bit4@MottoIN Team

手册的作用：

系统管理员常常站在电脑安全的第一线，这个手册的目的式帮助系统管理员找到系统入侵的迹象。

在周期性登陆系统时，可以快速地过一遍以下步骤以发现电脑被入侵的恶意行为。这些命令都是在系统本地执行的。

首次分为以下部分：

1. 不正常的进程和服务
2. 不正常的文件
3. 不正常的网络使用情况
4. 不正常的计划任务
5. 不正常的账号
6. 不正常的日志记录
7. 其他不正常的条码记录
8. 工具推荐

1、不正常的进程和服务

查看所有正在运行的进程

```
#ps -aux
```

熟悉“正常的”进程，查看不正常的进程，重点关注以 root 权限运行的。

如果你发现了不熟悉的进程，通过如下命令查看更多详情：

```
lsof  -p [pid]
```

这个命令显示所有被这个进程使用的文件和端口

如果你的系统上有安装 chkconfig，你可以运行 chkconfig 来查看不同的运行级别分别启用了哪些服务

```
#chkconfig --list
```

2、不正常的文件

查看不正常的 SUID 文件：

```
#find / -uid 0 -perm -4000 -print
```

这需要你有关于正常 SUID 文件的知识。

查看大小不正常的文件（大于 10MB）

```
#find / -size +1000k -print
```

查看文件名包含点和空格的文件（"..."，".."，"."，" "）

```
# find / -name "..." -print
# find / -name ".. " -print
# find / -name ". " -print
# find / -name " " -print
```

查看那些进程产生或访问的无连接文件，攻击者可能通过这些文件隐藏数据或者运行后门。

```
lsof +L1 (link 数上限为 1)
```

在一个用 RPM 安装的 linux 机器上，通过运行 RPM 工具去校验 RPM 包：

```
#rpm -Va | sort
```

这个命令会校验文件的大小，MD5 校验和，权限，类型，拥有者，和所属组，同 RPM 数据库获取到的数据进行比较，显示不相同的地方

输出包括：
S-文件大小的不同
M-模式不同（权限）
5-MD5 校验值
D-设备号不匹配
L-读符号链接(readLink)的值路径不匹配
U-用户所属关系不同
G-组所属关系不同
T-修改时间不匹配

需要特别关注 /sbin, /bin, /usr/sbin, and /usr/bin.相关的改变。

在一些 linux 版本中，这个分析可以通过内置的“check-packages”脚本完成。

3、不正常的网络使用情况

查看混杂模式，也就是监听模式。

```
# ip link | grep PROMISC
```

注意，在 linux 内核 2.4 版本中，ifconfig 不能真正检测到混杂模式，所以建议用 ip link 命令

查看不正常的监听端口：

```
# netstat -nap
```

获取正在运行的进程监听的端口：

```
# lsof -i
```

这些命令需要你知道，系统上通常使用哪些 TCP 和 UDP 端口。从中找出异常的端口。

查找不正常的 ARP 记录，局域网中不正确的 IP 和 MAC 的映射。

```
# arp -a
```

这个分析，需要知道在局域网上应该出现哪些 IP 地址。在小型或特殊的局域网（比如 DMZ 上），查找异常的 IP 地址。

4、不正常的计划任务

查找被 root 或者其他 UID 是 0 的账号设立的计划任务：

```
# crontab -u root -l
```

查找不正常的系统级别的计划任务：

```
# cat /etc/crontab
# ls /etc/cron.*
```

5、不正常的系统账号

查看 /etc/passwd 中的新账号，按照 UID 排序。

```
# sort -nk3 -t: /etc/passwd | less
```

查看其中的新账号，异常的账号，特别是 UID 小于 500 的。

也要注意查看 UID 为 0 的异样账号

```
# egrep ':0+:' /etc/passwd
```

在使用多重认证的方法的系统上使用以下命令：

```
# getent passwd | egrep ':0+:'
```

查找孤立文件，那可能是攻击者删除了的临时账号的一些踪迹。

```
# find / -nouser -print
```

6、不正常的日志记录

检查系统日志文件以查找恶意事件，包括：

"entered promiscuous mode" 包含了“进入混杂模式”关键词的日志
大量本地或远程访问工具的失败认证或登录事件（例如 telnetd，sshd，等）
包含大量（>20）奇怪字符的远程调用（RPC）日志（如， ^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM）
对于运行了 Web 服务器的系统：大于正常数量的错误日志
系统重新启动或应用程序重新启动日志

7、其他不正常内容

系统性能迟滞：

```
$ uptime - 看“平均负载”
```

内存过多使用：

```
$ free
```

可用磁盘空间的突然减少：

```
$ df
```

8、工具推荐

下面的工具通常不是内置在 Linux 操作系统中的，但可以用来更详细地分析它的安全状态。可在网站上免费下载。
Chkrootkit 查用户模式和内核模式 rootkit 引起的系统异常：
www.chkrootkit.org
Tripwire 寻找关键系统文件的变化：www.tripwire.org
AIDE 查看系统关键文件变化：http://www.cs.tut.fi/~rammer/aide.html
Linux 加固指南：www.cisecurity.org
自动化 Linux 系统的安全加固脚本：www.bastille-linux.org