



Aufgaben:

1) *IPsec-VPNs*

Beschreiben Sie, auf welche Weise IPsec-VPNs IP-Pakete verschlüsselt und verschleiert über das Internet transportieren.

2) *Akronyme*

Wofür stehen die folgenden Akronyme?

- HTML
- https
- SIP
- RTP
- TLS

Erläutern Sie kurz das jeweilige Konzept bzw. den jeweiligen Begriff. Geben Sie jeweils ein Anwendungsbeispiel an.

3) *SMTP mit TLS / SSL*

Was ist die Bedeutung der Akronyme SMTP und SSL? Erläutern Sie die sichere SMTP-Kommunikation mit TLS bzw. mit SSL. Wo liegen die Unterschiede?

4) *Internet-Adressen*

Wie ist eine Internet-Adresse (IPv4) aufgebaut? Was ist eine Netzwerkmaske und wofür wird sie eingesetzt? Was ist unter der Netzwerk-Basis-Adresse und was unter der Broadcast-Adresse zu verstehen? Wodurch unterscheiden sich Broadcasts von Unicasts, Anycasts und Multicasts?

5) *Port-Forwarding*

Die Applikation `ssh` (Wofür steht dieses Akronym?) bietet neben den normalen Anwendungen (Welche sind das?) die Fähigkeit der Dienstzugangspunktverlegung:

```
wmit03> ssh -L 8888:lsv0.studs:443 vnachnam@123.studs
```

Mit welcher lokalen URL auf dem Rechner `wmit03` können Sie auf `lsv0.studs:443` zugreifen? Zeichnen Sie eine Skizze mit den Teilverbindungsstrecken zwischen allen drei beteiligten Rechnern, kennzeichnen Sie Quell- und Zielport jeder Teilverbindungsstrecke und markierten Sie den sicheren, kodierten „Tunnel“.

Was sind privilegierte Portnummern? Um welchen Nummernbereich handelt es sich? Wo finden Sie auf UNIX-Rechnern eine Erläuterung der wichtigsten Portnummern?

Bearbeitungszeit: 2 Zeitstunden