

11. Übungszettel

Abgabe: Bis Dienstag, 13. Juli 2021 – 16:00 Uhr

Besprechung: Dienstag, 13. Juli 2021

Abgabe in Gruppen von 2-3 Personen (Name + Matrikelnummer angeben)

Abgabe via Artemis

Aufgabe 1 (6 Punkte)

- a) Welche Anforderungen an die Kommunikation haben Benutzer eines privaten Netzwerks?
- 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) Welche unterschiedlichen Modi gibt es bei IPSec?
- c) Bei welchem Modus ist IPSec ein Overlay-Netzwerk? Begründen Sie Ihre Antwort.

Aufgabe 3 (4 Punkte)

- a) Was ist der Unterschied zwischen einem "Tunnel" und einem "VPN"?
- b) Wofür stehen bei IPSec die Begriffe AH und ESP, worin unterscheiden sich diese?
- c) Beschreiben Sie die Aufgabe des SPD-Cache bei IPSec. Benötigen Sie diesen Cache bei eingehenden oder ausgehenden Verbindungen?
- d) Skizzieren Sie den Unterscheid zwischen einer Security Association und einer Security Policy

Aufgabe 4 (1,5 + 1 Punkte)

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