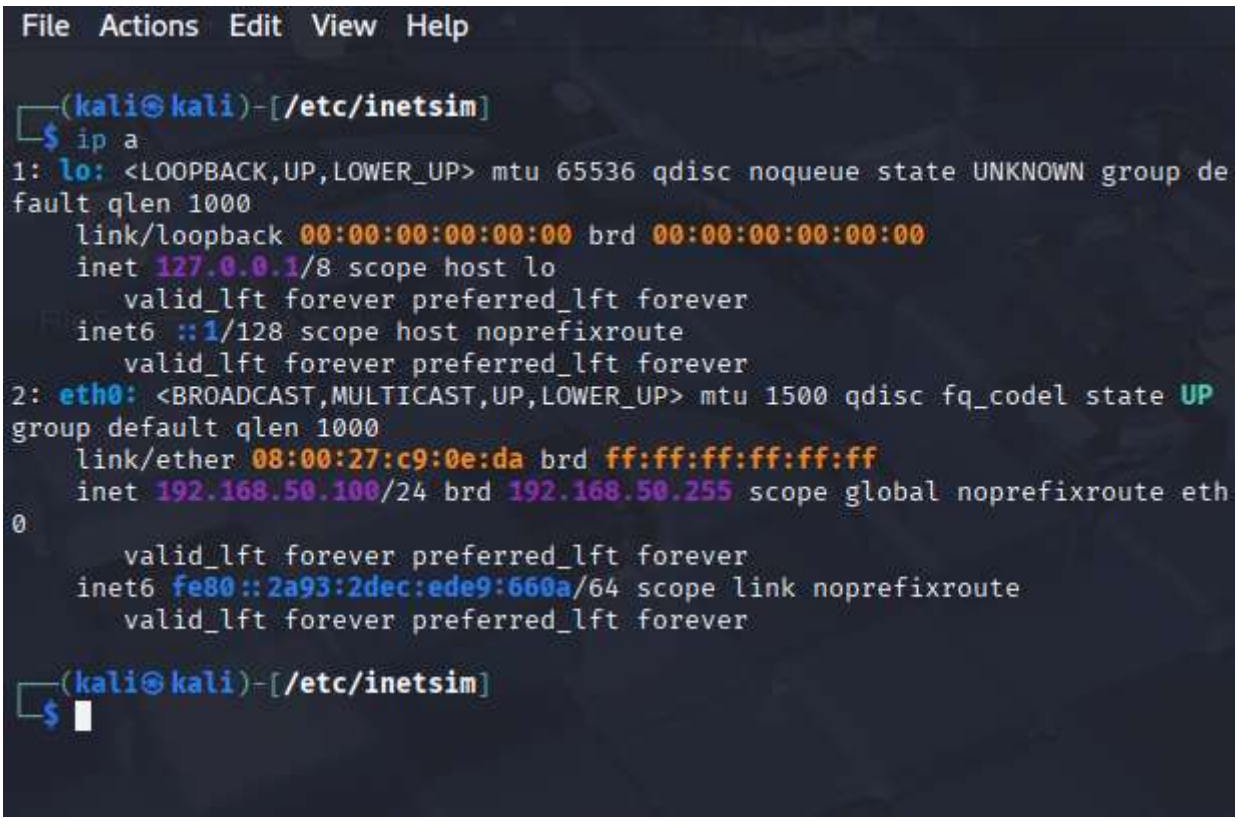
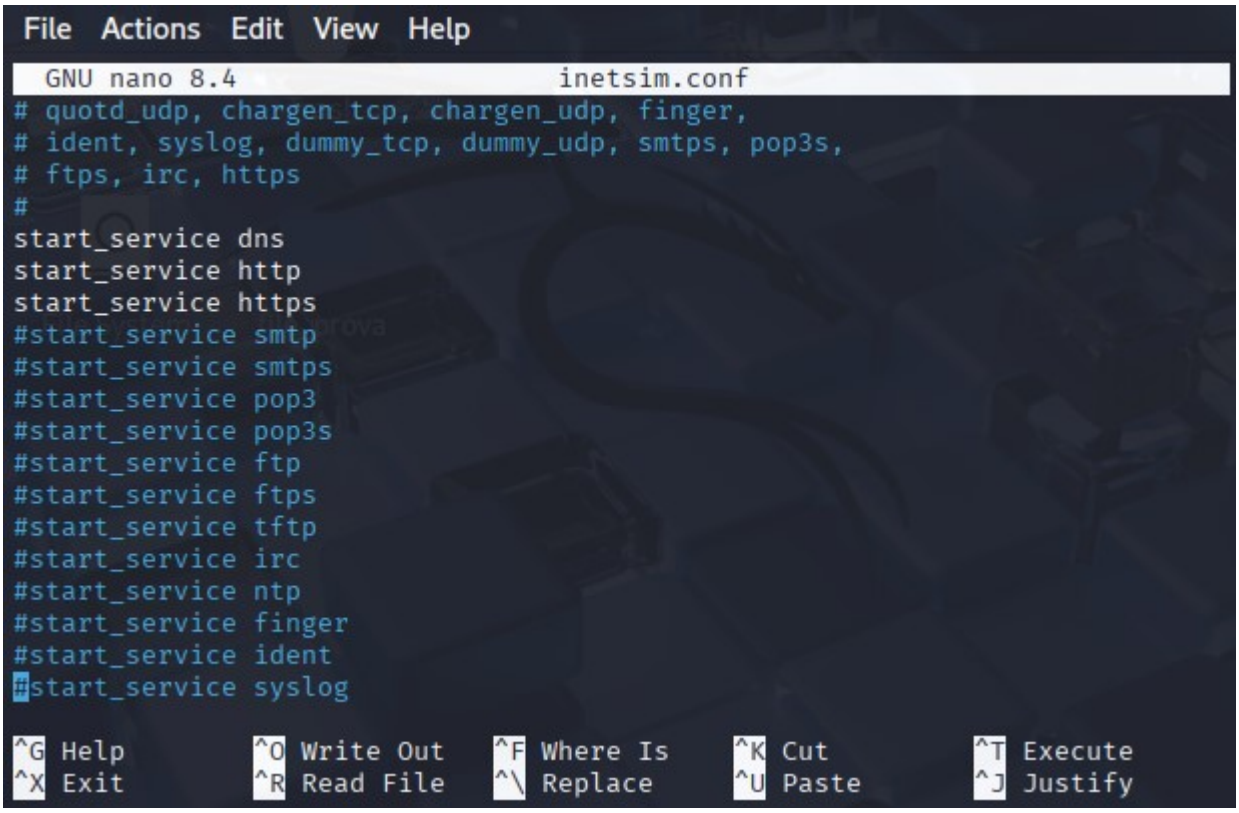
Progetto Finale

Abbiamo predisposto un laboratorio virtuale configurando una macchina Kali Linux con l'indirizzo IP statico 192.168.50.100. Successivamente, abbiamo modificato il file di configurazione inetsim.conf per attivare i servizi HTTP e HTTPS offerti da INetSim.

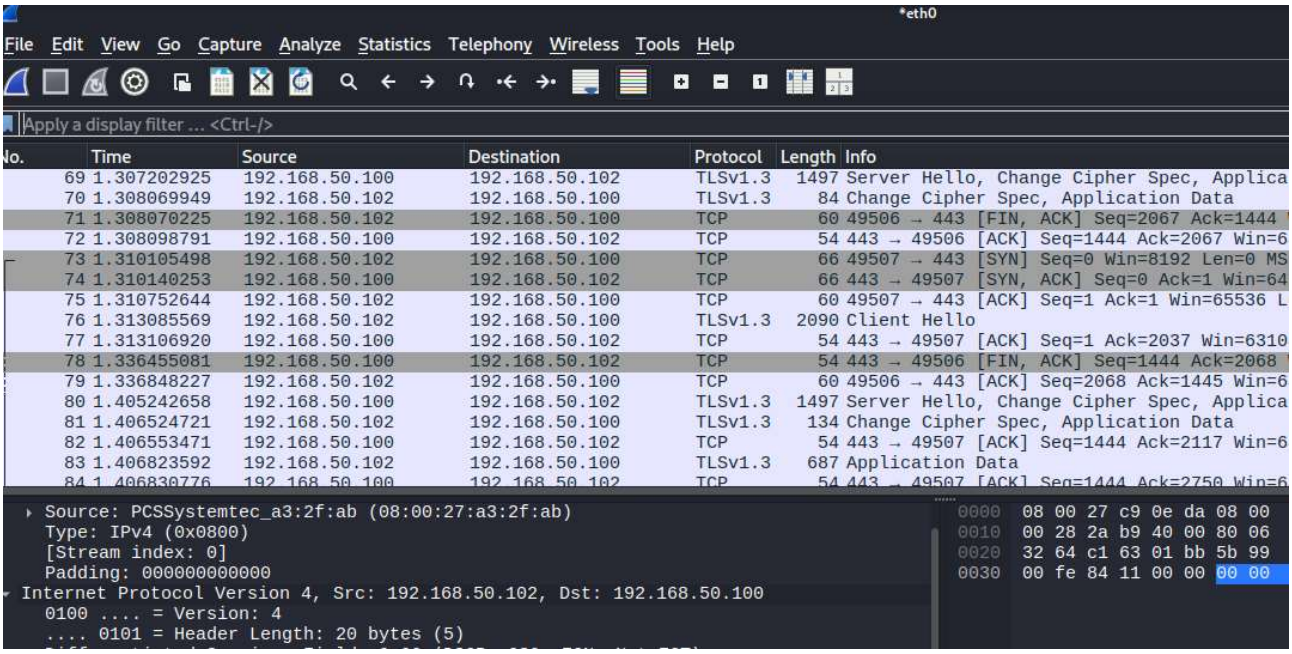


File di configurazione inetsim

File di configurazione inetsim



Con wireshark intercettiamo il traffico dei pacchetti e vedremo le richieste con mac address e anche il contenuto anche se l'https è cifrato quindi il contenuto non si puo vedere.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
69 1.307202925 192.168.50.100 192.168.50.102 TLSv1.3 1497 Server Hello, Change Cipher Spec, Applica
70 1.308069949 192.168.50.102 192.168.50.100 TLSv1.3 84 Change Cipher Spec, Application Data
71 1.308070225 192.168.50.102 192.168.50.100 TCP 60 49506 → 443 [FIN, ACK] Seq=2067 Ack=1444
72 1.308098791 192.168.50.100 192.168.50.102 TCP 54 443 → 49506 [ACK] Seq=1444 Ack=2067 Win=6
73 1.310105498 192.168.50.102 192.168.50.100 TCP 66 49507 → 443 [SYN] Seq=0 Win=8192 Len=0 MS
74 1.310140253 192.168.50.100 192.168.50.102 TCP 66 443 → 49507 [SYN, ACK] Seq=0 Ack=1 Win=64
75 1.310752644 192.168.50.102 192.168.50.100 TCP 60 49507 → 443 [ACK] Seq=1 Ack=1 Win=65536 L
76 1.313085569 192.168.50.102 192.168.50.100 TLSv1.3 2090 Client Hello
77 1.313106920 192.168.50.100 192.168.50.102 TCP 54 443 → 49507 [ACK] Seq=1 Ack=2037 Win=6310
78 1.336455081 192.168.50.100 192.168.50.102 TCP 54 443 → 49506 [FIN, ACK] Seq=1444 Ack=2068
79 1.336848227 192.168.50.102 192.168.50.100 TCP 60 49506 → 443 [ACK] Seq=2068 Ack=1445 Win=6
80 1.405242658 192.168.50.100 192.168.50.102 TLSv1.3 1497 Server Hello, Change Cipher Spec, Applica
81 1.406524721 192.168.50.102 192.168.50.100 TLSv1.3 134 Change Cipher Spec, Application Data
82 1.406553471 192.168.50.100 192.168.50.102 TCP 54 443 → 49507 [ACK] Seq=1444 Ack=2117 Win=6
83 1.406823592 192.168.50.102 192.168.50.100 TLSv1.3 687 Application Data
Source: PCSSystemtec_a3:2f:ab (08:00:27:a3:2f:ab)
Type: IPv4 (0x0800)
[Stream index: 0]
Padding: 000000000000
Internet Protocol Version 4, Src: 192.168.50.102, Dst: 192.168.50.100
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
0000 08 00 27 c9 0e da 08 00
0010 00 28 2a b9 40 00 80 06
0020 32 64 c1 63 01 bb 5b 99
0030 00 fe 84 11 00 00 00 00