清除Linux系统上的蠕虫程序Ramen PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022__E6_B8_85_E9_99_A4Linu_c103_145036.htm Linux系统中出现了一种称之为Ramen的蠕虫程序。它可能会入侵数千台运行RedHat 6.2/7.0 操作系统的服务器。Ramen利用了两个已知的Linux安全漏洞。它首先利用 RPC.statd 和 wu-FTP 的漏洞扫描网络上使用 RedHat 6.2/7.0 的服务器，然后尝试取得系统权限，一旦取得之后，会将一些一般的系统服务加以替换，并且将一个称之为“ root kit ”的程序码植入安全漏洞中，此外 Ramen 还会将站点上的首页给换成 : “ RameNCrew--Hackers looooooooooooove noodles ”的字样。最后，Ramen会寄两封信给两个电子信箱，并且开始入侵其他的RedHat服务器。Ramen只针对RedHat来进行侵入,不过危害不大，但是传播的速度却惊人，15分钟内可以扫描约 130,000 个站点。 Ramen是很善良的,在攻击完成后会自动把它攻击的3个漏洞给修补上(Redhat 6.2的rpc.statd、wu-ftpd,Redhat7.0的lpd),但是会在系统上起一个进程扫描下面的机器,会占去大量网络带宽。由此可能造成其他的主机的误会以及大量占用网络带宽，使系统瘫痪。 我们可以看出，该程序其实并不能称为病毒，而是一个利用了安全漏洞的类似蠕虫的程序。该程序的作者Randy Barrett也站出来声明说，这只是一个安全漏洞，类似于这样的安全漏洞在各种网络服务器上都存在，他在写Ramen程序的时候也不是针对Linux的。 防治的方法很简单,请升级你的redhat 6.2的 nfs-utils , wu-ftpd , redhat 7.0的LPRng,具体下载可以到ftp://0updates.redhat.com/。 检查系统是否被该程序侵入

的方法是，看看有没有/usr/src/.poop这个目录被建立，以及27374端口是否被打开，如果有的话就表明已经被Ramen侵入了。 看一个系统是否感染了Ramen蠕虫，主要基于以下几点： 1. 存在/usr/src/.poop目录 2. 存在/sbin/asp文件 3. 本地端口27374被打开（用netstat -an命令） 