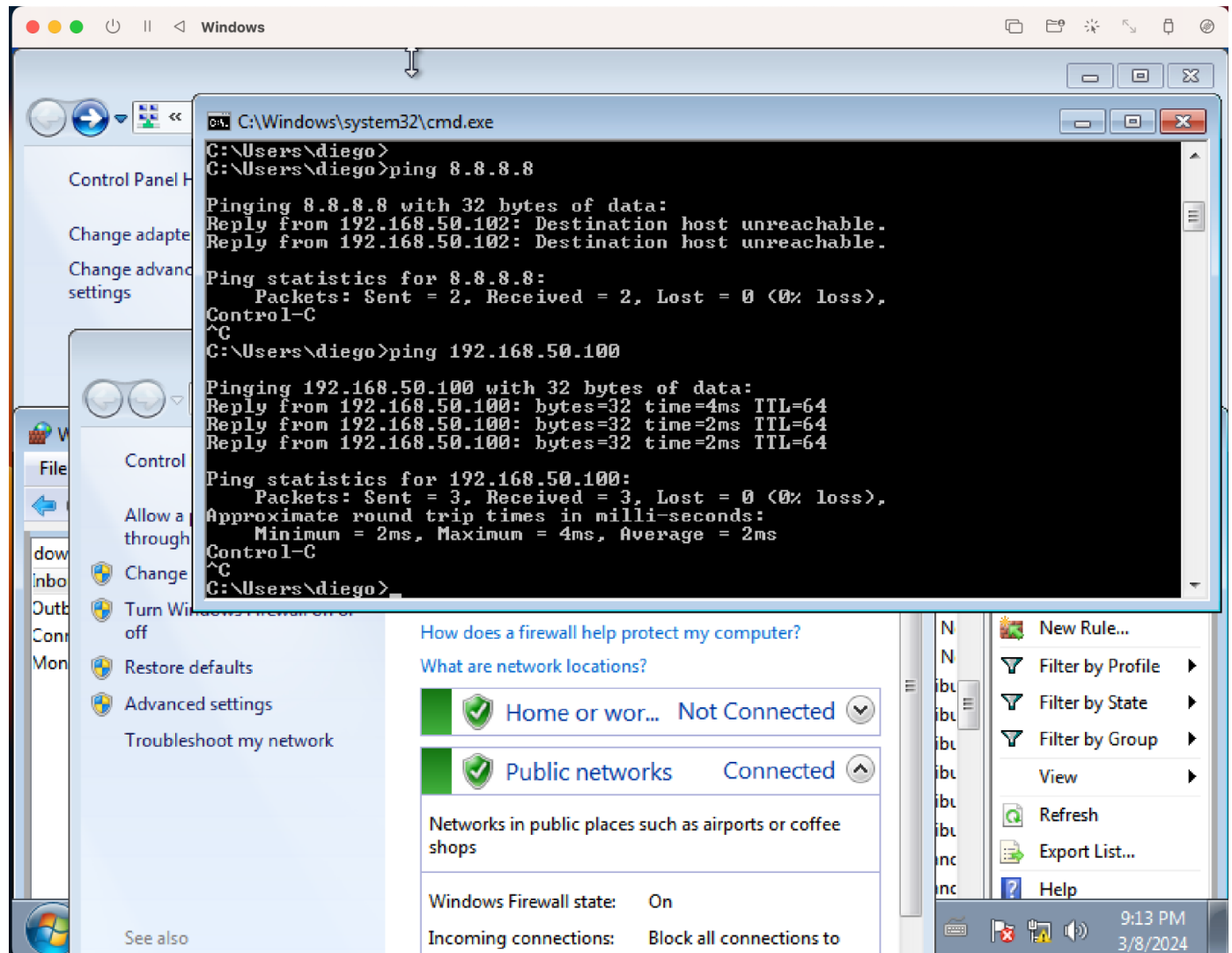


# creata policy su windows 7 firewall

creata policy su windows 7 firewall

e ping con Kali



e viceversa

```
kali@IMF501: ~  
File Actions Edit View Help  
inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255  
inet6 fe80::2858:d7d0:4798:49eb prefixlen 64 scopeid 0x20<link>  
ether ea:bc:f1:eb:9c:88 txqueuelen 1000 (Ethernet)  
RX packets 45 bytes 11301 (11.0 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 57 bytes 8971 (8.7 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 26 bytes 2192 (2.1 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 26 bytes 2192 (2.1 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@IMF501)-[~]  
$ 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=6.25 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=3.74 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=2.00 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=6.64 ms  
^C  
— 192.168.50.102 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3016ms  
rtt min/avg/max/mdev = 2.003/4.657/6.636/1.893 ms
```

cerco inetsim con il comando whereis

entro nella cartella e con con il comando ls vedo il contenuto della cartella

creo una copia del file inetsim.conf

```
(kali@IMF501)-[~]  
$ whereis inetsim  
inetsim: /usr/bin/inetsim /etc/inetsim /usr/share/inetsim /usr/share/man/man1/inetsim.1.gz  
  
(kali@IMF501)-[~]  
$ /etc/inetsim  
  
(kali@IMF501)-[/etc/inetsim]  
$ ls -l  
total 88  
-rw-r--r-- 1 root root 41691 Mar  9 23:40 inetsim.conf  
-rw-r--r-- 1 root root 41640 Mar  9 19:04 inetsim.conf.copy
```

una volta aperto il file con il comando sudo nano inetsim.conf

vado a modificarlo come in foto

```
kali@IMF501: /etc/inetsim
File Actions Edit View Help
kali@IMF501: /etc/inetsim x kali@IMF501: /etc/inetsim x
GNU nano 7.2 inetsim.conf *
#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

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 10.10.10.1

#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#
# Default: inetsim
#
#service_run_as_user nobody

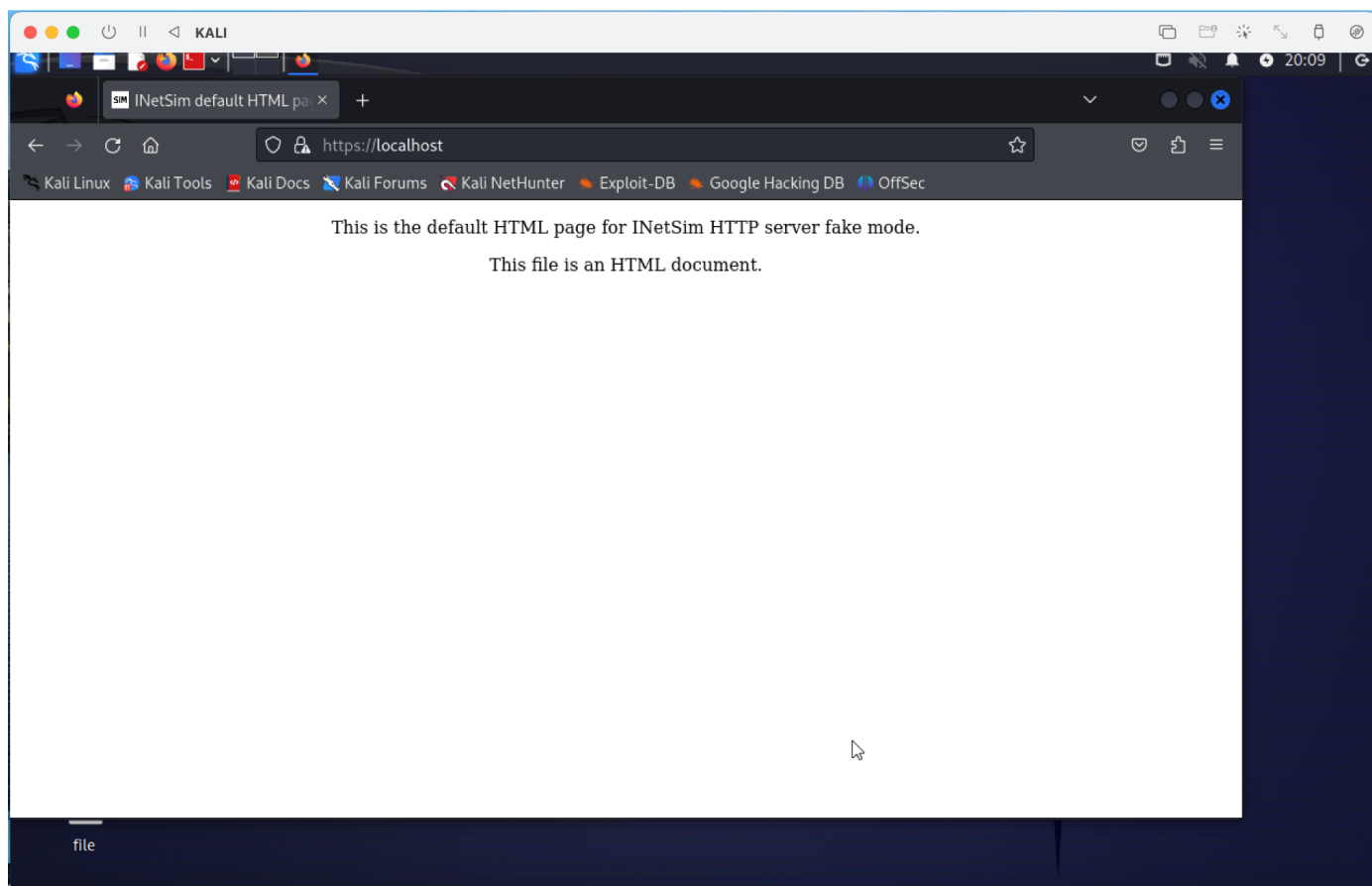
#####
# service_max_childs
#

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo      M-6 Copy
```

avvio

```
(kali@IMF501)-[/etc/inetsim]
$ sudo inetsim
sudo: unable to resolve host IMF501: Name or service not known
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 it ...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create it ...
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.
Warning: Unknown option 'Default' in configuration file '/etc/inetsim/inetsim.conf' line 201
Warning: Unknown option 'Syntax:' in configuration file '/etc/inetsim/inetsim.conf' line 203
Warning: Unknown option 'Default:' in configuration file '/etc/inetsim/inetsim.conf' line 205
Configuration file parsed successfully.
== INetSim main process started (PID 134767) ==
Session ID: 134767
Listening on: 127.0.0.1
Real Date/Time: 2024-03-09 20:08:44
Fake Date/Time: 2024-03-09 20:08:44 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 134769)
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.
* http_80_tcp - started (PID 134770)
* https_443_tcp - started (PID 134771)
done.
Simulation running.
```

apro firefox e inserisco l'indirizzo <http://localhost> e dovrà apparire la seguente pagina



avvio wireshark da terminale

seleziono any

e posso vedere la cattura del 3 way handshake con il localhost

127.0.0.1

