第1章 计算机网络安全概述

内容导读

今天，以互联网技术为代表的各种数字化应用已经渗透并影响到人们生活的方方面面。而随着网络的发展，计算机网络的安全问题成了新的热点，甚至关系到一个国家的政治、军事、经济等重要领域的安全和稳定。因此，提高对网络安全重要性的认识，增强防范意识，强化防范措施，是保证信息产业持续稳定发展的重要保障和前提条件。

本章将重点介绍计算机网络安全现状、面临的主要威胁、计算机网络安全内容等知识。

1.1 计算机网络安全现状

现在，整个社会进入了一个互联网广泛应用的全新时代，网络技术及应用全面地影响和改变着人们的生活，网络已经成为人们工作和生活不可缺少的一部分，并已经深入到生活的各个方面。但随之而来的，计算机网络安全也受到前所未有的威胁：一旦网络受到攻击而不能正常工作，很多企业和部门就会陷入瘫痪。

网络安全离我们的生活并不是特别远，最近几年发生了很多重大网络安全事故。

1. 网络间谍活动公之于世

2013 年 6 月曾经参加美国安全局网络监控项目的斯诺登披露“棱镜事件”：美国秘密利用超级软件监控网络、电话或短信，包括谷歌、雅虎、微软、苹果、Facebook、美国在线、PalTalk、Skype、YouTube 九大公司帮助提供漏洞参数、开放服务器等，使其轻而易举地监控有关国家机构或上百万网民的邮件、即时通话及相关数据等，如图 1-1 所示。

图 1-1 “棱镜事件”披露者爱德华·斯诺登

2. 金融网络安全引发担忧

孟加拉央行 8100 万美元巨款失窃，厄瓜多尔 Banco del Austro 银行约 1200 万美元被盗，越南先锋银行也被曝出黑客攻击未遂等。近一年来黑客利用 SWIFT 系统漏洞入侵了一家又一家金融机构。俄罗斯也赶上了 2016 年的末班车，其中央银行遭黑客攻击，3100 万美元不翼而飞。

3. 大规模网络设备故障

2016 年 11 月，德国电信遭遇一次大范围的网络故障，2000 万固定网络用户中的大约 90 万路由器发生故障 (约 4.5%)，并由此导致大面积网络访问受限。德国电信进一步确认了问题是由于路由设备的维护界面被暴露在互联网上，并且互联网上正在发生有针对性的攻击而导致。

4. 网站瘫痪

恶意软件 Mirai 控制的僵尸网络对美国域名服务器管理服务供应商 Dyn 发起 DDoS 攻击，从而导致许多网站的服务器在美国东海岸地区宕机，如 GitHub、Twitter、PayPal 等，用户无法通过域名访问这些站点。感染范围如图 1-2 所示。

图 1-2　Mirai 僵尸网络感染范围示意图

5. 勒索病毒全面爆发

2017 年 5 月，勒索病毒全面爆发，据卡巴斯基统计，在十几个小时内，全球共有 74 个国家的至少 4.5 万台计算机中招。此类敲诈 (勒索) 病毒，在一定时间内持续攻击用户计算机，一旦攻击成功，造成的损失无法抵挡，需要支付大额赎金才能恢复数据，如图 1-3 所示。当然也不排除支付赎金后被骗的情况发生。

图 1-3　勒索病毒勒索提示

2017 年 5 月 12 日，WannaCry 蠕虫通过 MS17-010 漏洞在全球范围大爆发，感染了大量的计算机，该蠕虫感染计算机后会向计算机中植入敲诈者病毒，导致计算机大量文件被加密。受害者计算机被黑客锁定后，病毒会提示支付价值相当于 300 美元的比特币才可解锁。

2017 年 5 月 13 日晚间，由一名英国研究员于无意间发现的 WannaCry 隐藏开关 (Kill Switch) 域名，意外地遏制了病毒的进一步大规模扩散。

2017 年 5 月 14 日，监测发现，WannaCry 勒索病毒出现了变种：WannaCry 2.0，与之前版本不同的是，这个变种取消了 Kill Switch，不能通过注册某个域名来关闭变种勒索病毒的传播，该变种传播速度可能会更快。广大网民需要尽快升级，安装 Windows 操作系统相关补丁，已感染病毒机器要立即断网，才能避免进一步传播感染。

6. Reaper 僵尸网络病毒

Reaper 僵尸网络病毒的主要攻击对象为连接到互联网的监控摄像和拍照录影设备，其病毒扩散程度规模宏大，在不知不觉中让计算机被指挥和利用。此类僵尸网络危害极大，在一定程度上传播木马程序到主机，再继续扩散，形成一个大面积僵尸网络群，危害指数非常高，如图 1-4 所示。

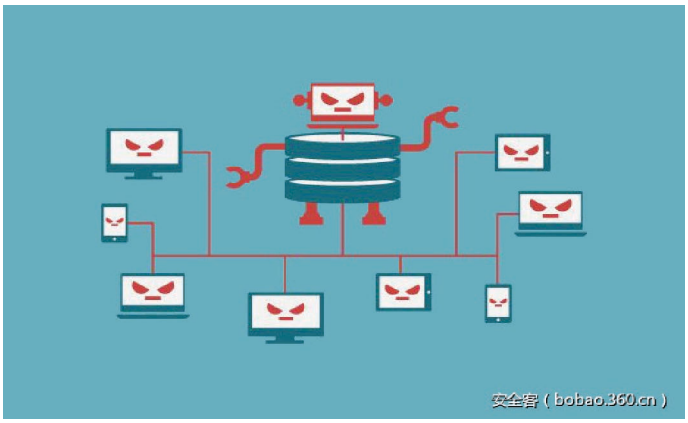

图 1-4　僵尸病毒感染范围广

7. 信息泄露屡创历史新高

信息泄露屡创新高，2017 年，仅上半年泄露或被盗的数据 (19 亿条)，就已经超过了 2016 年全年被盗数据总量，全年超过 50 亿条。其中，仅雅虎一家就达到了 30 亿条，如图 1-5 所示。

图 1-5　雅虎数据泄露通知

8. 电子邮件安全事件

2017 年腾讯安全通报一起大范围钓鱼邮件攻击事件，52 个国家的网站被利用，近 3 万家中国企业受影响，如图 1-6 所示。

图 1-6　警惕电子邮件钓鱼

9. 漏洞数量增长史无前例

CNNVD 公布的漏洞数量为 14 748 个，2016 年全年的漏洞总数为 8753 个，年增长率上升至少 70%。而自 CNNVD 正式统计漏洞数量以来，从 2010 年至 2016 年，增长率最高才为 20%，如图 1-7 所示。

图 1-7　CNNVD 公布的漏洞

Cisco IOS&IOS XE Software CMP 出现远程代码执行漏洞 (CVE-2017-3881)，允许未授权访问，远程攻击者可以重启设备、执行代码、提升权限等。

苹果设备 WiFi 芯片出现任意代码执行缓冲区溢出漏洞，该漏洞影响 iPhone 5 及以上版本，iPad 4 代及更新机型，还有 iPod touch 6 代及更新版本等。

1.2 网络安全面临的威胁

互联网是对全世界都开放的网络，任何单位或个人都可以在网上方便地传输和获取各种信息，如图 1-8 所示。互联网这种具有开放性、国际性、自由性的特点对计算机网络安全提出了挑战。互联网的不安全性与互联网络的特性有关。

图 1-8　全球网络化

1. 网络的开放性

网络技术是全开放的， 使得网络所面临的攻击来自多方面，或是来自物理传输线路的攻击，或是来自对网络协议的攻击，以及对计算机软件、硬件的漏洞实施攻击等。

2. 网络的国际性

网络的国际性意味着对网络的攻击不仅是来自于本地网络的用户， 还可以是互联网上其他国家的黑客，所以，网络的安全性面临着国际化的挑战。

3. 网络的自由性

大多数的网络对用户的使用没有技术上的约束，用户可以自由地上网、发布和获取各类信息。

1.2.1 网络面临的主要安全威胁

对计算机网络构成不安全的因素及产生的原因多种多样，从广义上来说，有人为因素、自然因素等；从目的性来说，有利益驱使、炫耀技术、企业竞争等。下面介绍一些主要的安全问题影响因素。

1. 物理安全问题

除了物理设备本身的问题外，物理设备安全问题还包括设备的位置安全、限制物理访问、物理环境安全和地域因素等。物理设备的位置极为重要，所有基础网络设施都应该放置在严格限制来访人员的地方，如图 1-9 所示，以降低出现未经授权访问的可能性。同时，还要注意严格限制对接线柜和关键网络基础设施所在地的物理访问。物理设备也面临着环境方面的威胁，这些威胁包括温度、湿度、灰尘、供电系统对系统运行可靠性的影响，由于电子辐射造成信息泄露以及自然灾害对系统的破坏等。

2. 方案设计的缺陷

由于实际中网络的结构往往比较复杂，包含星形、总线形和环形等各种拓扑结构，结构的复杂给网络系统管理拓扑设计带来很多问题，如图 1-10 所示。为了实现异构网络间信息的通信，往往要牺牲一些安全机制的设置和实现，从而提出更高的网络开放性要求。

图 1-9　专业网络机房

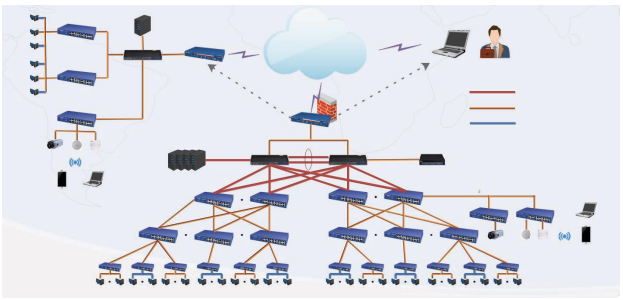

图 1-10　网络结构设计

3. 安全漏洞

随着软件系统规模的不断扩大，系统中存在安全漏洞或后门也不可避免，比如常用的 Windows 系统存在一些安全漏洞，各类服务器、浏览器、数据库等都被发现存在过安全隐患，可以说任何一个软件系统都可能会因为程序员的一个疏忽、设计中的一个缺陷等原因而存在漏洞，这也是网络安全问题的主要根源之一，如图 1-11 所示。

图 1-11　Windows 漏洞及说明

4. 人的因素

人的因素包括人为无意的失误和人为的恶意攻击等；网络建设单位、管理人员和技术人员缺乏安全防范意识，没有采取主动的安全措施加以防范等；网络管理人员和技术人员缺乏必要的专业安全知识，不能安全地配置和管理网络，不能及时发现已经存在的和随时可能出现的安全问题，对突发的网络安全事件不能做出积极有序和有效的反应等。

1.2.2 网络威胁的主要形式

网络威胁造成的危害是有目共睹的，而网络威胁的主要因素及主要表现形式如下。

1. 病毒、木马程序

病毒和木马程序可以直接侵入用户的计算机并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开，或者将含有木马程序的邮件附件从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序，它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在自己的计算机中，并在自己的计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当计算机连接到因特网上时，这个程序就会通知黑客，并报告用户 IP 地址以及预先设定的端口。黑客收到这些信息后，利用这个潜伏的程序，就可以任意地修改计算机的参数设定、复制文件、窥视整个硬盘中的内容等，从而达到控制计算机及窃取财产的目的，如图 1-12 所示。

图 1-12　病毒危害

2. 系统漏洞

操作系统是由数以万计的文件构成的，庞大的数量意味着繁多的功能，功能一多必将导致种种安全漏洞的产生。由于每个系统或多或少都会存在这样或那样的漏洞，所以黑客们入侵计算机系统时，总会先查找有无系统漏洞以方便进入。

此外，漏洞不仅仅来源于 Windows 等系统，如果其他软件使用不当，也可能会导致漏洞的出现。比如，服务器的安全配置很好，但是安装的 FTP 服务器软件却有漏洞，这也会间接导致服务器被黑客入侵。

虽然系统漏洞在出现后很快就会有补丁可供下载，如图 1-13 所示，但是往往人为因素会导致无法更新补丁、无法检测漏洞等情况发生。

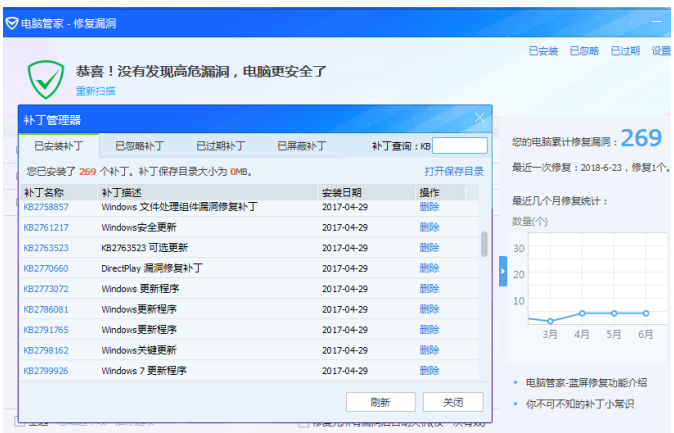

图 1-13　使用第三方工具安装漏洞补丁

3. 后门程序

由于程序员设计一些功能复杂的程序时，一般采用模块化的程序设计思想，将整个项目分割为多个功能模块，分别进行设计、调试，这时的后门就是一个模块的秘密入口。在程序开发阶段，后门便于测试、更改和增强模块功能。正常情况下，完成设计之后需要去掉各个模块的后门，不过有时由于疏忽或者其他原因 (如将其留在程序中，便于日后访问、测试或维护)，后门没有去掉，一些别有用心的人会利用穷举搜索法发现并利用这些后门，然后进入系统并发动攻击，如图 1-14 所示。

4. 信息炸弹

信息炸弹是指使用一些特殊工具软件，短时间内向目标服务器发送大量超出系统负荷的信息，造成目标服务器超负荷、网络堵塞、系统崩溃的攻击手段。比如向未打补丁的 Windows 系统发送特定组合的 UDP 数据包，会导致目标系统死机或重启；向某型号的路由器发送特定数据包致使路由器死机 ；向某人的电子邮箱发送大量的垃圾邮件将此邮箱“撑爆”等。目前常见的信息炸弹有邮件炸弹、逻辑炸弹等，现在又出现了微信群炸弹，即向微信群发出大量信息，导致点开这个内容时，系统性能短时间被大量消耗，从而出现卡屏或软件崩溃等。如图 1-15 所示，可以让群失去作用，手机瘫痪。

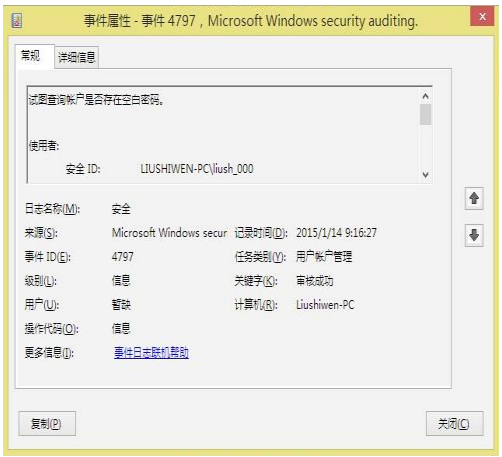

图 1-14　日志记录的安全

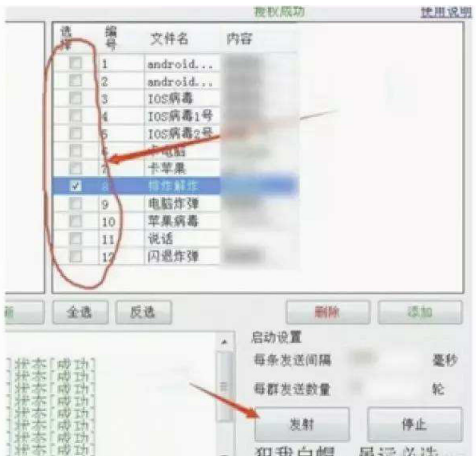

图 1-15　微信群炸弹

5. 拒绝服务

拒绝服务又叫分布式 DoS 攻击，它是使用超出被攻击目标处理能力的大量数据包消耗系统可用系统、带宽资源，最后致使网络服务瘫痪的一种攻击手段。作为攻击者，首先需要通过常规的黑客手段侵入并控制某个网站，然后在服务器上安装并启动一个可由攻击者发出的特殊指令来控制的进程，攻击者把攻击对象的 IP 地址作为指令下达给进程的时候，这些进程就开始对目标主机发起攻击。这种方式可以集中大量的网络服务器带宽，对某个特定目标实施攻击，因而威力巨大，顷刻之间就可以使被攻击目标带宽资源耗尽，导致服务器瘫痪。现在已经有了 DDoS 攻击检测系统，如图 1-16 所示。

图 1-16　DDoS 攻击检测

6. 密码破解

密码破解当然也是黑客常用的攻击手段之一，一般有暴力猜解和键盘记录等方式。黑客使用编译好的程序对目标进行有穷枚举，从而获取安全性较低的服务器中存储的管理员或用户信息，如图 1-17 所示，从而达到获取利益的目的。

7. 通信协议固有缺陷

网络协议的原旨是实现终端间的通信过程，因此，网络协议中的安全机制是先天不足的，这就为利用网络协议的安全缺陷实施攻击提供了渠道。如 SYN 泛洪攻击、源 IP 地址欺骗攻击、地址解析协议欺骗攻击等，如图 1-18 所示。

图 1-17　RAR 密码破解

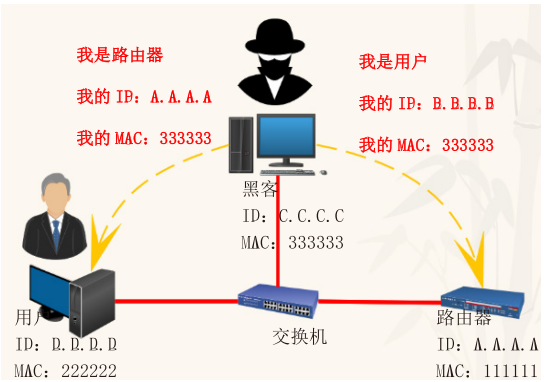

图 1-18　ARP 欺骗

8. 软、硬件固有缺陷

上面提到的操作系统漏洞就属于该类型。除了操作系统漏洞，还有网络设备等的固件漏洞、应用软件的漏洞等，都会被恶意者利用，进行网络攻击。

9. 人为因素

这里的人为因素比较宽泛，从实际应用角度讲，人为因素包括恶意因素、水平因素、使用不当以及管理员的管理问题等。人为因素是最常见的影响网络安全的因素。以上所有问题都可以归结到人为因素中，因为网络的创建者、使用者都是人，所以该因素是最为致命的。

1.3 黑客概述

“黑客”(Hacker)，是指专门研究、发现计算机和网络漏洞的计算机爱好者，他们伴随着计算机和网络的发展而成长。黑客对计算机有着狂热的兴趣和执着的追求，他们不断地研究计算机和网络知识，发现计算机和网络中存在的问题，喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补漏洞的方法。

黑客属于人为因素，而且属于对网络安全具有重大威胁的因素。由于利益的驱动，科技和网络的发展及大规模普及，更为黑客的活动提供了温床。在与黑客的较量中，首先需要了解黑客以及黑客的手段，才能进行防范和对抗。

世界上每年都有很多的黑客比赛与大会，用于黑客间的交流，如图 1-19 所示。

图 1-19　2016 美国黑帽大会

1.3.1 黑客、骇客、红客

“黑客”大体上应该分为“正”“邪”两类，“正”派黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善，而“邪”派黑客则是通过各种黑客技能对系统进行攻击、入侵或者做其他一些有害于网络安全的事情，因为“邪”派黑客所从事的事情违背了《黑客守则》，所以他们真正的名字叫“骇客”(Cracker)，而非“黑客”(Hacker)。

无论哪类黑客，其最初的学习内容都属于网络安全范畴，而且掌握的基本技能也都是一样的。即便日后他们各自走上了不同的道路，但是所做的事情也差不多，只不过出发点和目的不一样而已。

红客 (Honke) 是指维护国家利益，不利用网络技术入侵自己国家电脑，而是“维护正义，为自己国家争光的黑客”。红客是一种精神，它是一种热爱祖国、坚持正义、开拓进取的精神。所以只要具备这种精神并热爱计算机技术的计算机爱好者都可称为红客。红客通常会利用自己掌握的技术去维护国内网络的安全，并对外来的进攻进行还击，如图 1-20 所示。

图 1-20　中国红客联盟

1.3.2 黑客入侵的主要过程

黑客的入侵并不是使用软件，简单地点两下鼠标就可以了，而是进行了有针对性的探测与环境构建，下面介绍入侵的主要步骤。

1. 收集网络系统中的信息

信息的收集并不对目标产生危害，只是为进一步的入侵提供有用信息。黑客可能会利用公开协议或工具，收集驻留在网络系统中的各个主机系统的相关信息。

2. 探测目标网络系统的安全漏洞

在收集到待攻击目标的一定量信息后，黑客们会探测目标网络上的每台主机，来寻求系统内部的安全漏洞。

3. 建立模拟环境，进行模拟攻击

根据收集探测到的信息，建立一个类似攻击对象的模拟环境，然后对此模拟目标进行一系列的攻击。在此期间，通过检查被攻击方的日志，观察检测工具的攻击回馈信息，可以进一步了解在攻击过程中留下的“痕迹”及被攻击方的状态，以此来制定一个较为周密的攻击策略。

4. 具体实施网络攻击

入侵者根据前几步所获得的信息，同时结合自身的水平及经验总结出相应的攻击方法，在进行模拟攻击的实践后，等待时机，实施真正的网络攻击。

1.3.3 黑客入侵后的现象

黑客在入侵了计算机后总会留下一些蛛丝马迹，仔细辨别这些迹象，有利于用户的判断并及时做出防范措施。

1. 进程异常

用 Ctrl+Alt+Del 组合键调出任务管理器，查看运行的进程，如图 1-21 所示。如发现陌生

进程就要多加注意，可以关闭一些可疑的程序，如果发现不正常的情况恢复了正常，那么就可以初步确定计算机是中了木马了；发现有多个名字相同的程序在运行，而且可能会随时间的增加而增多，这也是一种可疑的现象，也要特别注意。如果是在计算机连入 Internet 或局域网后才发现这些现象，需要尽快查看是否有木马或者病毒在作怪。

2. 可疑启动项

可疑程序的另一特点是随系统启动而运行。用户可以运行“Msconfig”命令，启动“系统配置”程序，在弹出对话框的“启动”选项卡中，查看是否有可疑的程序随系统启动，如图 1-22 所示。可以禁用这些可疑程序，从系统稳定性上判断该程序是否为病毒或者木马程序。用户也可以使用第三方软件来禁用可疑启动项。

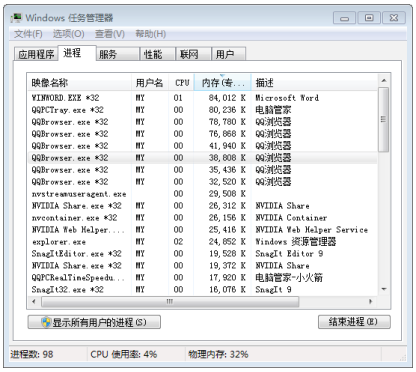

图 1-21　查看系统进程

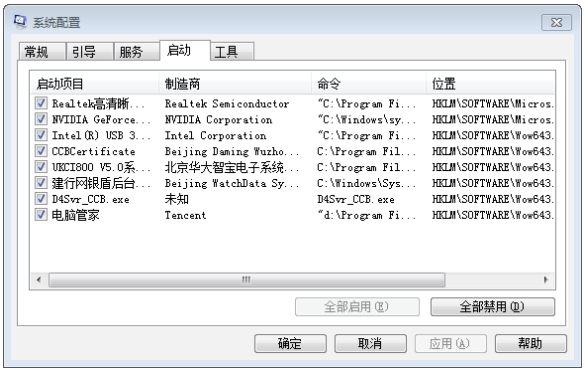

图 1-22　查看启动项

3. 注册表异常

该操作涉及比较专业的层次，用户最好在修改前先对注册表进行备份。运行“Regedit”命令调出注册表编辑器，如图 1-23 所示。查看相应的条目和值是否正常，如果有异常，有可能是被黑客侵入了。

4. 开放可疑端口

黑客有可能在侵入系统后，留下后门程序用来监听客户端请求。用户可以通过命令查看计算机是否开启了可疑端口。在命令提示符界面中，使用“netstat–an”命令来查看异常端口，如图 1-24 所示。

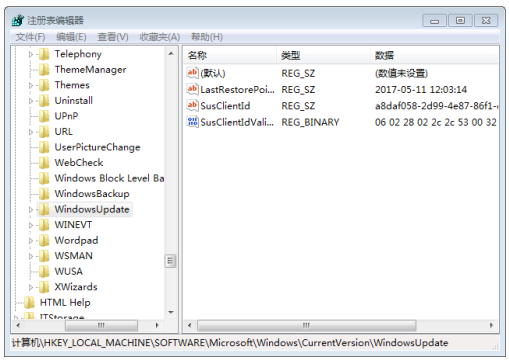

图 1-23　查看注册表项

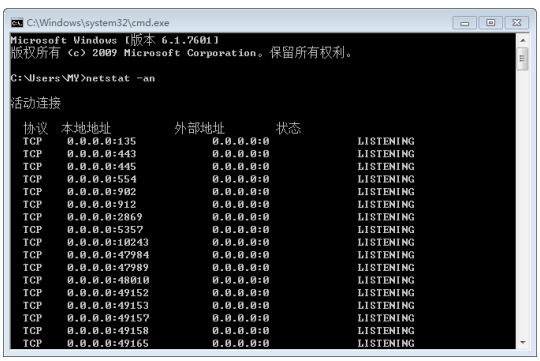

图 1-24　查看系统端口信息

5. 查看日志文件

一般黑客在侵入后，会将关于登录的信息删除，但是，不排除有部分黑客技术实力较弱或者大意之下，留下了蛛丝马迹。用户可以通过查看日志文件，确定是否有黑客侵入。

在“计算机”图标上右击，在弹出的快捷菜单中选择“管理”选项，在弹出的“计算机管理”对话框中选择“事件查看器—Windows 日志”选项，并在下拉列表中选择“安全”选项，如图 1-25 所示。通过查看登录记录、时间来判断是否有黑客的异常登录。另外，可以通过其他日志信息来判断是否有恶意程序运行、篡改系统文件。

6. 存在陌生用户

黑客在侵入计算机系统后，会创建有管理员权限的用户，以便使用该账户远程登录计算机或者启动程序及服务等。用户可以使用命令查看到是否有新建的陌生账户，如图 1-26 所示。如果存在，应该及时删除该账户。

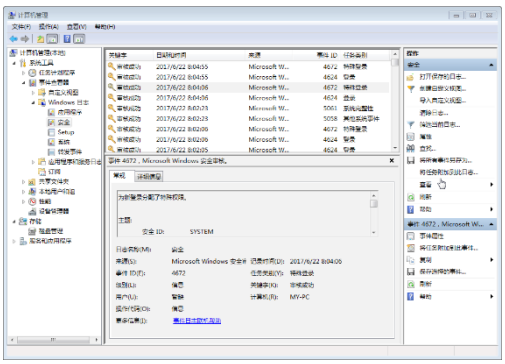

图 1-25　查看系统日志文件

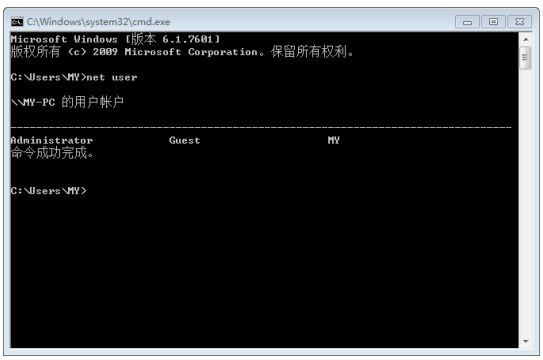

图 1-26　查看系统用户

7. 陌生服务

黑客侵入或者木马程序会开启一些服务程序，为黑客提供各种数据信息。用户可以启动服务查看器查看是否存在异常的服务，如图 1-27 所示，并及时关闭异常服务，如图 1-28 所示。

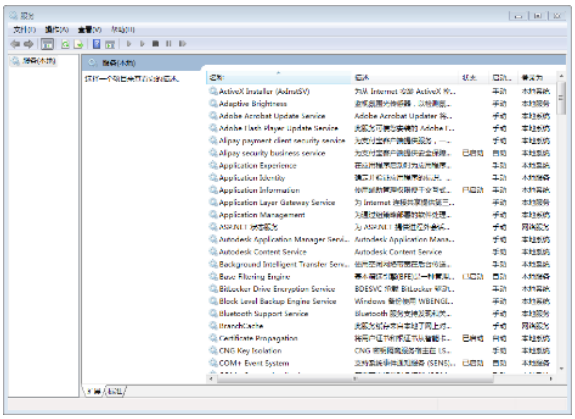

图 1-27　查看系统服务

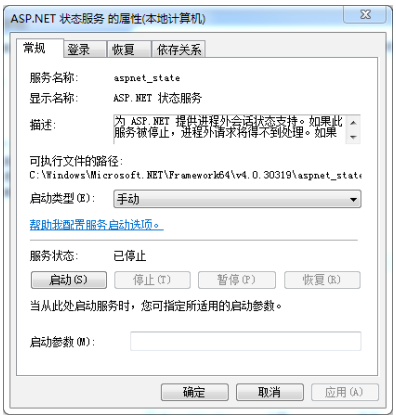

图 1-28　关闭系统服务