 对网络服务器的恶意网络行为包括两个方面：一是恶意的攻击行为，如拒绝服务攻击，网络病毒等等，这些行为旨在消耗服务器资源，影响服务器的正常运作，甚至服务器所在网络的瘫痪.另外一个就是恶意的入侵行为，这种行为更是会导致服务器敏感信息泄露，入侵者更是可以为所欲为，肆意破坏服务器。所以我们要保证网络服务器的安全可以说就是尽量减少网络服务器受这两种行为的影响。 如何避免恶意攻击行为 (一) 构建好你的硬件安全防御系统 选用一套好的安全系统模型。一套完善的安全模型应该包括以下一些必要的组件：防火墙、入侵检测系统、路由系统等。 防火墙在安全系统中扮演一个保安的角色，可以很大程度上保证来自网络的非法访问以及数据流量攻击，如拒绝服务攻击等.入侵检测系统则是扮演一个监视器的角色，监视你的服务器出入口，非常智能地过滤掉那些带有入侵和攻击性质的访问。 (二) 选用英文的操作系统 要知道，windows毕竟美国微软的东西，而微软的东西一向都是以Bug 和 Patch多而着称，中文版的Bug远远要比英文版多，而中文版的补丁向来是比英文版出的晚，也就是说，如果你的服务器上装的是中文版的windows系统，微软漏洞公布之后你还需要等上一段时间才能打好补丁，也许黑客、病毒就利用这段时间入侵了你的系统。 如何防止黑客入侵 首先，世界上没有绝对安全的系统。我们只可以尽量避免被入侵，最大的程度上减少伤亡。 (一) 采用NTFS文件系统格式 大家都知道

，我们通常采用的文件系统是FAT或者FAT32，NTFS是微软Windows NT内核的系列操作系统支持的、一个特别为网络和磁盘配额、文件加密等管理安全特性设计的磁盘格式。NTFS文件系统里你可以为任何一个磁盘分区单独设置访问权限。把你自己的敏感信息和服务信息分别放在不同的磁盘分区。这样即使黑客通过某些方法获得你的服务文件所在磁盘分区的访问权限，还需要想方设法突破系统的安全设置才能进一步访问到保存在其他磁盘上的敏感信息。 (二)做好系统备份 常言道，“ 有备无患 ”，虽然谁都不希望系统突然遭到破坏，但是不怕一万，就怕万一，作好服务器系统备份，万一遭破坏的时候也可以及时恢复。 (三) 关闭不必要的服务，只开该开的端口 关闭那些不必要开的服务，做好本地管理和组管理。Windows系统有很多默认的服务其实没必要开的，甚至可以说是危险的，比如：默认的共享远程注册表访问(Remote Registry Service)，系统很多敏感的信息都是写在注册表里的，如pcanywhere的加密密码等。 关闭那些不必要的端口。一些看似不必要的端口，确可以向黑客透露许多操作系统的敏感信息，如windows 2000 server默认开启的IIS服务就告诉对方你的操作系统是windows 2000。69端口告诉黑客你的操作系统极有可能是linux或者unix系统，因为69是这些操作系统下默认的tftp服务使用的端口。对端口的进一步访问，还可以返回该服务器上软件及其版本的一些信息，这些对黑客的入侵都提供了很大的帮助。此外，开启的端口更有可能成为黑客进入服务器的门户。 总之，做好TCP/IP端口过滤不但有助于防止黑客入侵，而且对防止病毒也有一定的帮助。 (四)软件防火墙、杀毒软件 虽然我们已经有了一套硬件的防御

系统，但是“ 保镖 ”多几个也不是坏事。 (五)开启你的事件日志 虽然开启日志服务虽然说对阻止黑客的入侵并没有直接的作用，但是通过他记录黑客的行踪，我们可以分析入侵者在我们的系统上到底做过什么手脚，给我们的系统到底造成了哪些破坏及隐患，黑客到底在我们的系统上留了什么样的后门，我们的服务器到底还存在哪些安全漏洞等等。如果你是高手的话，你还可以设置密罐，等待黑客来入侵，在他入侵的时候把他逮个正着。 编辑特别推荐: 轻松部署Windows2003的DHCP和DNS Windows系统十大病毒藏身之处 如何改进存储利用率节约空间 网上冲浪怎样才能最high