Honeypots / honeynets
Agenda

- Honeypots
- Honeynets
- Honeywall
Traffic

Problem:
- Vast quantities of normal traffic
- Find suspect bits
Honeypot

- Machine without normal task
- That is never mentioned

- So:
  - Machine that gets no normal traffic
  - Every network packet is suspect

- With
  - Contained environment
  - IDS (snort) and logging
Where

- Anywhere within net
- No specific place
- Built like production machine
- Without function
Definition

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

History

- **1990: real systems**
  - Deploy unpatched systems in default config on unprotected network (‘low-hanging fruit’)
  - Easy to deploy
  - High-interaction, high-risk
  - Nice reading: “Cuckoo’s Egg” by Clifford Stoll

- **1998: service / OS emulation**
  - Deception Toolkit, Cyber Cop Sting, KFSensor, Specter
  - Easy to deploy
  - Low-interaction, low-risk

- **1999-current: virtual systems**
  - HoneyD, Honeywall, Qdetect, Symantec Decoy Server(!’03/’04)
  - Less easy to deploy
  - Mid / high-interaction, mid / high-risk
History of the Honeynet Project

- 1999: Lance Spitzner (Sun) founds Honeynet Project
- 2001-2003, GenII: GenI + bridging (no TTL, harder to detect)
- 2003: Release of Eeyore Honeywall CD-ROM
- 2003-current, GenIII: GenII + blocking (Honeywall)
- 2005: Release of Roo Honeywall CD-ROM
- future: ‘GenIV’ refers to next-gen analysis capabilities

Honeynet.org is home to the ‘KYE papers’.
Take care!

- Machine must look real
- Outside traffic possible
  - Or clearly fake
- Capture all traffic
  - analyse
- Special restrictions on outgoing traffic
  - Everything is allowed
  - Low bandwidth (tarpit)
Purpose

- **Research**
  - Attract blackhats
  - Reveal blackhattactics, techniques, tools (KYE)
  - Reveal motives / intentions (?)
  - Mostly universities, governments, ISPs

- **Protection**
  - Deter blackhats from real assets
  - Provide early warning
  - Mostly governments, large enterprises

- **Purpose may determine honeypot functionality and architecture**
Definitions

- **Definition**
  - A honeynet is a network of [high-interaction] honeypots.

- **Definition**
  - A honeywall is a layer-2 bridge that is placed in-line between a network and a honeynet, or between a network and a honeypot, to uni- or bidirectionally capture, control and analyze attacks.

- **Definition**
  - A honeytoken is a honeypot which is not a computer.
Functional requirements of a honeypot

- Data control
- Data capture
- Data collection
- Data analysis
Entrapment

- Applies only to law enforcement
- Useful only as defence in criminal prosecution
- Still, most legal authorities consider honeypots non-entrapment
- Responsibility for everything done from our net
Low vs. High interaction

- **Low interaction**
  - Burglar alarm
  - Not to learn about new attacks
  - Simple

- **High interaction**
  - Research
  - Look at new things
  - Anatomy of new exploit
  - Invest resources (manpower)
Realness

- Make things look real
  - Windows services
  - Windows exploits
  - But Solaris network stack
How to organise

- Honeypot more than unpatched host
  - See what happens
  - Containment
  - Check logs
  - Limit outgoing traffic

- Don’t try this without thought!
Honeyd

- [http://www.honeyd.org](http://www.honeyd.org)

**Framework**
- Config file
- Scripts for emulated services
  - Internal (python interpreter in honeyd)
  - External (extern process)
  - Stdin+stdout = net, stderr = syslog
- Acts using nmap fingerprints
Honeyd

- Run on a single ip address
  - Several services on one address
- Run as honeynet
  - Several hosts on several addresses
  - Attract traffic
    - Static route in router
    - Have honeyd arp on addresses
Containment

- Honeywall
  - Appliance
  - Based on unix
  - 3 network interfaces
    - Management
    - Data (inside / outside bridge)
Sebek: spying on your intruder

- Honeynet.org: “Sebek is a tool designed for data capture, it attempts to capture most of the attackers activity on the honeypot, without the attacker knowing it (hopefully), then sends there covered data to a central logging system.”
- Linux kernel module that hooks sys_read()
- Covertly sends captured data to honeywall (UDP)
- Recovers keystrokes, uploaded files, passwords, IRC chats, even if they are encrypted by SSH, IPSec or SSL.
Sebek
Honeynet Requirements

- Data Control
- Data Capture

- [http://old.honeynet.org/alliance/requirements.html](http://old.honeynet.org/alliance/requirements.html)
No Data Control
Data Control

- **No Restrictions**
- **Honeypot**
- **Connections Limited**
- **Packet Scrubbed**

Diagram showing the flow of data from the Internet through a honeywall to honeypots with restrictions applied.
Honeynet Bridge

- SSH Connections
- Trusted Hosts

Internet

Eth0-NO IP

Administrative Interface

129.252.140.3
192.252.140.7
What is Data Control and Why?

- Process used to control or contain traffic to a honeynet
- Upstream liability – an attack from one of your honeypots
- Snort-inline – South Florida Honeynet Project
Connection Limiting Mode

Enemy

Data Control
Snort-Inline
IPTables

Hub

IPTables

DROP
Snort-Inline Drop Mode

![Diagram showing Snort-Inline Drop Mode]

- Enemy
- Data Control
- Snort-Inline
- IPTables
- Hub
- Drop
- IP Tables
- Ip_queue
- Snort-Inline
- Snort Rules=Drop
Snort-Inline Replace Mode

Diagram showing data flow from an enemy device, through a hub, to IP tables with Snort Inline rules, and to a bin/sh -> ben/sh process.
GEN II Data Control

Gen II:

- Incorporates a firewall and IDS in one system
- Provides more stealthy data control
- Can be implemented for layer 2 bridging or Layer 3 NAT translation
- Packets passed from internet to honeynet as layer 2 (datalink) layer packets
  - no TTL decrement
  - invisible
IPTables for GEN II Honeynet

- IPTables is a free, stateful, Open Source firewall for Linux 2.4.x and 2.5.x kernels
- Each packet header is compared to a set of “chains”
- Chains contain rules: ACCEPT, DROP, REJECT, Queue
- Custom Chains
  - tcpHandler
  - udpHandler
  - icmpHandler
Honeywall Bootable CD-ROM

- Standard ISO distribution
  - GenII Data Capture/Data Control features
  - Sebek
  - Simple User Interface
  - Auto-configure from floppy

- Customization features
  - “Template” customization (file system)
  - Run-time boot customization
Honeywall

- Standard intel PC
- 3 ethernet cards
  - Inside (honeypots)
  - Outside (internet)
  - Management
- Outside -> inside: bridge, no restrictions
- Inside -> outside: bridge, restrictions
- Management: hidden from outside world
Honeywall - Roo

Malware catching

- **Nepentes** ([http://nepenthes.carnivore.it](http://nepenthes.carnivore.it))
  - Malware-collecting mid interaction honeypot
  - Emulates known vulnerabilities
  - Captures malware trying to exploit them
  - Modular architecture

- First released in 2006
Nepentes
Real world uses

- Surfnet IDS
  - Honeypot in sensor
- Qnet
  - Quarantaine net sensor
  - Contain misbehaving host
- Louis mail relay
  - Try again later…