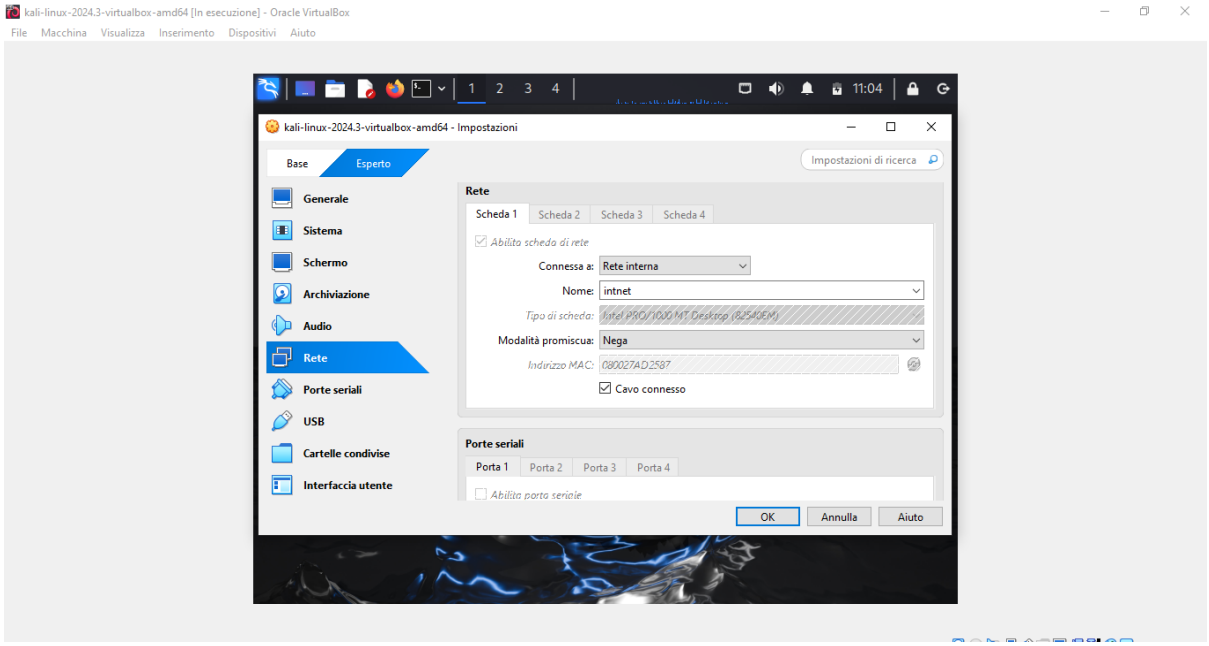
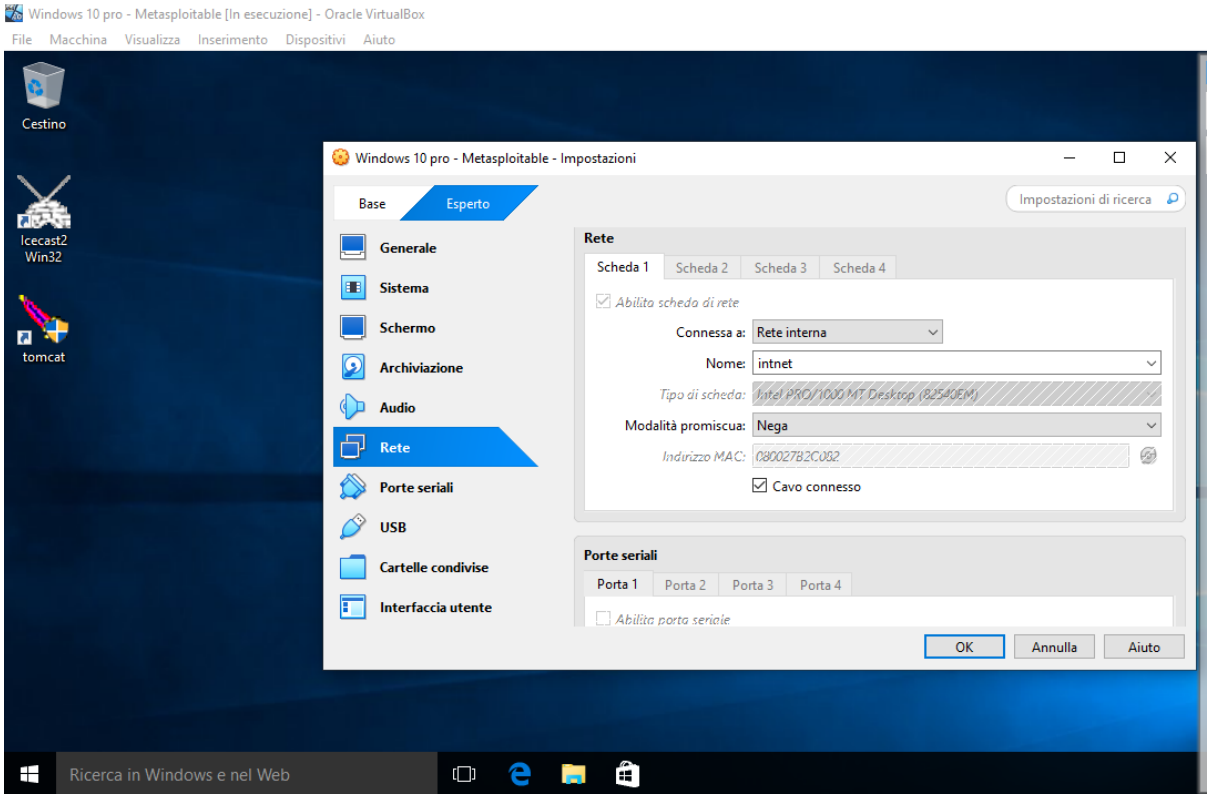
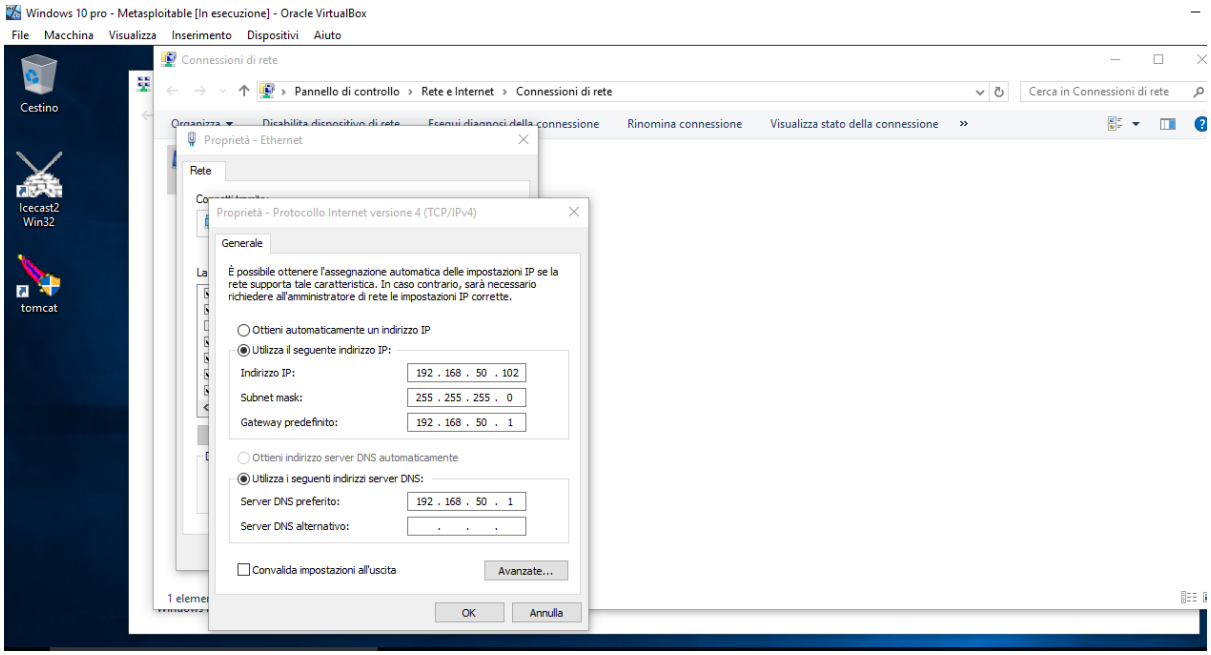
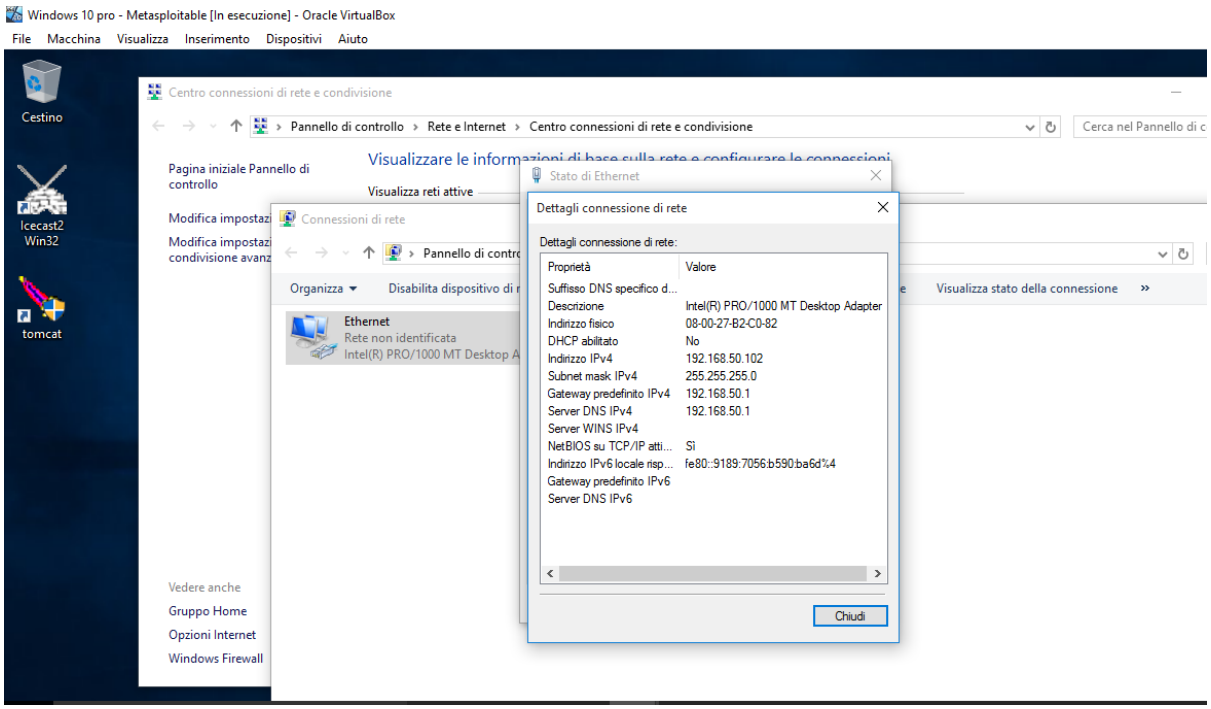
Affinché le due VM Kali e Windows 10 si possano collegare è necessario che stiano sulla medesima rete, quindi il primo controllo da effettuare è appunto la rete





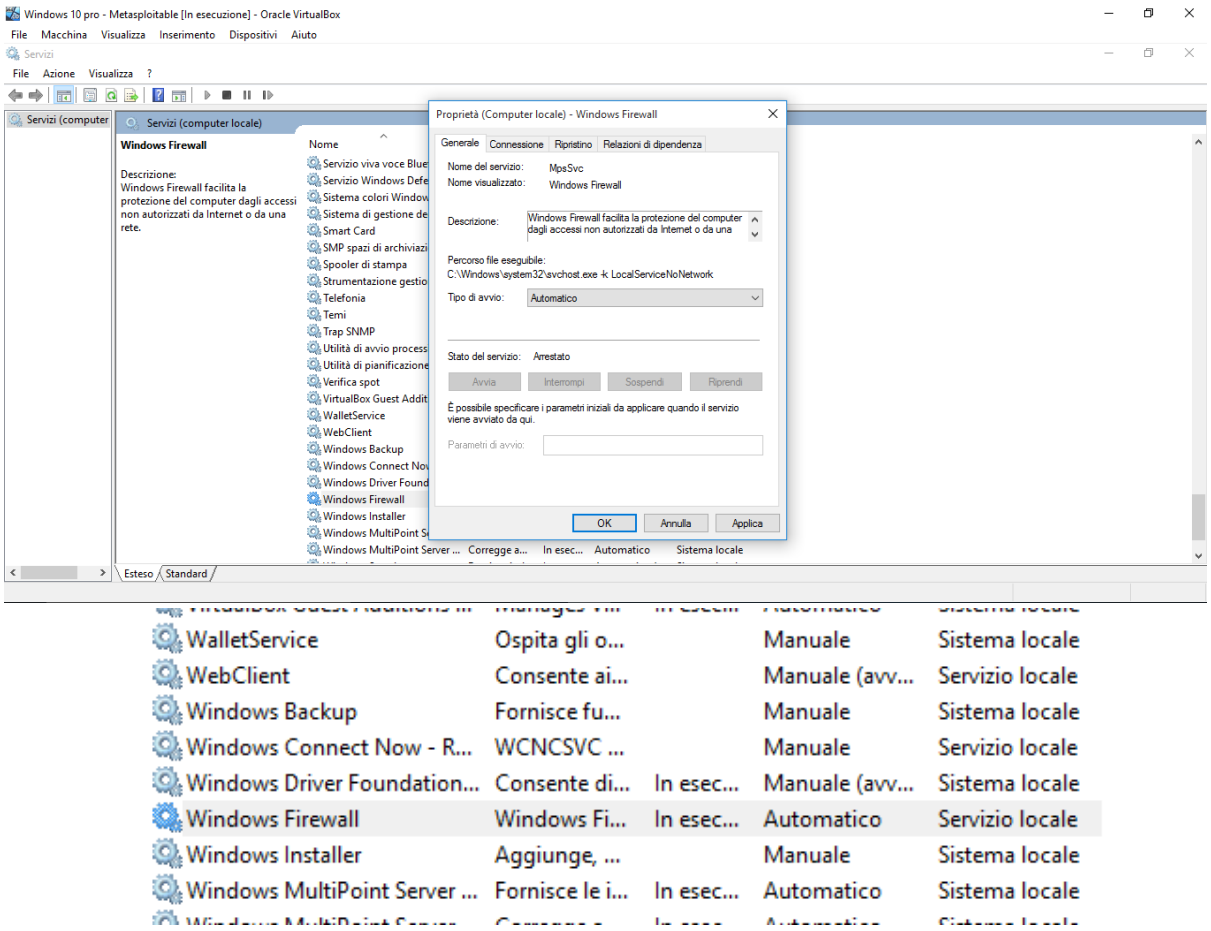
Il windows firewall è disabilitato quindi dal pannello di controllo inanzitutto inseriamo indirizzo IP



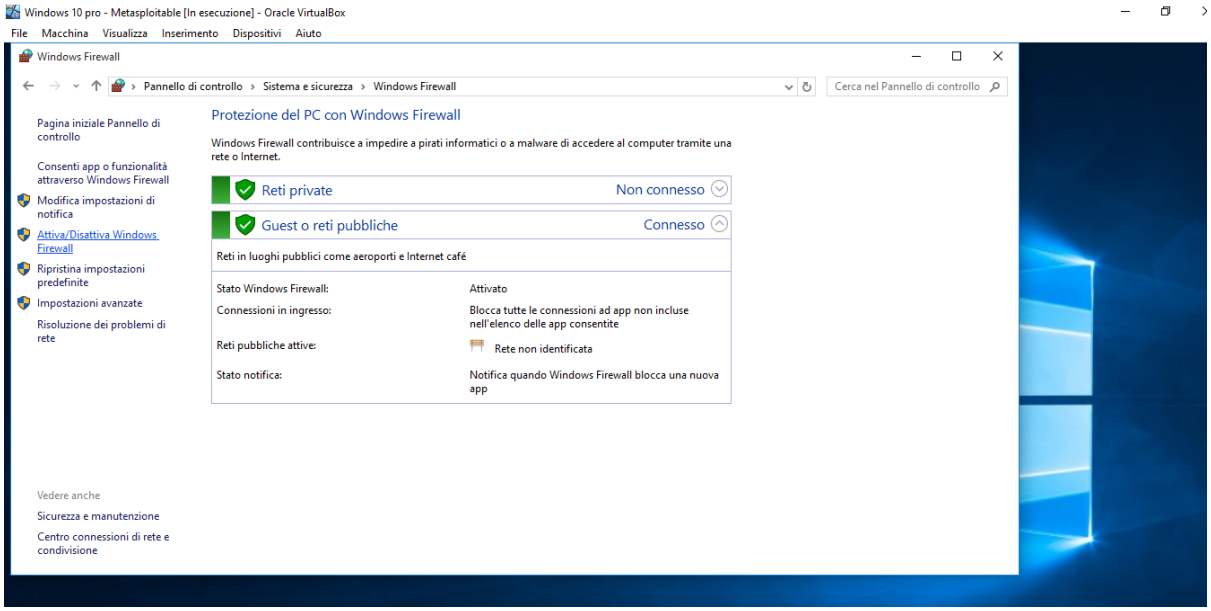


Ora che la scheda è stata configurata dobbiamo abilitare il windows firewall

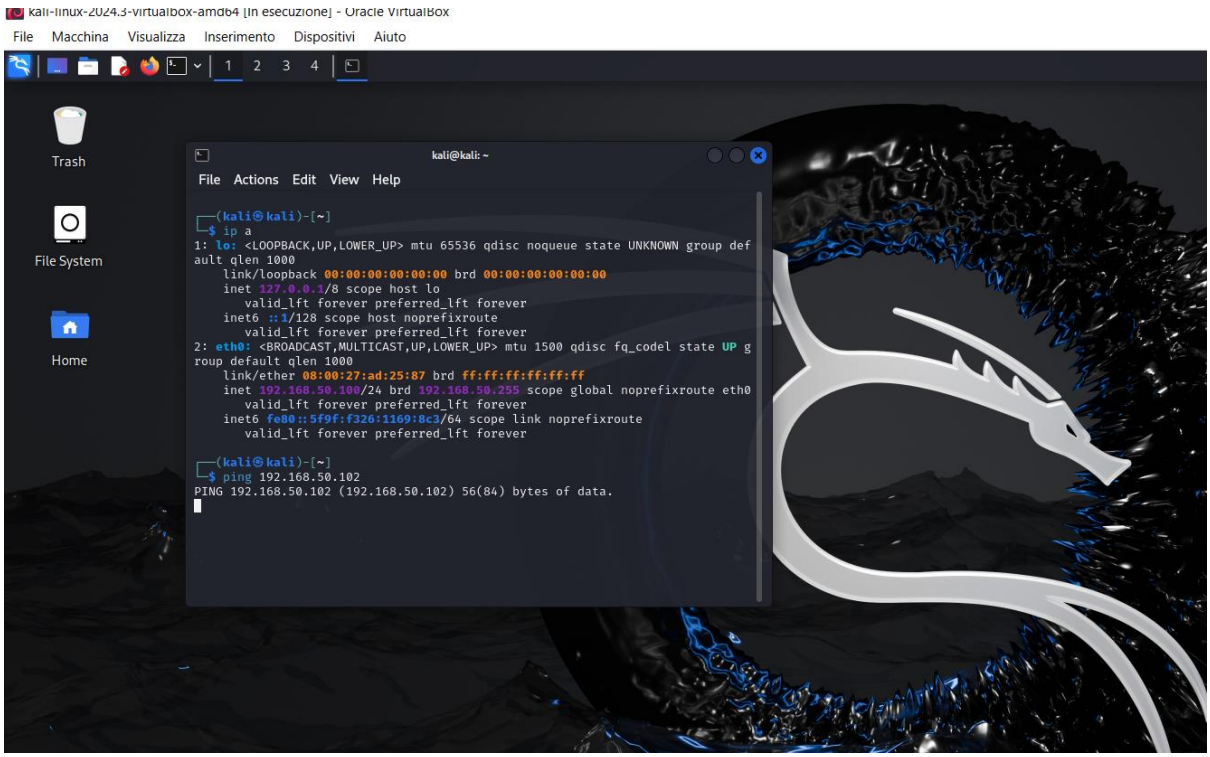
Dai servizi va avviato il windows firewall quindi imposto la tipologia di avvio su automatico e a seguito eseguo l'avvio



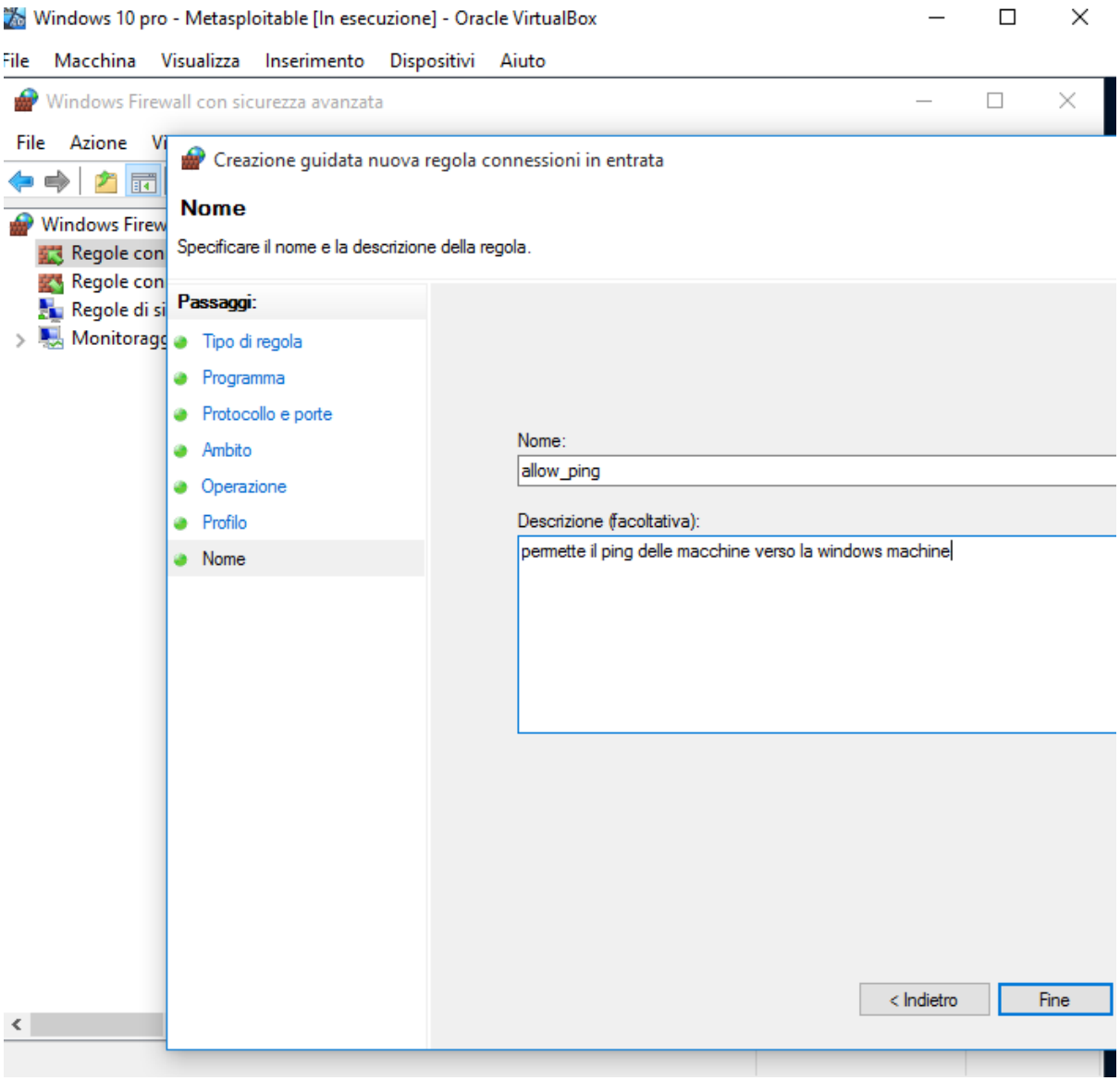
Dal pannello di controllo uso le impostazioni consigliate per connettere il firewall



Ping da Kali

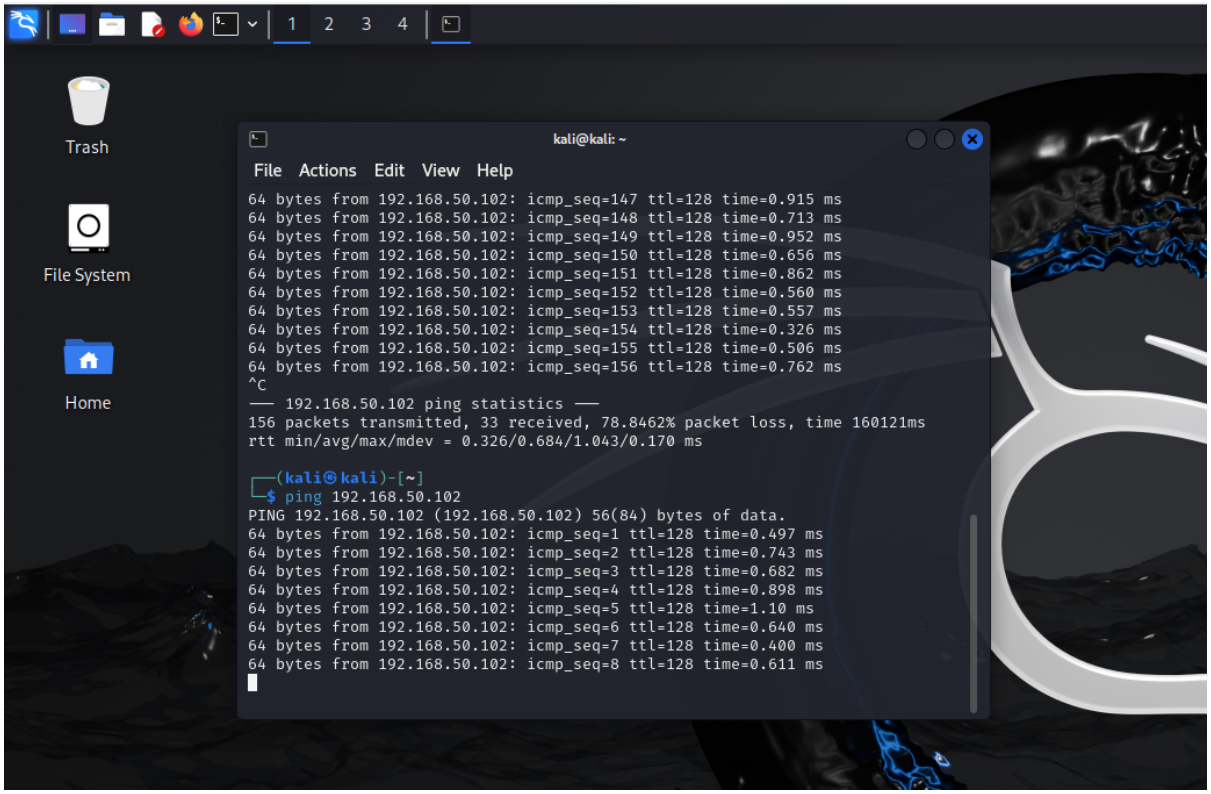


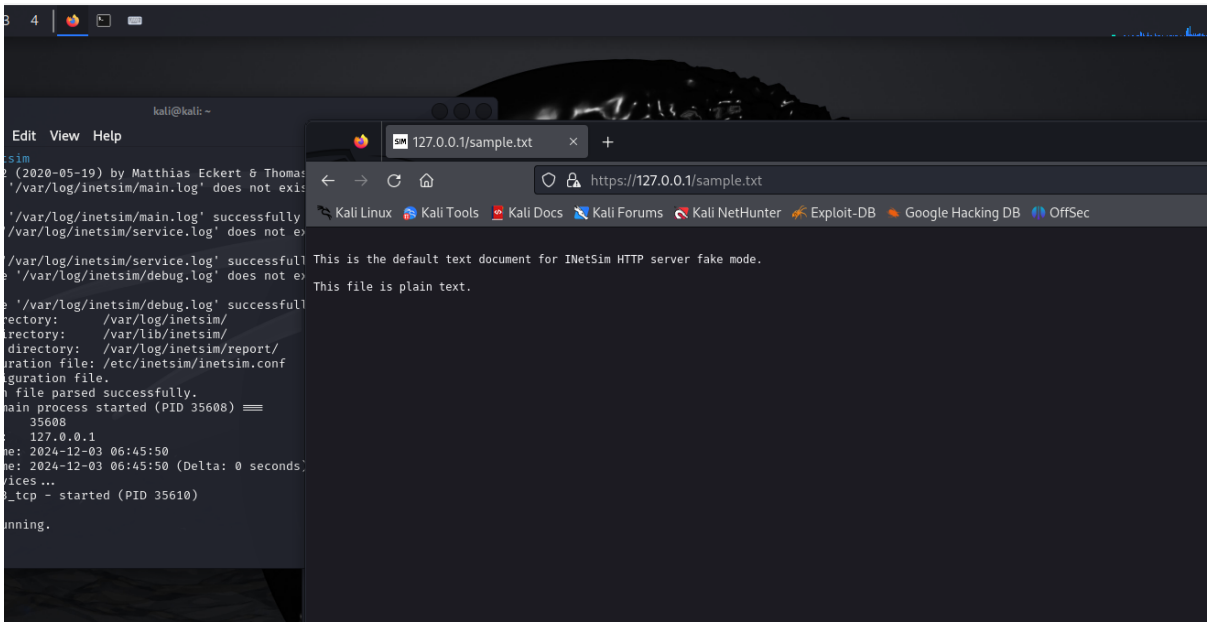
A seguito dell’attivazione del firewall devo andare a configurarlo inserendo la regola


Windows 10 pro - Metasploitable [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Windows Firewall con sicurezza avanzata
File Azione
Creazione guidata nuova regola connessioni in entrata
Nome
Specificare il nome e la descrizione della regola.
Passaggi:
Tipo di regola
Programma
Protocollo e porte
Ambito
Operazione
Profilo
Nome
Nome:
allow_ping
Descrizione (facoltativa):
permette il ping delle macchine verso la windows machine
< Indietro
Fine

kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox

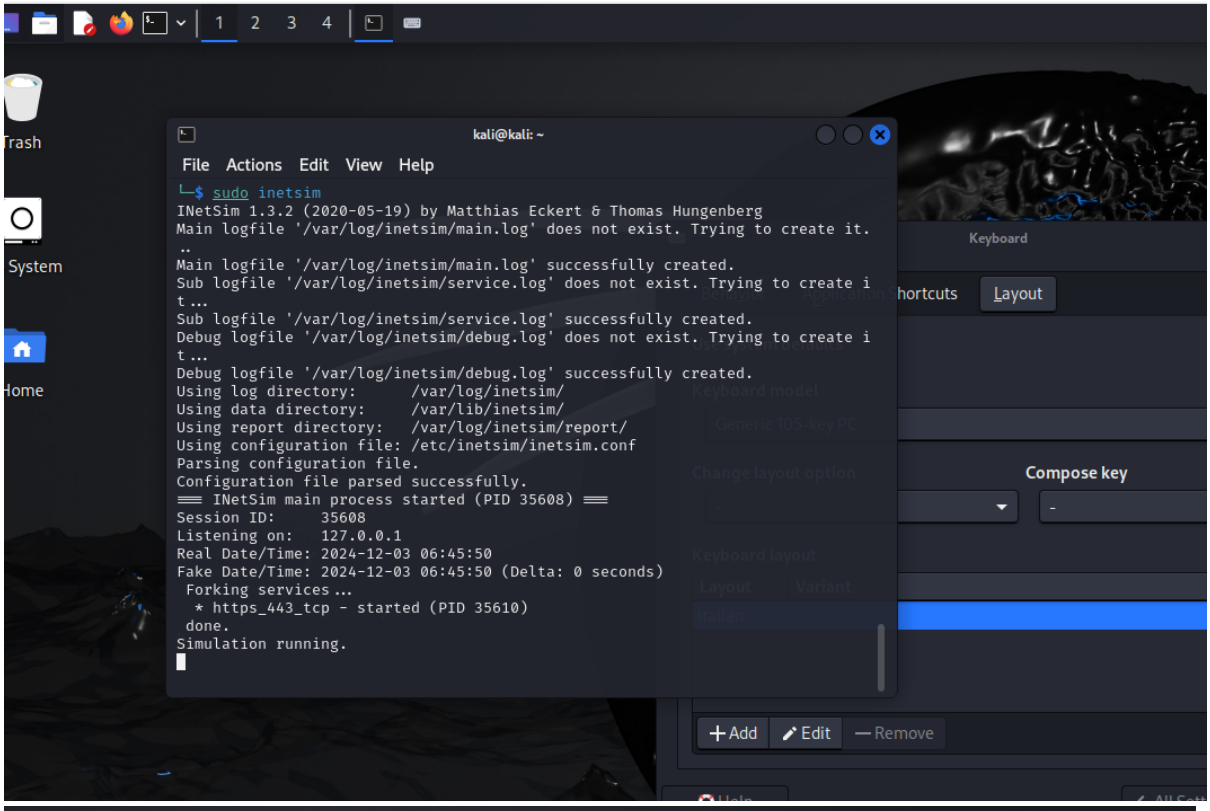
File Macchina Visualizza Inserimento Dispositivi Aiuto

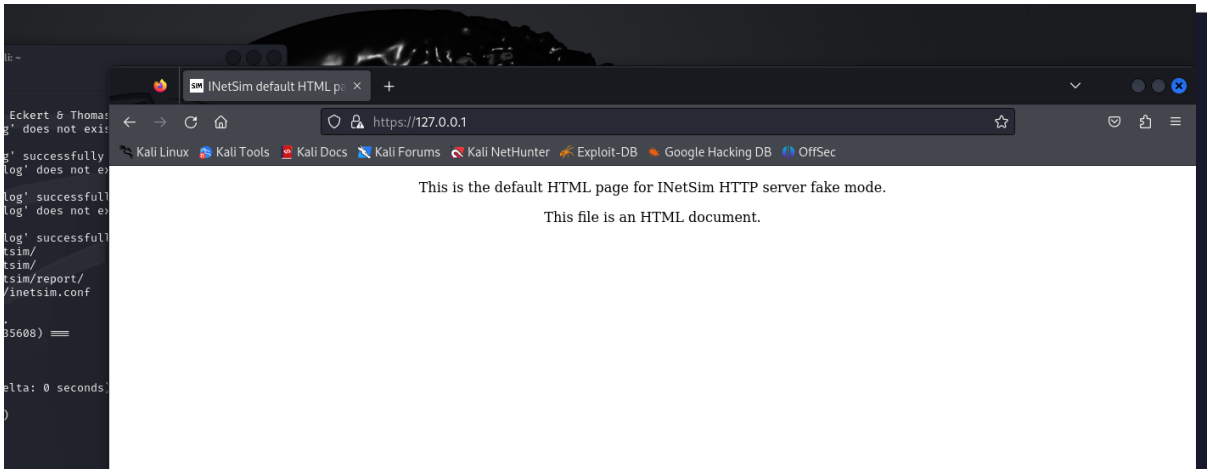


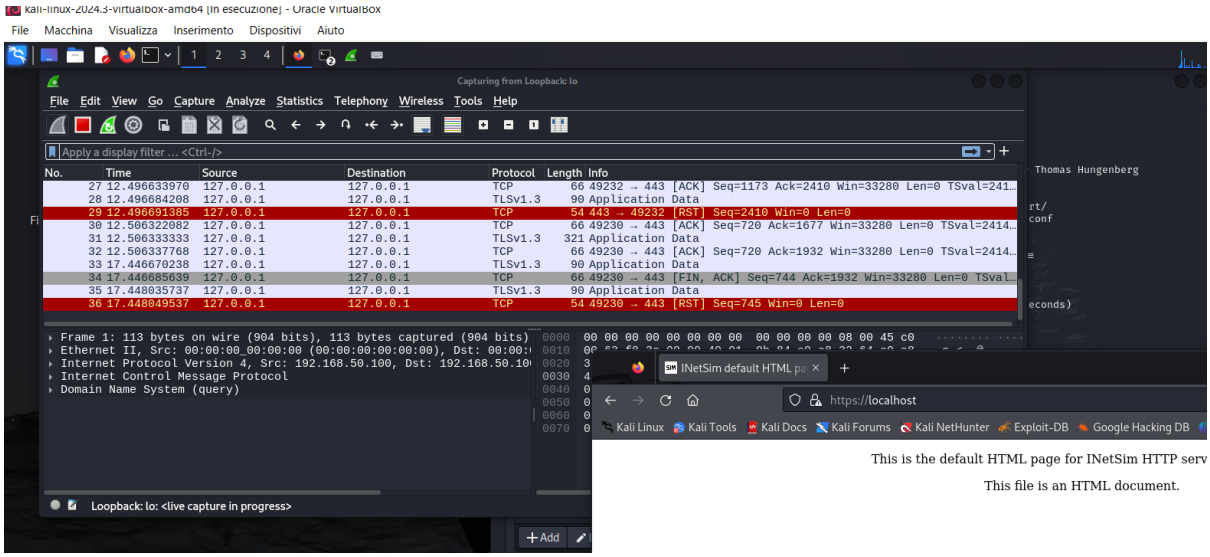


linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox

Macchina Visualizza Inserimento Dispositivi Aiuto






kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Capturing from Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
27 12.496633970 127.0.0.1 127.0.0.1 TCP 66 49232 → 443 [ACK] Seq=1173 Ack=2410 Win=33280 Len=0 TSval=241…
28 12.496684208 127.0.0.1 127.0.0.1 TLSv1.3 90 Application Data
29 12.496691385 127.0.0.1 127.0.0.1 TCP 54 443 → 49232 [RST] Seq=2410 Win=0 Len=0
30 12.506322082 127.0.0.1 127.0.0.1 TCP 66 49230 → 443 [ACK] Seq=720 Ack=1677 Win=33280 Len=0 TSval=2414…
31 12.506333333 127.0.0.1 127.0.0.1 TLSv1.3 321 Application Data
32 12.506337768 127.0.0.1 127.0.0.1 TCP 66 49230 → 443 [ACK] Seq=720 Ack=1932 Win=33280 Len=0 TSval=2414…
33 17.446670238 127.0.0.1 127.0.0.1 TLSv1.3 90 Application Data
34 17.446685639 127.0.0.1 127.0.0.1 TCP 66 49230 → 443 [FIN, ACK] Seq=744 Ack=1932 Win=33280 Len=0 TSval…
35 17.448035737 127.0.0.1 127.0.0.1 TLSv1.3 90 Application Data
36 17.448049537 127.0.0.1 127.0.0.1 TCP 54 49230 → 443 [RST] Seq=745 Win=0 Len=0
Frame 1: 113 bytes on wire (904 bits), 113 bytes captured (904 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.10
Internet Control Message Protocol
Domain Name System (query)
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 c0
Loopback: lo: <live capture in progress>
Add
Thomas Hungenberg
econds)
INetSim default HTML pa
https://localhost
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
This is the default HTML page for INetSim HTTP serv
This file is an HTML document.