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: The goal when setting this up is to init, as little as possible. 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 as much as possible.

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

   Filename: /etc/rc.boot
     Filename: /root/mail
     Filename: /root/Mail
     Filename: /root/.xsession-errors
```

---

[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/.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 comment out the whole directory. (you'll see an entry
in the file for /proc, put a # before that). 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
```

script.sh is just a script: (make sure it is executable with chmod +x^2)

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

Finally, the last change we might make, will be for any special directories
we want to watch. I put websites in the root at /sites/ so I will append the
following to /etc/tripwire/twpol.txt

---

[2]This script appears to be required in this setup.

```
# Ruleset for Website
(
  rulename = "Website Ruleset",
  severity= $(SIG_HI)
)
{
        /sites/          -> $(SEC_CRIT);
}
```

Now we will init, type

```
sudo tripwire --init
sudo twadmin -m P /etc/tripwire/twpol.txt
sudo tripwire --init
```

to reconfigure twcfg.txt run

/usr/sbin/twadmin –create-cfgfile -S site.key /etc/tripwire/twcfg.txt

if you get:

```
root@site:~# /usr/sbin/twadmin --create-cfgfile -S site.key /etc/tripwire/twcfg.txt
# Error: File could not be opened.
# Filename: /root/site.key
# No such file or directory
# Exiting...
```

You must cd to /etc/tripwire directory.

2.2   Configuring SSMTP

SSMTP is a program you configure once, and can reuse the configuration everywhere[3]. For starters, I'd recommend you install SSMTP according to this guide here:

```
https://wiki.zoneminder.com/How_to_get_ssmtp_working_with_Zoneminder
```

This is a thorough guide that explains debugging. Some steps are superfluous (given that the instructions pertain to different software) but the general directions are sound. And afterwards sending an email is as easy as

echo "Hello, World" — mail -s "My email check" user@email.com

---

[3]This is a strength of FOSS and let it remain that way.

This guide assumes you have configured SSMTP according to this guide correctly, tested it, and are able to mail from the command line. Once you've setup SSMTP once, you can reproduce this setup on other computers, simply by copying over the revaliases and ssmtp.conf of a valid configuration.

So let's do that. Copy over revaliases, and ssmtp.conf. test the configuration from the command line using the above echo and mail. Once that works, test out tripwire.

tripwire –test –email user@email.com

Done.