Esame di fine modulo, svolgimento logico

SACHELE

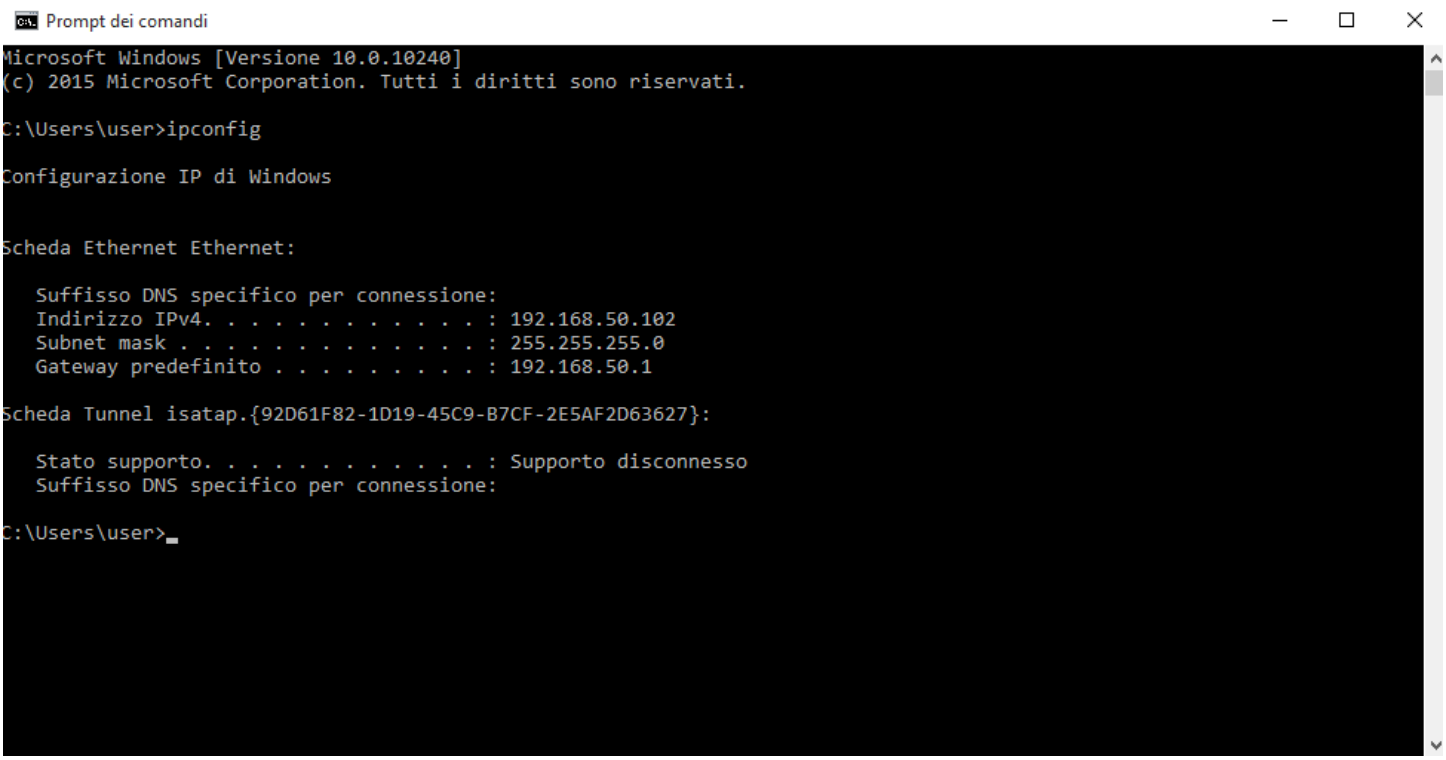
Traccia: Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.50.102 Windows richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.50.100 Kali.

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.

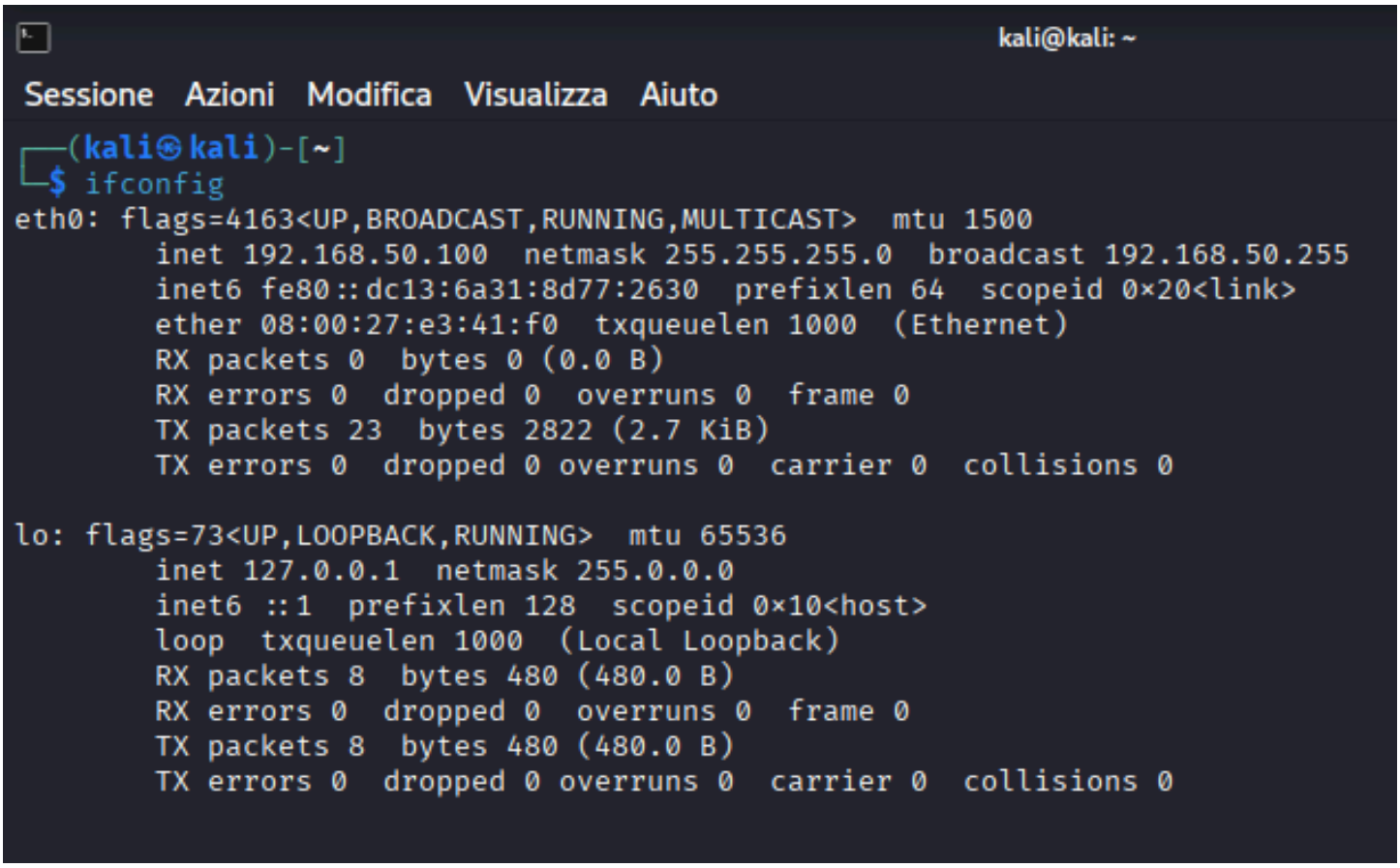
RAGIONAMENTO

I requisiti sono: avere **Kali** e **Windows** già con un IP assegnato, un HTTPS server attivo e servizio DNS attivo.

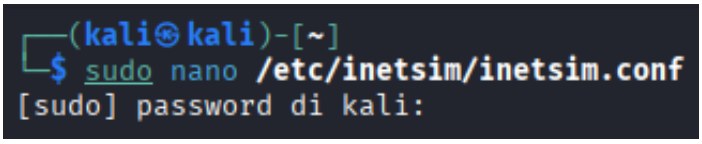
IP assegnato a **Windows**



IP assegnato a **Kali**

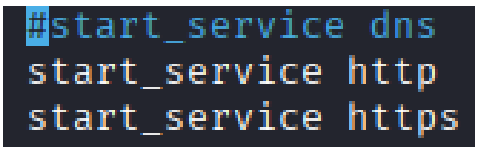


Apriamo Inetsim per iniziare a capire come configurare un servizio DNS:

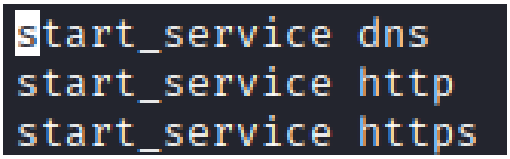


Scorrendo le opzioni, troviamo start_service DNS, lo modifichiamo e lo rendiamo attivo:

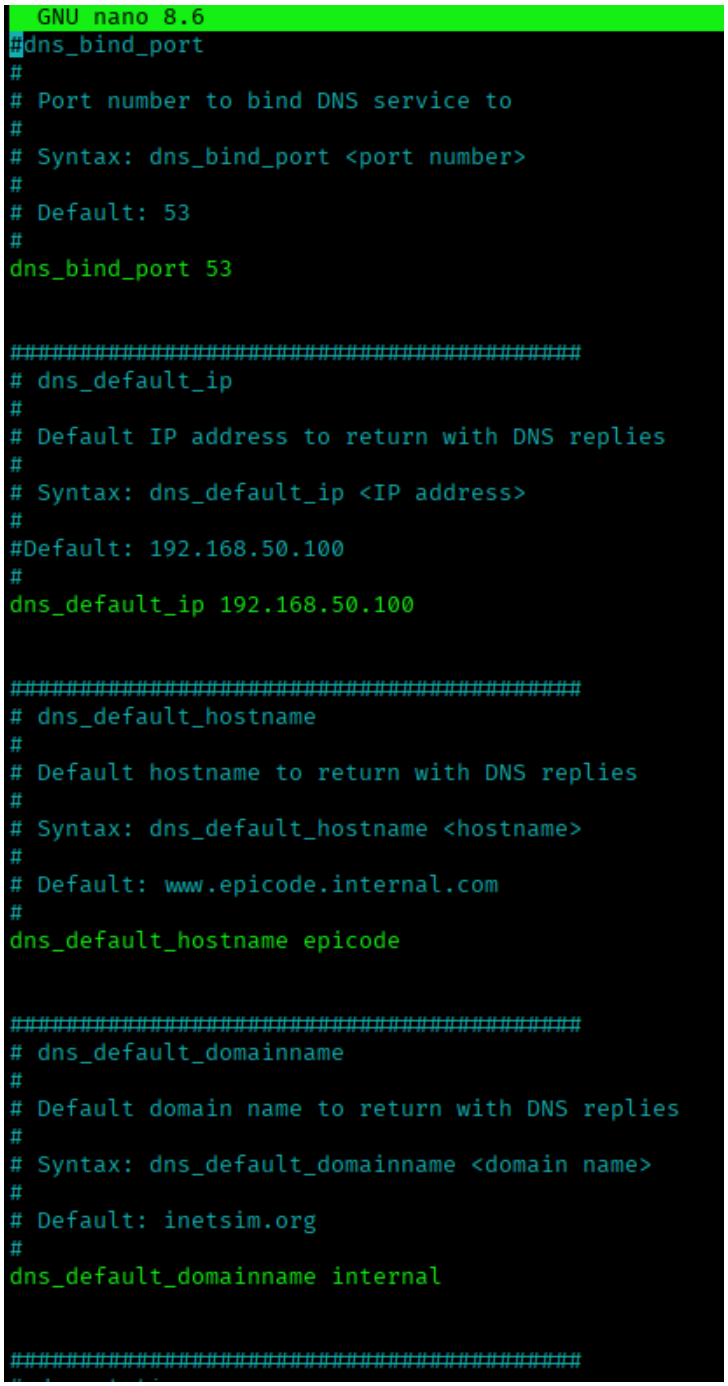
DNS service non attivo (in figura sotto)



DNS service attivo:



Proseguendo nella nostra cartella troviamo altre impostazioni che sono state modificate per poter configurare correttamente il DNS service:

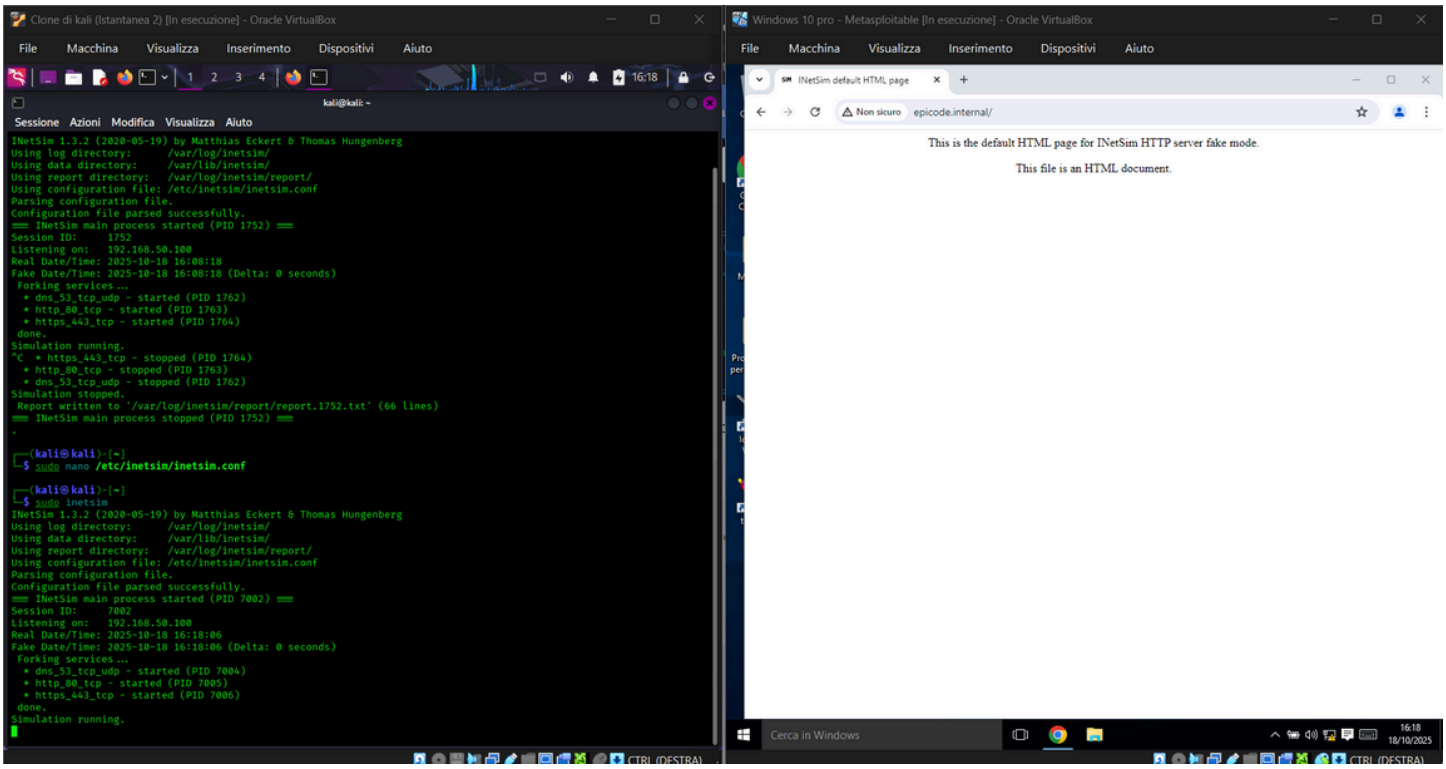


Salviamo le modifiche utilizzando il comando CTRL+O seguito da invio e CTRL+X

(nell'attivare InetSim ho riscontrato degli errori di compatibilità con perl, dopo svariate ricerche online, sono riuscito a trovare una soluzione downgradando perl e del dns di inetsim)

TEST FUNZIONAMENTO

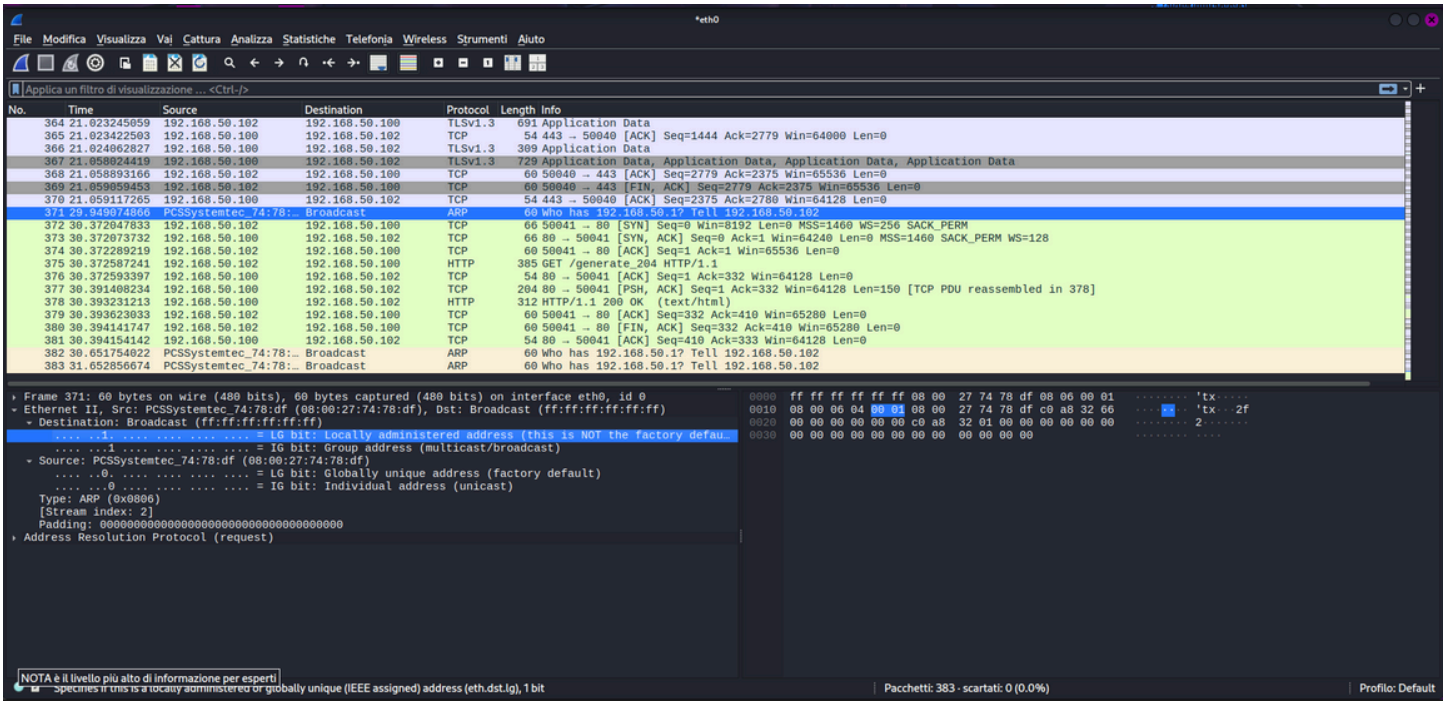
Attiviamo InetSim e verifichiamo che su Windows sia possibile accedere al nostro server.



Inetsim è attivo, di conseguenza Windows riesce a connettersi ad epicode tramite DNS hostname epicode.internal.

Passiamo adesso all'analisi dei pacchetti tramite Wireshark evidenziando le principali differenze tra l'utilizzo del protocollo http ed https.

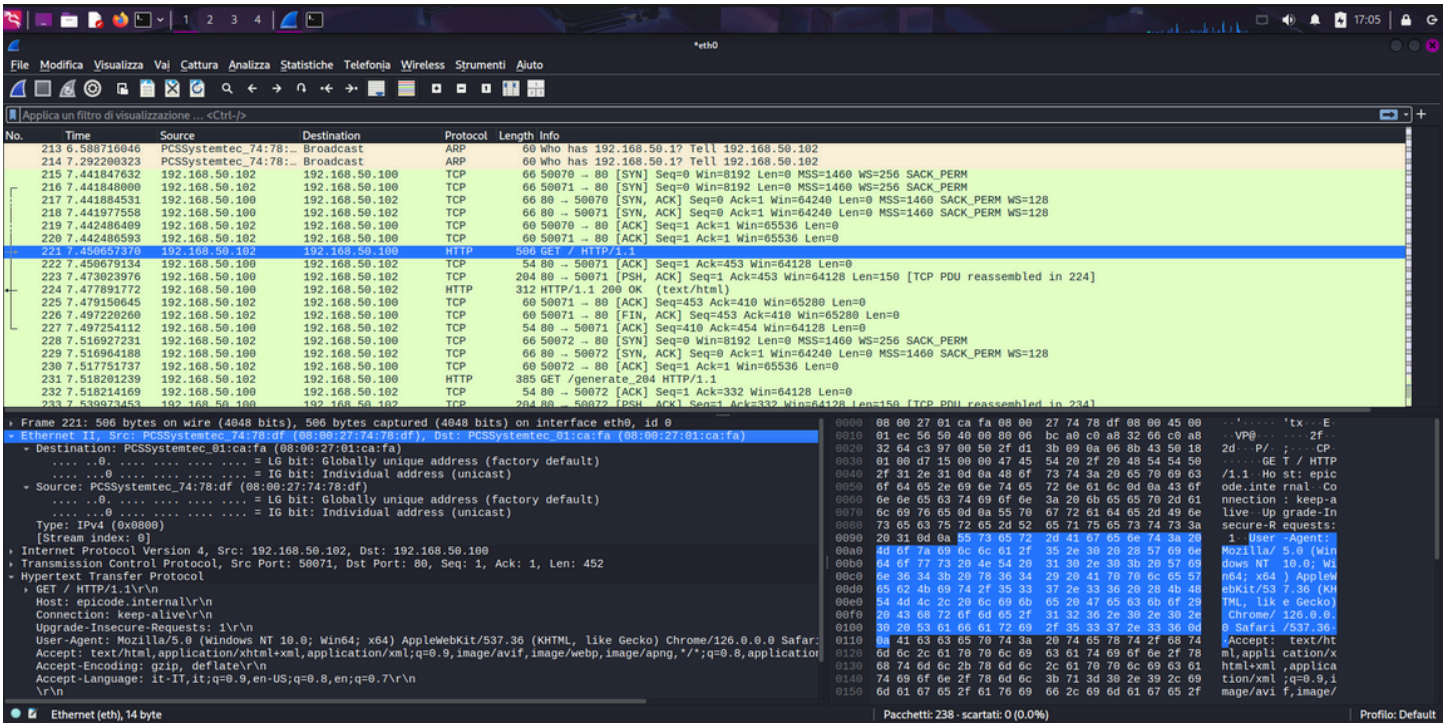
PROTOCOLLO HTTPS



Possiamo notare come sia possibile vedere il mac address del server ma non della macchina che richiede la connessione (windows 10 con ip 192.168.50.102)

Tutte le informazioni sui pacchetti trasmessi vengono criptate.

PROTOCOLLO HTTP



Nel protocollo http sono visibili molte più informazioni come il mac address di entrambe le macchine. I pacchetti non vengono criptati e possiamo visualizzare ulteriori informazioni come sistema operativo, risposta del server.