

# CSPT0524

## Esercitazione progetto finale modulo M1 W4 D4

### INFORMAZIONI DEL DOCUMENTO

- |                   |   |
|-------------------|---|
| 1. Autore         | Giovanni D'Abrosca                            |
| 2. Nome Documento | Esercitazione progetto finale modulo M1 W4 D4 |
| 3. Data Emissione | 29/11/24                                      |

### Requisiti e servizi:

- Kali Linux: IP 192.168.32.100
- Windows: 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) 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.

# Sommario

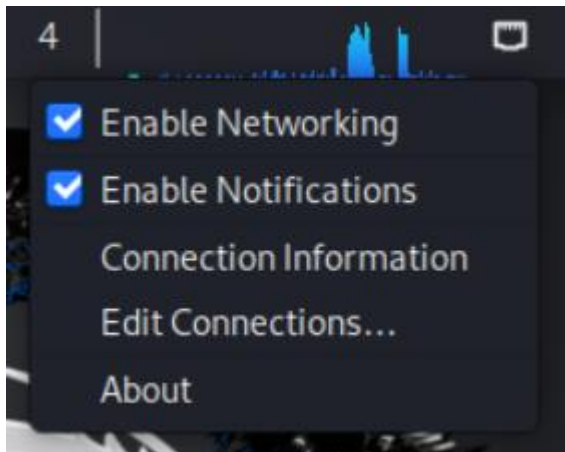
<b>Configurazione Kali Linux .....</b>	
Configurazione interfaccia di rete .....	
Configurazione DNS Server.....	
Configurazione servizio https.....	
Configurazione servizio http .....	
<b>Configurazione di rete Win10 .....</b>	
Configurazione interfaccia di rete .....	
Verifica funzionamento di connessione da web .....	
<b>Controllo traffico utilizzando wireshark.....</b>	
Controllo dei pacchetti trasmessi in https .....	
Controllo dei pacchetti trasmessi in http .....	
<b>Differenza di trasmissione pacchetti .....</b>	
Differenza di pacchetti trasmessi in https.....	
Differenza di pacchetti trasmessi in http .....	

## Configurazione Interfaccia di rete Kali Linux

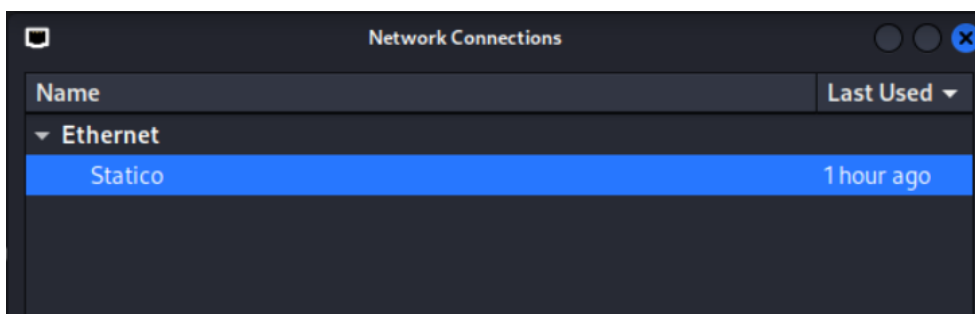
Di seguito ho impostato l'interfaccia di rete settando l'IP indicato dalla traccia.

Per impostare l'interfaccia di rete ho eseguito i seguenti passaggi:

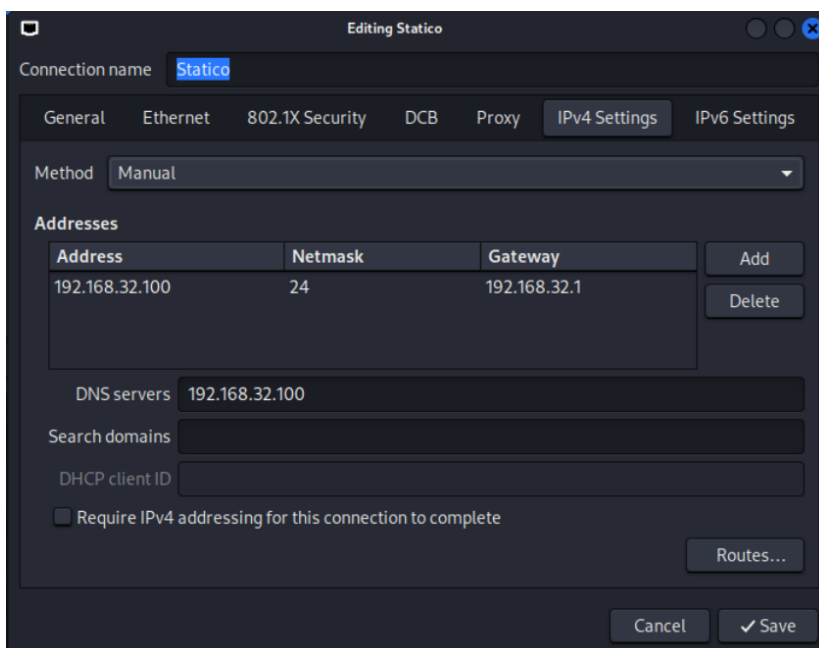
tasto destro sul network manager e di seguito doppio click su edit connections



Dopo aver cliccato su edit connectios si è aperta la seguente finestra:



Doppio click su statico e si apre la schermata per settare l'IP statico richiesto dalla traccia (192.168.32.100)



## Configurazione DNS Server

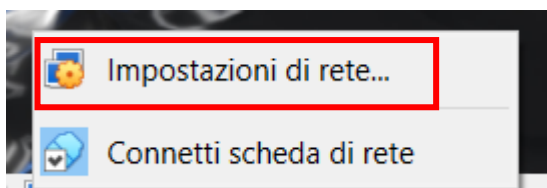
per configurare il servizio DNS è stato necessario modificare le impostazioni di Kali Linux,

si è dovuti togliere kali dalla rete intnet e impostarlo in nat dal pannello di virtualbox:

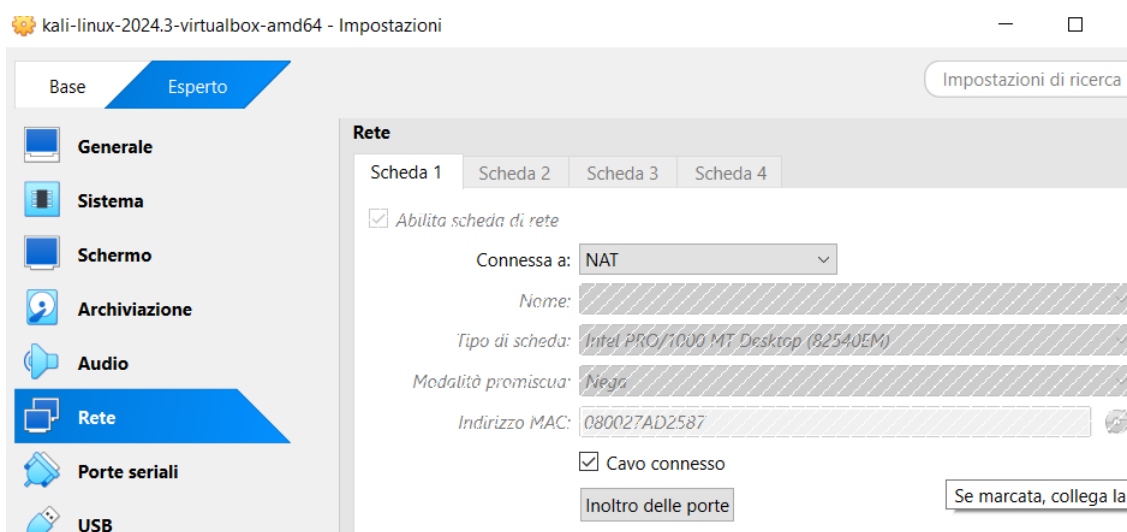
per accedere alle impostazioni di virtualbox fare click con il tasto destro sull'icona dei due pc di seguito uno screen:



Una volta cliccato con il tasto destro sull'icona ci apre la seguente schermata:



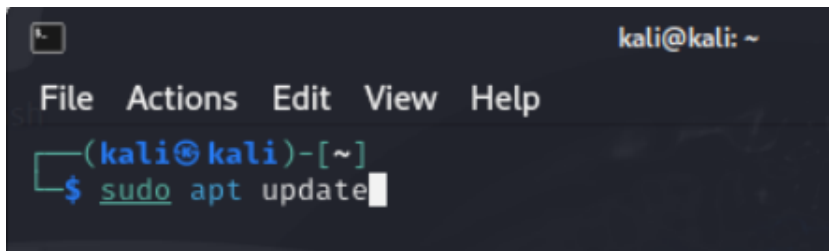
Cliccare su impostazioni di rete e si aprirà la finestra per settare la VM da intnet a nat



Questa procedura è stata fatta per consentire la navigazione in Internet alla VM di Kali

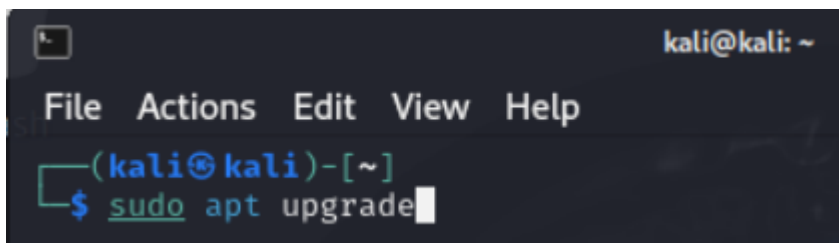
Fatto ciò, bisogna aprire un terminale e procedere ad aggiornare Kali digitando i seguenti comandi

Sudo apt update



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt update
```

Sudo apt upgrade

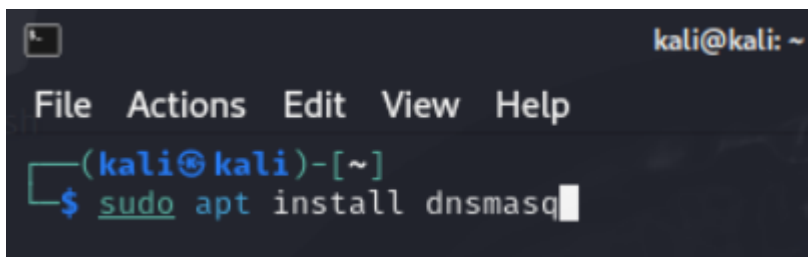


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt upgrade
```

I seguenti comandi vanno digitati e inviati singolarmente.

Terminati gli aggiornamenti bisogna scaricare il servizio DNS digitando il seguente comando:

sudo apt install dnsmasq



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt install dnsmasq
```

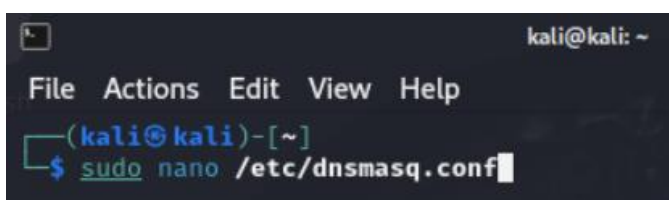
Dare invio e aspettare il termine.

Fatto ciò, dobbiamo modificare il file dnsmasq.conf che si trova al seguente path:

/etc/dnsmasq.conf

Per modificare il file bisogna da terminale digitare quanto segue:

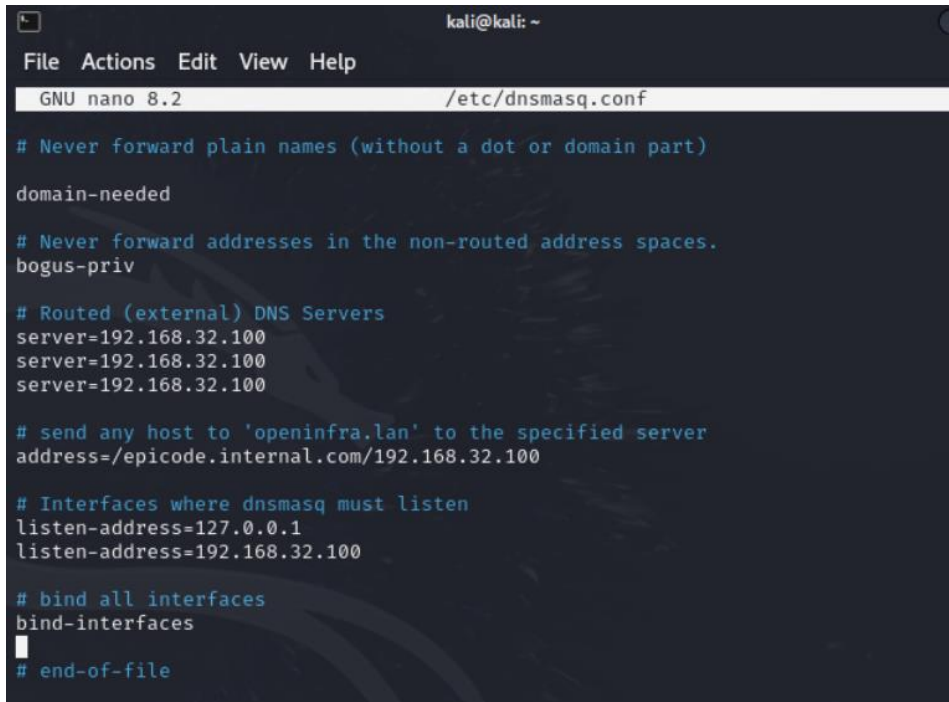
sudo nano /etc/dnsmasq.conf



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nano /etc/dnsmasq.conf
```

Fatto ciò, entreremo nel file di configurazione del DNSmasq

Una volta che stiamo nel file di configurazione bisogna configurare come segue:



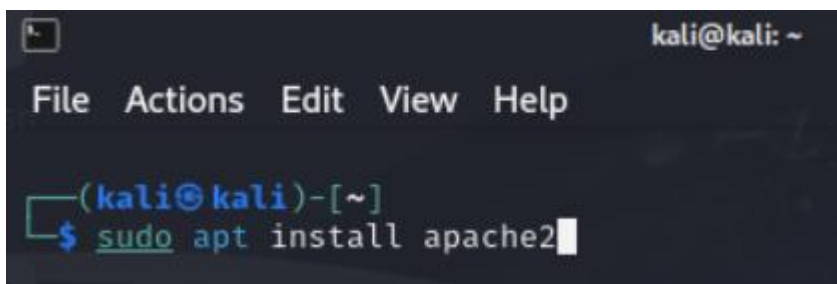
```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 8.2 /etc/dnsmasq.conf  
# Never forward plain names (without a dot or domain part)  
domain-needed  
  
# Never forward addresses in the non-routed address spaces.  
bogus-priv  
  
# Routed (external) DNS Servers  
server=192.168.32.100  
server=192.168.32.100  
server=192.168.32.100  
  
# send any host to 'openinfra.lan' to the specified server  
address=/epicode.internal.com/192.168.32.100  
  
# Interfaces where dnsmasq must listen  
listen-address=127.0.0.1  
listen-address=192.168.32.100  
  
# bind all interfaces  
bind-interfaces  
# end-of-file
```

Per salvare il file premere **ctrl x** digitare **y** e premere **invio**

ora bisogna scaricare apache2 per startare il server http/https

quindi sempre da terminale scaricare apache2 con il seguente comando:

`sudo apt install apache2`



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo apt install apache2
```

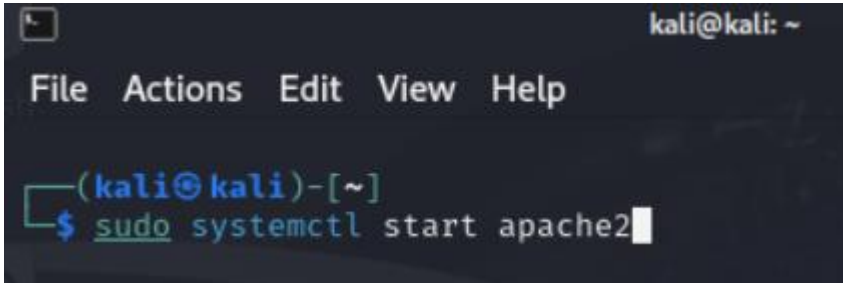
Terminata l'installazione bisogna riportare la VM in rete Intnet seguendo la procedura riportata a pag.4

Riportata la VM in rete internet bisogna far partire i servizi sia di apache2 che del dnsmasq

I comandi sono i rispettivi

Per far partire il servizio apache2

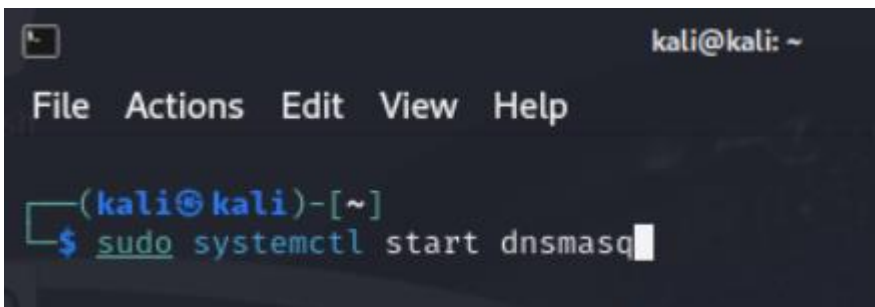
Sudo systemctl start apache2 e dare invio



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo systemctl start apache2
```

Per avviare il servizio dnsmasq dare il seguente comando

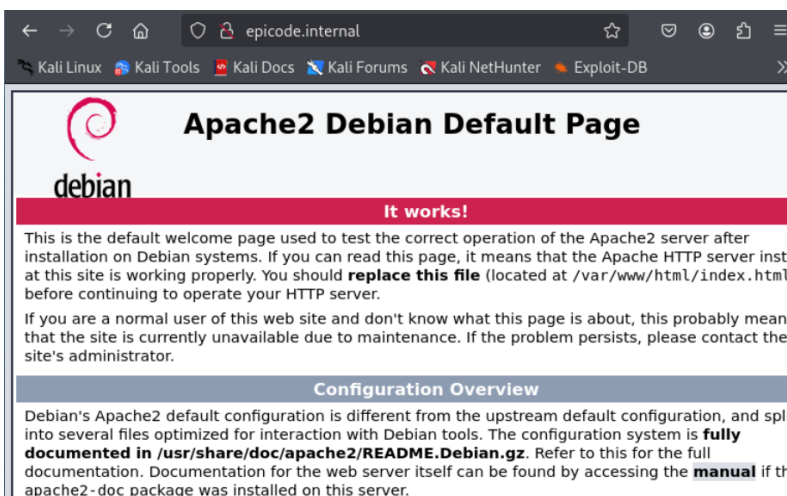
Sudo systemctl start dnsmasq



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo systemctl start dnsmasq
```

Avviati i servizi facciamo una prova che tutto funzioni

Bisogna aprire una pagina web e digitare epicode.internal.com, se tutto funziona, questo è la schermata che bisogna ricevere



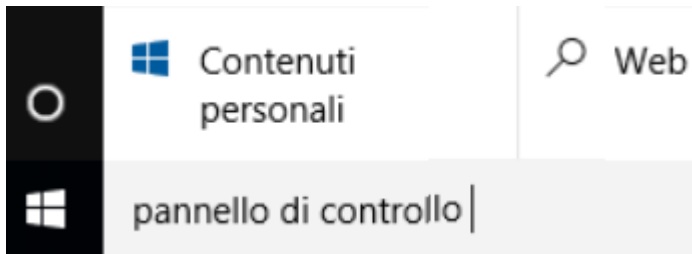
Fatto ciò, è necessario configurare l'interfaccia di rete della VM Win10

## Configurazione di rete Win10

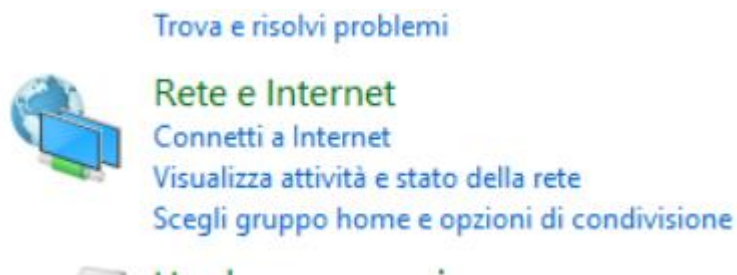
Configurazione interfaccia di rete Win10

Per configurare l'interfaccia di rete di win10 seguiamo i passaggi elencati:

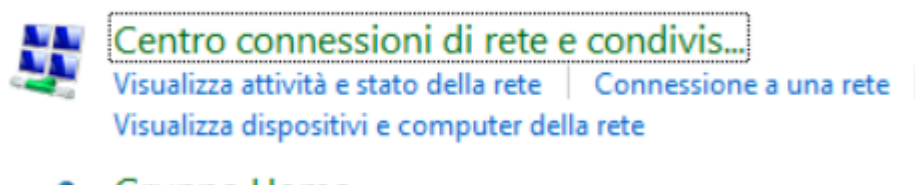
nella barra di ricerca scrivere pannello di controllo



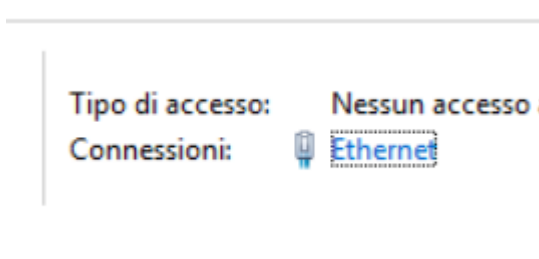
Avviare il pannello di controllo e cliccare su rete e internet



Arrivati a questo punto cliccare su Centro connessioni di rete e condivisione

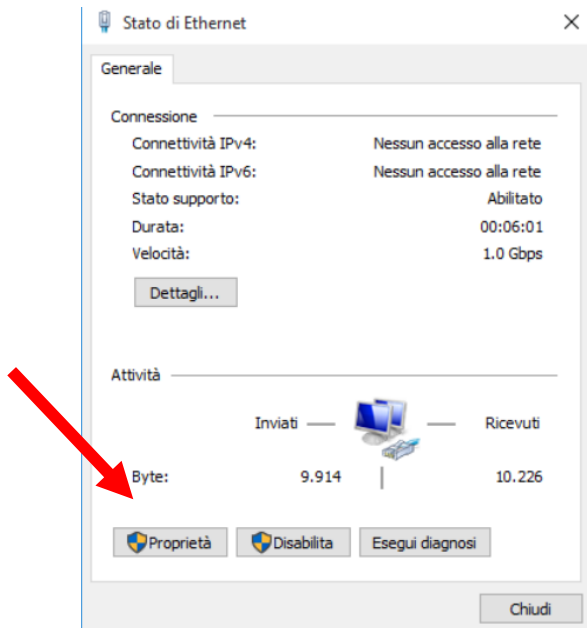


Aperto il centro connessione di rete e condivisione cliccare su ethernet

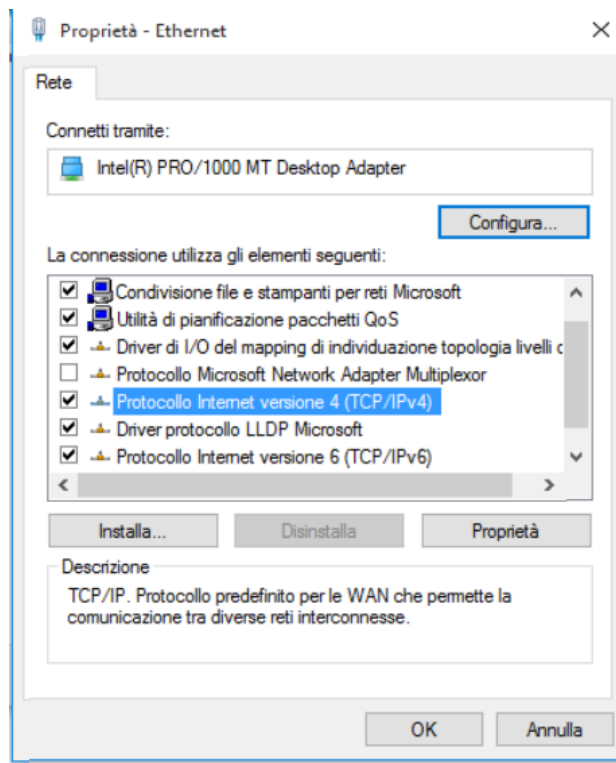




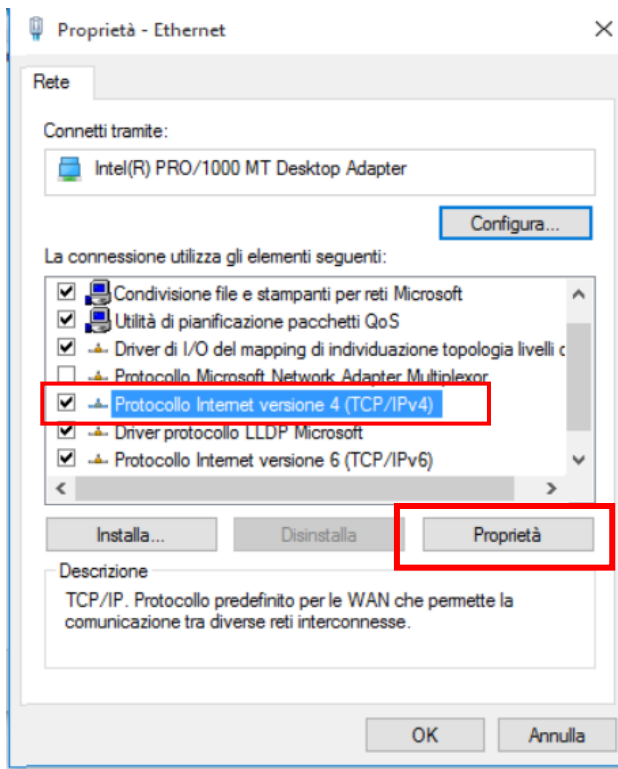
Cliccando su ethernet si apre la seguente schermata e clicchiamo su Proprietà:



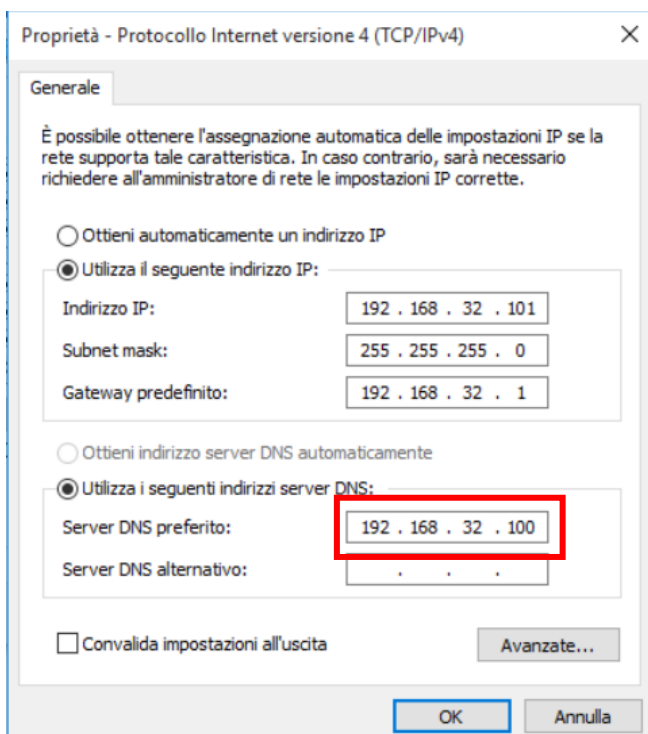
Cliccato su proprietà si apre la schermata come da screen successivo:



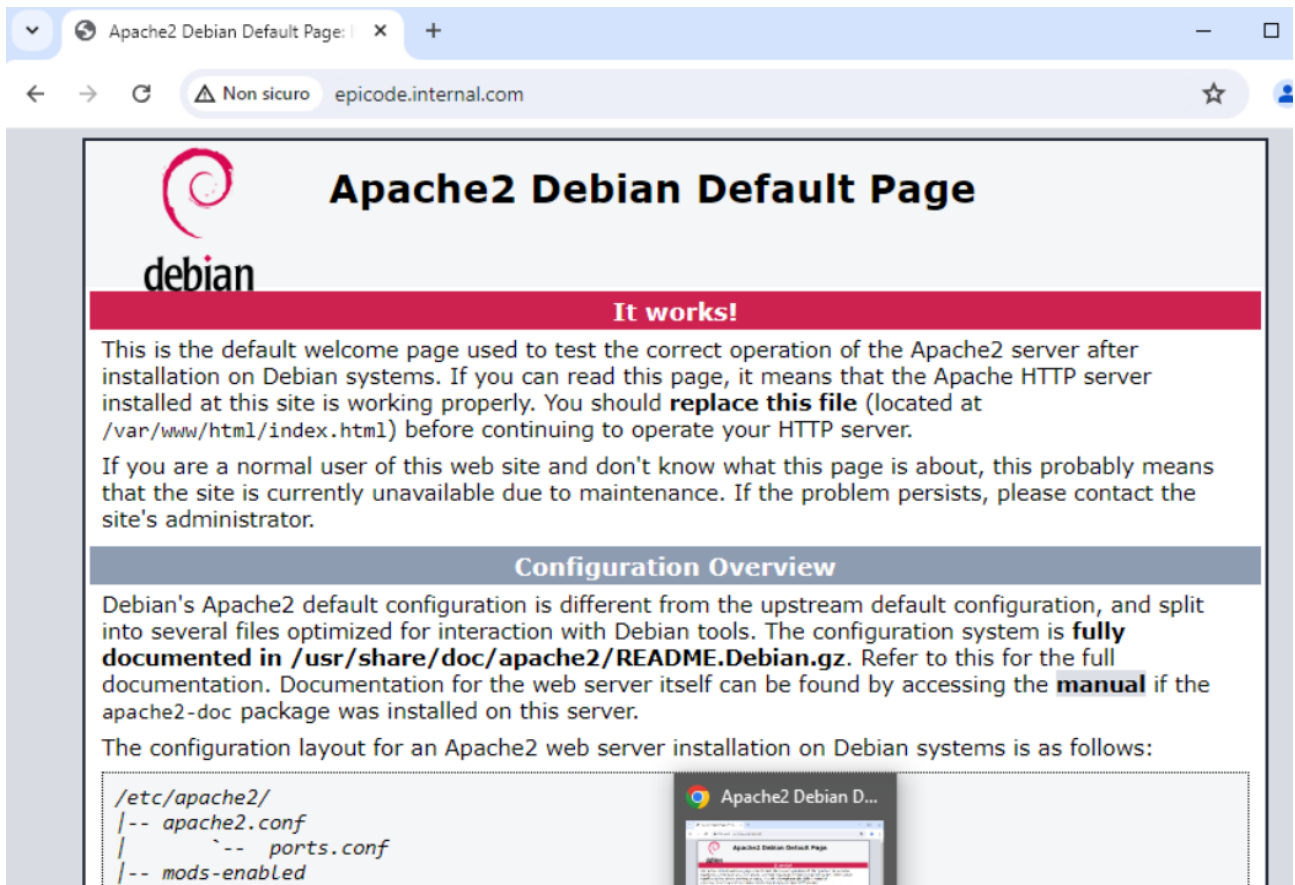
A questo punto selezionare protocollo internet versione 4 (TCP/IPv4) e cliccare di nuovo su proprietà



Fatto ciò, andremo a settare l'IP come segue; impostiamo il server DNS preferito con l'IP di Kali Linux



Ora se il tutto è configurato bene, andiamo ad aprire una pagina web e verifichiamo che viene rilasciata la seguente pagina:



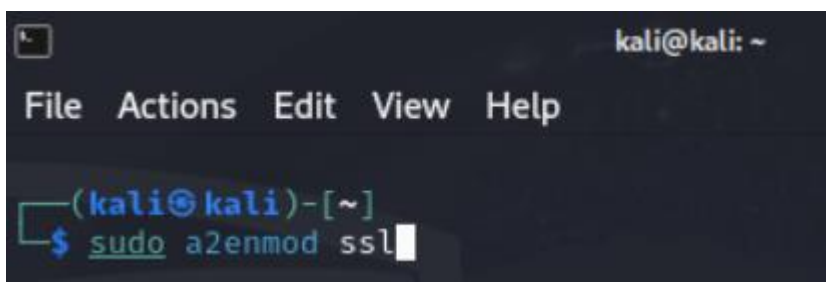
Ora bisogna configurare le chiavi di crittografia https

Ritorniamo su kali e dal terminale eseguire i seguenti step:

per abilitare il modulo SSL

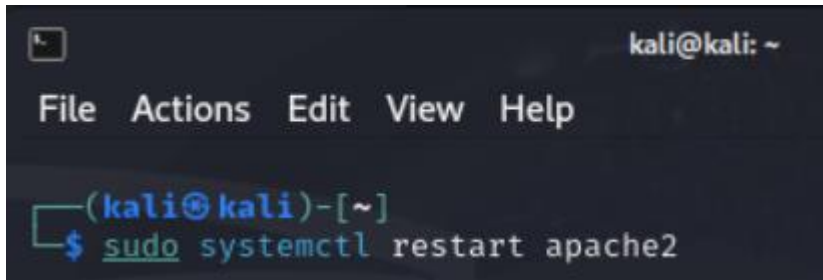
digitare il seguente comando:

sudo a2enmod ssl



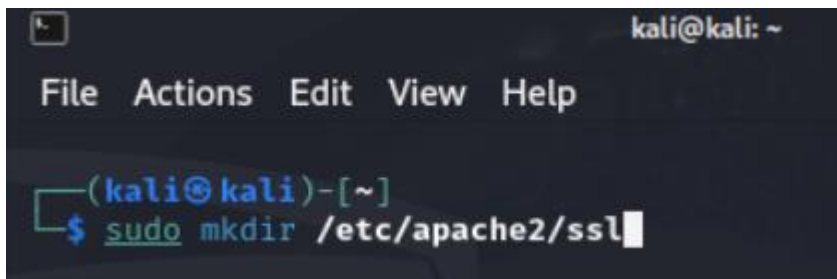
Ora bisogna fare il re-start di apache2 digitando il seguente comando:

`sudo systemctl restart apache2`

A terminal window with a dark background. The title bar shows a window icon and the text 'kali@kali: ~'. The menu bar contains 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~]'. The command '\$ sudo systemctl restart apache2' has been entered and executed.

Ora per una gestione e comodità di ricerca dei certificati SSL creiamo una directory

`Sudo mkdir /etc/apache2/ssl`

A terminal window with a dark background. The title bar shows a window icon and the text 'kali@kali: ~'. The menu bar contains 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~]'. The command '\$ sudo mkdir /etc/apache2/ssl' has been entered and executed.

Ora bisogna creare i certificati utilizzando il seguente comando

`sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/epicode.internal.key -out /etc/apache2/ssl/epicode.internal.crt`

A terminal window with a dark background. The title bar shows a window icon and the text 'kali@kali: ~'. The menu bar contains 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[/etc/apache2/ssl]'. The command '\$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/epicode.internal.key -out /etc/apache2/ssl/epicode.internal.crt' has been entered and executed.

Come si può notare dal comando, i certificati sono stati creati nella directory creata in precedenza, per verificare se il tutto è avvenuto correttamente spostiamoci nel path indicato e verifichiamo che i file siano stati creati.

Di seguito il comando per verificare la corretta creazione dei certificati ssl

`Cd /etc/apache2/ssl`

Con il comando cd ci spostiamo nelle directory

```
kali@kali: /etc/apache2/ssl
File Actions Edit View Help

(kali@kali)-[/]
$ cd /etc/apache2/ssl

(kali@kali)-[/etc/apache2/ssl]
$
```

Una volta che ci siamo recati nel path indicato per verificare che siano presenti i file digitiamo il comando ls -l

```
(kali@kali)-[/etc/apache2/ssl]
$ ls -l
total 8
-rw-r--r-- 1 root root 1399 Dec  2 16:26 epicode.internal.crt
-rw----- 1 root root 1704 Dec  2 16:25 epicode.internal.key
```

Controllato che i file sono stati generati bisogna configurare il file default-ssl.conf

Il file è nella seguente directory

/etc/apache2/sites-available/

Per modificare il file default-ssl.conf

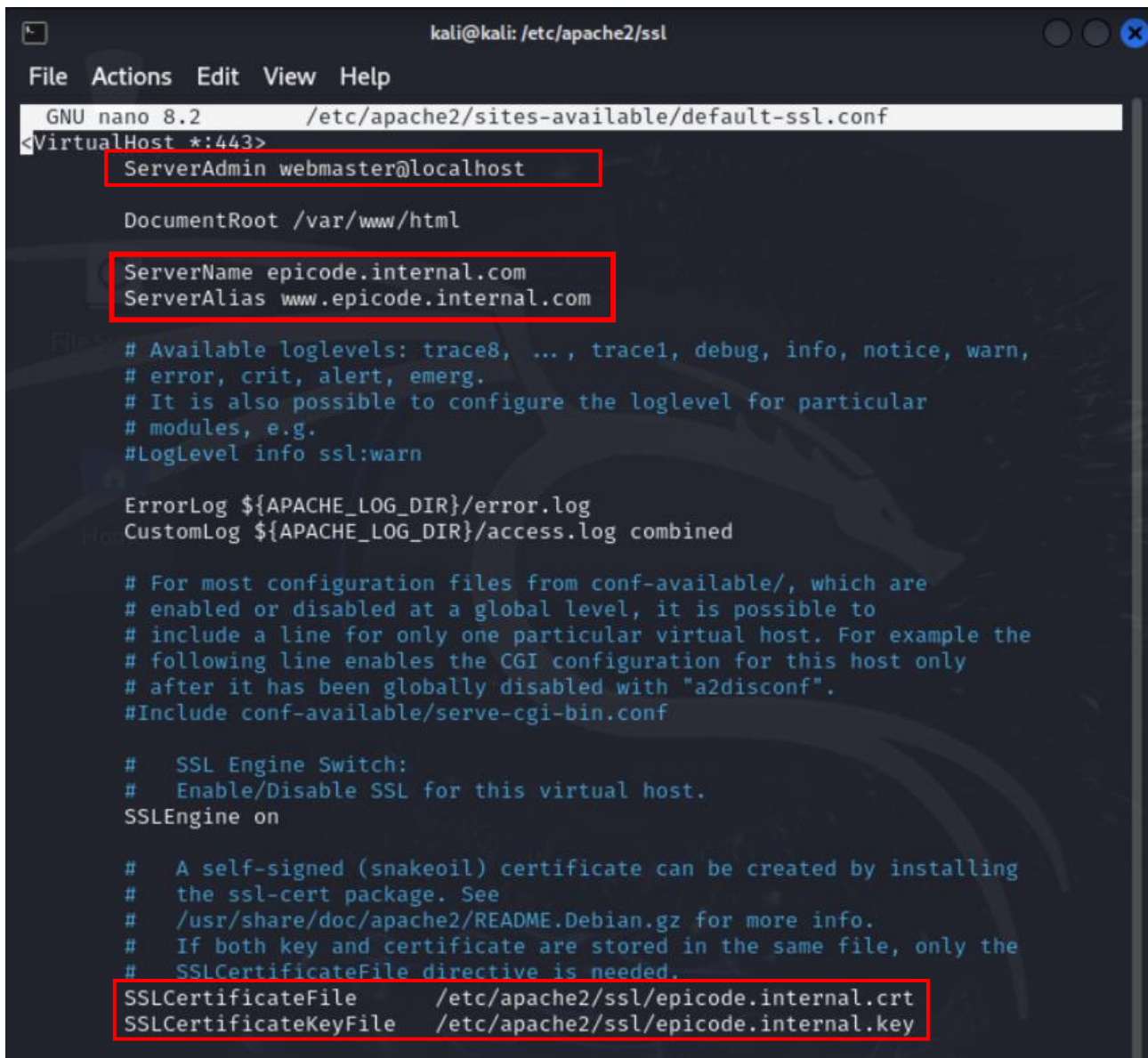
Digitiamo il seguente comando

Sudo nano /etc/apache2/sites-available/default-ssl.conf

```
kali@kali: /etc/apache2/ssl
File Actions Edit View Help

(kali@kali)-[/etc/apache2/ssl]
$ sudo nano /etc/apache2/sites-available/default-ssl.conf
```

Fatto ciò, entriamo nel file di configurazione e modificare quanto segue:



```
kali@kali: /etc/apache2/ssl
File Actions Edit View Help
GNU nano 8.2 /etc/apache2/sites-available/default-ssl.conf
<VirtualHost *:443>
  ServerAdmin webmaster@localhost

  DocumentRoot /var/www/html

  ServerName epicode.internal.com
  ServerAlias www.epicode.internal.com

  # Available loglevels: trace8, ..., tracel, debug, info, notice, warn,
  # error, crit, alert, emerg.
  # It is also possible to configure the loglevel for particular
  # modules, e.g.
  #LogLevel info ssl:warn

  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined

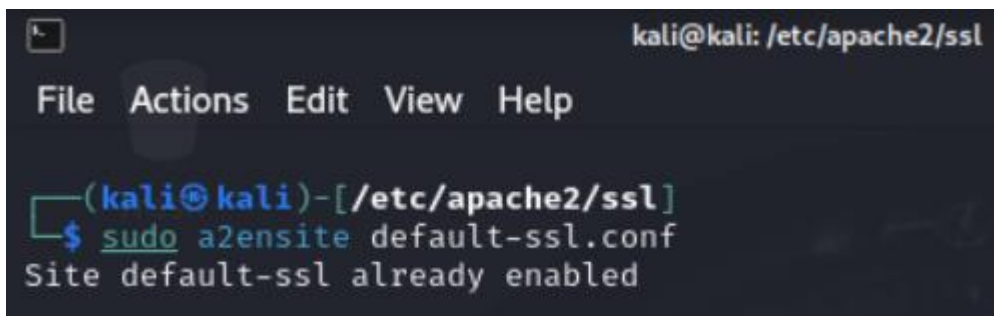
  # For most configuration files from conf-available/, which are
  # enabled or disabled at a global level, it is possible to
  # include a line for only one particular virtual host. For example the
  # following line enables the CGI configuration for this host only
  # after it has been globally disabled with "a2disconf".
  #Include conf-available/serve-cgi-bin.conf

  # SSL Engine Switch:
  # Enable/Disable SSL for this virtual host.
  SSLEngine on

  # A self-signed (snakeoil) certificate can be created by installing
  # the ssl-cert package. See
  # /usr/share/doc/apache2/README.Debian.gz for more info.
  # If both key and certificate are stored in the same file, only the
  # SSLCertificateFile directive is needed.
  SSLCertificateFile /etc/apache2/ssl/epicode.internal.crt
  SSLCertificateKeyFile /etc/apache2/ssl/epicode.internal.key
```

Di seguito alla modifica dobbiamo avviare e abilitare il servizio SSL di apache con il rispettivo comando

Sudo a2ensite default-ssl.conf



```
kali@kali: /etc/apache2/ssl
File Actions Edit View Help
(kali@kali)-[/etc/apache2/ssl]
$ sudo a2ensite default-ssl.conf
Site default-ssl already enabled
```



Ora bisogna fare il re-start del servizio apache con il seguente comando

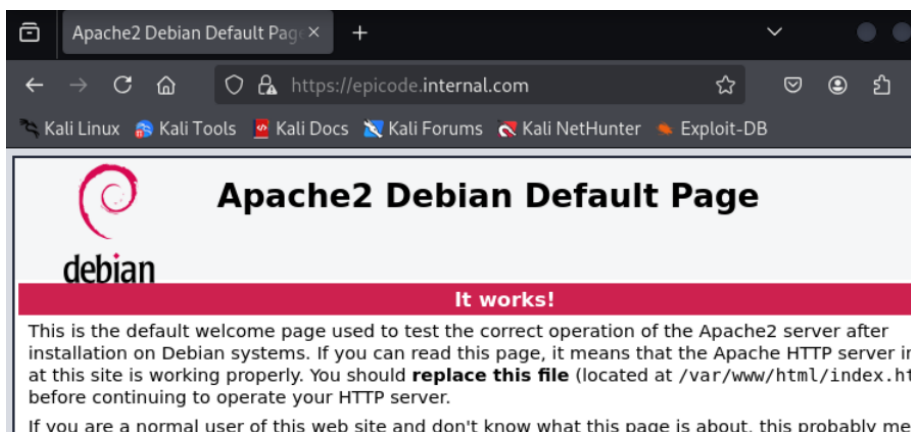
Sudo systemctl restart apache2

```
kali@kali: /etc/apache2/ssl

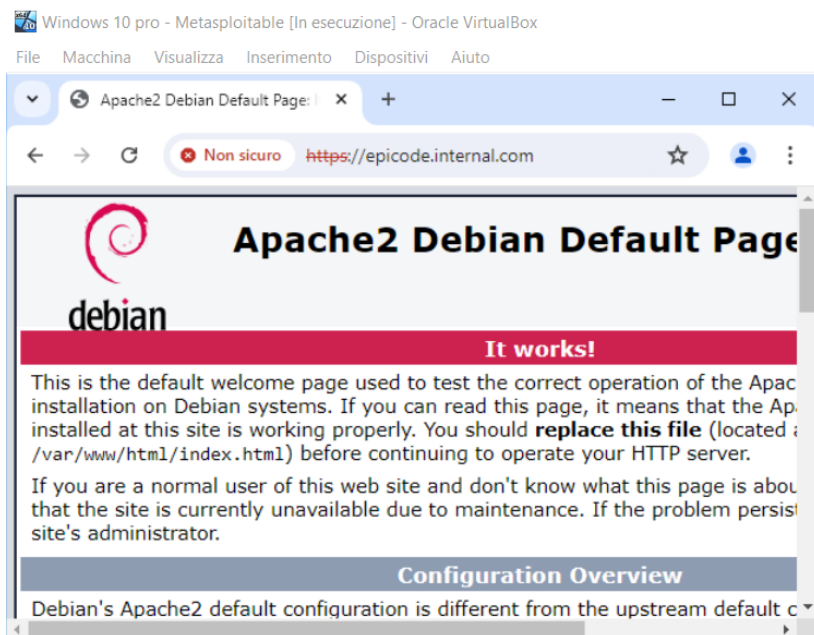
File Actions Edit View Help

(kali@kali)-[/etc/apache2/ssl]
$ sudo systemctl restart apache2
[sudo] password for kali:
```

Per verificare che il tutto funziona correttamente apriamo una pagina web e proviamo a raggiungere il sito in <https://epicode.internal.com>

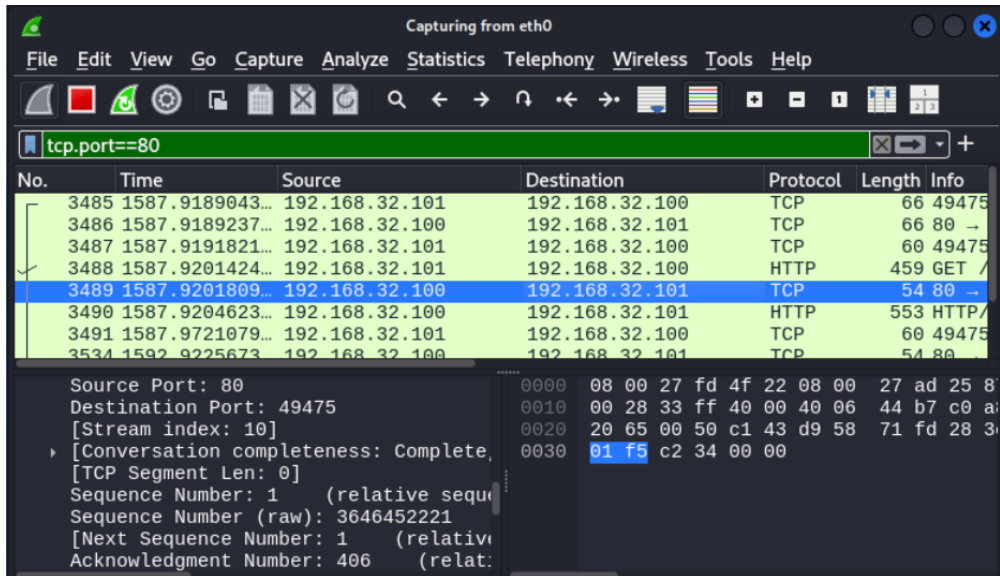


Facciamo la seguente prova anche dalla VM di Win10

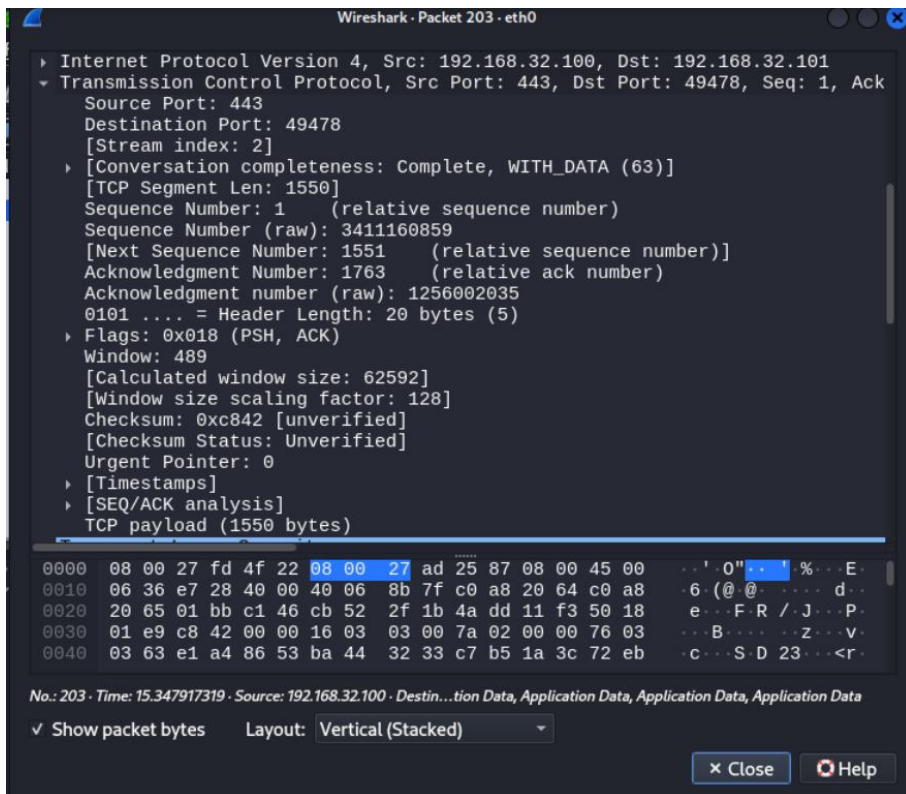


## Controllo rete utilizzando Wireshark

Di seguito lo sniff della rete in http port 80



Di seguito lo sniff della rete in https port 443



La differenza tra http e https è che l'http è in chiaro mentre l'https è crittografato