

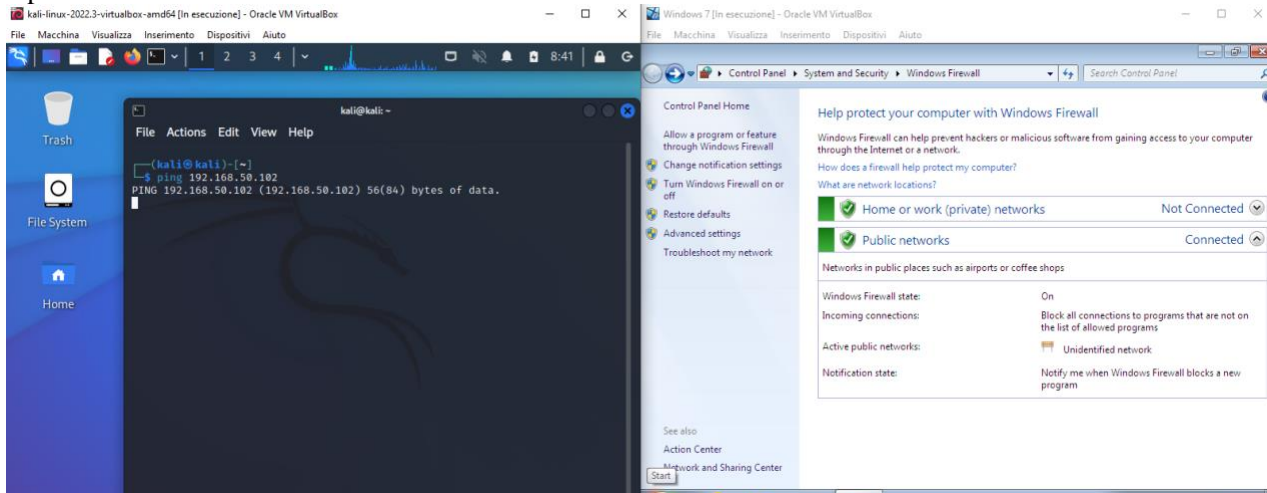
Documentazione esercitazione macchine virtuali

L'esercizio consiste nel:

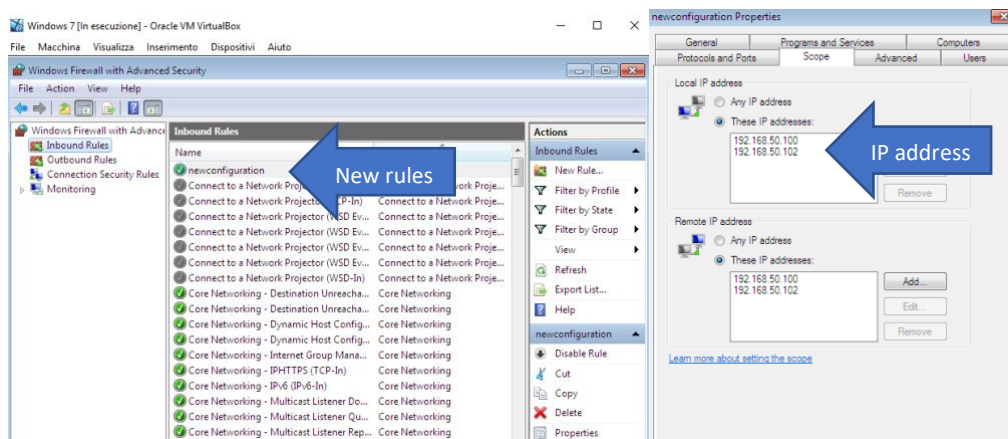
1. Configurare policy firewall per pingare da Linux a Windows
2. Utilizzare il tool pre-installato su Kali (InetSim) per emulare servizi internet
3. Catturare pacchetti con Whiteshark(sempre da Kali)

1.

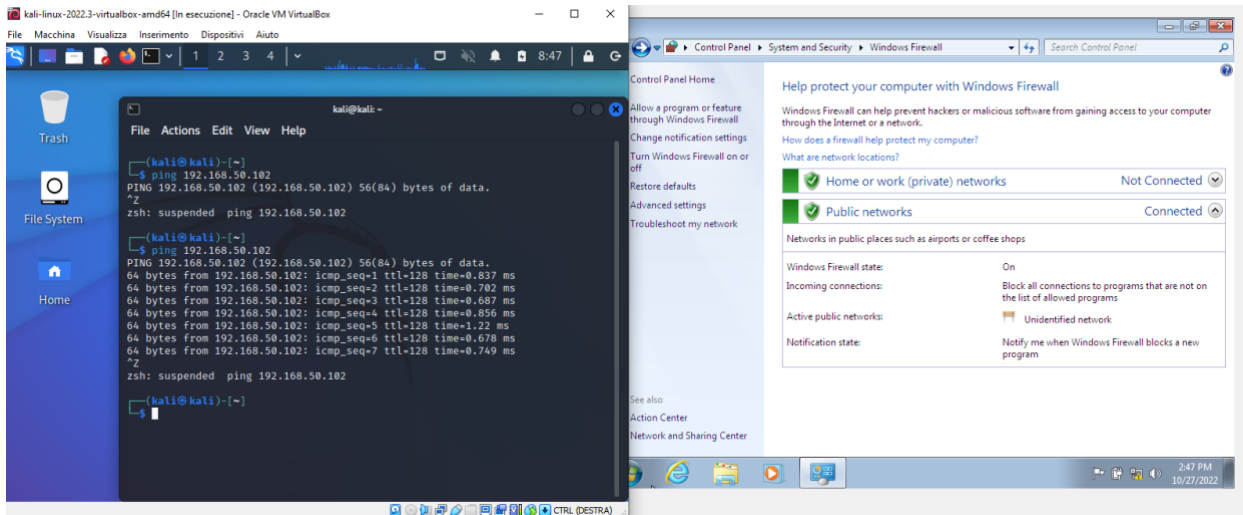
Inizialmente con firewall attivo se si prova a pingare dalla prompt dei comandi di Linux a Window con il comando “ping 192.168.50.102” dove 192.168.50.102 è l'indirizzo IP della macchina Window, non avremo risposta



Cambiando i permessi in “Inbound” all’interno delle impostazioni avanzate del firewall impostiamo gli indirizzi IP delle macchine virtuali per farli riconoscere al firewall e non far bloccare il procedimento di ping



Impostate le modifiche questo sarà il risultato



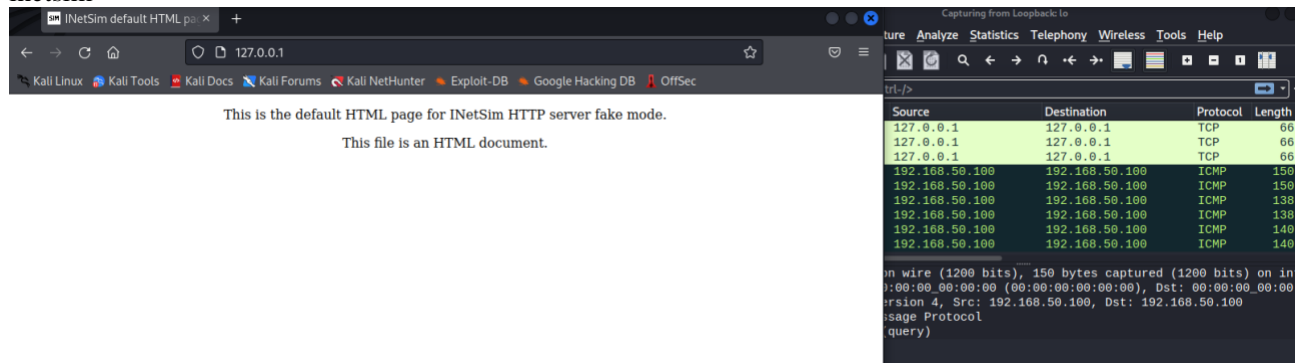
2.

Con il comando “sudo inetsim” richiamiamo un tool di kali che simulerà servizi internet, configurandoci una porta di ascolto. Di default la 127.0.0.1

```
└─$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Main logfile '/var/log/inetsim/main.log' does not exist. Trying to create it.
..
Main logfile '/var/log/inetsim/main.log' successfully created.
Sub logfile '/var/log/inetsim/service.log' does not exist. Trying to create i
t...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create i
t...
Debug logfile '/var/log/inetsim/debug.log' successfully created.
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 7411) ==
Session ID: 7411
Listening on: 127.0.0.1
Real Date/Time: 2022-10-27 08:52:39
Fake Date/Time: 2022-10-27 08:52:39 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 7417)
* finger_79_tcp - started (PID 7429)
* irc_6667_tcp - started (PID 7427)
* time_37_tcp - started (PID 7432)
* syslog_514_udp - started (PID 7431)
* ident_113_tcp - started (PID 7430)
* daytime_13_tcp - started (PID 7434)
* echo_7_tcp - started (PID 7436)
* ntp_123_udp - started (PID 7428)
* daytime_13_udp - started (PID 7435)
* discard_9_udp - started (PID 7440)
* quotd_17_tcp - started (PID 7441)
* discard_9_tcp - started (PID 7439)
* tftp_69_udp - started (PID 7426)
* time_37_udp - started (PID 7433)
* echo_7_udp - started (PID 7438)
* quotd_17_udp - started (PID 7445)
* chargen_19_tcp - started (PID 7446)
* pop3s_995_tcp - started (PID 7423)
* smtps_465_tcp - started (PID 7421)
```

3.

In conclusione, ricollegandoci al secondo punto dell'esercizio, apriamo wireshark per catturare i pacchetti che si scambiano tra client e server, aprendo il browser e inserendo nella barra di ricerca l'indirizzo localhost creato con inetsim



35	10.154492752	127.0.0.1	127.0.0.1	TCP	66	60704 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1104902390 TSecr=1104902390
36	10.172477423	127.0.0.1	127.0.0.1	HTTP	480	GET / HTTP/1.1
37	10.172493874	127.0.0.1	127.0.0.1	TCP	66	80 → 60704 [ACK] Seq=1 Ack=415 Win=65152 Len=0 TSval=1104902408 TSecr=1104902408
38	10.317209864	127.0.0.1	127.0.0.1	TCP	216	80 → 60704 [PSH, ACK] Seq=1 Ack=415 Win=65536 Len=150 TSval=1104902553 TSecr=1104902408 [T...
39	10.317263084	127.0.0.1	127.0.0.1	TCP	66	60704 → 80 [ACK] Seq=415 Ack=151 Win=65408 Len=0 TSval=1104902553 TSecr=1104902553
40	10.317295651	127.0.0.1	127.0.0.1	HTTP	324	HTTP/1.1 200 OK (text/html)
41	10.317304709	127.0.0.1	127.0.0.1	TCP	66	60704 → 80 [ACK] Seq=415 Ack=409 Win=65152 Len=0 TSval=1104902553 TSecr=1104902553
42	10.317363146	127.0.0.1	127.0.0.1	TCP	66	60704 → 80 [FIN, ACK] Seq=415 Ack=409 Win=65536 Len=0 TSval=1104902553 TSecr=1104902553
43	10.341794858	127.0.0.1	127.0.0.1	TCP	66	80 → 60704 [FIN, ACK] Seq=409 Ack=416 Win=65536 Len=0 TSval=1104902577 TSecr=1104902553
44	10.341842268	127.0.0.1	127.0.0.1	TCP	66	60704 → 80 [ACK] Seq=416 Ack=410 Win=65536 Len=0 TSval=1104902577 TSecr=1104902577

- Protocollo TCP = protocollo che si occupa della trasmissione di dati tra mittente e destinatario (livello trasporto)
- Protocollo HTTP = protocollo che si occupa della trasmissione d'informazioni sul web (livello applicazione)