## Progetto unit 1

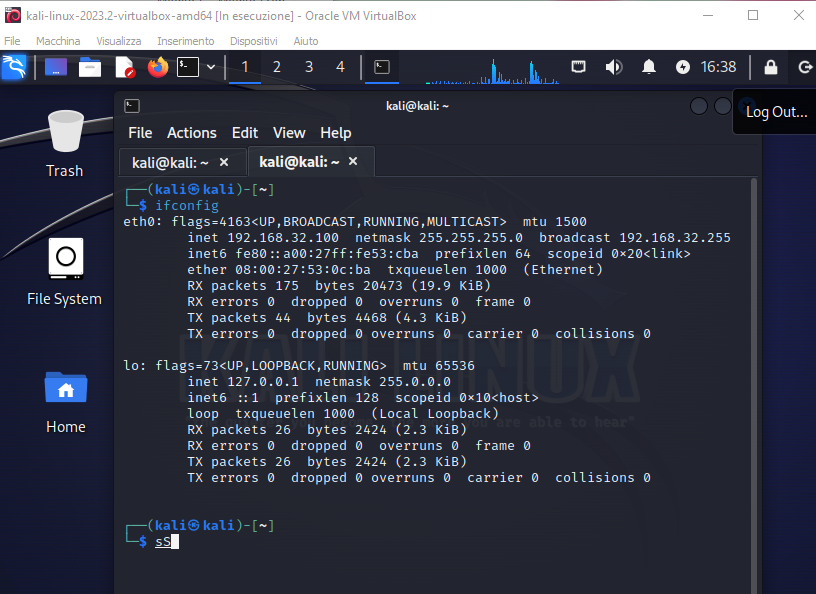
Traccia

Simulare, in un 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 HTTTPS. Spiegare, motivandole, le principali differenze se presenti.

Come prima cosa, ho cambiato gli indirizzi IP delle macchine virtuali



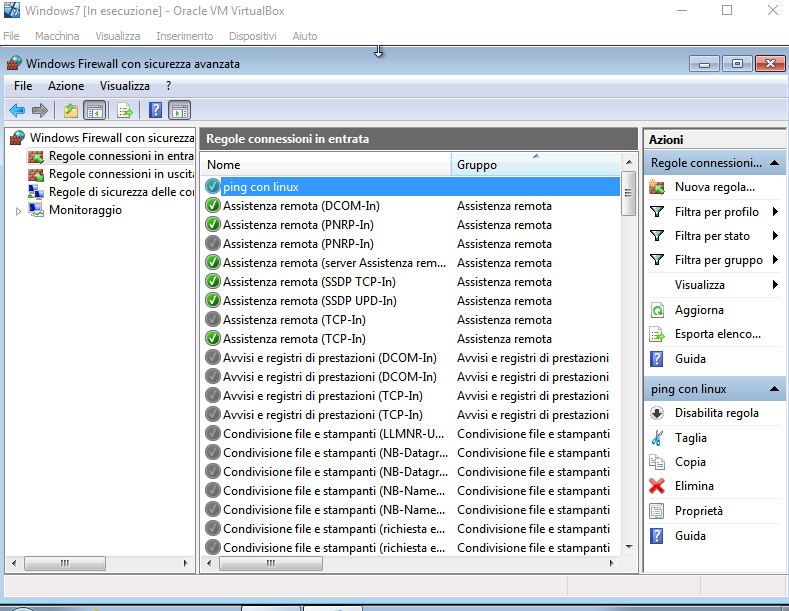
Per Kali ho aperto il terminale e tramite il comando ***sudo nano /etc/network/interfaces*** ho modificato l’indirizzo IP in 192.168.32.100.

Immagine che contiene testo, schermata, software, Icona del computer

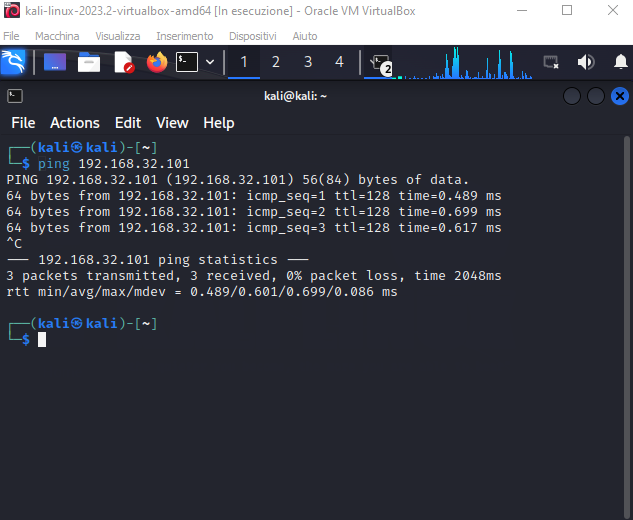
Descrizione generata automaticamente

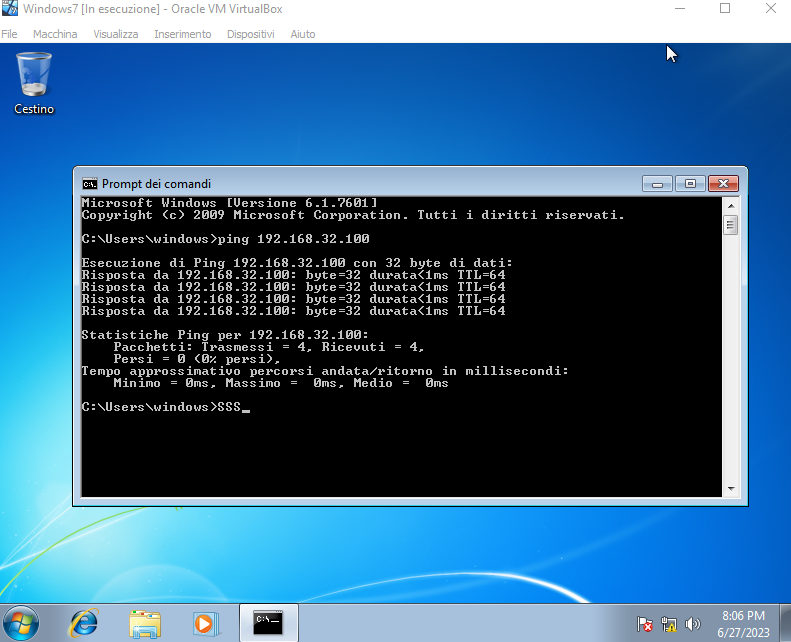
Per Windows 7 ho aperto la finestra proprietà di rete e ho modificato l’indirizzo IP in 192.168.32.101, per quanto riguarda il Gateway predefinito e il Server DNS preferito ho inserito l’indirizzo IP di Kali in quanto è la macchina HOST.

Nella macchina Client cioè Windows 7 il Firewall bloccava la connessione con la macchina sorgente Kali. Così l’ho modificato permettendo la connessione tra le due.



Per vedere se tutto funziona correttamente ho fatto pingare le due macchine.





Nel terminale di Kali ho impostato l’utility **Inetsim.**Tramite il comando ***sudo nano /etc/inetsim/inetsim.conf***  ho attivato i servizi dns, http e https Immagine che contiene testo, Carattere, schermata, tipografia

Descrizione generata automaticamente

Configurato l’IP address di default gate cioè quello di Kali

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

E l’IP del DNS sempre Kali

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Per trascrivere un sito in un indirizzo IP, ho dato al nome epicode. internal l’indirizzo IP di Kali

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Ho salvato e chiuso

Per completare il tutto ho avviato **Inetsim** tramite la dicitura ***sudo inetsim***

Cosi facendo aprendo il browser su Window 7 e cercando epicode.internal oppure l’IP 192.168.32.100 mi apre la pagina web d’interesse.

Immagine che contiene testo, schermata, software, Icona del computer

Descrizione generata automaticamente

Su Kali ho aperto l’applicazione Wireshark che mi permette di analizzare il traffico dei pacchetti tra le due macchine.

Immagine che contiene testo, elettronica, schermata, software

Descrizione generata automaticamente

Immagine che contiene testo, elettronica, schermata, software

Descrizione generata automaticamente

Nella prima immagine analizzo il traffico dati in https nella seconda invece in http  
In entrambi i casi si può notare l’indirizzo MAC Destination (Kali) e Source (Window 7) rimangono invariati  
In https che è un protocollo criptato non mi vengono date informazioni sul pacchetto mentre nel protocollo  
http mi vengono specificate le cartelle e anche la richiesta fatta sul browser.