The sys admin's daily grind: P3Scan

VIRUS-FREE

Checking email for viruses is typically the domain of the SMTP gateway or a server directly downstream of it. In this month's column, Charly decides to move this protection to the other side – that is, to the client connections with their SMTP and POP servers. **BY CHARLY KÜHNAST**

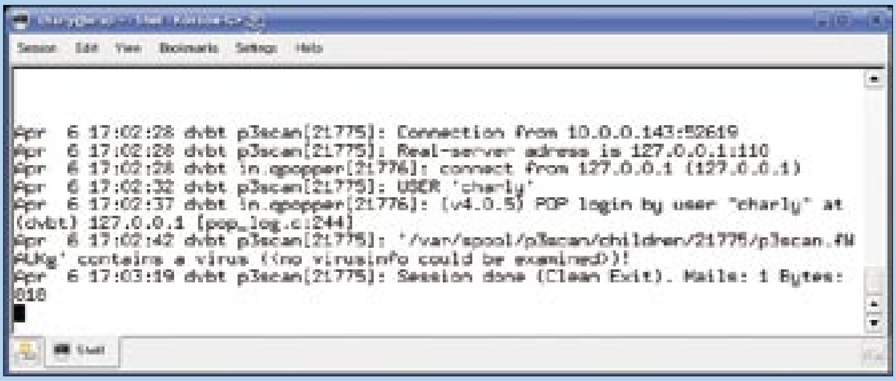
P3Scan [1] is a mail proxy that sets up shop in front of the SMTP and POP3 daemons and accepts connections from clients wanting to pick up, or get rid of, mail. It forwards client commands and checks emails for malevolent content before passing them on. P3Scan avoids exotic dependencies and just relies on the *pcre-devel* library, which most distributions are likely to have anyway.

Of course, P3Scan must rely on antivirus software. I chose ClamAV, but P3Scan will also work with F-Prot, F-Secure, Kaspersky, and probably other products, as long as they have a command-line client. P3Scan can also integrate SpamAssassin and DSPAM, giving it the ability to remove unsolicited advertising from mail.

Iptables gives admins the ability to use P3Scan as a transparent mail proxy. Users remain blissfully unaware of the program's existence, at least as long as incoming mail is clean. You could easily set up P3Scan on a Linux router. I run P3Scan on an unprivileged port – the default is 8110 – using iptables to send all POP3 connections to the required port:

```
iptables -t nat -I ➥
PREROUTING ! -i eth0 ➥
-p tcp -s 192.168.1.0/24 ➥
--dport 110 -j REDIRECT➥
--to-ports 8110
```

After doing this, P3Scan will accept POP3 connections, passing all POP commands – such as RETR, DELE, etc. – to the target server and fetching legitimate emails from the server. It will also feed mail through the virus scanner and, if needed, the spam filter.



```
Apr  6 17:02:28 dvbt p3scan[21775]: Connection from 10.0.0.143:52619
Apr  6 17:02:28 dvbt p3scan[21775]: Real-server adress is 127.0.0.1:110
Apr  6 17:02:28 dvbt in.qpopper[21776]: connect from 127.0.0.1 (127.0.0.1)
Apr  6 17:02:32 dvbt p3scan[21775]: USER 'charly'
Apr  6 17:02:37 dvbt in.qpopper[21776]: (v4.0.5) POP login by user "charly" at
(dvbt) 127.0.0.1 [pop_log.c:244]
Apr  6 17:02:42 dvbt p3scan[21775]: '/var/spool/p3scan/children/21775/p3scan.fW
ALKg' contains a virus (<no virusinfo could be examined>)!
Apr  6 17:03:19 dvbt p3scan[21775]: Session done (Clean Exit). Mails: 1 Bytes:
818
```

Figure 1: P3Scan protocol for an incoming mail. Luckily, this one is virus-free.

Configuration

P3Scan is controlled by the */etc/p3scan/p3scan.conf* file. The following entries are critical:

targetip: If you will be using P3Scan as a transparent proxy, you must enter *0.0.0.0*. If not, enter the IP address of the "real" server to which P3Scan will be forwarding client connections.

bytesfree = <byte>: You need at least *bytes* of free disk space; otherwise, P3Scan will quit. Note that the program forks a number of child processes (default: 10); in the worst case, all of them might need to handle large mail attachments at the same time.

scanner = <command>: Enter the command that launches your virus scanner here. Because I use ClamAV, my command line looks like this:

```
scanner = /usr/bin/clamdscan➥
--no-summary
```

viruscode =: P3Scan evaluates the return code from the virus scanner to determine whether the mail is infected or clean. Typically, the scanner will return a value of 0 if the message is clean, and 1 if it finds a virus. Some scanners use additional return codes. To tell P3Scan to evaluate these codes, you need to add a line to the file. If the scanner returns a value of 1, 5, or 13 for "Virus detected!", the line would be *viruscode = 1,5,13*. The same principle applies to return codes other than 0 that indicate "No virus detected!". The line would then start with *goodcode =*.

overwrite = /usr/bin/p3pmail: This line eliminates HTML inside emails. It prevents clients from autonomously loading images or the like while reading mail. This would be dangerous and also let the spammer know that the message had arrived and been opened. ■

INFO

[1] P3Scan: *http://p3scan.sourceforge.net*

THE AUTHOR

Charly Kühnast is a Unix System Manager at the data center in Moers, near Germany's famous River Rhine. His tasks include ensuring firewall security and availability and taking care of the DMZ (demilitarized zone).

SYSADMIN