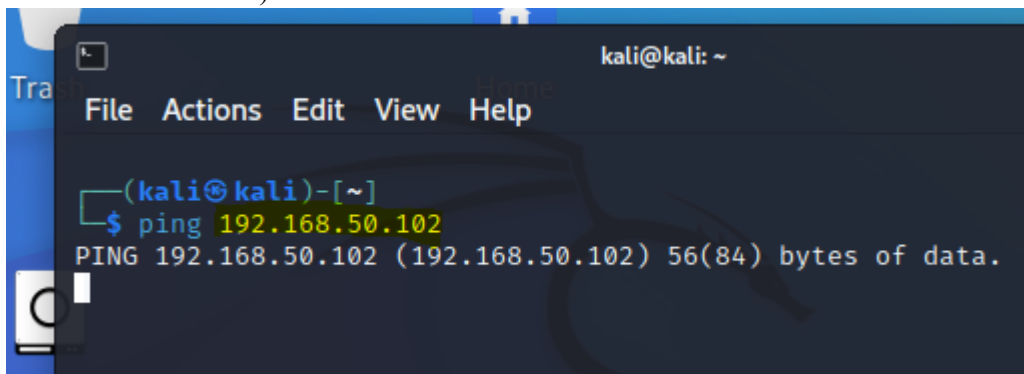
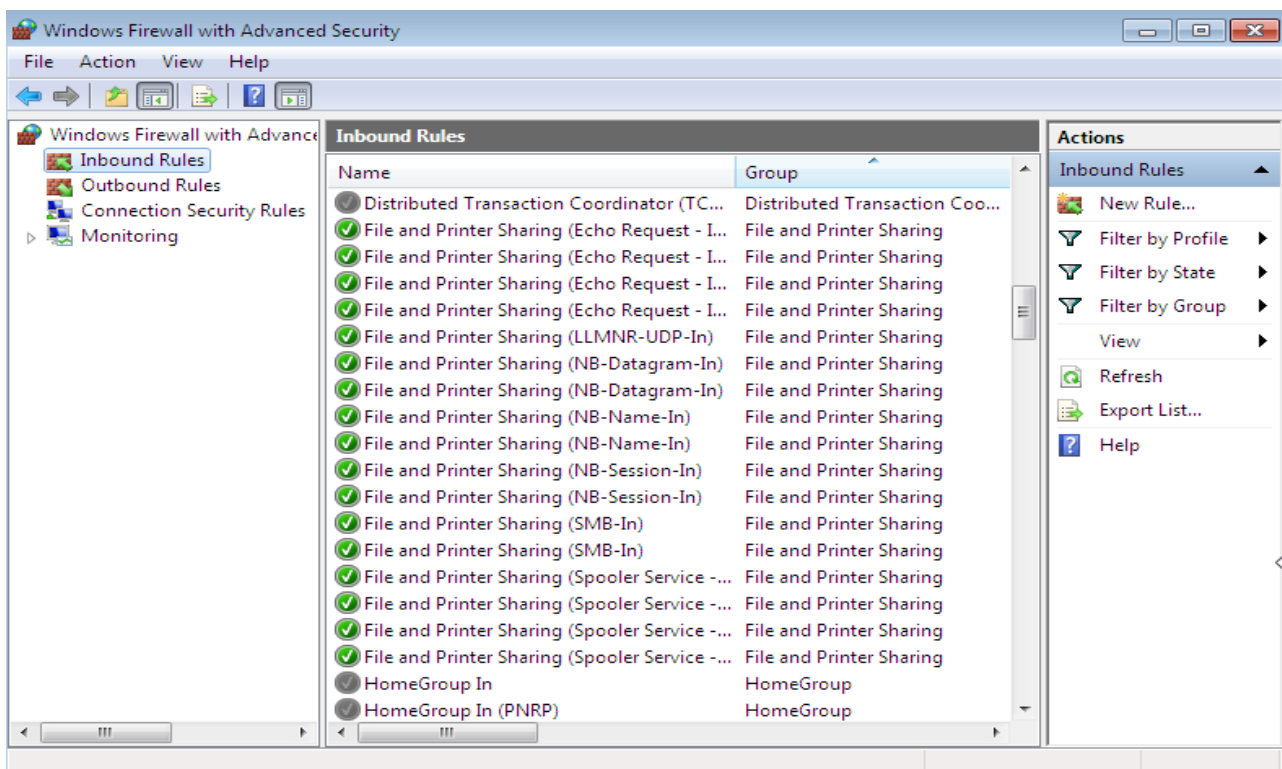


Report esercitazione configurazione Policy su Firewall Windows, Packet capture e simulazione di rete con Wireshark e InetSim su Kali**FASE 1**

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.

```
(kali@kali)-[~]
$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.505 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.554 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.611 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.560 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.665 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.724 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.392 ms
64 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=0.417 ms
64 bytes from 192.168.50.102: icmp_seq=9 ttl=128 time=0.615 ms
^Z
```

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 `sudo inetsim` e come possiamo vedere nella figura seguente l'applicazione fa partire una simulazione di rete e il suo relativo indirizzo ip `127.0.0.1` che vediamo evidenziato in giallo.

```
kali@kali: ~
File Actions Edit View Help

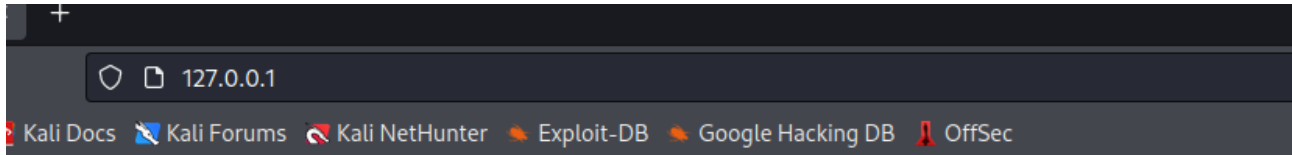
(kali@kali)-[~]
$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== INetSim main process started (PID 27037) ==
Session ID: 27037
Listening on: 127.0.0.1
Real Date/Time: 2022-10-27 10:10:06
Fake Date/Time: 2022-10-27 10:10:06 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 27044)
* ident_113_tcp - started (PID 27057)
```

```
kali@kali: ~
File Actions Edit View Help

* dummy_1_udp - started (PID 27072)
* daytime_13_tcp - started (PID 27061)
* quoted_17_tcp - started (PID 27067)
* dummy_1_tcp - started (PID 27071)
* discard_9_udp - started (PID 27066)
* ntp_123_udp - started (PID 27055)
* time_37_udp - started (PID 27060)
* tftp_69_udp - started (PID 27053)
* ftps_990_tcp - started (PID 27052)
* pop3_110_tcp - started (PID 27049)
* smtps_465_tcp - started (PID 27048)
* http_80_tcp - started (PID 27045)
* smtp_25_tcp - started (PID 27047)
* ftp_21_tcp - started (PID 27051)
* pop3s_995_tcp - started (PID 27050)
* https_443_tcp - started (PID 27046)
done.
Simulation running.
```

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.



This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

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.

