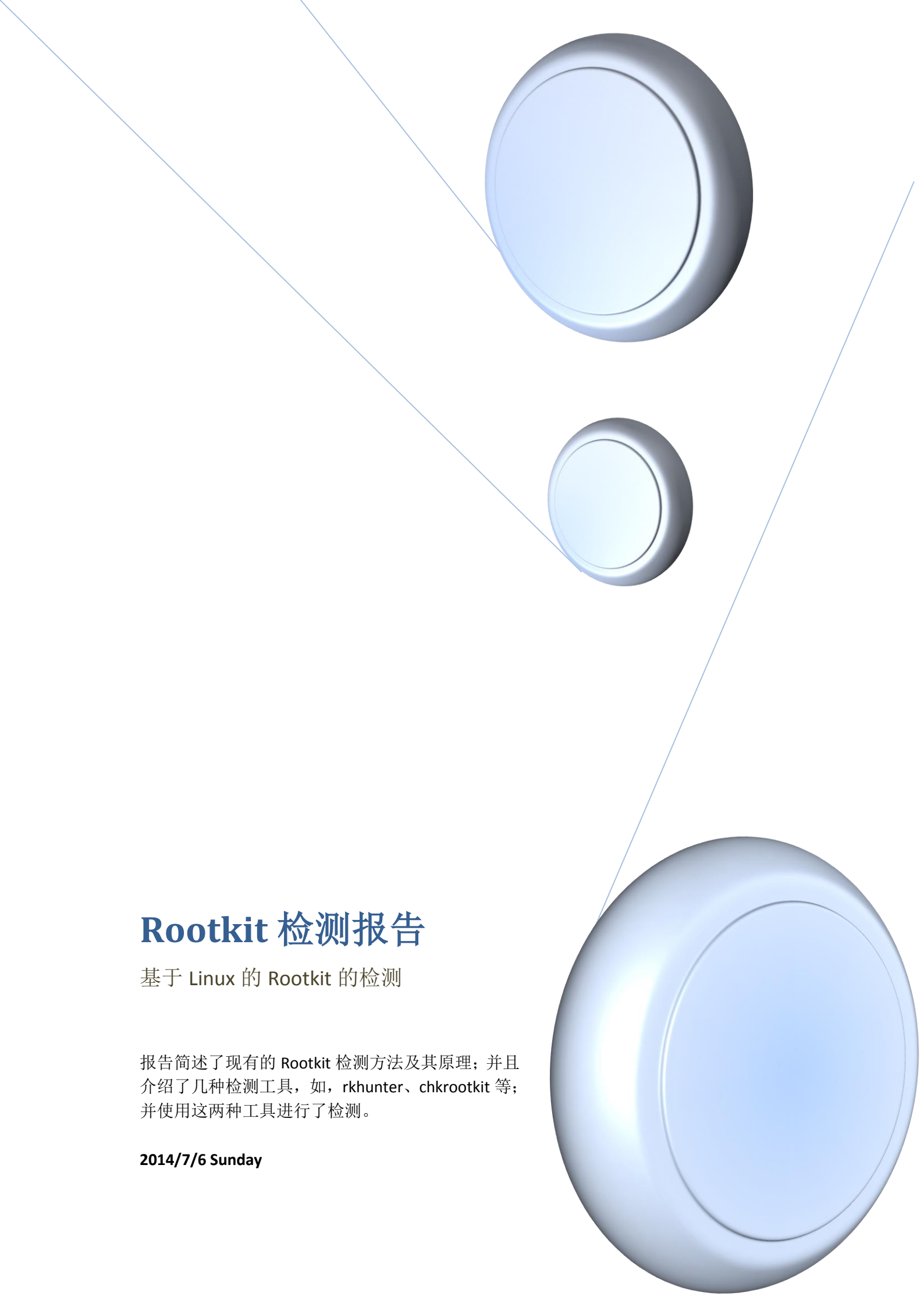

Rootkit 检测报告

基于 Linux 的 Rootkit 的检测

报告简述了现有的 Rootkit 检测方法及其原理；并且介绍了几种检测工具，如，rkhunter、chkrootkit 等；并使用这两种工具进行了检测。

2014/7/6 Sunday

目录

1. Rootkit 简介

Rootkit 隐藏技术主要是指恶意代码采取的一些使得自身进程端口文件等踪迹不被恶意代码检测程序所发现的技术。

Rootkit 之所以能够达到很高的隐藏性，主要有两个原因：

1) 操作系统设计上的隔离不充分。

虽然 Intel 和 AMD 等厂商将芯片分为四个特权，但是诸如 Windows 和 Linux 等主流的操作系统只使用了其中的两个特权级，即用户态和内核态。操作系统将系统内核驱动等都归为内核态，导致了安全性上的隐患。

2) 允许第三方程序加载驱动到系统的内核空间。

这也就意味着恶意代码可以通过加载恶意的驱动程序进入系统内核，并以此来获取和操作系统内核同样的权限。

2. Rootkit 检测方法介绍

为了隐藏恶意代码的行为和 Rootkit 自身，Rootkit 需要对系统或应用程序进行某些修改，检测软件则利用 Rootkit 修改留下的痕迹来检测 Rootkit 的存在。Rootkit 的检测方法分为: 文件完整性检测，谎言检测，基于硬件虚拟化的检测。

2.1 完整性检测

完整性检测技术分为磁盘文件完整性检测和内存数据的完整性检测，利用这种技术只能检测 Hook 和用户态系统文件替换的 Rootkit 的存在。

2.1.1 磁盘文件的完整性检测

该检测办法主要针对通过修改磁盘文件来进行隐藏的 Rootkit，如对 Linux 中 ps，netstat 等系统文件的替换。

该技术将系统中每个要监控的系统文件生成一个数字签名并存储起来，在以后运行时，如果发现现在生成的数字签名和初始化的数字签名不一致，则说明该系统文件被修改了。

如 Linux 系统下的 Tripwire。 该技术也可以应用于对 Windows 下 DLL 替换的检测。

2.1.2 内存数据完整性检测

内存态数据完整性检测通过检测内核中数据和地址是否异常来检测 Rootkit 的存在。该技术可以被用来检测采用挂钩 Hook 和内联函数替换的 Rootkit。

在操作系统中，每个模块导出的函数的地址都应该处于其模块地址的范围内。使用这种技术的检测程序认为：如果一个模块导出的函数地址不在其模块地址范围内，则认定该函数被 Rootkit 挂钩了；如果同一个系统版本的内核服务函数的代码不同，也认为该函数被 Rootkit 内联挂钩了。

如 Rootkit HookAnalyzer、IceSword、VICE 等检测程序都利用了这种技术来检测。

2.2 谎言检测

操作系统未被恶意代码感染之前，系统的各个层次获取的系统视图应该是一致的。如从用户态获取的进程数，应该和内核态看到进程列表中数量相一致。谎言检测技术假定：如果在不同的层次获取的系统视图不一致，必定有一方在说谎。

2.3 硬件虚拟化的检测办法

硬件虚拟化允许在裸机上直接运行虚拟机管理软件(VMM)，其上运行操作系统(无需修改系统)。由于使用硬件虚拟化能够提供很好的透明性，所以可以利用硬件虚拟化技术对恶意代码进行行为分析和检测。如美国乔治亚理工大学的 Ether、美国威斯康星大学的 Lycosid、清华大学开发 RKAnalyer 等都是利用硬件虚拟化技术开发的恶意代码的分析和检测工具。

Ether: Ether 利用开源硬件虚拟机管理软件 Xen(版本 3.0 之后) 开发的一个恶意代码行为分析系统。Ether 在设计上采用硬件虚拟化技术，它提供了对系统运行的细粒度跟踪和和粗粒度跟踪两种模式，可以监控目标系统中指令的运行内存写入系统的调用以及上下文的切换。由于在特权级上高于被分析的目标系统，Ether 能够欺骗恶意代码，保证了透明性。

但是 Ether 也并不是十全十美的: 其对内存的监控也只能精确到页面的力度；由于 VT-x 技术并没有对内存和 I/O 提供虚拟化的支持，Ether 可能招致内存重定向攻击；同时 Ether 只能支持单处理器。

Lycosid: Lycosid 是利用开源硬件虚拟机管理软件 Xen(版本为 3．0．3-testing) 开发的 Rootkit 检测程序，该系统利用了上文提到的谎言检测的办法。Lycosid 比传统谎言检测技术的创新之处在于它认为操作系统已经不可信了，它只信任虚拟机监视器 VMM(即虚拟机管理软件) 。它对系统中进程的检测，利用操作系统中进程的切换等同于对 CR3 寄存器的写入。通过设置 VMCS，每当客户系统(Guest OS)发生对 CR3 的写入，系统将从 VMXnon-root 切换到 VMXroot，Lycosid 记录下此时进程的 pid，从而来罗列系统的运行的进程。通过与从客户系统(Guest OS) 应用层获得的进程列表进行比较，查找被隐藏的进程.

该系统的缺点也是很明显的：首先对 CR3 的写入并不严格等于系统中进行的切换，如一些 Rootkit 插入干扰性的切换指令来干扰对其的探测；其次用户态罗列进程列表与 VMM 中罗列的进程列表很难达到同步，由于系统进程的创建和退出非常快，这就使得系统误报率比较高。

3. 几种检测工具的介绍和检测结果

3.1 rkhunter

3.1.1 工作原理

rkhunter 是 Linux 系统平台下的一款开源入侵检测工具，具有非常全面的扫描范围，除了能够检测各种已知的 rootkit 特征码以外，还支持端口扫描、常用程序文件的变动情况检查。

rkHunter 可检查用户系统上多种恶意软件行为，如 rootkit、后门程序以及利用本地漏洞

的程序。它可以运行多种测试，包括 MD5、HASH 比较、rootkit 默认文件名、二进制文件许可，以及在 LKM 和 KLD 模块中的可疑字符串.

rkhunter 就像杀毒软件，有着自己的病毒数据库，对每一个重点命令进行比对，当发现可疑代码则提示用户。它拥有并维护着一个包含 rootkit 特征的数据库，然后它根据数据库来检测系统中的 rootkit，需要对数据库进行升级：sudo rkhunter -update。

rkhuner 在进行检查时把相应的信息写到了日志中：/var/log/rkhunter/rkhunter.log

主要执行下面一系列的测试:

- ✧ MD5 校验测试，检测任何文件是否改动.
- ✧ 检测 rootkits 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.
- ✧ 检测大多常用程序的文件异常属性.
- ✧ 执行一些系统相关的测试 - 因为 rootkit hunter 可支持多个系统平台.
- ✧ 扫描任何混杂模式下的接口和后门程序常用的端口.
- ✧ 检测如/etc/rc.d/目录下的所有配置文件，日志文件，任何异常的隐藏文件等等
- ✧ 对一些使用常用端口的应用程序进行版本测试。

下载 Rootkit Hunter 地址：http://www.rootkit.nl/projects/rootkit_hunter.html

使用方法：

- ✧ 解压：tar -zxvf rkhuner-1.3.4(版本).tar.gz
- ✧ 进入目录后安装：./installer.sh --layout default --install
- ✧ 使用：rkhunter –checkall

3.1.2 检测结果

rkhunter 的检测分为 5 部分：

- ✧ 第一部分：检测重要文件的 MD5 码
- ✧ 第二部分：检测常见 rootkit 攻击文件和目录
- ✧ 第三部分：检测常见木马端口
- ✧ 第四部分：检测本机信息
- ✧ 第五部分：检测安全套件

安装 rootkit 以后，rkhunter 检测到了可疑的 rootkit。

- ➢ **纯净的系统的检测结果**

可以从检测结果清楚的看到上述的 5 部分。

从图 3.1.2_1~3.1.2_4（见最后附录章节 4.图表说明）的检测结果，我们看到未被感染的系统也会出现几个 warning。

从最终的简介结果（图 3.1.2_4）我们看到检测了 135 个文件，有 3 个可疑文件；无可能的 Rootkit，和可疑的应用（本小节截图最后一张）。

- ➢ **装有 rootkit 的系统的检测结果**

从最后结果图 3.1.2_5~3.1.2_10（见最后附录章节 4.图表说明）我们可以看到在“Performing malware checks”下的“Checking running processes for suspicious files”项目中出现红色 Warning 警告，并在最后的结果图 3.1.2_10 中显示除了有 3 个可疑文件以外，还有 1 个可能的 rootkit，name 是 Generic backdoor。

工具 rkhunter 检测到了我们的 Rootkit。

3.2 chkrootkit

3.2.1 工作原理

Chkrootkit 由 Nelson Murilo 和 Klaus Steding Jessen 开发，是一个灵活的便携式工具，它可以检查基于 linux 系统的 rootkit 入侵的行为。其特性包括：检测二进制的改变、检测对文件 utmp/wtmp/lastlog 的修改、检测恶意的内核模块等。

与 Rootkit Hunter 程序不同的是, chrootkit 不需要 installer 安装程序，你只需解开软件包后执行 chrootkit 即可，除了与 Rootkit Hunter 相同的测试外, Chkrootkit 还对一些重要的二进制文件进行检测，比如搜索入侵者已更改日志文件的特征信息等等.

- 如何安装 chkrootkit

  apt-get install chkrootkit
- 如果想列出已经测试的所有项目，你可以运行带有’-l’参数的命令:

  # chkrootkit -l
- 在测试过程中，如果你想在屏幕上看到更多有用的信息，执行下面命令:

  # chkrootkit -x

如果后面的是 not infected not tested 或 nothing found 之类的 则为正常，如果出现了 INFECTED 则说明你的服务器中招了

3.2.2 检测结果

chkrootkit 工具未检测到本 rootkit。

- **纯净的系统的检测结果**

图 3.2.2_1~3.2.3_3（见最后附录章节 4.图表说明）显示了未安装 Rootkit 之前的系统的检测结果，皆显示为“not found” “ not infected” “ noting found”等字眼。

- **装有 Rootkit 的系统的检测结果**

  未检测出 Rootkit 的踪迹，检测结果图无变化（图 3.2.2_1~3.2.3_3，见最后附录章节 4.图表说明）

3.3 结论和其他工具简介

- 在 Linux 上组合使用 Rootkit Hunter 和 Chkrootkit 工具是检测 rootkis 不错的办法。
- 还有一些其他的检测工具，但是这些工具难以检测到内核级 rootkit。例如：
  - ✧ **Tripwire**

Tripwire,是一款文件和目录集成检测工具。采用的技术核心就是对每个要监控的文件产生一个数字签名保留下来，当文件现在的数字签名与保留的数字签名不一致时，那么现在这个文件必定被改动过了。

Tripwire 首先使用特定的特征码函数为需要监视的系统文件和目录建立一个特征数据库，入侵者如果对文件进行了修改，会破坏文件的特征码。利用这个数据库，Tripwire 可以很容易地发现系统的变化。而且文件的特征码几乎是不可能伪造的。最后，需要能够把这个特征

码数据库放到安全的地方。

✧ **AIDE（类似于 Tripwire）**

AIDE(Adevanced Intrusion Detection Environment,高级入侵检测环境)是个入侵检测工具，主要用途是检查文档的完整性。AIDE 是个 Tipwire 的替代和扩展软件，他有一些 Tripwire 所不具备的特征。aide 当前具备的特征包括：多种完整性检验算法、把数据库输出到标准输出设备/文档的能力、通过配置文档进行配置连同数据库压缩支持。

4. 附录 • 图表说明

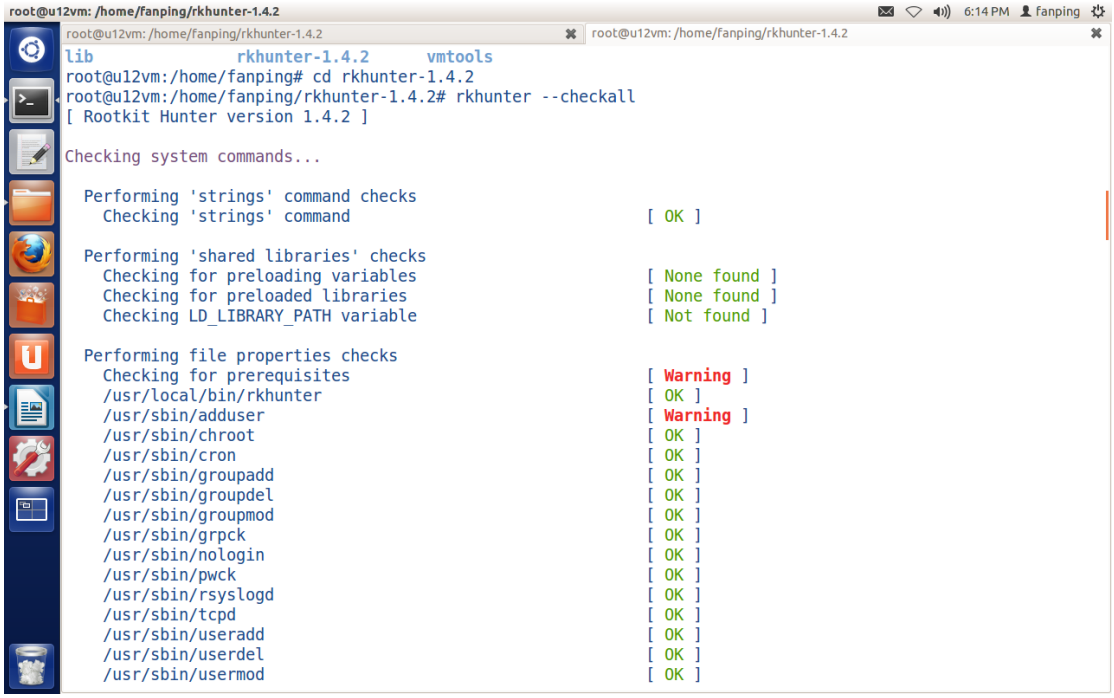

图 3.1.2_1

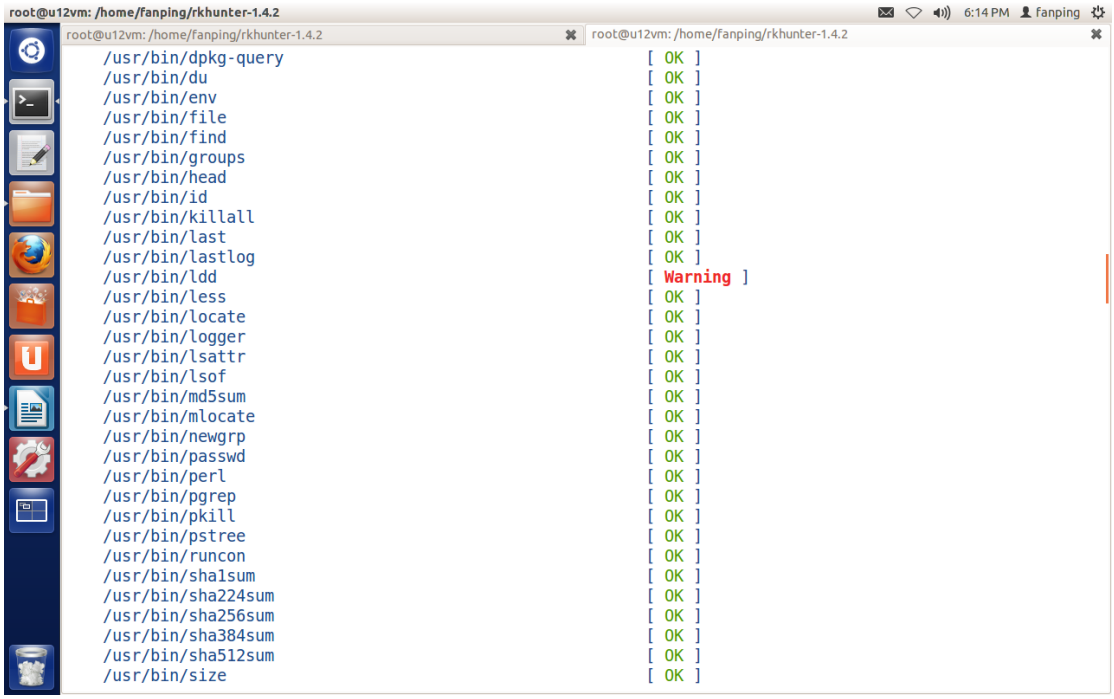

图 3.1.2_2

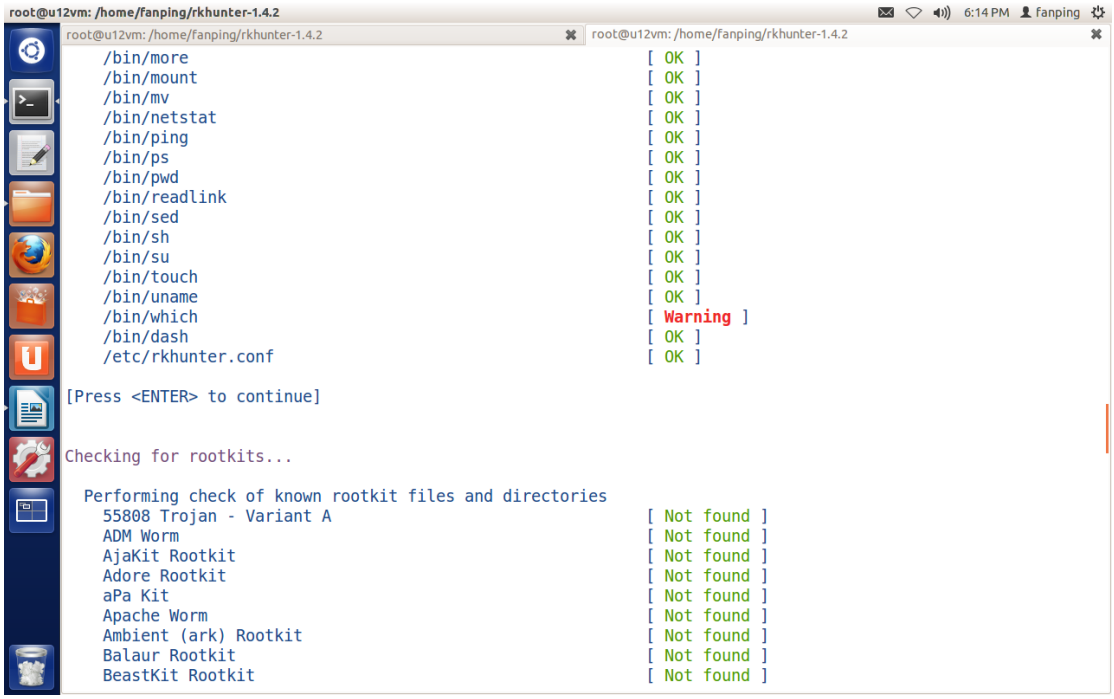
root@u12vm: /home/fanping/rkhunter-1.4.2
6:14 PM fanping
root@u12vm: /home/fanping/rkhunter-1.4.2
root@u12vm: /home/fanping/rkhunter-1.4.2
/bin/more [OK]
/bin/mount [OK]
/bin/mv [OK]
/bin/netstat [OK]
/bin/ping [OK]
/bin/ps [OK]
/bin/pwd [OK]
/bin/readlink [OK]
/bin/sed [OK]
/bin/sh [OK]
/bin/su [OK]
/bin/touch [OK]
/bin/uname [OK]
/bin/which [Warning]
/bin/dash [OK]
/etc/rkhunter.conf [OK]
[Press <ENTER> to continue]
Checking for rootkits...
Performing check of known rootkit files and directories
55808 Trojan - Variant A [Not found]
ADM Worm [Not found]
AjaKit Rootkit [Not found]
Adore Rootkit [Not found]
aPa Kit [Not found]
Apache Worm [Not found]
Ambient (ark) Rootkit [Not found]
Balaur Rootkit [Not found]
BeastKit Rootkit [Not found]

图 3.1.2_3

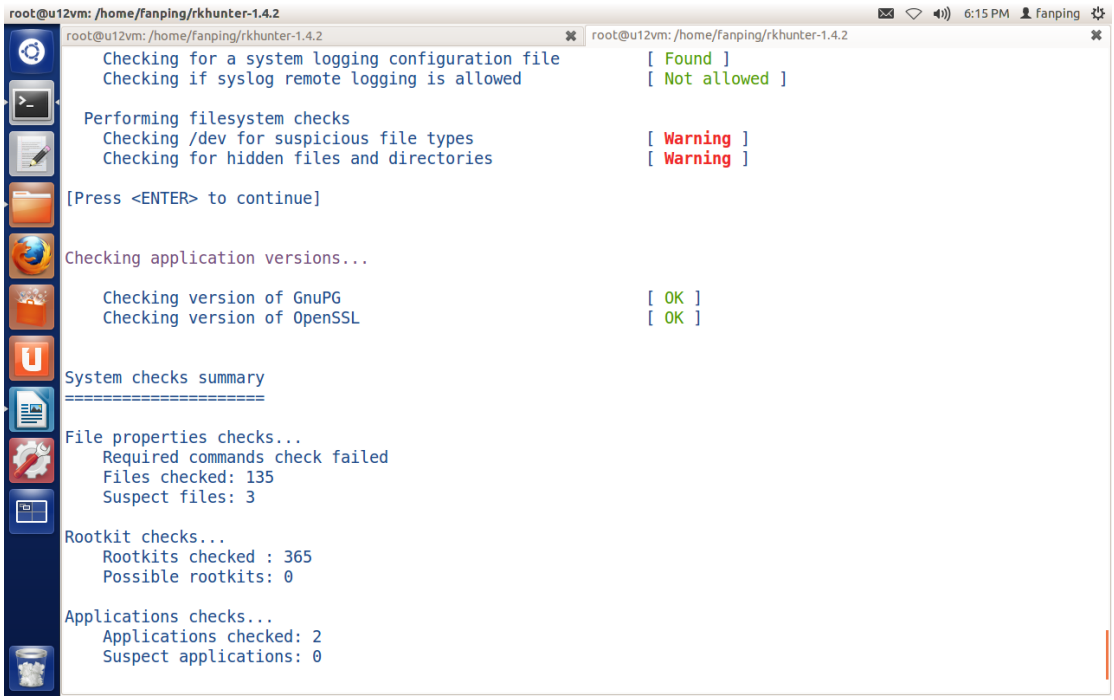
root@u12vm: /home/fanping/rkhunter-1.4.2
6:15 PM fanping
root@u12vm: /home/fanping/rkhunter-1.4.2
root@u12vm: /home/fanping/rkhunter-1.4.2
Checking for a system logging configuration file [Found]
Checking if syslog remote logging is allowed [Not allowed]
Performing filesystem checks
Checking /dev for suspicious file types [Warning]
Checking for hidden files and directories [Warning]
[Press <ENTER> to continue]
Checking application versions...
Checking version of GnuPG [OK]
Checking version of OpenSSL [OK]
System checks summary
File properties checks...
Required commands check failed
Files checked: 135
Suspect files: 3
Rootkit checks...
Rootkits checked : 365
Possible rootkits: 0
Applications checks...
Applications checked: 2
Suspect applications: 0

图 3.1.2_4

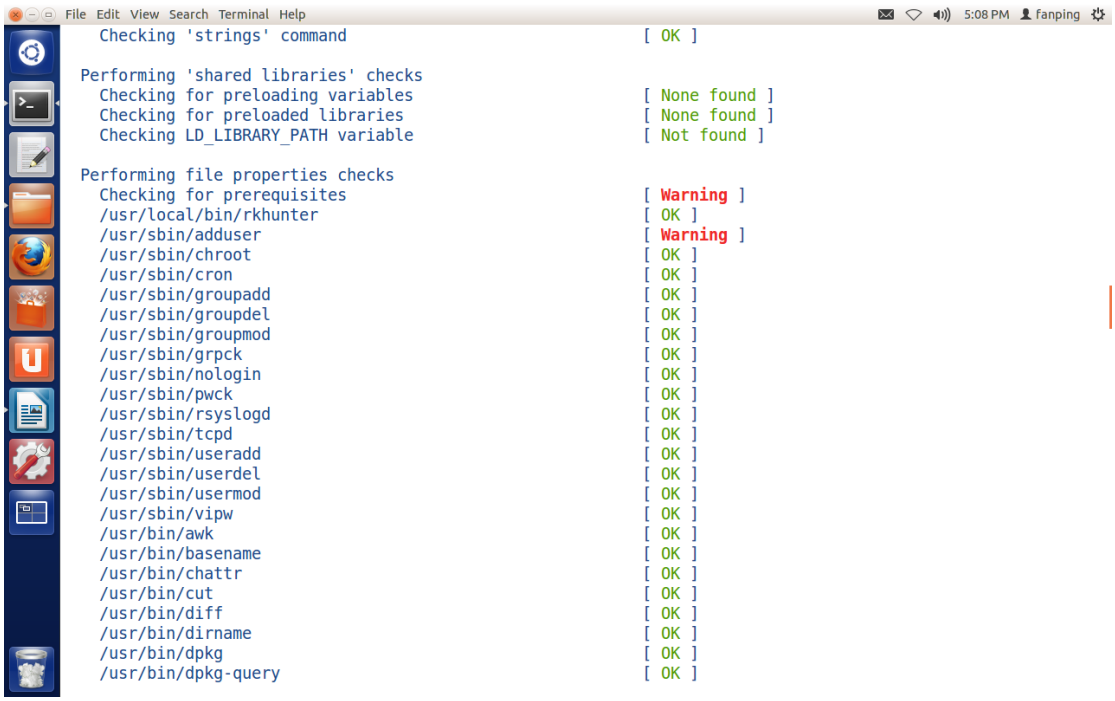
File Edit View Search Terminal Help
5:08 PM fanping
Checking 'strings' command [OK]
Performing 'shared libraries' checks
Checking for preloading variables [None found]
Checking for preloaded libraries [None found]
Checking LD_LIBRARY_PATH variable [Not found]
Performing file properties checks
Checking for prerequisites [Warning]
/usr/local/bin/rkhunter [OK]
/usr/sbin/adduser [Warning]
/usr/sbin/chroot [OK]
/usr/sbin/cron [OK]
/usr/sbin/groupadd [OK]
/usr/sbin/groupdel [OK]
/usr/sbin/groupmod [OK]
/usr/sbin/grpck [OK]
/usr/sbin/nologin [OK]
/usr/sbin/pwck [OK]
/usr/sbin/rsyslogd [OK]
/usr/sbin/tcpd [OK]
/usr/sbin/useradd [OK]
/usr/sbin/userdel [OK]
/usr/sbin/usermod [OK]
/usr/sbin/vipw [OK]
/usr/bin/awk [OK]
/usr/bin/basename [OK]
/usr/bin/chattr [OK]
/usr/bin/cut [OK]
/usr/bin/diff [OK]
/usr/bin/dirname [OK]
/usr/bin/dpkg [OK]
/usr/bin/dpkg-query [OK]

图 3.1.2_5

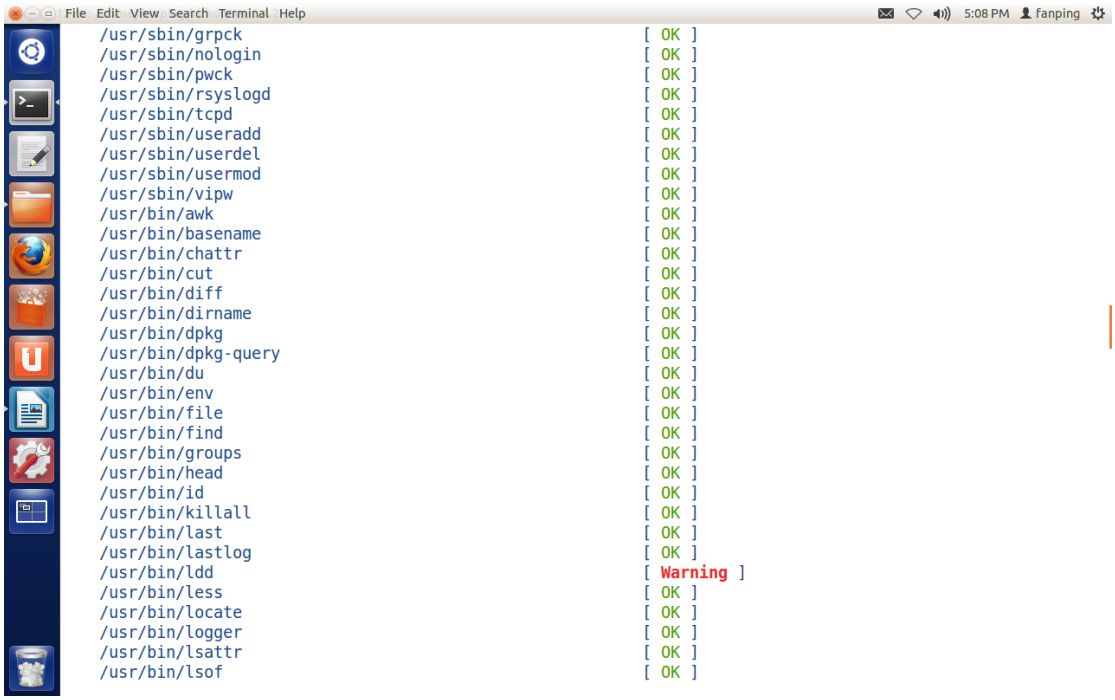
File Edit View Search Terminal Help
5:08 PM fanping
/usr/sbin/grpck [OK]
/usr/sbin/nologin [OK]
/usr/sbin/pwck [OK]
/usr/sbin/rsyslogd [OK]
/usr/sbin/tcpd [OK]
/usr/sbin/useradd [OK]
/usr/sbin/userdel [OK]
/usr/sbin/usermod [OK]
/usr/sbin/vipw [OK]
/usr/bin/awk [OK]
/usr/bin/basename [OK]
/usr/bin/chattr [OK]
/usr/bin/cut [OK]
/usr/bin/diff [OK]
/usr/bin/dirname [OK]
/usr/bin/dpkg [OK]
/usr/bin/dpkg-query [OK]
/usr/bin/du [OK]
/usr/bin/env [OK]
/usr/bin/file [OK]
/usr/bin/find [OK]
/usr/bin/groups [OK]
/usr/bin/head [OK]
/usr/bin/id [OK]
/usr/bin/killall [OK]
/usr/bin/last [OK]
/usr/bin/lastlog [OK]
/usr/bin/ldd [Warning]
/usr/bin/less [OK]
/usr/bin/locate [OK]
/usr/bin/logger [OK]
/usr/bin/lsattr [OK]
/usr/bin/lsof [OK]

图 3.1.2_6


File Edit View Search Terminal Help
5:08 PM fanping
/bin/date [OK]
/bin/df [OK]
/bin/dmesg [OK]
/bin/echo [OK]
/bin/ed [OK]
/bin/egrep [OK]
/bin/fgrep [OK]
/bin/fuser [OK]
/bin/grep [OK]
/bin/ip [OK]
/bin/kill [OK]
/bin/less [OK]
/bin/login [OK]
/bin/ls [OK]
/bin/lsmod [OK]
/bin/mktemp [OK]
/bin/more [OK]
/bin/mount [OK]
/bin/mv [OK]
/bin/netstat [OK]
/bin/ping [OK]
/bin/ps [OK]
/bin/pwd [OK]
/bin/readlink [OK]
/bin/sed [OK]
/bin/sh [OK]
/bin/su [OK]
/bin/touch [OK]
/bin/uname [OK]
/bin/which [Warning]
/bin/dash [OK]
/etc/rkhunter.conf [OK]

图 3.1.2_7

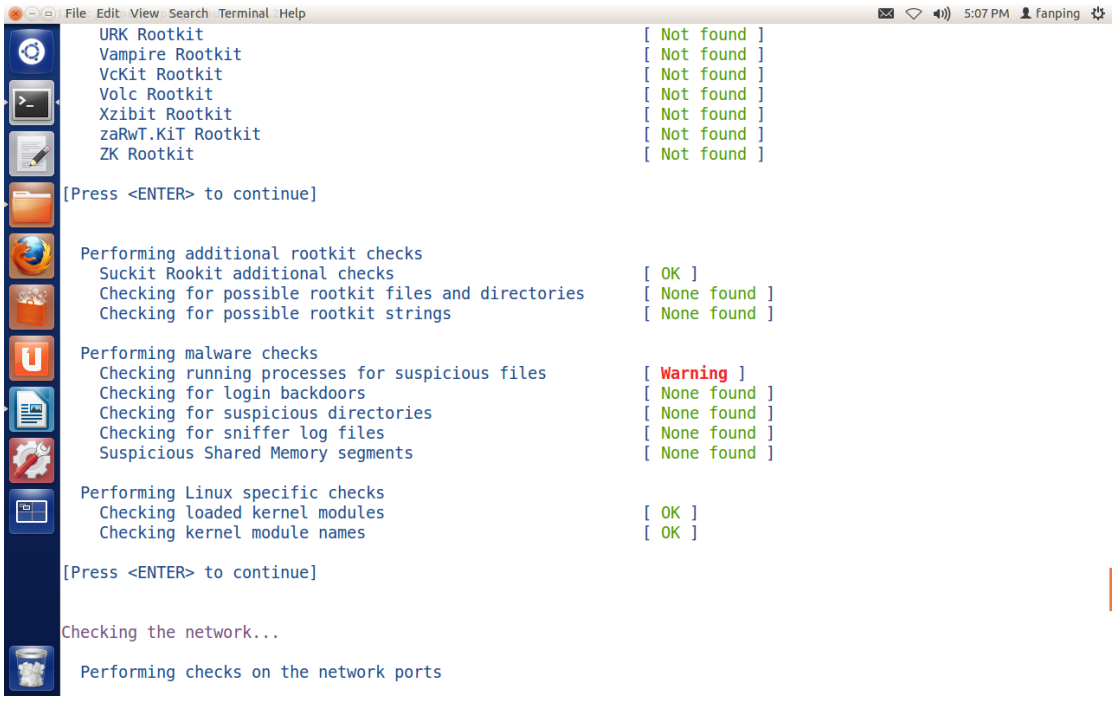
File Edit View Search Terminal Help
5:07 PM fanping
URK Rootkit [Not found]
Vampire Rootkit [Not found]
VcKit Rootkit [Not found]
Volc Rootkit [Not found]
Xzibit Rootkit [Not found]
zaRwT.KiT Rootkit [Not found]
ZK Rootkit [Not found]
[Press <ENTER> to continue]
Performing additional rootkit checks
Suckit Rookit additional checks [OK]
Checking for possible rootkit files and directories [None found]
Checking for possible rootkit strings [None found]
Performing malware checks
Checking running processes for suspicious files [Warning]
Checking for login backdoors [None found]
Checking for suspicious directories [None found]
Checking for sniffer log files [None found]
Suspicious Shared Memory segments [None found]
Performing Linux specific checks
Checking loaded kernel modules [OK]
Checking kernel module names [OK]
[Press <ENTER> to continue]
Checking the network...
Performing checks on the network ports

图 3.1.2_8

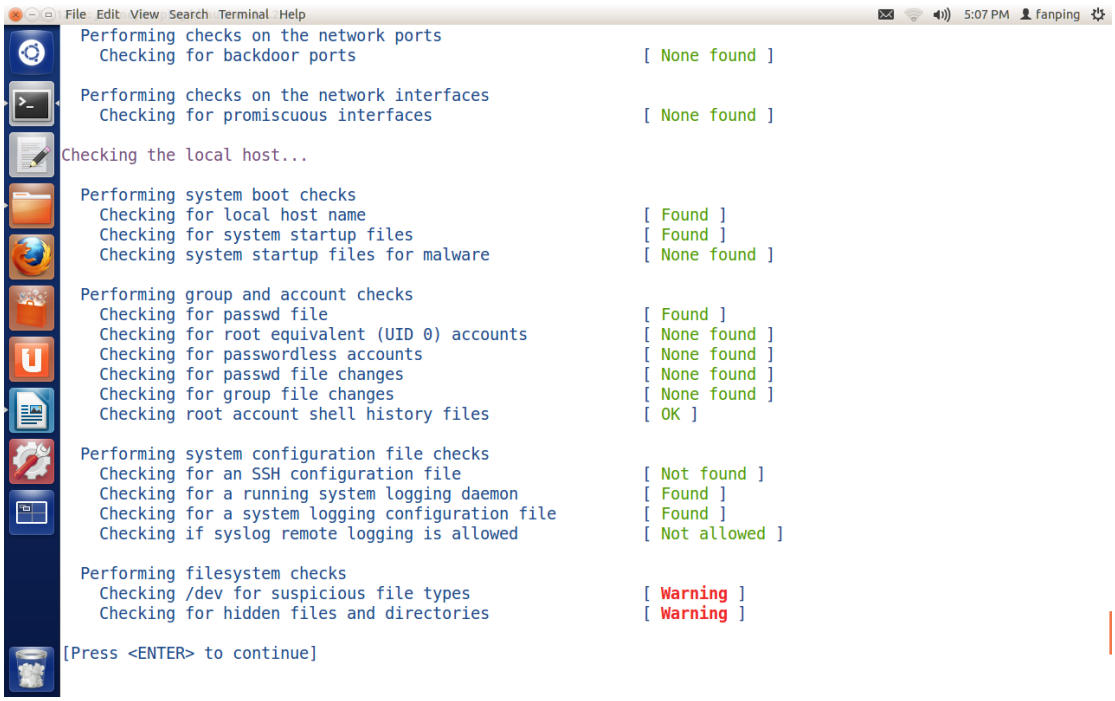

图 3.1.2_9

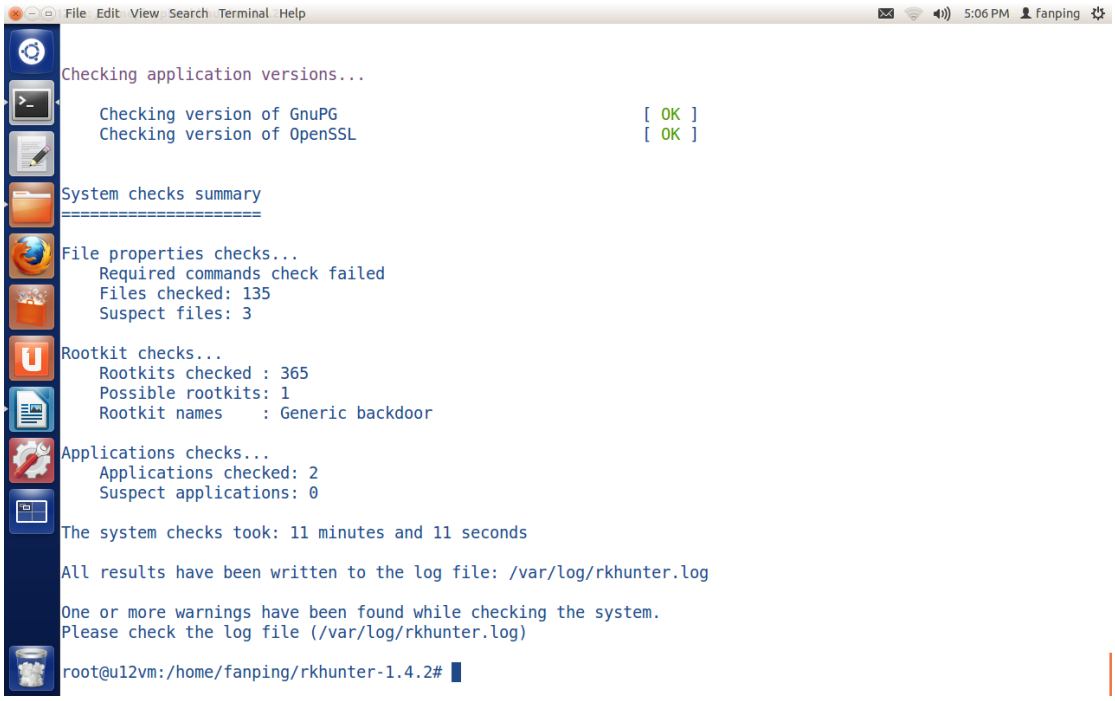

图 3.1.2_10

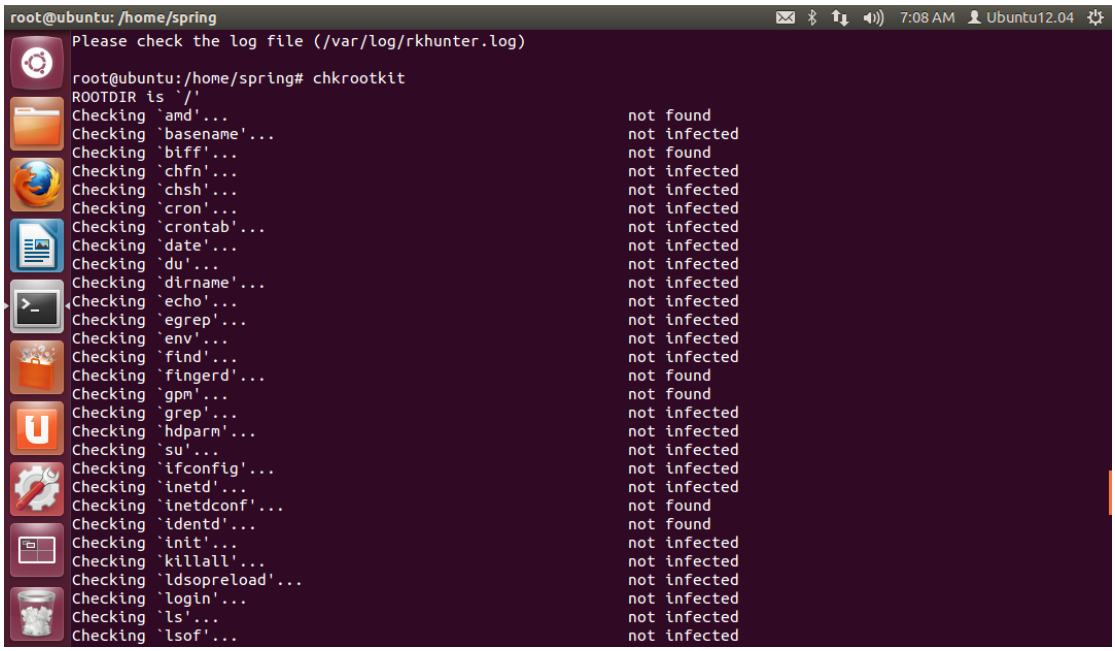
root@ubuntu: /home/spring
7:08 AM
Ubuntu12.04
Please check the log file (/var/log/rkhunter.log)
root@ubuntu:/home/spring# chkrootkit
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not infected
Checking `inetdconf'... not found
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... not infected
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not infected

图 3.2.2_1

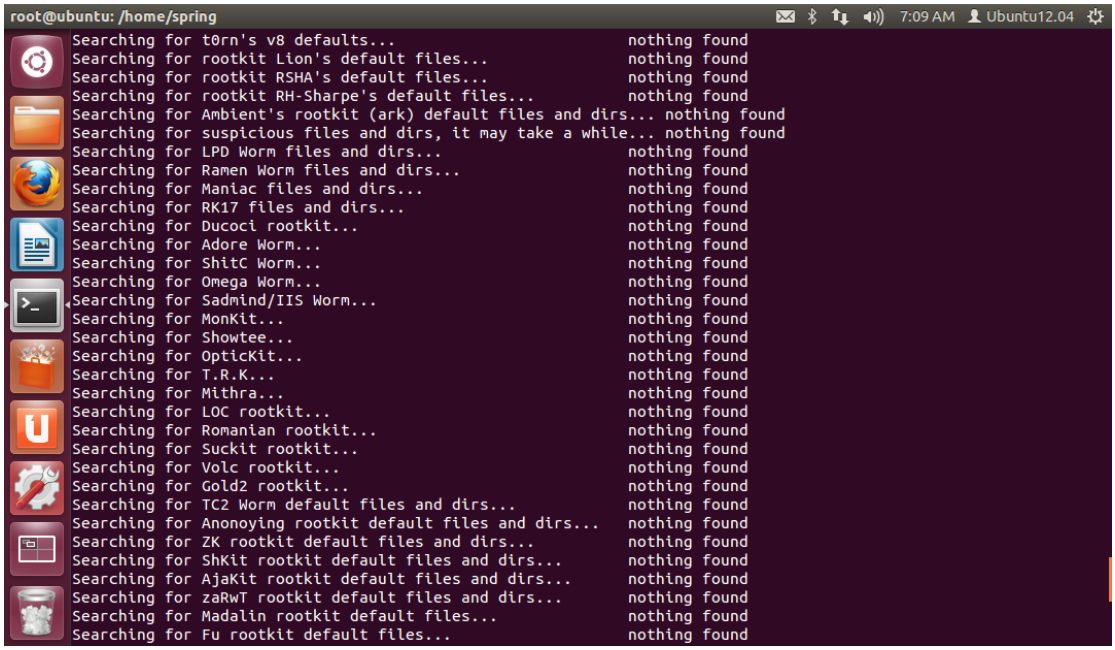
root@ubuntu: /home/spring
7:09 AM
Ubuntu12.04
Searching for t0rn's v8 defaults... nothing found
Searching for rootkit Lion's default files... nothing found
Searching for rootkit RSHA's default files... nothing found
Searching for rootkit RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while... nothing found
Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for LOC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for Suckit rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Gold2 rootkit... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for AjaKit rootkit default files and dirs... nothing found
Searching for zaRwT rootkit default files and dirs... nothing found
Searching for Madalin rootkit default files... nothing found
Searching for Fu rootkit default files... nothing found

图 3.2.2_2

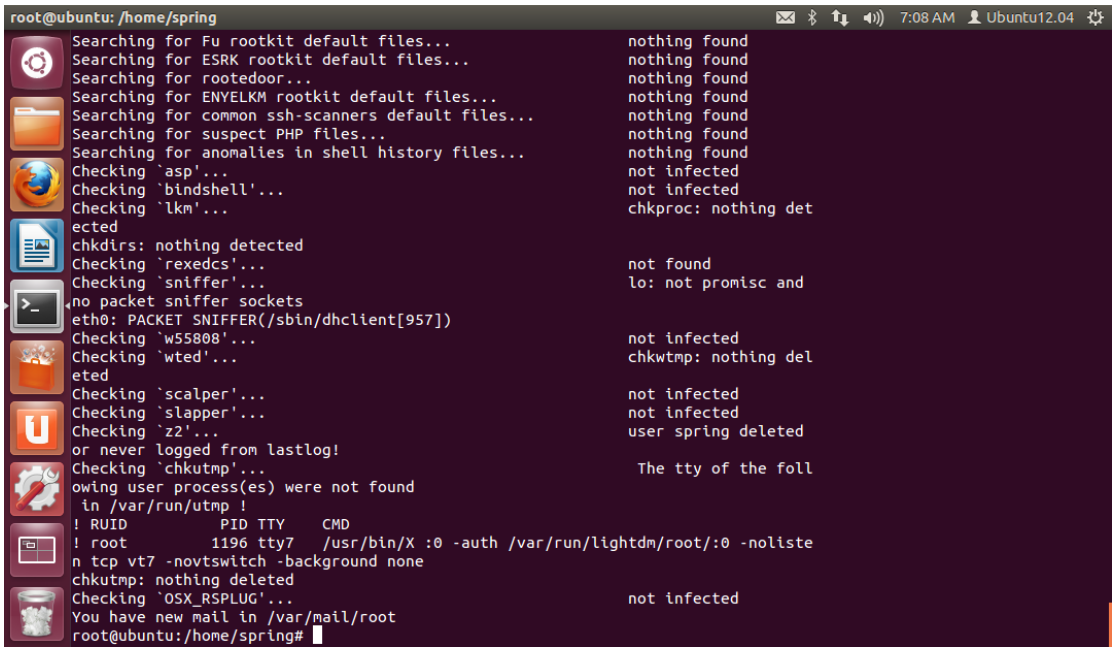
root@ubuntu: /home/spring
7:08 AM
Ubuntu12.04
Searching for Fu rootkit default files... nothing found
Searching for ESRK rootkit default files... nothing found
Searching for rootedoor... nothing found
Searching for ENYELKM rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for suspect PHP files... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... chkproc: nothing det
ected
chkdirs: nothing detected
Checking `rexedcs'... not found
Checking `sniffer'... lo: not promisc and
no packet sniffer sockets
eth0: PACKET SNIFFER(/sbin/dhclient[957])
Checking `w55808'... not infected
Checking `wted'... chkwtmp: nothing del
eted
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... user spring deleted
or never logged from lastlog!
Checking `chkutmp'... The tty of the foll
owing user process(es) were not found
in /var/run/utmp !
! RUID PID TTY CMD
! root 1196 tty7 /usr/bin/X :0 -auth /var/run/lightdm/root/:0 -noliste
n tcp vt7 -novtswitch -background none
chkutmp: nothing deleted
Checking `OSX_RSPLUG'... not infected
You have new mail in /var/mail/root
root@ubuntu:/home/spring#

图 3.2.2_3