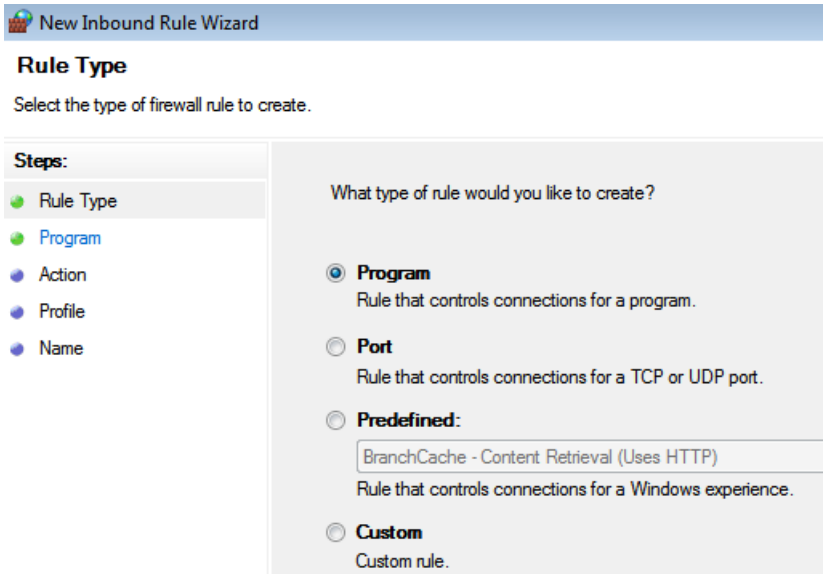
Configurazione del Firewall di Windows, Packet Capture con Wireshark e Simulazione di Servizi Internet con InetSim



Esercizio I: Configurazione della Policy del Firewall di Windows per il Ping da Macchine Linux a Windows 7

Obiettivo:

Configurare una policy nel firewall di Windows 7 per consentire il ping da macchine Linux nel laboratorio.

Procedure:

1. Accesso al Firewall di Windows:

   - Dal "Pannello di controllo", selezionare "Sistema e sicurezza" e quindi fare clic su "Firewall di Windows".

   - Accedere alle "Impostazioni avanzate" del firewall.

2. Creazione di una Regola In Entrata:

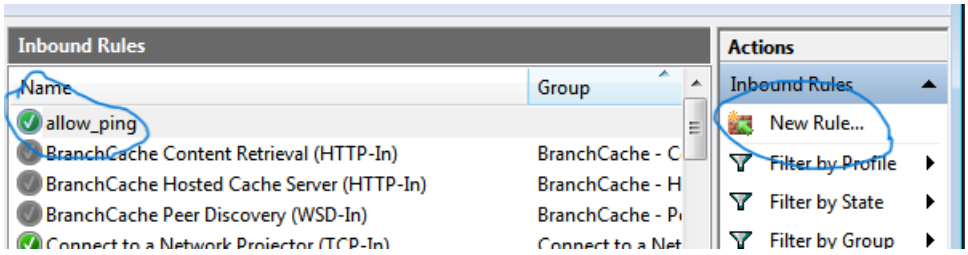
- Nella sezione "Monitoraggio del traffico", selezionare "Regole di connessione in entrata".

- Creare una nuova regola personalizzata, specificando il programma "icmpv4" (ping).

- Configurare la regola per consentire la connessione e assegnare il profilo di rete appropriato.

3. Risultati:

- Dopo l'implementazione della regola, le macchine Linux sono in grado di eseguire il ping con successo alla macchina Windows 7.



Questa immagine dimostra che la nuova regola è stata creata e attivata.

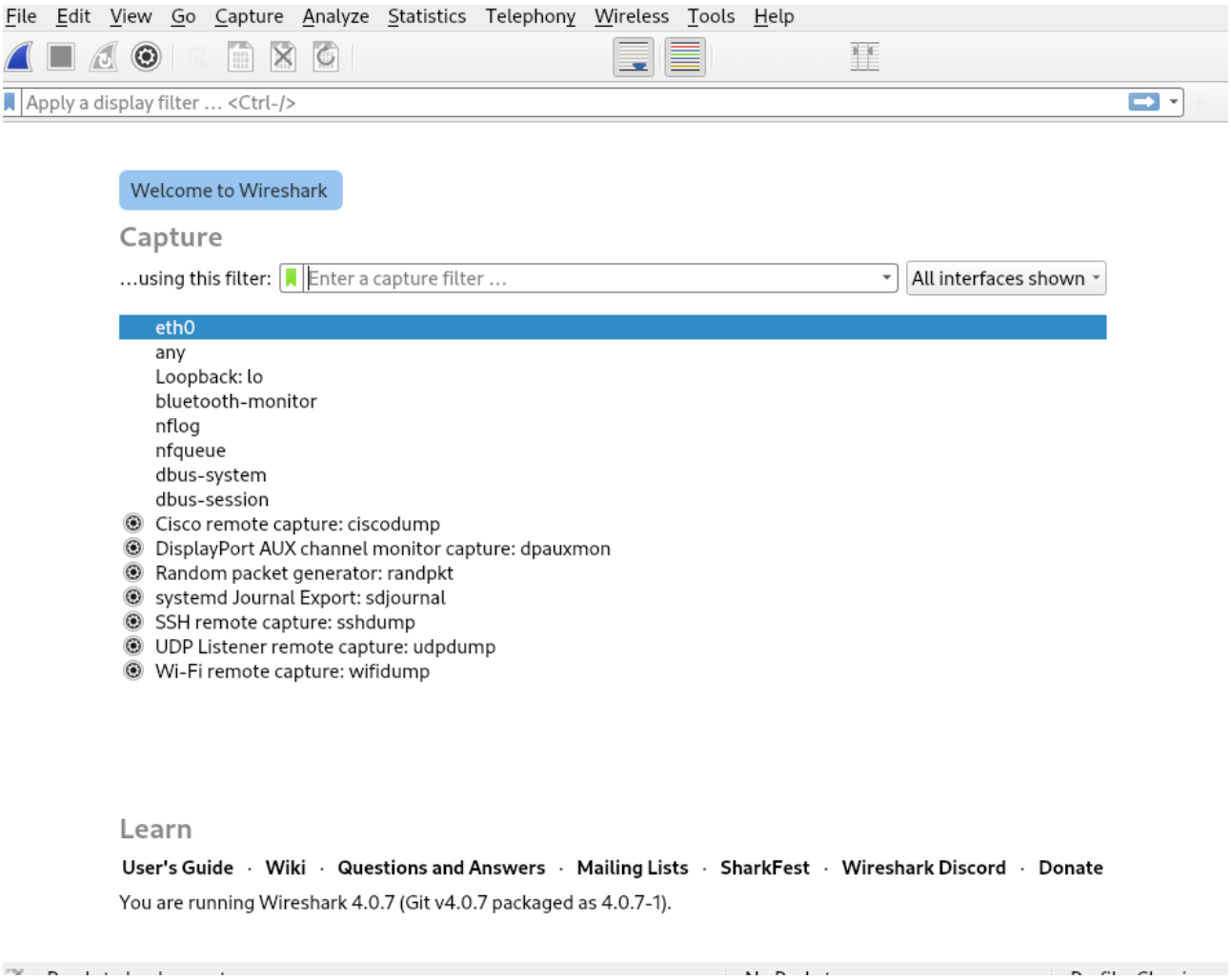
Esercizio II: Packet Capture con Wireshark

Obiettivo:

Effettuare una cattura dei pacchetti utilizzando Wireshark durante una sessione di ping dalla macchina Linux a Windows 7.

Procedure:

1. Avvio di Wireshark

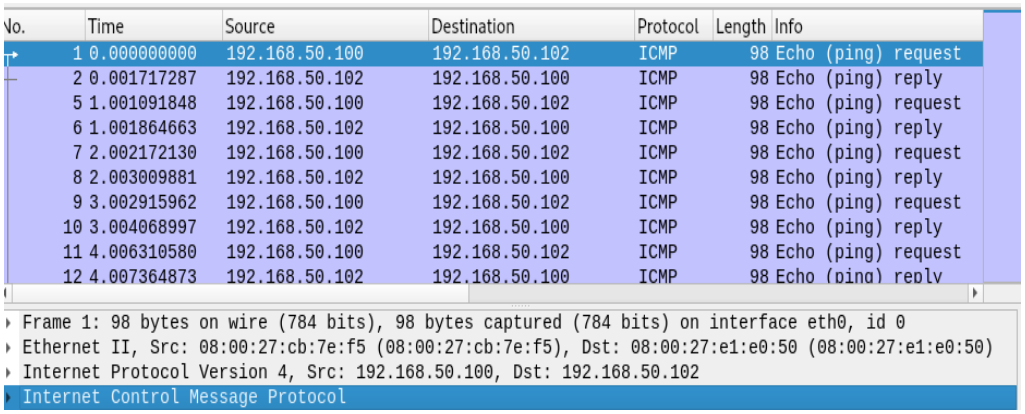


2. Avviao di ping dell'IP di Windows7

```
┌──(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=1.07 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.03 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=2.33 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.06 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=2.00 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.98 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=3.77 ms
64 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=1.56 ms
```

3. Risultati:

- La cattura dei pacchetti con Wireshark mostra il traffico ICMP generato durante la sessione di ping.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request
2	0.001717287	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply
5	1.001091848	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request
6	1.001864663	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply
7	2.002172130	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request
8	2.003009881	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply
9	3.002915962	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request
10	3.004068997	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply
11	4.006310580	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request
12	4.007364873	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply

```
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
Ethernet II, Src: 08:00:27:cb:7e:f5 (08:00:27:cb:7e:f5), Dst: 08:00:27:e1:e0:50 (08:00:27:e1:e0:50)
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.102
Internet Control Message Protocol
```

Esercizio III: Utilizzo di InetSim per l'Emulazione di Servizi Internet

Obiettivo: Configurare e utilizzare InetSim su Kali Linux per simulare servizi Internet.

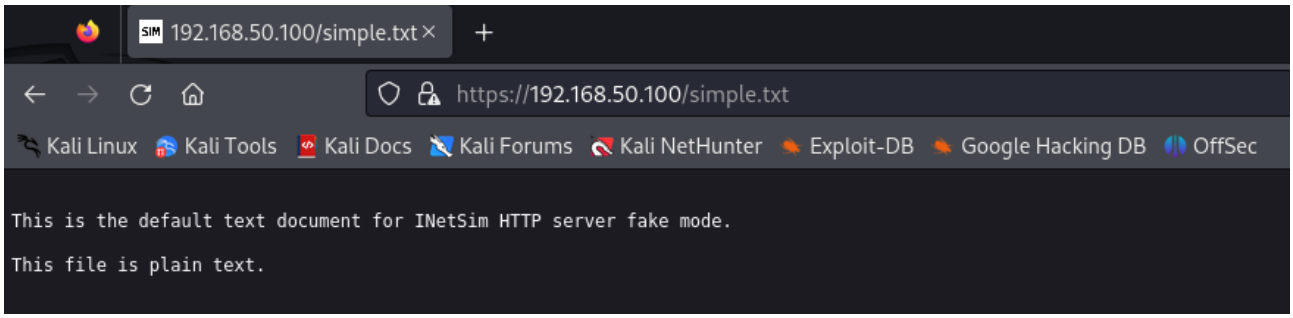
Configurare e utilizzare InetSim su Kali Linux per simulare servizi Internet.

```
#
#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


##################################
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <Indi
#
# Default: 127.0.0.1
#
service_bind_address 192.168.50.100

##################################
# service_run_as_user
#
# User to run services
#
```

1. Configurazione InetSim per HTTPS:
   - si commentano tutti i servizi lasciando solo HTTPS attivo.
   - cambio del **service_bind_adress** con l'IP di kali

```
########################################
# https_bind_port
#
# Port number to bind HTTPS service to
#
# Syntax: https_bind_port <port number>
#
# Default: 443
#
https_bind_port 443
```

2. Mettere 443 all https_bind-port



3. Risultati:

- InetSim emula vari servizi Internet, fornendo un ambiente di test controllato.

Conclusioni:

Questo laboratorio ha coperto con successo la configurazione del firewall di Windows, la cattura dei pacchetti con Wireshark durante il ping, e l'utilizzo di InetSim per simulare servizi Internet. L'implementazione corretta delle regole del firewall, la cattura dei pacchetti e la simulazione di servizi consentono un controllo dettagliato e un test efficace della rete.