

# W4D4

## TRACCIA:

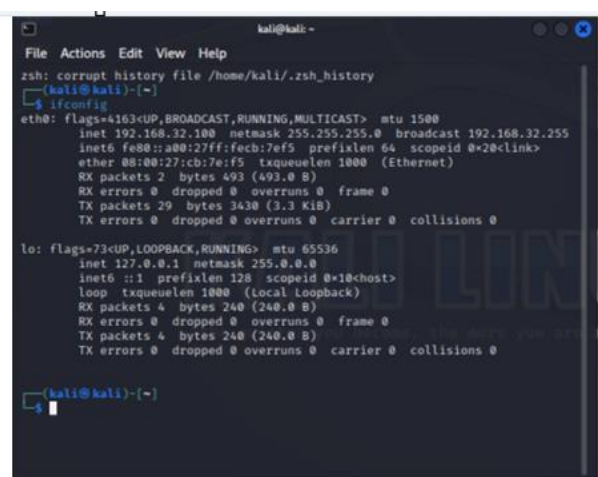
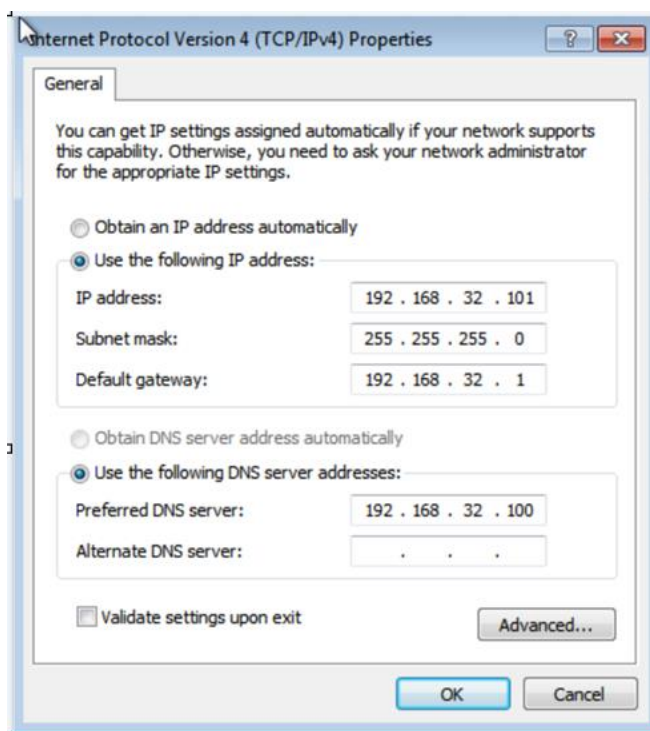
Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (Kali).

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.

## SOLUZIONE:

Come primo passaggio andiamo a configurare gli IP statici sulle due macchine come indicato nella traccia.



Successivamente passiamo alla configurazione di Inetsim che poi ci permetterà di simulare il traffico fra host e server.

In particolare, andiamo a settare il servizio DNS oltre all'HTTP e all'HTTPS.

```
GNU nano 7.2 /etc/inetsim/inetsim.conf *
#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: 192.168.32.100
service_bind_address 192.168.32.100

#
#####
# service_run_as_user
#
#

#####
# 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: 192.168.32.100
dns_default_ip 192.168.32.100

#####
# dns_default_hostname
#

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

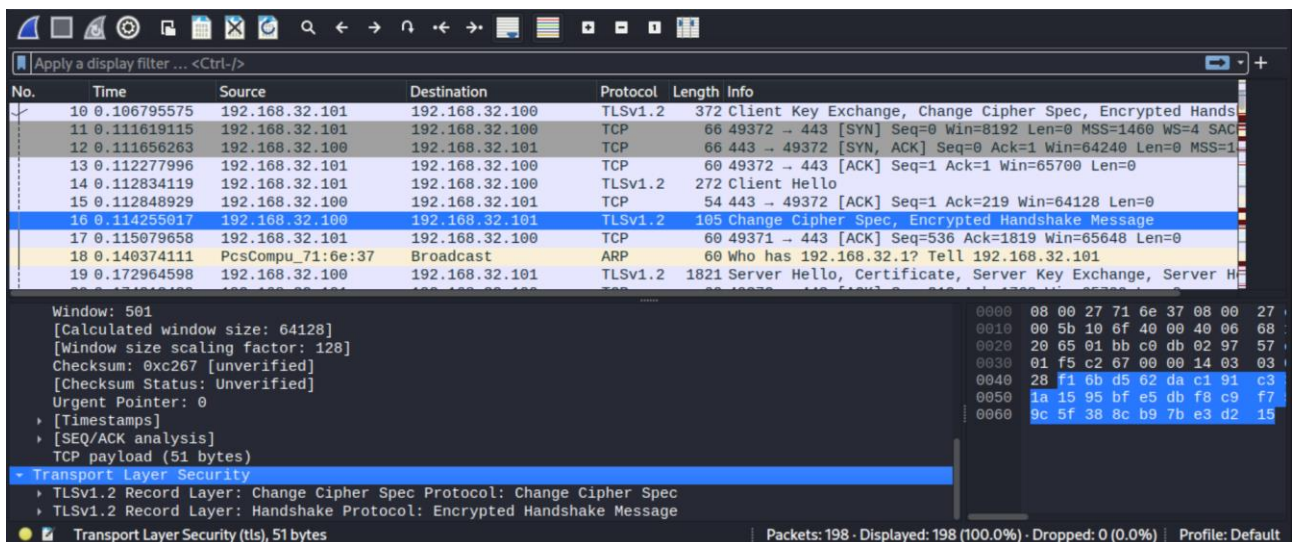
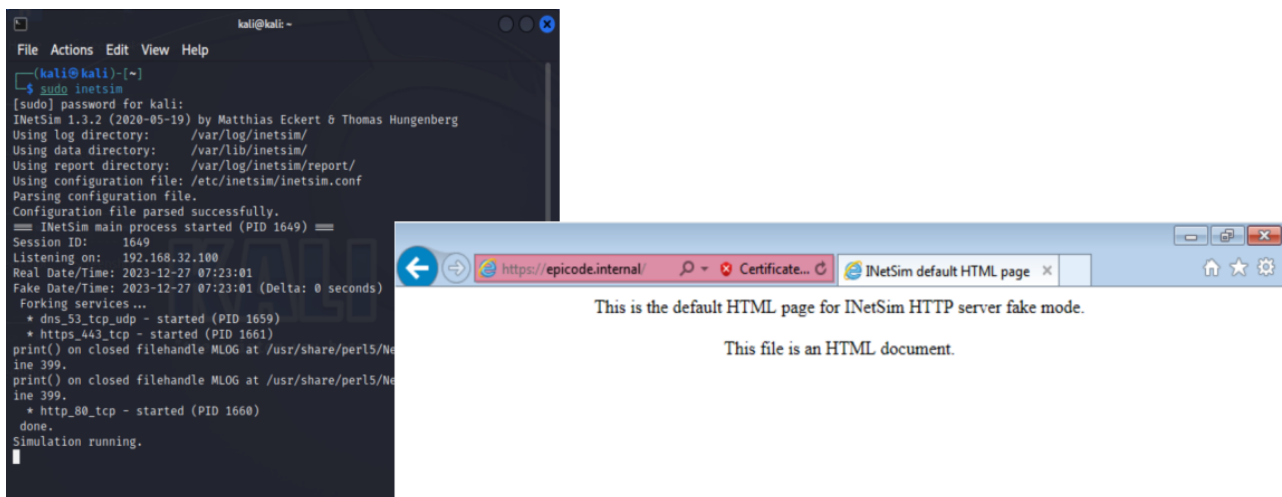
#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
dns_static epicode.internal 192.168.32.100
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30

#####
# dns_version
#
# DNS version
#

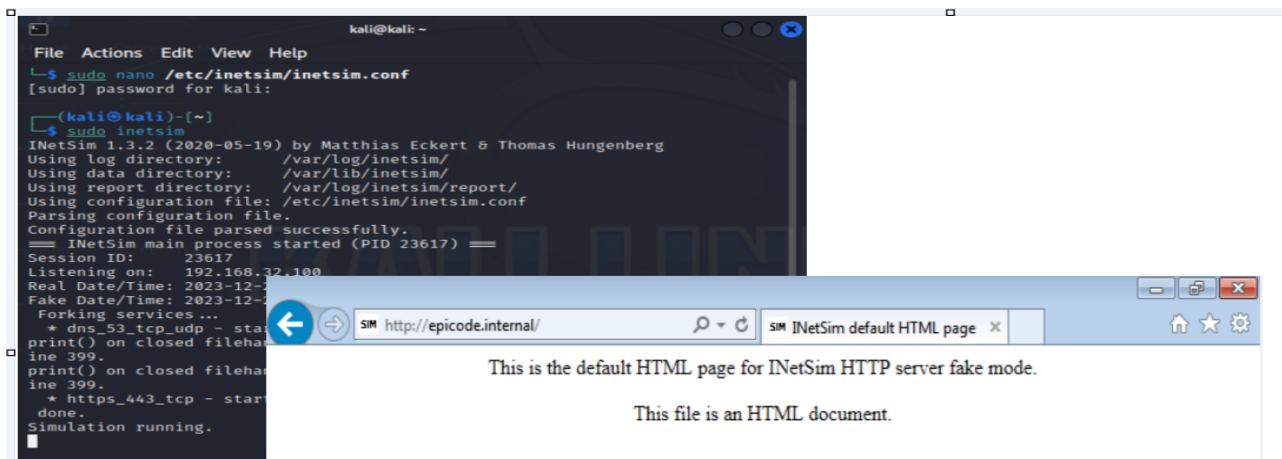
#####
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
```

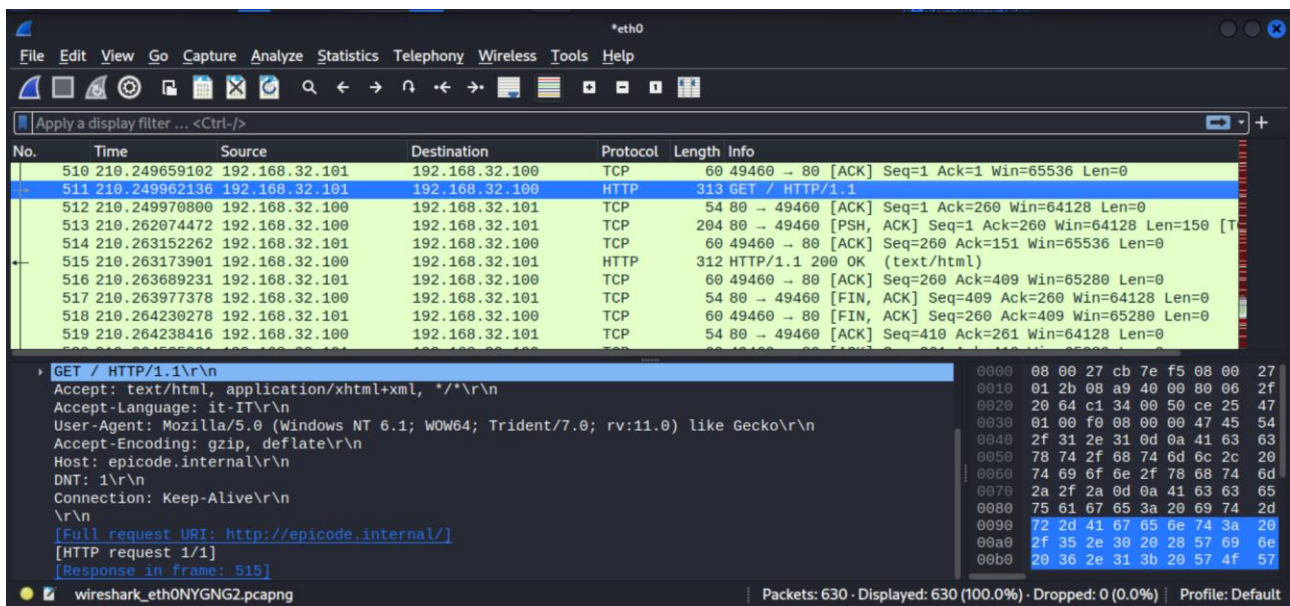
Dopo aver effettuato la configurazione di Inetsim e dei relativi servizi possiamo procedere ad analizzare i pacchetti che vengono scambiati fra host e server utilizzando il tool Wireshark.

## Analisi servizio HTTPS:



## ANALISI SERVIZIO HTTP:





## CONCLUSIONI:

La differenza sostanziale che si può notare fra l'HTTP e l'HTTPS è che nel primo, non essendo un protocollo sicuro, l'indirizzo richiesto dall'host è visibile mentre nel secondo, essendo un protocollo sicuro, i pacchetti sono crittografati mediante l'utilizzo del protocollo TLSv 1.2.