PROGETTO GIORNO 5

Requisiti e servizi:

- Kali Linux IP 192.168.32.100
- Windows 7 IP 192.168.32.101
- HTTPS server: attivo
- Servizio DNS per risoluzione nomi di dominio: attivo

Traccia:

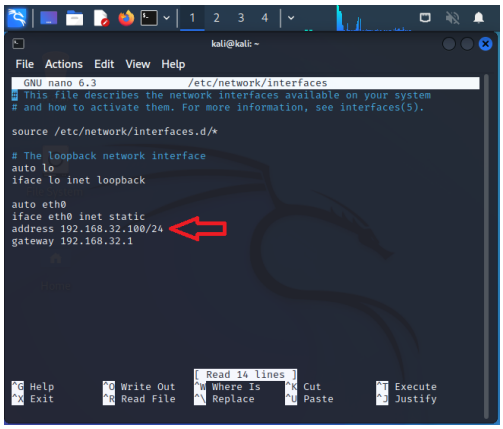
Simulare su VirtualBox un'architettura client-server in cui un client (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'IP di Kali Linux

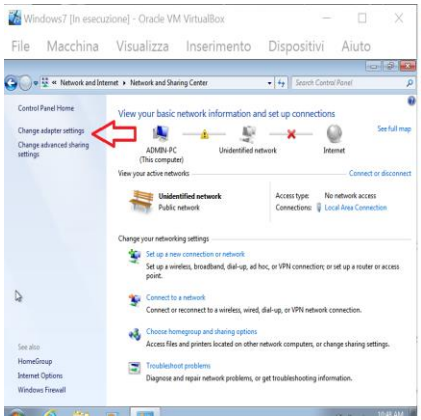
Itercettare poi la comunicazione con Wireshark evidenziando i MAC address di source e dest. ed il contenuto della richiesta HTTPS

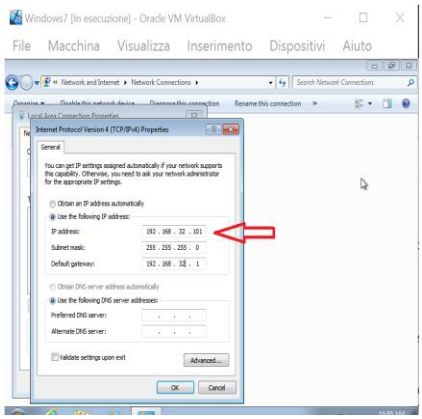
Ripetere sostituendo al server HTTPS il server http, intercettando nuovamente ed evidenziando le eventuali differenze tra i traffici catturati con HTTP e HTTPS.

Svolgimento:

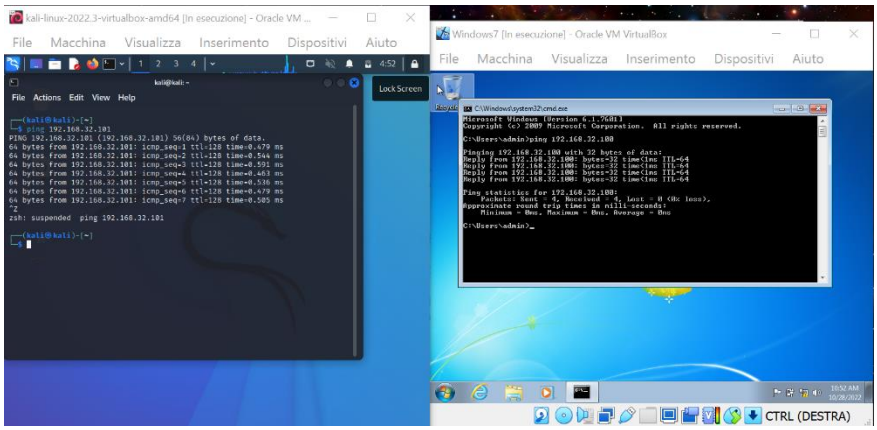
Cambiare IP di Kali e Windows come mostrato nelle figure







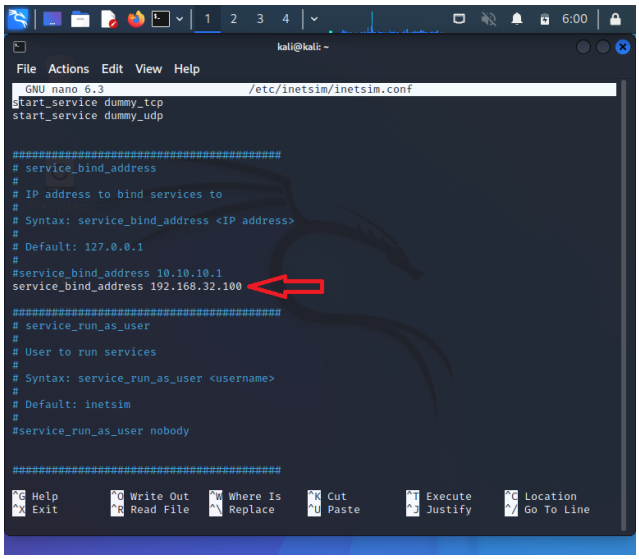
Verificare la connessione facendo fare il ping tra le due macchine

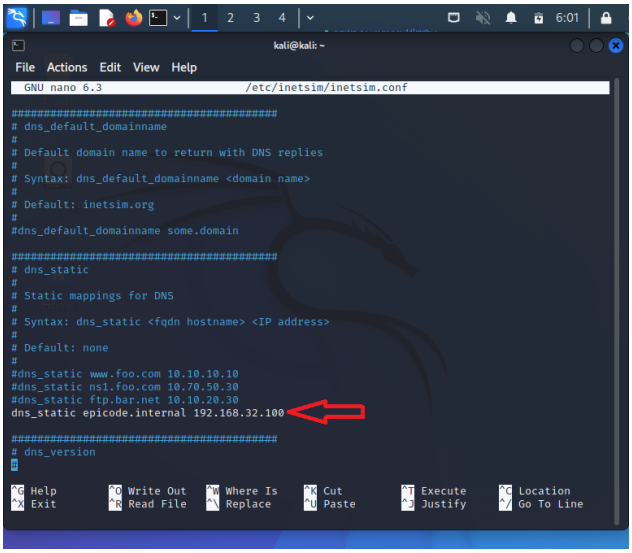


Attraverso il Terminal di Kali mettere il comando ping 192.168.32.101 (IP Windows 7).

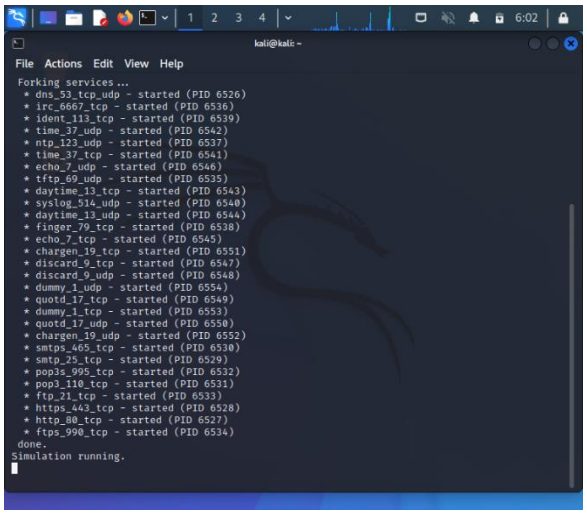
Attraverso il cmd di Windows 7 inserire il comando ping 192.168.32.100 (IP Kali).

Tramite il Terminal di Kali inserire il comando sudo nano /etc/inetsim/inetsim.conf e cambiare il bind address con IP 192.168.32.100 ed il DNS static con epicode.internal

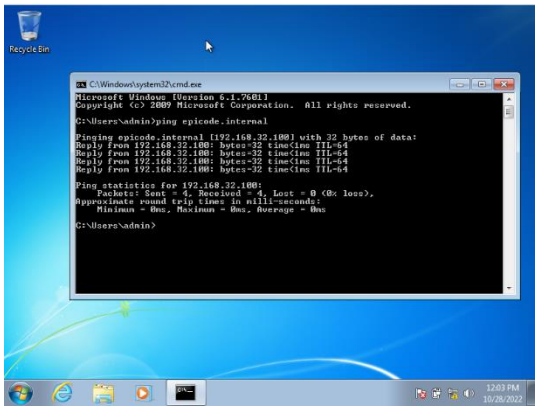




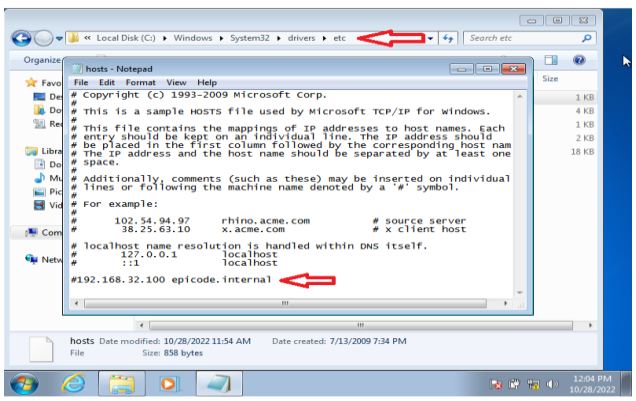
Tramite Terminal Kali avviare inetsim e verificare che le modifiche siano state fatte con successo

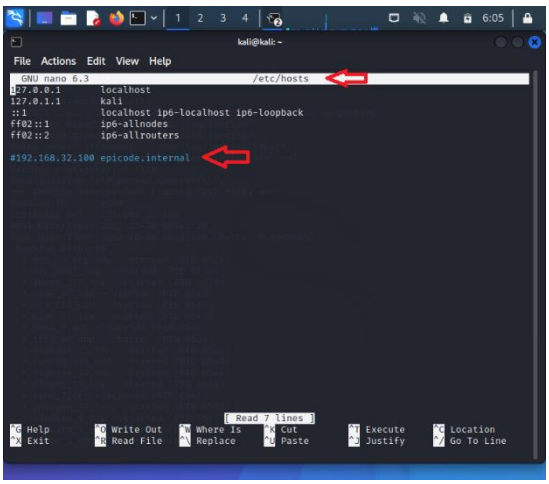


Ora vericare se Windows 7 riesce a fare il ping per il percorso epicode.internal:



Tramite i driver del System32 di Windows andare a modificare il file hosts e su Terminal Kali tramite sudo /etc/hosts inserendo Inserire #192.168.32.100 epicode.internal

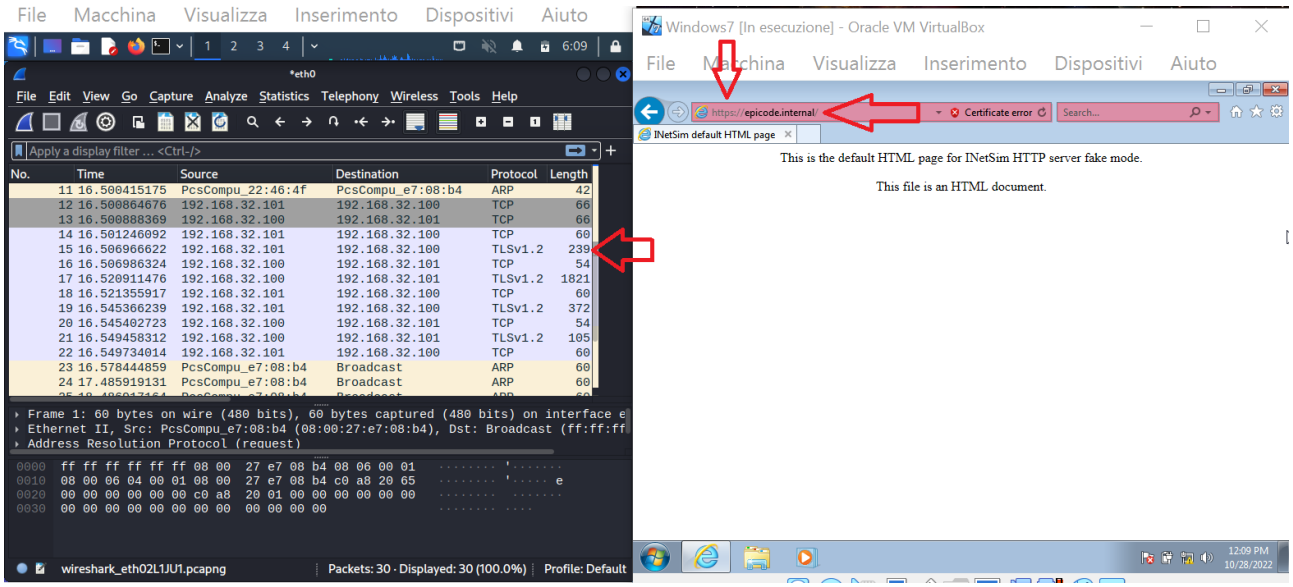


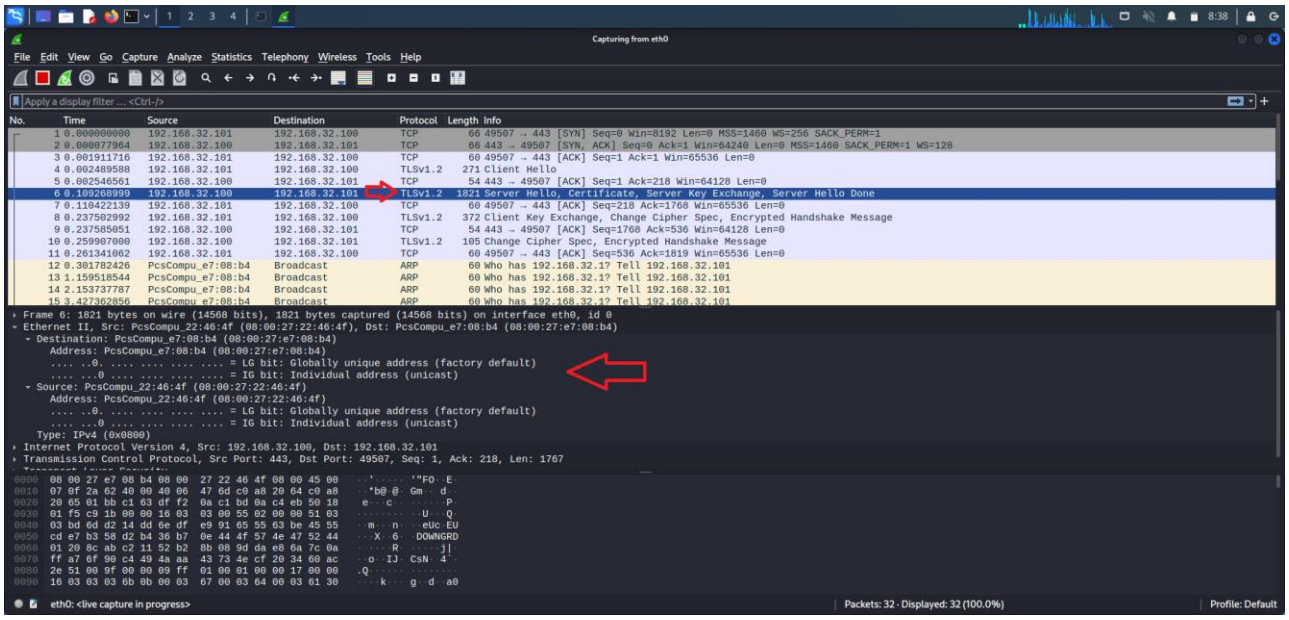


Così facendo il DNS convertirà epicode.internal nell'indirizzo IP specificato; Windows 7 si è collegato al DNS di Kali.

Mantenere aperta la finestra del terminal Kali di inetsim:

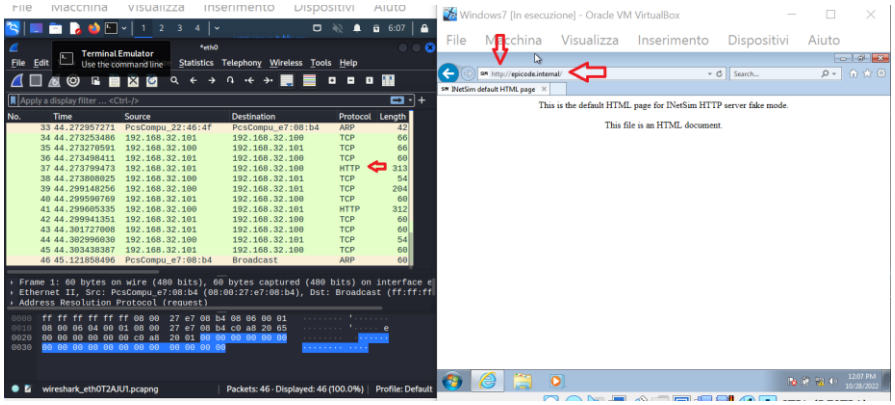
Aprire Internet Explorer su Windows 7 iniziando la ricerca HTTPS di "epicode.internal" e nello stesso tempo avviare la cattura dati di Wireshark su Kali

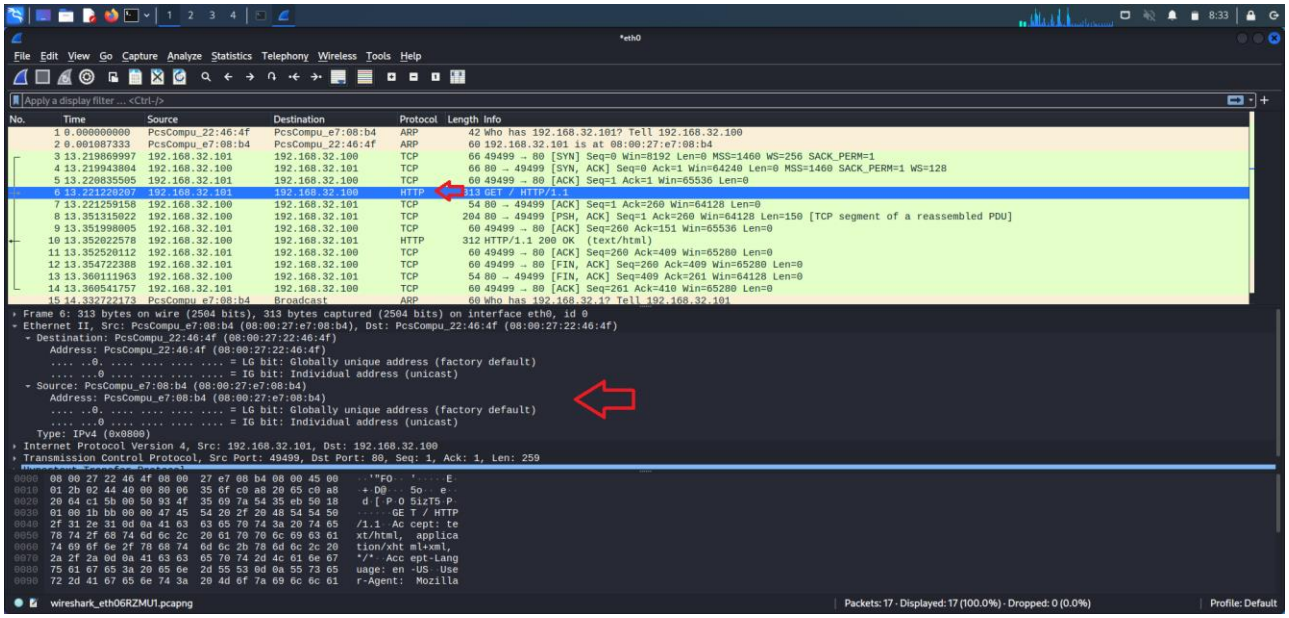




Durante la ricerca internet verificare il passaggio di pacchetti TLS con la cattura Wireshark ed evidenziare gli indirizzi MAC source e dest. come evidenziato in figura.

Ripetere lo stesso procedimento per HTTP





Come evidenziato nelle foto ci sono delle differenze negli indirizzi MAC lato client e server nei traffici HTTPS e HTTP.

HTTPS è un metodo per eseguire HTTP su un protocollo cifrato, come TLS (si può vedere in figura).

Le differenze del traffico catturato da Wireshark sarà quindi evidente dal tipo di messaggio catturato,

nel primo caso (HTTPS) sarà un TLS, mentre nel caso di HTTP sarà un TCP e saranno visibili le risposte di SYN e ACK.