矛与盾

——远程攻击与防御

魏宝琛 姜明 编著

人民邮电出版社
POSTS & TELECOMMUNICATIONS PRESS

矛与盾——远程攻击与防御

魏宝琛　姜明　编著

人民邮电出版社

图书在版编目(CIP)数据

矛与盾——远程攻击与防御 / 魏宝琛，姜明编著. —北京：人民邮电出版社，2003.3
ISBN 7-115-10936-2

I. 矛… II. ①魏…②姜… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字(2003)第 007767 号

内 容 提 要

本书系统地介绍了网络安全方面的基础知识，共分 4 篇 14 章。

入门篇：第 1 章至第 2 章，主要介绍了远程攻击与安全防御有关的背景知识。

基础篇：第 3 章至第 4 章，主要介绍了 IP 地址、端口、黑客攻击的层次和作业流程等进行攻击和防御的必备基础知识。

实战篇：第 5 章至第 11 章，主要介绍了各种形式的远程攻击与防御的实战过程，主要包括 E-mail 攻击、ICQ/OICQ 攻击、聊天室攻击、恶意网页攻击、密码破解、端口和系统漏洞扫描、远程控制工具的使用以及如何进行防范等内容，这一部分是本书的重点内容。

防御篇：第 12 章至第 14 章，主要介绍了如何防范黑客攻击，包括防火墙技术、系统安全检测以及系统安全设置等内容。这一部分也是本书的重点内容。

本书以远程攻击与防御实战步骤操作为核心，通过图文并用的步骤讲解，系统介绍了远程攻击与防御知识。本书适合广大想深入了解网络安全、黑客攻击技术以及安全防御技术的网络用户阅读。

矛与盾——远程攻击与防御

◆ 编　　著　魏宝琛　姜　明
责任编辑　屈艳莲　邹文波

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www. ptpress.com.cn
读者热线　010-67132692
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：22.25
字数：538 千字　　2003 年 3 月第 1 版
印数：1-5 000 册　　2003 年 3 月北京第 1 次印刷

ISBN7-115-10936-2/TP・3255

定价：35.00 元

前　言

因特网已经成为我们这个时代的标志。但是在因特网的快速发展过程中，因特网的阴影也在迅速扩展，而网络黑客，是所有威胁因特网发展的诸多因素中，最需要我们认真对待的一个问题。

黑客是什么样的人？黑客工具是什么样的软件？黑客为什么要入侵别人的计算机？黑客是如何发动进攻的？网络上正在流行哪些攻击手法？黑客入侵普通的网络用户吗？如何防御黑客攻击？面对这些问题时不是每一位网络用户都能够从容应对的。为此，我们编写了《矛与盾——远程攻击与安全防御》一书，谨献给想深入了解网络安全、黑客攻击技术以及安全防御技术的广大网络用户。

本书在介绍和评说当前网络安全问题和网络协议的基础上，提出了自己的防御黑客攻击主张：只有掌握黑客技术才可以真正防御黑客攻击。

本书共 14 章，分为入门篇、基础篇、实战篇和防御篇，在再现当前网络上常见的几种远程攻击的实施过程的同时，有针对性地介绍了通过诸如系统设置、防火墙和安全检测软件等技术手段来防范黑客入侵的方法。

本书注重图文结合和操作步骤的示范，尽量采用通俗易懂的语言解释专业术语，起点低、易学易用，最大程度地降低了读者学习的门槛。

对于任何人来说，黑客技术都是一把双刃剑，用之正道，不失为自我保护和帮助他人的好工具；用之邪道，则为凶器，必有伤及自己的一天。我们在附录部分特地全文收录了国家有关计算机技术和网络安全方面的 4 个法规条例，提醒各位读者坚决不要使用黑客手法攻击他人计算机和网络。

本书由魏宝琛、姜明等编著。由于时间仓促，编者水平有限，书中难免有不妥之处，欢迎广大读者批评指正。

编者
bookwood@vip.sina.com
2002.10

目 录

第一篇 入门篇

第二篇 基础篇

第三篇　实战篇

第四篇 防御篇

第一篇　入门篇


✧ 第 1 章　远程攻击与防御概述

- ☞ 谁发动了远程攻击
- ☞ 实施远程攻击的一般过程
- ☞ 应对远程攻击的基本方法
- ☞ 建立健全的个人网络防护体系

✧ 第 2 章　网络协议的安全隐患与系统缓存溢出

- ☞ 远程登录标准的安全隐患
- ☞ 缓冲溢出的远程攻击
- ☞ 缓冲溢出的防止

Chapter 1

第1章

远程攻击与防御概述

从纯粹的技术角度来看，远程攻击应隶属于远程控制技术，但通常人们把远程攻击看成黑客行为。黑客是指利用某种技术手段进入其权限以外的网络空间的人，是远程攻击的发动者。所以想探知远程攻击的发生过程，就要先了解黑客。在本章中，我们将介绍黑客历史、黑客群体和黑客发动远程攻击的动机等内容，同时本章还将介绍应对黑客攻击的简单方法，并进而提出了防范网络远程攻击的一般对策。

1.1 谁发动了远程攻击

远程攻击是一种黑客行为，黑客是远程攻击的发动者。那么什么是黑客呢？生活中人们对黑客的评价众说纷纭，有很多看法。刚刚“触网”的人，以为黑客只是好莱坞大片中的人物，抑或是一种媒体炒作，与电脑前的自己没有什么干系；厌倦用户名、密码的“网虫”，视其为打破集权、滑翔于数据空间的自由之神；网站安全管理人员，视其为最大的敌人；遭受攻击者，对其深恶痛绝，视其为恶贯满盈的网络害群之马；而拥有强烈民族自尊心的电脑高手，则视其为表达自己爱国之情的网络角色，并组建了黑客联盟组织，创立了黑客网站，以推动黑客技术的发展。为什么会有这么多看法？黑客到底是什么样的人？本节的内容将会帮助你揭开黑客的神秘面纱。

黑客的发展史可以追溯到20世纪50年代。在美国麻省理工学院的实验室中，有一个由程序设计员和网络专家所组成的文化群体。该群体的成员赋予了Hacker这个英文单词新的含义。Hacker源自动词Hack，本意为“劈砍”，引申为干一件非常漂亮的事。Hacker，中文音义为“黑客”，是这一群体为自己创造的称谓。

到了20世纪60年代，黑客利用分时技术允许多个用户同时执行多道程序，扩大了计算机及网络的使用范围。20世纪70年代，黑客倡导了一场个人计算机革命，打破了以往计算机技术只掌握在少数人手里的局面，同时黑客们也发明了一些侵入计算机系统的基本技巧，如破解密码（Passwordcracking）、开天窗（Trapdoor），等等。20世纪80年代，随着计算机重要性的提高，大型数据库越来越多，信息越来越集中在少数人手里，黑客开始为信息共享而奋斗，在这一时期，黑客开始频繁入侵各大计算机系统。

21世纪的黑客则呈多元化发展，黑客群体的成员越来越复杂，既有善意的以发现计算机系统漏洞为乐趣的“黑客”，又有玩世不恭好恶作剧的“骇客”，还有纯粹以私利为目的，任意篡改数据，非法获取信息的“怪客”。仅就传统意义上的黑客而言，也有很大的差别，有的喜欢一个人仗剑江湖，做孤傲的独行客；有的则结成一个联盟，靠集体的力量称雄网络；有的喜欢与黑客同仁交流技术和信息，在互相学习中提高黑客技术。所以对黑客群体进行分析，看一看黑客队伍中到底有一些什么类型的人，他们一般喜欢干些什么样的事是很有必要的。

男性化和年轻化是黑客群体的两个总体特征。这两个群体特征也是黑客具有攻击性和探索精神的主要原因。

我们可以从类型上来给黑客做一个划分，黑客群体因其行为动机和行为本身的不同，可以分为如下几类：

• 网络黑客：这是一种传统意义上的Hacker，早期的黑客和如今一些善意入侵计算机系统的人都属于此种类型。网络黑客以严谨的、天才般的思维感触这个世界，他们以漂亮、简洁、完美的编程为自豪，以发现计算机系统的漏洞为乐趣，以突破各种安全防范为资本。他们以严格的黑客职业道德要求自己。他们常常是一些具有侠义心肠而对网络秩序不满的年轻人。这些人多数以完善程序、完善网络为己任，他们常常突破计算机系统但一般不会破坏系统，他们有时会在计算机系统中修改几个程序以使其更完美，有时会提醒系统管理员系统并不是很安全。

• 网络骇客（Cyber bunk）：这类黑客类似于西方的“嬉皮士”，这些人往往玩世不恭，标新立异，视社会为玩物，把人生当游戏。这些人在网上也许能够给人带来乐趣，但他也会让你

叫苦不迭，当然他们还会提醒你：千万不要太认真。

• 网络怪客（Cracker）：这种黑客已经违背了早期黑客的传统，他们没有什么职业道德的限制。他们把个人利益放在第一位，他们利用自己的电脑技术在网络上从事着非法活动，这类黑客往往被人与罪犯联系起来，他们的行动往往会给其他人造成很大的经济损失。可以说“网络骇客”已成为网络安全的一大隐患。

应该指出的是，上面的分类只是一种大致的、概略的描述。在个性相异的黑客群体中，用贴标签的办法去寻找黑客，恐怕是不会有什么结果的。用简单粗暴的、千篇一律的办法去对待黑客也是错误的，并不是所有的黑客都是电脑捣蛋分子。

事实上黑客、骇客、怪客，是一字之别，对于掌握远程攻击的年轻人来说，是否信守真正意义上的黑客守则，能否继承黑客传统，更多地决定于自身的道德品质和价值取向。

1.2 远程攻击的一般过程和动机分析

可以肯定地说，黑客的价值是通过远程攻击体现出来的。黑客编写工具软件是为了远程攻击；黑客之间的交流更多的内容也是如何进行远程攻击。仅从纯粹技术角度来看，远程攻击是一种远程控制技术，但由于其发动者的区别，其性质也有所不同。但是有一点是肯定的，远程攻击未获得远程计算机使用者授权而登录并取得一定的控制权，无论是善意还是恶意的，都是一种入侵行为，这也是远程攻击与其他远程控制技术（如远程协助）本质上的区别。

1.2.1 远程攻击过程分析

完整意义上的远程攻击是一种动机明确、精心谋划、步骤严密的针对某一特定对象（如某网络服务器）而发生的计算机远程控制行为。下面对远程攻击的过程展开分析，通过这种分析，我们可以看到黑客入侵的作业流程和攻击计划的实施脉络。

1. 收集目标信息

正如狩猎者选择猎物之前，需要知晓猎物的生活习性和作息规律，黑客在进行远程攻击之前，要做的第一件事是通过网络收集攻击对象的信息。收集目标信息分为两个层次，收集攻击目标的一般信息和收集目标的管理员信息。后者的获得更有助于后面的攻击模拟测试和攻击实战操作，但获得该信息更具技术难度。当然，对于某些远程攻击行为来讲，知道对方的 IP 地址、信箱地址、网站主页就可以进行攻击了，不过这种攻击的打击力度相对要弱一些。

至于选择何者为攻击目标，收集目标的哪些信息，是由黑客的行为动机决定的，“为什么要做这件事？”这个问题只能由黑客自己回答，我们暂时对此不进行评论。我们关心的是，攻击是如何开始实施的。

2. 隐藏自身的 IP 地址

远程攻击是非法入侵行为，类似于入室行窃。资深的黑客都清楚隐藏自己的 IP 地址的重要性，留给对方的任何蛛丝马迹，都将意味着自己付出代价的那一天的提前来临。是否具备高明的“隐身术”已经是评判一个远程攻击者技术水平的重要标准。

3. 攻击模拟测试

进行攻击模拟测试的一个前提是确认对方所使用的操作系统，并熟知该操作系统的系统漏洞。在模拟测试中，要建立一个与攻击目标一致的环境（至少要有与攻击目标配置相同或配置基本一致的计算机系统）。

攻击模拟测试类似于自己和自己对弈，要求测试者从攻击方和防御方两个角度考虑问题：

一、该攻击行为对于攻击方来讲，能否达到预期目的；

二、而对于防御方来讲，该攻击行为看上去像什么。

通过检测“防御方”的日志文件，可以了解到攻击行为以及入侵“痕迹”留在目标系统的信息。这些信息无疑对攻击计划的实施具有指导作用，至少它能告诉入侵者应删除哪些文件来毁灭入侵的证据。

需要提及的是，模拟测试对于入侵者来讲，不仅在攻击筹划阶段很重要，在攻击阶段，如果攻击进程与实验进程不一致，进行相应的模拟测试，就更有重要意义了。模拟测试结果与实际情况越一致，下一步操作达到目的的几率将越高。

4. 准备攻击工具

远程攻击工具种类繁多，但黑客选择哪一类工具软件，一般来讲会考虑以下几个方面：

• 选择自己最熟悉的。那些边看软件“帮助”，边实施攻击的人，无疑失败和被捉住的机会更多一些。

• 在使用一个工具与使用两个工具皆可得的情况下，优先考虑两个工具配合使用。这些工具的配合使用是否方便，主要依赖于这些工具能否简单地作为外部模块附加到一个工具上，对此一般要预先进行工具配合使用的测试。配合得当的两个工具，强强联合，效果会更好。

• 选择和使用扫描工具要慎重。扫描工具是远程攻击最常用也是最重要的武器，但也是最危险的，一旦攻击目标的系统管理员使用了反扫描技术，扫描行为往往要暴露无遗。

• 使用自己编写的攻击软件。对于攻击目标进行缜密分析后，在对使用现成的攻击工具没有把握的情况下，自己动手给对方“量身定做”一个软件，是最有挑战性的，实际上许多攻击软件都是这样出炉的。

5. 实施攻击行动

实际上，从扫描目标系统开始即进入了攻击实战阶段，因为系统扫描已经被网络安全管理人员看成一种远程攻击行为。的确，系统扫描往往是进行攻击的第一步，黑客一旦找到系统漏洞，下一步就是藉此进入系统，进行删改、下载数据文件以及获得系统控制权或植入木马进行远程控制等活动。

1.2.2 远程攻击动机分析

人们常常困惑于这样一个问题，既然远程攻击是非法的，黑客为什么还要频频发动？他们的行为是什么驱使的？事实上不是所有的远程攻击动机都是居心险恶的，黑客远程攻击动机可

以归纳为下面几种。

1. 恶作剧

以 Funny Trojan 和 Ackcmd 等木马程序为代表的部分木马程序是恶作剧的高手的杰作，它们不具有窃取植入端密码、格式化磁盘驱动器等会造成重大伤害的功能，而只会调皮地打开 CD-ROM。黑客的恶作剧应该使那些对远程攻击和网络安全的重要性不以为然的人有所清醒。

2. 好奇心

有报道说，黑客们的年龄以 14～25 岁居多，好奇心是年轻人的共性。有些黑客将木马程序散布出去时，只是想要知道这只木马程序有什么功能，能把对方的计算机“玩”到什么地步。他可能在试完木马的功能后就把这程序给遗忘了，然而，这却会让有心者有机可趁，因为他们可以利用扫描工具找到这个被植入端的木马程序，然后利用它进行破坏。

3. 借取硬盘空间

有些人进行远程侵入只是要利用别人的计算机作为“储存中心”。有些计算机数据储存空间大、频带很宽且对于异常的网络传输量及存取速度没有洞察力，黑客常选择这样的计算机来寄存入侵工具。这种形式的受害者由于只有频宽及少许的储存空间被“借走”，所以受害者可能一直都不会发现。虽然目前的硬盘容量已经今非昔比，但有些黑客更倾向于使用这种方式来寄存攻击工具，因为这样做，虽然不方便，但对逃避检查却非常重要。

4. 窃取信息资料

信息资料电子化，对于我们这个时代的重要性是勿庸置疑的。不同的信息对于不同的人有不同的价值，黑客选择自己喜欢的信息，无论这种信息是否允许被打开，是否被加密。在各种信息中，有关金钱和商业信息是最有诱惑力的，通过窃取计算机上的商业信息获得个人经济利益或进行经济犯罪，是某些黑客们的惯用伎俩。

5. 建立跳板

攻击者首先控制一台远程计算机并植入木马或其他攻击程序，然后远程操作这些程序，通过该计算机，向真正的目标计算机发动进攻，我们所说的跳板，就是这台“中木马”的远程计算机。从外界的角度看起来，完全是“跳板”在发动攻击，这样，攻击者就隐藏了自己的踪迹。对于这种情况，认定攻击是中木马的远程计算机的自身行为，或是被别人利用，难度很大，因为黑客躲在幕后控制所有的攻击行动，得手之后会清除所有他认为不利于自己的“跳板”上的“痕迹”。成为跳板的计算机无疑是黑客攻击的“滩头堡”和日后追查责任的“替罪羊”。

“跳板”攻击又称“转向攻击”，现在已经成为一种攻击网站的重要手段。DDOS（Distributed Denial Of Service Attack，分布式拒绝服务攻击），就是利用很多的被植入端（即大量的跳板）同时发送大量的虚假服务请求封包给网站服务器端，消耗服务器的带宽，直至网站瘫痪。