

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

Road-Map

- 1 Hinweis
- 2 Retrospektive
- 3 Präsentation

- Wireshark
- ARP & NDP
- ARP-Spoofing

In English?

Soll die Veranstaltung, d.h. Hausaufgaben, Übungsblätter, Slides, Protokolle etc. in Englisch gehalten werden?

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.) Introduction 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...