Wireshark…attacchiamo la rete con lo squalo! (4° parte)

Ed eccoci arrivati al nostro quarto e ultimo (per adesso) appuntamento con **Wireshark**, come sempre consiglio la lettura degli articoli precedenti per avere un quadro più completo li trovate qui…**primo**..**secondo**…**terzo**!.
In questo articolo vedremo come si svolge un analisi di una **sessione MSN**, in pratica useremo Wireshark per esaminare il flusso di una conversazione MSN fra due client!
Iniziamo…
per prima cosa avviamo una sessione di chat con un qualunque contatto msg della nostra lista, chiaramente dovremmo tenere wireshark attivo per tutta la durata della sessione, in questo modo avremo il log di tutti i messaggi che verranno scambiati fra il client e il server principale. Al termine della conversazione fermiamo la cattura, e come sempre vedremo la finestra dei pacchetti popolata con tutto il traffico generato dalla rete. Se guardiamo con attenzione il listato noteremo che ci sono alcuni pacchetti con protocollo **MSNMS (MSN Messenger Service)**, dovremo quindi evidenziare questi pacchetti e lasciar lavorare il dissector.
Nella finestra **Filter** impostiamo il filtro **MSNMS**, e cerchiamo la stringa **JOI** che è il marcatore utilizzato dal protocollo MSN quando si avvia una chat. Evidenziamo il pacchetto, tasto destro e clicchiamo su **Follow TCP Stream**, questo per fare in modo che il filtro non escluda pacchetti importanti. Se scorriamo la finestra possiamo identificare anche i messaggi di chat. I comandi più interessanti sono **MSG**: indica l'arrivo di un messaggio, **USR**: conferma l'avvenuta connessione con un client, **BYE**: quando un utente remoto chiude la finestra dei messaggi.
Bene..spero che queste informazioni vengano usate solo per scopo didattico e per fare delle prove sulla propria rete…a voi la scelta!

Guida Scritta da Hackgeek di www.HackGeek.it