ESERCIZIO: **Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS**

In questo laboratorio, completa i seguenti obiettivi:

● Catturare e visualizzare il traffico HTTP

● Catturare e visualizzare il traffico HTTPS

Per svolgere l’esercizio ho usato la VM Cyberops. Una volta loggato ho aperto il terminale e inserito il comando *ip address* per visualizzare l’elenco delle interfacce di rete e i relativi IP.

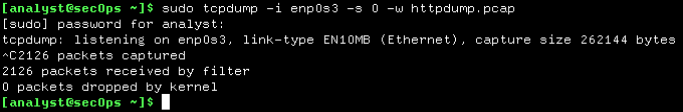


In questo caso a noi interessa la quarta interfaccia: **enp0s3 con 10.0.2.15**

Per registrare il traffico di rete HTTP inseriamo il seguente comando:

*sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap*

Questo comando avvia tcpdump e registra il traffico di rete sull'interfaccia enp0s3



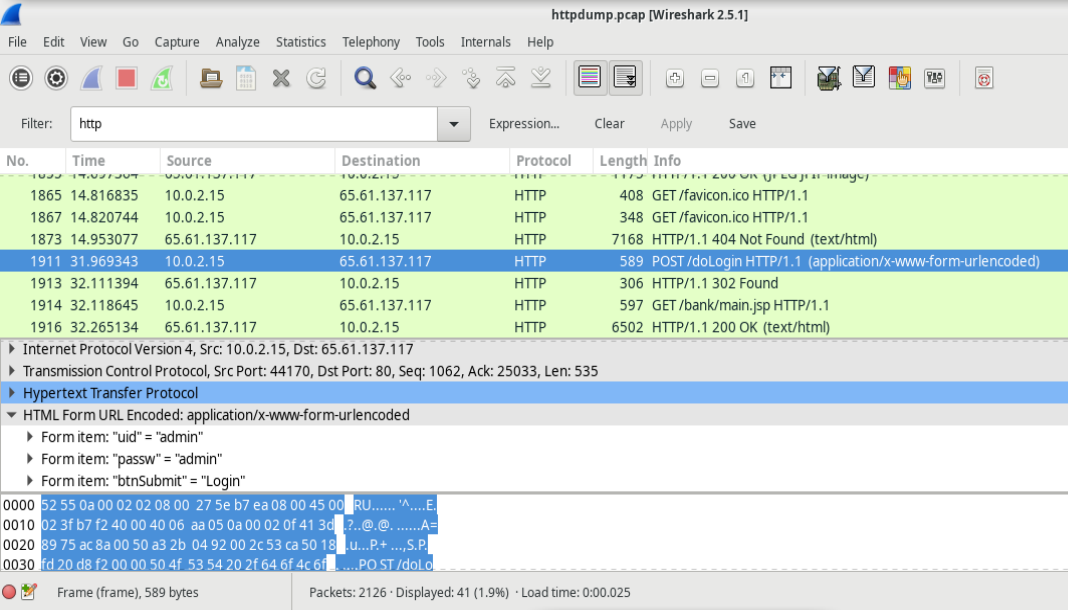
.

**-i opzione command:** consente di specificare l'interfaccia. Se non specificata, tcpdump catturerà tutto il traffico su tutte le interfacce.

**-s opzione command:** specifica la lunghezza dello snapshot per ogni pacchetto. Dovresti limitare snaplen al numero più piccolo che catturerà le informazioni di protocollo a cui sei interessato.

**-w opzione command:** viene utilizzata per scrivere il risultato del comando tcpdump in un file. Aggiungendo l'estensione .pcap si garantisce che i sistemi operativi e le applicazioni saranno in grado di leggere il file. Tutto il traffico registrato verrà stampato nel file httpdump.pcap nella directory home dell'analista utente.

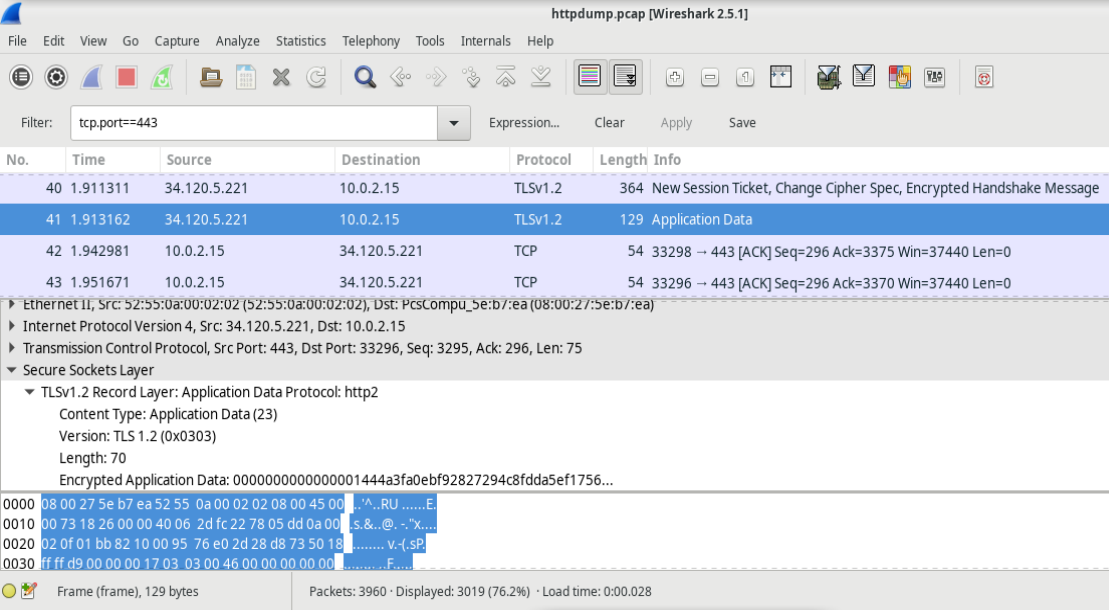
Dopo aver lanciato il comando ho aperto il browser e sono andato su un link a cui ho fatto l’accesso e ho chiuso subito. Sono tornato sul terminale e col comando CRTL + C ho interrotto la cattura dei pacchetti. Dopodichè ho aperto il file *httpdump.pcap* dalla cartella home dell’analista utente. A questo punto si apre wireshark e subito gli faccio filtrare il traffico per HTTP, selezionando il messaggio POST. Nella finestra inferiore viene visualizzato il messaggio. Espando la sezione **HTML Form URL.**



Come si vede, si può visualizzare sia il nome utente che la password dell’utente.

Traffico HTTP catturato correttamente!

Per il traffico HTTPS la procedura è identica. Una volta aperto wireshark bisogna solo cambiare l’istruzione del filtro e inserire **tcp.port==443.** Dai risultati cerchiamo e selezioniamo il messaggio *Application Data*. Estendo completamente la sezione *Secure Sockets Layer*.



Come si nota, Il payload dei dati è crittografato tramite TLS 1.2 e non può essere visualizzato.