

# Honeynets

## The Sticky Details

Presented by:  
The NEO Honeynet Group

Information Security Summit  
Warrensville Heights, Ohio  
October 2009

# Overview

- The Honeynet Project
- The NEO Honeynet Group
- Definitions
- History
- Uses
- Technology Tour
- Legal Issues
- Conclusion
- Q&A

# The HoneyNet Project

- International non-profit research organization
- Chapters around the world
- Dedicated to improving the security of the Internet
- Goal - make a difference
  - Raise awareness, provide information & tools
  - Know Your Enemy whitepapers
  - Scan of the Month challenges
  - Great selection of open source tools
  - Google Summer of Code
- [www.honeynet.org](http://www.honeynet.org)

# The Northeast Ohio Honeyynet Group

We are:

- A group of security professionals
- Interested in honeynet technologies
- Not a chapter of The Honeyynet Project at this time
- Just getting started
- Focused on practical, real-world application
- Interested in protecting real networks from real threats

# Definitions

## Honeypot

- A security resource whose value lies in being probed, attacked, or compromised
- Has no production value

## Variations / specific types

- Honeypot - a single system an attacker can interact with
- Honeyynet - an entire network of systems an attacker can interact with
- Other types will be covered in the Technology Tour

# History (Very Brief)

- 1990 - Clifford Stoll - *The Cuckoo's Egg*
- 1991 - Bill Cheswick - *An Evening with Berferd*
- 1997 - Fred Cohen's Deception Toolkit
  - Perl scripts to emulate known UNIX vulnerabilities
- 1998 - First commercial honeypots
  - Create simulated network of vulnerable hosts
- 1999 - The HoneyNet Project founded
- 2001 - Honeypot used to capture Code Red II worm
- 2008 - Darkmarket - FBI honeypot

# Uses

## Collect data on threats

- Detect network probing
- Learn attack techniques
- Identify malicious web sites / content
- Capture malicious code for analysis
- Identify internal threats
- Deflect attacker's attention away from real systems

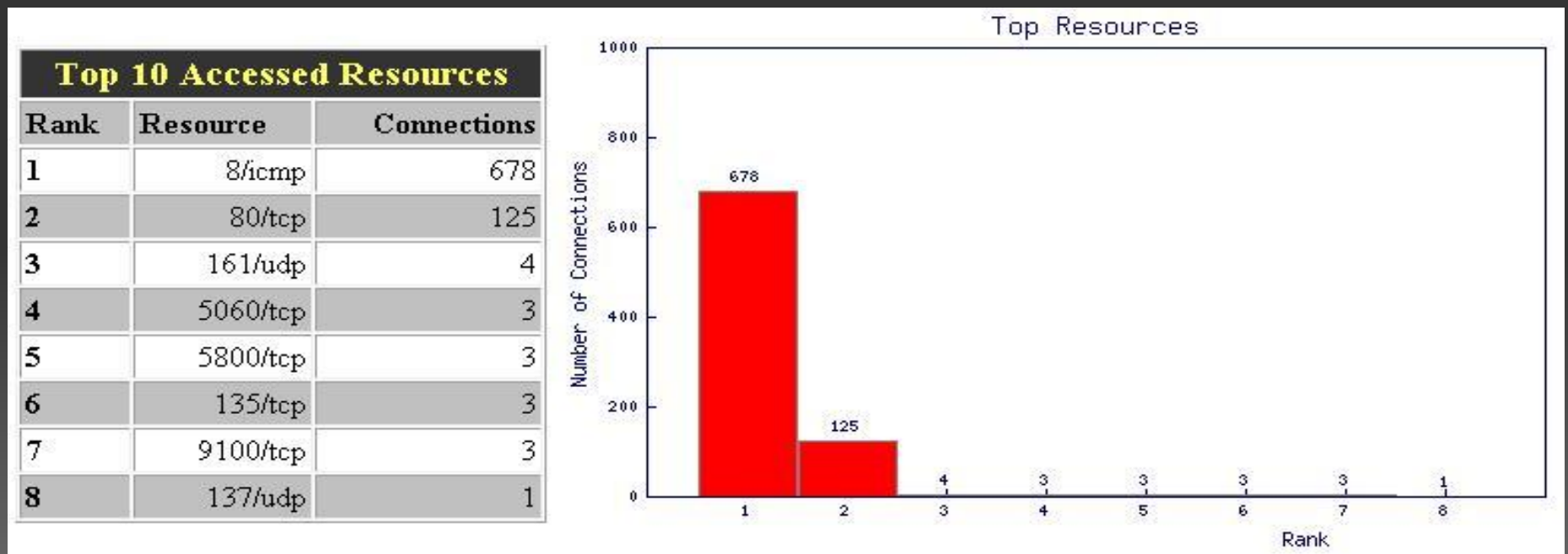
## Using honeypots on a shoestring budget

- Two examples
  - Honeyd
  - Wireshark

# Uses / Example 1

## Honeyd

- Emulates services / daemons (telnet, web server, .....
- Listens on one or many IP addresses
- Records all network traffic sent to it
- Relies on other tools to generate reports (honeydsum.pl)
- Any ideas what caused the results shown below?



# Uses / Example 2

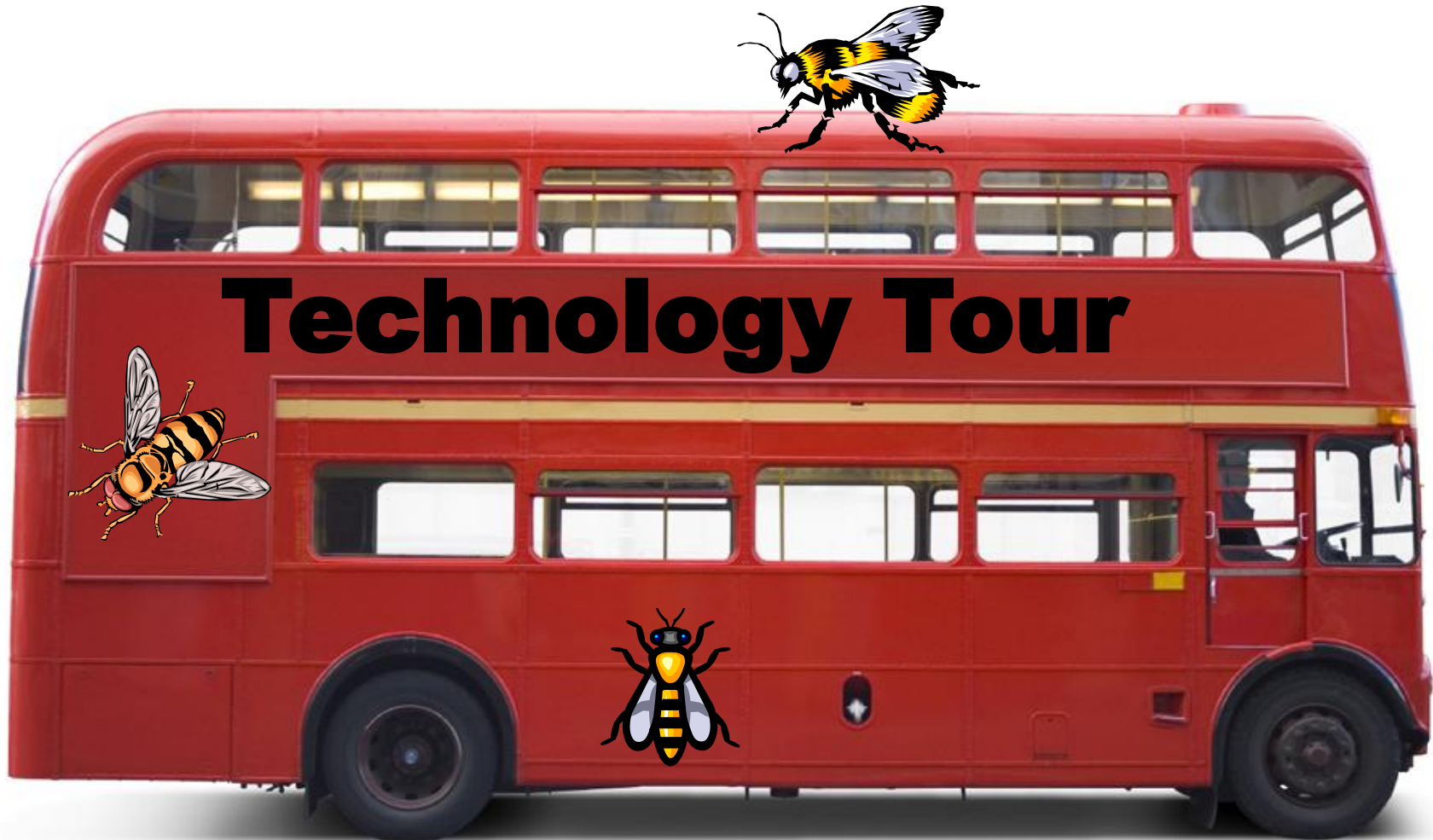
## Wireshark

- Install your org's default OS / software on an old workstation
- Run Wireshark using scripts / batch files
- Add Wireshark filters to eliminate uninteresting traffic
- Tune / improve filters over time
- Remaining traffic can be very interesting!
- Identify network probes, misconfigs, misbehaving devices,...

No. -	Time	Source	Destination	Protocol	Info
13	1.965225	74.125.95.103	192.168.168.8	TCP	[TCP segment of a reassembled PDU]
14	1.965305	192.168.168.8	74.125.95.103	TCP	19119 > http [ACK] Seq=549 Ack=2521 win=65535 L
15	1.965511	74.125.95.103	192.168.168.8	HTTP	HTTP/1.1 200 OK (text/html)
16	2.043214	192.168.254.2	192.168.168.8	TCP	epmap > 19103 [RST, ACK] Seq=0 Ack=0 win=0 Len=
17	2.073841	192.168.168.8	74.125.95.103	TCP	19119 > http [ACK] seq=549 Ack=3191 win=64865 L
18	3.601374	192.168.168.8	151.164.8.201	DNS	Standard query AAAA clients1.google.com
19	3.619561	192.168.168.8	74.125.95.103	HTTP	GET /csi?v=3&s=webhnp&action=&tran=undefined&e=2
20	3.645602	151.164.8.201	192.168.168.8	DNS	Standard query response CNAME clients.1.google.
21	3.650470	192.168.168.8	151.164.8.201	DNS	Standard query A clients1.google.com
22	3.694391	151.164.8.201	192.168.168.8	DNS	Standard query response CNAME clients.1.google.

0000	00 00 86 48 09 0d 00 40	10 13 76 8b 08 00 45 00	...	H...@ ..v...E.
0010	05 14 0a 1d 00 00 34 06	65 32 4a 7d 5f 67 c0 a8	.....	4. e2j}_g..
0020	a8 08 00 50 4a af 8a 62	85 d7 40 23 9d af 50 10	...	PJ..b ..@#..P.
0030	19 b0 1f ca 00 00 c0 56	64 2e 1a 96 6f d8 26 c1	.....	v d...o.&



# Technology Tour

# High-interaction vs. Low-interaction Honeypots

## High interaction:

- Threats exposed to real operating system
- Detection and analysis performed through system state comparison
- Complex and unknown attacker behavior can be analyzed
- Higher risk of the attacker turning the honeypot against you

## Low interaction:

- A program that emulates an operating system or application
- Lower risk of attacker owning the box
- Less chance of learning something unknown
- Detection primarily through log analysis
- Useful for high volume analysis and distributed architectures

# Server vs. Client Honeypots

## Server:

- Passively awaits connections over the network.
- Not advertised to users, so any access is suspicious.

## Client:

- Actively seeks threats by simulating a network client.
- Most research to-date revolves around web threats, however any kind of client could be simulated.

# Examples

## High Interaction : Server

VMware / UML  
Sebek  
Honeywall

## High Interaction : Client

MITRE HoneyClient  
Capture-HPC

## Low Interaction : Server

Honeyd  
DShield Web Honeypot  
Nepenthes

## Low Interaction : Client

HoneyC  
Monkey-Spider

# Examples

## High Interaction : Server

VMware / UML

Sebek

Honeywall

Virtualization is useful for quick rollback of compromised systems.

**Sebek** - kernel module that monitors high interaction honeypot systems for telemetry on attacker activity.

**Honeywall** - provides network activity monitoring and prevents misuse of honeypot. Designed with high-interaction server honeypots in mind, but has broader applications.

# Examples

**Honeyd** - emulates one or many hosts, services, networks; even emulates OS network stack.

**Web Honeyd** - emulates vulnerable web applications; data contributes to DShield project.

**Nepenthes** - special honeypot that collects malware specimens by emulating vulnerabilities and saving the malicious code used against it.

## Low Interaction : Server

Honeyd  
DShield Web Honeyd  
Nepenthes

# Examples

Implementations of the high-interaction honeyclient model drive client applications running within virtual machines to remote resources. System state is monitored for changes that might indicate malicious code.

Virtual machines typically controlled centrally, can be rolled back upon infection and provide feedback to a database on results of browsing activities.

## High Interaction : Client

MITRE HoneyClient  
Capture-HPC

# Examples

**HoneyC** - spiders websites using text file or Yahoo search for seed URL's, Snort signatures scan for malicious content.

**Monkey-Spider** - additional seed input methods, detection by anti-virus signatures.

Low Interaction : Client

HoneyC  
Monkey-Spider

# Examples (2)

Previous examples focus on research, but there are also some commercial implementations.

Websense

McAfee Siteadvisor

Both use intelligence to provide reputation based filtering services to customers.

SPECTRE (NETSEC)

ManTrap (Recourse Technologies)

Two examples of commercially available software; most commonly low-interaction server honeypots.

# Examples (3)

Not all honeypot concepts fit neatly into categories

- Honeytoken - Not a program at all. Data serving no production purpose (fake account number or SSN), if seen traversing the network may indicate misuse.
- Open Proxy Honeypot - Not the target of attack. Emulates an open proxy and permits observation of attacker behavior.

# Legal Issues



# Honeynets - The Sticky Legal and Ethical Aspects

- Challenging technique to deflect attackers from real systems and to contemporaneous and detailed forensic analysis
- With growing popularity concerns have been raised about legal risks of operation
- Careful risk/benefit analysis consisting of adequate information about legal situation

Overview of the legal situation (surely not complete I am not a lawyer) and some flashlights on the ethical aspects

# Main Legal Issues Concerning Operation of a Honeynet System

- Monitoring activities on a honeynet system (privacy)
- Misuse of the system
- Liability to harm of others
- Entrapment

# Monitoring Network Users (Privacy)

## U.S. Statutes

- Wiretap act (federal)
  - Electronic Communications Privacy Act *ECPA* (1986) forbids interception of **content** unless exceptions apply
    1. Provider protection exception
    2. Consent of party exception
    3. Computer trespasser exception
  - Pen register, trap and trace devices Statute  
Governs real-time collection of **non-content** traffic information, exceptions similar to those of wire tap act

**The more the honeynet protects real systems and the more transactional data it collects the less is the risk of violation of privacy laws**

# Misuse of Honeynets

- Network crimes were defined in the Federal Computer Fraud and Abuse Act beside others and state laws
- Provision covers "protected computers"
- Types of network crimes (attack has to result in "damage")
  - DoS and malicious code
  - Intrusions
  - Obtaining information even without damage of integrity or availability
  - Computer-related espionage
  - Trafficking passwords
  - Threatening damage to a computer
  - Attempt to commit a network crime
  - Contraband
  - Crimes committed by juveniles

# Plan What to do When a Honeynet Becomes the Scene of a Crime

- Involve law enforcement
- Establish relationship with law enforcement (i.e. InfraGard Program, field office of Federal Bureau of Investigation and U.S. Secret Service, Electronic Task Forces, state and local law enforcement)
- Call law enforcement as soon as possible not waiting to be called by the police (not for every worm infection!)
- Inform victims

# Liability to Others

- Possible exposure to suits from others harmed by the honeynet
- Still remained an academic discussion
- Ways to reduce risk to be left defendant in civil lawsuit
  - paging or notification system
  - taking honeynet offline while not being able to attend it
  - contact lawyer and law enforcement
  - careful planning and risk analysis with consultation of legal counsel

# Entrapment

*"Entrapment is a law enforcement officer's or government agent's inducement of a person to commit a crime by means of fraud or undue persuasion in an attempt to later bring a criminal prosecution against that person"*

(Blacks Law Dictionary 7th Ed.)

- Defense fails if defendant was not induced by government or was predisposed to commit the crime
- Entrapment defense is not based on constitutional rights
- Has not much use for a hacker breaking into a honeynet without government inducement

# Press Notes About Using Honeynets

- Very newsworthy (2008 and 2009)
- Throws flashlight on ethical aspects of honeynets
- Shows increasing attention of the public
- **Cybercrime supersite was FBI honeypot (10-14-2008)**  
Darkmarket. Was an online waterhole for thousands of identity thieves, hackers and credit card swindlers has been run by an FBI cyber crime agent for the last two years until its voluntary shutdown, FBI used DM to build intelligence briefs of its members (activity on site)
- **Luring hackers into honeypots (Aftenposten 06-26-2009)**  
an employee of Norwegian Security Authority NORCERT runs private surveillance of suspicious computer users by using several thousands of fake computers, NORCERT is not allowed to use honeynet based methods, unethical and unacceptable

# Conclusion

## Questions?

Northeast Ohio HoneyNet Group  
<http://www.neohoney.net>

# References

## General

- Spitzner, Lance *Honeypots : Tracking Hackers*. Addison-Wesley, 2002.
- The HoneyNet Project *Know Your Enemy*. Addison-Wesley, 2004.

## Legal issues

- The HoneyNet Project, *Know Your Enemy*, Addison-Wesley 2004, Chapter 8 Legal Issues by Richard Salgado
- Lance Spitzner, *Honeypots: Are they illegal ?* <http://www.securityfocus.com/infocus/1703>
- Ian Walden, Anne Flanagan, *Honeypots a sticky legal landscape?* <http://www.entrepreneur.com/tradejournals/article/106474528.html>
- *Cybercrime Supersite was FBI Honeypot* <http://www.wired.com/threatlevel/2008/10/darkmarket-post/>
- *Luring Hackers into honeypots*, Aftenposten 06-26-09, english translation with permission of Aftenposten on <http://www.honeynor.no>

# References (2)

## Technology

- Provos, N. & Holz, T. *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Addison-Wesley.
- Hubbard, Dan. *Next Generation Honeyclients* [presentation at RSA 2008]. [http://securitylabs.websense.com/images/alerts/rsa\\_2008\\_honeyclient\\_preso.mov](http://securitylabs.websense.com/images/alerts/rsa_2008_honeyclient_preso.mov).
- Spitzner, Lance. *Honeytokens: The Other Honeypot*. Security Focus, 7/17/2003. <http://www.securityfocus.com/infocus/1713>.
- Stewart, J. *Exposing the Underground: Adventures of an Open Proxy Server*. <http://www.infosecwriters.com/texts.php?op=display&id=54>.
- Sebek, <https://projects.honeynet.org/sebek/>.
- Honeywall, <https://projects.honeynet.org/honeywall>.
- MITRE HoneyClient, <http://www.honeyclient.org/trac>.
- Capture-HPC, <http://nz-honeynet.org/cabout.html>.
- HoneyD, <http://www.honeyd.org/>.
- DShield Web Honeypot, <http://sites.google.com/site/webhoneypotsite/>.
- Nepenthes, <http://nepenthes.carnivore.it/>
- mwcollect, <http://code.mwcollect.org/>.
- HoneyC, <https://projects.honeynet.org/honeyc>.
- Monkey-Spider, <http://monkeyspider.sourceforge.net/>.