Honeypots - The Latest

Purpose

Latest developments with honeypots.

Agenda

- Honeypots
- Low Interaction
- High Interaction

Honeypots

Initiative

Honeypots allow you to take the initiative, they turn the tables on the bad guys.

Honeypots

A security resource who's value lies in being probed, attacked, or compromised.

The Concept

- System has no production value, no authorized activity.

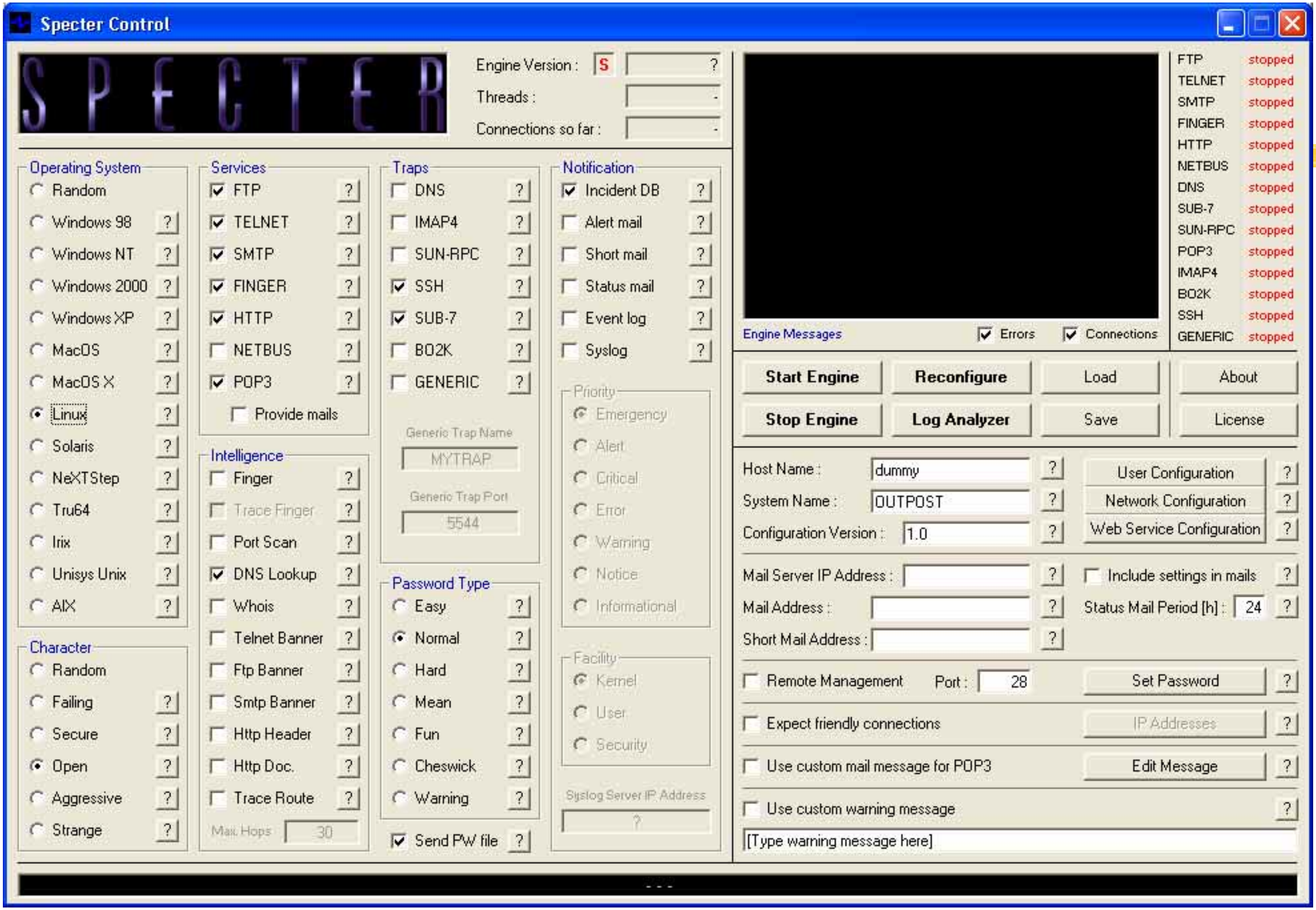
- Any interaction with the honeypot is most likely malicious in intent.

Flexible Tool

Honeypots do not solve a specific problem. Instead, they are a highly flexible tool with different applications to security.

Types of Honeypots

- Production (Low Interaction)
- Research (High Interaction)



Engine Version : S ?
Threads : -
Connections so far : -

Operating System
○ Random
○ Windows 98
○ Windows NT
○ Windows 2000
○ Windows XP
○ MacOS
○ MacOS X
● Linux
○ Solaris
○ NeXTStep
○ Tru64
○ Irix
○ Unisys Unix
○ AIX

Character
○ Random
○ Failing
○ Secure
● Open
○ Aggressive
○ Strange

Services
☑ FTP
☑ TELNET
☑ SMTP
☑ FINGER
☑ HTTP
□ NETBUS
☑ POP3
□ Provide mails

Intelligence
□ Finger
□ Trace Finger
□ Port Scan
☑ DNS Lookup
□ Whois
□ Telnet Banner
□ Ftp Banner
□ Smtp Banner
□ Http Header
□ Http Doc.
□ Trace Route
Max. Hops 30

Traps
□ DNS
□ IMAP4
□ SUN-RPC
☑ SSH
☑ SUB-7
□ BO2K
□ GENERIC
Generic Trap Name MYTRAP
Generic Trap Port 5544

Password Type
○ Easy
● Normal
○ Hard
○ Mean
○ Fun
○ Cheswick
○ Warning
☑ Send PW file

Notification
☑ Incident DB
□ Alert mail
□ Short mail
□ Status mail
□ Event log
□ Syslog

Priority
● Emergency
○ Alert
○ Critical
○ Error
○ Warning
○ Notice
○ Informational

Facility
● Kernel
○ User
○ Security

Syslog Server IP Address ?

Engine Messages ☑ Errors ☑ Connections

FTP stopped
TELNET stopped
SMTP stopped
FINGER stopped
HTTP stopped
NETBUS stopped
DNS stopped
SUB-7 stopped
SUN-RPC stopped
POP3 stopped
IMAP4 stopped
BO2K stopped
SSH stopped
GENERIC stopped

Host Name : dummy
System Name : OUTPOST
Configuration Version : 1.0
Mail Server IP Address :
Mail Address :
Short Mail Address :
□ Include settings in mails
Status Mail Period [h] : 24
□ Remote Management Port : 28
□ Expect friendly connections
□ Use custom mail message for POP3
□ Use custom warning message
[Type warning message here]

Emulated FTP Server

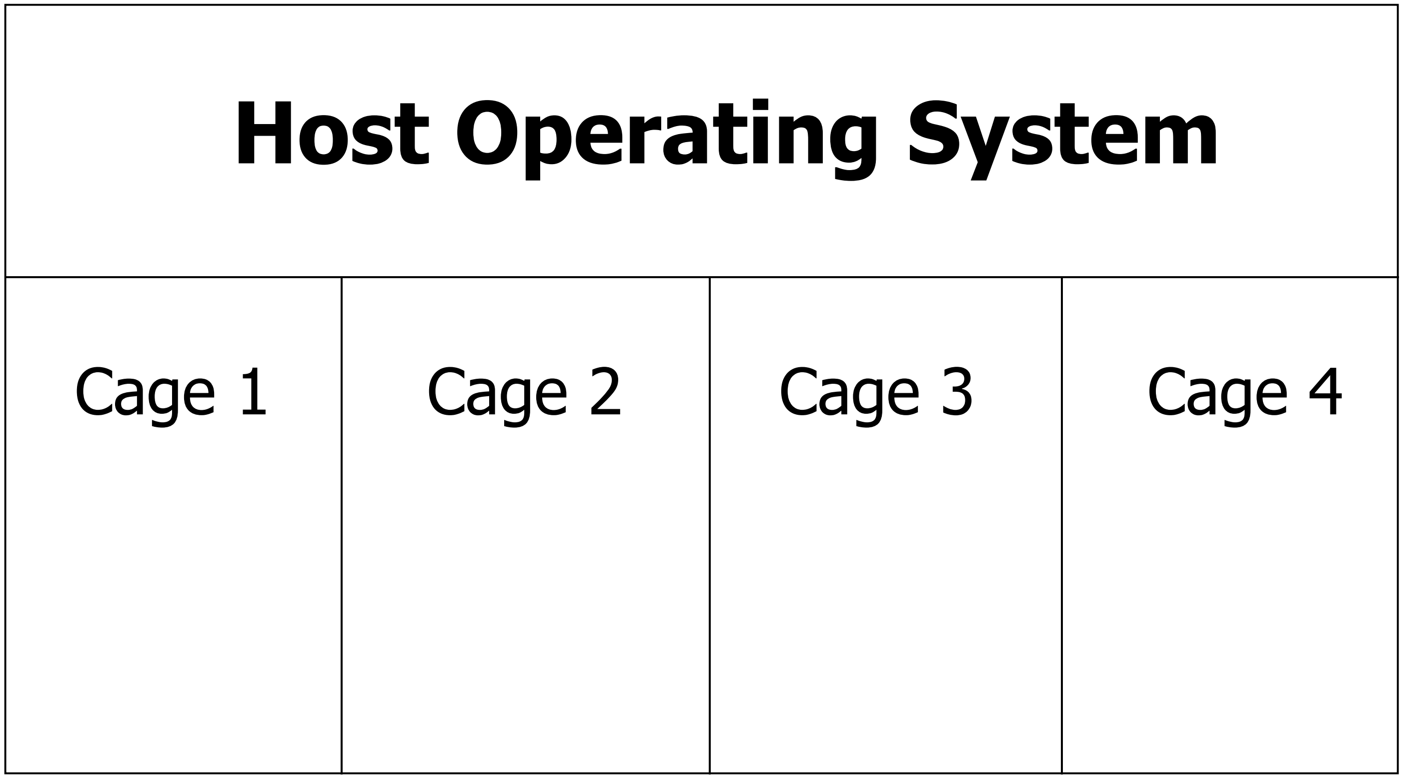
```
case $incmd_nocase in

   QUIT* )
       echo -e "221 Goodbye.\r"
       exit 0;;
   SYST* )
       echo -e "215 UNIX Type: L8\r"
       ;;
   HELP* )
       echo -e "214-The following commands are recognized (* =>'s unimplemented).\r"
       echo -e "   USER    PORT    STOR    MSAM*   RNTO    NLST    MKD     CDUP\r"
       echo -e "   PASS    PASV    APPE    MRSQ*   ABOR    SITE    XMKD    XCUP\r"
       echo -e "   ACCT*   TYPE    MLFL*   MRCP*   DELE    SYST    RMD     STOU\r"
       echo -e "   SMNT*   STRU    MAIL*   ALLO    CWD     STAT    XRMD    SIZE\r"
       echo -e "   REIN*   MODE    MSND*   REST    XCWD    HELP    PWD     MDTM\r"
       echo -e "   QUIT    RETR    MSOM*   RNFR    LIST    NOOP    XPWD\r"
       echo -e "214 Direct comments to ftp@$domain.\r"
       ;;
   USER* )
```

Research honeypots

- Used to gain information. That information has different value to different organizations.

- Does not emulate, but runs actual operating systems. Install FTP server.

ManTrap



Host Operating System

Cage 1

Cage 2

Cage 3

Cage 4

Low-Interaction Technology

Example - Honeyd honeypot

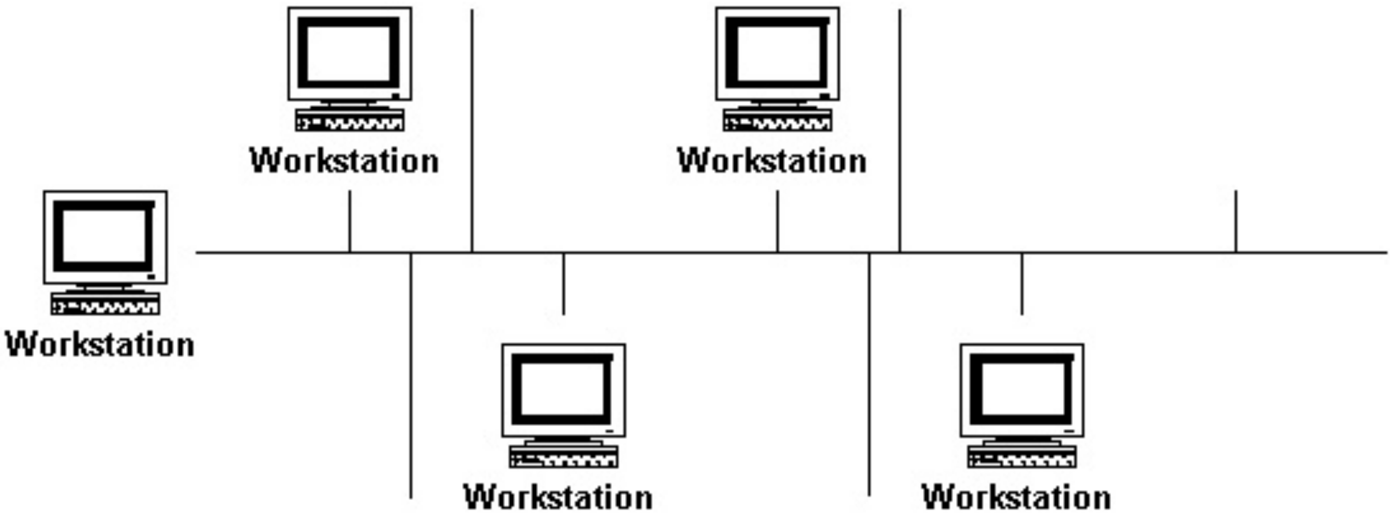
- OpenSource honeypot developed by Niels Provos.
- Production honeypot.
- Emulates services and operating systems.

How Honeyd works

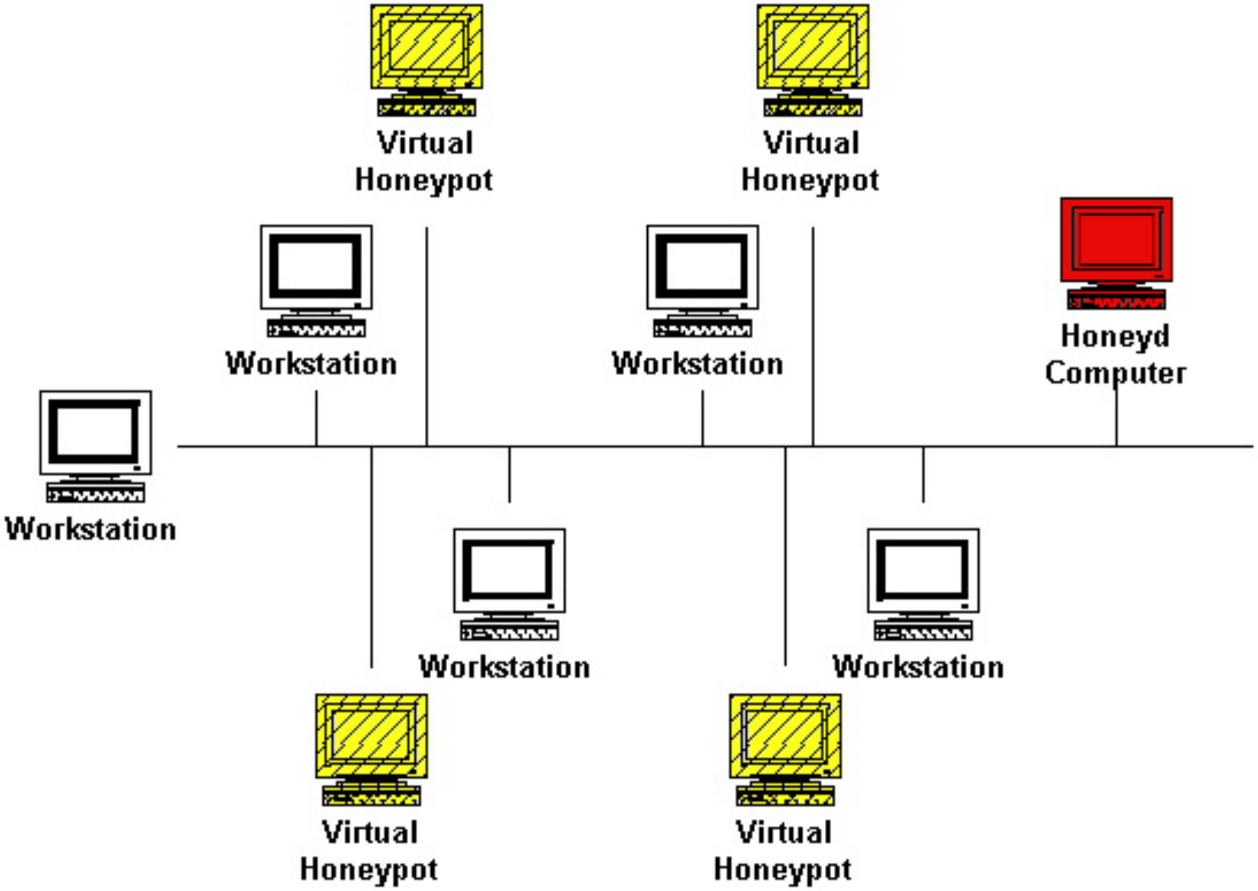
- Monitors unused IP space.
- When it sees connection attempt, assumes IP and interacts with attacks.

- Can monitor literally millions of IP addresses at the same time.

Network with unused IPs



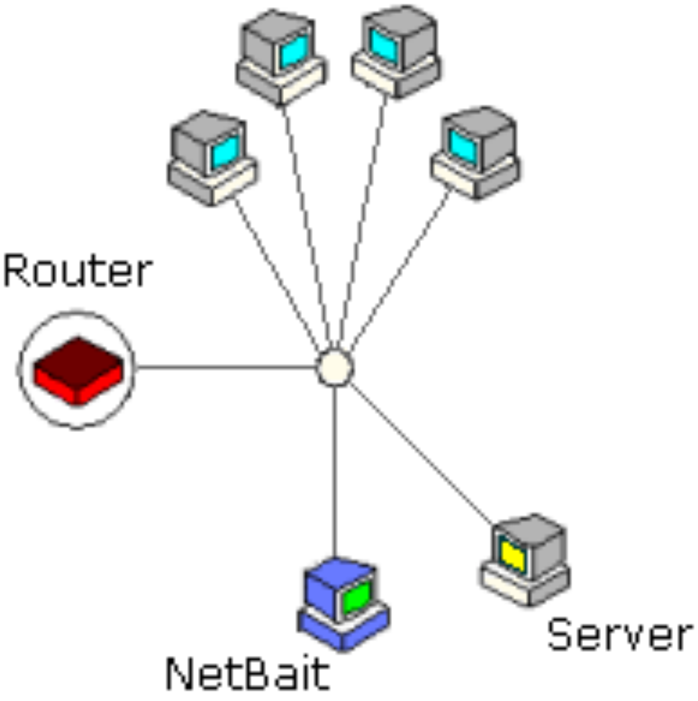
Honeyd monitoring unused IPs



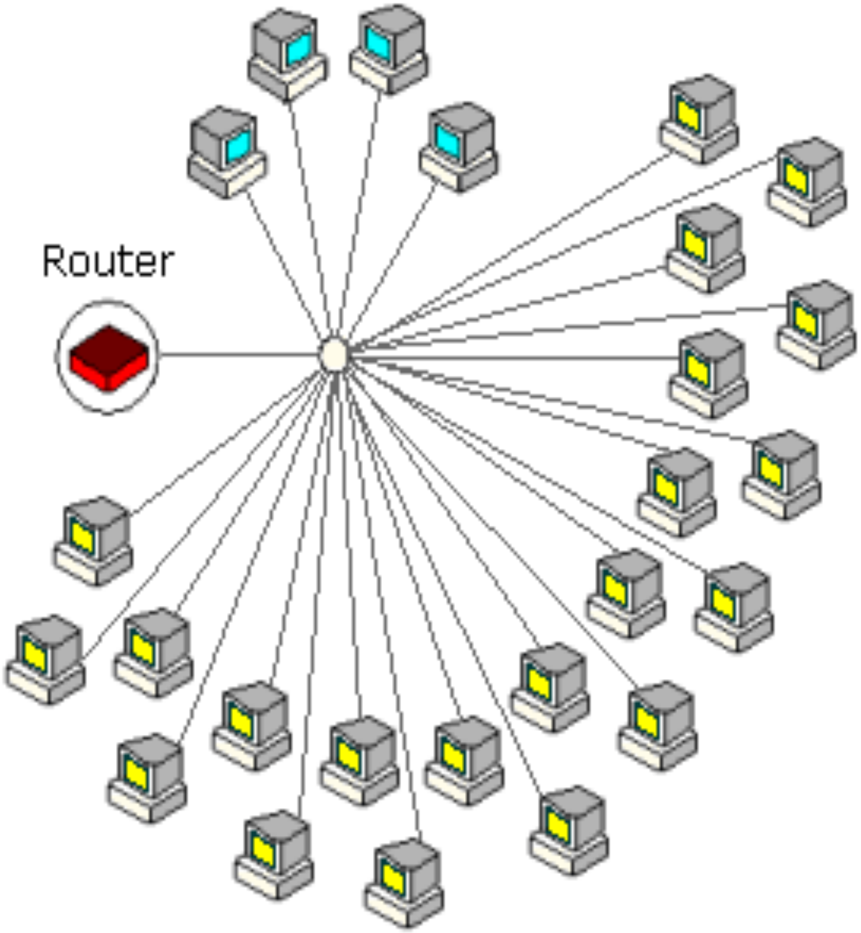
NetBait

- Not a product, a service.
- Attackers directed to honeypot pool, which can be located in a different, isolated network.

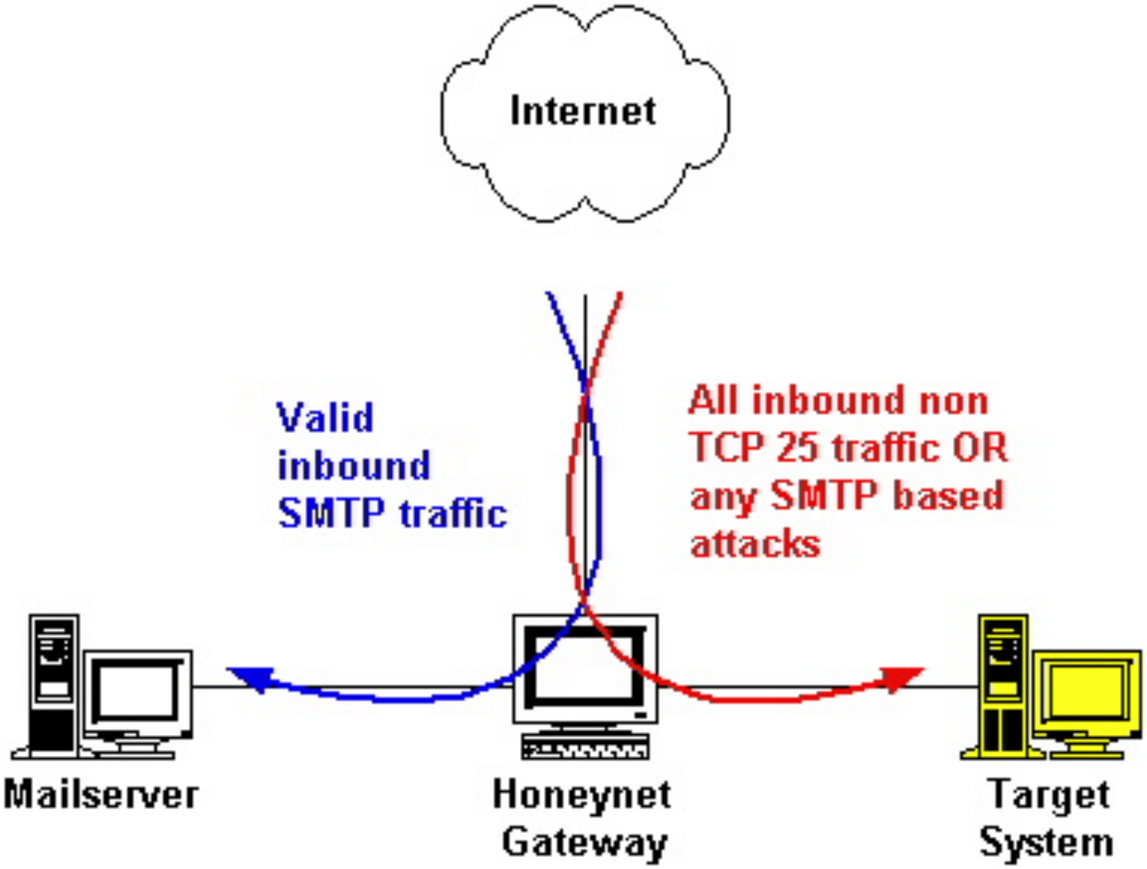
Real Network



Attacker Sees



Bait-n-Switch



Internet
Valid inbound SMTP traffic
All inbound non TCP 25 traffic OR any SMTP based attacks
Mailserver
Honeynet Gateway
Target System

High Interaction Technology

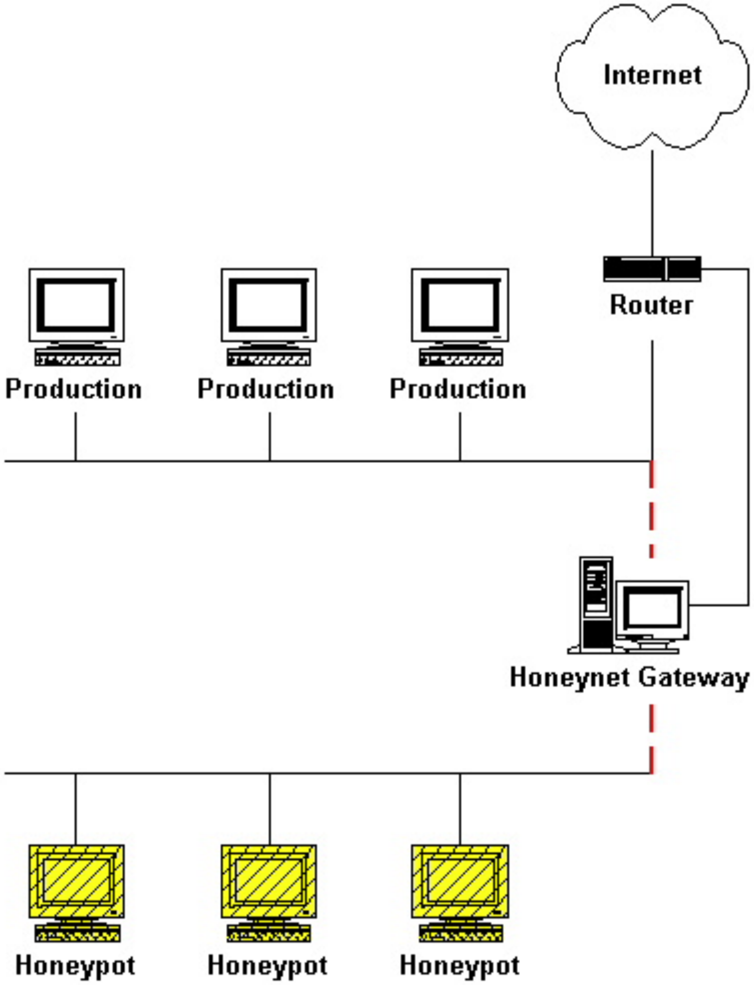
Honeynets

- Honeynets are a research honeypot.
- Not a product, but an architecture.
- An entire network of systems designed to be compromised.

Latest Developments

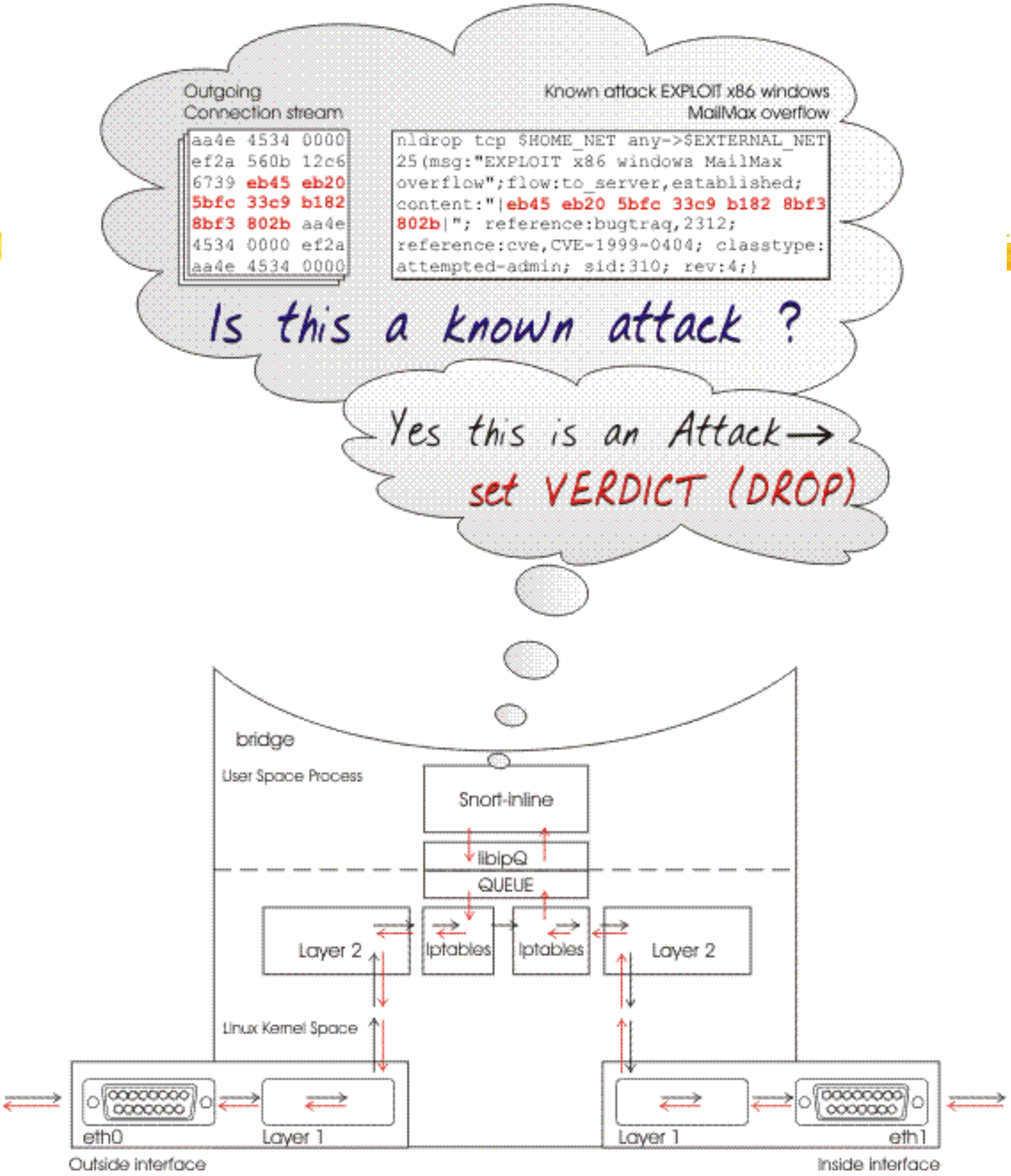
- Snort_Inline
- Sebek2
- Bootable CDROM
- User Interface

GenII Honeynet



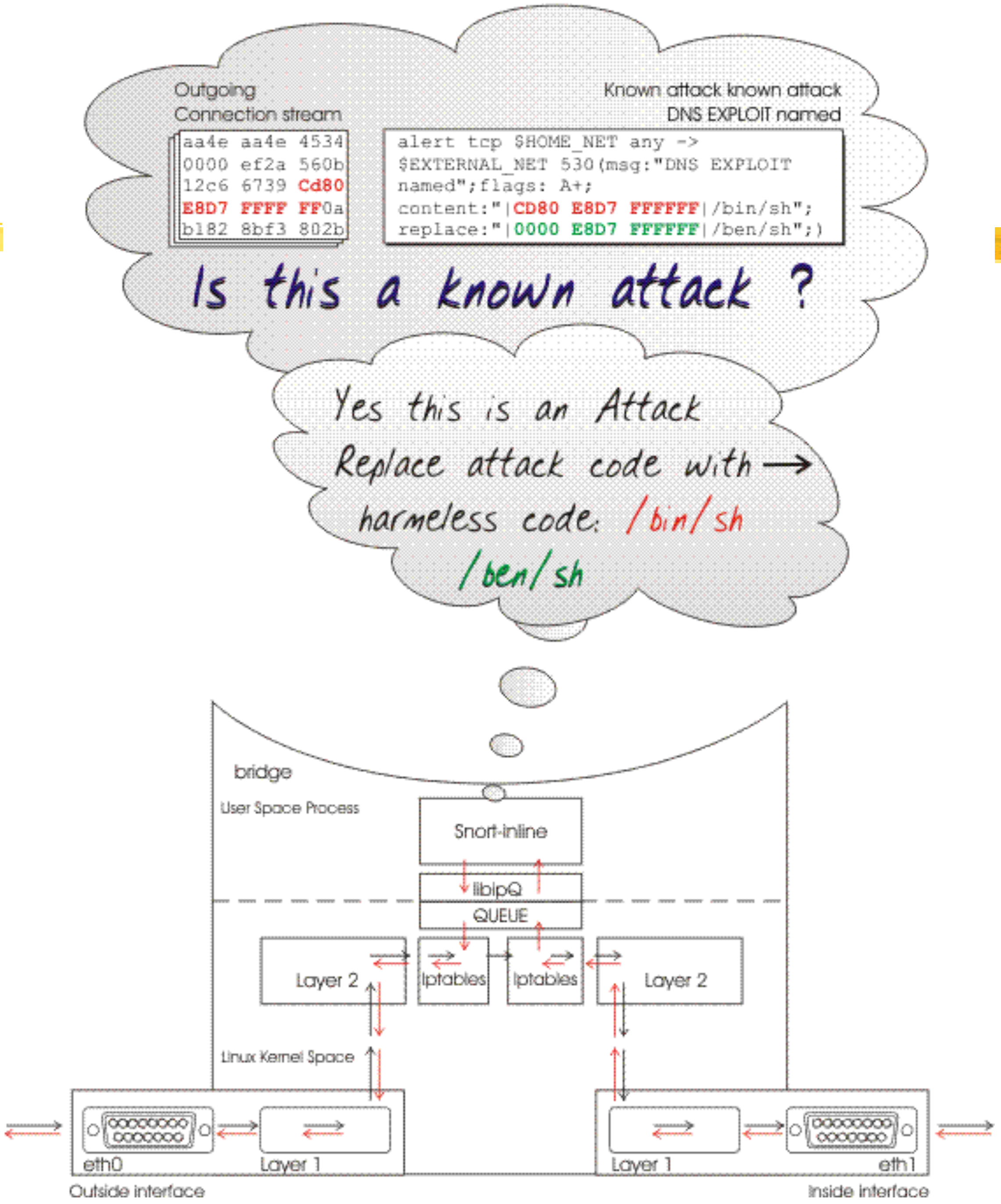
Snort-inline

```
drop tcp $EXTERNAL_NET any -> $HOME_NET 53
(msg:"DNS EXPLOIT named";flags: A+;
content:"|CD80 E8D7 FFFFFF|/bin/sh";


alert tcp $EXTERNAL_NET any -> $HOME_NET 53
(msg:"DNS EXPLOIT named";flags: A+;
content:"|CD80 E8D7 FFFFFF|/bin/sh";
replace:"|0000 E8D7 FFFFFF|/ben/sh";)
```



```
aa4e 4534 0000
ef2a 560b 12c6
6739 eb45 eb20
5bfc 33c9 b182
8bf3 802b aa4e
4534 0000 ef2a
aa4e 4534 0000
```

```
nldrop tcp $HOME_NET any->$EXTERNAL_NET
25(msg:"EXPLOIT x86 windows MailMax
overflow";flow:to_server,established;
content:"|eb45 eb20 5bfc 33c9 b182 8bf3
802b|"; reference:bugtraq,2312;
reference:cve,CVE-1999-0404; classtype:
attempted-admin; sid:310; rev:4;)
```



```
aa4e aa4e 4534
0000 ef2a 560b
12c6 6739 Cd80
E8D7 FFFF FF0a
b182 8bf3 802b
```

```
alert tcp $HOME_NET any ->
$EXTERNAL_NET 530(msg:"DNS EXPLOIT
named";flags: A+;
content:"|CD80 E8D7 FFFFFF|/bin/sh";
replace:"|0000 E8D7 FFFFFF|/ben/sh";)
```

Is this a known attack ?

Yes this is an Attack
Replace attack code with →
harmeless code: /bin/sh
/ben/sh

Sebek2

- Capture bad guys activities without them knowing.
- Insert kernel mods on honeypots.
- Mods are hidden
- Dump all activity to wire
- Bad guy can sniff any packet with pre-set MAC

Sebek2 Configuration

```
#----- sets destination IP for sebek packets
DESTINATION_IP="192.168.1.254"

#----- sets destination MAC addr for sebek packets
DESTINATION_MAC="00:01:C9:F6:D3:59"

#----- defines the destination udp port sebek sends to
DESTINATION_PORT=34557

#----- controls what SRC MAC OUIs to hide from users
FILTER_OUI="0A:0B:0C"
```

Sebek2 Output

```
06:06:25-2003/03/23 [0:mingetty:6785:vc/1:0]
06:06:26-2003/03/23 [0:mingetty:6785:vc/1:0]root
06:06:50-2003/03/23 [0:bash:13674:vc/1:0]ifconfig -a
06:06:58-2003/03/23 [0:bash:13674:vc/1:0]exec csh
06:07:08-2003/03/23 [0:csh:13674:vc/1:16]ftp ftp.openbsd.org
06:07:12-2003/03/23 [0:ftp:13738:vc/1:0]1bye
06:07:19-2003/03/23 [0:csh:13674:vc/1:16]vi /etc/resolv.conf
06:07:22-2003/03/23 [0:vim:13739:vc/1:0]1:q
06:07:28-2003/03/23 [0:csh:13674:vc/1:16]dig www.intel.com
06:09:39-2003/03/23 [0:csh:13674:vc/1:16]
```

Bootable CDROM

- Insert CDROM
- Boot
- Instant Honeynet Gateway (Honeywall)

User Interface

- Runs on Honeywall
- Analyze attacks in real time

Demo

Summary

- We are just beginning to see the potential for honeypots.

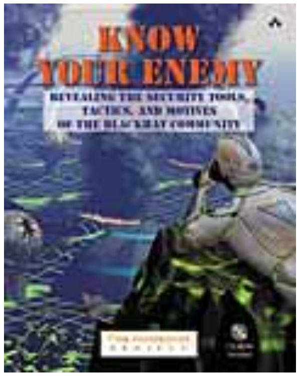
- Honeypots are where firewalls were ten years ago (*Marcus Ranum*)

Resources

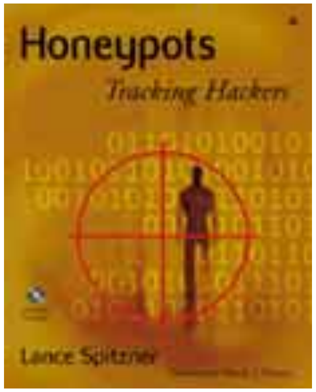
- Honeypot website
  - www.tracking-hackers.com
- Honeypots maillist
  - www.securityfocus.com/popups/forums/honeypots/faq.html

Resources - Books

- *Know Your Enemy*
  - www.honeynet.org/book/


KNOW YOUR ENEMY
REVEALING THE SECURITY TOOLS, TACTICS, AND MOTIVES OF THE BLACKHAT COMMUNITY

- *Honeypots: Tracking Hackers*
  - www.tracking-hackers.com/book/



?

Contact

Lance Spitzner
<lance@honeynet.org>