Progetto

Requisiti e servizi:

- **Kali Linux IP: 192.168.32.100**
- **Windows 7 IP: 192.168.32.101**
- **HTTPS server: attivo**
- **Server DNS per risoluzione nomi di dominio: attivo**

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.

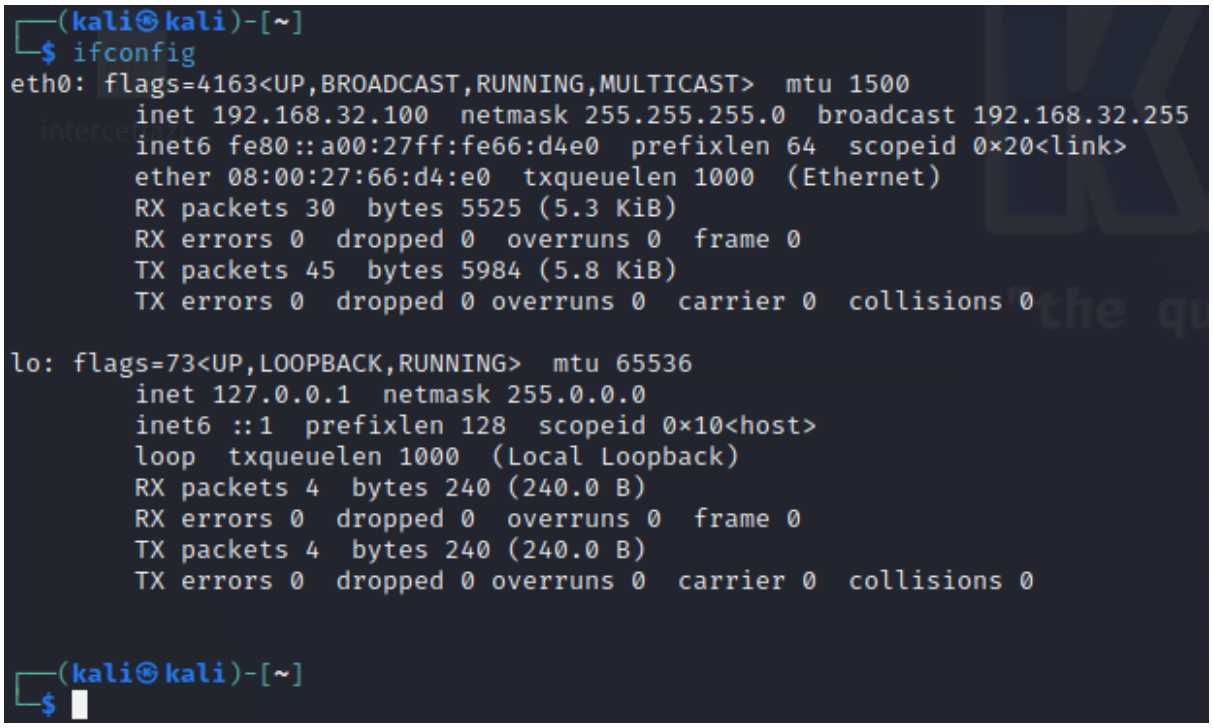
Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedentemente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

Svolgimento:

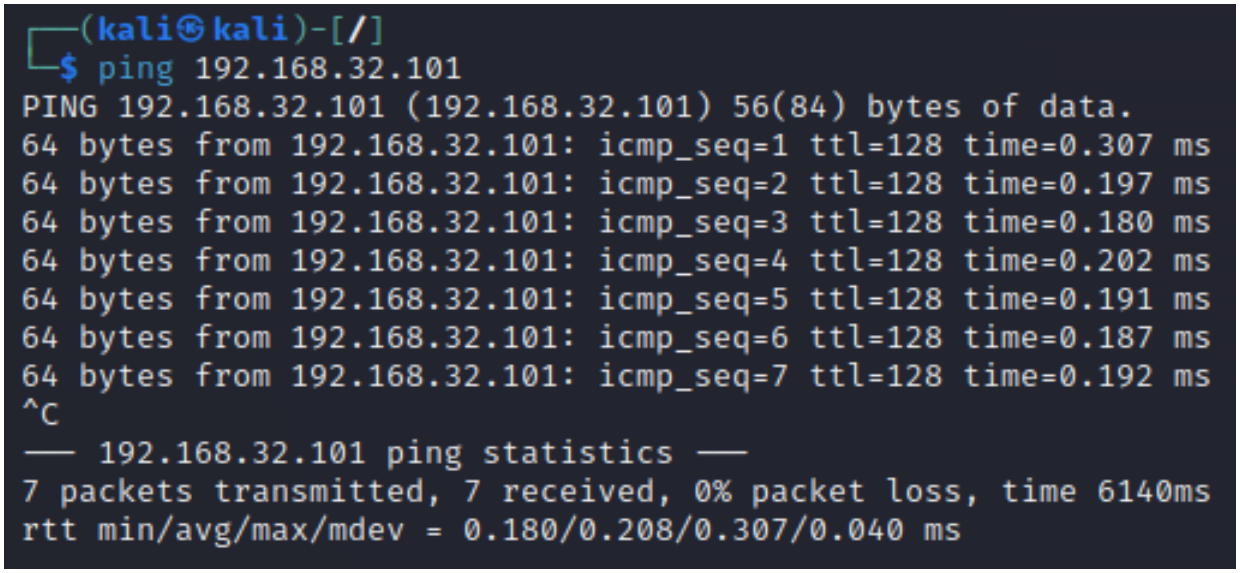
Windows 7:

```
C:\Users\Valerio>ipconfig /all

Configurazione IP di Windows

   Nome host . . . . . . . . . . . . : Valerio-PC
   Suffisso DNS primario . . . . . . :
   Tipo nodo . . . . . . . . . . . . : Ibrido
   Routing IP abilitato. . . . . . . : No
   Proxy WINS abilitato . . . . . . .  : No

Scheda Ethernet Connessione alla rete locale (LAN):

   Suffisso DNS specifico per connessione:
   Descrizione . . . . . . . . . . . : Scheda desktop Intel(R) PRO/1000 MT
   Indirizzo fisico. . . . . . . . . : 08-00-27-3A-A8-FE
   DHCP abilitato. . . . . . . . . . : No
   Configurazione automatica abilitata   : Sì
   Indirizzo IPv4. . . . . . . . . . : 192.168.32.101(Preferenziale)
   Subnet mask . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . : 192.168.32.1
   Server DNS . . . . . . . . . . . .  : 192.168.32.100
   NetBIOS su TCP/IP . . . . . . . . : Attivato
```

Kali:



Ping da Kali a Windows 7:



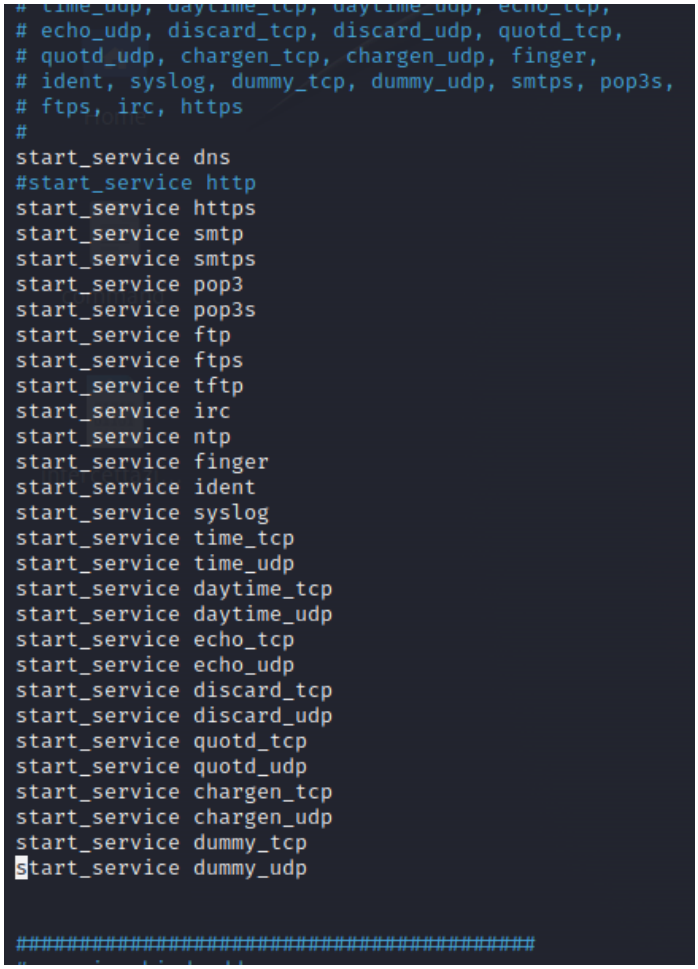
Ping da Windows 7 a Kali:

```
C:\Users\Valerio>ping 192.168.32.100

Esecuzione di Ping 192.168.32.100 con 32 byte di dati:
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.32.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.32.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo =  0ms, Medio =  0ms

C:\Users\Valerio>
```

Nel file di configurazione di InetSim aggiungere l'hostname:

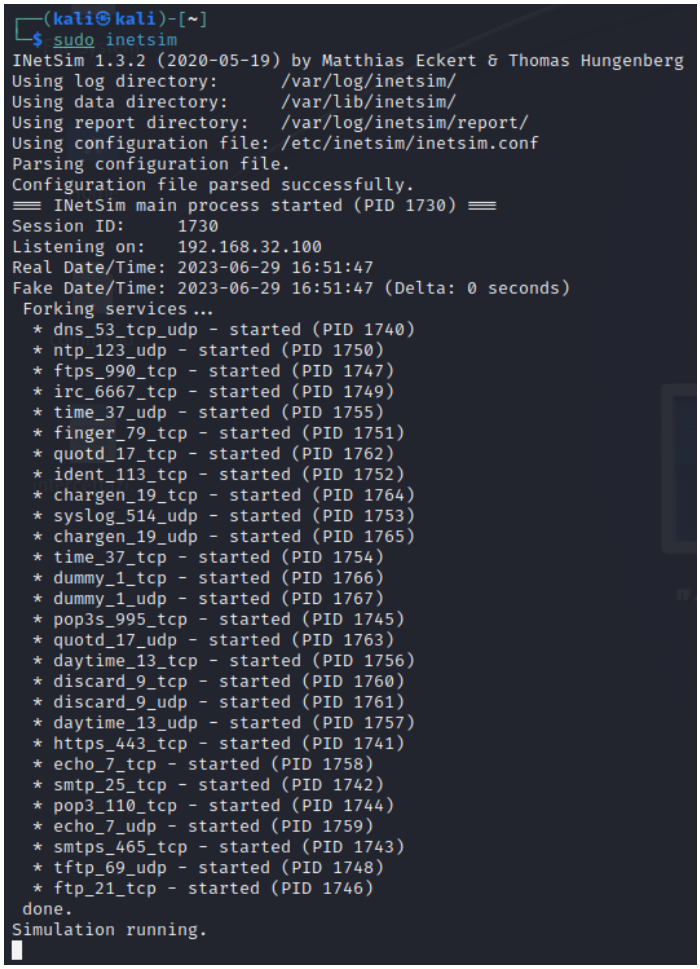
```
################################################
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
#dns_static www.foo.com 10.10.10.10
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
dns_static epicode.internal 192.168.32.100


################################################
```

Nel file di configurazione di InetSim lasciare attivi i servizi DNS e HTTPS disattivando i servizi HTTP:

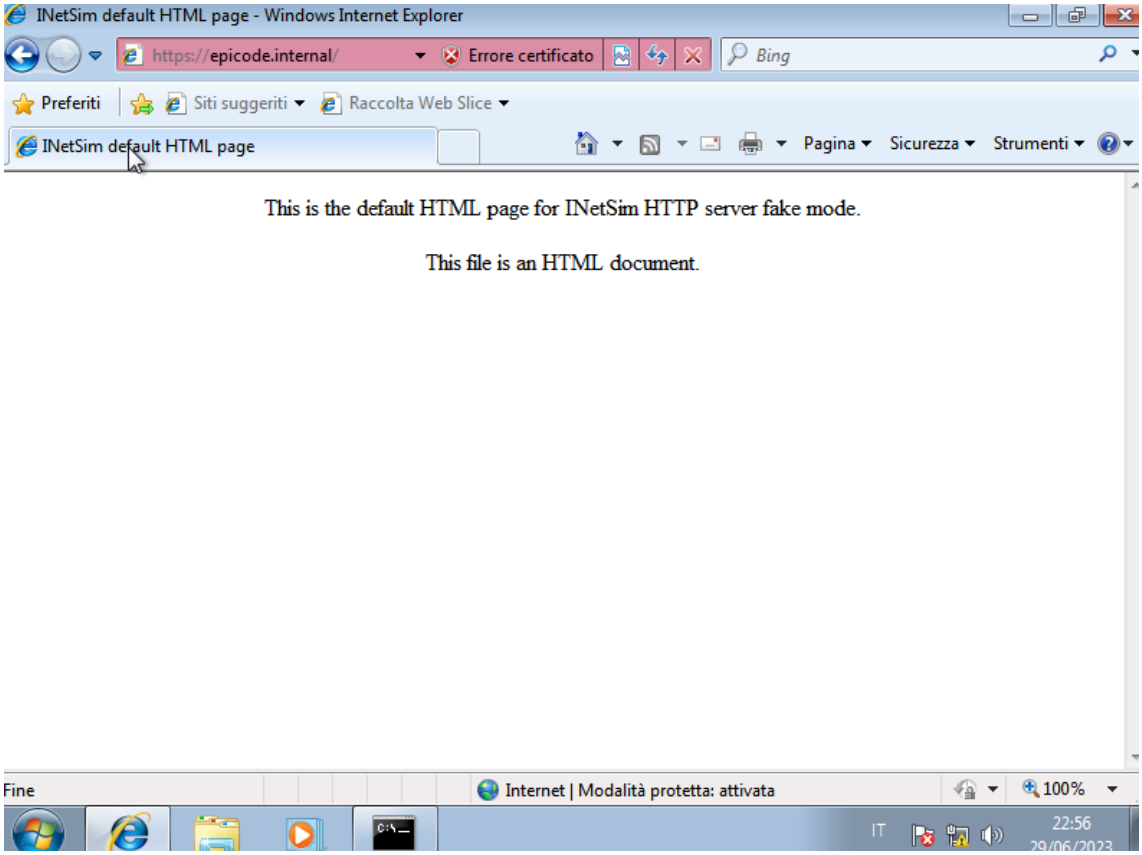


```
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
#start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
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


##########################################
```

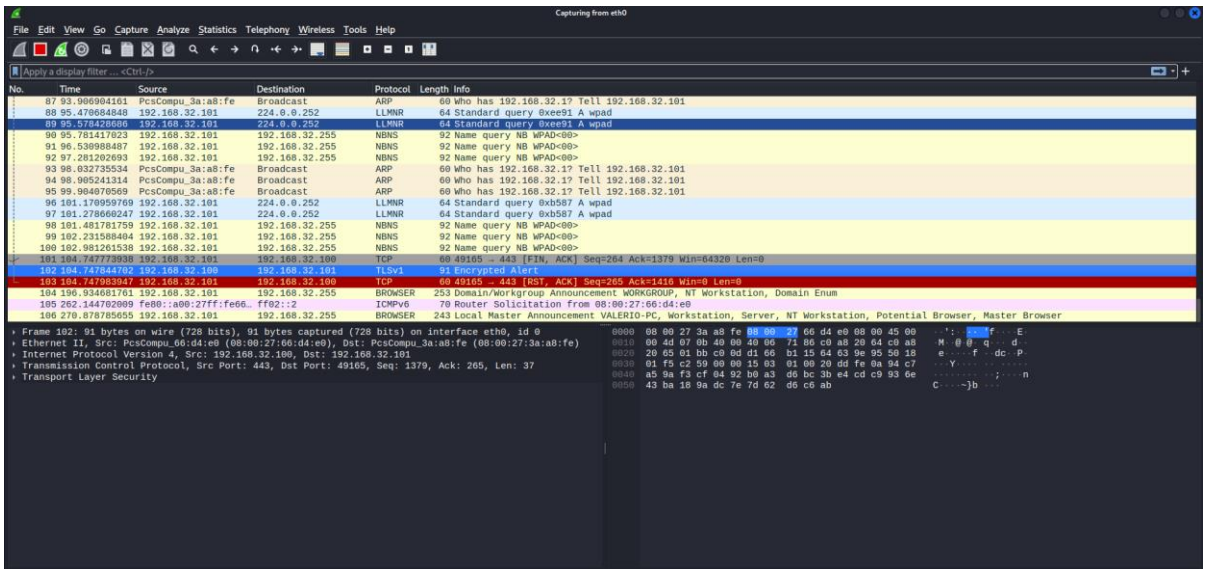
Lanciare InetSim:

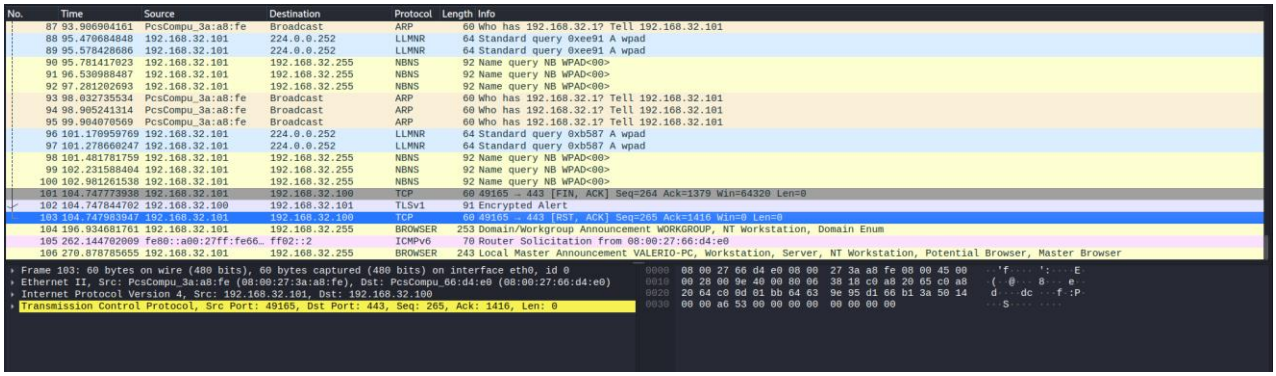


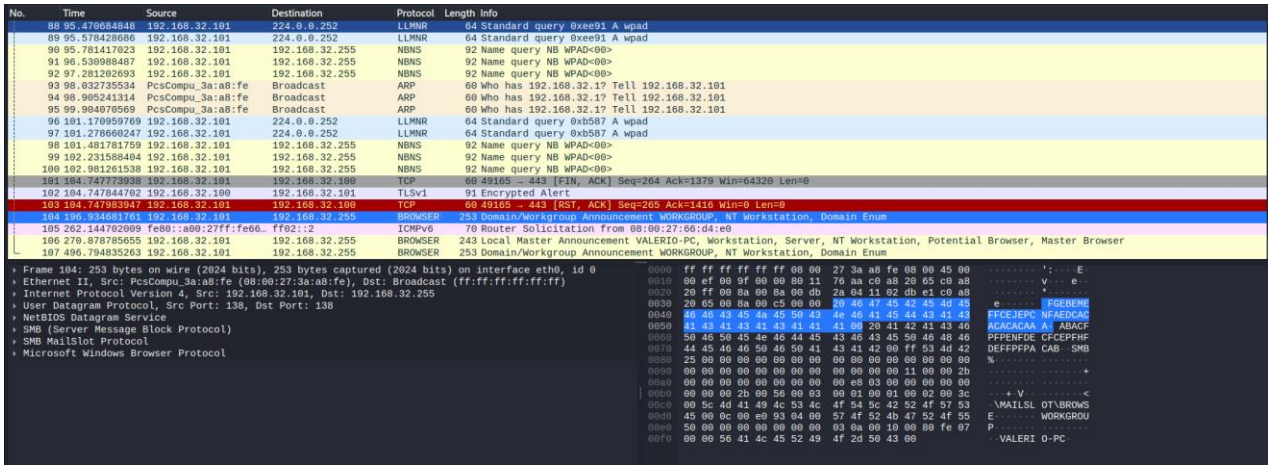
Richiesta web browser “epicode.internal”:



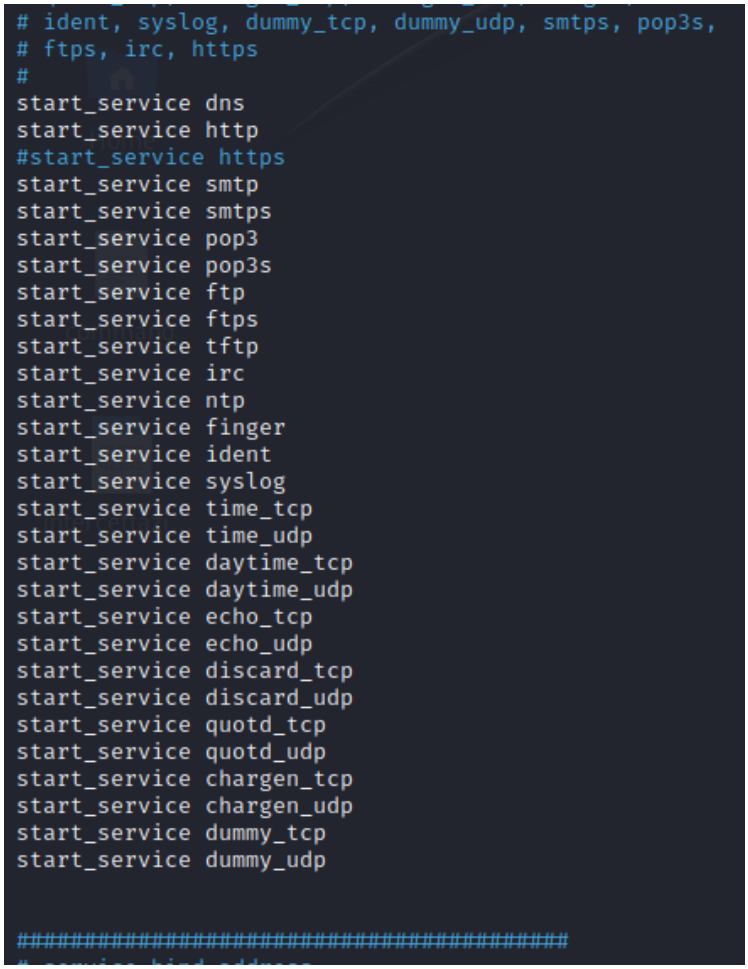
Cattura tramite wireshark dei pacchetti criptati:




No. Time Source Destination Protocol Length Info
87 93.906904161 PcsCompu_3a:a8:fe Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
88 95.470684848 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xee91 A wpad
89 95.578428686 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xee91 A wpad
90 95.781417023 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
91 96.530988487 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
92 97.281202693 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
93 98.032735534 PcsCompu_3a:a8:fe Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
94 98.905241314 PcsCompu_3a:a8:fe Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
95 99.904070569 PcsCompu_3a:a8:fe Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
96 101.170959769 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xb587 A wpad
97 101.278660247 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xb587 A wpad
98 101.481781759 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
99 102.231588404 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
100 102.981261538 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
101 104.747773938 192.168.32.101 192.168.32.100 TCP 60 49165 → 443 [FIN, ACK] Seq=264 Ack=1379 Win=64320 Len=0
102 104.747844702 192.168.32.100 192.168.32.101 TLSv1 91 Encrypted Alert
103 104.747983947 192.168.32.101 192.168.32.100 TCP 60 49165 → 443 [RST, ACK] Seq=265 Ack=1416 Win=0 Len=0
104 196.934681761 192.168.32.101 192.168.32.255 BROWSER 253 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
105 262.144702009 fe80::a00:27ff:fe66… ff02::2 ICMPv6 70 Router Solicitation from 08:00:27:66:d4:e0
106 270.878785655 192.168.32.101 192.168.32.255 BROWSER 243 Local Master Announcement VALERIO-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser
Frame 103: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_3a:a8:fe (08:00:27:3a:a8:fe), Dst: PcsCompu_66:d4:e0 (08:00:27:66:d4:e0)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49165, Dst Port: 443, Seq: 265, Ack: 1416, Len: 0
0000 08 00 27 66 d4 e0 08 00 27 3a a8 fe 08 00 45 00
0010 00 28 00 9e 40 00 80 06 38 18 c0 a8 20 65 c0 a8
0020 20 64 c0 0d 01 bb 64 63 9e 95 d1 66 b1 3a 50 14
0030 00 00 a6 53 00 00 00 00 00 00 00 00


No. Time Source Destination Protocol Length Info
88 95.470684848 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xee91 A wpad
89 95.578428686 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xee91 A wpad
90 95.781417023 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
91 96.530988487 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
92 97.281202693 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
93 98.032735534 PcsCompu_3a:a8:fe Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
94 98.905241314 PcsCompu_3a:a8:fe Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
95 99.904070569 PcsCompu_3a:a8:fe Broadcast ARP 60 Who has 192.168.32.1? Tell 192.168.32.101
96 101.170959769 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xb587 A wpad
97 101.278660247 192.168.32.101 224.0.0.252 LLMNR 64 Standard query 0xb587 A wpad
98 101.481781759 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
99 102.231588404 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
100 102.981261538 192.168.32.101 192.168.32.255 NBNS 92 Name query NB WPAD<00>
101 104.747773938 192.168.32.101 192.168.32.100 TCP 60 49165 → 443 [FIN, ACK] Seq=264 Ack=1379 Win=64320 Len=0
102 104.747844702 192.168.32.100 192.168.32.101 TLSv1 91 Encrypted Alert
103 104.747983947 192.168.32.101 192.168.32.100 TCP 60 49165 → 443 [RST, ACK] Seq=265 Ack=1416 Win=0 Len=0
104 196.934681761 192.168.32.101 192.168.32.255 BROWSER 253 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
105 262.144702009 fe80::a00:27ff:fe66… ff02::2 ICMPv6 70 Router Solicitation from 08:00:27:66:d4:e0
106 270.878785655 192.168.32.101 192.168.32.255 BROWSER 243 Local Master Announcement VALERIO-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser
107 496.794835263 192.168.32.101 192.168.32.255 BROWSER 253 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
Frame 104: 253 bytes on wire (2024 bits), 253 bytes captured (2024 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_3a:a8:fe (08:00:27:3a:a8:fe), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 08 00 27 3a a8 fe 08 00 45 00
0010 00 ef 00 9f 00 00 80 11 76 aa c0 a8 20 65 c0 a8
0020 20 ff 00 8a 00 8a 00 db 2a 04 11 02 db e1 c0 a8
0030 20 65 00 8a 00 c5 00 00 20 46 47 45 42 45 4d 45
0040 46 46 43 45 4a 45 59 43 4e 46 41 45 44 43 41 43
0050 41 43 41 43 41 43 41 41 41 00 20 41 42 41 43 46
0060 50 46 50 45 4e 46 44 45 43 46 43 45 50 46 48 46
0070 44 45 46 46 50 46 50 41 43 41 42 00 ff 53 4d 42
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 00 11 00 00 2b
00a0 00 00 00 00 00 00 00 00 00 e8 03 00 00 00 00 00
00b0 00 00 00 2b 00 56 00 03 00 01 00 01 00 02 00 3c
00c0 00 5c 4d 41 49 4c 53 4c 4f 54 5c 42 52 4f 57 53
00d0 45 00 0c 00 e0 93 04 00 57 4f 52 4b 47 52 4f 55
00e0 50 00 00 00 00 00 00 00 03 0a 00 10 00 00 fe 07
00f0 00 00 56 41 4c 45 52 49 4f 2d 50 43 00

Nel file di configurazione di InetSim lasciare attivi i servizi DNS e HTTP disattivando i servizi HTTPS:

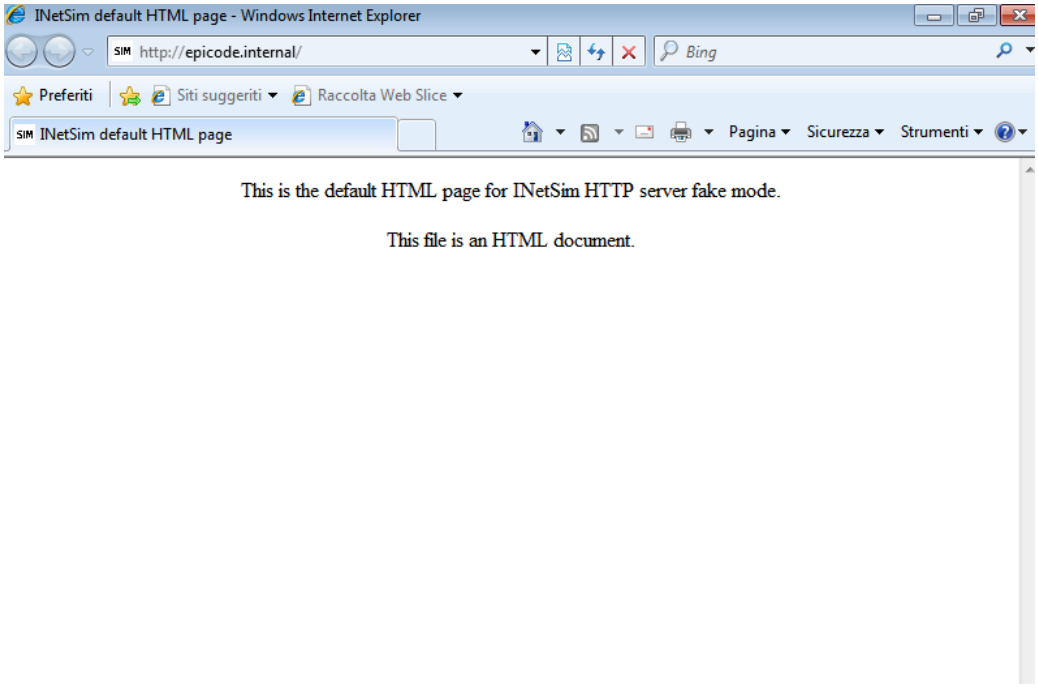


```
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
#start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
start_service tftp
start_service irc
start_service 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


##########################################
```

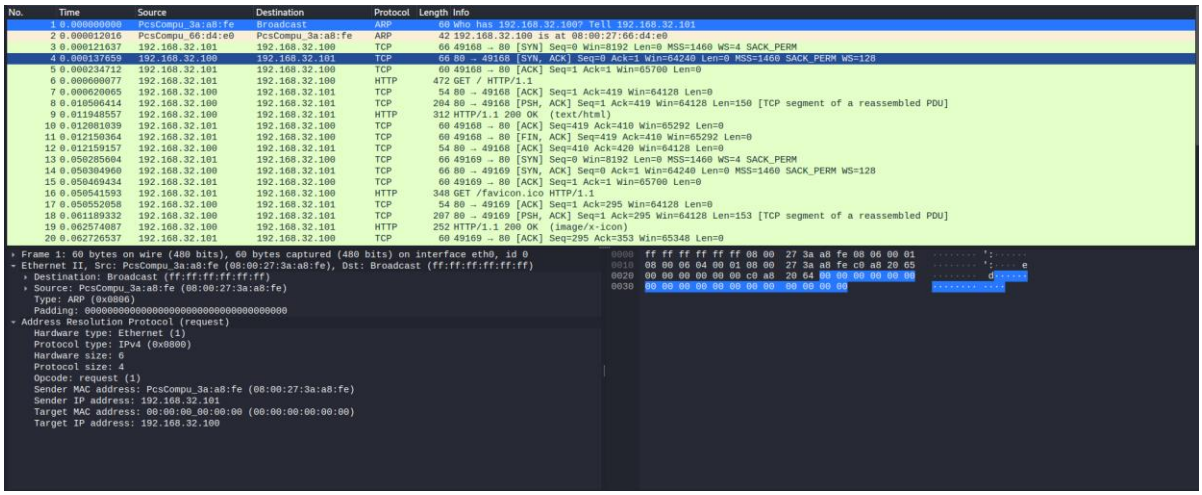
Lanciare InetSim:

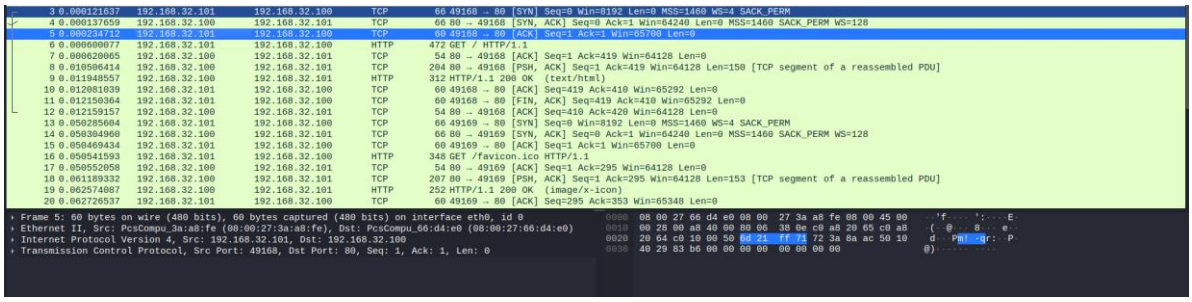
```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 9588) ===
Session ID:     9588
Listening on:   192.168.32.100
Real Date/Time: 2023-06-29 17:07:45
Fake Date/Time: 2023-06-29 17:07:45 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 9590)
  * irc_6667_tcp - started (PID 9599)
  * chargen_19_tcp - started (PID 9614)
  * finger_79_tcp - started (PID 9601)
  * quotd_17_udp - started (PID 9613)
  * dummy_1_udp - started (PID 9617)
  * echo_7_udp - started (PID 9609)
  * pop3s_995_tcp - started (PID 9595)
  * syslog_514_udp - started (PID 9603)
  * discard_9_udp - started (PID 9611)
  * quotd_17_tcp - started (PID 9612)
  * discard_9_tcp - started (PID 9610)
  * ntp_123_udp - started (PID 9600)
  * chargen_19_udp - started (PID 9615)
  * time_37_tcp - started (PID 9604)
  * http_80_tcp - started (PID 9591)
  * daytime_13_tcp - started (PID 9606)
  * ident_113_tcp - started (PID 9602)
  * smtp_25_tcp - started (PID 9592)
  * time_37_udp - started (PID 9605)
  * daytime_13_udp - started (PID 9607)
  * echo_7_tcp - started (PID 9608)
  * tftp_69_udp - started (PID 9598)
  * dummy_1_tcp - started (PID 9616)
  * smtps_465_tcp - started (PID 9593)
  * ftp_21_tcp - started (PID 9596)
  * ftps_990_tcp - started (PID 9597)
  * pop3_110_tcp - started (PID 9594)
 done.
Simulation running.
```

Richiesta web browser “epicode.internal”:



Cattura tramite wireshark dei pacchetti non criptati:





Conclusioni

La prima differenza che notiamo è che la connessione HTTP comunica sulla porta 80 mentre la connessione HTTPS comunica sulla porta 443 questo perché le informazioni che viaggiano su questa porta sono crittografate attraverso la tecnologia SSL/TLS. Come possiamo notare infatti la connessione HTTPS è protetta e le informazioni sono mantenute al sicuro durante il loro transito. Uno dei pacchetti intercettati infatti ha come info "Encrypted Alert". Per quanto riguarda invece la connessione HTTP è messa completamente in chiaro e compaiono all'interno dei pacchetti intercettati tutte le info come l'IP sorgente, l'IP di destinazione, il MAC Address sorgente ed il MAC Address di destinazione. Nella connessione HTTPS vediamo anche dai pacchetti intercettati che viene utilizzata la procedura denominata "three way handshake" la quale permette di instaurare in modo affidabile una connessione TCP.