Honeynets

Jonas Pfoh & Sebastian Vogl

I20, Chair for IT Security
Technische Universität München
Munich, Germany

April 16, 2013
Honeypot

“A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.”

[Vrable, et al., 2005]
Goals of a Honeynet

- Intrusion Detection
- Analyzing Attacks
- Harvesting Malware
- Testbed for Security Tools
- Teaching/Learning Tool
This course covers...

- Network Architectures
- Firewalls
- Network Monitoring/IDS
- Host Monitoring/IDS
- Penetration Analysis
- Malware Analysis
Expectations

All graded assignments are to be submitted at the beginning of the class session after they are assigned, unless otherwise specified. All homework may be submitted in German or English. Late submissions (without previously speaking to us) will be accepted up to one week after the due date, but the maximum grade you can attain is 3.0. Any submissions later than one week will not be accepted. While we will not be explicitly taking attendance or factoring in a participation grade, we reserve the right to adjust your grade based on either outstanding or very poor engagement.

Homework Submissions:
honeynet-homework@sec.in.tum.de
Grade Breakdown

Weekly Assignments *5  10% each
Setup Presentation  20%
Final Presentation  30%
Curriculum

Week 1  Introduction and Setup
Week 2  Honeynet Policy
Week 4  Firewall Implementation
Week 5  Monitor Implementation
Week 6  Setup Presentations
Week 8  Opening the Floodgates/Packet Analysis
Week 9  An Attacker’s Perspective
Week 10+ Analysis
Week 14 Final Presentations
We will split you into groups of two, each with their own honeypot. With this honeypot you are asked to install and maintain a OS and analyze attacks on that honeynet. Discussing, setting up, and using the monitoring and analysis infrastructure will also be part of our job as a group.

Mailing List: honeynet-praktikum@sec.in.tum.de