Subject: Confused with log...
Posted by miffee79 on Sun, 29 Oct 2006 11:12:54 GMT
View Forum Message <> Reply to Message

Hi All :)

Hoping you can help. I was looking at my log this morning and there is a lot of this:

Oct 29, 2006, 11:03:51 Session 0: Connection from xxx.xxx.xx.xxx accepted on ***.***.***.***:25
Oct 29, 2006, 11:03:51 Session 0: 220 mail.xxxxx.com
Oct 29, 2006, 11:04:00 Session 0: EHLO computer-9ccogs
Oct 29, 2006, 11:04:00 Session 0: 250-DSVR000915 Hello [217.174.249.81]
Oct 29, 2006, 11:04:00 Session 0: 250-SIZE 52428800
Oct 29, 2006, 11:04:00 Session 0: 250-AUTH LOGIN CRAM-MD5
Oct 29, 2006, 11:04:00 Session 0: 250 OK

Can anyone tell me if this is good or bad?

Cheers,

Matt

Post Edited (10-29-06 12:13)

Subject: Re: Confused with log...
Posted by Heidner on Sun, 29 Oct 2006 19:52:12 GMT
View Forum Message <> Reply to Message

That is a normal negotiation sequence for starting up a mail session.

I presume the ***.*** and the xxx.xxx are your changes.

Subject: Re: Confused with log...
Posted by miffee79 on Sun, 29 Oct 2006 19:57:42 GMT
View Forum Message <> Reply to Message

Hello :)

Thank you for your reply. Yes, they are my changes. The only reason I asked was because NST normally gets about 1500 emails a day and yesterday it got 6900 and only 63 were not spam, the rest were rejected as expected. It threw me a bit.

Thanks again :)

Matt

Subject: Re: Confused with log...
Posted by Heidner on Tue, 31 Oct 2006 06:36:51 GMT
View Forum Message <> Reply to Message

Occassionaly you'll see some really nasty spikes. I normally only see four or five hundred e-mails a day... but I also have seen spikes where it jumps up to seven or eight times the normal. When I see that happening - if I can see a pattern on the ip addresses - I just null route the whole IP block to cut down the noise. This time of the year it is tends to be much higher...

Subject: Re: Confused with log...
Posted by iyuvalk on Wed, 01 Nov 2006 14:35:05 GMT
View Forum Message <> Reply to Message

Hi,

Sometimes you'll see this because spammers occassionaly try to refresh their e-mail addresses by sending the spam to a@yourdomain, b@yourdomain, c@yourdomain etc.
We get that from time to time, what I usually do with this is to search the NST log for rejected email addresses that I could use as honeypot addresses and refresh my honeypot addresses list.

Hope that was a bit helpful for you,

Yuval.
