# Simulazione architettura Cliente Server

## Fernando Catrambone

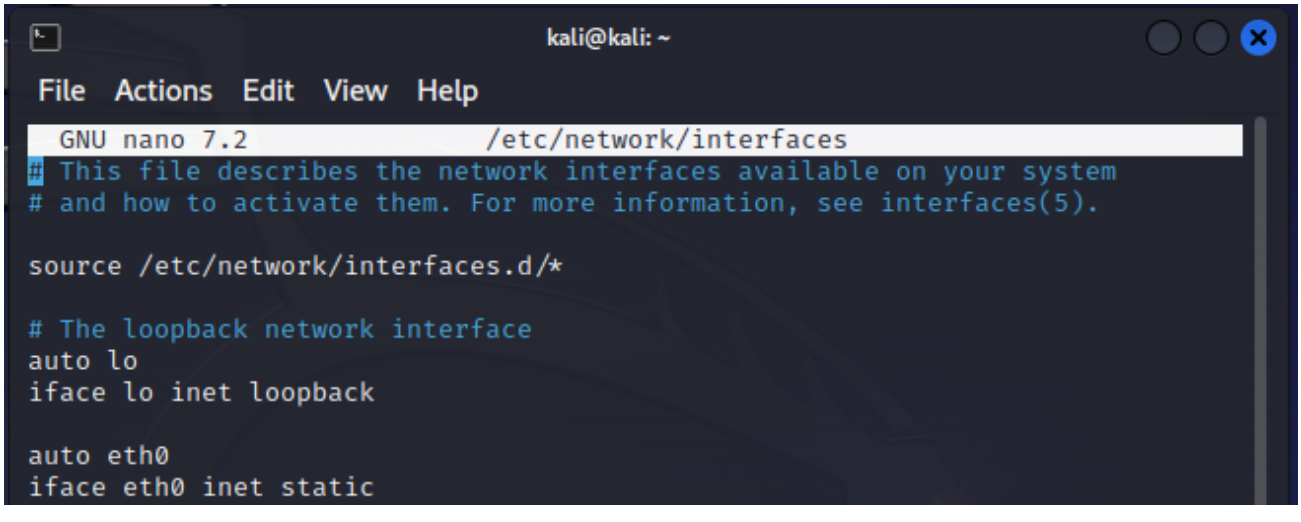
**In questo progetto andrò a simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100. Successivamente intercetterò la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS. Ripeterò la simulazione, sostituendo il server HTTPS, con un server HTTP. Intercettando nuovamente il traffico, evidenzierò le differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS.**

## Dettagli del progetto

### Configurazione VM

**-Ho configurato gli IP di Kali Linux e Windows**

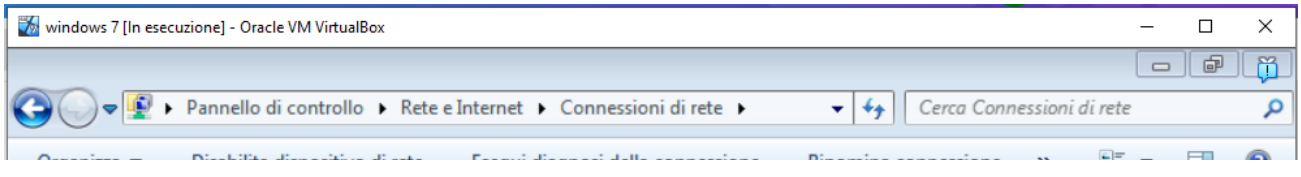
**Su Kali ho modificato il file /etc/network/interfaces assegnado l'IP 192.168.32.100**

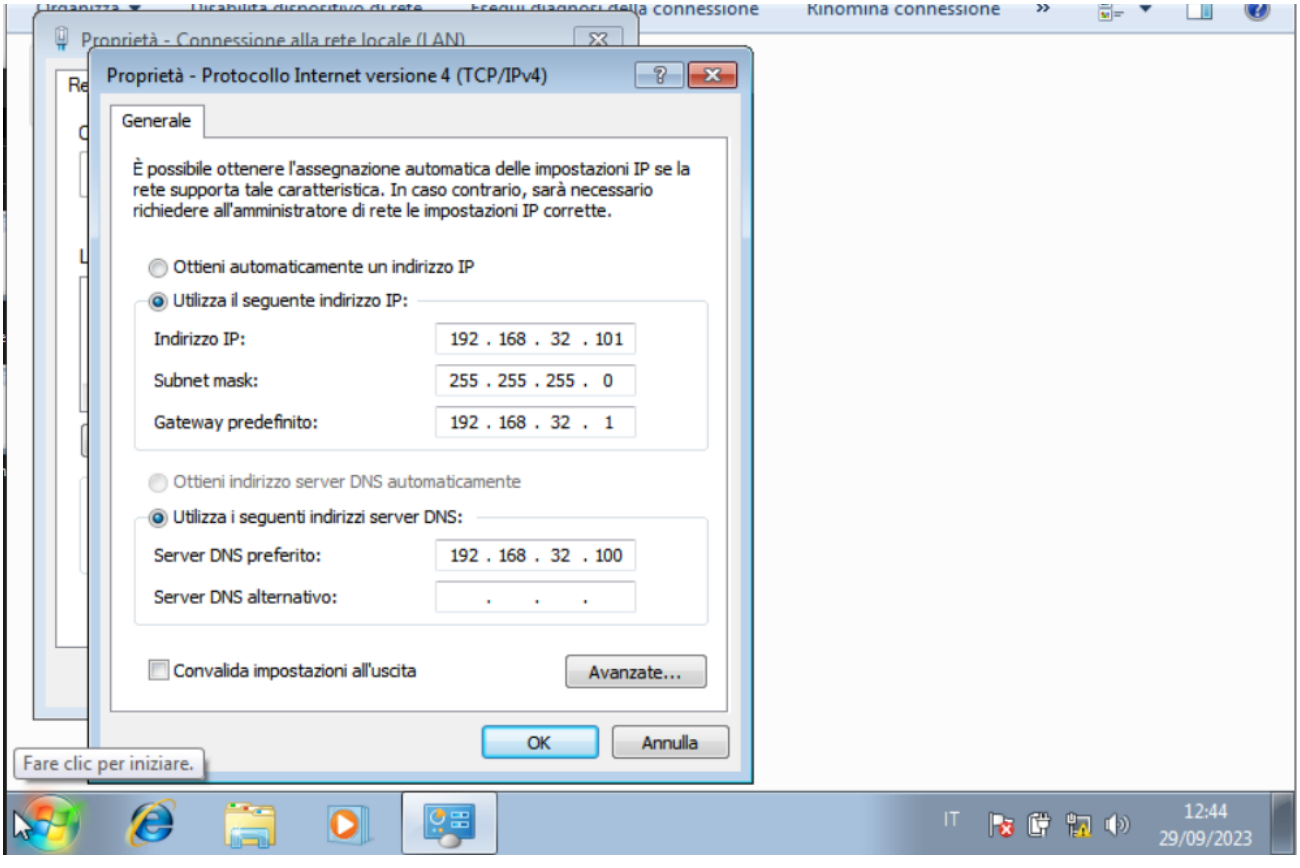


```
address 192.168.32.100
netmask 255.255.255.0
network 192.168.32.0
broadcast 192.168.32.255
gateway 192.168.32.1



                [ Read 16 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/network/interfaces

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.100  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::a00:27ff:fecb:7ef5  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 700  bytes 60521 (59.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 385  bytes 50529 (49.3 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 44  bytes 2240 (2.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44  bytes 2240 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$
```

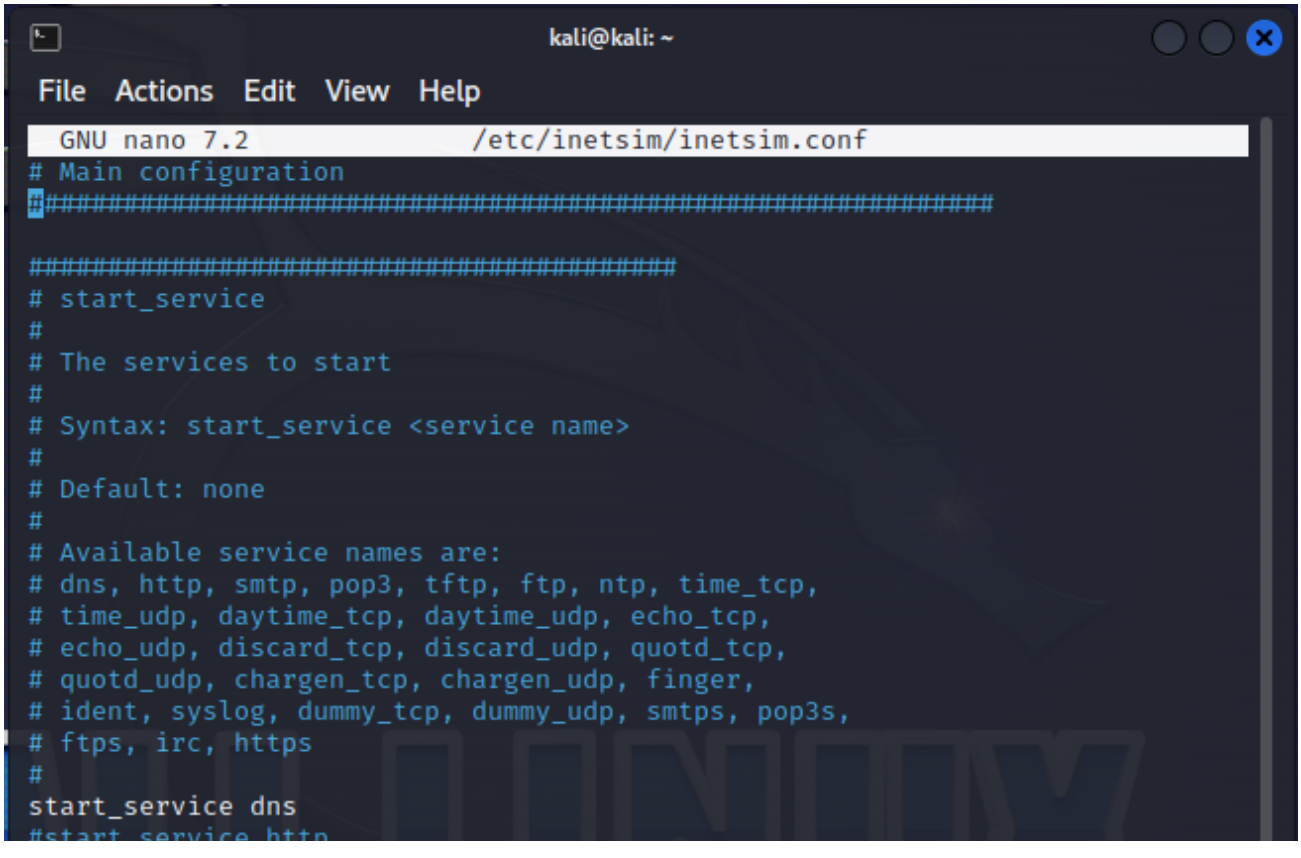
**Successivamente ho ho modificato l'IP di Windows 7 inserendo come indirizzo IP 192.168.32.101 e impostando come server DNS 192.168.32.100 ovvero l'indirizzo IP di Kali**





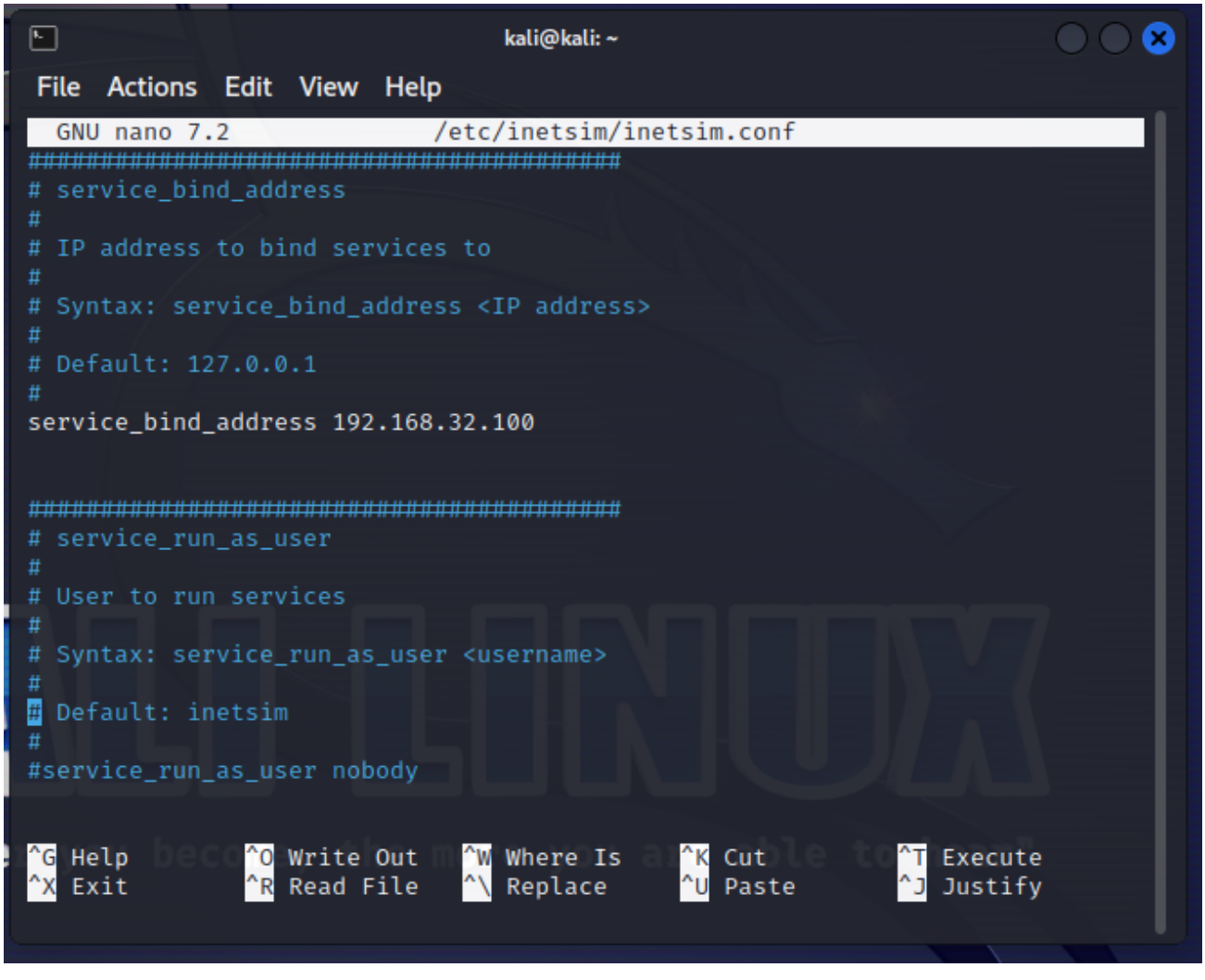

## Configurazione Inetsim

**-Attivazione servizio HTTPS e DNS**

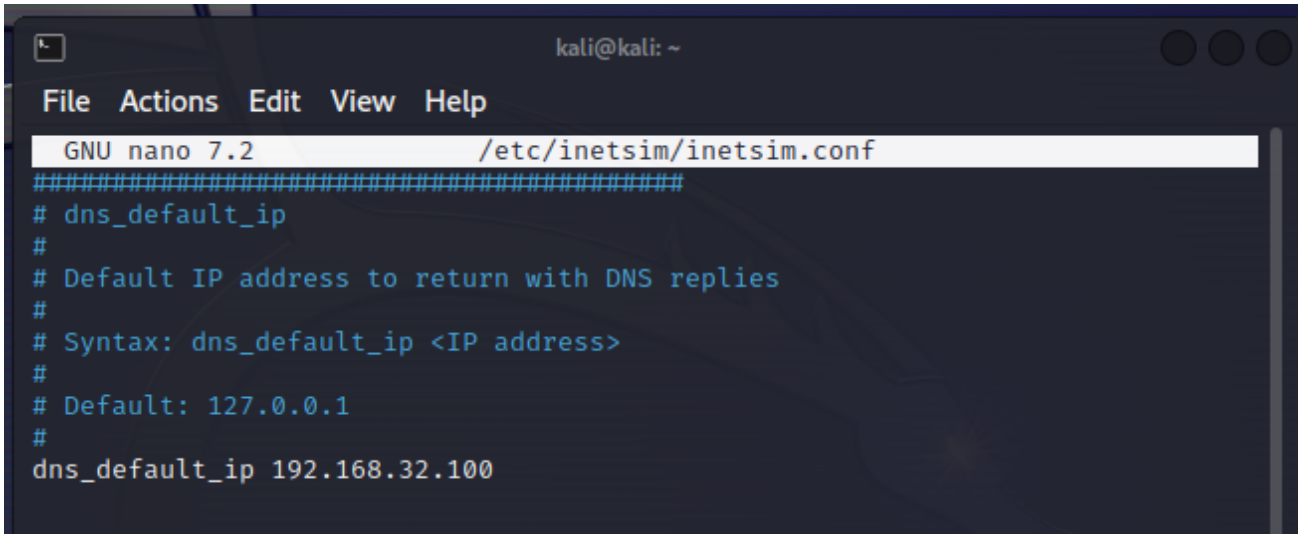


```
start_service https

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

**-Configurazione bind address all'indirizzo 192.168.32.100**




**-Configurazione server DNS all'indirizzo IP di Kali e il nome del dominio epicode.internal**



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

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

kali@kali: ~

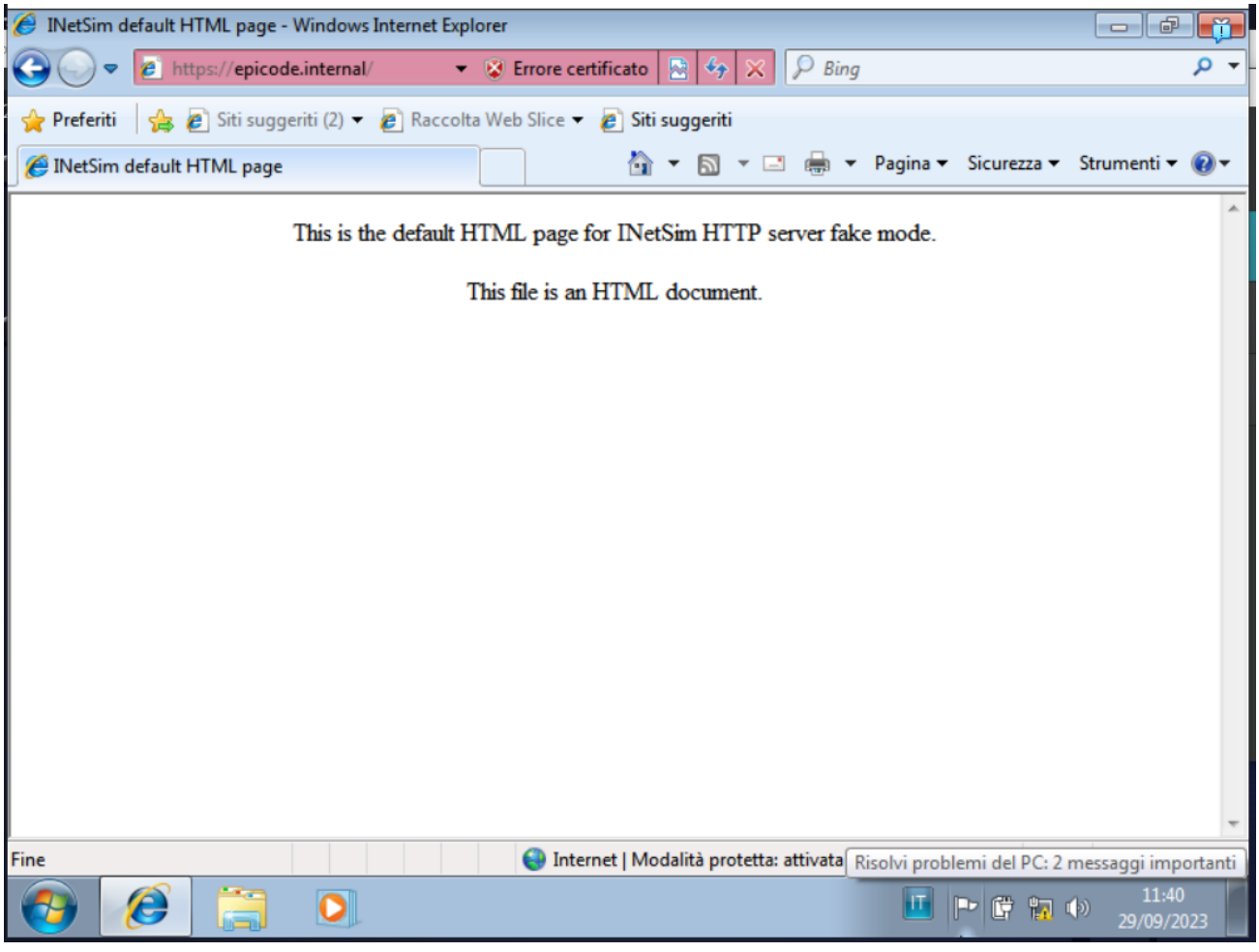
File Actions Edit View Help

```
  GNU nano 7.2                 /etc/inetsim/inetsim.conf
#dns_default_hostname somehost


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


##############################################
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none

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

## RIchiesta tramite browser del dominio epicode.internal

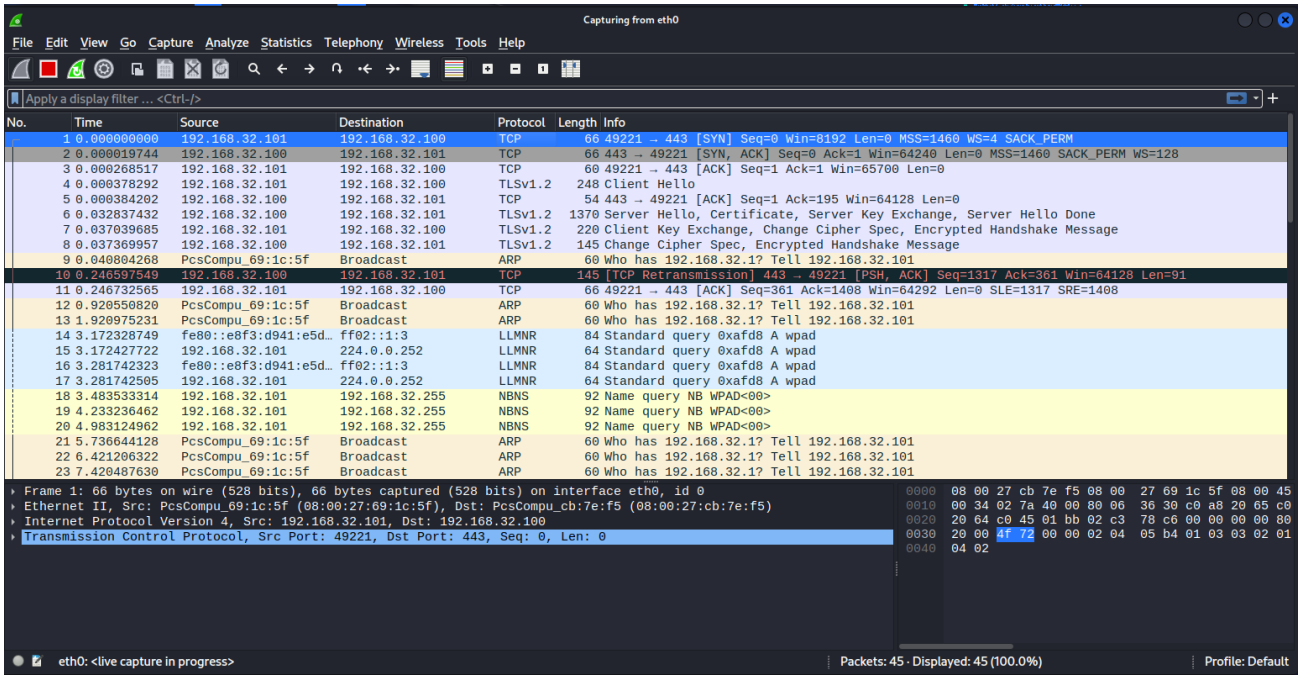
**-Su Windows 7 ho dato il consenso all'utilizzo dei certificati TLS e SSL ed ho inserito nella barra degli indirizzi il nome del dominio che ho assegnato precedentemente**

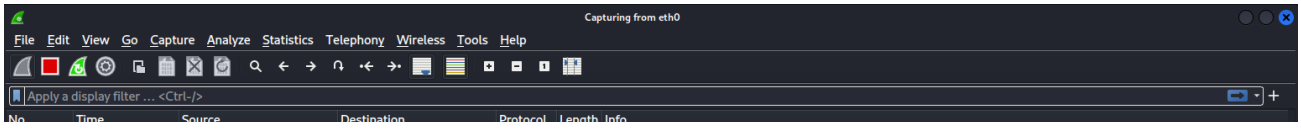
windows 7 [In esecuzione] - Oracle VM VirtualBox

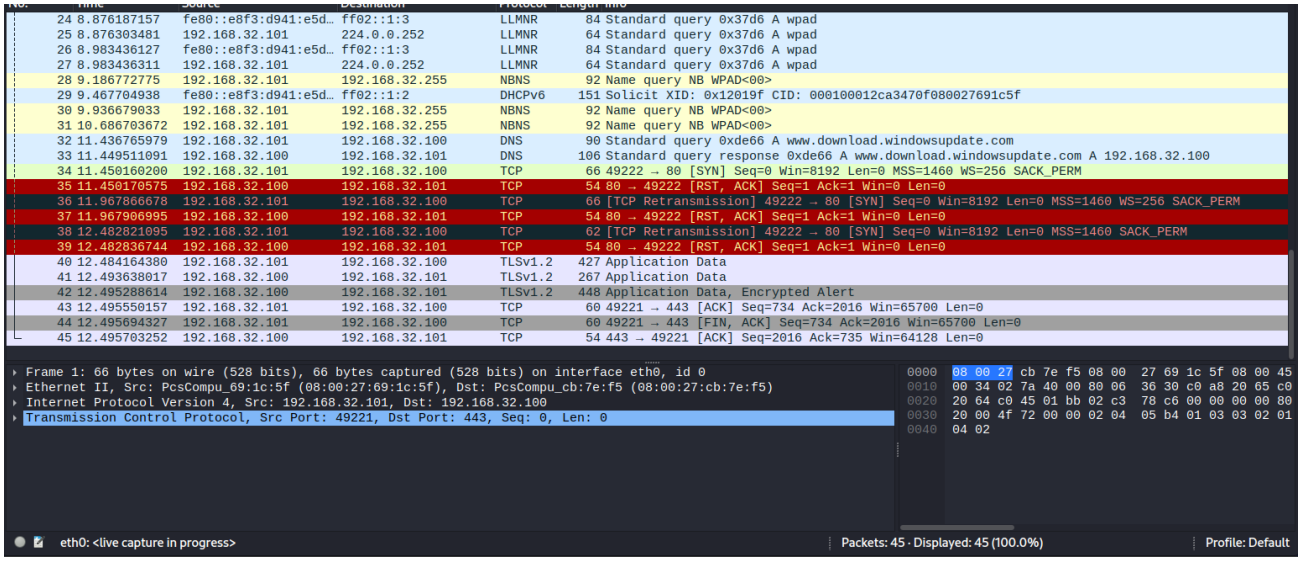



**Il browser restituisce la paggina predefinita di Inetsim**

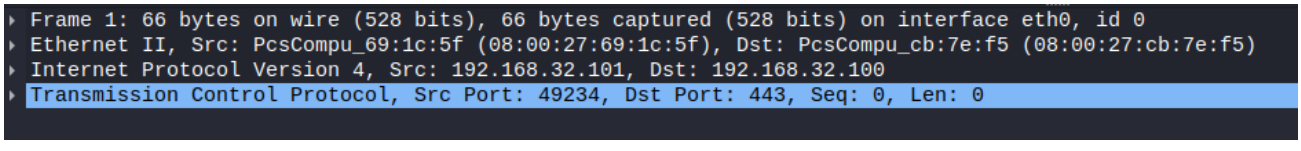
**-Intercetto con Wireshark la comunicazione tre Client e Server**





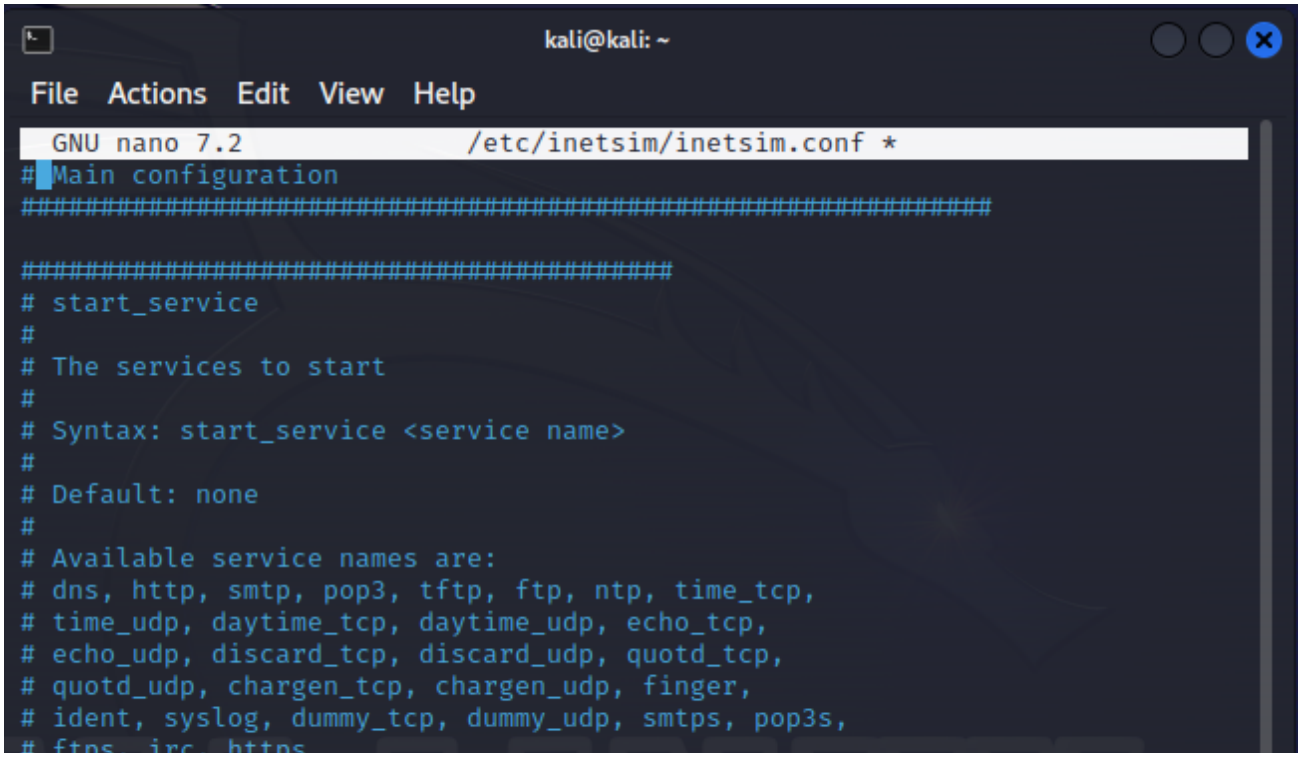

**Ecco i MAC Address dei due dispositivi**




**Nello screen si può notare che l'indirizzo sorgente è quello di Windows mentre il destinatario e Kali. Windows richiede i certificati TLS a Kali come da protocollo HTTPS affinchè la comunicazione tra i dispotivi sia sicura.**

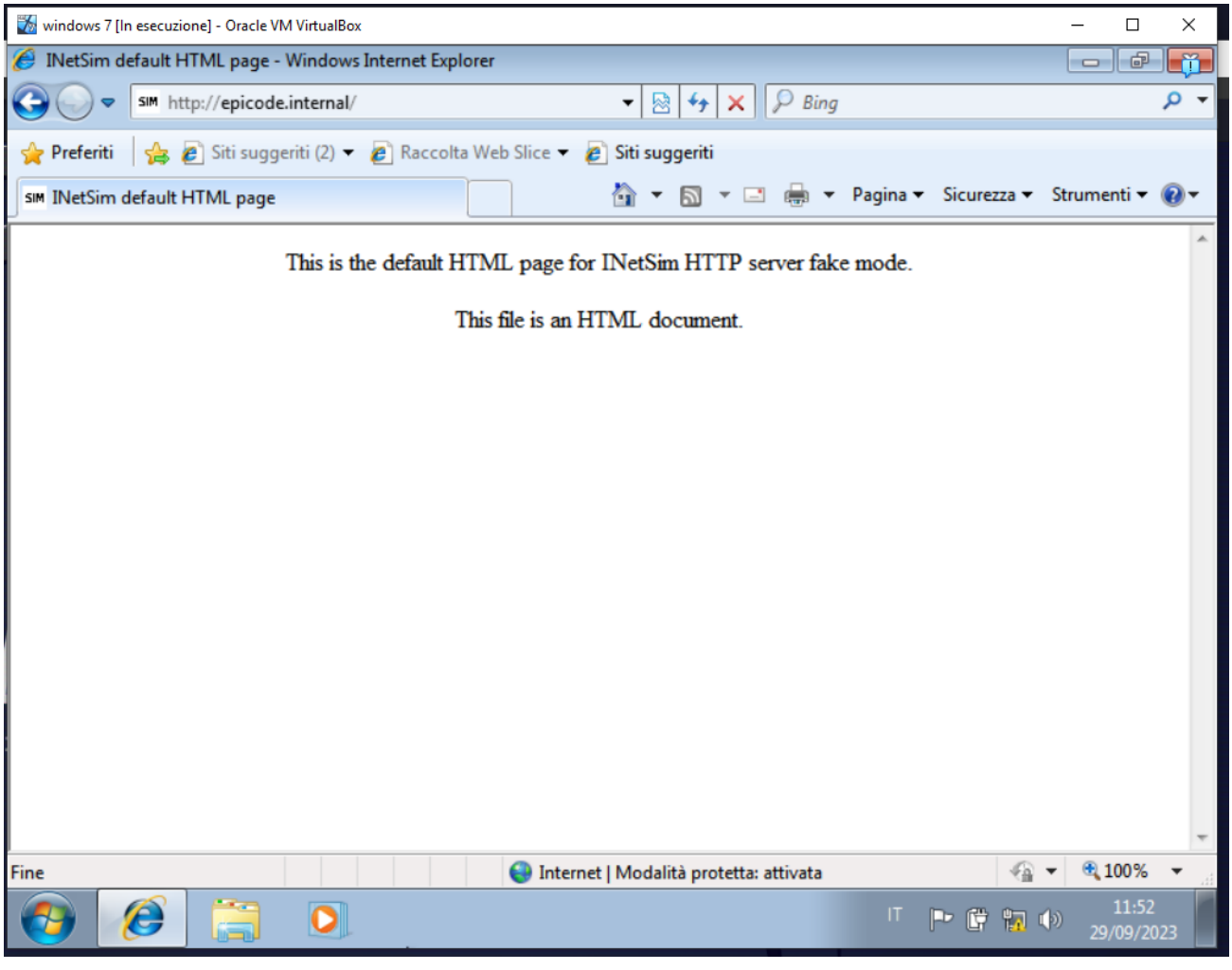
## Richiesta tramite server HTTP

**Ho attivato il servizio HTTP e disattivato quello HTTPS su Inetsim**



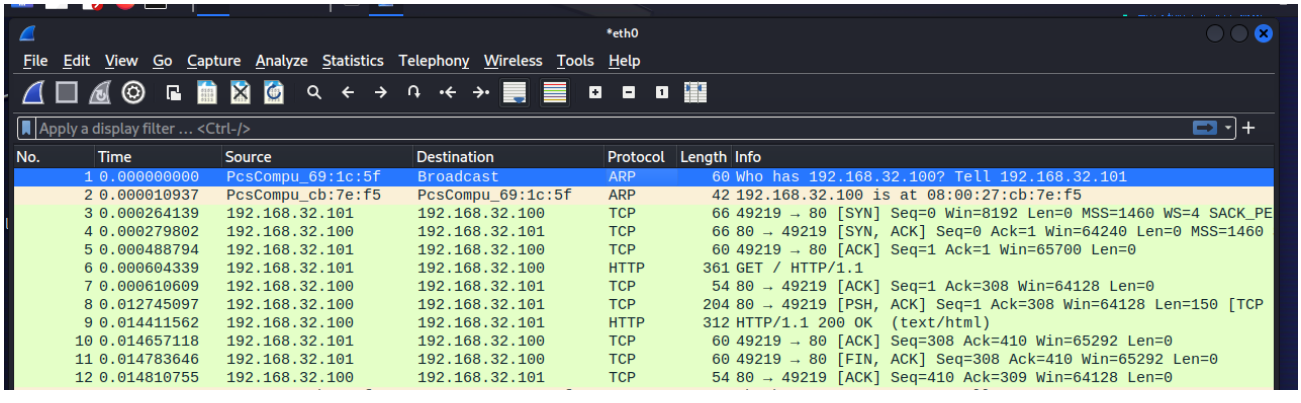
```
#
start_service dns
start_service http
#start_service https

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

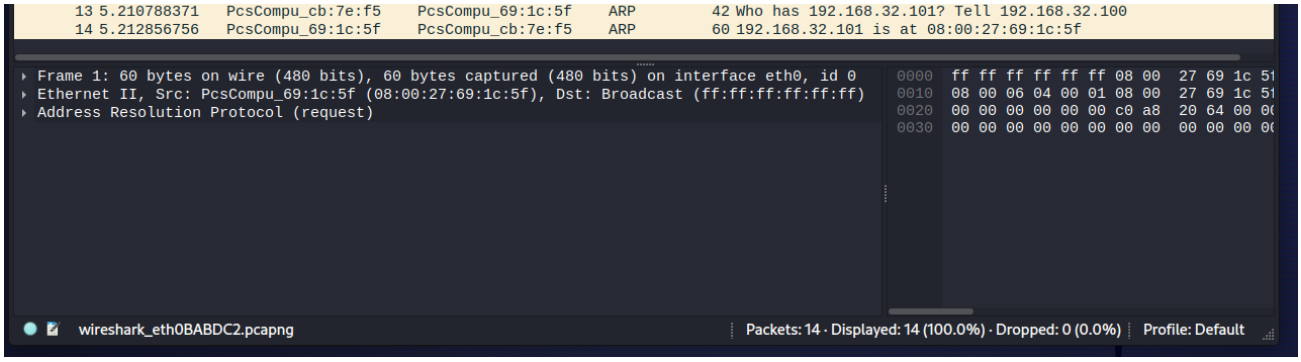
**Ho inserito il nome del dominio epicode.internal sul browser di windows**




**Come in precedenza il browser apre la pagina di default di Inetsim**

**-Analizzo il report di Wireshark**






**In questo caso possiamo notare che a differenza del HTTPS non richiede nessun certificato TLS e i file non sono criptati.**