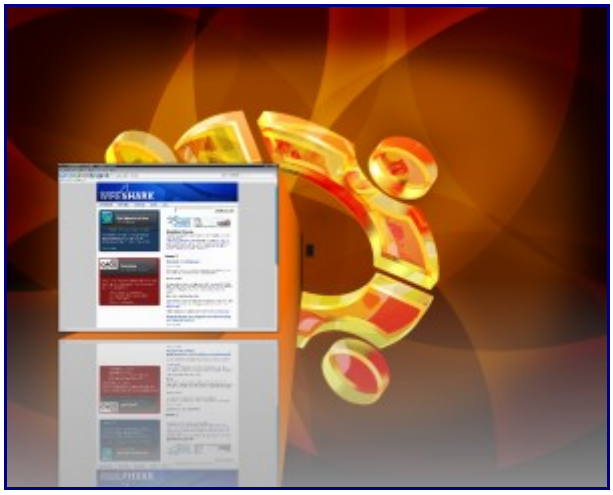
Wireshark…attacchiamo la rete con lo squalo! (3° parte)



Eccoci alla nostra terza puntata dedicata a Wireshark, come sempre consiglio di leggere anche la prima e la seconda per avere un quadro il più completo possibile.

Oggi vedremo come difendersi dalla scansione delle porte, in pratica useremo wireshark per identificare e isolare eventuali portscan effettuati sulle macchine della rete.
Iniziamo…**sudo wireshark**
Scegliamo l'interfaccia di rete su cui ascoltare e avviamo una live capture cliccando su **Capture/Start**. Cercheremo di individuare e isolare i tentativi di scansione delle porte effettuati tramite **Nmap**. Portiamoci su una seconda macchina di test ed effettuiamo con **Nmap** un **SYN Scan e un Xmas Scan**: **nmap -sS -F ip** e **nmap -sX -F ip** (l'opzione **-F** effettuerà la scansione solo sulle porte standard). Aspettiamo che l'operazione sia terminata e torniamo sulla macchina che sta effettuando la cattura del traffico.
Ci chiediamo: come facciamo per isolare un **Syn Scan** (paccheto SYN)?
Chiaramente dovremmo utilizzare un filtro che ci evidenzierà le richieste SYN formati da pacchetti di lunghezza 0, faremo così: **ip.proto==6 and tcp.flags==2 and tcp.len==0**. Questo filtro ci mostrerà solo i pacchetti di tipo TCP che hanno il flag SYN settato e che sono privi di payload.
Il filtro per l' **Xmas scan** è molto simile, basterà cambiare il parametro **tcp.flags** che dovremmo impostare uguale a **41**.
Con questi piccoli consigli potete sbizzarrirvi a discriminare moltre altre tipologie di scan….
Buon divertimento! Ci vediamo alla prossima e ultima (per adesso) puntata su Wireshark…vedremo come analizzare una sessione MSN….e quindi captare il flusso di conversazione MSN tra due client!!

Guida Scritta da Hackgeek di www.HackGeek.it