Challenges in Network Forensics

Introduction, Disclaimer and Agenda

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy

CIRCL - Computer Incident Response
Center Luxembourg

AIMS 2011

Introduction

- CIRCL (Computer Incident Response Center Luxembourg) is the national Computer Security Incident Response Team (CSIRT) coordination center for the Grand-Duchy of Luxembourg.
- I work there
- and network forensic is one of our daily challenge.

Disclaimer

"*Datasets used and presented in this session are for research only. They might contain sensitive information as well as offensive software like rootkits or malware.*"

Agenda

- (AM) Introduction to Honeypot Technologies.
- (AM) Packet Capture, Filtering and Analysis.
- (AM) Key-value Store - an Introduction to Redis.
- Lunch break
- (PM) Analysis 1*: What happened?
- (PM) Analysis 2†: Is there something suspicious?
- (PM) Analysis 3‡: What can we learn?

---

* honeypot HL5 2002

† DNS test sensor 20110530

‡ honeypot ML jubrowska