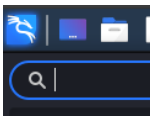
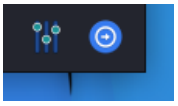
CREAZIONE DI UN SERVER HTTP, HTTPS E DNS

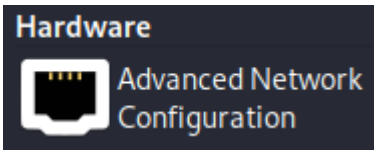
Per questa prova bisogna cambiare gli IP della macchina win7 e kali nei seguenti IP.
Kali: 192.168.32.100
WIN7: 192.168.32.101

Come cambiare gli IP:
Partendo da kali apriamo il menu a tendina e andiamo su impostazioni

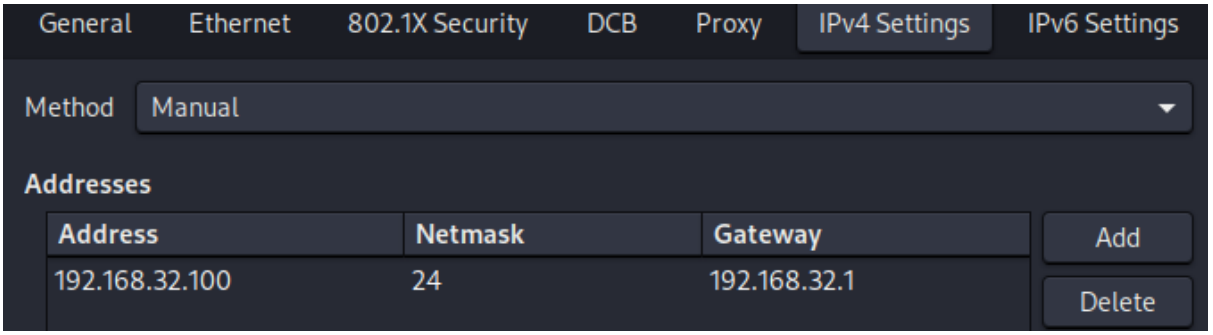




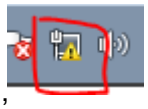
Poi cliccare su



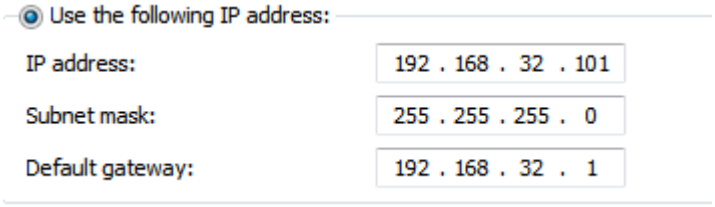
e impostare l'IP qui



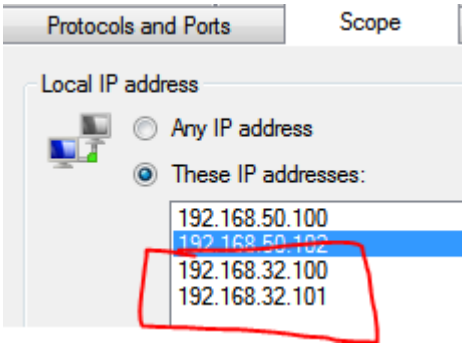
Per cambiare l'IP su win7 andiamo in basso a destra,

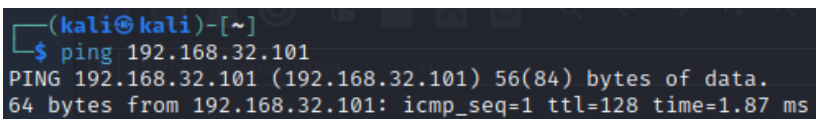


clicchiamo sopra e entriamo nelle impostazioni di rete, selezioniamo Change network adapter settings e sulle proprieta' della scheda di rete entriamo in IPv4 ed cambiamo il nuovo IP



Su win7 dobbiamo aggiungere prima le regola al firewall dei nuovi indirizzi IP:
Aprendo le impostazioni dei firewall andiamo sempre su Inbound Rules e apriamo la regola che abbiamo creato l'ultima volta, poi andando su Scope possiamo aggiungere nuovi indirizzi IP come qui sotto. E di seguito il ping per verificare il tutto





AVVIO E CONFIGURAZIONE SERVER HTTP, HTTPS E DNS

Apriamo la console di kali e andiamo sulle impostazioni di InetSim con il seguente comando

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/inetsim/inetsim.conf
```

Entriamo nelle impostazioni e aggiungiamo questi parametri
service_bind_address 192.168.32.100
dns_static epicode.internal 192.168.32.100

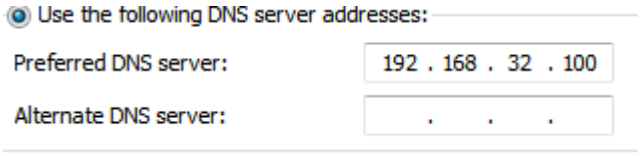
```
# Default: 127.0.0.1
#
#service_bind_address 10.10.10.1
service_bind_address 192.168.32.100
```

```
#dns_static ftp.bar.net 10.10.20.30
dns_static epicode.internal 192.168.32.100
```

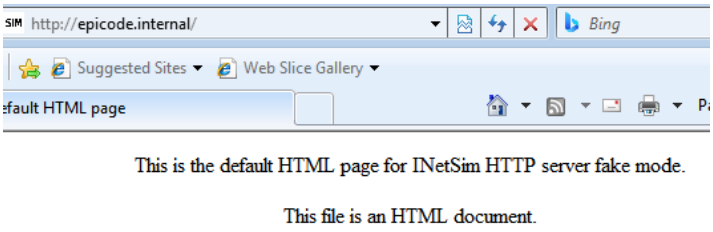
La prima opzione serve a mettere in locale il server http\https sull'IP di kali e la seconda serve ad aggiungere una nuova voce al server DNS, in questo cosa dice che epicode.internal e' associato all'IP 192.168.32.100.
Salviamo tutto e avviamo INetSim con il seguente comando: sudo inetsim

```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
```

Ora andiamo su win7 aggiungiamo nelle impostazioni di rete il server DNS di kali



Apriamo il browser e cerchiamo epicode.internal e vedremo che lo risolvera' in automatico grazie al nostro servizio DNS attivo da kali\inetsim.



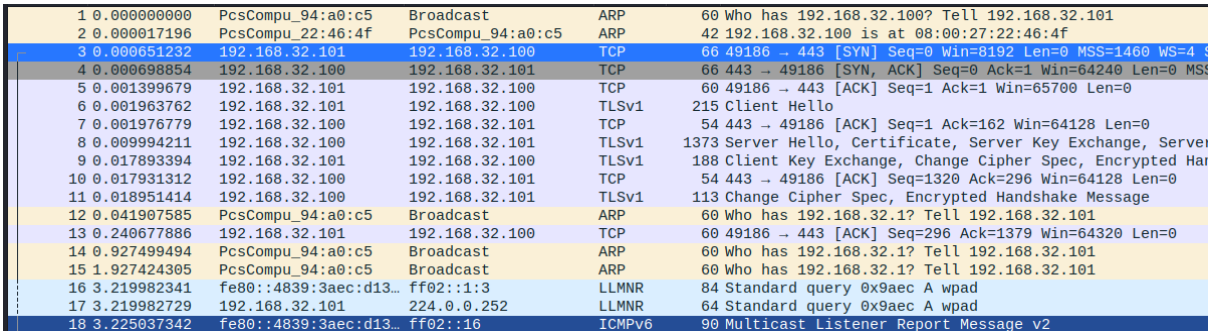
Possiamo anche aprirlo in HTTPS

CATTURA PACCHETTI CON WIRESHARK

Su kali apriamo wireshark ed incominciamo ad ascoltare su tutte le schede di rete, mentre su win7 ricarichiamo la pagina in modo tale da effettuare nuovamente l'accesso.
Questi saranno i pacchetti che vedremo su wireshark

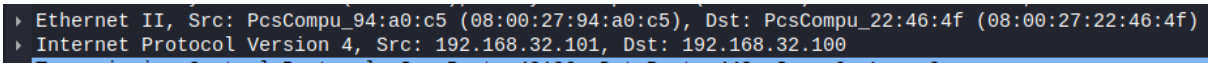
1	0.000000000	PcsCompu_94:a0:c5	Broadcast	ARP	60	Who has 192.168
2	0.000016979	PcsCompu_22:46:4f	PcsCompu_94:a0:c5	ARP	42	192.168.32.100
3	0.000746029	192.168.32.101	192.168.32.100	TCP	66	49185 → 80 [SYN
4	0.000810497	192.168.32.100	192.168.32.101	TCP	66	80 → 49185 [SYN
5	0.001495968	192.168.32.101	192.168.32.100	TCP	60	49185 → 80 [ACK
6	0.002045841	192.168.32.101	192.168.32.100	HTTP	361	GET / HTTP/1.1
7	0.002059166	192.168.32.100	192.168.32.101	TCP	54	80 → 49185 [ACK
8	0.025036285	192.168.32.100	192.168.32.101	TCP	204	80 → 49185 [PSH
9	0.028525418	192.168.32.100	192.168.32.101	HTTP	312	HTTP/1.1 200 OK
10	0.029231701	192.168.32.101	192.168.32.100	TCP	60	49185 → 80 [ACK
11	0.029619862	192.168.32.101	192.168.32.100	TCP	60	49185 → 80 [FIN
12	0.029637877	192.168.32.100	192.168.32.101	TCP	54	80 → 49185 [ACK
13	5.072978498	PcsCompu_22:46:4f	PcsCompu_94:a0:c5	ARP	42	Who has 192.168
14	5.073504509	PcsCompu_94:a0:c5	PcsCompu_22:46:4f	ARP	60	192.168.32.101

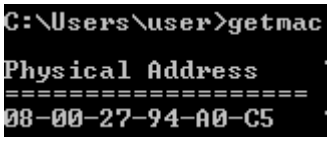
mentre questi entrando con l'https che sono molti di piu' infatti in immagine non ci stanno

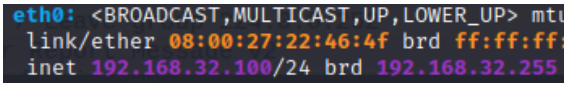


1	0.000000000	PcsCompu_94:a0:c5	Broadcast	ARP	60	Who has 192.168.32.100? Tell 192.168.32.101
2	0.000017196	PcsCompu_22:46:4f	PcsCompu_94:a0:c5	ARP	42	192.168.32.100 is at 08:00:27:22:46:4f
3	0.000651232	192.168.32.101	192.168.32.100	TCP	66	49186 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
4	0.000698854	192.168.32.100	192.168.32.101	TCP	66	443 → 49186 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS
5	0.001399679	192.168.32.101	192.168.32.100	TCP	60	49186 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
6	0.001963762	192.168.32.101	192.168.32.100	TLSv1	215	Client Hello
7	0.001976779	192.168.32.100	192.168.32.101	TCP	54	443 → 49186 [ACK] Seq=1 Ack=162 Win=64128 Len=0
8	0.009994211	192.168.32.100	192.168.32.101	TLSv1	1373	Server Hello, Certificate, Server Key Exchange, Server
9	0.017893394	192.168.32.101	192.168.32.100	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Har
10	0.017931312	192.168.32.100	192.168.32.101	TCP	54	443 → 49186 [ACK] Seq=1320 Ack=296 Win=64128 Len=0
11	0.018951414	192.168.32.100	192.168.32.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
12	0.041907585	PcsCompu_94:a0:c5	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
13	0.240677886	192.168.32.101	192.168.32.100	TCP	60	49186 → 443 [ACK] Seq=296 Ack=1379 Win=64320 Len=0
14	0.927499494	PcsCompu_94:a0:c5	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
15	1.927424305	PcsCompu_94:a0:c5	Broadcast	ARP	60	Who has 192.168.32.1? Tell 192.168.32.101
16	3.219982341	fe80::4839:3aec:d13…	ff02::1:3	LLMNR	84	Standard query 0x9aec A wpad
17	3.219982729	192.168.32.101	224.0.0.252	LLMNR	64	Standard query 0x9aec A wpad
18	3.225037342	fe80::4839:3aec:d13…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

Le differenze tra i due sono chiare, sull'http abbiamo i protocolli ARP, TCP e HTTP mentre su https ci sono i protocolli TLS al posto dei HTTPper la crittografia come possiamo vedere. Qui sotto aprendo il pacchetto TCP o TLS possiamo vedere i 2 IP e MACaddress delle 2 macchine



Il primo e' win7 

l'altro kali 

Anche aprendo un pacchetto TPC dalla scansione in http possiamo vedere i MAC e gli IP.