ESERCIZIO W4D4

TRACCIA:

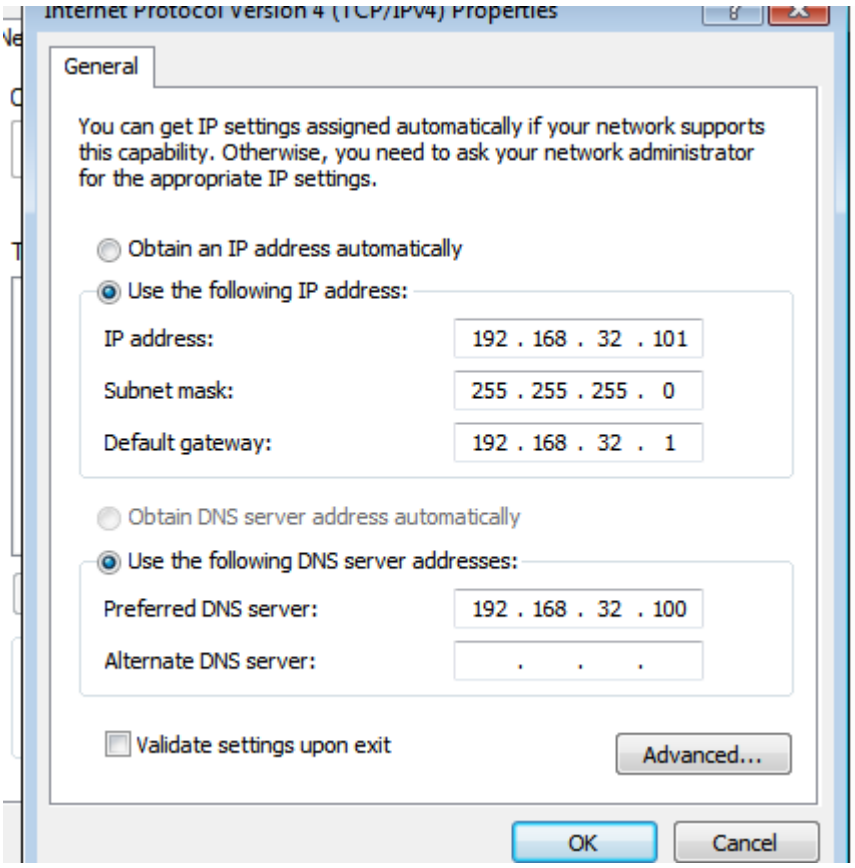
Simulare,in ambiente di laboratorio virtuale,un'architettura client server in cui un client con indirizzo IP 192.168.32.101 (windows7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (kali).

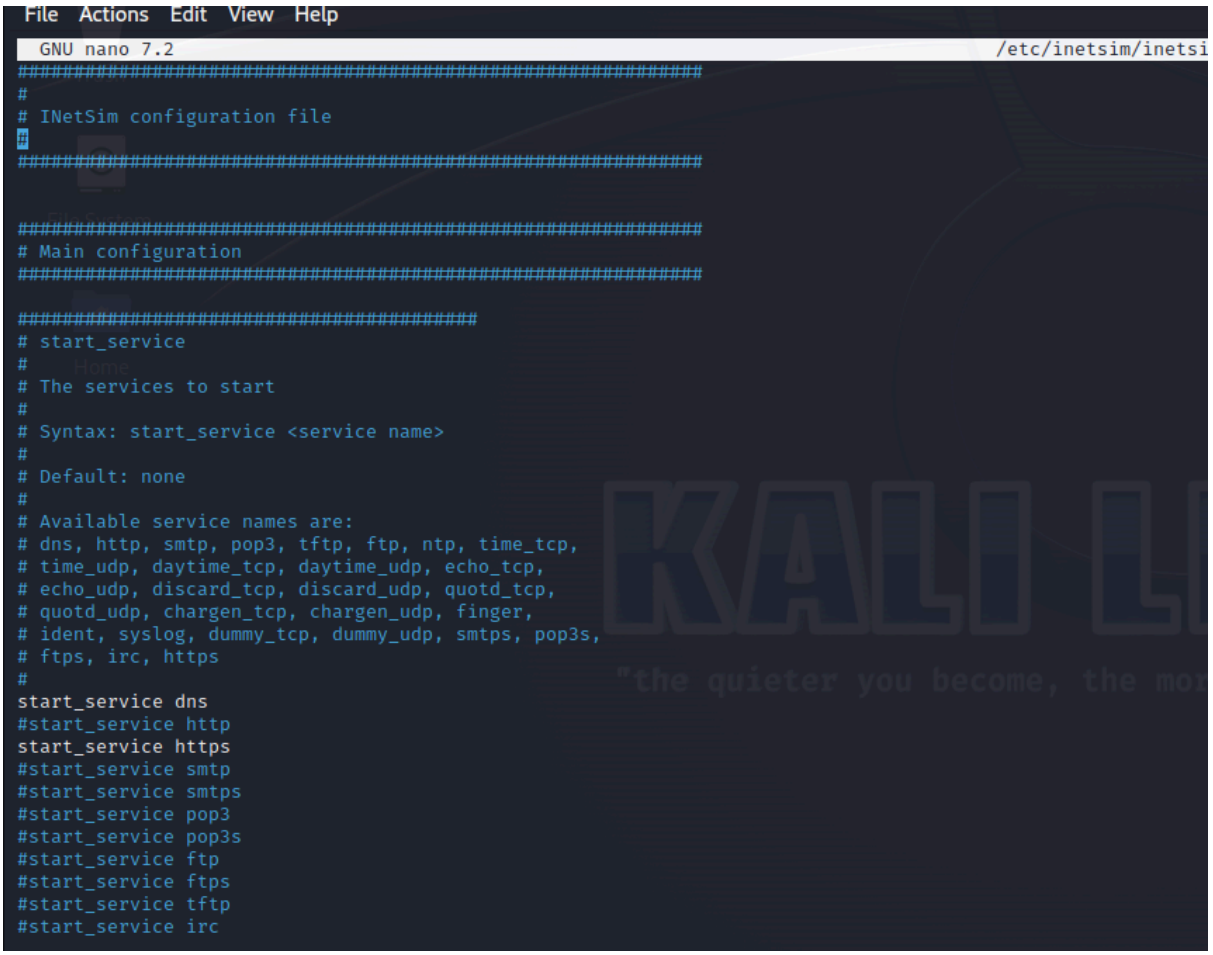
Si intercetti la comunicazione con Wireshark,evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

Ripetere l'esercizio,sostituendo il server HTTPS,con un server HTTP.
Si intercetti nuovamente il traffico,evidenziando le eventuali differenze tra il traffico catturato in HTTP e il traffico catturato in HTTPS.Spiegare,motivaandole,le principali differenze,se presenti.

ESECUZIONE

```
# 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
```


Internet Protocol Version 4 (TCP/IPv4) Properties
General
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
Advanced...
OK
Cancel


File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsi
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
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc

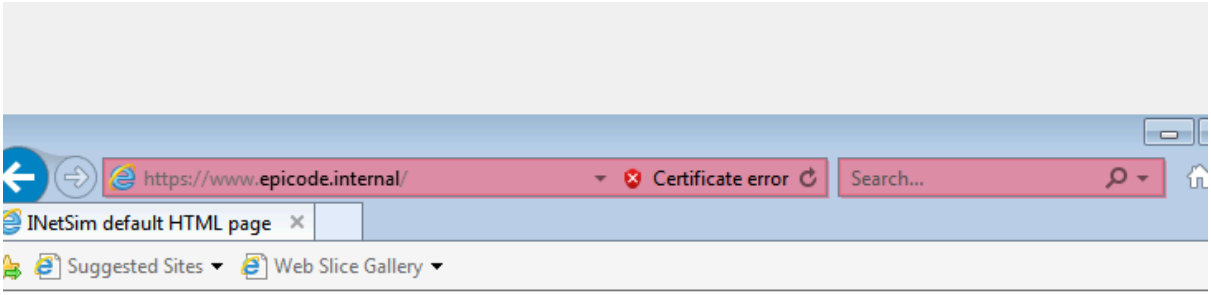
```
##########################################
# dns_bind_port
#
# Port number to bind DNS service to
#
# Syntax: dns_bind_port <port number>
#
# Default: 53
#
dns_bind_port 53


##########################################
# 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_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
#
#dns_static
dns_static epicode.internal  192.168.32.100
#dns_static ftp.bar.net 10.10.20.30
```

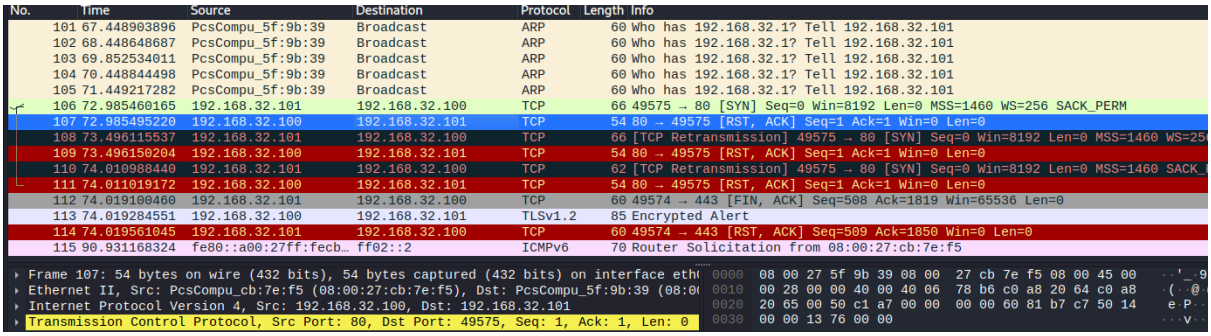
```
# https_fakefile
#
# Fake files returned in fake mode based on the file extension
# in the HTTPS request.
# The fake files must be placed in <data-dir>/http/fakefiles
#
# Syntax: https_fakefile <extension> <filename> <mime-type>
#
# Default: none
#
https_fakefile txt  sample.txt     text/plain
```

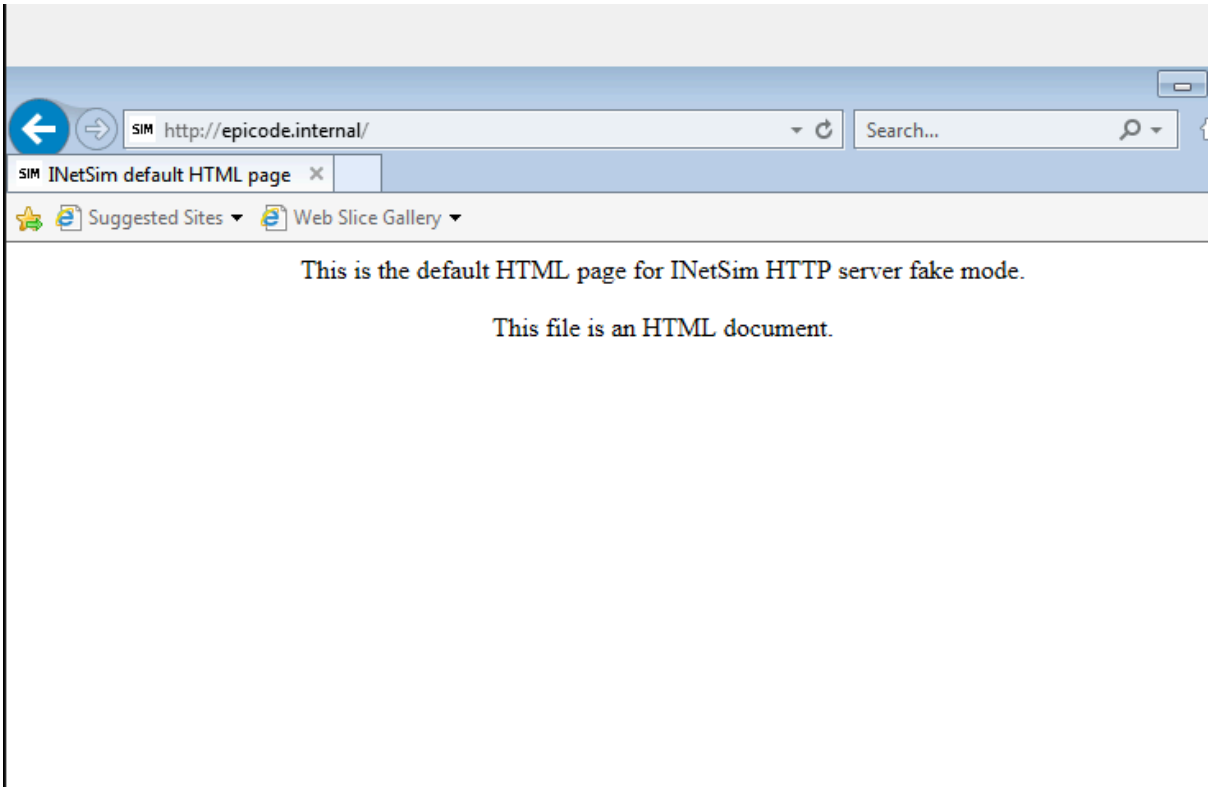
```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 58162) ===
Session ID:     58162
Listening on:   192.168.32.100
Real Date/Time: 2024-01-08 16:59:38
Fake Date/Time: 2024-01-08 16:59:38 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 58172)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
  * https_443_tcp - started (PID 58173)
 done.
Simulation running.
```

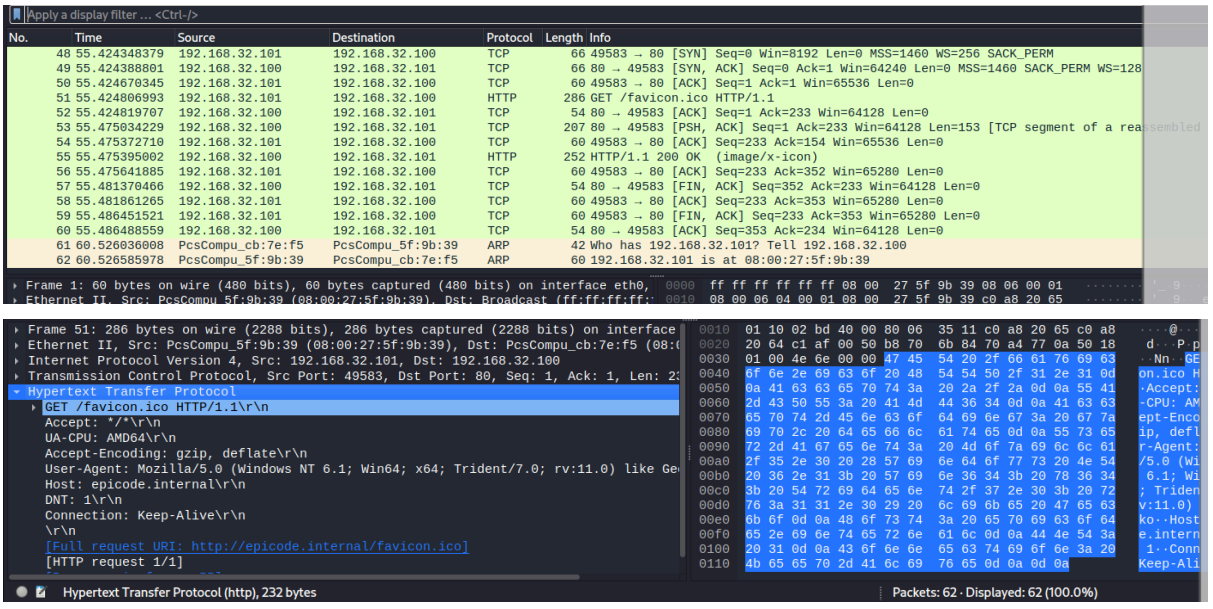


This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.







CONCLUSIONI:

con questo esercizio,abbiamo notato che,con il server HTTPS,i messaggi sono criptati,quindi saranno molto difficili da intercettare,mentre con il server HTTP,i contenuti sono leggibili e più facili da decifrare.Il contenuto è lo stesso per entrambi i server così come il MAC address,ma si deduce che il server HTTPS,garantisce

maggiore sicurezza nella protezione dei dati,nella cifratura del traffico e nella verifica di integrità del traffico stesso.