Honeypots
Your Speaker

Lance Spitzner
- Senior Security Architect, Sun Microsystems
- Founder of the Honeynet Project
- Author of \textit{Honeypots: Tracking Hackers}
- Co-author of \textit{Know Your Enemy}
- Moderator of \texttt{<honeypots@securityfocus.com>} maillist
- Former ‘tread head’.
Purpose

To introduce you to honeypots, what they are, how they work, their value.
Problem

- Variety of misconceptions about honeypots, everyone has their own definition.

- This confusion has caused lack of understanding, and adoption.
Honeypot Timeline

- 1990/1991 The Cuckoo’s Egg and Evening with Berferd
- 1997 - Deception Toolkit
- 1998 - CyberCop Sting
- 1998 - NetFacade (and Snort)
- 1998 - BackOfficer Friendly
- 1999 - Formation of the Honeynet Project
- 2001 - Worms captured
- 2002 - dtspcd exploit capture
Definition

Any security resource who’s value lies in being probed, attacked, or compromised
How honeypots work

• Simple concept

• A resource that expects no data, so any traffic to or from it is most likely unauthorized activity
Not limited to specific purpose

- Honeypots do not solve a specific problem, instead they are a tool that contribute to your overall security architecture.

- Their value, and the problems they help solve, depend on how build, deploy, and you use them.
Types

- Production (Law Enforcement)
- Research (Counter-Intelligence)

Marty’s idea
Value

- What is the value of honeypots?
- One of the greatest areas of confusion concerning honeypot technologies.
Advantages

- Based on how honeypots conceptually work, they have several advantages.
  - Reduce False Positives and False Negatives
  - Data Value
  - Resources
  - Simplicity
Disadvantages

- Based on the concept of honeypots, they also have disadvantages:
  - Narrow Field of View
  - Fingerprinting
  - Risk
Production

- Prevention
- Detection
- Response
Prevention

- Keeping the burglar out of your house.
- Honeypots, in general are not effective prevention mechanisms.
- Deception, Deterence, Decoys, are psychological weapons. They do NOT work against automated attacks:
  - worms
  - auto-rooters
  - mass-rooters
Detection

- Detecting the burglar when he breaks in.
- Honeypots excel at this capability, due to their advantages.
Response

- Honeypots can be used to help respond to an incident.
  - Can easily be pulled offline (unlike production systems.
  - Little to no data pollution.
Research Honeypots

- Early Warning and Prediction
- Discover new Tools and Tactics
- Understand Motives, Behavior, and Organization
- Develop Analysis and Forensic Skills
Early Warning and Prediction
Tactics
**Motives and Behavior**

**J4ck**: why don't you start charging for packet attacks?

**J4ck**: "give me x amount and I'll take bla bla offline for this amount of time"

**J1LL**: it was illegal last I checked.

**J4ck**: heh, then everything you do is illegal. Why not make money off of it?

**J4ck**: I know plenty of people that'd pay exorbitant amounts for packeting.
Level of Interaction

- Level of Interaction determines amount of functionality a honeypot provides.

- The greater the interaction, the more you can learn.

- The greater the interaction, the more complexity and risk.
Risk

- Chance that an attacker can use your honeypot to harm, attack, or infiltrate other systems or organizations.
Low Interaction

- Provide Emulated Services
- No operating system for attacker to access.
- Information limited to transactional information and attackers activities with emulated services.
High Interaction

- Provide Actual Operating Systems
- Learn extensive amounts of information.
- Extensive risk.
Honeypots

- BackOfficer Friendly

- SPECTER
  - http://www.specter.com

- Honeyd
  - http://www.citi.umich.edu/u/provos/honeyd/

- ManTrap
  - http://www.recourse.com

- Honeynets
  - http://project.honeynet.org/papers/honeynet/
BackOfficer Friendly
Specter
create default
set default personality "FreeBSD 2.2.1-STABLE"
set default default action open
add default tcp port 80 "sh /usr/local/honeyd/scripts/web.sh"
add default tcp port 22 "sh /usr/local/honeyd/scripts/test.sh"
add default tcp port 113 reset
add default tcp port 1 reset

create windows
set windows personality "Windows NT 4.0 Server SP5-SP6"
set windows default action reset
add windows tcp port 80 "sh /usr/local/honeyd/scripts/web.sh"
add windows tcp port 25 block
add windows tcp port 23 proxy real-server.tracking-hackers.com:23
add windows tcp port 22 proxy $ipsrc:22
set template uptime 3284460

bind 192.168.1.200 windows
ManTrap
Honeynets
None, they all have their advantages and disadvantages. It depends on what you are attempting to achieve.
Legal Issues

- Privacy
- Entrapment
- Liability
Legal Contact for .mil / .gov

Department of Justice, Computer Crime and Intellectual Property Section

– General Number: (202) 514-1026
– Specific Contact: Richard Salgado
  • Direct Telephone (202) 353-7848
  • E-Mail: richard.salgado@usdoj.gov

WWW.CYBERCRIME.GOV

Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice
Summary

Honeypots are a highly flexible security tool that can be used in a variety of different deployments.
Resources

Honeypots: Tracking Hackers

http://www.tracking-hackers.com