

L'esercizio di oggi mira a consolidare le conoscenze acquisite. Vedremo due esercizi:

I) la configurazione di una policy sul firewall windows;

II) una packet capture con Wireshark.

Vedremo anche come simulare alcuni servizi di rete con un tool pre-installato su Kali Linux (InetSim)

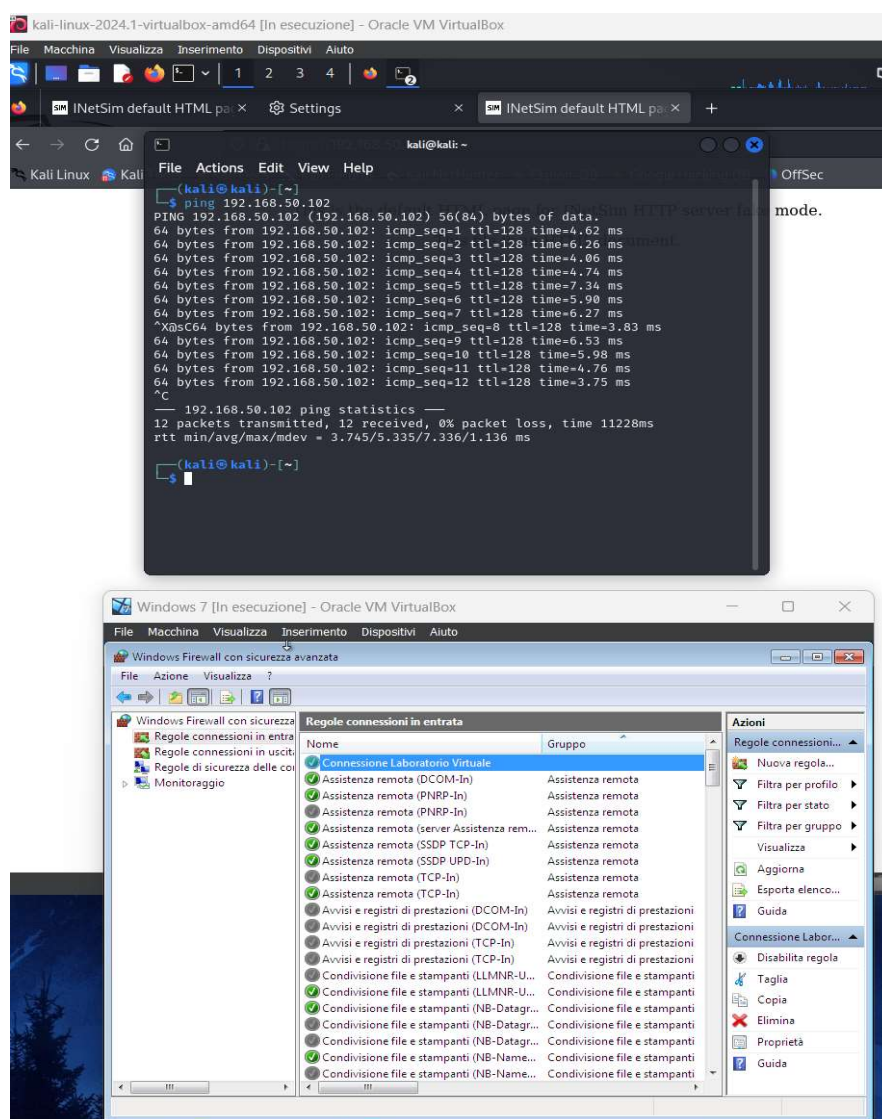
Esercizio:

➤ Configurare policy per permettere il ping da macchina Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall)

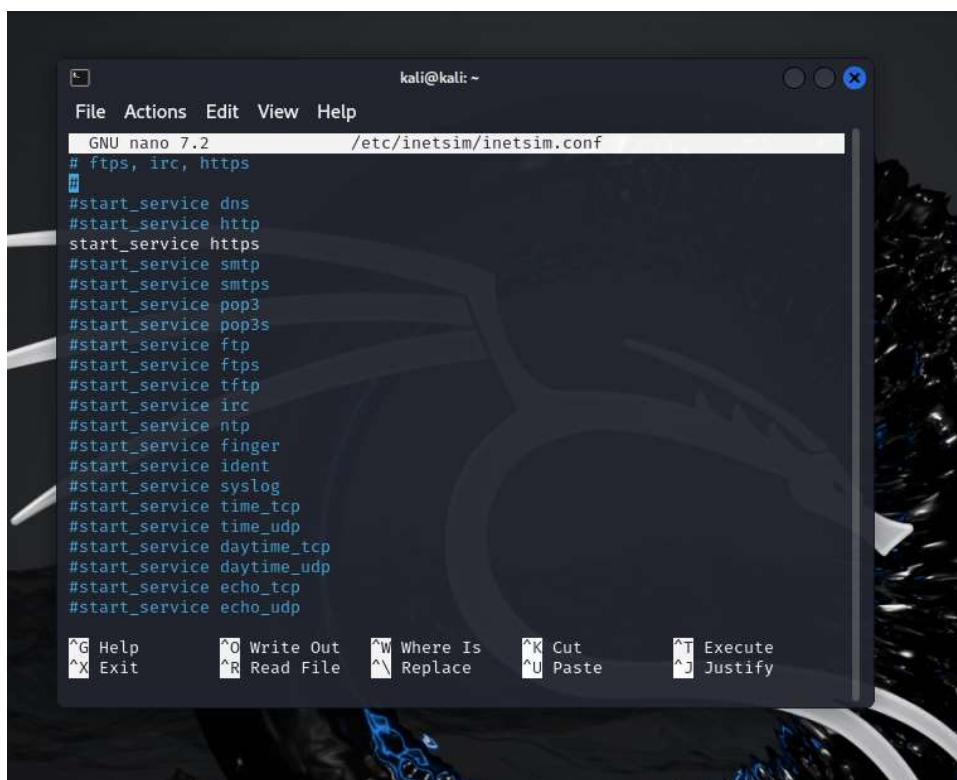
➤ Utilizzo dell'utility InetSim per l'emulazione di servizi Internet

➤ Cattura di pacchetti con Wireshark

Per prima cosa apriamo windows firewall e andiamo a inserire una nuova regola di connessione in entrata, una volta fatto possiamo aprire kali linux e fare un ping a windows 7



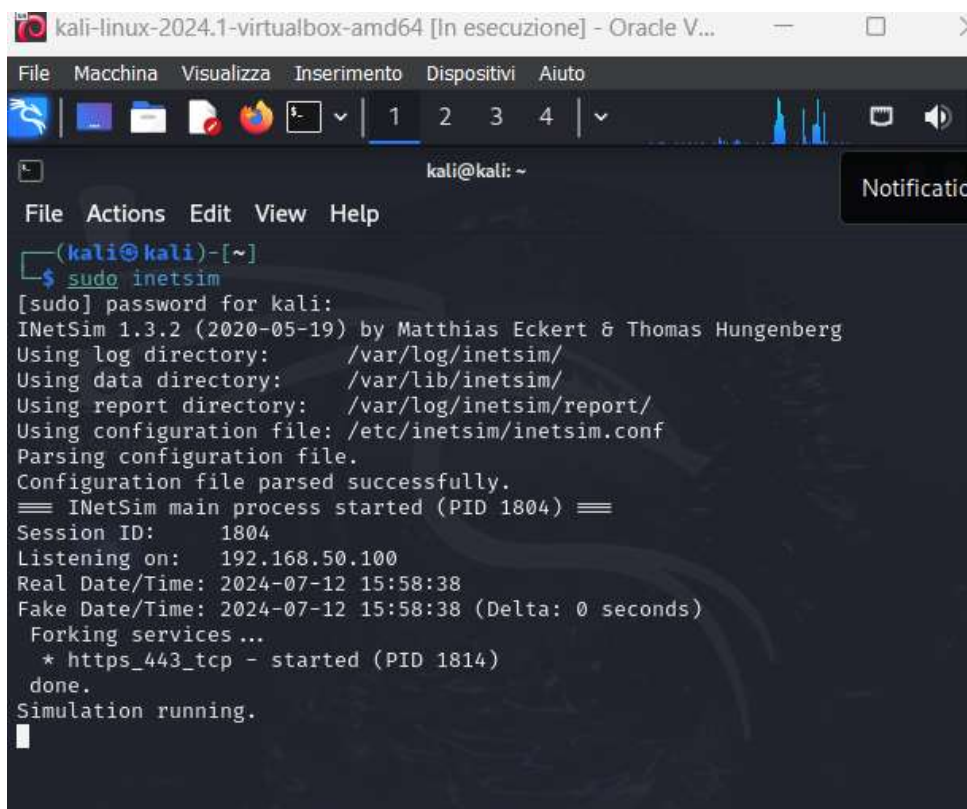
Adesso sempre con linux usiamo il comando *sudo nano /etc/inetsim/inetsim.conf* e mettiamo il cancelletto davanti a tutti i servizi che appaiono qui sotto **tranne** a https



```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsim.conf
# ftps, irc, https
#
#start_service dns
#start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp
#start_service echo_tcp
#start_service echo_udp

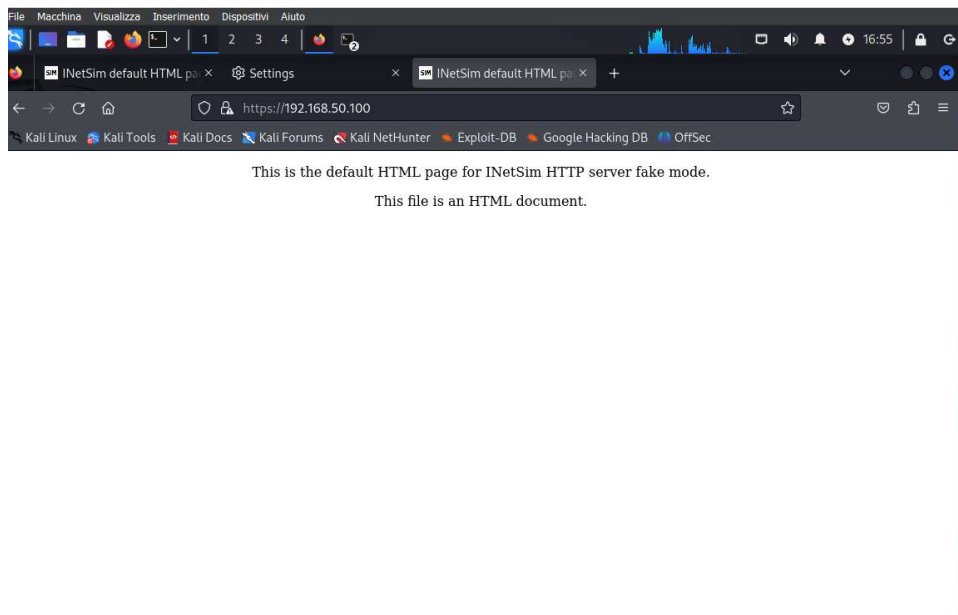
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Dopo aver salvato la configurazione andremo a scrivere *sudo inetsim* per avviare la simulazione



```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle V...
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
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 1804) ==
Session ID: 1804
Listening on: 192.168.50.100
Real Date/Time: 2024-07-12 15:58:38
Fake Date/Time: 2024-07-12 15:58:38 (Delta: 0 seconds)
Forking services...
* https_443_tcp - started (PID 1814)
done.
Simulation running.
```

Adesso possiamo aprire safari e scrivere il nostro IP nella barra di ricerca
<https://192.168.50.100>



Fatto ciò possiamo passare all'ultima parte dell'esercizio cioè quella di cattura dei pacchetti con WireShark

