RKHunter使用

# RKHunter简介

RKHunter是专业检测系统是否感染rootkit的一个工具，它通过执行一系列的脚本来确认服务器是否已经感染rootkit。在官方资料中，RKHunter可以做的事情有：

MD5校验测试，检测文件是否有改动

检测rootkit使用的二进制和系统工具文件

检测特洛伊木马程序的特征码

检测常用程序的文件属性是否异常

检测系统相关的测试

检测隐藏文件

检测可疑的核心模块LKM

检测系统已启动的监听端口

此工具也可以用于常用的入侵检测

# RKHunter安装

RKHunter的官方网站: <http://www.rootkit.nl/projects/rootkit_hunter.html>

这里我下载的版本是 rkhunter-1.4.6.tar.gz 接下来我们开始安装

# tar –xf /data/install/rkhunter-1.4.6.tar.gz

# cd /data/install/rkhunter-1.4.6

# ./installer.sh –layout default --install (这里默认安装到/usr/local/bin下)

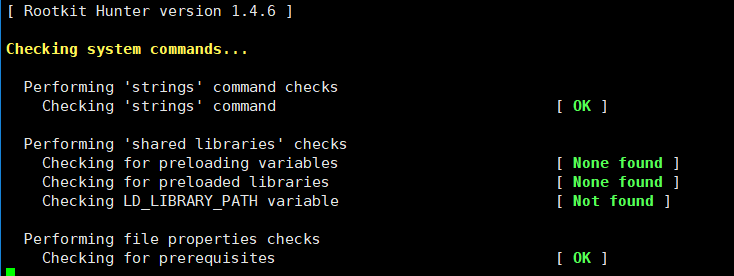
# RKHunter命令使用

RKHunter参数较多，可以rkhunter --help查看，这里我说一下常用的

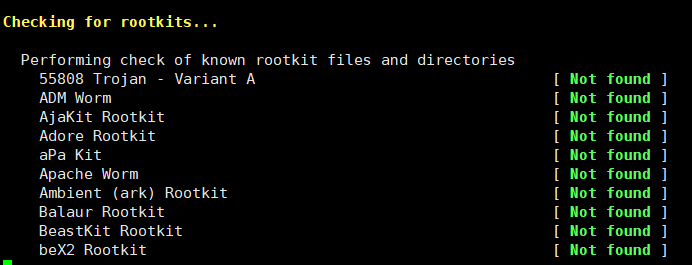
对整个系统进行检测：

# /usr/local/bin/rkhunter –c

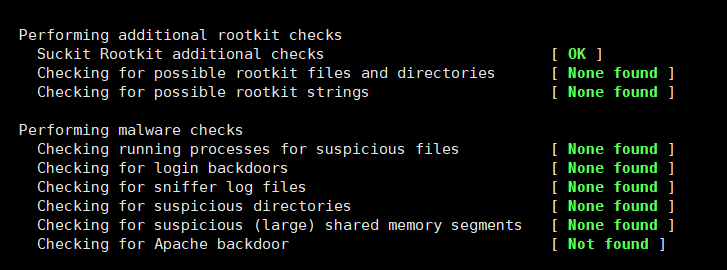
然后下面会分几部分，第一部分首先是对系统命令的检查，显示【ok】表示正常，显示warning表示有异常，需要注意，而显示not found则无需理会



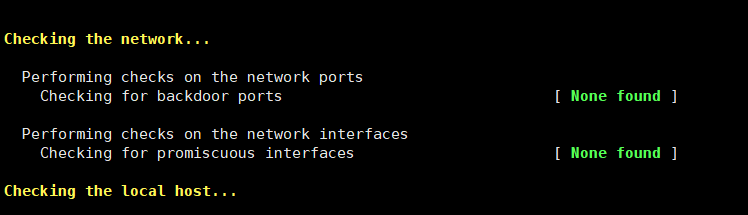
下面是第二部分，主要检测常见的rootkit程序，显示“Not found”表示系统未感染此rootkit



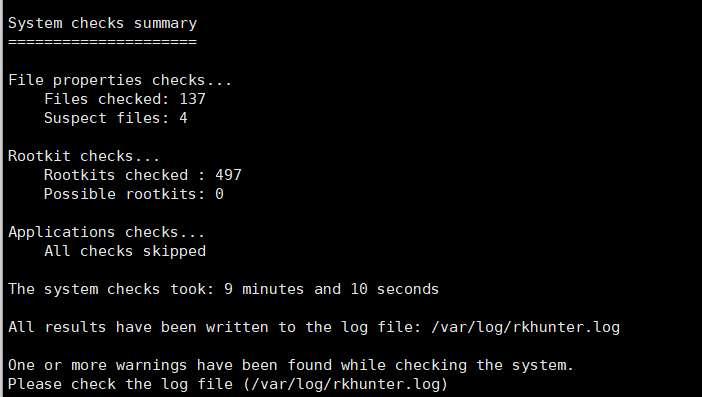
下面是第三部分，主要是一些特殊或附加的检测，例如对rootkit文件或目录检测、对恶意软件检测以及对指定的内核模块检测



下面是第四部分，主要对网络、系统端口、系统启动文件、系统用户和组配置、SSH配置、文件系统等进行检测



下面是第五部分，这一部分其实是上面输出的一个总结，通过这个总结，可以大概了解服务器目录的安全状态



上面每过一个阶段都需要暗回车键确认，如果想让程序自动运行：

#  /usr/local/bin/rkhunter --check --skip-keypress

放入计划任务执行，可以在crontab中加入

1 0 \* \* \*  /usr/local/bin/rkhunter --check –cronjob

这样，检测程序就会在，每天的0时1分执行一次，输出结果在上述提示的日志文件/var/log/rkhunter.log内