浅析计算机网络安全问题

柴天丽

（南皮县职业技术教育中心　河北　沧州　061500）

[摘　要]计算机网络的快速发展，给我们的日常生活带来了很大的便利，也对经济、文化与科学的发展产生了重要的影响，但是也不可避免地带来了一些新的社会、道德、政治与法律的问题。网络将彼此独立的计算机连在了一起，一旦出现安全问题，所产生的副作用也越来越大。因此，计算机网络安全是非常值得关注的，结合实际对计算机主要的安全隐患和防范措施我进行了详细探究，为提高计算机网络安全提供参考。

[关键词]计算机网络；病毒；黑客；防火墙

【DOI】10.12252/j.issn.2096-627X.2021.12.2189

网络为人们提供了很多的宝贵信息，使得人们可以不受地理位置与时间的限制，相互交换信息、合作研究、学习新的知识。但同时也存在着诸多的安全隐患，导致用户的信息和安全受到威胁，因此有关计算机网络安全问题的分析对广大计算机用户来说意义深远。

一、计算机网络安全的定义

从狭义上来说，网络安全是指计算机和网络系统的硬件、软件及其系统中的数据和信息资源受到保护，不因偶然或恶意原因而遭受破坏、威胁、泄露，能够让系统连续可靠正常地运行，并且网络服务不中断。

从广义上来说，只要是涉及计算机网络信息上的相关保密性、完整性、可用性和可控性的相关技术和理论都可以算是计算机网络安全的研究范畴。

二、计算机网络面临的威胁

计算机网络安全所面临的威胁主要可分为两大类：一是对网络中信息的威胁，二是对网络中设备的威胁。针对网络安全的威胁主要有以下内容：

（一）软件漏洞

软件漏洞是指硬件、软件等在策略上的缺陷，这种缺陷导致非法用户没有经过授权而访问系统或者突破权限来访问系统，因此造成一定程度上的网络安全的威胁。最常见的漏洞是缓冲区溢出，是由于研发人员预先分配缓冲区，来保存特殊的信息，并且在此过程中，代码没有对仔细地对比检查，因此临近的空间就会有被覆盖的风险，因而可以利用这一特点来导致程序崩溃，执行错误代码。

（二）计算机病毒

计算机病毒（Computer Virus）指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机正常使用并且能够自我复制的一组计算机指令。具有以下七大特点：传播性、隐蔽性、感染性、潜伏性、激发性、表现性和破坏性，并有一定的生命周期。

计算机病毒诞生于20世纪，经人为制造的对计算机具有破坏性的程序。它依附于其他的可执行程序之中，在计算机中病毒后，往往能够表现出机器运行速度减慢，甚至死机系统破坏，给用户带来损失。因此称这种具有破坏性作用的程序为病毒。

计算机病毒按存在的媒体分类可分为引导型病毒、文件型病毒和混合型病毒3种；按链接方式分类可分为源码型病毒、嵌入型病毒和操作系统型病毒等3种；按计算机病毒攻击的系统分类分为攻击DOS系统病毒，攻击Windows系统病毒，攻击UNIX系统的病毒。

（三）黑客

黑客最早产生于20世纪50年代，1994年以来，由于因特网的快速发展，提供了无限的自由和财富，信息时代充斥着生活，黑客出现了。

1.黑客的概念

“黑客”指的是喜爱钻研技术、精通计算机技术的程序员。有狂热的爱好兴趣伴随着执着的追求。发现计算机或者网络中的漏洞。然后向管理员提出解决和修补漏洞的方法。他们不受政治利用。并且推动了计算机和网络的发展。正是因为有了黑客的维护，才能一步一步的健全计算机技术。于是这些黑客有了新的称呼——“ 骇客”。后来又细分为白帽黑客（比如网络安全领域专家）、灰帽黑客（游走于法律的灰色地带）、黑帽黑客（窃取隐私和信息、搞黑色产业）。

2.黑客攻击方式

①网络报文嗅探

网络报文嗅探主要是指黑客利用采用网络监听的方式来获取用户的信息，利用用户信息侵入用户的计算机网络。并对用户的关键信息进行修改，比如修改用户的账号信息和密码等。同时也会在日后继续侵入该网络埋下隐患。

②放置木马程序

黑客会在网络中放置一些木马程序，例如蠕虫病毒等。蠕虫病毒利用网络进行复制和传播，传染途径是通过网络和电子邮件。最初的蠕虫病毒定义是因为在DOS环境下，病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形。

蠕虫病毒是自包含的程序（或是一套程序），它能传播它自身功能的拷贝或它的某些部分到其他的计算机系统中（通常是经过网络连接）。请注意，与一般病毒不同，蠕虫不需要将其自身附着到宿主程序，蠕虫病毒一般是通过1434端口漏洞传播

③ip欺骗

ip欺骗是利用计算机和主机之间的关联而进行的。由于ip的不稳定性，因此很容易让黑客入侵主机的ip路径，因而会让用户发送的信息传送到黑客指定的ip地址上。通过这样的途径可以让黑客利用非法途径获取用户的信息，进而实施各种违法行为。

④web欺骗

web欺骗是一种电子欺骗。黑客在网络中国构建完整的web世界。达到以假乱真的效果，让用户误以为这是真实的。Web欺骗可以实现网络连接，能够控制计算机出现故障，线路故障等。很难解决计算机网络操作系统的安全隐患。基于计算机网络环境具有开放性、大跨度的特点，才会让黑客的入侵变的更容易。

⑤信息泄露、信息污染、信息泄密

例如资源未授权侵用，系统拒绝信息流和系统否认等。个人或者组织处于非法目的。进行信息的破坏，和意识形态的信息渗透等。甚至通过网络进行政治颠覆，使合法利益受到威胁。

三、计算机网络全的防范措施

（一）防火墙技术

防火墙是连接计算机与网络之间的软件，它可以实现计算机内部网络与外网之间的隔离，可以在一定程度上保护计算机。防火墙技术不仅可以在不同网络之间，控制网络安全之间的信息控制，同时还可以根据计算机使用的具体情况实现不同的安全策略。使用防火墙的好处有：保护脆弱的服务，控制对系统的访问，集中地安全管理，增强保密性，记录和统计网络利用数据以及非法使用数据情况。防火墙的设计通常有两种基本设计策略：第一，允许任何服务除非被明确禁止；第二，禁止任何服务除非被明确允许。一般采用第二种策略。

从技术角度来看，目前有两类防火墙，即标准防火墙和双穴网关。标准防火墙使用专门的软件，并要求比较高的管理水平，而且在信息传输上有一定的延迟。双穴网关是标准防火墙的扩充，也称应用层网关，它是一个单独的系统，但能够同时完成标准防火墙的所有功能。它的优点是能够运行比较复杂的应用，同时防止在互联网和内部系统之间建立任何直接的连接，可以确保数据包不能直接从外部网络到达内部网络。

（二）漏洞扫描，申请防御

漏洞扫描会自动对网站进行安全漏洞、监控和修复漏洞，加速网站的运行，提升网站的保护等级。平时也可以帮助网站进行防御保护，保证网站的正常运行，避免网站被黑客入侵。

（三）访问控制，利用防火墙技术防范网络攻击

访问控制是网络安全防范和保护主要策略，它主要任务是保证网络资源不被非法使用和非法访问。从技术原理层面我们可将防火墙技术分为包过滤技术、状态检测技术及服务代理技术等。前者属于早期防火墙技术，需要依据路由器实施网络保护功能，具有筛选地址与协议特性，后者直接与应用程序连接，对接收数据包进行分析并提供一定访问控制。该项技术具有控制进程流量自如性与安全性、生成记录便利性，并具有透明加密机制，可与其他安全防控方式进行有效集成。网络权限控制。用户和用户组被赋予一定权限，网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源，可以指定用户对这些文件、目录、设备能够执行哪些操作，属性安全在权限安全基础上提供更进一步安全属性。

（四）使用有效的监控手段抓住入侵者。

经常使用“网威”等监控工具对网络和系统的运行情况进行实时监控，用于发现黑客或入侵者的不良企图及越权使用，及时进行相关处理（如跟踪分析、反攻击等），防范于未然。

（五）时常备份系统。若被攻击可及时修复。

这一个安全环节与系统管理员的实际工作关系密切，所以系统管理员要定期地备份文件系统，以便在非常情况下（如系统瘫痪或受到黑客的攻击破坏时）能及时修复系统，将损失减少到最低。

（六）加强防范意识，防止攻击。

加强管理员和系统用户的安全防范意识，可大大提高网络、系统的安全性能，更有效地防止黑客的攻击破坏。

（七）使用安全扫描工具发现黑客

经常使用“网威”等安全检测、扫描工具作为加强内部网络与系统的安全防护性能和抗破坏能力的主要扫描工具，用于发现安全漏洞及薄弱环节。当网络或系统被黑客攻击时，可用该软件及时发现黑客入侵的迹象，进行处理。

①基于应用的检测技术，它采用被动的，非破坏性的办法检查应用软件包的设置，发现安全漏洞。

②基于主机的检测技术，它采用被动的，非破坏性的办法对系统进行检测。通常，它涉及到系统的内核，文件的属性，操作系统的补丁等问题。这种技术还包括口令解密，把一些简单的口令剔除。因此，这种技术可以非常准确的定位系统的问题，发现系统的漏洞。它的缺点是与平台相关，升级复杂。

③基于目标的漏洞检测技术，它采用被动的，非破坏性的办法检查系统属性和文件属性，如数据库，注册号等。通过消息文摘算法，对文件的加密数进行检验。这种技术的实现是运行在一个闭环上，不断地处理文件，系统目标，系统目标属性，然后产生检验数，把这些检验数同原来的检验数相比较。一旦发现改变就通知管理员。

④基于网络的检测技术，它采用积极的，非破坏性的办法来检验系统是否有可能被攻击崩溃。它利用了一系列的脚本模拟对系统进行攻击的行为，然后对结果进行分析。它还针对已知的网络漏洞进行检验。网络检测技术常被用来进行穿透实验和安全审记。这种技术可以发现一系列平台的漏洞，也容易安装。但是，它可能会影响网络的性能。

当今信息化时代里，由于互联网络的开放性和通信协议的安全缺陷，以及在网络环境中数据信息存储和对其访问与处理的分布性特点，使得网络易受黑客、怪客、恶意软件和其他不轨攻击，存在诸如数据被人窃取，服务器不能提供服务等等网络安全漏洞。因此建立有效的网络安全防范体系就更为迫切。计算机病毒一旦发作轻则破坏文件，影响系统正常运行，重则感染整个机基本维修工具应配备齐全，一般故障应能够及时排除。不使用来历不明软件，也不使用非法解密或复制软件，要遵守网络使用规定，随意在网络上使用外来软件。安装一个具备实时拦截电子邮件病毒和恶意。

面对日益严峻网络安全漏洞问题，应通过严格访问控制、漏洞扫描、防火墙安装及病毒防范策略来实时地保证信息完整性和正确性，为网络提供强大安全服务。提高网络安全防范重视力度，用科学防火墙技术、重要的是必须明确网络安全的框架体系、安全防范的层次结构和系统设计的基本原则，分析网络系统的各个不安全环节，找到安全漏洞，做到有的放矢。网络漏洞攻击检测分析技术配合专用虚拟网络，设立权限访问控制，才能构建安全网络信息运营环境。

参考文献

[1]谢希仁.计算机网络（第4版）[M].北京：电子工业出版社，2003.

[2]蔡立军.计算机网络安全技术[M].中国水利水电出版社，2002.

作者简介：

柴天丽（1992-），女，河北省沧州市南皮县人，助理讲师，本科，主研计算机网络方向。