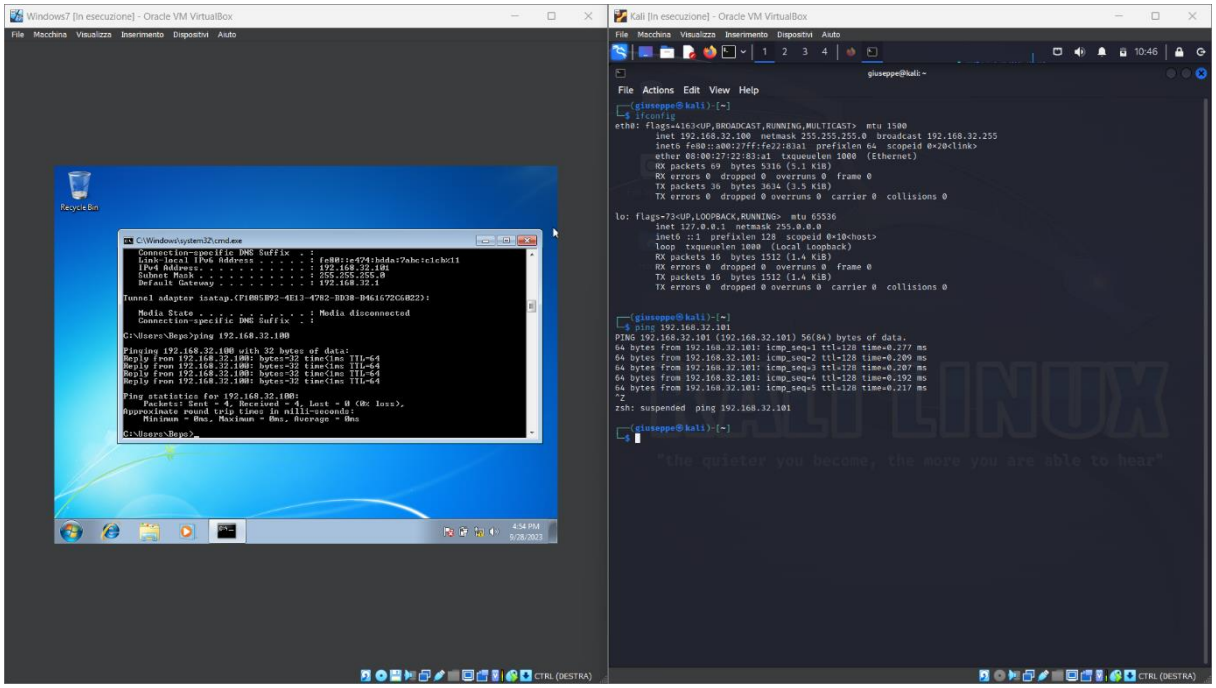
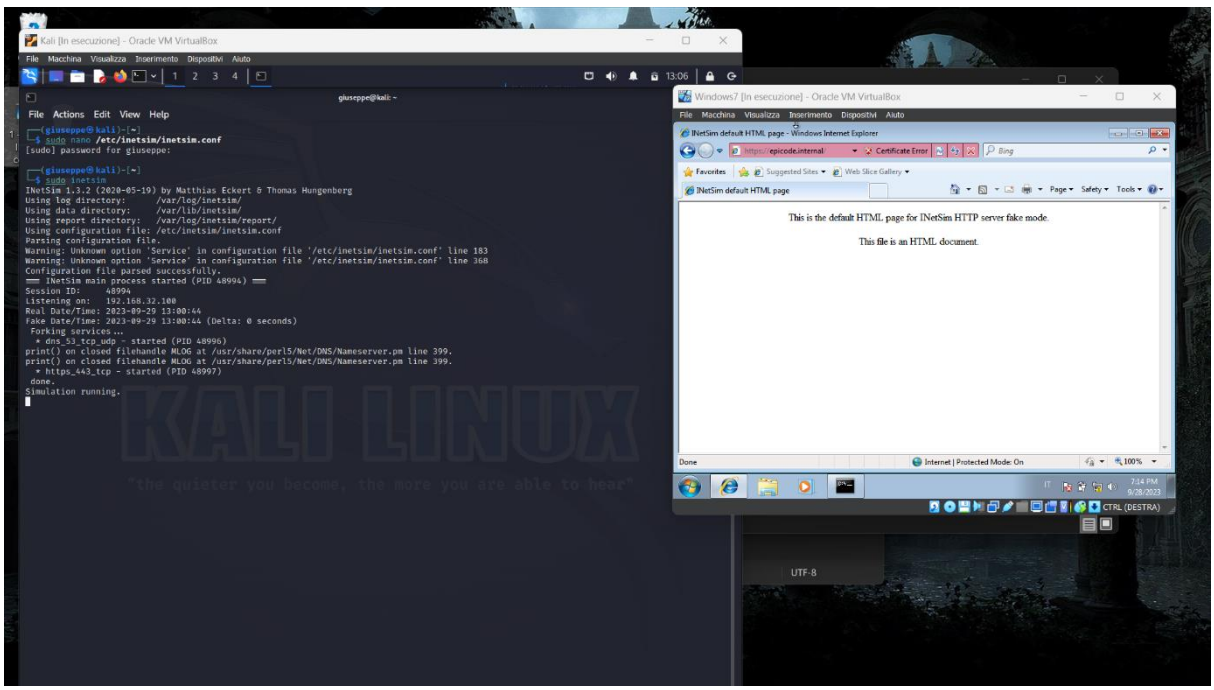
Progetto S1/L5: servizio DNS e intercettazione Wireshark

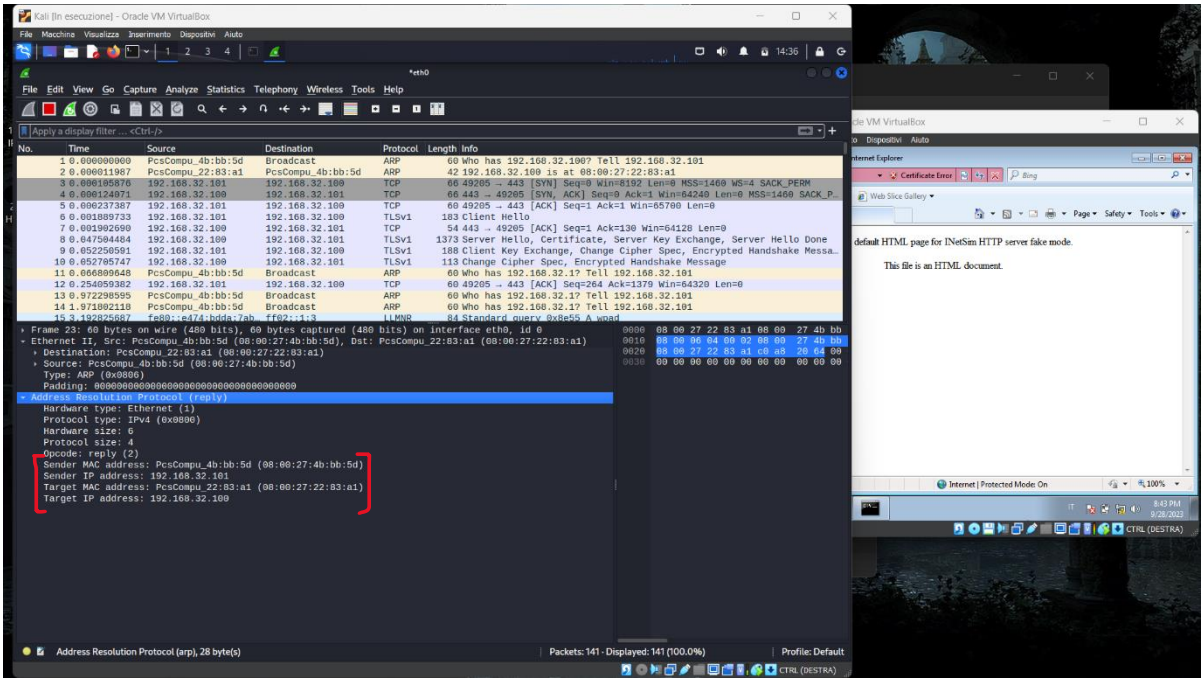
Obiettivo del progetto di oggi era creare un server DNS nella macchina virtuale Kali Linux richiamabile da macchina virtuale Windows 7, previo cambio di indirizzi IP statici in entrambi gli host, verificando infine il traffico dati con Wireshark ed evidenziano in questo gli indirizzi IP e MAC sia source che target.



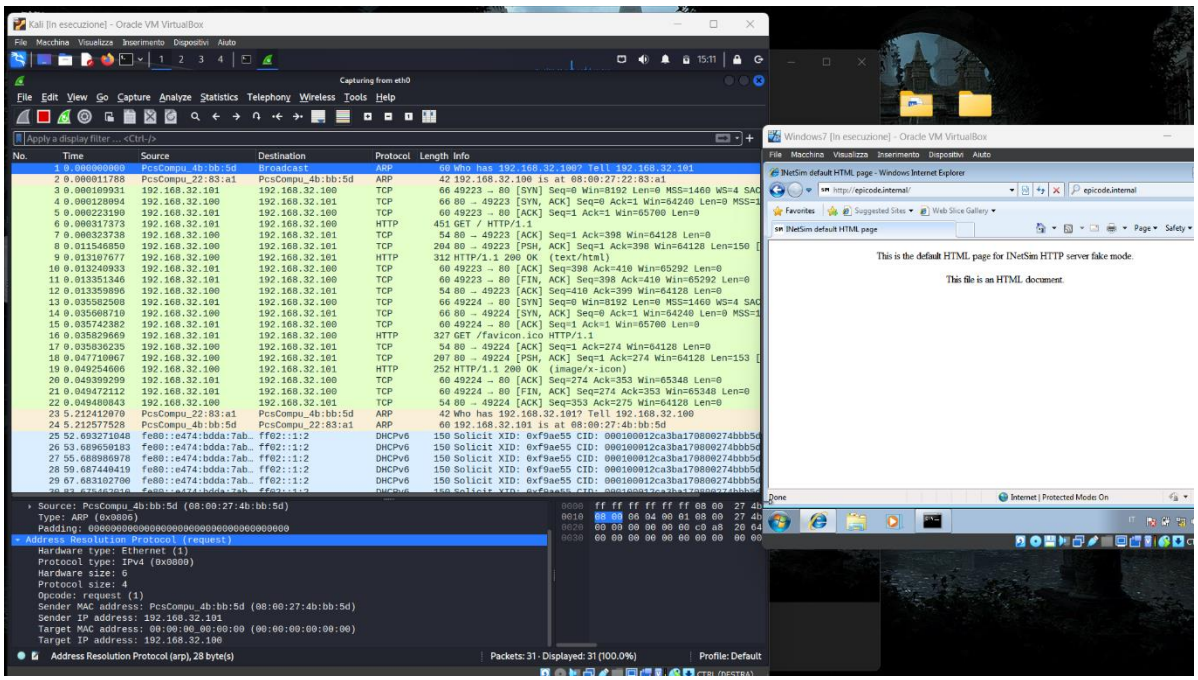
Nella figura 1, sono stati cambiati gli indirizzi IP statici di entrambe le macchine (aggiornando quindi anche gli IP gateway e i relativi permessi sul Firewall di Windows 7) ed è stato effettuato un ping in entrambe le direzioni per verificarne la comunicazione. In questo modo, si ha la certezza che le macchine comunicano e che gli indirizzi sono stati predisposti correttamente.



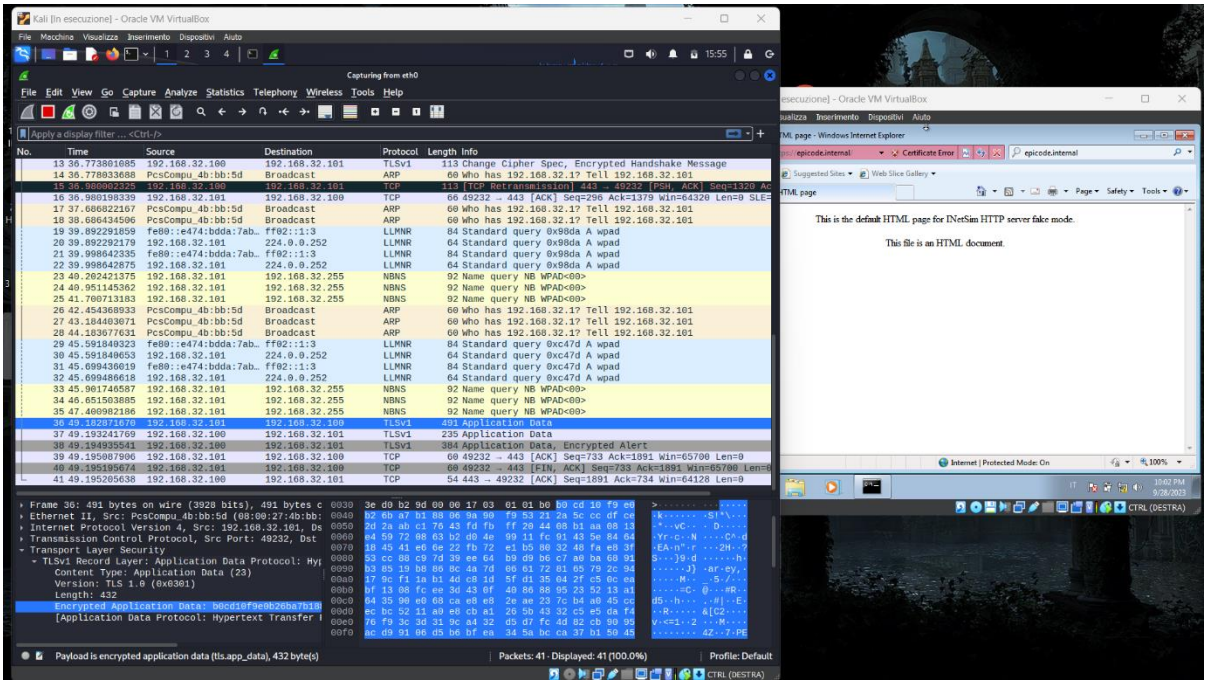
Nella figura 2, è stato impostato il server DNS in Kali utilizzando il comando “sudo nano /etc/inetsim/inetsim.conf”, avviata la simulazione (come si vede in Kali, a sinistra) con protocollo HTTPS e verificatone il corretto funzionamento richiamando la pagina da Windows 7, a destra.



Nella figura 3, è attivo il servizio di intercettazione dei pacchetti di Wireshark. Qui possiamo notare, nella parte evidenziata, sia gli indirizzi IP mittente e destinatario che gli indirizzi MAC mittente e destinatario, recuperati e associati ai rispettivi IP tramite protocollo ARP in seguito a una chiamata in broadcast. In particolare, sender si riferisce alla macchina Windows 7, mentre target alla macchina Kali.



Nella figura 4, è possibile notare la richiesta al server effettuata però tramite protocollo HTTP. In basso a sinistra, sono visibili gli indirizzi IP sia source che target ma solo l'indirizzo MAC source: questo perché è stato analizzato un pacchetto che non aveva ancora ricevuto risposta dal protocollo ARP.



Tra l'attività in Wireshark nella figura 3 e quella nella figura 4 sono visibili delle differenze, date dai due diversi protocolli utilizzati: nella prima infatti, dove è in uso HTTPS, vi sono dei pacchetti che utilizzano il protocollo per la criptografia TLS e vi è uno scambio di chiavi criptografiche.

Un' ulteriore differenza è visibile tra la figura 5 e la figura 6: usando HTTPS, la parte evidenziata risulta essere cifrata e quindi illeggibile, mentre con HTTP (riportata qui di seguito) la stessa parte è in chiaro e quindi leggibile.