Hochschule Darmstadt
Department of Computer Science
Bachelor of Computer Science
Christian Rathgeb, Ulrich Scherhag, Jannis Priesnitz

SS 2020
12. Juni 2020

IT-Sicherheit, Praktikum 4

Aufgabe 1 (Netzwerkanalyse)

In dieser Aufgabe sollen Sie den Netzwerkmitschnitt analysieren, der in der Datei `capture-270518.pcap` gespeichert ist.

(a) Geben Sie die Frame-Nummer, die IP-Adresse und die MAC-Adresse des Hosts an, auf dem der Mitschnitt erzeugt wurde. Dieser Host ist im Folgenden der Client.

(b) Geben Sie die Frame-Nummer, die IP-Adresse und die URL des Webservers an, mit dem der Client die erste HTTP-Verbindung aufbaut. Geben Sie jeweils auch die Client- und Serverseitigen Ports dieser HTTP-Verbindung an.

(c) Geben Sie die Frame-Nummern und die IP-Adresse des DNS-Servers der Verbindung auf die Webseite Wikipedia.de an. Analysieren Sie die Anfragen (Requests) an den DNS-Server und die dazugehörigen Antworten (Responses) und geben Sie an, welche IP-Adressen der DNS-Server an den Client gesendet hat.

(d) Sehen Sie sich nun die *zweite!* TLS-Verbindung an, die der Client aufbaut. Mit welcher URL will sich der Client verbinden? Im Folgenden heißt diese Verbindung 'sichere Verbindung'. Welche Frame-Nummern enthalten den TLS-Verbindungsaufbau?

(e) Geben Sie für die sichere Verbindung aus der vorherigen Aufgabe die Frame-Nummer, die verwendete CipherSuite an und bewerten Sie deren Sicherheit. Bestimmen Sie darüber hinaus die CommonName(s) der Zertifikatskette des Server-Zertifikats.

(f) Geben Sie für die sichere Verbindung auch an, welcher Kommunikationspartner sich authentisiert.

(g) Der Aufbau gesicherter Verbindungen kann durchaus fehlschlagen. Bei der Authentisierung des Servers ist die Korrektheit der im Zertifikat angegebenen Adresse absolut notwendig. Finden Sie heraus, weshalb der Verbindungsaufbau zur Webseite `www.trickdog-dueren.de` fehlgeschlagen ist. Skizzieren Sie die relevante Kommunikation zwischen dem Client und dem Aufruf der Webseite (d.h. von DNS-Auflösung bis einschließlich TCP-Verbindungsabbau) in eigenen kurzen Worten und geben Sie für jede Beschreibung die passende Frame-Nummer an.