Statistical Analysis
of
Open E-mail Relaying on the Internet

Version 1.2
4/19/2002

Michael McCafferty
M5 Computer Security
Http://www.m5computersecurity.com

Background:

Once upon a time, the Internet was a much smaller and much friendlier place. Many services, such as FTP, and SMTP were rarely configured for security or to prevent abuse. The Internet, then called ARPANET was not the robust commercial network that it is today. Frequently to communicate between two points, a user would need to use services of other computers on the network.

In the case of E-mail, a user could log on to a computer on someone else's network where they did not have a mail box, create a message with a return address to themselves on another network where they did have a mail box. While the practice allowed users to forge mail to appear as if it came from someone other than himself or herself, it wasn't a major concern at the time. The users on the network were primarily academic and mostly concerned with cooperating and collaborating. The ability to relay messages through other systems supported that concern.

When the Internet exploded into common use, the phenomenon of Unsolicited Commercial E-mail (UCE), also called "Spam" began to fill Internet users' mailboxes. E-mail users were not particularly thrilled as the number of UCE messages in their mailboxes grew. Service Providers began to enact policies banning the practice of sending UCE from their network. However, the open, free, e-mail relays, which allowed anyone to forge, and send mail from remote networks allowed this spamming to continue.

The battle over UCE still rages, but one thing is certain; it is now considered a mis-configuration of your mail server to allow mail relaying from unspecified networks. Allowing unchecked, open mail relaying from unspecified networks contributes to the problem of Spam.

Additionally, "Black Lists" of servers which allow relaying, Service Providers which allow spam to originate from their networks, and entities which use spam to market their products have been created. Many mail server owners subscribe to these lists, and set their servers to automatically reject or delete messages that originate from those sources. Many times, legitimate messages, which originate from these sources are also rejected or deleted.

The risks of having an Open Mail Relay on your network may include:

1) Loss of business or communication due to customers not receiving mail sent from a commercial domain that is black listed.
2) Loss of reputation and trust by customers due to the perception that you can not control your network security.
3) Damage to reputation due to a malicious user forging mail from your domain or users from your domain.
4) Loss of Service as a result of your Service Provider disconnecting your connectivity as a result of complaints that you are sending Spam or are allowing Spam to originate from your domain.
5) Drawing the attention or rage of malicious anti-spammers, who may perpetrate an attack on your network or server.

Purpose:

To compile statistical information on the number of E-mail servers on the Internet which are configured to allow open relaying of messages.

Test #1 – Test of Two Contiguous DSL IP Ranges

Methodology:

Using a product called "Relay Sniper" (http://arkysoft.com/sniper/), we scanned a total of 22 Class C IP networks (5,630 addresses). The software attempts to send a message through remote mail servers. Immediately following this test, we scanned the same IP ranges to determine the number of hosts in the IP address ranges we tested, and to determine the number of hosts responding to TCP port 25. The SMTP protocol, which is used for sending e-mail, operates on TCP port 25. If a host has TCP port 25 open, it is considered a mail server, in this study.

The IP ranges we scanned were chosen because at least part of the ranges were DSL customer addresses, physically located in San Diego, CA. M5 Computer Security primarily markets our services to small businesses in San Diego County. These ranges seemed like as good a place to start as any. All scanning was performed from RoadRunner cable modem address space, which is totally unrelated to the addresses being tested.

The Results:

IP Range A:

208.57.10.0 - 208.57.20.255 (11 Class C's)

All of these networks are assigned to Mpower by IANA. Mpower is a DSL provider. 96 IP addresses of the 2815 total addresses are reserved for dialup connections. The remainder is for allocation to high-speed connections. These addresses serve customers in Southern California and Las Vegas Nevada.

Time for this scan	00:02:45
Total IP's Scanned	2815
Open Relays	6
Number of messages not delivered	1
Confirmed Open Relays	5
Blind Relays	0
Non-Relays	2809
Number of Hosts found	253
Number of hosts with TCP port 25 closed	234
Number of hosts with 25 filtered	5
Number hosts with 25 open	14
Successful Relays	5
% of hosts with 25/tcp open	5.53% (14 of 253)
% of hosts allowing relays	1.97% (5 of 253)
% of hosts with 25/tcp open allowing open relays	35.71% (5 of 14)

Relays Found:	Assigned to (anonymized):	Mail Server software	Black-listed?
208.57.x.x	DSL customer, Las Vegas NV	MERAK 2.10.260	Yes
208.57.x.x	DSL customer, San Diego CA	Microsoft Exchange 5.5	No
208.57.x.x	Industrial Radio Dist., El Segundo, CA	Microsoft Exchange 5.5	Yes
208.57.x.x	Forms mfr., El Monte CA	Netscape Mail Server v2.01	Yes
208.57.x.x	Undetermined	IMail 5.05 18710-1	Yes

IP Range B:

63.200.201.0 - 63.200.211.255 (11 class C's)
All of this range is assigned to Pacific Bell, by IANA. As best we can tell from WHOIS records, all of this address range is used for DSL and other high-speed connections in California.

Time for this scan	00:02:48
Total IP's Scanned	2815
Open Relays	10
Number of messages not delivered	4
Confirmed Open Relays	6
Blind Relays	0
Non-Relays	2805
Number of Hosts found	250
Number of hosts with TCP port 25 closed	209
Number of hosts with 25 filtered	15
Number hosts with 25 open	26
Successful Relays	10
% of hosts with 25/tcp open	10.4% (26 of 250)
% of hosts allowing relays	2.4% (6 of 250)
% of hosts with 25/tcp open allowing open relays	23.07% (6 of 26)

Relays Found:	Assigned to (anonymized):	Mail Server software	Black-listed?
63.200.x.x	Biotech Co., Carlsbad CA	Microsoft Exchange 5.0	Yes
63.200.x.x	Undisclosed, unknown CA	ArGoSoft Mail Server, Version 1.61	Yes
63.200.x.x	Undisclosed, unknown CA	GroupWise Internet Agent 5.5.4.1	No
63.200.x.x	Faux Tree mfr., CA	Microsoft Exchange 5.5	Yes
63.200.x.x	Individual, San Diego CA	Microsoft Exchange 5.5	Yes
63.200.x.x	Regional Bank, San Diego CA	Microsoft Exchange 5.5	No

Test #2 – Test of Randomly Selected Internet IP Addresses

Methodology:

We randomly scanned the Internet for hosts which responded to a "TCP Ping" on port 25, then determined if TCP port 25 was open, filtered, or closed. Once a list of systems was compiled, the list was scanned using "Relay Sniper" as in Test #1.

We used "Nmap" (http://www.insecure.org) to perform the random host discovery scan. The following command was used:

nmap -sT -iR -PT25 -p 25 >> Random-mail.txt

The scan was run until we had located 128 hosts with TCP port 25 open. A Perl script written by Mark Grimes (http://www.stateful.net/) was used to convert the Nmap output to a plain text list of IP addresses of the hosts which either had 25/tcp "filtered" or "open". The plain text list of IP addresses was then fed to "Relay Sniper".

All scanning was performed from RoadRunner cable modem address space, which is totally unrelated to the addresses being tested.

The Results:

IP Range C:

Random IP addresses

Time for this scan	Undetermined
Total IP's Scanned	Undetermined
Open Relays	2
Number of messages not delivered	0
Confirmed Open Relays	2
Blind Relays	0
Non-Relays	Undetermined
Number of Hosts found	517
Number of hosts with TCP port 25 closed	327
Number of hosts with 25 filtered	62
Number hosts with 25 open	128
Successful Relays	2
% of hosts with 25/tcp open	5.53% (128 of 517)
% of hosts allowing relays	0.39% (2 of 517)
% of hosts with 25/tcp open allowing open relays	1.56% (2 of 128)

Relays Found	**Assigned to:**	**Mail Server software**	**Black-listed?**
128.163.x.x	University of Kentucky	Undetermined	No
208.187.x.x	Broadcasting, Las Vegas NV	Sendmail 8.9.3/8.9.3	Yes

Conclusions:

The number of Open E-mail Relays on the Internet is high. It is easy to find and exploit large numbers of them in a relatively short amount of time. In one test, we found 10 open relays in less than 3 minutes. The number of systems found on the various Black Lists, or eligible to be placed on these lists is also high. As a result a large number of e-mail users may not be able to successfully send e-mail to other e-mail users if the recipients service provider subscribes to these black lists and uses them to reject or delete incoming mail.

There is a striking statistical difference between the randomly tested IP address group and the DSL groups. The random scan found just 1.56% of mail servers allowed open relaying, compared to 23.07% and 35.71% for the DSL networks tested. This tends to support the logical notion that DSL customers, who are perhaps more likely to be small businesses, may not have the training, experience, or resources to properly configure their mail servers. One must also conclude that some weight should be placed on outsourcing their e-mail services to those that specialize in or can prove proficiency in e-mail server support.

For more information on how to test the relaying configuration of your e-mail server, or performing a more comprehensive Information Security Assessment, please contact us at:

M5 Computer Security
http://www.m5computersecurity.com
info@m5computersecurity.com