Honeynet & Malware Forensics WS18

Fabian Franzen, Julian Kirsch

Chair for IT Security / I20
Prof. Dr. Claudia Eckert
Technische Universität München

26th June 2018
Time and place

When?  Thursday, 14:00 - 16:00
Where? 01.05.013
Goals

▶ What attacks occur regularly on the Internet?
  ▶ Set up an honeypot to collect attack samples
  ▶ Record and analyze them

▶ How does malware look like?
  ▶ get some reversing/forensic skills
  ▶ Comparison with other malware zoos
Honeynets

- We will set up machines and...
- ...build up a test network for packet analysis and separation.
  - Docker, Virtualization, iptables, bridging, intrusion detection.
- ...install different vulnerable software systems.
  - Webshops / CMS, Insecure SSH, Samba shares
- ...Learn how to analyse attacks
  - Wireshark, Logfile analysis, VMI, ...
Registration

► **NO** letter of motivation! Please solve the qualification task...
► ...can be found on our webpage
► Submit the "secret" stored inside the task **and** a "proof of work"
  ► aka. a short description how you solved the task
  ► **NOT** more than 100-150 words!
► Submit till **04.07.18, 23:59**
► Registration using the **matching system** required
► **16** slots

---

1[https://www.sec.in.tum.de/i20/teaching/ws2018/honeynet-praktikum](https://www.sec.in.tum.de/i20/teaching/ws2018/honeynet-praktikum)
Phase I:
- "Usual" practical course (weekly meetings and exercise sheets)
- Set up of your own honeynet and collecting samples.
- Iterative addition of vulnerable services

Phase II:
- "Usual" practical course (weekly meetings and exercise sheets)
- Analysis of incoming connections
- Analysis of given malware samples (from VirusShare) or the ones we collected.

Phase III:
- Final project (under discussion)
Questions?