

Progetto S1/L5

Richiesta

Si ha un laboratorio su VirtualBox con due sistemi virtualizzati, ovvero: Kali Linux e Windows 7.

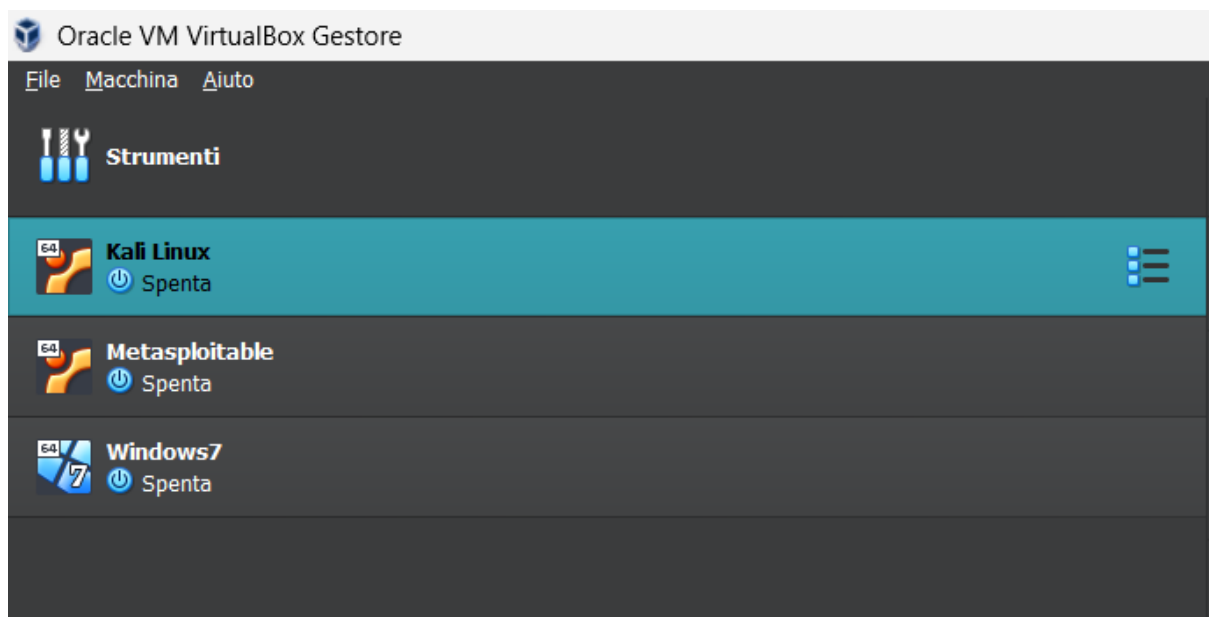
Si richiede di:

- assegnare l'IP 192.168.32.100 a Kali Linux
- assegnare l'IP 192.168.32.101 a Windows 7
- attivare il server HTTPS
- attivare il servizio DNS

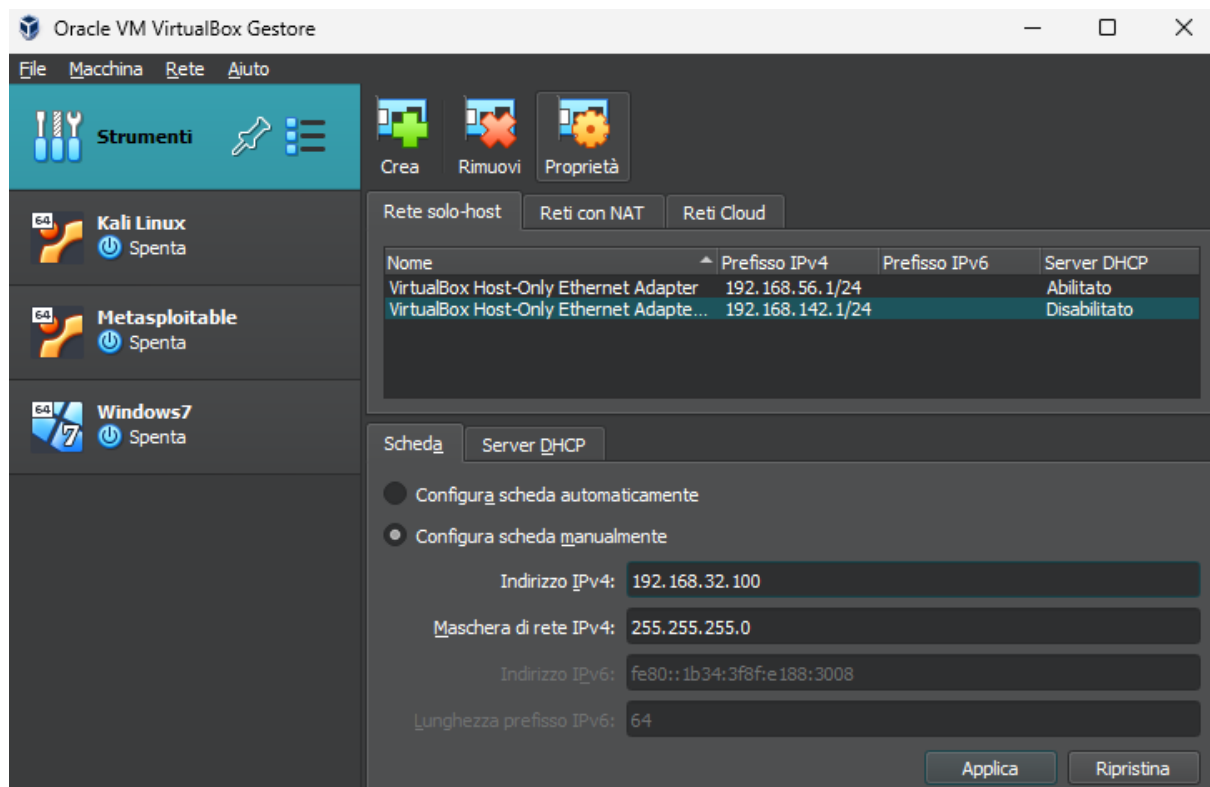
Va simulata un'architettura client server in cui un client con indirizzo 192.168.32.101 richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 e si deve intercettare la comunicazione con Wireshark.

Operato

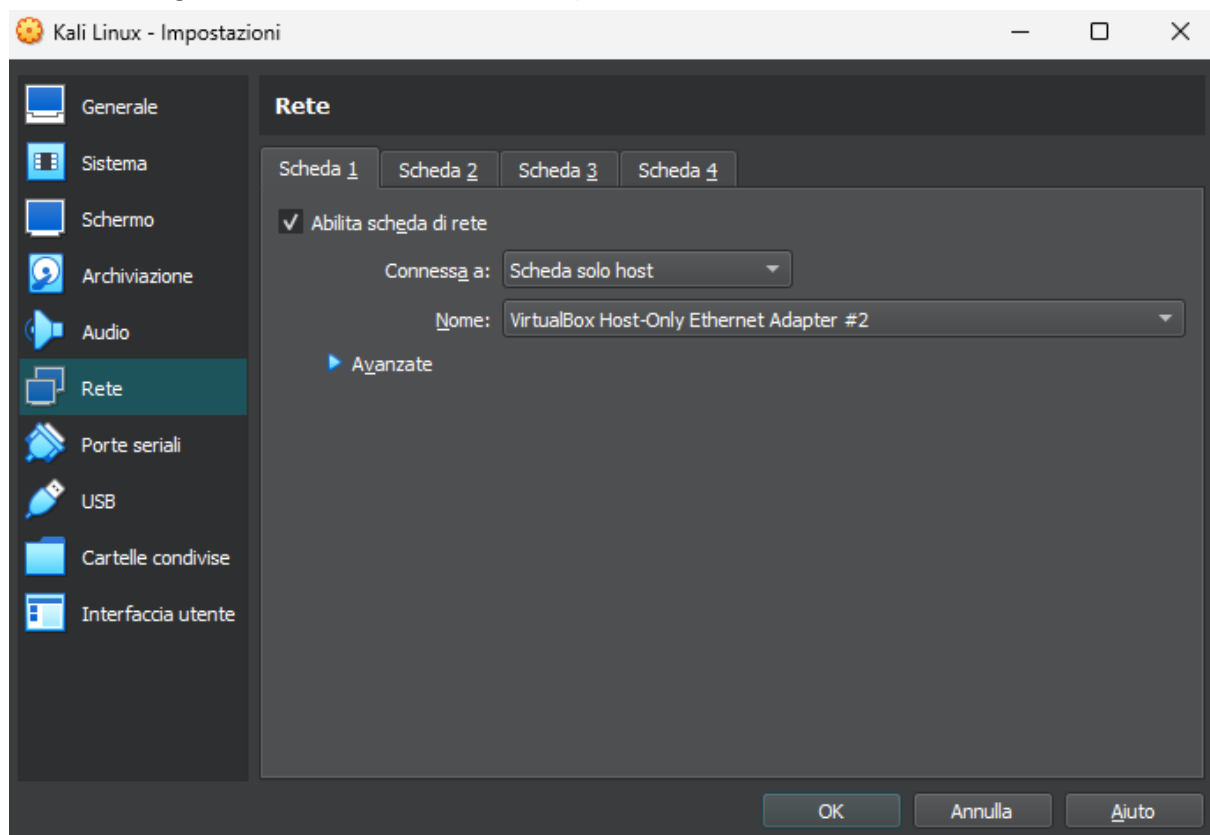
Ho avviato l'ambiente virtuale su VirtualBox



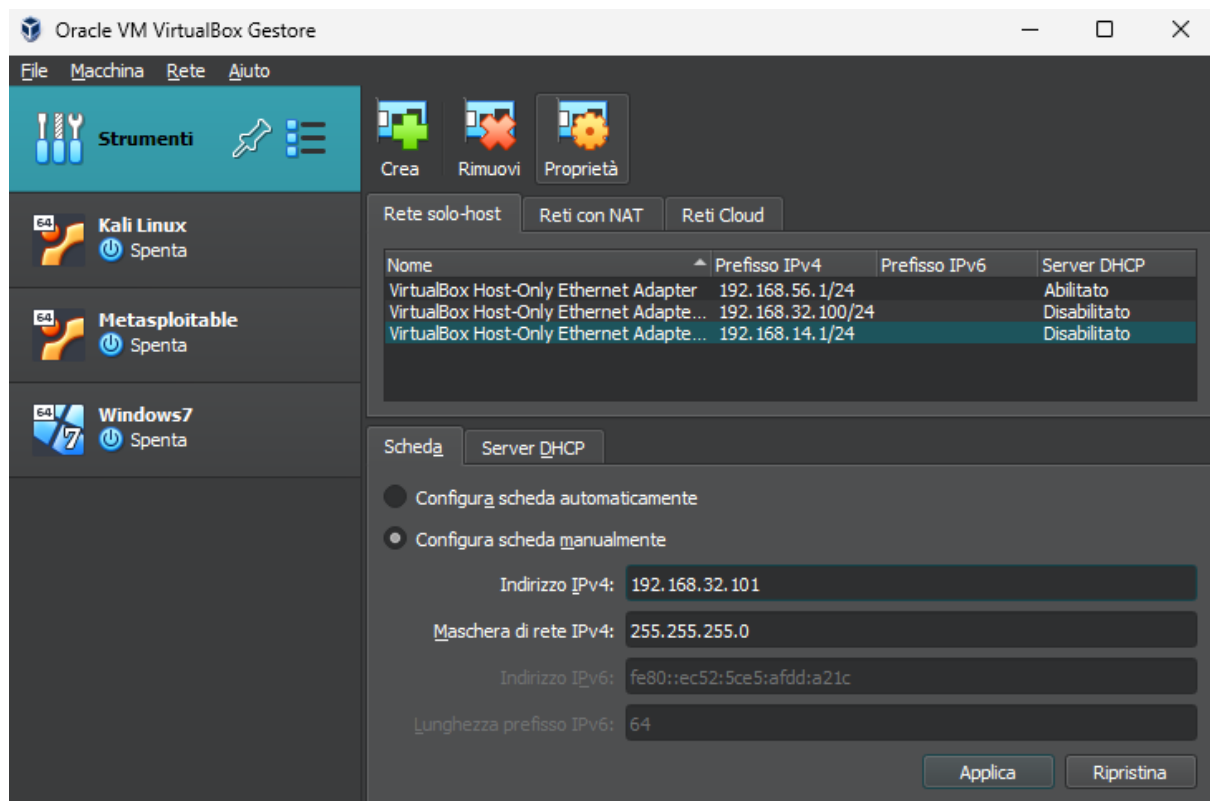
Ho settato l'IP di Kali



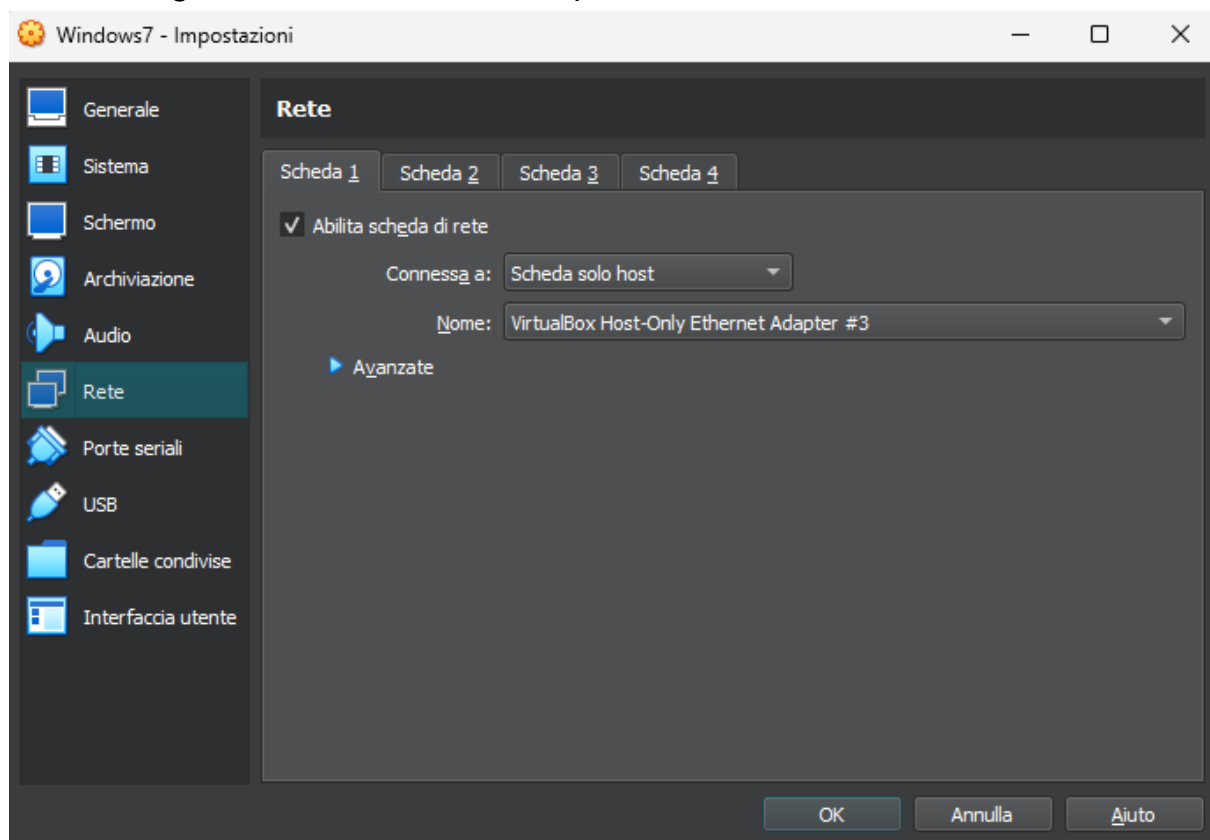
e l'ho assegnato alla macchina corrispondente



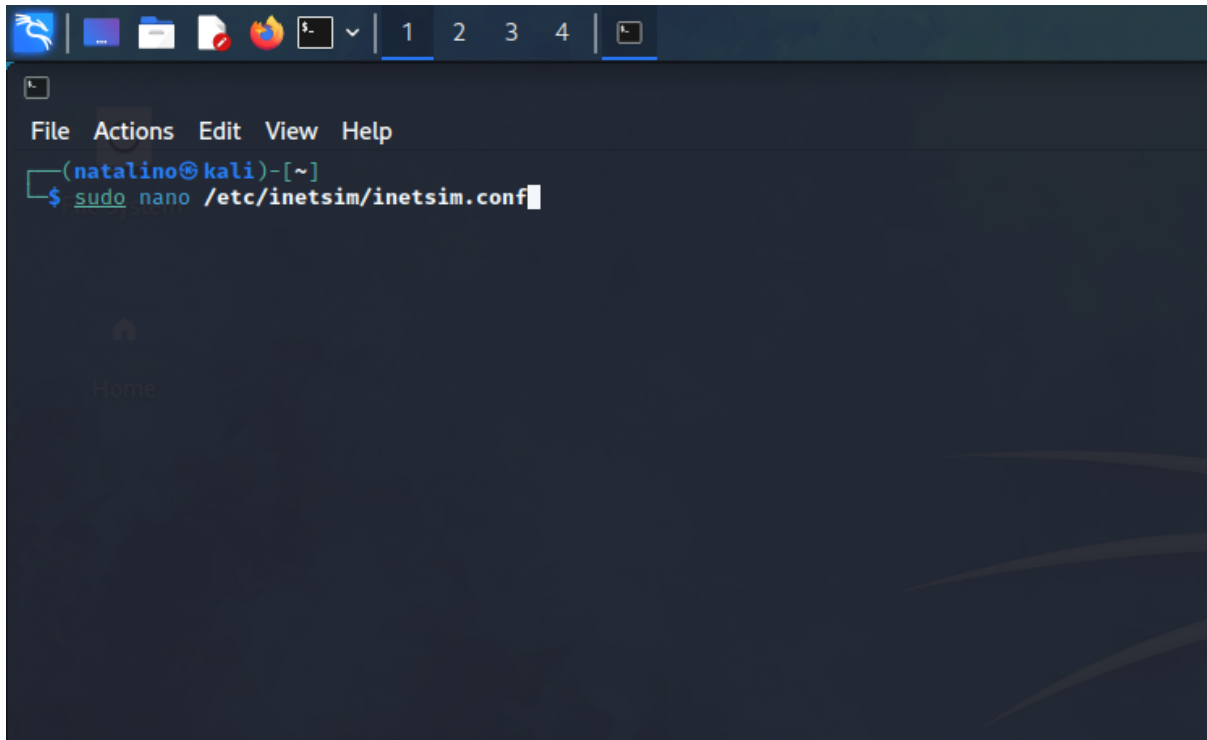
Ho settato l'IP di Windows 7



e l'ho assegnato alla macchina corrispondente

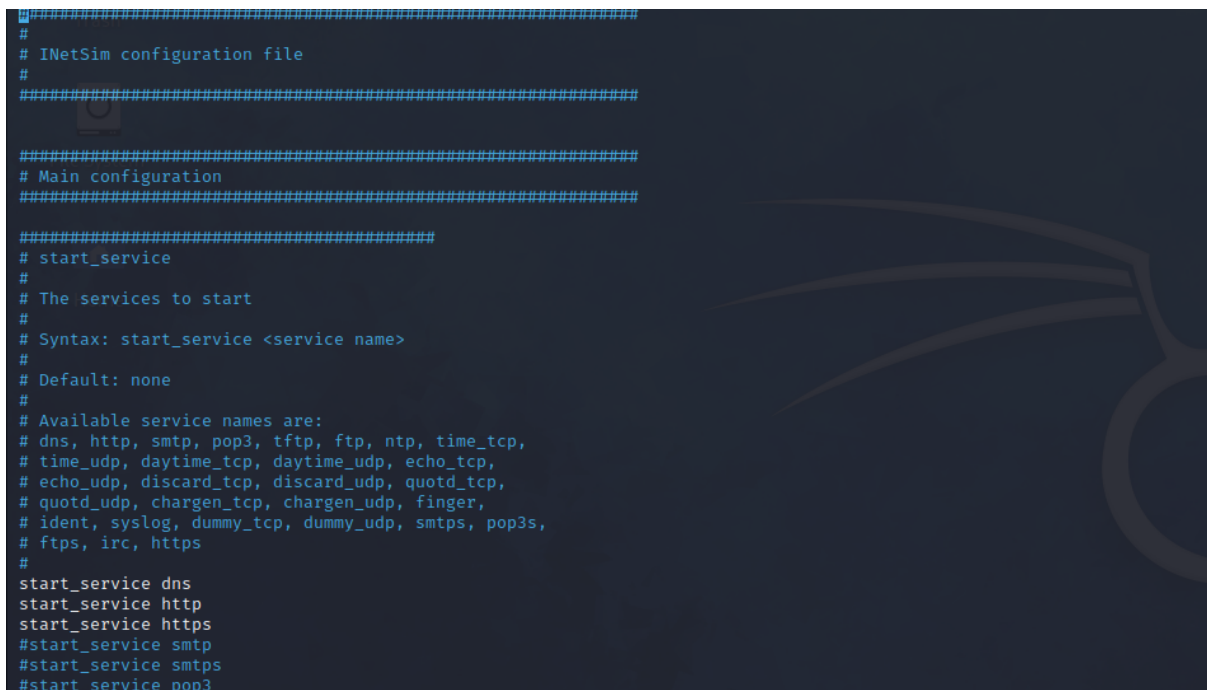


Ho avviato Kali e sulla shell ho lanciato il comando
`sudo nano /etc/inetsim/inetsim.conf`



The screenshot shows a Kali Linux desktop environment. The terminal window is open, displaying the command prompt `(natalino@kali)~` and the command `sudo nano /etc/inetsim/inetsim.conf` being entered. The terminal has a dark background with a light blue cursor. The desktop background is dark with a subtle pattern. The top of the window shows a taskbar with various application icons.

Qui innanzitutto sono andato ad attivare DNS, HTTP e HTTPS



The screenshot shows the `/etc/inetsim/inetsim.conf` file being edited in nano. The file contains configuration options for starting services. The visible text is as follows:

```
#####  
#  
# INetSim configuration file  
#  
#####  
  
#####  
# Main configuration  
#####  
  
#####  
# start_service  
#  
# The services to start  
#  
# Syntax: start_service <service name>  
#  
# Default: none  
#  
# Available service names are:  
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,  
# time_udp, daytime_tcp, daytime_udp, echo_tcp,  
# echo_udp, discard_tcp, discard_udp, quotd_tcp,  
# quotd_udp, chargen_tcp, chargen_udp, finger,  
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,  
# ftps, irc, https  
#  
start_service dns  
start_service http  
start_service https  
#start_service smtp  
#start_service smtps  
#start_service pop3
```

Poi sono andato a modificare l'IP

```
GNU nano 7.2 /etc/
#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

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100

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

```
#####
# dns_bind_port
#
# Port number to bind DNS service to
#
# Syntax: dns_bind_port <port number>
#
# Default: 53
#
#dns_bind_port 53

#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip 192.168.32.100

#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
#
#dns_default_hostname somehost
```

Il dominio

```
GNU nano 7.2
#
#dns_default_hostname somehost

#####
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: epicode.internal
#
dns_default_domainname www.epicode.internal.com
None

#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
#dns_static www.foo.com 10.10.10.10
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
dns_static www.epicode.internal.com 192.168.32.100

#####
# dns_version
#
# DNS version
#
# Syntax: dns_version <version>
#
# Default: "INetSim DNS Server"
#
#dns_version "9.2.4"
```

Ho attivato la porta

```
GNU nano 7.2
# Syntax: http_static_fakefile <path> <filename> <mime-type>
#
# Default: none
#
#http_static_fakefile /path/ sample_gui.exe x-msdos-program
#http_static_fakefile /path/to/file.exe sample_gui.exe x-msdos-program

File System
#####
# Service HTTPS
#####

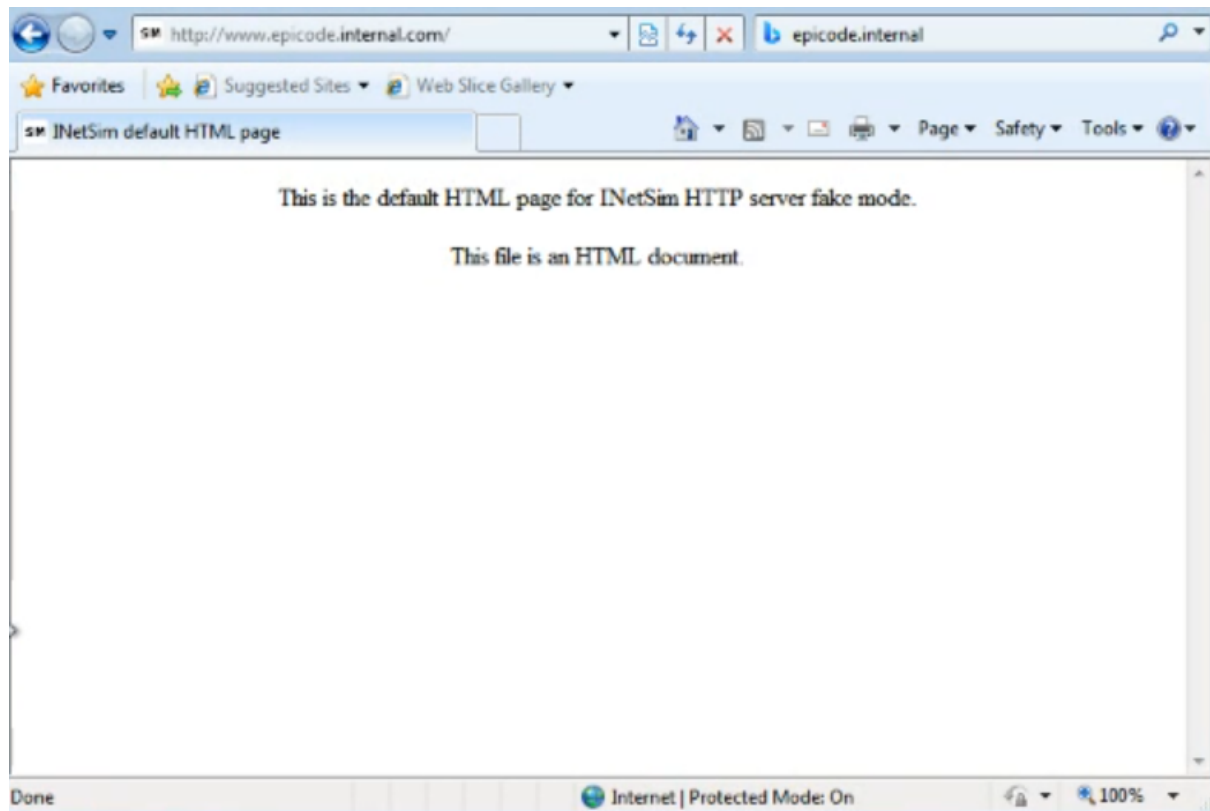
#####
https_bind_port
#
# Port number to bind HTTPS service to
#
# Syntax: https_bind_port <port number>
#
# Default: 443
https_bind_port 443

#####
# https_version
#
# Version string to return in HTTPS replies
#
# Syntax: https_version <string>
#
# Default: "INetSim HTTPs server"
#
#https_version "Microsoft-IIS/4.0"

#####
# https_post_limit
#
# Size limit for HTTPS POST requests
```

Ho salvato la nuova configurazione, sono uscito e ho avviato inetsim.

Poi ho puntato da Windows 7 al server con il dominio appena settato su Kali e ho ottenuto questo



Ho verificato che punta al server Kali con entrambi i protocolli, e analizzando il tutto con Wireshark ho potuto vedere questo

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000100745	192.168.32.101	192.168.32.100	TCP	60	60 80 -> 49179 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
4	0.000200127	192.168.32.100	192.168.32.101	TCP	60	49179 -> 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
5	0.000310520	192.168.32.101	192.168.32.100	HTTP	348	GET / HTTP/1.1
6	0.000492900	192.168.32.101	192.168.32.100	TCP	54	80 -> 49179 [ACK] Seq=1 Ack=295 Win=64128 Len=0
7	0.000591739	192.168.32.100	192.168.32.101	TCP	204	80 -> 49179 [PSH, ACK] Seq=1 Ack=295 Win=64128 Len=150 [TCP segment of a reassembled PDU]
8	0.220444210	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
9	0.220930879	192.168.32.100	192.168.32.101	TCP	60	49179 -> 80 [ACK] Seq=295 Ack=410 Win=65292 Len=0
10	0.222164028	192.168.32.101	192.168.32.100	TCP	60	49179 -> 80 [FIN, ACK] Seq=295 Ack=410 Win=65292 Len=0
11	0.222265399	192.168.32.101	192.168.32.100	TCP	54	80 -> 49179 [ACK] Seq=410 Ack=296 Win=64128 Len=0
12	0.222278529	192.168.32.100	192.168.32.101	TCP	54	80 -> 49179 [ACK] Seq=410 Ack=296 Win=64128 Len=0