

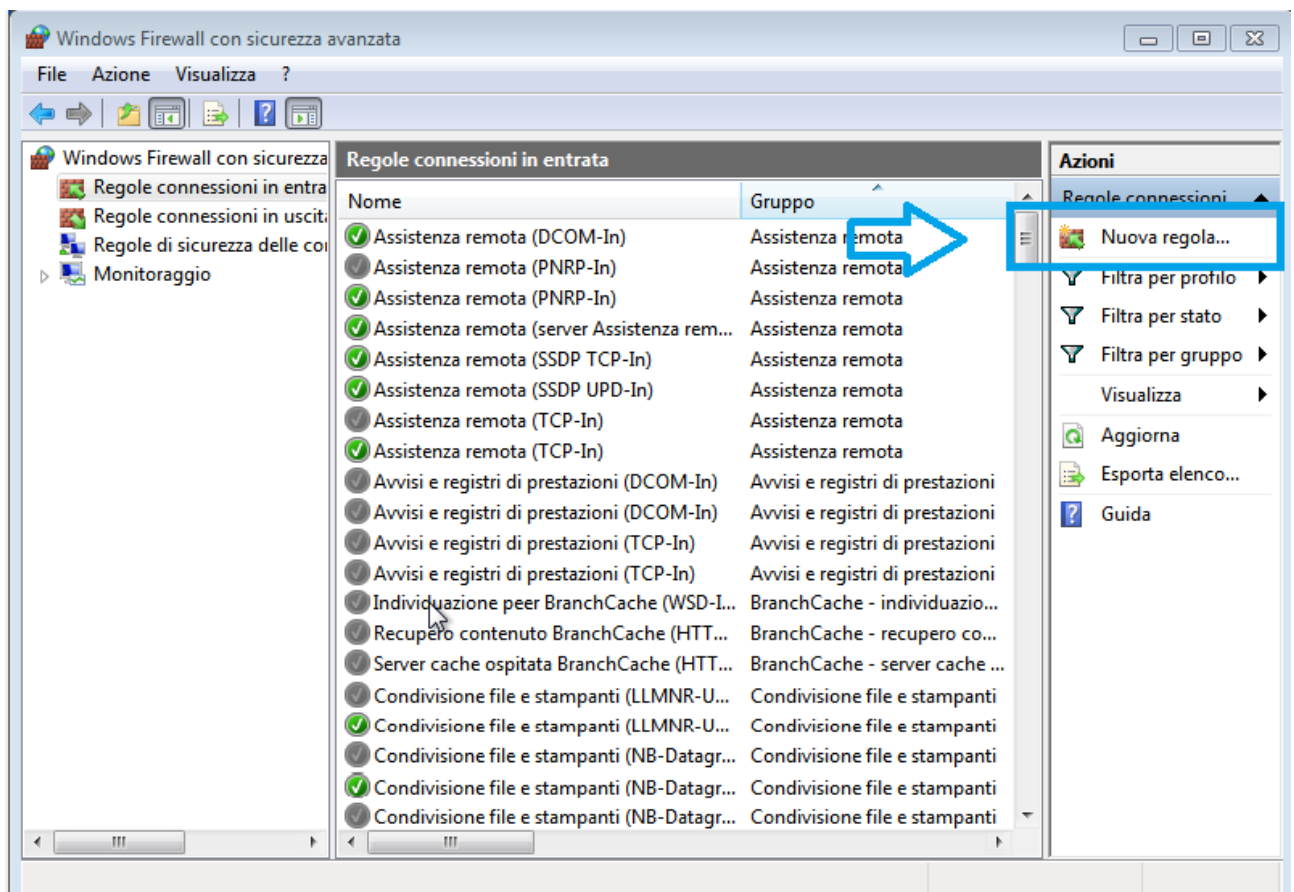
# RESERCIZIO W3D4 POLICY FIREWALL + WIRESHARK

In questo esercizio andremo a svolgere due operazioni

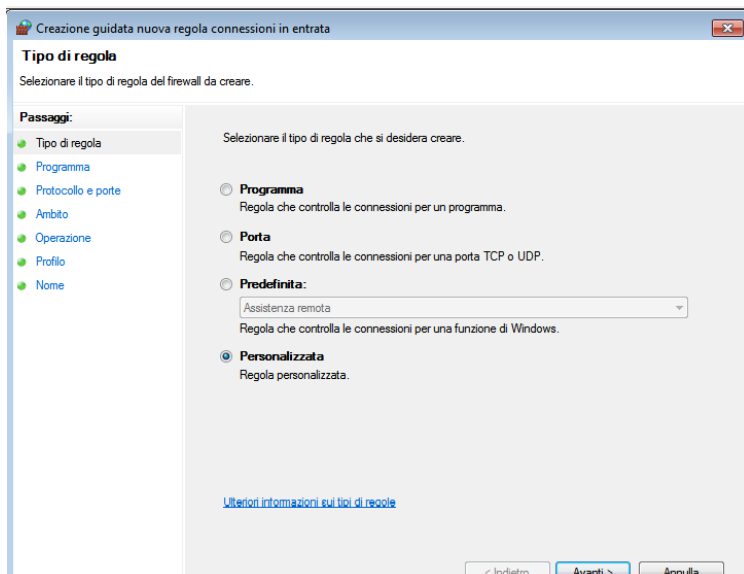
- Configurare le impostazioni nel firewall di Windows 7 applicando una regola che consenta la connessione tramite ping tra le macchine Kali/Meta a Windows 7
- Monitorare il flusso/scambio di pacchetti tramite il tool **Wireshark**

## IMPOSTARE UNA POLICY AL FIREWALL SU WINDWOS 7

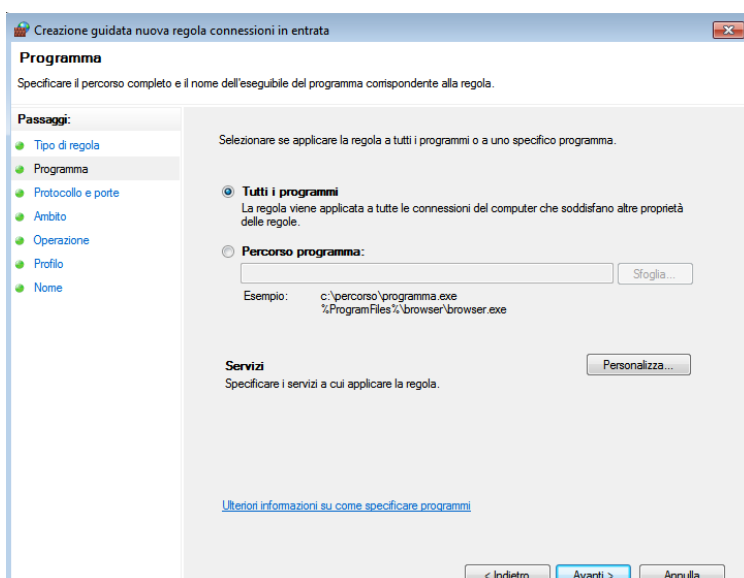
1. Come prima cosa andiamo ad aprire le impostazioni avanzate di **Windows Firewall** su **Windows 7** e poi clicchiamo a destra su “Nuova regola connessione in entrata” come mostrato in figura:



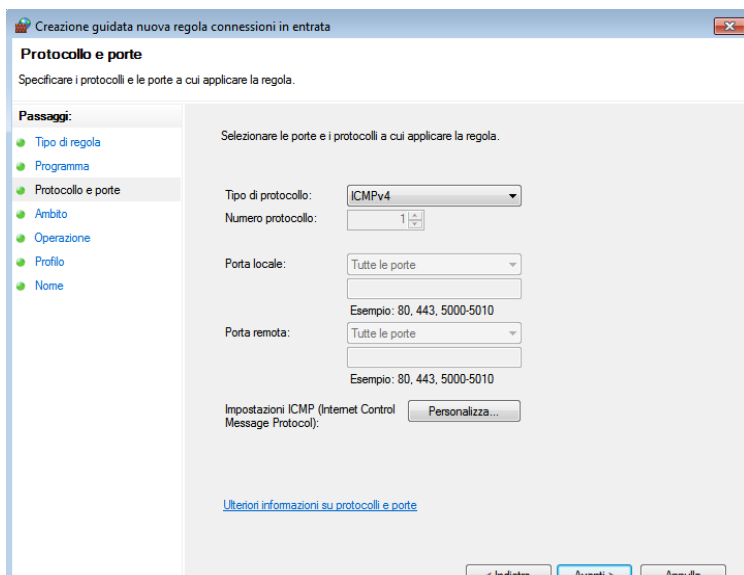
## 2. Come Tipo di regola impostiamo personalizzata:



## 3. Su Programma lasciamo "Tutti i programmi"



## 4. Nella scheda Protocollo e porte invece dobbiamo mettere come Tipo di protocollo il protocollo ICMPv4



## 5. Nella sezione ambito lasciamo Qualsiasi indirizzo IP

The screenshot shows the 'Ambito' step of the 'Creazione guidata nuova regola connessioni in entrata' wizard. The left sidebar lists the steps: Tipo di regola, Programma, Protocollo e porte, Ambito (selected), Operazione, Profilo, and Nome. The main area is titled 'Ambito' and contains the instruction 'Specificare gli indirizzi IP locale e remoto a cui applicare la regola.' Below this, there are two sections: 'Selezionare gli indirizzi IP locali a cui applicare la regola.' and 'Selezionare gli indirizzi IP remoti a cui applicare la regola.' Both sections have radio buttons for 'Qualsiasi indirizzo IP' (selected) and 'Questi indirizzi IP:'. Each section has a text input field and buttons for 'Aggiungi...', 'Modifica...', and 'Rimuovi'. There is also a 'Personalizza...' button. At the bottom, there are navigation buttons: '< Indietro', 'Avanti >', and 'Annulla'.

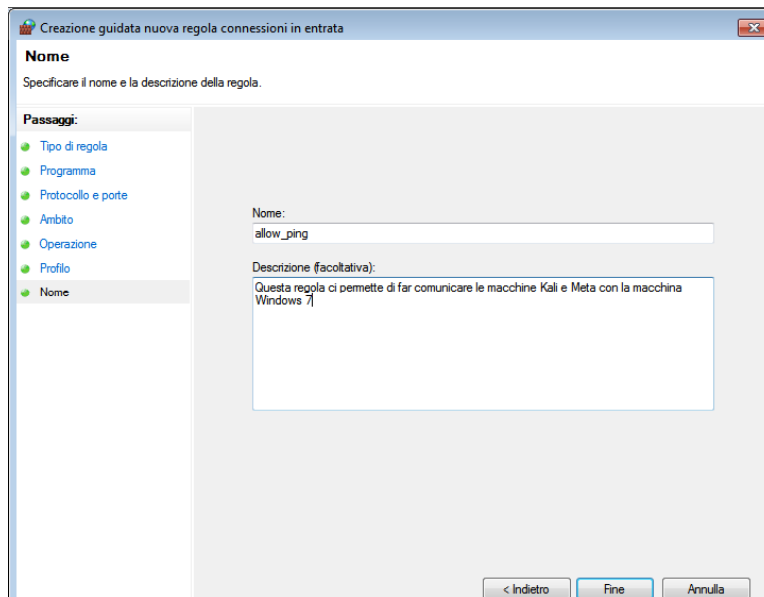
## 6. Lasciamo Consenti la connessione nella sezione Operazione

The screenshot shows the 'Operazione' step of the 'Creazione guidata nuova regola connessioni in entrata' wizard. The left sidebar lists the steps: Tipo di regola, Programma, Protocollo e porte, Ambito, Operazione (selected), Profilo, and Nome. The main area is titled 'Operazione' and contains the instruction 'Specificare l'operazione da eseguire quando una connessione corrisponde alle condizioni specificate nella regola.' Below this, there are three radio button options: 'Consenti la connessione' (selected), 'Consenti solo connessioni protette', and 'Blocca la connessione'. The 'Consenti la connessione' option has a description: 'Include le connessioni protette con IPsec e quelle non protette.' The 'Consenti solo connessioni protette' option has a description: 'Include solo le connessioni autenticate mediante IPsec. Le connessioni saranno protette con le impostazioni delle regole e proprietà IPsec nel nodo Regole di sicurezza delle connessioni.' There is a 'Personalizza...' button. At the bottom, there are navigation buttons: '< Indietro', 'Avanti >', and 'Annulla'.

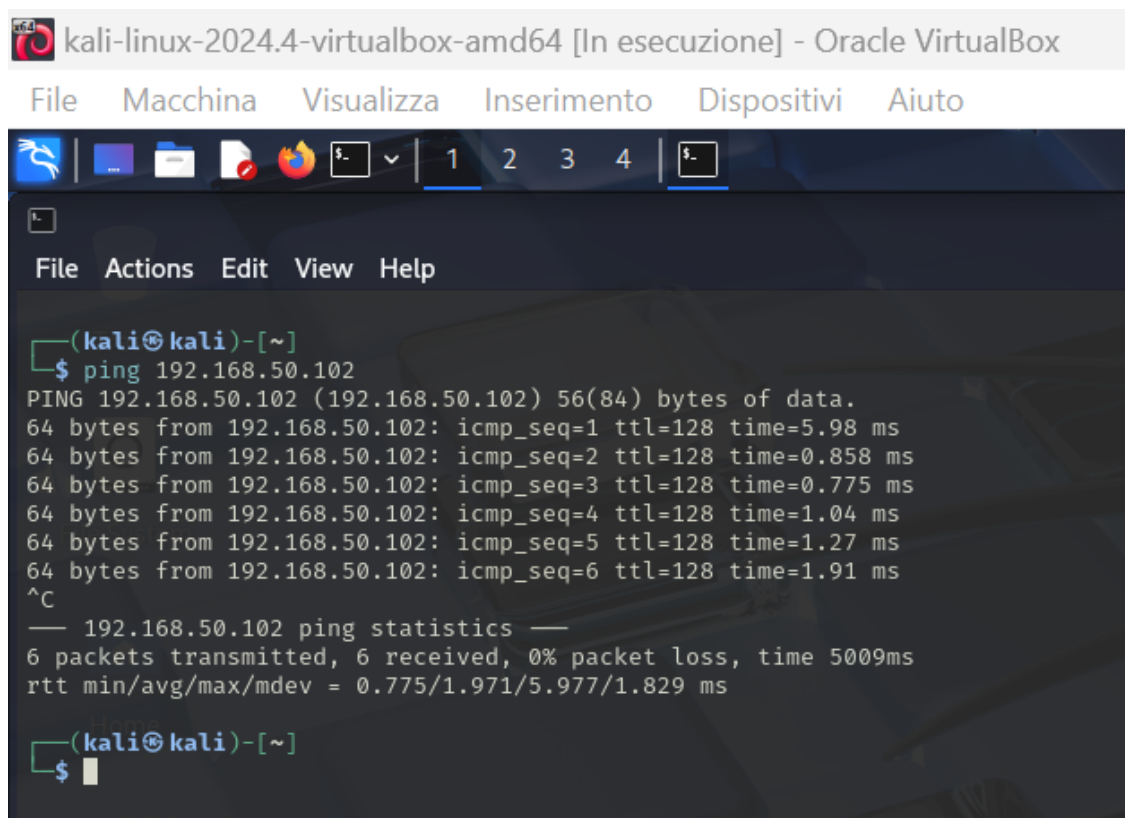
## 7. Nella sezione Profilo selezioniamo tutti i tipi di profilo (Dominio, Privato e Pubblico)

The screenshot shows the 'Profilo' step of the 'Creazione guidata nuova regola connessioni in entrata' wizard. The left sidebar lists the steps: Tipo di regola, Programma, Protocollo e porte, Ambito, Operazione, Profilo (selected), and Nome. The main area is titled 'Profilo' and contains the instruction 'Specificare i profili a cui si applica la regola.' Below this, there is a section titled 'Selezionare il tipo di applicazione della regola.' with three checked radio button options: 'Dominio' (Regola applicabile ai computer connessi al rispettivo dominio aziendale.), 'Privato' (Regola applicabile ai computer connessi ad un percorso di rete privato.), and 'Pubblico' (Regola applicabile ai computer connessi ad un percorso di rete pubblico.). There is a 'Personalizza...' button. At the bottom, there are navigation buttons: '< Indietro', 'Avanti >', and 'Annulla'.

8. Nell'ultima sezione andremo a dare un nome alla nostra regola e a descrivere a cosa serve. La chiamiamo **Allow\_ping** e scriveremo cosa ci permette di fare. Premiamo poi su Fine.



9. Come ultimo step andiamo ad effettuare un test di ping dalla macchina Kali per verificare che la regola appena creata consenta la connessione e comunicazione tra le due macchine (**Kali → Windows 7**)



# UTILIZZO DEI TOOLS INETSIM E WIRESHARK

Ora andremo a vedere e utilizzare due tools presenti nel sistema operativo **Kali Linux**:

- **Inetsim**: Permette la simulazione di diversi servizi applicativi (**HTTP, HTTPS, DNS** ecc.)
- **Wireshark**: È un tool che permette di monitorare e analizzare i pacchetti scambiati all'interno della rete

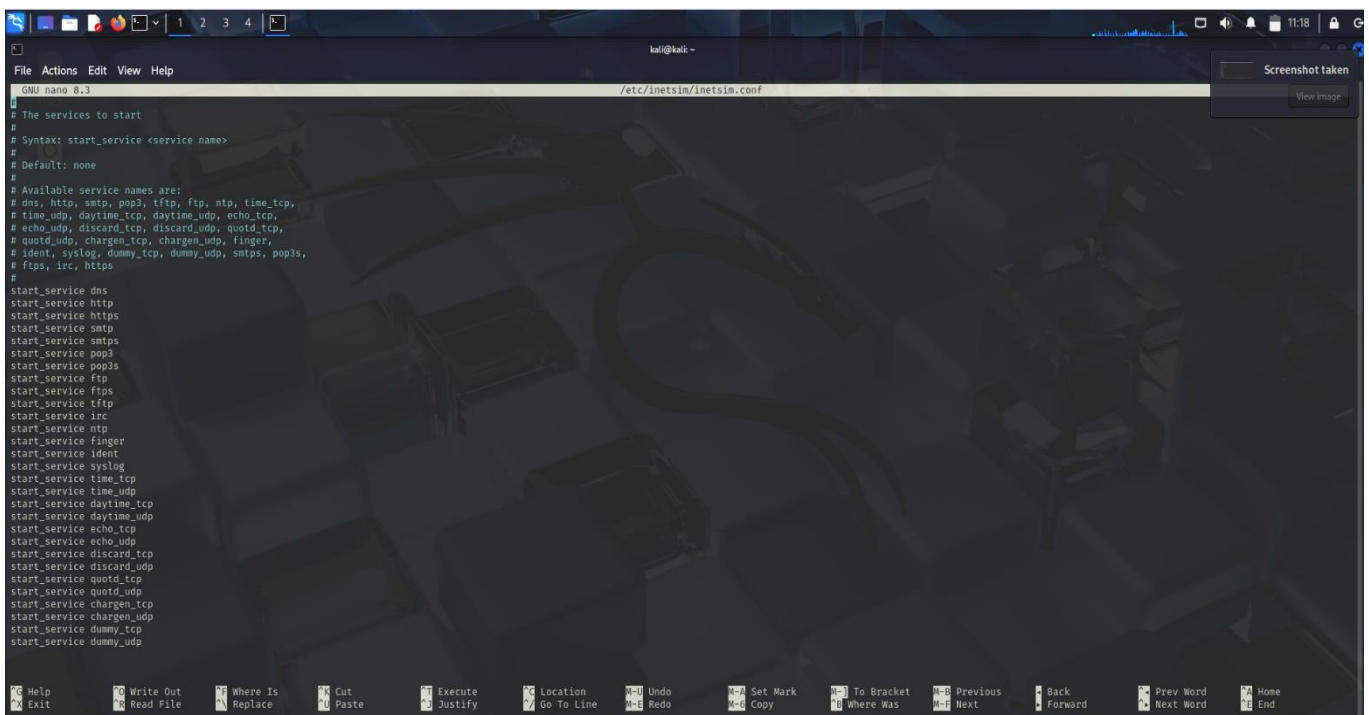
## INETSIM

Inetsim è un tool preconfigurato su Kali Linux che emula una gran quantità di servizi internet, come ad esempio i protocolli **HTTP, HTTPS, DNS, FTP** e molti altri servizi.

Noi in questo esercizio andremo ad emulare solamente il servizio **HTTPS**, andando ad escludere l'emulazione di tutti gli altri servizi. Per far ciò dobbiamo andare a modificare il file di configurazione di Inetsim aprendo il file **inetsim.conf** tramite il seguente comando da terminale:

**sudo nano /etc/inetsim/inetsim.conf**

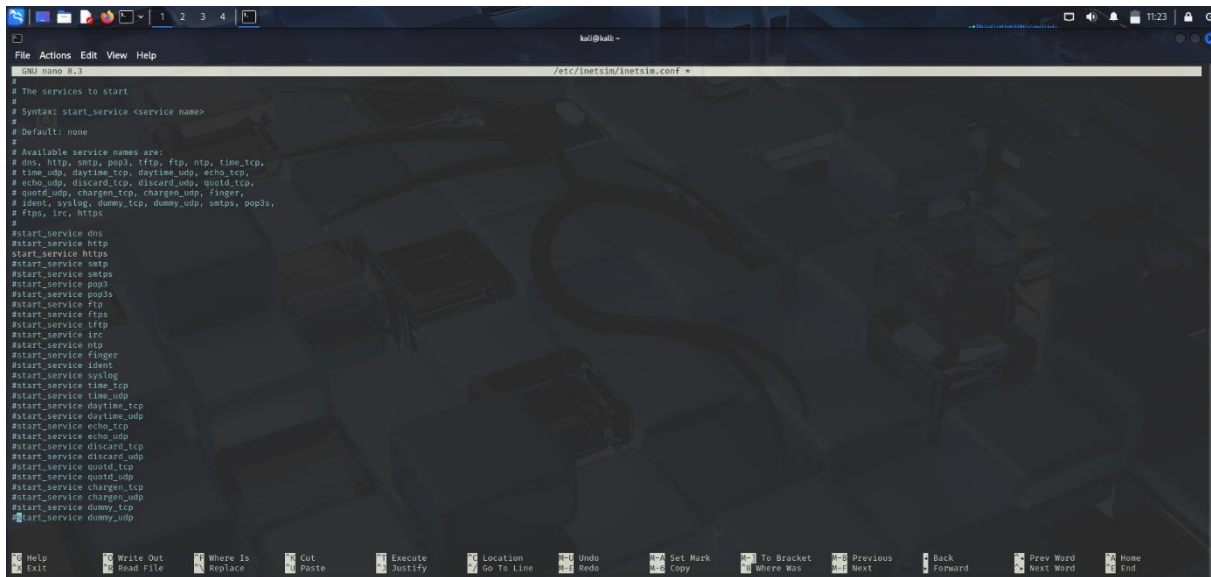
Ci troveremo di fronte ad una finestra come in questa immagine:



```
File Actions Edit View Help
GNU nano 8.3 /etc/inetsim/inetsim.conf
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, 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
```

Ora dobbiamo andare a “commentare” tutti i servizi che non abbiamo bisogno di emulare, perciò andremo ad inserire il carattere “#” (cancellotto) davanti a tutti i servizi (**start\_service ‘NOME PROTOCOLLO’**) che non siano di tipo **HTTPS**.

Otterremo il seguente risultato:

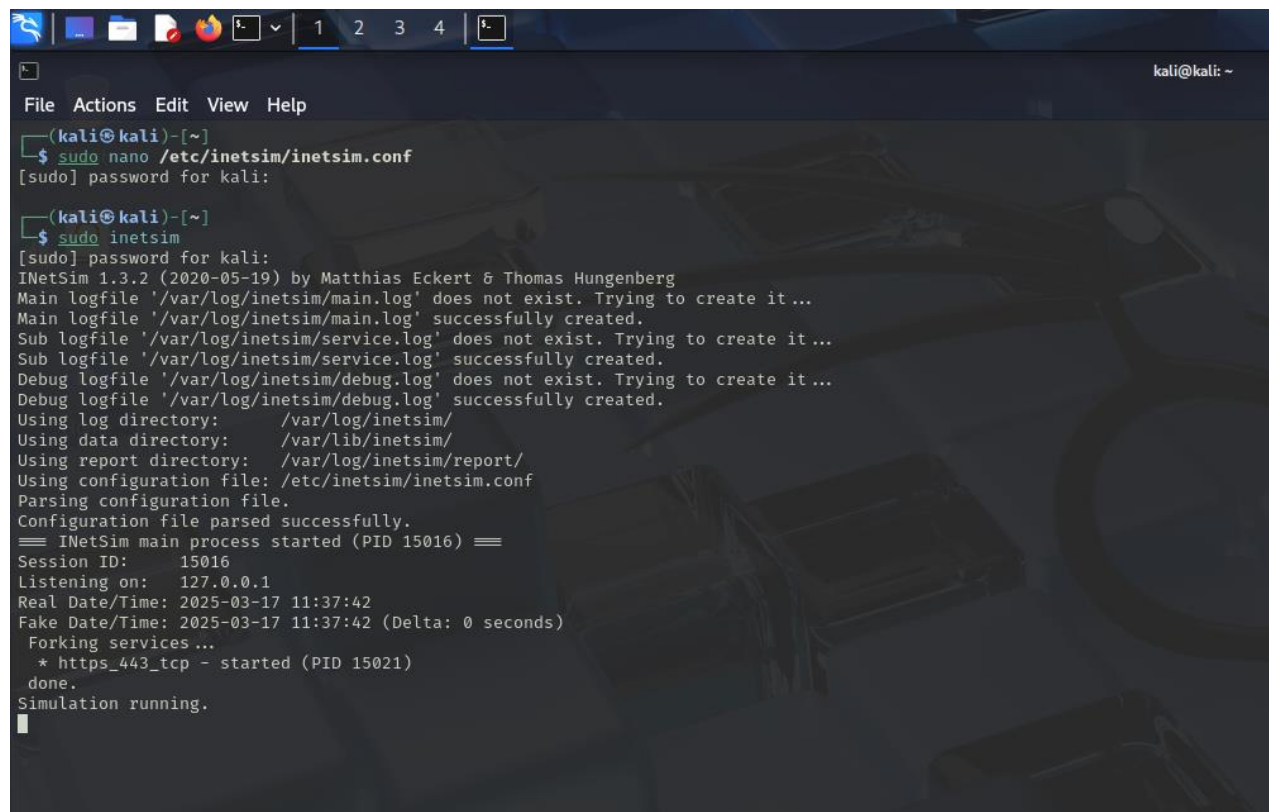


```
GNU nano 2.9.3 /etc/inetsim/inetsim.conf
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, ftp, ntp, time, tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quid_tcp,
# quid_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 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 quid_tcp
#start_service quid_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp
```

Ora salviamo premendo la combinazione **CTRL + X** e poi premendo il tasto **Y** per salvare ed uscire.

Non ci resta che andare ad avviare **Inetsim** lanciandolo da terminale avviandolo sempre con privilegi di amministratore (**sudo**) tramite il seguente comando: **sudo inetsim**

Dalla seguente immagine possiamo capire che il servizio **HTTPS** è in ascolto sulla porta **443** del localhost **127.0.0.1**

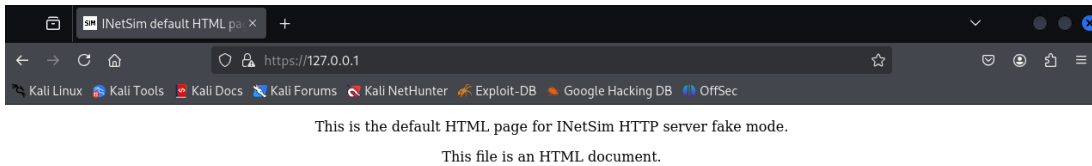


```
(kali@kali)-[~]
$ sudo nano /etc/inetsim/inetsim.conf
[sudo] password for kali:

(kali@kali)-[~]
$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Main logfile '/var/log/inetsim/main.log' does not exist. Trying to create it...
Main logfile '/var/log/inetsim/main.log' successfully created.
Sub logfile '/var/log/inetsim/service.log' does not exist. Trying to create it...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create it...
Debug logfile '/var/log/inetsim/debug.log' successfully created.
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 15016) ==
Session ID: 15016
Listening on: 127.0.0.1
Real Date/Time: 2025-03-17 11:37:42
Fake Date/Time: 2025-03-17 11:37:42 (Delta: 0 seconds)
Forking services ...
* https_443_tcp - started (PID 15021)
done.
Simulation running.
```

Eseguiamo ora un test, apriamo il browser web di Kali Linux e proviamo a connetterci alla porta **443** del localhost **127.0.0.1** digitando nella barra degli indirizzi <https://127.0.0.1>

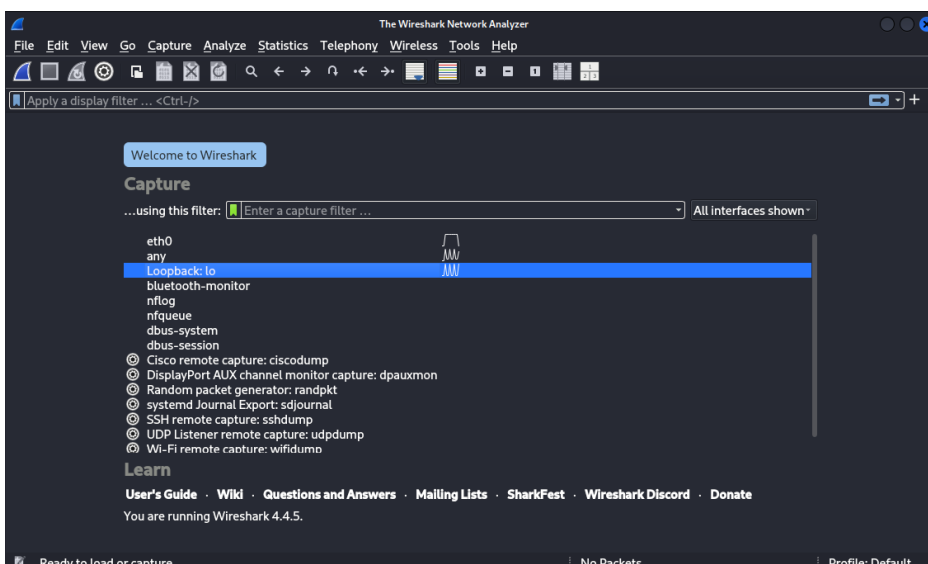
Dovremmo trovarci di fronte a questa situazione (immagine sottostante), il che vuol dire che il servizio è attivo e raggiungibile sul localhost



## WIRESHARK

Come ultimo scopo del nostro esercizio, andremo ad avviare il tool **Wireshark** dal terminale di **Kali Linux**.

Una volta avviato, ci connettiamo all'interfaccia di **loopback** cliccandoci sopra due volte:





Nella seguente “tabella” che ci viene mostrata possiamo notare e monitorare il flusso di pacchetti con ogni dettaglio che potrebbe essere utile, tra cui vari indirizzi, tipi di protocollo e soprattutto la sequenza “3-way-handshake” (**SYN**, **SYN+ACK** e **ACK**) sul protocollo **TCP**

The image shows a Wireshark capture of network traffic. The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
16	6.970755322	127.0.0.1	127.0.0.1	TCP	74	36460 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=754166...
17	6.970761849	127.0.0.1	127.0.0.1	TCP	54	80 → 36460 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	6.972918739	127.0.0.1	127.0.0.1	TCP	74	36470 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=754166...
19	6.972923967	127.0.0.1	127.0.0.1	TCP	54	80 → 36470 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	6.973081149	127.0.0.1	127.0.0.1	TCP	74	36478 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=754166...
21	6.973083944	127.0.0.1	127.0.0.1	TCP	54	80 → 36478 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	6.984328866	127.0.0.1	127.0.0.1	TCP	74	57106 → 443 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=75416...
23	6.984356239	127.0.0.1	127.0.0.1	TCP	74	443 → 57106 [SYN, ACK] Seq=0 Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM ...
24	6.984366636	127.0.0.1	127.0.0.1	TCP	66	57106 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=754166276 TSecr=754...
25	6.987496501	127.0.0.1	127.0.0.1	TLSv1.2	1228	Client Hello
26	6.987511397	127.0.0.1	127.0.0.1	TCP	66	443 → 57106 [ACK] Seq=1 Ack=1163 Win=72576 Len=0 TSval=754166279 TSecr=...
27	7.116541688	127.0.0.1	127.0.0.1	TLSv1.3	1487	Server Hello, Change Cipher Spec, Application Data, Application Data, A...
28	7.116553946	127.0.0.1	127.0.0.1	TCP	66	57106 → 443 [ACK] Seq=1163 Ack=1422 Win=78976 Len=0 TSval=754166408 TSe...
29	7.125515028	127.0.0.1	127.0.0.1	TLSv1.3	146	Change Cipher Spec, Application Data
30	7.125525065	127.0.0.1	127.0.0.1	TCP	66	443 → 57106 [ACK] Seq=1422 Ack=1243 Win=72576 Len=0 TSval=754166417 TSe...
31	7.125684635	127.0.0.1	127.0.0.1	TLSv1.3	321	Application Data
32	7.127360203	127.0.0.1	127.0.0.1	TLSv1.3	507	Application Data

The packet details pane for the first frame (No. 16) shows the following structure:

- Frame 1: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interf...
- Ethernet II, Src: 00:00:00\_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00\_00:00...
- Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.100
- Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII format.