Vorlesung Netzwerksicherheit – Sommersemester 2023

3. Übungszettel

Abgabe bis Dienstag, 9. Mai 2023 – 16:00 Uhr
Besprechung: Dienstag, 9. Mai 2023

Abgabe in festen Gruppen (Namen + Matrikelnummern angeben)

Abgabe via Artemis: https://alpro.besec.uni-bonn.de

Aufgabe 1 (5 Punkte)

Geben Sie die Funktionsweise des in der Vorlesung gezeigten TLS Handshake Protocol in eigenen Worten wieder. Erläutern Sie dabei ausführlich, welche Informationen in den einzelnen Schritten geteilt oder abgefragt werden und welchem Zweck die einzelnen Schritte dienen.

Aufgabe 2 (5 Punkte)

TLS lässt sich, bezogen auf das ISO/OSI-Schichtenmodell, in den Schichten Session und Presentation verorten. Begründen Sie diese Tatsache für beide Schichten ausführlich und stellen Sie den Zusammenhang von der Transport- bis zur Anwendungsschicht dar.

Aufgabe 3 (3 Punkte)

Begründen Sie ausführlich, auf welcher Schicht des TCP/IP-Modells Sie TLS verorten und welche Folgen dies für den Zusammenhang zwischen Transport- und Anwendungsschicht hat.

Aufgabe 4 (5 + 2 Punkte)

In der Vorlesung wurde diskutiert, dass Webbrowser und Webserver nicht alle TLS Cipher Suites unterstützen.

a) Finden Sie heraus, welche Cipher Suites Ihre TLS-Bibliothek (OpenSSL, Gnutls etc.) zur Verfügung stellt und vergleichen Sie diese mit der Liste in Ihrem Webbrowser. Dokumentieren Sie die durchgeführten Schritte und geben Sie Zwischenergebnisse an.
b) Ermitteln Sie die Cipher Suites, mit denen Sie eine Verbindung zur Weseite der Vorlesung und Übung (https://net.cs.uni-bonn.de) aufbauen können. Dokumentieren Sie die durchgeführten Schritte und geben Sie Zwischenergebnisse an.