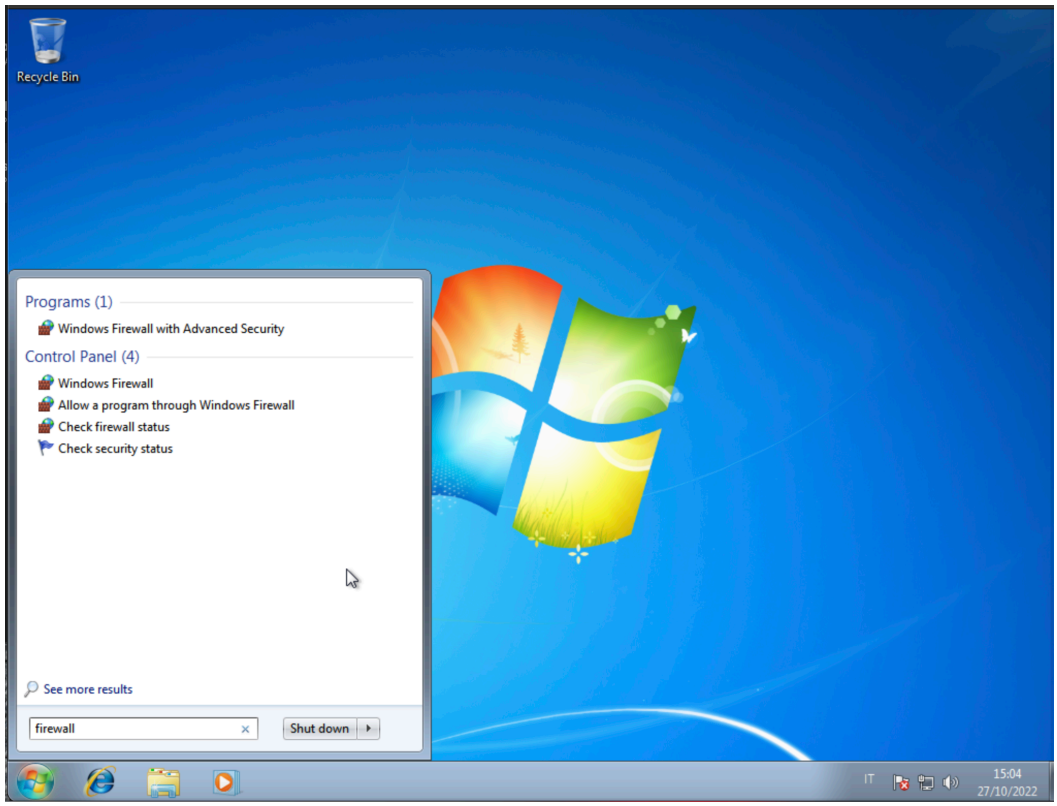
# CONFIGURAZIONE FIREWALL E APPLICATIVI

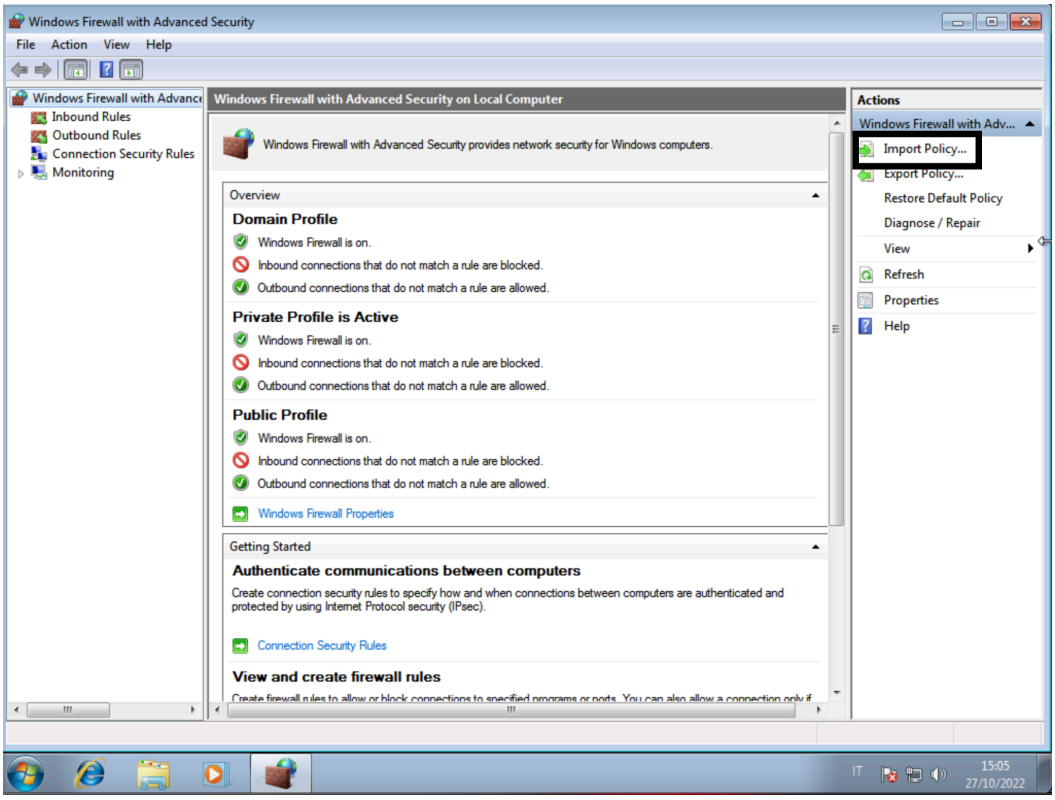
L'esercizio di oggi prevede:

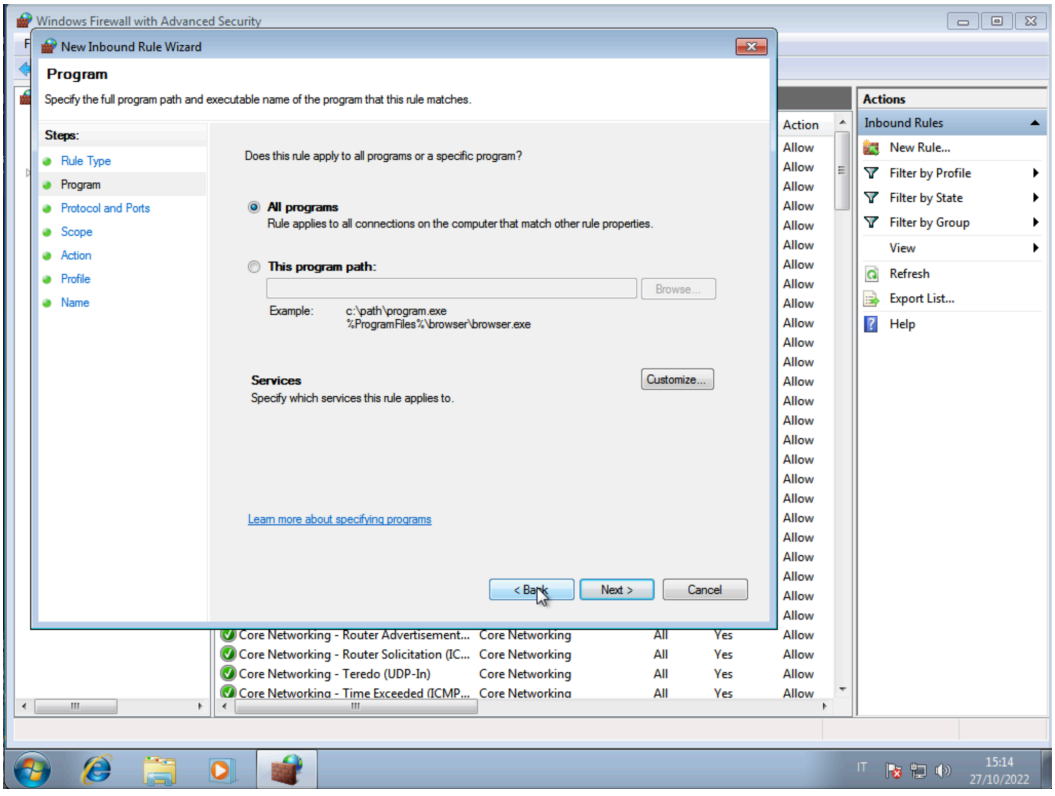
1. La configurazione manuale del firewall di windows per poter effettuare ping attraverso la macchina virtuale tra Kali Linux e Windows 7.
2. L'utilizzo dell'utility Inetsim
3. Cattura di pacchetti con Wireshark

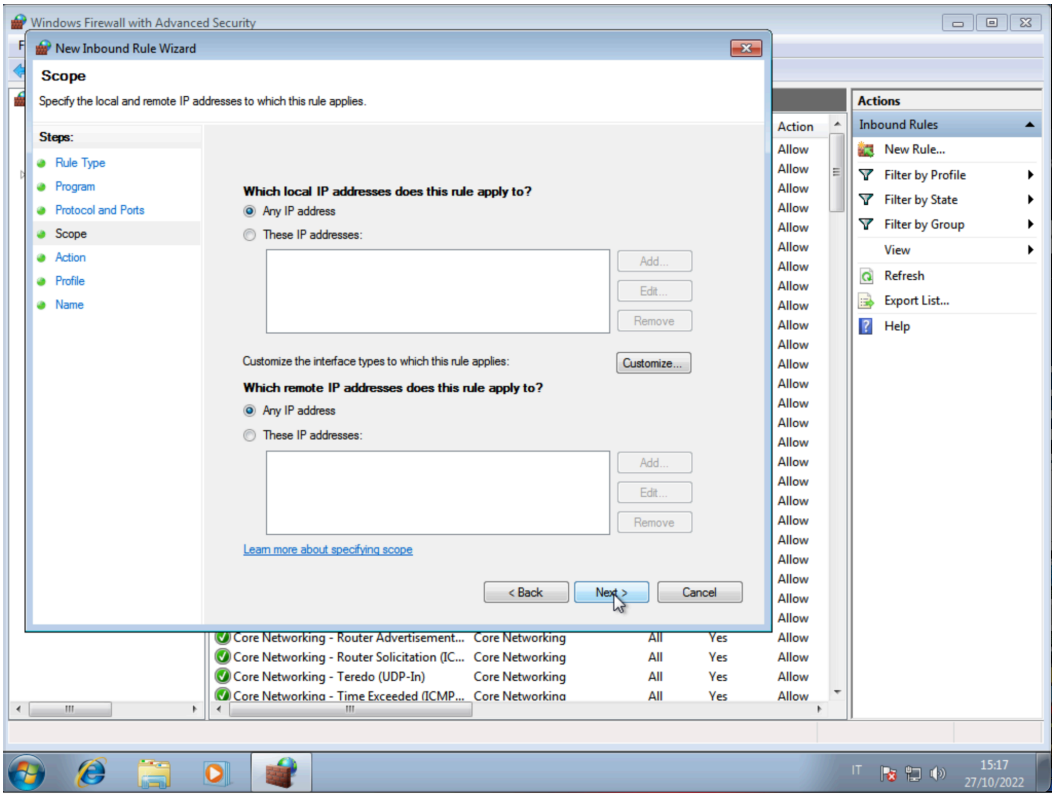
- Per prima cosa procediamo col primo esercizio che prevede di aprire il firewall sulla ricerca dei programmi e file di windows.

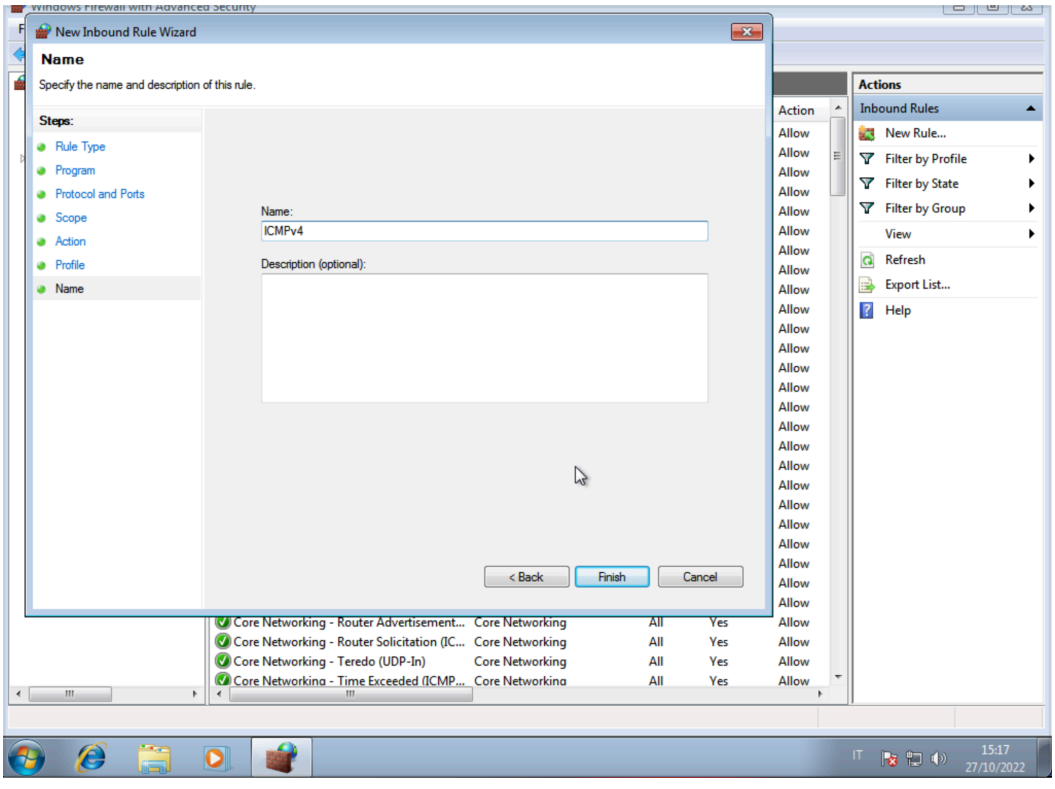


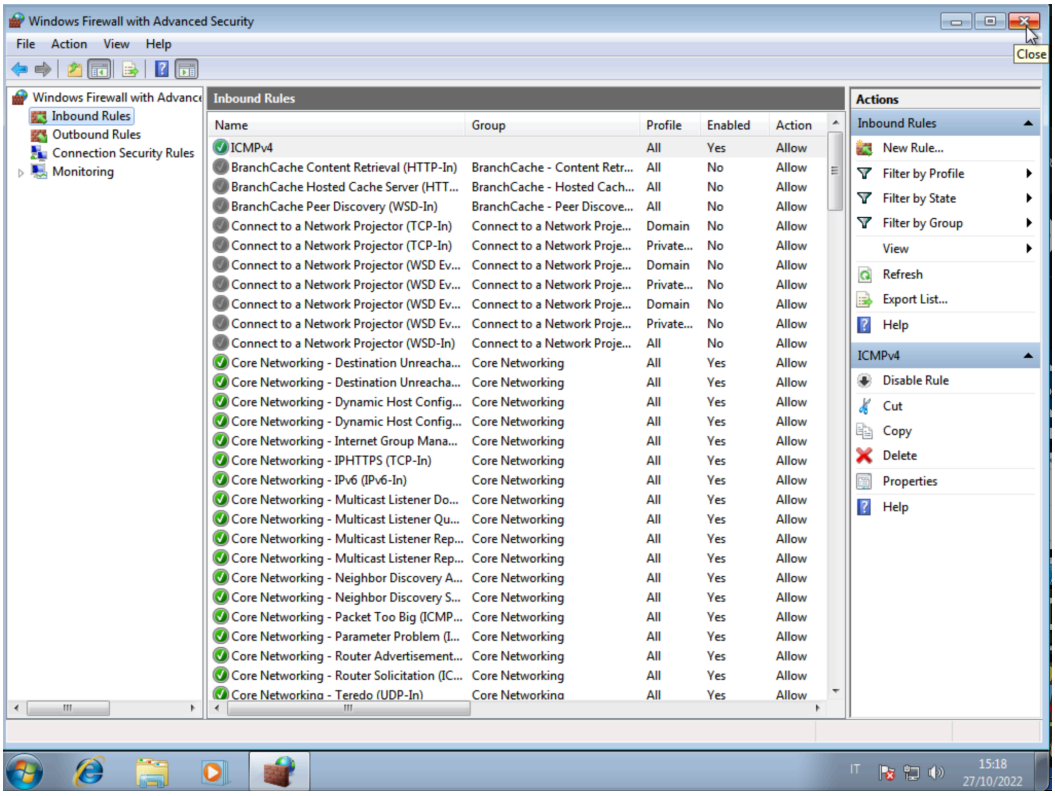

- Una volta all'interno cliccare su import policy e applicare modifiche.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Actions
Windows Firewall with Adv...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
IT
15:05
27/10/2022


Windows Firewall with Advanced Security
New Inbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
Browse...
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
Services
Specify which services this rule applies to.
Customize...
Learn more about specifying programs
< Back
Next >
Cancel
Action
Allow
Core Networking - Router Advertisement...
Core Networking - Router Solicitation (IC...
Core Networking - Teredo (UDP-In)
Core Networking - Time Exceeded (ICMP...
Core Networking
All
Yes
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
IT
15:14
27/10/2022


Windows Firewall with Advanced Security
New Inbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
Customize the interface types to which this rule applies:
Customize...
Which remote IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
Learn more about specifying scope
< Back
Next >
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Action
Allow
Core Networking - Router Advertisement...
Core Networking - Router Solicitation (IC...
Core Networking - Teredo (UDP-In)
Core Networking - Time Exceeded (ICMP...
Core Networking
All
Yes
IT
15:17
27/10/2022


New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Name:
ICMPv4
Description (optional):
< Back
Finish
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Action
Allow
Core Networking - Router Advertisement...
Core Networking - Router Solicitation (IC...
Core Networking - Teredo (UDP-In)
Core Networking - Time Exceeded (ICMP...
Core Networking
All
Yes
IT
15:17
27/10/2022



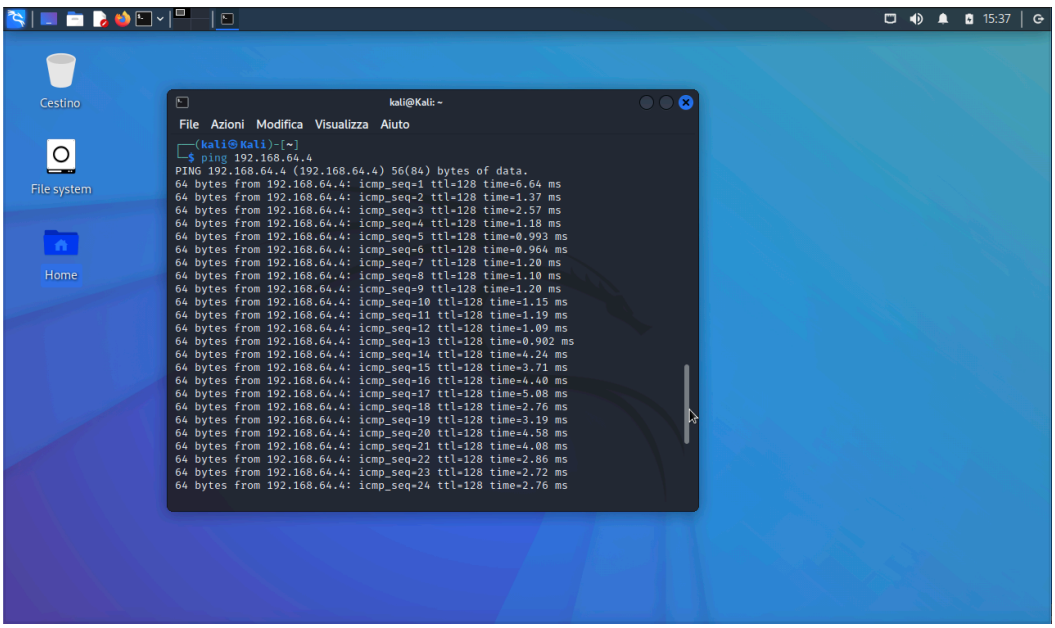

- Abilitare la connessione con tutti i pc e configurare il tutto creando un indirizzo ICMPv4 in modo da poter effettuare un ping con Kali Linux.

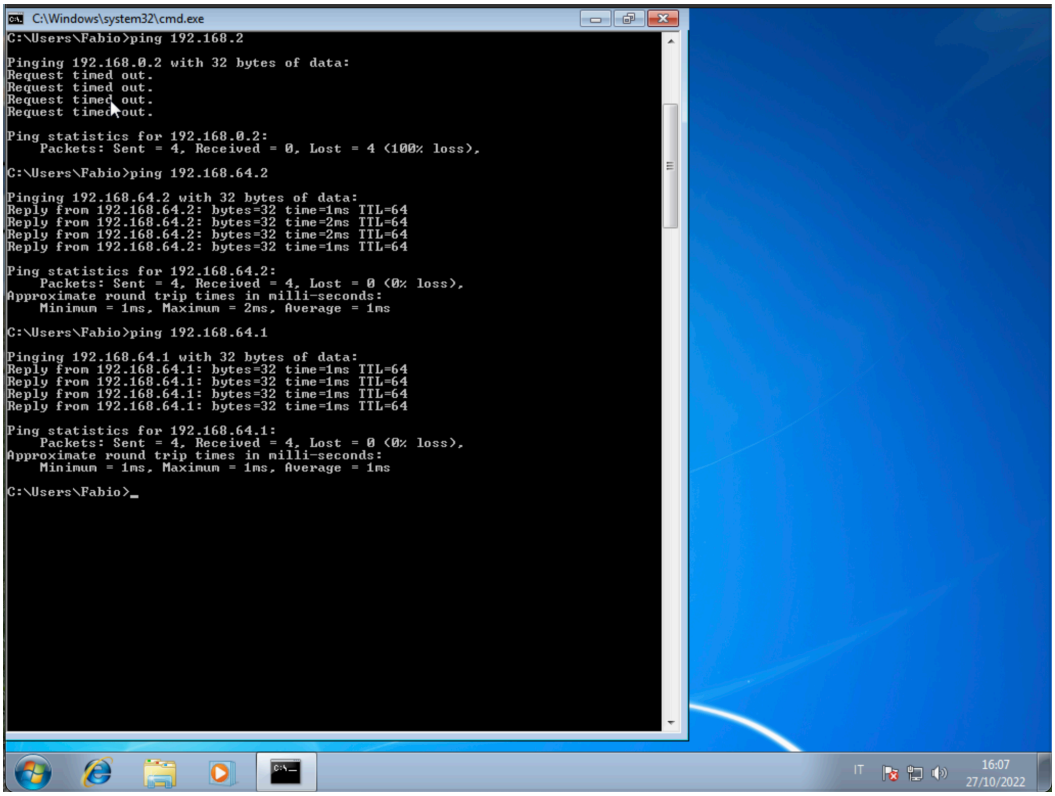
Compiuti questi passaggi provare a connettere i vari dispositivi virtuali attraverso gli indirizzi IP dedicati.

*Ps. Gli indirizzi IP sono consultabili nella zona comandi con indirizzi:

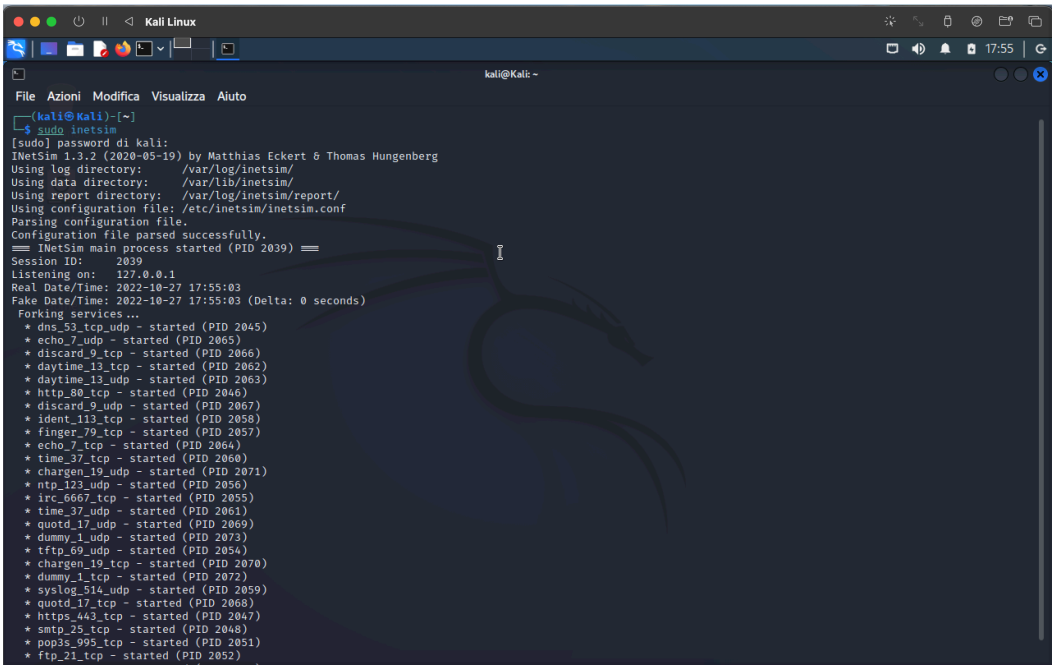
.Kali linux"ifconfig

.Windows "ip configuration"

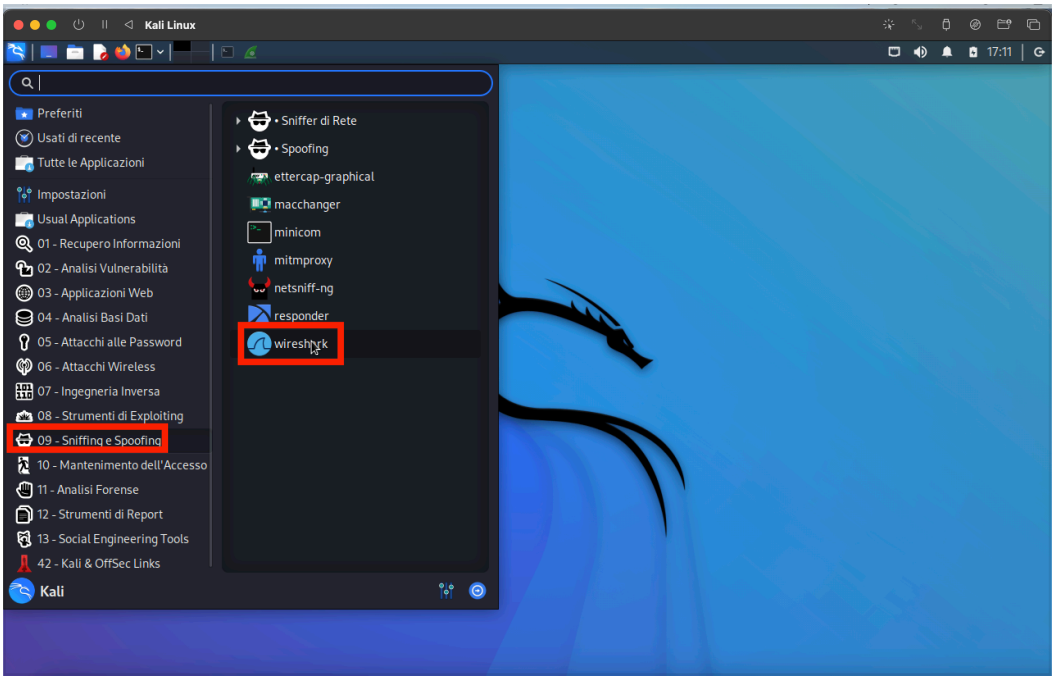


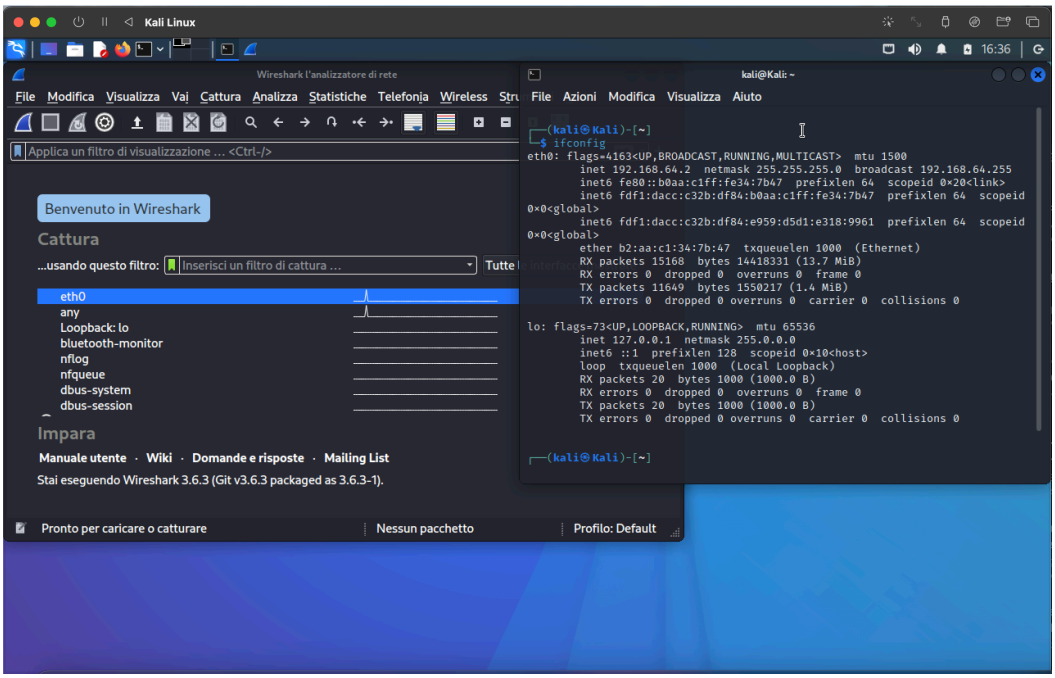


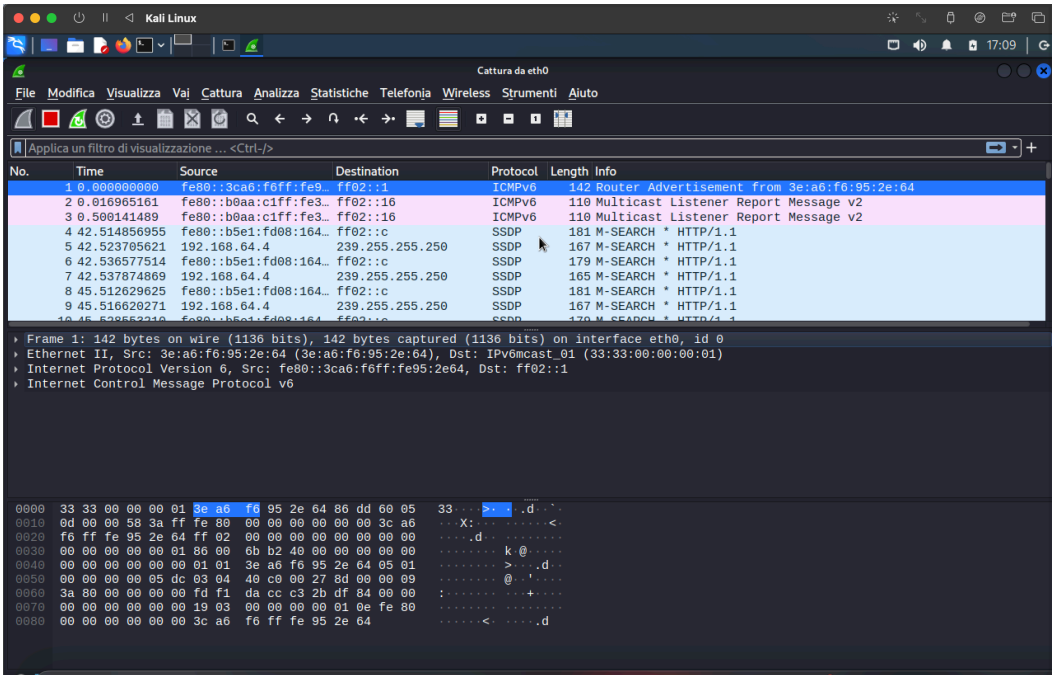

Per simulare un collegamento a Inetsim bisogna effettuare l'accesso a Kali e digitare nei comandi "sudo inetsim" cosi da simulare un accesso al sito come illustrato nell'immagine.




- Per quanto riguarda l'applicativo di Wireshark ci viene fornito di default da Kali Linux. Per poter controllare lo stato dei pacchetti in entrata e in uscita, andare nella sezione dedicata come illustrato nelle immagini.


Kali Linux
17:11
Preferiti
Usati di recente
Tutte le Applicazioni
Impostazioni
Usual Applications
01 - Recupero Informazioni
02 - Analisi Vulnerabilità
03 - Applicazioni Web
04 - Analisi Basi Dati
05 - Attacchi alle Password
06 - Attacchi Wireless
07 - Ingegneria Inversa
08 - Strumenti di Exploiting
09 - Sniffing e Spoofing
10 - Mantenimento dell'Accesso
11 - Analisi Forense
12 - Strumenti di Report
13 - Social Engineering Tools
42 - Kali & OffSec Links
Kali
• Sniffer di Rete
• Spoofing
ettercap-graphical
macchanger
minicom
mitmproxy
netsniff-ng
responder
wireshark


Kali Linux
16:36
Wireshark l'analizzatore di rete
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless
Applica un filtro di visualizzazione … <Ctrl-/>
Benvenuto in Wireshark
Cattura
…usando questo filtro: Inserisci un filtro di cattura …
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Impara
Manuale utente · Wiki · Domande e risposte · Mailing List
Stai eseguendo Wireshark 3.6.3 (Git v3.6.3 packaged as 3.6.3-1).
Pronto per caricare o catturare
Nessun pacchetto
Profilo: Default
kali@Kali: ~
File Azioni Modifica Visualizza Aiuto
(kali㉿Kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.64.2 netmask 255.255.255.0 broadcast 192.168.64.255
inet6 fe80::b0aa:c1ff:fe34:7b47 prefixlen 64 scopeid 0×20<link>
inet6 fdf1:dacc:c32b:df84:b0aa:c1ff:fe34:7b47 prefixlen 64 scopeid 0×0<global>
inet6 fdf1:dacc:c32b:df84:e959:d5d1:e318:9961 prefixlen 64 scopeid 0×0<global>
ether b2:aa:c1:34:7b:47 txqueuelen 1000 (Ethernet)
RX packets 15168 bytes 14418331 (13.7 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 11649 bytes 1550217 (1.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 20 bytes 1000 (1000.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20 bytes 1000 (1000.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿Kali)-[~]


Kali Linux
17:09
Cattura da eth0
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 fe80::3ca6:f6ff:fe9… ff02::1 ICMPv6 142 Router Advertisement from 3e:a6:f6:95:2e:64
2 0.016965161 fe80::b0aa:c1ff:fe3… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
3 0.500141489 fe80::b0aa:c1ff:fe3… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
4 42.514856955 fe80::b5e1:fd08:164… ff02::c SSDP 181 M-SEARCH * HTTP/1.1
5 42.523705621 192.168.64.4 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
6 42.536577514 fe80::b5e1:fd08:164… ff02::c SSDP 179 M-SEARCH * HTTP/1.1
7 42.537874869 192.168.64.4 239.255.255.250 SSDP 165 M-SEARCH * HTTP/1.1
8 45.512629625 fe80::b5e1:fd08:164… ff02::c SSDP 181 M-SEARCH * HTTP/1.1
9 45.516620271 192.168.64.4 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
Frame 1: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface eth0, id 0
Ethernet II, Src: 3e:a6:f6:95:2e:64 (3e:a6:f6:95:2e:64), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::3ca6:f6ff:fe95:2e64, Dst: ff02::1
Internet Control Message Protocol v6
0000 33 33 00 00 00 01 3e a6 f6 95 2e 64 86 dd 60 05
0010 0d 00 00 58 3a ff fe 80 00 00 00 00 00 00 3c a6
0020 f6 ff fe 95 2e 64 ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 01 86 00 6b b2 40 00 00 00 00 00
0040 00 00 00 00 00 00 01 01 3e a6 f6 95 2e 64 05 01
0050 00 00 00 00 05 dc 03 04 40 c0 00 27 8d 00 00 09
0060 3a 80 00 00 00 00 fd f1 da cc c3 2b df 84 00 00
0070 00 00 00 00 00 00 19 03 00 00 00 00 01 0e fe 80
0080 00 00 00 00 00 00 3c a6 f6 ff fe 95 2e 64