

EPICODE

ESERCIZIO W3D4

Esercizio:

- Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall)
- Utilizzo dell'utility InetSim per l'emulazione di servizi Internet
- Cattura di pacchetti con Wireshark

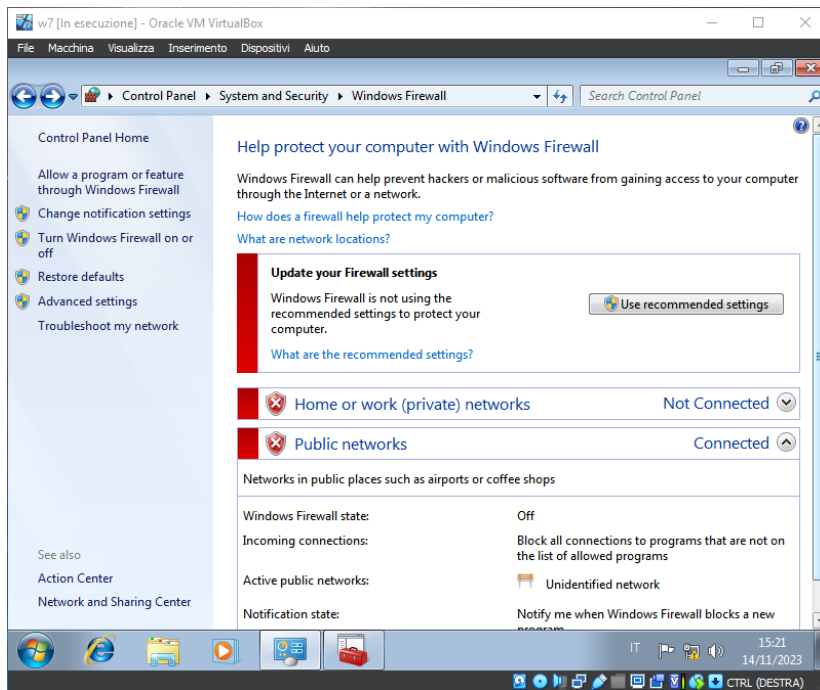
Prendiamo in considerazione il nostro laboratorio, creato nelle lezioni precedenti, composto da:

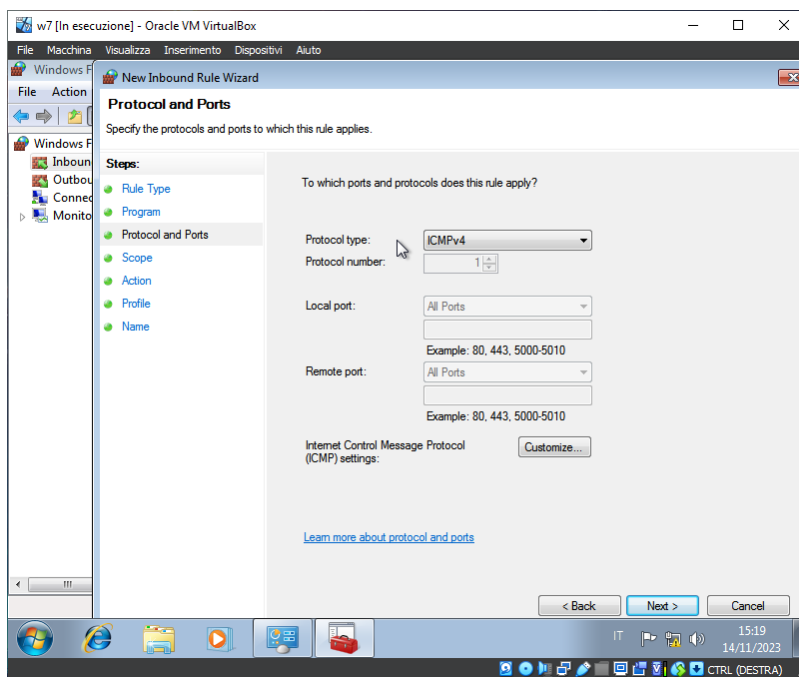
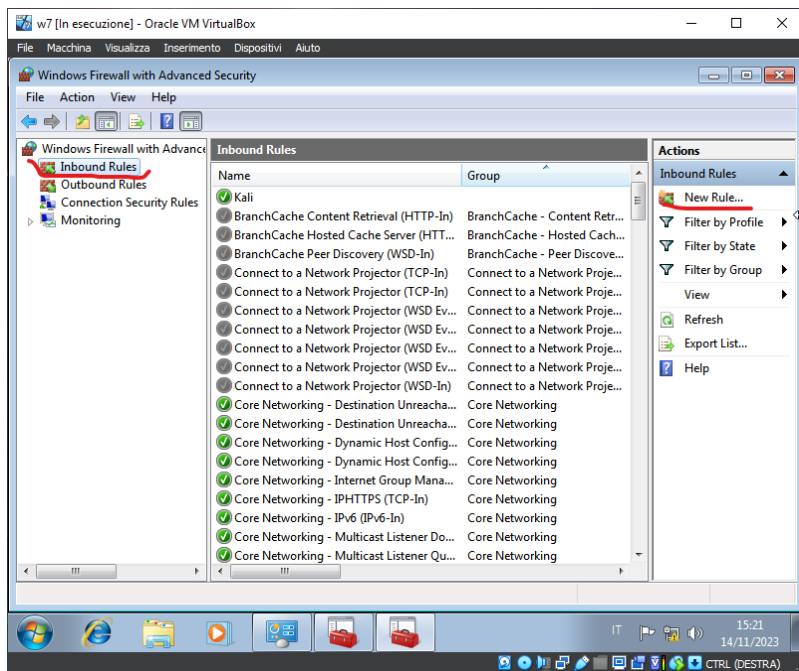
- ☐ Kali Linux, con IP 192.168.50.100
- ☐ Windows 7, con IP 192.168.50.102
- ☐ Metasploitable, con IP 192.168.50.101

1. Configurazione policy firewall Win7

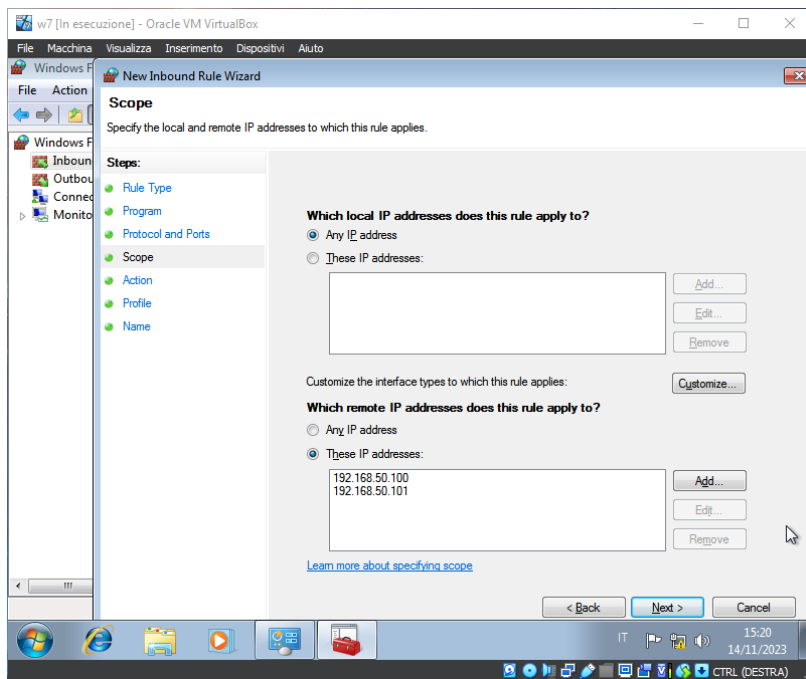
Il percorso da seguire è il seguente:

- A. Control panel
- B. System and security
- C. Windows Firewall
- D. Advanced settings
- E. Inbound rules
- F. New rule

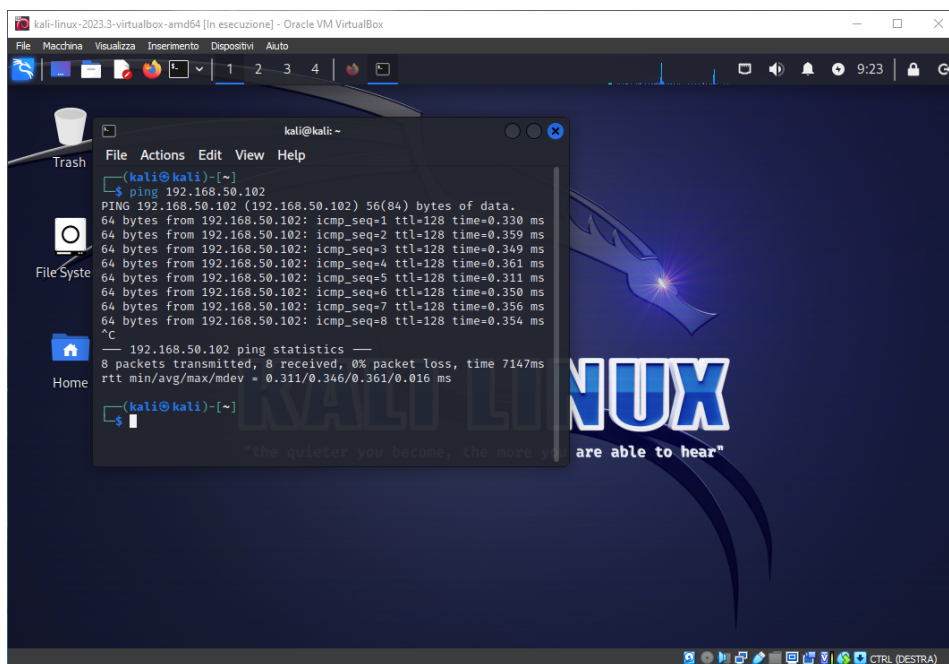




In <Scope> Aggiungere gli IP di Kali Linux e Metasploitable negli IP Remoti:



dopo aver impostato il tutto apriamo Kali Linux e proviamo il ping verso verso Win7

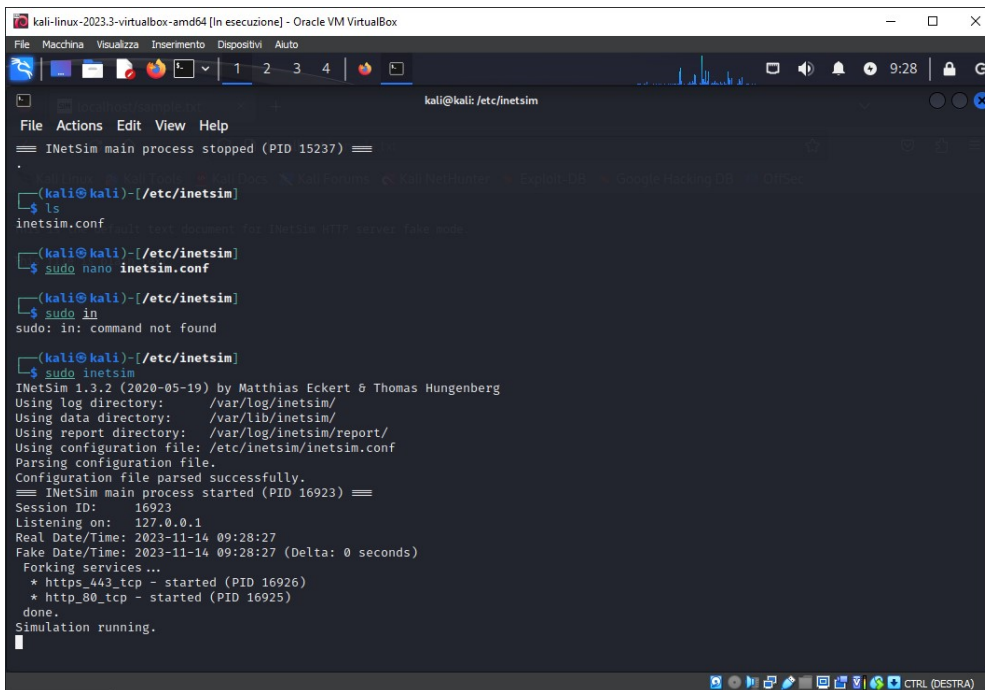


2. INETSIM

Inetsim è un pacchetto che ci permette di simulare degli scambi in rete in un ambiente di laboratorio;

Configurazione su Kali:

- ☐ `cd /etc/inetsim`
- ☐ `ls (inetsim.conf)`
- ☐ `sudo nano inetsim.conf` *[aperto il testo bisogna commentare inserendo # tutte le voci eccetto HTTP e/o HTTPS]*
- ☐ `sudo inetsim`



```
kali@kali: /etc/inetsim
File Actions Edit View Help
== INetSim main process stopped (PID 15237) ==
.
(kali@kali)-[/etc/inetsim]
$ ls
inetsim.conf
(kali@kali)-[/etc/inetsim]
$ sudo nano inetsim.conf
(kali@kali)-[/etc/inetsim]
$ sudo in
sudo: in: command not found
(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 16923) ==
Session ID: 16923
Listening on: 127.0.0.1
Real Date/Time: 2023-11-14 09:28:27
Fake Date/Time: 2023-11-14 09:28:27 (Delta: 0 seconds)
Forking services...
* https_443_tcp - started (PID 16926)
* http_80_tcp - started (PID 16925)
done.
Simulation running.
```

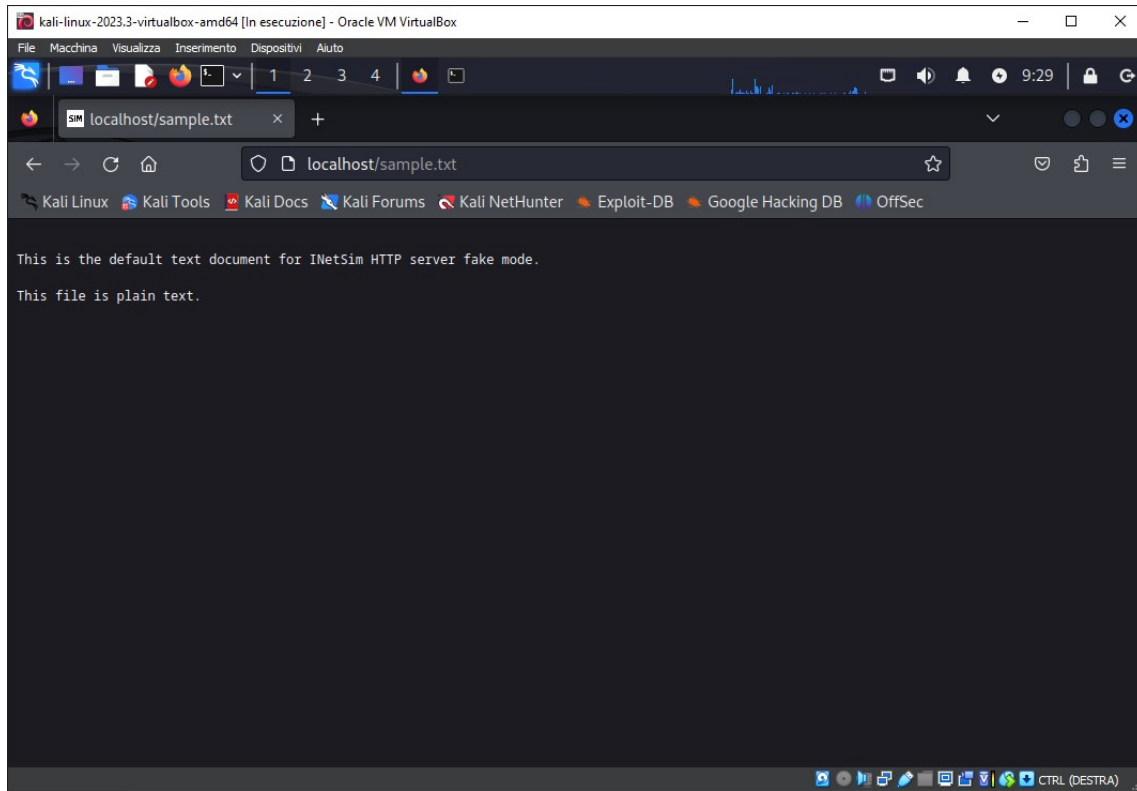
```
kali@kali: /etc/inetsim
GNU nano 7.2 inetsim.conf *
#start_service discard_udp
#start_service quotd_tcp
#start_service quotd_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp

# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
# service_bind_address 127.0.0.1
#
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#
# Default: inetsim
#
```

```
kali@kali: /etc/inetsim
GNU nano 7.2 inetsim.conf
#
#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
```

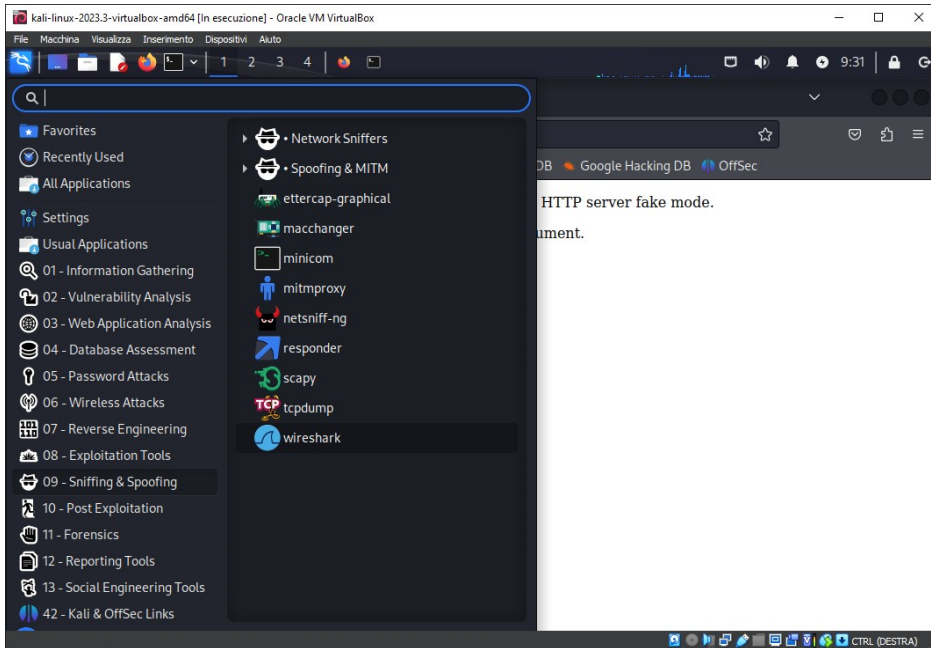
al termine per salvare le modifiche andiamo a premere la combinazione di tasti "ctrl(sx)+x", confermiamo con "Y" ed infine il tasto Invio.

Impostando tutto correttamente, apriamo Firefox, inseriamo nella barra di ricerca ["http://localhost/sample.txt"](http://localhost/sample.txt)

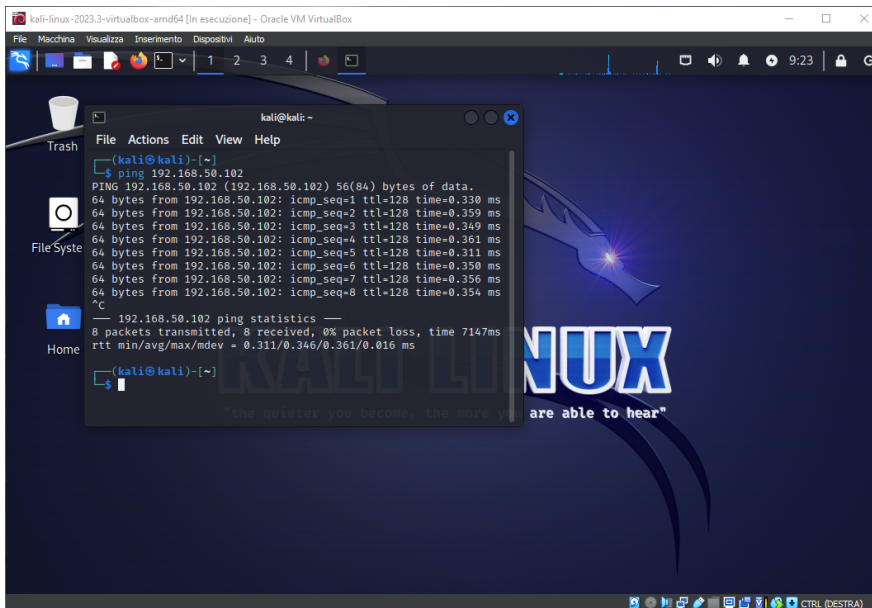


3. Wireshark

Sempre su Linux apriamo Wireshark, quindi andiamo nel menù delle applicazioni, apriamo la voce **"09 - Sniffing & Spoofing"**, e in fondo troviamo Wireshark



quindi apriamo il terminale e digitiamo il ping di win7 192.168.50.102



avviamo Wireshark, selezioniamo l'interfaccia e vediamo il traffico di pacchetti ICMP tra le due macchine

