HONEYPOTS

By Cosmin Stejerean

Definition

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

  Lance Spitzner

Advantages

- Data
  - Eliminates “noise level” of production systems
  - Provide precise information quickly
- Resource
  - Require limited resources
  - Eliminates problems with resource exhaustion
- Simplicity
- Justify value of security investments

Disadvantages

- Narrow Field of View
  - Can only detect attacks directed at them
- Fingerprinting
  - Attacker can identify true nature of honeypot
- Risk
  - Break out of the controlled environment

Types of Honeypots

- Low Interaction
  - BOF
  - Honeyd
  - Specter
- Medium Interaction
  - ManTrap
  - Chroots and jails
- High Interaction
  - Honeynets

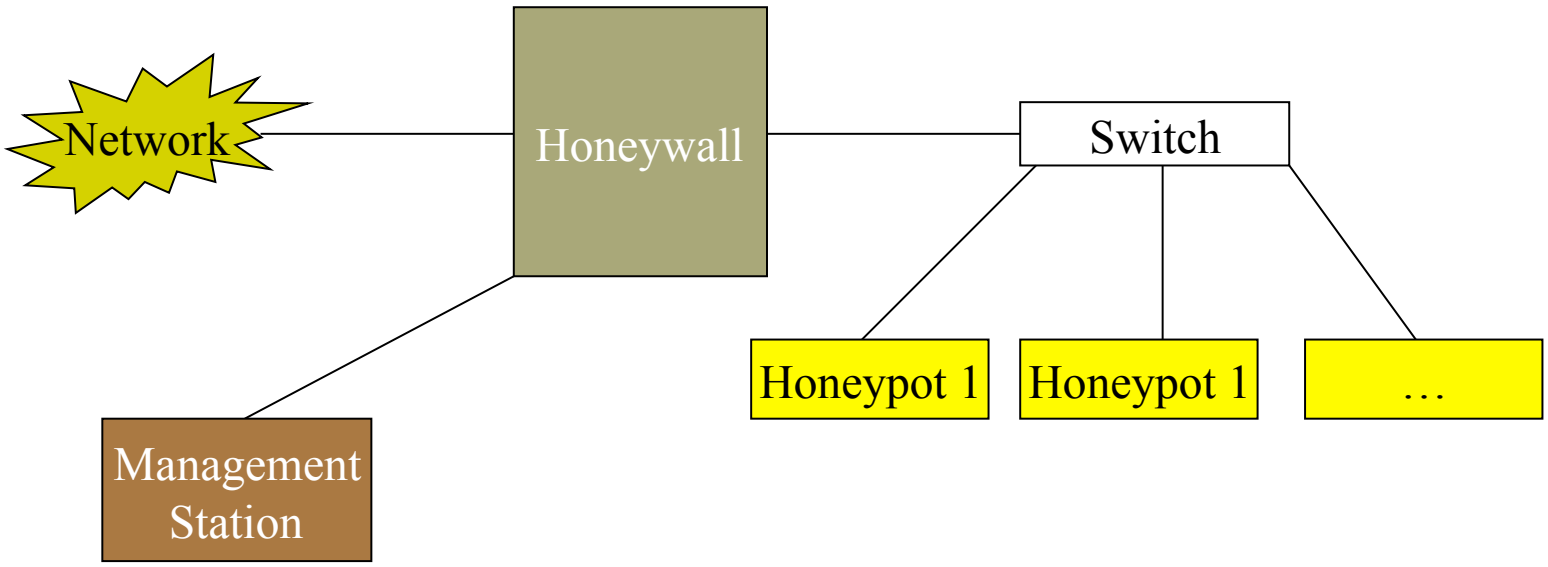
Honeynet

- A highly controlled network environment
- Provides a high interaction honeypot
- Can gather most information about attackers
- Can identify unknown attacks or tools
- Can capture highly skilled hackers
- Can connect more than one honeypot

Gen II Honeywall

- A modified Linux install
- Acts as an Ethernet bridge
- Logs all traffic
- Provides data control

Honeynet Diagram



Honeynet CDROM

- Bootable CD to install a honeynet
- Is almost ready to go; needs customization
- http://www.honeynet.org/tools/cdrom
- Latest version is still in Beta

Features

- Can provide email alerts
- Walleye web interface
- Can limit outgoing traffic (minute, hour, etc)
- Management interface
- Snort inline to filter outgoing traffic
- Easy to deploy and manage

More information

- http://www.honeynet.org/tools/cdrom/roo
- http://www.honeynet.org/papers/
- Books
  - Know Your Enemy, 2nd Edition
  - Honeypots – Tracking Hackers