

Compito W3D1 – Pratica

Corso: Cybersecurity Analyst – Epicode

Studente: Daniele Taormina

Data: 10/10/2025

Introduzione

In questo esercizio ho lavorato sulla configurazione di una policy firewall su Windows, sull'emulazione di servizi di rete con INetSim in Kali Linux e sulla cattura e analisi del traffico con Wireshark.

Obiettivo dell'esercizio

L'obiettivo dell'esercitazione era:

1. Configurare una policy nel firewall di Windows per permettere il ping da Kali Linux.
2. Utilizzare l'utility INetSim su Kali Linux per emulare servizi di rete HTTP e HTTPS.
3. Effettuare la cattura dei pacchetti con Wireshark e analizzare il contenuto.

Indirizzi Macchine:

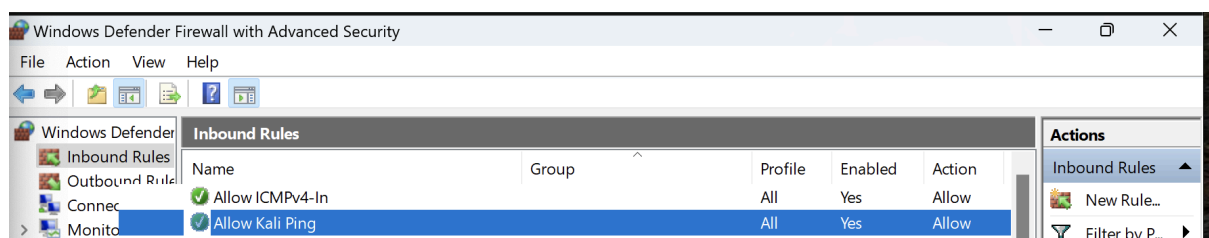
Kali: 192.168.50.100

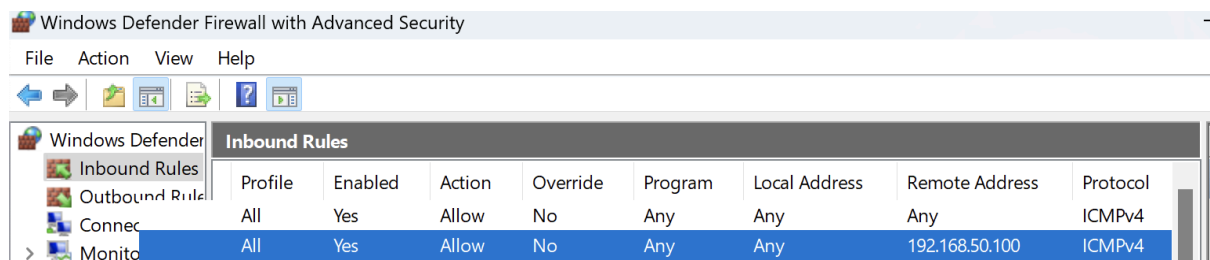
Metasploitable2: 192.168.50.101

Windows: 192.168.50.102

Esecuzione

Per prima cosa ho settato una regola di firewall Inbound sulla macchina Windows per permettere a Kali di effettuare una richiesta Ping su Windows. Nonostante la regola di Allow ICMPv4-In configurata su Any (qualsiasi indirizzo IP) dovevamo implementare un'ulteriore regola che permettesse questa connessione.





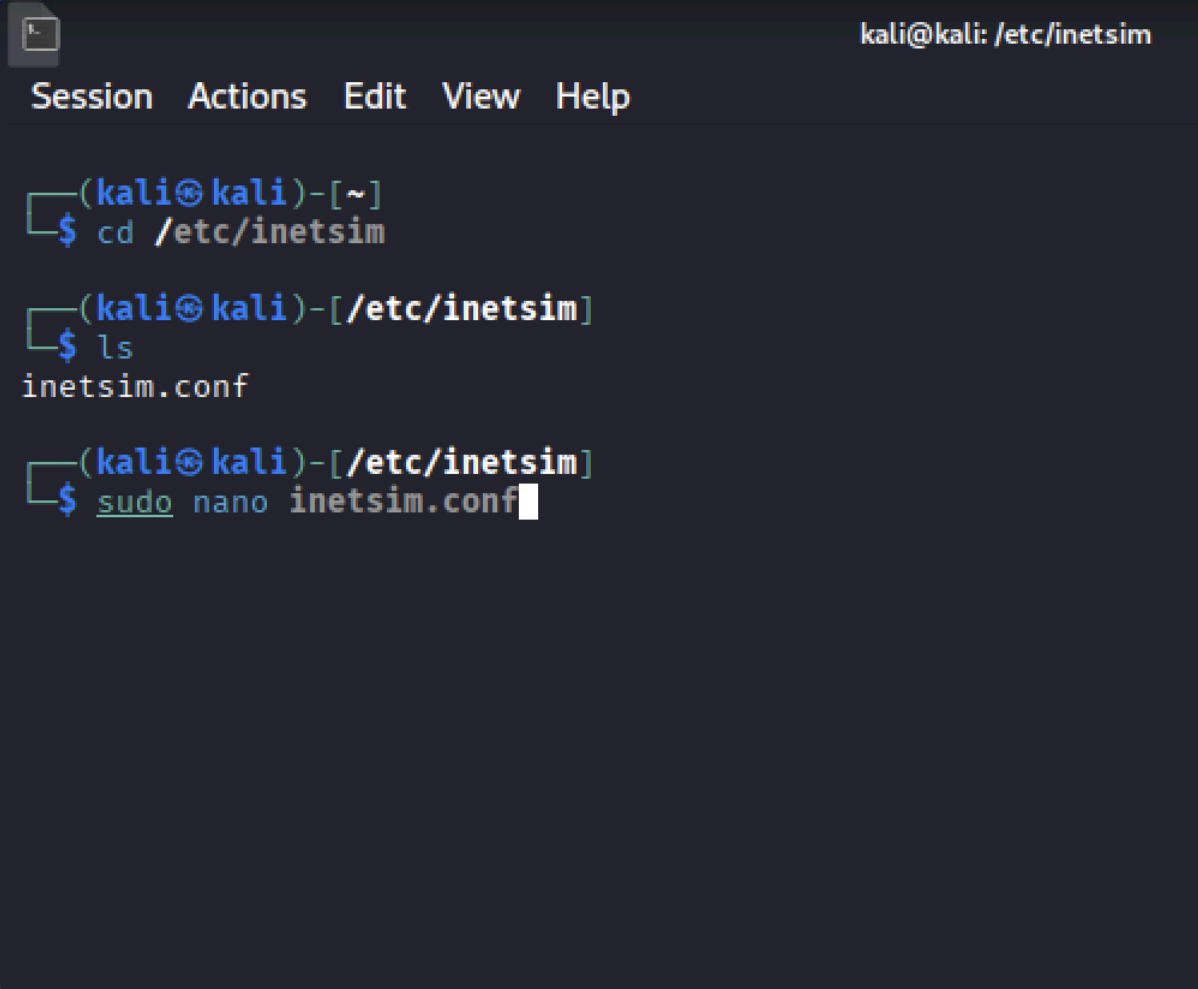
Notiamo come la regola adesso è stata configurata, adesso quindi non resta che testare e “pingare” Windows da Kali.

```
kali@kali: ~  
Session Actions Edit View Help  
  
(kali@kali)-[~]  
$ ping -c 4 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.  
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.563 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.592 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.562 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.563 ms  
  
— 192.168.50.102 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3076ms  
rtt min/avg/max/mdev = 0.562/0.570/0.592/0.012 ms  
  
(kali@kali)-[~]  
$
```

Test riuscito.

Obiettivo 2 - Utilizzare l'utility INetSim su Kali Linux per emulare servizi di rete HTTP e HTTPS.

Per prima , prima di utilizzare INetSim, dobbiamo configurarlo inserendo l'indirizzo IP della macchina in questione, ovvero Kali (192.168.50.100).

A terminal window with a dark background and light-colored text. The title bar at the top right says 'kali@kali: /etc/inetsim'. Below the title bar is a menu bar with 'Session', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows three commands being executed: 'cd /etc/inetsim', 'ls', and 'sudo nano inetsim.conf'. The output of 'ls' is 'inetsim.conf'. The cursor is at the end of the 'sudo nano inetsim.conf' command.

```
kali@kali: /etc/inetsim
Session Actions Edit View Help
(kali@kali)-[~]
$ cd /etc/inetsim
(kali@kali)-[/etc/inetsim]
$ ls
inetsim.conf
(kali@kali)-[/etc/inetsim]
$ sudo nano inetsim.conf
```

quindi navighiamo all'interno della cartella in cui si trova il file di configurazione e con permessi di root andiamo a modificarlo per poi salvarlo.

```
kali@kali: /etc/inetsim
Session Actions Edit View Help
GNU nano 8.6 inetsim.conf
# 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 192.168.50.100

#####
# service_run_as_user
#
```

gli unici servizi che ci interessano sono HTTP e HTTPS, quindi commento il resto dei servizi mettendo (#) davanti ad ogni stringa che non voglio attivare.

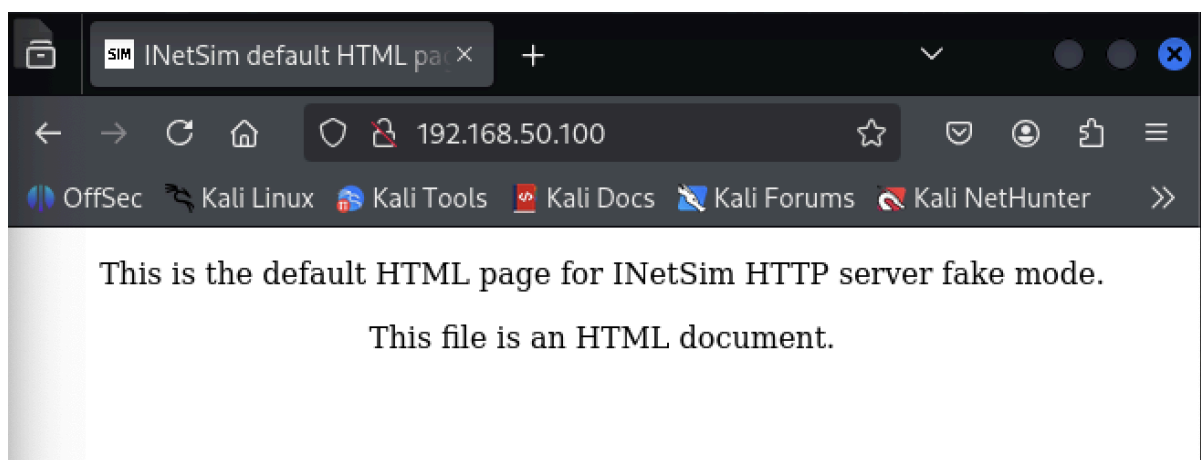
Attivo il servizio : **service_bind_address 192.68.50.100**

Lancio il comando : **sudo inetsim**

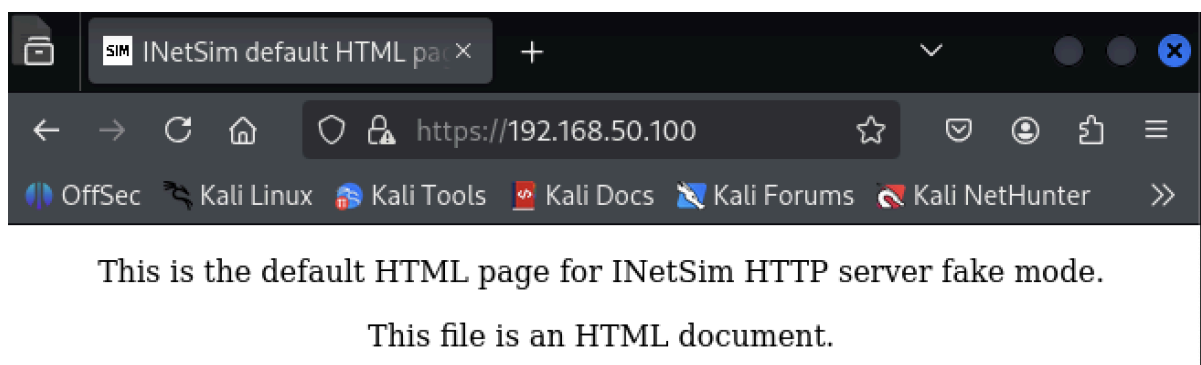
```
kali@kali: /etc/inetsim
Session Actions Edit View Help
[sudo] password for kali:

(kali@kali)-[/etc/inetsim]
$ 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 8111) ===
Session ID:      8111
Listening on:    192.168.50.100
Real Date/Time:  2025-10-15 22:09:43
Fake Date/Time: 2025-10-15 22:09:43 (Delta: 0 seconds)
Forking services ...
  * https_443_tcp - started (PID 8114)
  * http_80_tcp  - started (PID 8113)
done.
Simulation running.
```

ed ecco qua che il servizio è attivo con l'indirizzo IP configurato.
Faccio un test da Browser per essere certo che il servizio è realmente attivo sia in HTTP che in HTTPS.



HTTP.



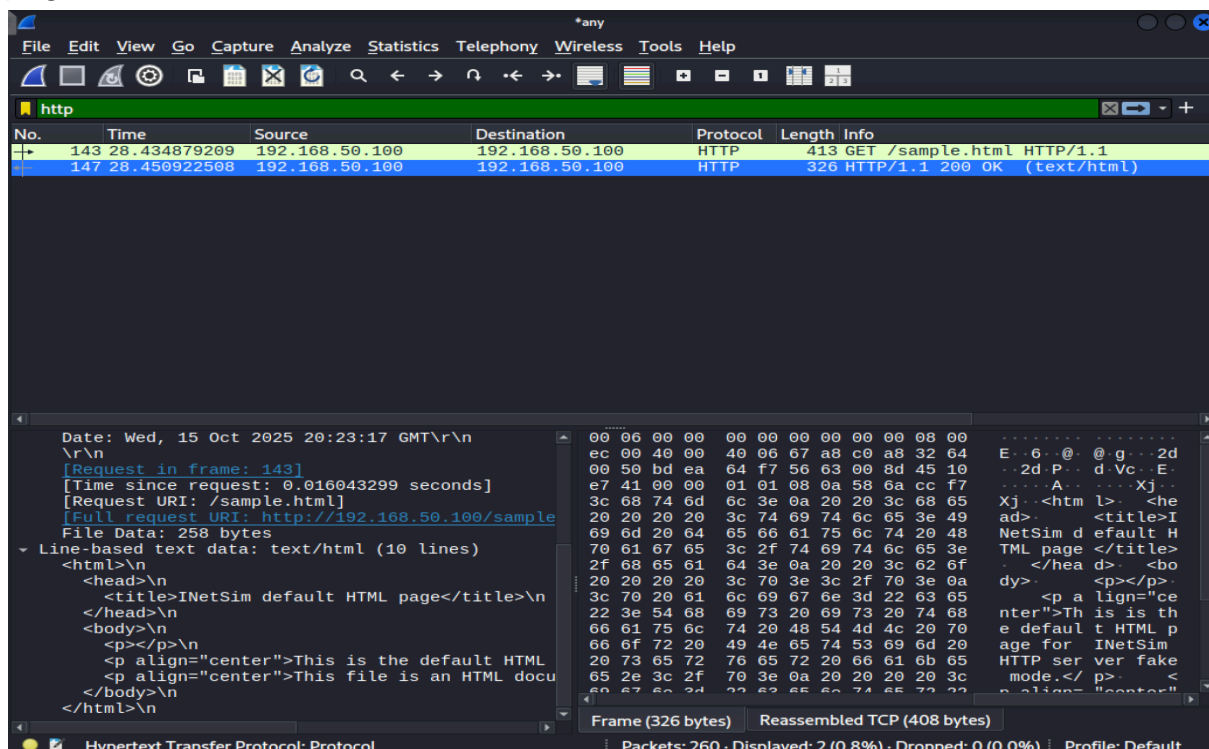
HTTPS.

Obiettivo 3 - Effettuare la cattura dei pacchetti con Wireshark e analizzare il contenuto.

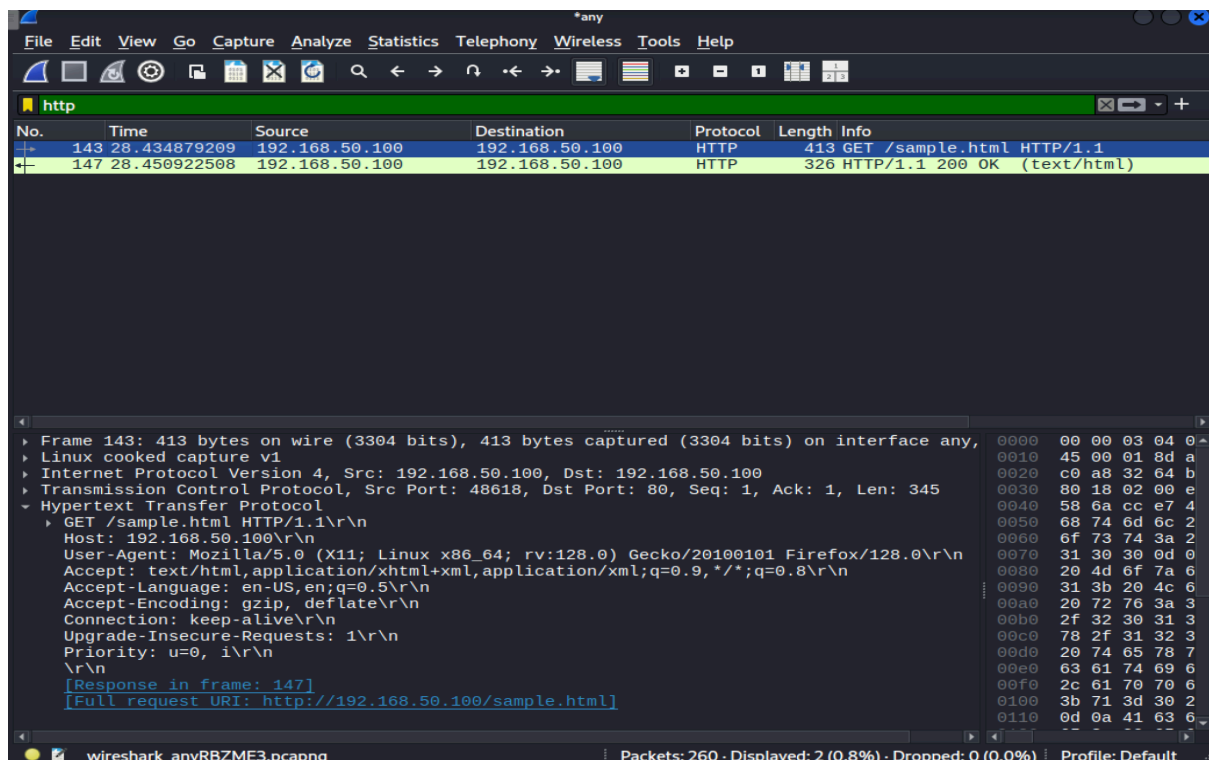
Con Wireshark (packet sniffer) completo l'ultimo obiettivo di questa consegna andando ad "ascoltare" e ad analizzare il contenuto dei pacchetti che stò simulando da INetSim.

```
(kali@kali)-[~]
$ sudo wireshark
[sudo] password for kali:
** (wireshark:8929) 22:21:42.641112 [Capture MESSAGE] -- Capture Start ...
** (wireshark:8929) 22:21:42.703869 [Capture MESSAGE] -- Error message from child: "Promiscuous mode not supported on the "any" device.", ""
** (wireshark:8929) 22:21:47.323351 [Capture MESSAGE] -- Capture started
** (wireshark:8929) 22:21:47.323394 [Capture MESSAGE] -- File: "/tmp/wireshark_any61TVE3.png"
** (wireshark:8929) 22:21:53.530744 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:8929) 22:21:53.591628 [Capture MESSAGE] -- Capture stopped.
** (wireshark:8929) 22:22:34.238265 [Capture MESSAGE] -- Capture Start ...
** (wireshark:8929) 22:22:34.321128 [Capture MESSAGE] -- Error message from child: "Promiscuous mode not supported on the "any" device.", ""
** (wireshark:8929) 22:22:35.416494 [Capture MESSAGE] -- Capture started
** (wireshark:8929) 22:22:35.416534 [Capture MESSAGE] -- File: "/tmp/wireshark_anyRBZME3.png"
** (wireshark:8929) 22:23:32.182779 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:8929) 22:23:32.231355 [Capture MESSAGE] -- Capture stopped.
```

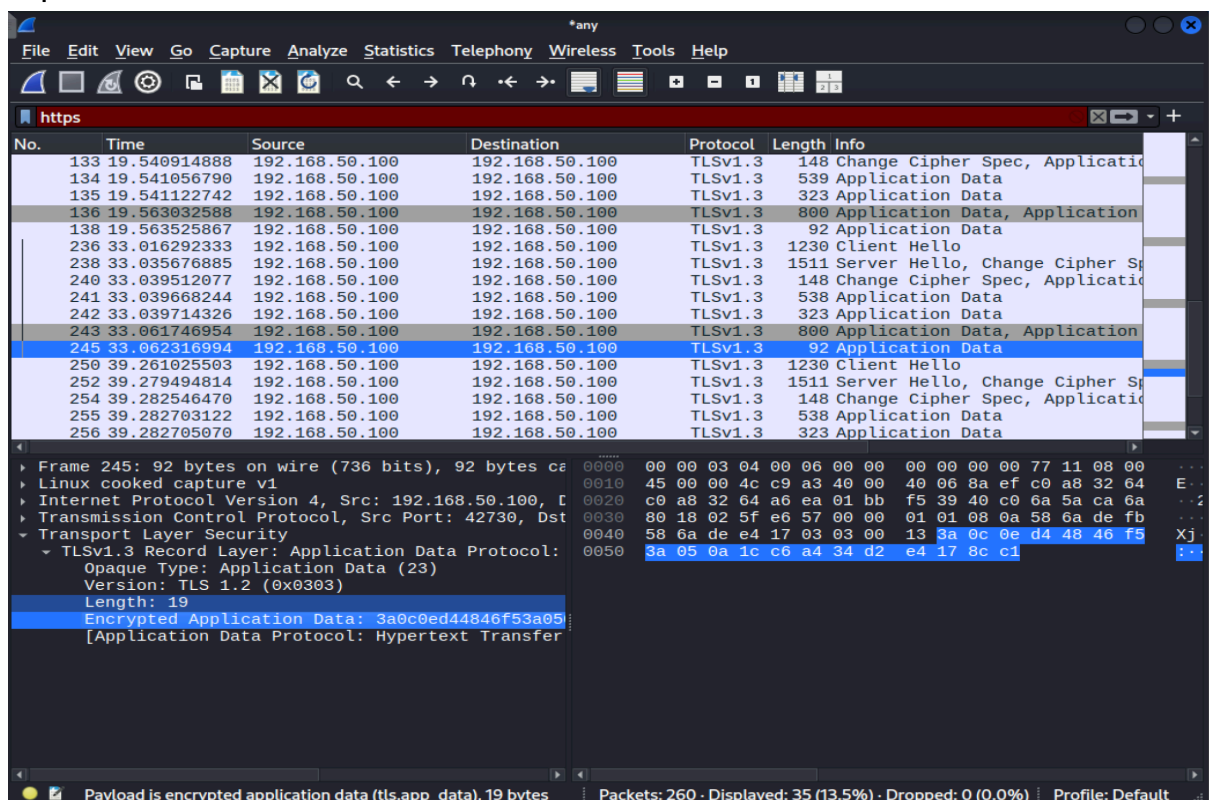
Applicando il filtro HTTP vado ad analizzare le richieste 143 e 147 , all'interno trovo molti dati tra cui il Line-Based text data ovvero il testo contenuto nella pagina visualizzata nel Browser.



Trovo anche informazioni sensibili come User-Agent e Lingua.



Mentre invece se filtro con protocollo HTTPS tutte le informazioni sono criptate.



Conclusione

Tutti gli obiettivi sono stati raggiunti, questa consegna rende chiara l'idea di quanto sia importante usare protocolli sicuri per navigare in rete e soprattutto quanto è importante saper impostare dei firewall perché questi ultimi possono dare e togliere la possibilità di connettersi a una rete e di limitare l'ut