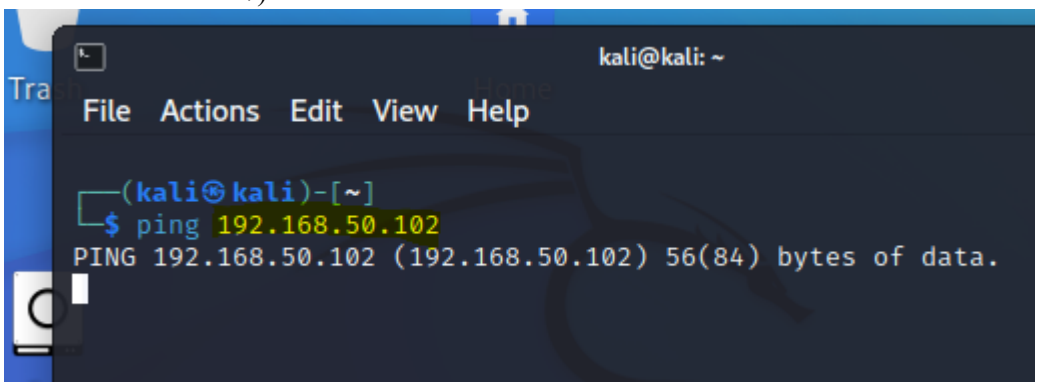
Gabriele Di giampietro **Data 27/10/2022**

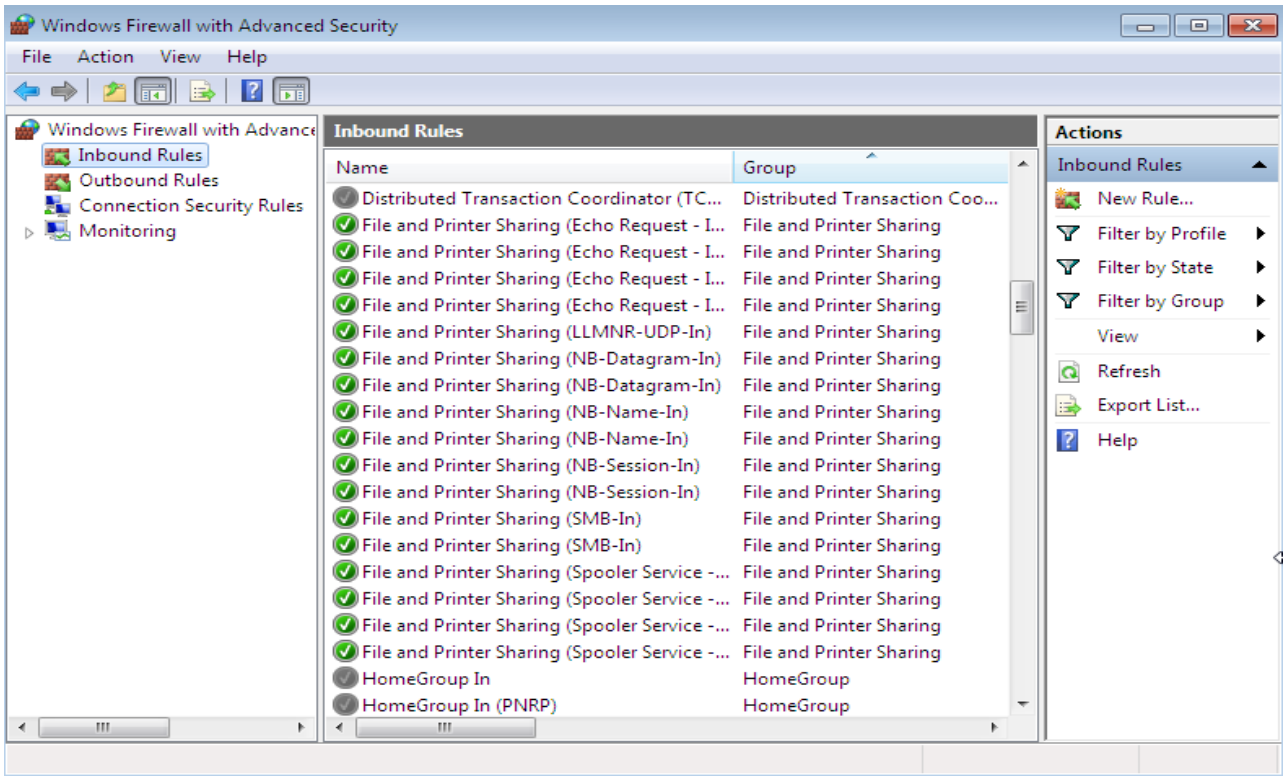
Report esercitazione configurazione Policy su Firewall Windows, Packet capture e simulazione di rete con Wireshark e InetSim su Kali

FASE 1

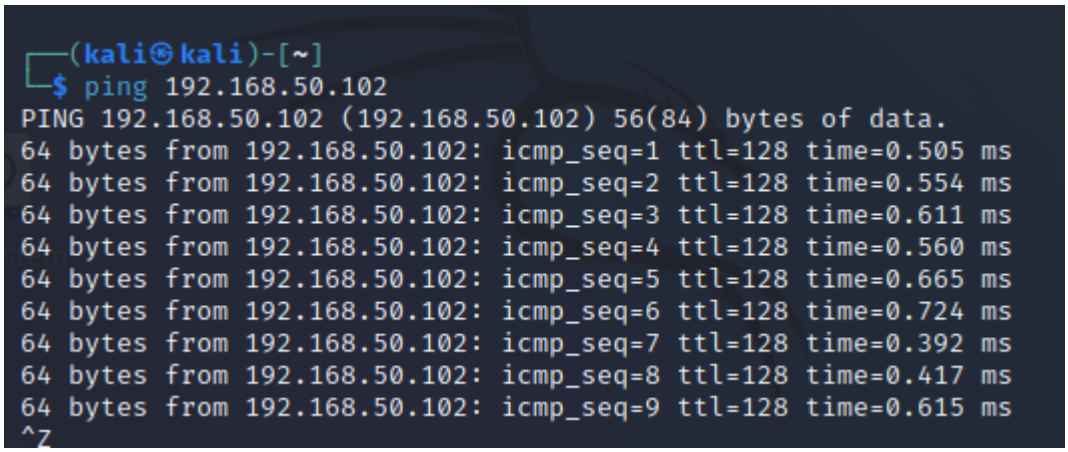
Nella prima fase della nostra esercitazione ho verificato che effettivamente tra le nostre macchine virtuali non c'è comunicazione: attraverso la VM Kali chiamando il comando ping verso l'ip della VM Windows 7 non abbiamo risposta, come possiamo vedere nell'immagine seguente. (Evidenziato in giallo abbiamo l'ip della VM Windows 7)



Per permettere la comunicazione, sono andato a configurare la Policy di Windows 7, attraverso il Control Panel e poi in System and security entriamo nella finestra del Windows Firewall, che ovviamente è attivo, clicchiamo poi nella sezione advanced setting e selezioniamo la riga Inbound rules dove troviamo una lista di cosa il Firewall permette di far entrare nella macchina. Andiamo quindi ad attivare tutte le righe con la dicitura File and printer sharing ponendole con la spunta verde, dando così la possibilità di fare passare i nostri dati in entrata da Kali.

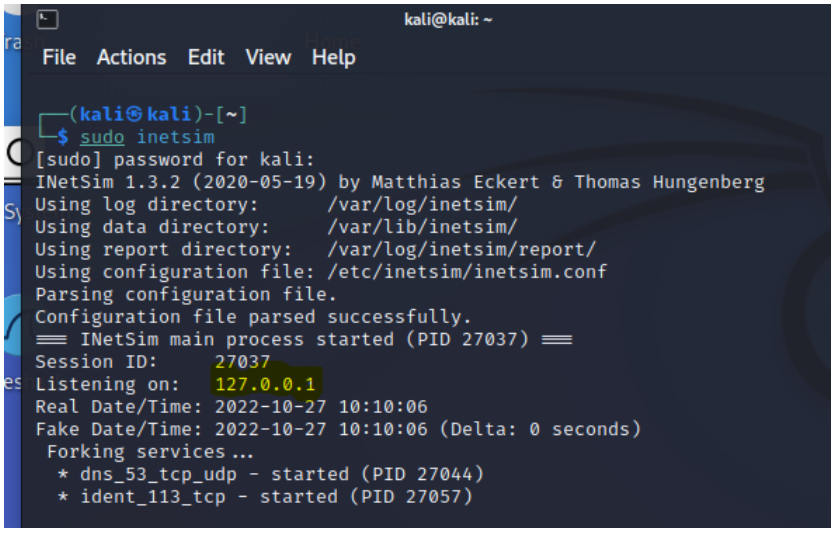


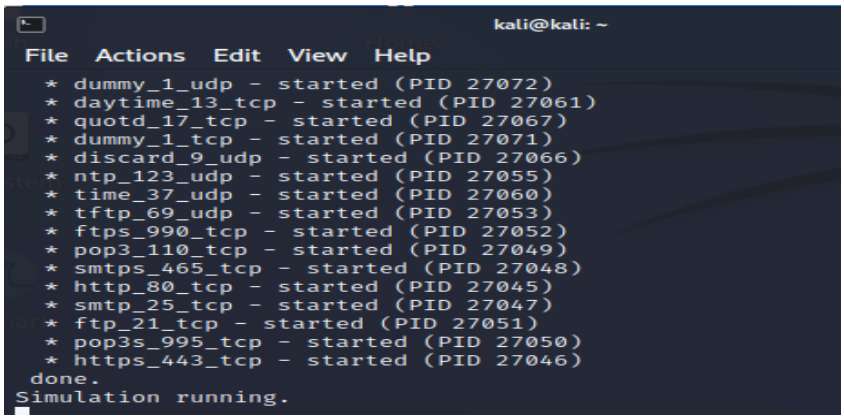
Andiamo infine a controllare sulla Vm Kali che ci sia effettivamente comunicazione, che possiamo confermare dalla risposta del ping che vediamo nell'immagine seguente.



FASE 2

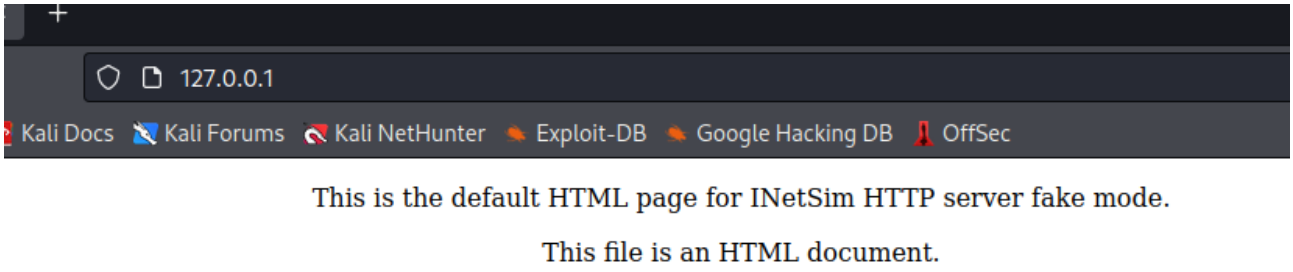
In questa fase andiamo sulla VM Kali e facciamo partire il tool InetSim, che simulerà la creazione di un server con dei servizi internet. Aprendo l'interfaccia dei comandi utilizziamo il comando sudoinetsim e come possiamo vedere nella figura seguente l'applicazione fa partire una simulazione di rete e il suo relativo indirzzo ip 127.0.0.1 che vediamo evidenziato in giallo.





FASE 3

Nell'ultima fase, sempre sulla VM Kali andiamo ad utilizzare l'applicazione Wireshark che funge da cattura pacchetti dati. Dopo aver avviato la nostra simulazione di rete con Inetsim, apriamo il browser su Kali e andiamo a inserire nella barra di indirizzo il nostro ip 127.0.0.1 della simulazione di rete raggiungendo una simulazione di sito internet, indicato infatti come vediamo nella schermata HTTP server fake mode.



Nel mentre utilizzando Wireshark, selezioniamo la stringa loopback:lo (ci troviamo in una rete interna e chiusa) e vediamo il passaggio di tutti i vari pacchetti dati che sta catturando l'applicazione, nel nostro caso in una simulazione di rete internet.