

Tugas 03 – Memahami protocol TCP

Tujuan

- Memahami cara kerja protocol TCP
- Mampu menggunakan aplikasi *Wireshark* untuk analisis packet

Sifat tugas

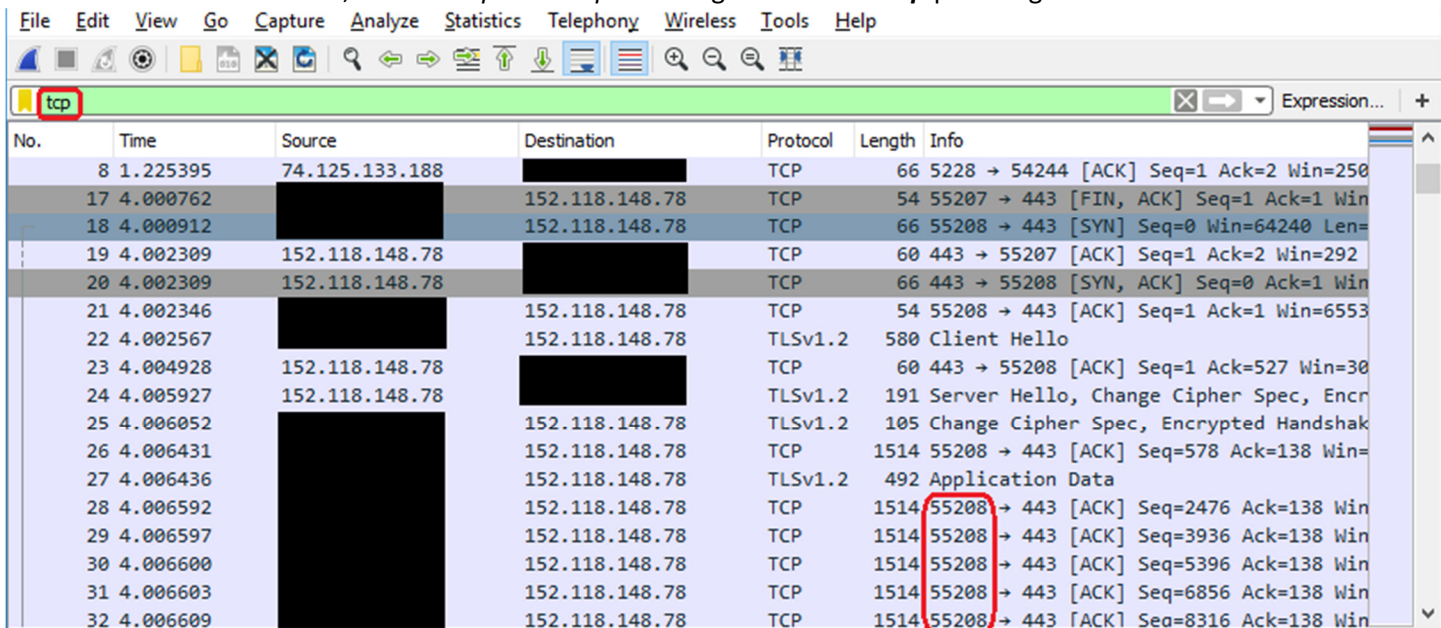
Individu

Deadline

Kamis, 17 Oktober 2019, pukul 23.55 WIB

Instruksi

1. Unduh file `alice.txt` yang ada pada tautan: <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>.
2. Buka tautan berikut: <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html>. Klik tombol *Browse* untuk memilih file `alice.txt` yang sebelumnya diunduh. Tapi jangan klik tombol *Upload alice.txt file* dulu!
3. Jalankan aplikasi *Wireshark* dan mulai *packet capture* (Catatan: pastikan memilih *network interface* yang digunakan oleh perangkat kalian untuk mengakses internet saat memulai capture)
4. Klik tombol *Upload alice.txt file* untuk mengunggah file `alice.txt`, lalu tunggu hingga file selesai diunggah.
5. *Stop packet capture* pada *Wireshark*, jika perlu simpan hasil *packet capture* tersebut (*File -> Save*)
6. Untuk memudahkan analisis, filter hasil *packet capture* dengan kata kunci ***tcp*** pada bagian kiri atas



No.	Time	Source	Destination	Protocol	Length	Info
8	1.225395	74.125.133.188	[REDACTED]	TCP	66	5228 → 54244 [ACK] Seq=1 Ack=2 Win=250
17	4.000762	[REDACTED]	152.118.148.78	TCP	54	55207 → 443 [FIN, ACK] Seq=1 Ack=1 Win=
18	4.000912	[REDACTED]	152.118.148.78	TCP	66	55208 → 443 [SYN] Seq=0 Win=64240 Len=
19	4.002309	152.118.148.78	[REDACTED]	TCP	60	443 → 55207 [ACK] Seq=1 Ack=2 Win=292
20	4.002309	152.118.148.78	[REDACTED]	TCP	66	443 → 55208 [SYN, ACK] Seq=0 Ack=1 Win=
21	4.002346	[REDACTED]	152.118.148.78	TCP	54	55208 → 443 [ACK] Seq=1 Ack=1 Win=6553
22	4.002567	[REDACTED]	152.118.148.78	TLSv1.2	580	Client Hello
23	4.004928	152.118.148.78	[REDACTED]	TCP	60	443 → 55208 [ACK] Seq=1 Ack=527 Win=30
24	4.005927	152.118.148.78	[REDACTED]	TLSv1.2	191	Server Hello, Change Cipher Spec, Encr
25	4.006052	[REDACTED]	152.118.148.78	TLSv1.2	105	Change Cipher Spec, Encrypted Handshak
26	4.006431	[REDACTED]	152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=578 Ack=138 Win=
27	4.006436	[REDACTED]	152.118.148.78	TLSv1.2	492	Application Data
28	4.006592	[REDACTED]	152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=2476 Ack=138 Win=
29	4.006597	[REDACTED]	152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=3936 Ack=138 Win=
30	4.006600	[REDACTED]	152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=5396 Ack=138 Win=
31	4.006603	[REDACTED]	152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=6856 Ack=138 Win=
32	4.006609	[REDACTED]	152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=8316 Ack=138 Win=

7. Lalu agar tidak tercampur dengan koneksi TCP yang lain, filter lagi dengan port yang digunakan oleh perangkat kalian untuk mengunggah file ke slot di `gaia`, dengan melihat *source port* yang bernilai sama dan beberapa kali melakukan pengiriman segmen secara berturut-turut. Pada contoh di atas port yang digunakan adalah ***55208***. Filter yang digunakan kali ini adalah: ***tcp.port == 55208***

tcp.port == 55208							Expression...	+
No.	Time	Source	Destination	Protocol	Length	Info		
18	4.000912		152.118.148.78	TCP	66	55208 → 443 [SYN] Seq=0 Win=64240 Len=		
20	4.002309	152.118.148.78		TCP	66	443 → 55208 [SYN, ACK] Seq=0 Ack=1 Win=		
21	4.002346		152.118.148.78	TCP	54	55208 → 443 [ACK] Seq=1 Ack=1 Win=6553		
22	4.002567		152.118.148.78	TLSv1.2	580	Client Hello		
23	4.004928	152.118.148.78		TCP	60	443 → 55208 [ACK] Seq=1 Ack=527 Win=30		
24	4.005927	152.118.148.78		TLSv1.2	191	Server Hello, Change Cipher Spec, Encr		
25	4.006052		152.118.148.78	TLSv1.2	105	Change Cipher Spec, Encrypted Handshak		
26	4.006431		152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=578 Ack=138 Win=		
27	4.006436		152.118.148.78	TLSv1.2	492	Application Data		
28	4.006592		152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=2476 Ack=138 Win=		
29	4.006597		152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=3936 Ack=138 Win=		
30	4.006600		152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=5396 Ack=138 Win=		
31	4.006603		152.118.148.78	TCP	1514	55208 → 443 [ACK] Seq=6856 Ack=138 Win=		

8. Jawablah pertanyaan-pertanyaan berikut dengan screen shot yang relevan!

Pertanyaan

1. Berapa alamat IP dan port yang digunakan oleh perangkat kalian untuk mengunggah file ke *gaia*?
2. Berapa sequence number dari segmen TCP SYN yang digunakan untuk menginisiasi koneksi TCP antara perangkat kalian dengan server *gaia*? Informasi apa yang terdapat pada header yang menandakan bahwa segmen tersebut merupakan segmen TCP SYN?
3. Berapa sequence number dari segmen SYNACK yang dikirim oleh server *gaia* ke perangkat kalian sebagai *reply* dari SYN? Berapa ACK number pada segmen SYNACK tersebut? Bagaimana server *gaia* menentukan nilai tersebut (ACK number)? Informasi apa yang menandakan bahwa segmen tersebut merupakan segmen SYNACK?
4. Berapa sequence number dari segmen TCP yang merupakan packet TLS dan berisi informasi *Client Hello*? Berapa panjang dari segmen TCP tersebut?
5. Berapa panjang masing-masing 6 (enam) segmen TCP yang pertama selain dari packet TLS (dari *client* ke *server*)?
6. Berapa ukuran *receive window* minimum dari keseluruhan trace *Wireshark* yang kalian dapatkan? Dari contoh tersebut (dengan screen shot), jelaskan apakah nilai *receive window* tersebut dimiliki oleh *client* (perangkat kalian) atau *server* (*gaia*)?
7. Apakah ada segmen yang di-transmisikan ulang (*retransmission*)? Bagaimana cara mengetahui adanya segmen tersebut pada hasil trace *Wireshark*?
8. Berapa jumlah segmen yang di *acknowledge* oleh server *gaia* dalam satu ACK (Pada ACK ke – 2, selain ACK pada *three-way handshake*)? Adakah kasus dimana server *gaia* mengirimkan ACK setelah menerima 1 segmen (lagi-lagi selain ACK pada *three-way handshake*)?

Lakukan hal berikut untuk pertanyaan 9 – 10. Pilih menu: *Statistics* -> *TCP Stream Graphs* -> *Time-Sequence (Stevens)*. Lalu kalian akan melihat plot dari segmen-segmen yang dikirim ke server *gaia* terhadap waktu.

9. Dapatkan kalian menunjukkan kapan *TCP slow start* dimulai dan berakhir?
10. Berikan penjelasan terkait perbedaan hasil *packet capture* dengan karakteristik *TCP congestion control* yang ideal seperti yang dipelajari di kelas!

Pengumpulan

Kumpulkan file **t3_NPM-Nama.doc/docx/odt/pdf**

Selamat mengerjakan