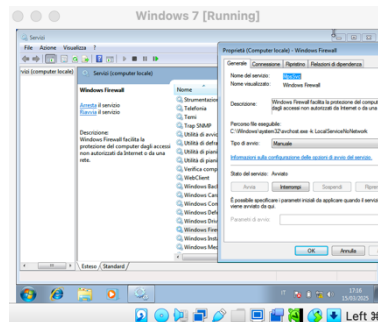


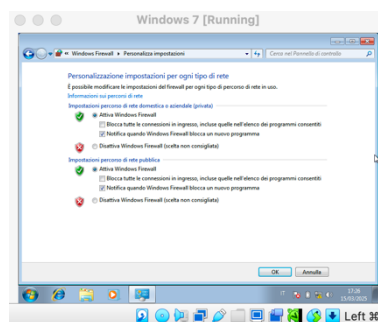
## POLICY & PACKET CAPTURE W3D4

1. Configuro una policy sul Firewall Windows, per permettere il ping dalla VM Kali Linux alla VM Windows:

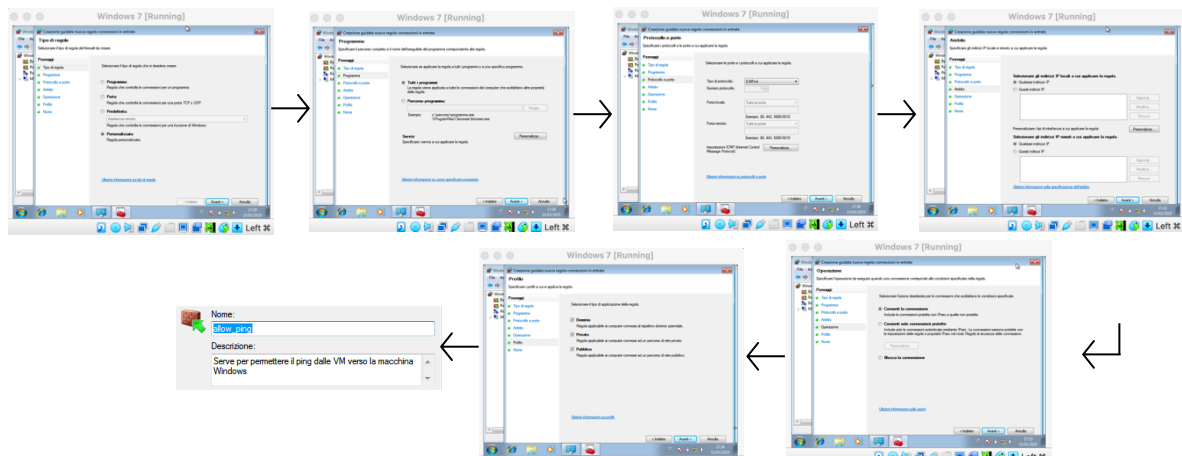
Accendo la macchina virtuale Windows → cerco Servizi → cerco Windows Firewall → lo imposto Manuale → Applica → Avvia



Vado su Pannello di controllo → Tutti gli elementi del Pannello di controllo → Windows Firewall → modifica impostazioni di notifica



Torno su Windows Firewall → impostazioni avanzate → regole connessioni in entrata → nuova regola → Personalizzata → Avanti → tutti i programmi → Avanti → tipo di protocollo: ICMPv4 → Avanti → qualsiasi indirizzo IP (ad entrambe le selezioni) → Avanti → consenti la connessione → Avanti → seleziono tutti i profili → Avanti → inserisco un nome e una descrizione (come in figura) → Fine



Mando la richiesta di ping dalla macchina virtuale Kali:

```
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=28.5 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.35 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=8.36 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=2.52 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=8.36 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.21 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.828 ms
^C
--- 192.168.50.102 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6029ms
rtt min/avg/max/mdev = 0.828/7.299/28.465/9.160 ms
```

Senza questa configurazione il ping non funzionerebbe:

```
kali@kali:~$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data:
From 192.168.50.100 icmp_seq=1 Destination Host Unreachable
From 192.168.50.100 icmp_seq=5 Destination Host Unreachable
From 192.168.50.100 icmp_seq=6 Destination Host Unreachable
From 192.168.50.100 icmp_seq=7 Destination Host Unreachable
From 192.168.50.100 icmp_seq=8 Destination Host Unreachable
From 192.168.50.100 icmp_seq=9 Destination Host Unreachable
From 192.168.50.100 icmp_seq=10 Destination Host Unreachable
From 192.168.50.100 icmp_seq=11 Destination Host Unreachable
From 192.168.50.100 icmp_seq=12 Destination Host Unreachable
From 192.168.50.100 icmp_seq=13 Destination Host Unreachable
From 192.168.50.100 icmp_seq=17 Destination Host Unreachable
^C
--- 192.168.50.102 ping statistics ---
21 packets transmitted, 0 received, +11 errors, 100% packet loss, time 20496ms
pipe 4
```

2. Configuro InetSim tramite la VM Kali:

Apro il terminale → do il comando “sudo nano /etc/inetsim/inetsim.conf” → metto “#” davanti a tutti i servizi, tranne https → salvo ed esco

```
GNU nano 8.2 /etc/inetsim/inetsim.conf
#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
#start_service discard_tcp
```

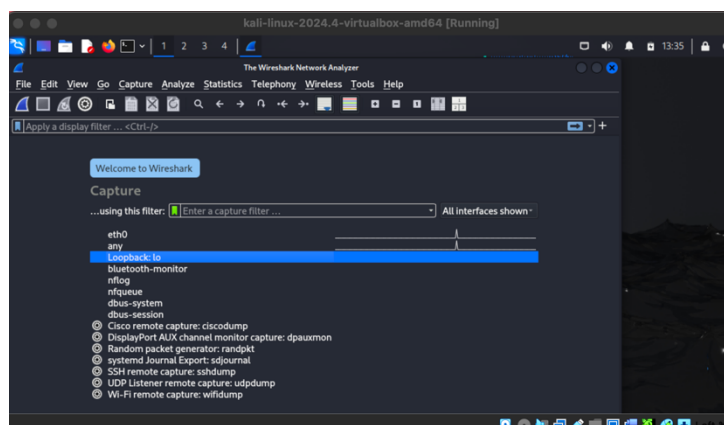
Do il comando “sudo inetsim”

```
kali@kali:~$ sudo inetsim
* irc_6667_tcp - stopped (PID 52882)
Simulation stopped.
== iNetSim main process stopped (PID 52854) ==

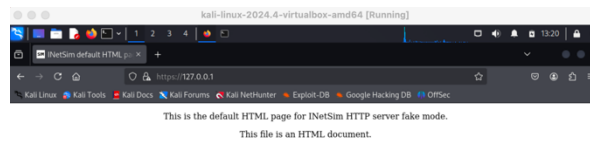
(kali@kali)~$ sudo nano /etc/inetsim/inetsim.conf
(kali@kali)~$ sudo inetsim
InetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== iNetSim main process started (PID 61611) ==
Session ID: 61611
Listening on: 127.0.0.1
Real Date/Time: 2025-03-14 16:10:40
Fake Date/Time: 2025-03-14 16:10:40 (Delta: 0 seconds)
Forking services...
* https_443_tcp - started (PID 61621)
done.
Simulation running.
```

3. Configuro una packet capture con Wireshark:

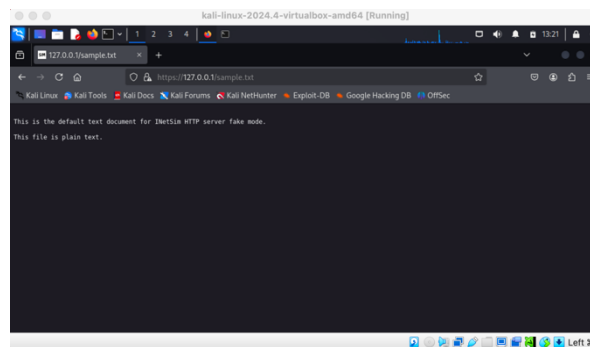
Apro l'app Wireshark sulla VM Kali → clicco su Loopback



Apro Firefox e cerco “https://127.0.0.1”



Cerco anche “https://127.0.0.1/sample.txt”



Su Wireshark monitoro il traffico di rete per verificare i pacchetti inviati e ricevuti

