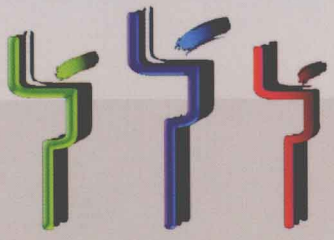
AnQuan

普通高校信息安全系列教材
北京市重点学科共建项目：计算机应用技术

主　编　杜　晔　梁　颖
副主编　黎妹红　张如辉　何永忠

网络信息对抗

WANGLUO
XINXI DUIKANG



北京邮电大学出版社
www.buptpress.com

内容简介

本书详细地介绍了信息对抗基本概念、原理与方法，详尽、具体地披露了攻击技术的真相，以及防范策略和技术实现措施。全书共分3个部分，内容由浅入深，分技术专题进行讨论。第1部分介绍了网络信息对抗的基础知识、计算机及网络系统面临的威胁与黑客攻击方法、网络信息对抗的基础知识及典型的安全评估标准和模型。第2部分是本书的核心内容，介绍了有代表性的网络攻击技术，包括网络扫描、嗅探、欺骗、缓冲区溢出、拒绝服务攻击、恶意代码等手段的原理与实现技术。第3部分根据网络边界防护的要求着重讨论了防御手段，详细介绍了身份认证技术、访问控制技术和两种得到广泛应用的安全设备，即防火墙和入侵检测系统。

本书既可作为信息安全、信息对抗、计算机、通信等专业本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相关技术人员参考和阅读。

图书在版编目(CIP)数据

网络信息对抗/杜晔，梁颖主编. —北京：北京邮电大学出版社，2011.1
ISBN 978-7-5635-2502-7

Ⅰ.①网… Ⅱ.①杜…②梁… Ⅲ.①计算机网络—安全技术 Ⅳ.①TP393.08

中国版本图书馆CIP数据核字(2010)第250277号

书　　名：网络信息对抗
主　　编：杜　晔　梁　颖
责任编辑：付兆华
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京源海印刷有限责任公司
开　　本：787 mm×960 mm　1/16
印　　张：15
字　　数：323千字
印　　数：1—3 000册
版　　次：2011年1月第1版　2011年1月第1次印刷

ISBN 978-7-5635-2502-7　　定　价：27.00

前言

网络给全世界的人们带来了无限的生机，真正实现了无国界的地球村。随着信息化进程的加快，针对网络系统的各种非法入侵、黑客行动及其他的犯罪活动也随之增多，如商业机密被窃取、军事情报遭泄漏、巨额资金被盗取、网络系统被致瘫等。由于多年来网络系统累积下了无数的漏洞，现在我们将面临着更大的威胁，网络中潜伏的攻击者将会以此作为缺口渗入系统。网络信息系统的安全也不再是一个单纯的技术问题，而是一个涉及军事、经济等行业的综合社会问题。

网络战是一场革命，它对未来战争所产生的影响将是巨大的。为在网络战中取得主动权，必须能有效地保证己方网络控制和使用的权力，并阻止敌方控制和使用网络，这必然导致了战争中网络的对抗将日趋激烈。只有牢牢把握对网络的控制权，才能挫败敌人的网上渗透、破坏和攻击，在未来网络战中立于不败之地。

网络信息对抗是研究有关防止敌方攻击信息系统、检测敌方攻击信息系统、恢复破坏的信息系统及如何攻击破坏敌方信息系统的理论和技术的一门科学。在计算机网络日益普及的今天，信息对抗实际上是保护己方的信息、信息处理、信息系统和计算机网络安全空间的同时，并为破坏敌方的信息、信息处理、信息系统和计算机网络空间安全采取的各种行动。

“知己知彼，百战不殆。”要想防，首先要知道如何攻。书中总结了目前网络攻击现状与发展趋势，详细地介绍了计算机及网络系统面临的威胁和黑客攻击方法，具体、详尽地披露了攻击技术的真相及防范策略和技术实现措施。采用尽可能简单的方式向读者讲解技术原理，希望读者在读完这本书后，能对网络信息对抗技术有了进一步的了解。

本书围绕网络攻击和防护技术为中心内容进行展开，共分 3 个部分，内容由浅入深，按照黑客攻击通常采用的步骤进行组织，分技术专题进行讨论。

第 1 部分介绍了网络信息对抗基础，使读者建立起网络信息对抗的基本概念。第 2 部分是本书的核心内容，介绍了代表性的网络攻击技术，包括网络扫描、嗅探、欺骗、缓冲区溢出、拒绝服务攻击、恶意代码等手段的原理与实现技术。第 3 部分着重介绍防御技术，讨论了两种典型安全防护机制，即身份认证与访问控制技术，以及两种得到广泛应用的安全设备，即防火墙与入侵检测系统。

本书分别对每个技术专题制定了详细的实验方案，并对实验的每一个步骤进行了演练。使读者学习后可以参照教程进行实际操作，并通过实践深入理解技术原理。本书可作为信息安全、计算机、通信等专业本科生、硕士研究生的教科书，也适合于网络管理人员、安全维护人员和相关技术人员参考、阅读。

本书编写的目的是为了帮助读者了解网络信息对抗技术与内幕，建立安全意识，增强对于黑客攻击的防范能力，绝不是为怀有不良动机的人提供支持，也不承担因为技术被滥用而产生的连带责任。

在本书的编写过程中，参考了互联网上公布的研究论文和相关资料，主要源于各大学、科研机构、安全网站、安全公司及一些研究网络安全问题的个人，在此向他们表示感谢。由于资料较多，无法一一注明出处。写作过程中所参考的这些资料，其原文版权属于原作者，特此声明。

本书第1～2章由杜晔编写，第3～7章由梁颖编写，第8～9章由黎妹红编写，第11～12章由张如辉编写，第10章由何永忠、黎妹红共同编写，全书由杜晔完成统稿。北京交通大学信息安全体系结构中心的王星、杨爽等参与了编写工作。本书的编写还得到了哈尔滨工程大学王桐，北京交通大学袁中兰、张大伟等多位老师的帮助，在此对他们表示衷心的感谢。本书受到北京市重点学科共建项目：计算机应用技术(XK100040519)、中央高校基本科研业务费(2009JBM023)的资助，在此表示感谢。

由于作者水平有限，书中难免会出现疏漏，加之网络对抗技术纵深宽广，在内容取舍与编排方面，难免有考虑不周之处，恳请广大读者批评指正。

作　者

目 录

第 1 部分 网络信息对抗基础

第 2 部分 攻击技术

第 3 部分 防护技术

第 1 部分
网络信息对抗基础

第1章 绪 论

1.1 网络信息安全现状

随着信息技术的发展，计算机网络已经渗透到人们生活的方方面面，影响到人们的日常生活，改变着人们的生活节奏。从网上游戏到网络课堂，从网上购物到网上炒股，都可以在计算机前完成。根据中国互联网络信息中心 2010 年 7 月发布的《中国互联网络发展状况统计报告》中的显示，截至 2010 年 6 月底，我国网民规模已经突破 4 亿关口，达到了 4.2 亿，较 2009 年年底增加了 3 600 万人，如图 1.1 所示。手机网民用户达到 2.77 亿，在整体网民中的占比攀升至 65.9%，相比 2009 年年底增加了 4 334 万人，增幅达 18.6%。其中，大约有 4 914 万的网民只使用手机上网，占网民总数的 11.7%。互联网商务化程度迅速提高，全国网络购物用户达到 1.4 亿，网上支付、网络购物和网上银行半年用户增长率均在 30%左右，远远超过其他类网络应用。

在网络给人们带来自由开放和极大便利的同时，网络安全事件不断出现，计算机病毒网络化趋势愈来愈明显，垃圾邮件日益猖獗，黑客攻击成指数增长，利用互联网传播有害信息的手段日益翻新……CNNIC 调查显示，仅 2010 年上半年，就有 59.2%的网民在使用互联网过程中遇到过病毒或木马攻击；30.9%的网民账号或密码被盗过；电子商务网站访问者中 89.2%的人担心假冒网站，其中，86.9%的人表示如果无法获得该网站进一步的确认信息，将会选择退出交易。可见，网络与信息安全越来越受到人们的关注，已经成为一个社会话题。

以下是近几年发生的在社会上造成较大影响的网络安全攻击事件。

(1) 熊猫烧香

人们对 2007 年“熊猫烧香”病毒大战记忆犹新，因为病毒在计算机里面生成了很多举着 3 柱香的熊猫图案，一度引起全国计算机用户的议论和恐慌。“熊猫烧香”是一个由 Delphi 工具编写的蠕虫，能终止大量的反病毒软件和防火墙软件进程。病毒会删除扩展

名为.gho 的文件,使用户无法使用 ghost 软件恢复操作系统。“熊猫烧香”病毒能感染系统的.exe、.com、.pif、.src、.html 及.asp 文件,会自动添加病毒网址,导致用户一打开这些网页文件,IE 就会自动链接到指定的病毒网址中下载病毒。在硬盘各个分区下生成文件 autorun.inf 和 setup.exe,可以通过 U 盘和移动硬盘等方式进行传播,并且利用 Windows 系统的自动播放功能来运行,搜索硬盘中的.exe 可执行文件并感染。“熊猫烧香”病毒还可以通过共享文件夹、系统弱口令等多种方式进行传播。

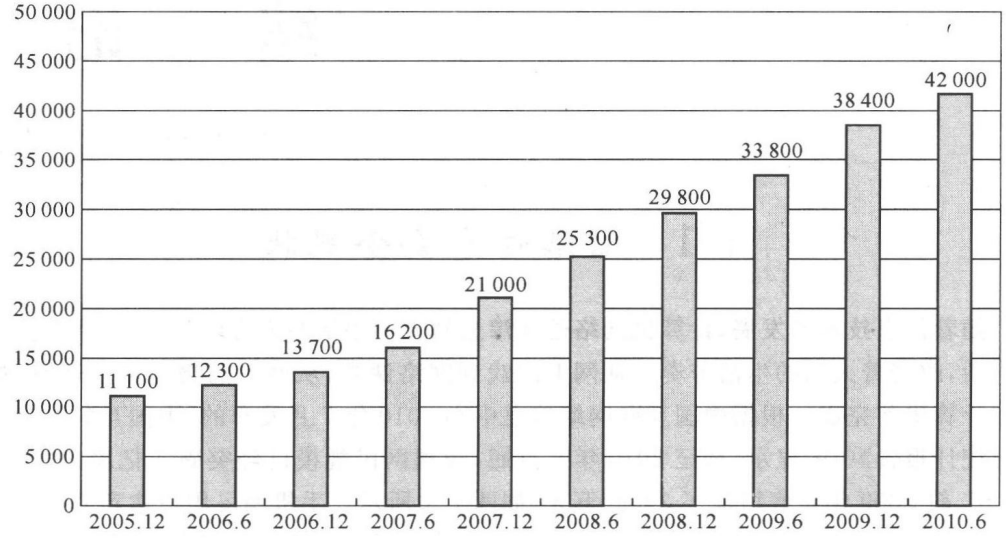


图 1.1 中国网民规模(单位:万人)

(2) 灰鸽子

“灰鸽子”是一个“中国制造”的隐蔽性极强的木马,连续数年被反病毒厂商列为年度十大病毒。当在合法情况下使用时,“灰鸽子”是一款优秀的远程控制软件。但如果拿它做一些非法的事,“灰鸽子”就成了很强大的黑客工具。用户一旦被入侵,计算机将沦为肉鸡,任人宰割。“灰鸽子”使用远程注入、Ring3 级 Rookit 等手段达到隐藏自身的目的。一般它会被人蓄意捆绑到一些所谓的免费软件中,并放到互联网上,诱骗用户下载。因为其具有很强的隐蔽性,所以用户一旦从不知名网站下载并误运行了这些软件,机器就会被控制,而且很难发觉。攻击者可以对感染机器进行多种任务操作,如文件操作、注册表操作、强行视频等。

(3) AV 终结者

“AV 终结者”的特点:①禁用所有杀毒软件及大量的安全辅助工具,让用户计算机失去安全保障;②破坏安全模式,致使用户根本无法进入安全模式清除病毒;③强行关闭带有病毒字样的网页,只要在网页中输入“病毒”相关字样,网页遂被强行关闭,即使是一些安全论坛也无法登录,用户无法通过网络寻求解决办法;④在磁盘根目录下释放

autorun.inf，利用系统自播放功能，如果不加以清理，重装系统以后也可能反复感染。

(4) 磁碟机

“磁碟机”病毒主要通过U盘和局域网ARP攻击传播，中毒的机器无法访问各个安全软件站点，或者从安全站点的官网上下载的安装程序。病毒感染系统可执行文件，能够利用多种手段终止杀毒软件运行，并可导致被感染计算机系统出现蓝屏、死机等现象，严重危害被感染计算机的系统和数据安全。与其他关闭杀毒软件的病毒所不同的是，该病毒利用了多达6种强制关闭杀毒软件和干扰用户查杀的反攻手段，许多自身保护能力不够强壮的杀毒软件在病毒面前纷纷被斩。病毒在每个磁盘下生成pagefile.exe和autorun.inf文件，并每隔几秒检测文件是否存在，修改注册表键值，破坏“显示系统文件”功能。每隔一段时间会检测自己破坏过的显示文件、安全模式、病毒文件等项，如被修改则重新破坏。病毒执行后，会删除病毒主体文件。病毒会链接恶意网址下载大量木马病毒。

(5) 魔兽木马

“魔兽木马”病毒为Windows平台下专门针对魔兽世界网络游戏，以盗取用户游戏账号、密码信息的木马。病毒运行后将自身伪装成系统正常文件，以迷惑用户，通过修改注册表项使病毒在计算机开机时可以自动运行，同时病毒通过线程注入技术绕过防火墙的监视，利用键盘钩子技术在后台记录用户输入的账号、密码信息，并通过鼠标钩子获取用户游戏角色和装备信息，并且病毒尝试链接特定的网站进行病毒的自我更新；病毒还可以修改用户机器重要注册表项，使用户更加难以清除。

(6) QQ尾巴

一种利用QQ传播的木马病毒，俗称“QQ尾巴”或“QQ木马”。该病毒会偷偷藏在用户的系统中，发作时会寻找QQ窗口，给在线上的QQ好友发送诸如“快去这里看看，里面有蛮好的东西”、“我更新了照片，快来看看”之类的假消息，诱惑用户单击进入一个网站，如果有人信以为真单击该链接的话，就会被病毒感染，然后成为毒源，继续传播。

(7) 百度网站被黑

2010年1月12日上午6点左右，全球最大中文搜索引擎——百度——突然出现大规模无法访问的情况，主要表现为跳转到雅虎出错页面、伊朗网页图片等，范围涉及四川、福建、江苏、吉林、浙江、北京、广东等国内绝大部分省市。这次百度大面积故障长达5个小时，也是百度2006年9月以来最大的一次严重断网事故，在国内外互联网界造成了重大影响，称为“史无前例”的百度安全灾难。

(8) 全国断网事件

2009年5月19日，中国十多个省市数以亿计的网民遭遇了罕见的“网络塞车”，这是继2006年中国台湾地震造成海底通信光缆发生中断之后，中国发生的又一起罕见的互联网网络大瘫痪，大多数网民的上网质量都受到了影响。事故当天，由于暴风影音网站域名解析系统遭受黑客攻击，导致电信DNS服务器访问量突增，网络处理性能下降，一时间形成大规模网络瘫痪。

(9) 美军攻击伊拉克防空系统

2003 年伊拉克战争爆发前不久,美国获悉伊拉克从法国购买了用于防空系统的新型计算机打印机,准备通过约旦首都安曼运送到巴格达。美军特工在安曼机场偷梁换柱,将带有病毒的芯片置入打印机内。战争爆发后,美军用指令激活病毒,随后病毒通过打印机侵入伊军防空系统,致使其整个防空系统瘫痪,美军完全掌握了制空权。

(10) 网银诈骗

2009 年 3 月 15 日,央视 3·15 晚会曝光了一名叫"顶狐"的黑客,通过自己制造的木马程序,盗取大量用户的网上银行信息,用很低廉的价格在网上出售,危及大量网银用户的安全。"顶狐"通过木马程序,盗取个人的网银信息,后对盗取回来的信息分类、整理,将密码等信息廉价出售,而网上银行用户信息则以 400 元/GB 的价格打包售出。这导致大量的网银用户存款被盗。沦为"肉鸡"的计算机,除了网银账号受到威胁外,黑客还可以轻易获得用户的炒股账号、网游账号及密码等信息。此外,还会通过远程控制用户的摄像头曝光隐私;窃取沦为"肉鸡"的计算机里的虚拟财产及商业机密。

1.2 网络信息对抗概述

1.2.1 网络信息对抗概念

21 世纪的战争形式将会是什么样的呢? 数字化部队、数字化战场、非线性作战、全维作战、立体空间作战、信息战争、机器人战士、智能战争……新论颇多。冷静观察,这场军事革命狂飙的重心是信息战,实质是推动机械化战争向信息化战争的转变。

1985 年,美国人小阿尔贝·加洛塔首次提到了信息战的概念。信息战旨在以信息为主要武器,打击敌方的认识系统和信息系统,影响、制止或改变敌方决策者的决心及由此引发的敌对行为。单就军事意义来讲,信息战是指战争双方都企图通过控制信息和情报的流动来把握战场主动权,在情报的支援下,综合运用军事欺骗、作战保密、心理战、电子战和对敌方信息系统的实体摧毁、阻断敌方的信息流,并制造虚假的信息,来影响和削弱敌方指挥控制能力。同时,确保自己的指挥控制系统免遭敌人类似的破坏。

信息战的基本模式与传统的作战模式相似,也有防御与进攻,即是一个信息对抗的过程。1991 年的海湾战争虽称不上是一场真正意义上的信息战,但信息战武器在其中功勋卓著。多国部队取得了绝对意义上的"控制信息权",通过计算机病毒武器攻击伊拉克的指挥控制网络系统,使其完全失效,整个伊军就像一盘散沙,只能任人宰割。时隔 8 年,1999 年北约部队对南联盟发动空袭的同时,也利用信息战技术破坏无线电传输、电话设施、雷达传输系统等,以瓦解其电信基础设施。幸亏南联盟政府不具备太多的因特网基础,其军事信息似乎也并不利用互联网进行传输,从而确保其军事力量未遭受空前的削弱。但总体说来,由于敌对双方在电子信息技术方面相差太大,并未出现实际意义上的大

规模信息对抗。由于信息对抗是一个比较新的概念，有关理论仍在发展之中，在此我们做以下初步的探讨。

网络信息对抗是指在信息网络环境中，以信息网络系统为载体，以计算机或计算机网络为目标，围绕信息侦查、信息干扰、信息欺骗、信息攻击，为争夺信息优势而进行的活动的总称。其作战目的是夺取制网络权，作战对象是敌方的计算机网络和信息，作战区域是广阔的计算机网络空间，作战手段是根据计算机技术研制的各种病毒、逻辑炸弹和芯片武器等。

1.2.2 网络信息对抗的基本原理

网络信息对抗的“秘密”武器是智能信息武器，它是计算机病毒、抗计算机病毒程序及对网络实施攻击的程序的总称。智能武器作为一种新型的电子战武器，它的攻击目标就是网络上敌方电子系统的处理器。终极目的就是在一定控制作用下，攻击对方系统中的资源(数据、程序等)，造成敌方系统灾难性的破坏，从而赢得战争的胜利。其作战步骤如下。

① 通过传播，把智能攻击武器注入敌方系统的最薄弱环节(无保护的链路之中)。

② 智能武器通过感染将病毒传播到下一个节点——有保护的链路之中，从而对有保护的节点构成威胁。

③ 通过一级级地感染，最终到达预定目标——敌方指挥中心的计算机系统，用特定的事件和时间激发，对敌方系统造成灾难性的破坏。网络信息对抗与传统的电子对抗的主要差别在于电子对抗的目标是电子系统的接收设备，而信息对杭的目标是敌方系统的处理器(即计算机)。

1.2.3 网络信息对抗的特点

(1) 以夺取和控制制网络权为首要目的

以夺取和控制制网络权为首要目的，是计算机网络战区别于其他作战样式的重要标志。计算机网络将各级指挥控制机构与作战部队甚至单兵有机地组织成一个整体，如果在作战中保持了制网络权，就意味着具有强大的战斗力，如果丧失了制网络权，即使己方人员、装备完好无损，也仍然是一盘散沙，不能形成战斗力。未来战场，谁在作战中控制网络的能力更强、更持久，谁就将夺取战争的胜利。

(2) 人员素质要求高且技术性强

计算机网络战是高技术战争，计算机网络战士要求有很高的专业技术水平。现在博士和科学家也冲到了战争的最前线，发动“计算机战”。在计算机网络战中，网络战士将使用各种先进的网络战武器向敌方进行攻击。此外，计算机网络战涉及的微电子技术、计算机技术、网络安全技术、网络互联技术、数据库管理技术、系统集成技术、调制解调技术、加(解)密技术、人工智能技术及信息获取、传递、处理技术等都是当今的高、精、尖技术。

(3) 行动更加隐蔽且突然

当今社会计算机网络已遍布世界各地,大大缩短了人们的时间、空间距离,因此以网络为依托的计算机网络战也就打破了以往战争中时空距离的限制,可以随时、随地向对方发起攻击。目前,对计算机网络可能的攻击手段,不仅有传统的兵力、火力打击等"硬"的一手,还有诸多"软"的手段,而且许多手段非常隐蔽,不留下任何蛛丝马迹。被攻击者可能无法判定攻击者是谁、它来自何方,难以确定攻击者的真实企图和实力,甚至可能在受到攻击后还毫无察觉。

(4) 效费比高

计算机网络对抗是把攻防联系得更为紧密的作战样式,这种攻防兼备的作战形式提高了计算机网络战的作战效益。一是计算机网络对抗攻防范围广泛。进攻行动隐蔽,攻击速度快,危害性大,危及面宽;计算机网络防御在己方整个计算机网络上实施,对保证整个系统正常运行有巨大作用。二是计算机网络攻防重点是敌我双方的核心系统。一旦核心系统遭受攻击或破坏,就会造成指挥中断。三是计算机网络对抗战的成本低,手段隐蔽,破坏力强。研制新型的计算机病毒武器比研制其他高新技术武器成本要低,而破坏力却并不低,因此,效费比高。

(5) 破坏性是长久的、持续的

在干扰发生以后,它仍然在继续行动,而传统的电子对抗只是在干扰发生期间起作用。所以,网络信息对抗的效果要比电子对抗大许多,它是唯一能胜任破坏战术操作能力的对抗技术。

(6) 网络信息对抗的战斗力可以准确地进行控制

它可以通过编程的方法搜索特定的敌方系统,一旦找到,智能武器就潜伏下来,等待时机行动。网络信息对抗的战斗力包括偷偷地改变系统功能,使系统关机,破坏数据文件和战术程序等。

1.3 网络信息对抗的层次

网络信息对抗主要有以下几个层次。

(1) 实体层次的计算机网络对抗

以常规物理方式直接破坏、摧毁计算机网络系统的实体,完成目标打击和摧毁任务。在平时,主要指敌对势力利用行政管理方面的漏洞对计算机系统进行的破坏活动;在战时,指通过运用高技术明显提高传统武器的威力,直接摧毁敌方的指挥控制中心、网络节点及通信信道。这一层次计算机安全的首要任务是做好重要网络设施的保卫工作,加强场地安全管理,做好供电、接地、灭火的管理,与传统意义上的安全保卫工作的目标相吻合。

(2) 能量层次的计算机网络对抗

敌对双方围绕着制电磁频谱权而展开的物理能量的对抗。敌对双方一方面通过运用