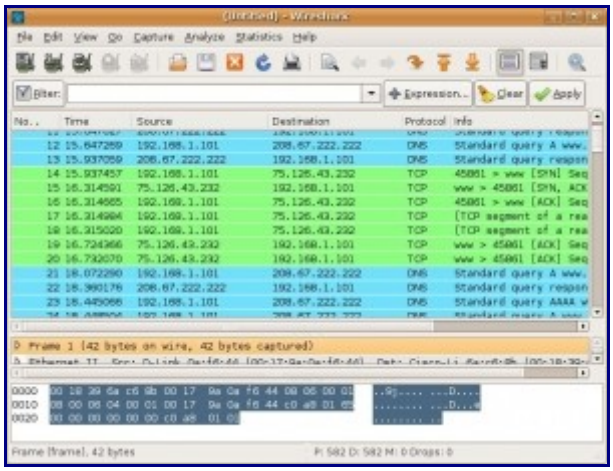
Wireshark…attacchiamo la rete con lo squalo! (1° parte)

In questo articolo/guida voglio parlarvi di un programma molto utile.. chiaramente spetta a voi deciderne l'utilizzo che ne volete fare…

Wireshark consente di analizzare la struttura di una rete a caccia di eventuali errori di configurazione, inoltre è in grado di identificare molti tipi di incapsulamento e di isolare e visualizzare tutti i campi che compongono un pacchetto. Funziona anche da packet-sniffer….in modo simile a tcpdump.
Inziamo con l'installare il programma…in che modo? Semplice: **sudo apt-get install wireshark** (debian/Ubuntu) **emerge wireshark** (Gentoo) **yum install wireshark** (RedHat/Fedora).



Bene ….partiamo….sudo wireshark

Vediamo come scoprire una password di una sessione FTP, così , intercettando una connessione tra un client e un server possiamo scoprire i dati di accesso all'account!
Iniziamo con il catturare il traffico: avviamo Wireshark, clicchiamo quindi su **Capture/Interfaces** e scegliamo l'interfaccia che va verso la rete (per esempio eth0)…clicchiamo su **Start**, da questo momento la nostra interfaccia potra ricevere tutti i pacchetti in transito sulla rete!
Adesso apriamo un secondo terminale e proviamo ad effettuare una normale sessione FTP verso l'IP di un server FTP che usiamo per il nostro test…inseriamo la password per il login e diamo qualche comando…chiudiamo la sessione.
Adesso possiamo tornare nella finestra principale di Wireshark, vedremo che ci sono molti pacchetti che sono transitati in rete dal momento in cui abbiamo avviato la cattura…clicchiamo su **Stop Capture (Ctrl+E)** e esaminiamo il traffico acquisito…
Capire qualcosa tra tutto il traffico non è certo cosa semplice….quindi ricorreremo ad un filtro BPF, cioè quello che ci mostrerà soltanto i pacchetti che fanno parte di una connessione FTP, quindi nel campo **Filter** digitiamo **ftp**. Sarà immediatamente evidenziato il traffico della nostra sessione e la password!!!
Bene…adesso potete divertirvi come meglio volete…
Questa era solo la prima spiegazione di un possibile utilizzo di questo strumento…ho intenzione di scrivere nei prossimi giorni altri tre articoli:

- Cattura di una sessione HTTP
- Difendersi dalla scansione delle porte
- Analisi di una sessione MSN

ci vediamo alla prossima….

Guida Scritta da Hackgeek di http://www.hackgeek.it