Esercitazione di Laboratorio - NA03

Riccardo Persello

9 giugno 2021

Apertura di connessioni TCP e scambio dati

Mediante il comando DOS `nslookup`, interrogate il DNS per individuare l'indirizzo IP del server web `allegro.diegm.uniud.it`. Attivate la cattura dei pacchetti sul vostro calcolatore. Aprite una pagina web e accedete al sito `http://allegro.diegm.uniud.it`. Terminate la cattura dei pacchetti e analizzate quelli relativi all'apertura della connessione TCP.

1. **Individuate la sequenza di pacchetti relative all'apertura della connessione. Che numeri di sequenza e di acknowledge contengono?**

SYN	Mittente	Destinatario	SEQ	ACK
1	client	server	*2602003989*	0
1	server	client	**2025975981**	*2602003990*
0	client	server	*2602003990*	**2025975982**

2. **I successivi messaggi con ogni probabilità sfrutteranno il piggybacking. Riuscite ad individuarli? Provate a verificare la correttezza dei numeri di acknowledge rispetto ai numeri di sequenza contenuti nei pacchetti immediatamente precedenti a quelli osservati. Scrivete i numeri di sequenza, lunghezza e acknowledge di tre pacchetti consecutivi e verificate la coerenza della numerazione:**

Mittente	Destinatario	SEQ	ACK	LEN
client	server	*2602003990*	**2025975982**	*637*
server	client	**2025975982**	*2602004627*	0
server	client	**2025975982**	*2602004627*	**806**
client	server	*2602004627*	**2025976788**	0

(Si è riportato un pacchetto in più per poter mostrare l'acknowledge

rispetto al precedente).

3. **Individuate ora alcuni pacchetti contenenti i dati relativi alla pagina web visualizzata e identificate, nella vista esadecimale del pacchetto, le buste di livello trasporto, rete, LLC e MAC, riportando i valori dei campi più significativi discussi a lezione.**

```
0000   a0 78 17 83 57 03 52 7a c5 ab f2 64 08 00 45 00
0010   03 5a 70 27 00 00 3d 06 99 bb 9e 6e 1c 32 ac 14
0020   0a 07 00 50 cb 06 78 c1 f0 ae 9b 17 70 93 80 18
0030   03 d9 2c bf 00 00 01 01 08 0a d7 75 80 90 ab b5
0040   cd 58 .. .. .. .. .. .. .. .. .. .. .. .. .. ..
```

MAC

- `a0 78 17 83 57 03`: Indirizzo fisico del dispositivo mittente (unicast).
- `52 7a c5 ab f2 64`: Indirizzo fisico del dispositivo destinatario (unicast).
- `08 00`: Protocollo di livello superiore: IPv4

IP

- `45` = `0100 0101` = `0x04 << 4 | 0x05`: IPv4, lunghezza intestazione: 5 blocchi da 32 bit (20 byte).
- `00` = `000000 00`: *Type of Service*/DSCP+ECN, tutto default (primi sei bit: *class selector* 0, *best effort*, ultimi due bit: *Non-ECN Capable Transport*).
- `03 5A` = **858**: Lunghezza totale della trama IP.
- `70 27`: Identificatore del pacchetto, sequenziale rispetto agli altri pacchetti inviati dal server.
- `00`: *Flags*, tutti spenti (Reserved: 0, DF: 0, MF: 0).
- `00`: Offset del frammento: 0 (in quanto il pacchetto non è frammentato).
- `3D` = **61**: TTL.
- `06`: Protocollo di livello superiore: TCP.
- `99 BB`: Somma di controllo dell'intestazione.
- `9E 6E 1C 32` = **158.110.28.50**: Indirizzo IP del mittente.
- `AC 14 0A 07` = **172.20.10.7**: Indirizzo IP del destinatario (privato).

TCP

- `00 50` = **80**: Numero della porta di partenza.
- `CB 06` = **51974**: Numero della porta di arrivo.
- `78 C1 F0 AE` = **2025975982**: *Sequence number*.
- `9B 17 70 93` = **2602004627**: *Acknowledgement number*.

- `8. ..`: Lunghezza intestazione: 32 byte (8 blocchi da 32 bit).
- `.0 18`: *Flags*: ACK, PSH.
- `03 D9` = **985**: Window size.
- `2C BF`: Checksum.
- `00 00`: Urgent pointer.
- `01 01 08 0A D7 75 80 90 AB B5 CD 58`: Opzioni.

Segmenti TCP

1. **Eseguite i più volte i programmi (`winsize`) premendo invio in successioni differenti. Cosa osservate?**

   La quantità di dati ricevuta dal server in ogni pacchetto è variabile. Inoltre, se si comincia a trasmettere dati prima che il server sia in ascolto, i dati si accumulano.

2. **Se disponete di due computer, ripetete l'esperimento durante la cattura del traffico tramite Wireshark e analizzate i pacchetti relativi a tale connessione. Riportate nel seguito la sequenza di valori del campo window size che avete osservato.**

Sempre pari a 6379 (in un setup con singolo dispositivo in configurazione loopback).

Messaggi UDP

Si effettui una interrogazione al DNS tramite nslookup durante una sessione di cattura del traffico. Si osservino i pacchetti relativi alla richiesta e alla relativa risposta e si riportino nel seguito i dati relativi alla busta del livello di trasporto.

Sia la richiesta che la risposta sono trasmesse via messaggi UDP. Per la richiesta, la porta di partenza è la 49250, mentre quella di destinazione è la 53. Per la risposta, la situazione è opposta.

La lunghezza della richiesta è di 48 byte, di cui 40 di payload. La lunghezza della risposta è di 64 byte, di cui 56 di payload.

Entrambe presentano due byte di checksum, `0x550c` per la richiesta e `0x4821` per la risposta.

La sorgente del documento è disponibile al seguente indirizzo: https://github.com/persello/esercizi-rdc. Documento generato con pandoc.