

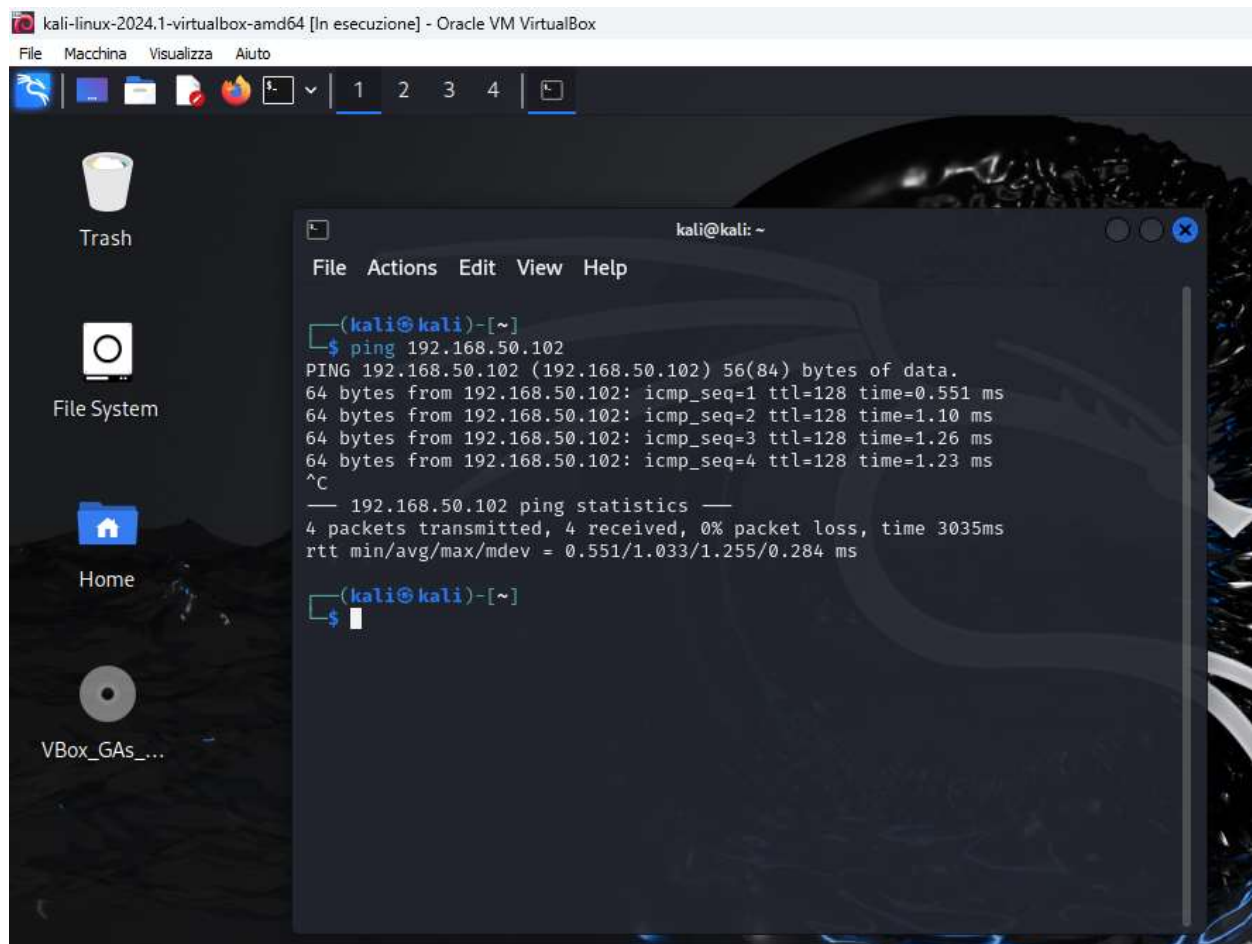
Consegna week 3 day 2

1 - Configurare policy per permettere il ping da macchina Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall).

Le macchine hanno i seguenti IP

-KALI 192.168.50.100

-WINDOWS 7 192.168.50.102



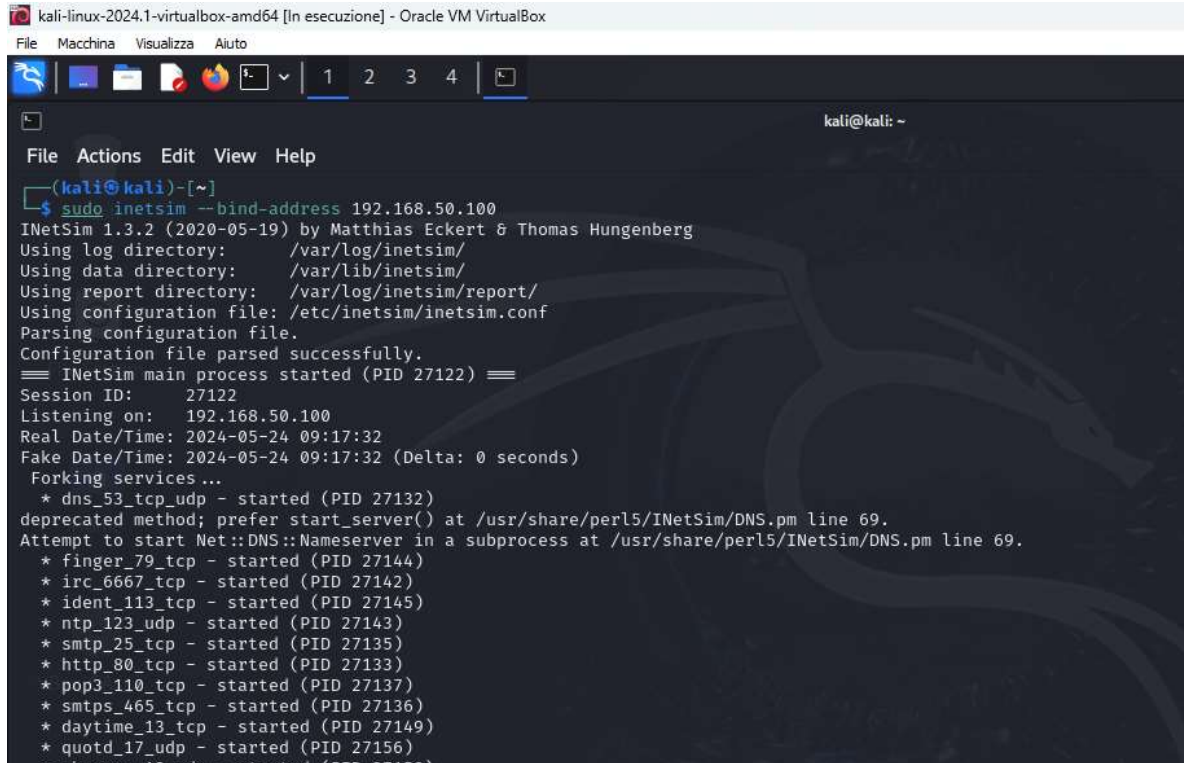
The screenshot shows a Kali Linux virtual machine window titled "kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox". The desktop background is dark with a blue and white abstract pattern. On the left sidebar, there are icons for "Trash", "File System", "Home", and "VBox_GAs_...". A terminal window is open in the center, displaying the following output:

```
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:  
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.551 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.10 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.26 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.23 ms  
^C  
— 192.168.50.102 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3035ms  
rtt min/avg/max/mdev = 0.551/1.033/1.255/0.284 ms  
  
(kali@kali)-[~]  
$
```

Riescono a comunicare tra di loro nonostante il firewall sia attivo su windows 7. Questo perché ho attivato le regole (basta filtrarle per il protocollo desiderato, in questo caso ICMPv4)

2 -Utilizzo dell'utility InetSim per l'emulazione di servizi Internet

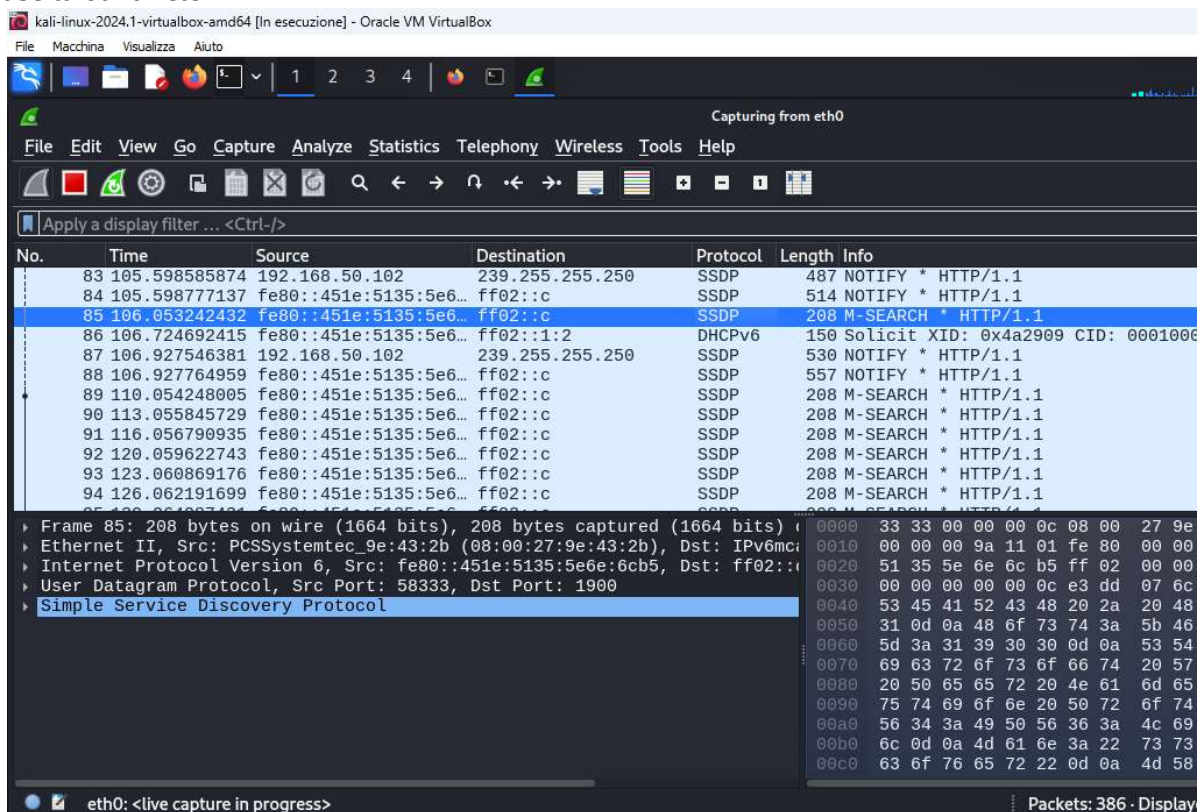
Inetsim è un software che simula servizi su una rete. Ho necessità di metterlo in ascolto correttamente quindi nelle impostazioni di configurazione (lanciate con privilegi di root su kali) ho impostato il software in ascolto sull'indirizzo IP della macchina kali 192.168.50.100



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo inetsim --bind-address 192.168.50.100  
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg  
Using log directory: /var/log/inetsim/  
Using data directory: /var/lib/inetsim/  
Using report directory: /var/log/inetsim/report/  
Using configuration file: /etc/inetsim/inetsim.conf  
Parsing configuration file.  
Configuration file parsed successfully.  
=== INetSim main process started (PID 27122) ===  
Session ID: 27122  
Listening on: 192.168.50.100  
Real Date/Time: 2024-05-24 09:17:32  
Fake Date/Time: 2024-05-24 09:17:32 (Delta: 0 seconds)  
Forking services ...  
* dns_53_tcp_udp - started (PID 27132)  
deprecated method; prefer start_server() at /usr/share/perl5/INetSim/DNS.pm line 69.  
Attempt to start Net::DNS::Nameserver in a subprocess at /usr/share/perl5/INetSim/DNS.pm line 69.  
* finger_79_tcp - started (PID 27144)  
* irc_6667_tcp - started (PID 27142)  
* ident_113_tcp - started (PID 27145)  
* ntp_123_udp - started (PID 27143)  
* smtp_25_tcp - started (PID 27135)  
* http_80_tcp - started (PID 27133)  
* pop3_110_tcp - started (PID 27137)  
* smtps_465_tcp - started (PID 27136)  
* daytime_13_tcp - started (PID 27149)  
* quotd_17_udp - started (PID 27156)  
* chargen_19_udp - started (PID 27158)
```

3 - Cattura di pacchetti con Wireshark

Adesso ho lanciato Wireshark che è uno sniffer e cioè cattura i pacchetti che passano in entrata e uscita dalla rete



No.	Time	Source	Destination	Protocol	Length	Info
83	105.598585874	192.168.50.102	239.255.255.250	SSDP	487	NOTIFY * HTTP/1.1
84	105.598777137	fe80::451e:5135:5e6...	ff02::c	SSDP	514	NOTIFY * HTTP/1.1
85	106.053242432	fe80::451e:5135:5e6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
86	106.724692415	fe80::451e:5135:5e6...	ff02::1:2	DHCPv6	150	Solicit XID: 0x4a2909 CID: 0001000
87	106.927546381	192.168.50.102	239.255.255.250	SSDP	530	NOTIFY * HTTP/1.1
88	106.927764959	fe80::451e:5135:5e6...	ff02::c	SSDP	557	NOTIFY * HTTP/1.1
89	110.054248005	fe80::451e:5135:5e6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
90	113.055845729	fe80::451e:5135:5e6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
91	116.056790935	fe80::451e:5135:5e6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
92	120.059622743	fe80::451e:5135:5e6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
93	123.060869176	fe80::451e:5135:5e6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
94	126.062191699	fe80::451e:5135:5e6...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1

Frame 85: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on eth0
Ethernet II, Src: PCSystemtec_9e:43:2b (08:00:27:9e:43:2b), Dst: IPv6multicast (01:00:5e:00:00:00)
Internet Protocol Version 6, Src: fe80::451e:5135:5e6:6cb5, Dst: ff02::c
User Datagram Protocol, Src Port: 58333, Dst Port: 1900
Simple Service Discovery Protocol