PROGETTO: SIMULAZIONE DI UNA RETE COMPLESSA

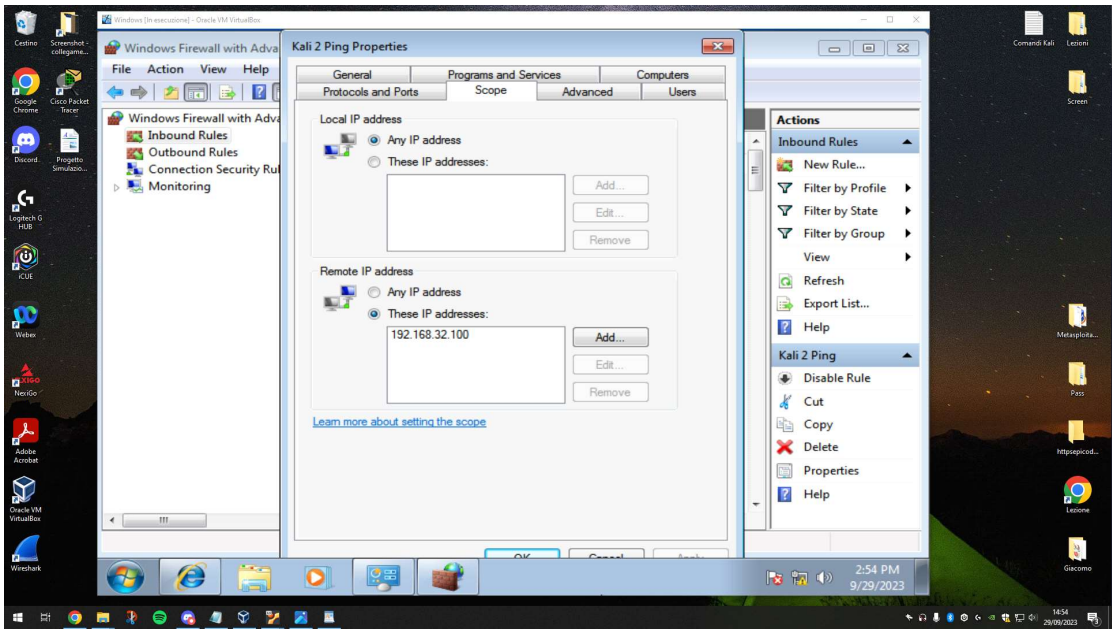
Nell'esercizio di oggi dobbiamo simulare, in ambiente virutale, un'architettura client server, creato con Kali Linux, in cui un client esterno, windows 7, richiede tramite web browser una risorsa all'hostname epicode.internal.

Come prima cosa ho reimpostato gli indirizzi IP delle due macchine virtuali:

IP KaliLinux 192.168.32.100

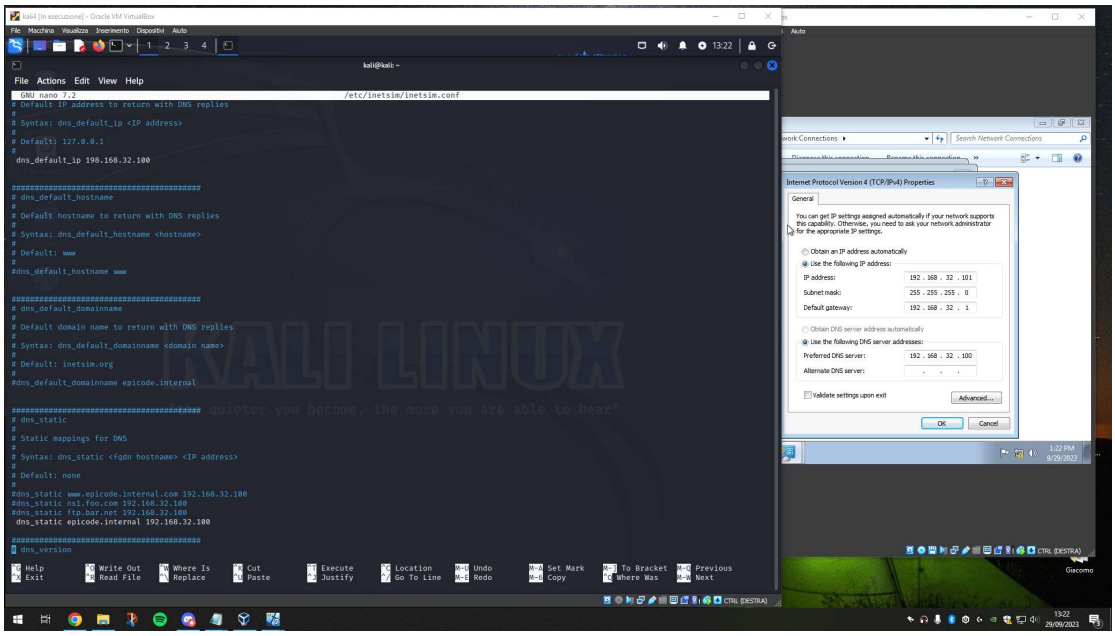
IP Windows 7 192.168.32.101

e attivando la funzione DNS su KaliLinux, ho creato un'eccezione al firewall di Windows7 per poter rendere possibile il collegamento tra le due macchine.

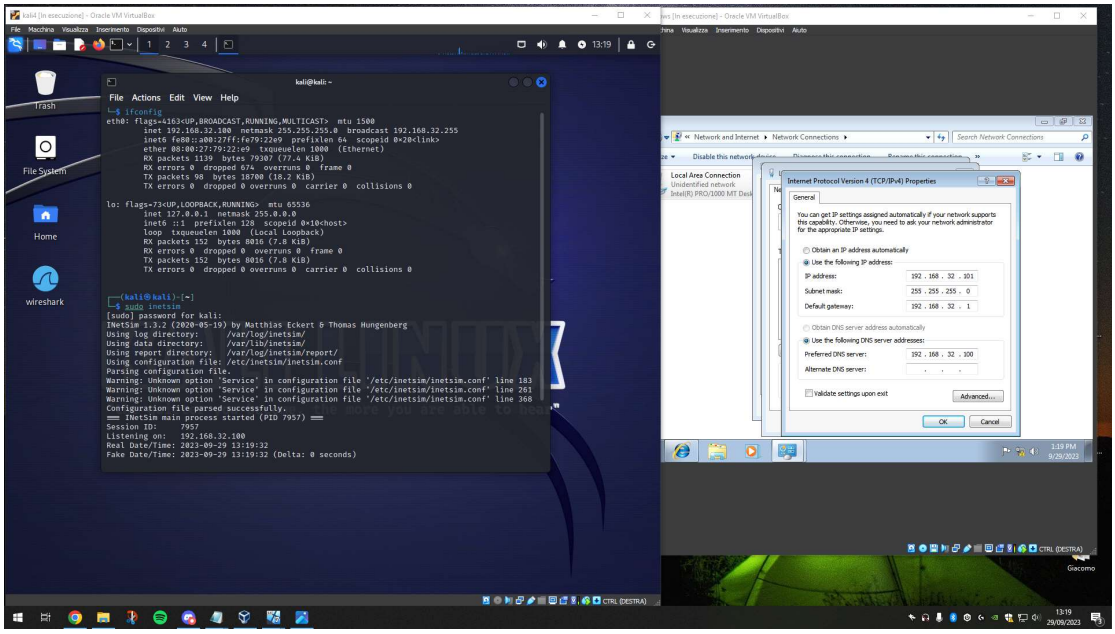


Una volta fatto ciò ho impostato la rete da Kali attaverso il comando

sudo nano /etc/inetsim/inetsim.conf impostando i vari valore di DNS così da poter comunicare con la macchina di Windows7, poi sempre su inetsim ho lavorato su HTTP e HTTPS per avere la possibilità di fare ciò che mi chiedeva il compito ossia cercare su internet explorer da W7 la pagina epicode.internal.

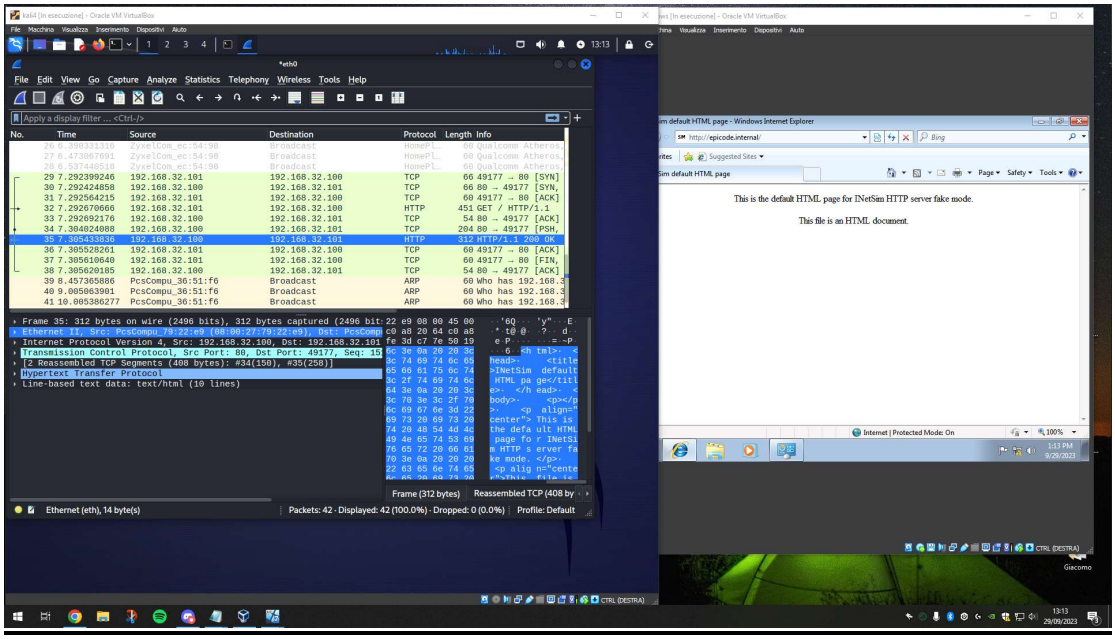


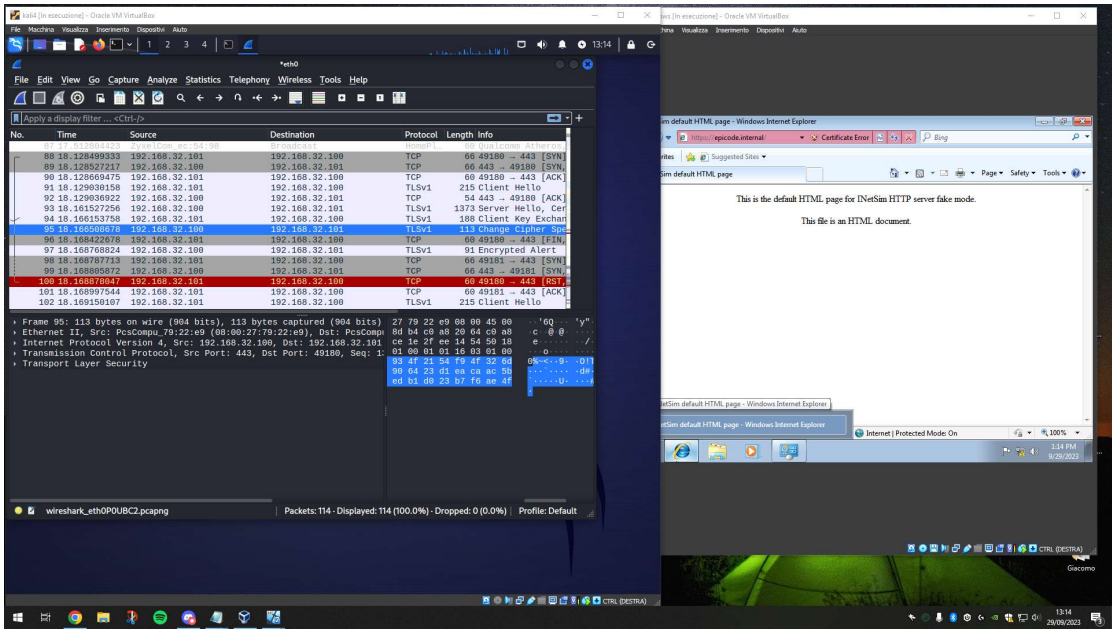
Una volta fatto ciò ho avviato il comando sudo inetsim così da far comunicare le due macchine in DNS.



Fatto ciò sono passato alla fase finale dell'esercizio che prevedeva di sniffare la comunicazione con Wirshark tra le due macchine con IP 192.168.32.100 e IP 192.168.32.101.

Questa comunicazione avviene attraverso la ricerca su Internet Explorer della pagina epicode.internal, prima configurando l'indirizzo HTTP e poi HTTPS.





Le principali differenze tra le due sniffate sono:

-Le porte utilizzate per il passaggio di dati HTTP porta 80 mentre HTTPS porta 443 ;

-Ma la cosa più importante e che differenzia HTTP da HTTPS sono i pacchetti criptati durante la sniffata di HTTPS mentre in HTTP sono chiaramente visibili.

-Altra cosa che ho notato è che la pagina HTTPS è più lenta della pagina HTTP a caricarsi e questo perchè tutti i pacchetti sono criptati quindi i dati si trasferiscono più lentamente.