

Esercitazione su Wireshark e Windows firewall

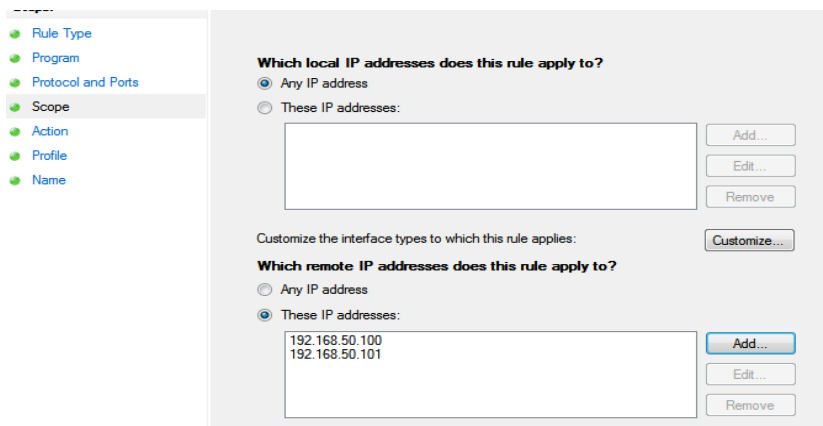
Traccia:

- Configurare policy per permettere il ping dalla macchina Linux alla macchina Windows 7 nel nostro laboratorio;
- Utilizzo dell'utility inetsim per l'emulazione di servizi internet;
- Cattura dei pacchetti con Wireshark;

1. Configurazione di una nuova policy firewall su windows 7

Per consentire il ping da una macchina all'altra sotto la stessa rete dobbiamo configurare una nuova Policy Firewall dalle impostazioni avanzate di Windows che di Default non consente il traffico dati.

Su scope impostiamo abbiamo impostato come local IP address quello di Windows 7. Mentre su scope andiamo ad inserire gli IP delle macchine a cui è consentita la comunicazione (Metasploitable e Kali Linux)



Su protocol and ports impostiamo come tipo di protocollo ICMPv4.

Protocol and Ports
Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports**
- Scope
- Action
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type:

Protocol number:

Local port:

Remote port:

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

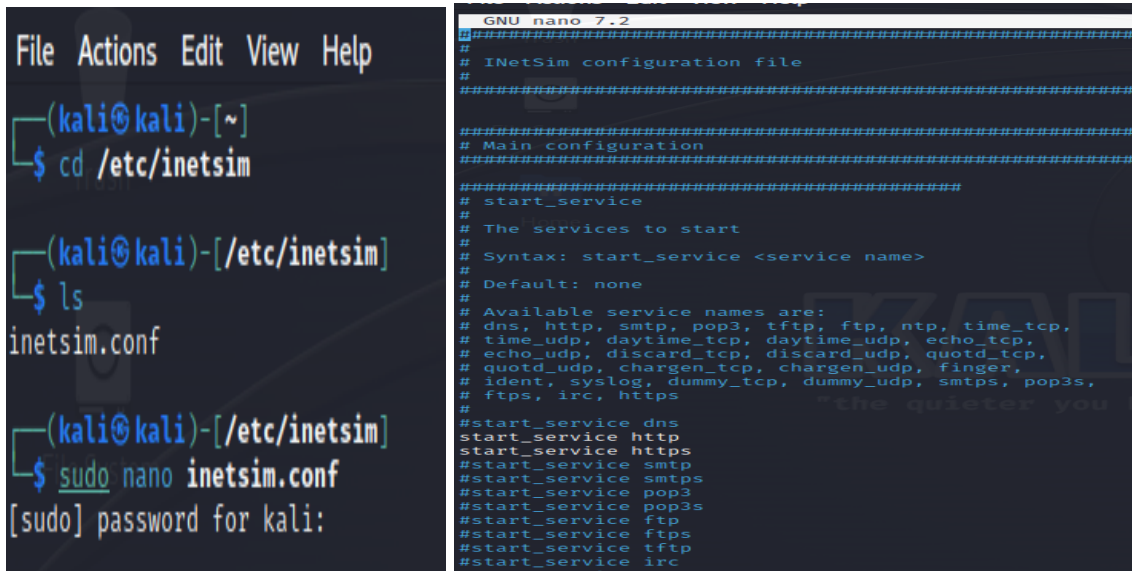
Kali grazie alla nuova policy firewall di Windows 7 può quindi comunicare con esso.

```
File Actions Edit View Help
(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=3.97 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.486 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.898 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.515 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.551 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.911 ms
^C
--- 192.168.50.102 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5051ms
rtt min/avg/max/mdev = 0.486/1.221/3.965/1.239 ms
(kali@kali)-[~]
$ sudo nano /etc/network/interfaces
```

2. Utilizzo di inetsim per l'emulazione di pacchetti di internet.

Da Kali adesso procediamo con la configurazione di inetsim per emulare pacchetti.

Questi sono i comandi da utilizzare per poter successivamente entrare nell'impostazione del file e modificarle:

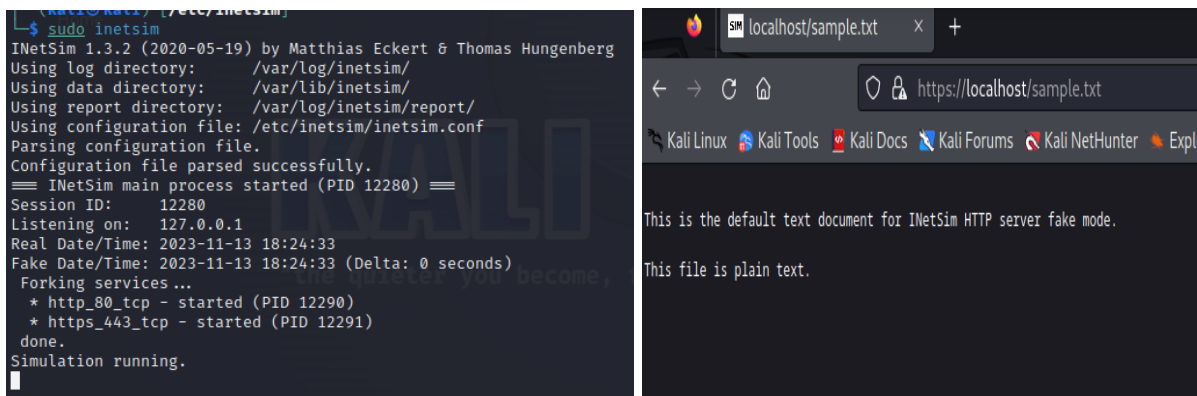


```
File Actions Edit View Help
(kali@kali)-[~]
$ cd /etc/inetsim
(kali@kali)-[/etc/inetsim]
$ ls
inetsim.conf
(kali@kali)-[/etc/inetsim]
$ sudo nano inetsim.conf
[sudo] password for kali:

GNU nano 7.2
#
# INetSim configuration file
#
#####
# Main 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
```

A questo punto andremo a commentare tutti i servizi a parte quelli http e https che ci consentiranno di accedere ad internet.

Tramite il comando “sudo inet inetsim” facciamo partire la simulazione e proviamo ad aprire il sito internet con l’indirizzo “<http://localhost/>”



```
(kali@kali)-[/etc/inetsim]
$ 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 12280) ==
Session ID: 12280
Listening on: 127.0.0.1
Real Date/Time: 2023-11-13 18:24:33
Fake Date/Time: 2023-11-13 18:24:33 (Delta: 0 seconds)
Forking services...
* http_80_tcp - started (PID 12290)
* https_443_tcp - started (PID 12291)
done.
Simulation running.
```

localhost/sample.txt

https://localhost/sample.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

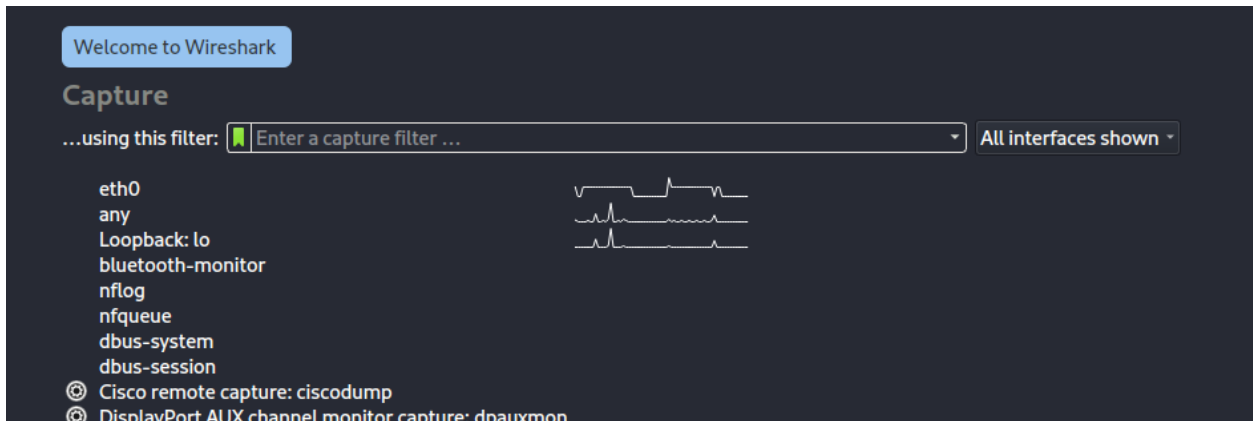
This is the default text document for INetSim HTTP server fake mode.

This file is plain text.

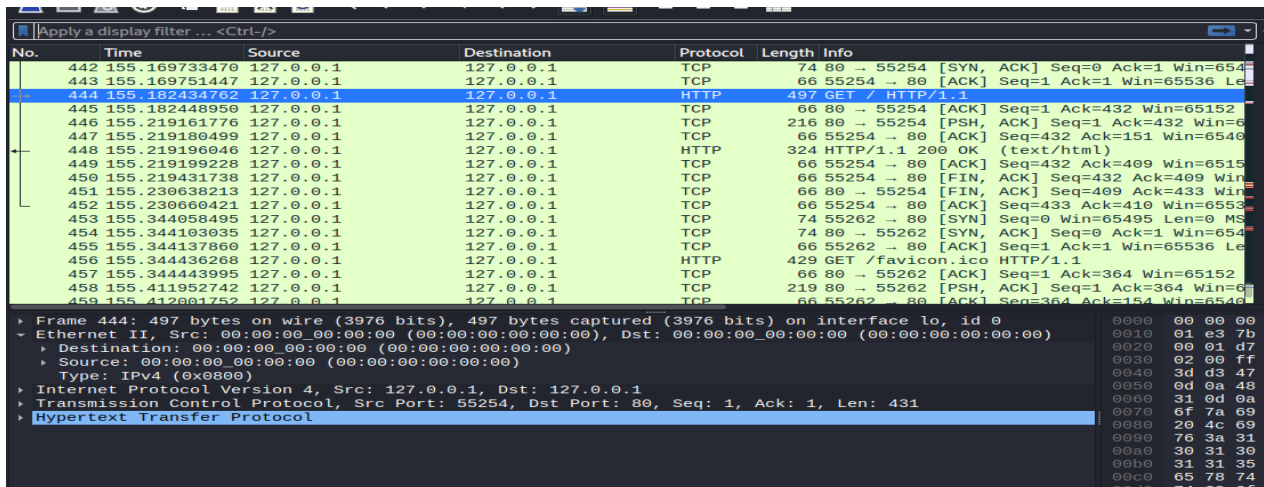
3. Cattura dei pacchetti con Wireshark.

Le principali caratteristiche di Wireshark includono la capacità di catturare dati in tempo reale o da file di cattura precedentemente salvati, filtrare e analizzare pacchetti in base a diversi criteri, visualizzare dettagli specifici dei protocolli di rete e fornire statistiche dettagliate sul traffico di rete.

- Traffico che passa per l'interfaccia di loopback



Qui siamo riusciti ad intercettare i pacchetti dell'interfaccia di loopback.



- **Intercettare i pacchetti tra Kali e Windows 7**

Andiamo a questo punto a effettuare il ping della macchina Windows 7 per generare traffico e andiamo a controllare la cattura dei pacchetti su Wireshark.

Time	Source	Destination	Protocol	Length	Info
5 1.216440105	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x7140, seq=9/2
6 1.216916633	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x7140, seq=9/2
7 2.047418503	PcsCompu_10:c3:bd	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.1
8 2.216950749	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x7140, seq=10/
9 2.217286029	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x7140, seq=10/
10 3.071846154	PcsCompu_10:c3:bd	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.1
11 3.231724062	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x7140, seq=11/
12 3.232188205	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x7140, seq=11/
13 4.095262791	PcsCompu_10:c3:bd	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.1
14 4.255533215	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x7140, seq=12/
15 4.256010610	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x7140, seq=12/
16 5.120356967	PcsCompu_10:c3:bd	Broadcast	ARP	42	Who has 192.168.50.1? Tell 192.168.50.1
17 5.255713805	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x7140, seq=13/
18 5.256404594	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x7140, seq=13/