高校校园网络的安全管理研究

马弘伟[1] 史 娜[2]
（1、牡丹江师范学院，黑龙江 牡丹江 157011 2、黑龙江林业职业技术学院信息工程系，黑龙江 牡丹江 157011）

摘 要：文章对校园网络的安全管理进行研究，指出高校校园网络存在的安全隐患，并提出相应的防范措施。

关键词：校园网络；网络安全；网络管理

1 概述

如何减少网络漏洞及缺陷等安全隐患带来的弊端，更好的发挥校园网的功能，越来越受到人们的重视。

2 校园网络面临的威胁

2.1 操作系统的漏洞。对于超级用户是系统中权限最大的，它不仅可以管理其他用户，而且可以任意删除文件，一旦超级用户出现误操作，就有可能引起系统的崩溃。

2.2 口令破解。随着计算机硬件和软件技术的发展，使口令攻击更为有效，由于 CPU 的高速以及网络的普及和分段攻击算法的应用，使攻击者有了更加高效的破解手段。

2.3 计算机病毒。通过用户的交换磁盘以及网络传输，病毒就可以从一台计算机传播到另一台计算机。从而影响计算机使用，破坏计算机系统(如重映射键盘)，破坏硬盘中的内容或删除某种类型的文件等。

2.4 木马程序。当用户无意运行木马程序时，非法操作开始执行，然后通过网络使得编程者可以回收非法操作的结果，对用户造成损失。

2.5 后门。黑客们利用所安装的后门可以轻而易举的绕开系统管理员所设置的安全防护措施，获取系统访问权限。

2.6 网络攻击。网络攻击是指网络用户未经授权的访问或未经授权的使用等行为，其攻击目标主要是盗取信息、破坏和伪造数据以及使系统不能正常运行和提供服务等。在攻击实施阶段，根据是否拥有目标系统的控制权划分为两大类——入侵攻击和非入侵攻击。

2.7 社会工程攻击。社会工程攻击指攻击者通过某些社会活动，获得访问网络的信息，这是通过技术手段无法克服的安全问题。一些网络用户可能轻易地告诉别人关于网络的重要信息，或者是他人以贿赂或欺骗手段来获取网络口令及相关信息。

3 校园网络安全措施

在对网络和系统进行安全配置之前，首先要确定安全需求。即对于 ISO 的五项网络安全服务，应根据实际需要，确定出本系统重点提供的服务，有了安全需求之后，就可以对网络安全系统进行设计。

3.1 网络安全模型。传统的网络安全模型侧重于信息的安全，强调对信息的保护，随着网络入侵活动越来越频繁，面对网络安全实际的迫切要求，基于主动防御思想的可适应性动态网络安全模型逐渐地形成，这些模型的设计思想摆脱了目前网络安全体系设计简单的沿袭加密、签名、认证、防火墙等通用的网络安全模式，以承认漏洞、加强防护、实时检测、快速反应为指导思想，为计算机网络安全系统的设计与实现提供了有利的理论工具。其中典型的是 P2DR 模型和 PDRR 模型。

3.2 操作系统的选择。在确定网络安全模型之后，系统设置的第一步是选择安全性较好、漏洞少的操作系统。Linux 操作系统开放源代码，由全世界的 Linux 爱好者共同开发和更新，并在 Linux 内核基础上研究安全操作系统。因此它的漏洞和缺陷不断得到修补，使得系统更加完善。

3.3 系统的安全配置。在选择一个比较安全的操作系统后，对系统进行安全配置是很重要的一项工作，首先要注意的是在安装时不使用缺省的系统安装方式，而是根据系统的实际情况，只打开绝对必要的服务应用，关闭所用不需要的应用，如关闭 TFTP、NIS、部分 RCP 服务等，同时应加强已开启服务的安全性。对于一些存在有大量的安全漏洞，但是又常常是必须的重要服务器，如 sendmail、ftp 等，为安全起见，首先应减少提供这类服务的主机个数，如不是专门提供 Mail Server 和 FTP Server 的则不提供该服务；其次，对于必须提供服务的主机，则减少其他服务类型，以降低被组合攻击的风险；最后，应定期根据获得的安全信息修补相应的服务器。

3.4 口令保护。网络管理员应督促用户使用安全性高的口令，安全性高的口令包括：字母数字序列；大小写混合；采用特殊字符等。口令应当被存为加密文件或加密数据库，以防止某些用户读取其他用户的口令并使用这些口令登录。

3.5 防火墙。对于大型网络来说，网络中一些主机具有较高的性能和较低的安全需求(如服务器)而另一些主机则具有较低的性能和较高的安全需求(如普通 PC 机)。当使用防火墙后，将会降低前者的使用效率，提高后者的安全性。是否配置防火墙，即是在安全和效率之间的侧重与平衡。一般说来，对于中型或大型局域网都应设置防火墙，特别是那些内部主机安全管理不太严格的大型组织机构。

3.6 入侵检测系统。入侵检测是通过检查网络中传输的数据包信息，判断是否有违背安全策略或危及系统安全的行为或活动，从而保护系统不受外来的攻击，防止数据的泄露、篡改和破坏。入侵检测的目的不是阻止入侵的发生，而是在于发现入侵者和入侵行为，从而及时进行网络安全应急响应，避免对系统的恶意访问和破坏。入侵检测技术主要分为两大类型：异常入侵检测和误用入侵检测。

3.7 文件完整性检查。大多数情况下，黑客渗入系统后会立即修改某些系统文件以创建后门，如用准备好的替代物换掉系统中原有的 /bin/login 文件以使其不用口令便能登录系统；然后再修改某些文件，例如 /bin/ls 等，以便隐藏其行径。

文件完整性检查是检查文件系统是否被修改或某些文件是否被改动，可以使用 CRC 校验或 MD5 校验，帮助安全管理员发现什么文件被修改，是谁进行的修改，以判断系统是否遭受攻击。

3.8 备份。备份是指备份数据和完整的系统，当系统出现问题或崩溃时可用来快速恢复系统。定期进行备份非常重要，如不进行数据备份，那么可能会因一次硬盘错误、擦除或损坏而丢失系统所有的数据。当前最流行的备份网络系统的方法是磁带备份，该方法简单并且相对经济。

3.9 日志审计。日志记录了系统中发生的所有事件，并分等级存储，系统管理员可以通过检查日志的方式来查看系统是否存在异常情况或攻击行为。

3.10 用户培训。用户的培训与教育是加强网络安全的重要措施。网络管理员通过培训和教育用户，使得网络中的用户都熟悉网络的安全策略、安全配置，并指导用户实施安全口令，防止社会工程攻击。

4 结论

随着校园网络的不断发展，网络安全问题也将面临更大的考验，对于校园网络管理人员来说，一定要提高网络安全意识，加强网络安全管理，同时还应加强学生网络道德管理，规范上网行为，为高校师生营造一个良好的工作、学习环境。

参考文献

[1]高巍.大学校园网络高效配置与安全管理[M].北京：中国轻工业出版社.2012，9.

基金项目：牡丹江市科学技术计划项目(编号：Z2012S0050) 项目名称：大学校园网络高效配置与安全管理。

作者简介：马弘伟(1981.1-)，男，牡丹江师范学院讲师，硕士，研究方向：软件工程、网络。