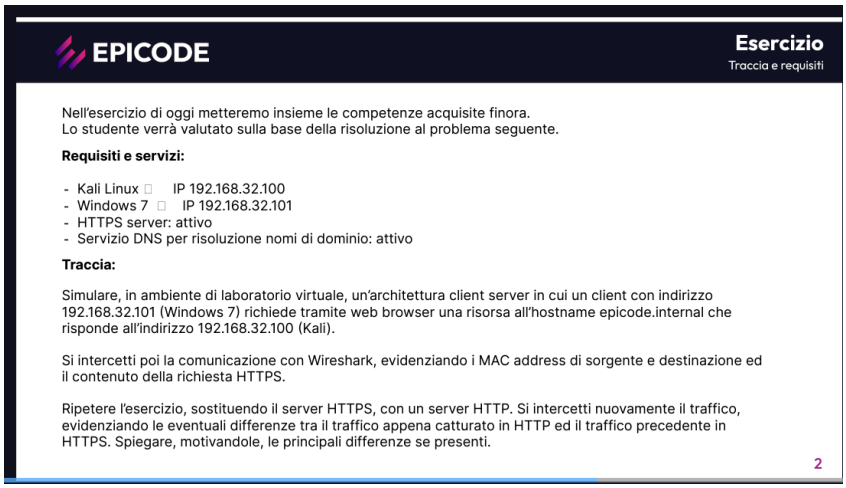


EPICODE

Esercizio
Traccia e requisiti

Nell'esercizio di oggi metteremo insieme le competenze acquisite finora.
Lo studente verrà valutato sulla base della risoluzione al problema seguente.

Requisiti e servizi:

- Kali Linux IP 192.168.32.100
- Windows 7 IP 192.168.32.101
- HTTPS server: attivo
- Servizio DNS per risoluzione nomi di dominio: attivo

Traccia:

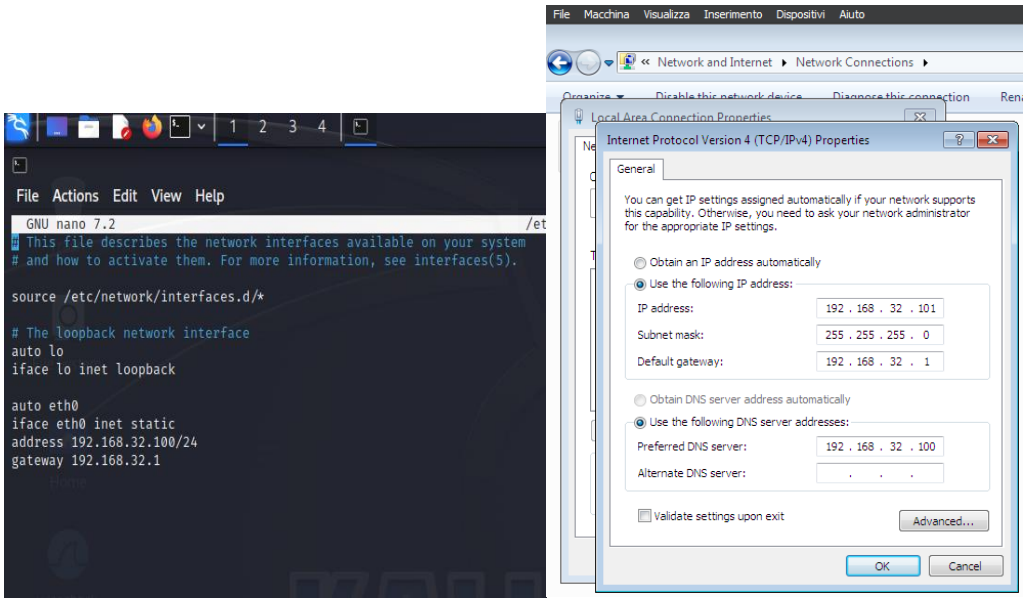
Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (Kali).

Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

2

Data la traccia sovrastante verrà creato un laboratorio virtuale dove verrà settato i vari ip, gateway e dns nelle rispettive macchine



Per quanto riguarda il DNS di windows , verrò impostato come DNS server quello della macchina di kali

Successivamente andranno emulati sul server i servizi DNS, HTTP e HTTPS tramite inetsim

```
##############################################
# 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


##############################################
```

Verrà impostato come bind address l'ip richiedente dei servizi inetism

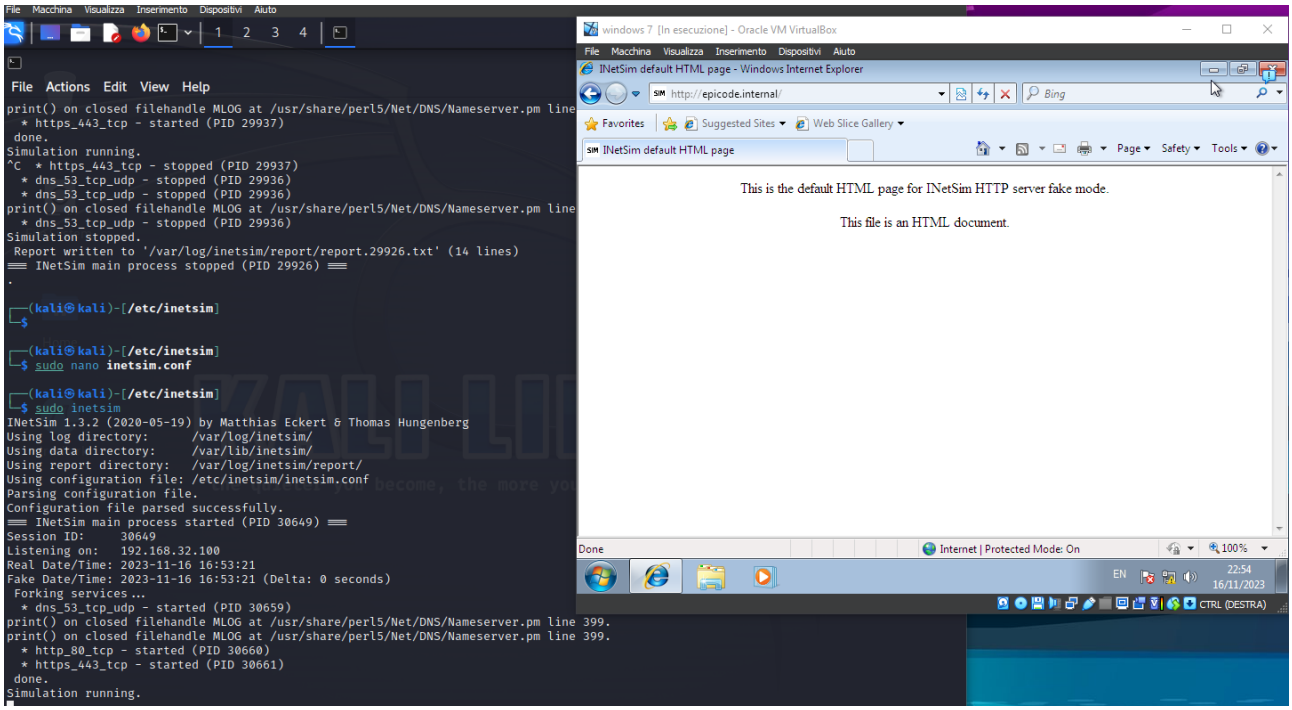
Ed impostato un DNS statico con dominio epicode.internal

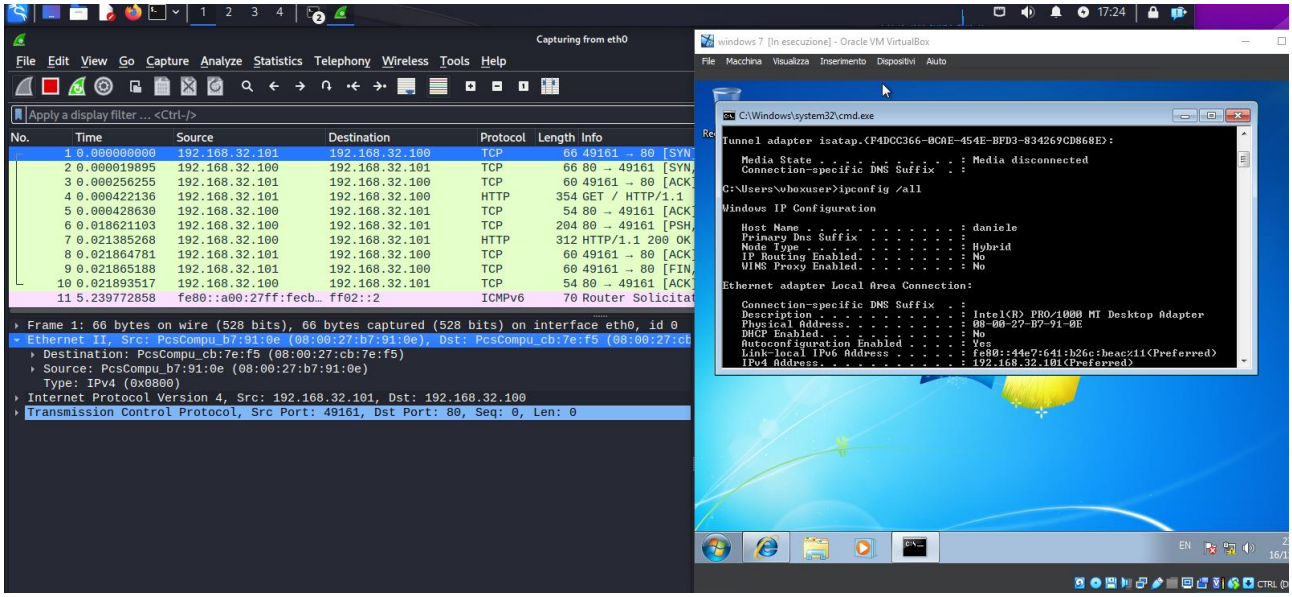
```
##############################################
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
dns_static epicode.internal 192.168.32.100
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30


##############################################
```

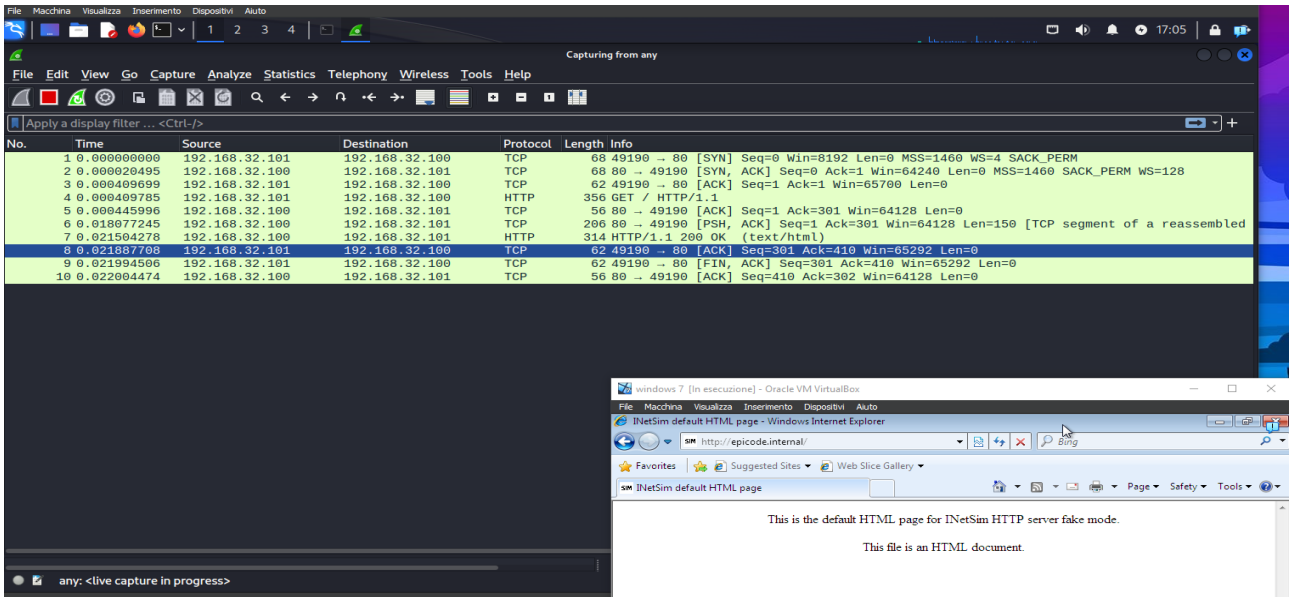
Una volta settato inetsim verranno simulati i rispettivi servizi e si passerà a windows dove tramite browser ci connettemo a epicode.internal http/https, successivamente verrà sniffato il traffico della rete con wireshark per entrambi i protocolli.

Connessione ad http://epicode.internal/

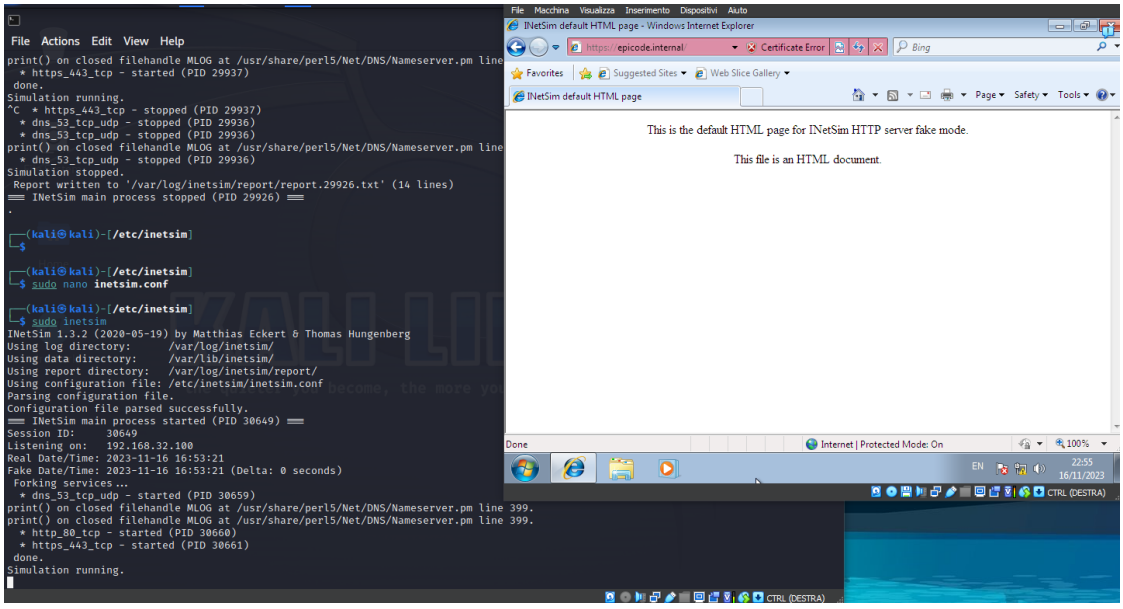




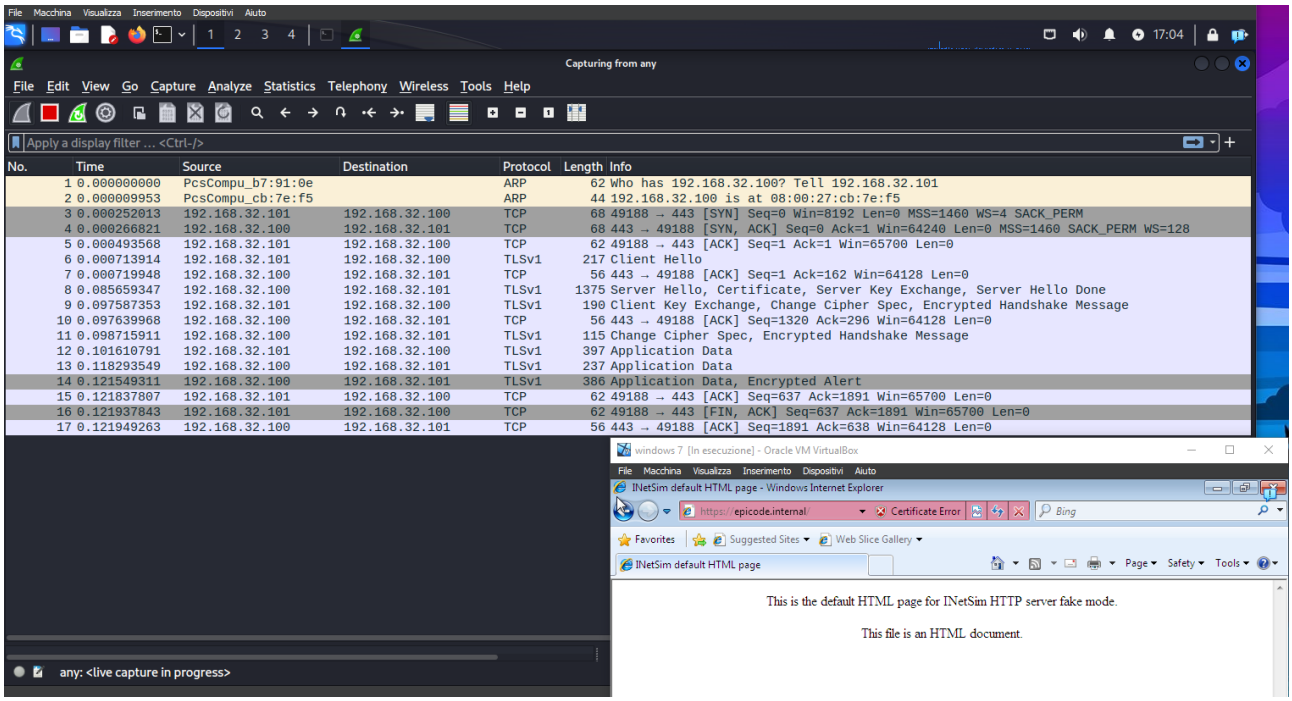
Sniff dei dati con wareshark

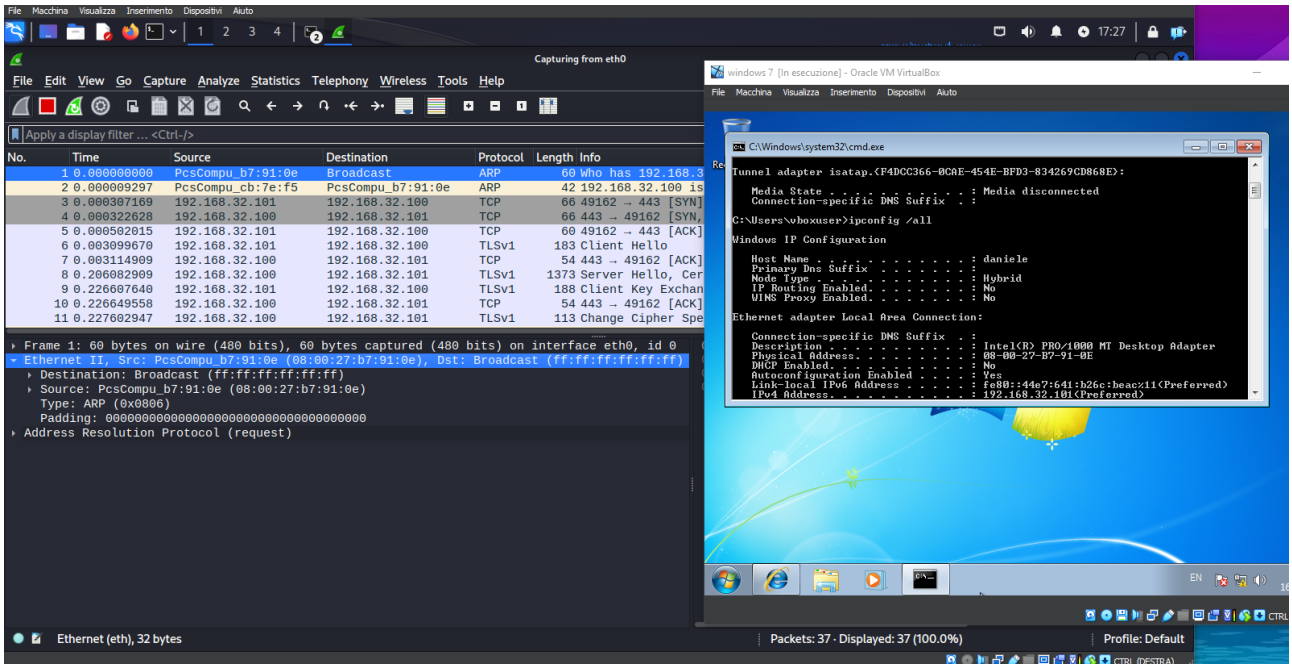


Successivamente verrà ripetuta la stessa azione con https



E sniffati nuovamente i dati





Confrontando i dati acquisiti tramite wireshark potremmo riscontrare che la differenza sostanziale tra le due richieste sta nel protocollo TLS ovvero lo scambio di chiavi crittografiche, per non rendere visibile la comunicazione, mentre nell'acquisizione tramite http tutti i dati saranno "leggibili", difatti potremmo leggere quello che c'è scritto nella richiesta GET e la risposta 200 OK.