

Ho impostato la macchina Kali Linux(server) e la macchina Windows7(client) sulla stessa rete configurandola manualmente.

Su Kali ho modificato idirizzo ip, subnet, e gateway entrando da terminal con 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/*

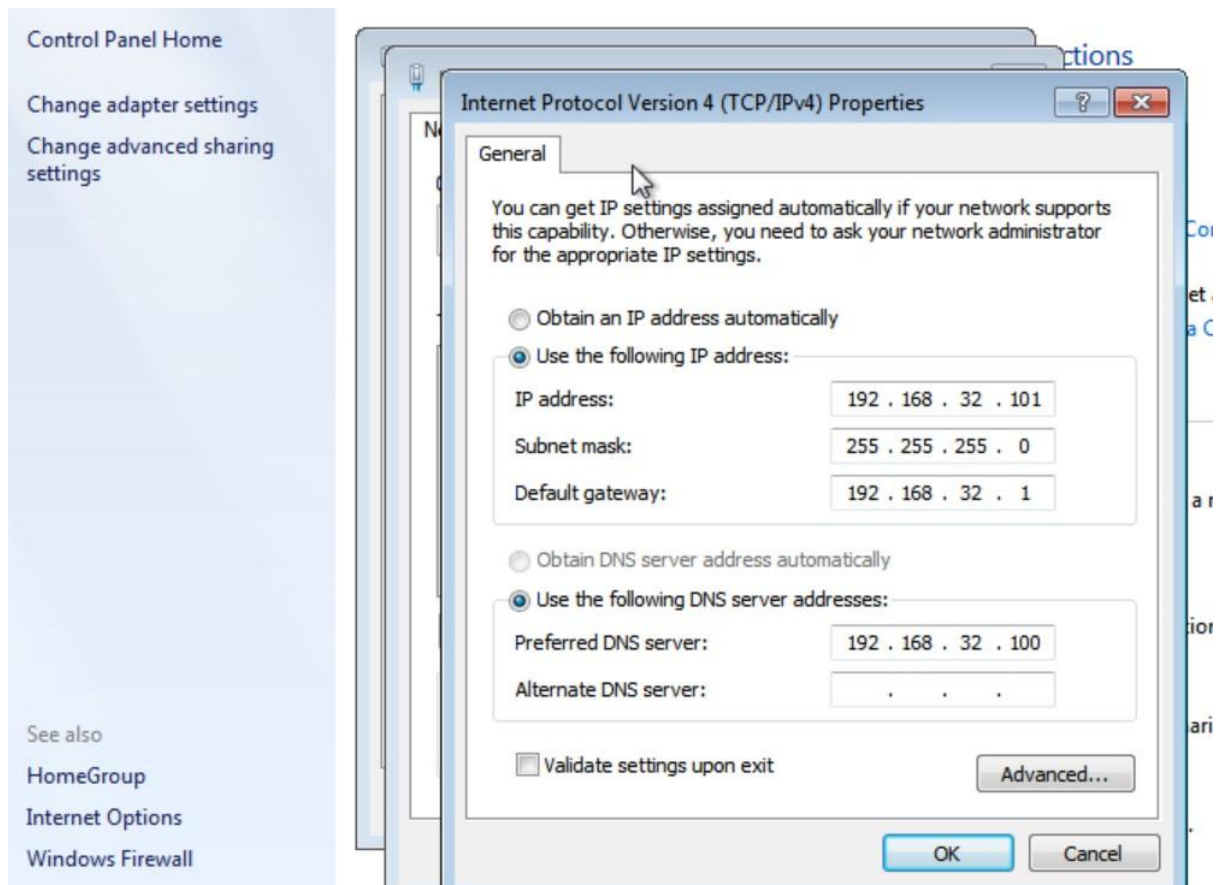
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.32.100/24
gateway 192.168.32.1
```

ifconfig, check delle modifiche

```
(simone@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:feaa:dfff prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:aa:df:ff txqueuelen 1000 (Ethernet)
    RX packets 7 bytes 584 (584.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 2448 (2.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Lo stesso su windows7 via interfaccia grafica, impostando ip di Kali come DNS server



ipconfig da terminale

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ vboxuser>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : broadband
    Link-local IPv6 Address . . . . . : fe80::c438:31c0:ea30:e2dd%11
    IPv4 Address. . . . . : 192.168.32.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.32.1

Tunnel adapter isatap.{F34D6E70-3AB2-4C98-9873-A5278F0675AF}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : broadband
```

Successivamente ho impostato l' Honey pot Inetsim su Kali, macchina server, in modo da creare un ambiente di laboratorio virtuale per simulare i servizi DNS, Http, 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
```

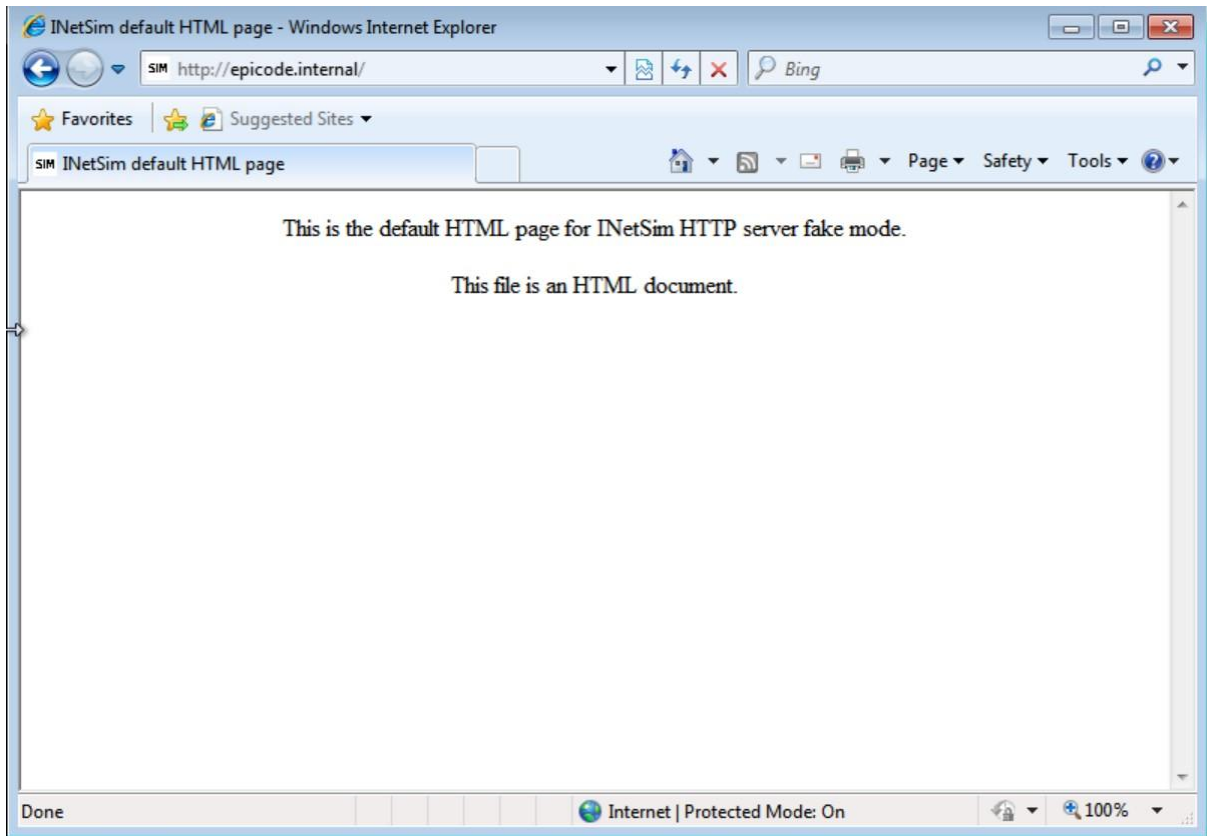
```
# service_bind_address enable BIND at /usr/share/ports/www/
# * http_80_tcp - started (PID 9737)
# IP address to bind services to (9738)
# none
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100
```

```
dns_default_ip 192.168.32.100 # Nathan's Eckert & Thomas Hunt
```

```
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
dns_static epicode.internal 192.168.32.100
```

Il dns andrà a tradurre il nome di dominio “epicode.internal con l’indirizzo ip della macchina server.

Utilizzando il browser del client Windows7 ho fatto una richiesta della pagina epicode.internal con protocollo http ricevendo al pagina html.



Sulla macchina Linux ho potuto visionare i pacchetti con WireShark andando a visualizzare l'indirizzo MAC della macchina client.

6	3.515140600	Technico_b1:25:38	Broadcast	ARP	60 Who has 192.168.1.2147
7	4.467221117	PcsCompu_b7:32:55	Broadcast	ARP	60 Who has 192.168.32.100
8	4.467234197	PcsCompu_aa:df:ff	PcsCompu_b7:32:55	ARP	42 192.168.32.100 is at 6
9	4.467769814	192.168.32.101	192.168.32.100	TCP	66 49193 → 80 [SYN] Seq=6
10	4.467788268	192.168.32.100	192.168.32.101	TCP	66 80 → 49193 [SYN, ACK]
11	4.468013691	192.168.32.101	192.168.32.100	TCP	60 49193 → 80 [ACK] Seq=1
12	4.468225923	192.168.32.101	192.168.32.100	HTTP	340 GET / HTTP/1.1
13	4.468232438	192.168.32.100	192.168.32.101	TCP	54 80 → 49193 [ACK] Seq=1
14	4.484982566	192.168.32.100	192.168.32.101	TCP	204 80 → 49193 [PSH, ACK]
15	4.486297786	192.168.32.100	192.168.32.101	HTTP	312 HTTP/1.1 200 OK (text
16	4.486699725	192.168.32.101	192.168.32.100	TCP	60 49193 → 80 [ACK] Seq=2
17	4.487105595	192.168.32.101	192.168.32.100	TCP	60 49193 → 80 [FIN, ACK]
18	4.487117312	192.168.32.100	192.168.32.101	TCP	54 80 → 49193 [ACK] Seq=4
19	5.172741949	fe80::c438:31c0:ea3...	ff02::16	ICMPv6	90 Multicast Listener Rep
20	6.711026160	192.168.1.157	224.0.0.251	IGMPv2	60 Membership Report grou
21	6.711026462	fe80::e9ad:6af4:ebb...	ff02::16	ICMPv6	90 Multicast Listener Rep

Frame 12: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface eth0, id 0  
 Ethernet II, Src: PcsCompu\_b7:32:55 (08:00:27:b7:32:55), Dst: PcsCompu\_aa:df:ff (08:00:27:aa:df:ff)  
 Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100  
 Transmission Control Protocol, Src Port: 49193, Dst Port: 80, Seq: 1, Ack: 1, Len: 286  
 Hypertext Transfer Protocol

Physical Address. . . . . : 08-00-27-B7-32-55  
 DHCP Enabled. . . . . : No



Inoltre si può notare che sulla richiesta GET ,utilizzando il protocollo http, posso visualizzare delle informazioni in chiaro.

The image shows a Wireshark network traffic capture on the interface eth0. The packet list pane displays a series of packets, with packet 12 highlighted. This packet is an HTTP GET request from 192.168.32.101 to 192.168.32.100. The packet details pane shows the structure of the HTTP request, including the GET method, the path /, and various headers like User-Agent (Mozilla/4.0) and Accept-Charset (\*/\*).

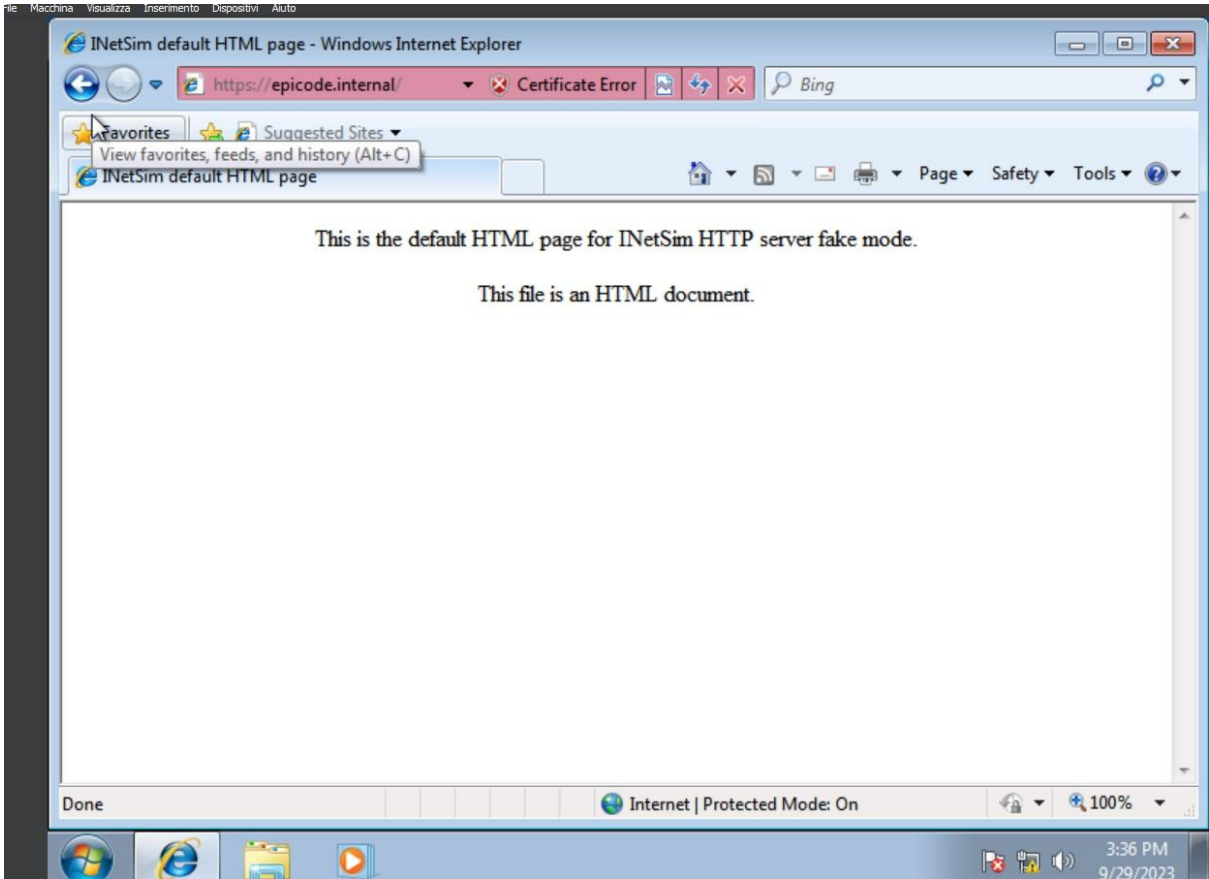
No.	Time	Source	Destination	Protocol	Length	Info
6	3.515140600	Technico_b1:25:38	Broadcast	ARP	60	Who has 192.168.1.214?
7	4.467221117	PcsCompu_b7:32:55	Broadcast	ARP	60	Who has 192.168.32.100?
8	4.467234197	PcsCompu_aa:df:ff	PcsCompu_b7:32:55	ARP	42	192.168.32.100 is at 08:00:27:aa:df:ff
9	4.467769814	192.168.32.101	192.168.32.100	TCP	66	49193 → 80 [SYN] Seq=604000000
10	4.467788268	192.168.32.100	192.168.32.101	TCP	66	80 → 49193 [SYN, ACK] Seq=604000000
11	4.468013691	192.168.32.101	192.168.32.100	TCP	60	49193 → 80 [ACK] Seq=604000000
12	4.468225923	192.168.32.101	192.168.32.100	HTTP	340	GET / HTTP/1.1
13	4.468232438	192.168.32.100	192.168.32.101	TCP	54	80 → 49193 [ACK] Seq=604000000
14	4.484982566	192.168.32.100	192.168.32.101	TCP	204	80 → 49193 [PSH, ACK] Seq=604000000
15	4.486297786	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK (text/html)
16	4.486699725	192.168.32.101	192.168.32.100	TCP	60	49193 → 80 [ACK] Seq=604000000
17	4.487105595	192.168.32.101	192.168.32.100	TCP	60	49193 → 80 [FIN, ACK] Seq=604000000
18	4.487117312	192.168.32.100	192.168.32.101	TCP	54	80 → 49193 [ACK] Seq=604000000
19	5.172741949	fe80::c438:31c0:ea3...	ff02::1:6	ICMPv6	90	Multicast Listener Report
20	6.711026160	192.168.1.157	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
21	6.711026462	fe80::e9ad:6af4:ebb...	ff02::1:6	ICMPv6	90	Multicast Listener Report

Frame 12: 340 bytes on wire (2720 bits) captured on interface eth0  
Ethernet II, Src: PcsCompu\_aa:df:ff, Dst: 192.168.32.100  
Internet Protocol Version 4, Src: 192.168.32.101, Dst: 192.168.32.100  
Transmission Control Protocol, Src Port: 49193, Dst Port: 80  
Hypertext Transfer Protocol

0000 08 00 27 aa df ff 08 00 27 b7 32 55 08 00 45 00 .....

Packets: 21 · Displayed: 21 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Mentre se vado a utilizzare il protocollo https per richiedere la pagina html...



posso notare con Wireshark che il pacchetto è criptato attraverso il protocollo TLSv1 che fa da tunnel alle informazioni.

No.	Time	Source	Destination	Protocol	Length	Info
49	26.954454887	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
50	26.954461984	192.168.32.100	192.168.32.101	TCP	54	443 → 49196 [ACK] Seq=
51	26.984100914	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certific
52	26.989874625	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, C
53	26.990225681	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Er
54	26.993662305	192.168.32.101	192.168.32.100	TCP	60	49196 → 443 [FIN, ACK]
55	26.993738938	192.168.32.100	192.168.32.101	TLSv1	91	Encrypted Alert
56	26.994843906	192.168.32.101	192.168.32.100	TCP	60	49196 → 443 [RST, ACK]
57	26.994844047	192.168.32.101	192.168.32.100	TCP	66	49197 → 443 [SYN] Seq=
58	26.994864084	192.168.32.100	192.168.32.101	TCP	66	443 → 49197 [SYN, ACK]
59	26.998374879	192.168.32.101	192.168.32.100	TCP	60	49197 → 443 [ACK] Seq=
60	26.998375009	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
61	26.998399016	192.168.32.100	192.168.32.101	TCP	54	443 → 49197 [ACK] Seq=
62	27.022489158	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certific
63	27.027672756	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, C
64	27.028148029	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Er

▶ Frame 55: 91 bytes on

▶ Ethernet II, Src: PcsC

▶ Internet Protocol Vers

▶ Transmission Control F

▶ Transport Layer Securi

0000 08 00 27 b7 32 55 08 00 27 aa df ff 08 00 45 00 ..'.2U..'....E.

0010 00 4d 0d 92 40 00 40 06 6a ff c0 a8 20 64 c0 a8 .M..@.@.j...d..

0020 20 65 01 bb c0 2c f5 ac df 18 c8 fe 10 30 50 18 e... ..0P.

0030 01 f5 c2 59 00 00 15 03 01 00 20 a3 91 df a8 6a ...Y.....j

0040 22 22 a7 e6 28 92 d8 87 a6 86 d7 59 49 69 a2 8d ""..(.....YIi..

0050 76 6b 49 f9 e5 96 de 2f 57 ff 3e vkI.... / W->