

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

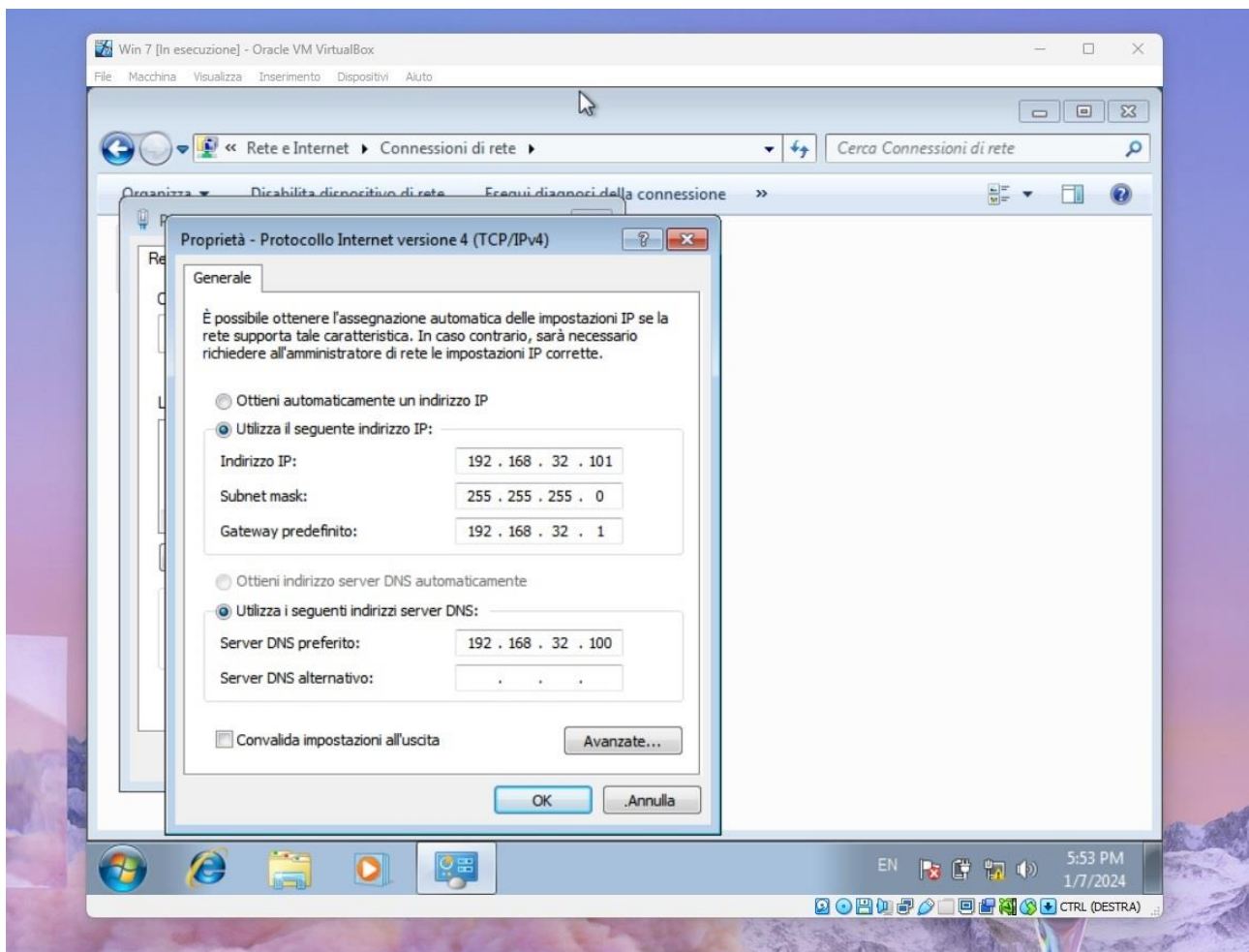
Traccia: Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname `epicode.internal` che risponde all'indirizzo 192.168.32.100 (Kali).

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

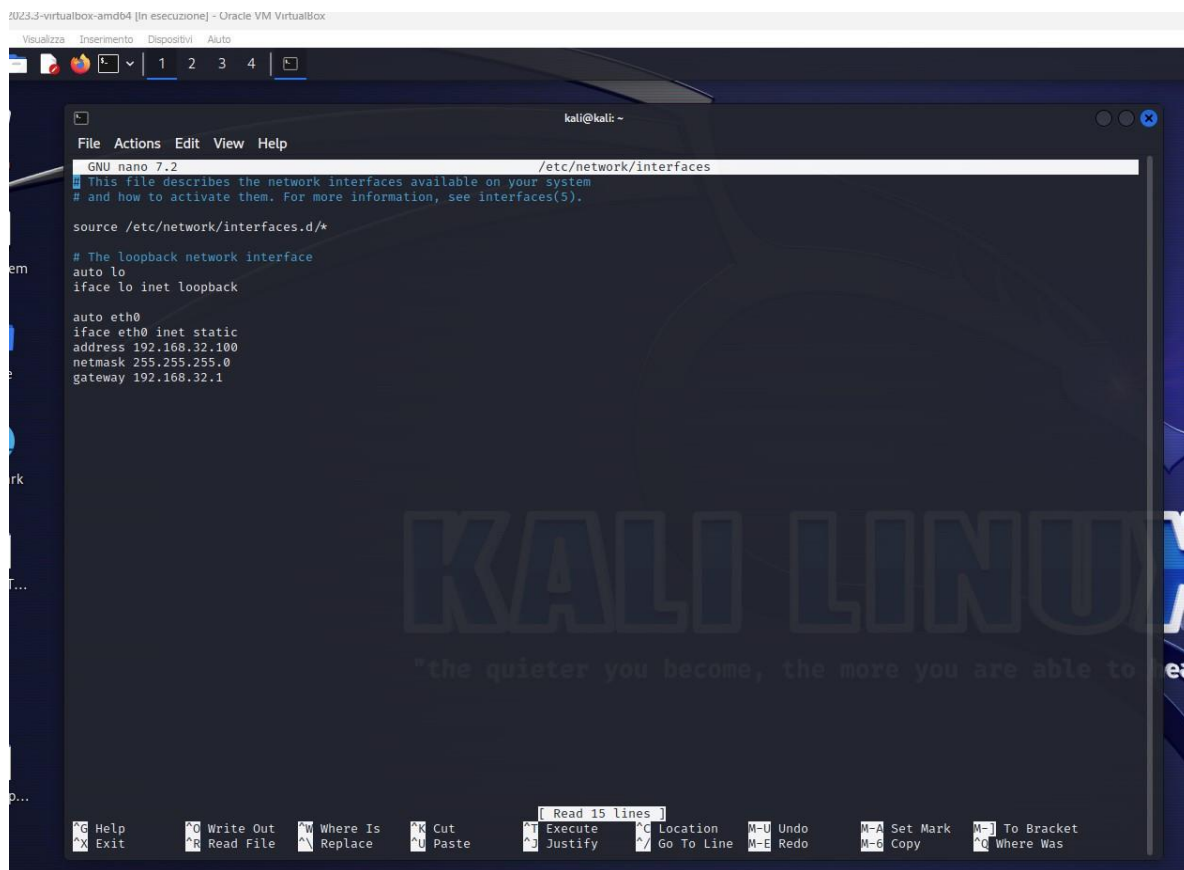
Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

Svolgimento:

Configurazione IP e DNS server su terminale Window7 con IP 192.168.32.101, gateway predefinito 192.162.32.1 e DNS 192.168.32.100 (IP Kali).



Configurazione IP Kali 192.168.32.100 con comando sudo /etc/network/interfaces



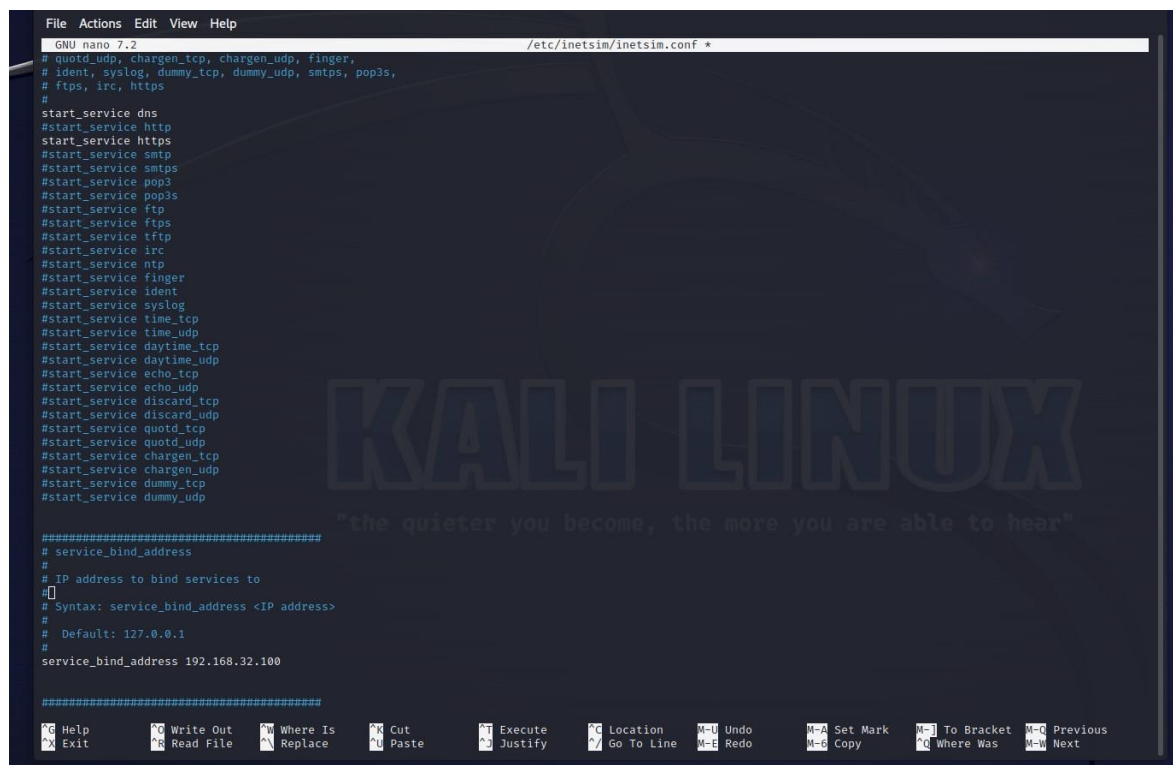
```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

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
netmask 255.255.255.0
gateway 192.168.32.1
```

Configurazione Inetsim Kali Pt1: Attivazione servizio HTTPS + DSN + abilitazione bind address con IP Kali 192.162.32.100. Comando sudo nano /etc/intesim/inetsim.conf



```
GNU nano 7.2 /etc/inetsim/inetsim.conf *
# 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
#start_service ntp
#start_service finger
#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 192.168.32.100

#####
```

Configurazione Inetsim Kali Pt2: Attivazione DNS default IP (192.168.32.100) + attivazione DSN default dominname (epicode.internal) + attivazione DSN Static (www.epicode.internal + 192.168.32.100)

```
File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsim.conf *
# 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_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
#
# dns_default_hostname epicode.internal

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

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

#####
# https_fakefile
#
# The default fake file returned in fake mode if the file extension
# in the HTTPS request does not match any of the extensions
# defined above.
#
# The default fake file must be placed in <data-dir>/http/fakefiles
#
# Syntax: https_default_fakefile <filename> <mime-type>
#
# Default: none
#
https_default_fakefile sample.html text/html

#####
# https_static_fakefile
#
# Fake files returned in fake mode based on static path.
# The fake files must be placed in <data-dir>/http/fakefiles
#
# Syntax: https_static_fakefile <path> <filename> <mime-type>
#
# Default: none
#
#https_static_fakefile /path/ sample_gui.exe x-msdos-program
#https_static_fakefile /path/to/file.exe sample_gui.exe x-msdos-program

#####
# https_ssl_keyfile
#
# Name of the SSL private key PEM file.
# The key MUST NOT be encrypted!
#
# The file must be placed in <data-dir>/certs/
#
#
```

Attivazione fakefile https

```
File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsim.conf *
https_fakefile gif sample.gif image/gif
https_fakefile jpg sample.jpg image/jpeg
https_fakefile jpeg sample.jpg image/jpeg
https_fakefile png sample.png image/png
https_fakefile bmp sample.bmp image/x-ms-bmp
https_fakefile ico favicon.ico image/x-icon
https_fakefile exe sample_gui.exe x-msdos-program
https_fakefile com sample_gui.exe x-msdos-program

#####
# https_default_fakefile
#
# The default fake file returned in fake mode if the file extension
# in the HTTPS request does not match any of the extensions
# defined above.
#
# The default fake file must be placed in <data-dir>/http/fakefiles
#
# Syntax: https_default_fakefile <filename> <mime-type>
#
# Default: none
#
https_default_fakefile sample.html text/html

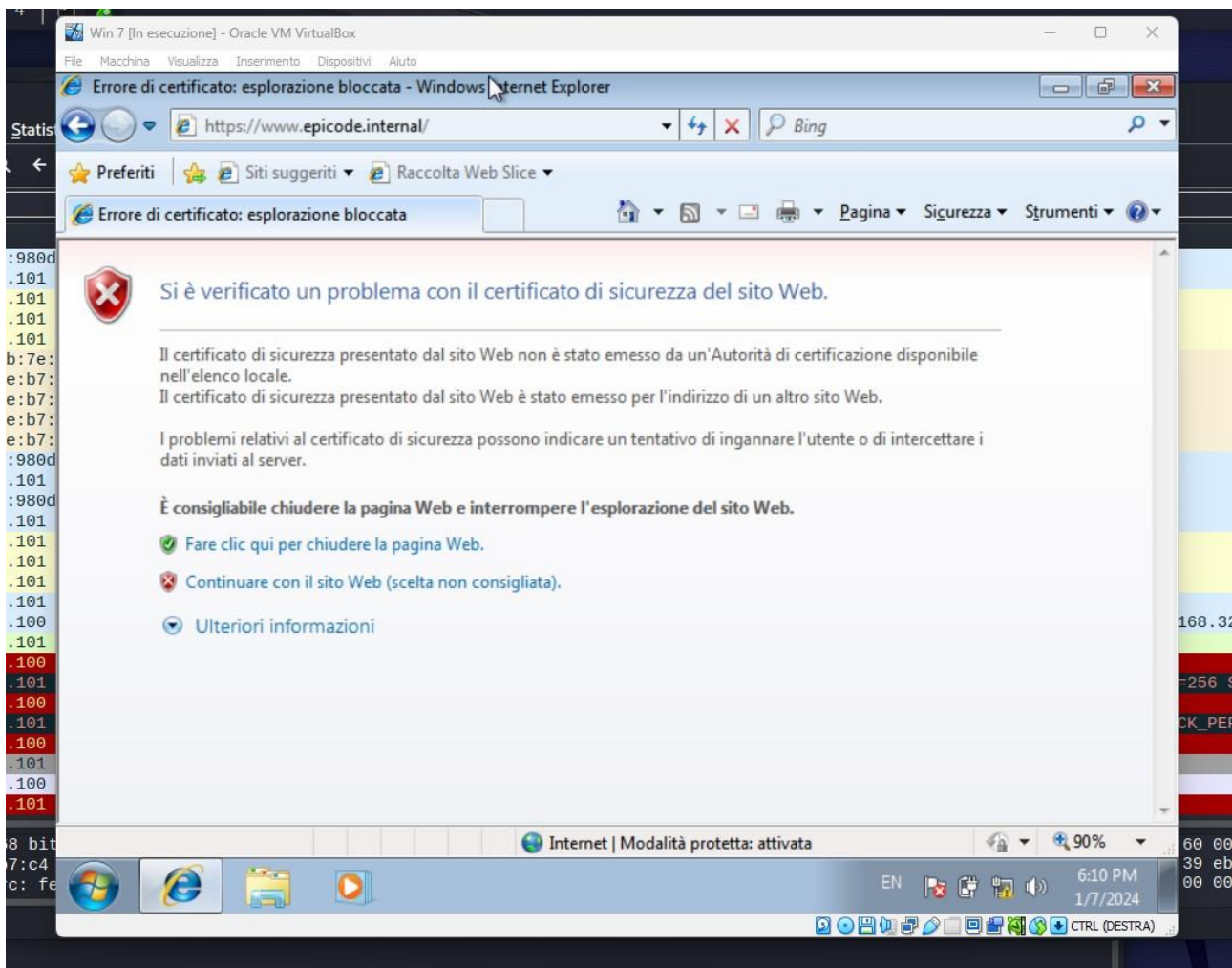
#####
# https_static_fakefile
#
# Fake files returned in fake mode based on static path.
# The fake files must be placed in <data-dir>/http/fakefiles
#
# Syntax: https_static_fakefile <path> <filename> <mime-type>
#
# Default: none
#
#https_static_fakefile /path/ sample_gui.exe x-msdos-program
#https_static_fakefile /path/to/file.exe sample_gui.exe x-msdos-program

#####
# https_ssl_keyfile
#
# Name of the SSL private key PEM file.
# The key MUST NOT be encrypted!
#
# The file must be placed in <data-dir>/certs/
#
#
```

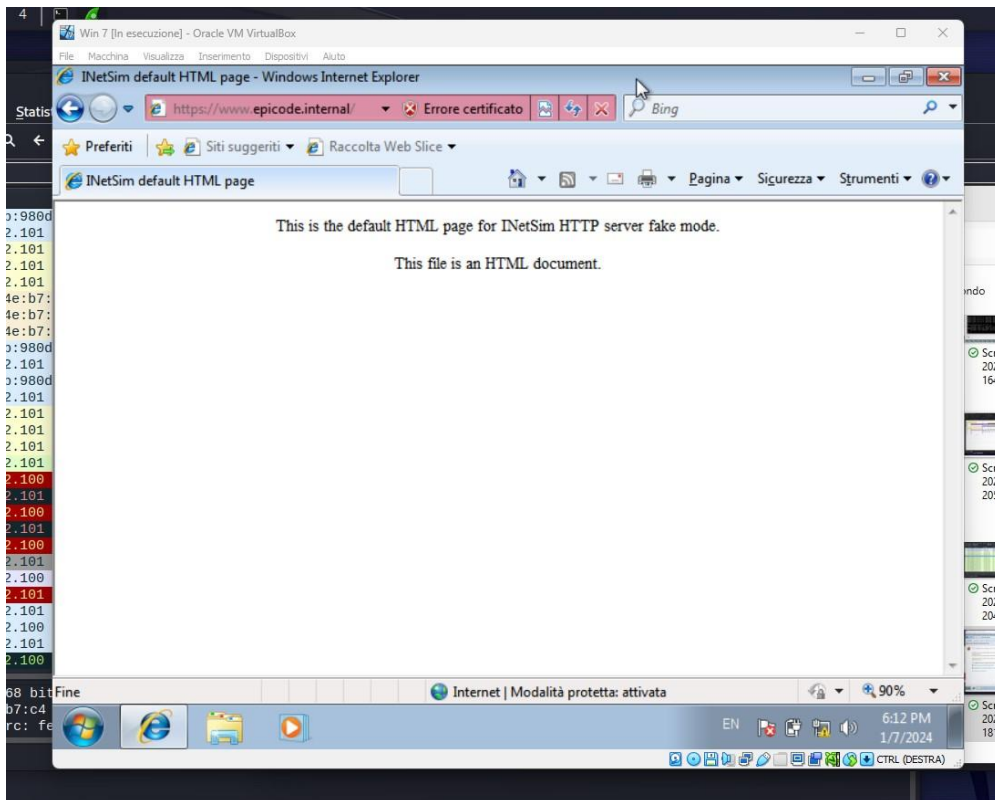
Attivazione processo Inetsim: comando sudo inetsim. Processo avviato, in ascolto su 192.168.32.100 con porta 443

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo nano /etc/network/interfaces  
[sudo] password for kali:  
kali@kali:~$ sudo nano /etc/inetsim/inetsim.conf  
kali@kali:~$ sudo inetsim  
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 10330) ==  
Session ID: 10330  
Listening on: 192.168.32.100  
Real Date/Time: 2024-01-07 12:07:56  
Fake Date/Time: 2024-01-07 12:07:56 (Delta: 0 seconds)  
Forking services ...  
* dns_53_tcp_udp - started (PID 10340)  
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 10341)  
done.  
Simulation running.  
KALI LINUX  
"the quieter you become, the more you are able to hear"
```

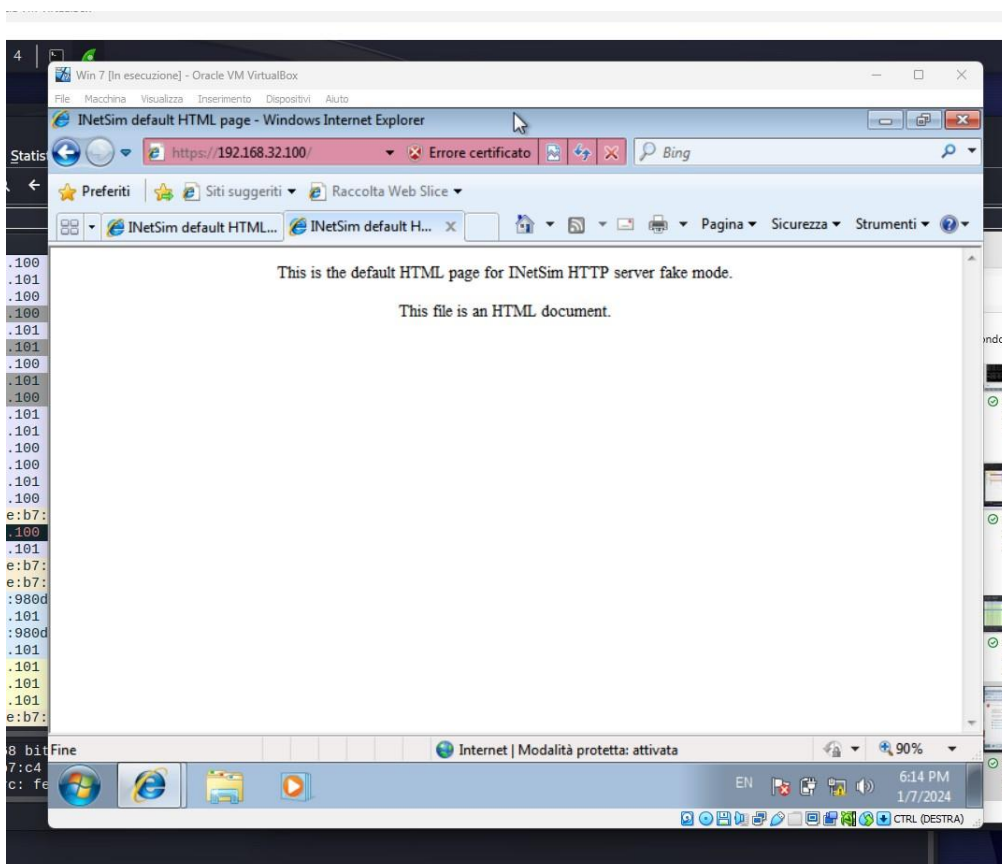
Richiesta da client window7 pt1: Richiede tramite web browser una risorsa all'hostname epicode.internal.



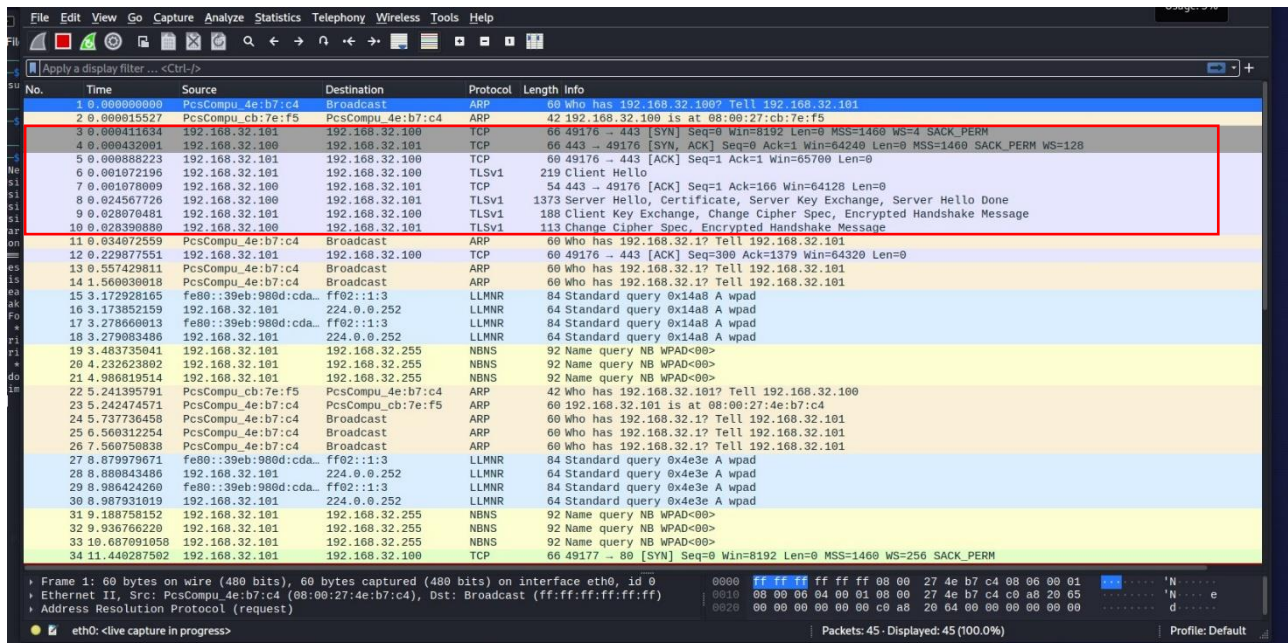
Richiesta da client window7 pt2: Richiede tramite web browser una risorsa all'hostname epicode.internal.
Risoluzione Indirizzo <https://www.epicode.internal>



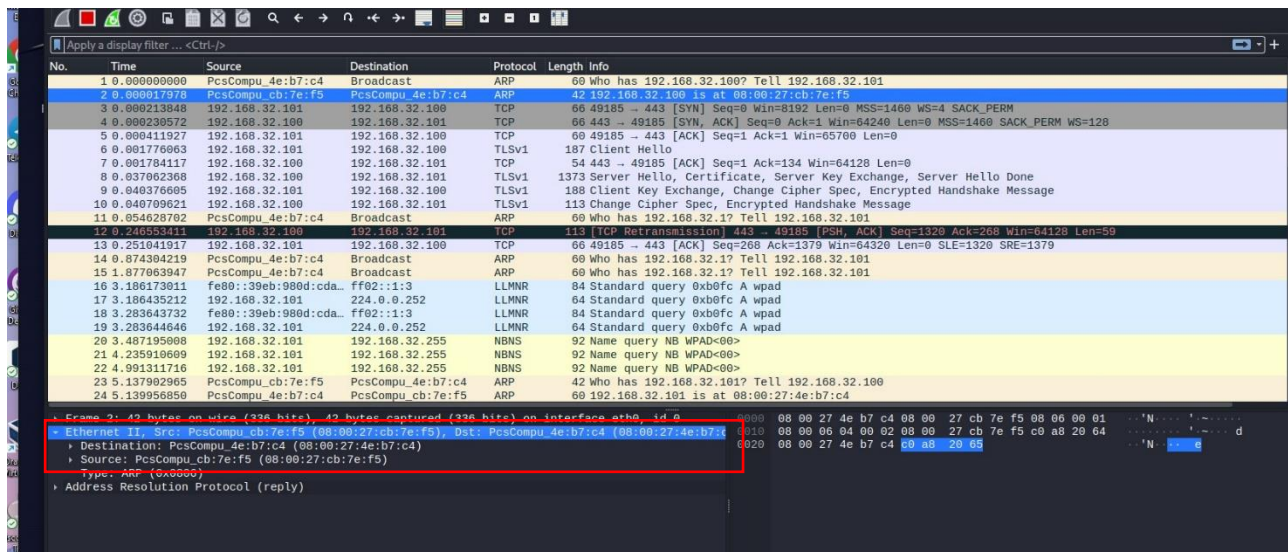
Richiesta da client window7 pt2: Richiede tramite web browser una risorsa all'hostname epicode.internal.
Risoluzione da Indirizzo 192.168.32.100



Cattura Wireshark comunicazione TCP tra client (windows7 192.168.32.101) e server (Kali 192.168.32.100).
SYN – SYN ACK – ACK e il contenuto della richiesta HTTPS.



MAC address di sorgente e destinazione. Source MAC Kali 08:00:27:cb:7e:f5 – MAC destination Windows7 08:00:27:4e:b7:c4



Configurazione Inetsim Kali Pt1: Attivazione servizio HTTP + DSN + abilitazione bind address con IP Kali 192.162.32.100. Comando sudo nano /etc/intesim/inetsim.conf

```
File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsim.conf *
#
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
#start_service ntp
#start_service finger
#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 192.168.32.100

#####
# service_run_as_user
#
# User to run services

#####
# 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_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
dns_default_hostname epicode.internal

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

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

Qui lascio tutto come sopra per il servizio https

```
File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsim.conf *
#
# 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_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
dns_default_hostname epicode.internal

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

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

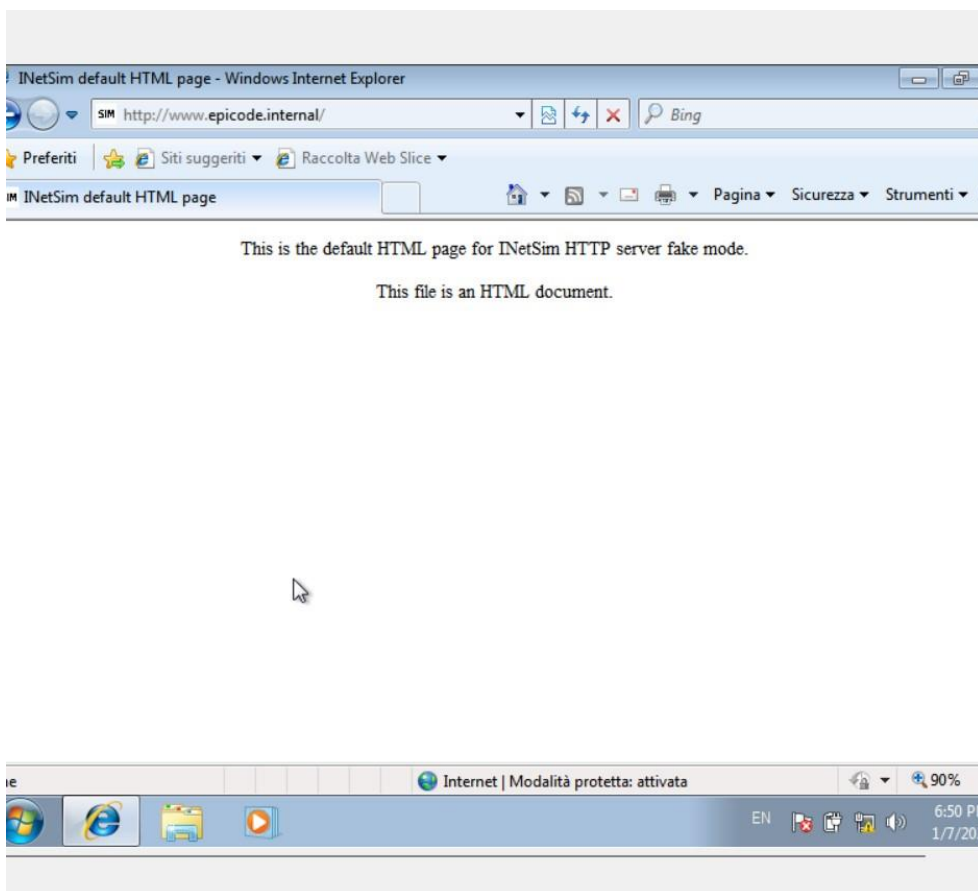
Attivazione fakefile http

```
File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsim.conf *
#
# Default: none
#
http_fakefile txt sample.txt text/plain
http_fakefile htm sample.html text/html
http_fakefile html sample.html text/html
http_fakefile php sample.html text/html
http_fakefile gif sample.gif image/gif
http_fakefile jpg sample.jpg image/jpeg
http_fakefile jpeg sample.jpg image/jpeg
http_fakefile png sample.png image/png
http_fakefile bmp sample.bmp image/x-ms-bmp
http_fakefile ico favicon.ico image/x-icon
http_fakefile exe sample_gui.exe x-msdos-program
http_fakefile com sample_gui.exe x-msdos-program

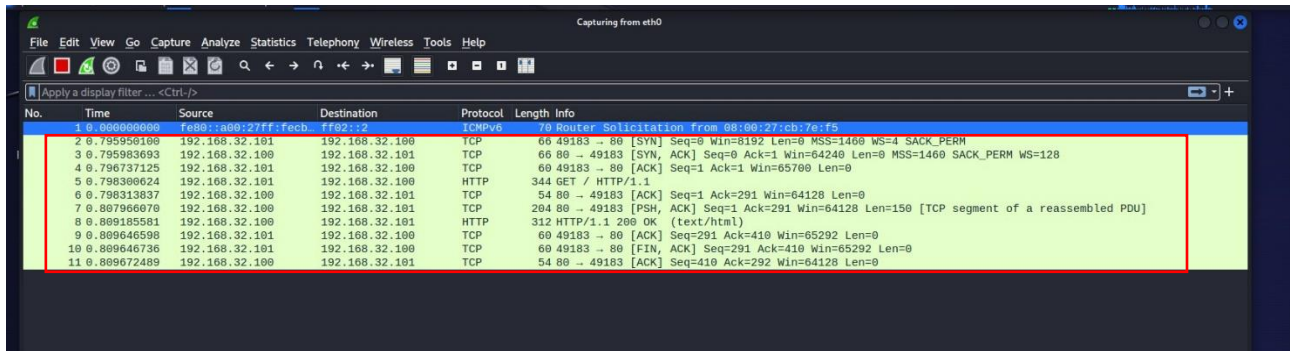
#####
# http_default_fakefile
#
# The default fake file returned in fake mode if the file extension
# in the HTTP request does not match any of the extensions
# defined above.
#
# The default fake file must be placed in <data-dir>/http/fakefiles
# Syntax: http_default_fakefile <filename> <mime-type>
# Default: none
http_default_fakefile sample.html text/html

#####
# http_static_fakefile
#
# Fake files returned in fake mode based on static path.
# The fake files must be placed in <data-dir>/http/fakefiles
# Syntax: http_static_fakefile <path> <filename> <mime-type>
# Default: none
#
#http_static_fakefile /path/ sample_gui.exe x-msdos-program
#http_static_fakefile /path/to/file.exe sample_gui.exe x-msdos-program
```

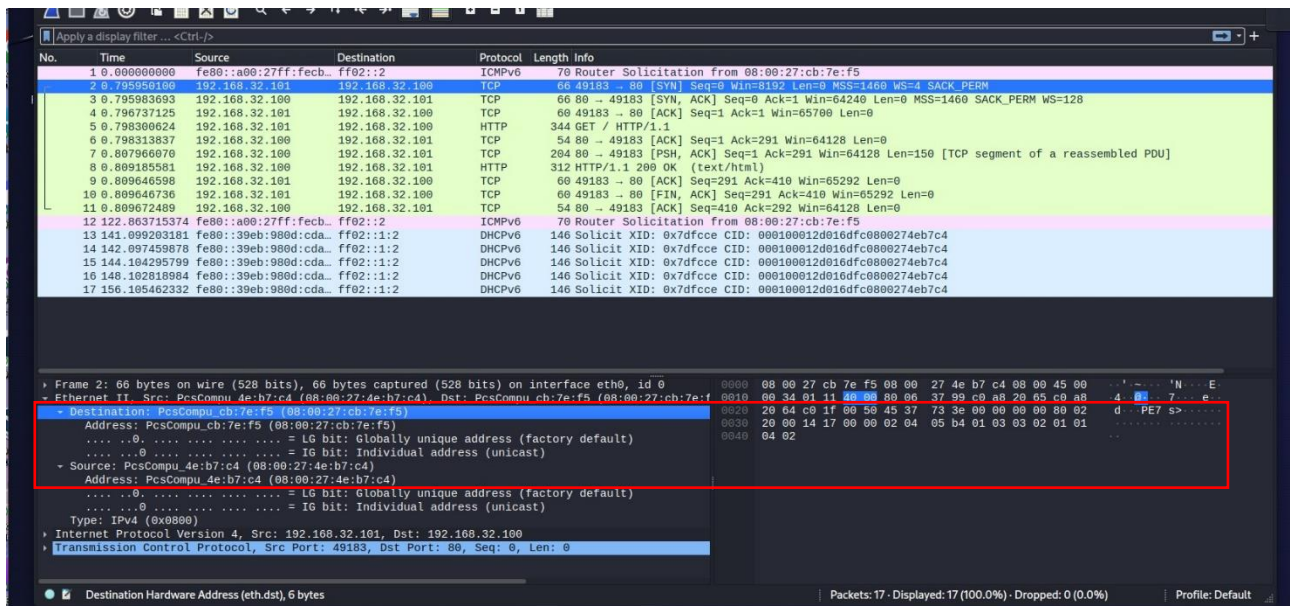
Richiesta da client window7: Richiede tramite web browser una risorsa all'hostname epicode.internal.
Risoluzione Indirizzo <http://www.epicode.internal>



Cattura Wireshark comunicazione TCP tra client (windows7 192.168.32.101) e server (Kali 192.168.32.100).
SYN – SYN ACK – ACK e il contenuto della richiesta http



MAC address di sorgente e destinazione. Source MAC Windows7 08:00:27:4e:b7:c4 - Destination MAC Kali 08:00:27:cb:7e:f5



Sintesi differenza:

HTTP (Non Sicuro):

Le sessioni TCP in HTTP sono non sicure perché i dati vengono trasmessi in chiaro attraverso la rete.

La comunicazione non è cifrata, il che significa che se un attaccante intercetta la trasmissione, può leggere e comprendere facilmente i dati scambiati tra il client e il server.

HTTPS (Sicuro):

Le sessioni TCP in HTTPS sono sicure grazie all'aggiunta del layer di sicurezza TLS (Transport Layer Security)

Tutti i dati trasmessi tra il client e il server attraverso una connessione HTTPS sono cifrati. Questo significa che, anche se un attaccante intercetta i dati, non può leggere facilmente le informazioni sensibili.

Handshake TLS:

Quando si utilizza HTTPS, viene eseguito un handshake TLS tra il client e il server durante l'inizio della connessione. Questo processo stabilisce una chiave di sessione segreta che verrà utilizzata per cifrare e decifrare i dati durante la sessione.

Porte Standard:

HTTP utilizza la porta standard 80 per la comunicazione non sicura, mentre HTTPS utilizza la porta standard 443 per la comunicazione sicura.

URL:

Le risorse web servite tramite HTTPS iniziano con "https://" nell'URL, mentre quelle servite tramite HTTP iniziano con "http://".

In sintesi, la principale differenza tra le sessioni TCP in HTTP e HTTPS è la sicurezza. HTTPS aggiunge uno strato di crittografia tramite TLS, rendendo la comunicazione tra client e server più sicura e protetta contro potenziali intercettazioni o manipolazioni dei dati durante il trasferimento.