Netzwerke – Übung WiSe2018/19

Application Layer

Benjamin.Troester@HTW-Berlin.de
PGP: ADE1 3997 3D5D B25D 3F8F 0A51 A03A 3A24 978D D673

Benjamin Tröster

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

Road-Map

1. Retrospektive
2. Präsentation
   - DNS
3. Krypto
4. SSH

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

Retrospektive

- Vorlesung

Retrospektive

- Vorlesung
  - Retrospektive der Vorlesung – was haben Sie behandelt?

Retrospektive

- Vorlesung
  - Retrospektive der Vorlesung – was haben Sie behandelt?
  - Fragen?

Hochschule für Technik und Wirtschaft Berlin
University of Applied Sciences

1.) DNS

- Erläutern Sie kurz was DNS ist und welche Komponenten das DNS im wesentlichen benötigt um Domainnamen aufzulösen.
- Wie können Domainnamen aufgelöst werden? Wie sieht die Auflösung in der Realität aus?
- Erläutern Sie anhand eines Beispiels, wie die Namensauflösung stattfinden kann.
- Erläutern Sie die Semantik und Syntax der Tool *dig* und *host*.
- Wozu kann (konnte) das Tool *whois* genutzt werden?

2.) Krypto I

- Erläutern Sie kurz, was unter den Begriffen Kryptologie, Kryptografie, Kryptoanalyse verstanden wird.
- Welche Aufgaben sollen mithilfe Kryptografie gewährleistet werden?
- Welche Maßnahmen setzen die eben genannten Aufgaben um?
- Erläutern Sie was unter dem Begriff Kerckhoff'sche Prinzip verstanden wird.

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

3.) Krypto II

- Erläutern Sie kurz welche beiden Verschlüsselungsverfahren ganz grundsätzlich unterschieden werden.
- Was wird unter dem Begriff Hashing verstanden, wie wird diese Idee in der Kryptografie angewandt?
- Erläutern Sie die Aufgabe von kryptografischen Signaturen!

4.) SSH

- Erläutern Sie wo die grundlegenden Konfigurationsdateien liegen und was deren Aufgabe ist.
- Was ist ein Fingerprint in Bezug auf SSH?
- Lassen sich die kryptografischen Schlüssel die in SSH erzeugt wurden wiederverwenden? Oder muss für jeden Teilnehmer ein neues Schlüsselpaar generiert werden?
- Erläutern Sie was unter einem VPN verstanden wird!