Differenze tra HTTP e HTTPS

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.

Esecuzione:

Come richiesto dalla traccia sopra riportata sono andato ad impostare gli IP statici su entrambe le macchine virtuali: tramite interfaccia grafica in Windows e invece tramite terminale in Kali Linux usando il comando: "sudo nano /etc/network/interfaces". (***Screenshot 1)***

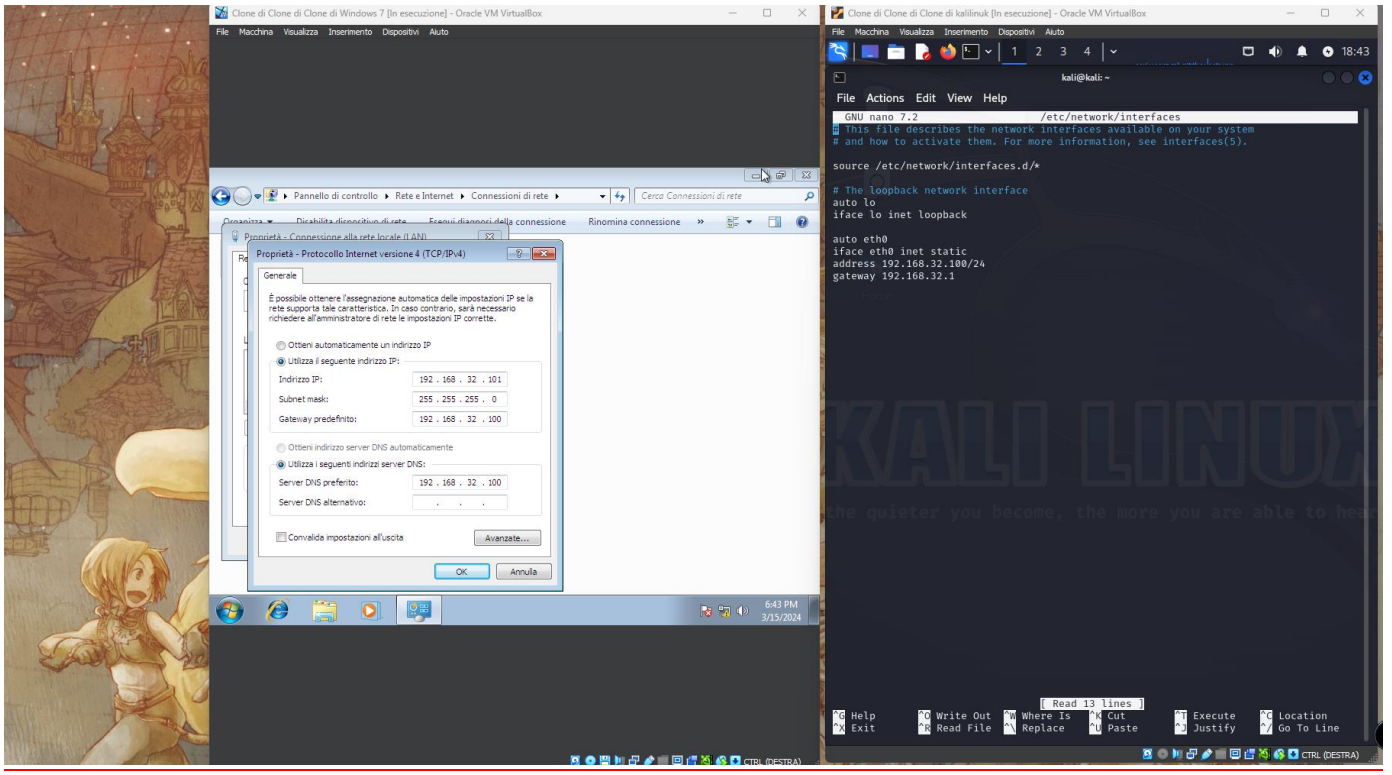
Fatto ciò tramite il comando "sudo nano /etc/inetsim/inetsim.conf" sono andato ad attivare e impostare il servizio DNS su Kali Linux e i servizi HTTP e HTTPS, per ultimo punto sono tornato in Windows e ho impostato nell'interfaccia di rete tramite pannello di controllo il DNS di Kali Linux per poter "puntare" correttamente e risolvere il dominio con successo. ***(Screenshot 2)***

A questo punto ero pronto alla cattura dei pacchetti tramite il programma Wireshark presente in Kali Linux. Dopo aver avviato Wireshark sono tornato sulla macchina di windows 7 e tramite internet explorer mi sono diretto sul sito: epicode.internal e ho analizzato i pacchetti ***(Screenshot 3)***

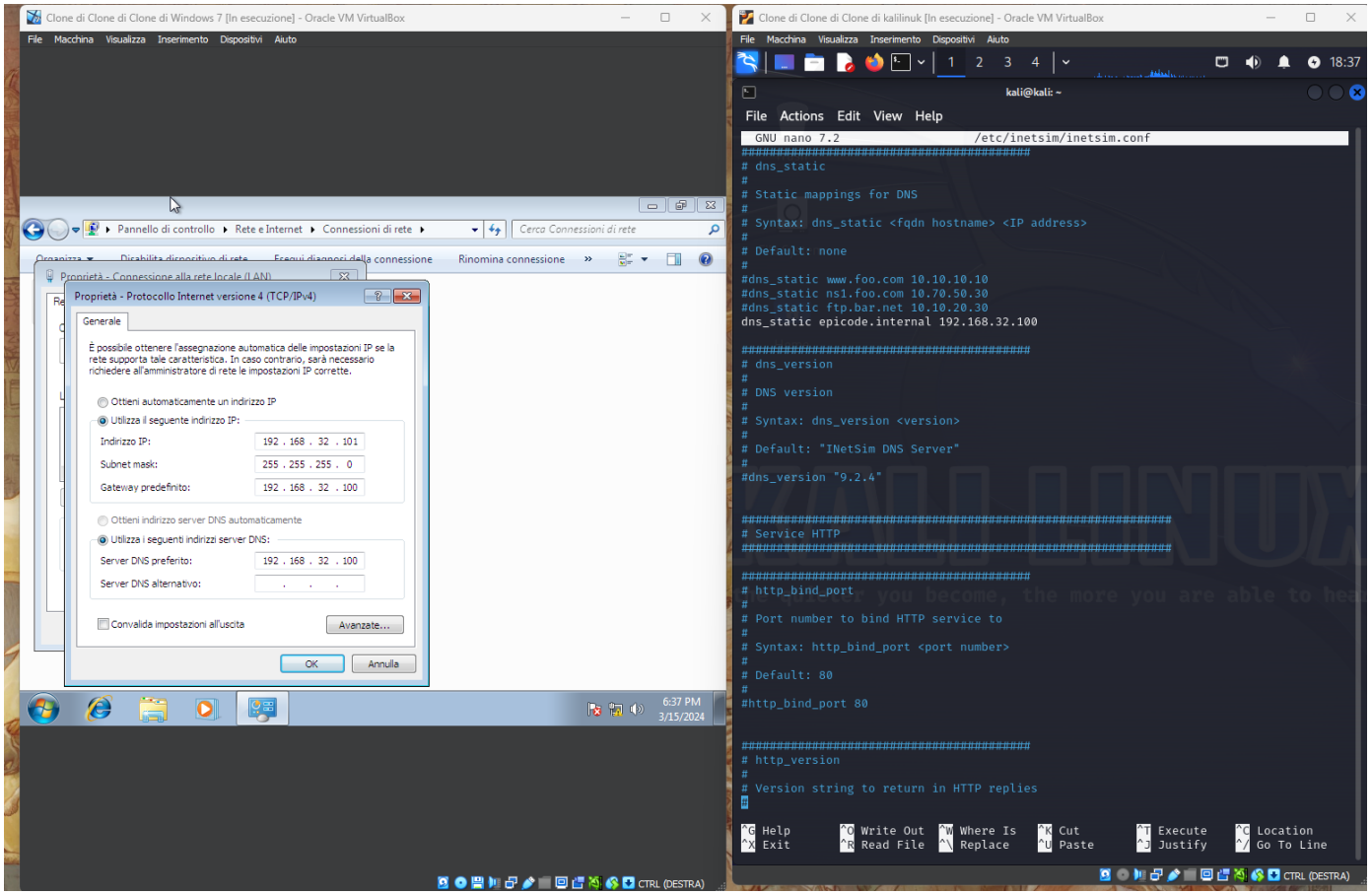
Dopo una prima fase di cattura di pacchetti del protocollo HTTP ho ricercato tramite la barra degli indirizzi la versione del sito in HTTPS e analizzato i pacchetti ***(Screenshot 4 e 5)***

Dopo gli screenshot riporterò le principali differenze riscontrate tra HTTP e HTTPS

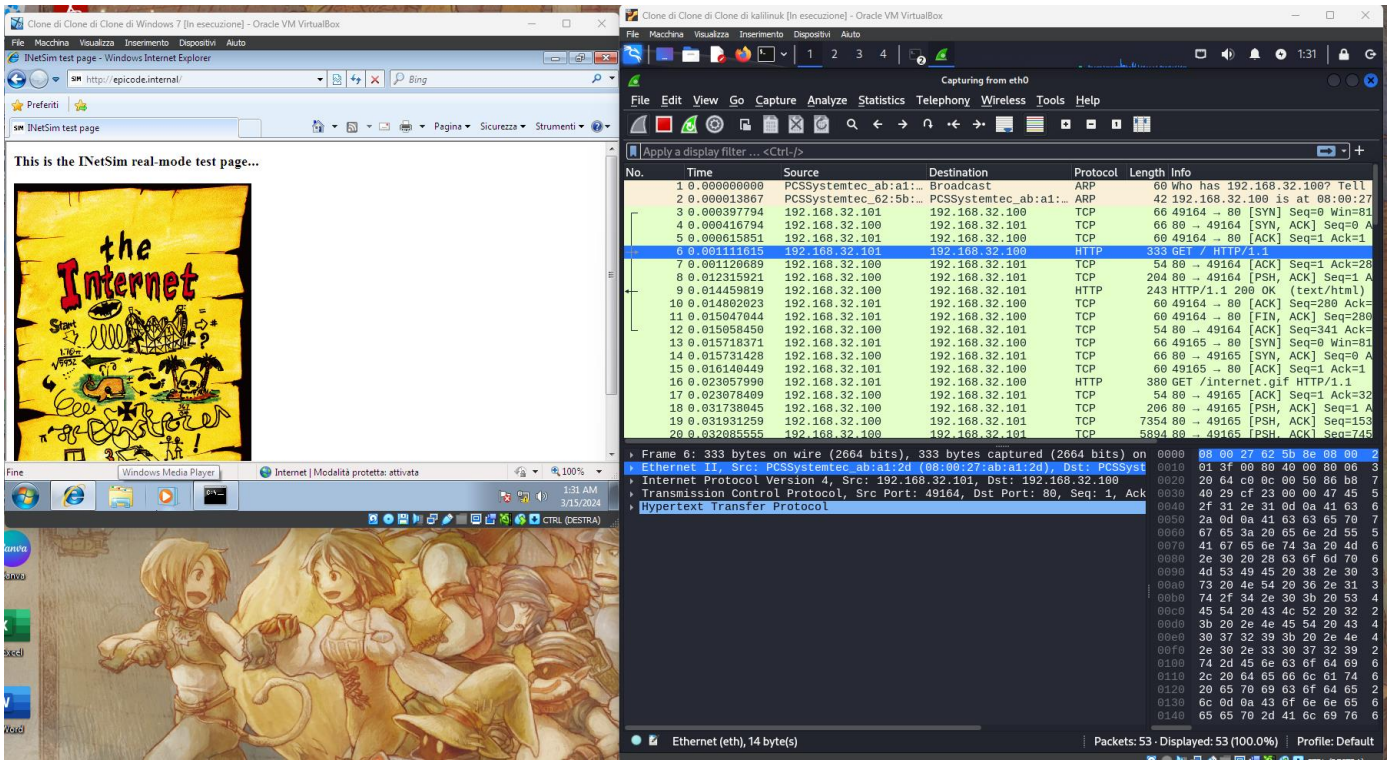
Screenshot 1



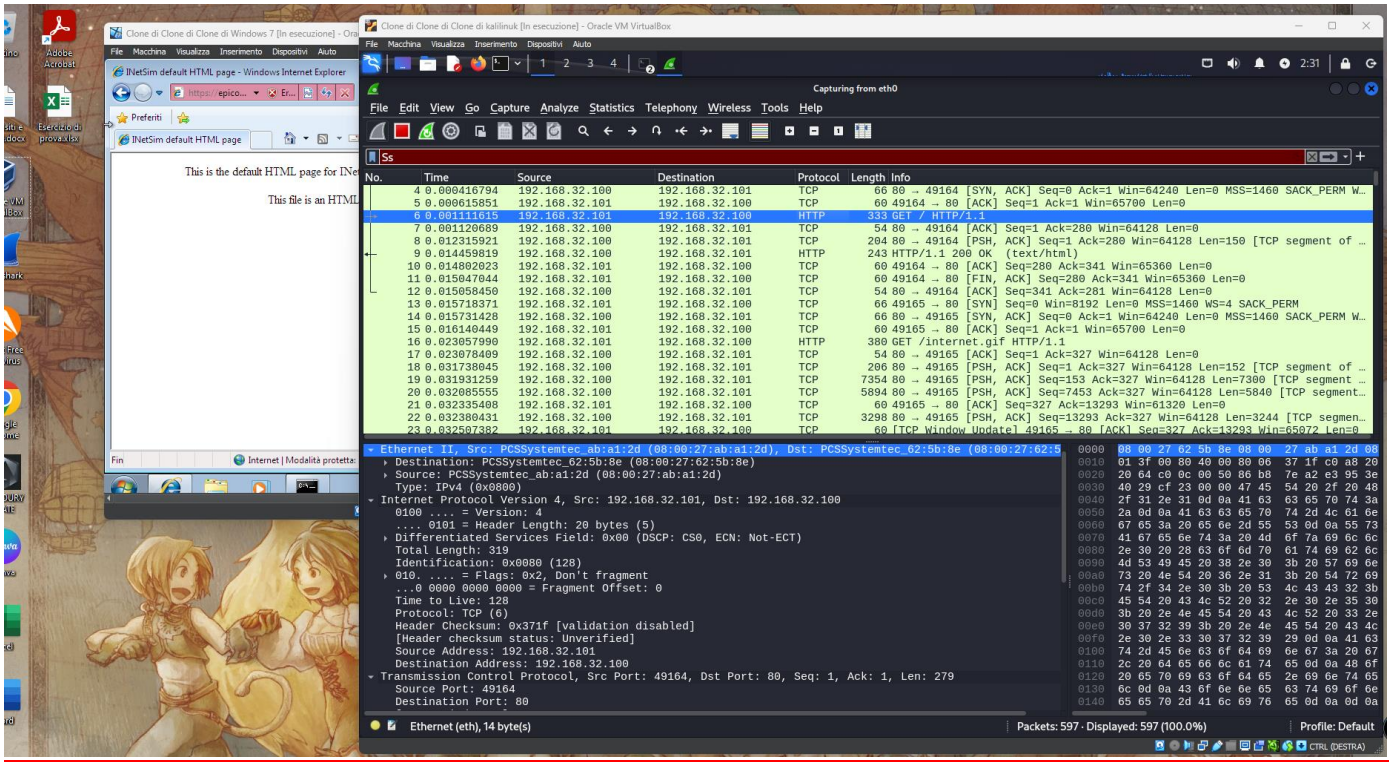
Screenshot 2



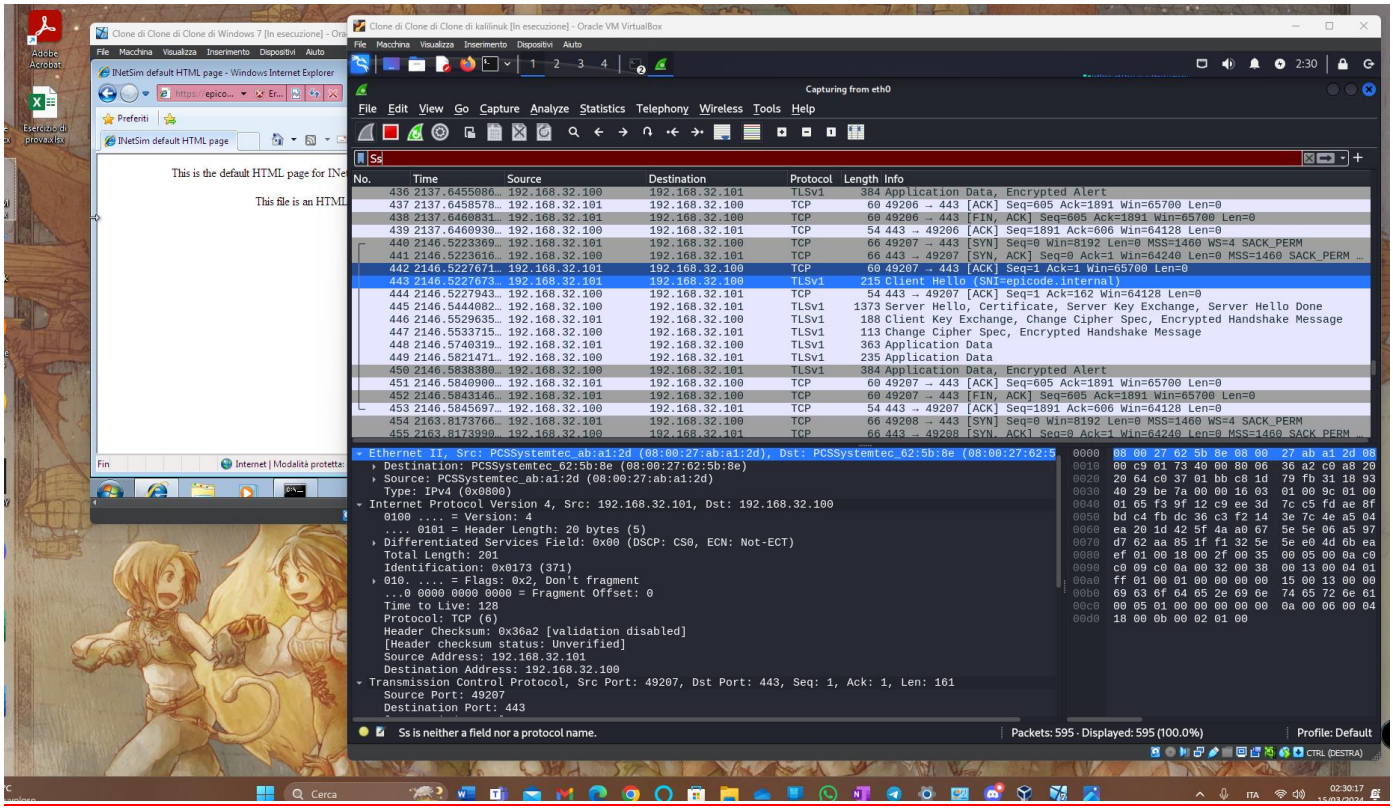
Screenshot 3



Screenshot 4



Screenshot 5



Sono andato ad esplorare le informazioni sui pacchetti catturati in maniera più approfondita nei ***Screenshot 4 e 5*** ed ecco le mie conclusioni:

Prima di tutto la quantità delle informazioni catturate e visibile in chiaro è diversa, questo ci porta in evidenza la prima grande differenza tra HTTP e HTTPS, infatti il traffico HTTPS è crittografato e non sono in grado di vedere il contenuto della richiesta e della risposta in chiaro invece visibile nel http

MAC address Destination: (08:00:27:62:5b:8e)

MAC address Source: (08:00:27:ab:a1:2d)

La seconda differenza sta appunto nei protocolli utilizzati mentre per la trasmissione in chiaro vengono utilizzati HTTP e TCP nella trasmissione crittografata possiamo notare anche il protocollo TLSv1 un protocollo che si usa appunto per trasmissione di dati crittografata

La terza delle principali differenze che ho notato sta nell'uso delle porte, come si può vedere in fondo agli ***Screenshot 4 e 5*** Infatti HTTP usa la porta 80 per la comunicazione invece HTTPS usa la porta 443

In conclusione si può affermare che HTTPS fornisce un livello di sicurezza aggiuntivo, proteggendo i dati dalle intercettazioni.

Grazie per l'attenzione

Simone Cisbaglia