Progetto - Modulo 1

Maurizio Cavazzoni

Nell’esercizio di oggi metteremo insieme le competenze acquisite finora.
Lo studente verrà valutato sulla base della risoluzione al problema seguente.

Requisiti e servizi:

- Kali Linux □ IP 192.168.32.100
- Windows 7 □ IP 192.168.32.101
- HTTPS server: attivo
- Servizio DNS per risoluzione nomi di dominio: attivo

Traccia:

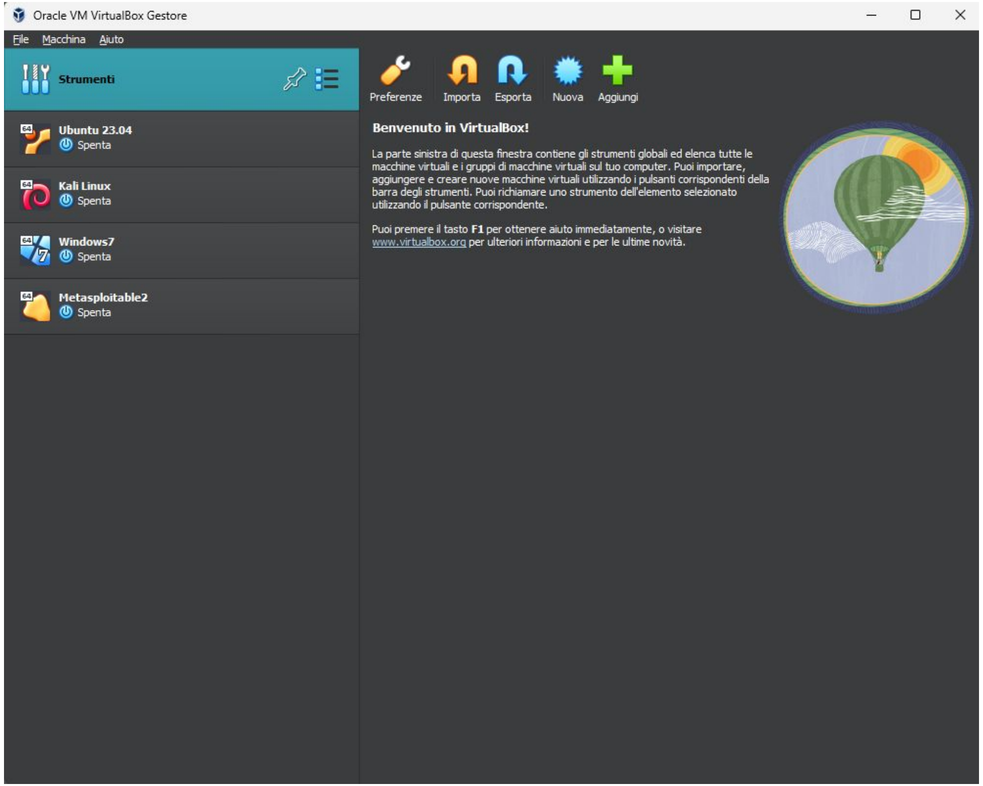
Simulare, in ambiente di laboratorio virtuale, un’architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all’hostname epicode.internal che risponde all’indirizzo 192.168.32.100 (Kali).

Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

Ripetere l’esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

Oracle VirtualBox

Questa è la VirtualBox installata nel mio PC con le macchine virtuali utilizzate nella prima settimana di corso



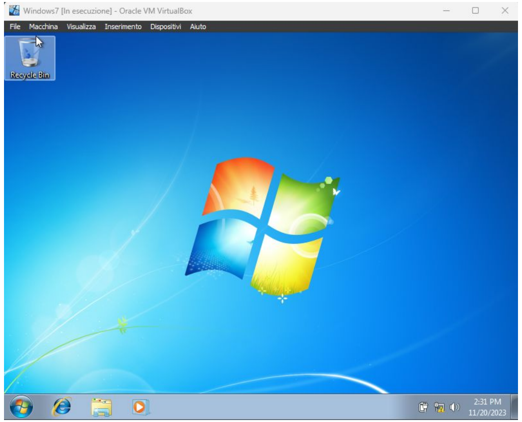
Benvenuto in VirtualBox!

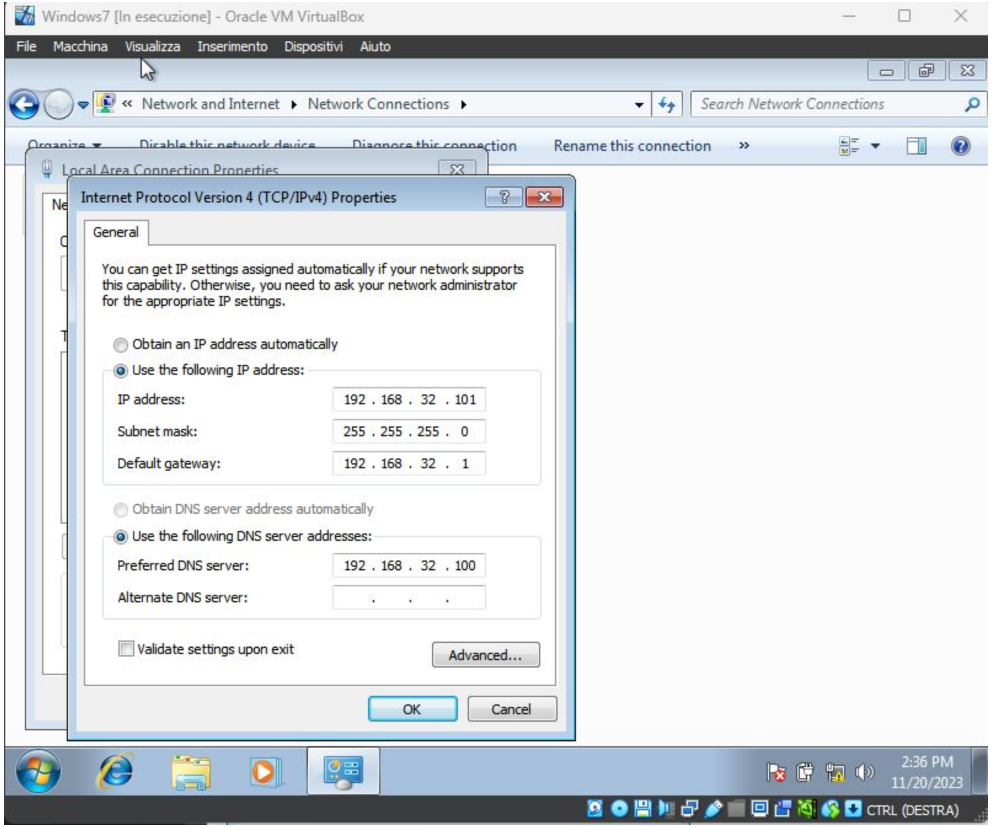
La parte sinistra di questa finestra contiene gli strumenti globali ed elenca tutte le macchine virtuali e i gruppi di macchine virtuali sul tuo computer. Puoi importare, aggiungere e creare nuove macchine virtuali utilizzando i pulsanti corrispondenti della barra degli strumenti. Puoi richiamare uno strumento dell'elemento selezionato utilizzando il pulsante corrispondente.

Puoi premere il tasto **F1** per ottenere aiuto immediatamente, o visitare www.virtualbox.org per ulteriori informazioni e per le ultime novità.

Windows 7

Accendo la macchina Windows 7, inserisco l'IP della macchina e l'indirizzo per il DNS


Windows7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Recycle Bin
2:31 PM
11/20/2023


Windows7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾ Disable this network device Diagnose this connection Rename this connection »
Local Area Connection Properties
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Advanced...
OK
Cancel
2:36 PM
11/20/2023
CTRL (DESTRA)

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 32 . 101
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 32 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 32 . 100
Alternate DNS server:	. . .

□ Validate settings upon exit

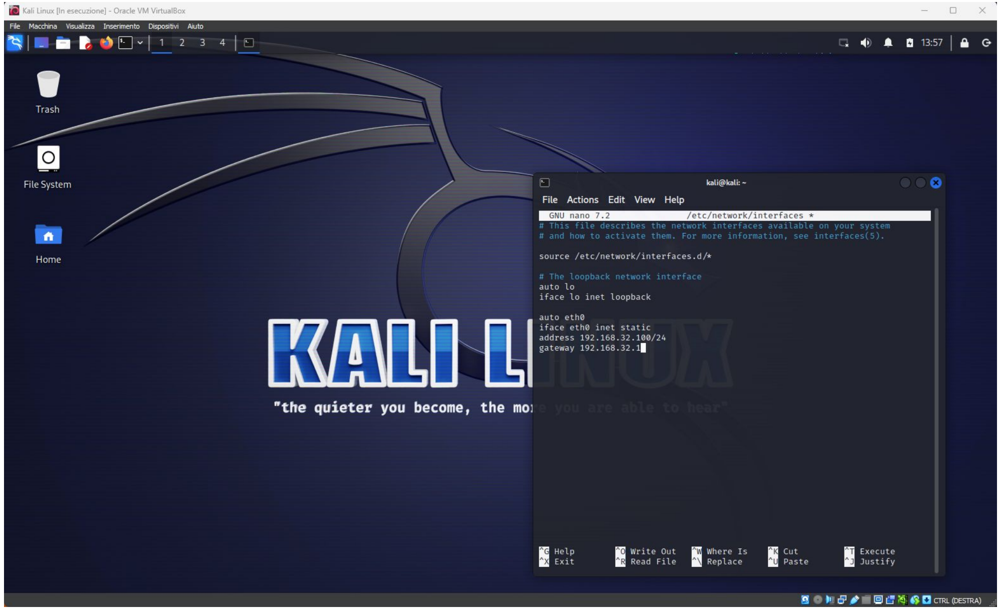
Kali Linux

sudo nano /etc/network/interfaces

è il comando per configurare la rete

sudo ci consente di eseguire un comando con i diritti di super amministratore del sistema

nano è un editor di testo con il quale noi possiamo interagire e scrivere un file



```
  GNU nano 7.2                /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.32.100/24
gateway 192.168.32.1
```

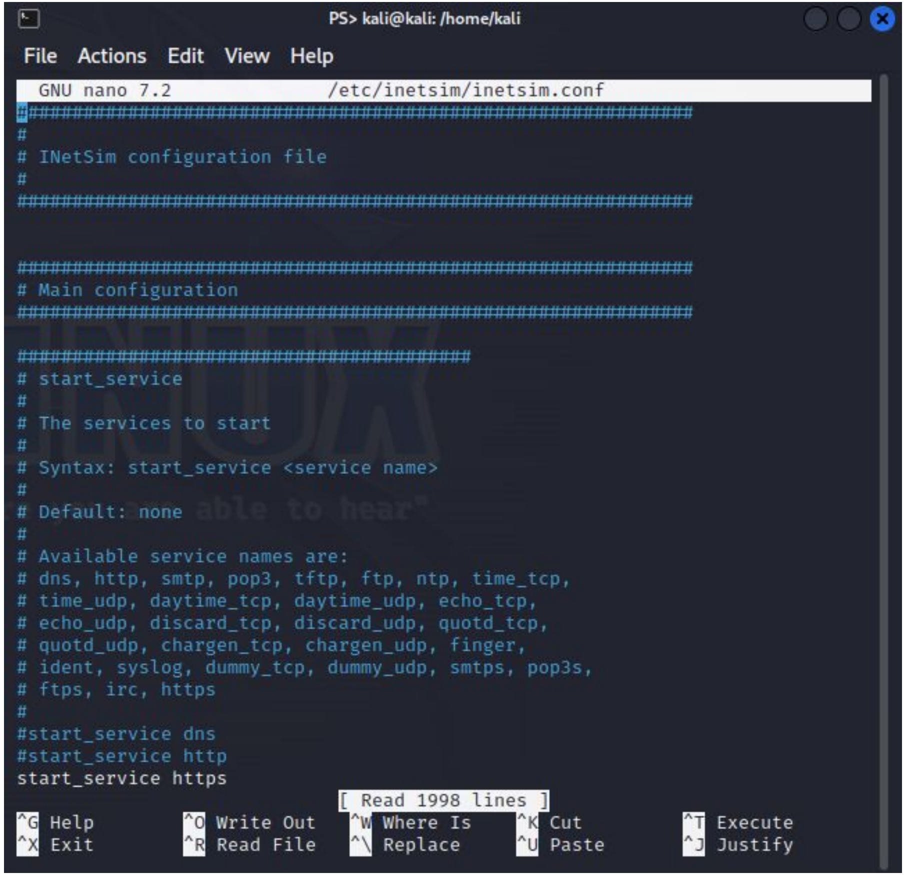
```
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

InetSim

Utilizziamo InetSim, simulatore di servizi internet preinstallato in Kali Linux

I comandi per abilitare la configurazione sono

sudo nano /etc/inetsim/inetsim.conf



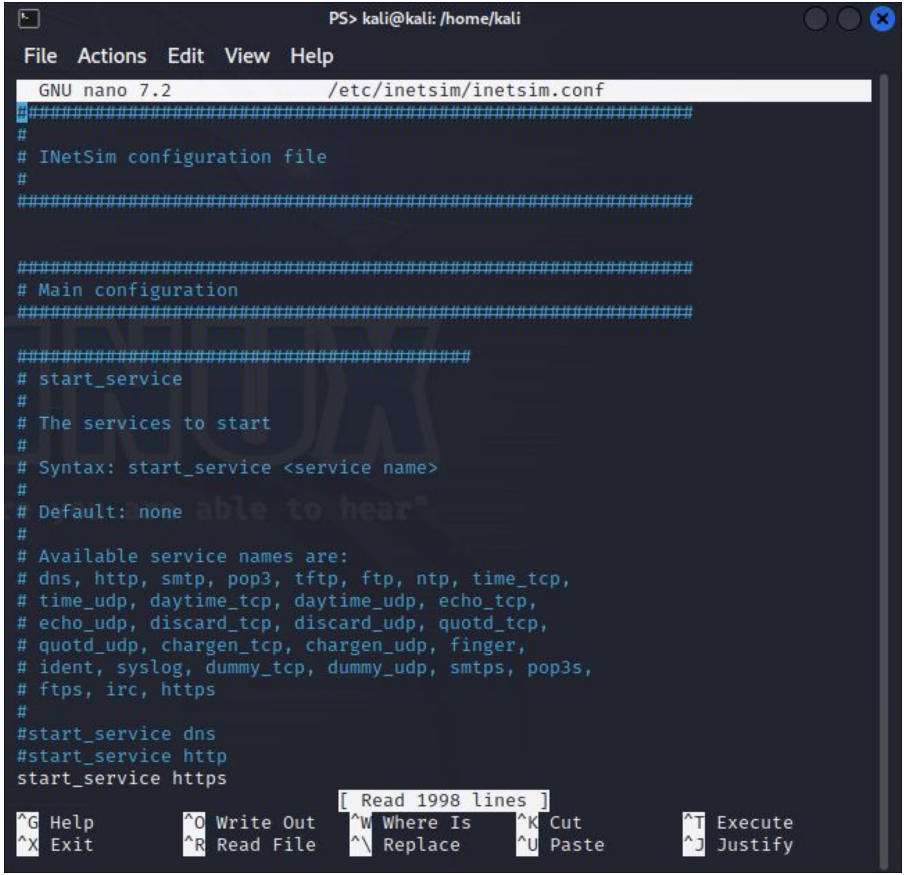
```
  GNU nano 7.2                  /etc/inetsim/inetsim.conf
#############################################################
#
# INetSim configuration file
#
#############################################################


#############################################################
# 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
                             [ Read 1998 lines ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify
```

InetSim

Utilizziamo InetSim, simulatore di servizi internet preinstallato in Kali Linux

I comandi per abilitare la configurazione sono

sudo nano /etc/inetsim/inetsim.conf



```
  GNU nano 7.2              /etc/inetsim/inetsim.conf
#############################################################
#
# 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
                             [ Read 1998 lines ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

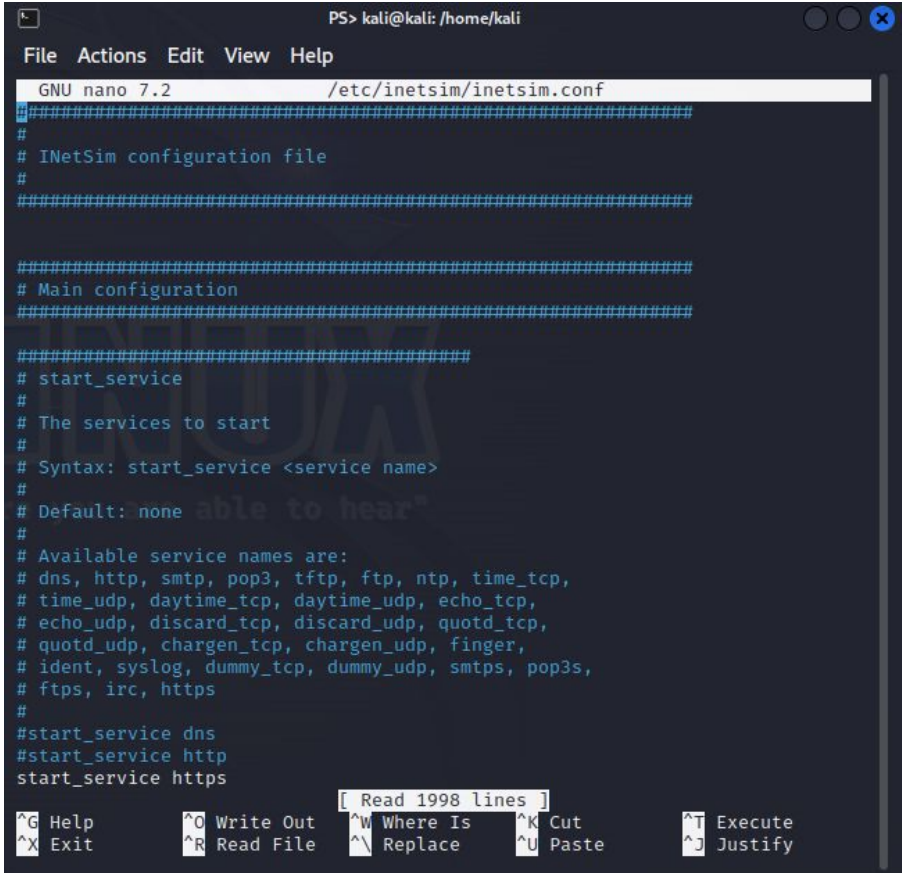
InetSim

Le sezioni da configurare sono:

-la sezione del DNS

-La sezione dei protocolli

-La sezione del bind address (dove dobbiamo inserire l'indirizzo di Windows) o, per semplificare, 0.0.0.0.



```
  GNU nano 7.2                /etc/inetsim/inetsim.conf
#############################################################
#
# 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
                             [ Read 1998 lines ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

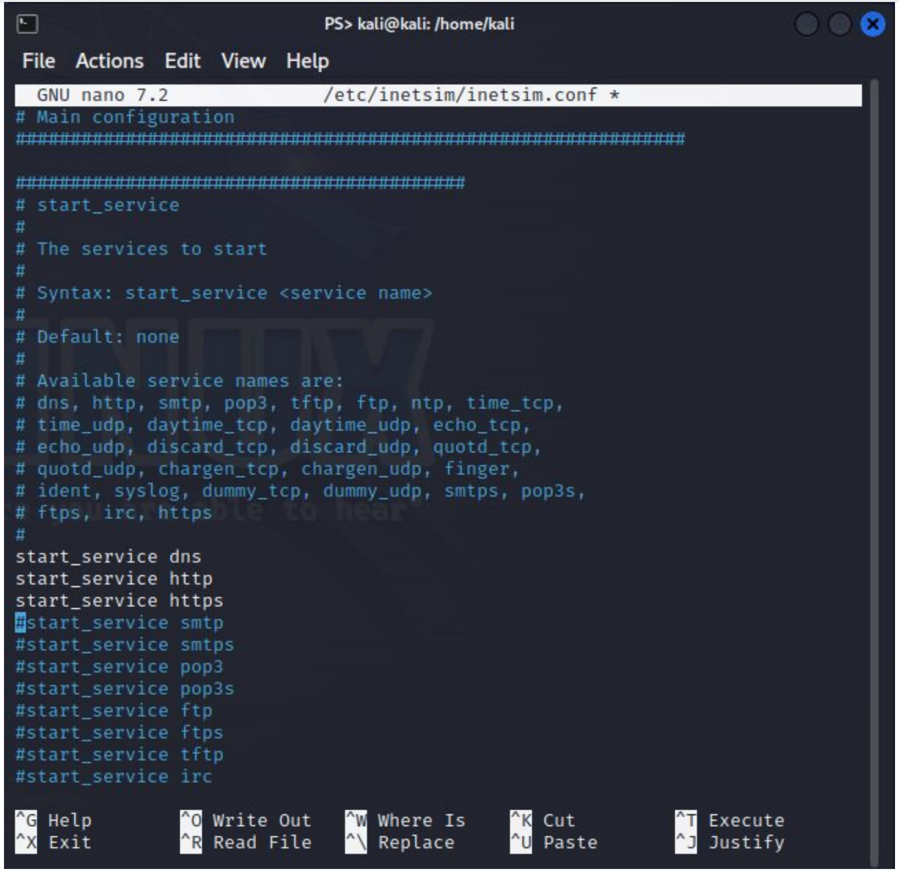
InetSim

Abilito i servizi:

- DNS

- HTTP

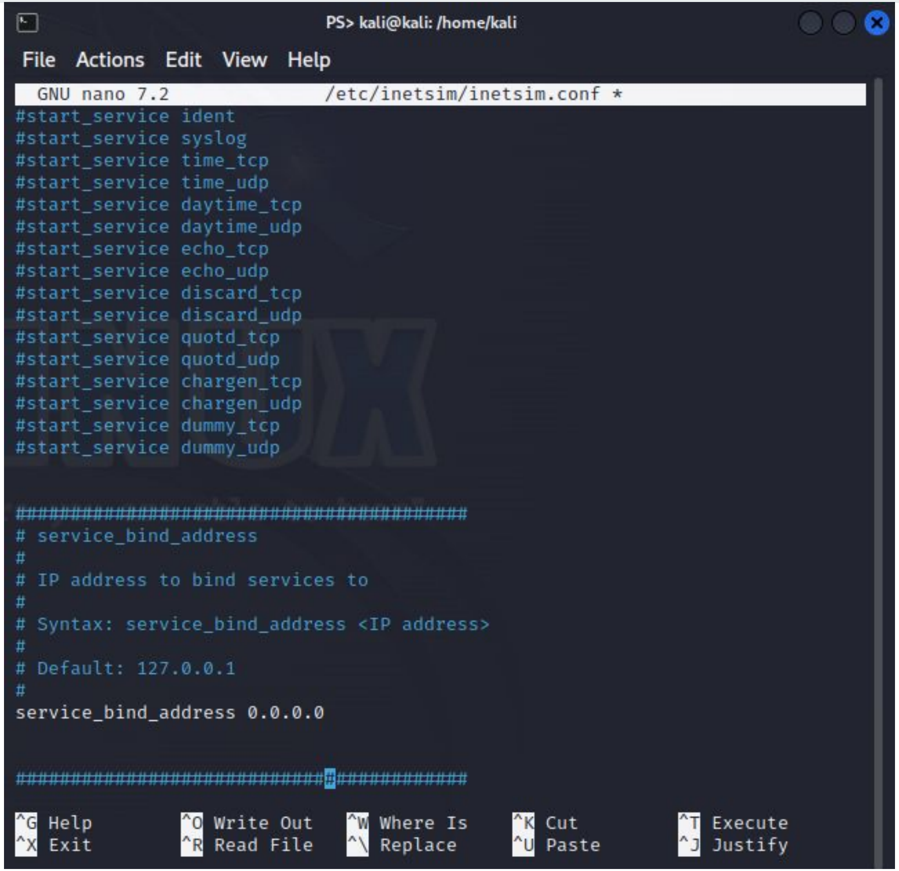
- HTTPS



```
  GNU nano 7.2                    /etc/inetsim/inetsim.conf *
# 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
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc

^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

InetSim

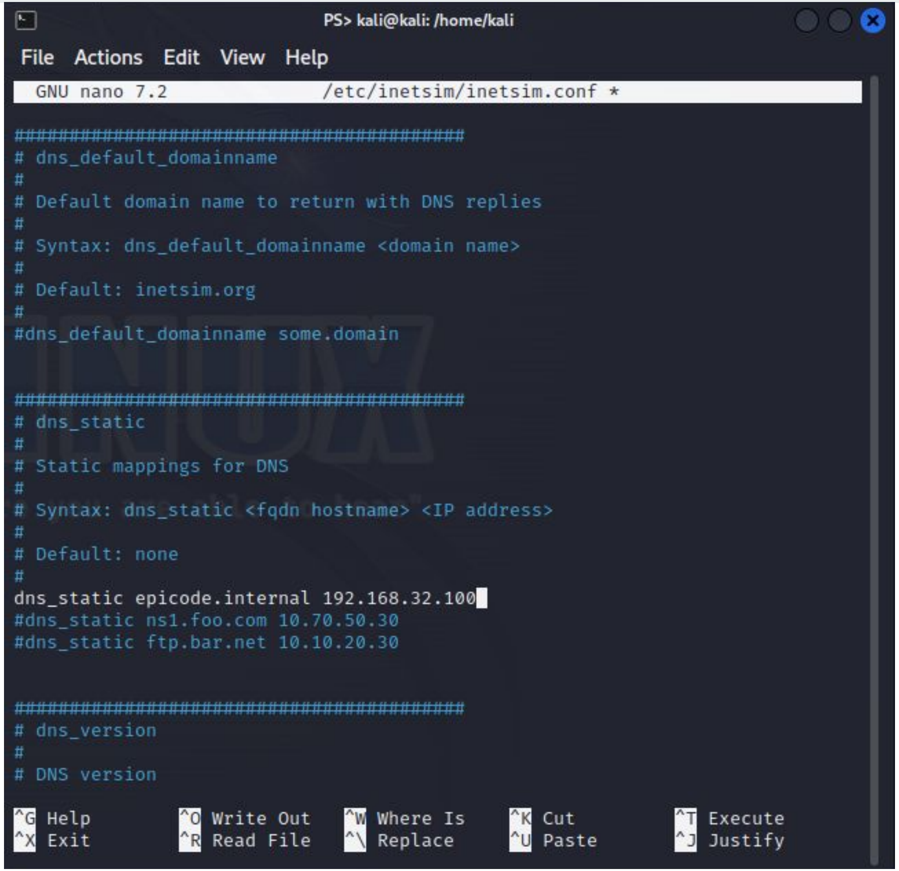
Configuro la sezione del bind address inserendo, per semplificare, 0.0.0.0.



```
  GNU nano 7.2                    /etc/inetsim/inetsim.conf *
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp
#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 0.0.0.0


#########################################

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify
```

InetSim

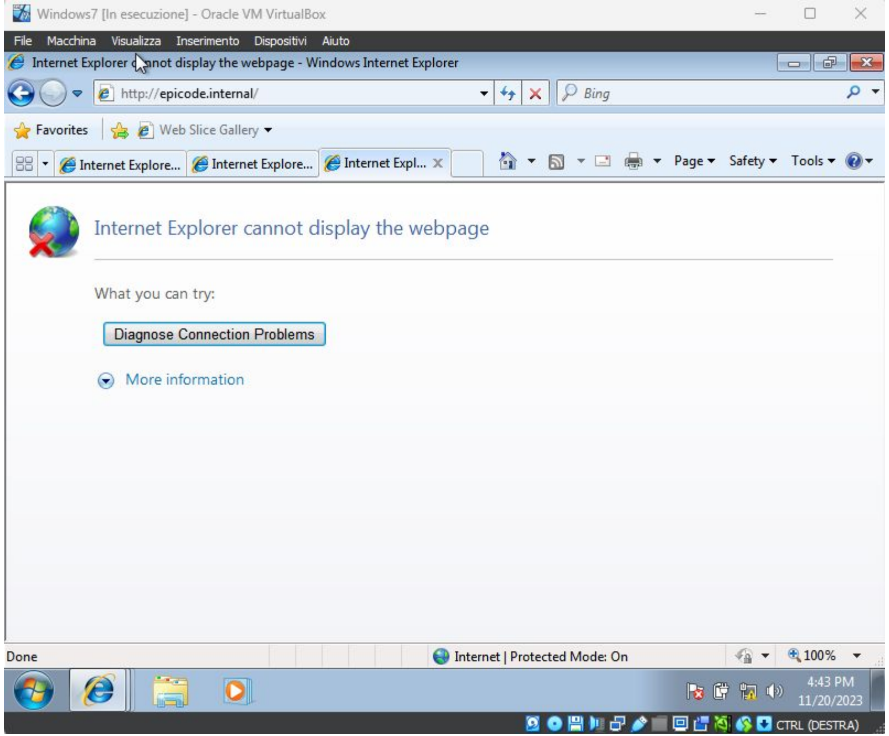
Configuro la sezione del DNS inserendo l'hostname epicode.internal e l'indirizzo IP (della macchina Kali) al quale corrisponde



```
  GNU nano 7.2                   /etc/inetsim/inetsim.conf *

#########################################
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
#dns_default_domainname some.domain


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


#########################################
# dns_version
#
# DNS version
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify
```

Navigazione della pagina

Apro Explorer in Windows 7 e provo a raggiungere epicode.internal ma non si apre la pagina


Windows7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Internet Explorer cannot display the webpage - Windows Internet Explorer
http://epicode.internal/
Bing
Favorites
Web Slice Gallery
Internet Explore...
Internet Explore...
Internet Expl...
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%
4:43 PM
11/20/2023
CTRL (DESTRA)

Internet Explorer cannot display the webpage

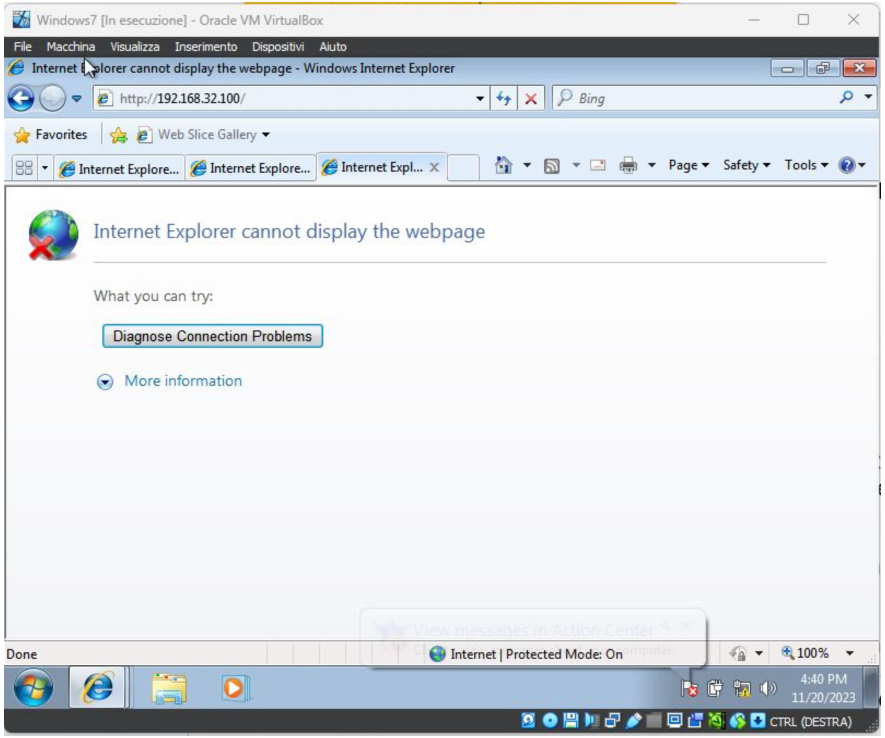
What you can try:

Diagnose Connection Problems

More information

Navigazione della pagina

Non si apre nemmeno con l’IP



Internet Explorer cannot display the webpage

What you can try:

Windows7 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Internet Explorer cannot display the webpage - Windows Internet Explorer
http://192.168.32.100/
Bing
Favorites
Web Slice Gallery
Internet Explore...
Internet Explore...
Internet Expl...
Page
Safety
Tools
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: On
100%
4:40 PM
11/20/2023
CTRL (DESTRA)