Netzwerke – Übung WiSe2018/19

OSI-Stack & Wireshark

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

Semesterendspurt: Klausur

- Die Klausuren rücken näher...
- Jetzt ist der ideale Zeitpunkt um sich auf Klausuren vorzubereiten.
- Stellen Sie fragen zu den VL, Übungsblättern, etc.
- Teilen Sie sich Ihre Zeit sorgfältig ein, lernen Sie konsequent – es lohnt sich!
  - Für die Freunde der Didaktik: Pomodoro-Technik
  - `https://de.wikipedia.org/wiki/Pomodoro-Technik`

Retrospektive

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

1.) Introdcution to Wireshark

- Erläutern Sie was ein Network-Sniffer ist.
- Erklären Sie was Filter sind und wozu diese genutzt werden können.
- Zeigen Sie anhand von Beispielen:
  - Wie stellen Sie Netzwerkinterfaces ein – auf welchem Interface soll der Mitschnitt laufen.
  - Wie filtern Sie nach Protokollen?
  - Wie filtern Sie *MAC*-Adressen?
  - Wie filtern Sie *IP*-Adressen?

2.) ARP

- Wie sieht das Adressschema für MAC-Adressen aus?
- Erläutern Sie wie die Adressauflösung von logischer Adresse (IP) zu physikalischer Adresse vonstatten geht.
- Erläutern Sie die Nutzung der beiden Tools *arp* und *ip neigh* anhand von Beispielen.
- Nennen und erklären Sie was unter den Begriffen ARP-Tabele und ARP-Cache zu verstehen ist.

3.) ARP-Spoofing

- Erläutern Sie was sich hinter dem Akronym *MITM* verbirgt.
- Erläutern Sie weiterhin, was APR-Spoofing und ARP-Cache-Poisoning ist.
- Diskutieren Sie die Vorgehensweise bei den eben genannten Angriffen.
- **Anmerkung:** Möglicherweise hilft Ihnen eine Skizze...

4.) OSI-Modell

- Diskutieren Sie das ISO-OSI-Modell. Wie ist dies aufgebaut. Welche Eigenschaften sind diesem Modell inhärent. Gibt es womöglich auch Nachteile?
- Erläutern Sie die Aufgabe des Link Layers unter Bezugnahme auf Ethernet-Protokolle.
- Erläutern Sie analog dazu den Network-Layer unter Bezugnahme von IP.
- Zeigen Sie für beide Protokolle Beispiele. Erläutern Sie diese Beispiele.

5.) UDP & TCP

- Erläutern Sie die Aufgabe des Transport-Layers im OSI-Modell.
- Erklären Sie was UDP ist und erläutern Sie anhand eines Beispiels wie dieses Protokoll aussieht.
- Erklären Sie was TCP ist und erläutern Sie anhand eines Beispiels wie dieses Protokoll aussieht.
- Worin unterscheiden sich die beiden hier erläuterten Protokolle? Diskutieren Sie die Unterschiede!

6.) Traceroute & Paris-Traceroute

- Erläutern Sie was *Traceroute* ist und wie die Umsetzung des erfolgt.
- Nennen und erklären Sie die Limitationen von *Traceroute*!
- Erläutern Sie die Anomalien die bei verfolgen von Routen entstehen können und warum *Paris-Traceroute* diese auflösen kann.
- Erklären Sie anhand von Beispielen die Syntax von *Traceroute* und *Paris-Traceroute*.