Laboratorio di Sistemi & Reti

Esercitazione di Wireshark – protocollo UDP

classe 4.ta G . a.s. 2017/2018

Scopo di questa esercitazione è quello di studiare, dal punto di vista pratico, il protocollo di trasporto UDP, attraverso l’analisi dei pacchetti trasmessi in rete.

Per farlo occorre avviare il programma Wireshark (anche nella modalità legacy) e svolgere quanto descritto di seguito.

**Il compito**

1. Avviare Wireshark
2. Aprire il file *udp1.pcap* contenente traffico di rete catturato e memorizzato pronto per l’analisi
3. Impostare il filtro in maniera che vengano visualizzati solo i

pacchetti UDP

1. Facendo riferimento al primo di questi pacchetti (n.ro **76**), espandere i campi UDP nella finestra dei dettagli
2. Riconoscere il numero dei campi presenti nell’intestazione UDP:
3. Denominare i campi osservati:

– Source port,destination port, lenght,checksum header

1. Determinare la lunghezza (in Byte) di ognuno dei campi dell'intestazione UDP

– 2 byte (16bit)

1. Qual è il significato del valore del campo “Length”?

– Contiene la lunghezza totale del datagramma udp (header+dati)

1. Verificare la risposta data al punto 8. controllando altri pacchetti UDP catturati (es.77,78)

1. Qual è il massimo numero di Byte che può essere incluso nel “carico” di un pacchetto UDP?

– 4 byte

1. Qual è il valore più grande possibile per il numero di porta sorgente?

– 65535

1. Qual è il numero del protocollo UDP? Dare la risposta sia in esadecimale che in decimale.

– 0/17 00 11

1. Quali sono i campi su cui viene calcolato il checksum UDP?

– source ip,destination ip, udp protocol, padding-lenght,udp source port,udp destination port,udp lenght,udp data

1. Esaminare una coppia di pacchetti UDP per la quale il primo pacchetto è mandato dall’host locale e il secondo pacchetto è una risposta al primo. Descrivere la relazione esistente tra i numeri di porta dei due pacchetti.

la source port e la destination port risultano invertiti

1. Calcolare il valore checksum secondo l’algoritmo espresso nell’RFC 1071, su un pacchetto UDP (es. n.ro 76) e verificarne la corrispondenza con il valore del checksum espresso nel pacchetto.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_