SMTP Psychosis

TEFLONRABBIT ARTICLE No.182

Unique Identifier:912784f5-5f1e-4f98-946c-d630cdf87acc


SPAM!

Spam is in the eye of ....

Thursday, January 6, 2005 - 11:21

PDF Version
Aroma
Image not found or type unknown
20
Rumness
Image not found or type unknown
30
Subscription Only
Off
SMTP *Email* *Spammers*

Maintaining an smtp server, no zen here. Despite daily updates of the banned IP list, my fresh new Mercury install was being mercilessly pillaged by some outrageous smtp hunter daemons hosted by a group most likely hiding behind a compromised mail server at http://www.daum.net So, some more banning of the majority of the eastern pacific rim IP blocks, and mod'ing the firewall to cut them at source (prior to their entry into the dmz). This still left the cold hard truth that what started as a straight forward exercise in networking, turned into a heinous nightmare starring the mailer version of Godzilla. Time for a slightly different approach, enter the honeypot : Took the host offline, uninstalled the server, replaced it with an attractive sacrificial lamb which appeared open on all the favourite ports and simply moved the server to a new host on radically different ports. It's been a month now, and not one single unsolicited connection has made it through to the mail server, meanwhile the honeypot continues to log attempts by these utter miscreants, and my users have unfettered email harmony. (Touch wood)