Fighting Spam with pf
Introducing

• Dan Langille

• http://langille.org/

• http://www.freebsd-diary.org/pf.php
What is spam?
Warning
Where does spam come from?

- open relays
- spam bots
- “friends” and family
- people on your mailing lists
spam networks

- compromised machines
- open relays (not so much any more)
- massive volume
- ignore errors, get the mail through!

![Diagram of centralized, decentralized, and distributed networks]
The Perfect Solution

- requires no changes to your existing mail server
- reduces load on virus scanners and mail servers
- MTA agnostic
What is pf

• pf is a packet filter produced by the OpenBSD project
• spamd also from OpenBSD
• ported
• damn fine product
• use it if you can
• highly recommended
• Absolute OpenBSD – Michael W. Lucas
pf

- tables
- reloaded programatically
- macros
- simple and powerful rules
- stateful
A Packet Filter?

WTF?
Spammers are lazy

- maximum return
- minimum effort
- queues?
- volume
Connection Profiling

- whitelist – good
- blacklist – bad
- greylist - undecided
greylisting

- exploit the protocol
- If you're not on the blacklist or the whitelist, you are unknown
- hence, greylist
- prove yourself
- move
- tuple
smtp is a simple protocol

- text based protocol
- you can type commands by hand via telnet
- for example...
Simplified SMTP conversation

Hi, I'm Ed

I have a message from Dan Langille

It's for Jordan Hubbard

here it is

Eh? I'll come back later.
temporary errors

- defined in RFC
- sending server must re-queue and retry
- disk space
- network problems
- etc
Logical

- not to scale
- not all paths shown

sender → pf → spamd
pf → your MTA[s]

greylist → pf → blacklist → whitelist

Fighting Spam with pf

LISA'08
pf directives

table <spamd> persist

table <spamd-white> persist

table <spamd-mywhite> persist file "/usr/local/etc/spamd-mywhite"
pf directives (2)

MYSELF="64.147.113.42"

# redirect to spamd
rdr pass inet proto tcp from <spamd-mywhite> to $MYSELF port smtp -> 127.0.0.1 port smtp
rdr pass inet proto tcp from <spamd> to $MYSELF port smtp -> 127.0.0.1 port spamd
rdr pass inet proto tcp from ![spamd-white] to $MYSELF port smtp -> 127.0.0.1 port spamd
spamd

- daemon
- AKA tarpit
- very small footprint
- easy on resources
- handles a large volume of connections
- Runs on OpenBSD, FreeBSD, NetBSD, and DragonflyBSD
spamdb

- database
- list of entries known to pf
- unique tuples (src IP, sender email, receiver email, ?)
- GREY
- TRAP
- TRAPPED
grey scanning

- First connection causes a retry
- During the retry, scan the logs
- bad addresses
- bad domains
- multiple emails
- make up whatever you want
trapping

• honeypot addresses
• old addresses
• message-ids
OK, not so perfect

- some claim it is not RFC compliant
- some claim it unreasonably delays email
- some claim false positives
- some claim it breaks other anti-spam measures
- http://nolisting.org/
- My claims?
$ grep pf /etc/rc.conf
pf_enable="YES"
pflog_enable="YES"
obspamd_enable="YES"
obspamd_flags="-v -n 'Postfix - Special Edition'"
obspamlogd_enable="YES"
Finish

http://www.freebsd-diary.org/pf.php