 在UNIX系统遭受入侵后，确定损失及入侵者的攻击源地址相当重要。虽然在大多数入侵者懂得使用曾被攻陷的计算机作为跳板来攻击你的服务器，但是他们发动正式攻击前所做的目标信息收集工作(试探性扫描)常常是从他们的工作计算机开始的，下面介绍如何从遭受入侵的系统的日志中分析出入侵者的IP并加以确定的。 1. messages /var/adm是UNIX的日志目录(Linux下则是/var/log)。其中有相当多ASCII格式的日志文件，当然，让我们把焦点首先集中在messages个文件上，这一般也是入侵者所关注的文件，它记录了来自系统级别的信息。下面是显示版权或者硬件信息的记录信息： Apr 29 19：06：47 www login[28845]： FAILED LOGIN 1 FROM xxx.xxx.xxx.xxx ， User not known to the underlying authentication module 这是登录失败的记录信息： Apr 29 22：05：45 game PAM_pwdb[29509]： (login) session opened for user ncx by (uid=0)。 第一步应该是 Kill -HUP cat `/var/run/syslogd.pid`，当然，有可能入侵者已经做过了。 2. wtmp，utmp logs，FTP日志 你可以在/var/adm ，/var/log，/etc目录中找到名为wtmp，utmp的文件，这些文件记录着用户是何时、何地远程登陆到主机上的，在黑客软件中有一个最老也是最流行的zap2(编译后的文件名一般叫做z2，或者叫wipe)，也是用来“ 抹 ”掉在这两个文件中用户登录的信息的，然而由于懒惰或者网络速度过于缓慢，很多入侵者没有上载或编译这个文件。管理员可以使用lastlog这个

命令来获得入侵者上次连接的源地址(当然，这个地址有可能是他们的一个跳板)。FTP日志一般是/var/log/xferlog，该文件详细的记录了以FTP 方式上传文件的时间、来源、文件名等等，不过由于该日志太明显，所以稍微高明些的入侵者几乎不会使用FTP来传文件，他们一般使用的是RCP。 3. sh_history 获得 root 权限后，入侵者就可以建立他们自己的入侵帐号，更高级的技巧是给类似 uucp，lp 等不常使用的系统用户名加上密码。在遭受入侵后，即使入侵者删除了.sh_history 或者.bash_hi-story 这样的文件，执行kill -HUP `cat /var/run/inetd.conf`即可将保留在内存页中的bash命令记录重新写回到磁盘，然后可执行find / -name.sh_historyprint，仔细查看每个可疑的 shell 命令日志。你可在/usr/spool/lp(lp home dir)，/usr/lib/uucp/等目录下找到.sh_history 文件，还有可能在其中发现类似 FTP xxx.xxx.xxx.xxx 或者rcpnobody@xxx.xxx.xxx.xxx：/tmp/backdoor /tmp/backdoor 这样能显示出入侵者IP或域名的命令。 4. HTTP服务器日志 这是确定入侵者的真实攻击发源地址的最有效方法了。以最流行的Apache服务器为例，在$/logs/目录下你可以发现access.log这个文件，该文件记载了访问者的IP，访问的时间和请求访问的内容。在遭受入侵后，我们应该可以在该文件中发现类似下面的信息： record ：xxx.xxx.xxx.xxx[28/Apr/2000：00：29：05 -0800] "GET/cgi-bin/rguest.exe"404 -xxx.xxx.xxx.xxx[28/Apr/2000：00：28：57 -0800] "GET /msads/Samples/SELECTOR/showcode.asp" 404 这表明是来自 IP 为 xxx.xxx.xxx.xxx的入侵者在 2000 年 4 月 28 号的 0 点 28 分试

图访问/msads/Samples/SELECTOR/showcode.asp文件，这是在使用web cgi扫描器后遗留下的日志。大部分的web扫描器的入侵者常选择离自己最近的服务器。结合攻击时间和IP，我们就可以知道入侵者的大量信息。 5. 核心dump 一个安全稳定的守护进程在正常运行的时候是不会“ dump ”出系统的核心的，当入侵者利用远程漏洞攻击时，许多服务正在执行一个getpeername的socket 函数调用，因此入侵者的IP也保存在内存中。 6. 代理服务器日志 代理服务器是大中型企业网常使用来做为内外信息交换的一个接口，它忠实地记录着每一个用户所访问 的内容，当然也包括入侵者的访问信息。以最常用的squid代理为例，通常你可以在/usr/local/squid/logs/下找到access.log 这个庞大的日志文件。你可以在以下地址获得 squid 的日志分析脚本：http ：//www.squid-cache.org/Doc/Users-Guide/added/st .html 通过对敏感文件访问日志的分析，可以知道何人在何时访问了这些本该保密的内容。 7. 路由器日志 默认方式下路由器不会记录任何扫描和登录，因此入侵者常用它做跳板来进行攻击。如果你的企业网被划分为军事区和非军事区的话，添加路由器的日志记录将有助于日后追踪入侵者。更重要的是，对于管理员 来说，这样的设置能确定攻击者到底是内贼还是外盗。当然，你需要额外的一台服务器来放置router.log文件。 注意! 对于入侵者来说，在实施攻击的整个过程中不与目标机试图建立TCP连接是不太可能的，这里有许多入侵者主观和客观原因，而且在实施攻击中不留下日志也是相当困难的。百考试题－全国最大教育类网站(www．Examda。com) 如果我们花上足够的时间和精力，是可以从大量的日志中分析出入侵

者的信息。就入侵者的行为心理而言， 们在目标机上取得的权限越大，他们就越倾向于使用保守的方式来建立与目标机的连接。仔细分析早期的日志，尤其是包含有扫描的部分，我们能有更大的收获。 日志审计只是作为入侵后的被动防御手段，主动的是加强自身的学习，及时升级或更新系统，做到有备无患才是最有效的防止入侵的方法。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com