经典后门实例之网页后门

从后门的技术角度来看，后门可以分为网页后门、线程插入后门、拓展后门等，本篇主要详细介绍网页后门的使用并且通过著名的网页后门软件海阳顶端为大家提升网页后门的安全知识。

后门作为黑客入侵的经典工具，不仅应该被黑客所熟识，网络管理员也应该掌握后门技术，以方便对后门入侵的防范与管控。后门根据技术分类可以分成很多种，本篇文章就着重介绍网页后门及网页后门的知名软件。

网页后门

近段时间网络上针对系统漏洞的攻击事件渐渐少了，因为大家在认识到网络安全的重要性之后，最简单却又最有效的防护办法：升级，都被大家所认同，所以系统漏洞在以后的岁月中存活的周期会越来越短，而从最近的趋势来看，肢本漏洞已经渐渐取代了系统漏洞的地位，非常多的人开始研究起却本漏洞来，sql 注入也开始成为各大安全站点首要关注热点，而说到脚本、网页后门当然就是不得不说的重头戏了，现在国内入侵的主流趋势是先利用某种脚本漏洞上传脚本后门，然后浏览服务器内安装和程序，找到提升权限的突破口，进而拿到服务器的系统权限。

海阳顶端 ASP 木马

这是 ASP 脚本方面流传非常广的一个脚本后门了，在经过几次大的改革后，推出了“海阳顶端 ASP 木马 XP 版”、“海阳顶端 ASP 木马红粉佳人版”等功能强大、使用方便的后门，想念经常接解脚步本安全的朋友对这些都不会陌生。

类型：网页木马

使用范围：支持 ASP、WEB 访问

隐蔽程序：★★★★☆

使用难度：★☆☆☆☆

危害程序：★★★☆☆

查杀难度：★★★☆☆

现在的服务器系统配置都相对安全，公开的系统漏洞存在的机会很少，于是脚本方面的漏洞就开始火起来。首先我们通过某种途径获得一个服务器的页面权限(比如利用论坛上传达室类型未严格设置、SQL 注入后获得 ASP 系统的上传权限、对已知物理路径的服务器上传特定程序) ,然后我们可以通过简单的上传 ASP 程序或者是直接复制海阳项端的代码，然后通过 WEB 访问这个程序，就能很方便地查阅服务器上的资料了，下面举个简单的便子(由于只是简单的介绍，下文便子不会太难或者太普遍，希望大家理解)。

运用举便

leadbbs2.77 曾经风靡网络 ,它是个很典型的 ASP 论坛 ,屏蔽了很多可以 SQL 注入的寺方 ,但是很多傻瓜级别的网络管理员总是喜欢默认安装 ,然后启用论坛，我们只需要很简单地在 IE 中输入：WWW。***。COM/BBS/DATA/LEADBBS。MDB 就能够直接下载该论坛的数据库了，而且没有 MD5 加密哦!，我们直接找到管理员的账户和密码，然后登录论坛，到管理界面将论坛的“联系我们”、“帮助”等 ASP 文件替换成我们的海阳项端代码，然后执行 GUEST 权限的 CMD 命令，方便的上传/下载将定程序、远程执行程序等，这样一个隐藏的后门就建好了!取得服务器的 SYSTEM 权限就看大家自己的办法了。

一般来讲，海洋的功能是非常强大的，而且不容易被查杀(一个朋友采取的方式是：先利用某个脚本漏洞上传网页后门，再通过海洋上传另一个后门到隐蔽的路径，然后通过最后上传的后门来删除第一次上传的海洋，这样后门的存放路径就可以放得非常深了，普通管理员是很难发现的)，如果管理员觉得自己可能中了这里边样的后门，可以利用论坛备份来恢复自己的页面系统，再配合系统日志、论坛日志等程序检查系统，发现可疑 ASP 文件打开看看海洋是很好识别的，再删除就可以了。

脚本方面的网页后门还有 CGI 和 PHP 两面三刀大类，使用原理都差不多，这里就不再多介绍，在黑防论坛也收录了这三种后门，大家可以下载后自己研究。