Reference URL

http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/ch-tripwire.html

1. Tripwire

Tripwire data integrity assurance software monitors the reliability of critical system files and directories by identifying changes made to them. It does this through an automated verification regimen run at regular intervals. If Tripwire detects that a monitored file has been changed, it notifies the system administrator via email. Because Tripwire can positively identify files that have been added, modified, or deleted, it can speed recovery from a break-in by keeping the number of files which must be restored to a minimum. These abilities make Tripwire an excellent tool for system administrators seeking both intrusion detection and damage assessment for their servers.

Tripwire works by comparing files and directories against a database of file locations, dates they were modified, and other data. This database contains *baselines* — which are snapshots of specified files and directories at a specific point in time. The contents of the baseline database should be generated before the system is at risk of intrusion, meaning before it is connected to the network. After creating the baseline database, Tripwire compares the current system to the baseline and reports any modifications, additions, or deletions.

While Tripwire is a valuable tool for auditing the security state of Red Hat Linux systems, Tripwire is not supported by Red Hat, Inc. If you need more information about Tripwire, a good place to start is the project's website located at http://www.tripwire.org.

1.1. How to Use Tripwire

The following flowchart illustrates how Tripwire works:

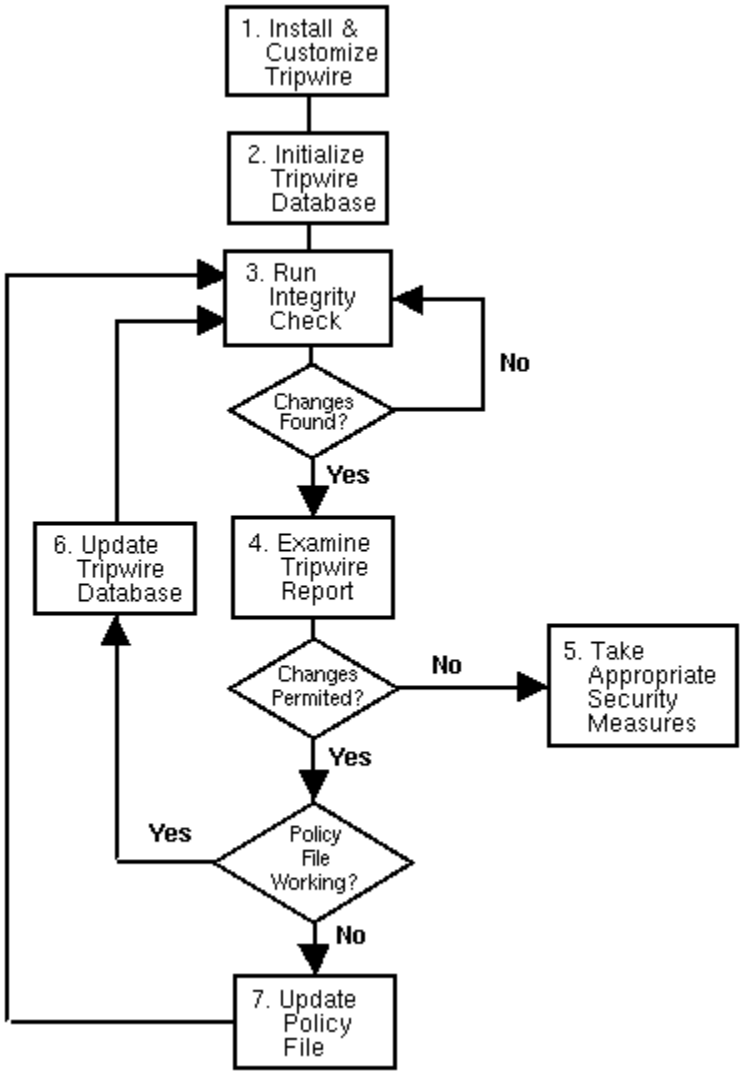

Figure 1-1. Using Tripwire

The following describes in more detail the numbered blocks shown in Figure 19-1.

1. Install Tripwire and customize the policy file.

Install the Tripwire RPM (see Section 1.2 *Installing the Tripwire RPM*). Then, customize the sample configuration and policy files (`/etc/tripwire/twcfg.txt` and `/etc/tripwire/twpol.txt` respectively), and run the configuration script, `/etc/tripwire/twinstall.sh`. For more information, see Section 19.3 *Customizing Tripwire*.

2. Initialize the Tripwire database.

Build a database of critical system files to monitor based on the contents of the new, signed Tripwire policy file, `/etc/tripwire/tw.pol`. For more information, see Section 19.4 *Initialize the Tripwire Database*.

3. Run a Tripwire integrity check.

Compare the newly-created Tripwire database with the actual system files, looking for missing or altered files. For more information, see Section 19.5 *Running an Integrity Check*.

4. Examine the Tripwire report file.

View the Tripwire report file using `/usr/sbin/twprint` to note integrity violations. For more information, see Section 19.6.1 *Viewing Tripwire Reports*.

5. If unauthorized integrity violations occur, take appropriate security measures.

If monitored files have been altered inappropriately, you can either replace the original files from backup copies, reinstall the program, or completely reinstall the operating system.

6. If the file alterations are valid, verify and update the Tripwire database file.

If the changes made to monitored files are intentional, edit Tripwire's database file to ignore those changes in subsequent reports. For more information, see Section 19.7 *Updating the Tripwire Database*.

7. If the policy file fails verification, update the Tripwire policy file.

To change the list of files Tripwire monitors or how it treats integrity violations, update the supplied policy file (`/etc/tripwire/twpol.txt`), regenerate a signed copy (`/etc/tripwire/tw.pol`), and update the Tripwire database. For more information, see Section 19.8 *Updating the Tripwire Policy File*.

Refer to the appropriate sections within this chapter for detailed instructions on each step.

1.2. Installing the Tripwire RPM

The easiest way to install Tripwire is to select the Tripwire RPM during the Red Hat Linux installation process. However, if you have already installed Red Hat Linux, you can use the `rpm` command or the **Package Management Tool** (`redhat-config-packages`) to install the Tripwire RPM from the Red Hat Linux 9 CD-ROMs.

If you are not sure whether Tripwire is installed, type the following command at a shell prompt:

```
rpm -q tripwire
```

If Tripwire is installed, this command will return the following:

```
tripwire-<version-number>
```

In the above output, `<version-number>` is the version number of the package.

If Tripwire is not installed, the shell prompt will return.

The following steps outline how to find and install Tripwire from CD-ROM using the RPM command line application:

1. Insert ***CD 2*** of the Red Hat Linux 9 installation CD-ROMs.
2. If the CD-ROM does not automatically mount, type the following command:

```
mount /mnt/cdrom
```

3. Verify that the Tripwire RPM is on the CD-ROM by typing:

```
ls /mnt/cdrom/RedHat/RPMS/ | grep tripwire
```

   If the RPM is on the CD-ROM, this command will display the package name.

   If the RPM is *not* on the CD-ROM, the shell prompt will return. In this case, you will need to check the other Red Hat Linux 9 installation CD-ROMs by first unmounting the CD-ROM and then repeating steps one through three.

   Unmount the CD-ROM by right-clicking on the CD-ROM icon and selecting **Eject** or by typing the following command at the shell prompt:

```
umount /mnt/cdrom
```

4. Once you have located the Tripwire RPM, install it by typing the following command as the root user:

```
rpm -Uvh /mnt/cdrom/RedHat/RPMS/tripwire*.rpm
```

You will find release notes and README files for Tripwire in the `/usr/share/doc/tripwire-<version-number>/` directory (where `<version-number>` is the version number of the software). These documents contain important information about the default policy file and other topics.