TEST DI VALUTAZIONE MODULO 1

Andrea Ferrantino

La prova chiede di constatare le competenze avute fino ad ora..

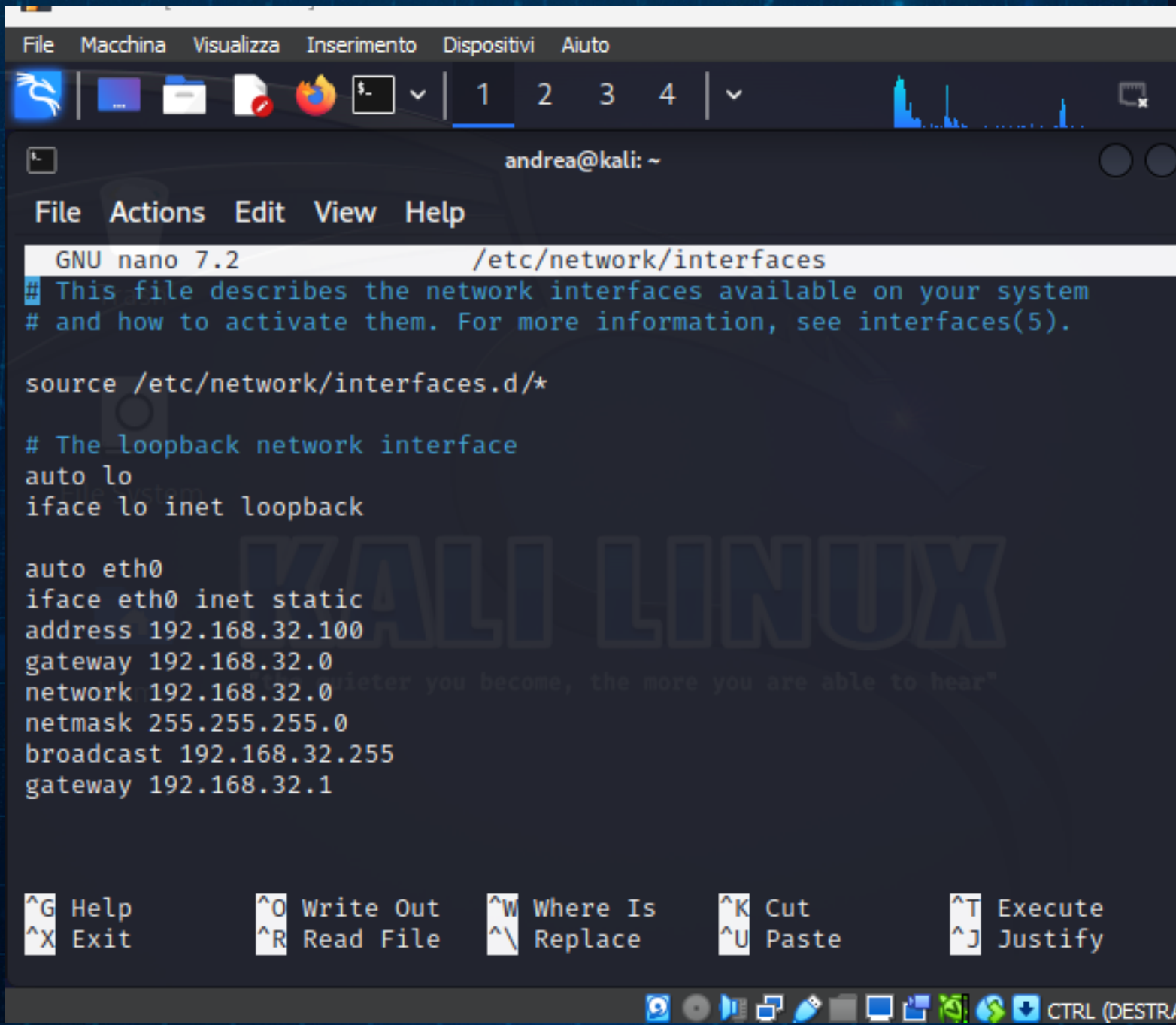
- **Settaggio IP Kali Linux VM (192.168.32.100)**
- **Settaggio IP Windows 7 VM (192.1342.32.101)**
- **HTTPS server attivo**
- **Servizio DNS per risoluzione nomi domini attivo**

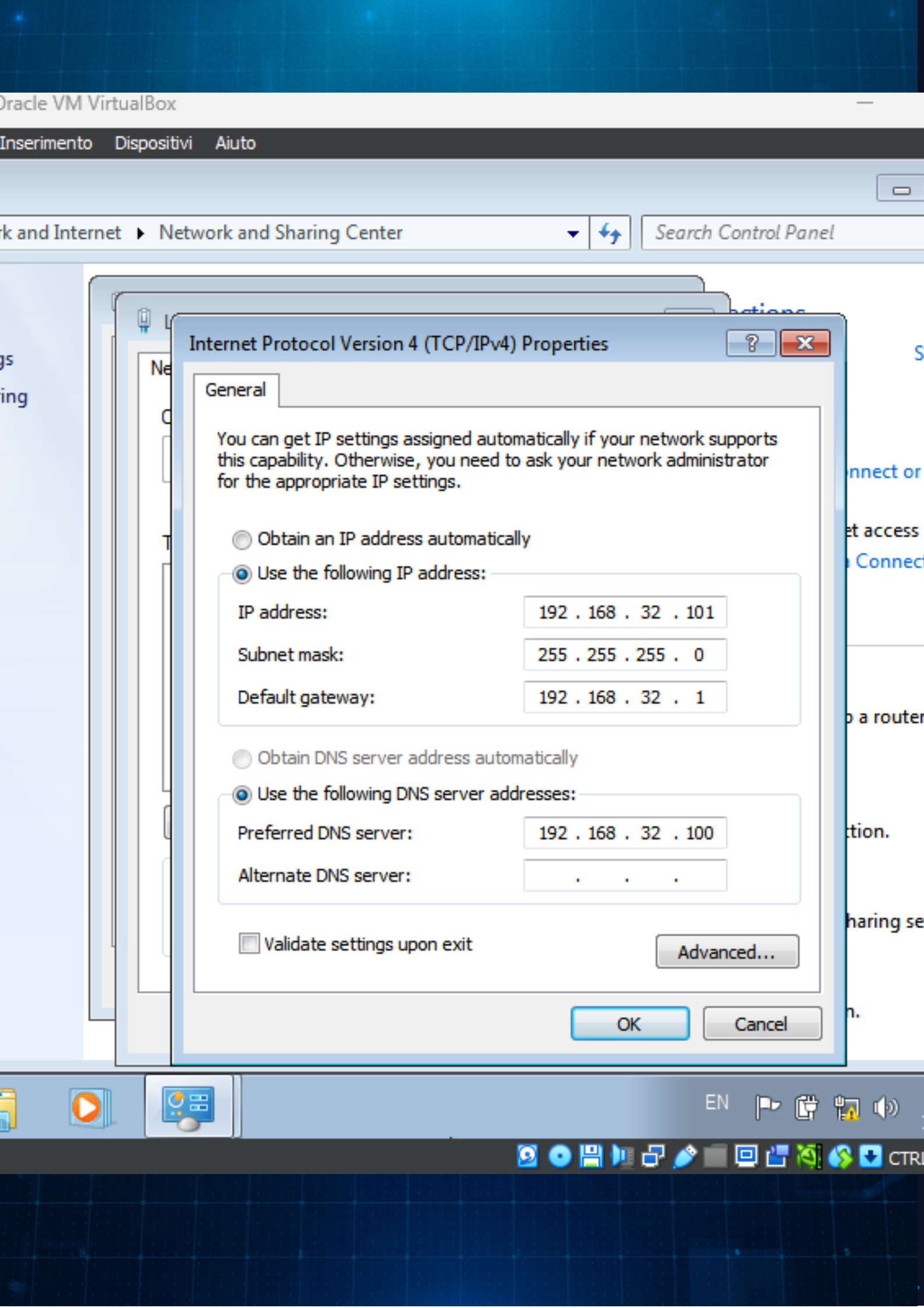
Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (Kali). Si intercetti poi la comunicazione con Wireshark,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

Configurazione IP Kali e Windows 7

Come prima cosa dobbiamo configurare gli indirizzi ip delle macchine virtuali come da traccia:

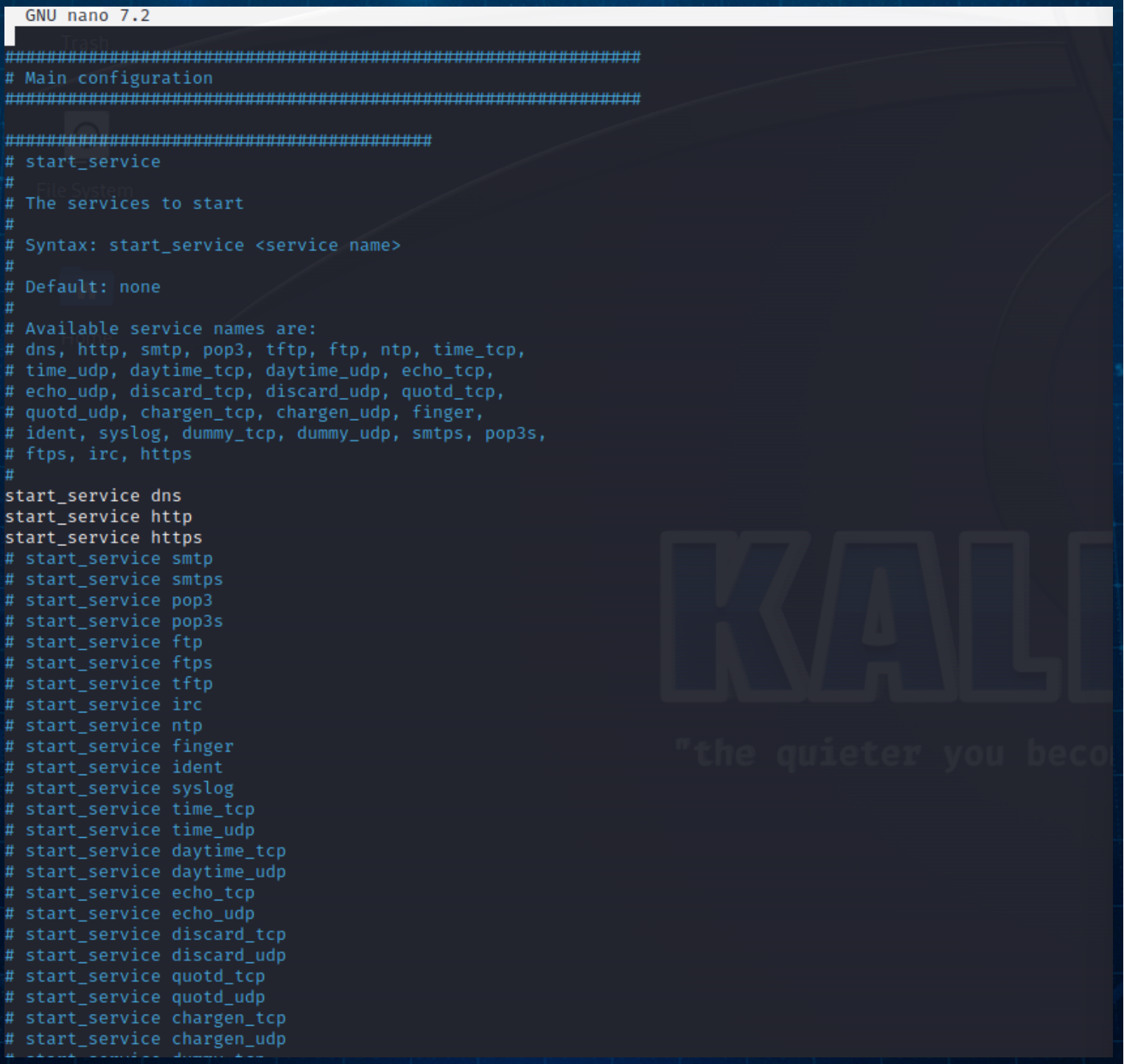
Utilizziamo il comando (sudo nano /etc/network/interfaces)



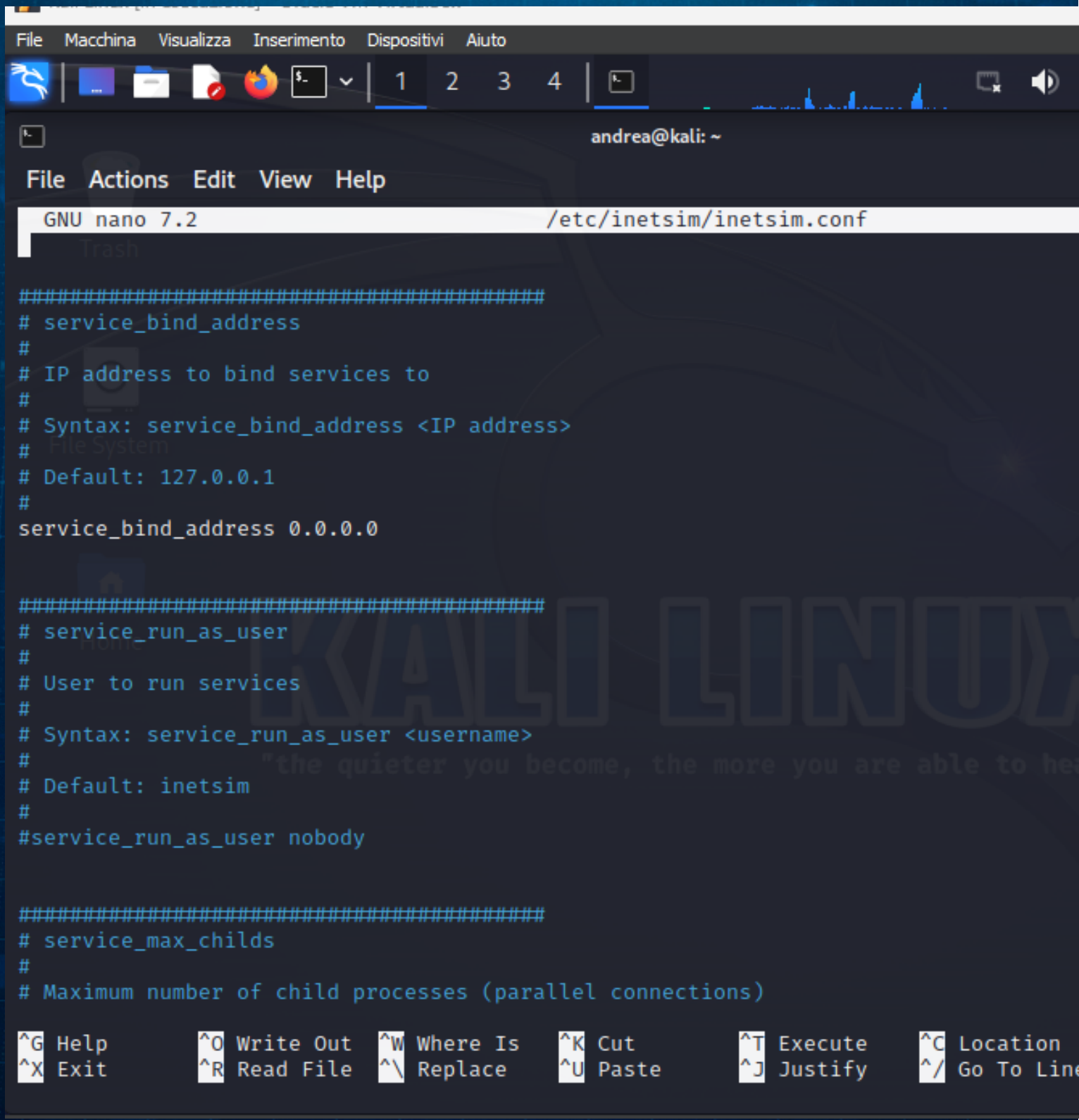

Oracle VM VirtualBox
Inserimento
Dispositivi
Aiuto
rk and Internet
Network and Sharing Center
Search Control Panel
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 32 . 101
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168 . 32 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
192 . 168 . 32 . 100
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
EN

Configurazione Intesim.conf

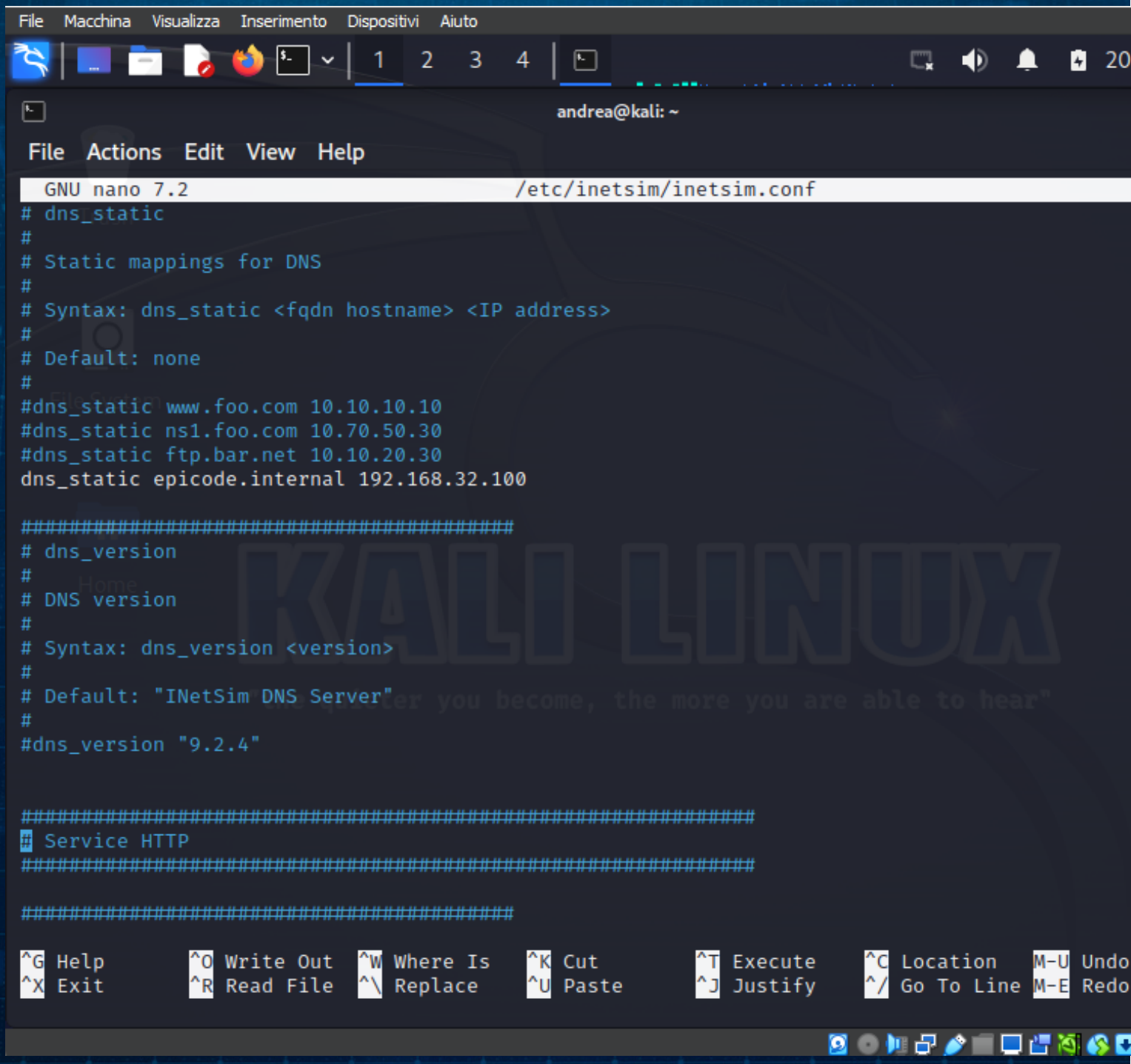
Successivamente dobbiamo andare all'interno di inetsim.conf avviando da Kali e digitando il comando (sudo nano /etc/inetsim/inetsim.conf) cosi andremo ad abilitare i service DNS,HTTP,HTTPS togliendo l'# davanti alla voce come screen qui sotto:



Successivamente impostiamo il “service_bind_address con l’IP “0.0.0.0” che va bene con tutte le piattaforme.

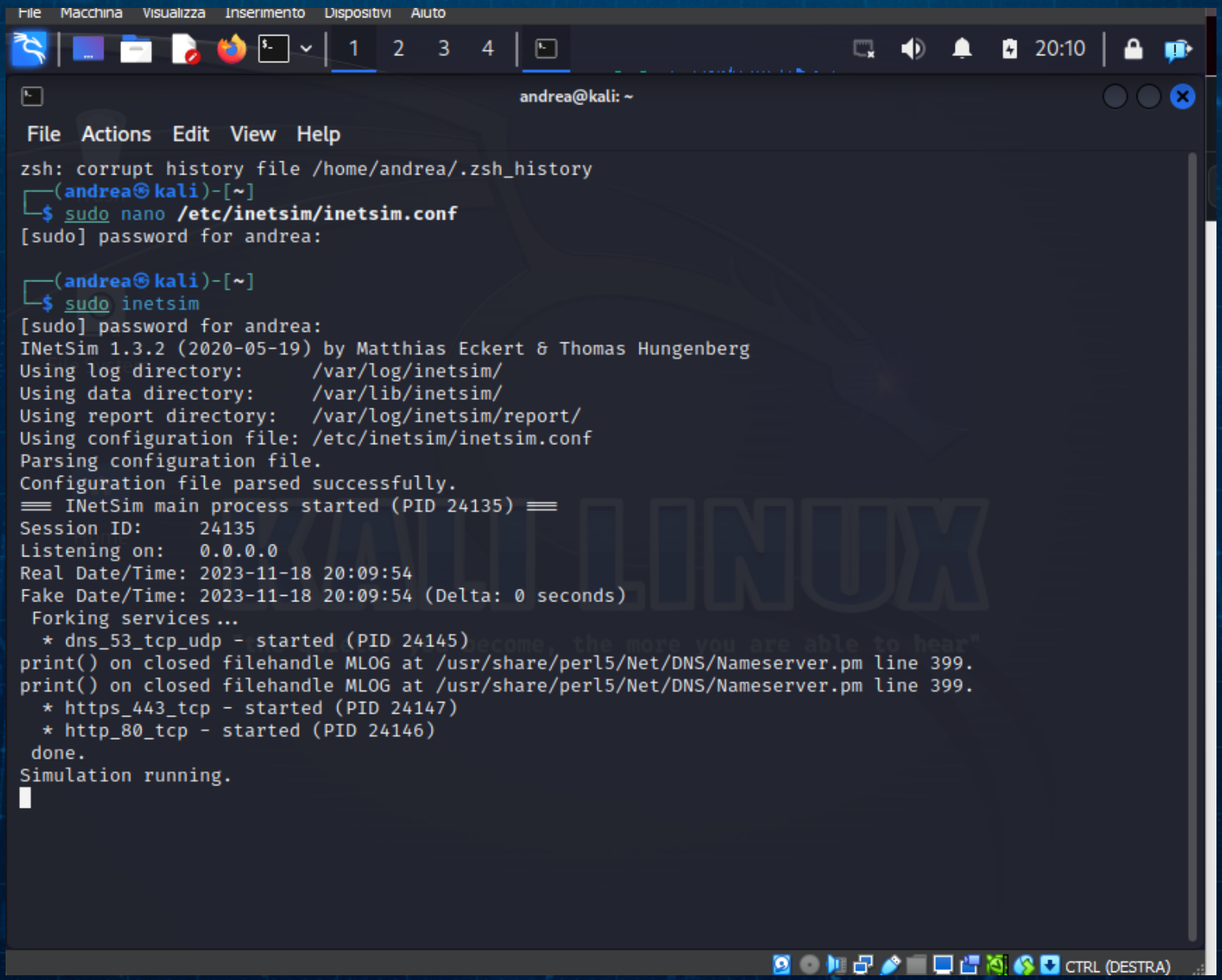


Ora per risolvere l'hostname "epicode.internal associando come "dns_static" lo stesso ip di Kali:



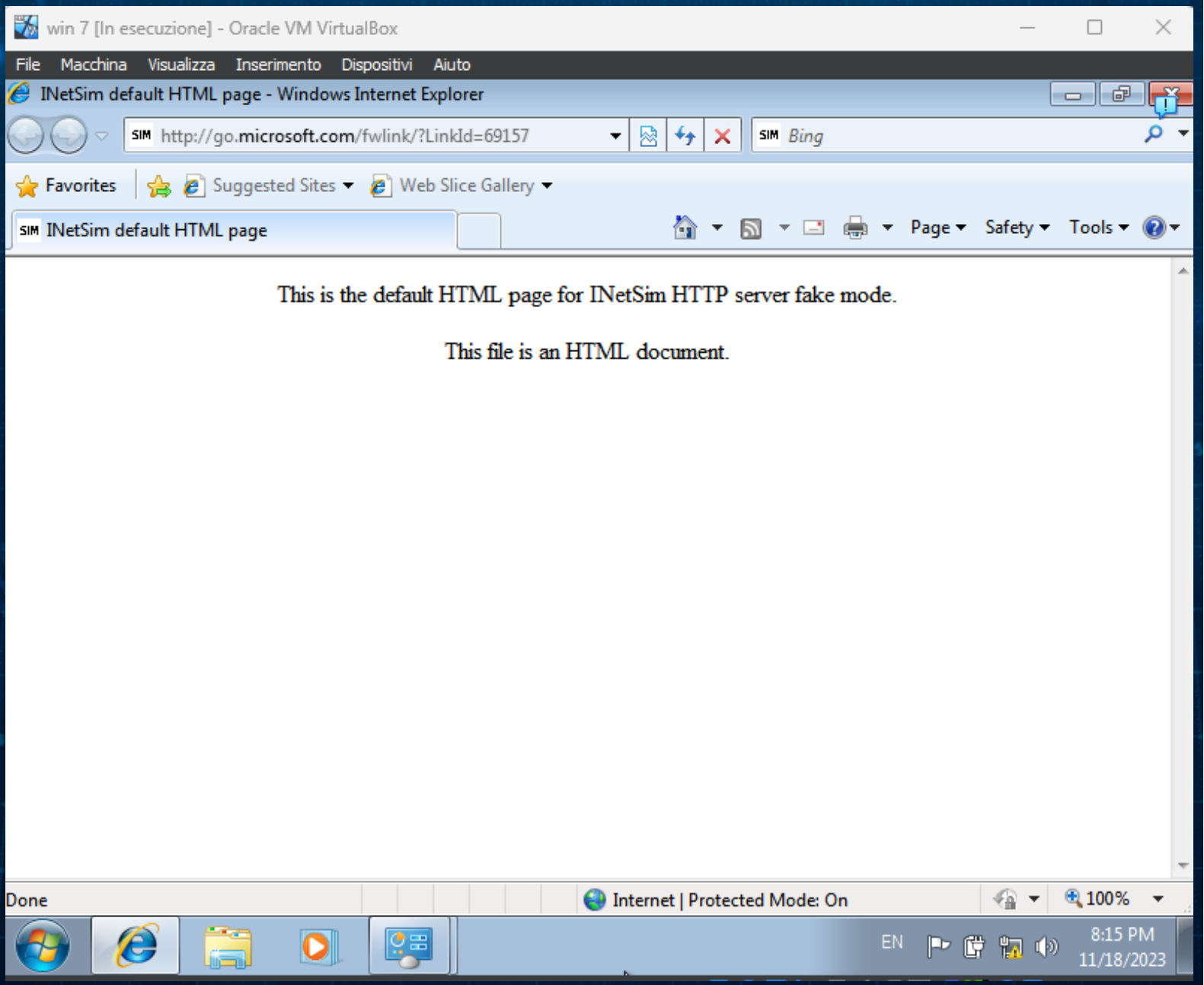
Simulazione Inetsim

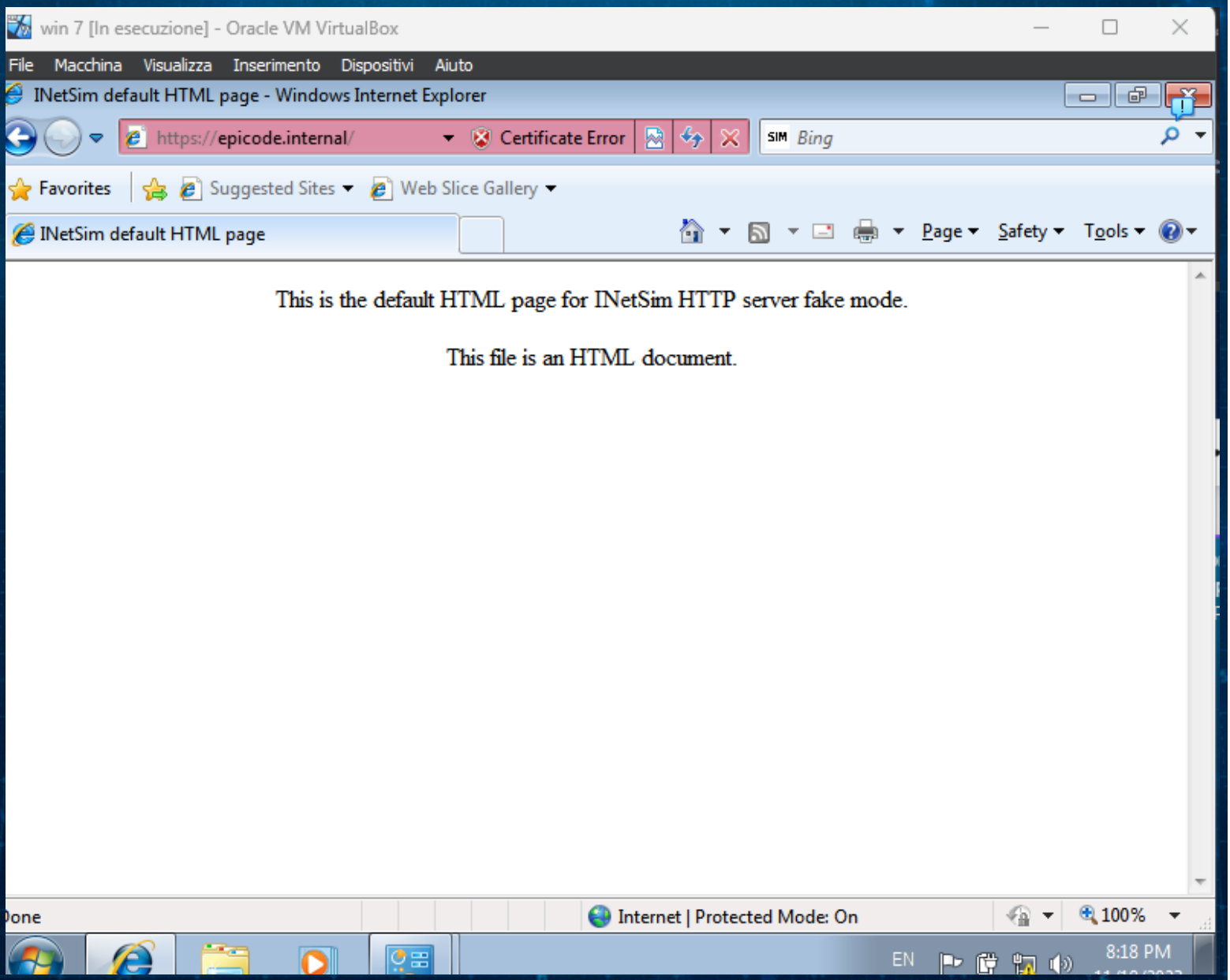
Digitando il comando “sudo inetsim” sul terminale di Kali partirà il client del server:



Fatto ciò se tutto sarà settato correttamente attraverso Internet Explorer su Windows 7 possiamo collegarci sia con HTTP che con HTTPS ai seguenti:

- http://epicode.internal
- https://epicode.internal

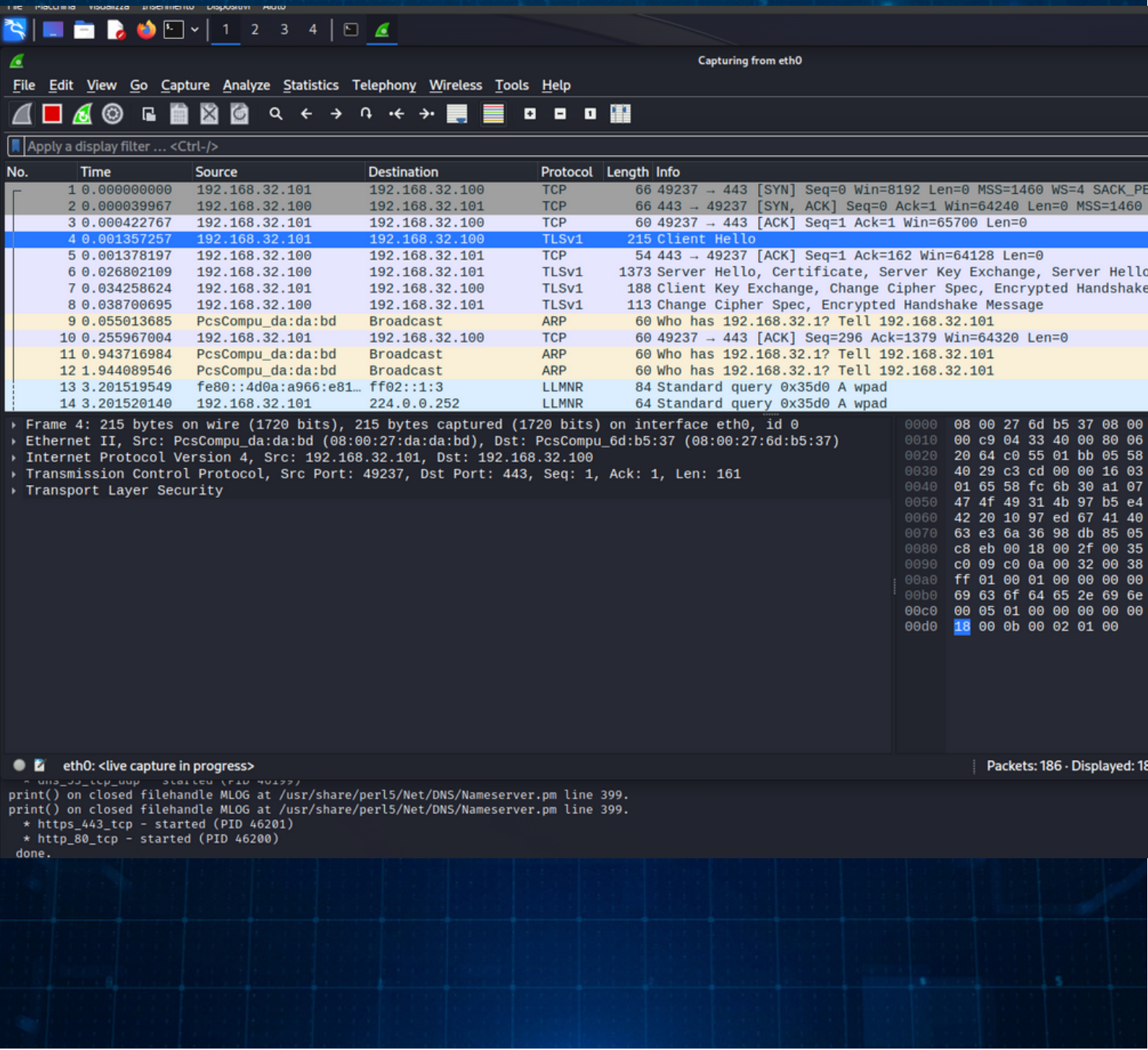



win 7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
INetSim default HTML page - Windows Internet Explorer
https://epicode.internal/
Certificate Error
Bing
Favorites
Suggested Sites
Web Slice Gallery
INetSim default HTML page
Page
Safety
Tools
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.
Done
Internet | Protected Mode: On
100%
EN
8:18 PM

Packet Capture con Wireshark

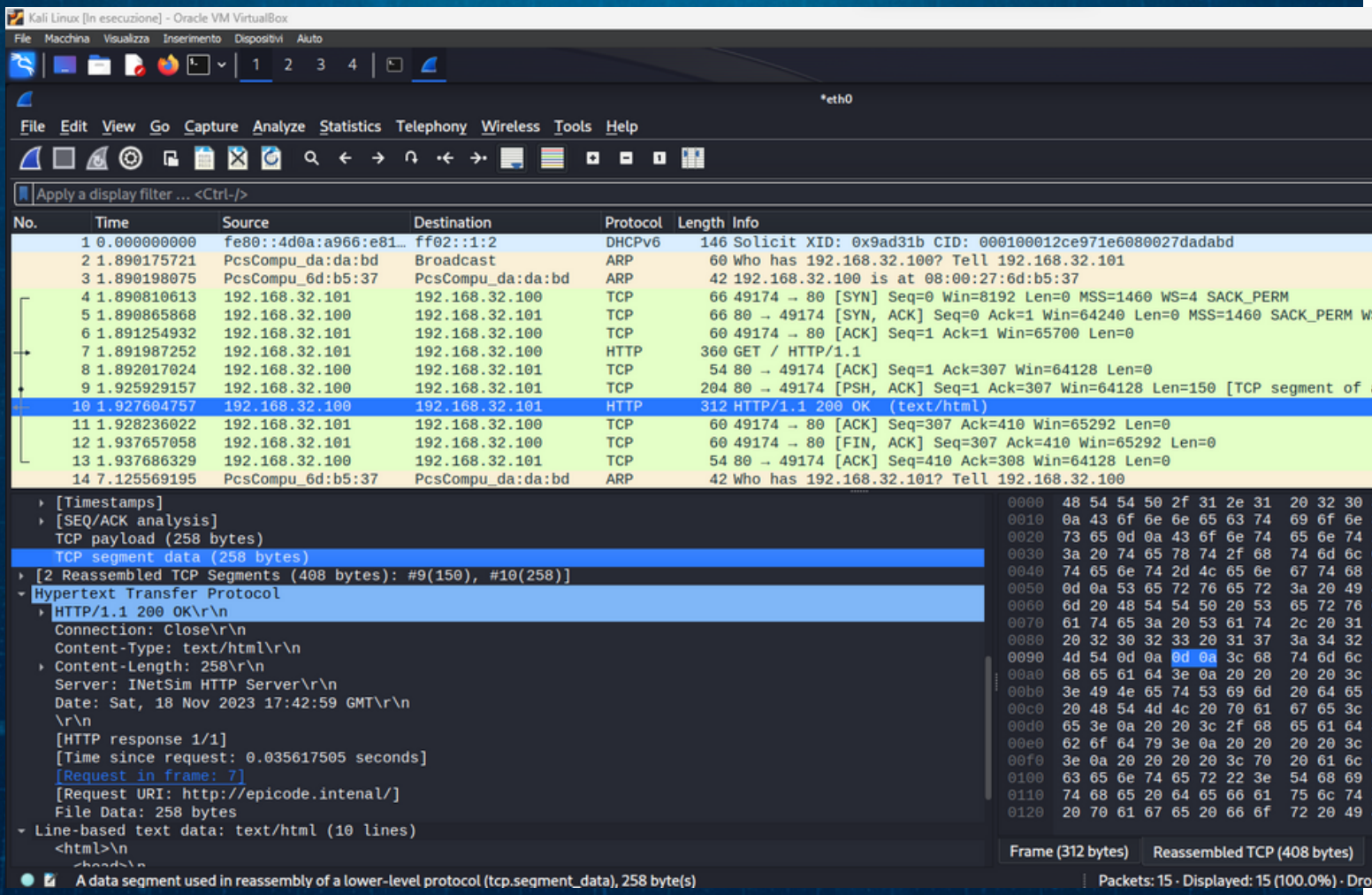
Verifichiamo che i pacchetti tra Windows 7 e Kali trasmettano correttamente attraverso il tool Wireshark effettuando il packet capture attraverso l'interfaccia di rete "eth0"

- Traffico HTTPS:



Ne protocollo HTTPS i dati sono criptati,infatti possiamo notare la three-way-handshake dove avviene uno scambio di pacchetti TLS che serve pe garantire i dati sensibiliil

- Traffico HTTP:



Possiamo notare uno scambio di pacchetti ARP.Nel primo pacchetto la macchina windows chiede un messaggio broadcast a tutti i dispositivi della rete,nel secondo Kali risponde di avere l'indirizzo ip richiesto (192.168.32.101)

Successivamente abbiamo la three-hand-shake

Subito dopo abbiamo una richiesta GET Windows 7 a HTTP,con la riposta del codice 200 che conferma la trasmissione a Windows.

Inoltre cliccando sul pacchetto 40 possiamo vedere il contenuto in chiaro alla pagina HTML: