

用 RPM 校验文件

September 11, 2000

Sinbad Technical Publications

Website: <http://sinbad.zhoubin.com>

© Copyright 2000, All Rights Reserved

原作: **Chris Brenton**
翻译: **Sinbad**

有些事情对我们系统管理员来说至少发生过一次，就是你感觉到你的系统好像不对劲，开始怀疑有人已经突破了你的防御。确定此事是否发生的途径之一就是检查系统文件有没有变化，你需要安装 **TripWire** 或者其他审计工具来帮忙。

幸运的是，**Red Hat** 的程序员们开发了一个工具，叫作 **Red Hat Package Manager**，简称为 **RPM**。在 **Red Hat** 的 **Linux** 系统中是默认存在的。

1.RPM 能为我做些什么？

RPM 是一个强大的工具，用来安装、升级和校验 **Red Hat** 系统上的软件包。它的校验功能可以用来确认文件是否被修改或覆盖，这正是本文所要讨论的。除了文件的大小和时间戳，**RPM** 还能检查文件的信息文摘或 **MD5** 签名。

在 **RFC 1321** 中有 **MD5** 的详细描述。简单的说，**MD5** 根据文件的内容用算法产生一个唯一的 128 位签名，用任何方法改变文件都会导致签名改变。尽管人们一直在讨论修改文件后能保持签名不变的理论可能性，但截止到目前还没有人能够做到。所以在文件使用前各作一次 **MD5** 检查，能够 99.9999% 的保证文件没有改变。

2.如何使用 RPM 来检查文件？

有一些 **RPM** 的参数你需要注意。第一个是 “-V”，它检查与某一 **RPM** 包相关所有文件的完整性。语法为：

```
rpm -V package_name_to_verify
```

比如系统上运行了 **sendmail**，通过以下命令检查所有相关文件的完整性：

```
rpm -V sendmail
```

输出看来是这样的：

```
[root@fubar /root]# rpm -V sendmail
S.5....T c /etc/aliases
missing /etc/mail/ip_allow
S.5....T c /etc/mail/relay_allow
S.5....T c /etc/sendmail.cf
S.5....T c /etc/sendmail.cw
S.5....T /usr/sbin/sendmail
S.5....T /var/log/sendmail.st
[root@fubar /root]#
```

只有校验失败的文件才被列出，没有列出的文件应该是完好无损的。左边给出了为什么校验失败的原因，具体解释如下：

S = 大小改变
M = 权限改变
5 = MD5 改变
L = 连接改变
D = 设备改变
U = 用户改变
G = 组改变
T = 日期和时间改变
missing = 文件丢失

从上面的输出可见，文件 `aliases`, `relay_allow`, `sendmail.cf` 和 `sendmail.cw` 的大小、时间日期和 MD5 发生了改变。由于它们是配置文件，应该没什么关系。但是 `/usr/bin/sendmail` 的改变就要引起注意了，它是一个监听在 25 端口的可执行文件，用来接受信件。除非你升级了 `sendmail`，否则它不应该校验失败，很明显有人修改或者覆盖了原来的 `sendmail` 文件，可能带有木马或者后门。

输出还显示 `ip_allow` 文件被删除或者被改名。这是用来检查和控制 SPAM 的一个文件，它的丢失某种程度上表明相关的二进制文件可能被修改。

当观察 RPM 输出的时候，在检查日期时间和文件大小的同时，要特别注意 MD5 是否变化，入侵者经常修改或覆盖某些文件来隐藏他们的踪迹。

挨个检查软件包很费时间，用“-a”选项可以一次性检查所有 RPM 包：

```
rpm -Va > /root/rpm_chk.txt &
```

这条命令让 RPM 检查服务器上安装的 RPM 包，结果输出到 `rpm_chk.txt` 文件，最后的可选项“&”表示命令在后台运行，给出 shell 提示符可以作其他事情。

最后一个技巧，当你想要检查某个文件而不知道它属于哪个 **RPM** 包，可以用“-qf”选项查看哪个软件包安装了此文件：

```
[root@fubar /root]# rpm -qf /usr/sbin/sendmail
sendmail-8.8.7-20
[root@fubar /root]#
```

这表明此 **sendmail** 文件是 **sendmail-8.8.7-20** **RPM** 包的一部分。如果一个文件没有关联的 **RPM** 包，输出大概是这样的：

```
[root@fubar /root]# rpm -qf /sbin/.vile_stuff
file /sbin/.vile_stuff is not owned by any package
[root@fubar /root]#
```

小心你系统上运行的不能被校验的程序！

3.如何开始？

首先，你必须有 **root** 权限来运行 **RPM**。当以普通用户身份来运行 **RPM** 校验时，它的输出信息是不正确的，因为普通用户对某些文件可能都没有 **read** 权限。这意味着只有 **root** 才能检查整个系统文件的完整性。

RPM 二进制文件在 **/bin** 目录下，它的数据库文件在 **/var/lib/rpm** 下。

最安全的方法是在服务器连到 **Internet** 之前，把这些数据文件和 **RPM** 二进制文件保存到软盘或 **CD** 上，这能够保证你的工具自身是安全的。

第一件事是检查 **/var/lib/rpm**，这些数据文件的日期和时间应该和安装系统当时的情况一样，如果你发现日期不对，就要小心了。

其次，我们可以使用 **RPM** 来校验自身的完整性：

```
[root@fubar /root]# rpm -V rpm
[root@fubar /root]#
```

没有输出表示 **RPM** 应该没有什么问题。但这不是绝对的，因为二进制文件如果本身可疑就很难说。所以要尽可能使用 **CD** 上的工具，如果你没有比较安全的工具，用 **RPM** 校验自身在一般情况下也足够了。

现在我们知道 RPM 自身没有问题了，对整个系统作个检查：

```
rpm -Va > /root/rpm_chk.txt &
```

一个简单的技巧就是定期检查整个系统，然后比较不同时期的 rpm_chk.txt，从而发现哪些不正常的文件改动。

4.总结

尽管 RPM 不是专门设计用来审计文件的，但它可以帮你不少忙。目前 Red Hat Linux 各个版本中都默认自带 RPM，这意味着你完成 Red Hat Linux 安装以后，就可以使用 RPM 了，同时 MD5 提供了一种高精确度的文件校验方法。唯一注意的是要保证 RPM 自身和它所有数据文件的完整性，以防止入侵者修改它们来隐藏踪迹。