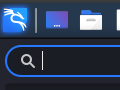
CREAZIONE DI UN SERVER HTTP, HTTPS E DNS

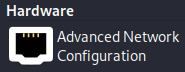
Per questa prova bisogna cambiare gli IP della macchina win7 e kali nei seguenti IP.

Kali: 192.168.32.100

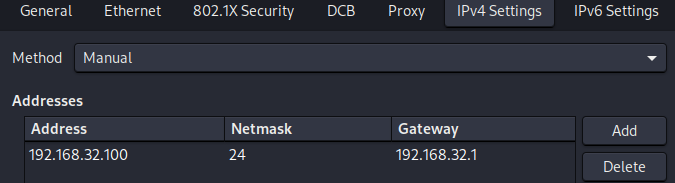
WIN7: 192.168.32.101



**Come cambiare gli IP:**

Partendo da kali apriamo il menu a tendina e andiamo su impostazioni

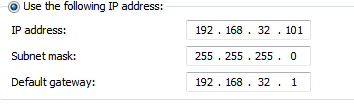
Poi cliccare su

e impostare l’IP qui

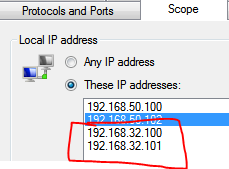
Per cambiare l’IP su win7 andiamo in basso a destra,

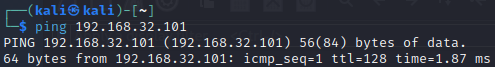
clicchiamo sopra e entriamo nelle impostazioni di rete,

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

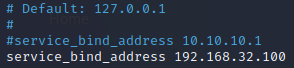
Apriamo la console di kali e andiamo sulle impostazioni di InetSim con il seguente comando



Entriamo nelle impostazioni e aggiungiamo questi parametri

service\_bind\_address 192.168.32.100

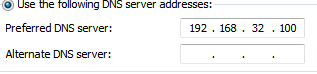
dns\_static epicode.internal 192.168.32.100



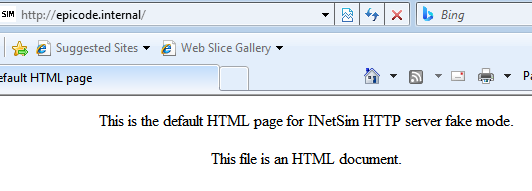
La prima opzione serve a mettere in locale il server http\https sull’IP di kali e la seconda serve ad aggiungere una nuova voce al server DNS, in questo cosa dice che epicode.internal e’ associato all’IP 192.168.32.100.

Salviamo tutto e avviamo INetSim con il seguente comando: sudo inetsim

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.

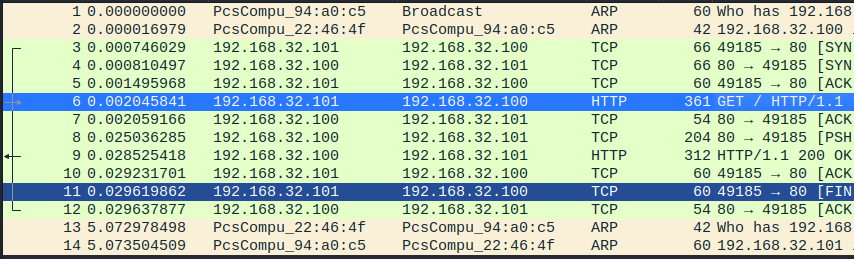


Possiamo anche aprirlo in HTTPS

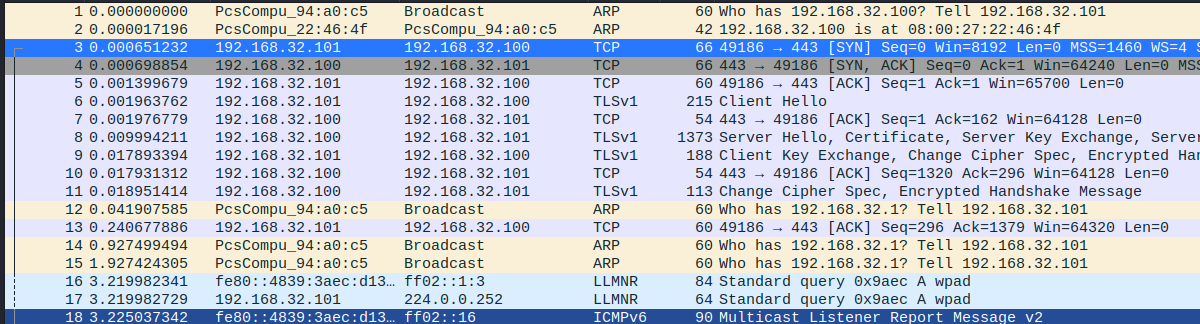
CATTURA PACCHETTI CON WIRESHARK

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

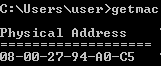


mentre questi entrando con l’https che sono molti di piu’ infatti in immagine non ci stanno



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.