

Honeypots / Honeynets



Your Speaker

▼ Lance Spitzner

- Senior Security Architect for Sun Microsystems Inc.
- Founder of the HoneyNet Project
- Former Tank Officer

▼ Ask Questions

- This is NOT a monologue, feel free to ask questions at anytime.



Purpose

To explain what honeypots/Honeynets are and their value to the security community.



Problem

- ▼ Security focuses on defensive actions
 - firewalls, IDS, and encryption
- ▼ Badguys have the initiative.
- ▼ Organizations wait for a failure in their defenses.



An alternative

▼ Passive Surveillance

- Lie in wait for the bad guys
- Watch what they do
- See what they're after
- Learn what to defend and how to do it effectively
- Predict Future attacks

▼ To lure them to where we watch, we use honeypots



What is a honeypot?

(Traditionally), a single host that emulates

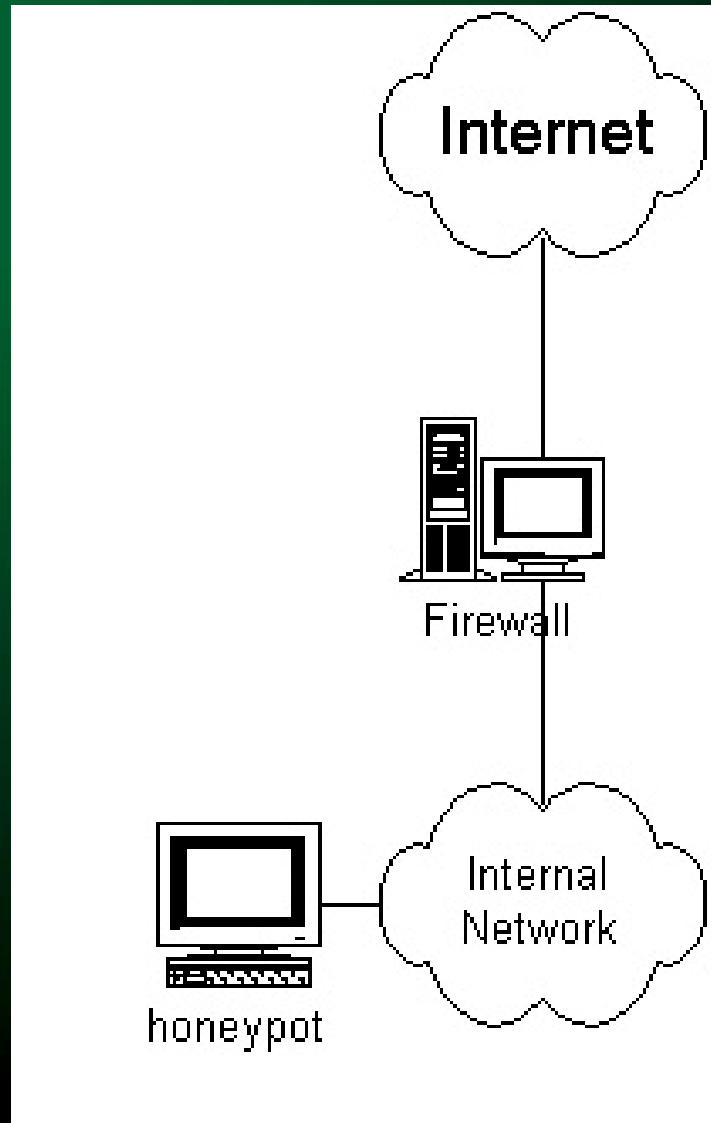
- systems,
- IP stacks,
- Services
- or vulnerabilities.

Not a new concept,

- introduced over ten years ago by security icons:
 - Cliff Stoll with the "Cukoo's Egg"
 - Steve Bellovin and Bill Cheswick's "An Evening with Berferd."



Honeypot





honeypot examples

- ▼ The Deception Toolkit
 - <http://www.all.net/dtk>
- ▼ Specter
 - <http://www.specter.com>
- ▼ Mantrap
 - <http://www.recourse.com>



Honeypots limitations

- ▼ Do not teach you what the bad guys do once they compromise a system.
- ▼ Potentially easy to detect.
- ▼ Limited to what the vendor provides



Intelligence

As a Army Tank officer, I crawled around the inside of Soviet T-72 tanks to better understand the enemy and their capabilities.

This military strategy of gaining intelligence on the enemy applies to information security.

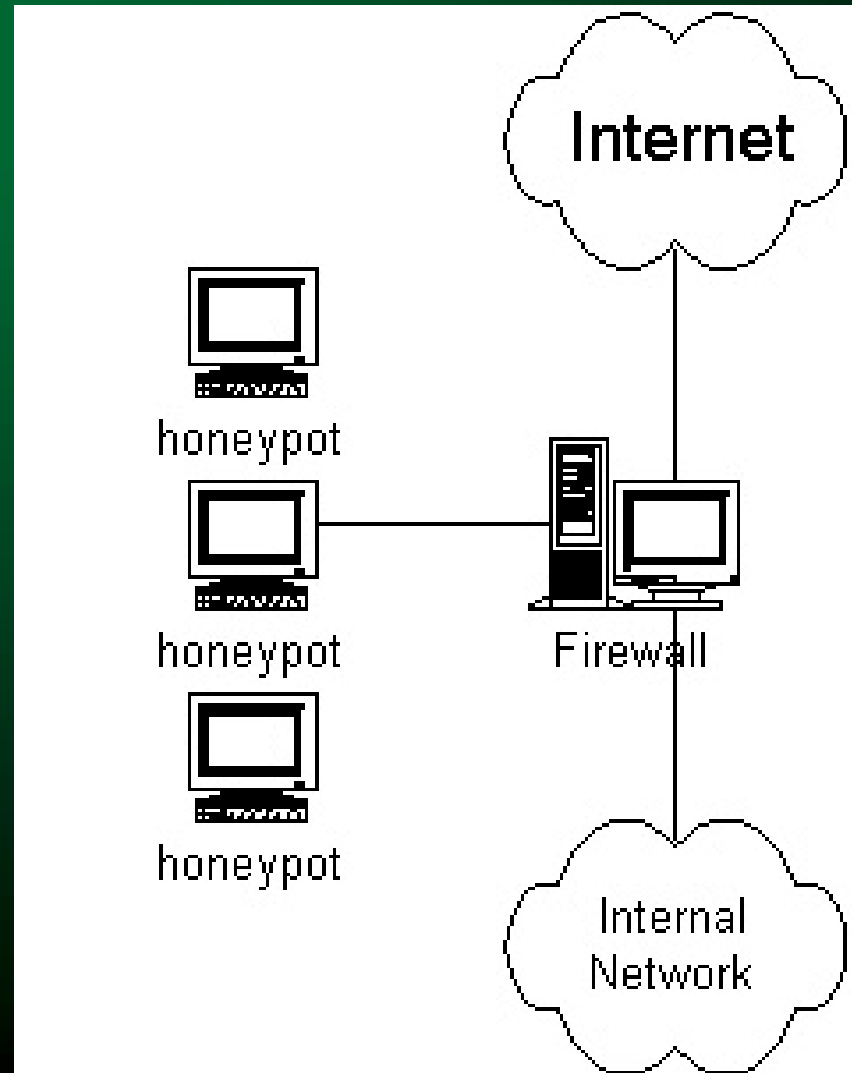


What is a Honeynet

A Honeynet is the primary tool we use to learn about the badguys. A Honeynet is a network of production systems designed to be compromised. Once compromised, we analyze the data and learn the tools, tactics, and motives of the blackhat community.



Honeynet





The Systems

The systems used within the Honeyynet are actual production systems. Nothing is emulated, nor is anything done to make the systems more insecure.



Value

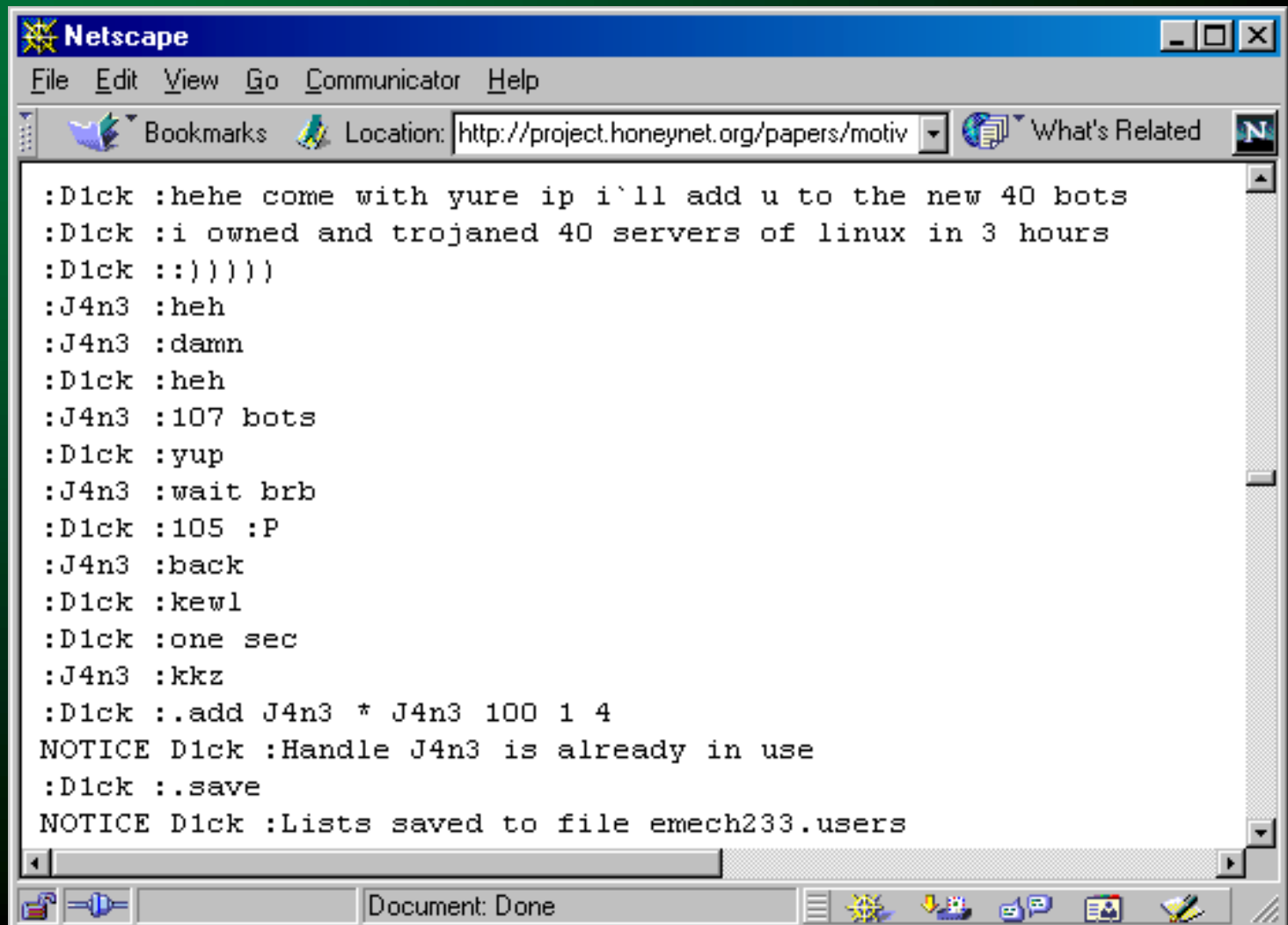
Since all of the Honeynet systems are production systems (nothing is emulated) the risks and vulnerabilities identified apply to many organizations.



Examples

- ▼ Aggressive behavior
 - fastest compromise, 15 minutes
 - DDoS attacks
- ▼ Tool analysis (Linux auto-rooter)
- ▼ Motives (captured IRC chats)

Hacker talk



A screenshot of a Netscape browser window. The title bar reads "Netscape". The menu bar includes "File", "Edit", "View", "Go", "Communicator", and "Help". The address bar shows the URL "http://project.honeynet.org/papers/motiv". The main content area displays a chat log with the following text:

```
:D1ck :hehe come with yure ip i`ll add u to the new 40 bots
:D1ck :i owned and trojaned 40 servers of linux in 3 hours
:D1ck ::))))
:J4n3 :heh
:J4n3 :damn
:D1ck :heh
:J4n3 :107 bots
:D1ck :yup
:J4n3 :wait brb
:D1ck :105 :P
:J4n3 :back
:D1ck :kewl
:D1ck :one sec
:J4n3 :kkz
:D1ck :.add J4n3 * J4n3 100 1 4
NOTICE D1ck :Handle J4n3 is already in use
:D1ck :.save
NOTICE D1ck :Lists saved to file emech233.users
```

The status bar at the bottom shows "Document: Done" and various system icons.



Risks / Issues

- ▼ Time consuming (40 hours per compromise)
- ▼ Risk (ensuring not used as a launching point)
- ▼ Maintenance (firewall patches, reviewing logs, IDS status).



The HoneyNet Project

We are a group of thirty security professionals dedicated to improving the security of the Internet community. We do this on our own time with our own resources.

Know Your Enemy papers

Forensic Challenge

Scan of the Month

Know Your Enemy - book



Conclusion

Honeypots and Honeynets can add value to the security community.

Honeypots, traditionally systems that emulate vulnerabilities or other systems, add value in alerting and deception. Honeynets add value as an intelligence gathering tool.



Resources

▼ <http://project.honeynet.org>

▼ ***Know Your Enemy:** Revealing the security tools, tactics and motives of the blackhat community.*