USING POP WITH PROXY

Generally we (the paranoid people) like to disable POP3 access to external sites due to its easily abused nature and setup, but sometimes we just have no choice. For those times it is immensely useful to implement a proxy to help secure it, and a transparent proxy is even better so as not to require changes to the client-side machines. This is where *p3scan* steps in. Small, easy and free - who can ask for more?

Needed?
A linux box, a firewall to do address translation (like *iptables*), *clamav*, *spamassassin* is useful and of course *p3scan*. Once you have downloaded *p3scan* (I am using the development version) you go through the usual 3 step linux installation dance..

```
./configure -disable ripmime ; make ; make install
```

Configuration?
P3scan can be used with a good couple of virus scanners and can also use *dspam* for spam checking. I will be focusing on *spamassassin* and *clamav* as they are probably the most widespread of the choices. You need to edit the */etc/p3scan/p3scan.conf* file, I change/enable the following settings..

```
checkspam = /usr/bin/spamc
debug
debug-scanning
footer = /usr/bin/clamdscan -V
logopt = 3
logfac = 24
```

Now you can start it upon machine start by using a full sysint script or */etc/rc.d/rc.local*. I'll go with the lazy option, so edit */etc/rc.d/rc.local*..

```
nohup /usr/bin/p3scan 2>/var/log/p3scan.debug &
```

Now after *rc.local* is run, you should see a listening port at 8110.

Transparency?
This is where the firewall rules come in. The firewall must redirect all POP3 traffic to the server with *p3scan* listening at 8110. So assuming *p3scan* and the firewall were both on the same linux box your rules would look something like..

```
iptables -A OUTPUT -s <$FWIP> -p tcp -m tcp --dport 110 -o <$EXT> -j ACCEPT
iptables -t nat -A OUTPUT -s <$FWIP> -p tcp -m tcp --dport 110 -o <$EXT> -j ACCEPT
iptables -t nat -A PREROUTING -s <$LANIP> -i <$LAN> -m tcp -p tcp --dport 110 -j DNAT
--to-dest <$FWIP>:8110
iptables -t nat -A PREROUTING -s <$LANIP> -i <$LAN> -d <$FWIP> -m tcp -p tcp --dport
8110 -j ACCEPT
iptables -A INPUT -s <$LANIP> -d <$FWIP> -p tcp -m tcp --dport 8110 -j ACCEPT
```

Now all POP3 traffic traversing the firewall will be transparently redirected to the *p3scan* server.

Final Words
It really is simple to get this program going, and it is very useful. It has all sorts of other features to play with - footers, blacklists, whitelists, SMTP proxying, etc. It is well worth playing around and tweaking. Also remember that a proxy might not solve all the woes of using a protocol like POP3 but it does help. As always have fun and learn.