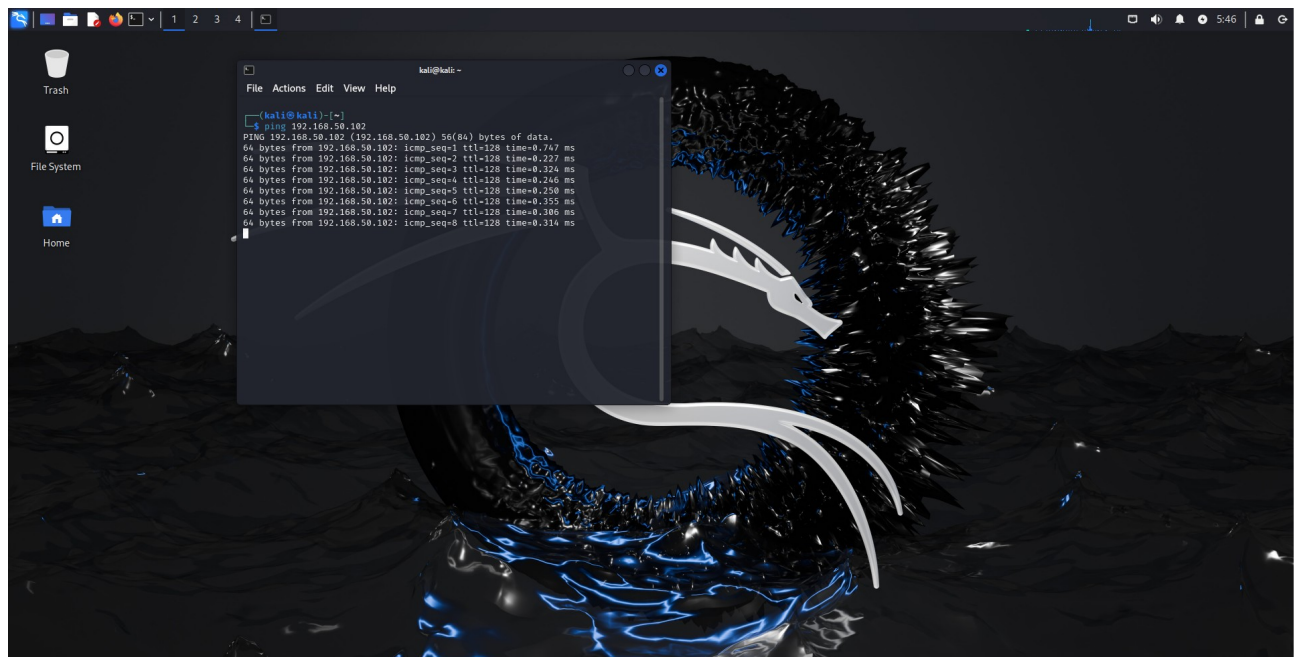


## 1) TENTATIVO DI PING DA KALI LINUX a WINDOWS 10

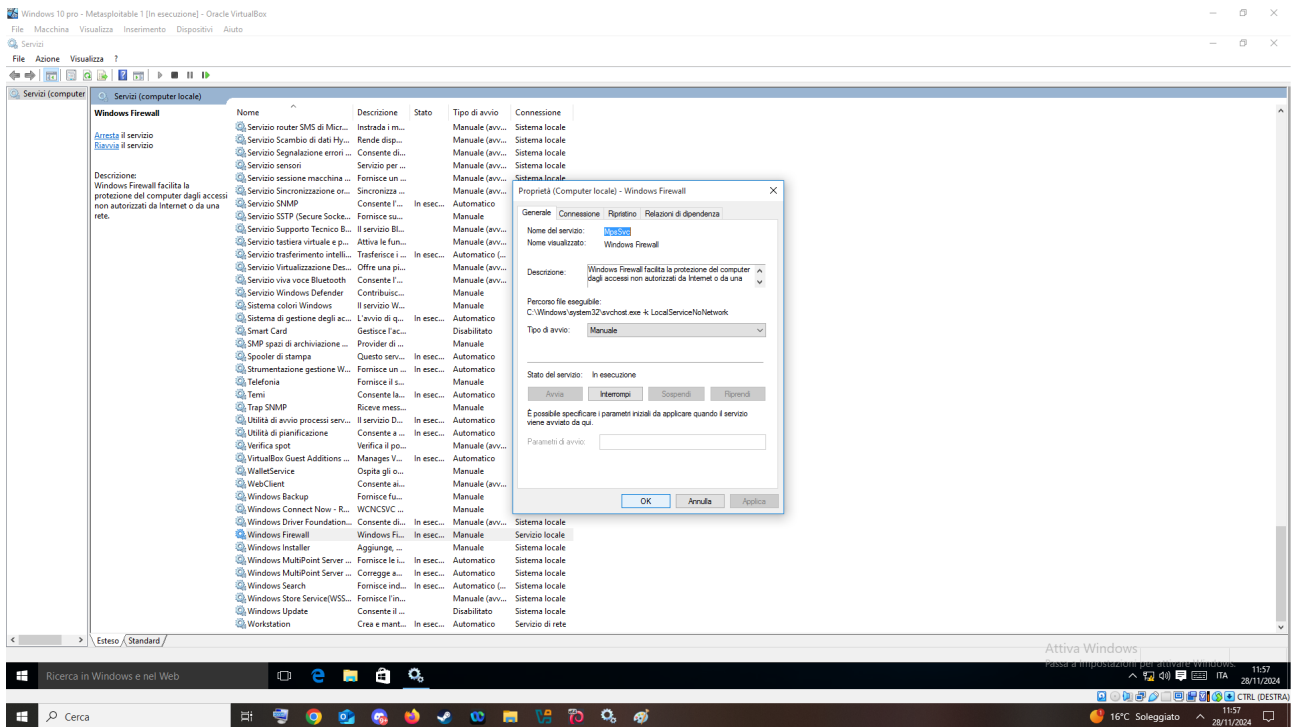


A causa delle impostazioni precedentemente configurate , non riusciamo ad eseguire il comando di Ping.

## 2) ATTIVAZIONE WINDOWS FIREWALL

Al fine di permettere che le nostre VM comunichino, è necessario impostare correttamente il Firewall di Windows 10.

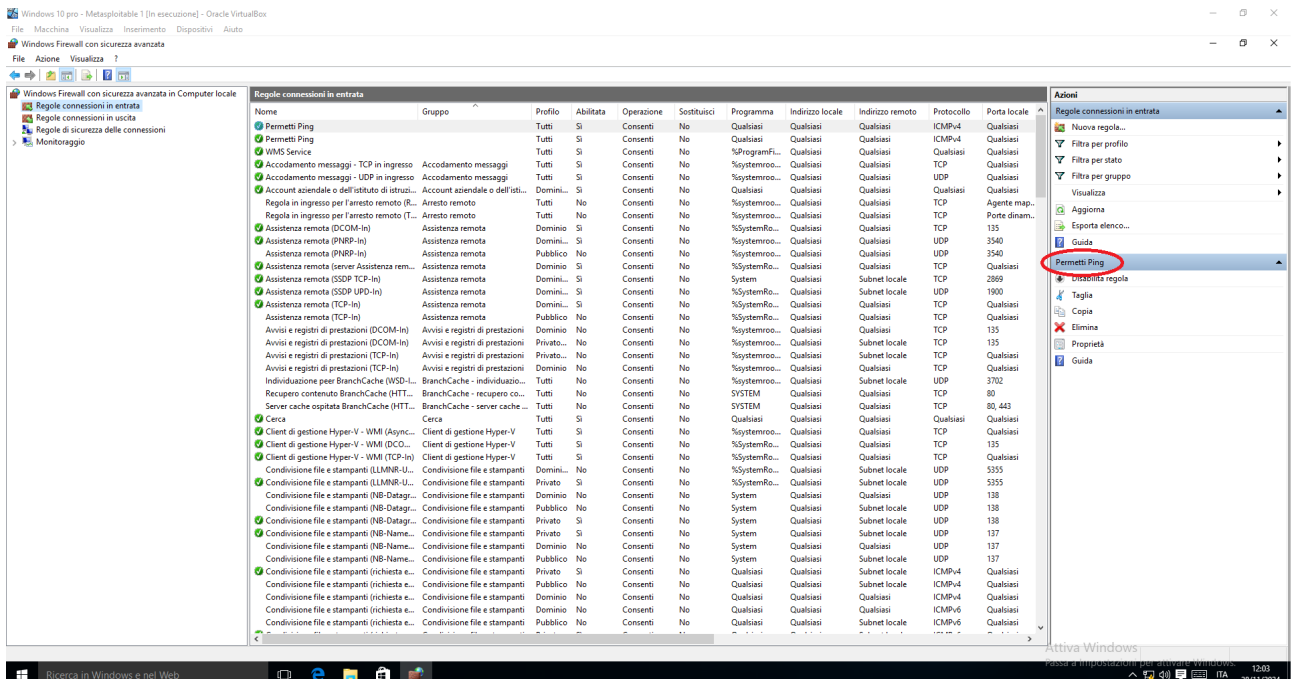
Eseguiamo le operazioni riportate nelle seguenti figure:



Avremo dunque bisogno di:

- Accedere a “servizi”;
- Individuare la voce “Windows Firewall”;
- Impostare la voce “Tipo di avvio” su manuale e applicare.
- Abilitare quindi il Firewall manualmente (Partendo dal Pannello di controllo)

### 3) CREAZIONE NUOVA REGOLA



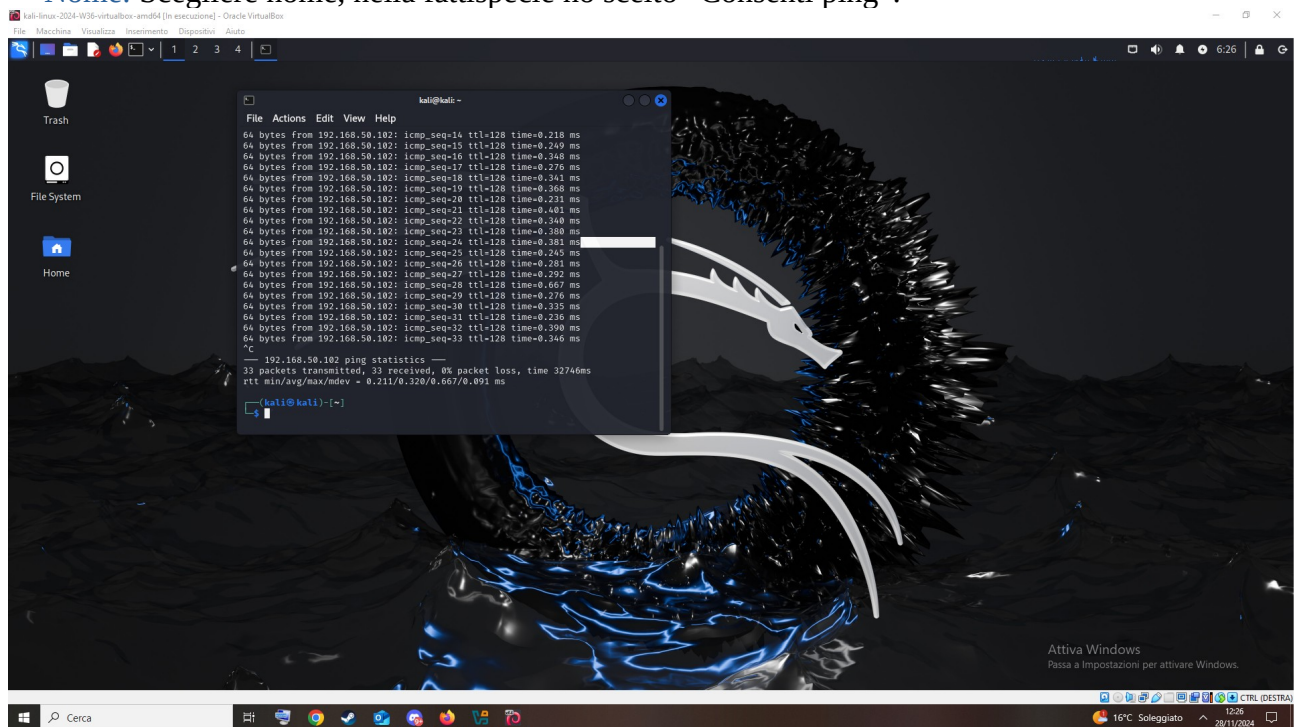
1-Apro: Pannello di controllo/ Sistema e Sicurezza/ Windows Firewall;

2-Selezione “Regole connessioni in entrata”

3-Click su “Nuova regola”

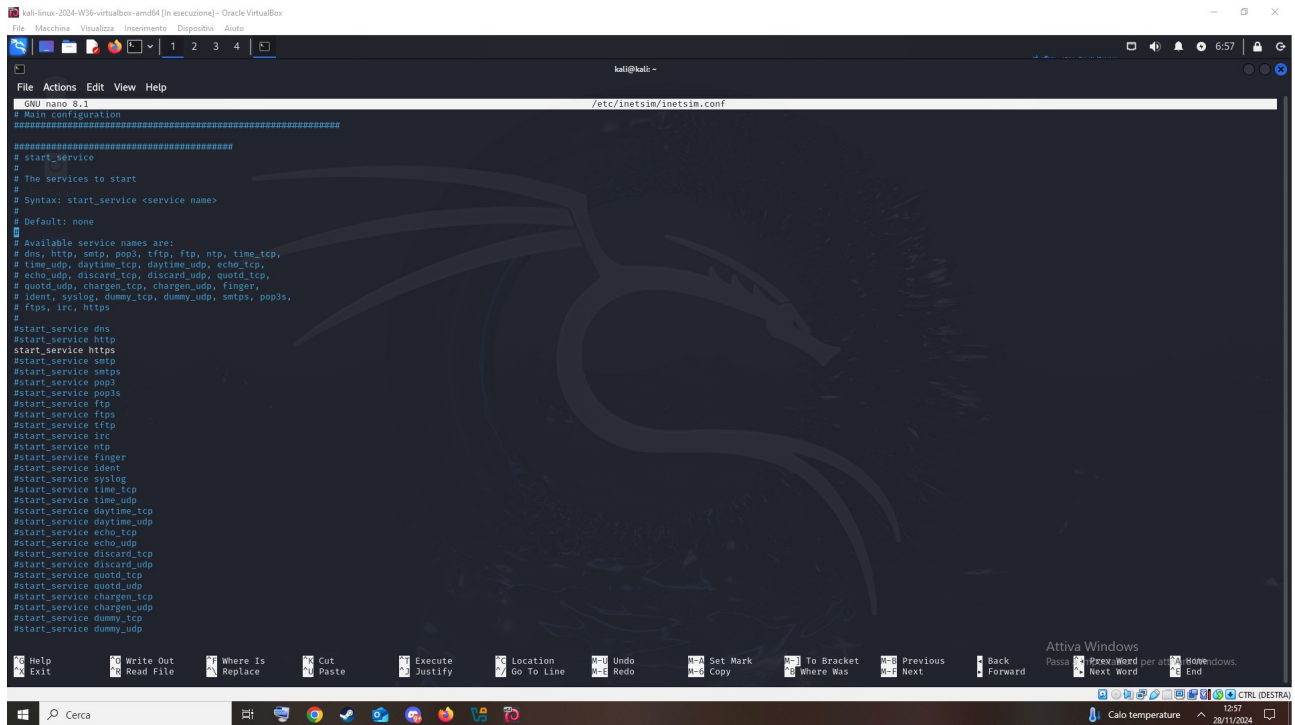
4-Imposto la Nuova regola con:

- Tipo di regola:** Click su “Personalizzata” ;
- Programma:** Selezionare “Tutti i Programmi” ;
- Protocollo e porte:** Tipo di protocollo: ICMPv4;
- Ambito:** Selezionare “Qualsiasi indirizzo IP” ;
- **Operazione:** Selezionare “Consenti la connessione”
- **Nome:** Scegliere nome, nella fattispecie ho scelto “Consenti ping”.



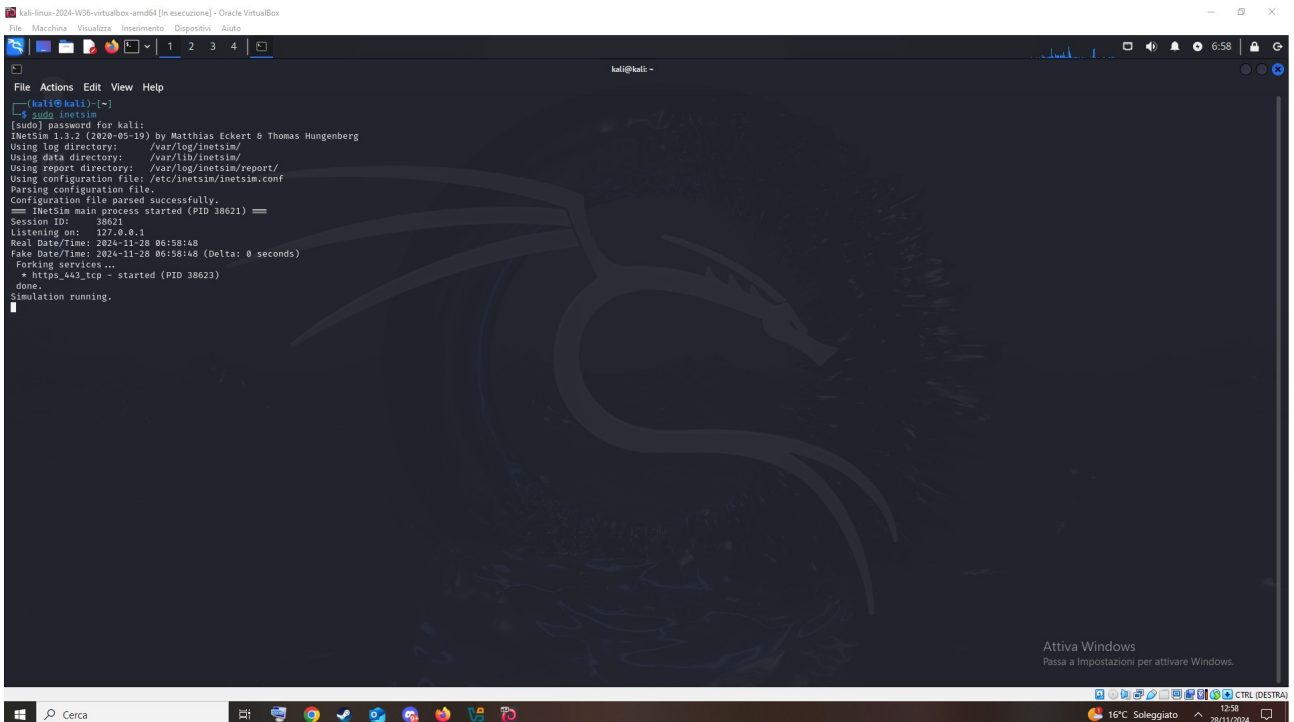
Tornato su Kali, ritento con successo ad eseguire il ping tra le due VM.

## 4) IMPOSTARE INETSIM



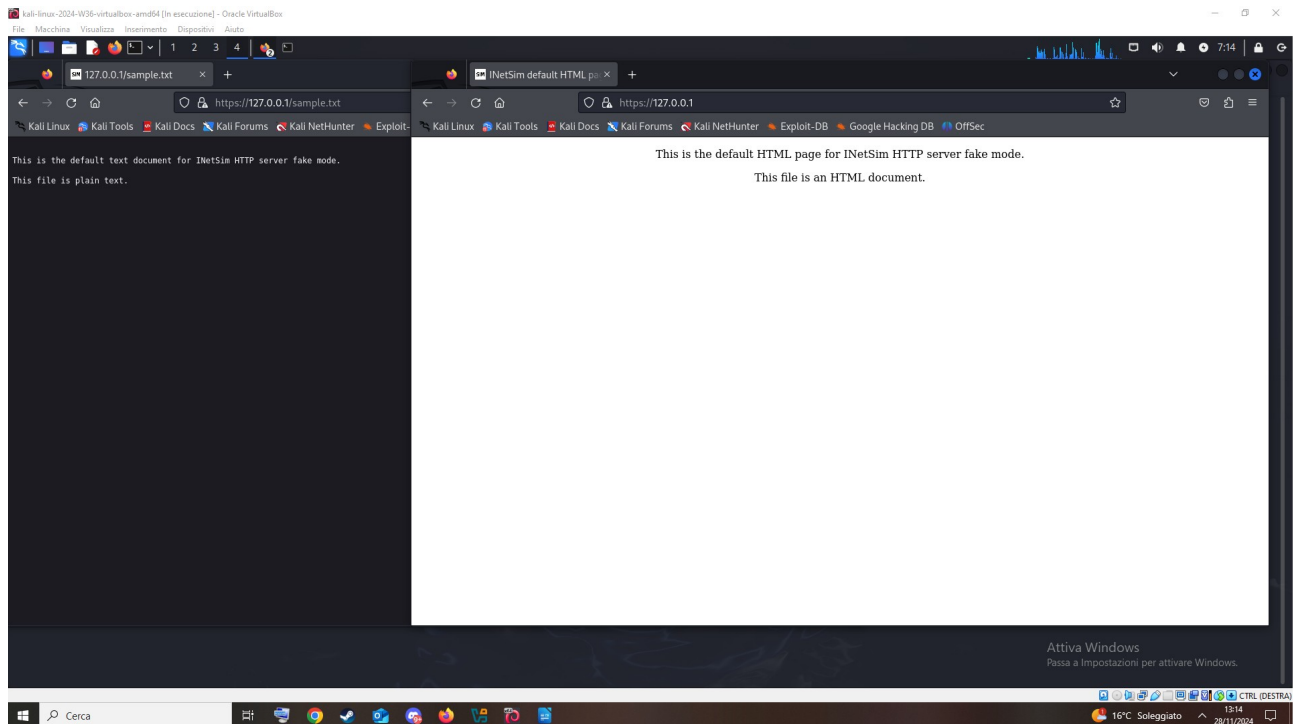
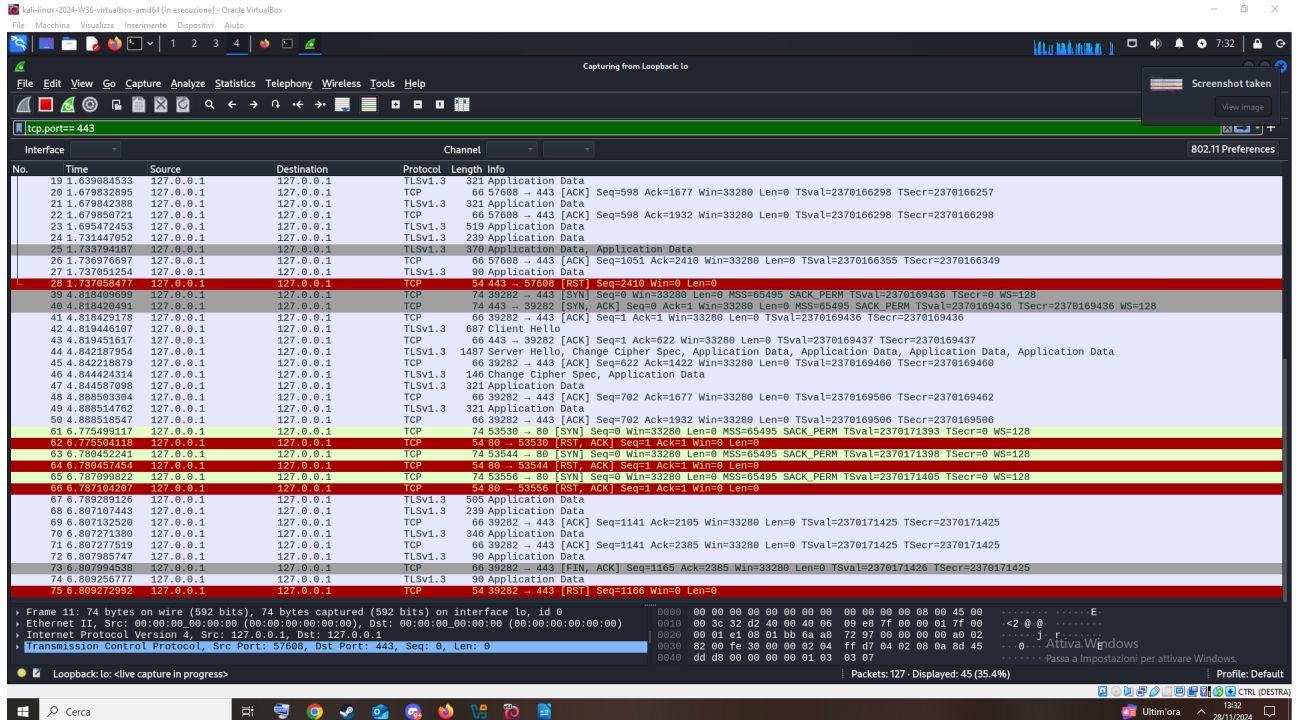
```
kali@kali:~$ nano /etc/inetsim/inetsim.conf
# inetsim configuration
# =====
# start_service
#
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# 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
# start_service discard_tcp
# start_service discard_udp
# start_service quotd_tcp
# start_service quotd_udp
# start_service chargen_tcp
# start_service chargen_udp
# start_service dummy_tcp
# start_service dummy_udp
```

- [Apro Terminale](#);
- [Eseguo il comando](#): “`sudo nano /etc/inetsim/inetsim.conf`” per attivare soltanto il servizio HTTPS. Digiterò quindi con il carattere “#” prima di ogni riga, come riportato in figura.
- [Eseguo](#) :” `sudo inetsim`”, come mostrato in figura, al fine di avviare l’emulazione.



```
kali@kali:~$ sudo inetsim
[sudo] password for kali:
Inetsim 1.32 (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 38621)
Session ID: 38621
Listening on: 127.0.0.1
Real Date/Time: 2024-11-28 06:58:48
Fake Date/Time: 2024-11-28 06:58:48 (Delta: 0 seconds)
Forking services...
+ https.443.tcp - started (PID 38623)
done.
Simulation running.
```

## 4) WIRESHARK



- Avvio Wireshark, imposto su “loopback” e scrivo :”Tcp.port== 443”
- Apro browser e raggiungo l’indirizzo :” https://127.0.0.1”
- Apro browser e raggiungo l’indirizzo :” https://127.0.0.1/sample.txt”
- Rilevo i dati grazie a Wireshark.

