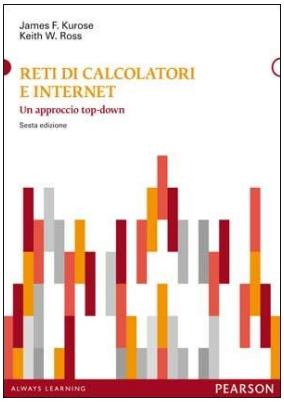
Laboratorio Wireshark: UDP



In questo laboratorio, daremo un rapido sguardo al protocollo di trasporto UDP. Come abbiamo visto nel capitolo 3, UDP è un protocollo snello e senza fronzoli. Poiché UDP è molto semplice, saremo in grado di coprirlo molto velocemente in questo laboratorio. Se avete un altro impegno tra 30 minuti, non preoccupatevi, dovreste essere in grado di finire questo laboratorio con un ampio margine di tempo.

A questo punto, dovreste essere degli esperti di Wireshark. Pertanto, non spiegheremo nel dettaglio i singoli passi come fatto per i laboratori precedenti. In particolare, non forniremo screenshot di esempio per tutti i passi.

Il compito

Iniziate a catturate pacchetti in Wireshark e fate qualcosa che induca il vostro host ad inviare e ricevere vari pacchetti UDP. (Un modo di farlo è di usare il comando nslookup, come abbiamo visto nel laboratorio Wireshark su DNS. Se non potete eseguire Wireshark su una connessione di rete dal vivo, potete scaricare un file con una traccia dei pacchetti catturati da uno dei computer degli autori seguendo i primi due passi della sezione su nslookup del laboratorio Wireshark DNS[1]). Dopo aver interrotto la cattura dei pacchetti, impostate il filtro in maniera che vengano visualizzati solo i pacchetti UDP inviati e ricevuti dal/al vostro sistema terminale. Prendete uno di questi pacchetti UDP ed espandete i campi UDP nella finestra dei dettagli.

Quando possibile, nel rispondere alle domande dovreste consegnare anche una stampa dei pacchetti all'interno della traccia che avete usato per rispondere. Annotate la stampa per spiegare la risposta. Per stampare un pacchetto, usate *File → Print*, scegliete *Selected packet only*, scegliete *Packet summary line*, e selezionate la minima quantità di informazioni sui pacchetti che è necessaria per rispondere alle domande.

1. Selezionare un pacchetto UDP. Da questo pacchetto, determinare quanti campi ci sono in una intestazione UDP. (Non guardate il libro di testo! Rispondere a queste domande direttamente da quello che osservate nella traccia del pacchetto). Dare i nomi di questi campi.
2. Dalla finestra con il contenuto del pacchetto, determinare la lunghezza (in byte) di ognuno dei campi dell'intestazione UDP.
3. Il valore nel campo “Length” è la lunghezza di cosa? (Potete consultare il libro di testo per questa domanda) Verificate la vostra ipotesi con i pacchetti UDP catturati.
4. Qual è il massimo numero di byte che può essere incluso nel carico di un pacchetto UDP?

1 Scaricare il file zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip ed estrarre il file udp-wireshark-trace.pcap- Le tracce nel file zip sono state raccolte da Wireshark da uno dei computer dell'autore, seguendo i passati indicati nella lezione. Una volta scaricata la traccia, potete caricarla dentro Wireshark usando il menù a discesa *File*, scegliendo *Open* e selezionando il file udp-wireshark-trace.pcap.

(Suggerimento: la risposta a questa domanda può essere determinata dalla risposta alla domanda 2)

5. Qual è il valore più grande possibile per il numero di porta sorgente? (Vedere suggerimento per la domanda 4)
6. Qual è il numero del protocollo UDP? Date la risposta sia in esadecimale che in decimale. Per rispondere a questa domanda, dovete guardare nell'intestazione del datagramma IP contenente il segmento UDP (vedere Figura 4.13 nel libro di testo e la discussione sui campi dell'intestazione IP).
7. Esaminare una coppia di pacchetti UDP per la quale il primo pacchetto è mandato dal vostro host e il secondo pacchetto è una risposta al primo. Descrivere la relazione esistente tra i numeri di porta dei due pacchetti.