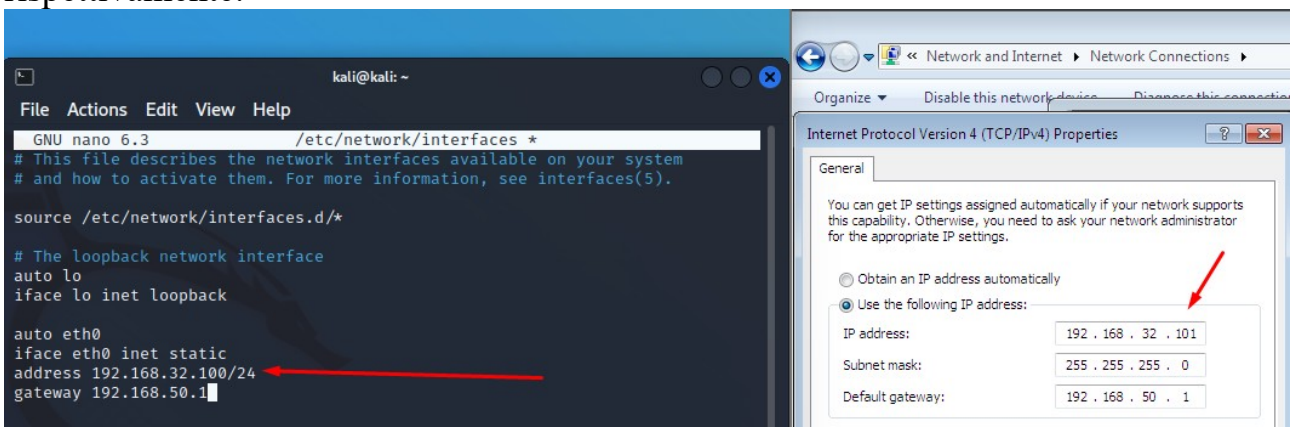
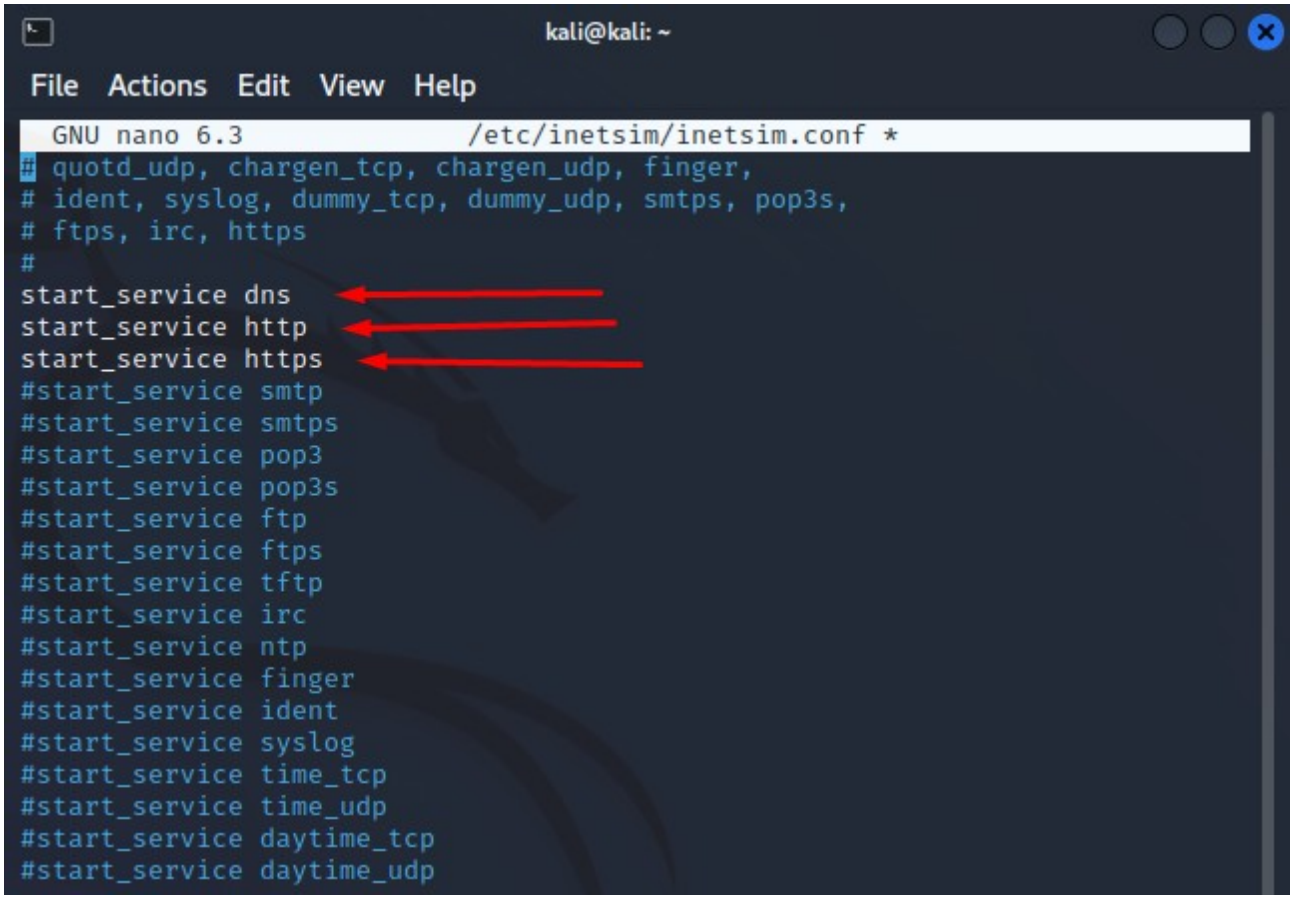
Alaimo Alessandro
28/10/2022

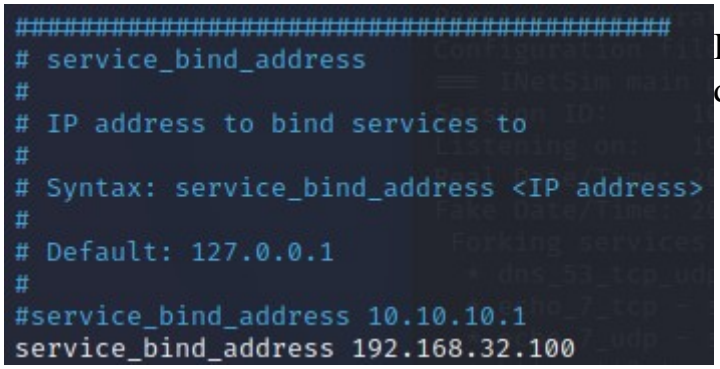
Esercizio Weekend

Come prima cosa andiamo ad impostare i nuovi indirizzi IP alle macchine virtuali, rispettivamente:



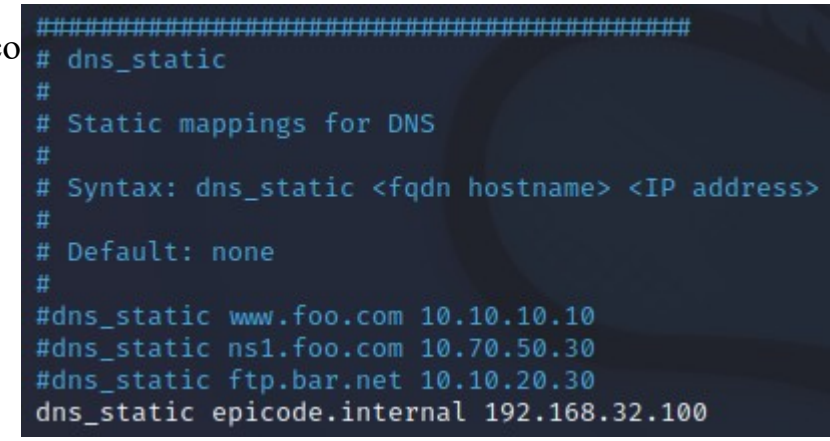
Ora andiamo a configurare il servizio INETSIM andando anche a disabilitare i servizi non richiesti:



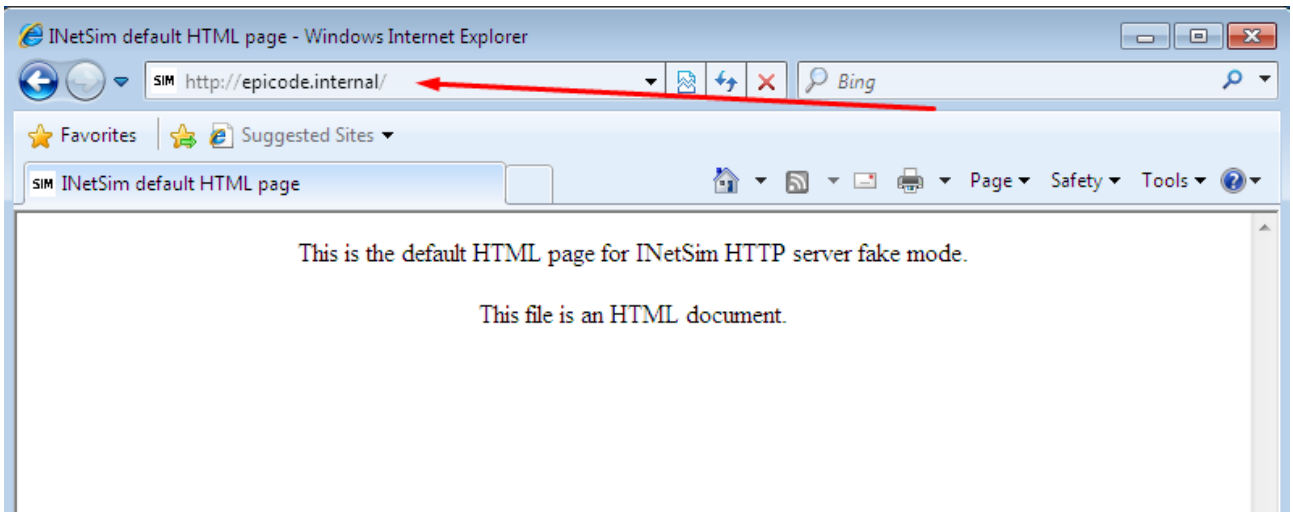


Imposto come IP del DNS, quello della macchina Kali Linux

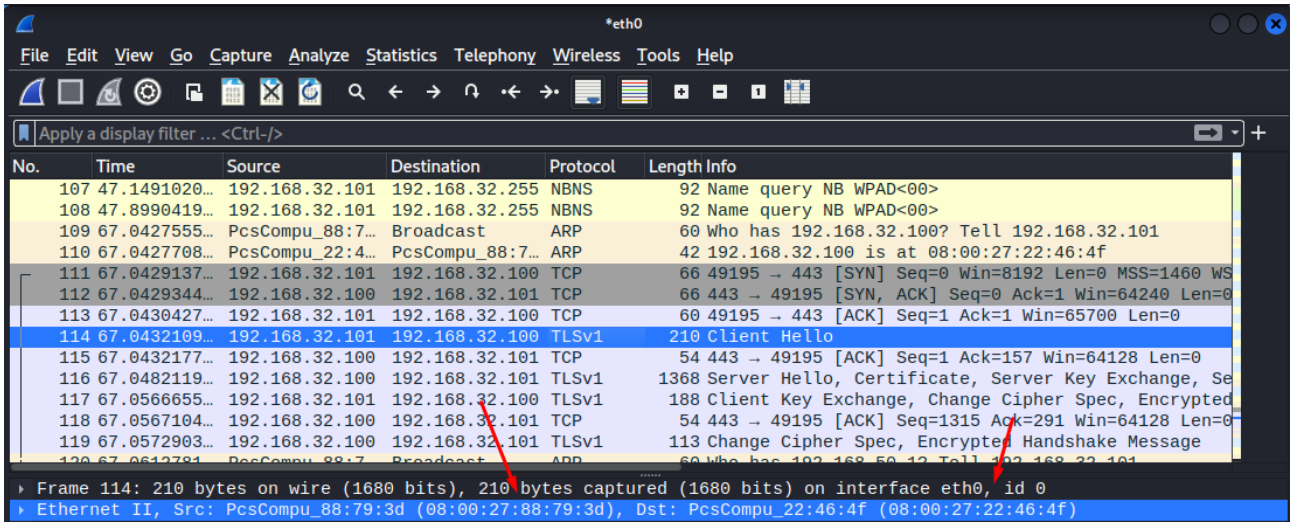
Adesso impostiamo come dns statico epicode.internal



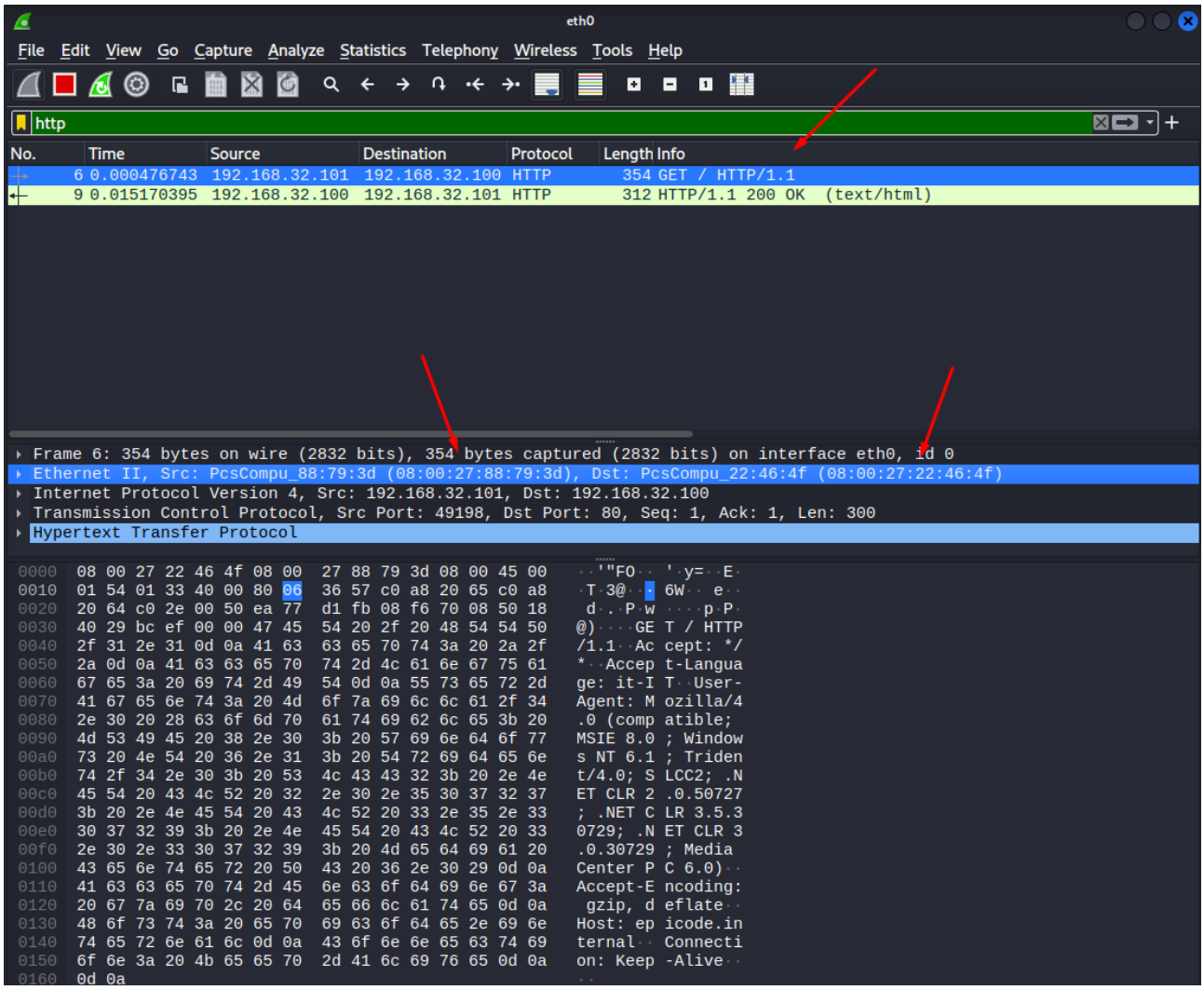
Fatto ciò ora non rimane altro che verificare se viene effettuata la connessione al DNS server da Windows 7:



Ora aprendo Wireshark, andiamo a controllare i pacchetti inviati nel server HTTPS:



08:00:27:88:79:3d (Win7)
08:00:27:22:46:4f (Kali)



Le principali differenze che possiamo notare sono:

- Il protocollo usato nei pacchetti dei siti web, ossia HTTP e TLSv1;
- Il pacchetto TLSv1 non può essere analizzato poiché prima dell'invio dei pacchetti, viene creato un tunnel sicuro in cui si scambiano le chiavi, criptandone il messaggio, cosa che non succede nell'invio di pacchetti con protocollo HTTP.