

W4D4 – Michele Ungolo -

Soluzione:

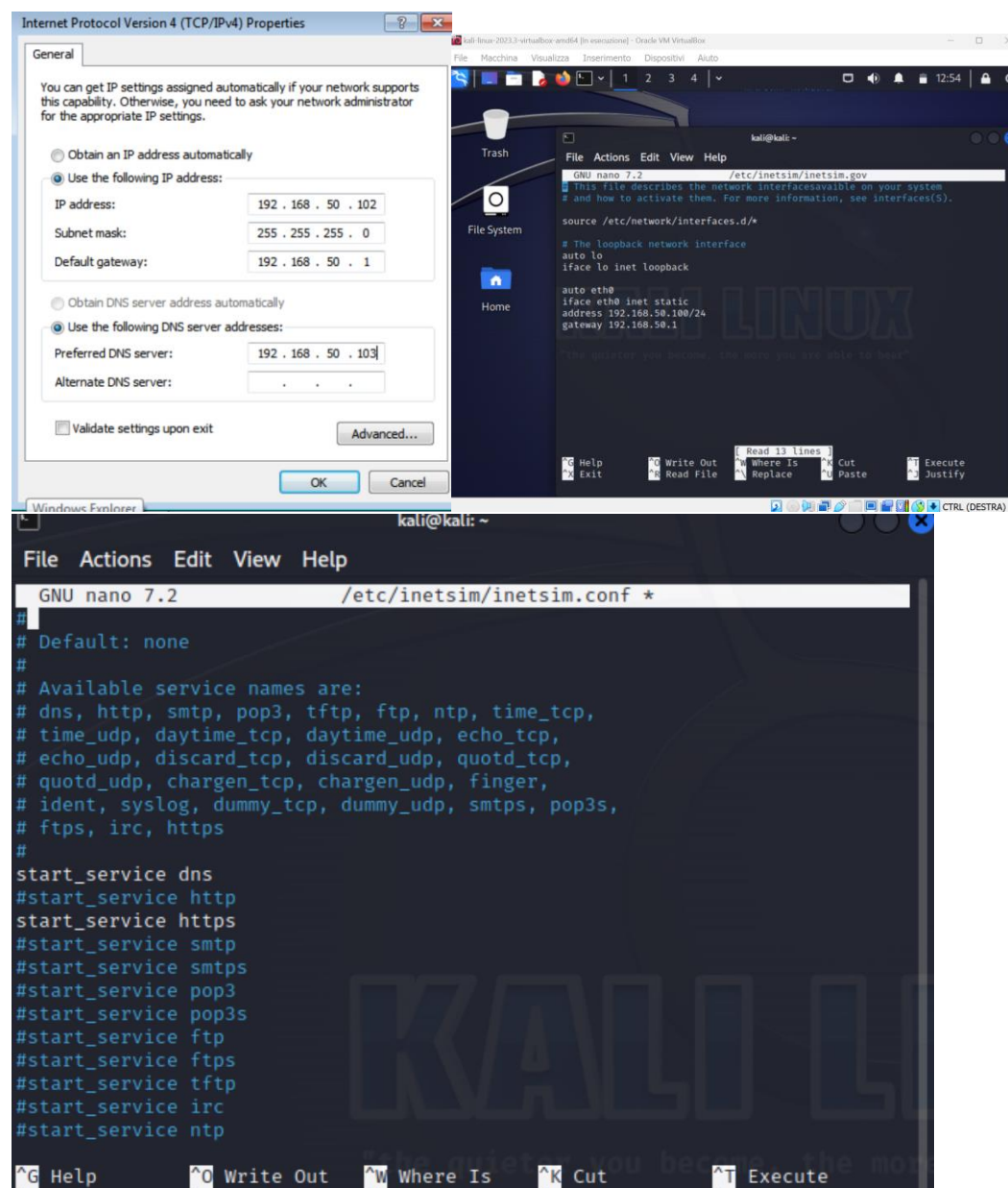
1. Configurazione IP Kali Linux e Windows:

Kali Linux: IP 192.168.32.100

Windows 7: IP 192.168.32.101

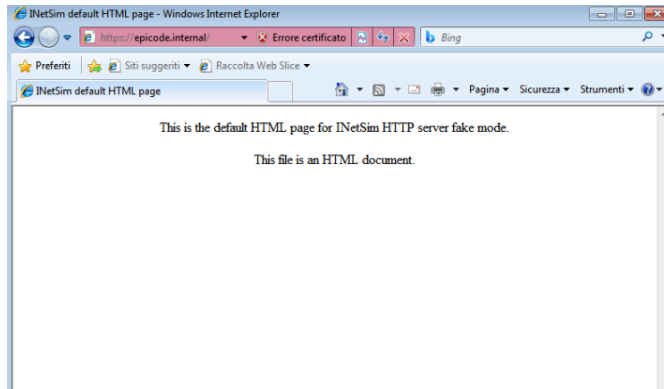
Inserimento dell'IP DNS su Windows 7: IP 192.168.32.100 - HTTPS server: Attivo

Servizio DNS: Attivo



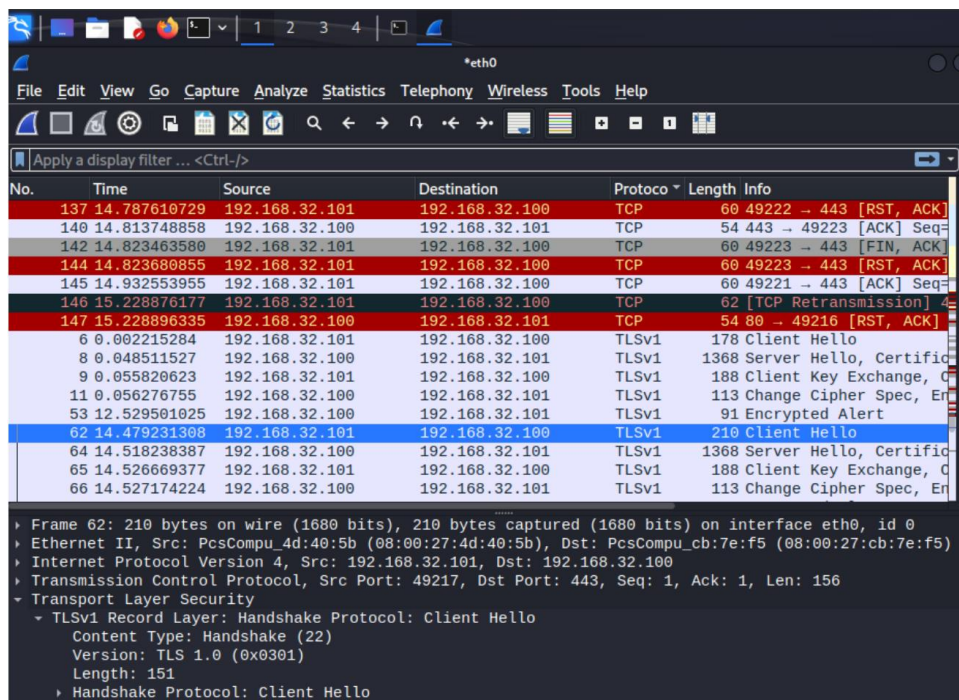
2. Comunicazione tramite HTTPS

Richiesta HTTPS: - Il client (Windows 7) richiede tramite web browser una risorsa all'hostname "epicode.internal" al server HTTPS (Kali Linux).



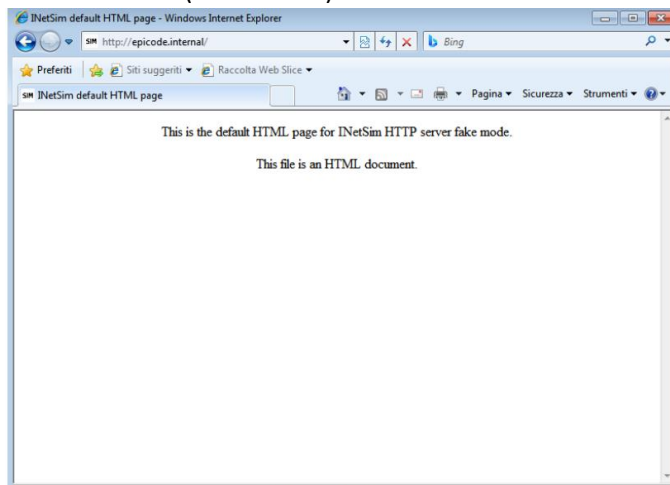
Utilizzando Wireshark, intercettiamo la comunicazione.

- Sorgente MAC: [MAC_Address_Client], Destinazione MAC: [MAC_Address_Server] - Contenuto richiesta HTTPS: [Contenuto_Richiesta_HTTPS].

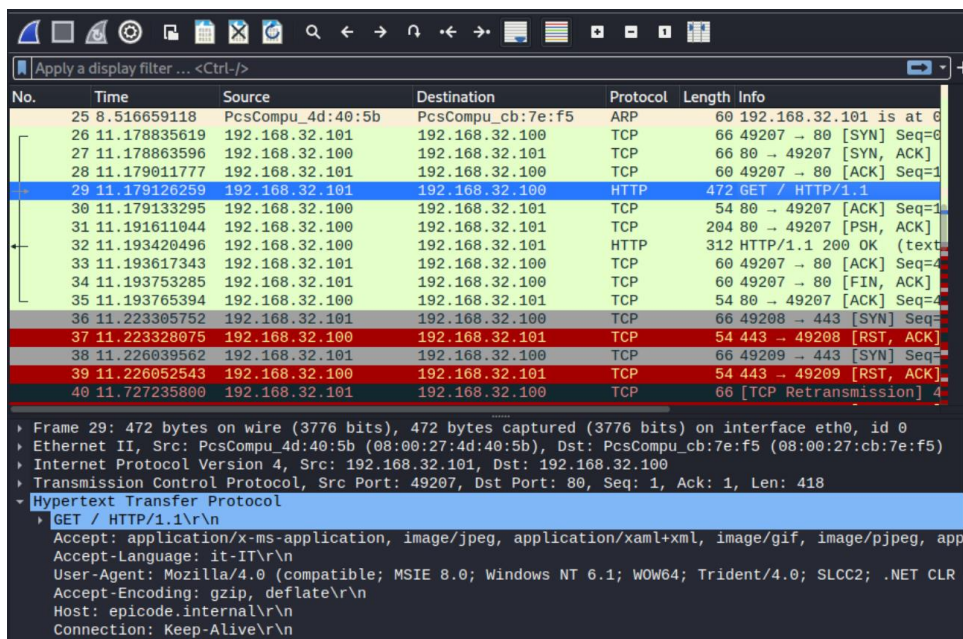


3. Comunicazione tramite HTTP

Dopo aver Modificato il Server con un server HTTP su Kali Linux, effettuiamo una nuova richiesta HTTP: -Il client (Windows 7) effettua una nuova richiesta tramite web browser.

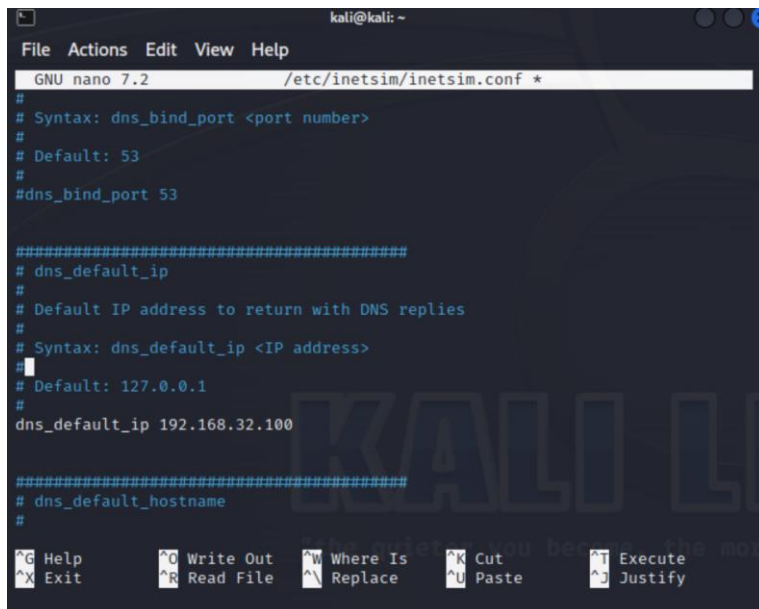


Successivamente aprima Wireshark Capture (HTTP) e notiamo come la comunicazione sia stata intercettata. - Sorgente MAC: (MAC_Address_Client), Destinazione MAC: (MAC_Address_Server) - Contenuto richiesta HTTP: (Contenuto_Richiesta_HTTP)



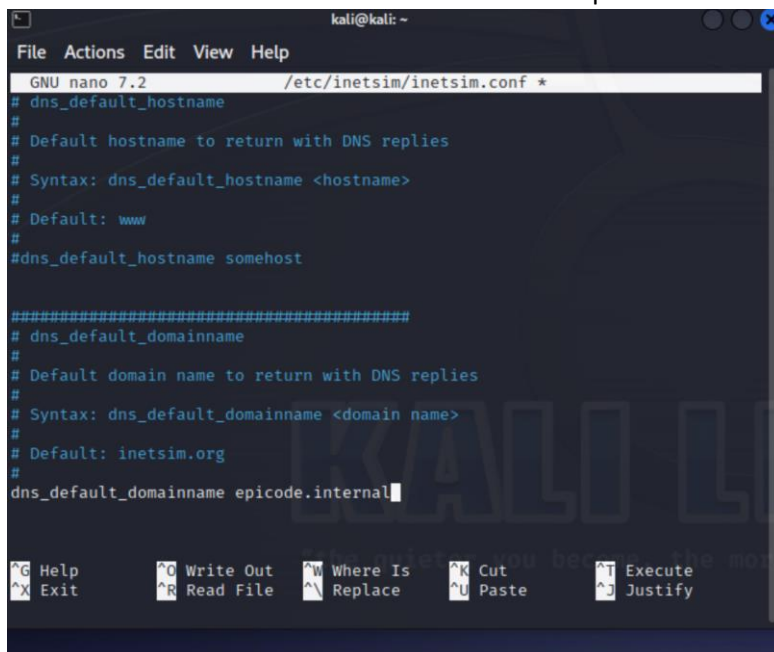
Impostazione SERVIZI DNS su Kali Linux

Ho impostato il DNS default IP: 192.168.32.100, Kali è il nostro server, nell'IP del DNS va inserito il suo stesso IP.



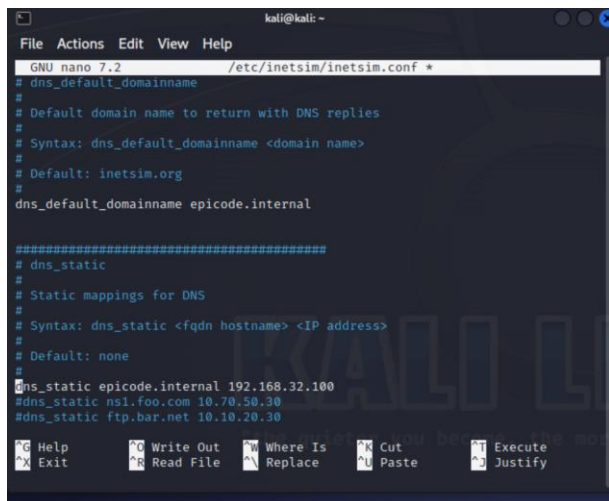
```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/inetsim/inetsim.conf *  
#  
# Syntax: dns_bind_port <port number>  
#  
# Default: 53  
#  
#dns_bind_port 53  
  
#####  
# dns_default_ip  
#  
# Default IP address to return with DNS replies  
#  
# Syntax: dns_default_ip <IP address>  
#  
# Default: 127.0.0.1  
#  
dns_default_ip 192.168.32.100  
  
#####  
# dns_default_hostname  
#  
#####  
# 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
```

Il Domain name come richiesto dall'esercizio è "epicode.internal"



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

Nel DNS static viene associato il Domain name all'IP: epicode.internal.



```
GNU nano 7.2 /etc/inetsim/inetsim.conf *
# 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 epicode.internal 192.168.32.100
#dns_static nsl.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30

Help      Write Out  Where Is  Cut       Execute
Exit      Read File  Replace   Paste     Justify
```

CONCLUSIONI:

In conclusione, possiamo dire che nel traffico HTTPS, il contenuto della richiesta è crittografato e garantisce sicurezza, mentre nel traffico HTTP, il contenuto, leggibile e chiaro, potrebbe essere a rischio intercettazione. La principale differenza tra i due sta proprio nella sicurezza.