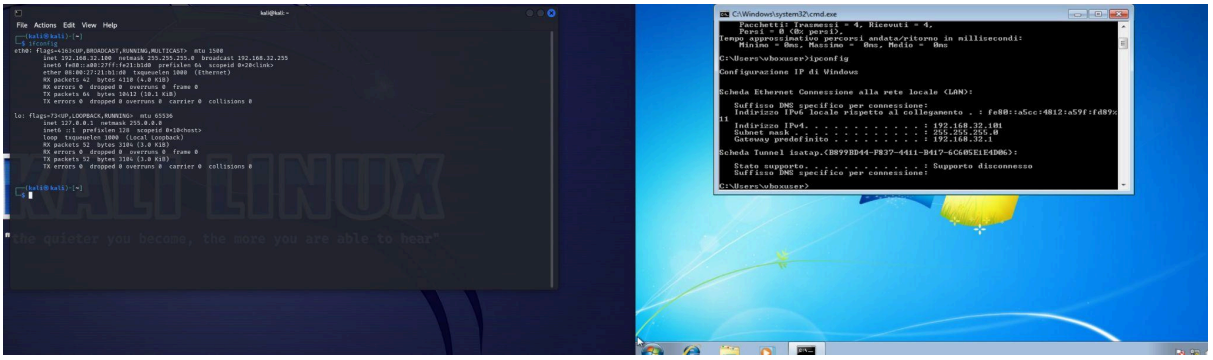
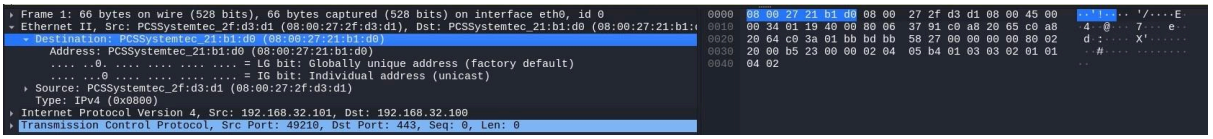
ESERICITAZIONE M1 W4 D4

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.

Creazione del laboratorio con le specifiche richieste:

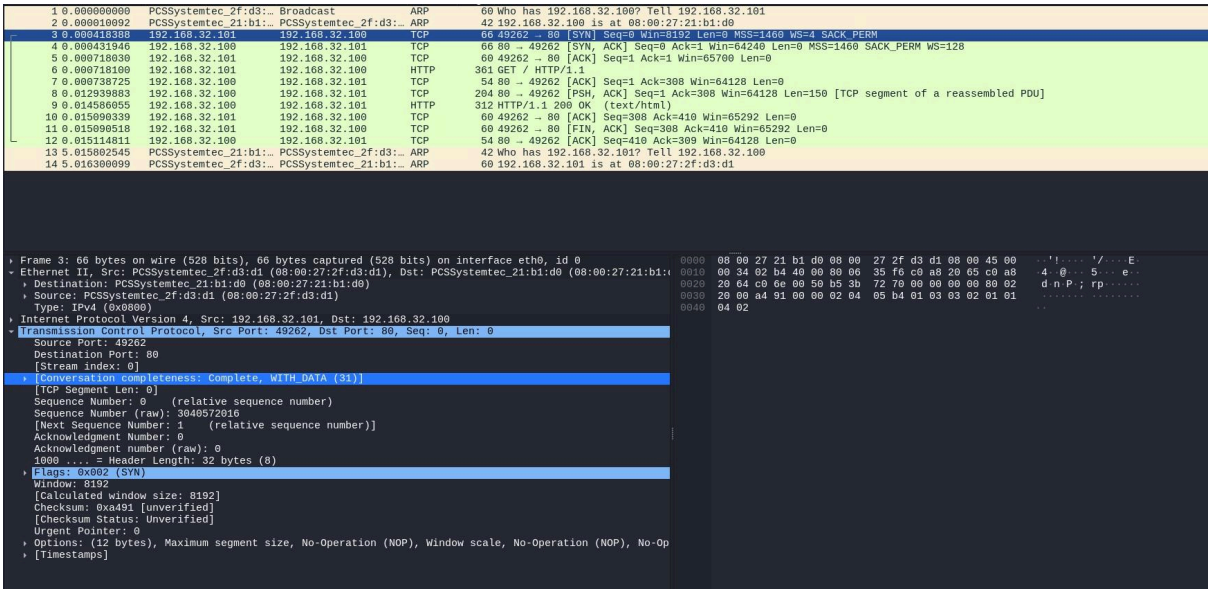


Evidenziamento del MAC source (08:00:27:2f:d3:d1)
MAC destination (08:00:27:21:b1:d0)



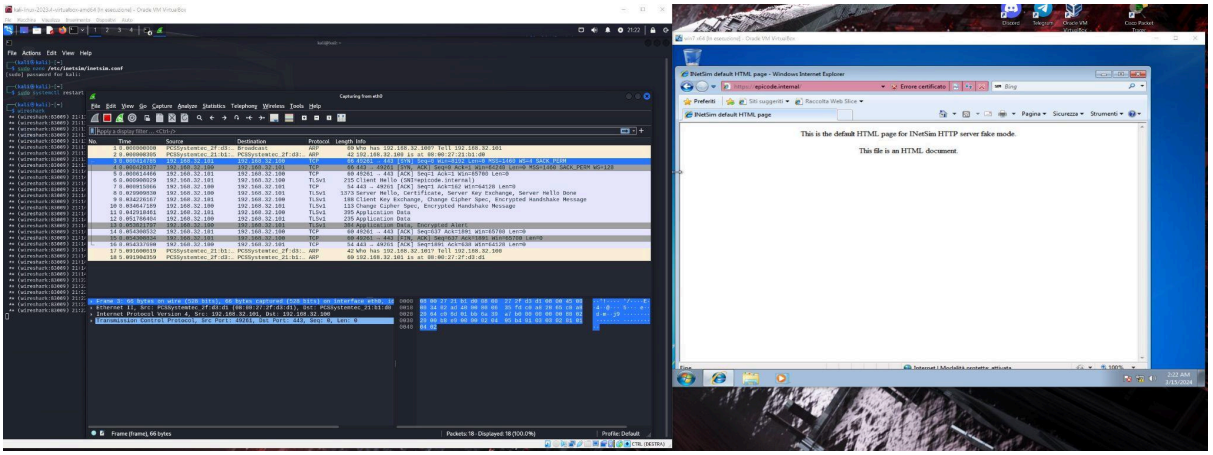
Tramite inetsim andremo a usufruire dei servizi di HTTP,HTTPS e DNS impostando kali come server DNS assegnando lo stesso ip della VM di kali e attivando la fakemode_http. Successivamente andremo a settare il server DNS dicendo di risolvere epicode.internal in 192.168.35.100. Dopo si avvia inetsim e wireshark su kali.

Richiesta tramite Win7 Http://epicode.internal.



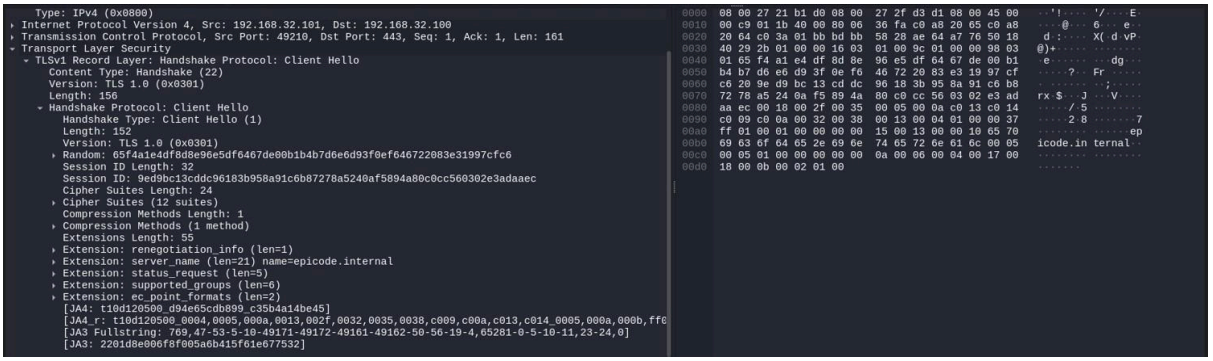
Possiamo notare come avviene l'instaurazione del collegamento tra il fake server e il browser di win7.
Il primo protocoll troviamo l'ARP, collega un indirizzo IP in continua evoluzione a un indirizzo fisso del computer fisico chiamato MAC. Essendo la chace dell'ARP ha necessità di sapere quale MAC corrisponde a quell'IP, cosi da non ripetere molto spesso questa procedura.
Successivamente avviene l'instaurazione del TCP che va a chiedere una connessione nelle porte richieste. Si può notare l'avvio della richiesta della della connessione alle porte e l'instaurazione del protocollo SYN SYN ACK. Dopo essere andato a buon fine inizia la trasmissione del HTTP e infine notiamo che il 192.168.32.101 richiede al TCP il FIN, ACK per la chiusura della connessione.

Richiesta tramite WIN7 https:/epicode.internal



Instaurazione del collegamento avviene come nel precedente caso dell'http fino alla conferma del canale di comunicazione con il protocollo TCP e l'avvio del SYN SYN ACK, ma successivamente notiamo l'instaurazione del TLS.

Il funzionamento del protocollo TLS può essere suddiviso in tre fasi principali
Negoziazione fra le parti dell'algoritmo da utilizzare
Scambio delle chiavi di autenticazione
Cifratura simmetrica e autenticazione dei messaggi



Nella prima fase, il client e il server negoziano il protocollo di cifratura che sarà utilizzato nella comunicazione sicura, il protocollo per lo scambio delle chiavi e l'algoritmo di autenticazione nonché il Message authentication code (MAC).Si nota come tutto il layer applicativo sia sotto protocollo LSV e quindi crittografato. La chiusura avverrà sempre sotto richiesta del client (VM win7) che richiedere un FIN ACK tramite protocollo TCP e successiva risposta di ACK del server (kali).