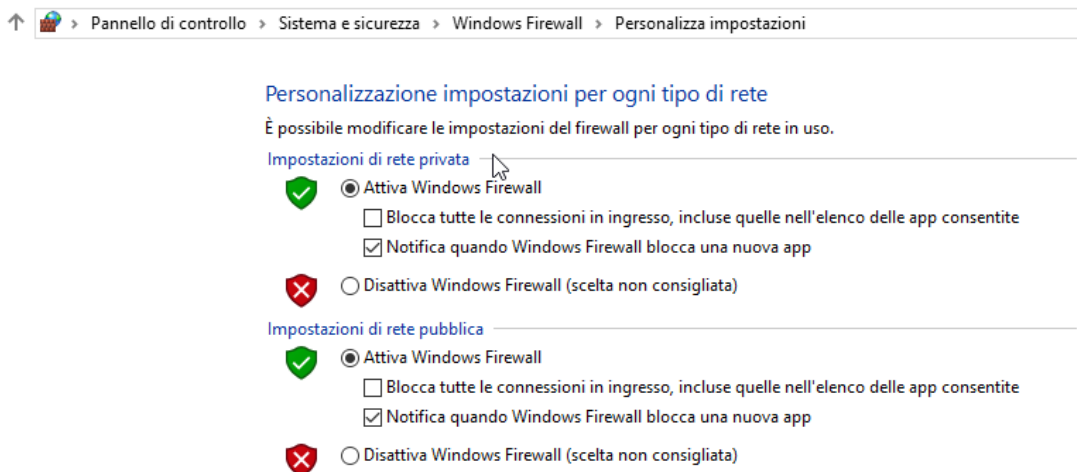


## CORSO CYBER SECURITY W3D4

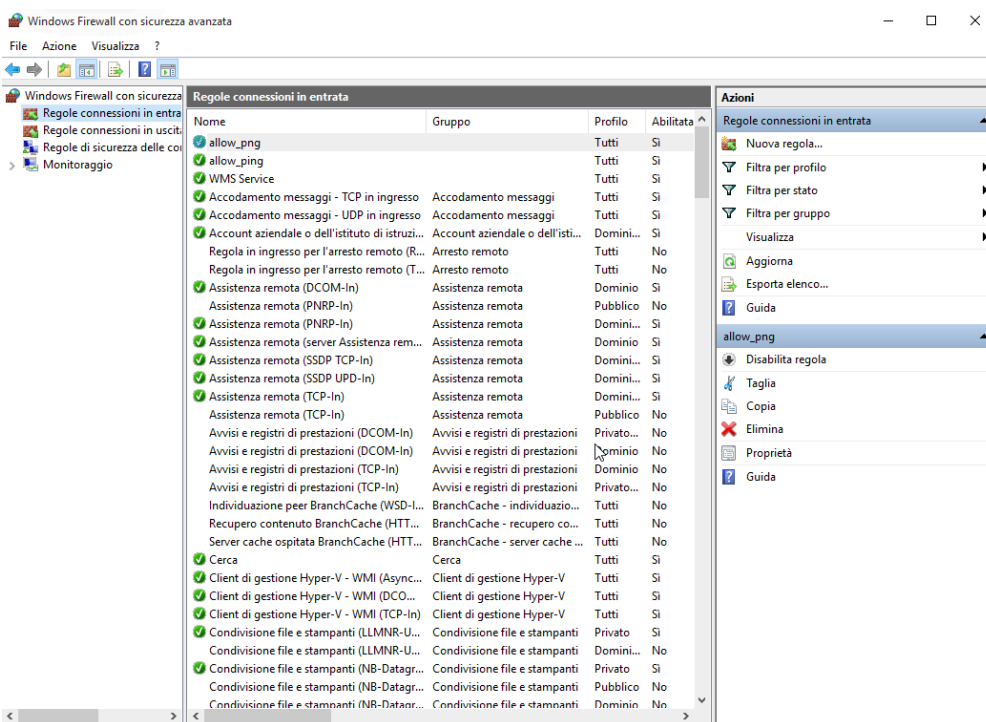
Studente: Orazio Morgillo

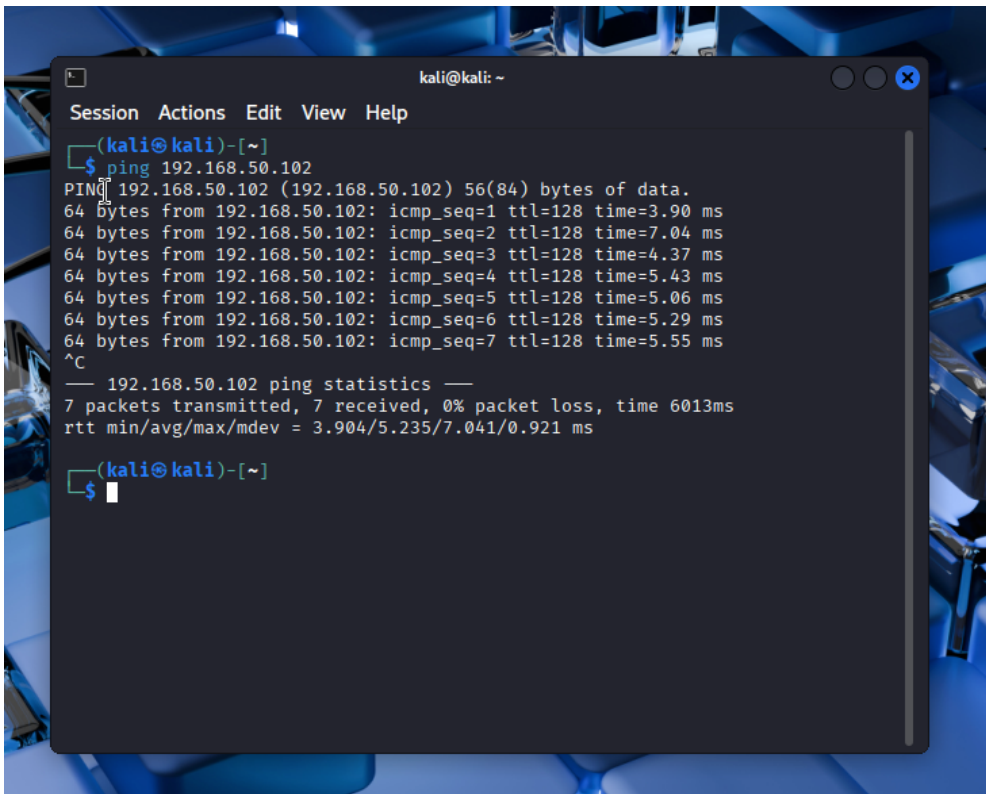
### PRIMA PARTE

L'obiettivo della prima parte dell'esercizio è attivare il firewall sulla macchina virtuale windows, poiché di base esso risulta disattivato, e a pingarlo con la macchina virtuale Kali Linux.



Dopodiché, creiamo su windows firewall una nuova regola personalizzata con protocollo ICMP (utilizzato dal ping) aperto a tutti gli indirizzi IP e testiamo da Kali che il ping sia stato correttamente instaurato tra le due macchine virtuali.



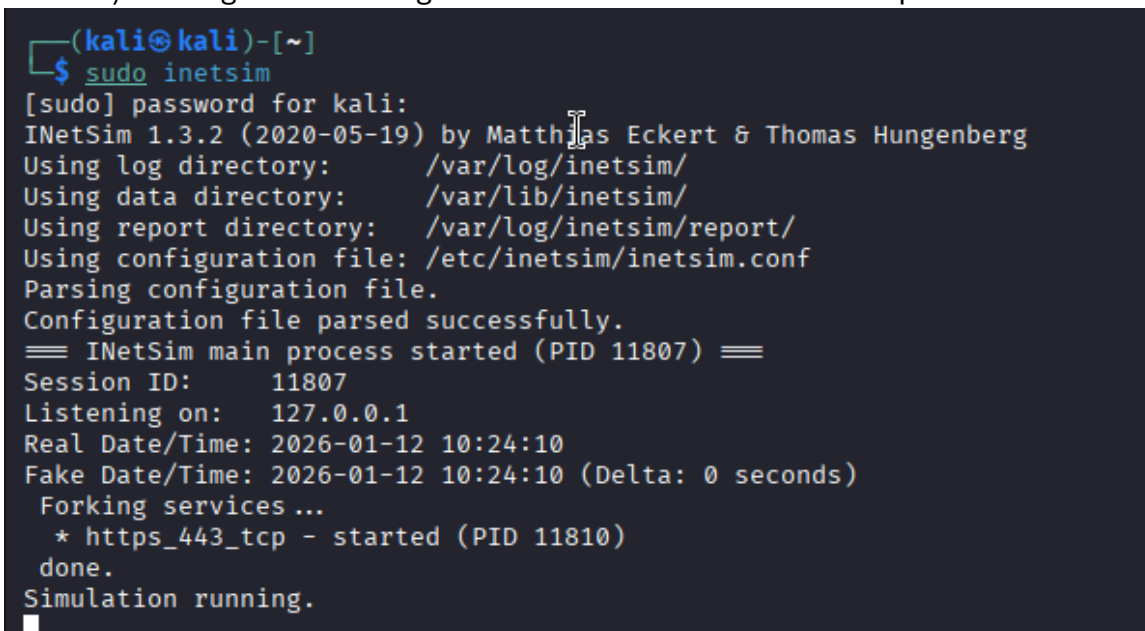
A screenshot of a terminal window titled 'kali@kali: ~'. The window has a menu bar with 'Session', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a user prompt '(kali@kali)-[~]' followed by the command '\$ ping 192.168.50.102'. The output shows seven successful ping requests with varying response times between 3.90 ms and 5.55 ms. Below the ping results, it shows '192.168.50.102 ping statistics' with 7 packets transmitted, 7 received, 0% packet loss, and a total time of 6013ms. The user then presses '^C' to exit the command.

```
(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=3.90 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=7.04 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=4.37 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=5.43 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=5.06 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=5.29 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=5.55 ms
^C
--- 192.168.50.102 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6013ms
rtt min/avg/max/mdev = 3.904/5.235/7.041/0.921 ms
(kali@kali)-[~]
$
```

Come si vede dallo screenshot sopra, i pacchetti sono stati trasmessi quindi vuol dire che il ping tra le macchine virtuali è andato a buon fine.

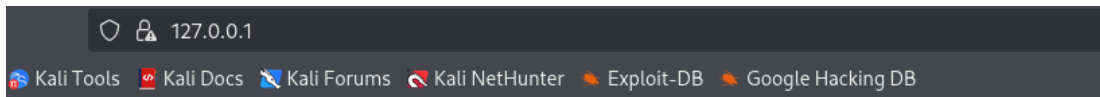
La seconda parte dell'esercizio, invece, consiste nell'utilizzare il software Wireshark preinstallato in Kali per la cattura dei pacchetti e l'analisi del contenuto.

Utilizziamo prima inetsim (un altro software preinstallato in Kali, un simulatore di servizi internet) e configuriamolo scegliendo di avviare solo il servizio https.

A screenshot of a terminal window showing the execution of the 'inetsim' command. The user enters '\$ sudo inetsim' at the prompt '(kali@kali)-[~]'. The terminal shows the password prompt '[sudo] password for kali:' and then the output of the 'inetsim' command. The output includes version information (INetSim 1.3.2), log and data directories, report directory, configuration file, and status messages indicating that the main process started (PID 11807) and the https service (PID 11810) is running.

```
(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 11807) ==
Session ID: 11807
Listening on: 127.0.0.1
Real Date/Time: 2026-01-12 10:24:10
Fake Date/Time: 2026-01-12 10:24:10 (Delta: 0 seconds)
Forking services...
* https_443_tcp - started (PID 11810)
done.
Simulation running.
```

Lanciando dal terminale il servizio inetsim con il comando `sudo inetsim`, notiamo che il servizio HTTPS è in ascolto sulla porta 443. Successivamente testiamo su internet se effettivamente tutto è andato a buon fine collegandoci ad un indirizzo <https://127.0.0.1>. Riceviamo come schermata di output la pagina fittizia di inetsim. Vuol dire che il servizio è attivo e raggiungibile dalla macchina.



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

This file is an HTML document.

```
kali@kali: ~  
Session 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 1587) ===  
Session ID: 1587  
Listening on: 127.0.0.1  
Real Date/Time: 2026-01-12 12:01:28  
Fake Date/Time: 2026-01-12 12:01:28 (Delta: 0 seconds)  
Forking services ...  
* https_443_tcp - started (PID 1597)  
done.  
Simulation running.  
█
```

Adesso andiamo su whireshark in loopback e avviamo il software.

Per semplicità possiamo aggiungere il filtro TCP che ricerca solo questo protocollo e possiamo notare, tramite la parentesi a sinistra, whireshark ha “preso un frame” (un insieme di pacchetti).

La source e la destination coincidono quindi stiamo operando nello stesso ambiente.

In info leggiamo che dalla porta 51064 alla porta 443 abbiamo mandato una richiesta di ping e abbiamo ricevuto una risposta dalla porta 443 alla porta 51064.

