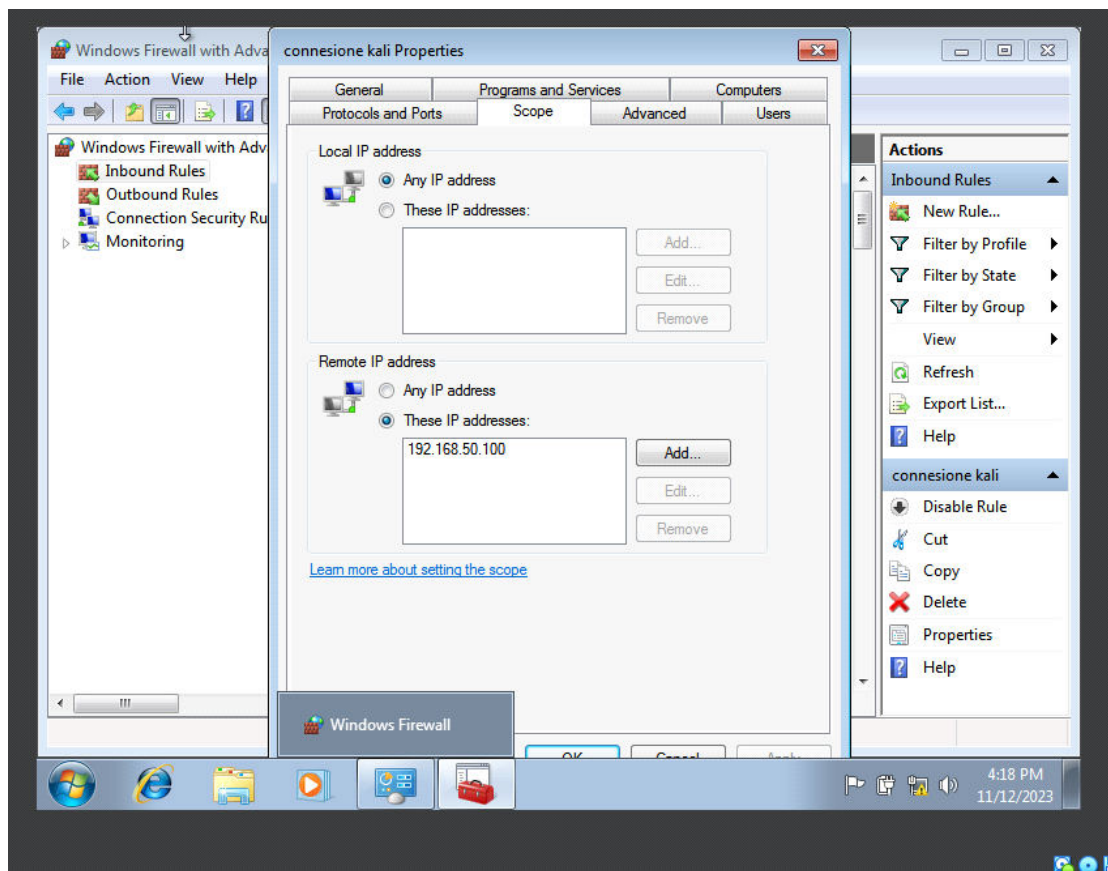


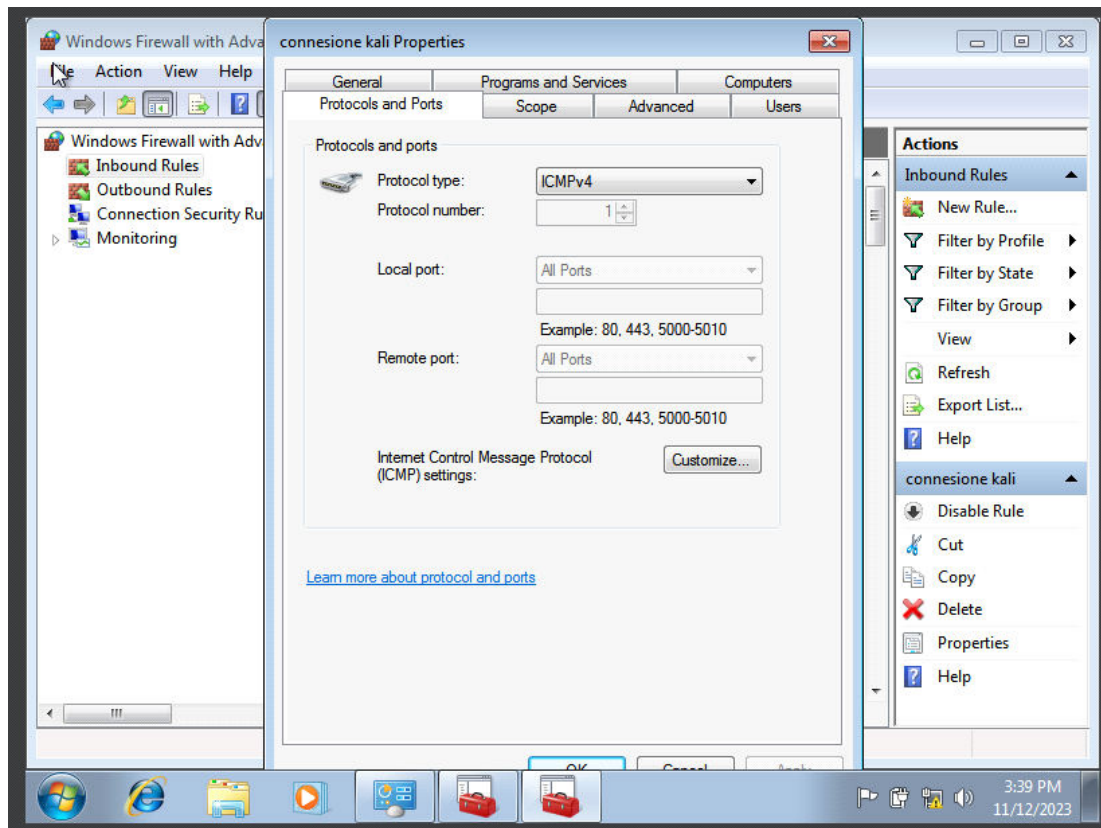
W3D4 ESERCIZIO

Di Peticaru Florin Eugen

L'esercizio di oggi richiedeva di configurare una regola di policy per windows firewall che permette il ping tra macchine Linux e Windows 7 all'interno del laboratorio virtuale, quindi scriviamo una regola in inbound con lo scopo di far attraversare solo le comunicazioni dall'IP di Kali Linux, in questo caso *192.168.50.100*



Utilizzando come protocollo per la regola l'ICMPv4



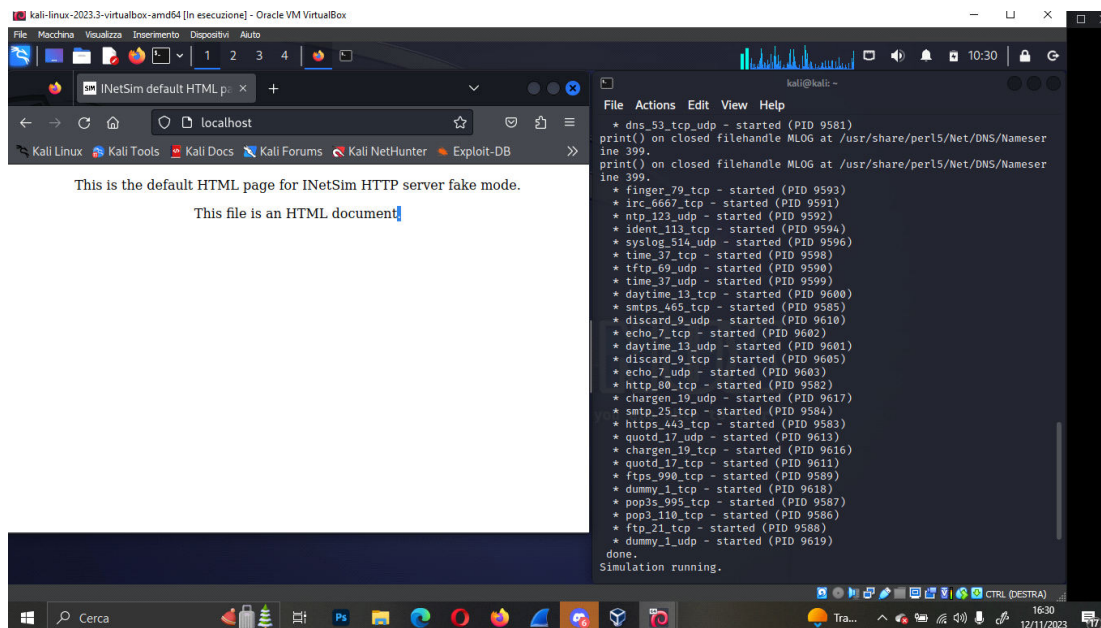
Quindi adesso riavviamo la macchina di windows per applicare correttamente la regola e avviamo la macchina di Kali per effettuare il ping e vedere se la regola del firewall

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.  
^C  
— 192.168.50.102 ping statistics —  
4 packets transmitted, 0 received, 100% packet loss, time 3063ms  
  
(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=1.46 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.01 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.863 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.757 ms  
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.846 ms  
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.760 ms  
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=1.02 ms  
^C  
— 192.168.50.102 ping statistics —  
7 packets transmitted, 7 received, 0% packet loss, time 6018ms  
rtt min/avg/max/mdev = 0.757/0.959/1.464/0.227 ms  
  
(kali@kali)-[~]  
$
```

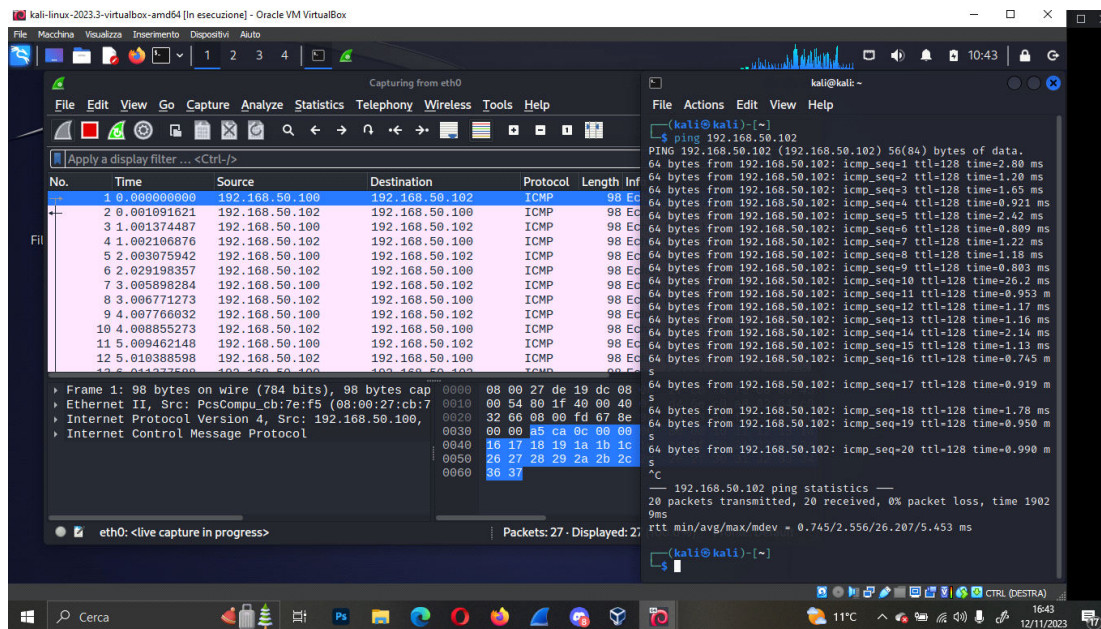
finita questa consegna dell'esercizio, passiamo al secondo punto ovvero utilizzare lo strumento di InetSim di Kali per emulare i servizi di internet, quindi mettiamo come commenti tutti i servizi tranne quello di http e https all'interno del file inetsim.conf

```
File Macchina Visualizza Inserimento Dispositivi Auto  
1 2 3 4  
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/inetsim/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  
  
Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark Copy To Bracket Where Was Previous Next  
CTRL (DESTRA)
```

quindi salviamo il file e testiamo il corretto funzionamento



Infine per l'ultimo punto dell'esercizio di oggi dovevamo catturare dei pacchetti con wireshark, il tool è già preinstallato all'interno di kali e quindi facciamo la prova della cattura dei pacchetti in Eth0 ovvero la comunicazione dei ping tra la macchina di Kali e quella di windows e la cattura dei pacchetti in loopback ovvero il servizio di internet emulato con InetSim



Kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM 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
3	0.594211127	127.0.0.1	127.0.0.1	TCP	74	58276 → 443 [SYN] Seq=0 Win=65495
4	0.594251241	127.0.0.1	127.0.0.1	TCP	74	443 → 58276 [SYN, ACK] Seq=0 Ack=
5	0.594291756	127.0.0.1	127.0.0.1	TCP	66	58276 → 443 [ACK] Seq=1 Ack=1 Win=
6	0.633668596	127.0.0.1	127.0.0.1	TLSv1.3	583	Client Hello
7	0.633743472	127.0.0.1	127.0.0.1	TCP	66	443 → 58276 [ACK] Seq=1 Ack=518 W
8	1.474464308	127.0.0.1	127.0.0.1	TLSv1.3	1487	Server Hello, Change Cipher Spec,
9	1.474603141	127.0.0.1	127.0.0.1	TCP	66	58276 → 443 [ACK] Seq=518 Ack=142
10	1.492637525	127.0.0.1	127.0.0.1	TLSv1.3	98	Application Data
11	1.492715645	127.0.0.1	127.0.0.1	TCP	66	443 → 58276 [ACK] Seq=1422 Ack=54
12	1.499861288	127.0.0.1	127.0.0.1	TCP	66	58276 → 443 [FIN, ACK] Seq=542 Ac
13	1.540449811	127.0.0.1	127.0.0.1	TCP	66	443 → 58276 [ACK] Seq=1422 Ack=54
14	1.558458734	127.0.0.1	127.0.0.1	TCP	66	443 → 58276 [FIN, ACK] Seq=1422 A

Frame 15: 66 bytes on wire (528 bits), 66 bytes captured on interface 0, 66 bytes from 127.0.0.1 to 127.0.0.1 on interface 0

Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 58276, Dst Port: 443

Loopback: lo: <live capture in progress> Packets: 15 - Displayed: 15 (100.0%) Profile: Default 0 seconds)

Forking services ...
* dns_53_tcp_udp - started (PID 9581)

11°C 16:40 12/11/2023