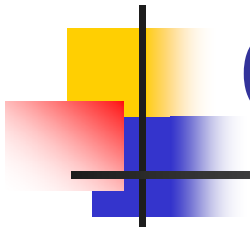
Honeynet

A platform for studying Hacker Behaviors and Computer Forensics

Alan S H Lam
CUHK
24 July 2003

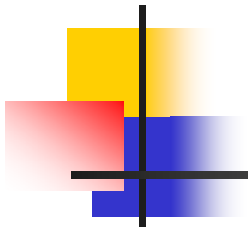


Outlines

- Objectives of our Honeynet
- What is a Honeynet and how it works
- Hackers' Activities (with live demo)
- Forensic Tools
- How Honeynet May Help E-banking
- Future Development
- Q & A

Objectives of our Honeynet

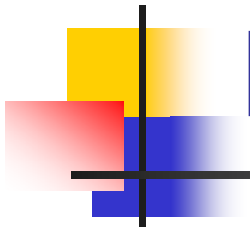
- To learn from the hackers
- To give early warning of potential attacks
- To collect research material for our computer forensic lab
- To improve our skill in security incident response



Honeypot

- Definition
  - A honeypot is security resource whose value lies in being probed, attacked, or compromised

    From Lance Spitzner
- Type of Honeypot
  - Low-Interaction VS High-Interaction



Honeynet

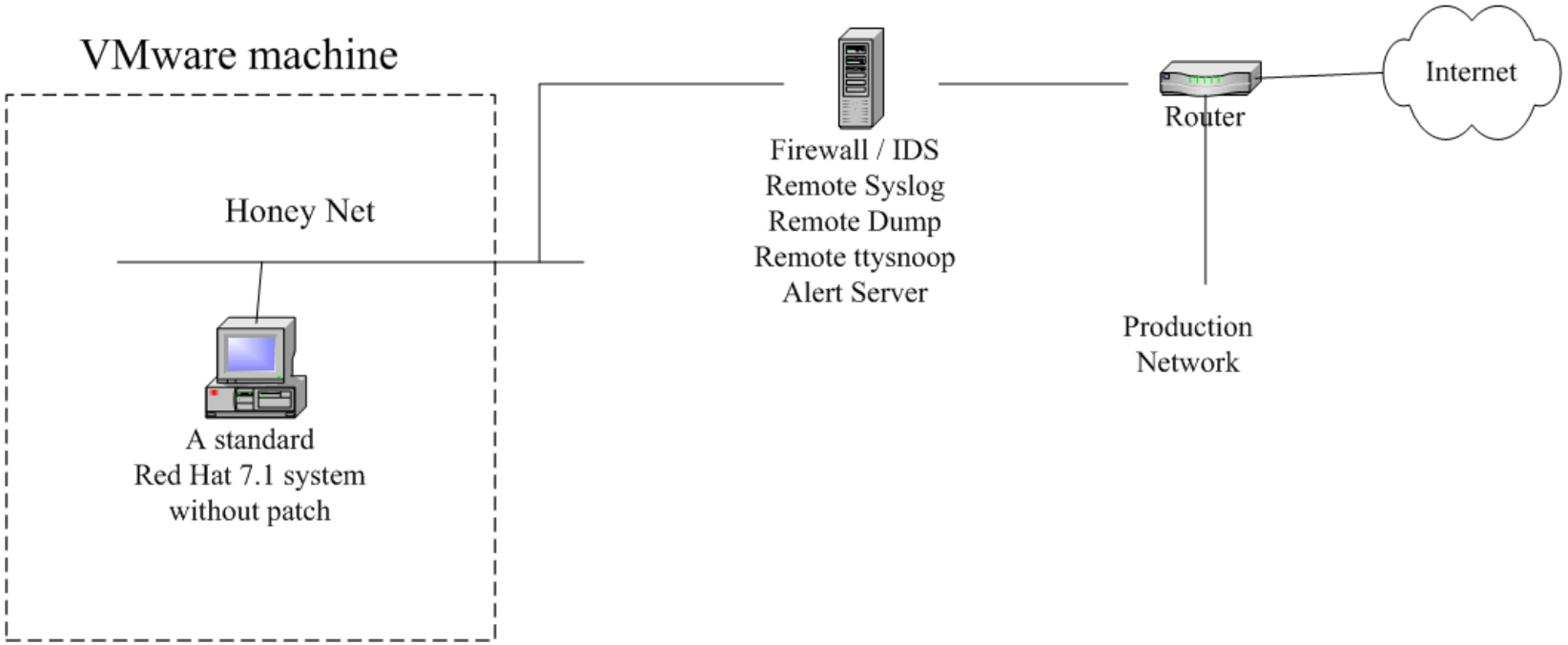
- Honeynet is a network of high-interaction honeypots
- Build a network of standard production systems
- Put these network of systems behind firewalls
- Watch what happens

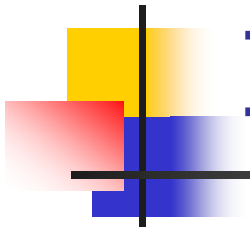
Requirements of building a Honeynet

- Data Control
- Data Capture
- Data Collection

  only for organizations that have multiple Honeynets in distributed environments

Existing Honeynet Network Infrastructure



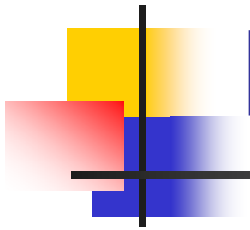


Implementation

- Data Control
  - Egress filter rule
  - IPtable rule in firewall to cut Honeypot connection when
    - NIDS detects any attack originated from Honeypot
    - Packet rate higher than R
    - After N outbound connections from Honeypot
    - After M packets go through the Honeynet
  - An alert message will be sent to the system admin when the connection is cut

Implementation (cont')

- Data Capture
  - Capture all network packets in/out the Honeynet
  - Capture hackers' keystroke by a trojaned login shell in Honeypot
  - Remote syslog
  - Dump backup
  - SNORT NIDS log
  - All data captured are stored in the firewall host

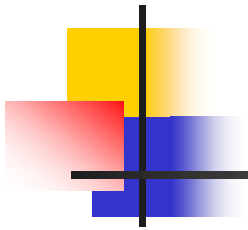


Hackers' Activities

- Identify/locate the victim by some scanning tools
- Break-in the victim through system security holes. The following vulnerabilities were used by the hackers to break-in our Honeynet.
  - sshd CRC32 Overflow
  - Buffer overflow in openssl
  - WU-FTP RNFR ././ attack
  - execve/ptrace race condition

Hackers' Activities (cont')

- After break-in, the hackers may
  - Install rootkit to setup backdoor, sniffer, or IRC proxy
  - Use victim as a stepping stone to find and attack other victims
  - Fix the victim vulnerability and undo other hackers jobs
  - Send back the victim information through e-mail
  - Propagate the attack to other victims
  - Deface/remove victim web page



Forensic Tools

- scp, dd, tar, nc
- tcptrace, tcpdump, snort
- ps, netstat, lsof, fuser, kill -STOP, pcat, ltrace, strace, /dev/kmem
- /proc directory
- find, ldd, strings, gbd, od, bvi, icat
- chkrootkit

How Honeynet May Help E-banking

- Provide intelligence information to banks:
  - latest hacking techniques and new attack patterns
  - behavior, characteristics, and culture of hacking community
  - early warning of potential hacking wave
  - techniques for security incident handling such as data recovery
- Collect tools for penetration test

Future Development

- Enhance the Honeynet to include more other OS systems
- “Honey” the Honeypots so as to attract different classes of hackers (e.g. building a web portal or on-line bank)
- Set up a forensic lab

Q & A

- Questions
- Comments
- Suggestions

You can review this presentation at
http://www.ie.cuhk.edu.hk/~shlam/talk/hkab/

Thank You

alan@ie.cuhk.edu.hk