Honeynet

A platform for studying Hacker Behaviors and Computer Forensics

Alan S H Lam

CUHK

30 August 2003

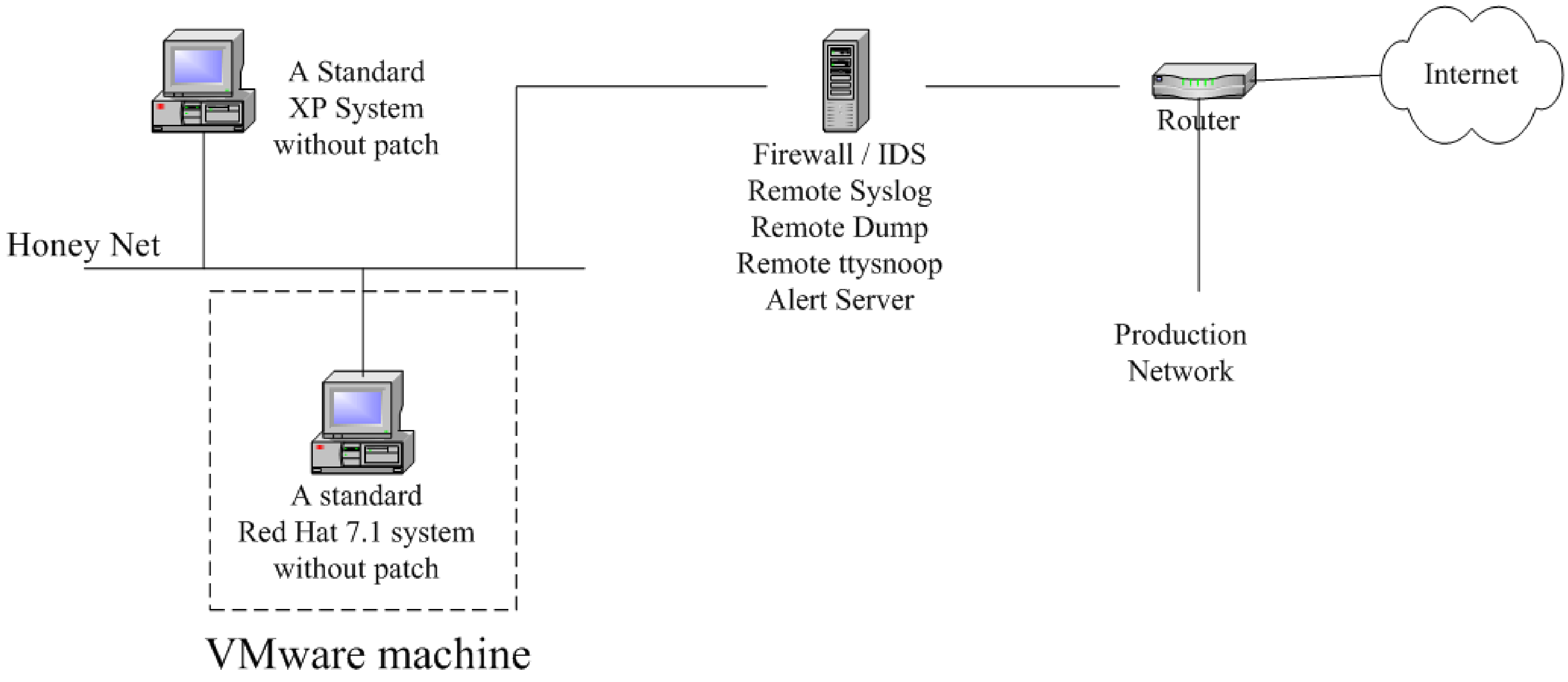
Outlines

- Objectives of our Honeynet
- Implementation of our Honeynet
- Intruders' Activities and Forensics Techniques (with live demo)
- Deployment Tips
- 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

Existing Honeynet Network Infrastructure



Implementation

- Data Control
  - Egress filter rule
  - IPtable rule in firewall to drop or cut Honeypot traffic 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
  - Firewall and SNORT NIDS log
  - All data captured are stored in the firewall host

Intruders' 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
    - Microsoft's DCOM RPC (W32/BlasterA/D Worm)

Intruders' Activities (cont')

- After break-in, the hackers may
  - Install rootkit to setup backdoor, sniffer, IRC proxy, or streaming server
  - 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, coreography
- /proc directory
- find, ldd, strings, gbd, od, bvi, icat, elfsh
- Coroner’s Toolkit (TCT), Chkrootkit

Deployment Tips

- Do not deploy your Honeynet unless you are sure about your data control
- Start with tight data control first
- Capture data at different levels
- Make sure your Honeynet does not violate your company policy

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

Thank You

alan@ie.cuhk.edu.hk