Insider Tips: Critical Mailing Lists

Finding The Answer

Knowledge is power. In a networked environment, don't make the mistake of thinking you can do without it – the consequences could be disastrous. Loss of data may result in a loss of jobs, so it is worth taking the time to find the answers.

BY MARC ANDRÉ SELIG

Attackers, whether human or automated worms, are just waiting to take control. An effective defensive strategy needs up-to-date information. Good admins will derive that information from multiple sources.

Successful attacks on computers across the Internet are nearly always due to configuration errors, or known vulnerabilities. Zero day exploits, attacks based on security holes that are not public knowledge, are comparatively rare. This may be due to the fact that it takes a lot of skill and know-how to find and exploit a new vulnerability, whereas most attacks are carried out by automated tools, or more-or-less ignorant script kiddies.

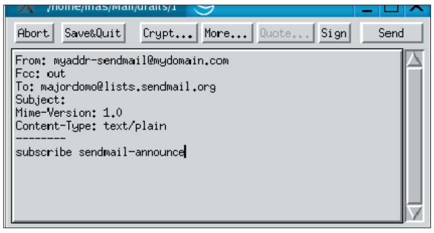
Diligence on the part of a well-trained admin will help you avoid configuration errors. Well-planned and timely updates are your best defense against known vulnerabilities (see box "Update Strategies"). Disabling a service may be your only option for want of a patch, although this depends on how important the vulnerable service is to your enterprise.

The most important thing is to react as quickly as possible. When an advisory is published, there is typically a slight lull before the the first wave of attackers and copycats hits home. This gives you an opportunity to think before you leap – be quick, but not too quick. The sooner you take note of an issue, the better your chances of patching the hole in a timely manner are.

Advisory Lists

Admins and developers started exchanging information a long time ago, and your Linux distributor's advisories are required reading. More or less every distributor uses a list to describe security issues and patches. Check out the table in the InSecurity News section in any issue of Linux Magazine for some important sources.

Manufacturers tend to withhold important information until they have completed work on a patch, the advantage being that admins can use automated tools to install the patch. This is where the Red Hat Network, *apt-get update; apt-get upgrade* for Debian, or Suse's YaST2 online update, to just name a few, can be a big help. Unfortunately,



```
From: myaddr-sendmail@mydomain.com
Fcc: out
To: majordomo@lists.sendmail.org
Subject:
Mime-Version: 1.0
Content-Type: text/plain
--------
subscribe sendmail-announce
```

Figure 1: Add a suffix to your own address when subscribing to a mailing list to allow you to automatically filter received messages later. Qmail sends *myaddr-List@Domain* to *myaddr@Domain* (*myaddr+List@Domain* for Sendmail).

Get the Picture with Procmail

The major issue with security mailing lists is separating really interesting facts from a huge amount of background noise, and doing so in a timely fashion. Spam and virus filters are your first obstacle. Messages describing vulnerabilities often include elements that are typically indicative of spam, such as exclamation marks, unusual formatting, unknown source addresses, and even executable code. Make sure that you whitelist the security lists you are interested in.

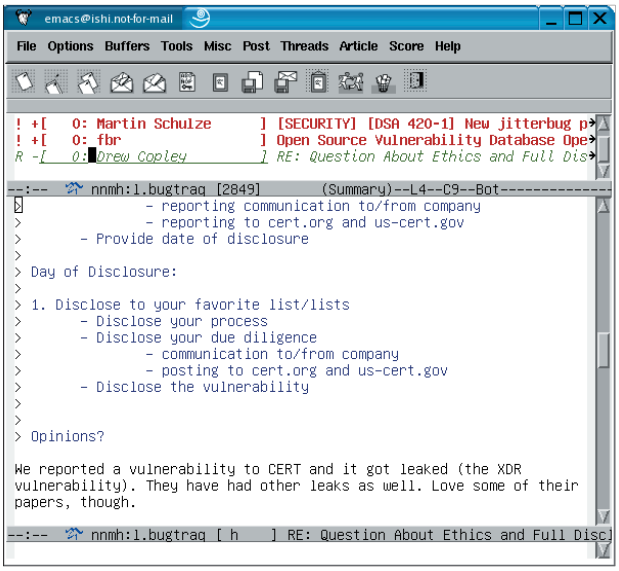
Another thing you might like to do is to store incoming security messages in separate folders to help you get a clear picture. The following Procmail recipe provides an example. Used as a prefix to a *~/.procmailrc* statement, this rule will store Bugtraq messages in *list/bugtraq*:

```
:0:
* ^List-Id:.*bugtraq\.list-
id\.securityfocus\.com
list/bugtraq
```

you can't afford to leave your critical computer systems hanging around for a week or two waiting for your distributor to come up with an appropriate patch for the vulnerability.

To avoid doing so, admins are well-advised to read the advisories for any mission-critical system programs they use. These will typically be services such as Sendmail [1], Postfix [2], Qmail [3], Apache [4], MySQL [5], or OpenLDAP [6]. Of course, this list would not be complete without SSH [7].

BSD systems were an important source for many Linux applications. Although the programs may be quite at home running on Linux, the code basis is still identical. Thus, security issues reported for OpenBSD [8], FreeBSD [9] or NetBSD [10] can be an early indicator of trouble brewing for Linux.


emacs@ishi.not-for-mail
File Options Buffers Tools Misc Post Threads Article Score Help

```
! +[   0: Martin Schulze        ] [SECURITY] [DSA 420-1] New jitterbug p
! +[   0: fbr                   ] Open Source Vulnerability Database Ope
R -[   0:Drew Copley            ] RE: Question About Ethics and Full Dis
--:--   nnmh:1.bugtraq [2849]        (Summary)--L4--C9--Bot-------------
>               - reporting communication to/from company
>               - reporting to cert.org and us-cert.gov
>       - Provide date of disclosure
>
> Day of Disclosure:
>
> 1. Disclose to your favorite list/lists
>       - Disclose your process
>       - Disclose your due diligence
>               - communication to/from company
>               - posting to cert.org and us-cert.gov
>       - Disclose the vulnerability
>
>
> Opinions?

We reported a vulnerability to CERT and it got leaked (the XDR
vulnerability). They have had other leaks as well. Love some of their
papers, though.
--:--   nnmh:1.bugtraq [ h    ] RE: Question About Ethics and Full Disc
```

Figure 2: The Gnus newsreader is an excellent tool for mailing lists with high traffic volumes, providing users with numerous rating and filtering features, including a practical killfile.

Bugtraq

Bugtraq [11] is, without any doubt, one of the most famous security mailing lists. Bugtraq provides a platform where hackers, crackers, and security experts can publicize new vulnerabilities long before they reach the version-specific lists referred to thus far. Many advisories contain working exploits.

Caution is advisable when using the Bugtraq list. For one thing, not all the code published here is harmless. Instead of an exploit, some advisories may contain Trojans or other miscellaneous malware. For another thing, Bugtraq is not merely an advisory list. Instead it is a platform for discussions on disclosed issues. Traffic volumes can be uncomfortably high. If security is not part of your core business, you might lose a lot of time dredging the lists for relevant information.

In any case, it makes sense to use a capable mail client to handle Bugtraq messages. The client should be capable of separating Bugtraq messages by subject, or preferably by thread, and it should have a working killfile to allow you to discard less interesting topics. Fortunately, Linux has a whole gamut of suitable programs. Refer to the box "Get the Picture with Procmail" for a Procmail rule that stores messages from a mailing list in a separate folder.

Bugtraq [11] hosts several interesting lists. Check out "Security Events", "Security Papers", and "Security Tools" as useful references.

CERT

Computer Emergency Response Teams (CERT) are one of the traditional mainstays of IT security information. For example, US-CERT publishes two technical lists [12] providing a kind of alert mechanism for particularly critical issues. Due to extensive quality assurance procedures, there is typically a considerable delay before publishing CERT messages. However, they can still perform a useful role, as your safety net. When a CERT message arrives, you know it is high time for a patch to be installed. ■

Update Strategies

Timely updates are important, but some updates can be downright dangerous. After all, it doesn't make much sense to plug a security hole on your Web server with a patch that takes your server down. Your staff and customers will lose access, and that means loss of revenue.

A two-stage process is your best option when updating critical systems. You should have identically configured backup systems for any really important machines on your server farm. One machine can handle mission critical tests while you are modifying the configuration on the other, prior to modifying the production system.

After updating a machine, you need to establish the effectiveness of those changes. To save time, you might like to use automatic or semi-automatic regression tests, which can check off a list of critical jobs in the shortest possible time. Remember to test other critical services that interact with the modified service, and not only the parts you have changed. For example, you could tell your Web server to connect to your database or credit card billing system.

Make sure that the backup machine is performing to your satisfaction, and without any unpleasant side effects, before deploying the changes on your production machine. This whole process should not take up too much of your valuable time, but it does provide you with a safety net.

INFO

[1] Sendmail announcement list: *mailto:majordomo@lists.sendmail.org*

[2] Postfix announcement list: *mailto:majordomo@postfix.org*

[3] Qmail advisory list: *mailto:qmailannounce-subscribe@list.cr.yp.to*

[4] Apache news: *http://httpd.apache.org/lists.html#http-announce*

[5] MySQL lists: *http://lists.mysql.com/announce/*

[6] OpenLDAP news: *OpenLDAP-announce-request@OpenLDAP.org*

[7] OpenSSH: *http://www.mindrot.org/mailman/listinfo/openssh-unix-announce*

[8] OpenBSD: *http://lists.openbsd.org/cgi-bin/mj_wwwusr?func=lists-long-full&extra=security-announce*

[9] FreeBSD: *http://lists.freebsd.org/mailman/listinfo/freebsd-security-notifications*

[10] NetBSD: *http://www.netbsd.org/MailingLists/#netbsd-announce*

[11] Bugtraq: *http://www.securityfocus.com/subscribe?listname=1*

[12] US-CERT National Cyber Alert System: *http://www.us-cert.gov/cas/signup.html*