

## Re: Need urgent help regarding security

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-11/0022.html>

---

*ray\_at\_redshift.com*

**Date:** 11/17/05

Date: Wed, 16 Nov 2005 17:48:38 -0800

To: Mark Jayson Alvarez <jay2xra@yahoo.com>, freebsd-security@freebsd.org

At 05:25 PM 11/16/2005 -0800, Mark Jayson Alvarez wrote:

| Good Day!

|  
| I think we have a serious problem. One of our old  
| server running FreeBSD 4.9 have been compromised and  
| is now connected to an ircd server..  
| 195.204.1.132.6667 ESTABLISHED

|  
| However, we still haven't brought the server down in  
| an attempt to track the intruder down. Right now we  
| are clueless as to what we need to do..

| Most of our servers are running legacy operating  
| systems(old versions mostly freebsd) Also, that  
| particular server is running – ProFTPD Version 1.2.4  
| which someone have suggested to have a known  
| vulnerability..

|  
| I really need all the help I can get as the  
| administration of those servers where just transferred  
| to us by former admins. The server is used for ftp.

|  
| Thanks..

Hi Mark,

Good luck tracking them. The IP# is out of Canada if that helps any.

195.204.1.132 CA CANADA ONTARIO WAWA UNDERNET-IRC

Looks like it is coming from another IRC network – although I am no IRC expert. Someone is probably using your machine to exchange software or run a bot network or something along those lines. Who knows.

Try doing a ps -aux and see if something like eggdrop or some IRC bot is running on there (assuming you still have the root password). You might even be able to figure out if you are hosting an IRC room :-). Maybe everyone from the FreeBSD hacker list can meet there and party :-). Just kidding.

## FreeBSD–Security: Re: Need urgent help regarding security

Anyway, tracking them is probably a waste of time, unless some valuable corporate information has been stolen. The best bet is to just wipe the machine and start over, unless you need something on there that you can't backup, etc. In cases like these, unless you are running something that has built check sums of all your system files, it's difficult to work back wards and know for sure you have returned everything back to a secure status. Best just to start at square 1 and work forward.

In the future, you might consider running a fire wall, such as ipf – or putting the server on a non–public IP# behind a router that acts as a fire wall – then only allow traffic in (and out) on ports you really need. If you run ipf, you might also block out going traffic on ports such as 21, 6666–6669, etc. so that anything that does get into the machine can't "phone home".

If your root password has been changed on you, you'll need to boot into single user mode and change the password back. You might also check files like /etc/rc.local or the like to see if something is setup to auto load at boot, such as an IRC server, or IRC bot, etc.

Anyway, just some ideas off hand.

good luck!

Ray

---

freebsd–security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd–security>

To unsubscribe, send any mail to "freebsd–security–unsubscribe@freebsd.org"