



LABORATORIO VIRTUALE

FIREWALL, INETSIM & WIRESHARK

1

Sommario

Consegna esercizio.....	2
Requisiti e premesse	2
1. Configurazione di una policy sul firewall Windows 7	3
2. InetSim	4
3. Cattura di pacchetti con Wireshark.....	6



Consegna esercizio

1. *Configurare policy per permettere il ping da macchina Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall);*
2. *Utilizzo dell'utility InetSim per l'emulazione di servizi Internet;*
3. *Cattura di pacchetti con Wireshark;*

2

Requisiti e premesse

Come punto di partenza prendiamo le macchine virtuali del nostro laboratorio virtuale configurato nell'esercizio del M1 W1 D5, vedi precedente report.

Indirizzi IP statici del laboratorio virtuale:

192.168.50.1	Gateway
192.168.50.100	Kali Linux
192.168.50.101	Mestaploitable2
192.168.50.102	Windows 7

Partendo da questi requisiti proseguiamo con quanto sotto.

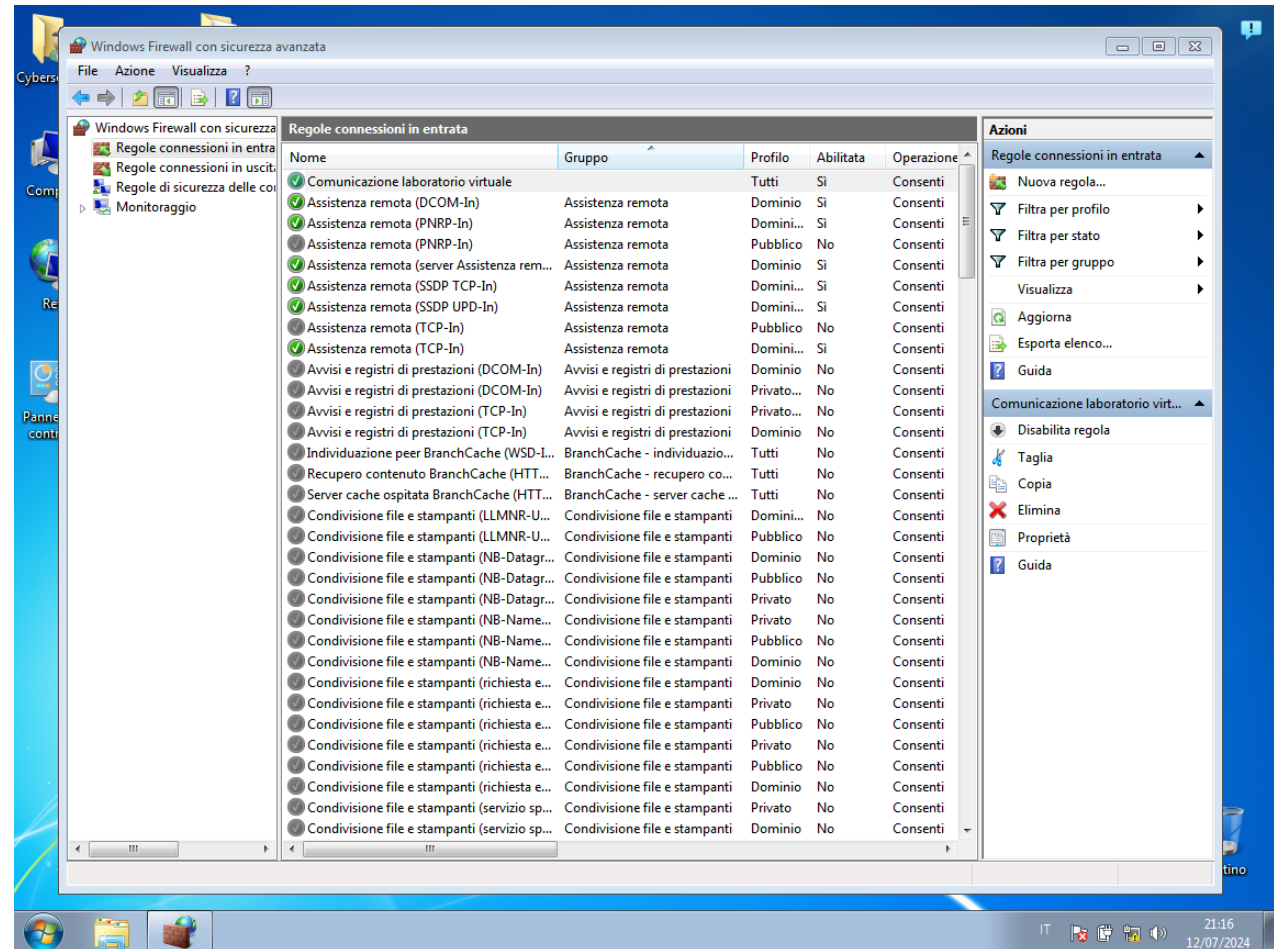


1. Configurazione di una policy sul firewall Windows 7

Configuriamo il Firewall di Windows cercando Firewall sul tasto di ricerca oppure da pannello di controllo > opzioni avanzate e aggiungiamo una nuova regola per le connessioni in entrata.

Per praticità e future implementazioni abbiamo configurato che tutti i client nella stessa rete locale possano effettuare un flusso in entrata.

Per cui “nuova regola” > “personalizzata” > “tutti i programmi” > “qualsiasi” su protocollo > “qualsiasi indirizzo IP” > “consenti connessione” > lasciato il resto invariato e abbiamo dato un nome come da screenshot sottostante.



Verifica con PING 192.168.50.102 da Kali Linux

```
(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=2.03 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.614 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.779 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.845 ms
^C
— 192.168.50.102 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.614/1.066/2.027/0.561 ms
```



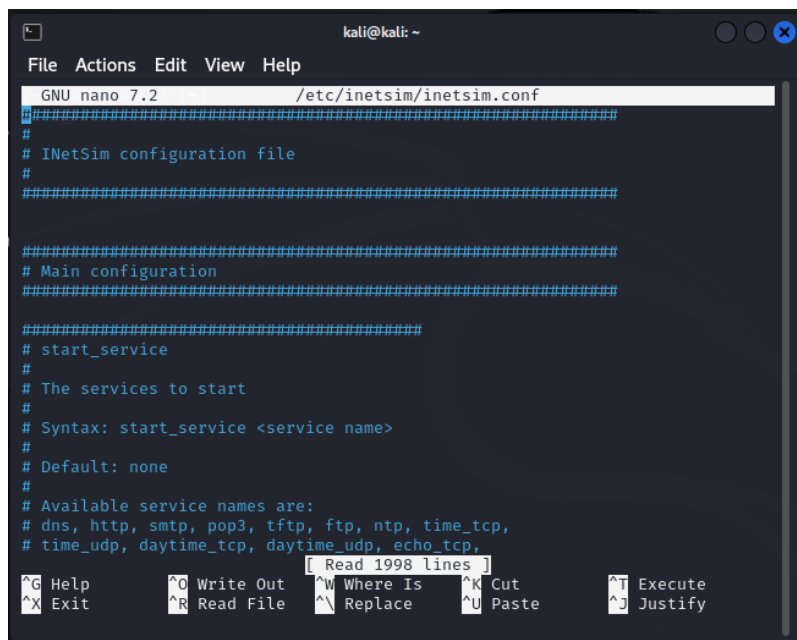
2. InetSim

su Kali Linux scarichiamo InetSim scrivendo sul terminale “sudo nano /etc/inetsim/inetsim.conf”
bisogna fare attenzione che su Kali Linux la tastiera di default ha il layout inglese e quindi lo slash “/” si trova dove c’è l’apostrofo della tastiera con layout italiano.

In caso di errori si aggiorna il sistema Kali, ma prima bisogna ripristinare in DHCP e dare connessione internet:

1. `sudo apt update && sudo apt upgrade -y`

2. `sudo apt install inetsim -y`

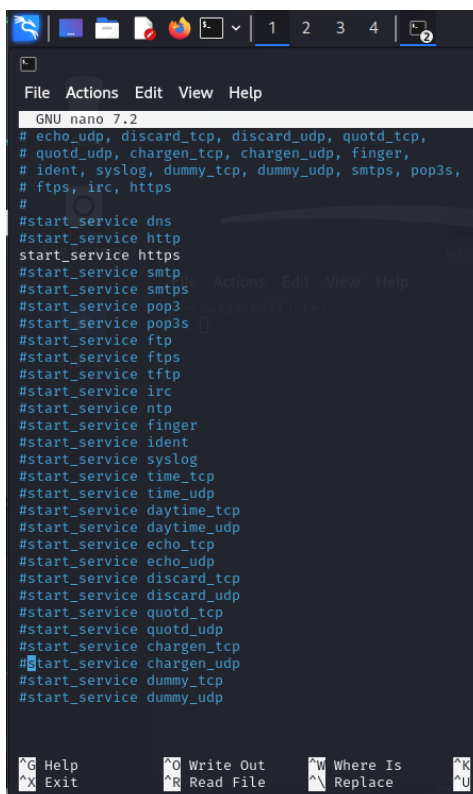


```
GNU nano 7.2 /etc/inetsim/inetsim.conf
#
# InetSim configuration file
#
#####

# 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 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
```

Aggiungiamo # cancelletto davanti a tutti, tranne HTTPS per evitare di iniziare gli altri servizi facendoli diventare un commento.



```
GNU nano 7.2
# 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 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
```



Cerchiamo il servizio “service_bind_address” e attiviamo il servizio modificando l’ip di KALI

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

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

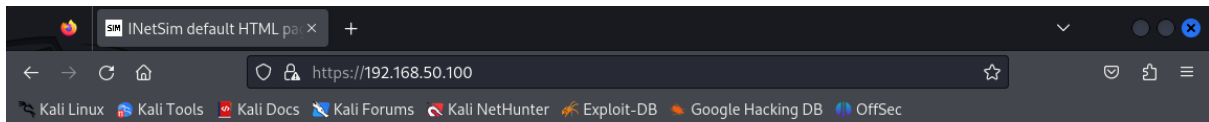
^G Help      ^O Write Out
^X Exit      ^R Read File
            ^W Where Is
            ^\ Replace
```

5

Salviamo con CTRL+O, ENTER e CTRL+X, ENTER

Avviamo inetsim con terminale “sudo inetsim”


Poi ci rechiamo sul browser Mozilla in questo caso IP al link <https://192.168.50.100>



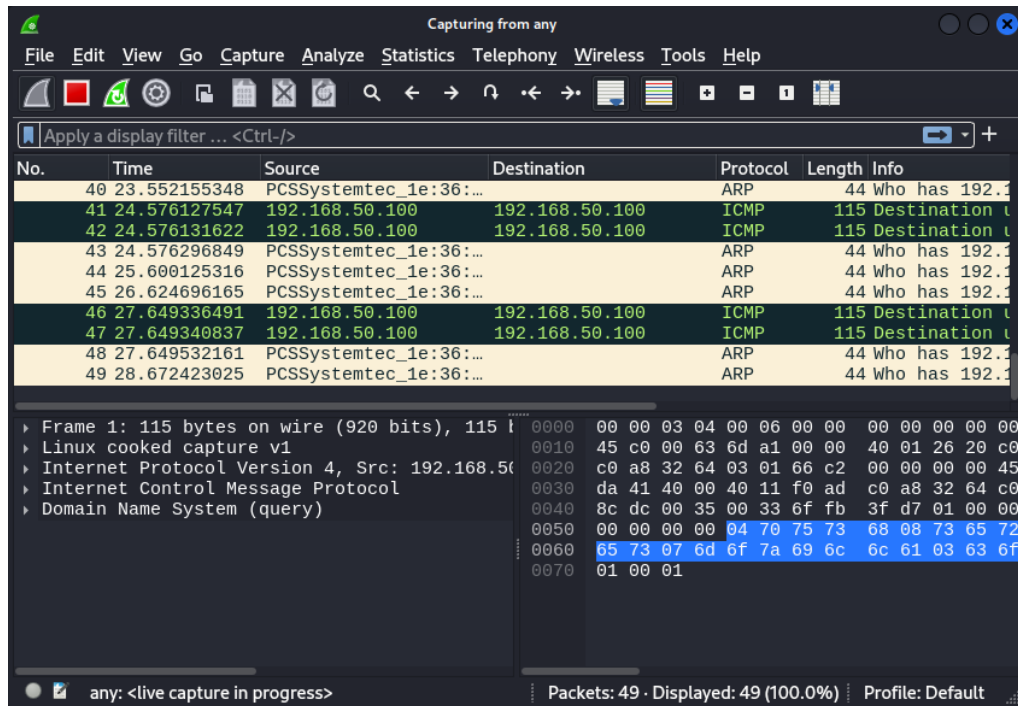
This is the default HTML page for INetSim HTTP server fake mode.
This file is an HTML document.



3. Cattura di pacchetti con Wireshark

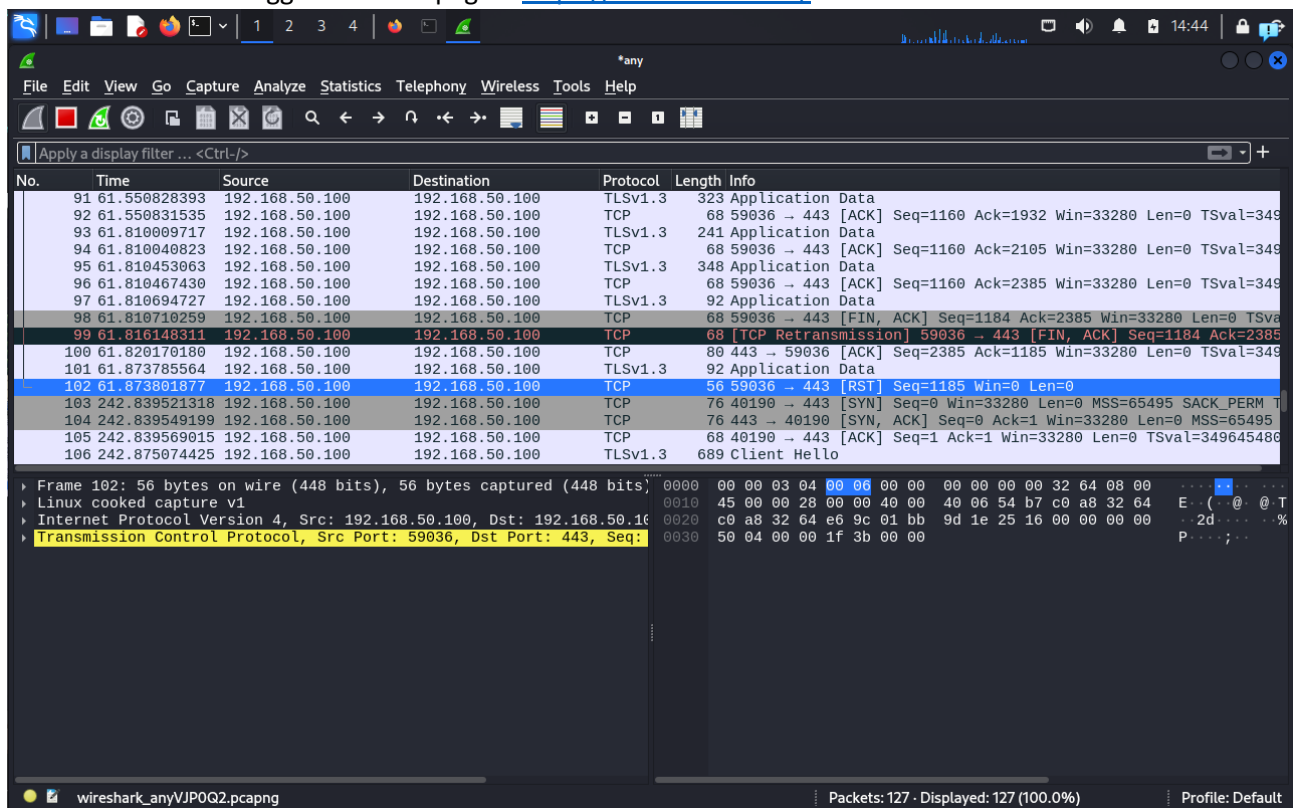
Apriamo Wireshark mettiamo su “any” e avvia la cattura con la pinna. 

Ecco il risultato



6

Torniamo su Mozilla aggiorniamo la pagina <https://192.168.50.100/>



Pacchetti catturati, a maggior conferma, troviamo sul protocollo TCP il SYN, SYN/ACK e ACK.