Network and Systems Audit Report for Some Random Internet (Sample.com)

Presented

July 16, 2004

Table of Contents

Note for sample report readers – All IP addresses and domain names have been changed to protect the identity of customers. If any of the names used in here actually match real-life persons, organizations or such, it is purely coincidental.

Executive Summary

Some Random Internet (aka Sample.com) was audited in June of 2004. Follow-on auditing and investigations were performed during June and July of 2004 based on examination of preliminary results. After analysis of the results, this network would be classified as having moderate security. There are several systems, with vulnerabilities that are found in the FBI/SANS Top 20 lists. See the web page http://www.sans.org/top20/ for detailed information. It is strongly recommended that these vulnerabilities be addressed first and others addressed later on, since these represent where the majority of successful attacks occur. The list of hosts which have vulnerabilities found on that list are highlighted in the "FBI/SANS Top 20 Candidates" table at the end of this report.

One key additional problem is that the name servers (DNS) are not up-to-date, complete, or accurate. This led specifically to the difficulty of the audit software finding problems that could not be pinned down to a specific system without performing other tests. This list includes several systems with vulnerabilities on the FBI/SANS Top 20 lists. It is recommended that this audit be re-performed after the name servers are cleaned up and identifiable vulnerabilities addressed.

It is also recommended that more in the way of written and endorsed/enforced standards are adopted and all technical staff trained on these. A number of vulnerabilities, oversights and mistakes appear to be a result of lack of follow-up or good training on procedures with the technical staff. These are detailed further in the main body of the report.

The networks audited were divided into two groups

- Internal and Hosting Operations (specified by VP of Operations)
- Customer premises IP address ranges

The security vulnerabilities found fell into four main categories:

- Five servers have MySQL databases which Nessus determined to be unprotected by passwords (2 are Sample.com and 3 are of Sample's customers)

- Seven Apache Web servers are running code with known vulnerabilities in several related classes:
  1. Outdated Apache software (Web server itself)
  2. Outdated OpenSSL software (Encryption methods)
  3. Outdated PHP software

- Unnecessary services which themselves pose a security risk:
  1. The "r" commands (from Berkeley Unix) and "telnet"
  2. TCP/IP Simple Services which serve no useful purpose.
  3. Software installed by default and left unconfigured (IIS home pages, SMTP (email) servers (open relays), and sample files left in place.

- Assorted vulnerabilities that have been discovered, for which patches may (or may not) have been applied, but due to poor version control on the part of the developers, must be manually verified.

Observations and Recommendations

All Systems in General

There are many systems that exhibit a number of security weaknesses of one sort or another in common. Collectively these are:

Service		Recommendation
• Rsh • Rexec	• Login • Telnet	Use SSH instead.
• Nfs		Shared (exported) file systems - filter
• TCP Simple Services		Disable on all systems
• SMTP on non-mail servers		Disable where appropriate
• SNMP “Public” and “Private”		Disable or change to a unique name
• Daytime		Disable or filter
• ICMP Time Stamps		Disable or filter
• RPC Services (Sprayd, Rstatd, Rusersd, etc.)		Disable or filter
• ToolTalk (Solaris systems)		Disable or filter
• Non Routing equipment (hubs, switches, UPS, Cameras, etc.		Renumber to “hidden” private IP space or filter from outside.

There is one key flaw that appears to have been deliberately configured. IP addresses within Sample’s range are trusted (compared to those from the outside world which are not). Since any of the hundreds of unprotected DSL systems could use these permissions to compromise some of Sample’s equipment, it is recommended that Sample narrow the scope of trusted addresses with respect to their hosted, and network equipment to further protect their own systems.

Web Servers

About half a dozen web servers were found with various outdated forms of software. It is recommended that Sample use one of the Retina class C web server scanners (Free from eeye.com) to simply identify the build and version of all web servers, and thereafter, keep a log of all systems and versions built, and make the maintenance of that a formal part of the build and updating process.

There were also four servers which appear to have their default welcome pages set: maui.Sample.com, (http/s) spruce.Sample.com (http/s), ns-green.Sample.com (http), and 06.amateur.com (https).

Once that process is set up or brought up to date, most of the web servers should be tightened down to:

• Update all code revisions to the latest stable version, with all patches in place.
• Prevent the actual server maker and build identification from being publicly displayed.

• Prevent many of the “Cross-Site-Scripting” vulnerabilities
• Disable the TRACE and TRACK methods on all Web servers
• Matt Wright’s “FormMail” software should be upgraded
• Check the UserDir module on all Apache servers
• CGI’s which are known to contain vulnerabilities, and ALL sample files
• Use Tripwire (commercial or public) to generate checksums on all O/S components to validate files against tampering.

Customers

Based on the NetBIOS (TCP port 139) and Name Service (DNS at UDP port 53) scans, security awareness and practices for many customers are non-existent or sketchy. This poses a potential liability risk for Some Random Internet if customer’s systems engage in harmful activity (DOS/DDOS, spreading worms, SPAM, etc.) and Sample does not take specific action to curtail and/or prevent this, then it is possible that they may be subject to liability under tort law. See the referenced article at: http://www.tisc2001.com/newsletters/43.html.

A significant number of vulnerable systems were found within the DSL and other areas of Some Random Internet. There is the very real possibility that some of these systems could be used in DDOS (Distributed Denial of Service), spamming, and other undesirable and possibly illegal activities. It is recommended that Some Random Internet begin a program of educating their customers as to their (the customer’s) responsibilities with respect to system and network security.

DNS Servers

The data in the DNS servers is poorly and inconsistently maintained. There are numerous examples of “abandoned” names, use of names (e.g. empty.com) that do not belong to Sample.com, at least one block of data that was copied and pasted from elsewhere, but never corrected for the new address range.

There is especially inconsistency in the management of addresses that are no longer in use. These vary from what is presumed to be a former customer (although it might be a backup site), empty.sample.com, www.empty.com, www.empty.net and simply the normal reverse (PTR) records. The domains empty.com and empty.net should be eliminated immediately, since they belong to someone else.

Audit Methodology

The audit is performed in several discrete steps. The first task is to identify all hosts (any server, workstation, network equipment, etc.) identifiable by one or more IP addresses.

All of the responding IP addresses – within the ranges identified by V.P. of Operations as being office, servers, and hosting, are then scanned for all 65,535 possible TCP ports. Most of those are commonly associated with well-known services, but there are a number of responding ports that are not known to belong to any particular service. These are detailed in the port summary where the service was not known to allow for further investigation by Sample staff.

The range of IP addresses belonging to the "office" range was then subjected to an audit by Nessus – with all known DoS (Denial of Service) disabled. A few notes are in order here – some "vulnerabilities" are found in the Nessus report – such as DNS servers allowing zone transfers, or Mail Servers allowing for "spam" forwarding. These reports have been "grayed-out" where it has been verified that these were only allowed within the address space of Sample and refused when attempted from outside Sample.

The name servers (and their contents) were analyzed in detail both from a forward zone (Sample.com and Sample.net), and a reverse zone (e.g. 29.16.172.in-addr.arpa) perspective using two different tools – DNS Expert from Men and Mice software, and Solar Winds DNS Audit tool from SolarWinds.net.

The type of errors searched for included whether or not a given IP address would resolve to a name, and whether or not that name would resolve back to the same (or multiple) IP Addresses. For forward lookups, zone transfers were done to find problems such as "CNAME" chains – where one alias points to another alias, where name servers listed as authoritative turned out NOT to be authoritative, and other such inconsistencies.

All "office" address ranges were also scanned with a number of tools to detect known vulnerabilities that are caught by Nessus, but due to deliberate redundancy are separately checked for. They are the publicly available vulnerability scanners (from eeye.com, Microsoft.com, ISS.net and other sources) and the SolarWinds suite of tools.

The RAPS (Remote Access Perimeter Scanner) tool from Symantec was run against the "office" IP range to detect various remote control applications, both legitimate and illegitimate (e.g. pcAnywhere, Carbon Copy, LapLink, Remotely Possible, VNC, X-Windows, Dameware, SubSeven, Back Orifice, etc.)

All "non-office" IP addresses were scanned very lightly for two identifiers:

1. NetBIOS (TCP port 139) which would indicate a machine running one of the following: Windows, MS-DOS, PC-DOS, Unix/Linux running Samba/PC-Link, or Macintosh running DAVE
2. DNS lookup (UDP port 53), which often indicates an Apple Macintosh running Mac OS 9 or X.

The purpose of this is to identify home systems (and others) which are not using a firewall, proxy or other mechanism to protect the network or computer(s).

The data produced from these tests is then analyzed in detail for severity, appropriateness (meaning, if an error is identified, is it *actually* an error within the context of the audit), clues to further potential problems, and then reduced to tables for your review.

During the process of analyzing the data, any anomalies and severe reports are analyzed (where possible) for further resolution. By way of example, Nessus reported some FTP sites as “world-writeable” based on the directory permissions. This was incorrect because the server appeared to be protected by TCP-Wrappers or a similar product. As a result, that item was grayed out in the vulnerability report.

Due to the large amount of data processed, the results tables are highlighted or color-coded to indicate items recommended for immediate attention, as opposed to those that are judged less severe. The host summary table (below) shows a count of those systems showing one or more vulnerabilities (holes), warnings, or open ports, as seen by Nessus. This allows the reader to quickly look up the details for those systems in the vulnerability reports themselves.

Categories are as follows:

Red Highlight – SANS/FBI Top 20 Vulnerability

Yellow Highlight – High or Medium Priority or Easy fix

Pink Highlight – Easy Fix, Highly Recommended

Light Blue Highlight – Inconclusive Results

One key item, which was deliberately NOT tested for, is the ability to mount and read or write to Windows/Unix/Macintosh systems with exported file systems via NetBIOS.

The following aspects of the Internal Operations networks were examined:

- Full TCP port scan to identify open services on all responding systems
- Full forward and reverse audits of all identifiable name servers (DNS)
- Full Nessus audit of all known services – web servers, databases, etc.
- Specific tests for SQL Server, Microsoft IIS, Apache Web servers
- Full SNMP Scans for default community names (public & private)
- Un-patched Windows, Unix, Linux systems
- Unnecessary (and possibly vulnerable) services
- Email servers that allow unrestricted forwarding (SPAM)
- File systems exposed to the Internet (NFS, FTP, Windows, Databases, etc.) which could “leak” information, or worse, allow alteration.
- Infrastructure equipment which has no reason to be exposed to the Internet

FBI / SANS Top 20 and High Risk Systems List

Those systems which present vulnerabilities found in the FBI/SANS Top 20 lists (10 for Unix/Linux, 10 for Windows platforms) are highlighted in Red in the list below, High priority vulnerabilities NOT in the Top 20 list are highlighted in Yellow below. Ordering is in order of holes, Warnings, Open Ports found.

Host	Holes	Warnings	Open ports
redwood.Sample.com	22	76	33
ultra.nulldevice.net	16	108	59
ns-blue.sample.net	10	26	21
redwood-en0.Sample.com	9	27	21
windmill-en0.Sample.com	6	38	23
ns-green.sample.net	6	37	9
spider.sample.net	6	32	17
noc-cam2.Sample.com – Why is a security camera on the net?	6	6	2
spruce.Sample.com	5	37	9
pile-hole2.sample.net.60.21.172.in-addr.arpa	5	21	12
schwei.Sample.com	5	18	7
pile-hole3.sample.net.60.21.172.in-addr.arpa (Missing Dot?)	5	14	11
o6.amateur.com	4	48	9
ash.Sample.com	4	43	15
cedar.Sample.com	4	34	22
namebase-yellow.Sample.com	4	18	11
stinky.sample.net	3	34	22
empty.Sample.com	3	31	3
digger.Sample.com	3	26	12
hayes-pwr1.sample.net – Is this a UPS on the net?	3	16	5
noc-radio-ethernet.sample.net	3	11	2
hill-linuxbb.Sample.com	3	11	2
quake.Sample.com	2	43	21
www.xyz.net	2	43	19
www.empty.com Does not belong on Sample.com	2	37	13
www.bbx.net	2	35	13
228.wwwblock.sample.net	2	28	14
227.wwwblock.sample.net	2	25	14
229.wwwblock.sample.net	2	24	14
235.wwwblock.sample.net	2	20	13

236.wwwblock.sample.net	2	20	13
hotdog.Sample.com	2	14	4
g-airhead.Sample.com	2	11	5
189.dhcp-160.sample.net	2	8	3
wb6zvw.Sample.com	2	7	1
oahu.Sample.com	1	41	10
ns-red.sample.net	1	38	20
226.wwwblock.sample.net	1	38	14
www.sometown.com	1	37	19
maui.Sample.com	1	35	8
232.wwwblock.sample.net	1	24	13
birch.Sample.com	1	24	12
230.wwwblock.sample.net	1	22	14
my.Sample.com	1	18	13
phoenix.sample.net	1	18	8
pile-hole1.sample.net.60.21.172.in-addr.arpa	1	16	7
240.wwwblock.sample.net	1	15	14
238.wwwblock.sample.net	1	14	12
noc-pwr4.Sample.com.160.195.208.in-addr.arpa – Is this a UPS on the net? – Also – likely missing dot in DNS data file.	1	13	4
h-cam1.Sample.com – Why is a security camera on the net?	1	12	3
m2.proadmin.com	1	11	4
owall.Sample.com	1	11	2
h-sw1.Sample.com	1	11	2
m1.proadmin.com	1	10	2
www.changeintended.com	1	9	13
covad-dssi-ethernet.sample.net	1	9	2
dssi-dssifw.sample.net	1	8	3
www.thexyxyxyxyxfamily.com	1	7	13
noc-sw1.Sample.com	1	7	2
noc-sw2.Sample.com	1	6	2
pile-sw1.sample.net	1	6	2
172.21.60.126	1	6	1
ftp-yellow.Sample.com	1	5	11
sm-u1-nmc.Sample.com	1	5	1
hayes-sw1.sample.net	1	5	1
hill-sw1.Sample.com	1	4	1
sparky.not-there.net	1	3	2
239.p1.dialup.sample.net	1	1	4
225.wwwblock.sample.net	0	34	14

245.wwwblock.sample.net	0	27	13
241.wwwblock.sample.net	0	26	14
242.wwwblock.sample.net	0	25	14
237.wwwblock.sample.net	0	25	13
www.isabean.com	0	24	3
243.wwwblock.sample.net	0	23	13
www2.gimmedabiznesss.bz – Can’t find site	0	23	13
kauai.Sample.com	0	20	4
231.wwwblock.sample.net	0	18	13
244.wwwblock.sample.net	0	18	13
www.chokepeare.com	0	18	3
233.wwwblock.sample.net	0	17	13
tickets.countyfair.com	0	17	4
www.onionstore.com	0	16	13
234.wwwblock.sample.net	0	16	13
pine.Sample.com	0	15	8
clove-public.sample.net	0	13	2
239.wwwblock.sample.net	0	11	12
server2.Sample.com	0	10	3
server1.Sample.com	0	10	3
crews-bb.sample.net	0	9	3
172.21.5.250	0	8	4
seismo.Sample.com	0	8	3
server1-lo0.sample.net	0	8	3
server2-lo0.sample.net	0	8	3
shaky-lo0.sample.net	0	8	3
totoro-lo0.sample.net	0	8	3
noc-setengr.sample.net	0	8	3
noc-specz.sample.net	0	8	3
covad-dssi-cisco.sample.net	0	8	3
totoro-amp-cbean.sample.net	0	8	3
server1-fe0-0-2a.sample.net	0	8	3
server1-s2-3.sample.net	0	8	3
server1-tun0.sample.net	0	8	3
h-u1-arc.Sample.com	0	8	2
pile-ups1.sample.net – Is this a UPS on the net?	0	8	2
totoro.Sample.com	0	7	3
barnyard.Sample.com	0	7	3
noc-ups3.Sample.com – Is this a UPS on the net?	0	7	3
server1-fast-0-0-6.Sample.com	0	7	3

server2-winnco.Sample.com	0	7	3
172.21.5.249	0	7	3
server1-et0b.Sample.com	0	7	3
172.21.32.46	0	7	3
sm-disty.sample.net	0	7	3
server3-fe3-0-3.sample.net	0	7	3
server1-fe0-0-3.sample.net	0	7	3
server1-fe0-0-0a.sample.net	0	7	3
totoro-dssi.sample.net	0	7	3
server2-tun0.sample.net	0	7	3
br-server1.sample.net	0	7	3
172.21.60.97	0	7	3
hayes-bb.sample.net	0	7	3
pile-bb.sample.net	0	7	3
towne-bb.sample.net	0	7	3
crews-ups1.sample.net – Is this a UPS on the net?	0	7	3
tank-bb.sample.net	0	7	3
noc-pwr2.Sample.com – Is this a UPS on the net?	0	7	2
barnacles-lo0.sample.net	0	7	2
server2-barntel.Sample.com	0	6	3
noc-top-acre.sample.net	0	6	3
sm-u1-nmc.Sample.com	0	0	2
sm-charterbus.sample.net	0	6	3
sm-randye.sample.net	0	6	3
dssi-totoro.sample.net	0	6	3
sm-u1-arc.Sample.com	0	6	2
h-ups1.Sample.com – Is this a UPS on the net?	0	6	2
barntel-server2.Sample.com	0	6	2
specz-noc.sample.net	0	6	2
charterbus-sm.sample.net	0	6	2
disty-sm.sample.net	0	6	2
sakata-s0-0.sample.net	0	6	2
endive-sm.sample.net	0	5	3
noc-pwr3.Sample.com – Is this a UPS on the net?	0	5	2
noc-pwr1.Sample.com – Is this a UPS on the net?	0	5	2
noc-mux1.Sample.com	0	5	1
sm2.Sample.com	0	4	2
sm8.Sample.com	0	4	1
h-mux1.Sample.com	0	4	1
winnco-server2.Sample.com	0	4	1

ace-noc.sample.net	0	4	1
h-pwr1.Sample.com – Is this a UPS on the net?	0	3	2
sm1.Sample.com	0	3	1
noc-ups1.Sample.com – Is this a UPS on the net?	0	3	1
sm9.Sample.com	0	3	1
sm5.Sample.com	0	3	1
noc-ups2.Sample.com – Is this a UPS on the net?	0	3	1
hayes-ups1.sample.net – Is this a UPS on the net?	0	3	1
tank-ups1.sample.net – Is this a UPS on the net?	0	3	1
noc-hill.Sample.com – may need to be re-scanned	0	2	2
hill-noc.Sample.com	0	2	2
sm7.Sample.com	0	2	1
sm6.Sample.com	0	2	1
h3.Sample.com	0	2	1
towne-pwr1.sample.net – Is this a UPS on the net?	0	2	1
tank-pwr1.sample.net – Is this a UPS on the net?	0	2	1
hill-crews-ethernet.Sample.com	0	2	0
h1.Sample.com	0	1	1
h2.Sample.com	0	1	1
hill2-radio.sample.net	0	1	0
empty.sample.net	0	1	0
specialized-radio.sample.net	0	1	0
setengr-radio.sample.net	0	1	0
sakata-radio.sample.net	0	1	0
hill-900.sample.net	0	1	0
amp-cbean-totoro.sample.net	0	1	0
hill-crews-radio.sample.net	0	1	0
hayes-dist1.sample.net	0	1	0
pile-dist1.sample.net	0	1	0
pile-dist2.sample.net	0	1	0
towne-dist1.sample.net	0	1	0
crews-dist1.sample.net	0	1	0
tank-dist.sample.net	0	1	0
victor-bb.sample.net	0	1	0

Excerpts from the Full 64K TCP Port Scans

Red highlight = services listed on the FBI/SANS Top 20 list
Yellow highlight = services that are suspicious based on high port number
Blue highlight = services that are unaccounted for and should be verified.
Gray highlight = services that can probably be disabled.

```
Interesting ports on birch.Sample.com (172.16.160.158):
(The 65522 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp      open        ftp
22/tcp      open        ssh
23/tcp      open        telnet
24/tcp      open        priv-mail
25/tcp      open        smtp
53/tcp      open        domain
512/tcp     open        exec
513/tcp     open        login
514/tcp     open        shell
543/tcp     open        klogin
544/tcp     open        kshell
1334/tcp    open        unknown       (WriteSrv ?)`
9090/tcp    open        zeus-admin
```

```
Interesting ports on sm5.Sample.com (172.16.160.159):
(The 65533 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp      open        telnet
1643/tcp    open        unknown       (Isis-ambc ?)
```

```
Interesting ports on noc-pwr1.Sample.com (172.16.160.161):
(The 65533 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp      open        telnet
80/tcp      open        http
```

```
Interesting ports on noc-ups2.Sample.com (172.16.160.162):
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp      open        telnet
```

```
Interesting ports on noc-cam2.Sample.com (172.16.160.165):
(The 65532 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp      open        ftp
23/tcp      open        telnet
80/tcp      open        http
```

THE FOLLOWING SYSTEM TURNS OUT TO HAVE BEEN A HONEY-POT

```
Interesting ports on ultra.nulldevice.net (172.16.160.186):
Too many to even bother with until this is cleaned up.
(The 65483 ports scanned but not shown below are in state: closed)
Port       State       Service
1/tcp      open        tcpmux
11/tcp     open        systat
15/tcp     open        netstat
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
79/tcp     open        finger
80/tcp     open        http
110/tcp    open        pop-3
111/tcp    open        sunrpc
119/tcp    open        nntp
120/tcp    open        cfdptkt
139/tcp    open        netbios-ssn
143/tcp    open        imap2
389/tcp    open        ldap
443/tcp    open        https
444/tcp    open        snpp
515/tcp    open        printer
540/tcp    open        uucp
587/tcp    open        submission
635/tcp    open        unknown
898/tcp    open        unknown
1080/tcp   open        socks
1112/tcp   open        msql
1524/tcp   open        ingreslock
2000/tcp   open        callbook
3306/tcp   open        mysql
5222/tcp   open        unknown
5223/tcp   open        unknown
5269/tcp   open        unknown
5742/tcp   open        unknown
5987/tcp   open        unknown
6667/tcp   open        irc
7100/tcp   open        font-service
7997/tcp   open        unknown
8001/tcp   open        unknown
8080/tcp   open        http-proxy
8888/tcp   open        sun-answerbook
9119/tcp   open        unknown
12345/tcp  open        NetBus
12346/tcp  open        NetBus
20034/tcp  open        unknown
27442/tcp  open        unknown
27665/tcp  open        Trinoo_Master
31337/tcp  open        Elite
32771/tcp  open        sometimes-rpc5
```

Excerpt from the Reverse DNS Report for 172.16.160-191.0-254

172.16.160.252	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.160.253	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.160.254	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.160.255	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.0	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.1	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.2	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.3	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.4	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.5	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.6	www.12bpxyxy.cxm.161.195.208.xz-xyyy.xypx	< yxy zxz yxyxyvx >
172.16.161.7	**www.byxyyxmvxyyxyfxxyy.cxm**	172.21.1.254
172.16.161.8	**www.yycxzyxy.cxm**	208.45.228.7
172.16.161.9	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.10	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.11	**www.wxyxxzyxyxzcx.cxm**	172.21.1.254
172.16.161.12	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.13	**www.yxyxxbyxwz.cxm**	172.21.1.254
172.16.161.14	**www.yvccmy.xyg**	205.217.154.138
172.16.161.15	**www.byxckxyxby.cxm**	172.21.1.254
172.16.161.16	**www.xmpzy.cxm**	206.246.242.95
172.16.161.17	gxyyxc.ZXCyxyxx8.11.161.195.208.xz-xyyy.xypx	< yxy zxz yxyxyvx >
172.16.161.18	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.19	**www.yxxzybxxzy.cxm**	216.9.129.167
172.16.161.20	**www.xxmyxxyzy.cxm**	67.153.131.222
172.16.161.21	**www.cmcx.cxm**	208.187.160.206
172.16.161.22	**www.vxyxzxxcy.cxm**	172.21.1.254
172.16.161.23	**www.zxwzxfyxxmxy.cxm**	< yxy zxz yxyxyvx >
172.16.161.24	**www.yxzxyyxyx.cxm**	< yxy zxz yxyxyvx >
172.16.161.25	**www.vgcxmpxzxzzy.cxm**	< yxy zxz yxyxyvx >
172.16.161.26	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.27	**www.mxxzzmxyxzzx.xyg**	172.21.1.254
172.16.161.28	**www.yxyxxycxyxxyy.cxm**	216.206.7.230
172.16.161.29	**www.yxyzyxcz-11.xyg**	172.21.1.254
172.16.161.30	**www.xmpzy.cxm**	206.246.242.95
172.16.161.31	**www.mxygxzyxyy.cxm**	172.21.1.254
172.16.161.32	**www.yxyyxzg.cxm**	172.21.1.254
172.16.161.33	**www.cyxyzxyfxxyy-cx.cxm**	66.223.100.244
172.16.161.34	**www.cyxyxyxzyx.cxm**	172.21.1.254
172.16.161.35	**www.gxbxyxz.cxm**	199.44.153.100
172.16.161.36	**www.gxyyxcyyxppx.cxm**	172.21.1.250
172.16.161.37	**<zx yxvxyyx YZY yxypxzyx >**	
172.16.161.38	**www.xmpzy.cxm**	206.246.242.95

172.16.161.39	www.kyxzxyb.cxm	< yxy zxz yxyxyvx >
172.16.161.40	www.mxyxcyxpyxzzy.cxm	172.21.1.40
172.16.161.41	www.yxpxzzxzxwxzxyy.cxm	172.21.1.254
172.16.161.42	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.43	www.yxzbxzxzxyyxzzxy.cxm	172.21.1.254
172.16.161.44	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.45	www.xkzxybxzxy.cxm	172.21.1.254
172.16.161.46	www.mxyxzxyyxzzxqxxy.cxm	208.254.3.160
172.16.161.47	www.yxckxqxxpmxzz.cxm	172.21.1.254
172.16.161.48	www.vfy.zxz	172.21.1.222
172.16.161.49	www.cxwbxygxxy.cxm	172.21.1.254
172.16.161.50	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.51	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.52	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.53	www.gyxvzxz.cxm	212.159.9.131
172.16.161.54	www.ypyxxy-ypxczyxm.zx	< yxy zxz yxyxyvx >
172.16.161.55	www.z3ypxyzy.cxm	66.218.79.174 66.218.79.177 66.218.79.179 66.218.79.180 66.218.79.186 66.218.79.188 66.218.79.189 66.218.79.172
172.16.161.56	www.xcxyyyxczxy.cxm	172.21.1.254
172.16.161.57	www.xzzxvxxmxyzgxgx.cxm	216.218.213.149
172.16.161.58	www.jxffyzyxm.cxm	< yxy zxz yxyxyvx >
172.16.161.59	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.60	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.61	www.yxxyyx-yxgxzxy.cxm	172.21.1.254
172.16.161.62	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.63	www.gxyxzgxzx.cxm	172.21.1.254
172.16.161.64	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.65	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.66	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.67	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.68	www.xyxcyxyyxzg.cxm	172.21.1.254
172.16.161.69	<zx yxvxyyx YZY yxypxzyx >	
172.16.161.70	www.pxyfxymxzcx-yzxcky.cxm	< yxy zxz yxyxyvx >
172.16.161.71	www.cxyxwxyx.cxm	207.217.96.31 207.217.96.32 207.217.96.33 207.217.96.34 207.217.96.35 207.217.96.36 207.217.96.37 207.217.96.38

Excerpt from the Forward DNS Report for Sample.com

Detailed Forward DNS Report for zone Sample.com

5/17/2004, 7:53 AM, using the analysis setting "Normal"
==

Information

Serial number:656
Primary name server: ns.Sample.com.
Primary mail server: Sample.com.some-random.mail1.psmtp.com.
Number of records:409 (3 NS, 19 MX, 294 A, 92 CNAME, 0 PTR, 1 Other)

Errors for the zone Sample.com

- Non-authoritative data received from the server "auth03.ns.uu.net."
- The server "auth03.ns.uu.net." is listed as being authoritative for the domain, but it does not contain authoritative data for it.

- The name server "ns2.Sample.com." is not listed in delegation data. The server "ns2.Sample.com." is listed as being authoritative for the zone according to the zone data, but there is no NS record for that server in the delegation data. Delegation data and zone data should always match.

- Lame delegation received from "auth03.ns.uu.net." for "Sample.com."
- The server "auth03.ns.uu.net." is listed as being authoritative for "Sample.com.", but "auth03.ns.uu.net." does not contain authoritative data for the zone.

- Unable to resolve the host name "wind-en0.Sample.com." used in the CNAME record "mail-roam.Sample.com."
- It was not possible to resolve the host name "wind-en0.Sample.com." which is used in the CNAME record for "mail-roam.Sample.com." This indicates that a host with the name "wind-en0.Sample.com." does not exist.

- Unable to resolve the host name "sample.ispnews.com." used in the CNAME record "news-ispnews.Sample.com."
- It was not possible to resolve the host name "sample.ispnews.com." which is used in the CNAME record for "news-ispnews.Sample.com." This indicates that a host with the name "sample.ispnews.com." does not exist.

- Unable to resolve the host name "aa4re-1.Sample.com." used in the CNAME record "qb.Sample.com."
- It was not possible to resolve the host name "aa4re-1.Sample.com." which is used in the CNAME record for "qb.Sample.com.". This indicates that a host with the name "aa4re-1.Sample.com." does not exist.

• Unable to resolve the host name "mercury2.Sample.com." used in the CNAME record “wedgingt.Sample.com."
• It was not possible to resolve the host name "mercury2.Sample.com." which is used in the CNAME record for "wedgingt.Sample.com.” This indicates that a host with the name "mercury2.Sample.com." does not exist.
• (MISSING FINAL DOT?) • Unable to resolve the host name "87.int15.dsl.sample.net.Sample.com." used in the CNAME record "wilburc.Sample.com.". It was not possible to resolve the host name
• "87.int15.dsl.sample.net.Sample.com." which is used in the CNAME record for "wilburc.Sample.com.” This indicates that a host with the name "87.int15.dsl.sample.net.Sample.com." does not exist.
• An MX record for "dummy.Sample.com." refers to "mail-blue.Sample.com." which is a CNAME record • An MX record in the zone "dummy.Sample.com." refers to the mail server "mail-blue.Sample.com." The record "mail-blue.Sample.com." is a CNAME record, not an A record.
• An MX record for "quake.Sample.com." refers to "windmill.Sample.com." which is a CNAME record • An MX record in the zone "quake.Sample.com." refers to the mail server "windmill.Sample.com." The record "windmill.Sample.com." is a CNAME record, not an A record.
• An MX record for "sample.Sample.com." refers to "mail-yellow.Sample.com." which is a CNAME record An MX record in the zone "sample.Sample.com." refers to the mail server "mail-yellow.Sample.com." The record "mail-yellow.Sample.com." is a CNAME record, not an A record.
• An MX record for "hanna.Sample.com." refers to "mail-red.Sample.com." which is a CNAME record • An MX record in the zone "hanna.Sample.com." refers to the mail server "mail-red.Sample.com." The record "mail-red.Sample.com." is a CNAME record, not an A record.
• An MX record for "maillist.Sample.com." refers to "mail-yellow.Sample.com." which is a CNAME record An MX record in the zone "maillist.Sample.com." refers to the • mail server "mail-yellow.Sample.com." The record "mail-yellow.Sample.com." is a CNAME record, not an A record.
• An MX record for "mmc.Sample.com." refers to "mail-blue.Sample.com." which is a CNAME record An MX record in the zone "mmc.Sample.com." refers to the mail • server "mail-blue.Sample.com." The record "mail-blue.Sample.com." is a CNAME record, not an A record.

Excerpt from the DNS Scan Report for Sample.com

```
-------------------------------------------
Server:  [172.21.1.248]
Address:  172.21.1.248

Name:    my.Sample.com
Address:  172.21.1.248

-------------------------------------------
Server:  [172.21.1.249]
Address:  172.21.1.249

Name:    www2.gimme-da-bizness.bz
Address:  172.21.1.249

-------------------------------------------
Server:  [172.21.1.250]       Allowed Zone Transfers of base zone
Address:  172.21.1.250

Name:    www.sampleshoppe.com
Address:  172.21.1.250

-------------------------------------------
Server:  [172.21.1.251] Allowed Zone Transfers of base zone
Address:  172.21.1.251

Name:    www.changeintended.com
Address:  172.21.1.251

-------------------------------------------
Server:  [172.21.1.252]       Allowed Zone Transfers of base zone
Address:  172.21.1.252

Name:    www.thetompkinsfamily.com
Address:  172.21.1.252

-------------------------------------------
Server:  [172.21.1.253]
Address:  172.21.1.253

Name:    ftp-yellow.Sample.com
Address:  172.21.1.253

-------------------------------------------
Server:  [172.21.1.254]
Address:  172.21.1.254

Name:    namebase-yellow.Sample.com
Address:  172.21.1.254

-------------------------------------------
Server:  [172.21.4.33]
Address:  172.21.4.33
```

Excerpt from the full Nessus Vulnerability Report for Sample.com

ftp-yellow.Sample.com

Service	Severity	Description
daytime (13/tcp)	Info	Port is open
unknown (12/tcp)	Info	Port is open
smtp (25/tcp)	Info	Port is open
telnet (23/tcp)	Info	Port is open
http (80/tcp)	Info	Port is open
https (443/tcp)	Info	Port is open
mysql (3306/tcp)	Info	Port is open
ftp (21/tcp)	Info	Port is open
time (37/tcp)	Info	Port is open
domain (53/tcp)	Info	Port is open
ssh (22/tcp)	Info	Port is open
mysql (3306/tcp)	High	Your MySQL database is not password protected. Anyone can connect to it and do whatever he wants to access your data (deleting a database, adding bogus entries, ...) We could collect the list of databases installed on the remote host: Solution: Log into this host, and set a . SBHS. banderlog . bandwidthmeter . btfame . codeco . copelark . dlight . dtdisplays . eric4cp . eric4hi . eric4re . eric4web . sample-com

		password for the root user through the command 'mysqladmin -u root password <newpassword>' Read the MySQL manual (available on www.mysql.com) for details. In addition to this, it is not recommanded that you let your MySQL daemon listen to request from anywhere in the world. You should filter incoming connections to this port. Risk factor: High	. sample-photos . gurdeycounty . ib . countyfair . bass . meem . rotary . nitro . phplan . barnacle . printing . szzz . test . thenosuchfamily . webmessenger
http (80/tcp)	Low	This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by a plugin	
https (443/tcp)	Low	This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by a plugin	
general/icmp	Low	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. Solution: filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Risk factor: Low CVE: CAN-1999-0524	
daytime (13/tcp)	Low	The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port.	

		The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host. In addition to that, the UDP version of daytime is running, an attacker may link it to the echo port of a third party host using spoofing, thus creating a possible denial of service condition between this host and a third party. Solution: - Under Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry keys to 0: HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Then launch cmd.exe and type: net stop simptcp net start simptcp To restart the service. Risk factor: Low CVE: CVE-1999-0103