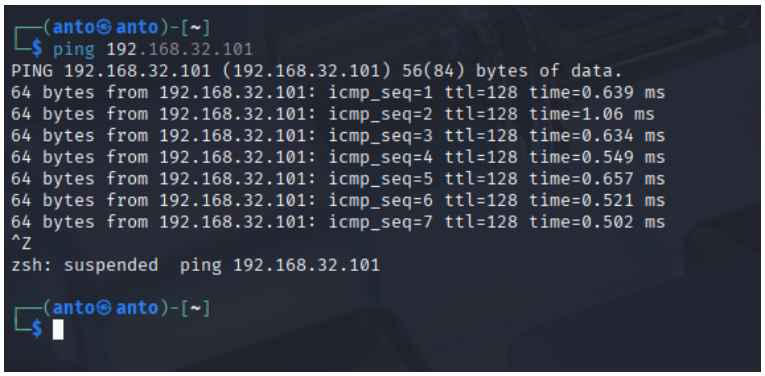
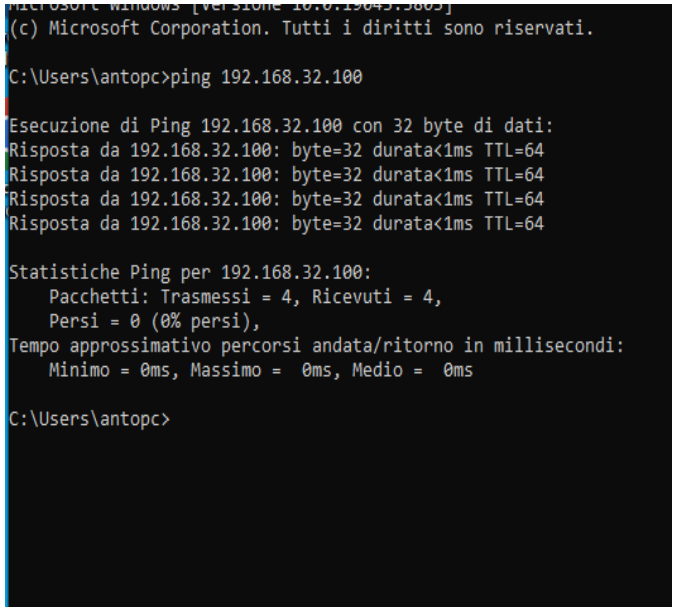
Progetto Finale – Primo Mese

Indice:

1) Configurazione Indirizzi IP Kali e Window

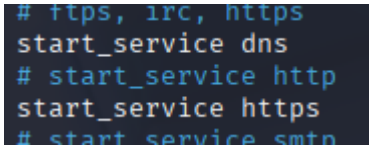
Come primo passaggio fondamentale per una simulazione corretta *client-server* ho configurato i seguenti indirizzi IP delle due macchine virtuali:
Kali: 192.168.32.100
Windows: 192.168.32.101
Successivamente ho eseguito un test del *ping* per controllare il corretto funzionamento dell'ambiente di laboratorio virtuale.



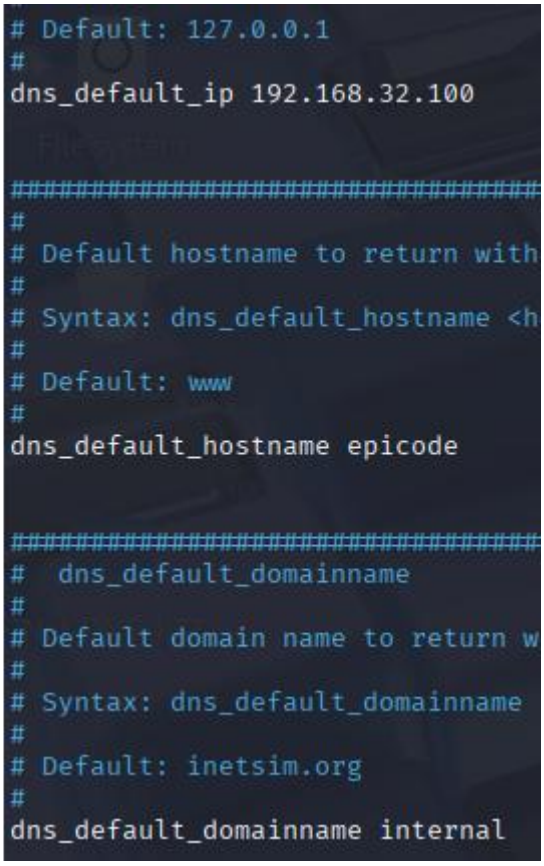


2) Configurazione HTTPS e DNS

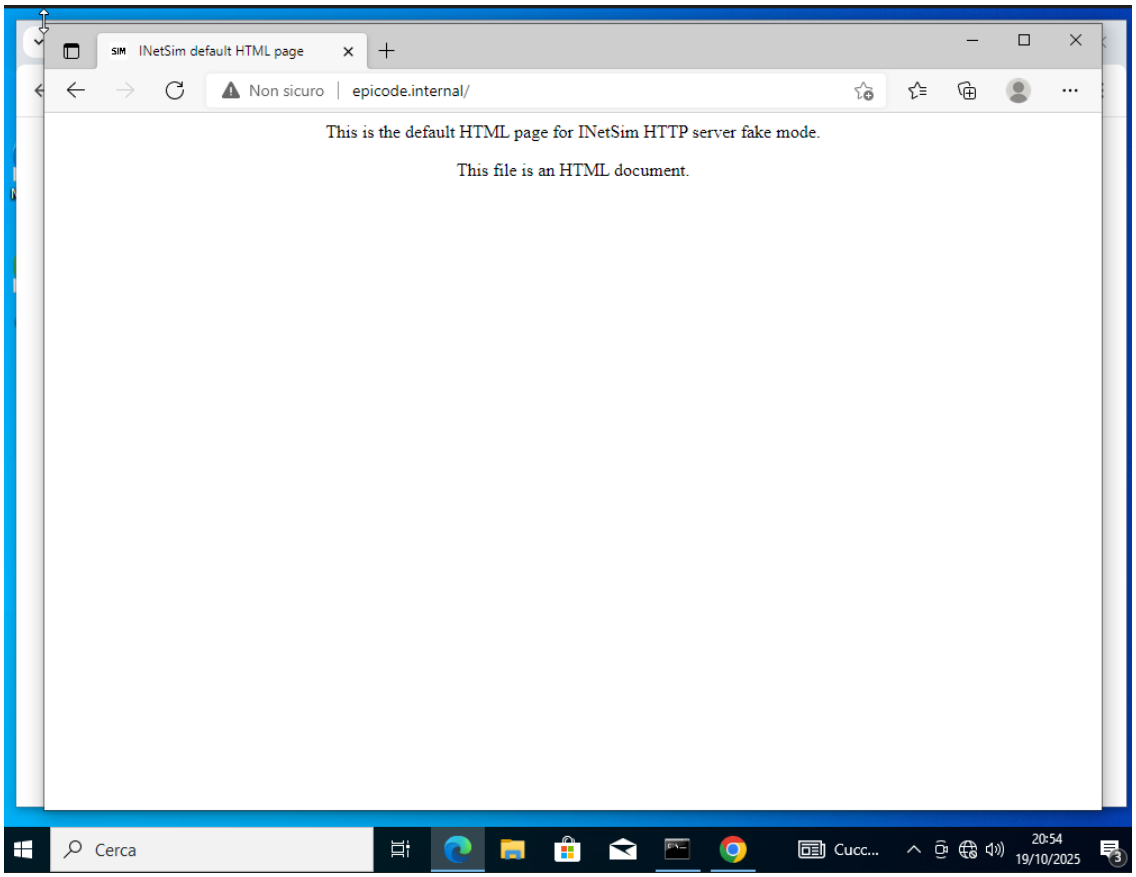
Successivamente attraverso lo strumento ***inetsim*** che permettente di simulare tutto una serie di servizi riguardanti la rete configuro il **DNS** attivando il relativo servizio e l'HTTPS.
La configurazione del DNS è un passaggio fondamentale poiché funge da tramite tra la richiesta di un domino in questo caso epicode.internal e l'indirizzo ip 192.168.32.100.

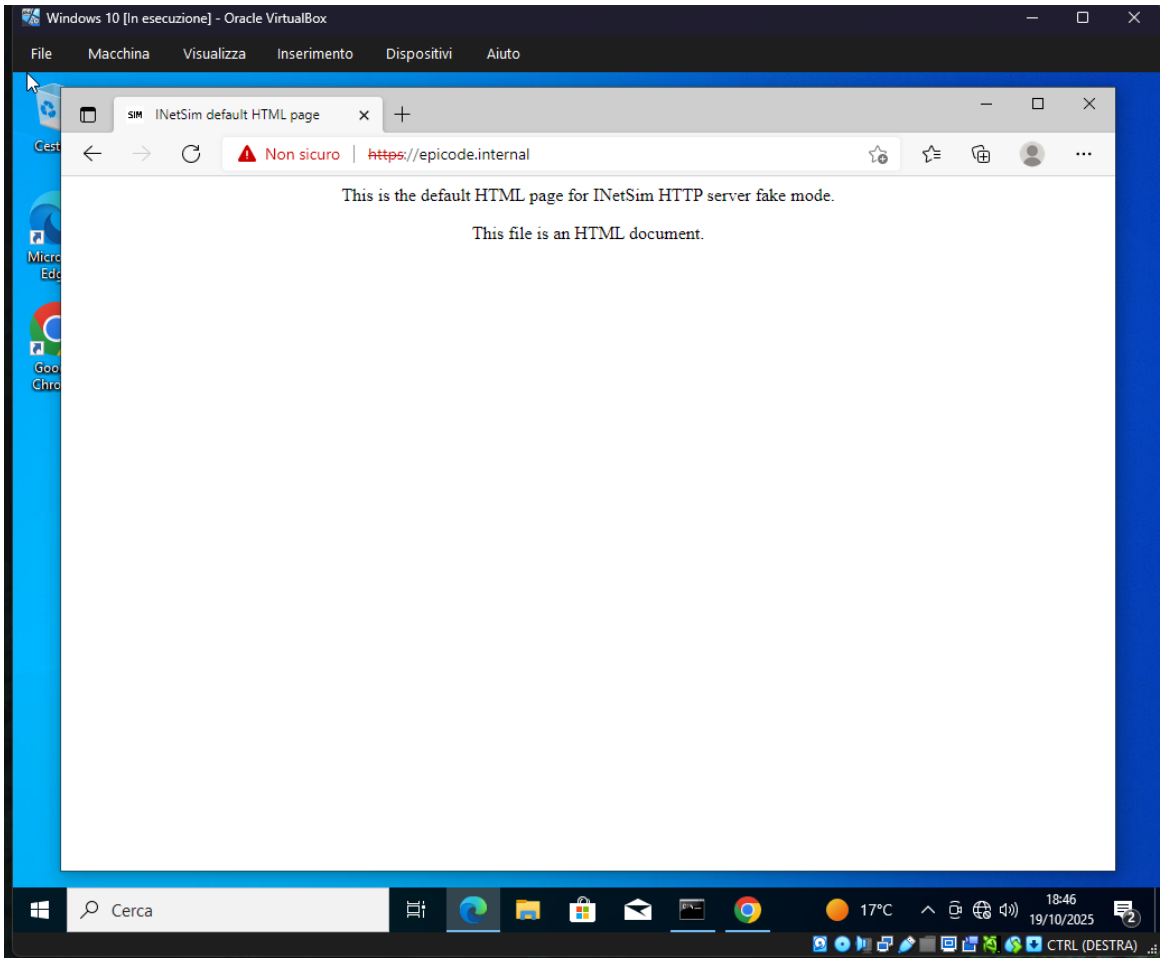


Una volta fatto ciò proseguo con il configurare più nel dettaglio la configurazione DNS:
- come riferimento DNS: 192.168.32.100 e
-come dominio e nome: epicode.internal
In questo modo le due macchine possono comunicare correttamente.



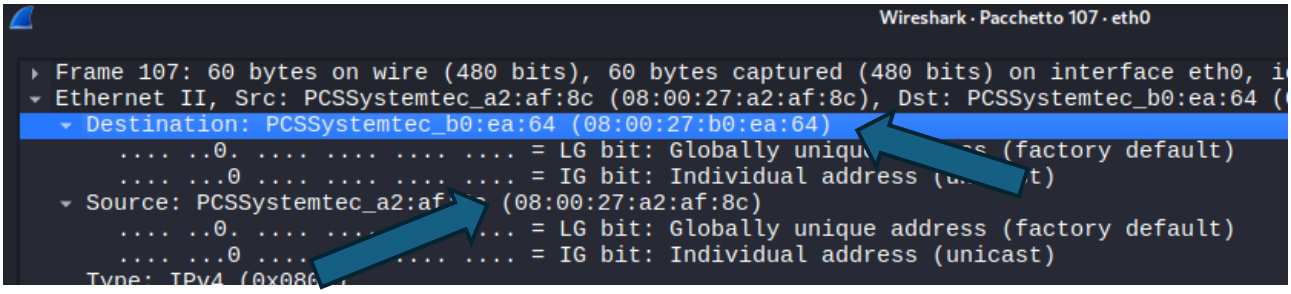
Una volta completata la configurazione mi sono spostato sulla macchina virtuale Windows per eseguire un test di connessione con il dominio *epicode.internal,* sia in HTTPS che in HTTP, verificando il corretto funzionato e risoluzioni della connessione:


INetSim default HTML page
Non sicuro
epicode.internal/
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Cerca
Cucc...
20:54
19/10/2025


Windows 10 [In esecuzione] - Oracle VirtualBox
File
Macchina
Visualizza
Inserimento
Dispositivi
Aiuto
INetSim default HTML page
Non sicuro
https://epicode.internal
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Cerca
17°C
18:46
19/10/2025
CTRL (DESTRA)

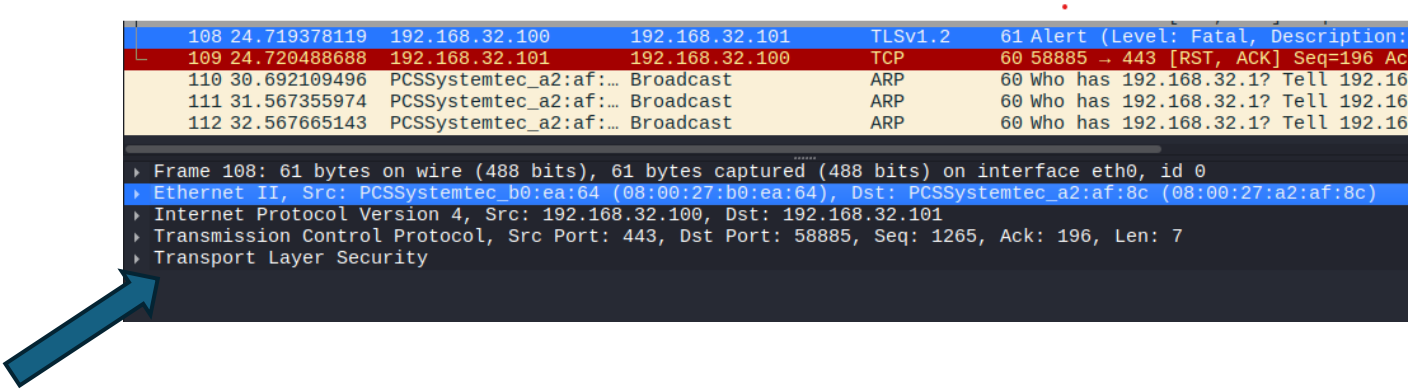
3) Intercettazione Comunicazione HTTPS e MAC address

Dopo aver verificato il corretto indirizzamento con il dominio epicode.internal, ho analizzato nel dettaglio il protocollo **HTTPS** e il **MAC address** delle due macchine virtuali. Per fare questo tipo di analisi dettagliata mi sono servito di un software specifico *wireshark* che analizza tutti i tipi di pacchetti che vengono scambiati tra i due Host.



Come possiamo notare da quest'immagine abbiamo trovato nel livello **Ethernet II** il MAC address di destinazione che quello della fonte. Importante soffermarsi ad analizzare il mac address poichè si tratta di un identificatore univoco legato al singolo dispositivo fisico ed è importate poiché ci permette di far comunicare in modo corretto le due macchine virtuali.

Successivamente grazie a Wireshark possiamo analizzare anche più nel dettaglio il protocollo **HTTPS**:

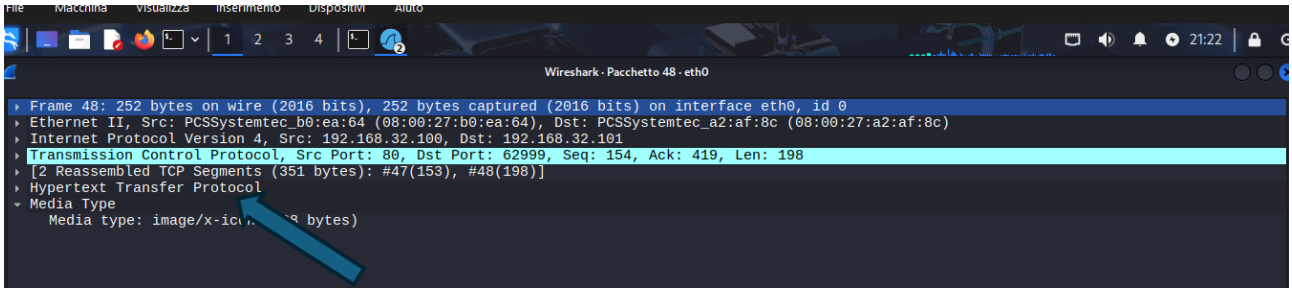


Questo protocollo è essenziale ai fini della trasmissione sicura delle infromazioni su internet, in quanto utilizza la crittografia per proteggere i dati, a differenza del protocollo HTTP.

Come mostrato dell'analisi, l'HTTPS possiede un ulteriore livello chiamato *Transport lateyer Security* (**TLS**) che permette di oscurare le informazioni. Solo chi è in possesso delle chiavi di cifratura può visualizzare le informazioni, garantendo la sicurezza nella trasmissione.

4) Intercettazione Comunicazione http

Analizzando invece il protocollo HTTP è possibile notare come, non essendo cifrato, ci permetta di visualizzare molte più informazioni anche dopo una singola analisi del traffico. Questo dimostra quanto sia importante avere un protocollo cifrato come l'https per proteggere i nostri dati che scambiamo.



Nel caso dell'HTTP, infatti, non è presente il layer di sicurezza e si può chiaramente identificare il protocollo di trasferimento e il **media Type,** ovvero la categoria generale del dato trasmesso. (in questo caso vediamo trattarsi di un'immagine)

Antonio Amatrice
19/10/2025