Setting up Tripwire with SSMTP

This document is best read printed out on paper.

1 Overview

Tripwire is intrusion detection software for GNU Linux & BSD. Let's document how to set it up on a server with SSMTP configured for email notifications.

2 Steps

2.1 Configuring Tripwire

First install Tripwire. This will depend on your package manager. The two examples I have will be either Gentoo, or Debian/Devuan.

```
apt-get install tripwire mailutils ssmtp
OR
emerge -av tripwire mailutils ssmtp
```

2.1.1 Devuan/Debian

Devuan will prompt you for a few things in an ncurses gui. Answer all of the defaults (yes for a site key, yes for a user key, etc...). Record your password. [1] I use the same password for both.

After install

Now, there's a trick we will use here. Normally, the guides will tell you to init, and then init again after the errors. However, we will try to skip that, if possible, to save time. Each init is about 2-3 minutes, so time can be avoided, if you know what configs you need. Let's first edit the configs before doing an init.

```
when whitelisting, this is what needs to be commented out in devuan jessie/ascii for

   Filename: /etc/rc.boot
```

[1] For a full walkthrough of this process see this URL:https://www.howtoforge.com/tutorial/how-to-monitor-and-detect-modified-files-using-tripwire-on-ubuntu-1604/ This process includes most, but not all of what you need to know.

```
Filename: /root/mail
Filename: /root/Mail
Filename: /root/.xsession-errors
Filename: /root/.xauth
Filename: /root/.tcshrc
Filename: /root/.sawfish
Filename: /root/.pinerc
Filename: /root/.mc
Filename: /root/.gnome_private
Filename: /root/.gnome-desktop
Filename: /root/.gnome
Filename: /root/.esd_auth
Filename: /root/.elm
Filename: /root/.cshrc
Filename: /root/.bash_profile
Filename: /root/.bash_logout
Filename: /root/.amandahosts
Filename: /root/.addressbook.lu
Filename: /root/.addressbook
Filename: /root/.Xresources
Filename: /root/.Xauthority
Filename: /root/.ICEauthority
Filename: /proc/6136/fd/3
Filename: /proc/6136/fdinfo/3
Filename: /proc/6136/task/6136/fd/3
Filename: /proc/6136/task/6136/fdinfo/3
```

For proc, you simply whitelist the whole directory. After twpol, we are not done. We also need to edit the email settings.

In /etc/tripwire/twcfg.txt we will change the following:

```
MAILMETHOD    =SENDMAIL
MAILPROGRAM =/root/script.sh
```

root.sh is just a script:

```
#!/bin/bash
/usr/sbin/sendmail -s youremail@domain.com
```

2.2 Configuring SSMTP