Armando Battaglino
28/10/2022

Week 1 - Esercizio 4

Configurazione Firewall Windows 7

Consegna

Nell'esercizio di oggi metteremo insieme le competenze acquisite finora. Lo studente verrà valutato sulla base della risoluzione al problema seguente.

Requisiti e servizi:

- Kali Linux IP 192.168.32.100
- Windows 7 IP 192.168.32.101
- HTTPS server: attivo
- Servizio DNS per risoluzione nomi di dominio: attivo

Traccia:

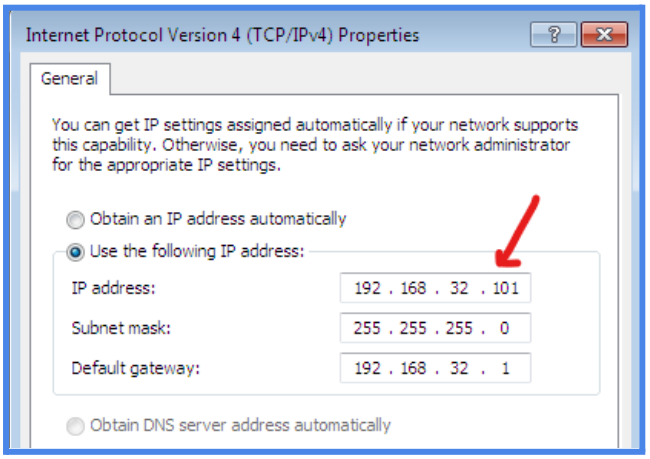
Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100.

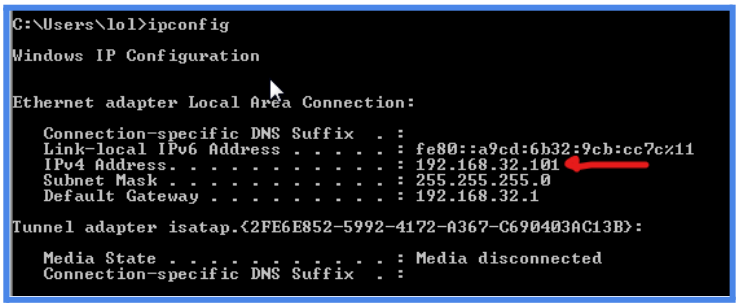
Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze.

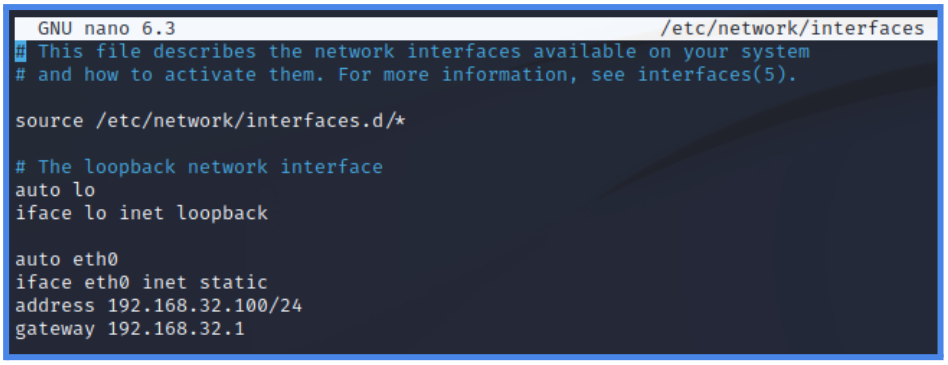
Procedimento

1. Vado innanzitutto a cambiare l'indirizzo della macchina Windows 7

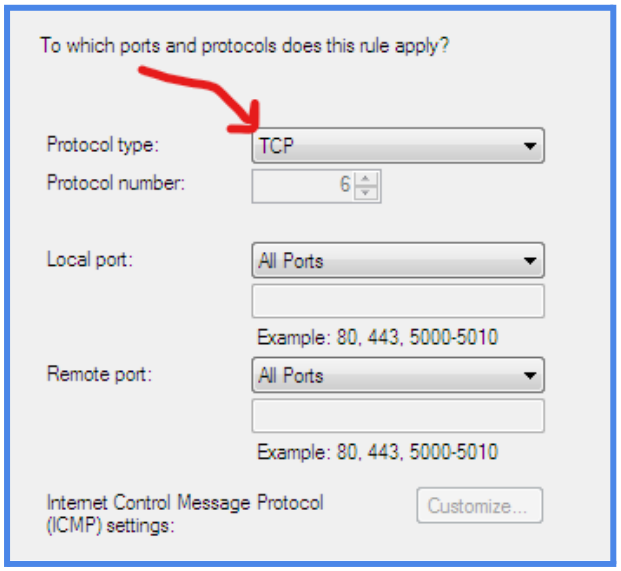


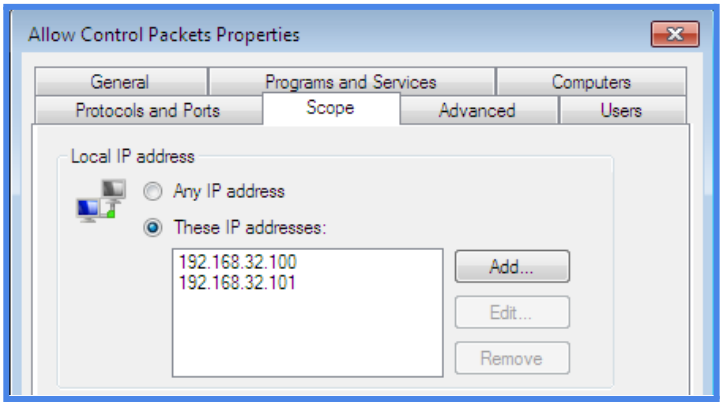


2. Cambio anche quella di Kali

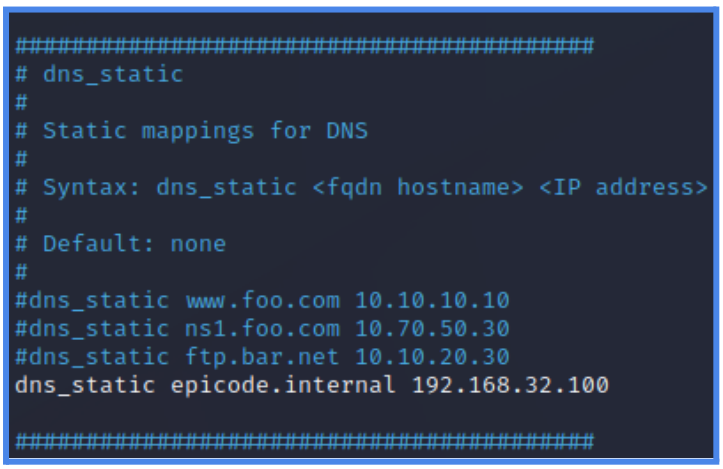


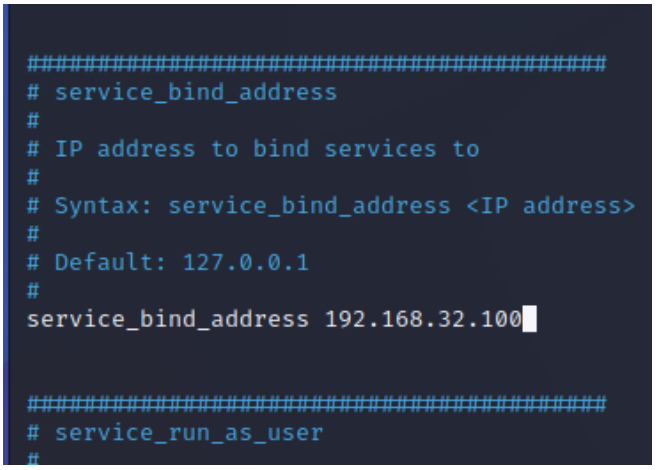
3. Modifico poi le policy del firewall per fare in modo che le due macchine possano comunicare (Protocollo TCP sia in entrata che in uscita)



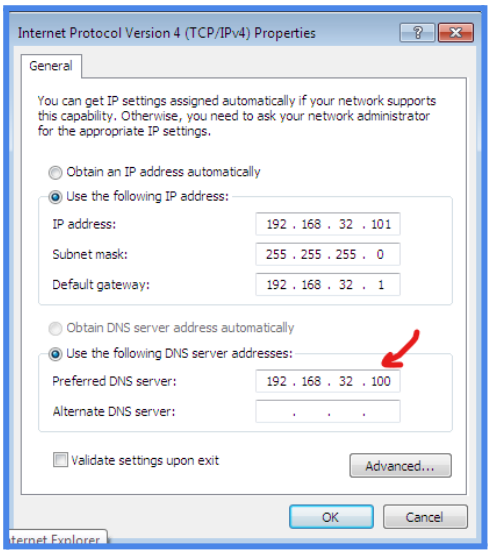


4. Vado poi a configurare il DNS Service nel file **inetsim.conf** e lo cambio con **dns_static epicode.internal 192.168.32.100** come richiesto nella consegna. Stessa cosa con **service_bind_address**

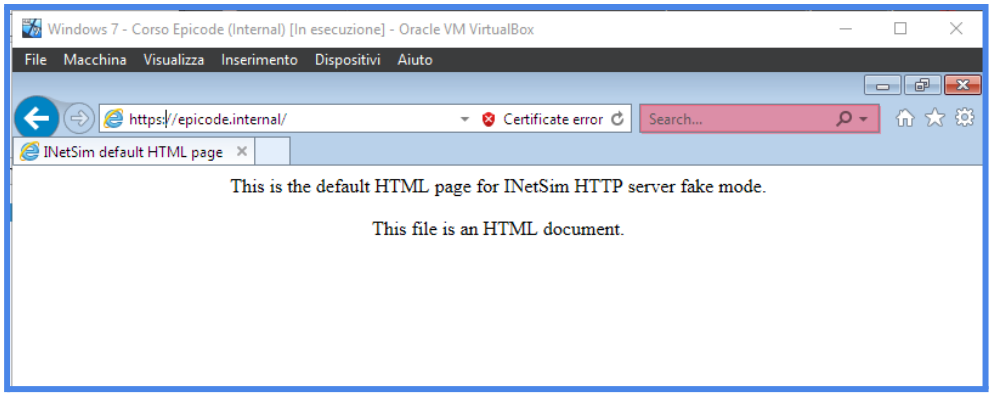




5. Avvio la simulazione attraverso il comando **inetsim** con la nuova configurazione
6. Successivamente vado a cambiare il server DNS a cui si deve collegare la macchina con Windows 7

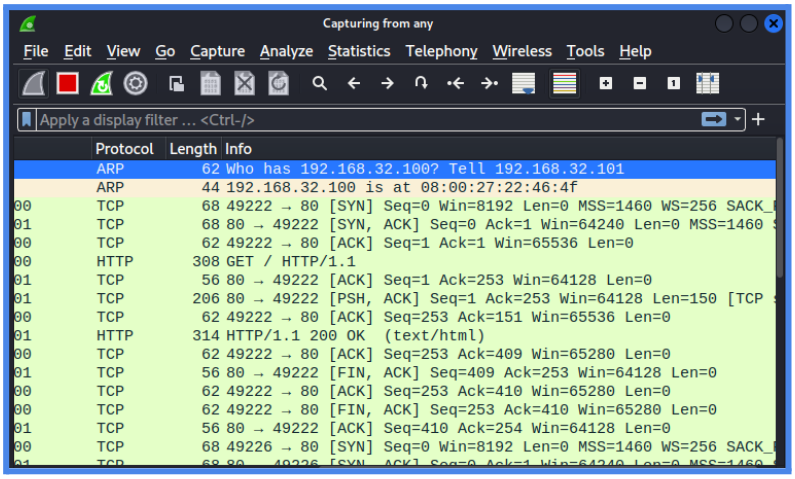


7. A questo punto ricerco dalla macchina Windows **epicode.internal** per verificare che la richiesta https può essere effettuata senza problemi

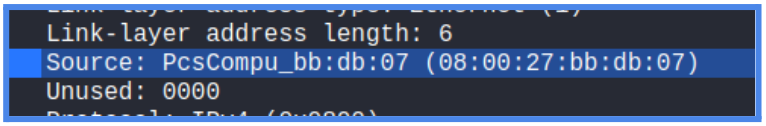


8. Apro Wireshark e vado a controllare i pacchetti scambiati tra le due macchine e Ricarico la pagina per analizzarli

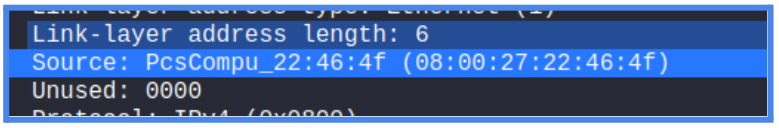
HTTP →



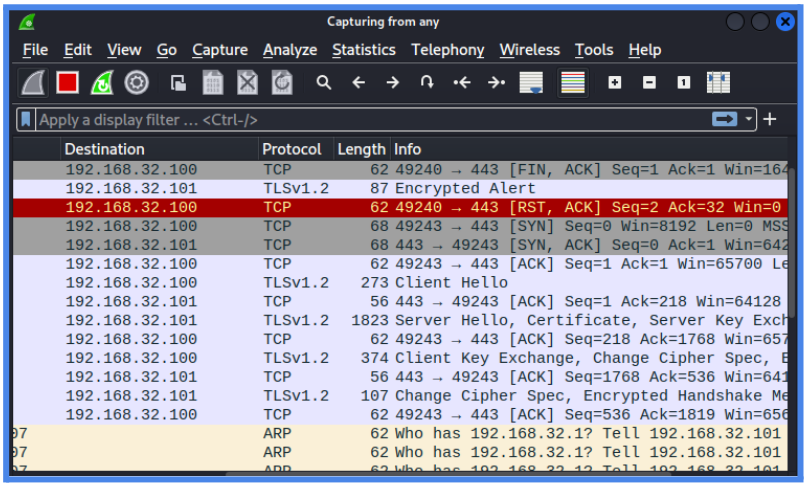
WINDOWS



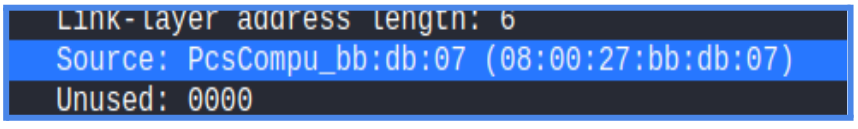
KALI



HTTPS →



WINDOWS



KALI