

Presentazione progetto

1- Impostazioni ip dell'host Kali e dell'host Windows7

IP Kali-Linux

```
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
```

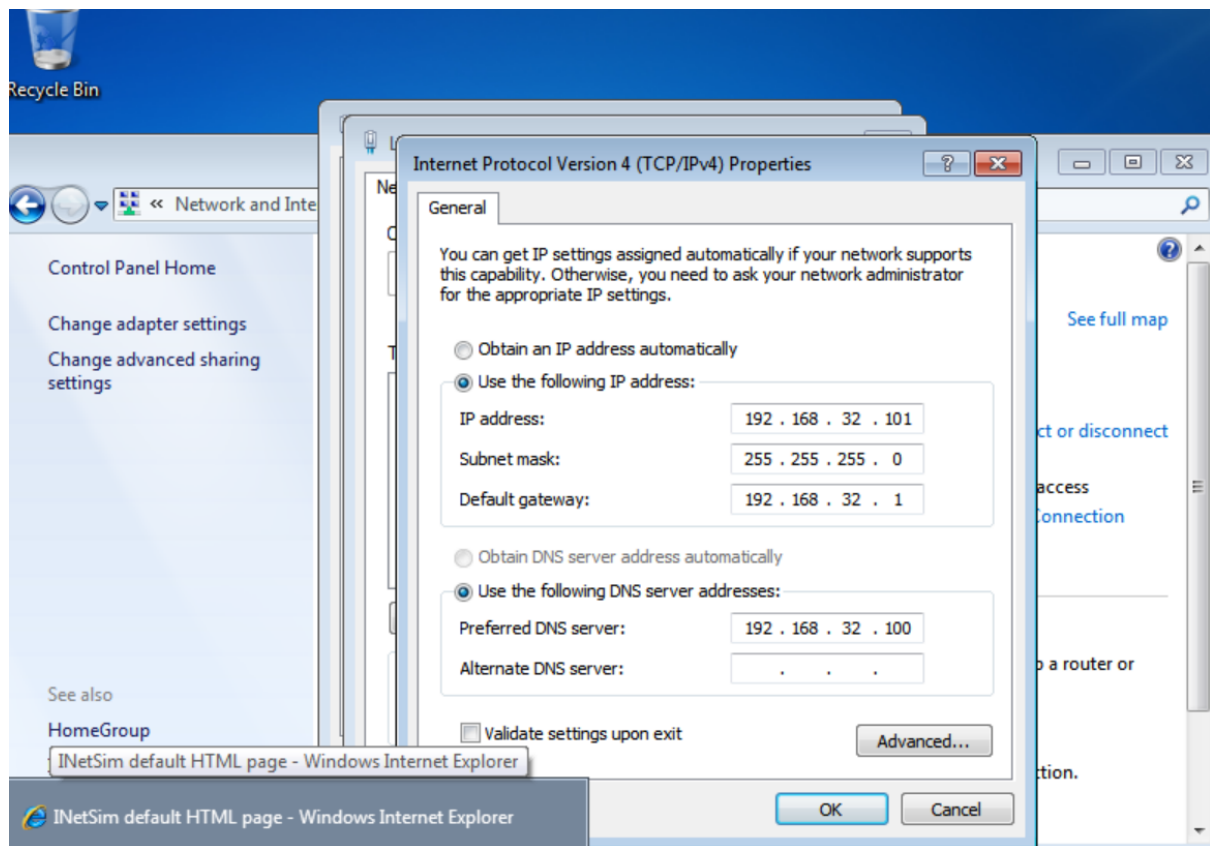
KALI LINUX

"the quieter you become, the more you are able to hear"

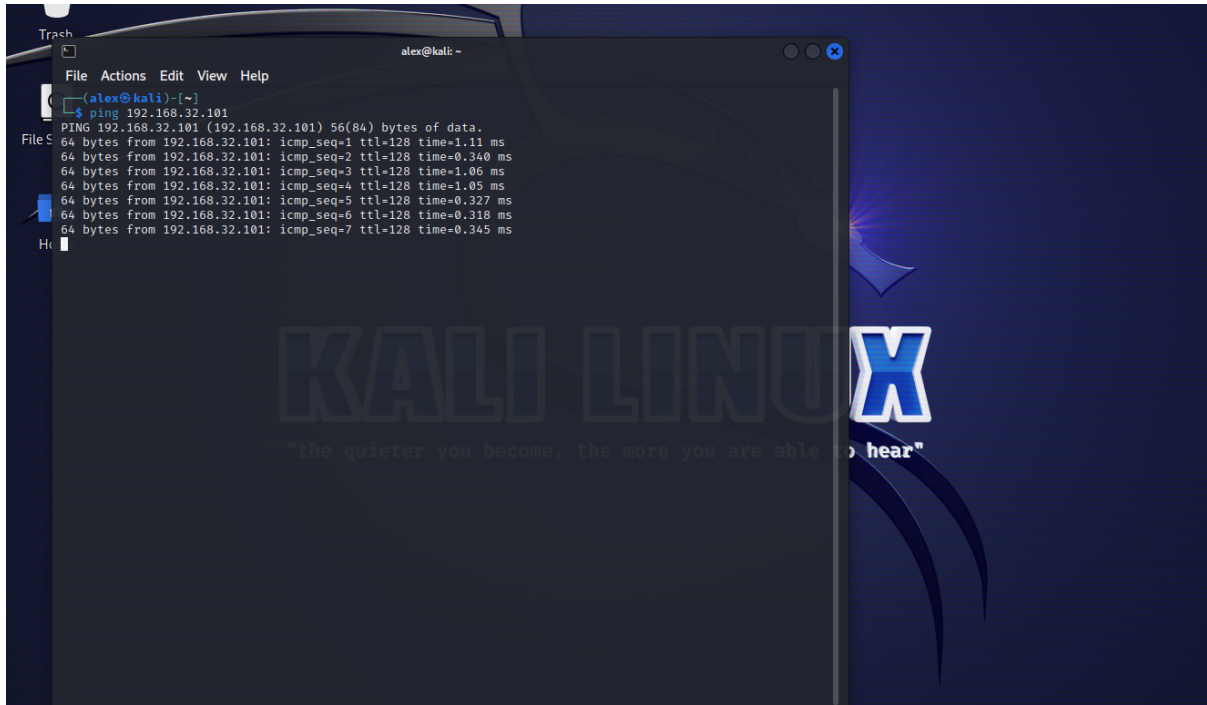
[Read 15 lines]

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

Ip Windows7



2-Dimostrazione che le macchine comunicano tra di loro



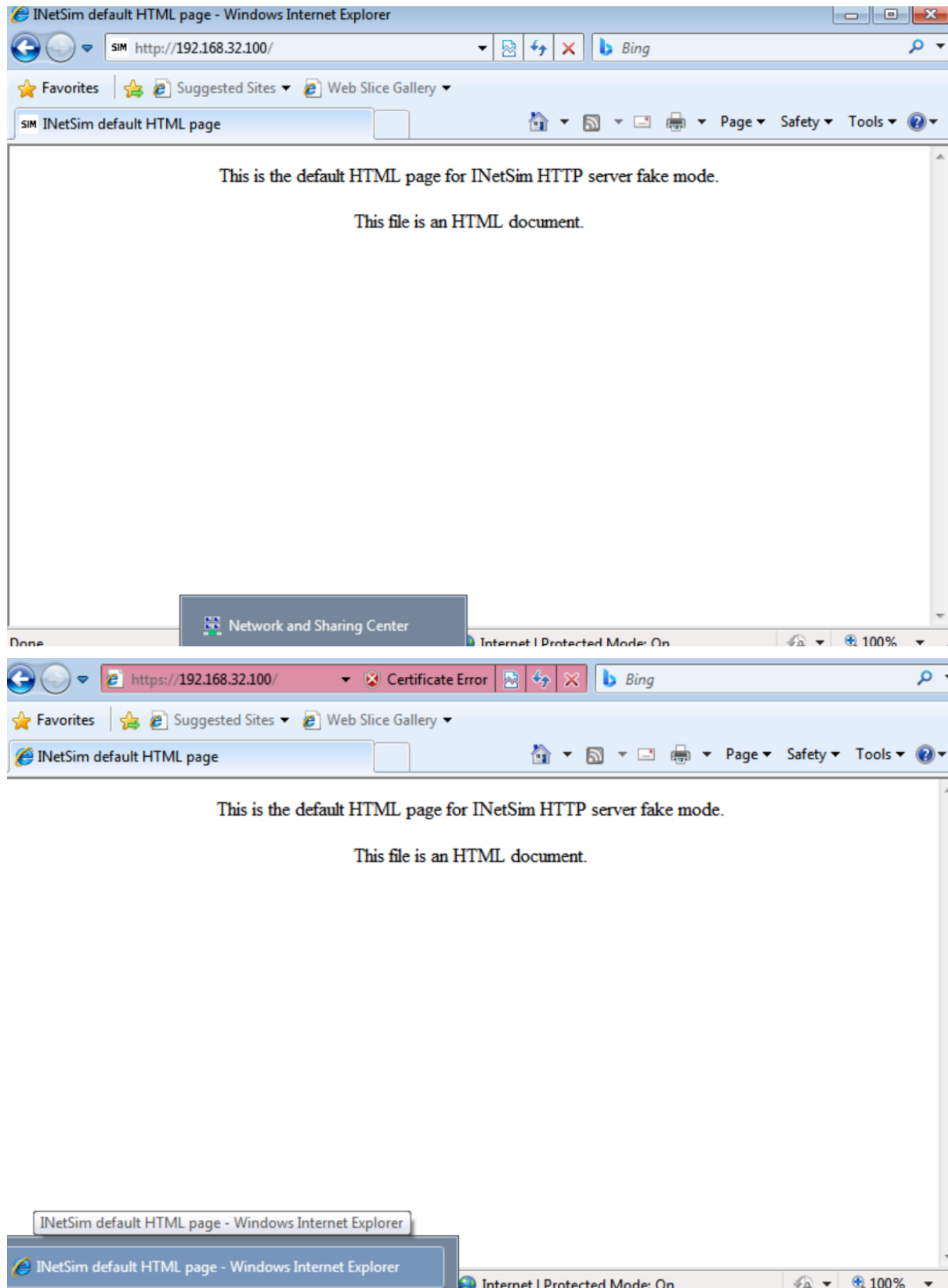
3- Impostazione di netsin : http ,https e dns

```
# 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
```

[Read 1999 lines]

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

4-dimostrazione del tutto: https e http



5-Dimostrazione dei pacchetti intercettati —http non criptato

The screenshot shows a Wireshark capture on the eth0 interface. The packet list displays several TCP and HTTP packets. Packet 13 is selected, showing the reassembled HTTP 200 OK response. The packet details pane shows the 'text/html' content type. The packet bytes pane displays the raw hex and ASCII data of the HTML page, which is a default INetSim page. The status bar indicates 93 packets displayed (10.8%).

No.	Time	Source	Destination	Protocol	Length	Info
5	2.498646768	192.168.32.101	192.168.32.100	TCP	66	49204 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK
6	2.498664485	192.168.32.100	192.168.32.101	TCP	66	80 → 49204 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1
7	2.498987788	192.168.32.101	192.168.32.100	TCP	60	49204 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
8	2.498987835	192.168.32.101	192.168.32.100	HTTP	338	GET / HTTP/1.1
9	2.499027730	192.168.32.100	192.168.32.101	TCP	54	80 → 49204 [ACK] Seq=1 Ack=285 Win=64128 Len=0
10	2.507084599	192.168.32.100	192.168.32.101	TCP	204	80 → 49204 [PSH, ACK] Seq=1 Ack=285 Win=64128 Len=150
13	2.508046593	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
14	2.509068639	192.168.32.101	192.168.32.100	TCP	60	49204 → 80 [ACK] Seq=285 Ack=410 Win=65292 Len=0
15	2.509068676	192.168.32.101	192.168.32.100	TCP	60	49204 → 80 [FIN, ACK] Seq=285 Ack=410 Win=65292 Len=0
16	2.509084908	192.168.32.100	192.168.32.101	TCP	54	80 → 49204 [ACK] Seq=410 Ack=286 Win=64128 Len=0

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</p>\n<p align="center">This file is an HTML document.</p>\n</body>\n</html>\n
```

Frame (312 bytes) Reassembled TCP (408 bytes)

Packets: 93 - Displayed: 10 (10.8%) Profile: Default

* dns_53_tcp_udp - started (PID 35291)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
* http_80_tcp - started (PID 35292)
* https_443_tcp - started (PID 35293)
done.
Simulation running.

—https criptato ,il tutto si nota dal fatto che il contenuto è leggibile

The screenshot shows a Wireshark capture on the eth0 interface. The packet list displays several TLS and TCP packets. Packet 49 is selected, showing the reassembled TLS record. The packet details pane shows the 'Application Data' protocol. The packet bytes pane displays the raw hex and ASCII data of the TLS record, which is encrypted. The status bar indicates 181 packets displayed (8.3%).

No.	Time	Source	Destination	Protocol	Length	Info
8	0.861643013	192.168.32.101	192.168.32.100	TLSv1	190	Client Hello
9	0.861647632	192.168.32.100	192.168.32.101	TCP	54	443 → 49199 [ACK] Seq=1 Ack=137 Win=64128 Len=0
10	0.861358505	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, S
11	0.884748991	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted
12	0.885149836	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
14	1.091547620	192.168.32.101	192.168.32.100	TCP	60	49199 → 443 [ACK] Seq=271 Ack=1379 Win=64320 Len=0
49	15.890523408	192.168.32.101	192.168.32.100	TLSv1	379	Application Data
50	15.896816167	192.168.32.100	192.168.32.101	TLSv1	235	Application Data
51	15.898305349	192.168.32.100	192.168.32.101	TLSv1	384	Application Data, Encrypted Alert
52	15.898759129	192.168.32.101	192.168.32.100	TCP	60	49199 → 443 [ACK] Seq=596 Ack=1891 Win=65700 Len=0

Frame 49: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bit)

Ethernet II, Src: PcsCompu_60:6a:9e (08:00:27:60:6a:9e), Dst: PcsComp

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

Transmission Control Protocol, Src Port: 49199, Dst Port: 443, Seq: 2

Transport Layer Security

TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer P

Content Type: Application Data (23)

Version: TLS 1.0 (0x0301)

Length: 320

Encrypted Application Data: 1035ffff0721e3a2c99414835a824f4d62437

[Application Data Protocol: Hypertext Transfer Protocol]

Payload is encrypted application data (tls.app_data), 320 byte(s)

Packets: 181 - Displayed: 15 (8.3%) Profile: Default

* dns_53_tcp_udp - started (PID 35291)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
* http_80_tcp - started (PID 35292)
* https_443_tcp - started (PID 35293)
done.
Simulation running.

6-MAC-address

Wireshark interface showing network traffic capture on eth0. The packet list displays several ARP and SSDP packets. The selected packet (No. 54) is an ARP request from 192.168.1.56 to 192.168.1.254.

No.	Time	Source	Destination	Protocol	Length	Info
92	44.324356428	PcsCompu_60:6...	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
93	45.536581548	192.168.1.56	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
94	45.537806347	192.168.1.56	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
95	45.916306214	SernetSu_3e:a...	Broadcast	ARP	60	Who has 192.168.1.56? Tell 192.168.1.254
96	46.539092537	192.168.1.56	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
97	46.539092727	192.168.1.56	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
98	47.540484476	192.168.1.56	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
99	47.540485006	192.168.1.56	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
100	48.540875045	192.168.1.56	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
101	48.540875584	192.168.1.56	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

Frame 54: 54 bytes on wire (432 bits), 54 bytes captured (432 bit) on interface eth0

Ethernet II, Src: PcsCompu_8d:45:28 (08:00:27:8d:45:28), Dst: PcsCompu_60:6a:9e (08:00:27:8d:45:28)

Source: PcsCompu_8d:45:28 (08:00:27:8d:45:28)

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: 49199, Seq: 35291, Win: 0, Len: 0

Packets: 101 - Displayed: 101 (100.0%) Profile: Default

```
* dns_53_tcp_udp - started (PID 35291)
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.
* http_80_tcp - started (PID 35292)
* https_443_tcp - started (PID 35293)
done.
Simulation running.
```