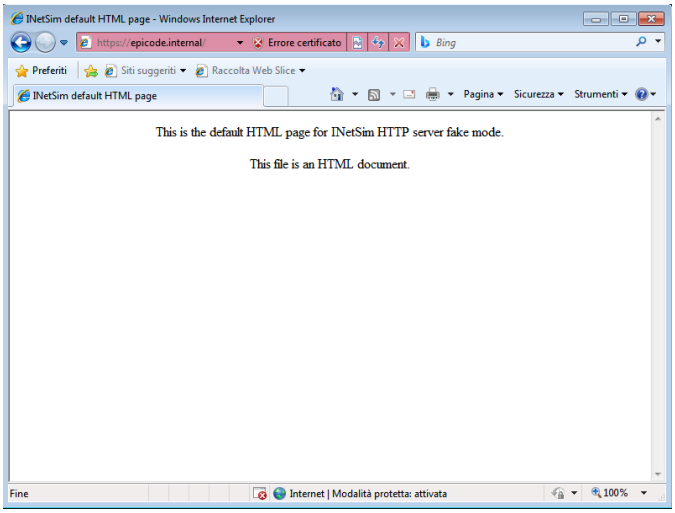
- Kali Linux e Windows 7 sono connessi nella stessa rete virtuale.

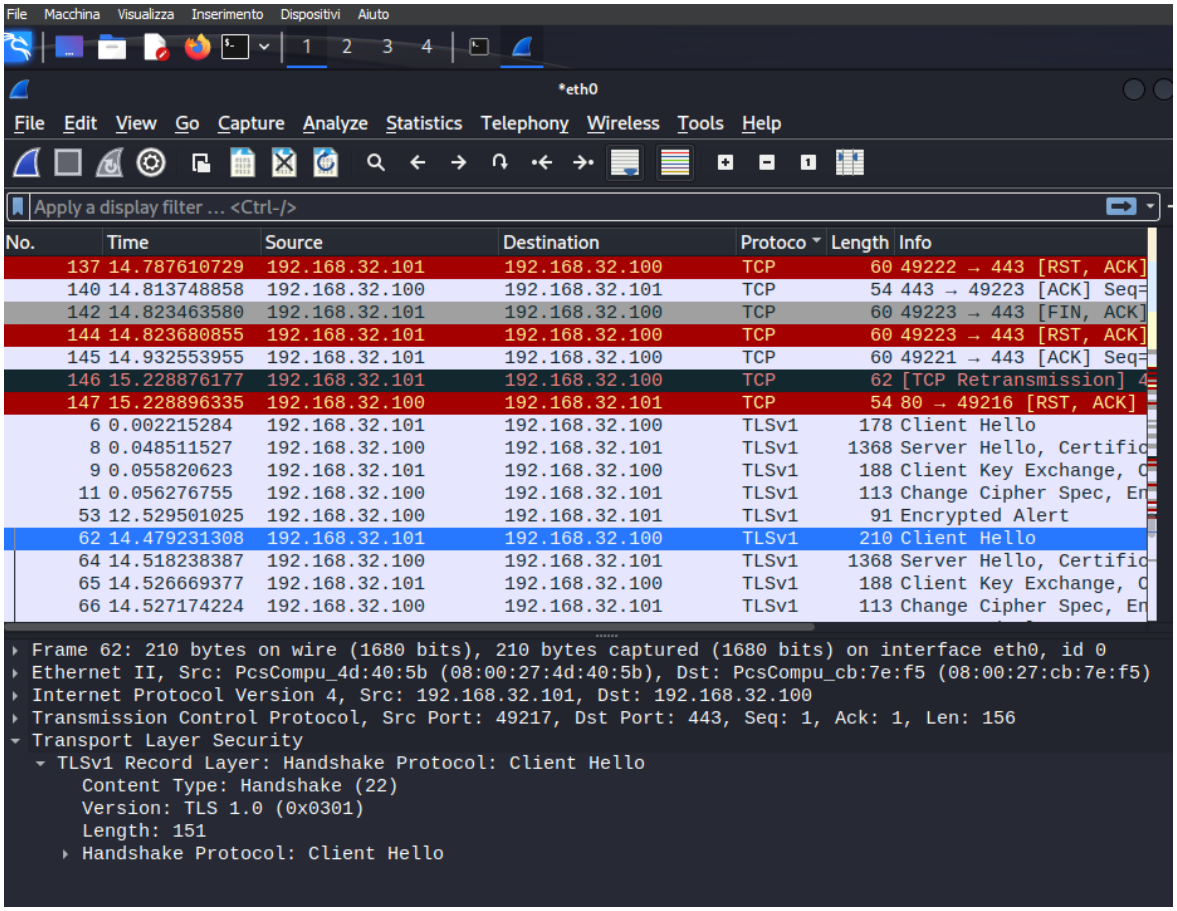
2. Richiesta HTTPS:

- Il client (Windows 7) richiede tramite web browser una risorsa all'hostname "epicode.internal" al server HTTPS (Kali Linux).

3. Wireshark Capture:

- Utilizzando Wireshark, abbiamo intercettato la comunicazione.
- Sorgente MAC: [MAC_Address_Client], Destinazione MAC: [MAC_Address_Server]
- Contenuto richiesta HTTPS: [Contenuto_Richiesta_HTTPS]





3. Fase 2: Comunicazione tramite HTTP

1. Modifica del Server:

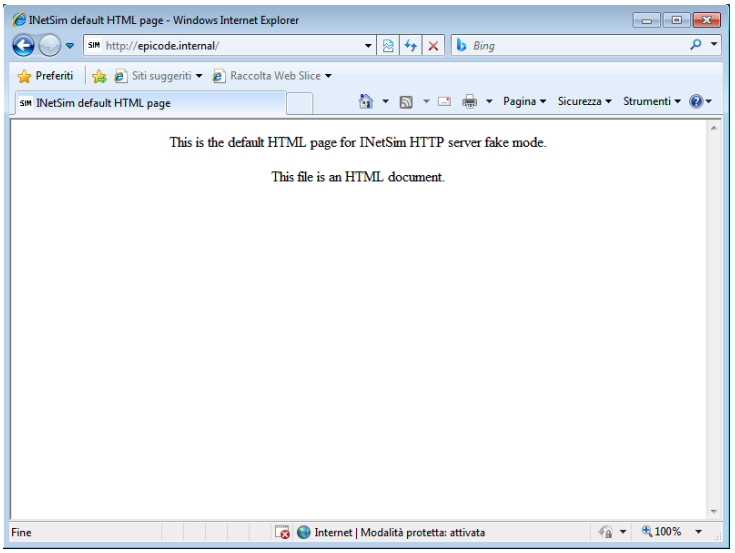
- Ho sostituito il server HTTPS con un server HTTP su Kali Linux.

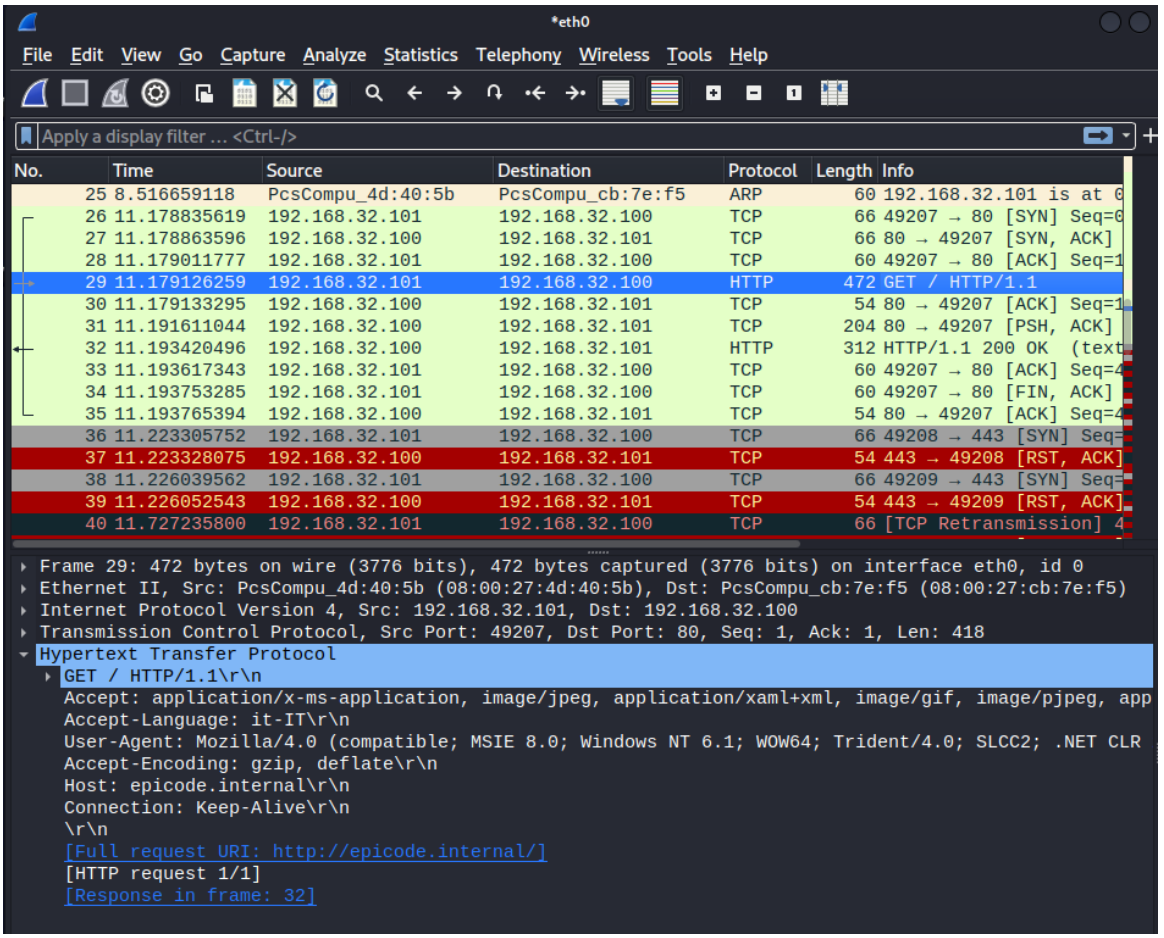
2. Richiesta HTTP:

- Il client (Windows 7) effettua nuovamente la richiesta tramite web browser.

3. Wireshark Capture (HTTP):

- La comunicazione è stata intercettata nuovamente.
- Sorgente MAC: [MAC_Address_Client], Destinazione MAC: [MAC_Address_Server]
- Contenuto richiesta HTTP: [Contenuto_Richiesta_HTTP]





4. Impostazione SERVIZI DNS su Kali Linux

- Ho impostato il DNS default IP: 192.168.32.100, per far si che Kali faccia da server, nell'IP del DNS va inserito il suo stesso IP
- Il Domain name è "epcode.internal" come richiesto dall'esercizio
- Nel DNS static viene associato il Domain name all'IP: epicode.internal

5. Analisi e Conclusioni

- Nel traffico HTTPS, il contenuto della richiesta è crittografato e garantisce sicurezza, mentre nel traffico HTTP, il contenuto è leggibile e chiaro, e potrebbe essere intercettato.
- La principale differenza tra il traffico HTTPS e HTTP è la sicurezza.
- I MAC address di sorgente e destinazione sono gli stessi in entrambe le fasi.
- La principale differenza tra il traffico HTTPS e HTTP è la sicurezza.

Inoltre HTTPS garantisce:

- l'identità dei dati e la loro riservatezza
- la cifratura del traffico
- la verifica di integrità del traffico