

RE: blocking IPs for FTP server

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-01/0404.html>

From: Rob Stevens (rob@linuxgawd.com)

Date: 01/24/03

From: "Rob Stevens" <rob@linuxgawd.com>

To: "Ng, Edward B" <edward.ng@eds.com>

Date: Thu, 23 Jan 2003 20:44:40 -0500

With Port Sentry you can use the Advanced Stealth Scan Detection. With that it scans ports below your specified "ADVANCED_PORTS" (commonly port 1024).

While having Port Sentry running it will watch for suspicious traffic from any outside connection. You can select the number of connection attempts from one IP before the alarm is triggered.

For example if an IP connects to ProFTPD more then twice in a row, and you have your SCAN_TRIGGER value set to 2 an alarm will go off (typically dropping the route). SCAN_TRIGGER is applicable to any port on the server, meaning if they are trying your SMTPd, IMAPd or any other service you are running Port Sentry will drop their route to your box.

-----Original Message-----

From: Ng, Edward B [<mailto:edward.ng@eds.com>]

Sent: January 23, 2003 7:52 PM

To: 'Rob Stevens'

Cc: 'security-basics@securityfocus.com'

Subject: RE: blocking IPs for FTP server

Hi Rob,

Thanks for the suggestions,

I am using RH 7.2 and ProFTP 1.25 . I have considered using Portsentry.

However, won't it detect legitimate users as intruders? All my users have usernames and passwords, however I do have a virtual server on one IP which has anonymous access. But the people who have been hammering me literally try all the IPs that the server is visible on and can sometimes end up holding too many open connections. I have recently restricted the server to a max of 3 open connections per host (which has helped!), but I feel that it would be nice if I can find a way to detect that someone has been trying so often that he can't be a legitimate user and then ban him for a while. In fact, lately some of these guys have been trying on my IMAP and SMTP ports also. I actually have qmail running and have webmail capability, so these guys know I have a live server, but they seem to be trying a form of brute force guessing game to try to get in.

SecurityFocus BASICS: RE: blocking IPs for FTP server

-----Original Message-----

From: Rob Stevens [mailto:rob@linuxgawd.com]
Sent: Friday, 24 January 2003 4:54 AM
To: Ng, Edward B
Subject: RE: blocking IPs for FTP server

Edward,

What distrobution are you using on the FTP server? You may want to use portsentry and setup a cronjob to flush the IP addresses once a day or something like that.

-----Original Message-----

From: Ng, Edward B [mailto:edward.ng@eds.com]
Sent: January 19, 2003 11:57 PM
To: security-basics@securityfocus.com
Subject: blocking IPs for FTP server

Hi Folks,

I run an FTP server on a public Linux box which is visible on the internet. For the last few months, I have had "visitors" who basically attempt to open multiple connections to the FTP server, and repeatedly try to login as anonymous. I have ignored this till now, but lately the FTP server has been shutting itself down because of too many simultaneous connections happening at the same time by these anonymous attempts. I was wondering is there an application out there which can do a temporary block on the IP of someone who has tried to login to FTP too many times and failed? I am currently running an iptables firewall, but I do not want IPs to be permanently blocked, just say blocked for 24 hours and then allowed again.

```
Jan 12 14:36:21 warp proftpd[5073]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) - FTP session opened.
Jan 12 14:36:22 warp proftpd[5074]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) - FTP session opened.
Jan 12 14:36:22 warp proftpd[5072]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) - no such user 'anonymous'
Jan 12 14:36:22 warp proftpd[5075]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) - FTP session opened.
Jan 12 14:36:22 warp proftpd[5073]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) - no such user 'anonymous'
Jan 12 14:36:22 warp proftpd[5072]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) - FTP session closed.
Jan 12 14:36:22 warp proftpd[5074]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) - no such user 'anonymous'
Jan 12 14:36:22 warp proftpd[5073]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) - FTP session closed.
Jan 12 14:36:22 warp proftpd[5074]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) - FTP session closed.
Jan 12 14:36:22 warp proftpd[5075]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) - no such user 'anonymous'
Jan 12 14:36:22 warp proftpd[5076]: warp.linux-server.com
```

RE: blocking IPs for FTP server

SecurityFocus BASICS: RE: blocking IPs for FTP server

(dclient217-162-35-70.hispeed.ch[217.162.35.70]) – FTP session opened.
Jan 12 14:36:22 warp proftpd[5077]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) – FTP session opened.
Jan 12 14:36:22 warp proftpd[5078]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) – FTP session opened.
Jan 12 14:36:22 warp proftpd[5079]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) – FTP session opened.
Jan 12 14:36:22 warp proftpd[5075]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) – FTP session closed.
Jan 12 14:36:22 warp proftpd[5080]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) – FTP session opened.
Jan 12 14:36:22 warp proftpd[5081]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) – FTP session opened.
Jan 12 14:36:22 warp proftpd[5083]: warp.linux-server.com
(dclient217-162-35-70.hispeed.ch[217.162.35.70]) – FTP session opened.

regards

Edward Ng

EDS Australia Pty. Ltd.
email : edward.ng@eds.com