TEST PRATICA FINE MODULO 01
AZZEDDINE EL HARIRI

Nell’esercizio di oggi metteremo insieme le competenze acquisite finora. Lo studente verrà valutato sulla base della risoluzione al problema seguente.

Requisiti e servizi:

- Kali Linux: IP 192.168.32.100
- Windows 7: IP 192.168.32.101
- HTTPS server: attivo
- Servizio DNS per risoluzione nomi di dominio: attivo

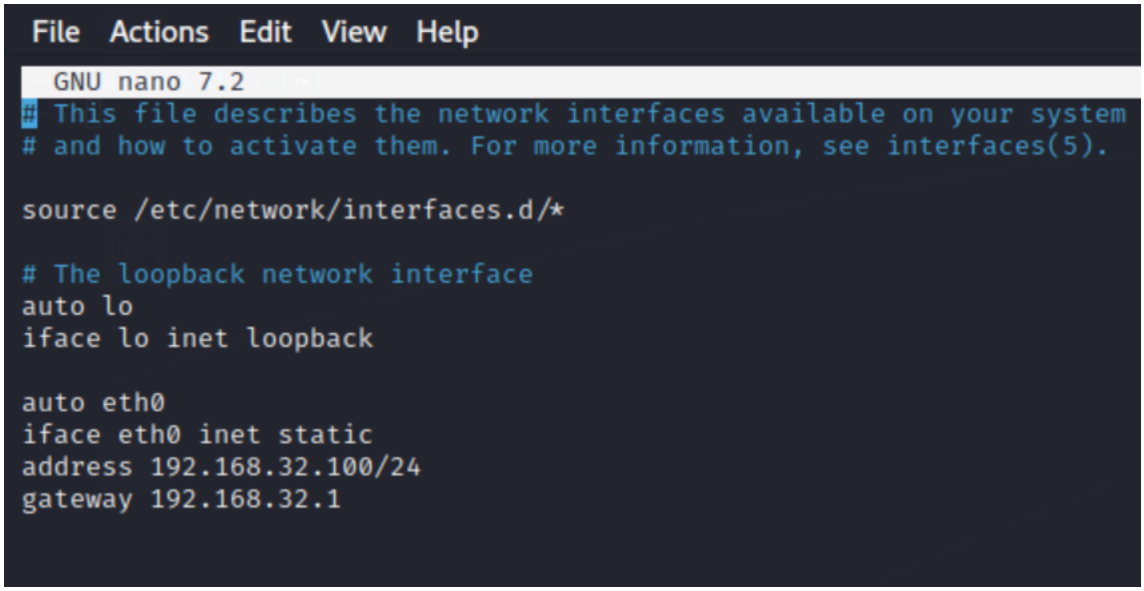
Traccia: Simulare, in ambiente di laboratorio virtuale, un’architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all’hostname epicode.internal che risponde all’indirizzo 192.168.32.100 (Kali Linux). Si intercetti poi la comunicazione 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.

Impostare IP statico a Kali Linux (192.168.32.100)

Per configurare un indirizzo ip statico su Kali Linux bisogna innanzitutto accedere a terminale, successivamente bisogna digitare i seguenti comandi:

```
sudo nano /etc/network/interfaces
```

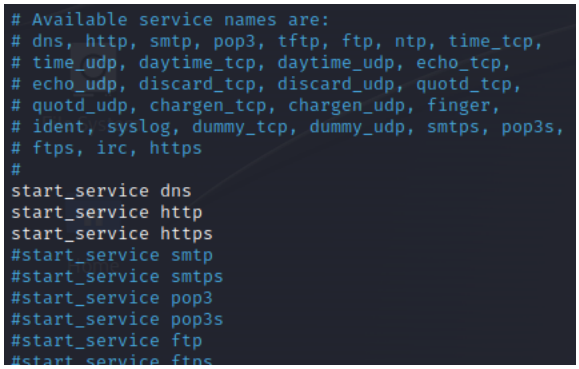
Una volta digitate I comandi vedremo la seguente schermata



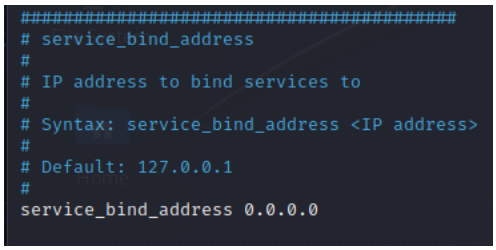
Una volta arrivati alla schermata di configurazione ci basterà digitare l'ip address come da consegna (192.168.32.100) e il conseguente Default Gateway (192.168.32.1).

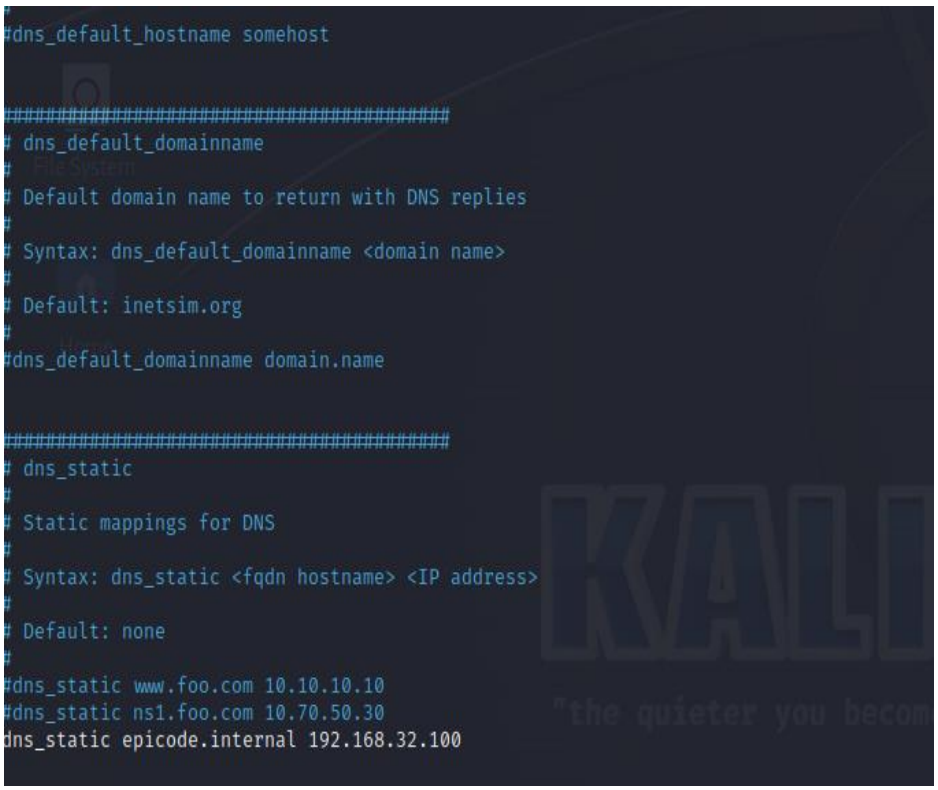
Attivazione servizi DNS, http, HTTPS su Kali Linux

Per attivare i servizi richiesti dalla traccia quali: HTTP, HTTPS e DNS, utili a richiamare le pagine web da Windows 7, innanzitutto è necessario configurare il servizio "inetSim" da Kali Linux.
Da terminale bisogna digitare i seguenti comandi per accedere alla pagina di configurazione:
sudo nano /etc/inetsim/inetsim.conf
Per attivare i servizi richiesti bisogna cancellare l' "#"
dai servizi che vogliamo attivare. In questo caso ci basterà attivi i servizi in bianco nell'immagine in basso.

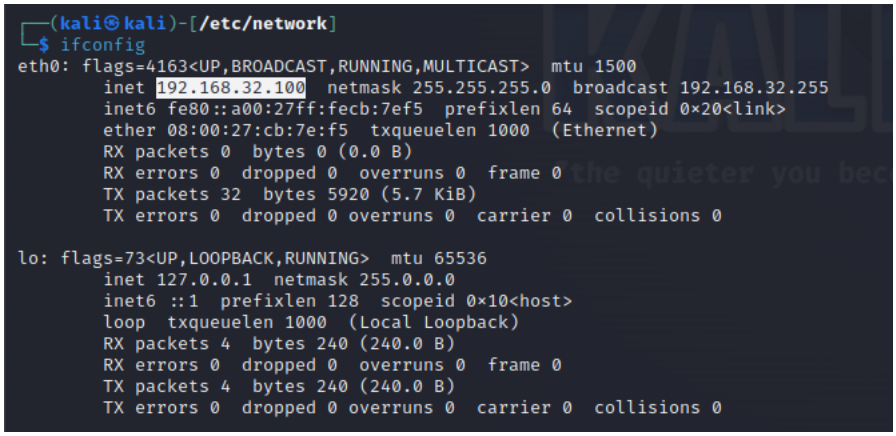


Successivamente per associare un IP ad inetSim è necessario decommentare la voce “service_bind_address”. In questo caso siamo andati ad associare l’indirizzo 0.0.0.0 in modo da permettere all’applicazione di comunicare a tutti gli ip disponibili in base alle schede di rete configurate.





Per attivare il servizio DNS statico sarà necessario decommentare la voce “`dns_static`” (come da immagine in alto) andando ad inserire la richiesta della traccia in quanto la chiamata deve essere fatta su “`epicode.internal`” relativo all’indirizzo IP `192.168.32.100` che sarà concomitante all’indirizzo associato a Kali in quanto quest’ultimo dovrà fungere da server application.



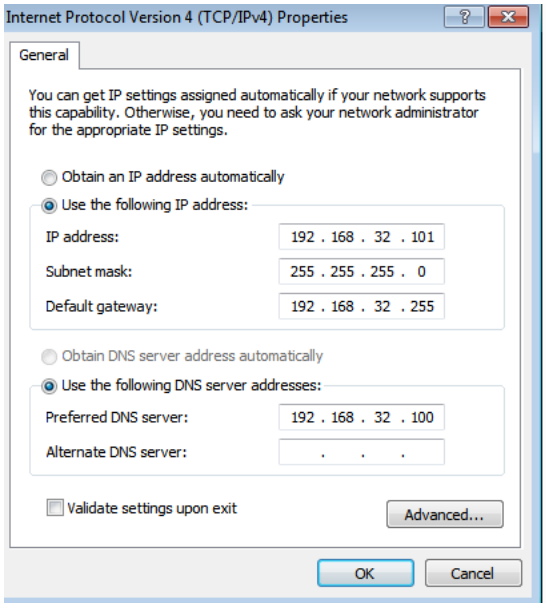
Una volta configurati i servizi, come da richiesta, è possibile verificare la corretta esecuzione dei comandi precedenti digitando da terminale il comando "`ifconfig`" come da figura in alto verificando la corretta associazione dell'IP statico.

Impostare Ip Statico Windows 7 (192.168.32.101)

Per impostare un IP statico su Windows 7 sarà necessario modificare i parametri di default seguendo il percorso in basso:

`Pannello di controllo -> Network and Internet -> Change adapter settings -> Tasto destro Local Area Connection -> Properties -> Internet protocol Version 4 (TCP/iPv4) -> Properties:`

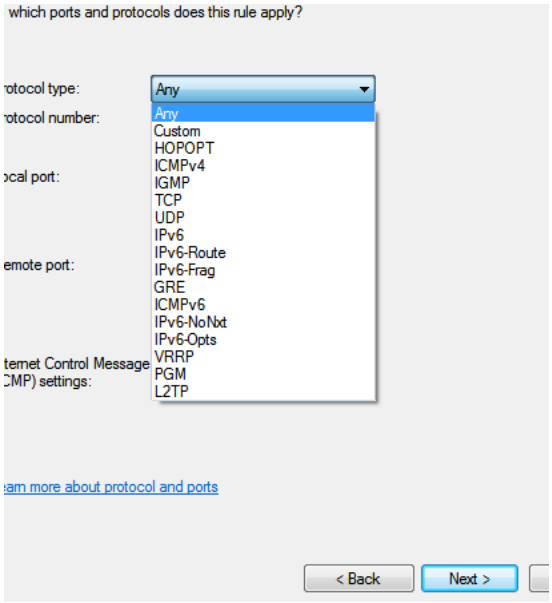
Una volta arrivati alla finestra di configurazione andremo ad inserire nella voce IP Address, l'IP statico che vogliamo associare alla macchina, il default Gateway di riferimento (il default Gateway è il canale di comunicazione che consente ad un dispositivo di collegarsi in rete tramite IP) e l'indirizzo IP statico associato al servizio DNS su Kali Linux per permettere al sistema Windows 7 di collegarsi a tale servizio. Ricordiamo che il DNS Domain è utile a mascherare un indirizzo IP in un indirizzo testuale.



Attivare regole Firewall Windows

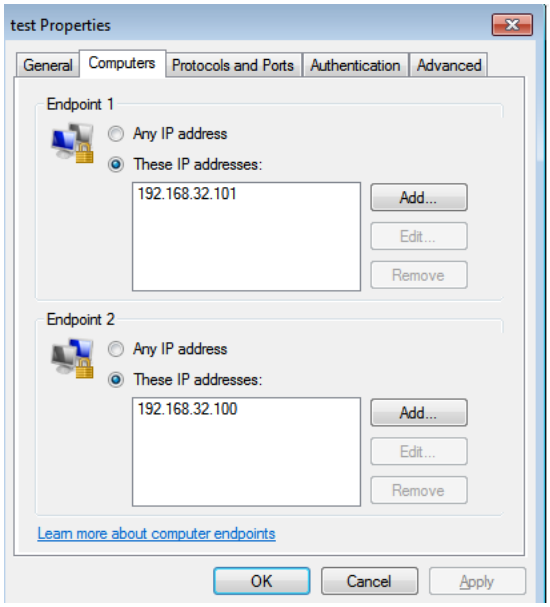
Per consentire la connessione tra le due macchine virtuali è necessario abilitare la regola di connessione entrata\uscita tramite firewall Windows seguendo il percorso descritto in basso:

`Control Panel -> System and Security -> advanced settings -> impostare inbound e outbound connection.`

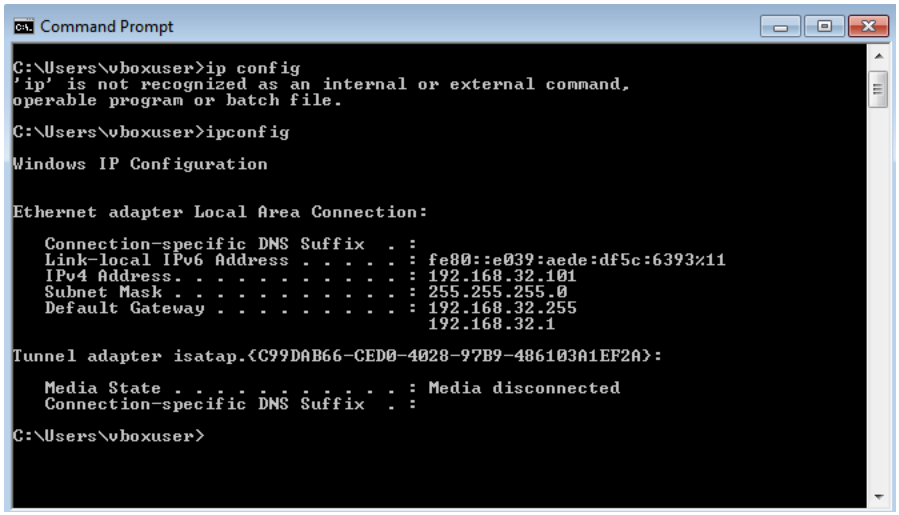


In questo abbiamo lasciato any in quanto su Windows, nella voce “Protocol Type” non è presente il protocollo IPv4 (come da immagine in alto), ossia il protocollo che noi stiamo andando ad autorizzare.

Di seguito le impostazioni “inbound” e “outbound” connection.

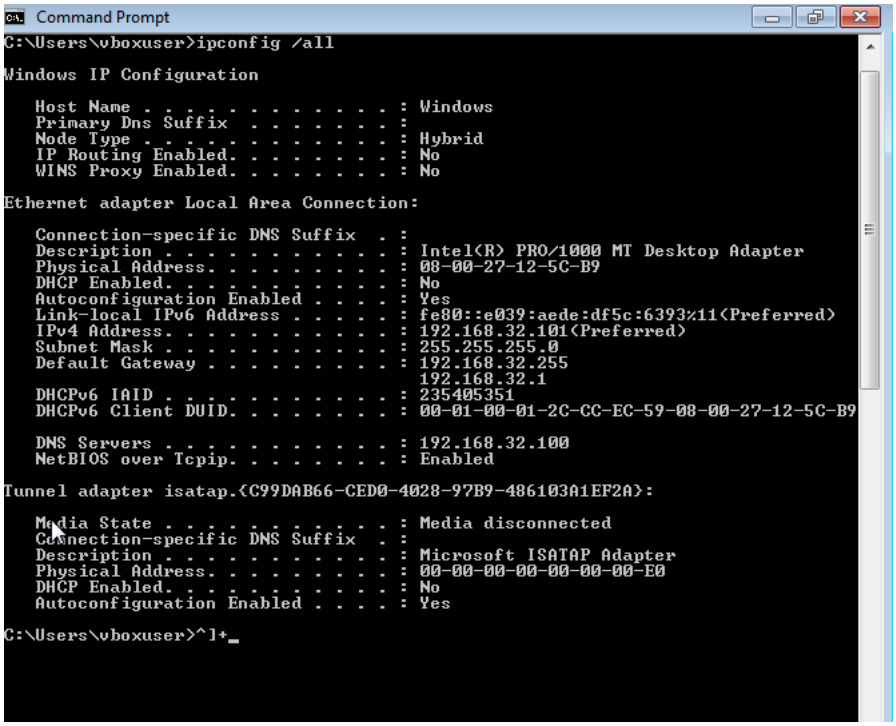


Infine, digitando "`ipconfig`" da terminale è possibile verificare la corretta esecuzione dei comandi precedentemente spiegati e come da immagine in basso possiamo dire che la procedura è stata eseguita correttamente.

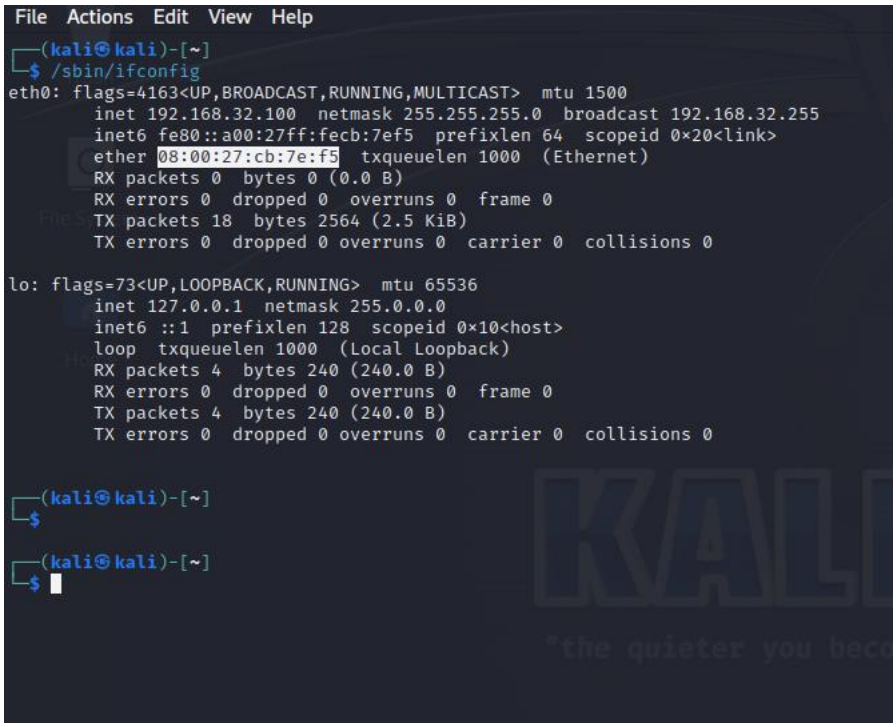


Lettura Mac Address Kali Linux e Windows

Per verificare i MAC Address, ossia gli indirizzi univoci associati ad ogni dispositivo fisico su windows sarà necessario rientrare nel comando “ipconfig” coma da immagine. In questo caso il nostro MAC Address sarà: **`08-00-27-12-5C-B9.`**



Per quanto riguarda il MAC Address di Kali Linux digitando “`ifconfig`” da terminale sarà possibile visualizzare tra le varie informazioni il MAC Address associato: **`08:00:27:cb:7e:f5`**

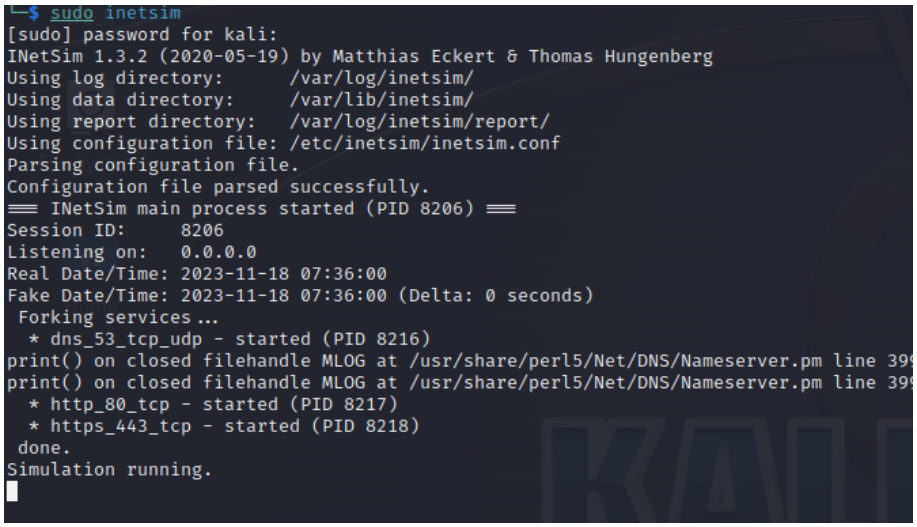


Avvio inetSim services

Per avviare i servizi HTTP, HTTPS e DNS bisognerà entrare in terminale da Kali Linux e digitare

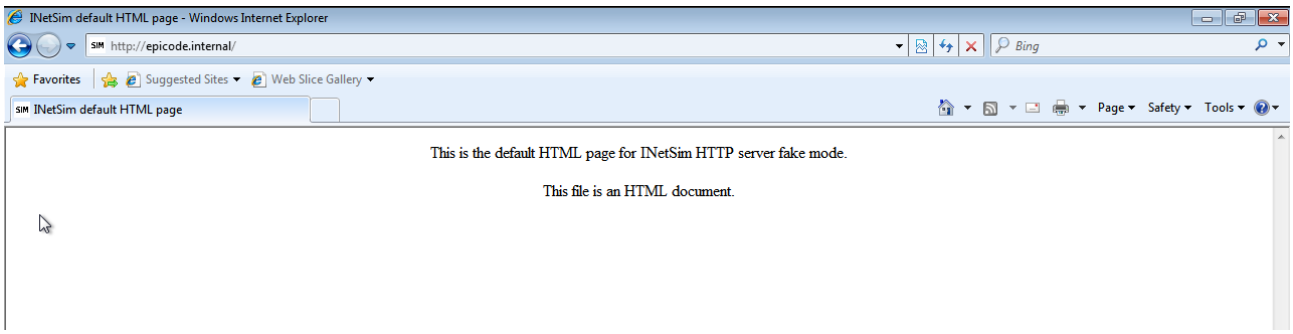
```
sudo inetsim
```

Una volta digitato il comando sarà possibile verificare l'avvio dei servizi "inetSim" come da immagine sottostante.

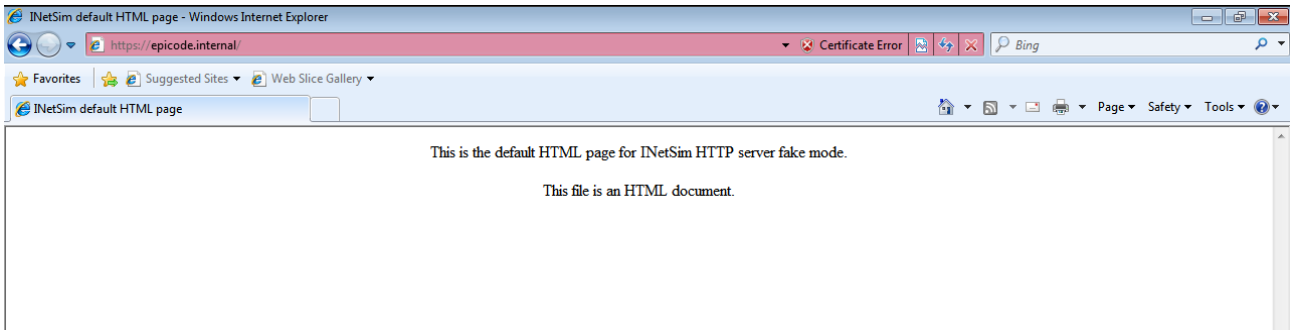


Richiesta servizi da Windows

Una volta avviata la simulazione inetSim bisognerà andare sul SO Windows 7, aprire una pagina con un web browser, ad esempio, Internet Explorer e richiamare il dominio "http://epicode.internal" come da immagine rispondendo ai quesiti di attivazione servizi HTTP e DNS su Kali Linux.

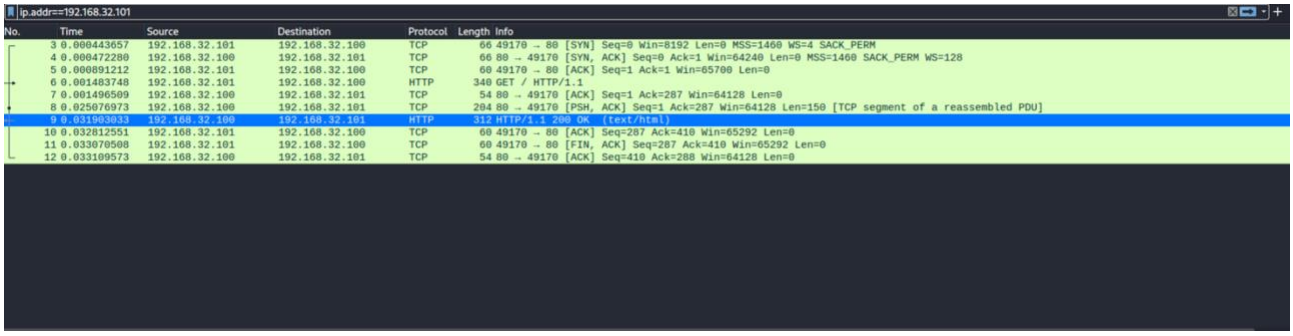


Inoltre, digitando nella barra di inserimento “https://epicode.internal” risponderemo ai quesiti di attivazione dei servizi HTTPS e DNS su Kali nonché la corretta comunicazione delle due macchine.

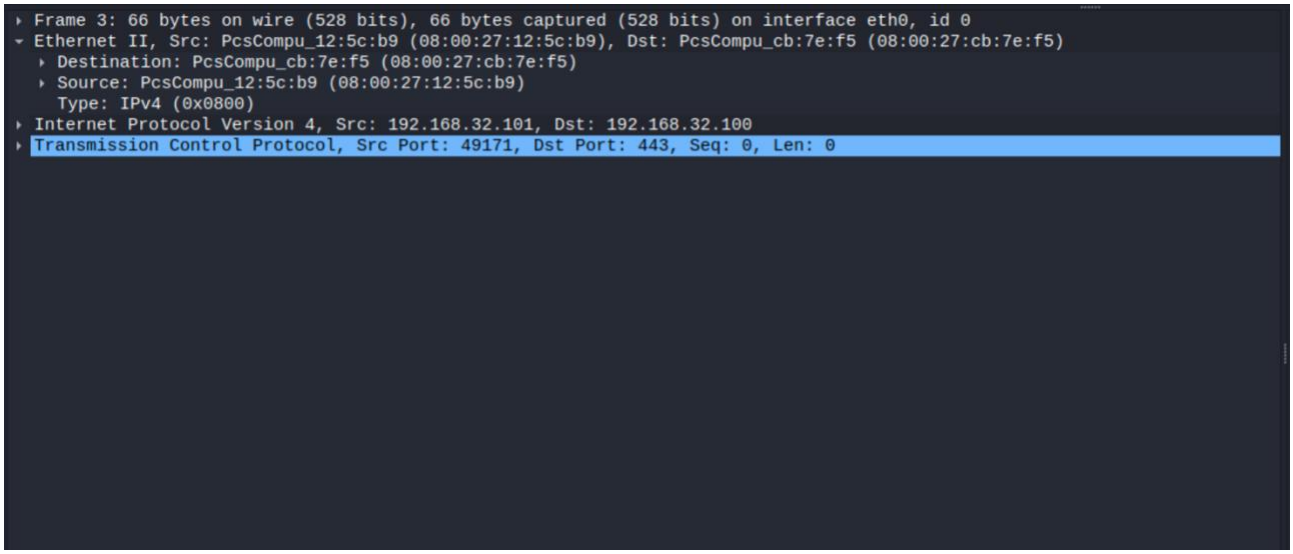


Intercettazione comunicazione con WireShark (http)

Prima di effettuare la ricerca da barra degli indirizzi da Windows sarà necessario innanzitutto aprire WireShark su Kali Linux e avviare la registrazione del traffico, dopodiché potremo andare su Windows ed effettuare la chiamata, da browser, HTTP. Seguita questa procedura WireShark registrerà il traffico di rete come da Immagine in basso. Innanzitutto, possiamo dire che il dispositivo chiamante ha indirizzo IP `192.168.32.101` mentre il dispositivo che risponde ha come indirizzo IP `192.168.32.100`. Come si può vedere alla riga numero 7 si legge una chiamata HTTP “GET” e la successiva risposta del server “200 OK”.

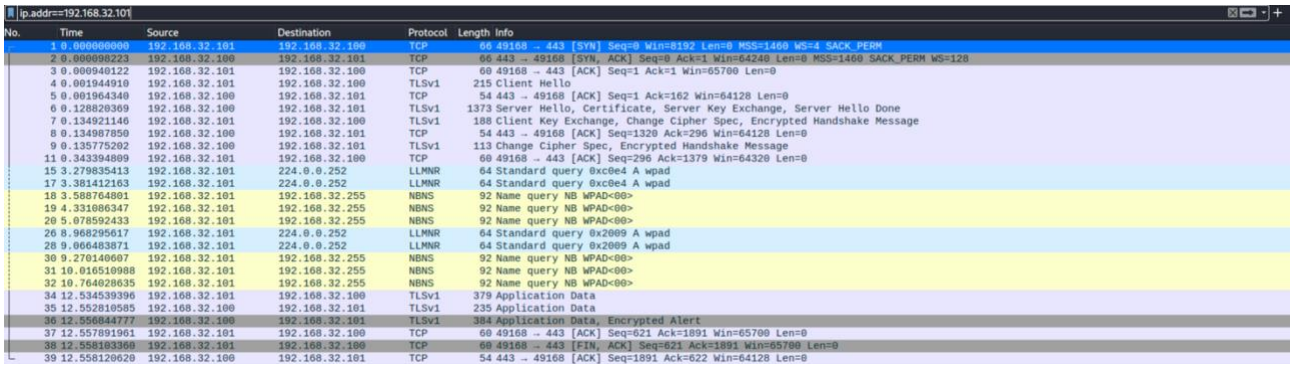


Analizzando la chiamata sulla voce Ethernet 2 potremo verificare la corretta associazione del MAC Address (sia in http che in https).



Intercettazione comunicazione con WireShark (https)

Stessa procedura si può eseguire per il protocollo HTTPS. In questo caso però vedremo delle differenze



- è possibile vedere la differenza tra protocolli in quanto la chiamata HTTPS è criptata, in quanto successivamente al three-way-handshake (SYN, SYN-ACK, ACK -> riga 1 -3) vengono scambiati pacchetti TLSv1 (TLS ricordiamo che consiste in “Transport Layer Security” ossia il protocollo di trasporto che fornisce sicurezza e integrità dei dati nelle comunicazioni in rete), nella riga 4 troviamo la risposta del server al client “Hello”, riga 6 il server scambia la chiave con il client e alla riga 7 troviamo lo scambio client server. Questo scambio di chiavi ci fa capire immediatamente che la richiesta è di tipo https e non http;

- per quanto riguarda lo scambio http nell' immagine sopra (Sez. Intercettazione comunicazione con WireShark (http)) possiamo notare una richiesta GET con successiva risposta del server -> 200 OK. Inoltre, analizzando nel dettaglio la risposta del server è possibile visualizzare il contenuto delle pagine html in quanto la comunicazione, nelle richieste http, non è criptata.

Conclusioni

Possiamo dire che viste le immagini viene specificato:

- l'assegnazione degli indirizzi IP statici alle macchine;
- la comunicazione tra le due macchine;
- l'attivazione dei servizi richiesti (HTTP, HTTPS e DNS) su inetSim;
- la comunicazione di Windows con i servizi attivati in Kali Linux attraverso web browser;
- la registrazione delle chiamate HTTP e HTTPS tramite WireShark;
- la corrispondenza dei MAC Address;