Honeynets and Digital Forensics

By

Lance Spitzner

Presented At

The Digital Forensic Research Conference

DFRWS 2004 USA Baltimore, MD (Aug 11th - 13th)

The Honeynet

PROJECT

Automating Forensics

Speaker

- Passion is honeypots.
- President, Honeynet Project
- Author *Honeypots: Tracking* and *Co-Author Know Your Enemy.*
- 8 Years in information security, four years senior security architect Sun Microsystems.
- Former life an officer in Army's Rapid Deployment Force.

Purpose

Challenges we face in forensics and data analysis.

Agenda

- Background on Honeynet Project and our research.
- Forensic challenges we face.

Honeynet Project

Problem

How can we defend against an enemy, when we don't even know who the enemy is?

One Possible Solution

To learn the tools, tactics, and motives of the blackhat community, and share the lessons learned.

Goals

- Awareness: To raise awareness of the threats that exist.
- Information: For those already aware, to teach and inform about the threats.
- Research: To give organizations the capabilities to learn more on their own.

Value of the Project

- Open Source, sharing all of our work, research and findings.
- Everything we capture is happening in the wild (there is no theory.)
- We have no agenda, no employees, nor any product or service to sell (*crummy business model*).

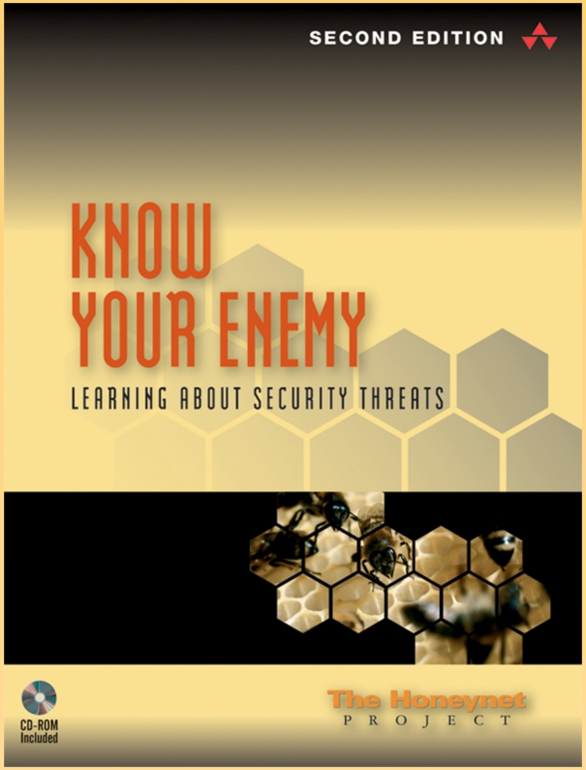
Project Organization

- Non-profit (501c3) organization
- Board of Directors
- No more then two members from any organization.
- Funded by the community, including the NIC.
- Diverse set of skills and experiences.
- Team works virtually, from around the world.

Alliance Members

- South Florida Honeynet Project
- Georia Technical Institute
- Azusa Pacific University
- Paladion Networks Honeynet Project (India)
- Internet Systematics Lab Honeynet Project (Greece)
- Mexico Honeynet (Mexico)
- Honeynet.BR (Brazil)
- Irish Honeynet
- Norwegian Honeynet
- UK Honeynet
- French Honeynet Project
- Italian Honeynet Project

Know Your Enemy: 2nd Edition



http://www.honeynet.org/book

Challenge of forensics

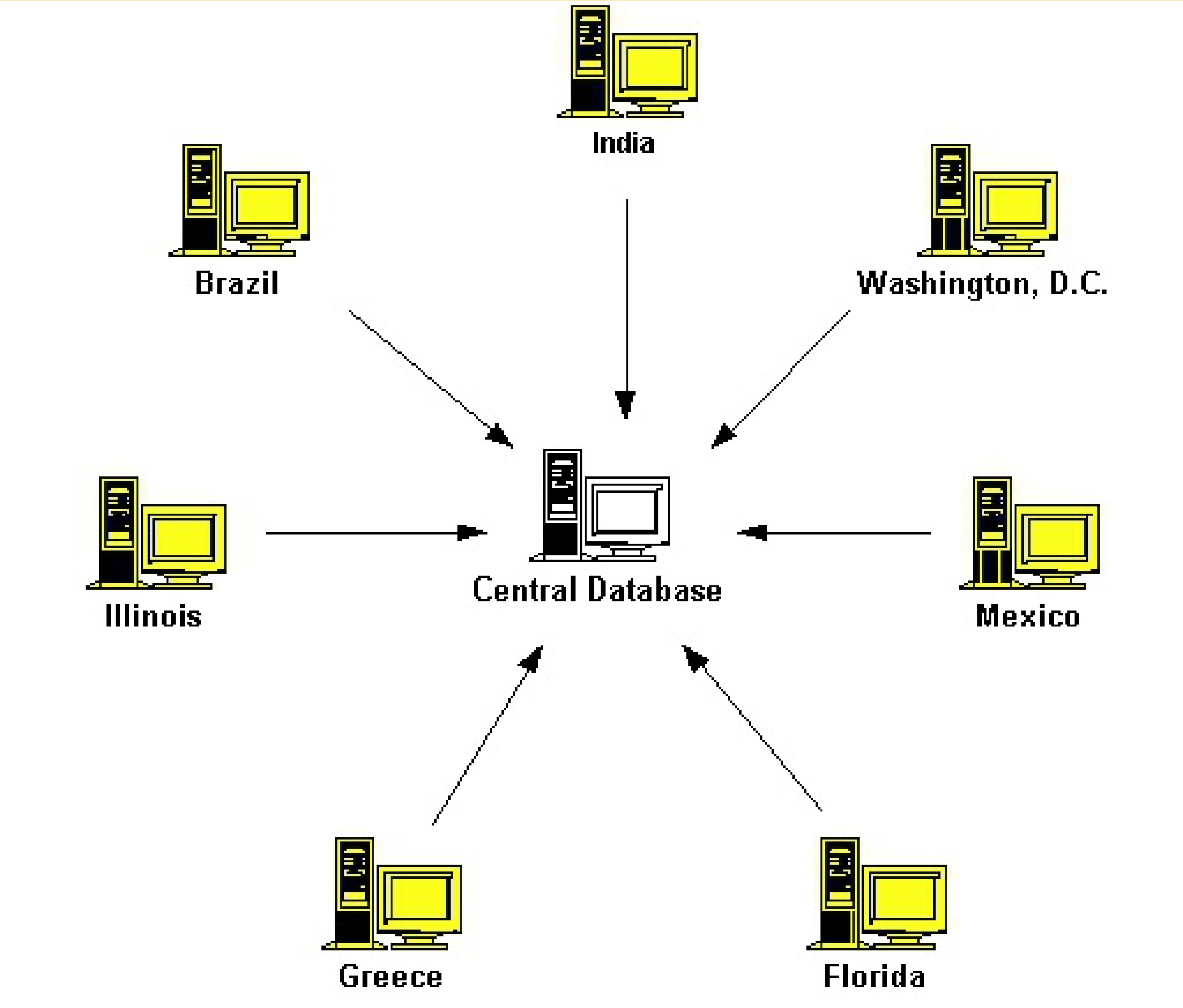
Our Biggest Problems

- Data Overload
- Time to Analyze
- Expertise to Analyze

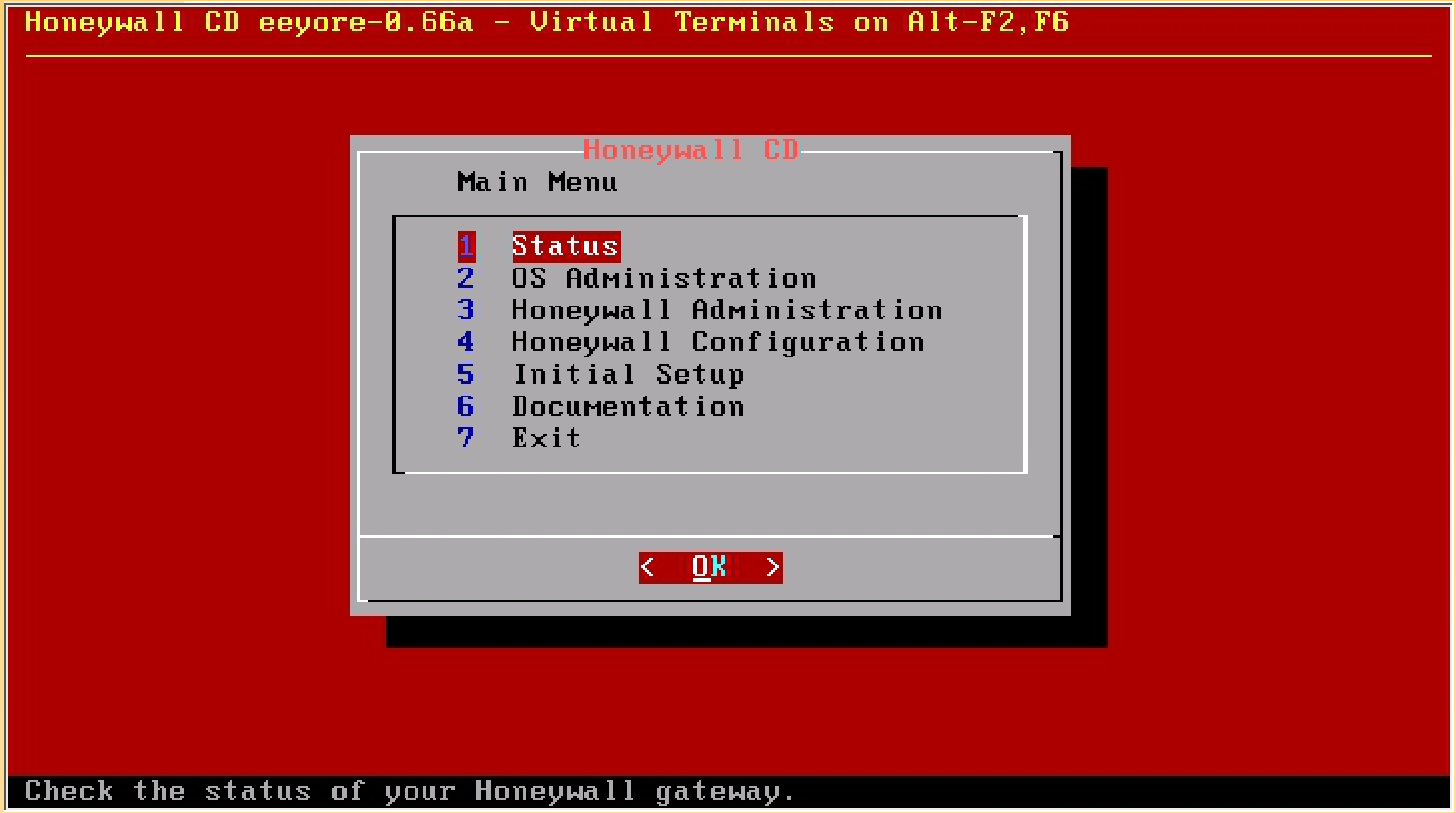
Data Overload

- For our research to be successful, we need to have a lot of different systems hacked around the world.
- That ends up being a lot of data centrally collected.

Distributed Capabilities



Bootable CDROM



```
Honeywall CD eeyore-0.66a - Virtual Terminals on Alt-F2,F6

                    Honeywall CD
      Main Menu

          1  Status
          2  OS Administration
          3  Honeywall Administration
          4  Honeywall Configuration
          5  Initial Setup
          6  Documentation
          7  Exit

                    <  OK  >

Check the status of your Honeywall gateway.
```

Time

- Forensic Challenge - 30 hours
- Reverse Challenge - 80 hours

Expertise

- No single person can know it all.
- Even on a single compromise, require different skill sets.
  - Network captures
  - Host processes, activity, and file systems
  - Reverse Engineering
  - Language skills
  - Profiling

Scan of the Month

- Monthly challenges, over 30 archived.
- No two people analyze the same data the same way.

Forensic Automation

- Method to automate as much of data collection and analysis as possible, minimizing human effort.

- Minimize need for different expertise.

Some Ideas

- Database of clean and hacked images (David Dittrich, University of Washington).
- MD5 checksums of data streams (Bill McCarty, University of Azusa).
- Sebek (Edward Balas of Indiana University).
- User Interface (Edward Balas of Indiana University)
- Automating Data Collection and Analysis(Brian Carrier, Purdue)
- Honeyd (Niels Provos, Google)

Conclusion

Biggest challenges we face

- Too much data
- Not enough time
- Not enough skilled people.

Solution is to automate the process as much as possible.

http://www.honeynet.org

<project@honeynet.org>