系统后门

系统后门一般是指那些绕过安全性控制而获取对程序或系统访问权的程序方法。在软件的开发阶段，程序员常常会在软件内创建后门程序以便可以修改程序设计中的缺陷。但是，如果这些后门被其他人知道，或是在发布软件之前没有删除后门程序，那么它就成了安全风险，容易被黑客当成漏洞进行攻击。

作用

大多数入侵者的后门实现以下二到三个目的:

即使管理员通过改变所有密码类似的方法来提高安全性，仍然能再次侵入，使再次侵入被发现的可能性减至最低。大多数后门设法躲过日志，大多数情况下即使入侵者正在使用系统也无法显示他已在线. 一些情况下，如果入侵者认为管理员可能会检测到已经安装的后门，他们以系统的 脆弱性作为唯一的后门，重而反复攻破机器. 这也不会引起管理员的注意. 所以在 这样的情况下，一台机器的脆弱性是它唯一未被注意的后门.

类型

密码破解后门

这是入侵者使用的最早也是最老的方法，它不仅可以获得对 Unix 机器的访问，而且可以通过破解密码制造后门. 这就是破解口令薄弱的帐号. 以后即使管理员封了入侵者的当前帐号,这些新的帐号仍然可能是重新侵入的后门. 多数情况下，入侵者寻找口令薄弱的未使用帐号,然后将口令改的难些. 当管理员寻找口令薄弱的帐号是，也不会发现这些密码已修改的帐号.因而管理员很难确定查封哪个帐号.

Rhosts + + **后门**

在连网的 Unix 机器中,象 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. 用户可以轻易的改变设置而不需口令就能进入. 入侵者只要向可以访问的某用户的 rhosts 文件中输入"+ +", 就可以允许任何人从任何地方无须口令便能进入这个帐号. 特别当 home 目录通过 NFS 向外共享时, 入侵者更热中于此. 这些帐号也成了入侵者再次侵入的后门. 许多人更喜欢使用 Rsh, 因为它通常缺少日志能力. 许多管

理员经常检查 "+ +", 所以入侵者实际上多设置来自网上的另一个帐号的主机名和用户名,从而不易被发现.

校验和及时间戳后门

早期,许多入侵者用自己的 trojan 程序替代二进制文件. 系统管理员便依靠时间戳和系统校验和的程序辨别一个二进制文件是否已被改变, 如 Unix 里的 sum 程序. 入侵者又发展了使 trojan 文件和原文件时间戳同步的新技术. 它是这样实现的: 先将系统时钟拨回到原文件时间, 然后调整 trojan 文件的时间为系统时间. 一旦二进制 trojan 文件与原来的精确同步, 就可以把系统时间设回当前时间. sum 程序是基于 CRC 校验, 很容易

骗过.入侵者设计出了可以将 trojan 的校验和调整到原文件的校验和的程序. MD5 是被大多数人推荐的,MD5 使用的算法目前还没人能骗过.

Login **后门**

在 Unix 里,login 程序通常用来对 telnet 来的用户进行口令验证. 入侵者获取 login.c 的原代码并修改,使它在比较输入口令与存储口令时先检查后门口令. 如果用户敲入后门口令,它将忽视管理员设置的口令让你长驱直入. 这将允许入侵

者进入任何帐号,甚至是 root.由于后门口令是在用户真实登录并被日志记录到 utmp 和 wtmp 前产生一个访问的，所以入侵者可以登录获取 shell 却不会暴露该帐号．管理员注意到这种后门后，便

用"strings"命令搜索 login 程序以寻找文本信息．许多情况下后门口令会原形毕露.入侵者就开始加密或者更好的隐藏口令，使 strings 命令失效．所以更多的管理员是用 MD5 校验和检测这种后门的.

Telnetd **后门**

当用户 telnet 到系统，监听端口的 inetd 服务接受连接随后递给 in.telnetd，由它运行 login.一些入侵者知道管理员会检查 login 是否被修改，就着手修改 in.telnetd.在 in.telnetd 内部有一些对用户信息的检验，比如用户使用了何种终端．典型的终端设置是 Xterm 或者 VT100.入侵者可以做这样的后门，当终端设置为"letmein"时产生一个不要任何验证的 shell．入侵者已对某些服务作了后门，对来自特定源端口的连接产生一个 shell．

服务后门

几乎所有网络服务曾被入侵者作过后门. finger, rsh, rexec, rlogin, ftp，甚至 inetd 等等的作了的版本随处多是．有的只是连接到某个 TCP 端口的 shell,通过后门口令就能获取访问.这些程序有时用刺娲□？ucp 这样不用的服务,或者被加入 inetd.conf 作为一个新的服务.管理员应该非常注意那些服务正在运行，并用 MD5 对原服务程序做校验.