后门程序

后门程序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。

原理

后门程序就是留在计算机系统中，供某位特殊使用者通过某种特殊方式控制计算机系统的途径。

后门程序，跟我们通常所说的"木马"有联系也有区别。联系在于：都是隐藏在用户系统中向外发送信息,而且本身具有一定权限,以便远程机器对本机的控制。区别在于：木马是一个完整的软件,而后门则体积较小且功能都很单一。后门程序类似于特洛依木马（简称"木马"），其用途在于潜伏在电脑中，从事搜集信息或便于黑客进入的动作。

后门程序和电脑病毒最大的差别，在于后门程序不一定有自我复制的动作，也就是后门程序不一定会“感染”其它电脑。

后门是一种登录系统的方法，它不仅绕过系统已有的安全设置，而且还能挫败系统上各种增强的安全设置。

而且,在病毒命名中，后门一般带有 backdoor 字样，而木马一般则是 Trojan 字样。

特点

后门包括从简单到奇特，有很多的类型。简单的后门可能只是建立一个新的账号，或者接管一个很少使用的账号;复杂的后门(包括木马)可能会绕过系统的安全认证而对系统有安全存取权。例如一个 login 程序，当你输入特定的密码时，你就能以管理员的权限来存取系统。

后门能相互关联，而且这个 技术被许多黑客所使用。例如，黑客可能使用密码破解一个或多个账号密码，黑客可能会建立一个或多个账号。一个黑客可以存取这个系统，黑客可能使用一些 技术或利用系统的某个漏洞来提升权限。黑客可能会对系统的配置文件进行小部分的修改，以降低系统的防卫性能。也可能会安装一个木马程序，使系统打开一个安全漏洞，以利于黑客完全掌握系统。

分类

后门可以按照很多方式来分类，标准不同自然分类就不同，为了便于大家理解，我们从技术方面来考虑后门程序的分类方法：

网页后门

此类后门程序一般都是服务器上正常 的 web 服务来构造自己的连接方式，比如非常流行的 ASP、cgi 脚本后门等。

网页后门，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，脚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脚本漏洞来，sql 注入也开始成为各大安全站点首要关注热点，找到提升权限的突破口，进而拿到服务器的系统权限。

asp、CGI、PHP 这三个脚本大类在网络上的普遍运用带来了脚本后门在这三方面的发展。

线程插入后门

利用系统自身的某个服务或者线程，将后门程序插入到其中，具体原理原来《黑客防线》曾具体讲解过，感兴趣的朋友可以查阅。这也是现在最流行的一个后门技术。

扩展后门

所谓的“扩展”，是指在功能上有大的提升，比普通的单一功能的后门有很强的使用性，这种后门本身就相当于一个小的安全工具包，能实现非常多的常见安全功能，适合新手使用————但是，功能越强，个人觉得反而脱离了后门“隐蔽”的初衷，具体看法就看各位使用者的喜好了。

c/s 后门

和传统的木马程序类似的控制方法，采用“客户端/服务端”的控制方式，通过某种特定的访问方式来启动后门进而控制服务器。