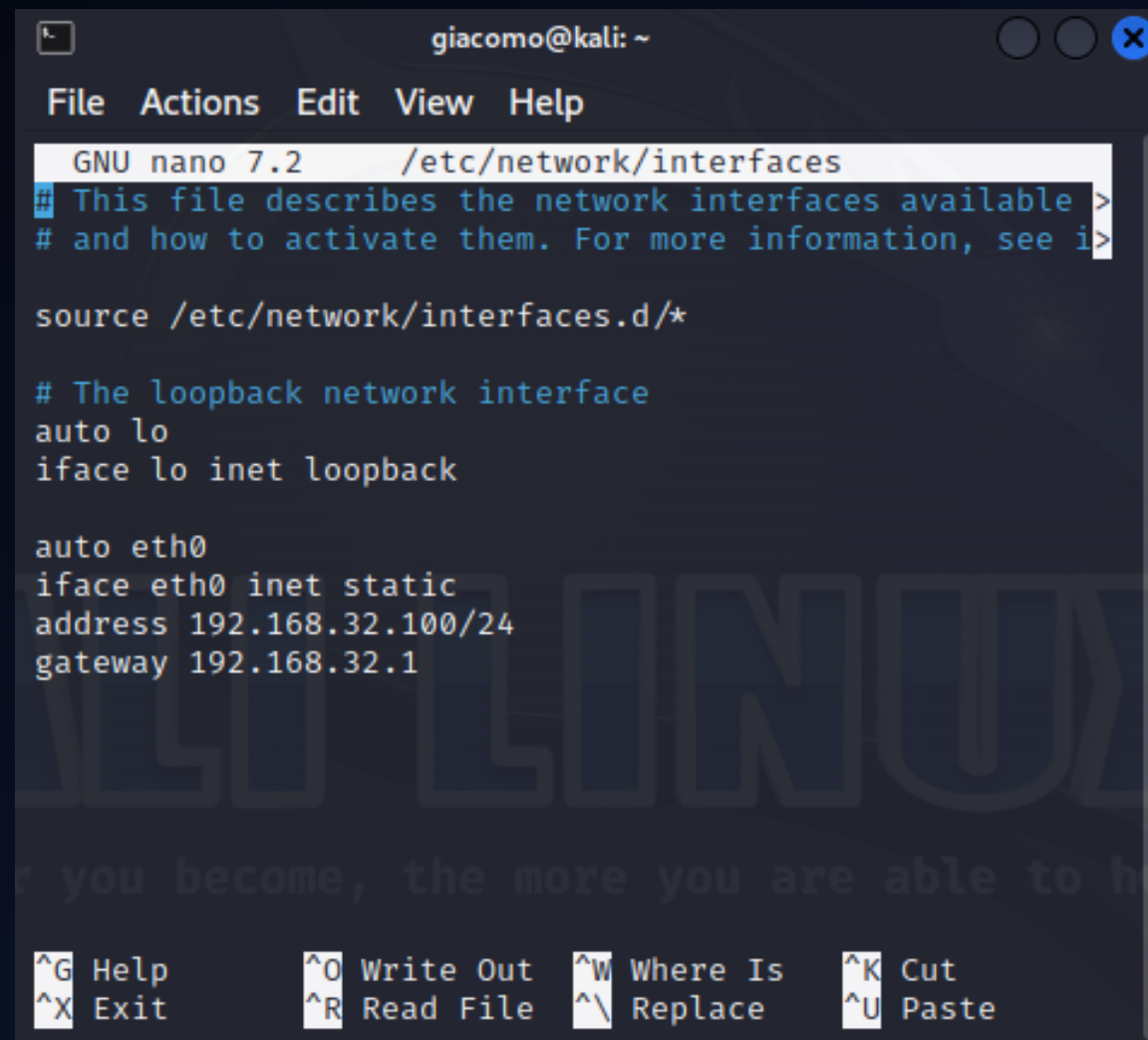


Progetto S1-L5

SIMULAZIONE RETE COMPLESSA E
INTERCETTAZIONE COMUNICAZIONI

Configurazione IP statico di Kali

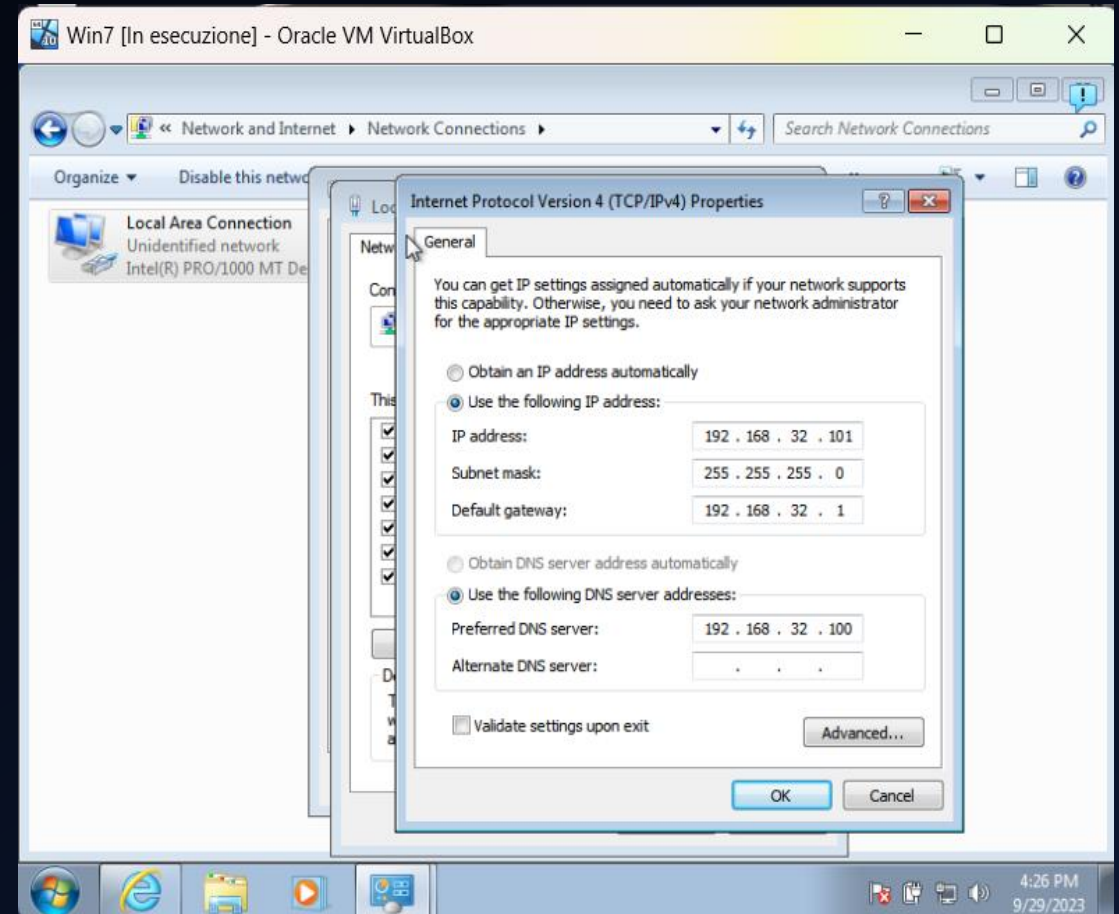
- Da terminale lancio comando
'sudo nano /etc/network/interfaces'
- Modifico IP statico a 192.168.32.100/24 e gateway a 192.168.32.1



```
giacomo@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/network/interfaces  
# This file describes the network interfaces available on  
# and how to activate them. For more information, see the  
# file /etc/network/interfaces.d/debian-installer  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
auto eth0  
iface eth0 inet static  
address 192.168.32.100/24  
gateway 192.168.32.1  
  
^G Help      ^O Write Out  ^W Where Is   ^K Cut  
^X Exit      ^R Read File  ^\ Replace    ^U Paste
```

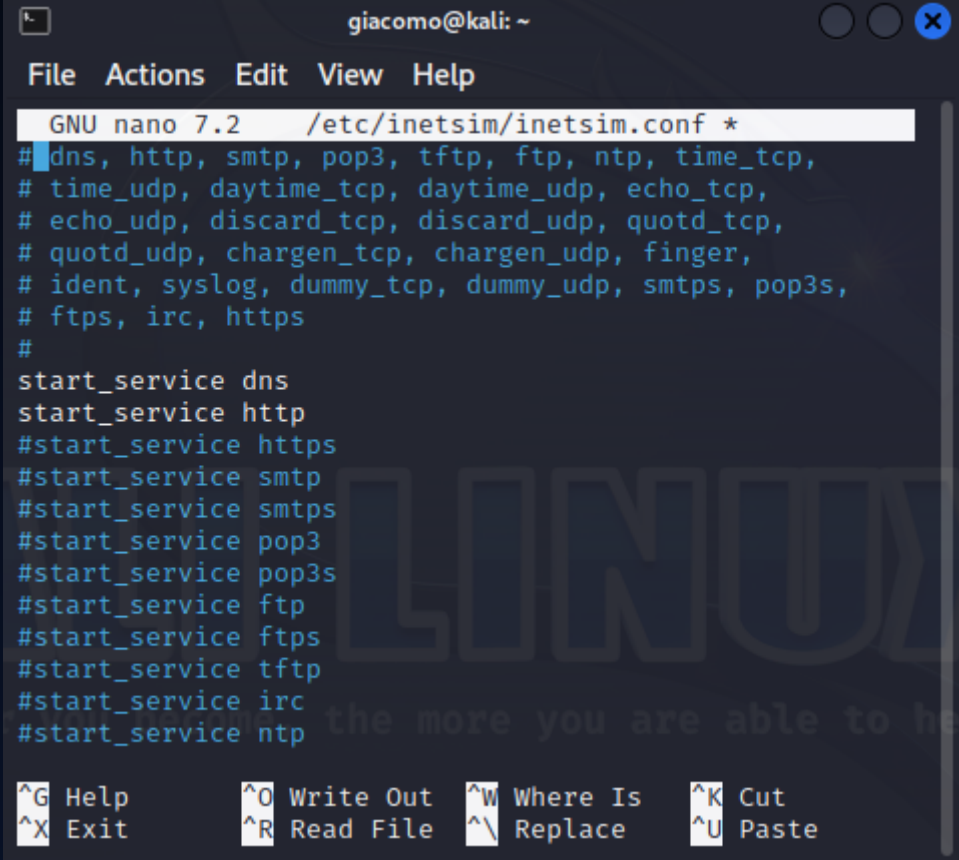
Configurazione IP statico Win7

- Dal pannello di controllo e impostazioni rete vado a impostare l'IP statico 192.168.32.101 e default gateway 192.168.32.1
- Imposto come IP DNS quello corrispondente alla macchina Kali



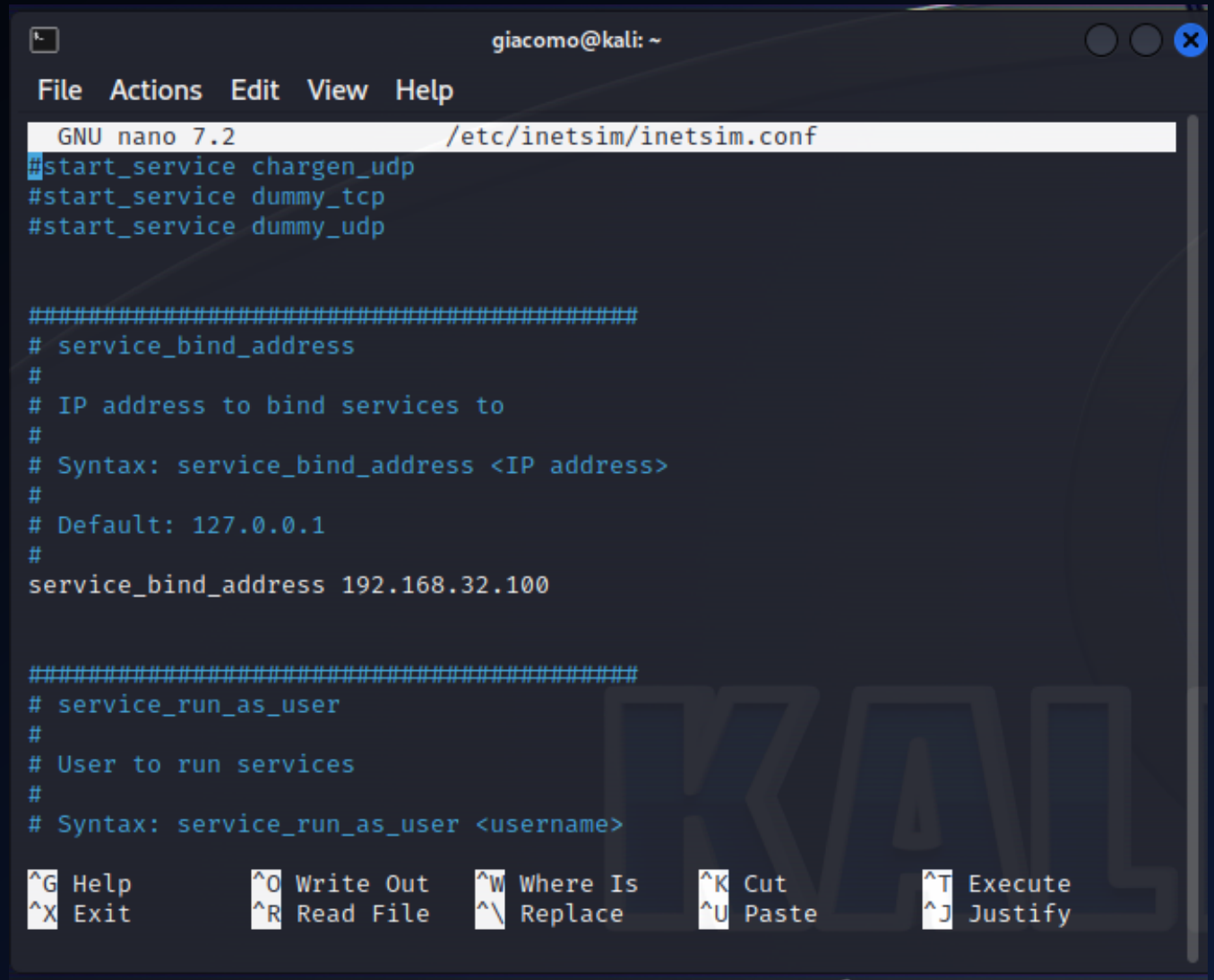
Attivazione servizi DNS e HTTP

- Da terminale apro le istruzioni del simulatore di rete con comando 'sudo nano /etc/inetsim/inetsim.conf
- Attivo i servizi DNS e HTTP eliminando # dalla riga in modo da attivarla



```
giacomo@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/inetsim/inetsim.conf *  
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,  
# 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  
the more you are able to he  
^G Help ^O Write Out ^W Where Is ^K Cut  
^X Exit ^R Read File ^_ Replace ^U Paste
```

- Modifico l'IP per il binding dei servizi inserendo quello della macchina kali 192.168.32.100 sostituendolo al precedente
- Rimuovo # per attivare la riga



```
giacomo@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsim.conf
#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 192.168.32.100

#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>

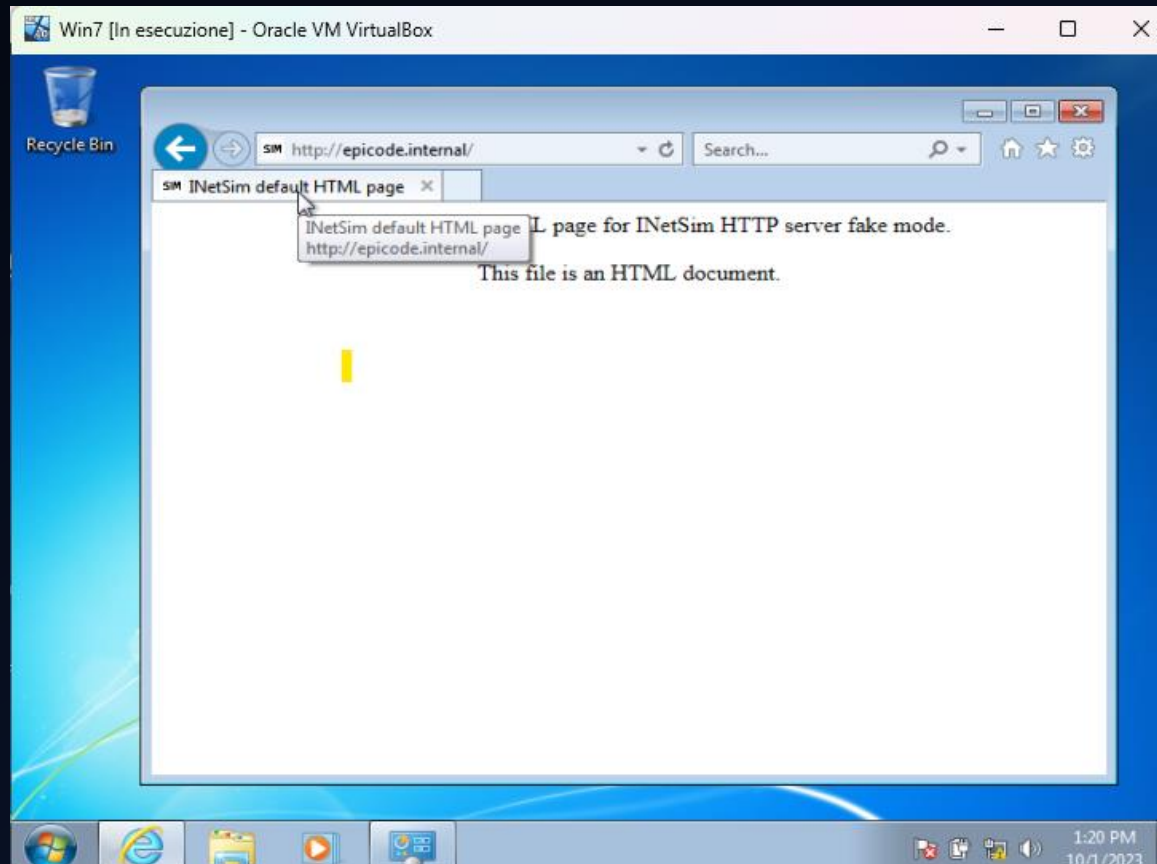
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

Associo l'IP di Kali al DNS statico andando ad aggiungere la riga con nome dominio 'epicode.internal' seguito dall'IP

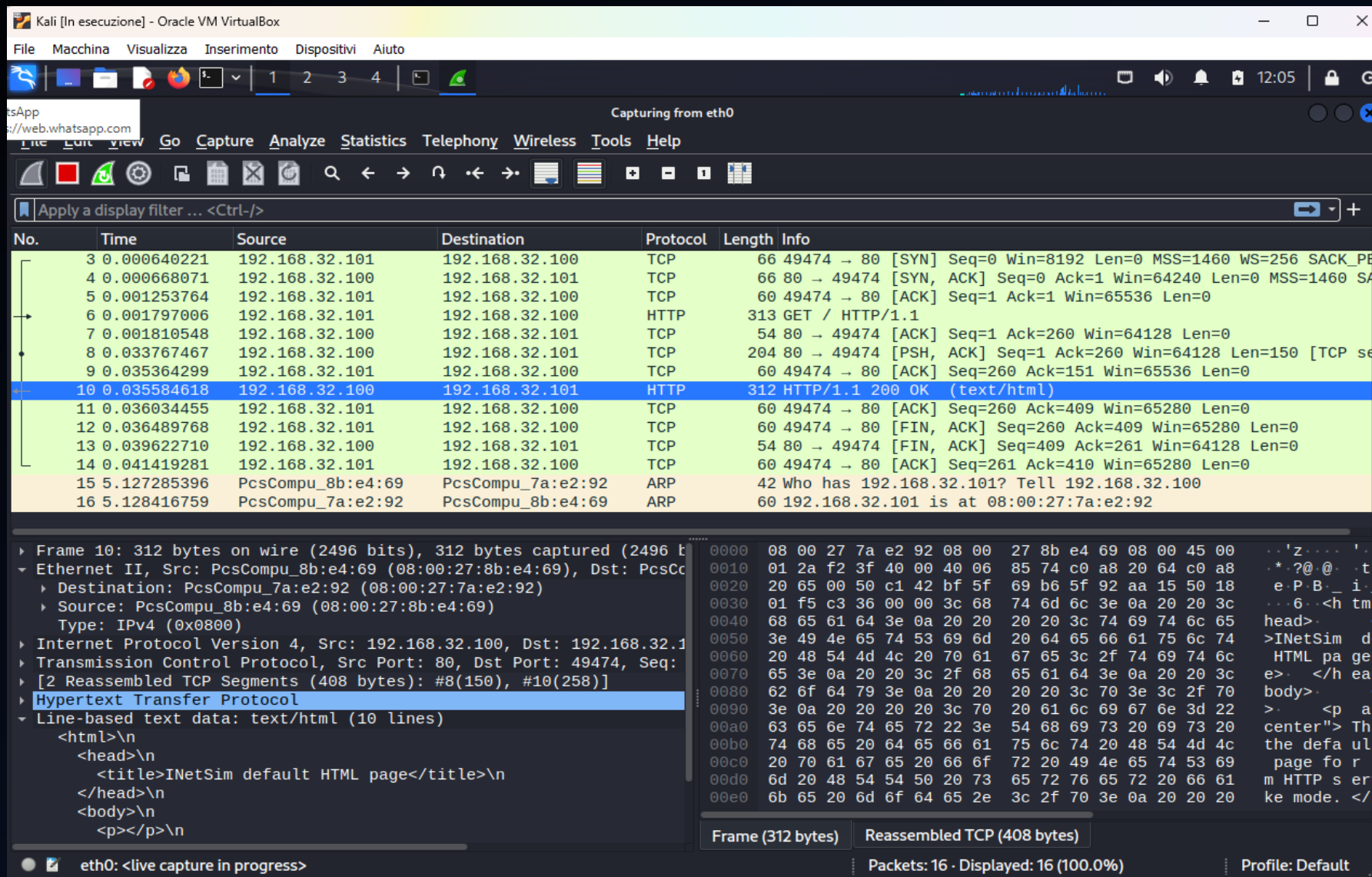
```
giacomo@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/inetsim/inetsim.conf *  
  
#####  
#dns_static  
#  
# Static mappings for DNS  
#  
# Syntax: dns_static <fqdn hostname> <IP address>  
#  
# Default: none  
#  
dns_static epicode.internal 192.168.32.100  
#dns_static ns1.foo.com 10.70.50.30  
#dns_static ftp.bar.net 10.10.20.30  
  
#####  
# dns_version  
#  
# DNS version  
#  
# Syntax: dns_version <version>#  
# Default: "INetSim DNS Server"  
#  
#dns_version "9.2.4"  
  
#####  
# Service HTTP  
#####  
  
#####
```


Faccio partire la simulazione inetsim e provo la connessione da win7 al servizio HTTP

```
giacomo@kali: ~  
File Actions Edit View Help  
== INetSim main process stopped (PID 1607) ==  
.  
(giacomo@kali)-[~]  
$ sudo nano /etc/inetsim/inetsim.conf  
(giacomo@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 9930) ==  
Session ID: 9930  
Listening on: 192.168.32.100  
Real Date/Time: 2023-09-29 11:10:41  
Fake Date/Time: 2023-09-29 11:10:41 (Delta: 0 seconds)  
Forking services...  
* dns_53_tcp_udp - started (PID 9940)  
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm l  
ine 399.  
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm l  
ine 399.  
* http_80_tcp - started (PID 9941)  
done.  
Simulation running.  
█
```



Su wireshark osservo i pacchetti scambiati



Kali [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

tsApp
://web.whatsapp.com

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000640221	192.168.32.101	192.168.32.100	TCP	66	49474 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PF
4	0.000668071	192.168.32.100	192.168.32.101	TCP	66	80 → 49474 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA
5	0.001253764	192.168.32.101	192.168.32.100	TCP	60	49474 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.001797006	192.168.32.101	192.168.32.100	HTTP	313	GET / HTTP/1.1
7	0.001810548	192.168.32.100	192.168.32.101	TCP	54	80 → 49474 [ACK] Seq=1 Ack=260 Win=64128 Len=0
8	0.033767467	192.168.32.100	192.168.32.101	TCP	204	80 → 49474 [PSH, ACK] Seq=1 Ack=260 Win=64128 Len=150 [TCP se
9	0.035364299	192.168.32.101	192.168.32.100	TCP	60	49474 → 80 [ACK] Seq=260 Ack=151 Win=65536 Len=0
10	0.035584618	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
11	0.036034455	192.168.32.101	192.168.32.100	TCP	60	49474 → 80 [ACK] Seq=260 Ack=409 Win=65280 Len=0
12	0.036489768	192.168.32.101	192.168.32.100	TCP	60	49474 → 80 [FIN, ACK] Seq=260 Ack=409 Win=65280 Len=0
13	0.039622710	192.168.32.100	192.168.32.101	TCP	54	80 → 49474 [FIN, ACK] Seq=409 Ack=261 Win=64128 Len=0
14	0.041419281	192.168.32.101	192.168.32.100	TCP	60	49474 → 80 [ACK] Seq=261 Ack=410 Win=65280 Len=0
15	5.127285396	PcsCompu_8b:e4:69	PcsCompu_7a:e2:92	ARP	42	Who has 192.168.32.101? Tell 192.168.32.100
16	5.128416759	PcsCompu_7a:e2:92	PcsCompu_8b:e4:69	ARP	60	192.168.32.101 is at 08:00:27:7a:e2:92

Frame 10: 312 bytes on wire (2496 bits), 312 bytes captured (2496 b
Ethernet II, Src: PcsCompu_8b:e4:69 (08:00:27:8b:e4:69), Dst: PcsCc
Destination: PcsCompu_7a:e2:92 (08:00:27:7a:e2:92)
Source: PcsCompu_8b:e4:69 (08:00:27:8b:e4:69)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.1
Transmission Control Protocol, Src Port: 80, Dst Port: 49474, Seq:
[2 Reassembled TCP Segments (408 bytes): #8(150), #10(258)]
Hypertext Transfer Protocol
Line-based text data: text/html (10 lines)
<html>\n<head>\n<title>INetSim default HTML page</title>\n</head>\n<body>\n<p></p>\n

0000 08 00 27 7a e2 92 08 00 27 8b e4 69 08 00 45 00 ..'z....'
0010 01 2a f2 3f 40 00 40 06 85 74 c0 a8 20 64 c0 a8 *.?@.@.t
0020 20 65 00 50 c1 42 bf 5f 69 b6 5f 92 aa 15 50 18 e.P.B.i
0030 01 f5 c3 36 00 00 3c 68 74 6d 6c 3e 0a 20 20 3c ..6.<h tm
0040 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65 head>
0050 3e 49 4e 65 74 53 69 6d 20 64 65 66 61 75 6c 74 >INetSim d
0060 20 48 54 4d 4c 20 70 61 67 65 3c 2f 74 69 74 6c HTML pa ge
0070 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c e> </h ea
0080 62 6f 64 79 3e 0a 20 20 20 20 3c 70 3e 3c 2f 70 body>
0090 3e 0a 20 20 20 20 3c 70 20 61 6c 69 67 6e 3d 22 > <p a
00a0 63 65 6e 74 65 72 22 3e 54 68 69 73 20 69 73 20 center"> Th
00b0 74 68 65 20 64 65 66 61 75 6c 74 20 48 54 4d 4c the defa ul
00c0 20 70 61 67 65 20 66 6f 72 20 49 4e 65 74 53 69 page fo r
00d0 6d 20 48 54 54 50 20 73 65 72 76 65 72 20 66 61 m HTTP s er
00e0 6b 65 20 6d 6f 64 65 2e 3c 2f 70 3e 0a 20 20 20 ke mode. </

Frame (312 bytes) Reassembled TCP (408 bytes)

eth0: <live capture in progress>

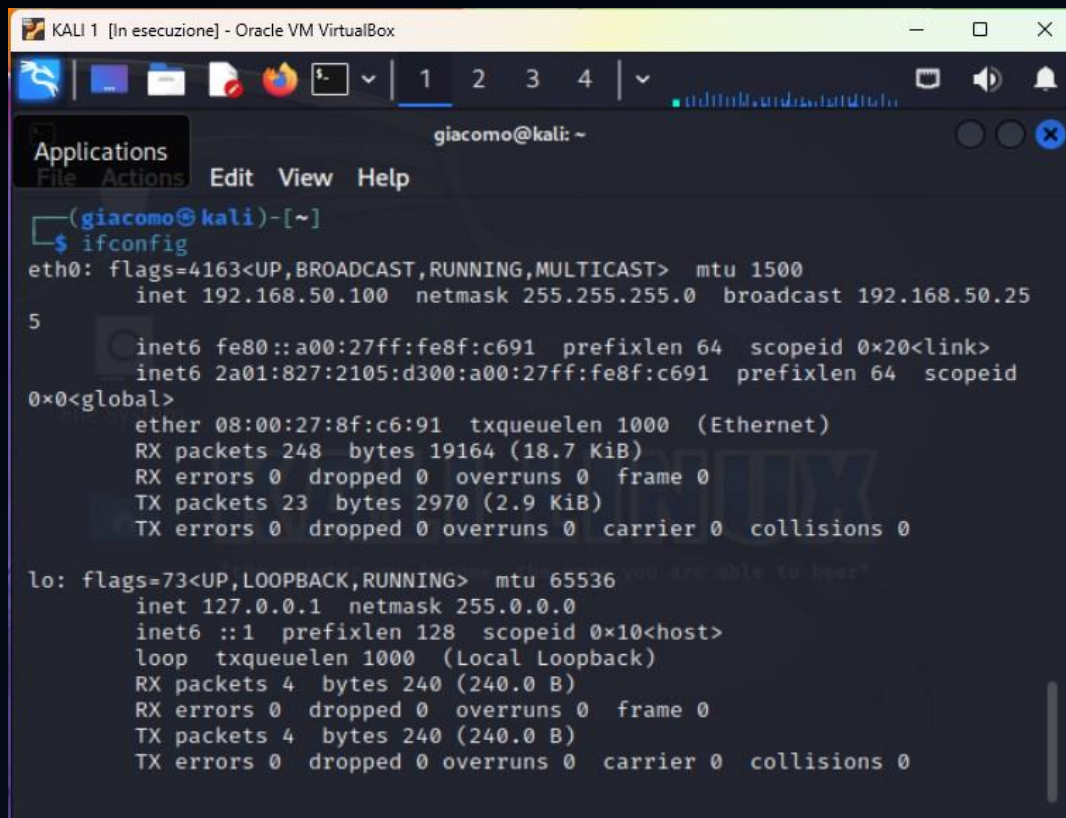
Packets: 16 · Displayed: 16 (100.0%) Profile: Default

- Interrompo la simulazione
- Disattivo il servizio http e attivo il servizio https

```
giacomo@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/inetsim/inetsim.conf *  
# Default: none  
#  
# Available service names are:  
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,  
# 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
```

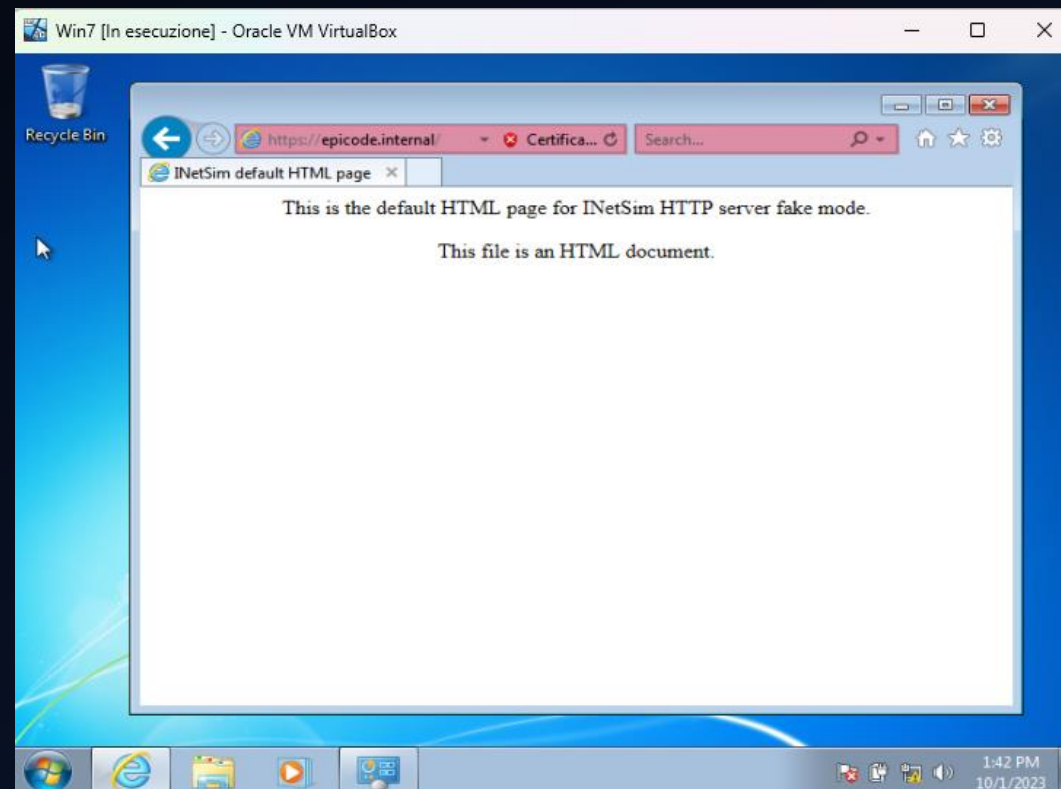
^G Help	^O Write Out	^W Where Is	^K Cut	^T Execute
^X Exit	^R Read File	^_ Replace	^U Paste	^J Justify

Riattivo la simulazione e faccio nuovamente richiesta del servizio da Win 7



```
KALI 1 [In esecuzione] - Oracle VM VirtualBox
giacomo@kali: ~
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255
    inet6 fe80::a00:27ff:fe8f:c691 prefixlen 64 scopeid 0x20<link>
    inet6 2a01:827:2105:d300:a00:27ff:fe8f:c691 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:8f:c6:91 txqueuelen 1000 (Ethernet)
    RX packets 248 bytes 19164 (18.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23 bytes 2970 (2.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



Catturo nuovamente i pacchetti da wireshark

Kali [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
37	2.070193285	192.168.32.100	192.168.32.101	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
38	2.070818500	192.168.32.101	192.168.32.100	TCP	60	49480 → 443 [ACK] Seq=532 Ack=1819 Win=65536 Len=0
39	2.073462840	192.168.32.101	192.168.32.100	TLSv1.2	342	Application Data
40	2.091963321	192.168.32.100	192.168.32.101	TLSv1.2	234	Application Data
41	2.092638192	192.168.32.101	192.168.32.100	TCP	60	49480 → 443 [ACK] Seq=820 Ack=1999 Win=65280 Len=0
42	2.093461339	192.168.32.100	192.168.32.101	TLSv1.2	341	Application Data
43	2.094279722	192.168.32.101	192.168.32.100	TCP	60	49480 → 443 [ACK] Seq=820 Ack=2286 Win=65024 Len=0
44	2.094827023	192.168.32.101	192.168.32.100	TCP	60	49480 → 443 [FIN, ACK] Seq=820 Ack=2286 Win=65024 Len=0
45	2.099385779	192.168.32.100	192.168.32.101	TLSv1.2	85	Encrypted Alert
46	2.101533886	192.168.32.100	192.168.32.101	TCP	54	443 → 49480 [FIN, ACK] Seq=2317 Ack=821 Win=64128 Len=0
47	2.101976003	192.168.32.101	192.168.32.100	TCP	60	49480 → 443 [RST, ACK] Seq=821 Ack=2317 Win=0 Len=0
48	2.119238649	192.168.32.101	192.168.32.100	TCP	60	49480 → 443 [RST] Seq=821 Win=0 Len=0
49	2.151054593	192.168.32.101	192.168.32.100	TCP	66	49483 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_F
50	2.151088249	192.168.32.100	192.168.32.101	TCP	66	443 → 49483 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 S
51	2.151699872	192.168.32.101	192.168.32.100	TCP	60	49483 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0

Frame 45: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface eth0

Ethernet II, Src: PcsCompu_8b:e4:69 (08:00:27:8b:e4:69), Dst: PcsCompu_7a:e2:92 (08:00:27:7a:e2:92)

Destination: PcsCompu_7a:e2:92 (08:00:27:7a:e2:92)

Source: PcsCompu_8b:e4:69 (08:00:27:8b:e4:69)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101

Transmission Control Protocol, Src Port: 443, Dst Port: 49480, Seq: 820, Len: 0

Transport Layer Security

TLSv1.2 Record Layer: Encrypted Alert

Content Type: Alert (21)

Version: TLS 1.2 (0x0303)

Length: 26

Alert Message: Encrypted Alert

0000 08 00 27 7a e2 92 08 00 27 8b e4 69 08 00 45 00 z

0010 00 47 11 20 40 00 40 06 67 77 c0 a8 20 64 c0 a8 G @ @ . gw .

0020 20 65 01 bb c1 48 69 79 3d 75 79 de 9b 3b 50 18 e

0030 01 f5 c2 53 00 00 15 03 03 00 1a db a2 44 de fc S

0040 24 bb 58 63 85 09 45 3c 98 da 74 d1 0a ea 6a ba \$. Xc . . E < . t

0050 74 d6 0c 7d 61 t . . } a

Content Type (tls.record.content_type), 1 byte(s)

Packets: 62 - Displayed: 62 (100.0%)

Profile: Default

CTRI (DEFTRA)

Dal confronto delle due catture possiamo osservare come usando il servizio HTTP abbiamo accesso al contenuto del pacchetto, mentre utilizzando il servizio HTTPS, i pacchetti saranno criptati. Con entrambe le catture possiamo individuare gli indirizzi MAC dei dispositivi coinvolti.

Kali [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Capturing from eth0

Applications

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
37	2.070193285	192.168.32.100	192.168.32.101	TLSv1.2	105	Change Cipher
38	2.070818500	192.168.32.101	192.168.32.100	TCP	60	49480 → 443
39	2.073462840	192.168.32.101	192.168.32.100	TLSv1.2	342	Application D
40	2.091963321	192.168.32.100	192.168.32.101	TLSv1.2	234	Application D
41	2.092638192	192.168.32.101	192.168.32.100	TCP	60	49480 → 443
42	2.093461339	192.168.32.100	192.168.32.101	TLSv1.2	341	Application D
43	2.094279722	192.168.32.101	192.168.32.100	TCP	60	49480 → 443
44	2.094827023	192.168.32.101	192.168.32.100	TCP	60	49480 → 443
45	2.099385779	192.168.32.100	192.168.32.101	TLSv1.2	85	Encrypted Ale
46	2.101533886	192.168.32.100	192.168.32.101	TCP	54	443 → 49480
47	2.101976003	192.168.32.101	192.168.32.100	TCP	60	49480 → 443
48	2.119238649	192.168.32.101	192.168.32.100	TCP	60	49480 → 443
49	2.151054593	192.168.32.101	192.168.32.100	TCP	66	49483 → 443
50	2.151088249	192.168.32.100	192.168.32.101	TCP	66	443 → 49483
51	2.151699872	192.168.32.101	192.168.32.100	TCP	60	49483 → 443

Frame 45: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface eth0

Ethernet II, Src: PcsCompu_8b:e4:69 (08:00:27:8b:e4:69), Dst: PcsCompu_7a:e2:92 (08:00:27:7a:e2:92)

Source: PcsCompu_8b:e4:69 (08:00:27:8b:e4:69)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101

Transmission Control Protocol, Src Port: 443, Dst Port: 443

Transport Layer Security

TLSv1.2 Record Layer: Encrypted Alert

Content Type: Alert (21)

Version: TLS 1.2 (0x0303)

Length: 26

Alert Message: Encrypted Alert

Alert Message (tls.alert_message), 26 byte(s)

Packets: 63 · Displayed: 63 (100.0%) Profile: Default

Kali [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000029155	PcsCompu_8b:e4:69	PcsCompu_7a:e2:92	ARP	42	192.168.32.100 is at 08:00:27:8b:e4:69
3	0.000642014	192.168.32.101	192.168.32.100	TCP	66	49552 → 80 [SYN] Seq=0 Win=8192 Len=0
4	0.000670436	192.168.32.100	192.168.32.101	TCP	66	80 → 49552 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
5	0.001415502	192.168.32.101	192.168.32.100	TCP	60	49552 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.001892889	192.168.32.101	192.168.32.100	HTTP	313	GET / HTTP/1.1
7	0.001902415	192.168.32.100	192.168.32.101	TCP	54	80 → 49552 [ACK] Seq=1 Ack=260 Win=65536 Len=0
8	0.036366100	192.168.32.100	192.168.32.101	TCP	204	80 → 49552 [PSH, ACK] Seq=1 Ack=260 Win=65536 Len=0
9	0.037259668	192.168.32.101	192.168.32.100	TCP	60	49552 → 80 [ACK] Seq=260 Ack=151 Win=65536 Len=0
10	0.038306499	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
11	0.042555126	192.168.32.101	192.168.32.100	TCP	60	49552 → 80 [ACK] Seq=260 Ack=409 Win=65536 Len=0
12	0.042555469	192.168.32.101	192.168.32.100	TCP	60	49552 → 80 [FIN, ACK] Seq=260 Ack=409 Win=65536 Len=0
13	0.045594872	192.168.32.100	192.168.32.101	TCP	54	80 → 49552 [FIN, ACK] Seq=409 Ack=260 Win=65536 Len=0
14	0.046895398	192.168.32.101	192.168.32.100	TCP	60	49552 → 80 [ACK] Seq=261 Ack=410 Win=65536 Len=0
15	0.085787503	192.168.32.101	192.168.32.100	DNS	77	Standard query 0xff71 A urs.microsoft.com
16	0.116799586	192.168.32.100	192.168.32.101	DNS	93	Standard query response 0xff71 A urs.microsoft.com

312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0

Ethernet II, Src: PcsCompu_8b:e4:69 (08:00:27:8b:e4:69), Dst: PcsCompu_7a:e2:92 (08:00:27:7a:e2:92)

Internet Protocol Version 4, Src: 192.168.32.100, Dst: 192.168.32.101

Transport Layer Security

TLSv1.2 Record Layer: Encrypted Alert

Content Type: Alert (21)

Version: TLS 1.2 (0x0303)

Length: 26

Alert Message: Encrypted Alert

Alert Message (tls.alert_message), 26 byte(s)

Packets: 16 · Displayed: 16 (100.0%) Profile: Default