计算机安全漏洞及防范研究*

李换双，潘 平，罗 辉
（贵州大学 计算机科学与信息学院，贵州 贵阳 550025）

摘 要：结合实际工作发现的安全漏洞，从访问控制、防火墙技术、病毒防范和入侵检测4个方面探讨了计算机网络安全防范措施。通过安全防范措施，保证了网络环境的安全，减少了被黑客攻击的可能性。

关键词：网络安全；计算机；漏洞；安全防范；黑客

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1674-7720(2013)07-0064-02

Computer security vulnerabilities and preventive measures

Li Huanshuang, Pan Ping, Luo Hui
(College of Computer Science & Information, Guizhou University, Guiyang 550025, China)

Abstract: The article combines with security vulnerabilities in practical work, discusses the computer network precaution measure from 4 aspects, including access control, firewall technology, intrusion detection and virus prevention. Through safety preventing, it ensures the network's safety and reduces the possibility of being attacked by hackers.

Key words: network security; computer; vulnerabilities; safety precautions; hacker

随着计算机技术和信息技术的迅猛发展，网络安全问题日渐显著。计算机网络向世界各个角落延伸，用户通过网络享受着巨大便利的同时，安全隐患令人担忧。近几年来网络攻击事件不断增多，计算机安全漏洞数量有增无减，因而造成的危害不断增多，影响恶劣，在一定程度上危害到人民群众的根本利益和社会经济发展的稳定性。但是，半数以上的攻击都是基于计算机本身存在的漏洞而进行的，各行业网络管理员及计算机用户应增强安全防范，构建完善的网络安全环境，科学地进行漏洞发现、漏洞分析及漏洞安全防范工作，避免造成不必要的损失。

1 计算机安全漏洞简单介绍

1.1 漏洞的定义

漏洞是在硬件、软件和协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

大多数用户对安全漏洞的概念或多或少会有一定的了解，但由于所处的领域不同、看待漏洞的角度不同和研究的程度不同，导致对漏洞的理解也不同。信息安全漏洞的最早定义是由美国著名的计算机安全专家DENNING D E R[1]博士于1982年提出的，他从访问控制角度，把漏洞定义为“导致操作系统执行的操作和访问控制矩阵所定义的安全策略之间相冲突的所有因素”。

1.2 漏洞的分类

当今世界每天所依赖的软件和网络应用确实存在着漏洞，这只是软件开发快速发展的必然结果。根据中国国家信息安全漏洞库(CNNVD)统计，2012年10月份新增安全漏洞772个，日平均新增漏洞数量约25个，与前5个月平均增长数量相比，增长速度有所上升。图1为近6个月漏洞新增数量统计图。

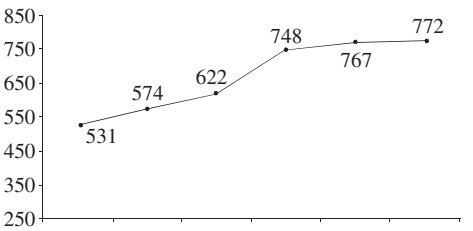


图1 2012年5月到2012年10月漏洞新增数量统计图

据析，新增漏洞主要为主流操作系统漏洞、TCP/IP协议缺陷漏洞及由安全策略引起的漏洞。

(1)操作系统本身漏洞及链路连接漏洞[2]

操作系统是一个人机交互便捷平台，要支持各种应

*基金项目：教育部信息安全类教育教学改革项目(JZW201211)

用，各种操作系统都存在着先天缺陷和不断增加新功能而带的漏洞。操作系统为用户提供的功能越多，应用越新，漏洞的数量及其存在漏洞的可能性越大，受到攻击的可能性越大；服务器或者 PC 安装的操作系统时期越长，用的人越多，暴露漏洞的概率越大，越容易受到攻击。黑客攻击防火墙或内部主机，一般都是先攻击操作系统，控制了操作系统就控制了防火墙或内部主机。计算机正常运行期间，需通过链路连接网络互通功能，一旦存在链接，相应的就会存在被攻击的可能性。链路连接攻击及基于数据链路的会话攻击等。

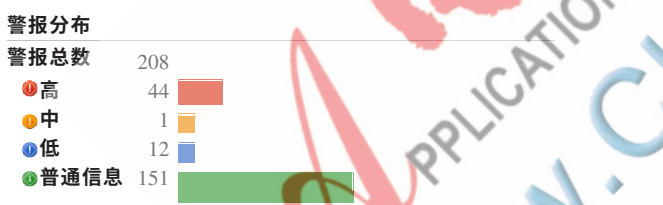
（2）TCP/IP 协议缺陷漏洞

TCP/IP 漏洞的根本所在就是目前其内在控制机制对源地址还无法进行有效的鉴别，无法证实 IP 地址准确无误地从哪里来。这就为网络攻击者利用侦听技术破坏计算机网络提供了很大的可能性，黑客利用此漏洞可以对数据进行检查，推测 TCP 的序列号，修改鉴别过程，插入非法数据流。

（3）安全策略漏洞

网络正常运行各项服务的正常开展都源于计算机端口开放功能。例如 80 端口开放，实现 HTTP 服务发挥功能；25 端口开放，则可以提供 SMTP 服务。端口正常开放，在给用户带来方便的同时，也增加了计算机遭受攻击的可能性，这时，传统的防火墙的防护功能已经显得苍白无力，很难发挥其有效的作用。

根据贵州省 2012 年信息安全评估示范项目过程中，漏洞扫描师对贵州省 ** 厅局进行的服务器外网漏洞扫描报告，分析得出漏洞分布情况如图 2 所示。



要点摘要

警报群组	严重程度	警报数量
ASP.NET Padding Oracle Vulnerability	High	1
Blind SQL Injection	High	43
HTML form without CSRF protection	Medium	1
ASP.NET debugging enabled	Low	2
Login page password-guessing attack	Low	1
Possible sensitive directories	Low	2
Slow response time	Low	7
Broken links	Informational	149
Password type input with autocomplete enabled	Informational	2

图 2 某服务器漏洞分布图

2 计算机安全漏洞防范措施

针对网络安全漏洞的类型，目前比较有效的防范措施主要有访问控制、防火墙技术、病毒防范和入侵检测技术等，其中对广大网络用户和网络管理员的安全培训也是至关重要的。

2.1 访问控制

针对操作系统本身漏洞，根据第三级安全标记保护级[3]主要从身份鉴别、自主访问控制、强制访问控制、数据流控制、安全审计、用户数据完整性和用户数据保密性进行功能加强。

2.2 防火墙技术

防火墙是设置在不同网络或网络安全域之间（可信网络与不可信网络）的一系列部件（软件与硬件）的组合，是目前最广泛、最经济有效的安全漏洞防范措施之一。通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制，从而防止不明身份黑客进入计算机用户网络，保护用户的信息免于遭受破坏。

2.3 防病毒技术

防病毒技术就是如何通过各种技术手段预防、查杀各种病毒代码，通过防范计算机遭受各种病毒（包括病毒、蠕虫、恶意代码、木马等）的感染、攻击和破坏，保证计算机的数据安全和应用安全。从防病毒产品的部署来看可分为主机型防病毒产品和网关型防病毒产品。防病毒网关设计安装在网络边缘，病毒侵入前进行实时地阻止，这样很好地解决了病毒在被单机防病毒软件查杀前已经进入网络的安全风险，且很好地避免了计算机用户不熟悉防病毒软件使用的风险[4]。

2.4 入侵检测技术

入侵检测系统具有更多的智能，它利用各种不同类型的引擎对系统进行实时或定期监控，获取系统的审计数据或网络数据包，然后将得到的数据进行分析，并判断系统或网络是否出现异常或入侵行为，一旦发现异常或入侵情况，发出报警并采取相应的保护措施。

2.5 加强网络管理员综合素质[5]

随着计算机防范技术的发展，黑客攻击技术水平也在不断提高，因此网络环境不存在绝对意义上的安全。应加强网络管理员安全培训，提高网络管理人员综合素质，健全安全管理。通过认识计算机安全漏洞、分析漏洞和加强防范措施，争取最大限度地确保计算机网络的安全性，减少被黑客攻击的可能性。

通过实践工作中发现的计算机安全漏洞并对其分析，找出其安全防范对策。主要从访问控制、防火墙、防病毒和入侵检测（正在发展为入侵防御）几个方面来加强防范，不给黑客留有可乘之机，确保网络用户的信息安全。

另外，在大型企业和政府部门，在服务器安全运维阶段，网络管理人员应对网络环境开展定期系统审计、漏洞扫描和渗透测试，进一步提升网络安全运维情况。在网络正常工作期间进行定期和不定期风险评估，以便

帮助确认网络环境保持的安全等级是否发生变化[6]。计算机安全漏洞及防范措施的研究是一项长期动态工作，需得到管理人员的鼎力支持，并具有继续研究下去的意义。

参考文献

[1] DENNING D E R. Crytography and data security[M]. USA, Boston: Addition-Wesley, 1982.

[2] 郑平.浅谈计算机网络安全漏洞及防范措施[J].计算机光盘软件与应用，2012(3)：31-46.

[3] GB/T20272-2006.信息安全技术操作系统安全技术要求[S].中国：中国国家质量监督检验检疫总局、中国国家标准化管理委员会，2006.

[4] 武春岭，李贺华.信息安全产品配置与应用[M].北京：电子工业出版社，2010.

[5] 倪灵芝.计算机网络安全漏洞及解决措施初探[J].信息与电脑，2012(1)：24-25.

[6] 范红.信息安全风险评估规范国家标准理解与实施[M].北京：中国标准出版社，2008.

（收稿日期：2012-12-02）

作者简介：

李换双，女，1986年生，硕士研究生，主要研究方向：信息安全。

潘平，男，1962年生，副教授，主要研究方向：信息处理及信息安全。