

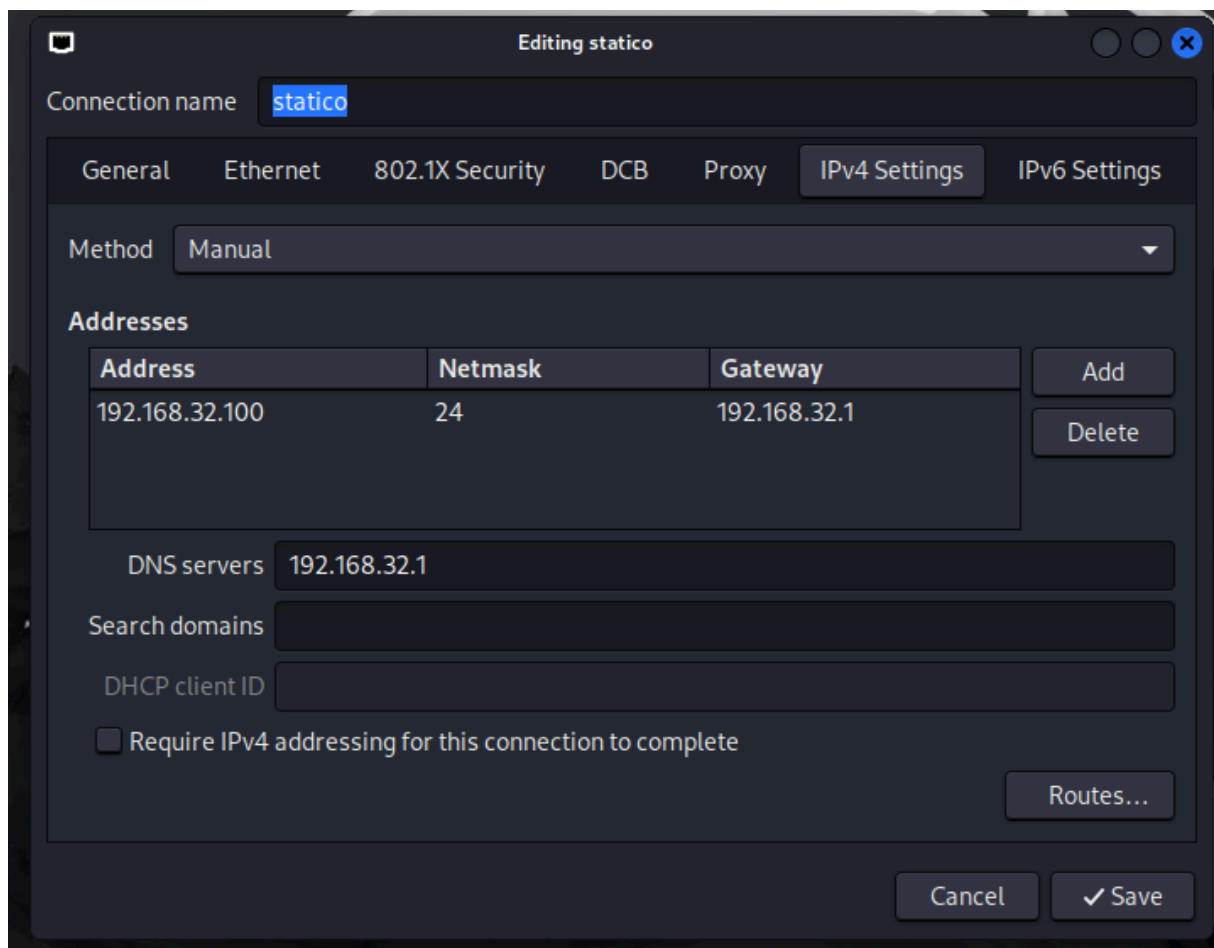
Esercitazione fine modulo **ANTRO FABIO MARCELLO**

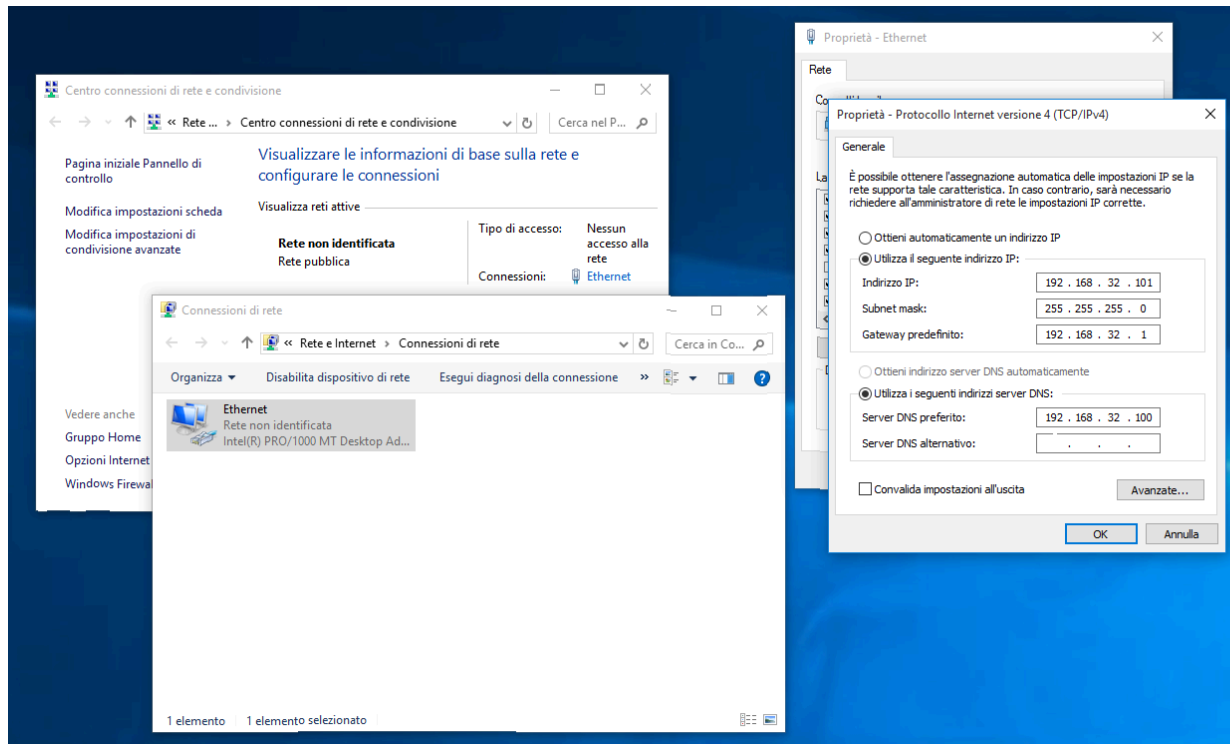
1. RICHIESTA HTTPS

1.1 IMPOSTAZIONE NUOVI IP SU VM WINDOWS E KALI

IMPOSTO, COME DA ESERCIZI PRATICI EFFETTUATI DURANTE IL MODULO, GLI IP DELLE VM KALI LINUX E WINDOWS 10.

ASSEGNO A KALI, CHE DOVRÀ FUNGERE DA SERVER, L'IP 192.168.32.100 E A WINDOWS (CLIENT) L'IP 192.168.32.101.





1.2

HO SCELTO DI UTILIZZARE APACHE PER IL SERVIZIO DNS, QUINDI ESEGUO COME PRIMA COSA QUESTA STRINGA DI COMANDO SU KALI PER ASSICURARMI DI AVERE LA VERSIONE CORRETTA DEL SW

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

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt install apache2
[sudo] password for kali:
apache2 is already the newest version (2.4.62-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
```


1.5 CONFIGURO APACHE PER HTTPS CON

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

MODIFICO LE IMPOSTAZIONI COME SEGUE

```
File Actions Edit View Help
GNU nano 8.1
VirtualHost *:443>
ServerAdmin webmaster@localhost

DocumentRoot /var/www/html

# Available loglevels: trace8, ..., trace1, 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/ssl/certs/apache-selfsigned.crt
SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
# huge file containing all of them (file must be PEM encoded)
# Note: Inside SSLCACertificatePath you need hash symlinks
# to point to the certificate files. Use the provided
# Makefile to update the hash symlinks after changes.
#SSLCACertificatePath /etc/ssl/certs/
#SSLCACertificateFile /etc/apache2/ssl.crt/ca-bundle.crt

# Certificate Revocation Lists (CRL):
# Set the CA revocation path where to find CA CRLs for client
# authentication or alternatively one huge file containing all
# of them (file must be PEM encoded)
# Note: Inside SSLCARevocationPath you need hash symlinks
# to point to the certificate files. Use the provided
# Makefile to update the hash symlinks after changes.
#SSLCARevocationPath /etc/apache2/ssl.crl/
#SSLCARevocationFile /etc/apache2/ssl.crl/ca-bundle.crl

# Client Authentication (Type):
# Client certificate verification type and depth. Types are
# none, optional, require and optional_no_ca. Depth is a
# number which specifies how deeply to verify the certificate
# issuer chain before deciding the certificate is not valid.
#SSLVerifyClient require
#SSLVerifyDepth 10

# SSL Engine Options:
# Set various options for the SSL engine.
# o FakeBasicAuth:
# Translate the client X.509 into a Basic Authorisation. This means that
# the standard Auth/DBMAuth methods can be used for access control. The
# user name is the 'one line' version of the client's X.509 certificate.
# Note that no password is obtained from the user. Every entry in the user
# file needs this password: 'xxj31ZMTZzkVA'.
# o ExportCertData:
# This exports two additional environment variables: SSL_CLIENT_CERT and
# SSL_SERVER_CERT. These contain the PEM-encoded certificates of the
# server (always existing) and the client (only existing when client
# authentication is used). This can be used to import the certificates
# into CGI scripts.
# o StdEnvVars:
# This exports the standard SSL/TLS related 'SSL_*' environment variables.
# Per default this exportation is switched off for performance reasons,
# because the extraction step is an expensive operation and is usually
# useless for serving static content. So one usually enables the
# exportation for CGI and SSI requests only.
# o OptRenegotiate:
# This enables optimized SSL connection renegotiation handling when SSL
# directives are used in per-directory context.
#SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(?:cgi|shtml|phtml|php)$">
  SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
  SSLOptions +StdEnvVars
</Directory>
/VirtualHost>
```

1.6 ABILITO IL SITO SSL CON

```
sudo a2ensite default-ssl
```

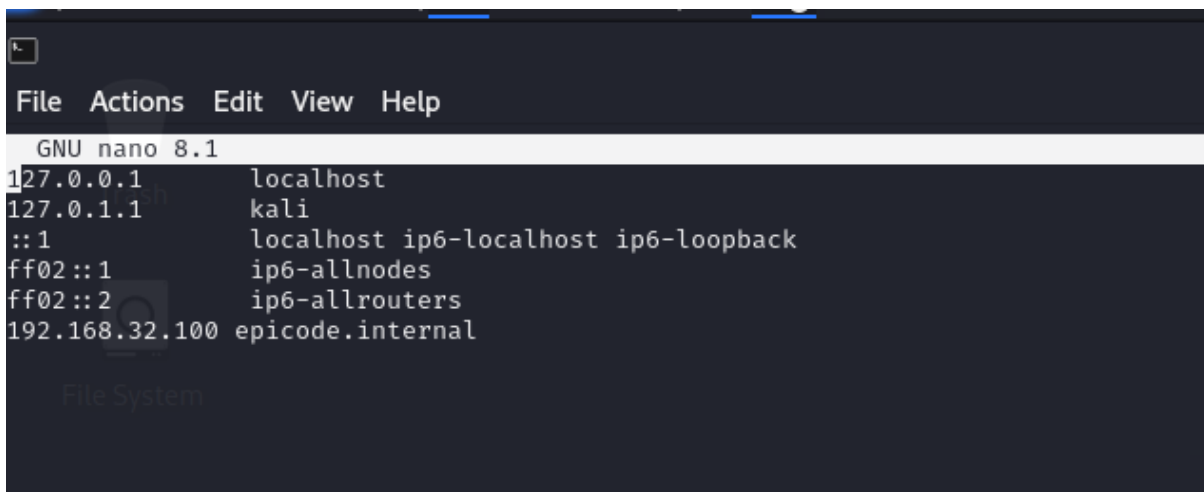
E RIAVVIO APACHE CON

```
sudo systemctl restart apache2
```

1.7 COME ULTIMO PASSAGGIO SU KALI ESEGUO IL SEGUENTE COMANDO

```
sudo nano /etc/hosts
```

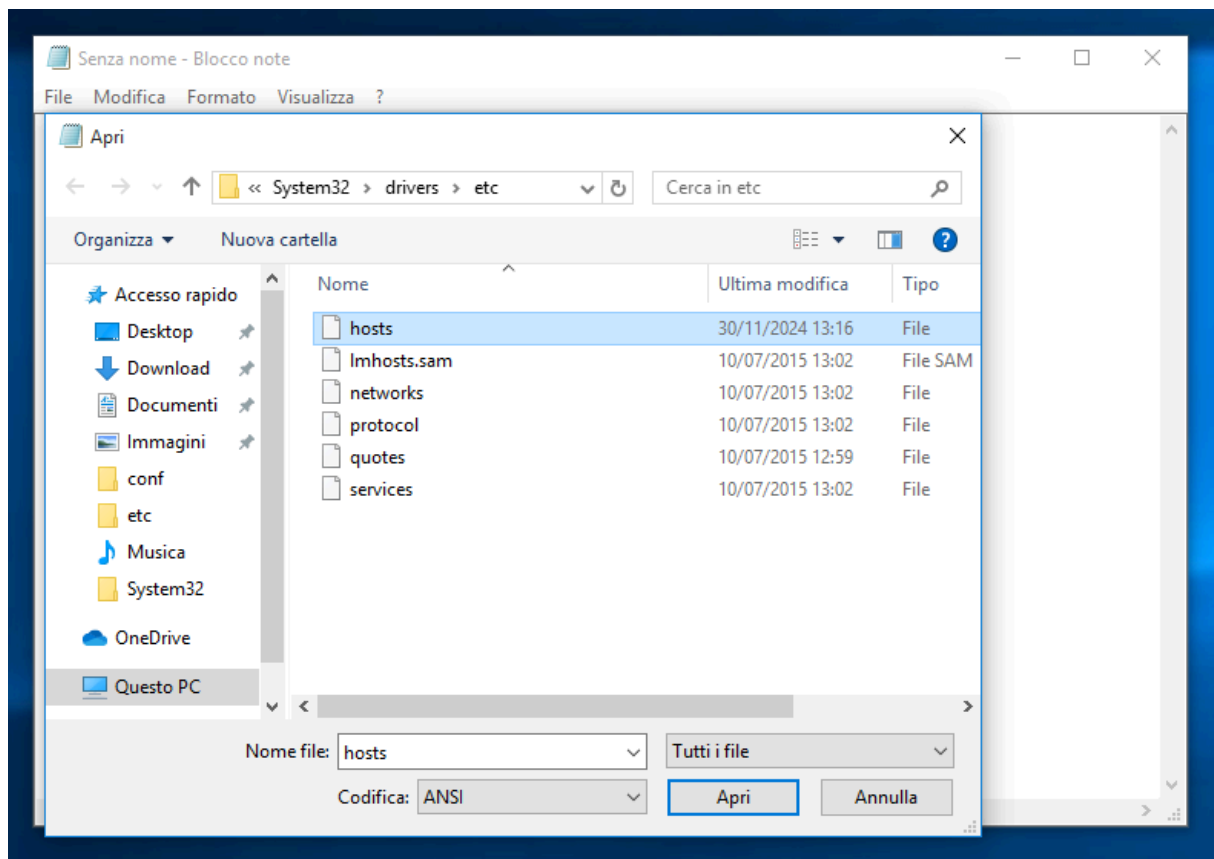
E INSERISCO IP E DOMINIO DEL SERVER



```
File Actions Edit View Help
GNU nano 8.1
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.32.100 epicode.internal
File System
```

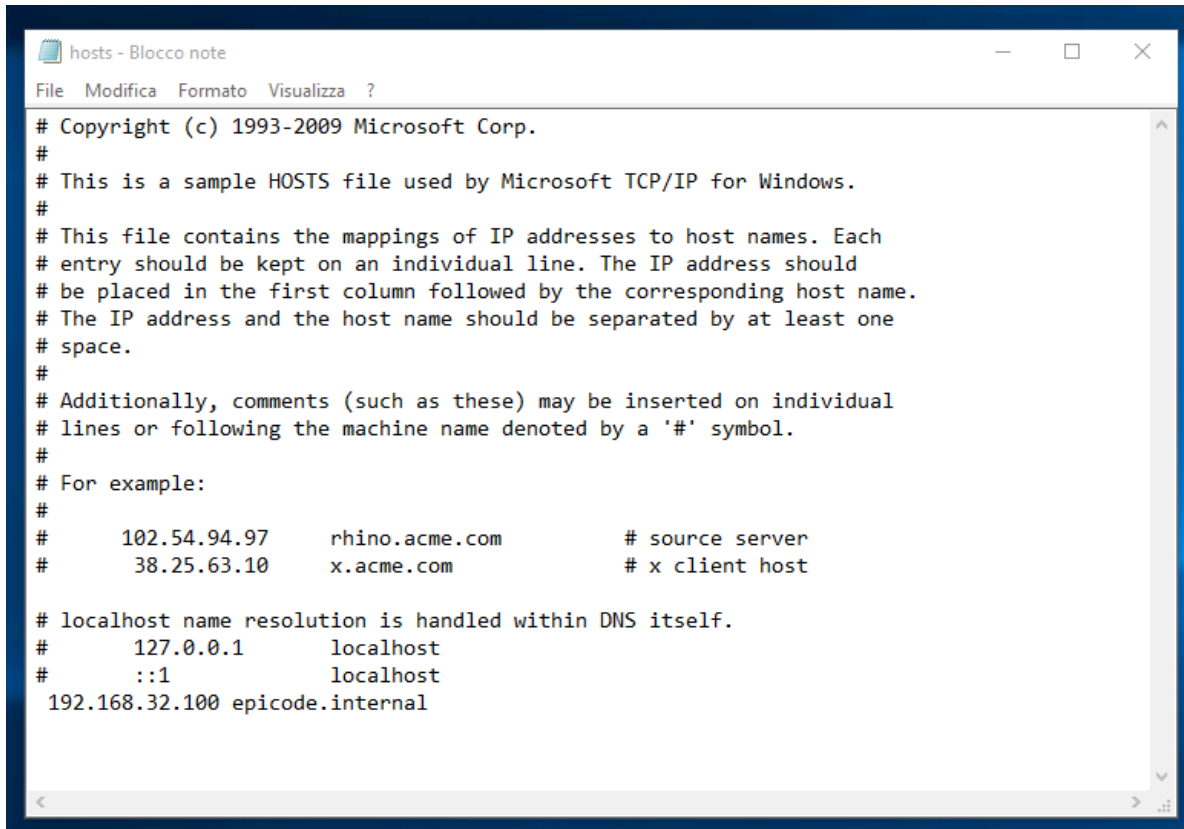
2. LATO WINDOWS

2.1 APRIRE BLOCCO NOTE COME AMMINISTRATORE, SELEZIONARE FILE E SEGUIRE QUESTO PERCORSO:



2.2 APRIRE IL FILE HOSTS E INSERIRE IP E DOMINIO COME DA TRACCIA

192.168.32.100 EPICODE.INTERNAL



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
192.168.32.100 epicode.internal
```

3. ESECUZIONE WIRESHARK

3.1 AVVIO WIRESHARK E MI METTO IN ASCOLTO SULL'INTERFACCIA DI RETE IN UTILIZZO

3.2 AVVIO RICHIESTA HTTPS DA WINDOWS, DIGITANDO NEL BROWSER

[HTTPS://EPICODE.INTERNAL](https://epicode.internal)

3.3 SU WIRESHARK ANALIZZO IL FLUSSO DI DATI. INDIVIDUO GLI INDIRIZZI MAC

Wireshark packet capture showing an HTTPS request. The packet list shows a standard query for beacon5.gvt2.com. The packet details show the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) layers. The packet bytes show the raw data.

Frame 338: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemec_d5:04:c5 (08:00:27:db:04:c5), Dst: PCSSystemec_ad:25:0f (08:00:27:ad:25:0f)

Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100

8160 = Version: 4

.... 8161 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total length: 48

Identification: 0x05a (16474)

816. = Flags: 0x2, Don't fragment

... 0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0xf85b [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.32.101

Destination Address: 192.168.32.100

Transmission Control Protocol, Src Port: 49438, Dst Port: 443, Seq: 2558, Ack: 5023, Len: 0

Source Port: 49438

Destination Port: 443

[Stream index: 2]

[Conversation completeness: Complete, WITH DATA (63)]

[TCP Segment Len: 0]

Sequence Number: 2558 (relative sequence number)

Sequence Number (raw): 2165849897

[Next Sequence Number: 2558 (relative sequence number)]

Acknowledgment Number: 5023 (relative ack number)

Acknowledgment number (raw): 2214615237

0101 = Header Length: 20 bytes (5)

0101 = Flags: 0x014 (RST, ACK)

Window: 0

[Calculated window size: 0]

[Window size scaling factor: 256]

Checksum: 0xb409 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

CONCLUSIONE

ESSENDO UNA RICHIESTA HTTP, IL CONTENUTO DEI DATI È CRIPTATO E L'ACCESSO CHE NE RICAVIAMO È LIMITATO COME DA SCREEN.

1. RICHIESTA HTTP

PER PROCEDERE AD ANALIZZARE IL FLUSSO DATI DI UNA RICHIESTA HTTP, ANDIAMO A CONFIGURARE IL SERVER HTTP SU KALI.

ESEGUIAMO I SEGUENTI COMANDI

```
sudo a2dissite default-ssl  
sudo a2ensite 000-default  
sudo systemctl restart apache2
```

PROCEDERE NUOVAMENTE ALLA RICHIESTA HTTP DA WINDOWS E INTERCETTARE IL FLUSSO DATI.

CONCLUSIONE

A DIFFERENZA DELL'HTTPS POSSIAMO NOTARE CHE IL CONTENUTO DEI PACCHETTI È TOTALMENTE VISIBILE.

The screenshot displays a Wireshark network capture of an HTTP GET request. The packet list on the left shows a GET request from 192.168.32.100 to 192.168.32.1. The packet details on the left show the structure of the HTTP request, including the status bar text 'SupportAssist?'. The packet bytes on the right show the raw data of the request, including the status bar text 'SupportAssist?'. A small dialog box in the bottom right corner asks to disable notifications for SupportAssist.

Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: PCSSystemtec_d5:64:c5 (08:00:27:d5:64:c5)

Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 3423

Identification: 0x8f26 (36646)

010. = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: TCP (6)

Header Checksum: 0xdc58 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.32.100

Destination Address: 192.168.32.101

Transmission Control Protocol, Src Port: 80, Dst Port: 49483, Seq: 1, Ack: 571, Len: 3383

Source Port: 80

Destination Port: 49483

[Stream index: 1]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 3383]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 3224499628

[Next Sequence Number: 3384 (relative sequence number)]

Acknowledgment Number: 571 (relative ack number)

Acknowledgment number (raw): 3658602184

0101 = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window: 249

[Calculated window size: 31872]

0000 08 00 27 d5 64 c5 08 00 27 ad 25 87 08 00 45 00 ...d...X..E..

0010 0d 5f 8f 26 40 09 40 06 dc 58 c0 a8 20 64 c0 a8 ...&@ @ X..d..

0020 20 65 00 50 c1 4b c0 31 f5 ac da 11 d6 c8 50 18 e P K 1P.

0030 00 f9 cf 6b 00 00 48 54 54 50 2f 31 2e 31 20 32 ...k HT/PT/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK .D ate: Sat

0050 2c 20 33 30 20 4e 6f 76 20 32 30 32 34 20 31 33 , 30 Nov 2024 13

0060 3a 35 35 3a 34 32 20 47 4d 54 0d 0a 53 65 72 76 :55:42 G MT. Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6

0080 32 20 28 44 65 62 69 61 6e 29 0d 0a 4c 61 73 74 2 (Debia n). Last

0090 2d 4d 6f 64 69 66 69 65 64 3a 20 53 75 6e 2c 20 -Modifie d: Sun,

00a0 31 38 20 41 75 67 20 32 30 32 34 20 31 39 3a 35 18 Aug 2 024 19:5

00b0 35 3a 32 32 20 47 4d 54 0d 0a 54 61 67 3a 20 5:22 GMT ..ETag:

00c0 22 32 39 63 66 2d 36 31 66 66 61 39 32 39 39 61 "29cf-61 ffa9299a

00d0 35 65 30 2d 67 7a 69 70 22 0d 0a 41 63 63 65 70 5e0-gzip ". Accep

00e0 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 0d t-Ranges : bytes-

00f0 0a 56 61 72 79 3a 20 41 63 65 70 74 2d 45 6e Vary: A ccept-En

0100 63 6f 64 69 6e 67 0d 0a 43 6f 6e 74 65 6e 74 2d coding.. Content-

0110 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 0d 0a Encoding: gzip ..

0120 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 Content- Length:

0130 33 30 34 34 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3044 .Ke ep-Alive

0140 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 78 : timeout t=5, max

0150 3d 31 30 30 0d 0a 43 6f 6e 6e 63 74 69 6f 6e =100 .Co nnection

0160 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f : Keep-A live. Co

0170 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 ntent-Ty pe: text

0180 2f 68 74 6d 6c 0d 0a 0d 0a 1f 8b 08 00 00 00 00 /html... ..

0190 00 00 03 bd 5a 5b 73 db 36 16 7e f7 af 40 05 e9 ...Z[s 6...@..

01a0 34 c9 48 a4 ed 24 ae 2d cb de 49 7c 99 64 26 6d 4 H .S-...[I] d&m

01b0 3c a9 ba bd 7d f2 42 24 24 61 0c 12 5c 00 84 ac <...} BS Sa .\...

01c0 5e fe fb 9e 83 80 14 6f a2 9c 0c 53 4e 53 89 24 A.....o ...LSNS \$

Frame 3427 bytes Uncompressed entity body (10703 bytes)

Packets: 299 Displayed: 24 (8.0%)

SupportAssist? Suggerimenti di notifica Disabilitare Non adesso