浅谈后门的概念与分类

本文通过介绍后门的概念以及举例说明网页后门、线程插入后门、扩展后门、c/s 后门以及 root kit 五种后门对后门有一个全面的概述，使得众多的网络管理员及用户能够提高自己的安全防范意识。

在网络安全的领域里，常听闻后门、木马云云，黑客在进行网络入侵活动时，常常在被入侵者系统中放置后门。对于企业的网络管理员来说，后门也是企业网络安全的死敌。那么究竟什么是后门，后门又有哪几种呢？本文就将为您介绍后门的概念和其几种分类方式。

后门的概念

后门程序又称特洛伊木马，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”其他电脑。

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。

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。

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，你当输入特定的密码时，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。黑客可能使用一些技术或利用系统的某个漏洞庭湖来提升权限。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。

以上是在网络上常见的对“后门”的解释，其实我们可以用很简单的一句话来概括它：后门就是留在计算机系统中，供某位特殊使用都通过某种特殊方式控制计算机系统的途径!——很显然，掌握好后门技术是每个网络安全爱好者不可或缺的一项基本技能!它能让你牢牢抓住肉鸡，让它永远飞不出你的五指山!

下文将以笔者从事网络安全多年的工作经验为基础，给广大的网络初级安全爱好者讲解一些网络上常用的后门的种类，希望大家能在最短的时间内学习到最好的技术，提升自己的网络安全技术水平!

后门的分类

我们了解后门的概念之后，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：

1.**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，比如现在非常流行的 ASP、cgi 脚本后门等。

2 **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。

3 **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，能实现非常多的常驻见安全功能，适合新手使用————但是，功能越强，个人觉得反而脱郭后门“隐蔽”的初衷，具体看法就看各位使用都的喜好了。

4.c/s **后门**

和传统的木马程序类似的控制方法，采用“客记端/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。

5.root kit

这个需要单独说明，其实把它单独列一个类在这里是不太恰当的，但是，root kit 的出现大大改变了后门程序的思维角度和使用理念，可以说一个好的 root kit 就是一个完全的系统杀手!后文我们讲涉及到这方面，想念一定不会让大家失望!

上面是按照技术做的分类，除了这些方面，正向连接后门、反向连接后门等分类也是很常见的，其实如何分类是编程者考虑的事，广大的使用者就不用考虑那么多了，我们看重的，只是功能!