如何监视和清除网络中非法计算机的入侵

金一长（工商银行浙江省绍兴市分行 312000）

本文假设计算机A遭到了计算机B和计算机C用telnet方式的登录，其中计算机A，计算机B，计算机C的地址分别为：170.88.36.237，170.88.36.108，170.88.36.109。而计算机A只允许计算机B的登录，不允许计算机C的登录。我们的目的是要在计算机A中保留计算机B的登录而清除计算机C的入侵。

1 检测计算机A是否遭到了其他计算机的登录，并获取登录者的进程号

在计算机A中输入如下命令：

#ps -elgrep telnetd

显示：1357 ? 0:00 telnetd

1383 ? 0:00 telnetd

从以上显示可见：计算机A已遭到其他计算机用telnet方式的两次登录，登录者的进程号分别是1357和1383。如果没有显示，则说明没有其他计算机用telnet方式的登录。如果要检测是否遭到了其他计算机用rlogin，ftp等方式的登录，可用以下命令：

#ps -elgrep rlogind

#ps -elgrep ftpd

2 获取登录到计算机A中的其他计算机的地址

在计算机A中输入如下命令：

#netstat -nlgrep ESTABLISHED

显示：

tcp 0 0 170.88.36.237.23 170.88.36.109.1242 ESTABLISHED

tcp 0 0 170.88.36.237.23 170.88.36.108.1488 ESTABLISHED

以上两行中第四个字段中170.88.36.237是本地计算机地址，23表示用telnet方式登录，如果用rlogin登录则该数值为153，如用ftp登录则为21；第五个字段中170.88.36.109和170.88.36.108为登录计算机的地址。

3 清除非法计算机的入侵

通过以上两步我们已经获取了登录到计算机A的登录者的地址和进程，但是这些信息是由两个不同的命令分别获得的，要想清除非法计算机的登录，还必须把登录者的地址和进程一一对应起来，否则就可能把允许登录的计算机清除掉。经过仔细分析发现，命令netstat -nlgrep ESTABLISHED是按登录者的先后逆序显示的。也就是第一行显示的是最后登录者的地址等信息，最后一行则显示最先登录者的信息，中间的则依次类推。而登录者的进程则是根据登录的先后顺序由计算机自动从小到大生成，这样，我们就可以把登录者的地址和进程逐一对应起来：netstat -nlgrep ESTABLISHED命令显示的第一行信息的登录者地址对应于最大的登录者进程；显示的第二行地址则对应第二大登录者进程；以下依次类推。例如本文所例举的两个登录者中，地址170.88.36.109对应进程号1383，地址170.88.36.108则对应进程号1357。由于不允许地址为170.88.36.109的计算机的登录，所以只要键入命令kill -9 1383就可以清除该计算机的非法入侵。

4 特殊情况的处理

如果一台服务器启动了多个业务程序，而这些程序需要消耗大量的进程，那么就有可能出现一种特殊情况：进程号小的不一定是系统先生成的，反之进程号大的不一定后生成，这是因为系统需要消耗大量的进程，当进程号超过系统定义的最大值(如30000)时，系统就会自动从0开始重新生成进程号。在这种情况下，我们就不能用第三步介绍的方法来清除非法计算机的入侵，而应该采用如下方法：

（下转第50页）

（上接第 51 页）

在被登录的计算机上输入命令：

#ps -ef|grep telnetd|grep -v gre

显示如下：

root 4193 317 0 09:13:48 ? 00:00:00 telnetd

root 175 317 0 09:54:20 ? 00:00:00 telnetd

其中时间为 09:13:48 的进程 4193 为先登录者的进程，对应 netstat -n|grep ESTABLISHED 命令中的地址为 170.88.36.108;而时间为 09:54:20 的进程 175 则为后者，对应 netstat -n|grep ESTABLISHED 命令中的地址为 170.88.36.109，清除非法计算机 170.88.36.109 登录的命令应为:kill -9 175。

更为复杂的是:如果上述两个进程的时间恰好相等，就需要对进程号间的差值进行判断。假如两个进程号之间的差值小于10000,可以直接按第三步的方法进行处理；假如其差值大于等于10000,应与第三步方法相反，即进程号大者属于先登录者，进程号小者属于后登录者。

通过以上方法就可以比较准确地清除掉那些用 telnet,rlogin, ftp等方式登录到自己所管理的服务器中的非法入侵者，确保服务器的安全运行。

本方法不仅适用于对企业内部局域网的管理，同样适用于接入 internet 的 UNIX 服务器的管理。■