HoneyNet

A platform for studying Hacker Behaviors and Computer Forensics

By
Alan S H Lam

Outlines

- Objectives
- Definition of Honeypot
- Types of Honeypot
- Honeynet (requirements, implementation and network infrastructure)
- Hackers’ activities
- Forensic Tools
- Forensic Challenge
- Computer Forensic Lab
- Q & A

Objectives

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

Definition of Honeypot

- An Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system.

From http://webopedia.internet.com

Definition of Honeypot (cont')

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

From Lance Spitzner

Type of Honeypot

- Low-Interaction Honeypots
  - Simple, safe but less information can be captured
- High-Interaction Honeypots
  - Complicated, high risk but extensive amount of information can be captured

Honeynet

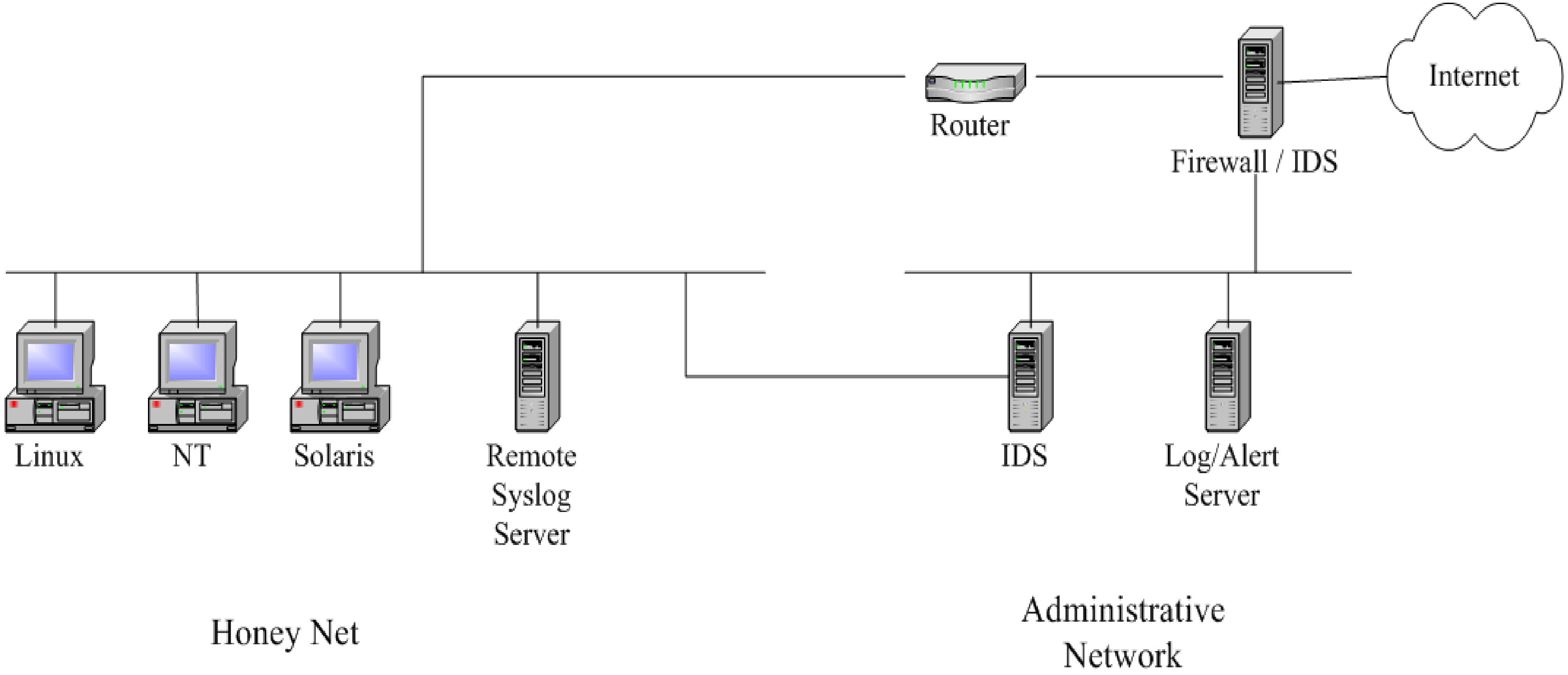
- Honeynets are high-interaction honeypots.
- Build a network of standard production systems
- Put these network of systems behind firewalls
- Then watch what happens

Requirements of building a Honeynet

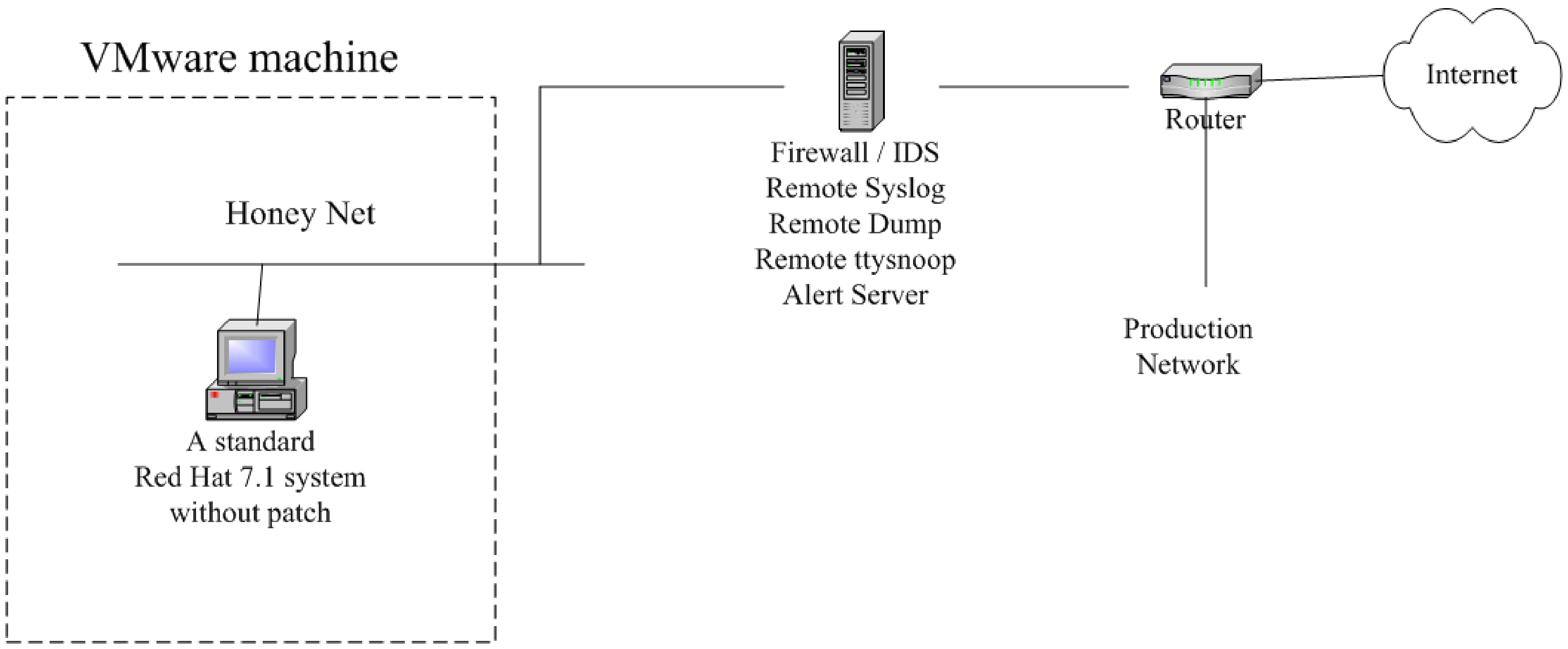
- Data Control
- Data Capture
- Data Collection

  only for organizations that have multiple Honeynets in distributed environments

A Typical Honeynet Network Infrastructure



Existing Honeynet Network Infrastructure



Implementation

- Data Control
  - Egress filter rule
  - IPtable rule in firewall to cut honeypot connection when
    - NIDS detects any attack from honeypot
    - Packet rate higher than S for T seconds
    - 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 the full length packets in/out the honeynet
  - Capture hackers’ keystroke by a trojan login shell in honeypot
  - Remote syslog
  - Dump 9 backup (daily or just after the attack from honeypot)
  - SNORT NIDS
  - All data captured are remotely stored in firewall host

Hackers’ Activities

- Identify/locate the victim by some scanning tools
- Break-in the victim through some remote exploits. 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-ins, the hackers may
  - Set up back door to secure later access
  - Get root access if needed
  - Download tools by wget or ftp
  - Install rootkit to cover their traces
  - Install sniffer to collect user/password information
  - Install IRC Bot or proxy to maintain IRC channels
  - Use victim as a stepping stone to locate and attack other victims

Hackers' Activities (cont')

- After break-ins, the hackers may (cont')
  - Fix the victim vulnerability so as to keep other hackers out.
  - Undo other hackers jobs such as kill other hackers' backdoor, IRC bot and reinstall their own rootkit and IRC bot.
  - Send back the victim information (such as network configuration and password file) through e-mail; duplicate the attack program and propagate the attack to other victims. This is what worm does.
  - 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

The Forensic Challenge

- To decrypt a hacker backdoor session
- To analysis a computer worm
- To analysis a rootkit package

Computer Forensic Lab

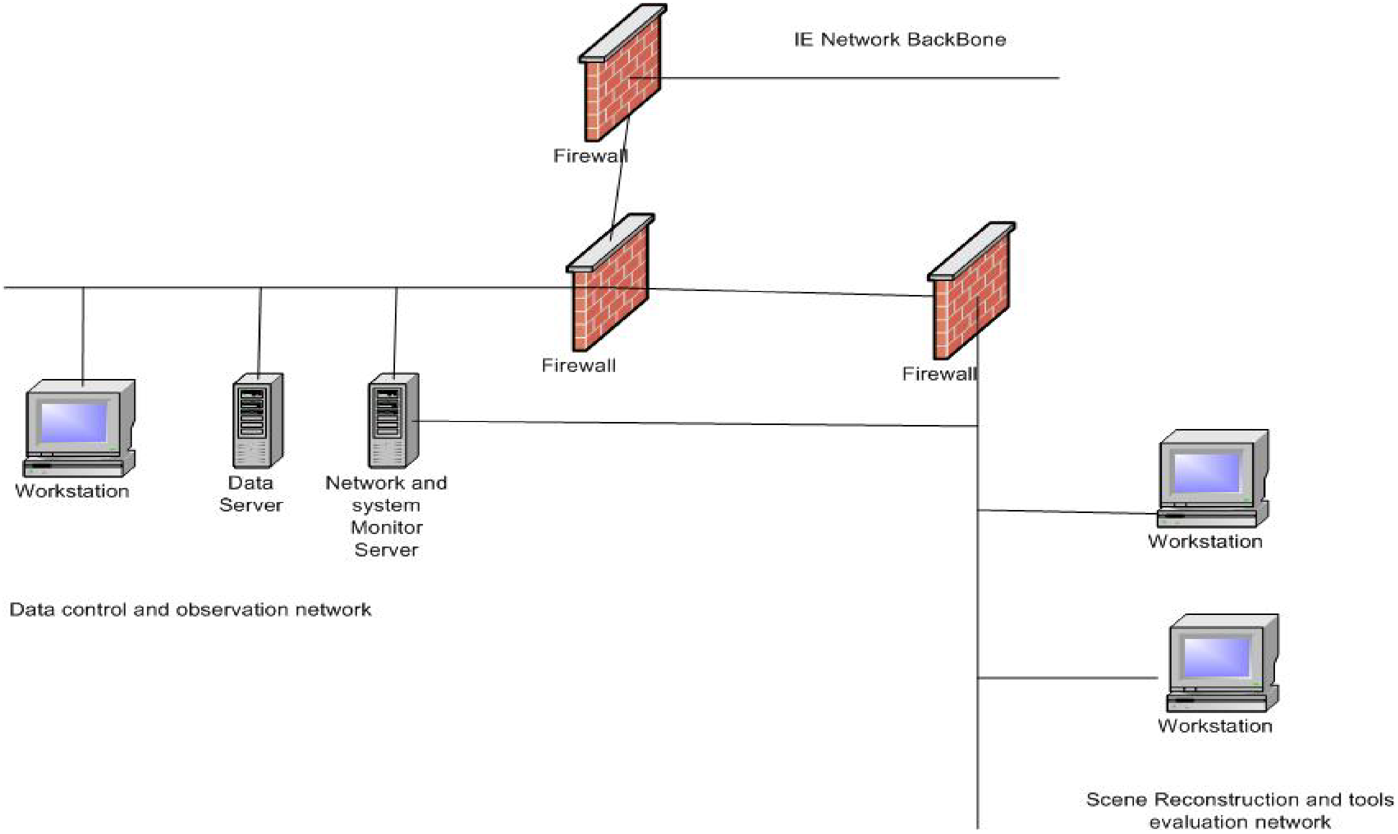
- Objectives
  - To evaluate the hackers' tools and data collected from Honeynet Project
  - To develop computer forensic tools and skill
  - To study hacking techniques and hacker culture
  - To develop counter hacking measures and models

Computer Forensic Lab (cont’)

- Operation
  - Set up a closed and well controlled network for
    - evaluating the hackers’ tools and data collected from Honeynet Project or hackers’ sites.
    - scene reconstruction of hacking in Honey Pot
    - observing hacking signature and aftermath events.
    - evaluating anti-hacking model and tools.

Computer Forensic Lab (cont’)

- Computer Crime Lab Infrastructure


IE Network BackBone
Firewall
Firewall
Firewall
Workstation
Data Server
Network and system Monitor Server
Data control and observation network
Workstation
Workstation
Scene Reconstruction and tools evaluation network

Computer Forensic Lab (cont’)

- Research Areas
  - Hacker’s Behaviors, Profiles, and Workflow
  - Distribution of hackers in the cyberspace and geographical region
  - Prorogation of attack wave and time latency between attack and exploit announcement
  - Hacker’s tools
  - Hacker’s community and culture
  - Enhancements and evaluation of
    - IDS and alert system
    - HoneyNet model and infrastructure
    - Firewall policy and architecture
    - Surveillance skill and technologies
    - Computer Forensic Skill