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:

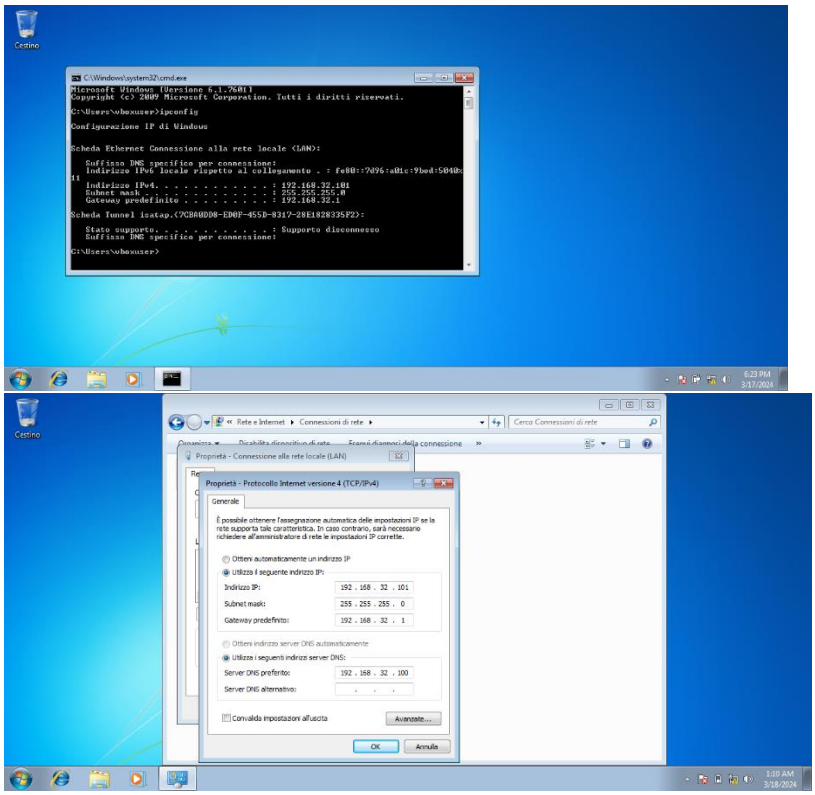
Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (Kali).

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.

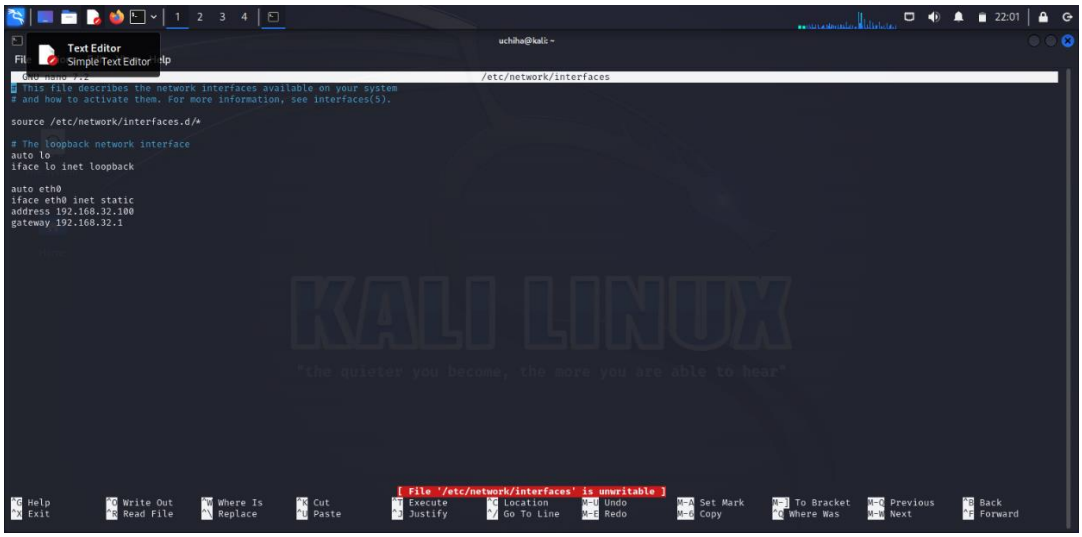
2

- Come 1 passo impostiamo l'indirizzo ip di windows 7 e il DNS di kali



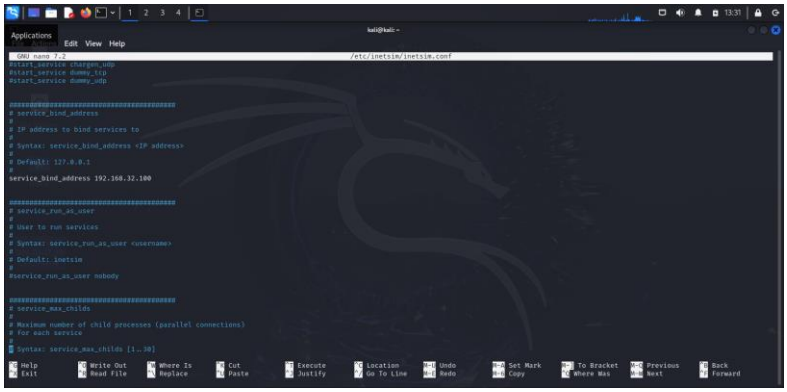
- Passaggio 2 configurazione ip kali linux

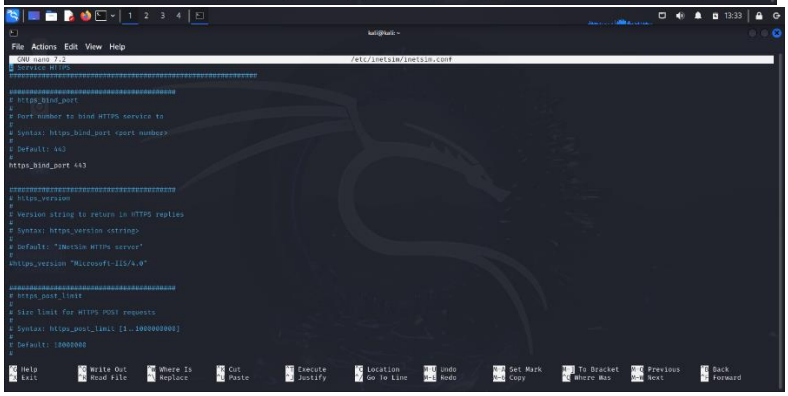
Per configurare manualmente l'indirizzo ip 192.168.32.100 utiliziamo il comando : sudo /etc/network/interfaces



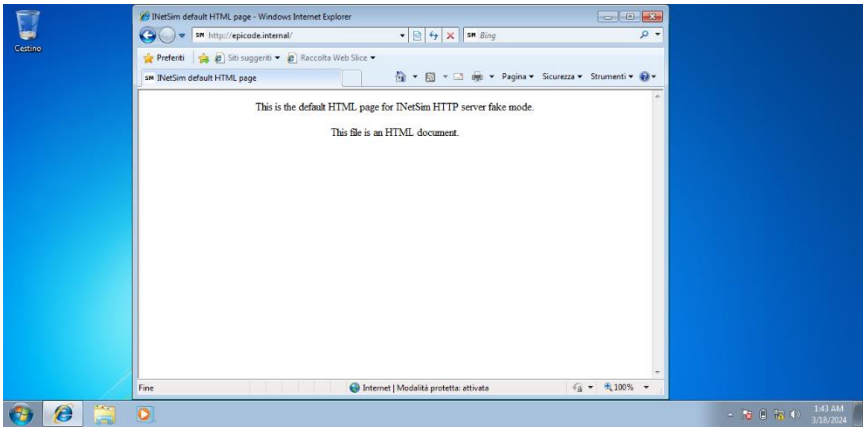
- Nel 3 passaggio andiamo a configurare i servizi richiesti dall'esercizio , andando a modificare le configurazioni di inetsim. Per farlo utilizziamo il comando : sudo /etc/inetsim/inetsim.conf

1. Configurazione **service_bind_address :** configuriamo questo servizio con l ip 192.68.32.100 per rendere più sicura la rete e permettere solo ai pc che hanno come indirizzo DNS 192.168.32.100
2. **Dns_default_ip:** configuriamo questo servizio con l'indirizzo ip 192.168.32.100
3. **Dns_default_domainname :** configuriamo questo servizio con il dominio **epicode.internal**
4. **http_bind_port 80:** dobbiamo solamente abilitare questa porta
5. **https_bind_port 443:** dobbiamo anche qui abilitare solamente questa porta

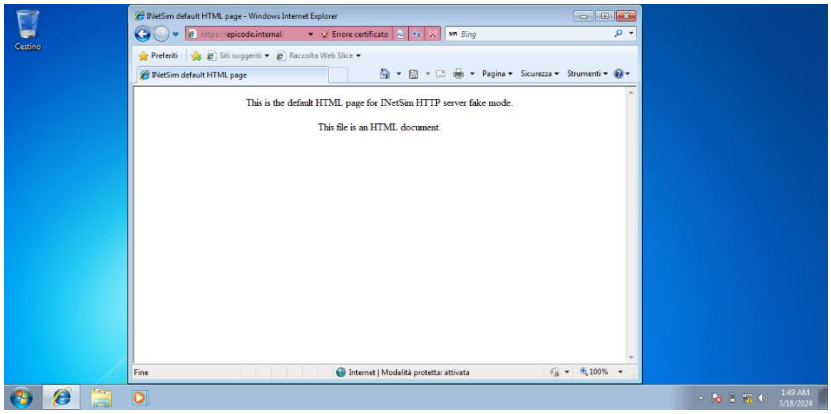




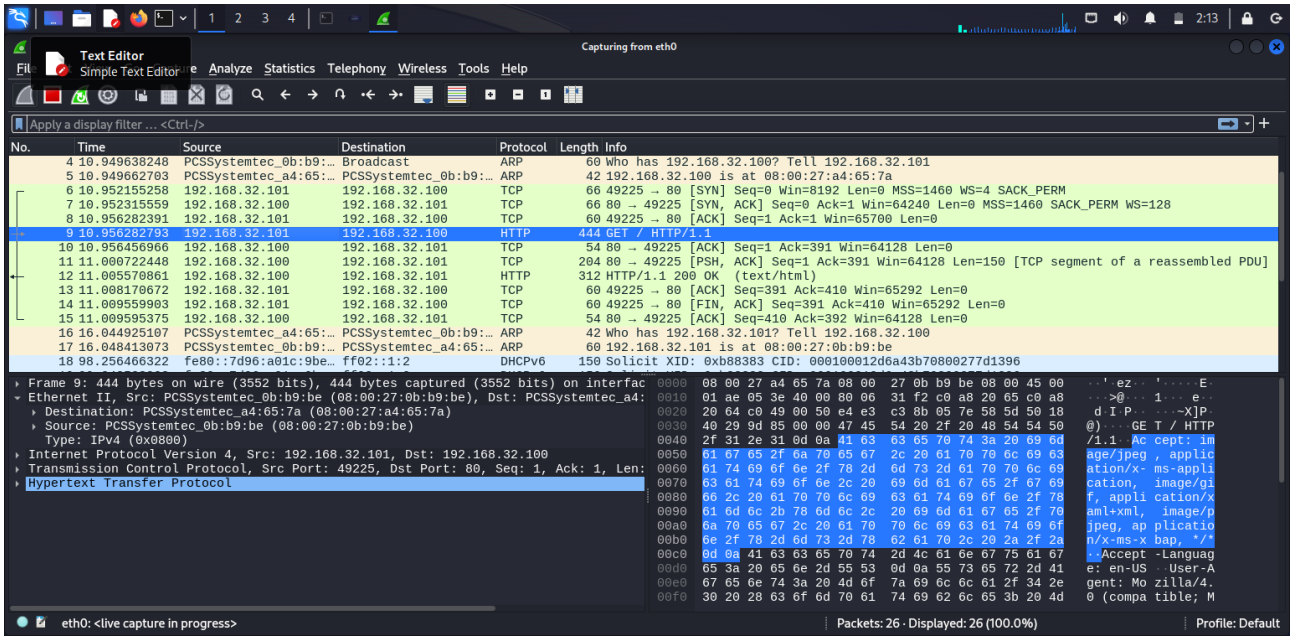
- nel 4 passaggio verifichiamo il raggiungimento del donimio epicode.internal da parte del browser del client windows 7 in http:



- nel 5 passaggio verifichiamo il raggiungimento di quest'ultima tramite https:

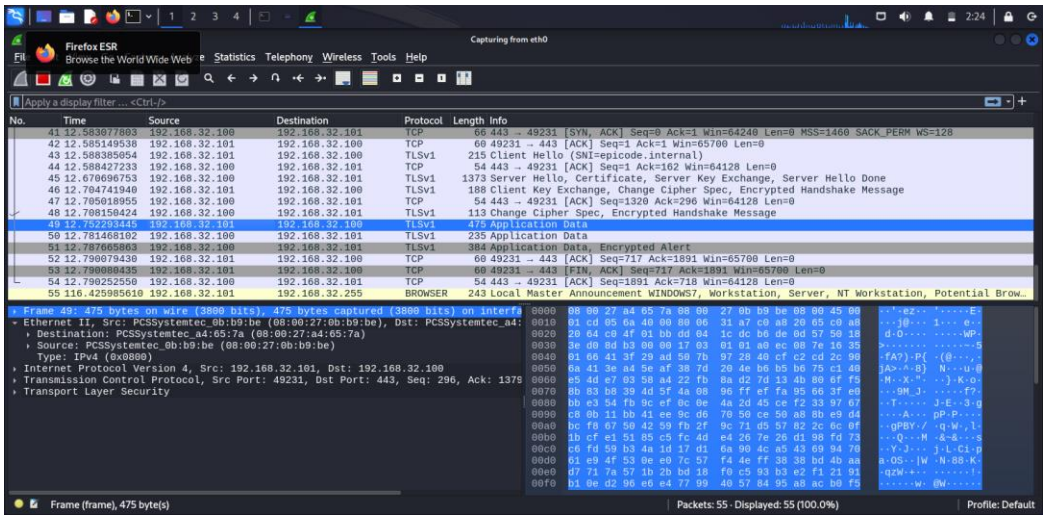


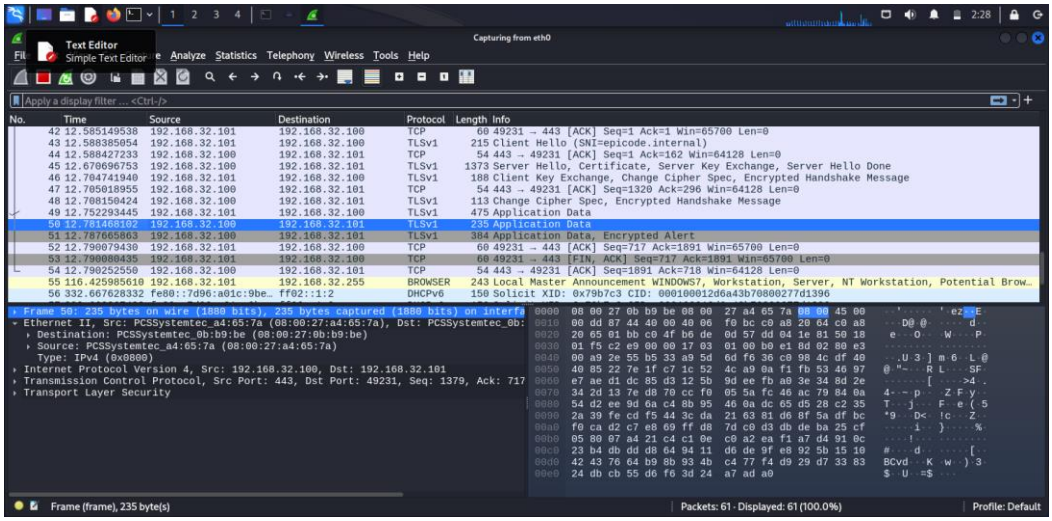
- Nel 6 passaggio avviamo wireshark per l'intercettazione del traffico http:



qui possiamo notare in chiaro http://epicode.internal/ e notiamo anche la richiesta GET che indica l'apertura della pagina e i Mac Address. **Destination** : 08:00:27:a4:65:7a e **Source:** 08:00:27:0b:b9:be

- Nel 7 passaggio analizziamo il traffico in https:





In questi 2 grafici possiamo notare i mac address e come variano tra loro .

- N.B : Abbiamo visto come aggiungere il dominio epicode.internal configurando il dns dinamico di inetsim ma possiamo benissimo svolgere l'esercizio richiesto , configurando il dns statico. Utilizzando l'ultimo metodo risulta essere ugualmente efficace e molto più semplice da configurare perché basta settare il dns statico e il port_bind_address per configurare tutto correttamente.