Global Information Assurance Certification Paper

Cynthia M. Peluso
SANS 2001 Conference, New Orleans
Level Two Advance Incident Handling and Hacker Exploits
GCIH Practical Assignment
Version 1.4
Current as of December 2000

Option 1 – Illustrate and Incident

Situation/Potential Incident

On February 21, 2001 our abuse e-mail address received a message from a very disgruntled individual citing ABC Company as being part of a SPAM incident. The e-mail cited one of ABC Company's hosts to be the generator of the SPAM. The individual writing the e-mail provided the original SPAM and IP header information. As ABC Company is a responsible commercial organization that would not like to be associated or to have been part of a spamming incident in anyway it warranted that this situation be investigated more thoroughly.

The reported Spam incident:

```
Please respond to RadicalSpamPerson@spammed.com
To:   abuse@abc.com, abuse@otherplacesalongtheway.com
cc:

Subject:    SPAM COMPLAINT Fwd: Home Loans for Any Credit - Get
Cash
Now!


AXON/AXONET,

You are party to illegal spam apparently generated from one of
your hosts
or an ICG host. Please plug this mail leak ASAP. If not resolved
you may
be liable under state law.

This email has reached a SPAM INTOLERANT domain that traces and
reports
all net abuse. It is suggested that you get this domain removed
from all
email lists to avoid further problems.
```

Spamming to or from California e-mail service providers against their
policy is now a civil offense under California Business and Professions
Code Section 17538.45
http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=6569414709+0+0+0&WAISaction=retrieve). Violation invokes damages of $50 per message.

The sending of any unsolicited email advertising messages to this domain,
located in California, will result in the imposition of civil liability
against you in accordance with Cal. Bus. & Prof. Code Section 17538.45.

Mail headers used for tracing and identifying spam origination and relay
points, as well as target domains follow:

Received: from somehost.email.msn.com [192.168.10.1] by spammed.com
[166.122.38.58]
        with SMTP (MDaemon.v2.8.5.0.R)
        for <RadicalSpamPerson@spammed.com>; Wed, 21 Feb 2001 08:20:36 -0800
Received: from _[10.10.10.1]_by ([192.182.10.4]) by somehost.email.msn.com with Microsoft SMTPSVC(5.0.2195.1600);
        Wed, 21 Feb 2001 08:20:29 -0800
Received: from [196.128.28.152] by _[10.10.10.1]_by with SMTP id A55C43E11 Wed, 21 Feb 2001 19:01:40 PDT
From: <HomeloanzNow!@xoip.com>
To: RadicalSpamPerson@spammed.com
Subject: Home Loans for Any Credit - Get Cash Now!
Mime-Version: 1.0
Content-Type: text/html; charset="us-ascii"
Date: Wed, 21 Feb 2001 19:18:57
Return-Path: HomeloanzNow!@xoip.com
Message-ID:
<CPIMSSMTPU03vR2GXbJ0000b979@cpimssmtpu03.email.msn.com>
X-OriginalArrivalTime: 21 Feb 2001 16:20:31.0994 (UTC)
FILETIME=[3648DDA0:01C09C22]
X-MDaemon-Deliver-To: RadicalSpamPerson@spammed.com
X-Return-Path: HomeloanzNow!@xoip.com
Reply-To: HomeloanzNow!@xoip.com
X-MBF-FILE: MDaemon Gateway to RFC822 (RFC822.MBF v1.0)

Interest rates are the lowest they have been in 18 months!

Refinance
Find out how much you can save by refinancing your existing mortgage.
Home Improvement

```
Cash in on your home's equity and use the money for home
improvements,
college tuition or any reason at all.
Debt Consolidation
Tired of high monthly bills and even higher interest rates? We
can take
all of your monthly bills and consolidate them into one low
monthly
payment.
Purchase
Buying a home? Let us get you pre-approved and find you a
mortgage at the
lowest available rate.


Applying is easy! Just complete
our online form.



=================================================================
                                Jim Asswall -
RadicalSpamPerson@spammed.com
                            "lack of information is a dangerous
thing"
   >> For a list of common Windows and PC tips see
www.spammed.com/tips <<
    "IRQ, DMA, & I/O" & "Troubleshooting Your PC" - MIS:Press/IDG
Books
* www.spammed.com * www.typc.com * www.bovine.org *
www.pcservicestation.com *
   ----->>>    Check out the NEW Windows Help Desk at
www.cnet.com
<<<------
=================================================================
```

Upon receiving the e-mail reporting the proposed SPAM incident by the ABC Company it was reviewed by the Information Security Department for further investigation.

The incident handler assigned the case reviewed the reported spamming. Upon reviewing the e-mail, the handler considered 2 options. Either ABC company was part of the spamming incident or it wasn't and the address information in the headers was spoofed. Still further investigation was warranted.

Preparation

In preparation of the investigation, I assembled my team. Right now, that consisted of myself, the system administrator of the box. The system administrator's supervisor and my supervisor were also part of the team. We

reviewed our findings and kept them abreast of the situation. They kept an eye on us so to speak, either concurring with our analysis and/or also helping us to discover areas we may have missed. Other members of the team included the disaster recovery team for the system, consisting of the disaster recovery lead, the backup lead and the system administrator and supervisor. To help in the identification of running services, application owners had to be brought in as well. A network administrator/analyst was also part of the team.

I had no tape recorder, but I did have my handy, dandy, bound notebook for recording notes. I made a special place in it just for this incident.

Identification

Host Vulnerability Analysis

The incident handler audited the server in question using Internet Security Systems' Internet Scanner to perform a vulnerability scan on the host implicated in the IP header information of the abuse report. The findings were as follows:

host.abc.com 10.10.10.1 AIX

RPC statd remote file creation and removal (CVE-1999-0019)	High
Sendmail 8.7.5 stack buffer overflow (CVE-1999-0131)	High
Files obtained	Medium
NFS exports outside domain	Medium
NFS mount daemon could allow remote attackers to determine whether files exist ~	Medium
NFS mount daemon operating on an unreserved port	Medium
TFTP	Medium
NFS exports	Low
NIS rstat service is running	Low
Rstat output	Low
Rusers output (CVE-1999-0626)	Low
SMTP daemon supports EHLO	Low
SNMP can reveal possibly sensitive information about hosts	Low
SNMP_Get able to retrieve Public Community Name (CAN-1999-0517)	Low

Sendmail 8.7.5 stack buffer overflow (CVE-1999-0131)

Sendmail versions 8.7.5 and earlier do not securely handle GECOS information. By supplying Sendmail with a very large GECOS field, a local user can overflow a buffer and execute arbitrary code on the computer, possibly compromising root privileges.

FIX

Upgrade to the latest version of Sendmail (8.7.6 or later), available from the Sendmail Consortium. See References.

As the system audit points out, the version of Sendmail running on this system could be compromised possibly resulting in root privileges. The RPC statd vulnerability was a false positive. The audit revealed a rpc.statd vulnerability, but

the ISS Internet Scanner reports this vulnerability as a false positive until you go to the system and verify the existence of /tmp/statd-vulnerable. If the file exists, then the system is vulnerable. This file did not exist for us. Also, the AIX OS level was above that which is reported in having the vulnerability, thus should be fixed in the version of AIX we were running. However, since this server is running AIX version 4.2.1, it was discovered that the ToolTalk version installed on this system is vulnerable to a buffer overflow exploit as explained in http://www.cert.org/advisories/CA-98.11.tooltalk.html. The vulnerability scanner did not pick up on this as running a vulnerability scanner for this exploit could have resulted in a denial of service condition on the server. Since the box was in production at the time that the scan was performed, we deemed not to perform this scan. The incident handler, upon reviewing the list of services installed on the system, remembered that there is a version of Tooltalk that is vulnerable to buffer overflow resulting in root access. Therefore, the system adiminstrator and the incident handler verified that the version of Tooltalk running was vulnerable. The trick is that Tooltalk gets updated with the OS update. There ends up being some complications in applying the system OS upgrade to this machine. This host is a managed node. Some years ago, IBM had a contract with ABC to deliver a new customer service system. As IBM was unsuccessful in delivering on the project, there was a impending lawsuit and as part of the settlement, ABC company got a lot of IBM hardware. AIX became a prevalant OS in ABC company as well as a bunch of RS6000's. This also included a AIX server that managed many other child servers. Wonderful IBM representative installed this state of the art system for ABC company. It seems, however that the knowledge transfer and training were insufficient. Apparently, the parent managing host OS needs to be upgraded before the managed hosts can be upgraded. Nobody in house knows how to upgrade this beast. Hence, there has been some resistance on the side of managment at upgrading this spider. The manager of the UNIX systems actually stated that it was running fine the way it is and there is no need to upgrade. The Information Security Dept. considers highly exploitable vulnerabilities to be sufficient reason to push for upgrades. So, even saying 'patch the system' can end up as a political nightmare and potentially a costly upgrade if it requires bringing in and IBMer or sending a system administrator to training to accomplish this. But, it is good judgement and practice and should be done way, so we will fight the battle until it's done.

We also ran ISS Internet Scanner to analyze the /bin/login file looking for embedded passwords. There were no results to make a positive indication of this.

Intrusion Detection Findings

It is true that ABC company's instrusion detection system and policies had not been quite up to snuff lately. It hadn't been properly tuned in a while and the incredible amount of false positives being fed into the system was making it difficult to ascertain by the NOC representatives whether to report an alarm or

not. Hence, they rarely did. The incident handler reviewed the intrusion detection system's logs for any activity involving the host in question. The findings were as follows:

Sig ID	Sub SigID	Protocol	Source IP		Dest IP		Source Port	Dest Port	Router IP
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
3010	0	TCP/IP	10.10.10.1	Innocenthost	10.10.12.10	anotherhost.abc.com	49	16663	0.0.0.0
3010	0	TCP/IP	10.10.10.1	Innocenthost	10.10.12.10	anotherhost.abc.com	49	16665	0.0.0.0
3010	0	TCP/IP	10.10.10.1	Innocenthost	10.10.12.10	anotherhost.abc.com	49	16678	0.0.0.0
3010	0	TCP/IP	10.10.10.1	Innocenthost	10.10.12.10	anotherhost.abc.com	49	16680	0.0.0.0
2100	0	TCP/IP	10.10.12.24	ahost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
3010	0	TCP/IP	10.10.10.1	Innocenthost	10.10.12.24	ahost.abc.com	21	4913	0.0.0.0
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
3010	0	TCP/IP	10.10.10.1	Innocenthost	10.10.12.28	goodhost.abc.com	21	3559	0.0.0.0
2005	0	TCP/IP	193.216.35.161		10.10.10.1	innocenthost	0	0	0.0.0.0
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0
2100	0	TCP/IP	10.10.12.28	goodhost.abc.com	10.10.10.1	innocenthost	0	0	0.0.0.0

The above picture is a truncated version of the intrusion detection logs of all alarms triggered involving innocenthost.abc.com with IP address 10.10.10.1 found in the original SPAM complaint. All the traffic in the log was valid internal traffic except the entry highlighted in red. Indeed, this IP address came from some source in Oslo, Norway as illustrated below in the WhoIs information. ABC company does not have any business or business partners in Norway.

```
193.216.35.161    02/26/01 11:57:44 whois 193.216.35.161@whois.ripe.net
                  Whois -h whois.ripe.net 193.216.35.161 ...
                  % Rights restricted by copyright. See http://www.ripe.net/ripencc/pub-services/db/copyright.html
                  Inetnum:     193.216.35.0 - 193.216.40.255
                  Netname:     C2INET1-NO
                  Descr:       Connect2Internet, Tele2 Norge AS
                  Descr:       Oslo, Norway
                  Country:     NO
                  Admin-c:     BCR6-RIPE
                  Tech-c:      BCR6-RIPE
```

Status: ASSIGNED PA
Mnt-by: AS2120-MNT
Changed: lene.elshaug@tele2.no 19980220
Changed: bcr@tele2.no 20001106
Source: RIPE

Route: 193.216.0.0/16
Descr: DAX-NET
Origin: AS2120
Mnt-by: AS2120-MNT
Changed: lene.elshaug@tele2.no 19980225
Source: RIPE

Person: Bernt Christopher Rosland
Address: Tele2 Norge AS
Address: Ulvenveien 75a
Address: N-0581 OSLO
Phone: +47 21 31 90 00
fax-no: +47 21 31 91 00
e-mail:
bcr@tele2.no
nic-hdl: BCR6-RIPE
changed: bernt.christopher.rosland@tele2.no 20000613
changed: bernt.christopher.rosland@tele2.no 20001003
changed: bernt.christopher.rosland@tele2.no 20001003
source: RIPE

The incident handler next scanned the intrusion detection systems logs for other alerts in connection with the foreign address. The findings were as follows:

Sig ID	Sub SigID	Protocol	Source IP	Dest IP	Source Port	Dest Port	Router IP
2005	0	TCP/IP	193.216.35.161	10.10.237.47	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.28.20	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.59.108	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.61.3	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.59.108	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.9.115	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.230.224	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.60.150	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.105.240	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.216.132	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.97.120	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.169.14	0	0	0.0.0.0

2005	0	TCP/IP	193.216.35.161	10.10.230.111	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.21.127	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.20.103	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.175.124	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.107.57	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.38.94	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.32.20	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.100.98	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.128.28	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.101.30	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.40.97	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.159.77	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.205.57	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.94.118	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.36.12	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.23.118	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.220.104	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.219.69	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.36.48	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.208.95	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.250.82	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.92.117	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.244.19	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.14.111	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.155.28	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.17.91	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.199.99	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.31.67	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.149.1	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.153.16	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.226.122	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.22.60	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.1.8	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.130.44	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.182.98	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.187.9	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.250.48	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.247.93	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.247.93	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.216.102	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.37.96	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.3.22	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.224.40	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.0.78	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.104.58	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.0.114	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.5.36	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.166.109	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.50.120	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.149.61	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.149.72	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.159.22	0	0 0.0.0.0

2005	0	TCP/IP	193.216.35.161	10.10.187.69	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.197.30	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.175.71	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.97.65	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.205.49	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.32.106	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.0.91	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.254.42	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.127.90	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.219.61	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.243.115	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.243.115	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.23.29	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.22.5	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.249.97	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.249.97	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.34.39	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.169.21	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.11.78	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.21.28	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.93.99	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.229.116	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.113.127	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.94.42	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.230.59	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.224.124	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.119.28	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.4.74	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.88.37	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.4.85	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.103.26	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.127.58	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.210.114	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.17.26	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.104.86	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.46.97	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.176.40	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.124.125	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.137.55	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.22.112	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.3.16	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.123.20	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.128.59	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.47.87	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.124.91	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.3.63	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.144.119	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.159.108	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.122.43	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.27.106	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.205.99	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.5.30	0	0 0.0.0.0

2005	0	TCP/IP	193.216.35.161	10.10.114.60	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.61.99	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.9.56	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.170.118	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.2.86	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.112.12	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.106.77	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.157.96	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.11.23	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.5.88	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.93.44	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.20.124	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.206.8	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.253.23	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.59.17	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.2.63	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.94.34	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.92.125	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.105.55	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.88.18	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.25.1	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.186.63	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.102.111	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.253.117	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.162.67	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.40.26	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.238.36	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.243.86	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.243.86	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.220.103	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.89.19	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.243.122	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.243.122	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.96.14	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.17.101	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.199.98	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.103.31	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.155.85	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.101.100	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.169.50	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.175.32	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.19.43	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.34.21	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.113.73	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.120.26	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.60.112	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.208.35	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.96.72	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.103.125	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.128.30	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.149.59	0	0 0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.23.50	0	0 0.0.0.0

2005	0	TCP/IP	193.216.35.161	10.10.178.49	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.176.12	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.32.2	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.88.71	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.20.166	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.60.150	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.173.79	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.177.143	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.177.143	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.177.143	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.177.143	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.163.21	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.105.206	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.105.206	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.105.206	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.178.49	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.4.6	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.60.212	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.103.106	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.60.157	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.226.220	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.24.186	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.123	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.60.193	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0

2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0

2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0a	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0

2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0

2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.179	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.12.51	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.24.186	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.24.186	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.105.180	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.91.91	0	0	0.0.0.0
2005	0	TCP/IP	193.216.35.161	10.10.10.1	0	0	0.0.0.0

The 2005 alarm signature corresponds to TTL Exceeded for a datagram. It looks like the Norway address has been mapping ABC company's network looking for hosts. It is also interesting that the host in question was the last host they scanned. They didn't get a host unreachable on this one. The scanning was random. They found one.

Closer analysis of the ids logs regarding 193.216.35.161 show that they have been attempting to scan our network over a long period of time. At first, they started out slow, probably to see if they were being watched. Some scans, however, came in and took hours that they were scanning our network, all night! The scans also came in as ttl exceeded messages which have an alert level of 2 on Netranger IDS. Probably wasn't looked for much at level 2. OK, not happy about this, but that's why I'm taking this class and am finishing this report now on the plane returning from the intrusion detection immersion curriculum (maybe I can use the same incident for my practical in that class with a different slant ☺). I'll include the log as an attachment. I also see quite clearly some of the downfalls of the comercial ids'. One can miss a lot. It would be nice to see what else tcpdump could find on this guy. ABC company has a class B address. It

looks like the perpetrator would scan us for a while, give up and come back at a later date and/or time.

There was no evidence of a spamming on the intrusion detection system which has a spam signature. Also, it is likely that this would also have been noticed as it is likely it would have consumed a large amount of network bandwith. Also, other than port mapping via TTL Exceeded, there were no other alarms or alerts on the intrusion detection system regarding the host in question. Note: at this time ABC company is not running tcpdump but a commercial ids that is signature based. Therefore, it is understood that critical packet or non-signature based information is missing. (see Lessons Learned)

Also, intrusion detection logs were combed investigating trusted hosts and their possible compromise. The only real system identified by the Oslo address or any other source for that matter happened to be the host id specified in the spam e-mail. All the other attempts at network mapping by Oslo were blank hits or misses.

The incident handler at this point is attempting to determine if any other sources indicate that the host reported in the SPAM incident may have been penetrated by an outside source. We found the vulnerability in the audit, now it looks as though an outsider has at least identified the systems existence.

Host Investigation

Next, the incident handler and the system administrator go to the system for a thorough examination to determine if the host was possibly compromised.

The system administrator identified the last known good binary backup and verified it. A dd image copy backup of the system was performed to a new tape in case it was necessary to preserve evidence. ABC company uses ADSM backup utility. A decision was made to keep the system connected to the network at this time until other evidence was uncovered indicating possible system compromise. This system was a very critical system and to halt it would have caused serious interruptions in business transactions. A spamming incident is unfortunate, but not fatal. Should other indications lead us to believe the system has otherwise been compromised then the decision will be re-evaluated.
The incident handler consulted the following documents as an aid to guide them through the detection phase of their analysis:

1. Incident Handling Step by Step: Unix Trojan Programs Version 2.3 from SANS Incident Handling/Hacking Exploits Curriculum.
2. Intruder Detection Checklist from CERT http://www.cert.org/tech_tips/intruder_detection_checklist.html

3. Steps for Recovering from a UNIX or NT System Compromise from Cert/CC Current Activity http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

The checks below were conducted. Nothing unusual turned up.

- check /etc/passwd file for entries that do not belong.
- check to see if /etc/inetd.conf has been modified.
- if you allow the "r-commands" (rlogin, rsh, rexec), ensure that there is nothing that does not belong in /etc/hosts.equiv or in any .rhosts files.
- check for new SUID and SGID files. The following command will print out all SUID and SGID files within your filesystem.

```
# find / \( -perm -004000 -o -perm -002000 \) -type f -print
```

- Check your system and network configuration files for unauthorized entries. In particular, look for '+' (plus sign) entries and inappropriate non-local host names in /etc/hosts.equiv, /etc/hosts.lpd, and in all .rhosts files (especially root, uucp, ftp, and other system accounts) on the system. These files should not be world-writable. Furthermore, confirm that these files existed prior to any intrusion and were not created by the intruder.
- Look everywhere on the system for unusual or hidden files (files that start with a period and are normally not shown by 'ls'), as these can be used to hide tools and information (password cracking programs, password files from other systems, etc.). A common technique on UNIX systems is to put a hidden directory in a user's account with an unusual name, something like '...' or '.. ' (dot dot space) or '..^G' (dot dot control-G). Again, the find(1) program can be used to look for hidden files, for example:

```
find / -name ".. " -print -xdev

find / -name ".*" -print -xdev | cat -v
```

Also, files with names such as '.xx' and '.mail' have been used (that is, files that might appear to be normal). The team also looked for " ..".

In addition, we checked pertinent log files for any signs of unusual activity of which we found none.

Netstat –a did not reveal any more, less, unusual or unknown services than that what we expected.

Network cards were not in promiscuous mode. We ran an ifconfig to look for the PROMISC flag. It did not exist.

We also compared ls –la results to that of echo *. The output was the same.

./rootme /bin/sh thankfully was ineffective as well. We were looking for the possible presence of a rootkit by doing this.

No unusual cron or at jobs or files were found.

CERT also indicated that there have been widespread compromises lately with the ramen toolkit as noted in CERT Incident Note IN-2001-01 -- Widespread Compromises via "ramen" Toolkit http://www.cert.org/incident_notes/IN-2001-01.html. The team thought it was a good idea to check for the possible existence of this root kit. At this time there were no other indications pointing to compromise, but they thought it would be good idea anyway. Below shows the the work done to look for possible indicators of the ramen toolkit.

When a host is compromised, the ramen toolkit is automatically copied to the compromised host, installed in "/usr/src/.poop", and started. The ramen toolkit is controlled by a series of shell scripts that make modifications to the compromised system and initiate attacks on other systems. Several notable system modifications are made in sequence after ramen is started. The team didn't find any "poop" on their systems.

- All 'index.html' files on the system are replaced with an intruder-supplied 'index.html' file . This system has no index.html and shouldn't.
- The system file '/etc/hosts.deny' is deleted. This system did not have a hosts.deny file, but the sysadmin was assured that was because the system was AIX. The incident handler has made a note to verify this at a later date. The handler is not that familiar with AIX and so will respect the expert opinion until knowledge is discovered to the contrary.
- The file '/usr/src/.poop/myip' is created and contains an IP address for the local system. Still we found no poop.
- A script is added to the end of '/etc/rc.d/rc.sysinit' to initiate scanning and exploitation during system startup. This did not exist.
- For systems with '/etc/inetd.conf'
    - an intruder supplied program is added as '/sbin/asp'. A service named 'asp' is added to '/etc/inetd.conf' and inetd is sent a signal to reload the configuration file. This causes inetd to listen on TCP socket number 27374 for incoming connections. /sbin/asp did not exist, nor was inetd listening on TCP socket number 27374
    - usernames 'ftp' and 'anonymous' are added to '/etc/ftpusers' . Did not exist.
    - services 'rpc.statd' and 'rpc.rstatd' are terminated
    - the system files '/sbin/rpc.statd' and '/usr/sbin/rpc.statd' are deleted

Successful exploitation results in the target host being root compromised. In addition, several actions are automatically taken on the newly compromised host that result in ramen being propagated from the attacker to the victim.

- the directory '/usr/src/.poop' is created on the victim host
- the 'ramen.tgz' toolkit is copied from '/tmp/ramen.tgz' on the attacking host to '/usr/src/.poop/ramen.tgz' on the victim host
- 'ramen.tgz' is copied to '/tmp/ramen.tgz' on the victim host
- 'ramen.tgz' is unpacked in '/usr/src/.poop' and the controlling shell script is started

The method of propagation is provided by the intruder-supplied 'asp' service. It receives connections on TCP port 27374 of the attacking host and responds by sending a copy of '/tmp/ramen.tgz' to the victim host.

Situation analysis and thinking:

When investigating the incident, the incident handler also went to the web site of the person reporting the spam. Making some inferrences and yes assumptions, this individual 'John' seems to view himself as some type of cyber-spam cop out to save the universe, rather righteous and of course a computer know it all. It should also be noted that if you look at the reported spam incident that the person reporting the incident included his own 'commercial' at the end of the spam report document. That's rather interesting. There were no other reports of abuse sent to ABC company other than this one source.

Other than the host scan into ABC's network, there was no other evidence indicating that the accused host was actually compromised, penetrated or otherwise involved in the spamming incident. We did, however, find somebody mapping out our network by this little exercise. That was fun and warrants that source id be added to our watch list.

Containment, Eradication and Recovery

Should the system need to be disconnected from the network, disaster recovery procedures would be put into place. Binary backups are performed on a weekly basis. The data is mirrored in realtime to a backup DASD farm at a remote location. This location also has a backup server in the event the production server went down or was compromised. The server is on the remote network. The applications are installed but not up. In the event of a disaster, the production node could be removed from the network. The applications would be brought up on the backup server and the data would be accessed on the mirrored DASD farm.

At this time, the incident handler has been unable to get the system adminstrators to verify the binaries on the system against an original version from CD. However, they are open to tripwire being installed on their systems. The Information Security Department is currently in negotiations with Tripwire for purchase of the product. My plan is to have them build a Golden server from CD, take a snapshot of it withTripwire at that time and then make them compare the binaries on the host in this paper as well as others. This may not be perfect, but I'll accept winning small battles at a time to win the war.

Another problem area is in definitively and positively identifying the services running on the servers. These boxes are very powerful boxes and as such run a

lot of services. It is difficult, without properly documenting the systems to know what's what after a while. The matter gets further complicated in the the system administrators may not know all the services as they could be installed by an application that requires the service. They system acts as a gateway to our IBM mainframe, holds the ACE server (RSA), and hosts other applications as well. We brought in the application owners to assist in the identification of services. There were some services on that do need to be turned off. The incident handler did check the updated list of ports used by trojans but didn't see anything suspicious. That is part of recovery, eradication and followup. We do have good disaster recovery procedures in place. We have off site mirrored data storage, backup, systems and redundant networks in place.

At this time, we have been unable to find evidence that this host was compromised in any way. No recovery procedures were taken at this time in terms of restore type recoveries.

Even though we were not able to prove system compromise, we made certain that the results of the vulnerability scan were corrected. Patches and upgrades were applied and the appropriate configuration changes were made. Ports not in use were closed.

Root passwords were changed on the suspect host and all trusted hosts. The network analyst put a filter on to log any network activity from the Oslo address. There were no more hits on this address. After the network monitor was taken off of logging, the ids system did turn up a few more benign attempts at network mapping. No hosts were identified in the scanning. And the scanning this time was short in duration and in scanning with no more attempts since. So far, it looks like they may have even given up. But, time will tell on that. ABC Company infrastructure also consists of a pretty sophisticated switched network. Their security may not be perfect, but it's not too bad either and we are constantly working to improve our security presence. I'm sure there are a lot easier targets out there to penetrate and exploit. We are watching for the perpetrator. Another instance of attempted network mapping and we will contact the ISP in an attempt to get this activity stopped. I am hesitant to put an ACL on the outside router. At least now I can watch the activity by this address and so far the address has been static. If I created and ACL to keep the address out, they may come back with another source ip address. I think this would only confuse things. How would I ever know if it was the same person?

Follow Up, Lessons Learned, Conclusions

1. We're totally wrong. The incident handling team is completely wrong, missed every thing pointing to this host being involved in the incident and the host was compromised and responsible for the spamming.

2. Lack of evidence. The IP address in the received information of the header information from the spam report was spoofed. If you look closely at this information, you will see that the host 10.10.10.1 is referenced twice. It seems unlikely that this would serve as a relay point 2 times in the same spamming. Also, you will notice that all the other ip addresses in the received lines of the header information include hostnames. The host 10.10.10.1 does not. The consensus of the incident handling team was to clean up the system vulnerabilities. This was already in progress because a security audit was recently performed. It was known that the version of AIX was out of date and Sendmail was too. The OS is in the process of being upgraded and then Sendmail will be upgraded too with anti-spam filters in place.

Intrusion detection logs are analyzed more thoroughly now on a daily basis. To tell the truth, this incident handler is a one-woman machine. I am the security department and this is relevant. It takes a lot of time to examine intrusion detection logs, shake out the false positives. One person to do all vulnerability analysis and follow up on hundreds of servers with multiple OS' ranging from NT to AIX, Solaris and HP. One person to make sure that systems are implemented securely and to sit in on project planning meetings at the beginning of a project. One person to make sure that firewall rules, router acl's and effective countermeasures are put in place, etc., etc. My immediate manager is newer to the department than I am and he is getting the idea that he needs more people. It is still very difficult to get upper management to buy in to the fact that this is all needed. Not to say I do this all myself, because I don't an couldn't. That team that is put together for incident handling is also part of a team to analysts and system adminstrators that work hand in hand daily to secure all the above. I only add this above because you want to know obstacles. Recognition of the problem and adequate staff to perform the work is a big obstacle.

We also recognize the fact that these two incidents aren't necessarily related, but separate issues. But, the Oslo address is the only address from the outside that accessed this machine. Furthermore, there wasn't any evidence of this coming from inside our network.

By the way, I cleansed the data in this report for nodes in ABC's (my) network. This really did happen. The 193, Oslow, Norway address is real as are the ids reports and all the other information. I did not report it at the time. You can also use this as a intrusion report.