SIMULAZIONE COMUNICAZIONE CLIENT – SERVER CON WIRESHARK

OBIETTIVI:

* Simulazione architettura client – server (il client Win7 richiede una risorsa al server Kali tramite browser)
* Intercettazione della comunicazione con Wireshark
* Confronto traffico HTTPS con HTTP

1. Come primo passaggio, provvediamo alla configurazione di rete.

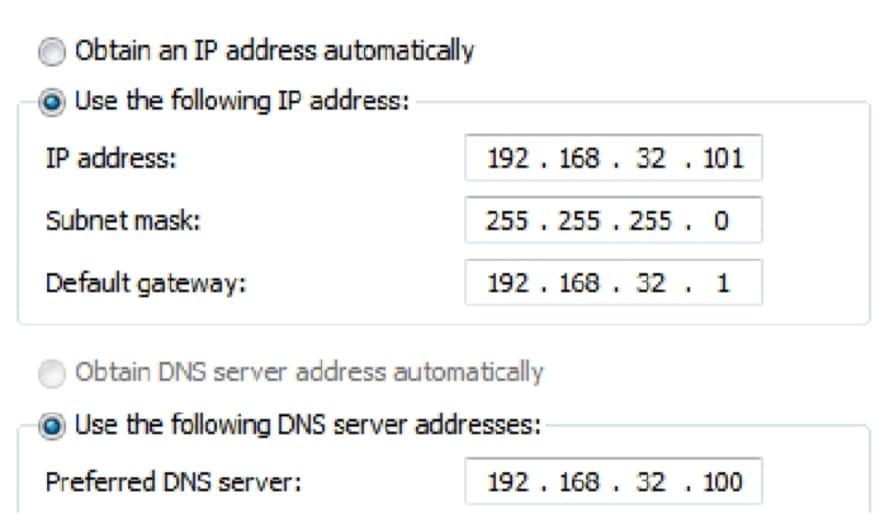
IP Kali Linux: 192.168.32.100

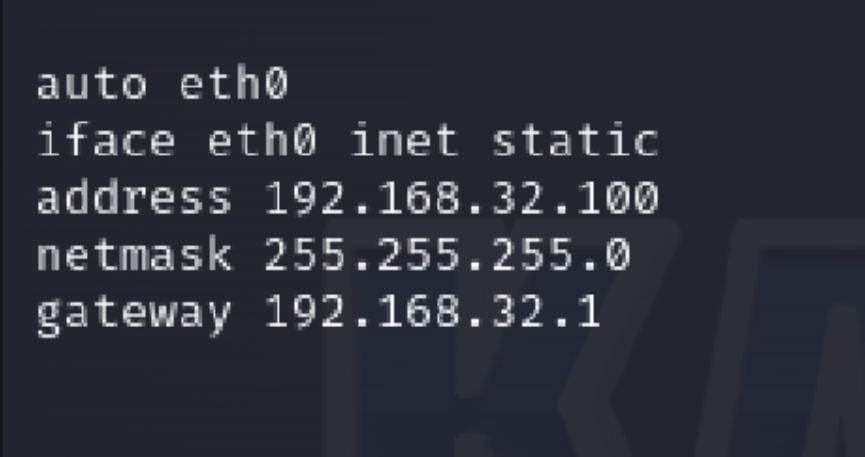
IP Win7: 192.168.32.101

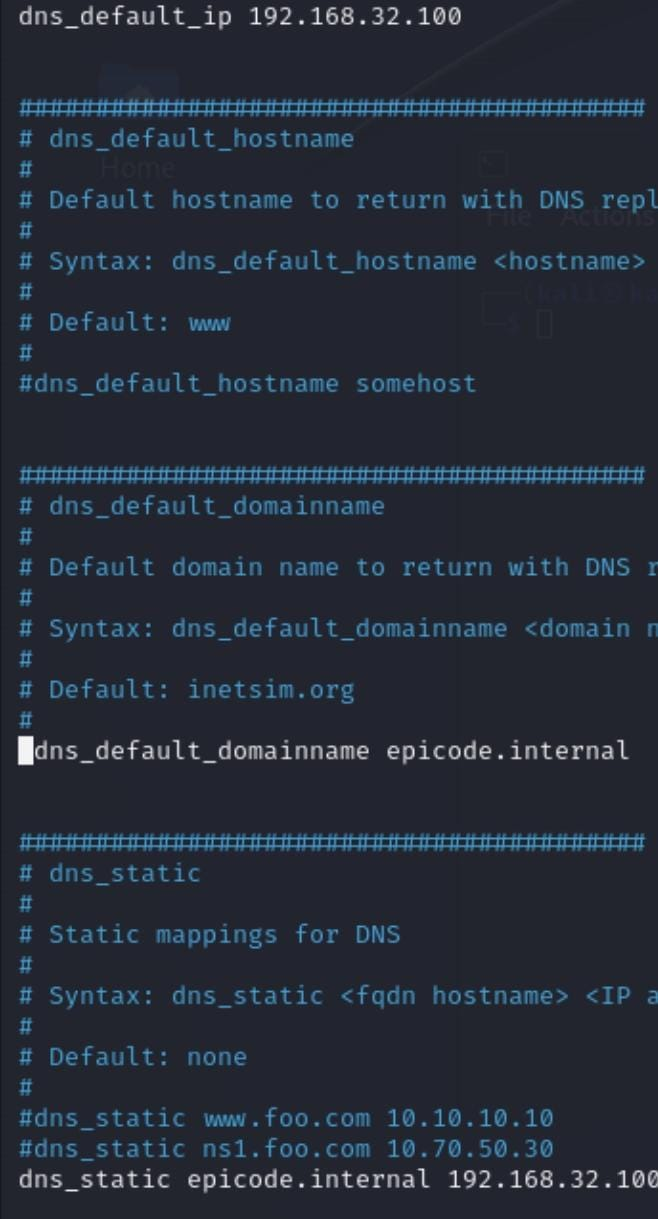
Inserisco poi l’IP DNS su Win7: 192.168.32.100 (considerato che Kali funge da server, nell’IP del DNS va inserito il suo IP)

Inserisco il Domain name “epicode.internal”

Associo all’IP del DNS static il Domain name “epicode.internal”







1. Comunicazione tramite HTTPS

Attivo l’HTTPS serve e il sevizio DNS, lasciando spenti gli altri servizi.



Kali e Win7 sono, ora, connessi sulla stessa rete virtuale.

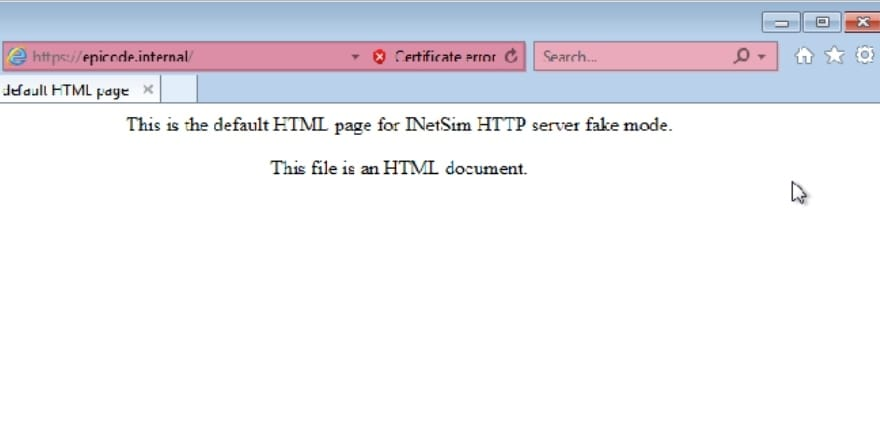
Win7 (client) fa la richiesta di una risorsa all’hostname “epicode.internal” a Kali (server https).

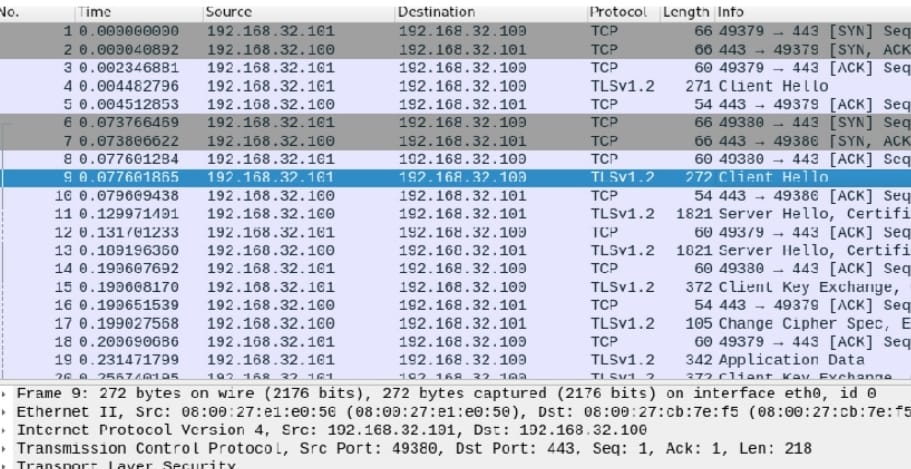
Si intercetta la comunicazione tramite Wireshark.

Sorgente MAC: [MAC\_ Address\_Client]

Destinazione MAC: [MAC\_Address\_Server]

Contenuto richiesta HTTPS: [Contenuto\_Richiesta\_HTTPS]





1. Comunicazione tramite http

Modifica del server HTTPS con HTTP su Kali.

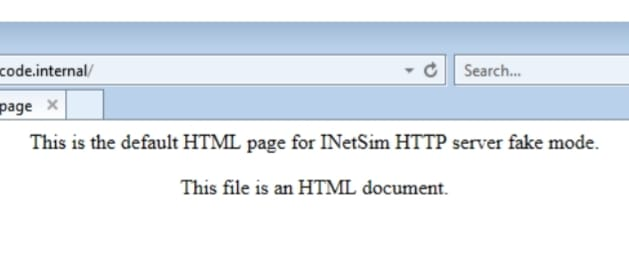
Dopo aver provveduto alla modifica, inoltro nuovamente la richiesta da Win7 tramite web browser.

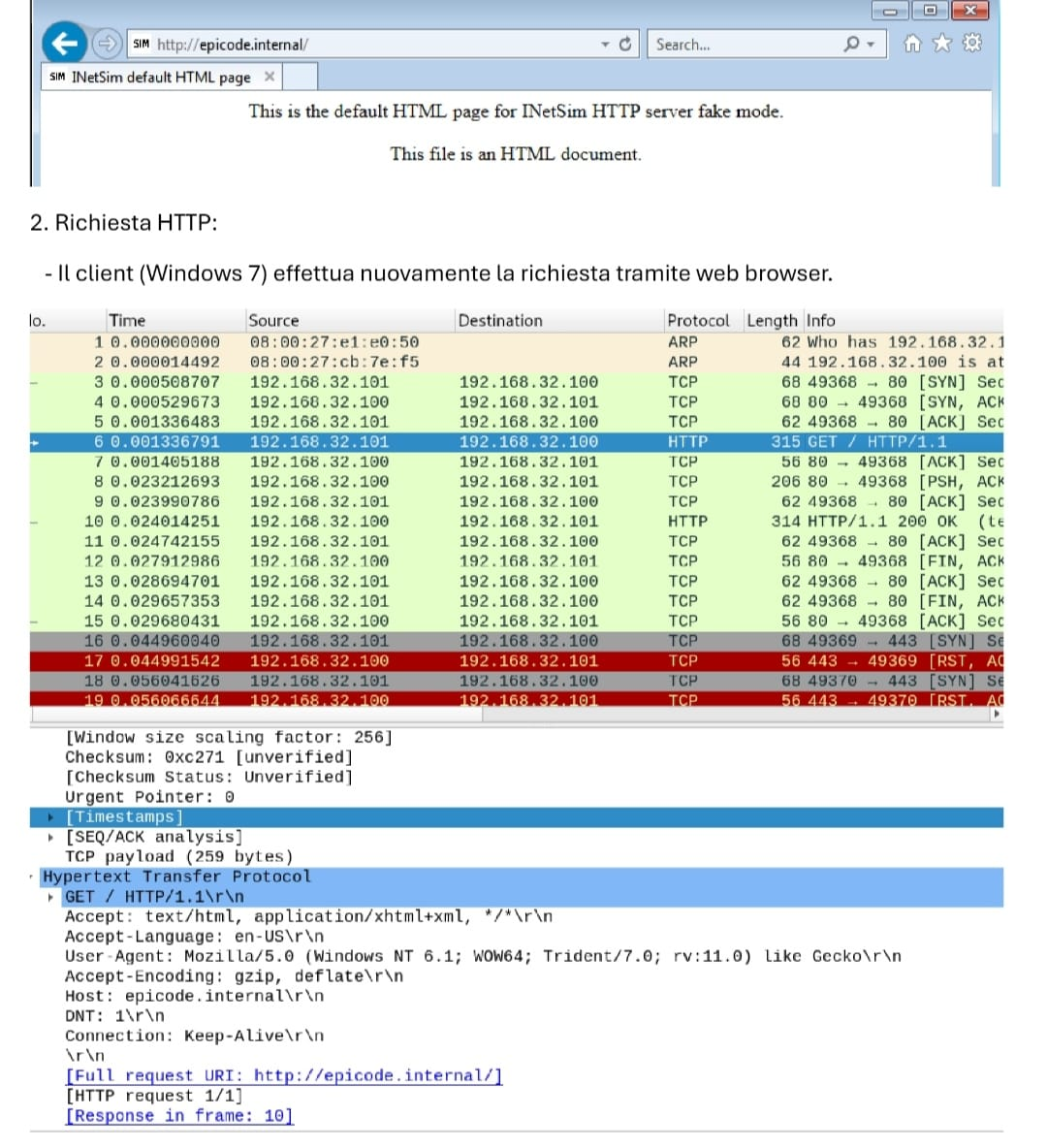
Con Wireshark intercetto la comunicazione.

Sorgente MAC: [MAC\_Address\_Client]

Destinazione MAC: [MAC\_Address\_Server]

Contenuto richiesta http: [Contenuto\_Richiesta\_HTTP]





1. Osservazioni e Conclusioni

Gli indirizzi MAC di sorgente e destinazione rimangono gli stessi in entrambe le modalità di navigazione, mentre il contenuto della richiesta è crittografato con l’https e in chiaro con l’http.

Dunque, la differenza sta nella sicurezza della comunicazione.