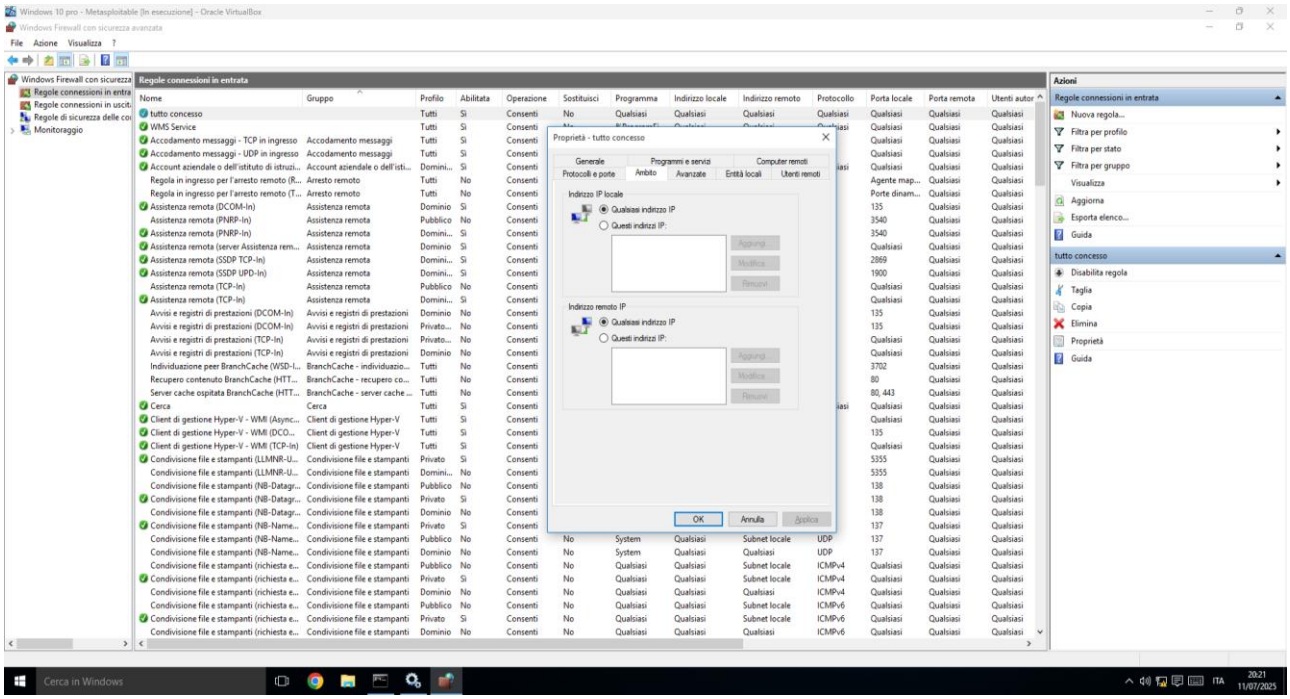
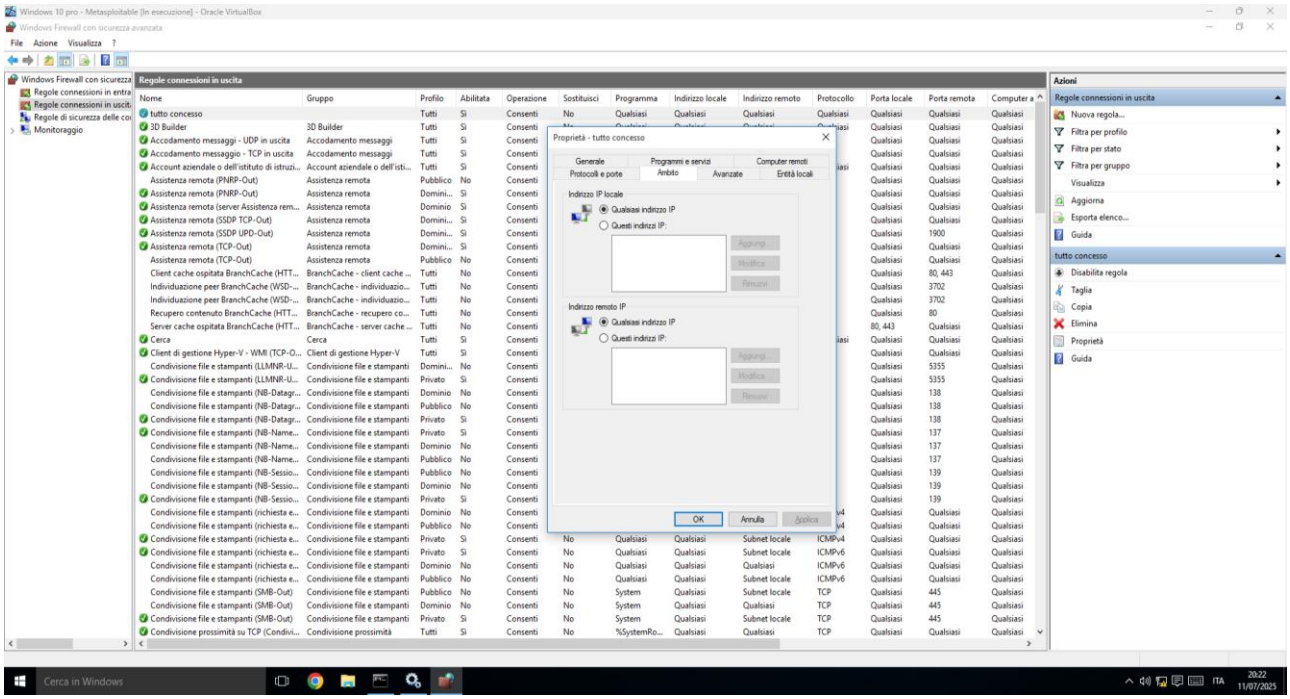
Esercizio W3 D5 pratica

Es1. Configurare policy per permettere il ping da macchina Linux a macchina Windows nel nostro laboratorio Windows firewall)

Abbiamo impostato il firewall per accettare tutte le comunicazioni sia in entrata che in uscita





Infatti facendo i due ping (windows verso kali e viceversa) abbiamo tutto in check.

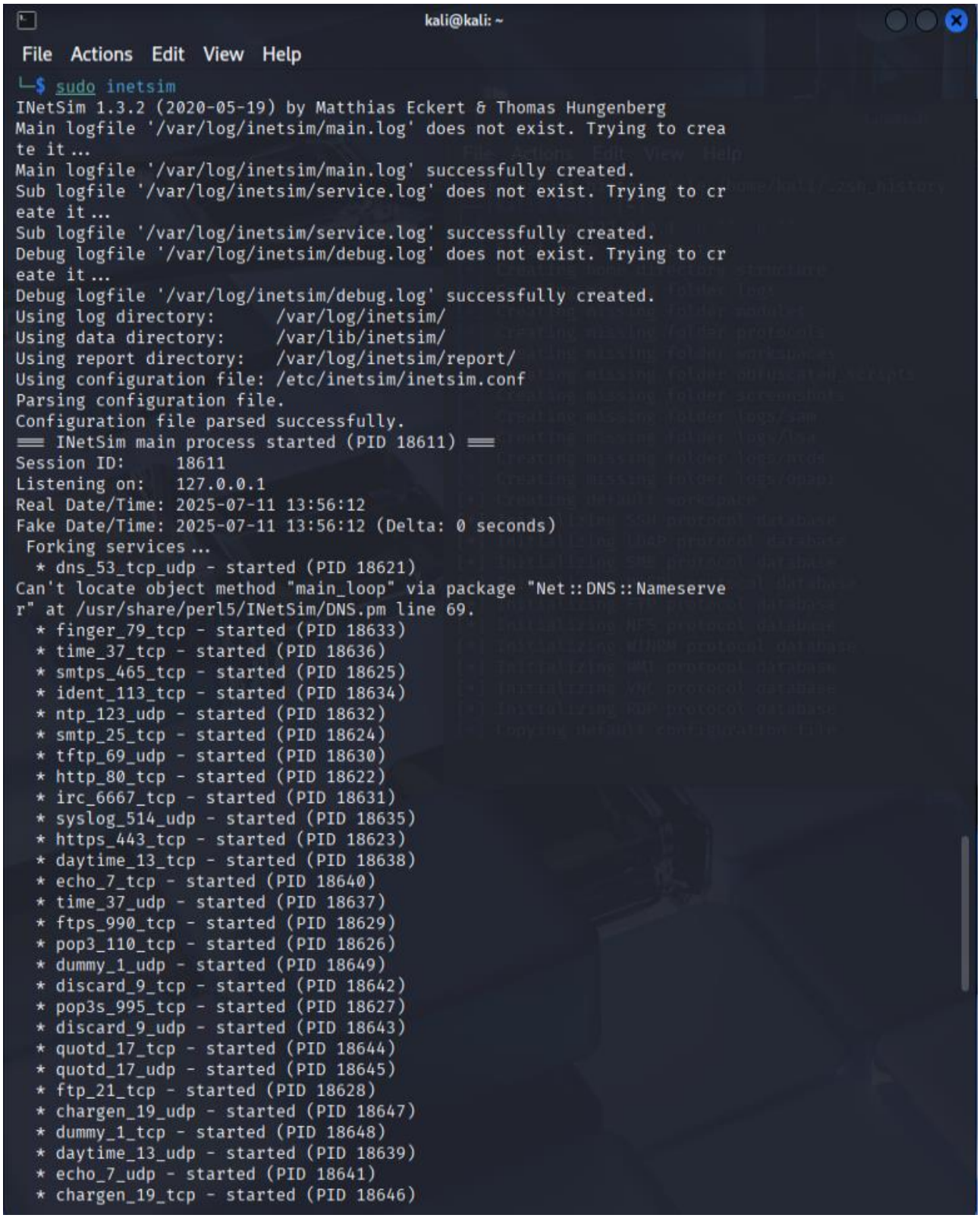
Prompt dei comandi

```
   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

C:\Users\user>

C:\Users\user>

C:\Users\user>

C:\Users\user>

C:\Users\user>ping 192.168.50.100

Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.50.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo =  0ms, Medio =  0ms

C:\Users\user>
```

```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 192.168.50.102
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=0.339 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.316 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.337 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.300 ms

── 192.168.50.102 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3065ms
rtt min/avg/max/mdev = 0.300/0.323/0.339/0.016 ms
```

Es2. Utilizzo dell'utility InetSim per l'emulazione di servizi Internet

(non so se va bene solo questo screen o bisognava fare altro nel caso mi scuso per la non comprensione della domanda)



Es3. Cattura di pacchetti con Wireshark

Sempre tramite la InetSim emuliamo la rete e facciamo un curl su 127.0.0.1

```
┌──(kali㉿kali)-[~]
└─$ curl http://127.0.0.1
<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>

┌──(kali㉿kali)-[~]
└─$
```

Ci siamo messi in ascolto su wireshark e vediamo il risultato della nostra ricerca:

```
329 270.150938610 127.0.0.1 127.0.0.1 TCP 74 60486 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=2598055261 TSecr=0 WS=128
330 270.150949534 127.0.0.1 127.0.0.1 TCP 74 80 → 60486 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=2598055261 TSecr=2598055261 WS=128
331 270.150959360 127.0.0.1 127.0.0.1 TCP 66 60486 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2598055261 TSecr=2598055261
332 270.151038514 127.0.0.1 127.0.0.1 HTTP 139 GET / HTTP/1.1
333 270.151036411 127.0.0.1 127.0.0.1 TCP 66 80 → 60486 [ACK] Seq=1 Ack=74 Win=65536 Len=0 TSval=2598055261 TSecr=2598055261
334 270.163296810 127.0.0.1 127.0.0.1 TCP 216 80 → 60486 [PSH, ACK] Seq=1 Ack=74 Win=65536 Len=150 TSval=2598055273 TSecr=2598055261 [TCP PDU reassembled in 336]
335 270.163330343 127.0.0.1 127.0.0.1 TCP 66 60486 → 80 [ACK] Seq=74 Ack=151 Win=65408 Len=0 TSval=2598055273 TSecr=2598055273
336 270.163344596 127.0.0.1 127.0.0.1 HTTP 324 HTTP/1.1 200 OK (text/html)
337 270.163348174 127.0.0.1 127.0.0.1 TCP 66 60486 → 80 [ACK] Seq=74 Ack=409 Win=65152 Len=0 TSval=2598055274 TSecr=2598055274
338 270.164372740 127.0.0.1 127.0.0.1 TCP 66 60486 → 80 [FIN, ACK] Seq=74 Ack=409 Win=65536 Len=0 TSval=2598055275 TSecr=2598055274
339 270.164927673 127.0.0.1 127.0.0.1 TCP 66 80 → 60486 [FIN, ACK] Seq=409 Ack=75 Win=65536 Len=0 TSval=2598055275 TSecr=2598055275
340 270.164943515 127.0.0.1 127.0.0.1 TCP 66 60486 → 80 [ACK] Seq=75 Ack=410 Win=65536 Len=0 TSval=2598055275 TSecr=2598055275
```

Esercizio facoltativo 1:

Simulare altri servizi con InetSim

```
┌──(kali㉿kali)-[~]
└─$ ftp 127.0.0.1 21
Connected to 127.0.0.1.
220 INetSim FTP Service ready.
Name (127.0.0.1:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get sample.txt
local: sample.txt remote: sample.txt
500 Unknown command.
200 PORT command successful.
150 Opening BINARY mode data connection for sample.txt (28 bytes).
    28       17.11 KiB/s
226 File send OK.
28 bytes received in 00:00 (0.66 KiB/s)
ftp> ^D
221 Goodbye.

┌──(kali㉿kali)-[~]
```