Esercitazione DNS, HTTP, HTTPS

In questo esercizio lo scopo era simulare una richiesta tramite web browser da parte di un client con IP 192.168.32.101 all'hostname epicode.internal con IP 192.168.32.100.

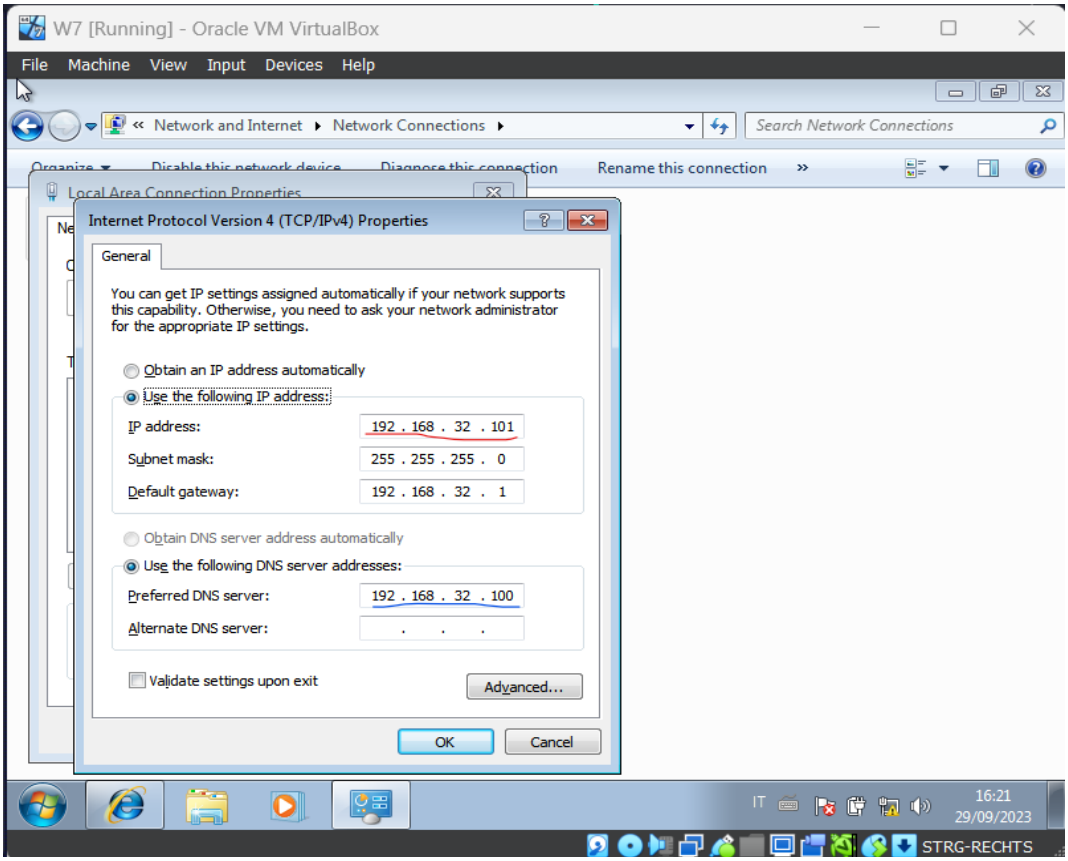
Per prima cosa ho configurato i nuovi IP per le due macchine.
Per primo l'IP del server che avrà funzione di DSN (su macchina Kali), tramite il comando *sudo nano /etc/network/interfaces* sul terminal di Kali:

```
kali@kali: ~
File  Actions  Edit  View  Help
  GNU nano 7.2                /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

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
gatewaz 192.168.32.1

                                [ Read 13 lines ]
^G Help      ^O Write Out   ^W Where Is    ^K Cut       ^T Execute
^X Exit      ^R Read File   ^\ Replace     ^U Paste     ^J Justify
```

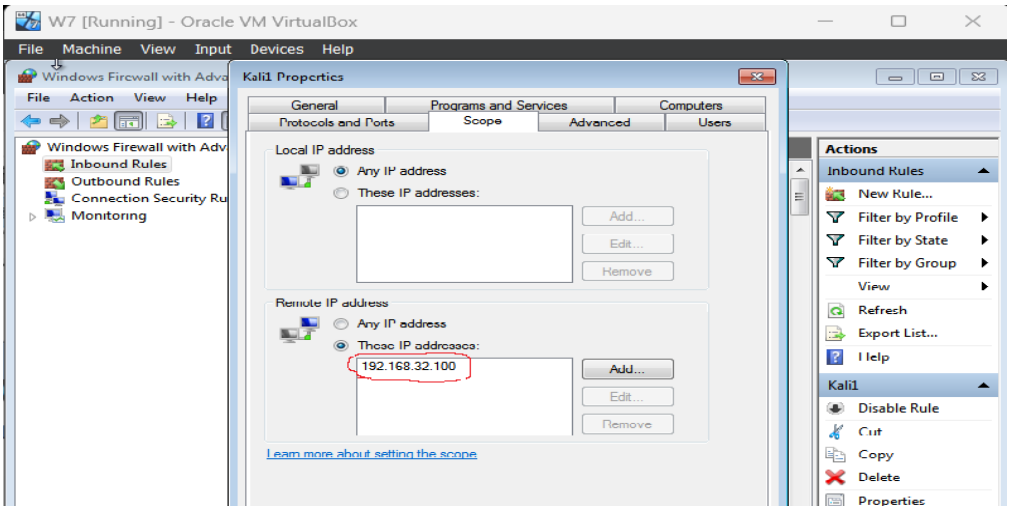
Tramite il comando ifconfig ho confermato il cambio di IP:

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/network/interfaces
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.100  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::a00:27ff:fecb:7ef5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 481  bytes 41707 (40.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 260  bytes 41585 (40.6 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 44  bytes 2240 (2.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44  bytes 2240 (2.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$
```

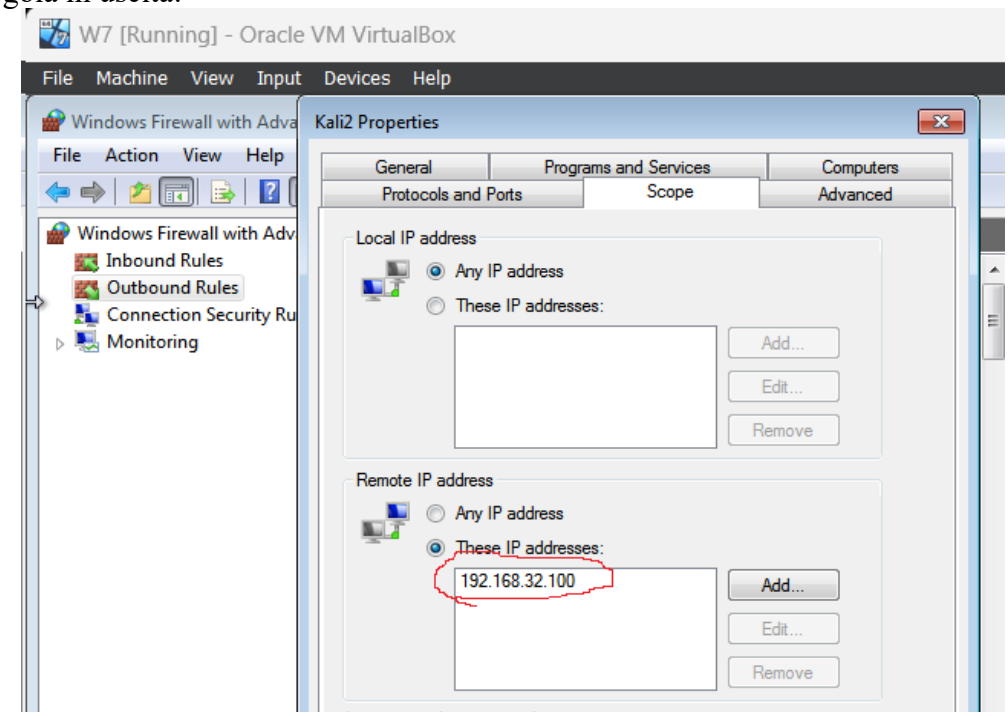
A seguire ho configurato l'IP del client (in rosso nell'immagine), su macchina Windows 7 ed ho indicato il server DNS preferito (in blu), corrispondente alla macchina Kali.



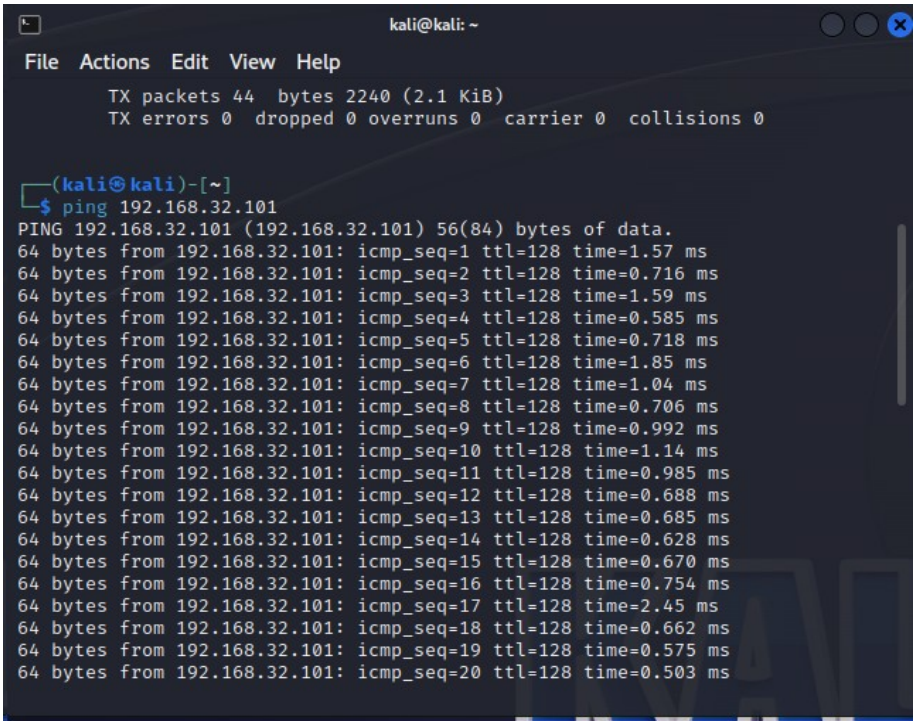
Sempre sul client ho impostato una regola nuova nel firewall per permettere alle due macchine di comunicare.
Qui la regola in entrata:



E qui la regola in uscita:



Per assicurarmi che client e server potessero comunicare, ho usato il comando *ping* nei rispettivi terminal:



```
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Marco>ping 192.168.32.100

Pinging 192.168.32.100 with 32 bytes of data:
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64
Reply from 192.168.32.100: bytes=32 time=14ms TTL=64

Ping statistics for 192.168.32.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\Users\Marco>_
```

A questo punto ho attivato i protocolli DNS e HTTPS in Kali, tramite il comando *sudo nano /etc/inetsim/inetsim.conf*:

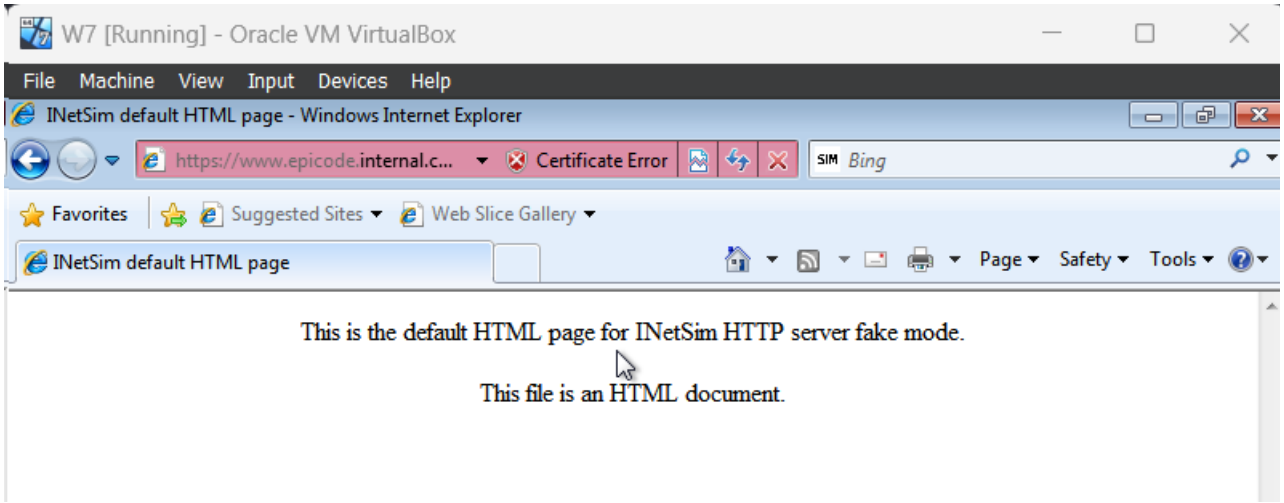
```
kali@kali: ~
File  Actions  Edit  View  Help
  GNU nano 7.2                /etc/inetsim/inetsim.conf
# ftps, irc, https
#
start_service dns
#start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#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

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

Dalla funzione Inetsim ho abilitato service_bind_address, Service DNS, dns_default_ip, dns_default domainname e dns_static www.epicode.internal.com 192.168.32.100.

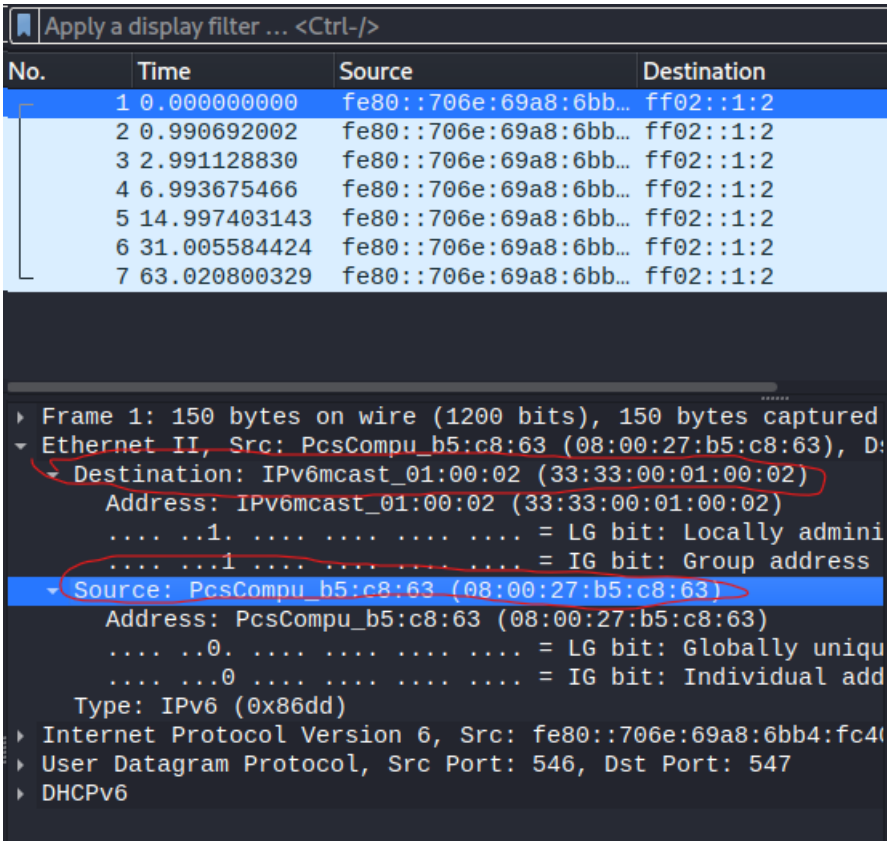
Ho quindi avviato l'honeypot Inetsim con il comando sudo inetsim:

```
kali@kali: ~
File  Actions  Edit  View  Help
└─$ 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.
Warning: Unknown option 'Service' in configuration file '/etc/inetsim/inetsim
.conf' line 183
Warning: Unknown option 'Service' in configuration file '/etc/inetsim/inetsim
.conf' line 369
Configuration file parsed successfully.
=== INetSim main process started (PID 43301) ===
Session ID:     43301
Listening on:   192.168.32.100
Real Date/Time: 2023-09-29 10:46:33
Fake Date/Time: 2023-09-29 10:46:33 (Delta: 0 seconds)
 Forking services ...
  * dns_53_tcp_udp - started (PID 43303)
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.
  * https_443_tcp - started (PID 43304)
 done.
Simulation running.
```

Ho quindi ricercato il dominio www.epicode.internal.com dal web browser del client:

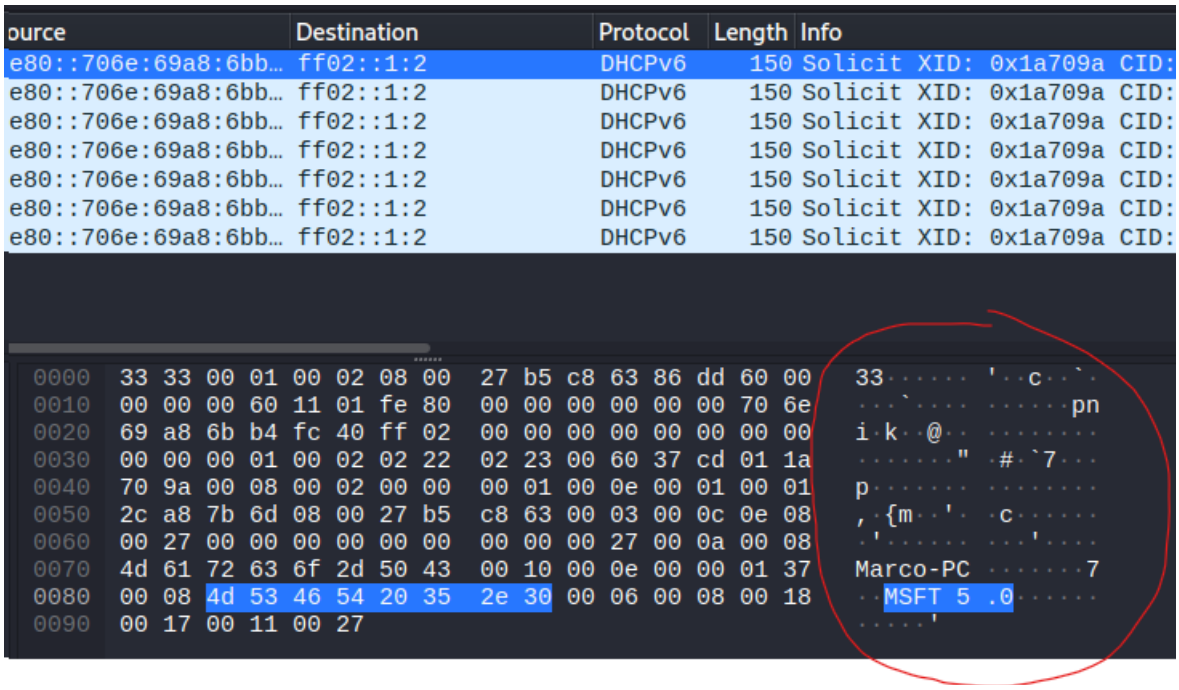


Infine ho usato il prgramma Wireshrk per intercettare la comunicazione (in rosso gli indirizzi MAC di origine e destinazione):



No.	Time	Source	Destination
1	0.000000000	fe80::706e:69a8:6bb…	ff02::1:2
2	0.990692002	fe80::706e:69a8:6bb…	ff02::1:2
3	2.991128830	fe80::706e:69a8:6bb…	ff02::1:2
4	6.993675466	fe80::706e:69a8:6bb…	ff02::1:2
5	14.997403143	fe80::706e:69a8:6bb…	ff02::1:2
6	31.005584424	fe80::706e:69a8:6bb…	ff02::1:2
7	63.020800329	fe80::706e:69a8:6bb…	ff02::1:2

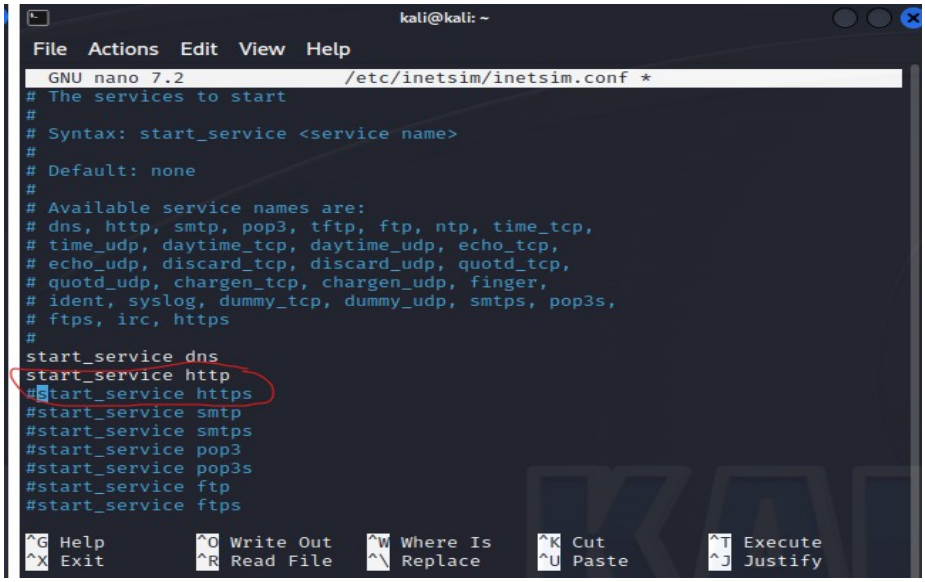
Da notare la cifratura del pacchetto:



```
ource                    Destination            Protocol  Length Info
e80::706e:69a8:6bb… ff02::1:2              DHCPv6       150 Solicit XID: 0x1a709a CID:
e80::706e:69a8:6bb… ff02::1:2              DHCPv6       150 Solicit XID: 0x1a709a CID:
e80::706e:69a8:6bb… ff02::1:2              DHCPv6       150 Solicit XID: 0x1a709a CID:
e80::706e:69a8:6bb… ff02::1:2              DHCPv6       150 Solicit XID: 0x1a709a CID:
e80::706e:69a8:6bb… ff02::1:2              DHCPv6       150 Solicit XID: 0x1a709a CID:
e80::706e:69a8:6bb… ff02::1:2              DHCPv6       150 Solicit XID: 0x1a709a CID:
e80::706e:69a8:6bb… ff02::1:2              DHCPv6       150 Solicit XID: 0x1a709a CID:
```

```
0000  33 33 00 01 00 02 08 00  27 b5 c8 63 86 dd 60 00   33······ '··c··`·
0010  00 00 00 60 11 01 fe 80  00 00 00 00 00 00 70 6e   ···`···· ······pn
0020  69 a8 6b b4 fc 40 ff 02  00 00 00 00 00 00 00 00   i·k··@·· ········
0030  00 00 00 01 00 02 02 22  02 23 00 60 37 cd 01 1a   ·······" ·#·`7···
0040  70 9a 00 08 00 02 00 00  00 01 00 0e 00 01 00 01   p······· ········
0050  2c a8 7b 6d 08 00 27 b5  c8 63 00 03 00 0c 0e 08   ,·{m··'· ·c······
0060  00 27 00 00 00 00 00 00  00 00 00 27 00 0a 00 08   ·'······ ···'····
0070  4d 61 72 63 6f 2d 50 43  00 10 00 0e 00 00 01 37   Marco-PC ·······7
0080  00 08 4d 53 46 54 20 35  2e 30 00 06 00 08 00 18   ··MSFT 5 .0······
0090  00 17 00 11 00 27                                  ·····'
```

A questo punto ho cambiato il protocollo del server da HTTPS ad HTTP, sempre usando il comando *sudo nano /etc/inetsim/inetsim.conf*.

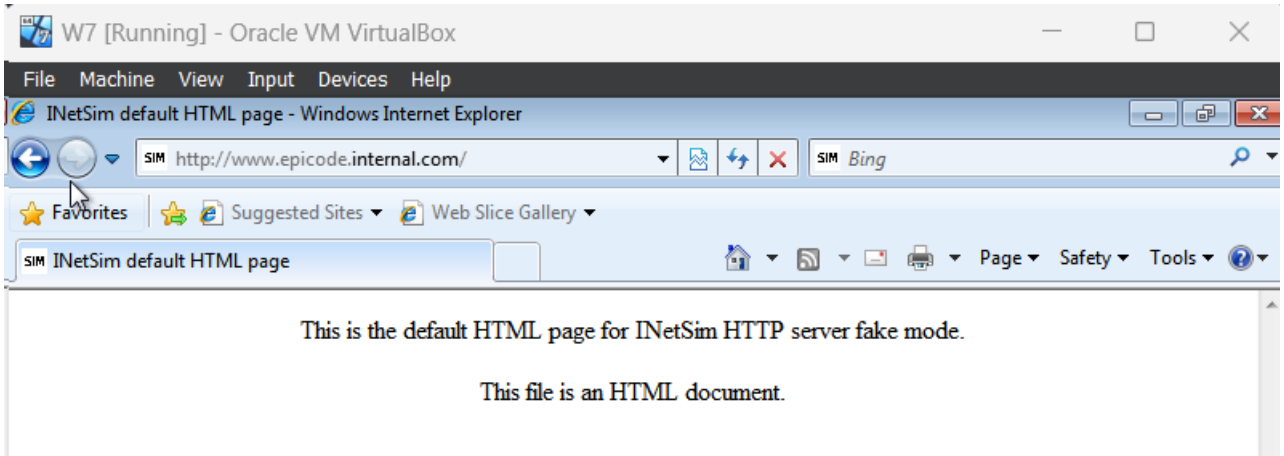


```
  GNU nano 7.2                /etc/inetsim/inetsim.conf *
# The services to start
#
# Syntax: start_service <service name>
#
# Default: none
#
# Available service names are:
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, 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

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

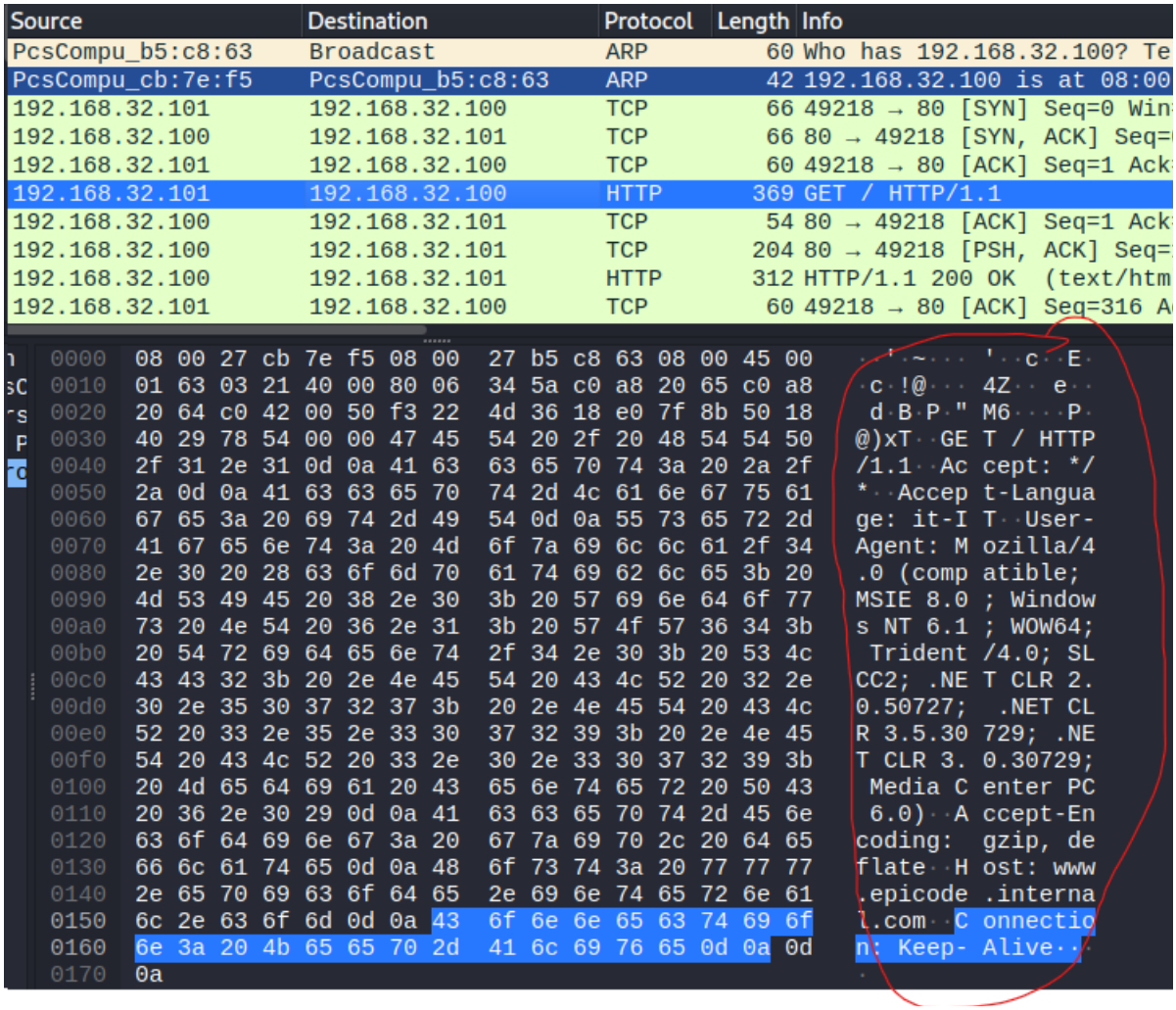
Ho avviato di nuovo Inetsim

```
kali@kali: ~
File  Actions  Edit  View  Help
└─$ 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.
Warning: Unknown option 'Service' in configuration file '/etc/inetsim/inetsim
.conf' line 183
Warning: Unknown option 'Service' in configuration file '/etc/inetsim/inetsim
.conf' line 262
Configuration file parsed successfully.
=== INetSim main process started (PID 45572) ===
Session ID:     45572
Listening on:   192.168.32.100
Real Date/Time: 2023-09-29 10:51:13
Fake Date/Time: 2023-09-29 10:51:13 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 45582)
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 45583)
 done.
Simulation running.
```

Ho di nuovo cercato il dominio www.epicode.internal.com, questa volta tramite HTTP:



Si può notare come con il protocollo HTTP la cifratura non comapre più quando si intercetta la comunicazione:



Source	Destination	Protocol	Length	Info
PcsCompu_b5:c8:63	Broadcast	ARP	60	Who has 192.168.32.100? Te
PcsCompu_cb:7e:f5	PcsCompu_b5:c8:63	ARP	42	192.168.32.100 is at 08:00
192.168.32.101	192.168.32.100	TCP	66	49218 → 80 [SYN] Seq=0 Win
192.168.32.100	192.168.32.101	TCP	66	80 → 49218 [SYN, ACK] Seq=
192.168.32.101	192.168.32.100	TCP	60	49218 → 80 [ACK] Seq=1 Ack
192.168.32.101	192.168.32.100	HTTP	369	GET / HTTP/1.1
192.168.32.100	192.168.32.101	TCP	54	80 → 49218 [ACK] Seq=1 Ack
192.168.32.100	192.168.32.101	TCP	204	80 → 49218 [PSH, ACK] Seq=
192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/htm
192.168.32.101	192.168.32.100	TCP	60	49218 → 80 [ACK] Seq=316 A

```
0000  08 00 27 cb 7e f5 08 00  27 b5 c8 63 08 00 45 00   ··'·~··· '··c··E·
0010  01 63 03 21 40 00 80 06  34 5a c0 a8 20 65 c0 a8   ·c·!@··· 4Z·· e··
0020  20 64 c0 42 00 50 f3 22  4d 36 18 e0 7f 8b 50 18    d·B·P·" M6····P·
0030  40 29 78 54 00 00 47 45  54 20 2f 20 48 54 54 50   @)xT··GE T / HTTP
0040  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1··Ac cept: */
0050  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 75 61   *··Accep t-Langua
0060  67 65 3a 20 69 74 2d 49  54 0d 0a 55 73 65 72 2d   ge: it-I T··User-
0070  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 34   Agent: M ozilla/4
0080  2e 30 20 28 63 6f 6d 70  61 74 69 62 6c 65 3b 20   .0 (comp atible;
0090  4d 53 49 45 20 38 2e 30  3b 20 57 69 6e 64 6f 77   MSIE 8.0 ; Window
00a0  73 20 4e 54 20 36 2e 31  3b 20 57 4f 57 36 34 3b   s NT 6.1 ; WOW64;
00b0  20 54 72 69 64 65 6e 74  2f 34 2e 30 3b 20 53 4c    Trident /4.0; SL
00c0  43 43 32 3b 20 2e 4e 45  54 20 43 4c 52 20 32 2e   CC2; .NE T CLR 2.
00d0  30 2e 35 30 37 32 37 3b  20 2e 4e 45 54 20 43 4c   0.50727;  .NET CL
00e0  52 20 33 2e 35 2e 33 30  37 32 39 3b 20 2e 4e 45   R 3.5.30 729; .NE
00f0  54 20 43 4c 52 20 33 2e  30 2e 33 30 37 32 39 3b   T CLR 3. 0.30729;
0100  20 4d 65 64 69 61 20 43  65 6e 74 65 72 20 50 43    Media C enter PC
0110  20 36 2e 30 29 0d 0a 41  63 63 65 70 74 2d 45 6e    6.0)··A ccept-En
0120  63 6f 64 69 6e 67 3a 20  67 7a 69 70 2c 20 64 65   coding:  gzip, de
0130  66 6c 61 74 65 0d 0a 48  6f 73 74 3a 20 77 77 77   flate··H ost: www
0140  2e 65 70 69 63 6f 64 65  2e 69 6e 74 65 72 6e 61   .epicode .interna
0150  6c 2e 63 6f 6d 0d 0a 43  6f 6e 6e 65 63 74 69 6f   l.com··C onnectio
0160  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 0d   n: Keep- Alive···
0170  0a                                                  ·
```