Wireshark…attacchiamo la rete con lo squalo! (2° parte)

Eccoci qua…come promesso alla seconda parte…

Per avere un quadro più completo consiglio di leggersi anche la prima parte…che si trova ***qua***!
In questo articolo tratteremo: Cattura di una sessione HTTP
Iniziamo…avviamo il nostro Wireshark, clicchiamo su **Edit/Preferences/Protocols/HTTP** e spuntiamo l'opzione **Uncompress entity bodies** per fare in modo che sia il programma che decomprimerà i contenuti web, che sono stati inviati in modo compresso.
Durante la cattura, dobbiamo spostarci nel box **Filter** dalla finestra principale e impostiamo un filtro per mostrare solo il trafficio HTTP, basterà quindi scrivere **http**. In questo momento ogni pagina che sarà visitata dagli utenti delle rete genererà questo tipo di traffico e noi saremo lì per catturarlo….
scegliamo un request http, selezioniamolo e faccoamo clic con il tasto destro e scegliamo l'opzione **Follow TCP Stream**, così facendo wireshark aprirà una nuova finestra contenente la ricostruzione di tutta la sessione HTTP in ordine cronologico che ha dato vita al request selezionato.
Possiamo anche isolare solo le richieste di ricerche effettuate su motori di ricerca, e estrarre le parole chiave ricercate dagli utenti. Per fare questo basterà inserire il filtro **http.request.uri contains "search"**, nel campo **Filter**
Bene….ci vediamo al prossimo appuntamento dove vi parlerò di come difendersi dalla scansione delle porte…

Guida Scritta da Hackgeek di www.HackGeek.it