

TEST DI VALUTAZIONE MODULO I



Andrea Ferrantino

La prova chiede di constatare le competenze avute fino ad ora..

- **Settaggio IP Kali Linux VM (192.168.32.100)**
- **Settaggio IP Windows 7 VM (192.1342.32.101)**
- **HTTPS server attivo**
- **Servizio DNS per risoluzione nomi domini attivo**

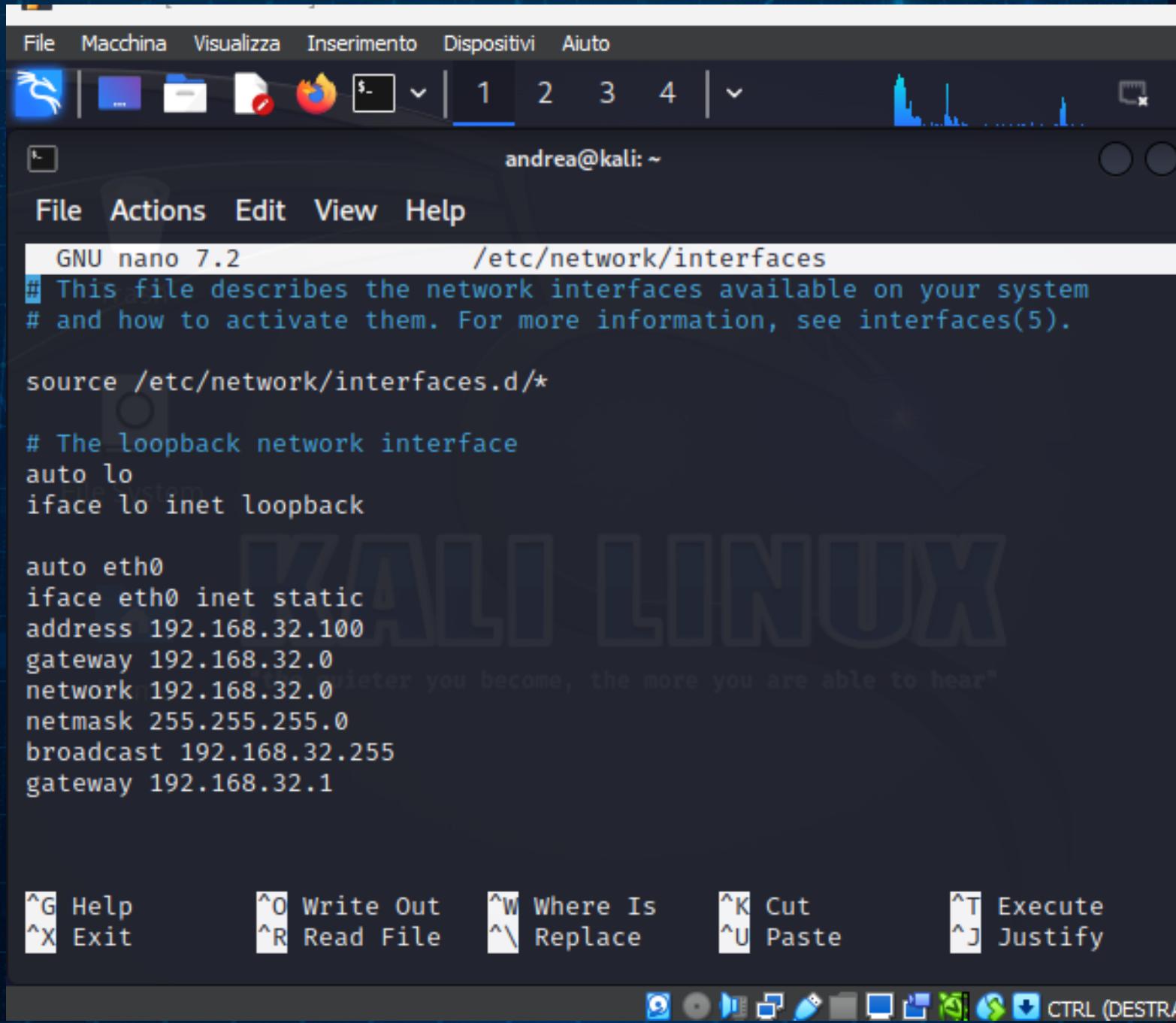
Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname episode.internal che risponde all'indirizzo 192.168.32.100 (Kali). Si intercetti poi la comunicazione con Wireshark, 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 precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

Configurazione IP

Kali e Windows 7

Come prima cosa dobbiamo configurare gli indirizzi ip delle macchine virtuali come da traccia:

Utilizziamo il comando (sudo nano /etc/network/interfaces)



```
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
gateway 192.168.32.0
network 192.168.32.0
netmask 255.255.255.0
broadcast 192.168.32.255
gateway 192.168.32.1
```

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:

192 . 168 . 32 . 101

Subnet mask:

255 . 255 . 255 . 0

Default gateway:

192 . 168 . 32 . 1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

192 . 168 . 32 . 100

Alternate DNS server:

• • • •

Validate settings upon exit

Advanced...

OK

Cancel



EN



CTRL

Configurazione Intesim.conf

Successivamente dobbiamo andare all'interno di inetsim.conf avviando da Kali e digitando il comando (sudo nano /etc/inetsim/inetsim.conf) così andremo ad abilitare i service DNS,HTTP,HTTPS togliendo l'# davanti alla voce come screen qui sotto:

```
GNU nano 7.2
#####
# Main configuration
#####

#####
# start_service
# File System
# 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
# 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
```



"the quieter you become,

Successivamente impostiamo il “service_bind_address con l’IP “0.0.0.0” che va bene con tutte le piattaforme.

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
GNU nano 7.2 /etc/inetsim/inetsim.conf
Trash

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
# File System
# Default: 127.0.0.1
#
service_bind_address 0.0.0.0

#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#           "the quieter you become, the more you are able to hear"
# Default: inetsim
#
#service_run_as_user nobody

#####
# service_max_childs
#
# Maximum number of child processes (parallel connections)

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

Ora per risolvere l'hostname "epicode.internal" associando come "dns_static" lo stesso ip di Kali:



```
File Macchina Visualizza Inserimento Dispositivi Aiuto
andrea@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 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

#####
# dns_version
#
# DNS version
#
# Syntax: dns_version <version>
#
# Default: "INetSim DNS Server"
#
#dns_version "9.2.4"

#####
# Service HTTP
#####

^G Help      ^O Write Out   ^W Where Is   ^K Cut        ^T Execute   ^C Location   M-U Undo
^X Exit      ^R Read File   ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line M-E Redo
```

Simulazione Inetsim

Digitando il comando “sudo inetsim” sul terminale di Kali partì il client del server:

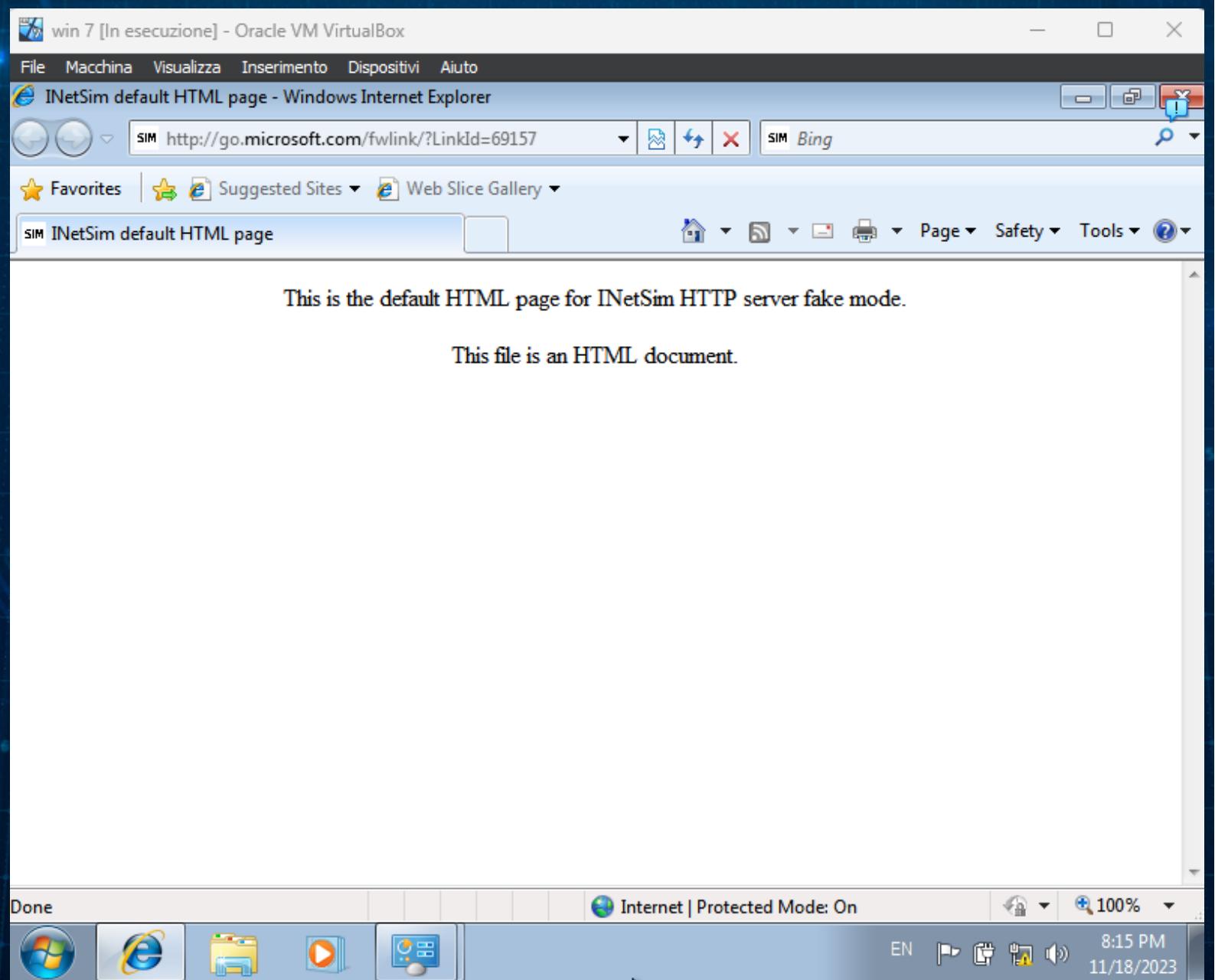
The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window has a dark background and contains the following text:

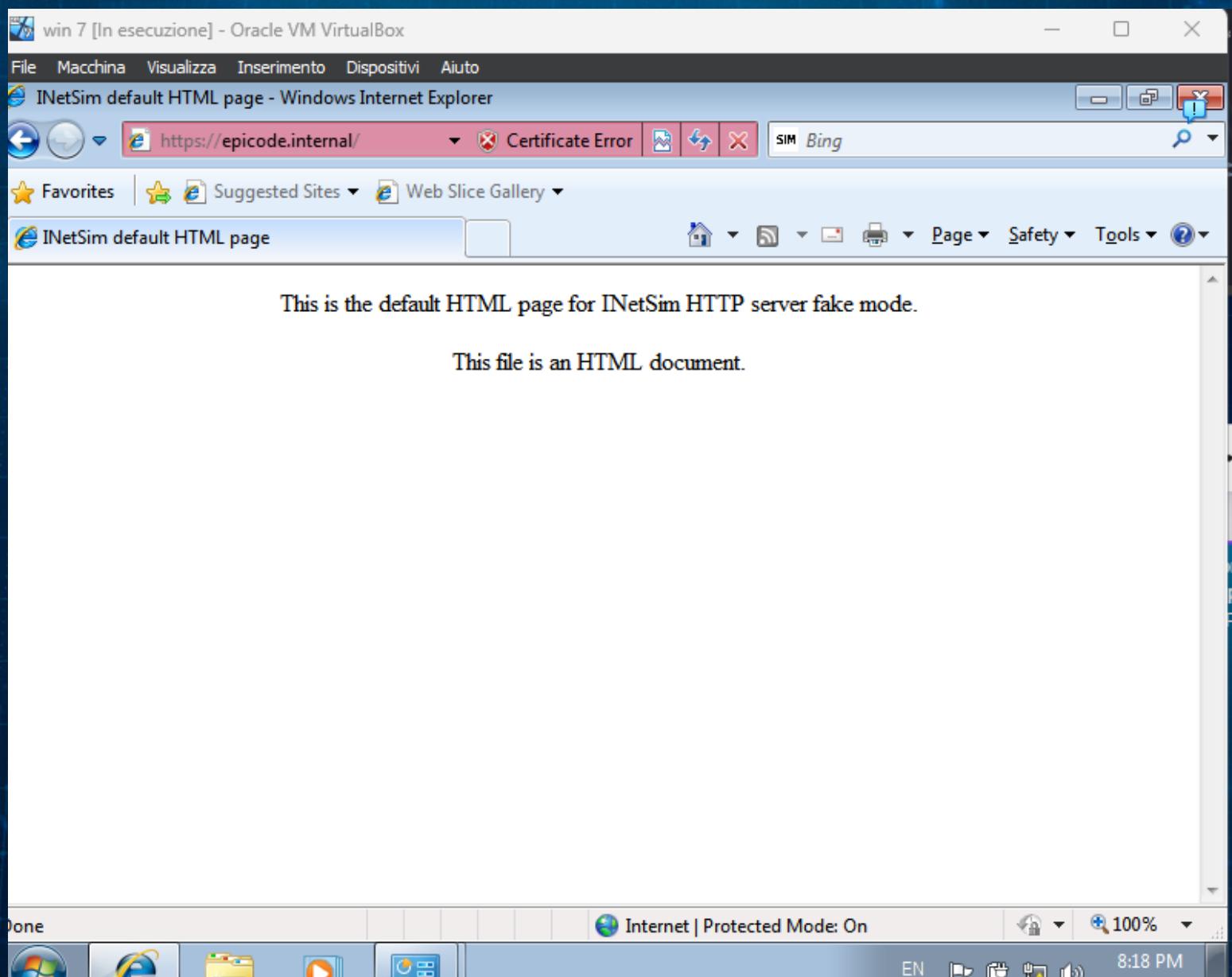
```
File Macchina Visualizza Inserimento Dispositivi Aiuto
andrea@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/andrea/.zsh_history
[andrea@kali)-[~]
$ sudo nano /etc/inetsim/inetsim.conf
[sudo] password for andrea:

[andrea@kali)-[~]
$ sudo inetsim
[sudo] password for andrea:
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 24135) ==
Session ID: 24135
Listening on: 0.0.0.0
Real Date/Time: 2023-11-18 20:09:54
Fake Date/Time: 2023-11-18 20:09:54 (Delta: 0 seconds)
Forking services ...
 * dns_53_tcp_udp - started (PID 24145)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
 * https_443_tcp - started (PID 24147)
 * http_80_tcp - started (PID 24146)
done.
Simulation running.
```

Fatto ciò se tutto sarà settato correttamente attraverso Internet Explorer su Windows 7 possiamo collegarci sia con HTTP che con HTTPS ai seguenti:

- <http://epicode.internal>
- <https://epicode.internal>





Done

Internet | Protected Mode: On

EN

8:18 PM
14.02.2012

Packet Capture con Wireshark

Verifichiamo che i pacchetti tra Windows 7 e Kali trasmettano correttamente attraverso il tool Wireshark effettuando il packet capture attraverso l'interfaccia di rete "eth0"

- Traffico HTTPS:

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

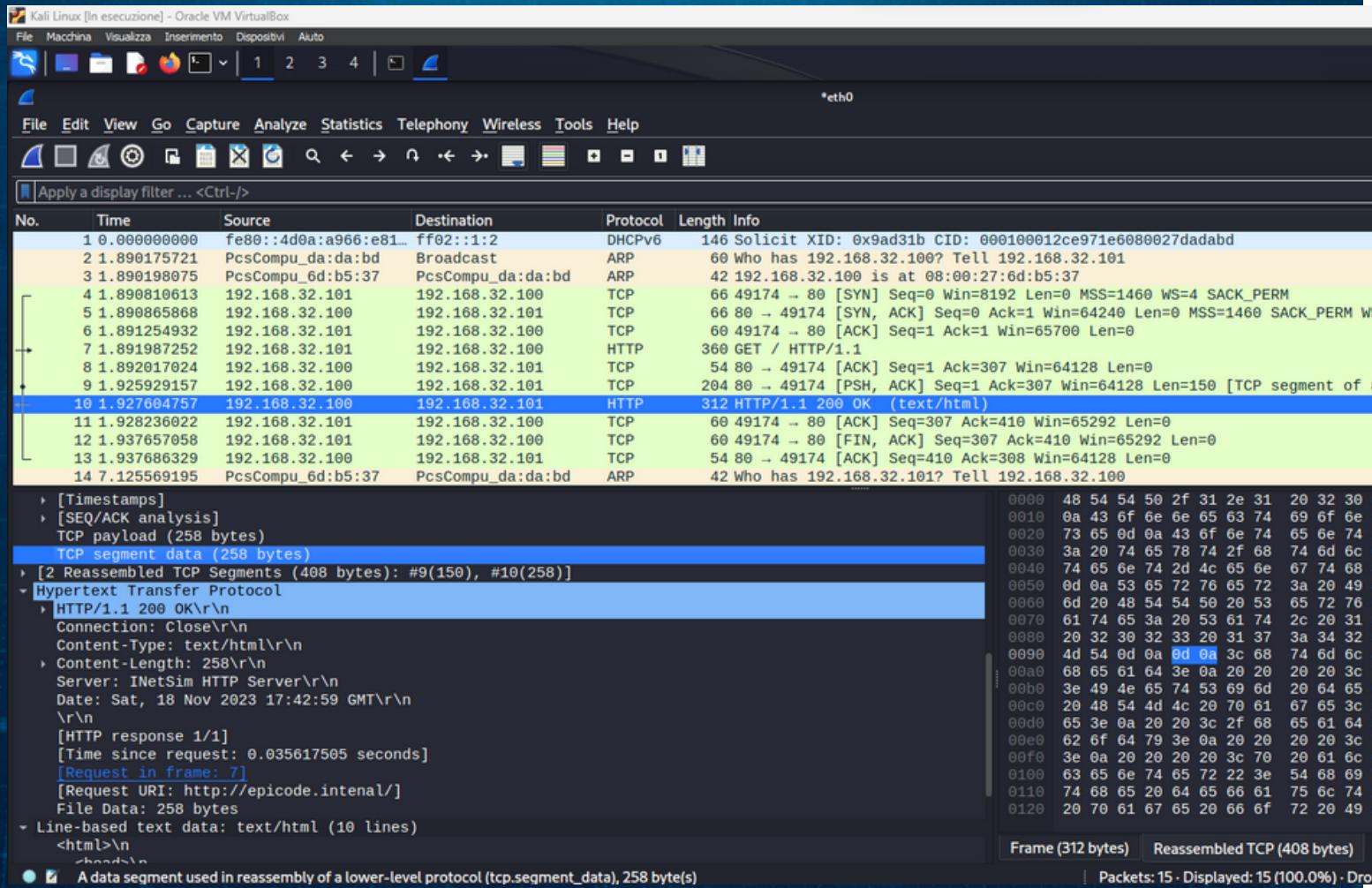
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.32.101	192.168.32.100	TCP	66	49237 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PEE
2	0.000039967	192.168.32.100	192.168.32.101	TCP	66	443 → 49237 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.000422767	192.168.32.101	192.168.32.100	TCP	60	49237 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.001357257	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
5	0.001378197	192.168.32.100	192.168.32.101	TCP	54	443 → 49237 [ACK] Seq=1 Ack=162 Win=64128 Len=0
6	0.026802109	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server Hello
7	0.034258624	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
8	0.038700695	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
9	0.055013685	PcsCompu_da:da:bd	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
10	0.255967004	192.168.32.101	192.168.32.100	TCP	60	49237 → 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0
11	0.943716984	PcsCompu_da:da:bd	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
12	1.944089546	PcsCompu_da:da:bd	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
13	3.201519549	fe80::4d0a:a966:e81... ff02::1:3		LLMNR	84	Standard query 0x35d0 A wpad
14	3.201520140	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x35d0 A wpad

Frame 4: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_da:da:bd (08:00:27:da:da:bd), Dst: PcsCompu_6d:b5:37 (08:00:27:6d:b5:37)
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100
Transmission Control Protocol, Src Port: 49237, Dst Port: 443, Seq: 1, Ack: 1, Len: 161
Transport Layer Security
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f 49 31 4b 97 b5 e4
0060 42 20 10 97 ed 67 41 40
0070 63 e3 6a 36 98 db 85 05
0080 c8 eb 00 18 00 2f 00 35
0090 c0 09 c0 0a 00 32 00 38
00a0 ff 01 00 01 00 00 00 00
00b0 69 63 6f 64 65 2e 69 6e
00c0 00 05 01 00 00 00 00 00
00d0 18 00 0b 00 02 01 00
0000 08 00 27 6d b5 37 08 00
0010 00 c9 04 33 40 00 80 06
0020 20 64 c0 55 01 bb 05 58
0030 40 29 c3 cd 00 00 16 03
0040 01 65 58 fc 6b 30 a1 07
0050 47 4f



Ne protocollo HTTPS i dati sono criptati, infatti possiamo notare la three-way-handshake dove avviene uno scambio di pacchetti TLS che serve per garantire i dati sensibili.

- Traffico HTTP:



Possiamo notare uno scambio di pacchetti ARP. Nel primo pacchetto la macchina windows chiede un messaggio broadcast a tutti i dispositivi della rete, nel secondo Kali risponde di avere l'indirizzo ip richiesto (192.168.32.101)

Successivamente abbiamo la three-hand-shake

Subito dopo abbiamo una richiesta GET Windows 7 a HTTP, con la riposta del codice 200 che conferma la trasmissione a Windows.

Inoltre cliccando sul pacchetto 40 possiamo vedere il contenuto in chiaro alla pagina HTML:

Kali Linux [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
28	8.920047011	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xc0
29	9.024818021	fe80::4d0a:a966:e81...	ff02::1:3	LLMNR	84	Standard query 0xc0
30	9.025729190	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0xc0
31	9.228320815	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<
32	9.978768143	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<
33	10.729284100	192.168.32.101	192.168.32.255	NBNS	92	Name query NB WPAD<
34	11.483941987	192.168.32.101	192.168.32.100	TCP	66	49186 → 80 [SYN] Se
35	11.484072835	192.168.32.100	192.168.32.101	TCP	66	80 → 49186 [SYN, AC
36	11.484371563	192.168.32.101	192.168.32.100	TCP	60	49186 → 80 [ACK] Se
37	11.484371623	192.168.32.101	192.168.32.100	HTTP	271	GET /msdownload/upd
38	11.484427880	192.168.32.100	192.168.32.101	TCP	54	80 → 49186 [ACK] Se
39	11.494170651	192.168.32.100	192.168.32.101	TCP	204	80 → 49186 [PSH, AC
40	11.495466205	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (t
41	11.496506956	192.168.32.101	192.168.32.100	TCP	60	49186 → 80 [ACK] Se
42	11.497093057	192.168.32.101	192.168.32.100	TCP	60	49186 → 80 [FIN, AC
43	11.497107463	192.168.32.100	192.168.32.101	TCP	54	80 → 49186 [ACK] Se
44	11.500705021	Reservato da host	Broadcast	ARP	60	Unk. hex 100 160 20

▶ 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    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>\n    <p align="center">This file is an HTML document.</p>\n  </body>\n</html>\n
```

wireshark_eth0G7RVE2.pcapng Packets: 46 · Displayed: 46