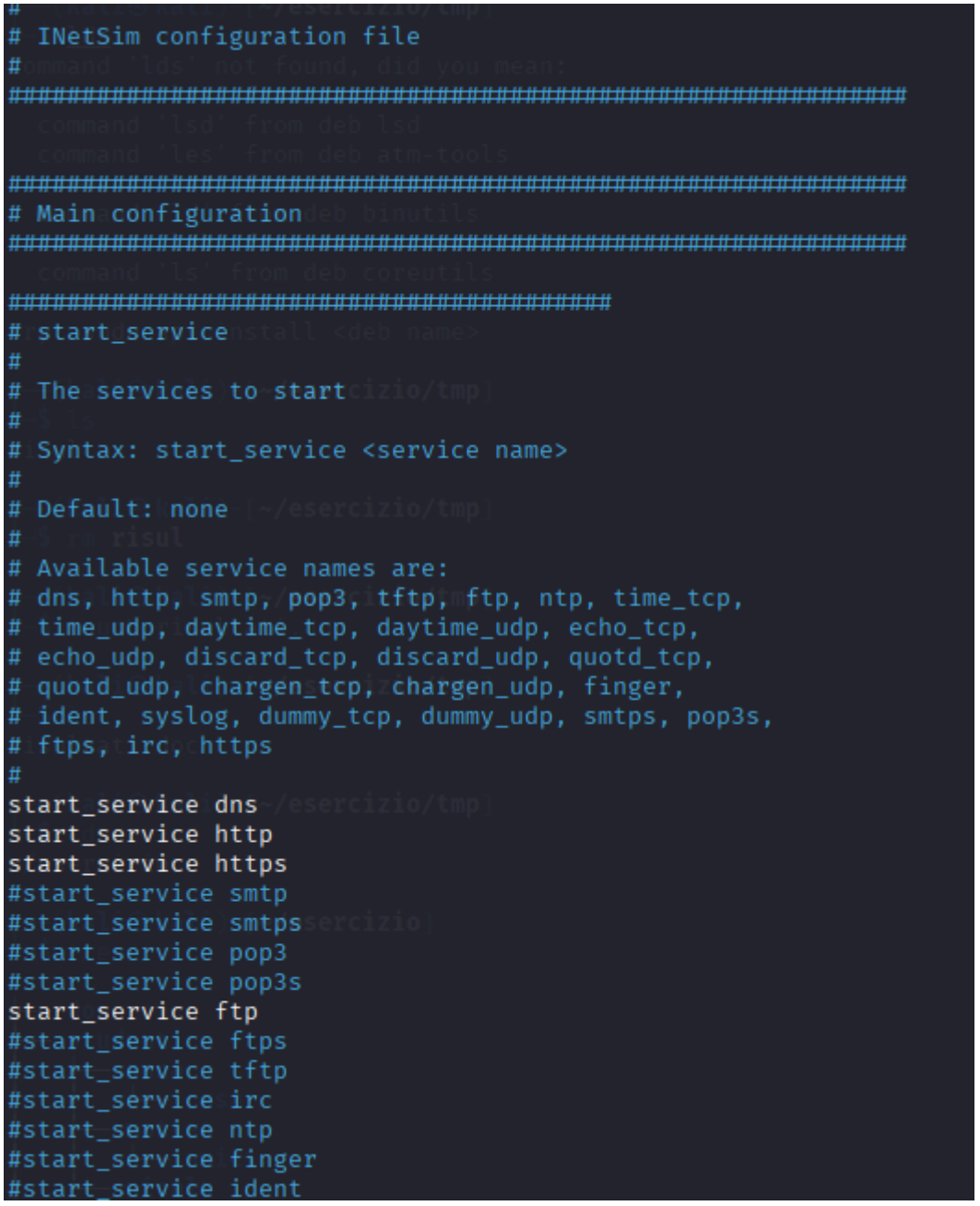
PROGETTO M1 - W4D4

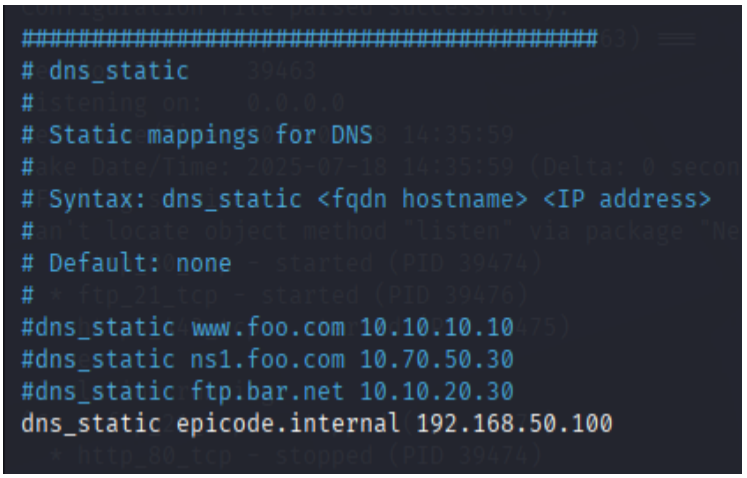
Introduzione all'Hacking

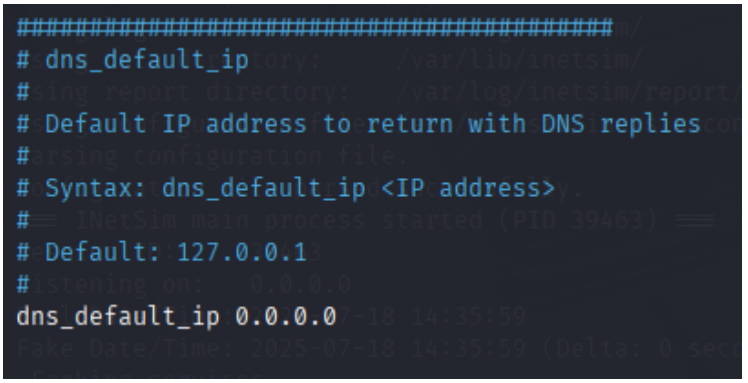
Configurazione IP
Kali: 192.168.50.100
Windows: 192.168.50.102

Per attivare i servizi **HTTPS** e **DNS** basta lanciare il comando "*sudo nano /etc/inetsim/inetsim.conf*", così aprendo, come si vede sotto in figura, la configurazione di **InetSim**, dopodiché basta levare l'hashtag per far sì che il comando venga eseguito, perché lasciando l'hashtag la linea diventa un commento e non sarà eseguibile.

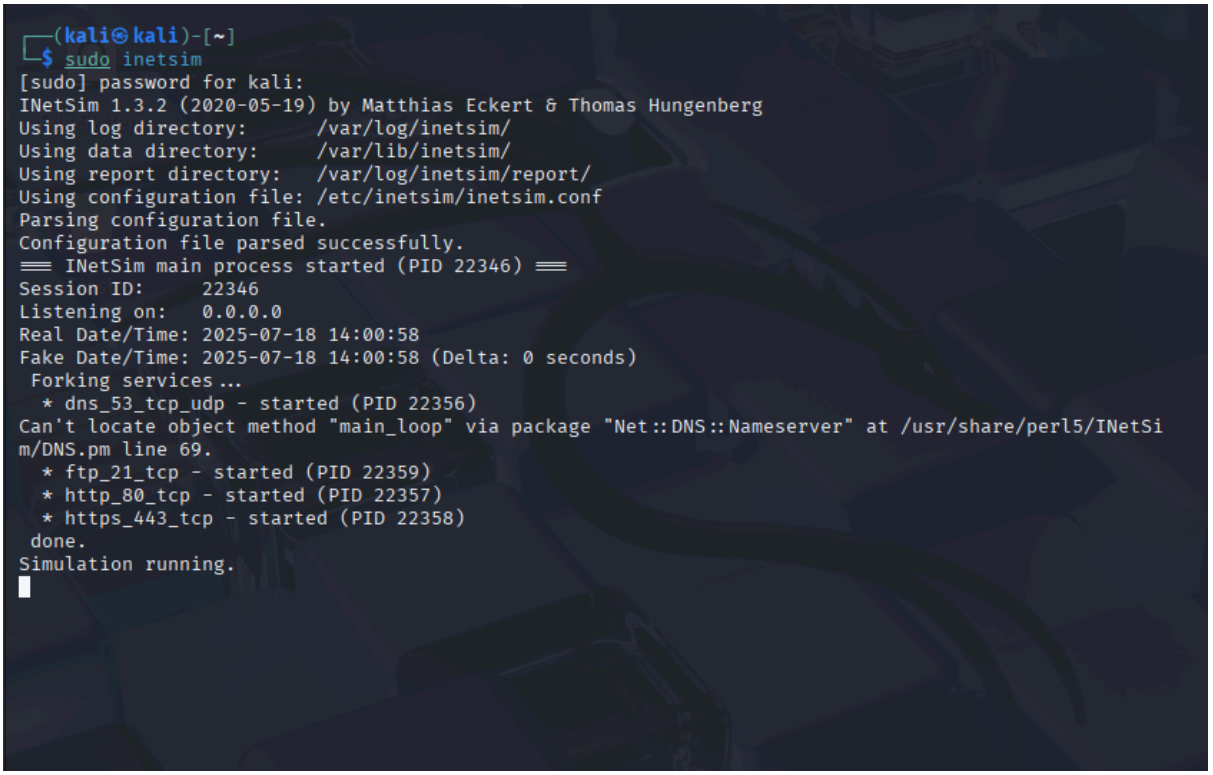


per configurare il servizio DNS, come nelle figure sotto, bisogna aggiungere la linea “dns_static epicode.internal 192.168.50.100” per configurare l’indirizzo IP (kali) con il nome epicode.internal, cosi da configurare il DNS, ovvero il servizio farà si che se cerchiamo epicode.internal si reindirizzerà al IP assegnato e viceversa, ricordiamo che il servizio DNS traduce i nomi di dominio in indirizzi IP per facilitare agli utenti gli accessi ai siti web. Inoltre si è configurato la parte dns_default_ip con 0.0.0.0 (tutti gli indirizzi).



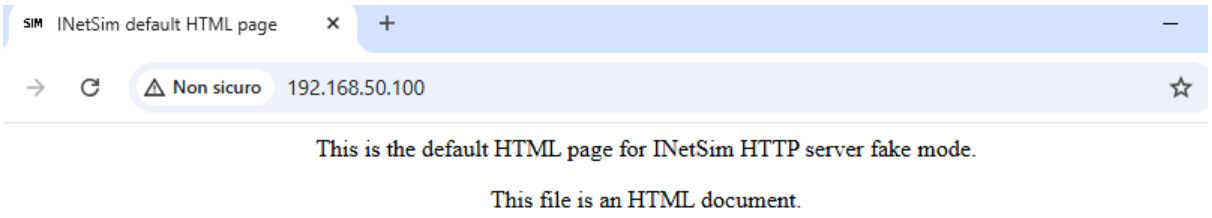


infine si può lanciare il comando “*sudo inetsim”* per avviarlo

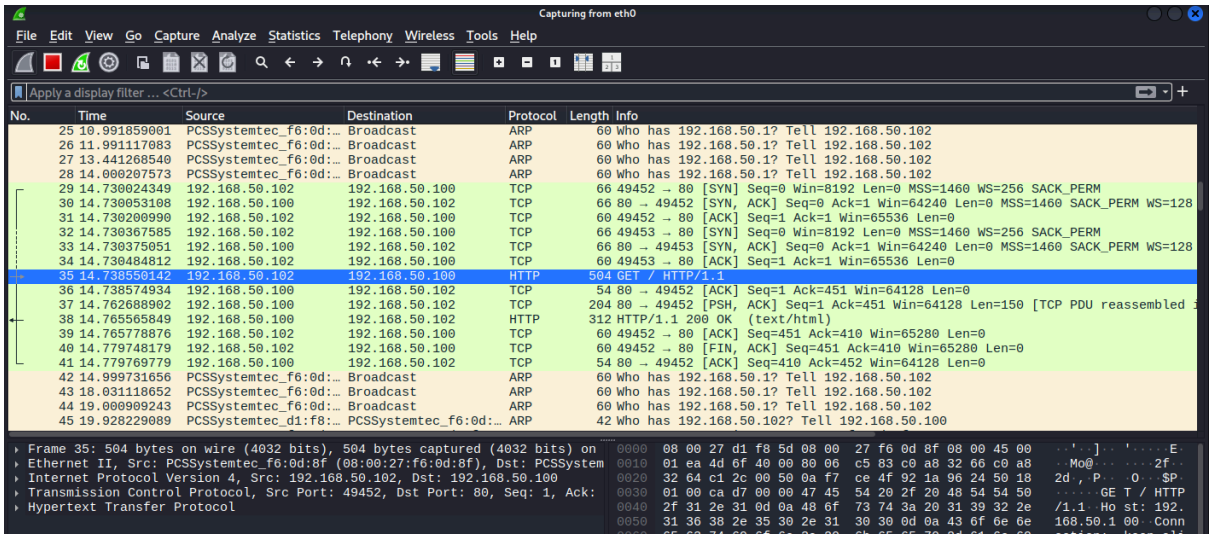


come si può vedere c’è stato un errore nel DNS (visto insieme a lezione)
nel mio caso ho lasciato attivo i servizi FTP, HTTP e HTTPS

Adesso se facciamo la prova su Windows, avviamo Chrome e cerchiamo http://192.168.50.100 ci da come risultato:



quindi funziona, se il DNS era in funzione bastava cercare http://epicode.internal e dava lo stesso risultato. Dava stesso risultato anche se si cercava https://192.168.50.100. Sotto si può vedere l'analisi da parte di Wireshark e si può notare il three-way-handshake (No.29 - 31) tra client (Windows) e server (Kali), che si tratta di una procedura per stabilire una connessione sicura tra i due dispositivi e viene utilizzata nel protocollo TCP



sempre nella figura precedente, si può vedere come cambiano gli indirizzi MAC source e destination

MAC address Source	**MAC address Destination**
Windows	Kali
Kali	Windows
Windows	Kali

(esempio. three way handshake, lo scambio dei paccheti tra i due dispositivi Kali e Windows)

Ecco il contenuto della richiesta HTTP (rosso client e blu server). Si può vedere la richiesta e la risposta da parte del server con lo status code 200 “OK”, ovvero la richiesta è stata ricevuta, elaborata e completata con successo.

A differenza del servizio HTTP (porta 80), Hyper Text Transfer Protocol, che trasferisce i dati in chiaro rendendoli vulnerabili e con facile accesso da terze parti, il servizio HTTPS (porta 443), HTTP Secure, protegge i dati usando la crittografia TLS/SSL così rendendo la trasmissione dei dati sicura e non facile da accedere.

Wireshark non è riuscito analizzare i pacchetti del servizio HTTPS perché appunto erano crittografati, se nel caso si potesse, la differenza con il contenuto HTTP (come in figura precedente) dove i dati sono leggibili, nel contenuto HTTPS non si riesce a leggere dato che sono cifrati