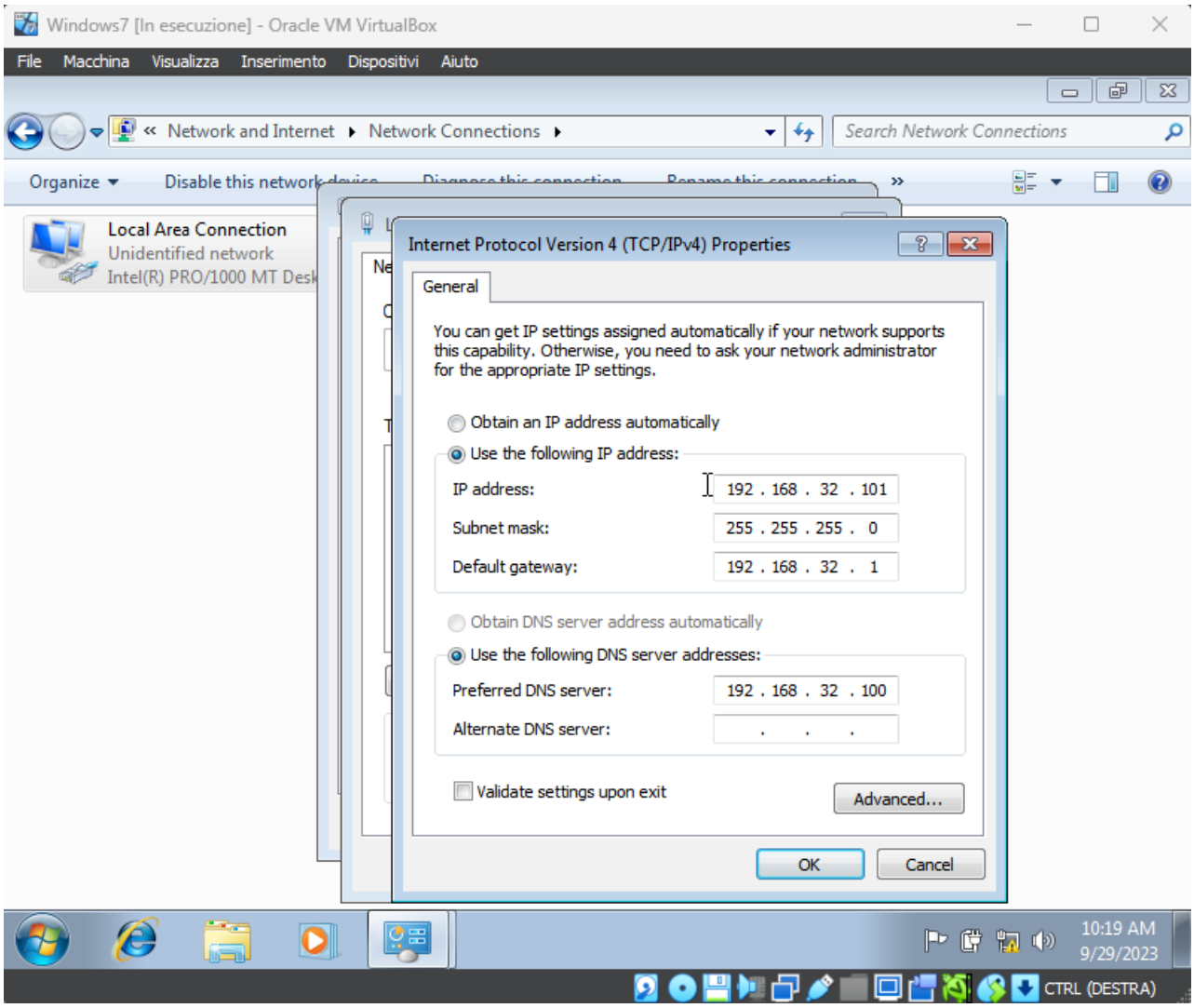
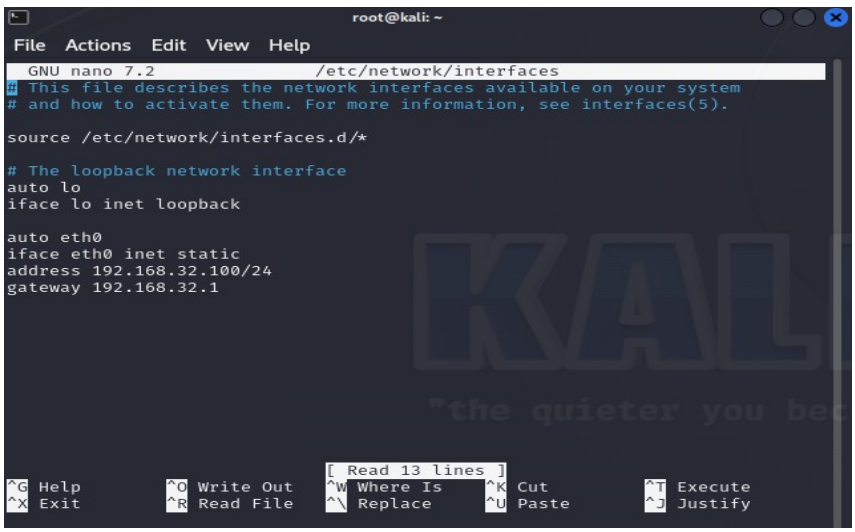
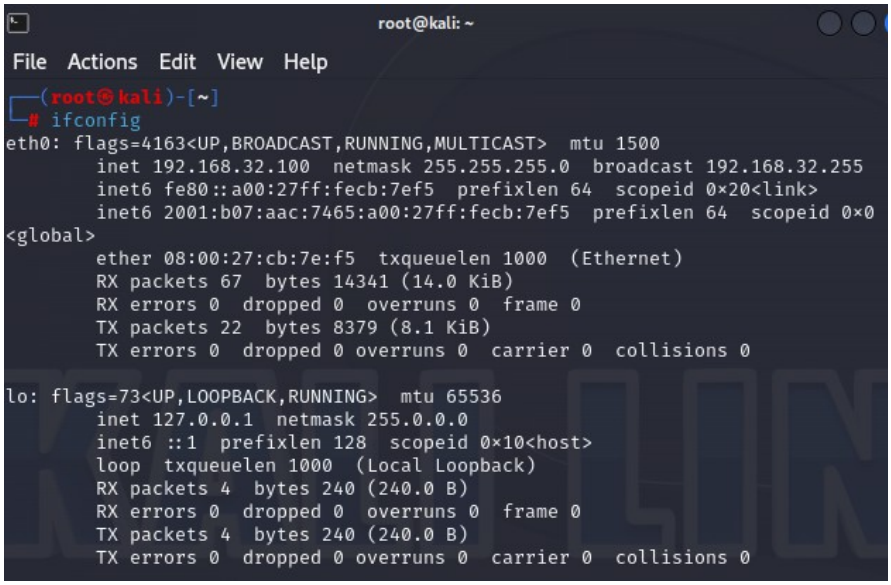
Progetto 29/09 - Luca Danelli

Imposto l'ip sulla macchina windows 7 configurando come server DNS l'ip che andrò ad assegnare alla macchina kali:

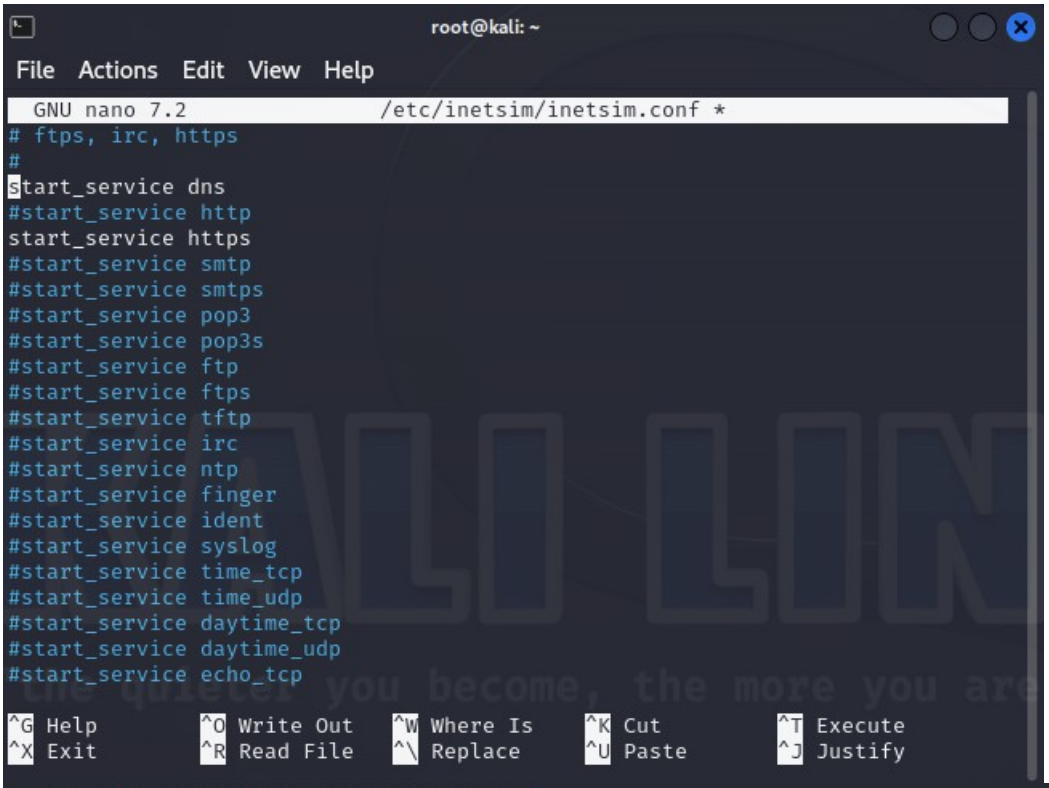


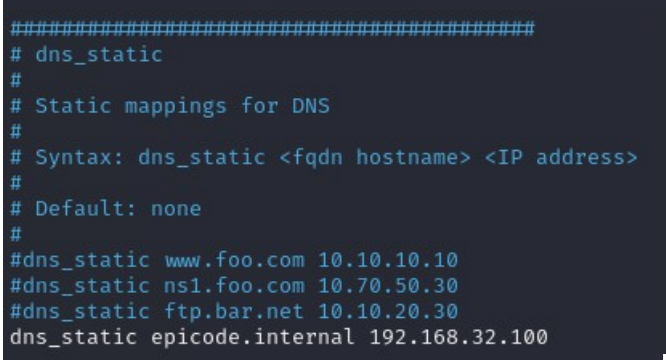
Imposto l'ip sulla macchina Kali con il comando **sudo nano /etc/network/interfaces**, andando quindi a modificare il file di configurazione di rete con l'editor nano, successivamente riavvio la macchina con il comando **sudo reboot** per applicare la configurazione:

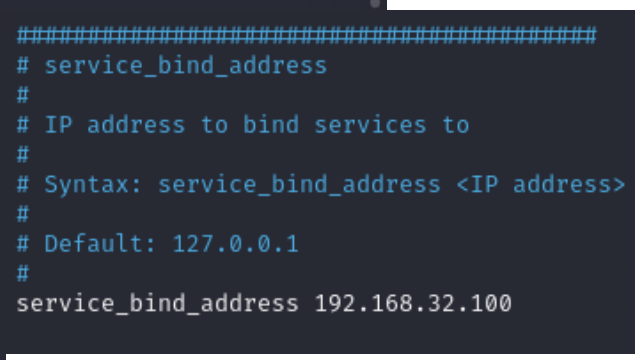




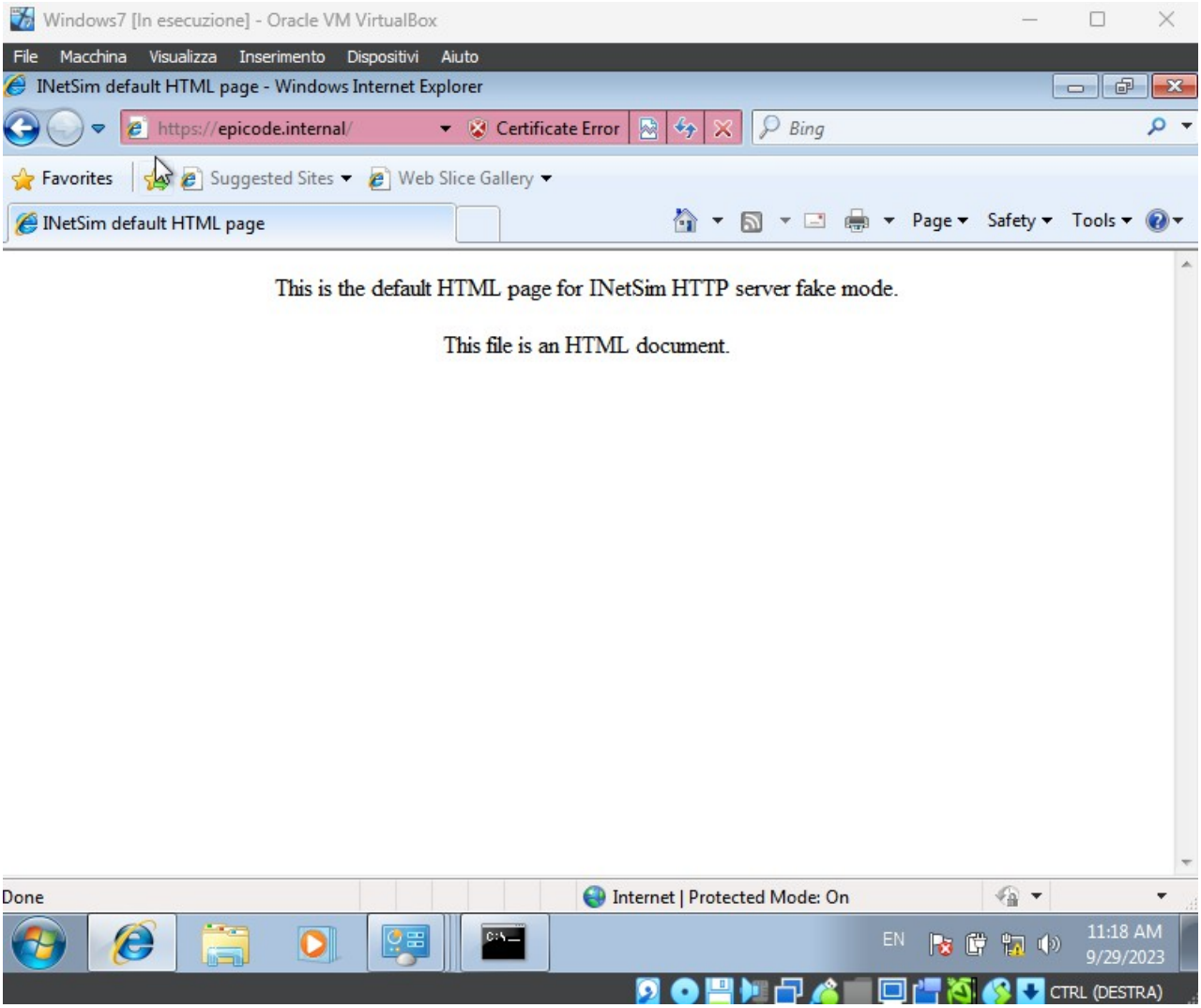
Con il comando **sudo nano /etc/inetsim/inetsim.conf** vado ad editare il file di configurazione di inetsim, andando ad attivare i servizi DNS e HTTPS come in figura e creando il record per associare epicode.internal all'indirizzo 192.168.32.100. Inoltre attivo i servizi sull'ip 192.168.32.100 modificando l'impostazione di default del bind address:



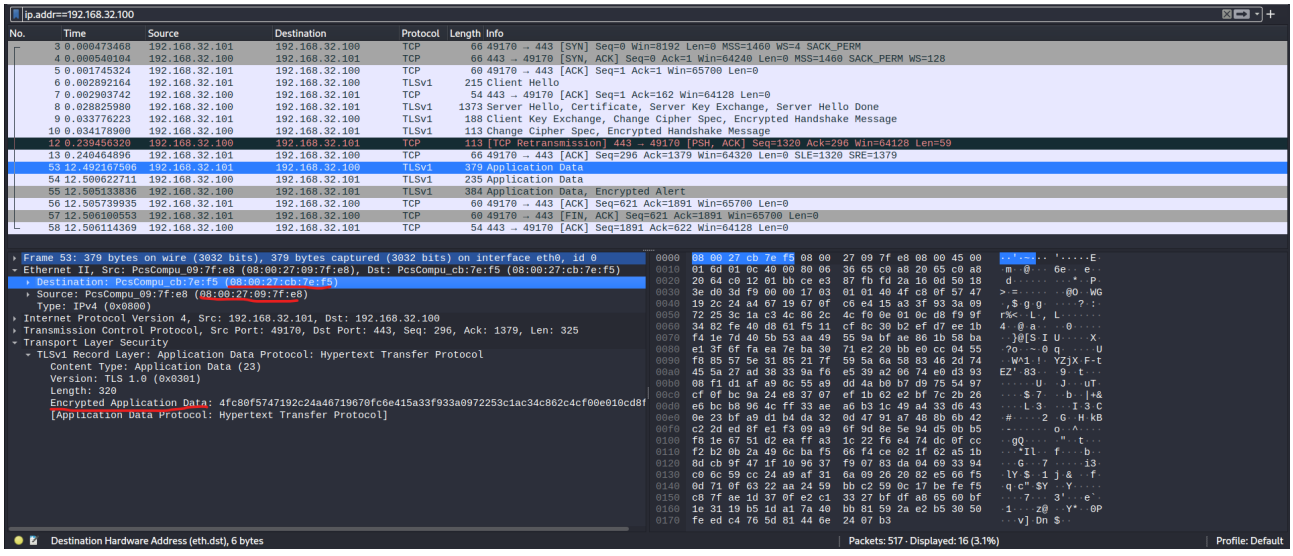




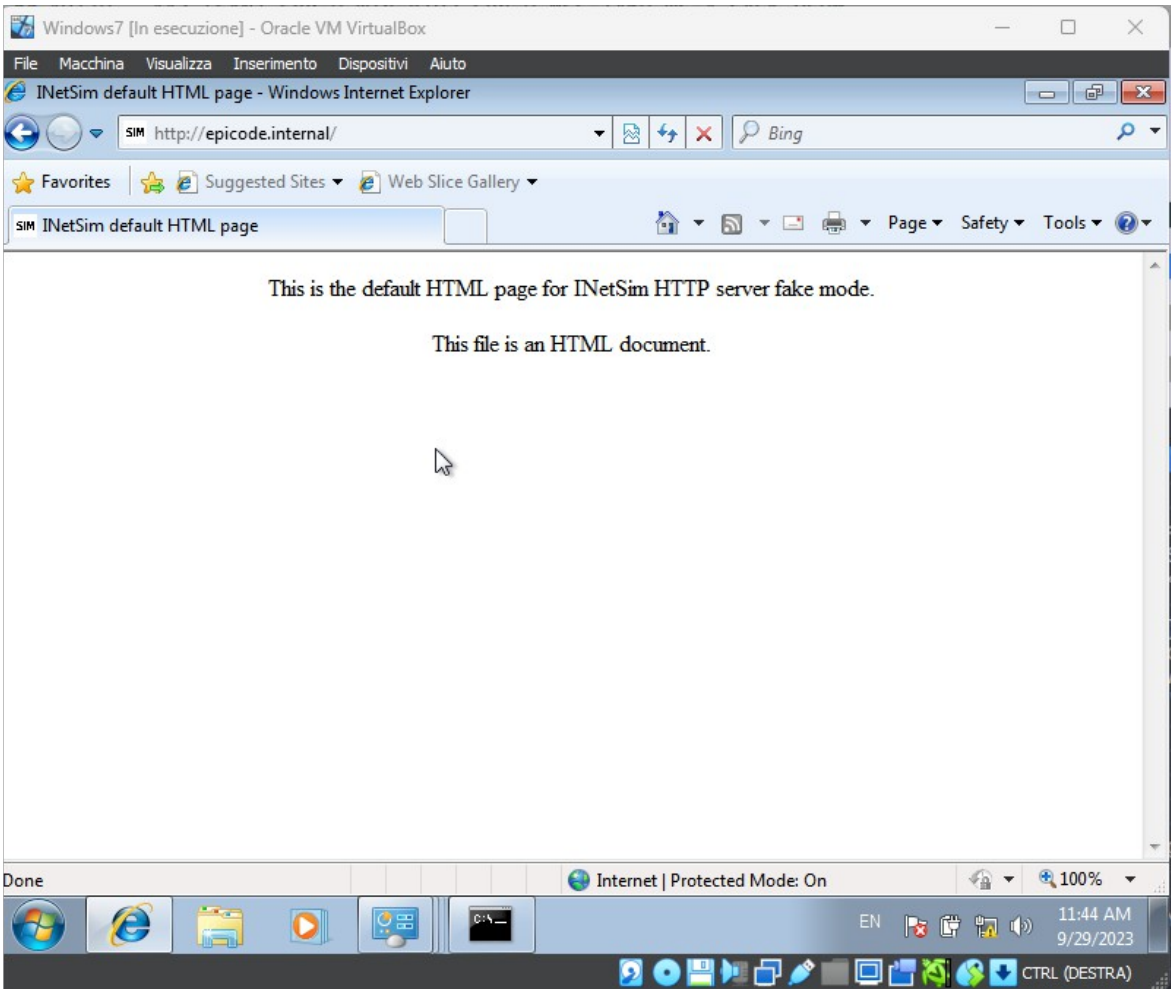
Successivamente da W7 punto da browser all'indirizzo epicode.internal. Accettando il rischio per la mancanza di certificato viene esposta questa pagina:



Di seguito la cattura con wireshark filtrata per ip 192.168.32.100, nell'immagine ho evidenziato in rosso i mac-address sorgente e destinazione di un pacchetto Application Data e la parte dove informa che il contenuto del payload è criptato:



Ripeto poi il procedimento visto sopra per attivare il servizio HTTP da inetsim andando a togliere il commento questa volta sul service_http su macchina Kali ed effettuo una richiesta HTTP da W7 verso Kali:



Traccio anche questa comunicazione con Wireshark da Kali. Noto che questa volta il testo html scambiato risulta visibile, evidenziato in rosso nell'immagine assieme ai mac-address. Questo perché il protocollo HTTP non si avvale di cifratura come l'HTTPS: