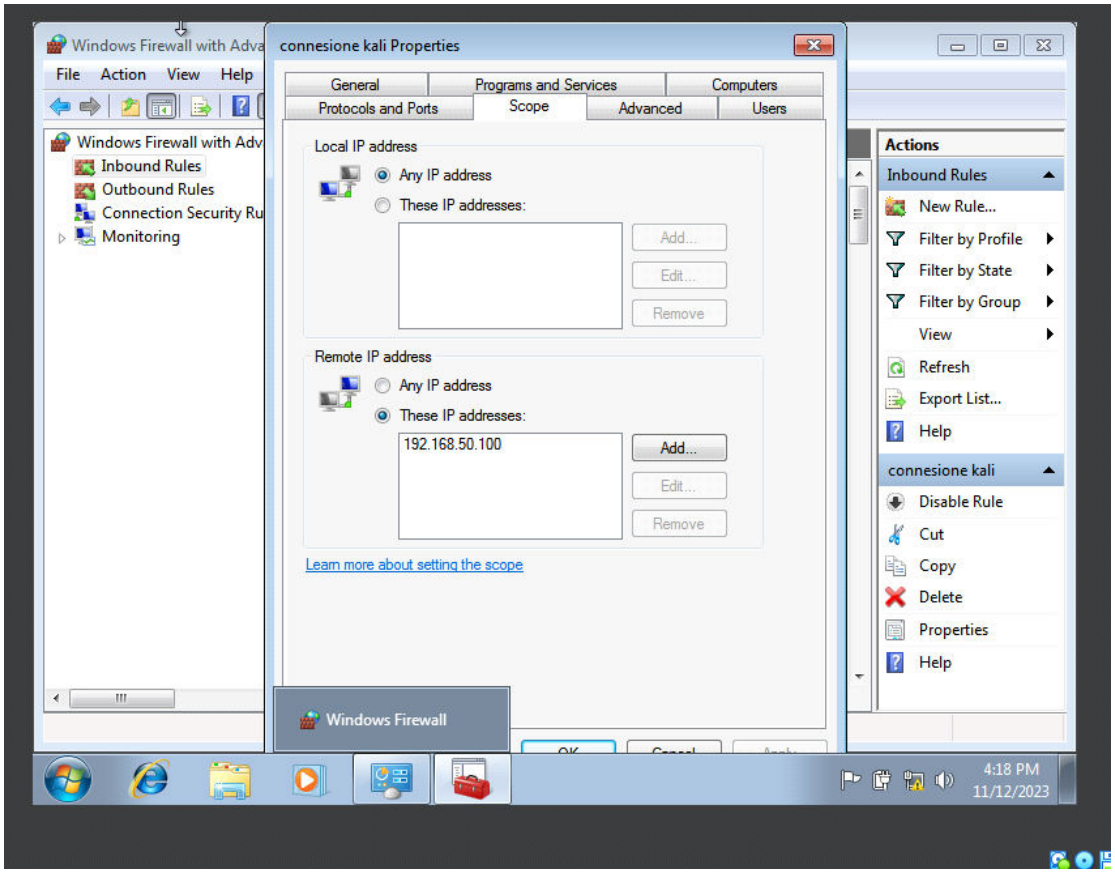
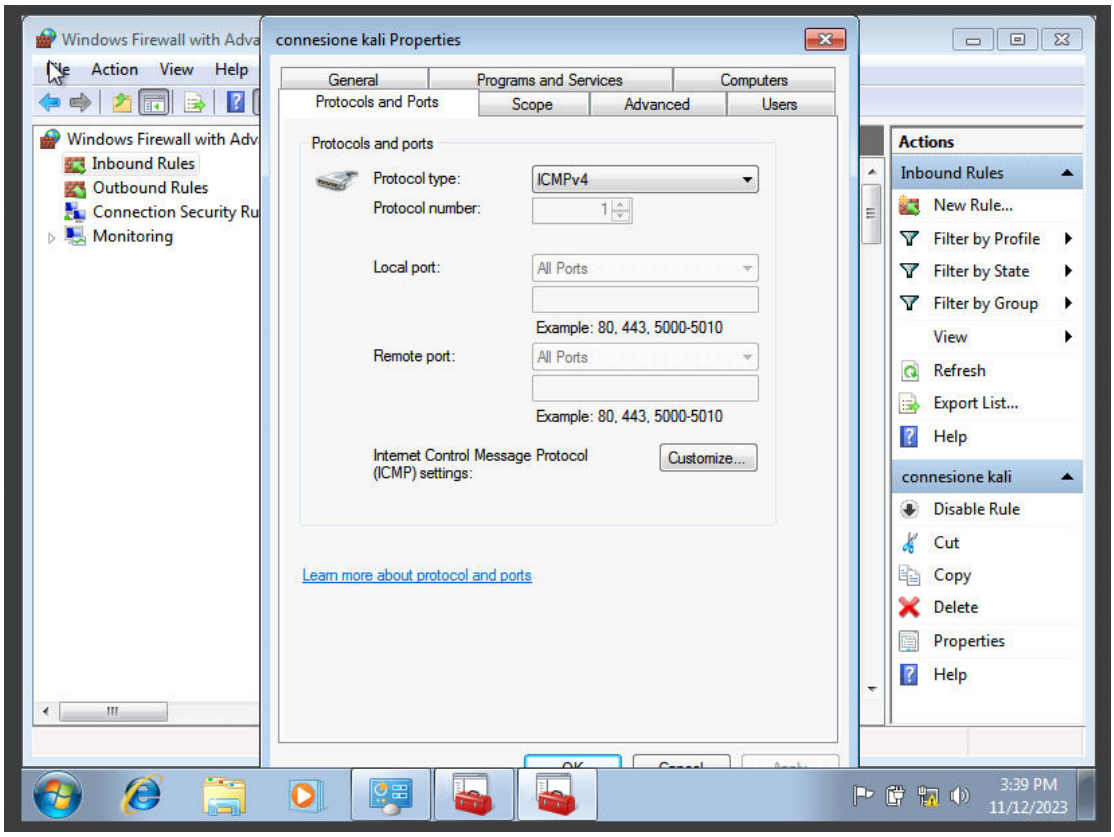
W3D4 ESERCIZIO

Di Peticaru Florin Eugen

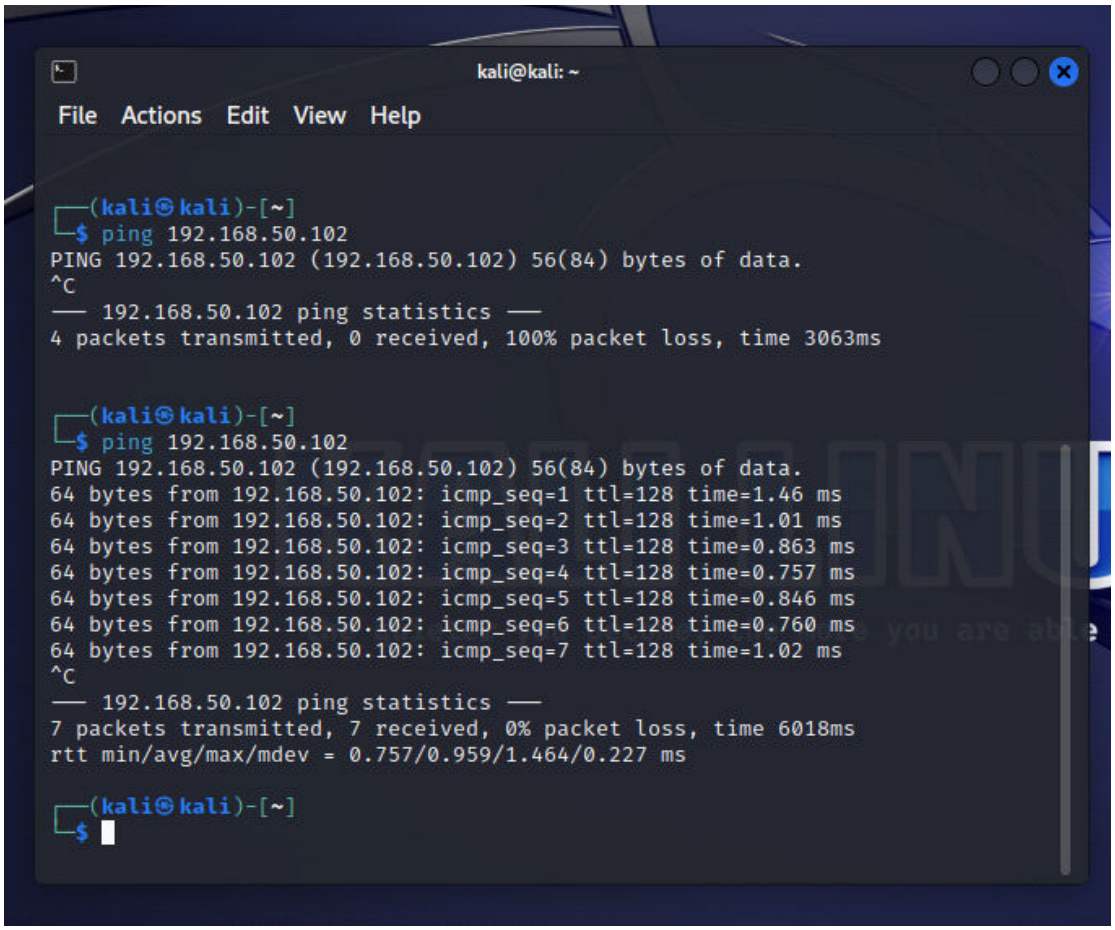
L'esercizio di oggi richiedeva di configurare una regola di policy per windows firewall che permette il ping tra macchine Linux e Windows 7 all'interno del laboratorio virtuale, quindi scriviamo una regola in inbound con lo scopo di far attraversare solo le comunicazioni dall'IP di Kali Linux, in questo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



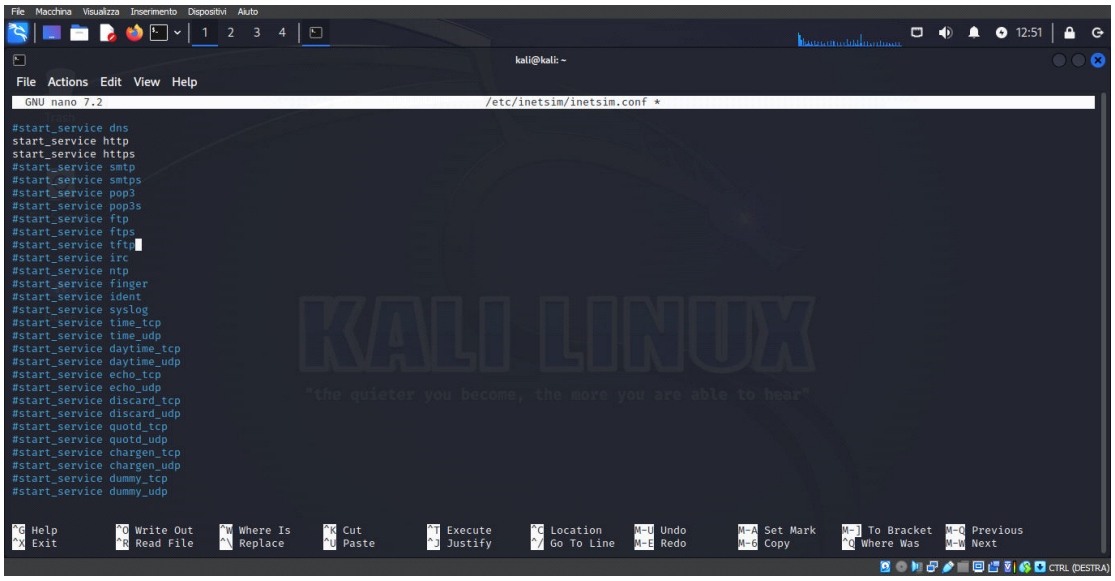
Utilizzando come protocollo per la regola l'ICMPv4



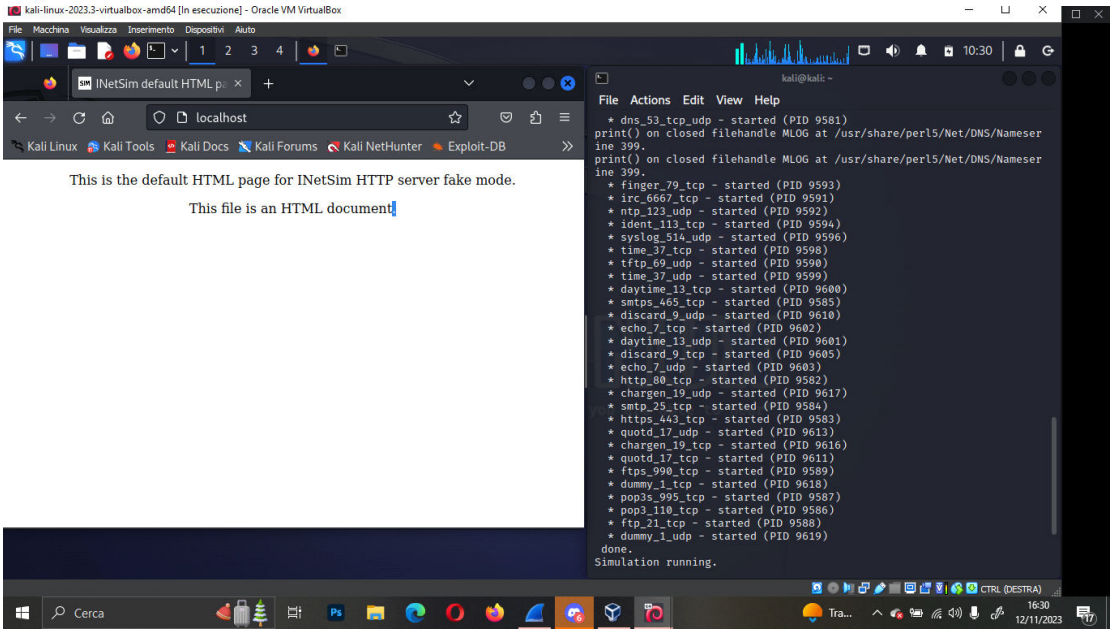
Quindi adesso riavviamo la macchina di windows per applicare correttamente la regola e avviamo la macchina di Kali per effettuare il ping e vedere se la regola del firewall



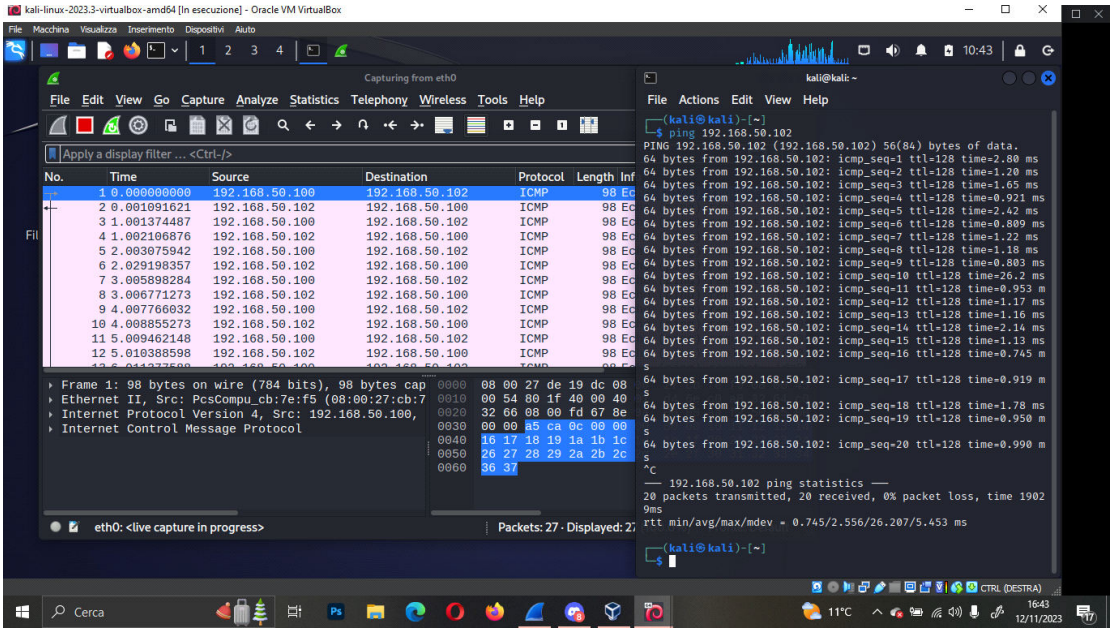
finita questa consegna dell'esercizio, passiamo al secondo punto ovvero utilizzare lo strumento di InetSim di Kali per emulare i servizi di internet, quindi mettiamo come commenti tutti i servizi tranne quello di http e https all'interno del file inetsim.conf

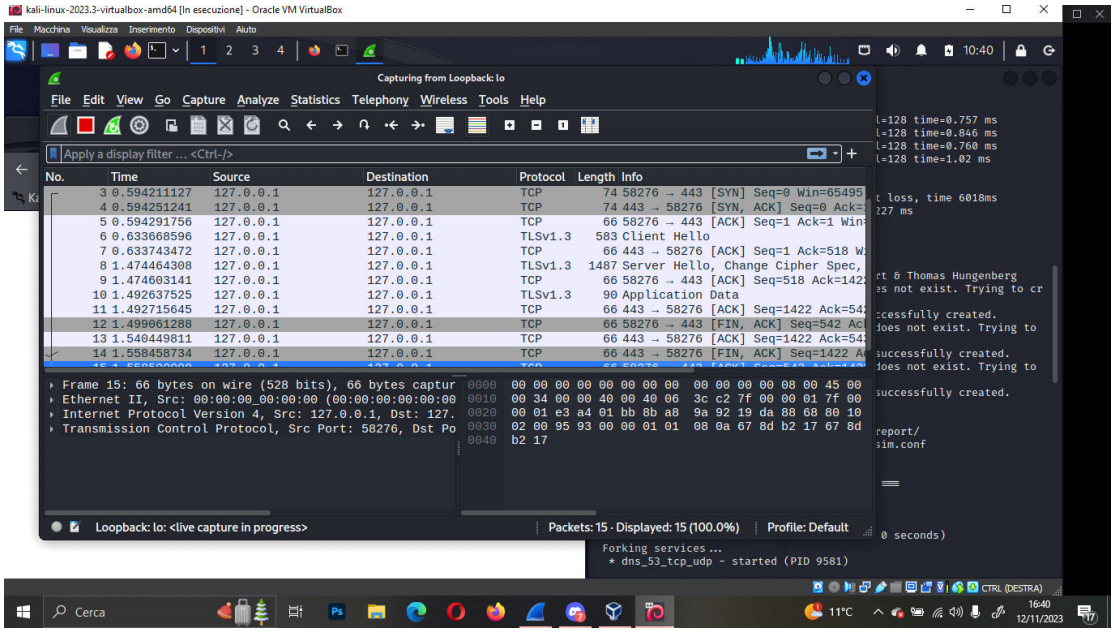


quindi salviamo il file e testiamo il corretto funzionamento



Infine per l'ultimo punto dell'esercizio di oggi dovevamo catturare dei pacchetti con wireshark, il tool è gia 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 90 Application Data
11 1.492715645 127.0.0.1 127.0.0.1 TCP 66 443 → 58276 [ACK] Seq=1422 Ack=54
12 1.499061288 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 captur
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.
Transmission Control Protocol, Src Port: 58276, Dst Po
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 34 00 00 40 00 40 06 3c c2 7f 00 00 01 7f 00
0020 00 01 e3 a4 01 bb 8b a8 9a 92 19 da 88 68 80 10
0030 02 00 95 93 00 00 01 01 08 0a 67 8d b2 17 67 8d
0040 b2 17
Loopback: lo: <live capture in progress>
Packets: 15 · Displayed: 15 (100.0%)
Profile: Default
Forking services ...
* dns_53_tcp_udp - started (PID 9581)
CTRL (DESTRA)
Cerca
11°C
16:40
12/11/2023