Ostbayerische Technische Hochschule Regensburg

K. Spörl

Lösungen zu TCPIP 4

(01.10.2017)

2 ANALYSE DER TCP SCHICHT

☑ Welche Nummer hat der FTP-Server Port? Welchen Port verwendet der Client?
Server = 21, Client = 1038

☑ Was ist bezüglich der Seq/Ack Nummerierung bei den Frames 4 bis 6 geschehen? Warum blieb der Zähler stehen?
Nur bei SYN wird ACK um 1 Inkrementiert. Bei Frame 5 Wurde nur das 2. ACK gesendet und keine Daten übertragen. Darum bleibt SEQ/ACK unverändert.

☑ Wie wird eine TCP-Verbindung eröffnet? Welche Bits im TCP-Header sind dafür nötig? Wie viele Frames werden dafür benötigt?
Drei Frames Nr.: 3, 4 und 5,, SYN-Flag

☑ Wie wird eine TCP-Verbindung geschlossen? Welche Bits im TCP-Header sind dafür nötig? Wie viele Frames werden dafür benötigt?
Drei oder Vier Frames Nr: 85, 88, 89 und 90. FIN-Flag

☑ Was ist bei den Frames 85 bis 87 geschehen?
Frames kamen in der falschen Reihenfolge an.

☑ Ist es möglich, dass IP-Frames nicht in der selben Reihenfolge ankommen, wie sie abgeschickt wurden?
Ja, siehe oben

☑ Mit welcher Sequenznummer startet die TCP-Verbindung wirklich?
0x25 cf d3 8b = 634377099

☑ Wie könnten Sie die Anzahl der mit TCP übertragenen Bytes in Frame Nr. 10 ermitteln, wenn Sie die Angabe der Länge (Len=...) nicht hätten?
Ack (Frame 11) - Seq (Frame 10) = 1350 - 343 =1007

- Verwenden Sie einen geeigneten Displayfilter und überprüfen Sie, ob Datenframes verloren gingen und wiederholt werden mussten (Retransmission).
tcp.analysis.retransmission
- Verwenden Sie einen geeigneten Displayfilter und überprüfen Sie, ob Bestätigungen (Ack) verloren gingen und wiederholt werden mussten.
tcp.analysis.duplicate_ack

3 EIGENE MESSUNGEN IM INTERNET

☑ Wer beginnt den Verbindungsaufbau auf TCP Ebene?
Labor-PC

☑ Wie viele TCP-Verbindungen werden für die Übertragung dieser einen Webseite geöffnet?
ip.dst==194.95.109.89 and tcp.flags.syn==1
Mehrere, da jedes Objekt eine extra Session bekommt.

☑ Welche Optionen werden auf IP- und TCP Ebene ausgehandelt ?
Diverse. Nachschlagen bei Wikipedia.

☑ Können Sie den Inhalt der übertragenen Webseite erkennen?
Ja, da unverschlüsselt übertragen wird.

☑ Welcher Record-Type brachte bei der DNS Namensauflösung Erfolg?
A

☑ Sind die TCP-Daten bei IPv4 wesentlich anders als bei IPv6?
Nein

☑ Sind die HTTP-Daten bei beiden Protokollen unterschiedlich?
Nein

☑ Welcher Record-Type brachte bei der DNS Namensauflösung Erfolg?
AAAA

4 MESSUNG MIT DATENVERSCHLÜSSELUNG

- Stoppen Sie die Aufzeichnung in Wireshark wieder und analysieren Sie die aufgezeichneten Datenpakete auf HTTP-Ebene. Verwenden Sie geeignete Displayfilter um nur die Frames von und zum HTTP-Server anzuzeigen.
  tcp.port==443 oder ip.addr==194.95.109. 89 oder ipv6.addr==2001:638:a01:3f80::8089

☑ Können Sie auf HTTP-Ebene den Inhalt der Webseite erkennen?
Nein

☑ Was wurde am Anfang zusätzlich übertragen bzw. ausgehandelt?
TLS v1.2

5 ANALYSE DER UDP-SCHICHT

☑ Welche Felder hat der UDP-Header im Wesentlichen?
Port Nummern

☑ Lässt das vermuten, dass es eine Datensicherung und/oder eine Flusskontrolle gibt?
Nein

☑ Was ist eigentlich die Aufgabe eines UDP-Protokolls?
Ports

☑ Was könnten Vorteile von UDP gegenüber TCP sein?
Weniger Overhead, Übermittlung auch auf unstabilen Übertragungswegen möglich.

☑ Was sind die Vorteile von TCP gegenüber UDP?
Datensicherung, Flusskontrolle