

## strange msg lines..

**Source:** <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2005-11/1837.html>

---

**From:** Ian Smith ([smithi\\_at\\_nimnet.asn.au](mailto:smithi_at_nimnet.asn.au))

**Date:** 11/17/05

Date: Fri, 18 Nov 2005 05:01:49 +1100 (EST)

To: dick hoogendijk <[dick@nagual.st](mailto:dick@nagual.st)>

Re: freebsd-questions Digest, Vol 113, Issue 12

> *Message: 28*

> *Date: Wed, 16 Nov 2005 23:56:06 +0100*

> *From: dick hoogendijk <[dick@nagual.st](mailto:dick@nagual.st)>*

> *I get a lot of these rules in my log file lately. Don't know why they*

> *are not logged in the error.log file. And if they are harmful or not.*

>

> =====

> 83.30.48.99 -- [16/Nov/2005:23:44:18 +0100] "GET / HTTP/1.1" 200

> 1860 "<http://puttane-grandi-tette.com>" "Mozilla/4.0 (compatible; MSIE

> 6.0b; Windows NT 5.0; .NET CLR 1.0.2914)"

> 85.106.229.37 -- [16/Nov/2005:23:44:24 +0100] "GET / HTTP/1.1" 200

> 1860 "<http://hosting-siti-adulti.com>" "Mozilla/4.0 (compatible; MSIE

> 6.0b; Windows NT 5.0; .NET CLR 1.0.2914)"

[.. etc ..]

I've seen Dinesh's reply, and your later response, but I've seen batches of these at various times too, and think it's something other than DNS (though it did look like maybe a test of a distributed fetch, many IPs)

> *These are not normal requests to my apache server. But it seems to*

> *"listen" to them. Am I 'in danger?'*

No, they're not errors, they're just requests for your home page (GET /) which is presumably 1860 bytes .. the Referer (sic) in each case is one of these apparent porn sites, but could easily be forged – it's unlikely that the pages at the URLs given do in fact have any link to your site; more than likely they want you go check out their stuff looking for one!

So there's no danger involved, unless there are enough of them to DoS your server. I tend to deal with such as these by blocking them in `apache|httpd.conf` so they just get a 403 access denied response, eg:

```
# 1/3/5 multiple browsers, multiple IPs, all the same referrer:
```

freebsd-questions: strange msg lines..

```
SetEnvIfNoCase Referer buy-vicodin-online\.us go_away
```

or in this other case, various different GETs attempting to access various porn URLs as wannabe proxy requests, all from the one IP:

```
# 6/10/5 porn link referers regularly, different browsers ..  
SetEnvIf Remote_Addr 209\.172\.35\.44 go_away
```

In your case, the browser identification, most likely bogus, is a common factor in each, and could be blocked with such as:

```
BrowserMatch "Mozilla/4\.0 \(\compatible; MSIE 6\.0b; Windows NT 5\.0; \.NET CLR 1\.0\.2914\)" go_away
```

or some unique part of that string. whereas others as above will cycle through different browser strings – there's usually some common thread to such bot-made requests. I only hit on them when they become annoying (but sometimes I'm easily annoyed :)

Then of course you'd need something along the lines of:

```
<Directory "/usr/local/www/data">  
[. other stuff ..]  
# 18Mar02 – allow only this file to otherwise denied bots  
<Files "robots.txt">  
  order allow,deny  
  allow from all  
</Files>  
order allow,deny  
allow from all  
deny from env=go_away  
</Directory>
```

Cheers, Ian

---

freebsd-questions@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@freebsd.org"