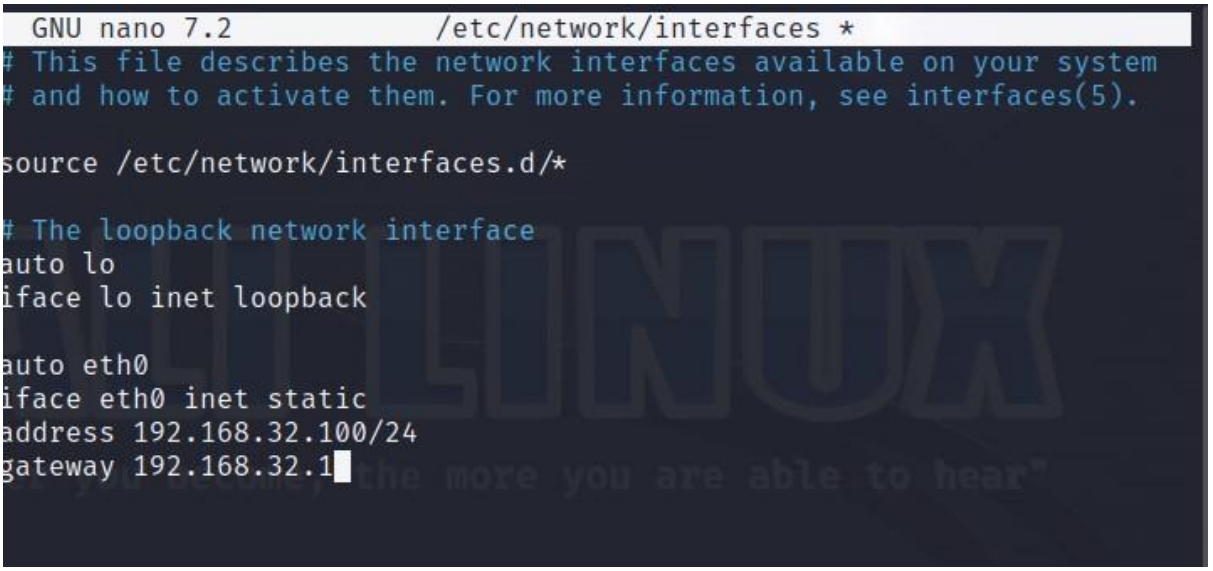
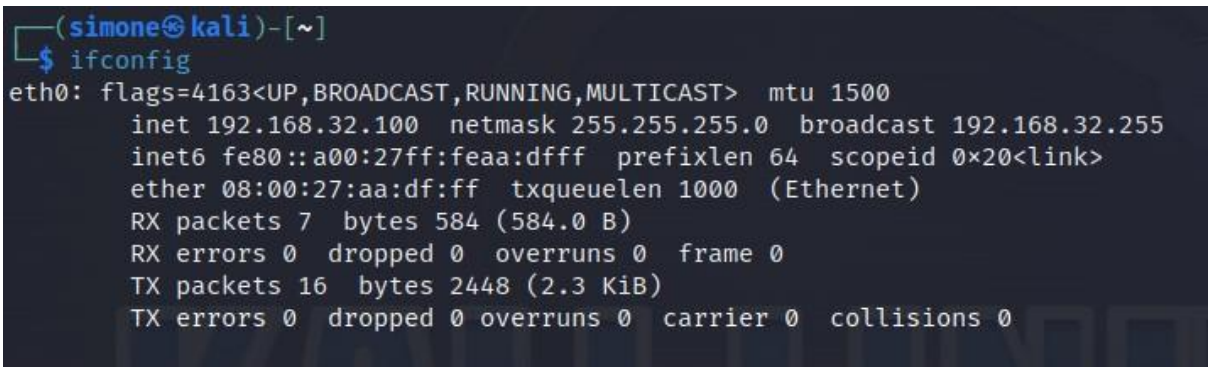
Simone Mininni
Relazione Progetto Epicode S1_L5

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

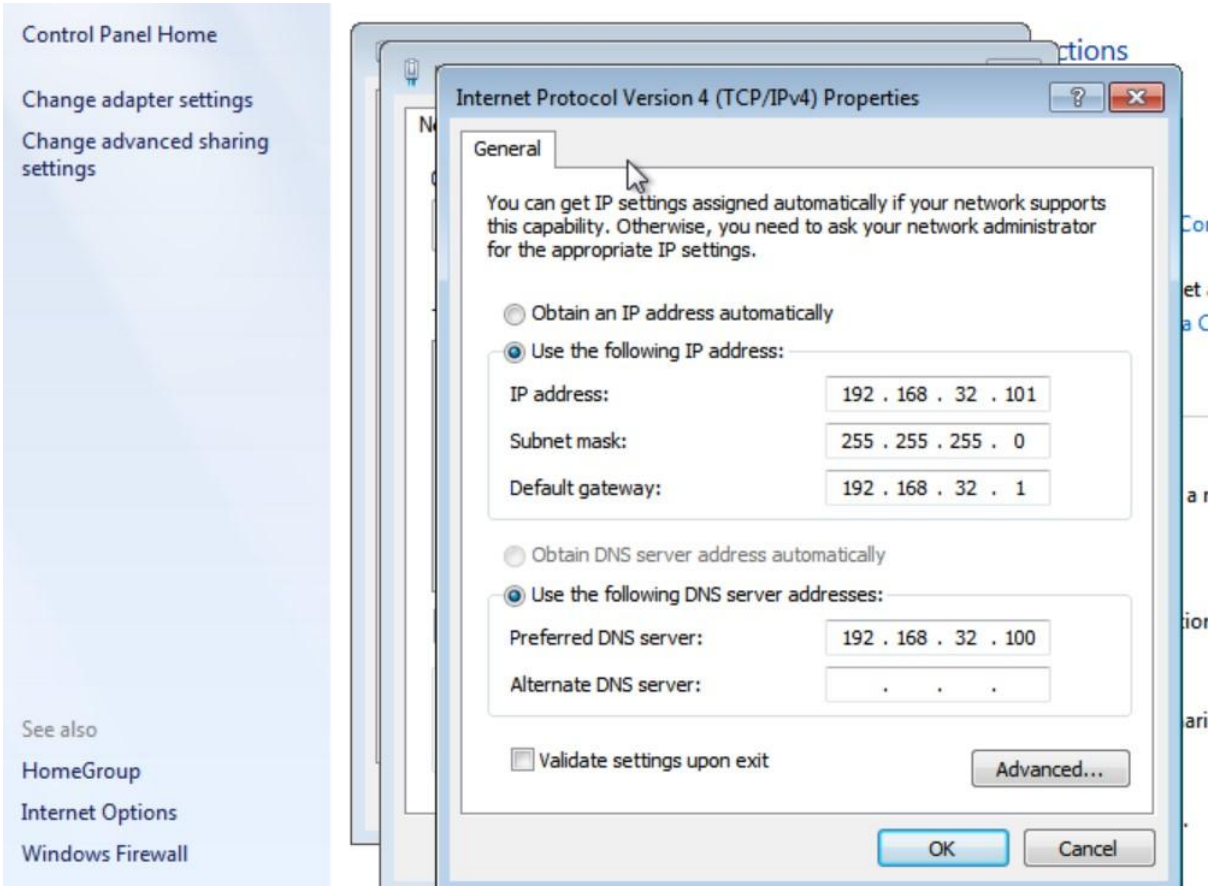
Su Kali ho modificato idirizzo ip, subnet, e gateway entrando da terminal con il comando sudo nano /etc/network/interfaces



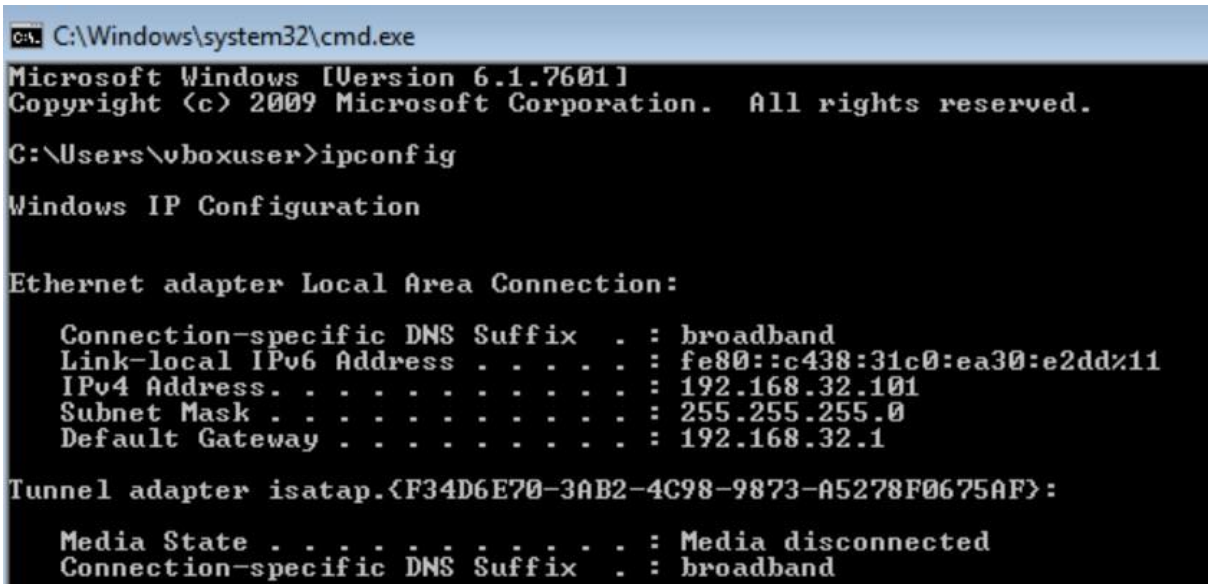
ifconfig, check delle modifiche



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



ipconfig da terminale



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
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100
```

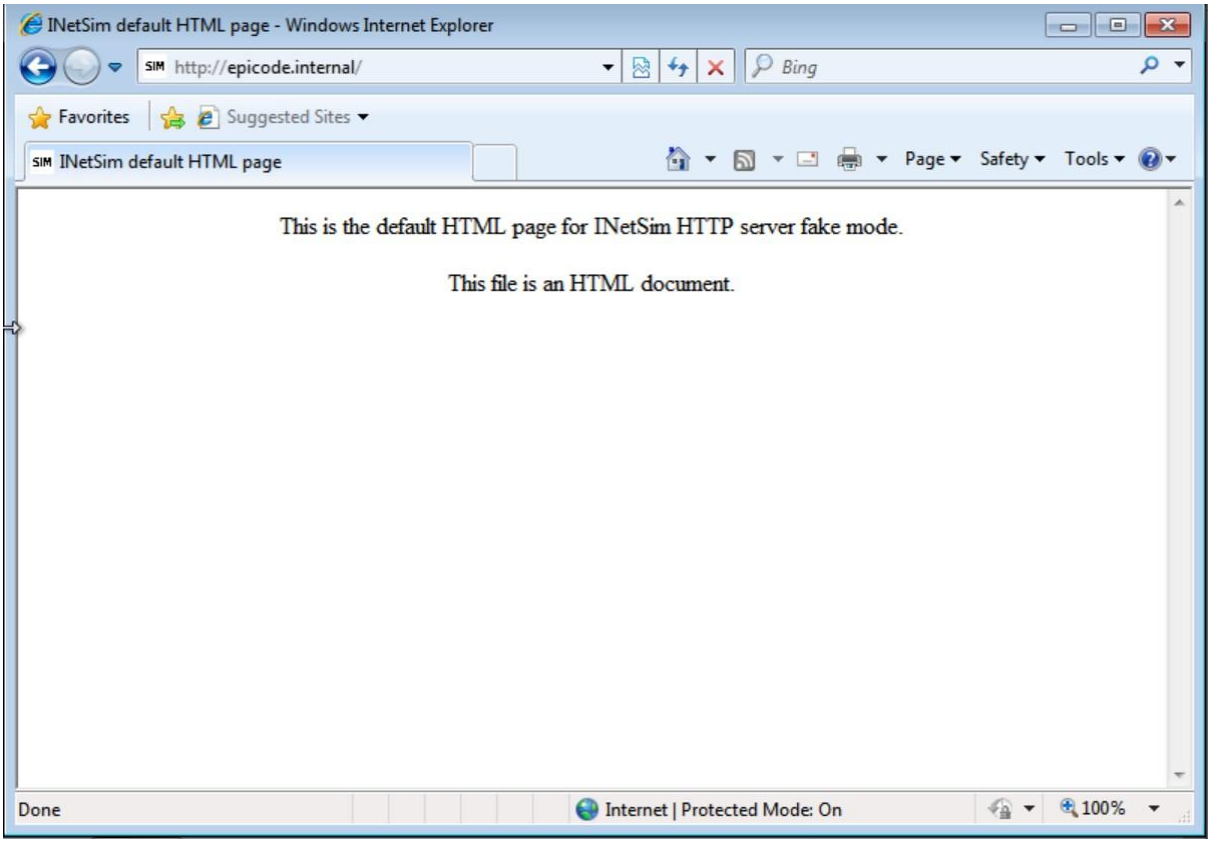
```
dns_default_ip 192.168.32.100
```

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

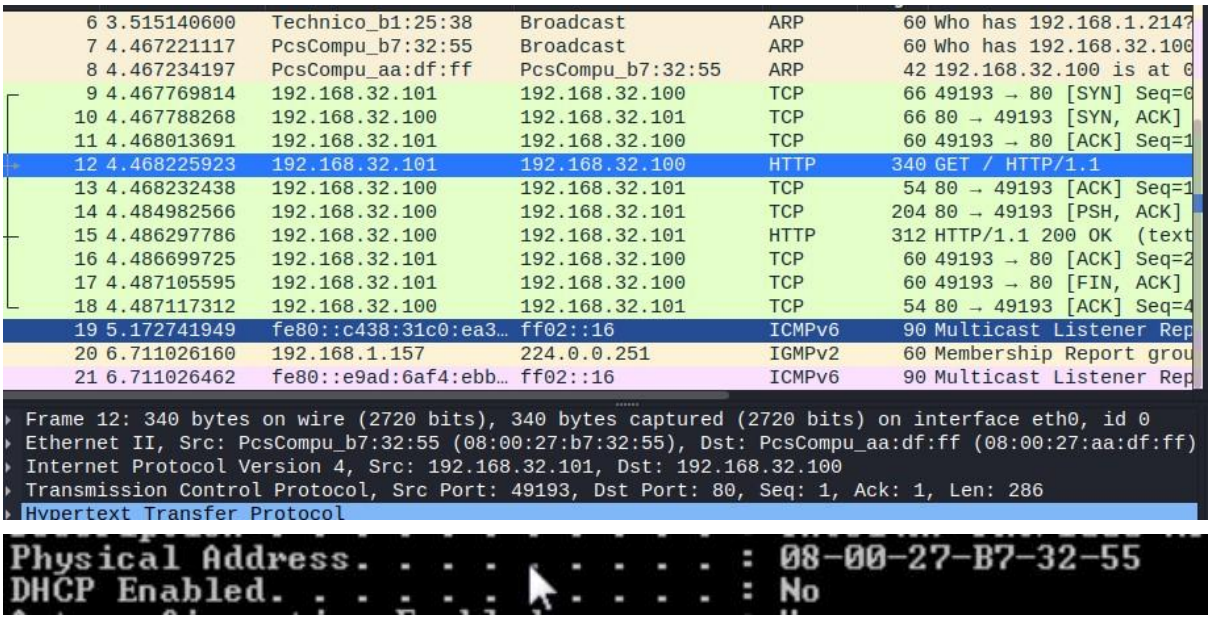
Il dns andrà a tradurre il nome di dominio “epicode.internal con l’indirizzo ip della macchina server.

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

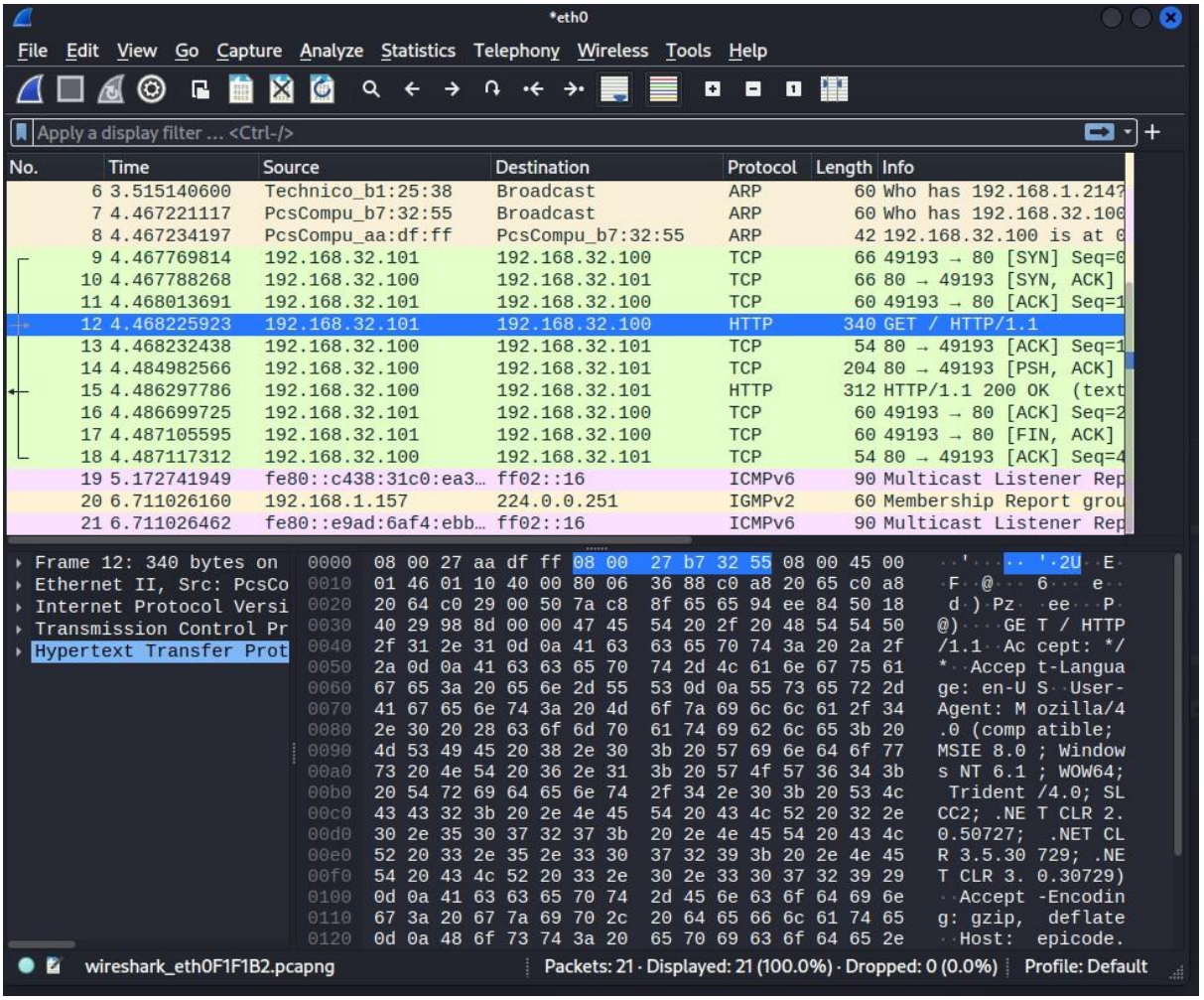
.



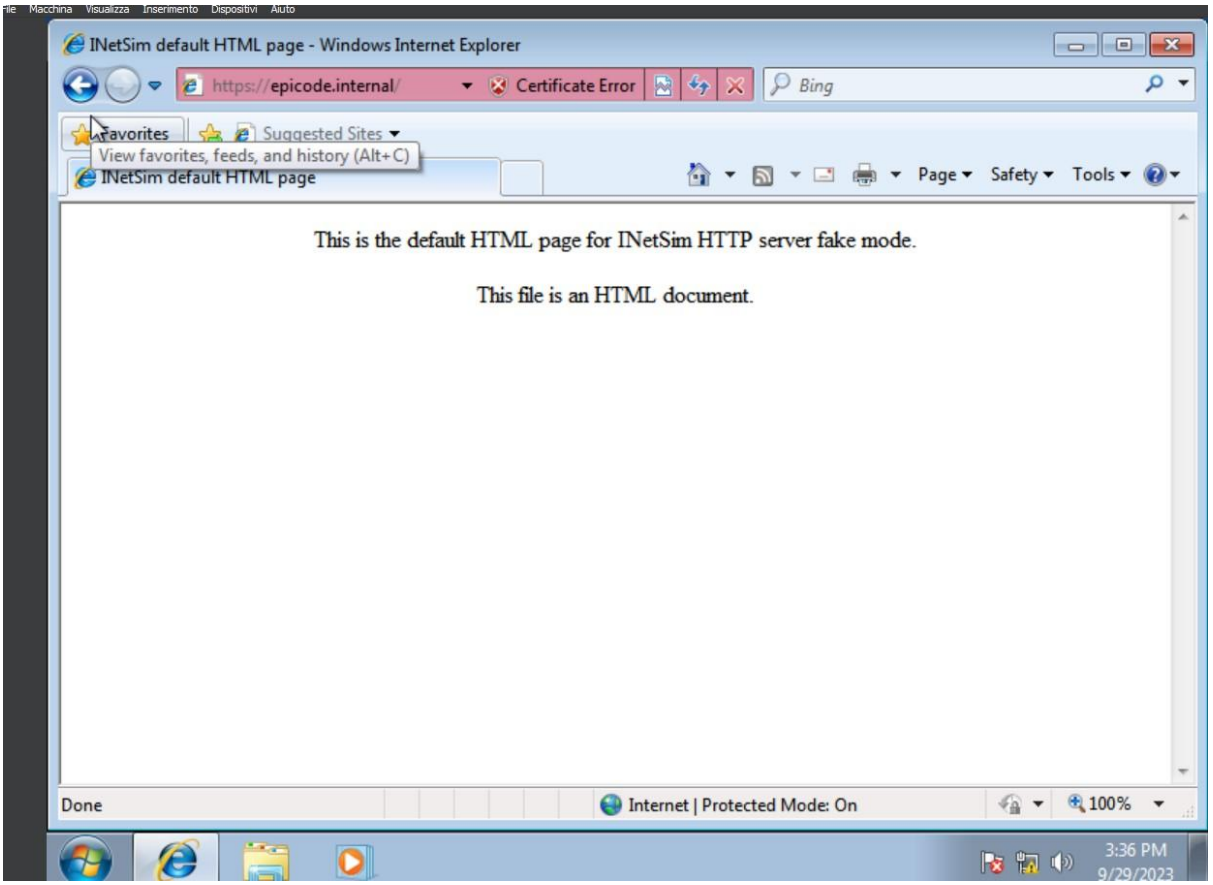
Sulla macchina Linux ho potuto visionare i pacchetti con WireShark andando a visualizzare l'indirizzo MAC della macchina client.



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



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.