## Asterisk and Hackers

As soon as you put an Asterisk server online, it will be targeted by hackers attempting to use it for placing long distance calls at your expense.

There are a number of things you need to do to prevent this.

The first is to install fail2ban and configure it to prevent attempts to SSH into your server.

**apt-get install fail2ban.**

By default, it is already set up to prevent attacks to gain root access to your box via SSH. You might want to limit the number of tries to 3 as the default is 6.

Note: In debian, you must **cp /etc/fail2ban/jail.conf** to **jail.local** and make any changes in the jail.local file. This is to prevent any updates for fail2ban from wiping out any custom settings you might have made in jail.conf.

Then you need to set **allowguest=no** in the sip.conf and iax.conf files under **[general].** This prevents users from just connecting to your server with a client and sending phone calls.

Then you need to try to block users who guess at extension numbers and their secret passwords.

I found this on the fail2ban wiki:

http://www.fail2ban.org/wiki/index.php/Asterisk

It would appear that most current versions of Asterisk, IE 1.8 or 11.8, now have a security log.

First the security log needs to be enabled in /etc/asterisk/logger.conf:

**messages => security, notice,warning,error**

Then add this stanza to the fail2ban jail.local file: I added it under the two existing Asterisk tcp and udp stanzas. Don't forget to change the **enabled=false** to **enabled=true** for the asterisk-tcp and asterisk udp stanzas.

**[asterisk-iptables]**
**# if more than 4 attempts are made within 6 hours, ban for 24 hours**
**enabled = true**
**filter = asterisk**
**action = iptables-allports[name=ASTERISK, protocol=all]**
**sendmail[name=ASTERISK, dest=you@yourmail.co.uk, sender=fail2ban@local.local]**
**logpath = /var/log/asterisk/messages**
**maxretry = 4**

**findtime = 21600**
**bantime = 86400**

Change the e-mail address to a local user if you do not have Exim configured to deliver mail to the Internet.

When done, it should look like this:

[asterisk-tcp]

enabled  = true
filter   = asterisk
port     = 5060,5061
protocol = tcp
logpath  = /var/log/asterisk/messages

[asterisk-udp]

enabled  = true
filter   = asterisk
port     = 5060,5061
protocol = udp
logpath  = /var/log/asterisk/messages

[asterisk-iptables]
# if more than 4 attempts are made within 6 hours, ban for 24 hours
enabled  = true
filter   = asterisk
action   = iptables-allports[name=ASTERISK, protocol=all]
           sendmail[name=ASTERISK, dest=george@localhost, sender=fail2ban@local.local]
logpath  = /var/log/asterisk/messages
maxretry = 4
findtime = 21600
bantime = 86400

Most of the other settings they mentioned are set that way by default.

Restart fail2ban with **/etc/init.d/fail2ban restart** to make the configuration changes effective.. Don't forget to run **logger reload** from the Asterisk **CLI** to make the change to security logging effective.

Once everything is restarted, it should work.

Within a short while I started getting mail like this which shows it is working:

From fail2ban@local.local Fri May 09 00:26:03 2014
Return-path: <fail2ban@local.local>
Envelope-to: george@localhost
Delivery-date: Fri, 09 May 2014 00:26:03 -0700
Received: from root by debian.Home with local (Exim 4.82)
	(envelope-from <fail2ban@local.local>)
	id 1WifBz-0006OZ-9I
	for george@localhost; Fri, 09 May 2014 00:26:03 -0700
Subject: [Fail2Ban] ASTERISK: banned 37.8.83.122 from debian
Date: Fri, 09 May 2014 07:26:03 +0000
From: Fail2Ban <fail2ban@local.local>
To: george@localhost
Message-Id: <E1WifBz-0006OZ-9I@debian.Home>
Status: RO

Hi,

The IP 37.8.83.122 has just been banned by Fail2Ban after
16 attempts against ASTERISK.

Regards,

Fail2Ban