Di Edoardo Castelli

Epicode Project 1

Traccia:

Simulare, in ambiente di laboratorio virtuale, un'architettura Client-Server in cui un client con IP 192.168.32.101 richieda tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100.

Si intercetti la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione e il contenuto della richiesta HTTPS.

Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le differenze tra quest'ultimo e la prima intercettazione.

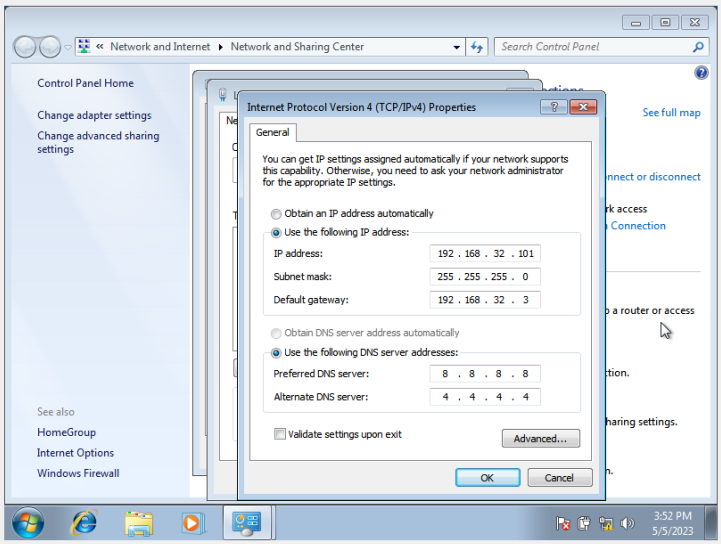
Svolgimento:

Il primo passo per poter eseguire l'esperimento, è configurare le macchine sulla medesima rete tramite configurazione manuale del protocollo Ipv4.

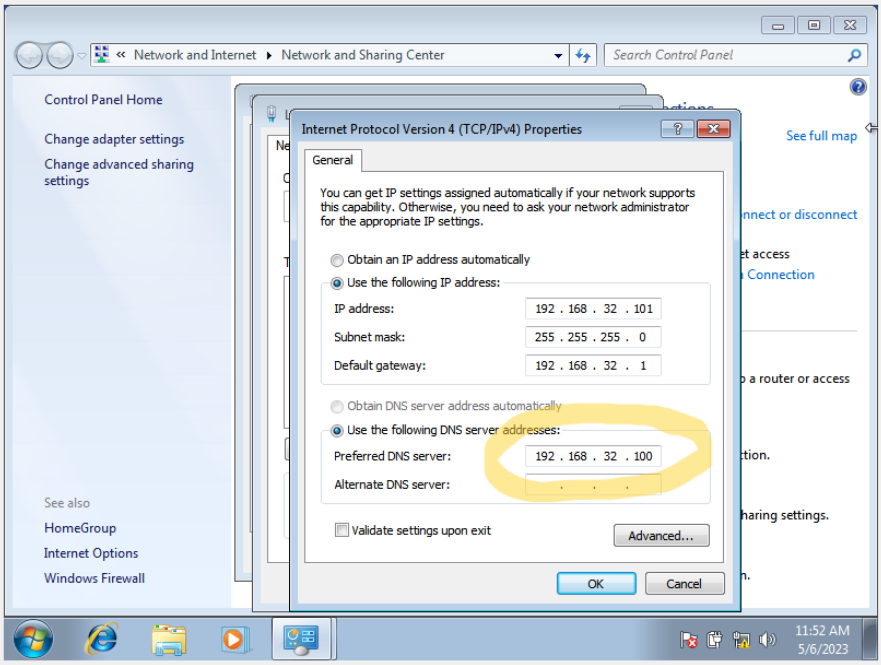
Una volta assicuratomi che entrambe le macchine sono dunque collegate alla rete interna della Virtual Box, procedo alla configurazione.

Windows 7:

Una volta selezionate le "properties" del protocollo Ipv4, sarà possibile inserire manualmente l'indirizzo IP del client. In questo caso inserisco l'IP richiesto: 192.168.32.101.

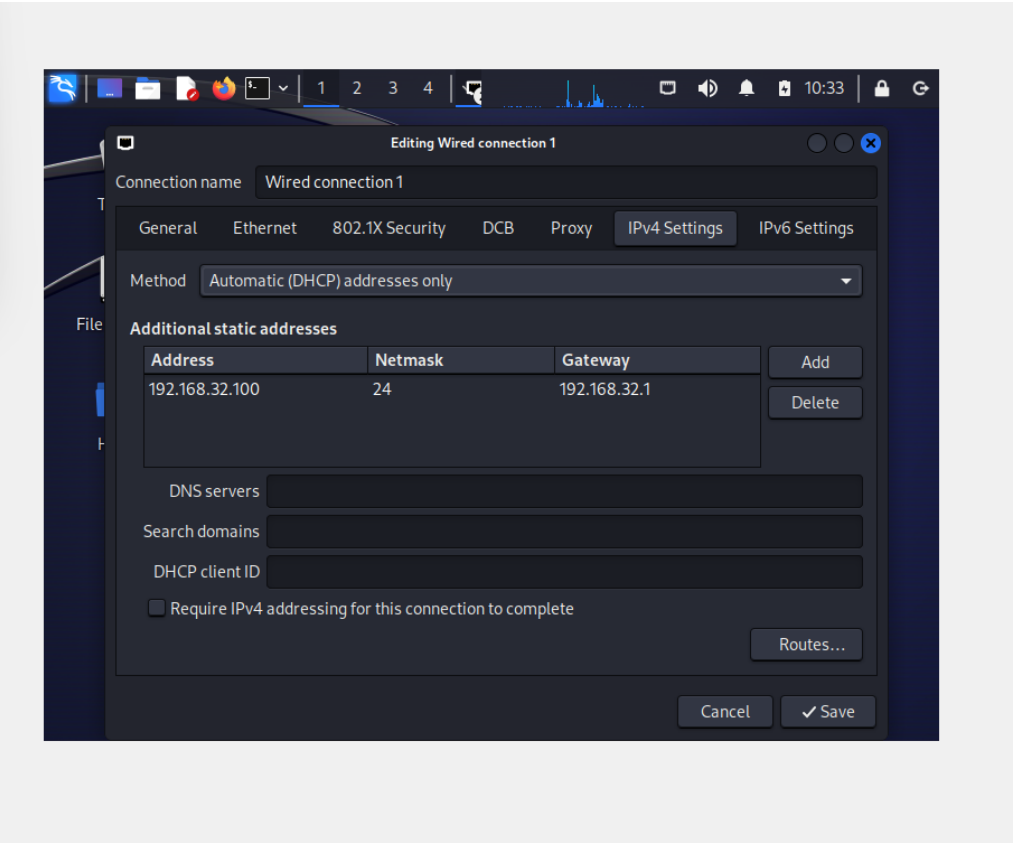


A questo punto, non resta che inserire l'indirizzo del server DNS che il client contatterà, InetSim farà il resto.



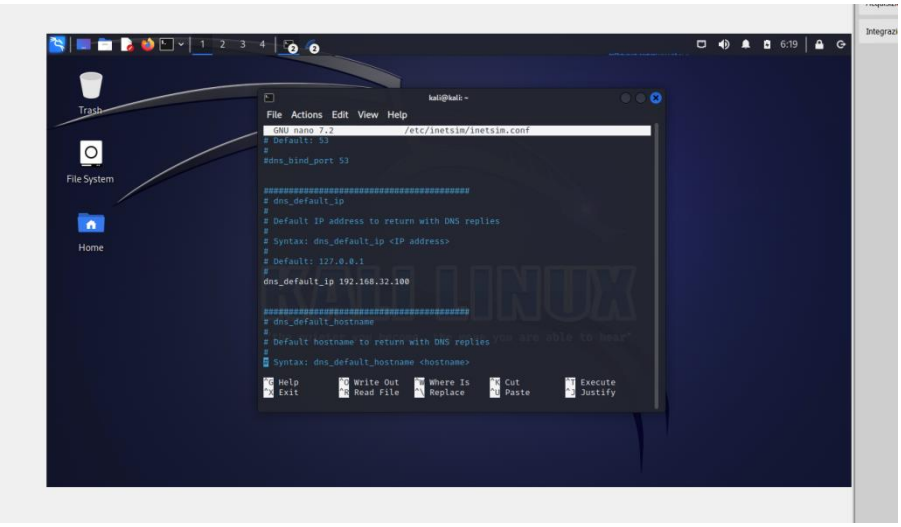
Kali:

Passo ora alla configurazione della seconda macchina, necessaria tanto per l'avvio di InetSim, con il quale editerò il server, quanto per il corretto funzionamento di WireShark. Anche in questo caso, dunque, come prima cosa opero manualmente sull'Ipv4, assegnando l'indirizzo IP richiesto 192.168.32.100, che ospiterà il server.

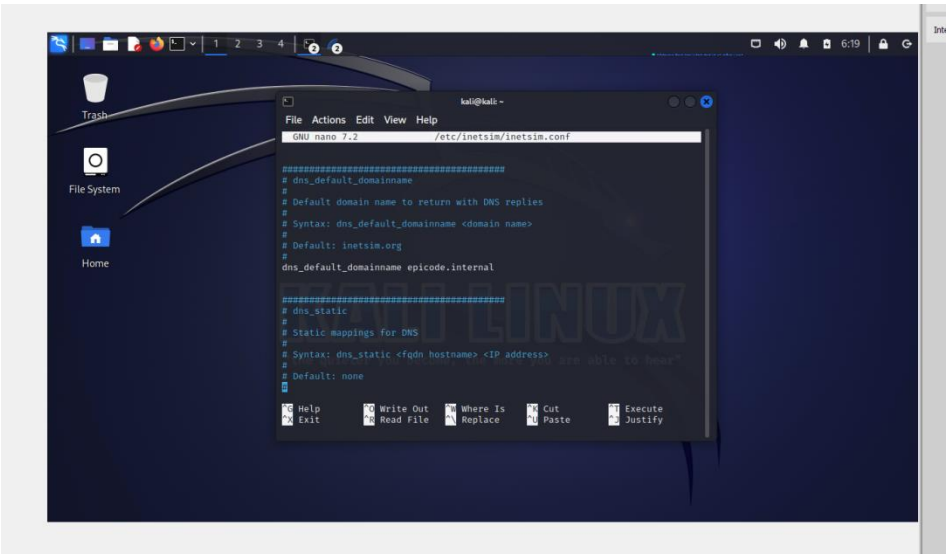


Fatto ciò basterà assegnare nella GUI il metodo manuale e salvare la configurazione per confermare l'IP richiesto.

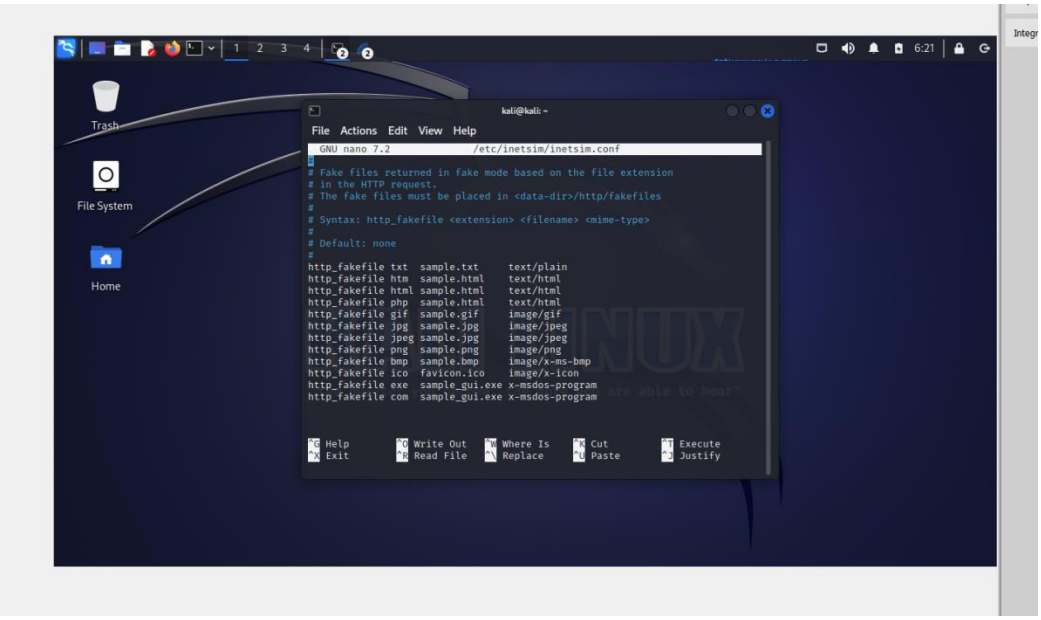
La configurazione di InetSim risulta essere abbastanza intuitiva: una volta richiamato l'apposito file tramite riga di comando (**sudo nano /etc/inetsim/inetsim.conf**), si procede attivando l'elenco dei servizi desiderati e salvando le modifiche.

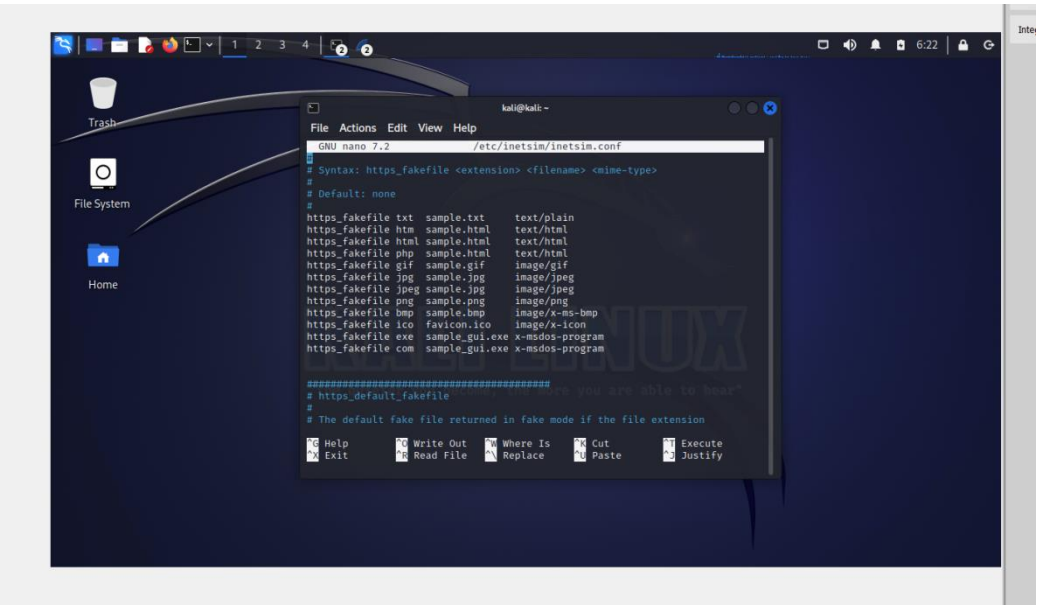


Una volta dato al DNS l'indirizzo IP richiesto, si aggiunge la risoluzione per i nomi di dominio, in questo caso, "epicode.internal", e si prosegue con la configurazione del DNS.



Per quanto riguarda i protocolli HTTP e HTTPS, essi possono essere mantenuti nella configurazione iniziale, o attivati manualmente uno alla volta.

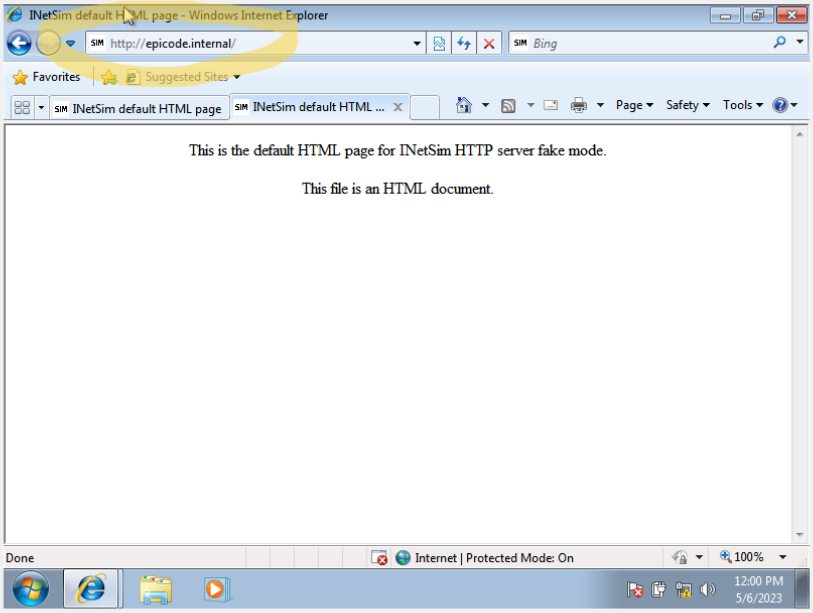




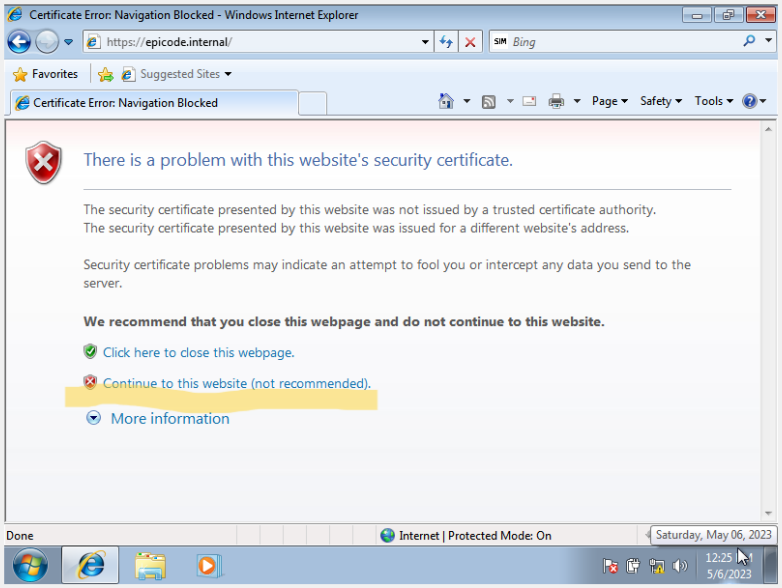
Una volta salvate le modifiche al file, con il prompt di Kali avvio INetSim e ne verifico lo stato. "Simulation is running" verrà visualizzato nel promtp in caso di corretto funzionamento (sudo /usr/bin/ inetsim).

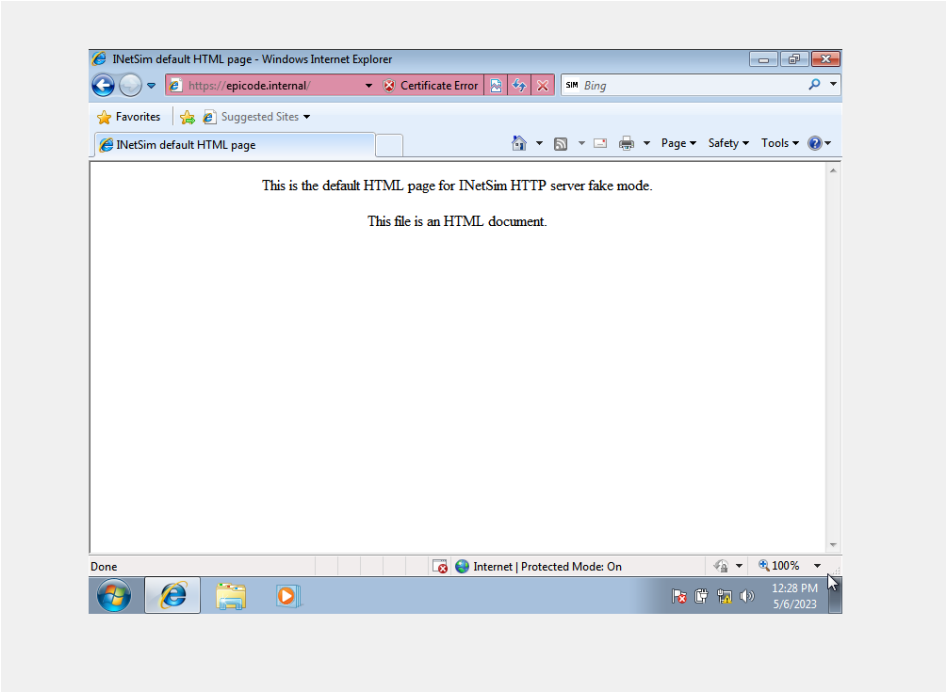
Sarà possibile a questo punto avviare Wireshark, iniziare ad intercettare il traffico e attendere che Windows7 comunichi con il server.

Lasciando INetSim alla sua configurazione base, nel browser di Microsoft apparirà una schermata spartana, ma che conferma l'avvenuto collegamento.

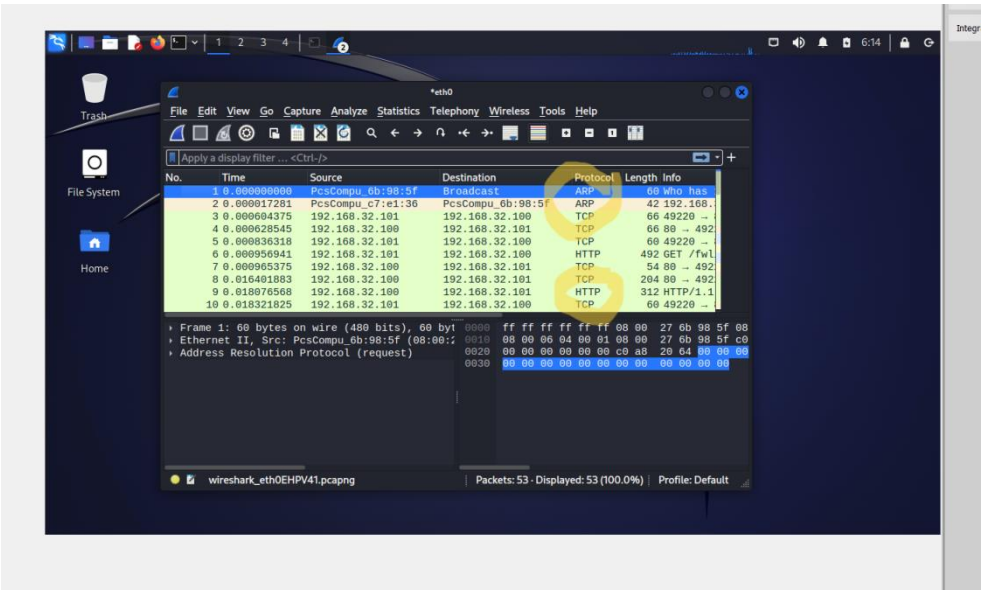


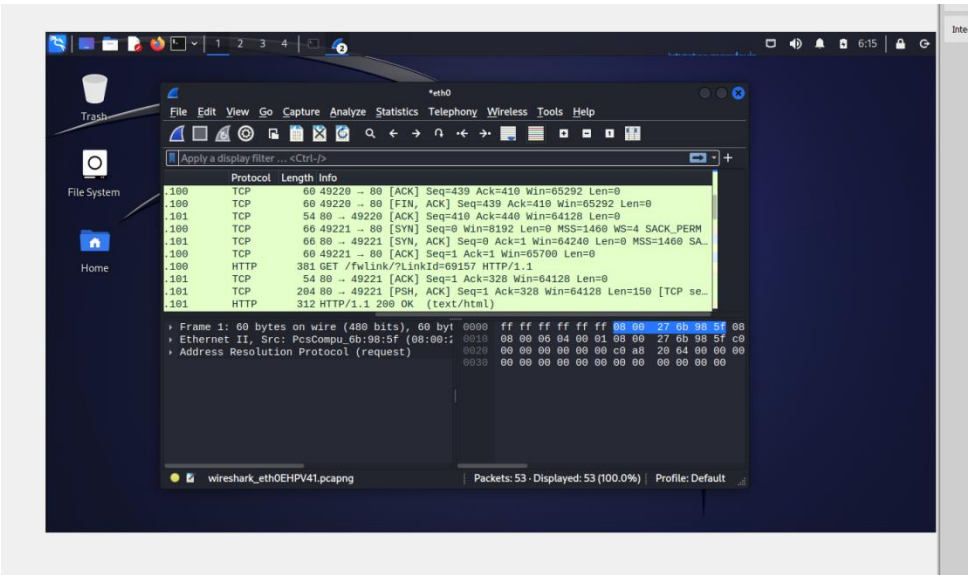
Utilizzando un servizio HTTPS, ho comunque modo di accedere al servizio, previo sblocco manuale del firewall windows se precedentemente configurato, e del "blocco HTTPS", che notifica la "non-sicurezza" del certificato HTTPS stesso.



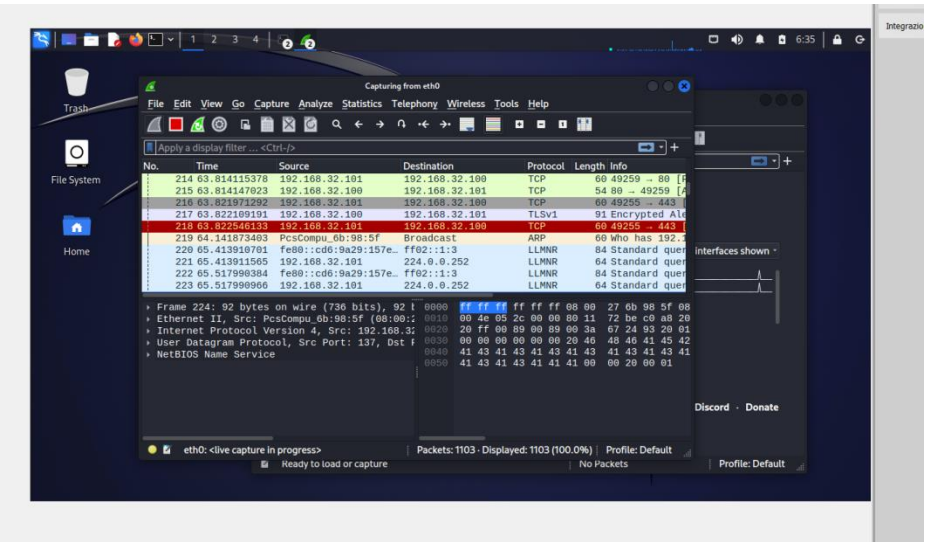


Non resta dunque che fermare "l'ascolto" di Wireshark e soffermarsi sui dettagli di quanto estratto. Si notino principalmente i protocolli ARP che hanno avuto luogo durante il collegamento, con la relativa associazione degli indirizzi MAC che richiedono il colegamnto, ed i protocolli HTTP in "chiaro", facilmente intercettati da Wireshark.





Al contrario, nel caso di richiesta HTTPS, il tool restituisce una serie di "encrypted alert", impedendo di fatto l'ascolto e la lettura di alcuni dati, tramite il protocollo di crittazione TLSv1.



Conclusioni:

Nonostante una piccola serie di rallentamenti iniziali dovuti ad un probabile errore di INetSim, e alla sua consequenziale risoluzione, l'esperimento può dirsi riuscito. Tutte le macchine hanno funzionato correttamente, così come i tool e il resto della strumentazione

necessaria. Una semplice lettura dei dati di Wireshark conferma quanto studiato sulla maggiore sicurezza di HTTPS rispetto ad HTTP.