第5章 chapter 5

黑客攻防与检测防御

黑客对网络系统的入侵与攻击现象频频出现，严重威胁着各种网络系统和应用的安全。网络安全问题成为学者、用户和安全保卫者研究的重要课题之一。网络安全管理的重要工作之一是防范黑客攻击与入侵检测和防御技术的研究。

教学目标

- 掌握黑客和入侵检测的概念。
- 熟悉黑客常用的攻击方法及步骤。
- 掌握黑客攻击防御措施和方法。
- 掌握入侵检测系统的功能、工作原理、特点及应用。
- 掌握入侵检测与防范技术的发展趋势。

5.1 网络黑客概述

【案例 5-1】 约翰·德雷珀出生于美国空军工程师家庭，1970 年发现口哨产生的2600Hz 的声波可用来欺骗电话交换机，系统收到这个频率信号以为通话中断，便停止计费，于是可以继续打免费电话。后人各种各样的入侵电话网络行为都可追溯到约翰·德雷珀，他不仅是盗打电话的“鼻祖”，也成为网络入侵行为的“先驱”。

5.1.1 黑客的概念及类型

1. 黑客及其演变

黑客是英文 Hacker 的译音，源于 hack，本意为“干了一件非常漂亮的事”。原指一群专业技能超群、聪明能干、精力旺盛，并且精通攻击和防御，可以发现威胁，并提出防御方案的人。后来“黑客”一词成为专门利用计算机进行破坏或入侵他人计算机系统的人的代名词。

在虚拟的网络世界里，黑客已成为一个特殊的社会群体。黑客攻击是网络面临的最严重的安全问题。国内外网络资源遭破坏和攻击现象呈现出急剧上升态势且种类多变，系统漏洞、网络资源应用已成为黑客的攻击目标。有不少黑客组织利用网站介绍攻击手

段，免费提供各种黑客工具和资料，致使普通用户也能很容易学会使用一些简单的黑客手段或工具对网络进行某种程度的攻击，进一步恶化了网络安全环境。

2. 中国黑客的形成与发展

1994 年 4 月 20 日，中国国家计算机与网络设施工程 NCFC（National Computing and Networking Facility of China）通过美国 Sprint 公司开通连入 Internet 的 64Kb/s 国际专线，实现了与 Internet 的全功能连接。中国成为直接接入 Internet 的国家。从那时起，中国黑客开始了原始萌动。1998 年，印度尼西亚爆发了大规模排华事件，中国黑客开始组织起来，用 ping 的方式攻击印尼网站。这次行动造就了中国黑客最初的团结与合作的精神。这事件之后，有些人又回到了现实生活中，有些人则从此开始了对黑客理想的执着追求。1999 年是网络泡沫高度泛滥的顶峰时期，刚刚起步的中国黑客开始划分自己的势力范围。从 1999 年到 2000 年，中国黑客联盟、中国鹰派、中国红客联盟等一大批黑客网站兴起。时至今日，国内黑客中却是为了牟取暴利而从事散发木马等行为的“毒客”占主流。中国互联网形成了惊人的黑客病毒产业链，从制造木马、传播木马、盗窃账户信息直到第三方平台销赃、洗钱，分工明确。从带着理想主义和政治热情的红客占主流到非法牟利的毒客横行，这是一个无奈的变化。

3. 黑客的类型

从最初的黑客一词逐渐分化出红客、蓝客、骇客等名词。

黑客，最早源自英文 hacker，早期在美国的计算机界是带有褒义的。都是水平高超的计算机专家，尤其是程序设计人员，算是一个统称。

红客声称维护国家利益，代表中国人民意志。

蓝客声称信仰自由，用自己的力量来维护网络的和平。

骇客是 Cracker 的音译，就是“破解者”的意思，他们从事恶意破解商业软件、恶意入侵别人的网站等活动。黑客与骇客本质上是相同的，都是闯入计算机系统/软件者，两者并没有一个十分明显的界限。

5.1.2 黑客攻击的途径

黑客和黑客技术对大多数用户而言还是非常陌生的，下面介绍有关黑客的基础知识。

1. 黑客攻击的主要原因——漏洞

漏洞又称缺陷，是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可使攻击者能够在未授权的情况下访问或破坏系统。从某种意义上来讲，黑客的产生与生存是由于计算机及通信技术设计等问题，计算机及网络系统的不健全，存在许多漏洞，才使黑客攻击有机可乘。造成漏洞的原因分析如下：

（1）网络协议本身的缺陷。如 Internet 基础协议 TCP/IP 协议组，早期没有考虑安全方面的问题，侧重开放和互联而过分信任协议，使得协议的缺陷更加突出。

(2) 系统开发的缺陷。软件开发没有很好地解决保证大规模软件可靠性问题,致使大型系统都可能存在 bug(缺陷)。bug 是指操作系统或系统程序在设计、编写或设置时考虑不周全,在遇到看似合理但实际上无法处理的问题时会引发不可预见的错误。漏洞的产生主要有 4 个方面的原因:操作系统基础设计错误;源代码错误(缓冲区、堆栈溢出及脚本漏洞等);安全策略施行错误;安全策略对象歧义错误。

(3) 系统配置不当。有许多软件是针对特定环境配置开发的,当环境变化或资源配置不当时,就可能使本来很小的缺陷变成漏洞。

(4) 系统安全管理中的问题。快速增长的软件的复杂性、训练有素的安全技术人员的不足以及系统安全策略的配置不当,都增加了系统被攻击的机会。

【案例 5-2】 2014 年 4 月 9 日,代号为 Heartbleed("心脏出血")的重大安全漏洞(CVE-2014-0160)被曝光。该漏洞来自 OpenSSL 这款开源的 SSL 套件,是由于在实现 TLS 的心跳扩展(heart beat extension)时没有对输入进行适当边界检查而导致的。攻击者利用该漏洞可以从服务器内存中读取用户名、密码和信用卡号等隐私数据。比如获取用户的敏感请求和响应,包括 POST 请求数据、会话 cookie 和密码等,从而劫持用户的身份。由于全球三分之二的网站使用 OpenSSL,该漏洞让数千万人的数据处于危险状态。

2. 黑客入侵通道——端口

端口(port)是设备与外界通信交流的出口。端口可分为虚拟端口和物理端口,其中虚拟端口指计算机内部或交换机路由器内的端口,不可见。例如计算机中的 80 端口、21 端口、23 端口等。物理端口又称为接口,是可见端口,计算机背板的 RJ45 网口,交换机路由器集线器等的 RJ45 端口。电话使用的 RJ11 插口都属于物理端口的范畴。网络之间的传输和黑客攻击都是通过各种端口作为入侵通道。更准确地说是虚拟端口,即逻辑意义上的端口,是指网络中面向连接服务和无连接服务的通信协议端口(protocol port),是一种抽象的软件结构。

知识拓展 有人曾经把服务器比作房子,而把端口比作通向不同房间(服务)的门。入侵者要占领这座房子,势必要破门而入,那么对于入侵者来说,了解房子开了几扇门,都是什么样的门,门后面有什么东西就显得至关重要。入侵者通常会用扫描器对目标主机的端口进行扫描,以确定哪些端口是开放的,从开放的端口,入侵者可以知道目标主机大致提供了哪些服务,进而猜测可能存在的漏洞,因此对端口的扫描可以帮助黑客了解目标主机,而对于管理员,扫描本机的开放端口也是做好安全防范的第一步。

【案例 5-3】 计算机 A 通过网络访问计算机 B 时,同时需要对方返回数据。A 随机创建一个大于 1023 的端口(A 源端口号),告诉 B 返回数据时把数据送到此端口,然后软件开始侦听此端口,等待数据返回。B 收到数据后会读取数据包及目的端口号,然后记录,当软件创建了要返回的数据后就把原来数据包中的源端口号作为目的端口号,而把自己的端口号作为源端口号,然后再将数据送回 A。A 再重复这个过程,如此反复,直到数据传输完成。当数据全部传输完以后,A 就把源端口释放出来,所以同一个软件每次传输数据时不一定是同一个源端口号。

端口分类标准有多种,按端口号可分为 3 种:

（1）公认端口（0～1023），又称常用端口，为已经公认定义或为将要公认定义的软件保留的。这些端口紧密绑定一些服务且明确表示了某种服务协议，如80端口表示HTTP协议。

（2）注册端口（1024～49 151），又称保留端口，这些端口松散绑定一些服务。例如，许多系统处理动态端口从1024左右开始。

（3）动态/私有端口（49 152～65 535）。理论上不为服务器分配这些端口。实际上，机器通常从1024起分配动态端口。但也有例外，SUN公司的RPC端口从32 768开始。

讨论思考

（1）什么是黑客？黑客都是破坏系统的吗？

（2）端口对计算机有什么作用？

（3）黑客在入侵时很容易锁定某一服务，通过漏洞入侵系统，请举例说明。

5.2 黑客攻击的目的及步骤

黑客实施攻击的步骤根据其攻击的目的、目标和技术条件等实际情况而不尽相同。本节概括性地介绍网络黑客攻击目的及过程。

5.2.1 黑客攻击的目的

黑客实施攻击的目的概括地讲有两种：其一，为了得到资金或物质利益；其二，为了满足精神需求。物质利益是指获取金钱和财物；精神需求是指满足个人心理欲望。

常见的黑客行为有：盗窃资料，攻击网站，恶作剧，告知漏洞，获取目标主机系统的非法访问权。

5.2.2 黑客攻击的步骤

黑客的攻击步骤变幻莫测，但其整个攻击过程有一定规律，一般可分为5个步骤。

1. 隐藏IP

隐藏IP就是隐藏黑客的位置，以免被发现。典型的隐藏真实的IP地址的技术是利用被侵入的主机作为跳板，有两种方式。

方式一：先入侵到互联网上的一台计算机（俗称“肉鸡”或“傀儡机”），再利用这台计算机进行攻击，即使被发现，也是“肉鸡”的IP地址。

方式二：做多级跳板“Socks代理”，这样在入侵的计算机上留下的是代理计算机的IP地址。例如，攻击某国的站点，一般选择远距离的另一国家的计算机为“肉鸡”，进行跨国攻击，这类案件很难侦破。

2. 踩点扫描

踩点扫描主要是通过各种途径对所要攻击的目标进行多方探察了解，确保信息准

确，以便确定攻击时间和地点。踩点的目的是搜集信息，勾勒出整个网络的布局，找出被信任的主机（可能是管理员使用的机器或是一台被认为是很安全的服务器）。扫描是利用各种扫描工具寻找漏洞。

3. 获取特权攻击

获取特权是指获取管理权限，目的是登录到远程计算机上，对其进行控制，达到攻击目的。获取权限方式分为 6 种：由系统或软件漏洞获取系统权限；由管理漏洞获取管理员权限；由监听获取敏感信息，进一步获取相应权限；以弱口令或穷举法获取远程管理员的用户密码；攻破与目标主机有信任关系的另一台计算机，进而得到目标主机的控制权；用欺骗等方式获取权限。

4. 种植后门

种植后门即黑客利用程序的漏洞进入系统后安装后门程序，以便日后可以不被察觉地再次进入系统。多数后门程序（木马）是预先编译好的，只需要想办法修改时间和权限就可以使用。黑客一般使用特殊方法传递这些文件，以便不留下 FTP 记录。

5. 隐身退出

黑客一旦确认自己是安全的，就开始实施攻击，为了避免被发现，黑客在入侵完毕后会及时清除登录日志以及其他相关日志，隐身退出。

【案例 5-4】 2011 年 3 月，RSA 公司遭受入侵，部分 SecurID 技术及客户资料被盗取。导致很多使用 SecurID 作为认证凭证建立 VPN 的公司，包括洛克希德·马丁、诺斯罗普·格鲁曼等美国国防外包商受到攻击，重要资料被盗窃。图 5-1 是攻击过程的示意图。

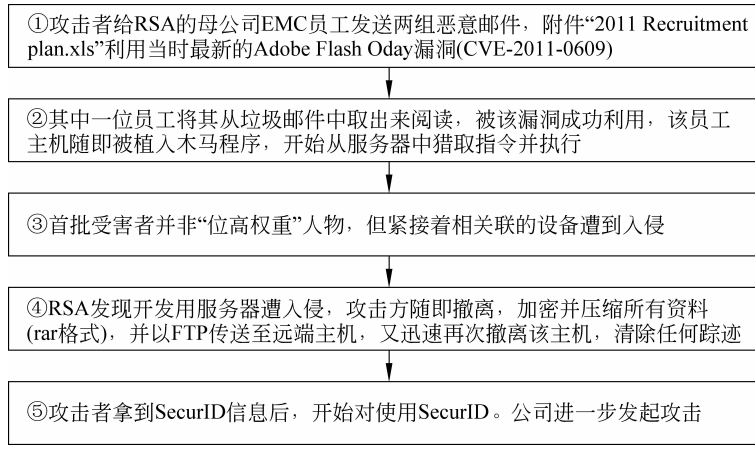

图 5-1 黑客攻击企业内部局域网过程示意图

讨论思考

（1）简述黑客攻击的目的与具体步骤。

（2）黑客找到攻击目标后，会继续哪几步操作？

（3）黑客的实际攻击行为有哪些？

5.3 常用黑客攻击防御技术

防范黑客攻击是网络安全工作的主要课题，掌握黑客攻击防御技术可以有效地预防攻击。本节将对端口扫描、网络监听、密码破解、特洛伊木马、缓冲区溢出和拒绝服务等常用黑客攻防技术进行分析。

5.3.1 端口扫描攻防

在网络传输中，各种服务采用不同的端口分别提供不同的服务。端口最大可以有65 535个，实际上常用的端口才几十个，由此可以看出更多的端口没有被使用。黑客入侵可以采用多种手段开启特定的端口，作为再次进入系统的通道，即通常的“后门”。还有一些应用不被应用，但是端口通常开放，这些端口经常被入侵者利用，成为入侵的便利渠道，因此端口扫描成为入侵锁定对象的重要方式。但是在系统安全防护过程中，端口扫描也成为管理员发现系统安全漏洞，加强系统安全管理，提高系统安全性能的有效方法。同时，端口扫描也成为黑客发现和获取主机信息的一种最佳手段。

1. 端口扫描及扫描器

一个端口就是一个潜在的通信通道，也就是一个入侵通道。对目标计算机进行端口扫描，能得到许多有用的信息，从而发现系统的安全漏洞。进行扫描的方法很多，可以是手工进行扫描，也可以用端口扫描软件进行扫描。

2. 端口扫描方式

端口扫描的方式有手工命令行方式和使用端口扫描工具进行扫描。在手工进行扫描时，需要熟悉各种命令，对命令执行后的输出进行分析，如ping命令、tracert命令（跟踪一个消息从一台计算机到另一台计算机所走的路径）、rusers和finger命令（这两个都是UNIX命令，能收集目标机上的有关用户的消息）等。

端口扫描工具及方式如下：

（1）TCP connect扫描。TCP connect是最基本的一种扫描方式。connect()是一种系统调用，由操作系统提供，其功能是打开一个连接。如果端口正在被监听，connect()就成功返回；否则，则说明端口不可访问。使用TCP connect不需要任何特权，任何UNIX用户都可以使用这个系统调用。

（2）TCP SYN扫描。SYN(synchronize)是TCP/IP建立连接时使用的握手信号。TCP SYN扫描常被称为半开扫描，因为并不是一个全TCP连接。发送一个SYN数据包，就好像准备打开一个真正的连接，然后等待响应（一个SYN/ACK表明该端口正在被监听，一个RST(复位)响应表明该端口没有被监听）。如果收到一个SYN/ACK，则通过

立即发送一个 RST 来关闭连接。这样做的好处是极少有主机记录这种连接请求。

另外，还一些免费端口扫描工具可供使用。如 SuperScan、X-Scan、Fluxay、Angry IP Scanner 和 NSE 等。SuperScan 软件下载后直接解压就可使用，没有安装程序，是一款绿色软件，与 IP 扫描有关的功能几乎全能做到，且每个功能都很专业。其功能如下：

- 通过 ping 来检验指定主机 IP 是否在线。
- IP 和域名相互转换。
- 检验目标计算机提供的服务类别。
- 检验一定范围目标计算机是否在线和端口情况。
- 自定义要检验的端口，并可以保存为端口列表文件。
- 自带一个木马端口列表 trojans.lst，并以此检测木马是否存在，可以自定义修改此列表。

3. 端口扫描攻击

端口扫描攻击采用探测技术，攻击者可将它用于寻找能够成功攻击的服务。常用端口扫描攻击如下：

(1) 秘密扫描。不能被用户使用审查工具检测出来的扫描。

(2) Socks 端口探测。Socks 是一种允许多台计算机共享公用 Internet 连接的系统。如果 Socks 配置有错误，将允许任意的源地址和目标地址通行。

(3) 跳跃扫描。攻击者快速地在 Internet 中寻找可供他们进行跳跃攻击的系统。FTP 跳跃扫描使用了 FTP 协议自身的一个缺陷。其他的应用程序，如电子邮件服务器、HTTP 代理、指针等都存在着攻击者可进行跳跃攻击的弱点。

(4) UDP 扫描。对 UDP 端口进行扫描，寻找开放的端口。UDP 的应答有着不同的方式，为了发现 UDP 端口，攻击者们通常发送空的 UDP 数据包，如果该端口正处于监听状态，将发回一个错误消息或不理睬流入的数据包；如果该端口是关闭的，大多数的操作系统将发回“ICMP 端口不可到达”的消息，这样，就可以发现一个端口到底有没有打开，通过排除方法确定哪些端口是打开的。

4. 应对扫描的防范对策

端口扫描的防范又称加固系统。在网络关键处打补丁并用防火墙对来源不明的有害数据过滤可有效减少端口扫描攻击。此外，防范端口扫描的主要方法有两种。

(1) 防止 IP 地址的扫描。IP 地址是为互联网中每一台主机分配的一个逻辑地址，对 IP 地址的扫描可以锁定一台计算机，由此对它进行攻击。这里可以通过代理服务器保护局域网的安全，起到防火墙的作用。对于使用代理服务器的局域网来说，在外部看来只有代理服务器是可见的，其他局域网的用户对外是不可见的，代理服务器为局域网的安全起到了屏障的作用。另外，通过代理服务器，用户可以设置 IP 地址过滤，限制内部网对外部的访问权限。

(2) 端口往往是系统入侵探测的重要途径，因此对端口进行安全防护是必要的，可以关闭闲置及有潜在危险的端口或设置系统不响应任何 ping 的请求。在 Windows 中要关

闭一些闲置端口是比较方便的，可以采用“定向关闭指定服务的端口”和“只开放允许端口的方式”。计算机的一些网络服务会由系统分配默认的端口，将一些闲置的服务关闭，其对应的端口也会被关闭。

5.3.2 网络监听攻防

1. 网络监听

网络监听是指通过某种手段监视网络状态、数据流以及网络上传输信息的行为。网络监听是主机的一种工作模式。在此模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。此时，如果两台主机进行通信的信息没有加密，只要使用某些网络监听工具可以轻而易举地截取包括口令和账号在内的信息资料（如 NetXray for Windows 95/98/NT，Sniffit for Linux、Solaries 等）。网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网服务器路由等。

2. 网络监听的检测

网络监听很难被发现，因为运行网络监听的主机只是被动地接收在局域网上传输的信息，不主动地与其他主机交换信息，也没有修改在网上传输的数据包。在 Linux 下对嗅探攻击的程序检测方法比较简单，一般只要检查网卡是否处于混杂模式就可以了；而在 Windows 平台中并没有现成的函数可供实现这个功能，可以执行 C:\Windows\Drwatson.exe 程序检查一下是否有嗅探程序在运行即可。

5.3.3 密码破解攻防

由于网络操作系统及其各种应用软件的安全主要靠口令认证方式来实现，所以黑客入侵的前提是得到合法用户的账号和密码。只要黑客能破解得到这些机密信息，就能够获取计算机或网络系统的访问权，并能得到任何资源。

1. 密码破解攻击的方法

密码破解攻击常采用以下几种方法：

（1）通过网络监听非法得到用户口令。这类方法有一定的局限性，但危害性极大。监听者往往能够获取其所在网段的所有用户账号和口令，对局域网安全威胁巨大，参见 5.3.2 节。

（2）利用 Web 页面欺骗。攻击者将用户浏览的网页 URL 地址改写成指向自己的服务器，当用户浏览目标网页时，如果用户在这个伪造页面中填写有关的登录信息，如账户名称、密码等，这些信息就会被传送到攻击者的 Web 服务器。攻击者在获取一个服务器上的用户口令文件（此文件称为 Shadow 文件）后，用暴力破解程序破解用户口令。该方法的使用前提是黑客获取口令的 Shadow 文件。

（3）强行破解用户口令。当攻击者知道用户的账号后，就可以利用一些专门的密码

破解工具进行破解。例如采用字典穷举法,此法采用破解工具自动从定义的字典中取出一个单词,作为用户的口令尝试登录,如果口令错误,就按序取出下一个单词再进行尝试,直到找到正确的口令或者字典的单词测试完成为止。这种方法不受网段限制,但攻击者要有足够的耐心和时间。

(4) 密码分析的攻击。对密码进行分析的尝试称为密码分析攻击。密码分析攻击方法需要有一定的密码学和数学基础。常用的密码分析攻击有 4 类:唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击。

(5) 放置木马程序。一些木马程序能够记录用户通过键盘输入的密码或密码文件并发送给攻击者,具体内容将在 5.3.4 节介绍。

2. 密码破解防范对策

要防止密码被破解,保持密码安全性能,系统管理员必须定期运行破译密码的工具来尝试破译 Shadow 文件,若有用户的密码被破译出,说明这些用户的密码设置过于简单或有规律可循,应尽快通知用户及时更改密码,以防黑客攻击,造成财产和其他损失。通常情况下用户应注意如下要点:

(1) 不要将密码写下来,以免遗失。

(2) 不要将密码保存在计算机文件中。

(3) 不要选取显而易见的信息做密码。

(4) 不要让他人知道密码。

(5) 不要在不同系统中使用同一密码。

【案例 5-5】 海康威视陷“安全门”事件。2014 年 8 月 19 日,海康威视 DVR、NVR 产品的返修数量非正常升高,发现系网络攻击导致。经排查,被攻击的设备均应用于互联网且未修改设备初始密码,黑客直接利用初始密码进行 Telnet 登录,并植入脚本文件,进而挟持、破坏设备固件。

5.3.4 特洛伊木马攻防

1. 特洛伊木马概述

特洛伊木马(Trojan horse)简称木马。据说这个名称来源于希腊神话《木马屠城记》。古希腊有大军围攻特洛伊城,久久无法攻下。于是有人献计制造一只高二丈的大木马,让士兵藏匿于巨大的木马中,大部队假装撤退而将木马摈弃于特洛伊城下。城中得知解围的消息后,遂将木马作为奇异的战利品拖入城内,全城饮酒狂欢。到午夜时分,全城军民进入梦乡,匿于木马中的将士开秘门缘绳而下,开启城门及四处纵火,城外伏兵涌入,部队里应外合,焚屠特洛伊城。后世称这只大木马为“特洛伊木马”。黑客程序借用其名,将隐藏在正常程序中的一段具有特殊功能的代码称木马,是一些具备破坏和删除文件、发送密码、记录键盘和攻击等特殊功能的后门程序。

特洛伊木马的特点是伪装、诱使用户将其安装在 PC 或者服务器上,直接侵入用户的计算机并进行破坏,没有复制能力。一般的木马执行文件非常小,如果把木马捆绑到其

他正常文件上，用户很难发现。特洛伊木马可以和最新病毒、漏洞一起使用，几乎可以躲过各大杀毒软件，尽管现在越来越多的新版的杀毒软件可以查杀一些木马了，但不要认为使用有名的杀毒软件就绝对安全，木马永远是防不胜防的。

一个完整的木马系统由硬件部分、软件部分和具体连接部分组成。一般的木马程序都包括客户端和服务端两个程序，客户端用于远程控制植入的木马，服务器端即是木马程序。

2. 特洛伊木马攻击过程

木马入侵的主要途径目前还是利用下载软件、邮件附件等先设法把木马程序以插件的方式放置到被攻击者的计算机系统里，然后通过提示故意误导被攻击者打开可执行文件(木马)。木马也可以通过 Scripts、ActiveX 及 ASP. CGI 交互脚本的方式植入，以及利用系统的一些漏洞进行植入，如微软著名的 US 服务器溢出漏洞。

【案例 5-6】 利用微软 Scripts 脚本漏洞对浏览者硬盘进行格式化的 HTML 页面。如果攻击者有办法把木马执行文件下载到被攻击主机的一个可执行的 WWW 目录里，就可以通过编制 CGI 程序在攻击主机上执行木马。

在客户端和服务端通信协议的选择上，绝大多数木马使用的是 TCP/IP 协议，但是，也有一些木马由于特殊的原因，使用 UDP 协议进行通信。当服务端程序在被感染计算机上成功运行以后，攻击者就可以使用客户端与服务端建立连接，并进一步控制被感染的计算机。木马会尽量把自己隐藏在计算机的某个角落，以防被用户发现；同时监听某个特定的端口，等待客户端与其取得连接，实施攻击。另外，为了下次重启计算机时木马仍然能正常工作，木马程序一般会通过修改注册表或其他方法成为自启动程序。

使用木马工具进行网络入侵的基本过程可以分为 6 个步骤：配置木马，传播木马，运行木马，获取信息，建立连接，远程控制。

3. 网页挂马

网页挂马本质上就是一个或者若干 Web 页面，通常挂接在被攻击成功的网站上，针对访问该页面的用户，利用 Web 浏览器、插件、客户端应用软件的缓冲溢出漏洞等向用户植入木马程序，从而窃取敏感信息和虚拟资产，如图 5-2 所示。

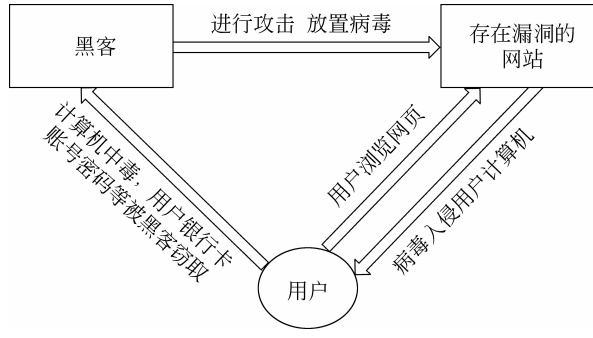

图 5-2 网页挂马过程