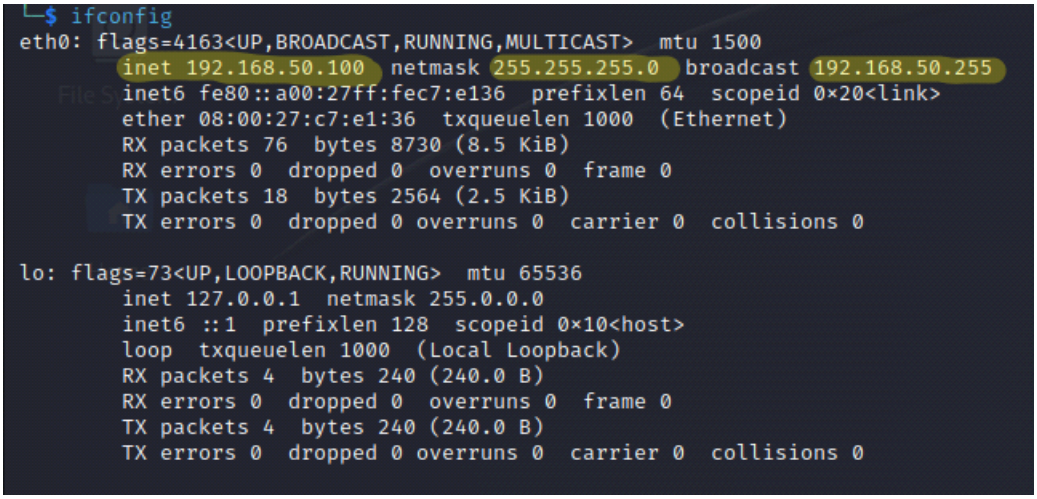
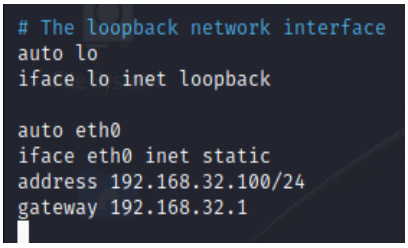
REPORT PROGETTO

In questo report spiegherò come creare in un ambiente virtuale su VirtualBox un architettura client server tra una macchina virtuale linux (kali), che sarà il nostro server e windows 7 (che sarà il nostro client).

Per prima cosa si cambia l'indirizzo ip sulla macchina linux:



Con il comando **sudo nano /etc/network/interfaces** sul cmd cambiamo l'indirizzo ip che ci viene richiesto:

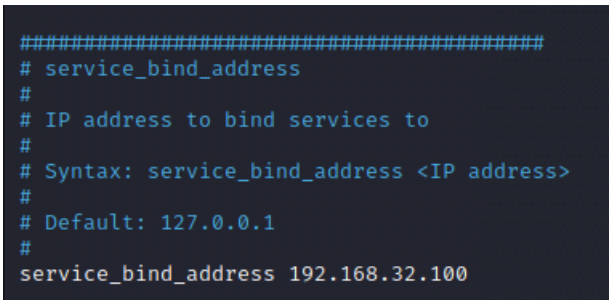


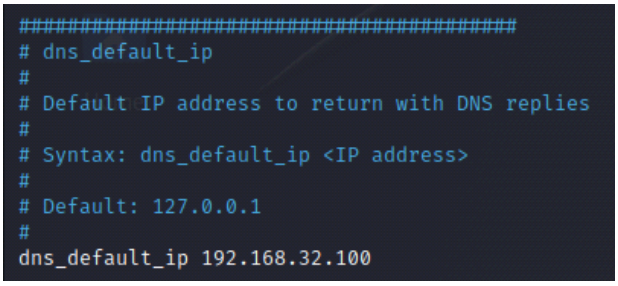
Cambiamo anche l'indirizzo ip su windows 7 andando a inserire anche l'ip del DNS statico:

...

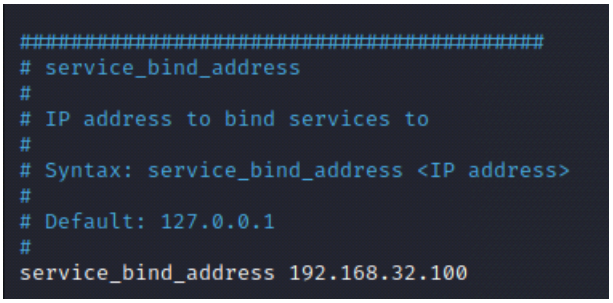
Andiamo a settare InetSim su Kali. InetSim che è tool open source per la simulazione di servizi Internet standard, come DNS, HTTP / HTTPS e così via. Anche se noi utilizzeremo principalmente questi tre nel progetto.

Usiamo il comando **sudo nano /etc/inetsim/inetsim.config** per andare a configurare il nostro server. Andiamo quindi a cambiare queste due righe di comando con l'ip che abbiamo associato a kali:



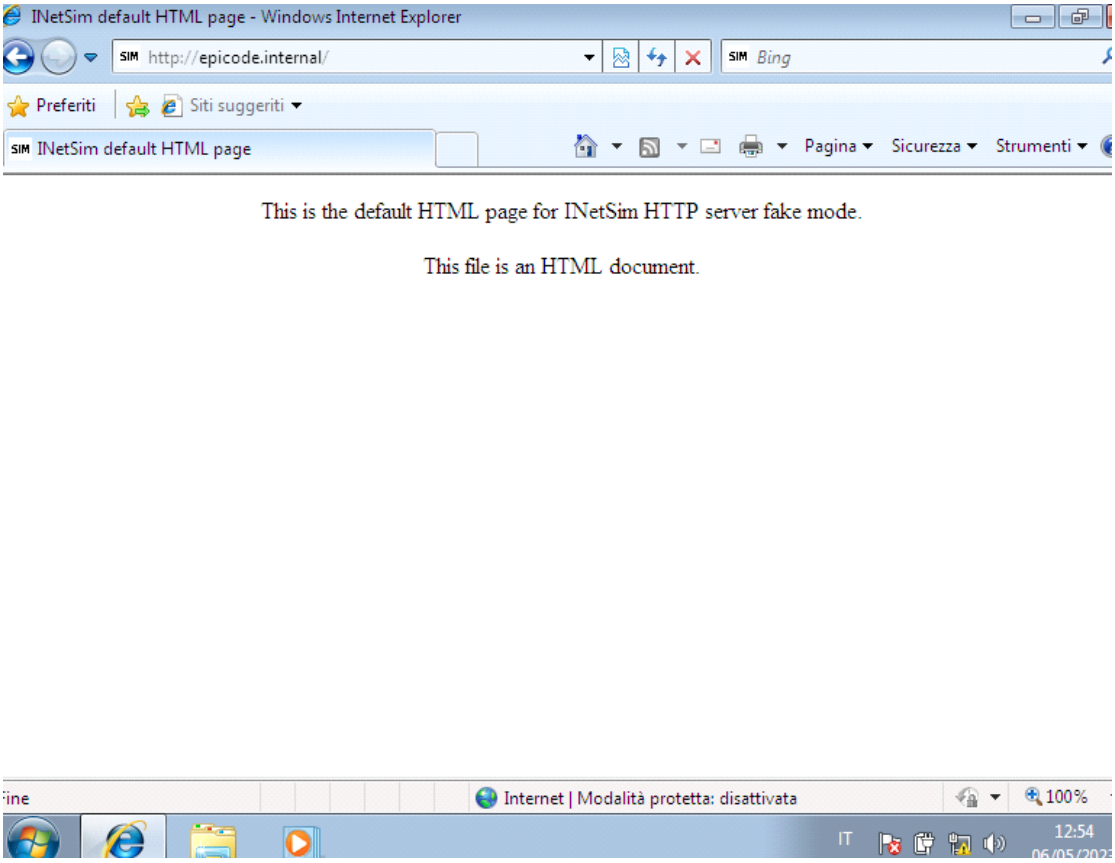


Succesivamente andiamo ad associare il nome **epicode.internal** al dns staticoassociato all'ip del server cioè **193.168.32.100**:



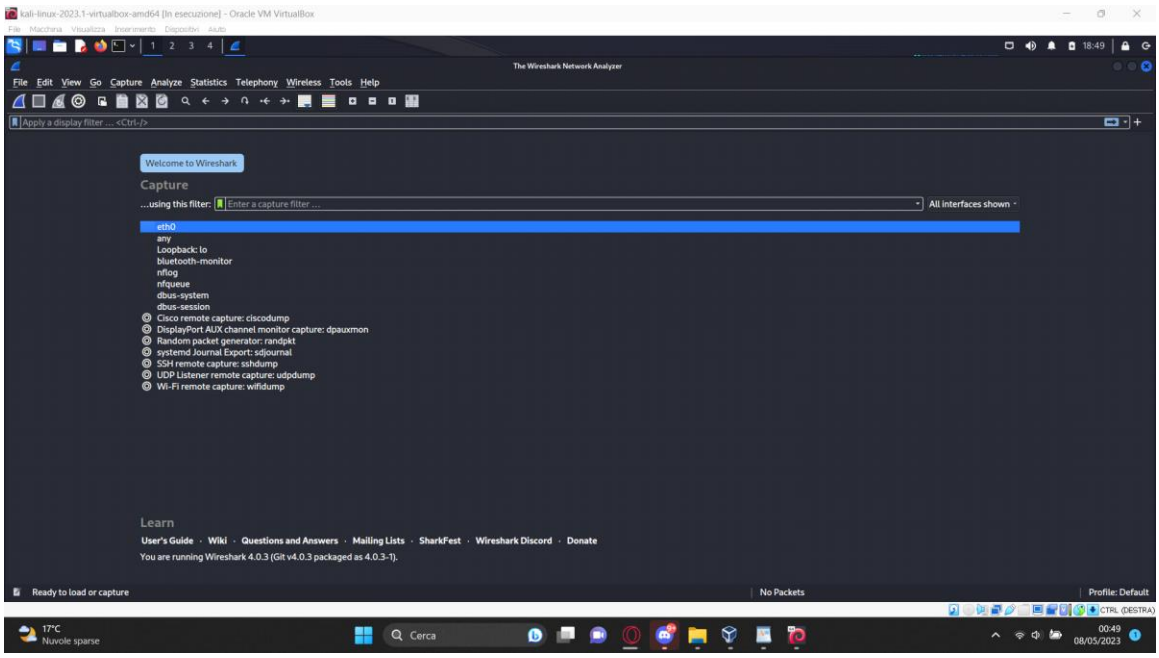
Ora che abbiamo completato l'operazione di configurazione del nostro server dns facciamo eseguire il programma InetSim con il comando: **sudo inetsim** .

Passiamo quindi a windows e apriamo il nostro browser web e cerchiamo il nostro server a cui chiederemo un servizio:

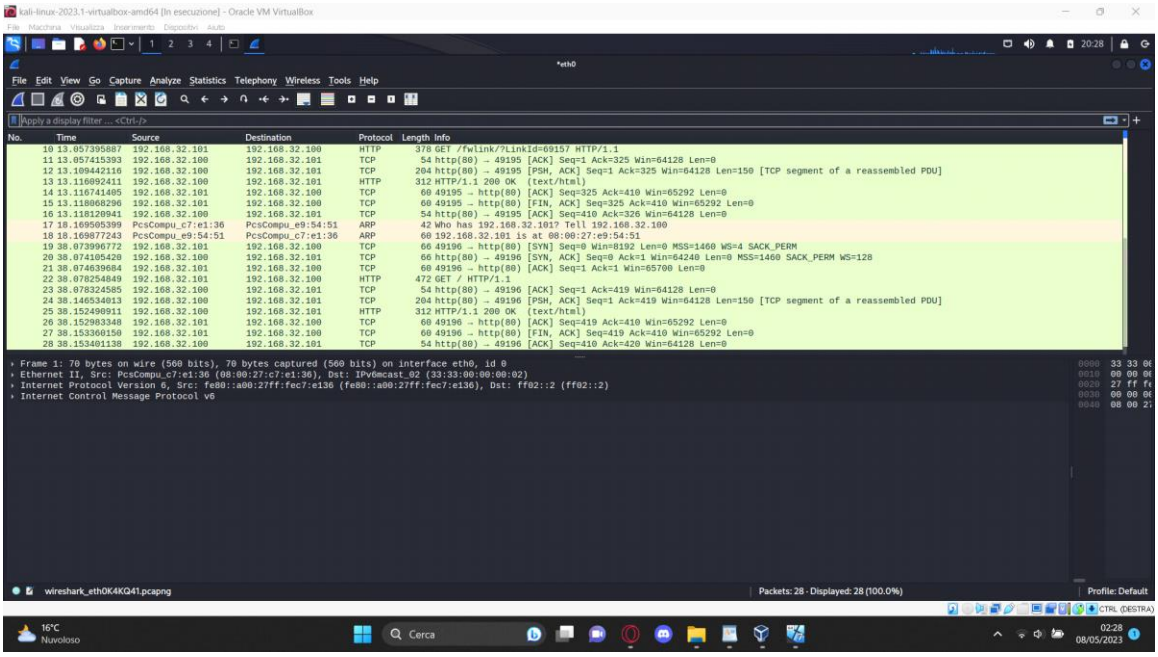


Questo nostro server ci restituisce una paggina in **HTML.**

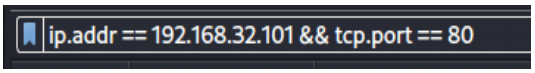
Ora andremmo ad osservare il traffico di dati tra il client e il server tramite un applicazione che si occupa dello **sniffing** : **Wireshark** .



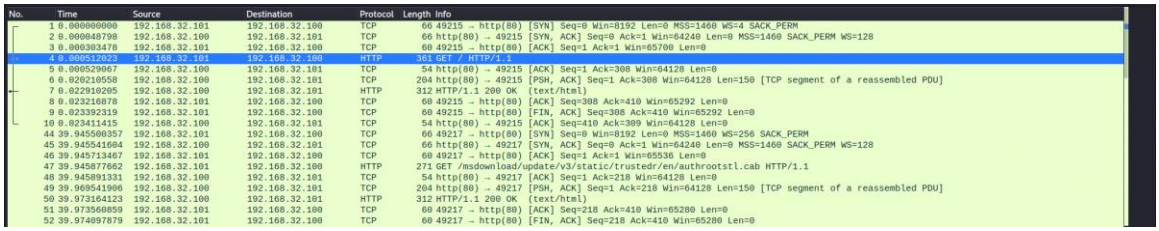
Prima di cercare di cercare il server clicchiamo su **Start capturing packets** per iniziare la cattura dei pacchetti. Dopo la ricerca sul browser otterremo la seguente schermata:



Ora nella riga di ricerca andremmo a cercare nello specifico i pacchetti del protocollo **HTTP** immettendo il seguente codice:



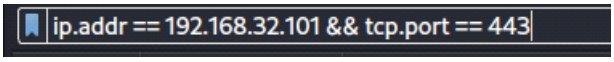
Ci restituirà la seguente schermata:



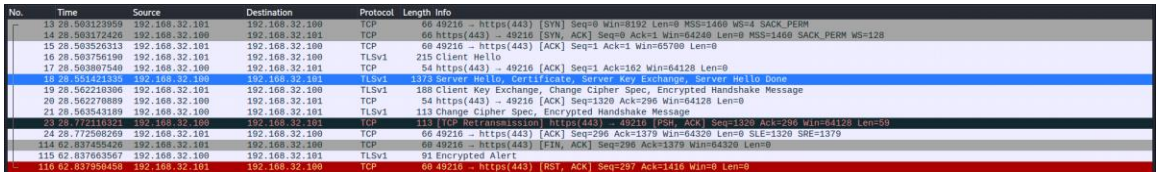
Questi sono tutti i processi del protocollo http.

Per vedere il protocollo **HTTPS** dovremmo prima andare nel browesr web e cambiare da http a https sulla barra di ricerca.

Mentre per vedere i pacchetti del controllo **HTTPS** andremmo a scrivere il codice:

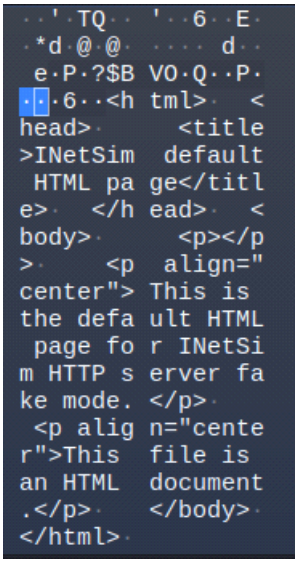


Ci restutirà la seguente schermata:

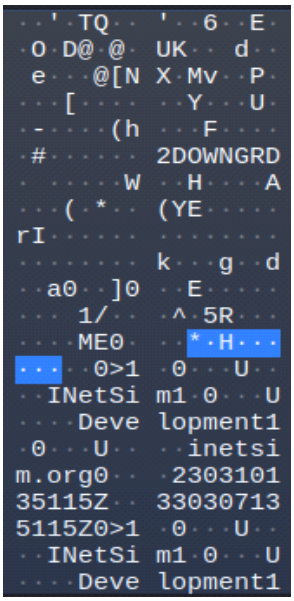


La differenza tra i due protocolli è la **cifratura** delle informazioni del pacchetto:

HTTP:



HTTPS:



Inoltre possiamo anche vedere l'indirizzamento dei pacchetti tramite l'indirizzo **MAC** che cambia ad ogni nodo e la sequenza **seq - ack** per l'operazione di handshake: