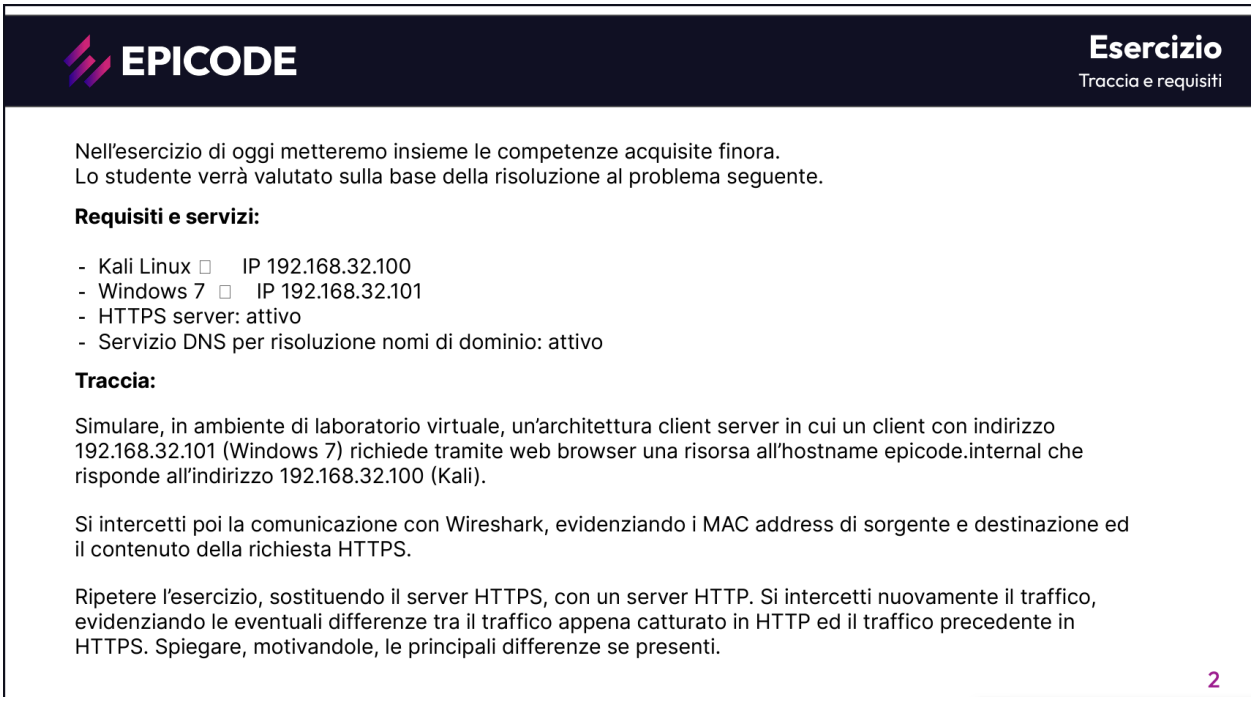
Epicode

17-11-2023

Paul Alarcon



EPICODE

Esercizio
Traccia e requisiti

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).

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.

2

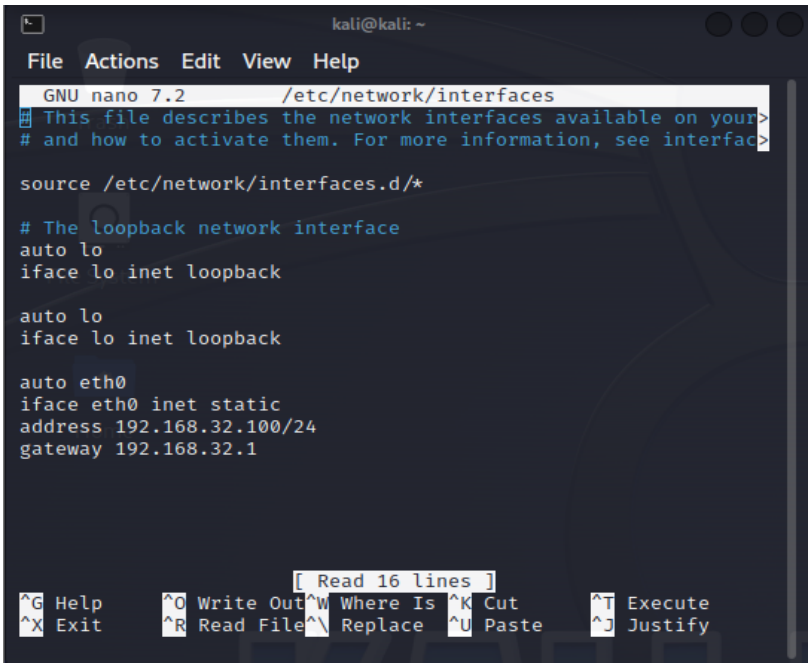
Per raggiungere gli obiettivi, è necessario prima configurare le due macchine sulla rete. Per la macchina Kali Linux, che ha come IP 192.168.50.100/24, questo dovrà essere sostituito con quello indicato nell'esercizio, ovvero 192.168.32.100/24. Per quanto riguarda la macchina Windows 7, l'IP 192.168.50.101/24 dovrà essere cambiato in 192.169.32.101/24. Come da consegna, imposterò anche l'IP per le connessioni DNS sulla macchina Kali. Dopo la configurazione degli IP, si può passare alla configurazione dei vari servizi che la macchina Kali Linux dovrà mettere a disposizione per la macchina Windows 7. Per la configurazione dei servizi, userò il tool inetsim e, per concludere l'esercizio, farò un'analisi del traffico di rete con Wireshark.

Configurazione IP su una macchina Kali linux

Per configurare l'indirizzo IP su una macchina Linux, ho aperto il terminale e utilizzato i seguenti comandi:

- `sudo nano /etc/network/interfaces`

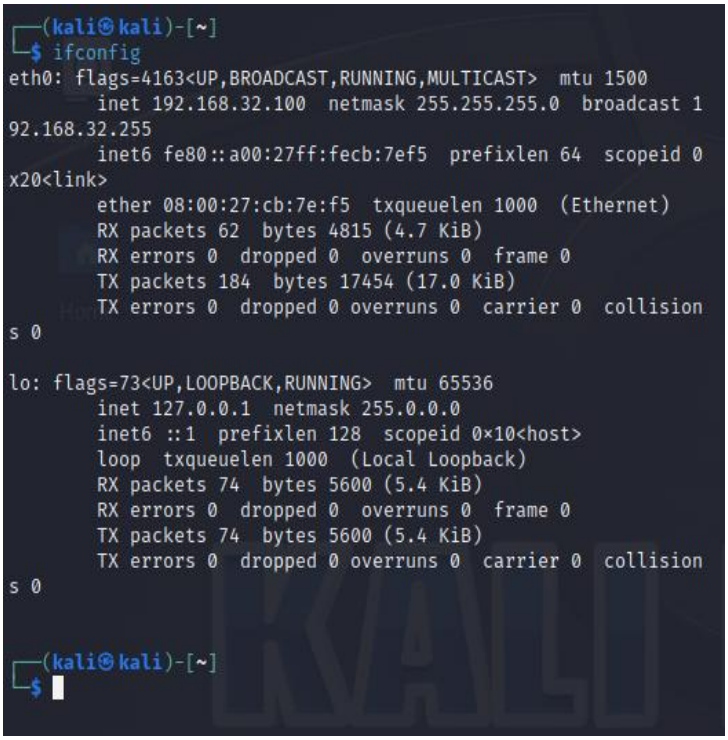
Questo comando apre il file di configurazione di rete, all'interno del quale è possibile impostare l'indirizzo IP della macchina.



Dopo aver apportato le modifiche, è necessario riavviare l'interfaccia di rete per caricare le modifiche. Questo può essere fatto con il comando:

- `sudo systemctl restart networking`commando

-Sudo systemct restart networking



Per verificare se le modifiche sono state applicate correttamente, ho utilizzato il comando:

ifconfig

Questo comando restituisce le informazioni di configurazione di rete. Come si può vedere dall'immagine, il nuovo indirizzo IP è stato impostato correttamente.

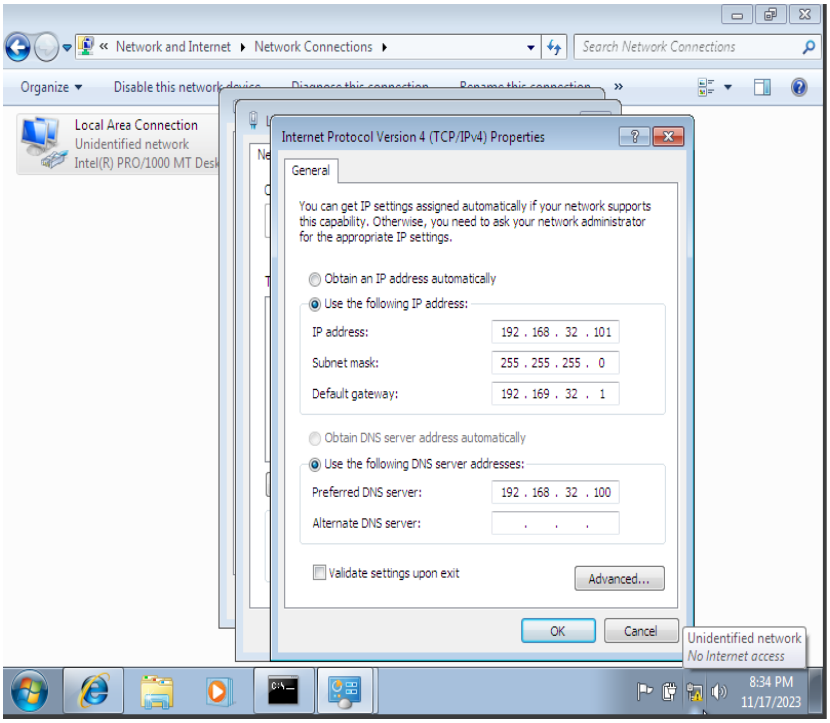
Configurazione IP su una macchina Windows 7

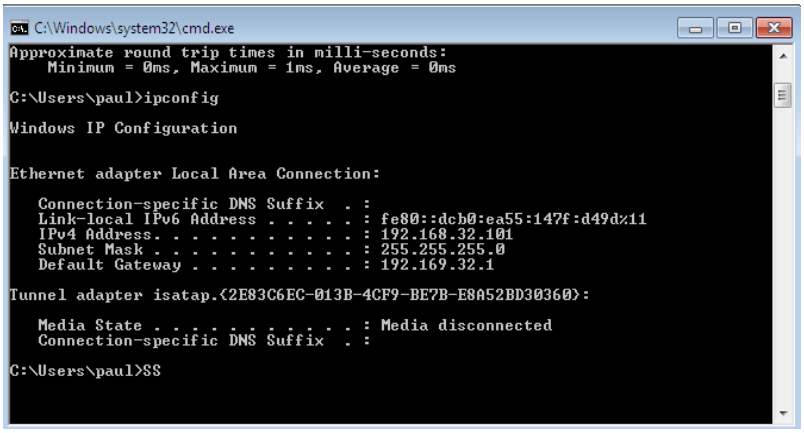
Impostare IP

Per impostare l'indirizzo IP della macchina **Windows 7**, ho acceduto al pannello di controllo, all'interno della configurazione di rete, e ho modificato l'IP del protocollo IPv4 nei connettori.

Nella stessa interfaccia, è possibile impostare il server per la connessione DNS. In questo campo, ho inserito l'IP della macchina **Kali Linux,** che conterrà il servizio DNS della rete.

Per concludere, ho disattivato il connettore e lo ho riattivato.





Controllo del nuovo IP

Con il comando `**ipconfig**`, hai confermato le modifiche. Dall'immagine, si può vedere che l'operazione è andata a buon fine. Ora puoi continuare con la configurazione dei servizi all'interno della macchina **Kali Linux.**

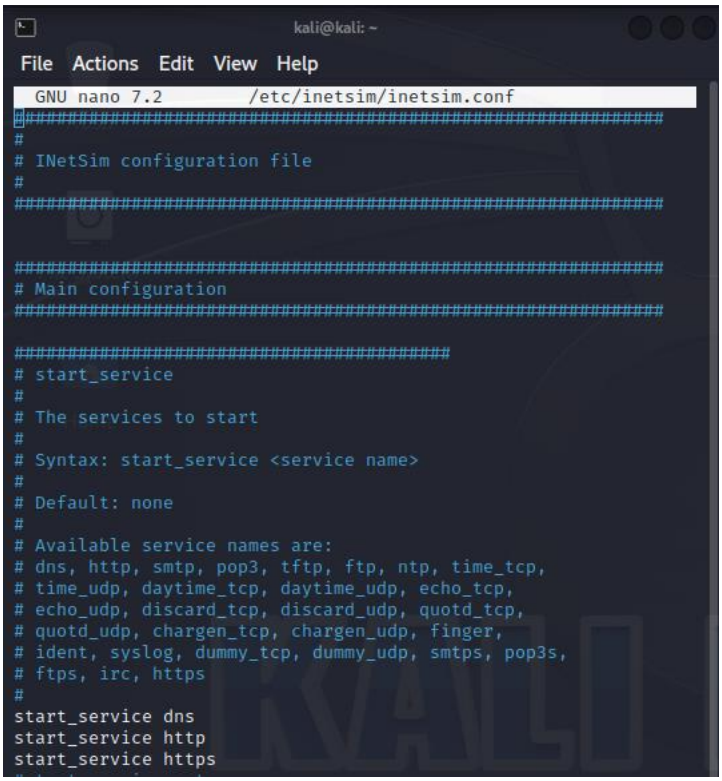
Configurazione di inetsim

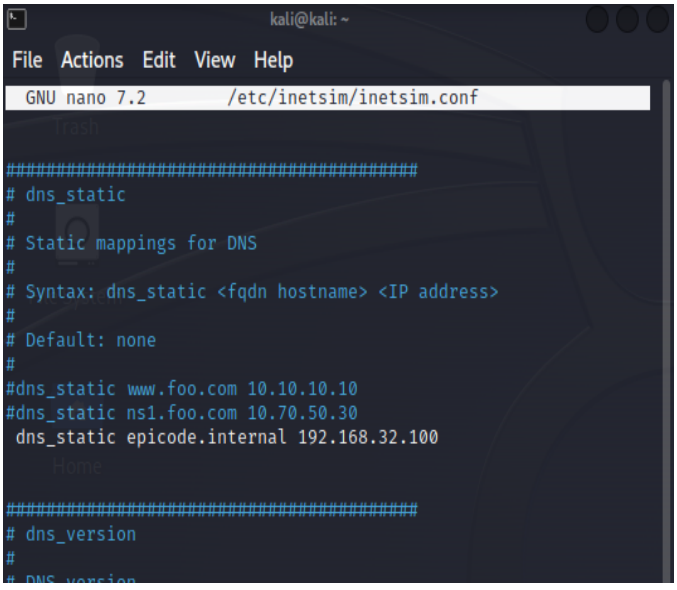
Attivare i servizi

Per configurare inetsim, è necessario modificare il file inetsim.conf, abilitando i servizi richiesti dalla consegna (HTTPS, HTTP, DNS). Per accedere al file di configurazione di inetsim, userai il tool nano, che permette la lettura e la scrittura di file all'interno del terminale di Kali Linux. Puoi accedere al file di configurazione di inetsim con il seguente comando:

- `sudo nano /etc/inetsim/inetsim.conf`

All'interno del file di configurazione, troverai un elenco di servizi. Per questo esercizio, hai bisogno solo dei servizi DNS, HTTPS e HTTP. Per attivare questi servizi, basta rimuovere il '#' prima del comando 'start_service'.





Configurazione DNS

I servizi HTTPS e HTTP sono pronti per l'uso. Per il servizio DNS, invece, è necessario impostare i domini che desideri associare all'interno della rete con un IP statico. In altre parole, devi indicare il nome della pagina e in quale macchina si può trovare il servizio. Nella rete che hai configurato, l'IP della macchina che contiene il servizio web coincide con quello del server DNS, quindi hai inserito l'IP dell'host Kali Linux.

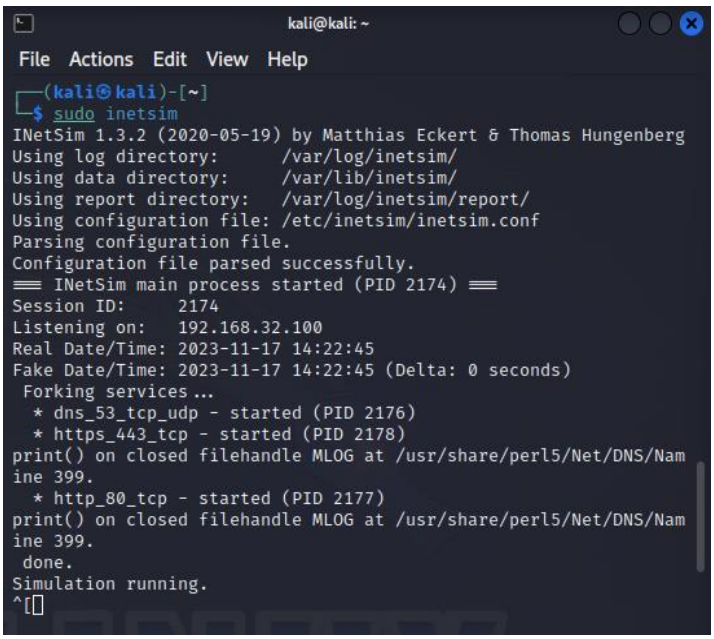
Per concludere, basta salvare il file e attivare Inetsim.

Attivaza Inetsim

Per attivare Inetsim, è sufficiente eseguire il comando:

- `sudo inetsim`

Sul terminale inizierà a visualizzare i dati della 'Simulation running' di Inetsim. A questo punto, puoi procedere a controllare la connessione su **Windows 7**.

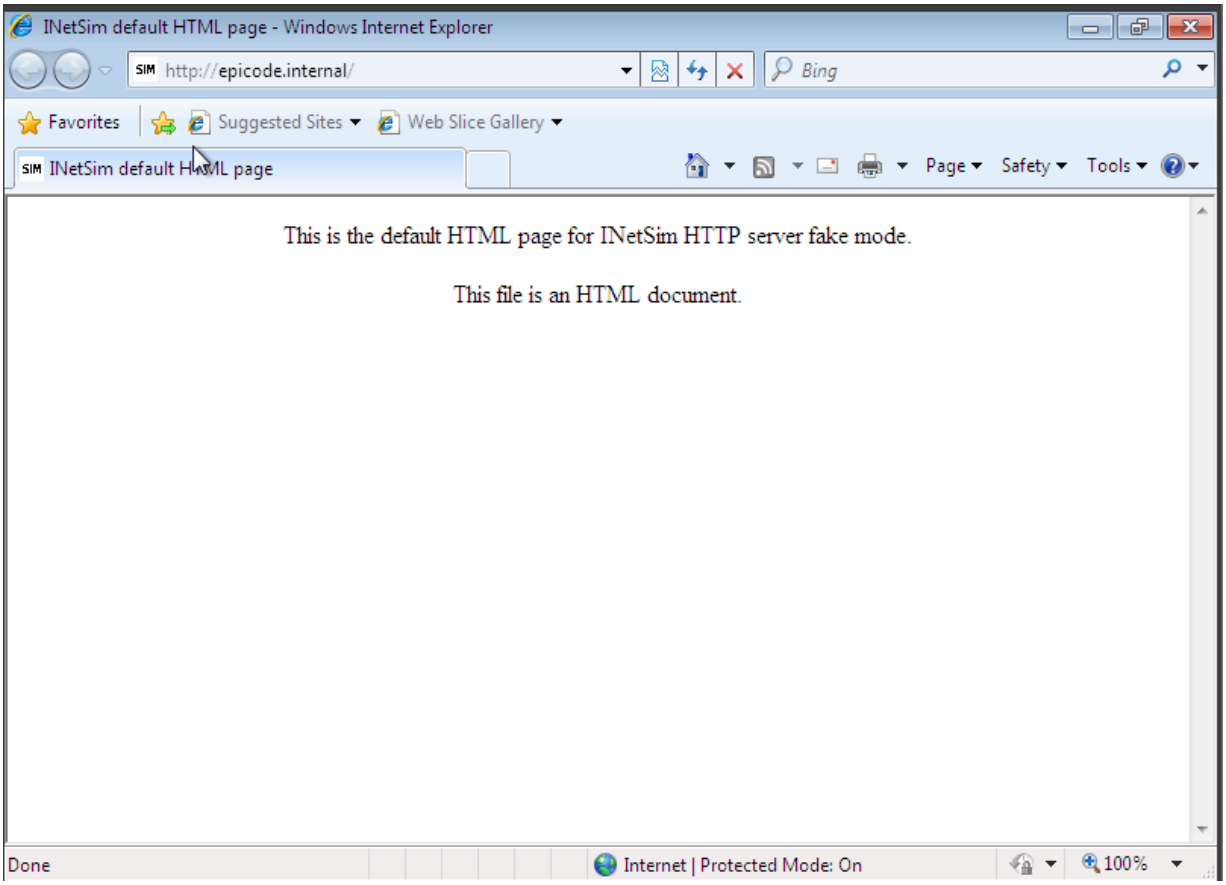


Concessione e controllo del corretto funzionamento della rete.

Connessione http

Dopo aver configurato gli IP sulle macchine e i servizi Web e DNS sull'host Kali Linux, hai proceduto a fare una richiesta HTTP dal browser di Windows 7 con il dominio del servizio web ('epicode.internal' come richiesto).

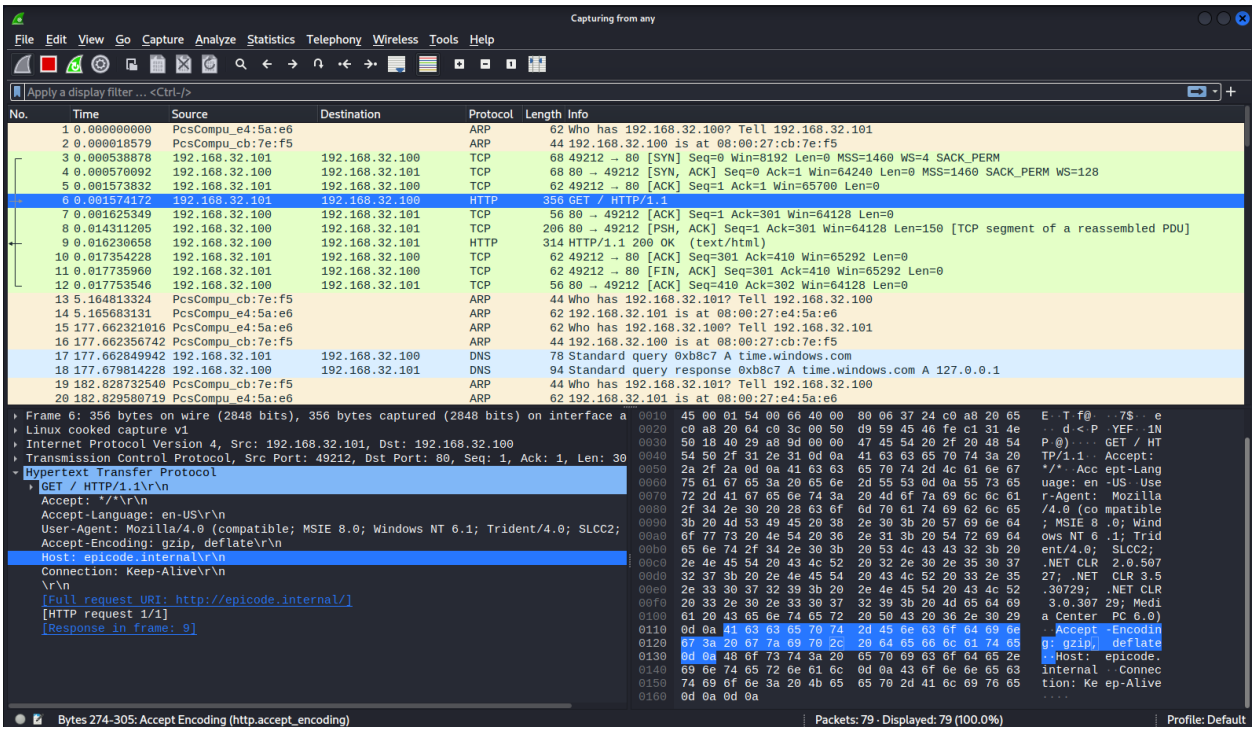
Dall'immagine, si può vedere che la richiesta del servizio HTTP è andata a buon fine e il server DNS sta funzionando perfettamente perché è riuscito a interpretare il dominio 'epicode.internal'. Questo è un ottimo risultato!



Analisi della rete http

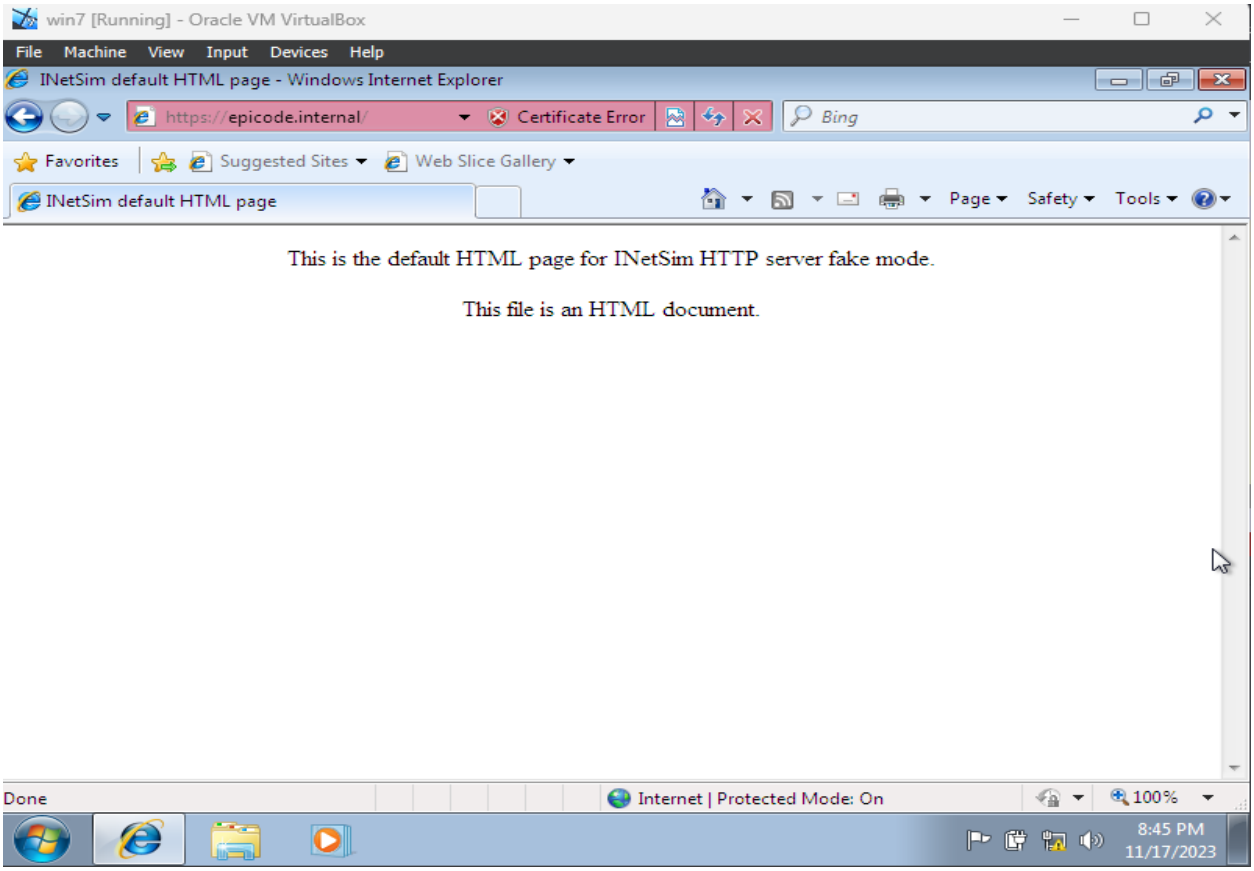
Utilizzando il tool Wireshark, è possibile visualizzare il traffico dei pacchetti e come il PC Windows 7 effettua una richiesta GET HTTP al server Kali. Questo è evidente dall'IP di origine (che coincide con quello del PC Kali Linux) e dall'IP destinatario (che coincide con quello del PC Windows 7).

È interessante notare che la comunicazione HTTP avviene in chiaro, mostrando tutti i dati della pagina. Questo è un aspetto importante da considerare per questioni di sicurezza e privacy.



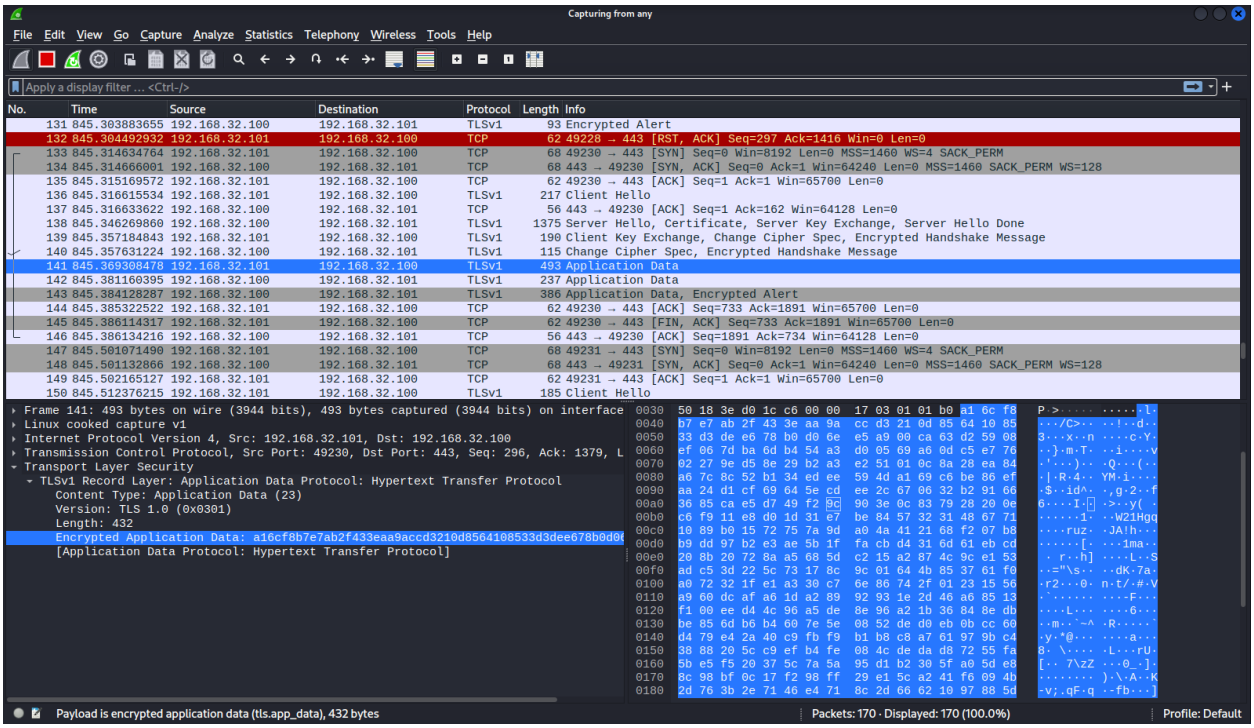
Connessione HTTPS

Eseguendo lo stesso test ma con il protocollo HTTPS, il browser riesce a connettersi anche in questo caso al dominio 'epicode.internal'. Si può notare che non trova un certificato valido, ma questo potrebbe essere dovuto al fatto che stiamo usando un servizio di provenienza ignota per il browser.



Analisi della reste HTTPS

Da Wireshark, si può notare che la situazione è simile a quella del protocollo HTTP. Ora, però, i pacchetti utilizzano il protocollo TCP e i dati non sono più in chiaro. Inoltre, ci sono più passaggi di connessione dovuti all'handshake tra le due macchine per impostare la chiave di crittografia. Questo è un aspetto fondamentale del protocollo HTTPS, che garantisce una comunicazione sicura tra client e server.



Indirizzo MAC

Un'informazione interessante che possiamo osservare all'interno del traffico di rete è l'indirizzo MAC della macchina che effettua la richiesta del servizio, in questo caso della macchina Windows. Dall'immagine, si può notare l'indirizzo MAC della macchina Windows 7 all'interno dei pacchetti TCP per la connessione HTTPS. Questo dettaglio può essere utile per l'analisi del traffico di rete e per identificare specifici dispositivi all'interno della rete.