Honeynet SS17

Bruno Bierbaumer, Thomas Kittel, Julian Kirsch, Sergej Proskurin

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

23 January 2017
Time and place

When? Tuesdays, 10:00
Where? 01.05.013
Registration

- **NO** letter of motivation! Just a task...
  - Visit 131.159.50.247
  - Solve the challenge, then follow instructions
  - Submit till **08.02.2016, 23:59**

- Registration using the **matching system** required
- **DON’T** register without solving the task!
- **DON’T** register without confirmation that you got the slot!
- **8** slots
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, ...
Process

Phase I (2 weeks):

- “Usual” practical course (weekly meetings and exercise sheets)
- Set up of own environment

Phase II (8 weeks):

- “Usual” practical course (weekly meetings and exercise sheets)
- Enhancements of own environment
- Iterative addition of vulnerable services
- Analysis of incoming connections
- Creation of Logfile Analysis Framework

Phase III (3 weeks):

- Final project (short paper and presentation)
Process

- **No teams**
- Every week: Introduction to a new topic
  - ...
- **Weekly exercise sheets**
  - Submission of solutions until the following week *before* the meeting
  - Private demonstration and short explanation of solution during the meeting
Questions?