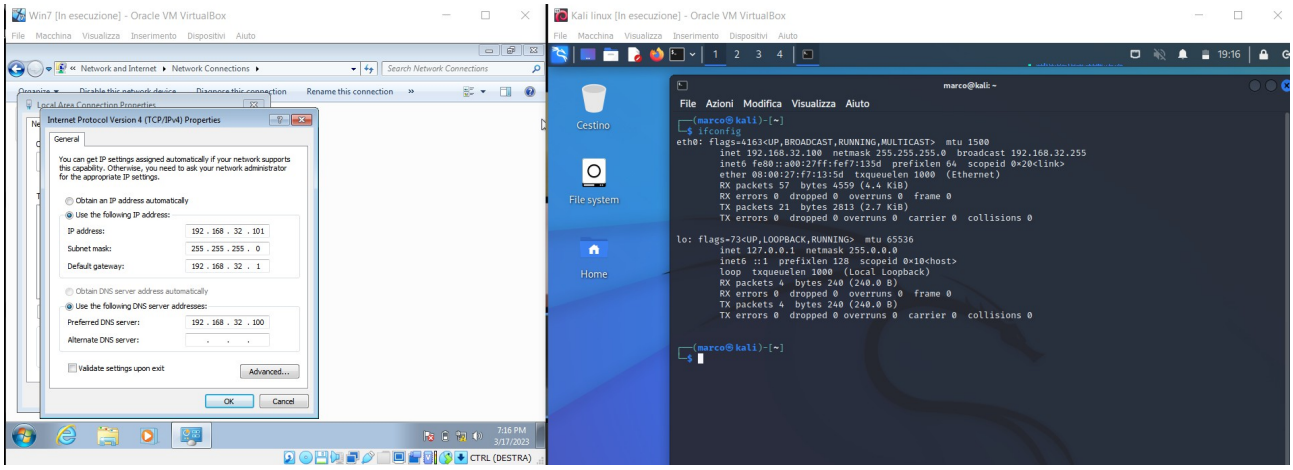
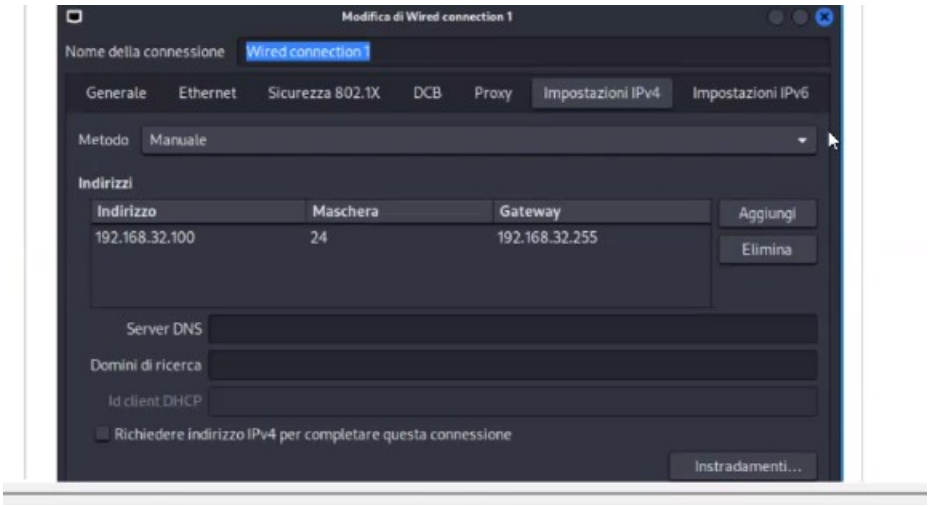
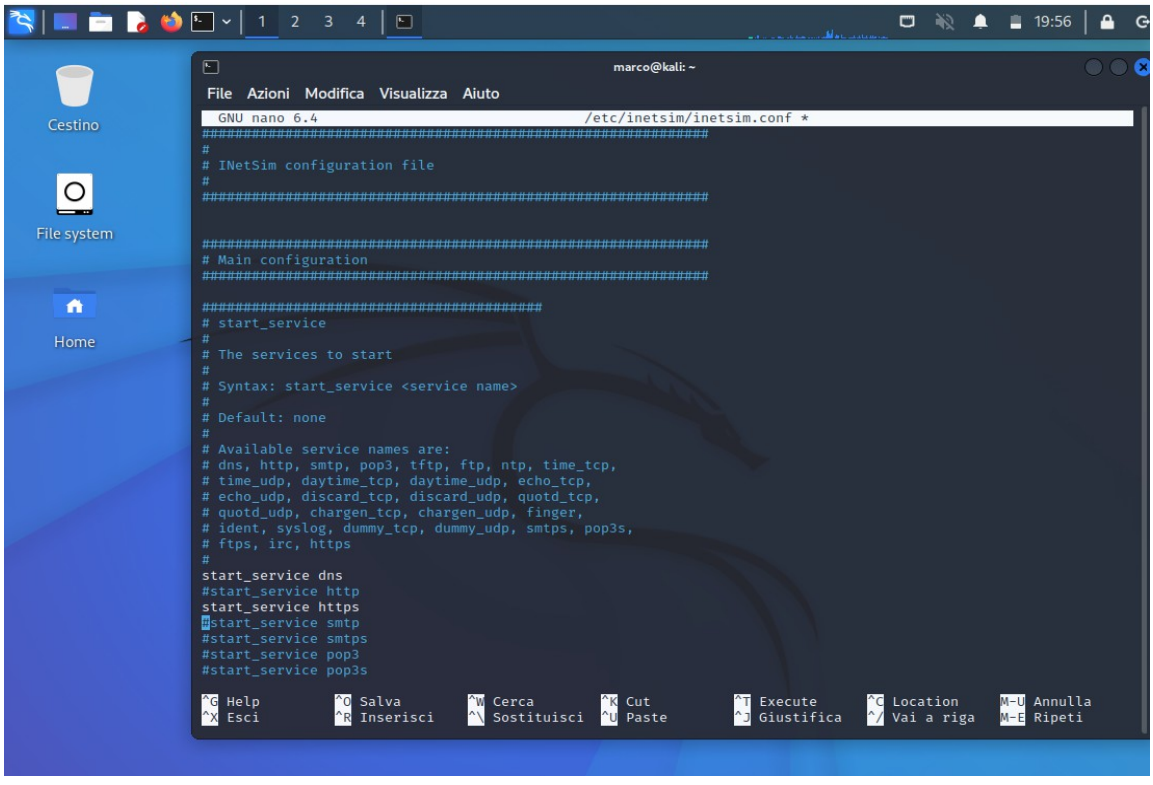
ESERCITAZIONE D8

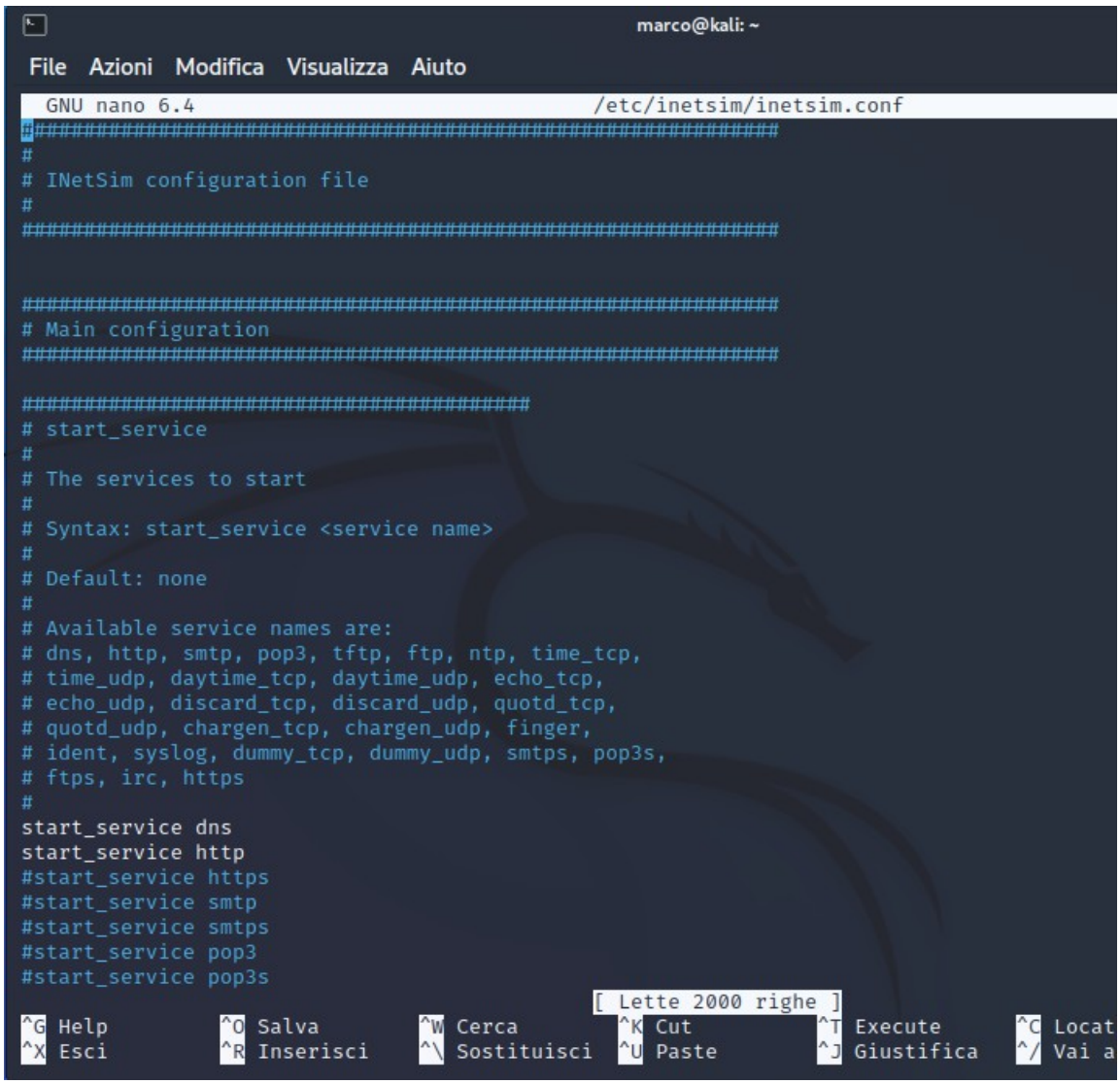
CONFIGURAZIONE IP STATICI DI CLIENT E SERVER



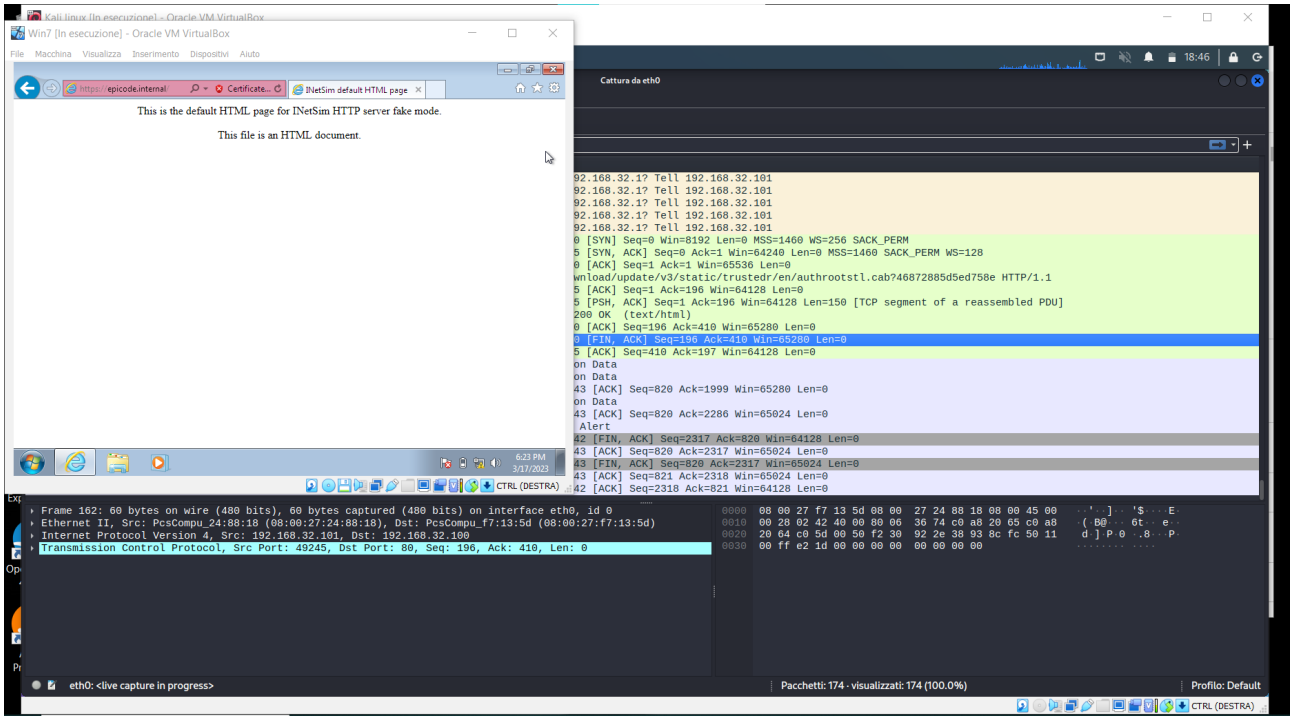


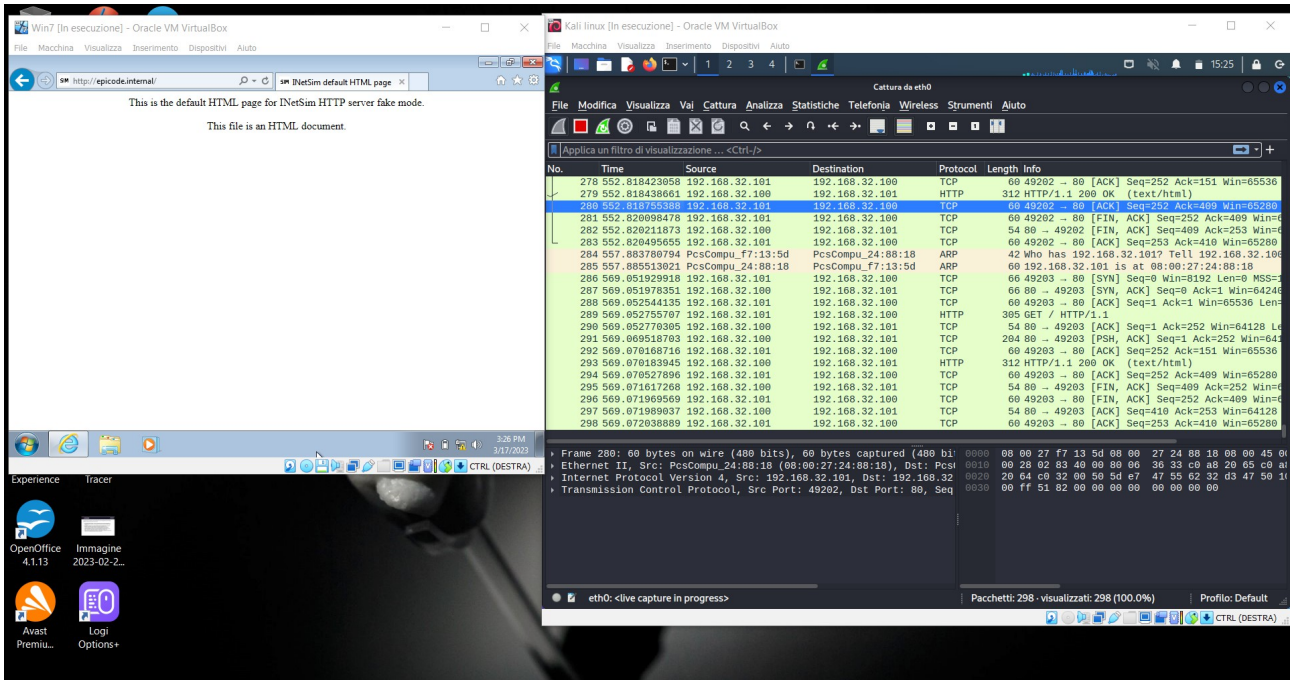
CONFIGURAZIONE SERVIZI DNS E HTTP E HTTPS



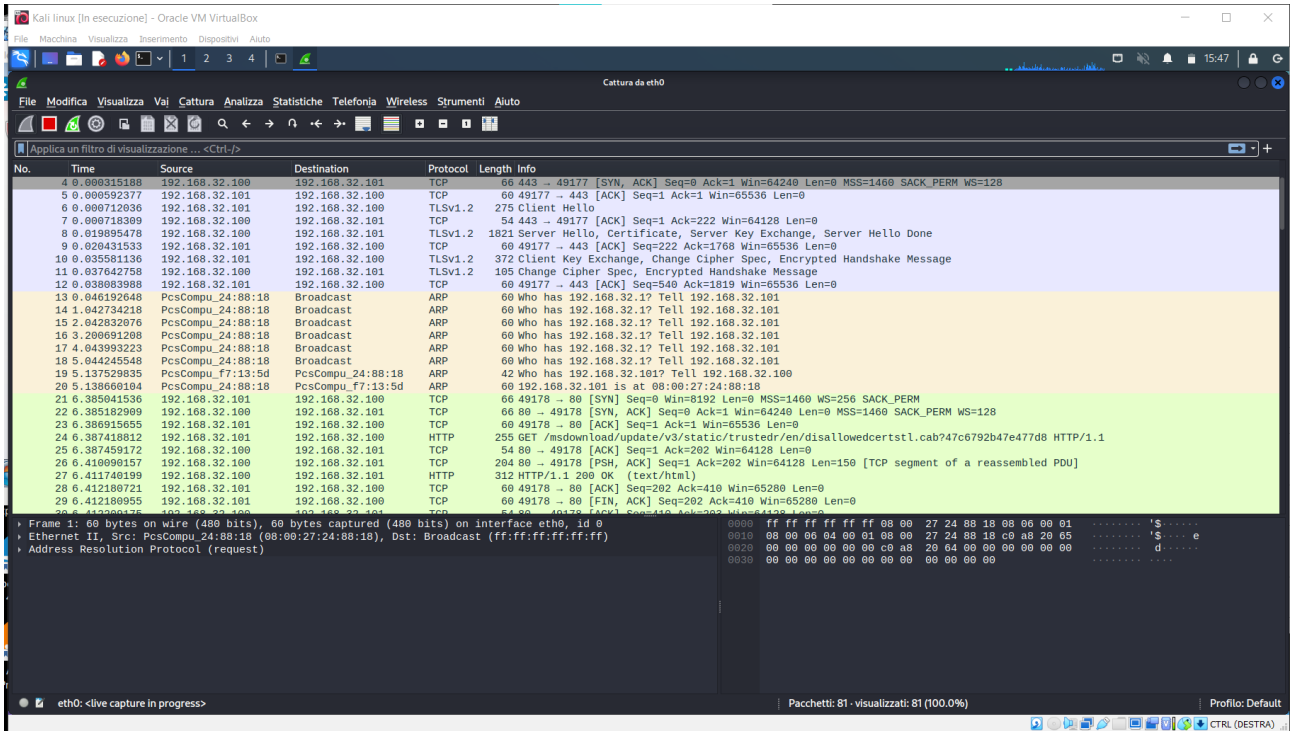


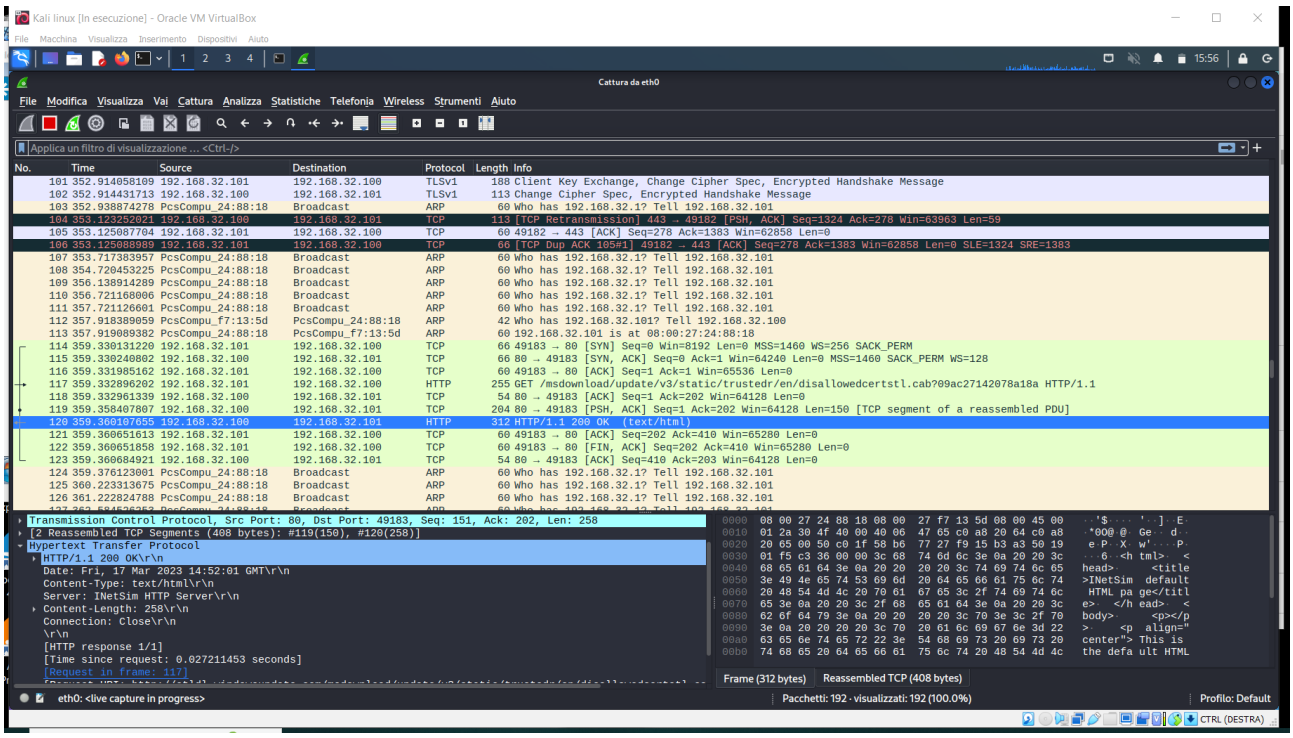
TEST CONNESSIONE WIN KALI



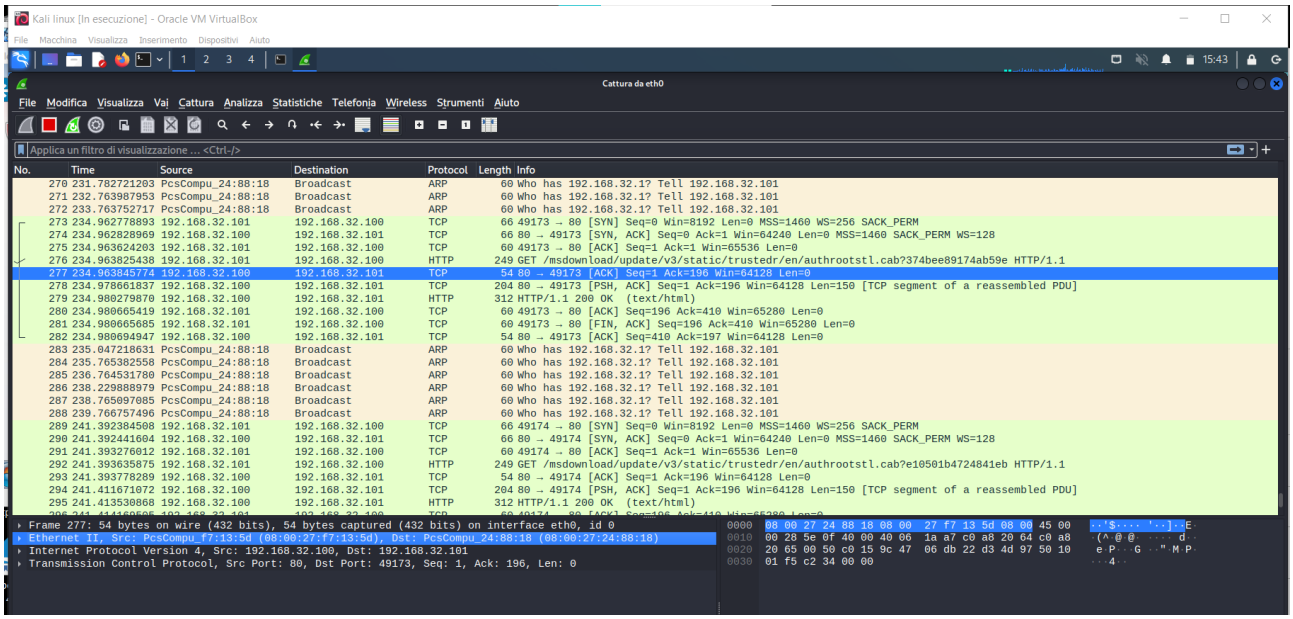


CATTURA WIRESHARK

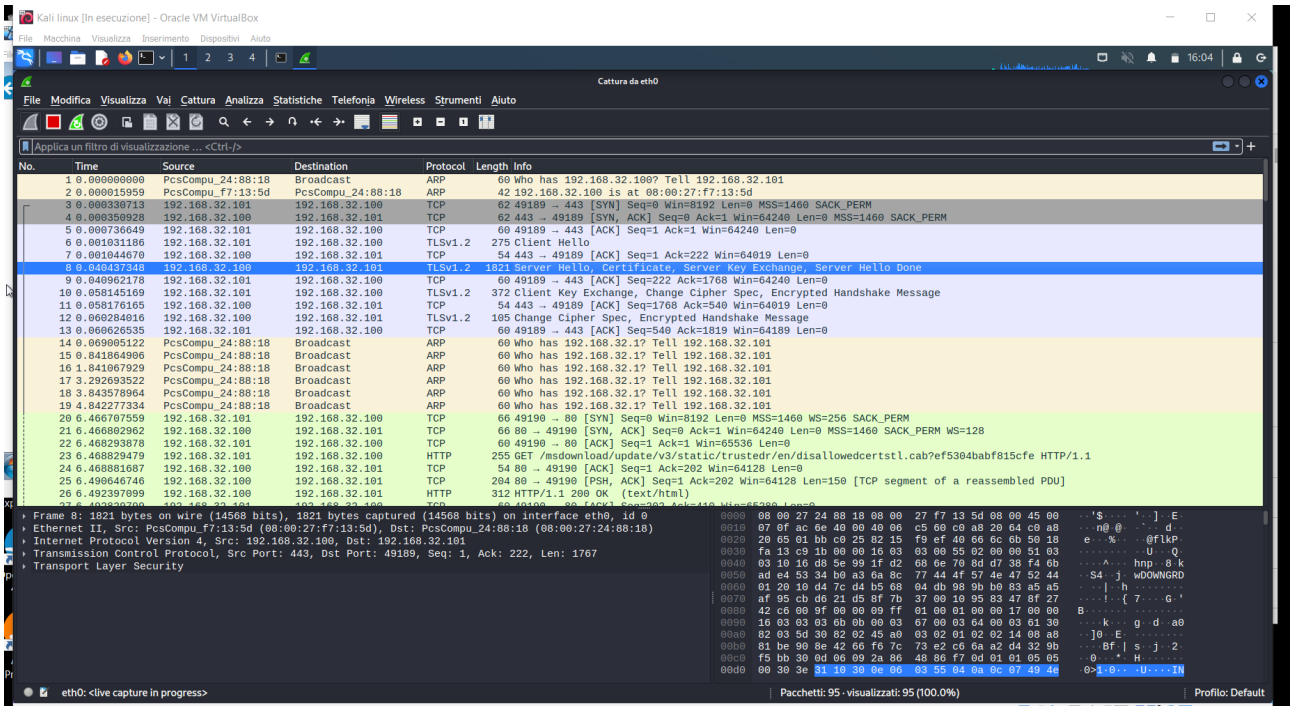


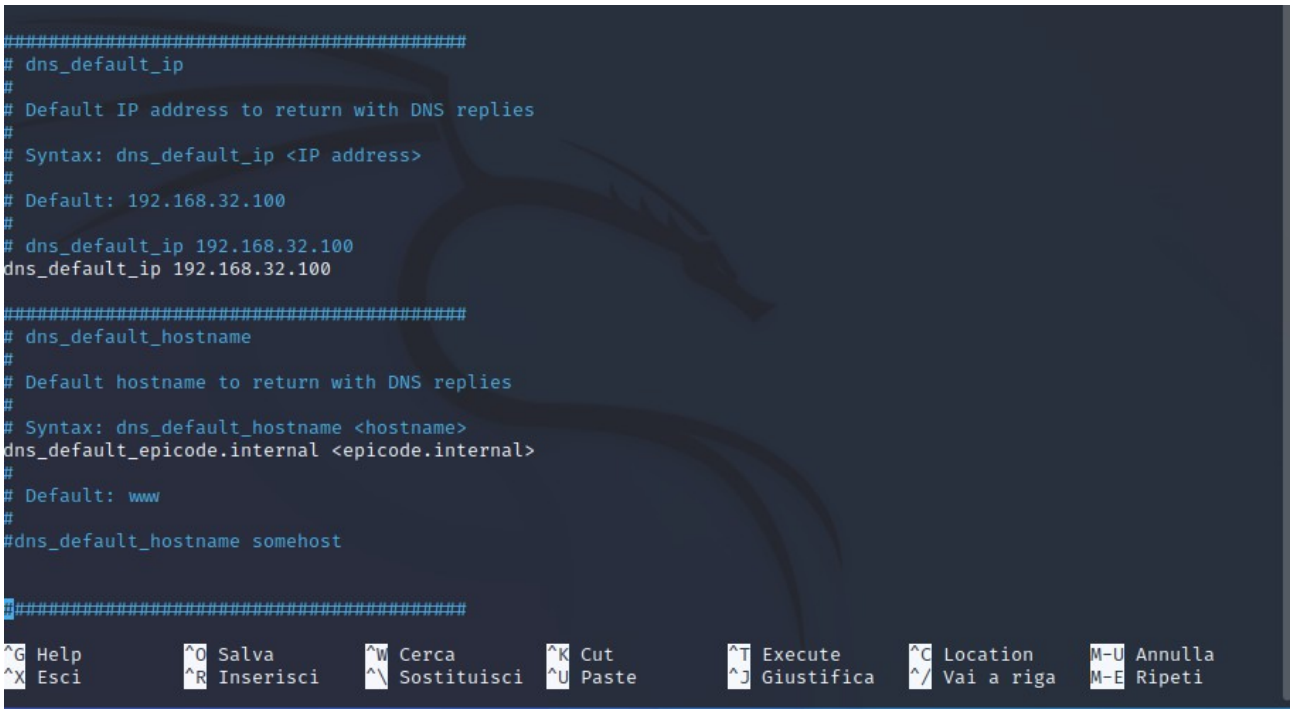

Kali linux [In esecuzione] - Oracle VM VirtualBox
Cattura da eth0
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
101 352.914058109 192.168.32.101 192.168.32.100 TLSv1 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
102 352.914431713 192.168.32.100 192.168.32.101 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
103 352.938874278 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
104 353.123252021 192.168.32.100 192.168.32.101 TCP 113 [TCP Retransmission] 443 → 49182 [PSH, ACK] Seq=1324 Ack=278 Win=63963 Len=59
105 353.125087704 192.168.32.101 192.168.32.100 TCP 60 49182 → 443 [ACK] Seq=278 Ack=1383 Win=62858 Len=0
106 353.125088989 192.168.32.101 192.168.32.100 TCP 66 [TCP Dup ACK 105#1] 49182 → 443 [ACK] Seq=278 Ack=1383 Win=62858 Len=0 SLE=1324 SRE=1383
107 353.717383957 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
108 354.720453225 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
109 356.138914289 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
110 356.721168006 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
111 357.721126601 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
112 357.918389059 PcsCompu_f7:13:5d PcsCompu_24:88:18 ARP 42 Who has 192.168.32.101? Tell 192.168.32.100
113 357.919089382 PcsCompu_24:88:18 PcsCompu_f7:13:5d ARP 60 192.168.32.101 is at 08:00:27:24:88:18
114 359.330131220 192.168.32.101 192.168.32.100 TCP 66 49183 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
115 359.330240802 192.168.32.100 192.168.32.101 TCP 66 80 → 49183 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
116 359.331985162 192.168.32.101 192.168.32.100 TCP 60 49183 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
117 359.332896202 192.168.32.101 192.168.32.100 HTTP 255 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?09ac27142078a18a HTTP/1.1
118 359.332961339 192.168.32.100 192.168.32.101 TCP 54 80 → 49183 [ACK] Seq=1 Ack=202 Win=64128 Len=0
119 359.358407807 192.168.32.100 192.168.32.101 TCP 204 80 → 49183 [PSH, ACK] Seq=1 Ack=202 Win=64128 Len=150 [TCP segment of a reassembled PDU]
120 359.360107655 192.168.32.100 192.168.32.101 HTTP 312 HTTP/1.1 200 OK (text/html)
121 359.360651613 192.168.32.101 192.168.32.100 TCP 60 49183 → 80 [ACK] Seq=202 Ack=410 Win=65280 Len=0
122 359.360651858 192.168.32.101 192.168.32.100 TCP 60 49183 → 80 [FIN, ACK] Seq=202 Ack=410 Win=65280 Len=0
123 359.360684921 192.168.32.100 192.168.32.101 TCP 54 80 → 49183 [ACK] Seq=410 Ack=203 Win=64128 Len=0
124 359.376123001 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
125 360.223313675 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
126 361.222824788 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
Transmission Control Protocol, Src Port: 80, Dst Port: 49183, Seq: 151, Ack: 202, Len: 258
[2 Reassembled TCP Segments (408 bytes): #119(150), #120(258)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Fri, 17 Mar 2023 14:52:01 GMT\r\n
Content-Type: text/html\r\n
Server: INetSim HTTP Server\r\n
Content-Length: 258\r\n
Connection: Close\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.027211453 seconds]
[Request in frame: 117]
0000 08 00 27 24 88 18 08 00 27 f7 13 5d 08 00 45 00
0010 01 2a 30 4f 40 00 40 06 47 65 c0 a8 20 64 c0 a8
0020 20 65 00 50 c0 1f 58 b6 77 27 f9 15 b3 a3 50 19
0030 01 f5 c3 36 00 00 3c 68 74 6d 6c 3e 0a 20 20 3c
0040 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65
0050 3e 49 4e 65 74 53 69 6d 20 64 65 66 61 75 6c 74
0060 20 48 54 4d 4c 20 70 61 67 65 3c 2f 74 69 74 6c
0070 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c
0080 62 6f 64 79 3e 0a 20 20 20 20 3c 70 3e 3c 2f 70
0090 3e 0a 20 20 20 20 3c 70 20 61 6c 69 67 6e 3d 22
00a0 63 65 6e 74 65 72 22 3e 54 68 69 73 20 69 73 20
00b0 74 68 65 20 64 65 66 61 75 6c 74 20 48 54 4d 4c
Frame (312 bytes)
Reassembled TCP (408 bytes)
eth0: <live capture in progress>
Pacchetti: 192 · visualizzati: 192 (100.0%)
Profilo: Default
CTRL (DESTRA)

MAC ADDRESS


Kali linux [In esecuzione] - Oracle VM VirtualBox
Cattura da eth0
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
270 231.782721203 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
271 232.763987953 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
272 233.763752717 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
273 234.962778893 192.168.32.101 192.168.32.100 TCP 66 49173 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
274 234.962828969 192.168.32.100 192.168.32.101 TCP 66 80 → 49173 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
275 234.963624203 192.168.32.101 192.168.32.100 TCP 60 49173 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
276 234.963825438 192.168.32.101 192.168.32.100 HTTP 249 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?374bee89174ab59e HTTP/1.1
277 234.963845774 192.168.32.100 192.168.32.101 TCP 54 80 → 49173 [ACK] Seq=1 Ack=196 Win=64128 Len=0
278 234.978661837 192.168.32.100 192.168.32.101 TCP 204 80 → 49173 [PSH, ACK] Seq=1 Ack=196 Win=64128 Len=150 [TCP segment of a reassembled PDU]
279 234.980279870 192.168.32.100 192.168.32.101 HTTP 312 HTTP/1.1 200 OK (text/html)
280 234.980665419 192.168.32.101 192.168.32.100 TCP 60 49173 → 80 [ACK] Seq=196 Ack=410 Win=65280 Len=0
281 234.980665685 192.168.32.101 192.168.32.100 TCP 60 49173 → 80 [FIN, ACK] Seq=196 Ack=410 Win=65280 Len=0
282 234.980694947 192.168.32.100 192.168.32.101 TCP 54 80 → 49173 [ACK] Seq=410 Ack=197 Win=64128 Len=0
283 235.047218631 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
284 235.765382558 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
285 236.764531780 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
286 238.229888979 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
287 238.765097085 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
288 239.766757496 PcsCompu_24:88:18 Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
289 241.392384508 192.168.32.101 192.168.32.100 TCP 66 49174 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
290 241.392441604 192.168.32.100 192.168.32.101 TCP 66 80 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
291 241.393276012 192.168.32.101 192.168.32.100 TCP 60 49174 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
292 241.393635875 192.168.32.101 192.168.32.100 HTTP 249 GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?e10501b4724841eb HTTP/1.1
293 241.393778289 192.168.32.100 192.168.32.101 TCP 54 80 → 49174 [ACK] Seq=1 Ack=196 Win=64128 Len=0
294 241.411671072 192.168.32.100 192.168.32.101 TCP 204 80 → 49174 [PSH, ACK] Seq=1 Ack=196 Win=64128 Len=150 [TCP segment of a reassembled PDU]
295 241.413530868 192.168.32.100 192.168.32.101 HTTP 312 HTTP/1.1 200 OK (text/html)
Frame 277: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_f7:13:5d (08:00:27:f7:13:5d), Dst: PcsCompu_24:88:18 (08:00:27:24:88:18)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101
Transmission Control Protocol, Src Port: 80, Dst Port: 49173, Seq: 1, Ack: 196, Len: 0
0000 08 00 27 24 88 18 08 00 27 f7 13 5d 08 00 45 00
0010 00 28 5e 0f 40 00 40 06 1a a7 c0 a8 20 64 c0 a8
0020 20 65 00 50 c0 15 9c 47 06 db 22 d3 4d 97 50 10
0030 01 f5 c2 34 00 00

TLS – HTTPS PROTOCOLLO CIFRATURA





Dopo aver simulato la richiesta da Win 7 in http e https si notano delle differenze, sniffando con wireshark il traffico:

- con https, dopo il three way handshake a buon fine si attiva il protocollo TLS (come da foto) Transport Layer Security che serve a proteggere il trasferimento di dati e informazioni, criptandolo in invioe decriptandolo giunto a destinazione. La comunicazione avviene tramite la porta 443. Accedendo da windows con https si registra un errore di certificato.

- con http una volta effettuato il three way handshake si passa direttamente al trasferimento di dati senza nessuna protezione, in chiaro. La comunicazione avviene tramite la porta 80. Nessun errore di certificato.

Gli indirizzi MAC si vedono in una foto specifica denominata MAC ADDRESS sottolineata in blu.