REPORT SIMULAZIONE RETE COMPLESSA WEEK 1

Per prima cosa abbiamo impostato i nuovi ip sulle macchine virtuali;

Kali(immagine 1)

Windows (immagine 2)

immagine 1

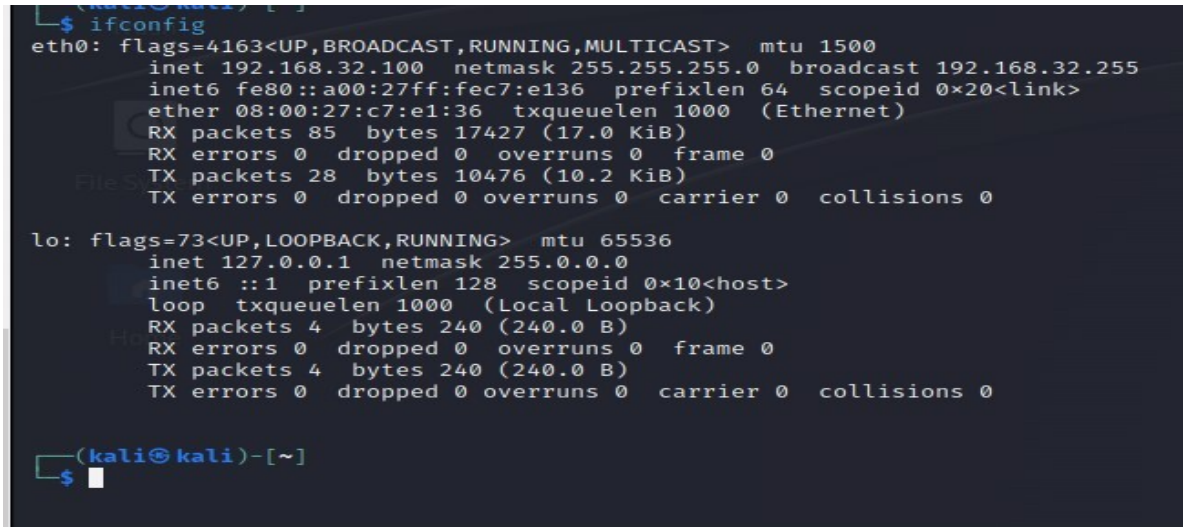
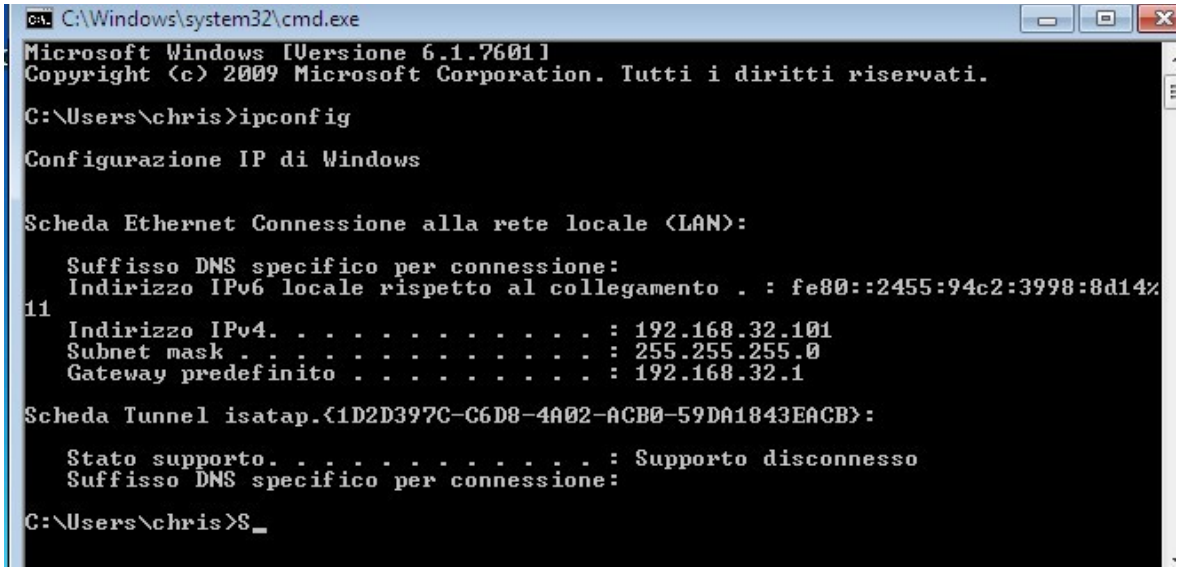


immagine 2



Successivamente mediante l'aiuto di InetSim (che ci permetterà di analizzare i comportamenti della rete),andiamo ad impostare sul terminale linux di kali andiamo a creare un server DNS e un server HTTPS,impostando:

indirizzo di collegamento al servizio

```
61 # service_bind_address
62 #
63 # IP address to bind services to
64 #
65 # Syntax: service_bind_address <IP address>
66 #
67 # Default: 127.0.0.1
68 #
69 #service_bind_address 10.10.10.1
70 service_bind_address 192.168.32.100
71
```

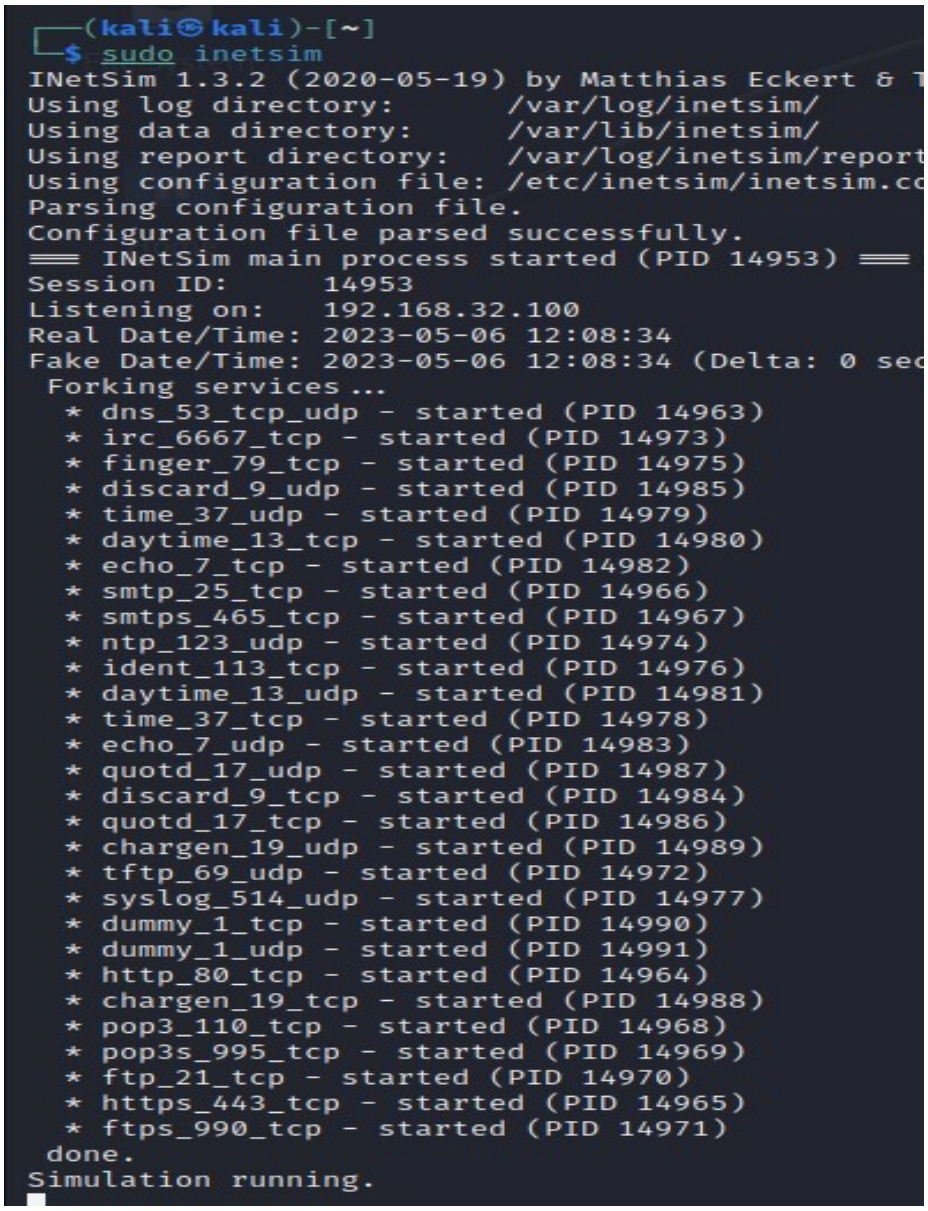
assegnamo un indirizzo ip al Server DNS

```
198 ##############################################
199 # dns_default_ip
200 #
201 # Default IP address to return with DNS replie
202 #
203 # Syntax: dns_default_ip <IP address>
204 #
205 # Default: 127.0.0.1
206 #
207 #dns_default_ip 10.10.10.1
208 dns_default_ip 192.168.32.100
209
```

infine assegnamo il nome “epicode.internal” al nostro server

```
235 # dns_static
236 #
237 # Static mappings for DNS
238 #
239 # Syntax: dns_static <fqdn hostname> <IP addr
240 #
241 # Default: none
242 #
243 #dns_static www.foo.com 10.10.10.10
244 #dns_static ns1.foo.com 10.70.50.30
245 #dns_static ftp.bar.net 10.10.20.30
246 dns_static epicode.internal 192.168.32.100
```

Dopo aver impostato tutti i parametri , sul terminale di kali eseguiamo la simulazione che ci permetterà di il nostro ambiente di analisi

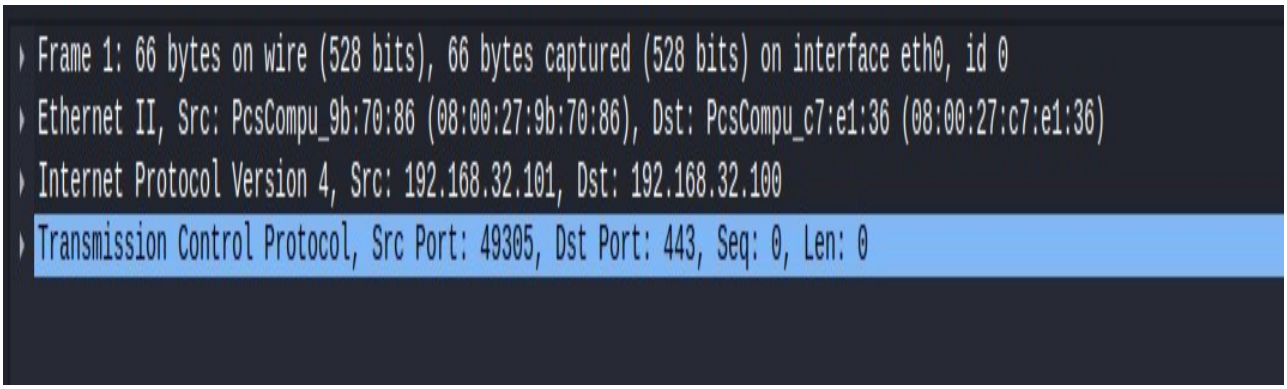


per analizzare il traffico di pacchetti utilizzeremo wireshark sulla sorgente eth0 che identifica il nostro ambiente virtuale

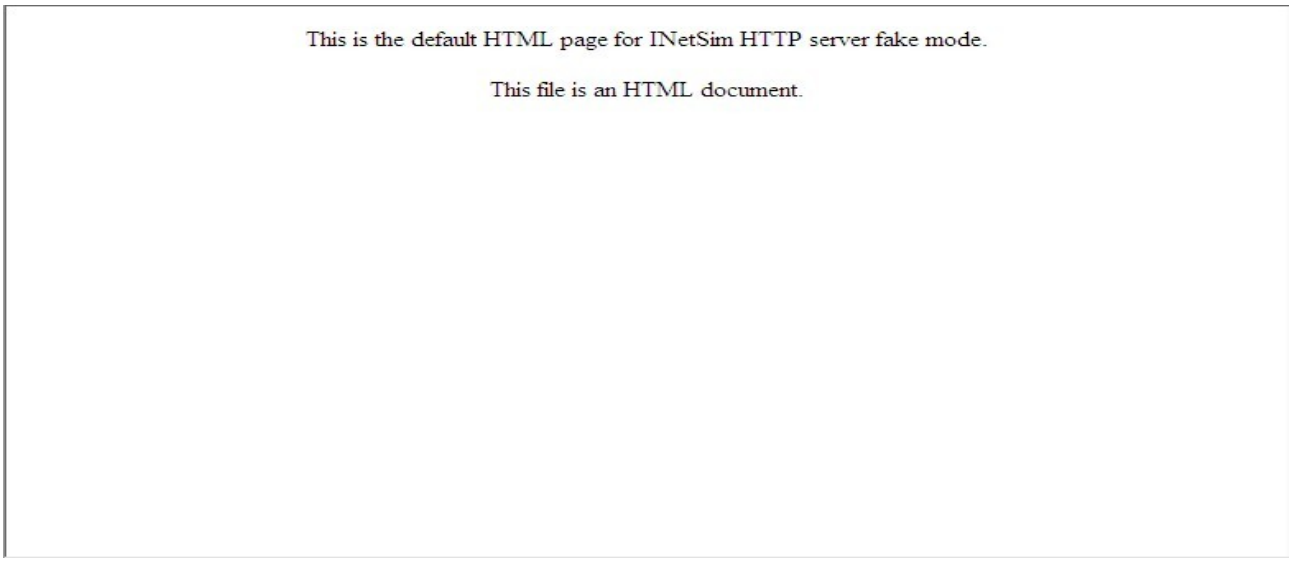
Avviata l'analisi sulla macchina relativa a windows 7,sul web browser nello spazio del codice URL "https://epicode.internal" dandoci questa risposta:

mentre su wireshark partirà un analisi di pacchetti di invio e risposta,e se andiamo ad analizzare un pacchetto che segue il protocollo tcp vedremo che il il nostro dns sta usando un protocollo sicuro con la porta 443(vedi immagine) che garantisce una connessione crittografata.

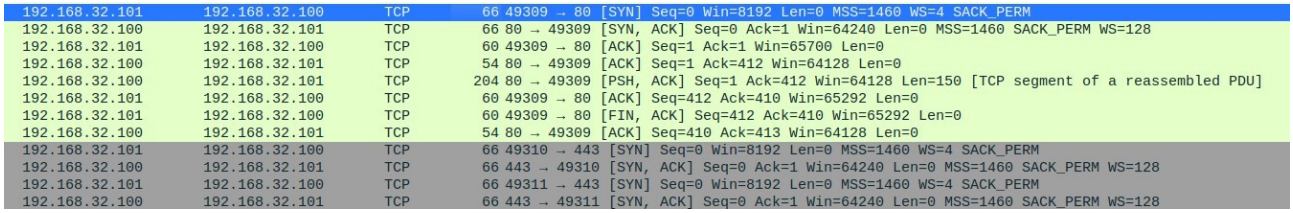
1	0.000000000	192.168.32.101	192.168.32.100	TCP	66 49305 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
2	0.000062456	192.168.32.100	192.168.32.101	TCP	66 443 → 49305 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3	0.000196270	192.168.32.101	192.168.32.100	TCP	60 49305 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0
5	0.000881412	192.168.32.100	192.168.32.101	TCP	54 443 → 49305 [ACK] Seq=1 Ack=130 Win=64128 Len=0
10	0.247687747	192.168.32.100	192.168.32.101	TCP	113 [TCP Retransmission] 443 → 49305 [PSH, ACK] Seq=1320 Ack=264 Win=64128 Len=59
11	0.247685799	192.168.32.101	192.168.32.100	TCP	60 49305 → 443 [ACK] Seq=264 Ack=1379 Win=64320 Len=0
12	0.247841553	192.168.32.101	192.168.32.100	TCP	66 [TCP Dup ACK 11#1] 49305 → 443 [ACK] Seq=264 Ack=1379 Win=64320 Len=0 SLE=1320 SRE=1379
34	11.435532159	192.168.32.101	192.168.32.100	TCP	66 49306 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
35	11.435572294	192.168.32.100	192.168.32.101	TCP	66 80 → 49306 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
36	11.435684979	192.168.32.101	192.168.32.100	TCP	60 49306 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
38	11.435769055	192.168.32.100	192.168.32.101	TCP	54 80 → 49306 [ACK] Seq=1 Ack=218 Win=64128 Len=0
39	11.446739179	192.168.32.100	192.168.32.101	TCP	204 80 → 49306 [PSH, ACK] Seq=1 Ack=218 Win=64128 Len=150 [TCP segment of a reassembled PDU]
41	11.448249216	192.168.32.101	192.168.32.100	TCP	60 49306 → 80 [ACK] Seq=218 Ack=410 Win=65280 Len=0

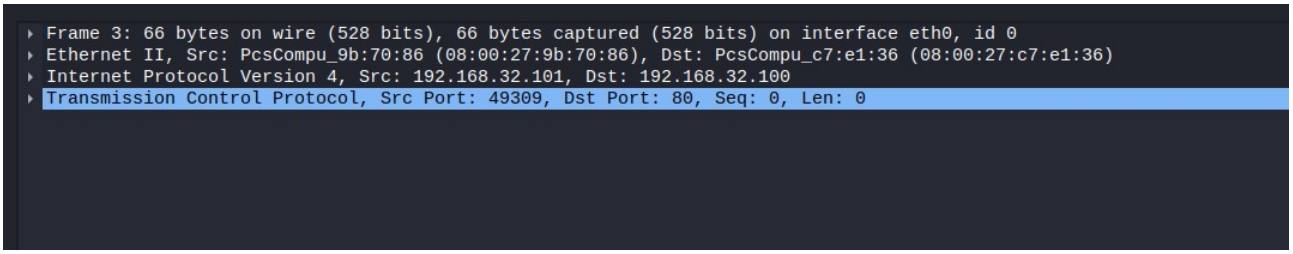


Utilizzando il protocollo http sempre sul web browser di windows 7 sempre cercando il nostro server “http://epicode.internal” ,apparirà una pagina così:



Mentre su Wireshark vedremo un analisi di pacchetti dove al contrario della precedente analisi usava la porta 443 ,il protocollo http userà la porta 80:





come visto nell'immagine del web browser di windows 7 viene mostrata la risposta di inetsim del nostro DNS server impostato precedentemente crittografata che non necessita certificazioni col protocollo http mentre a differenza del protocollo https che stabilisce connessioni crittografate.