Vorlesung Netzwerksicherheit – Sommersemester 2023

11. Übungszettel

Abgabe bis Dienstag, 11. Juli 2023 – 16:00 Uhr
Besprechung: Dienstag, 11. Juli 2023

Abgabe in festen Gruppen (Namen + Matrikelnummern angeben)

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

Aufgabe 1 (6 Punkte)

a) Beschreiben Sie, welche Anforderungen an die Kommunikation Benutzer:innen eines privaten Netzwerks haben.
b) Beschreiben Sie die Merkmale eines privaten Netzwerks und skizzieren Sie einen exemplarischen Aufbau.
c) Welche Möglichkeiten gibt es, ein gemeinsames privates Netzwerk über mehrere Standorte zu betreiben. In welche Netzwerkkategorie (PAN, LAN, WAN, …) gehört dieses Netzwerk?

Aufgabe 2 (7,5 Punkte)

a) Beschreiben Sie das Konzept eines Overlay-Netzwerks mit ihren eigenen Worten. Berücksichtigen Sie dabei die Position im TCP/IP-Protokollstapel sowie die verwendeten Protokolle von IP bis zum Anwendungsprotokoll.
b) Nennen Sie die unterschiedlichen Modi bei IPSec.
c) Bei welchem Modus ist IPSec ein Overlay-Netzwerk? Begründen Sie Ihre Antwort.

Aufgabe 3 (4 Punkte)

a) Erklären Sie den Unterschied zwischen einem „Tunnel“ und einem „VPN“.
b) Wofür stehen bei IPSec die Begriffe AH und ESP und worin unterscheiden sich diese?
c) Beschreiben Sie die Aufgabe des SPD-Cache bei IPSec und geben Sie an, ob dieser Cache bei eingehenden oder ausgehenden Verbindungen benötigt wird.
d) Skizzieren Sie den Unterscheid zwischen einer Security Association und einer Security Policy.

Aufgabe 4 (6 Punkte)

Beantworten Sie die folgenden Fragen zu Shared-Secrets:

a) Was ist ein Shared-Secret und wofür kann es verwendet werden?
b) Warum eignen sich Shared-Secrets zur Authentifikation im Internet?
c) Warum sollten Shared-Secrets beim Diensteanbieter nicht im Klartext abgespeichert werden und welche Verfahren kennen Sie, wo dies trotzdem notwendig ist?

Aufgabe 5 (1,5 + 1 Punkte)

a) Installieren Sie Wireguard, erzeugen Sie sich ein Schlüsselpaar und geben Sie den öffentlichen Schlüssel an.
b) Geben Sie an, welche Elliptische Kurve für die Erzeugung des Schlüsselpaars verwendet wurde.