现代电子信息工程理论与技术丛书

网络对抗原理

Principles of Network Countermeasure

胡建伟 汤建龙 杨绍全 编著

西安电子科技大学出版社
http://www.xdupf.com

现代电子信息工程理论与技术丛书

网络对抗原理

胡建伟　汤建龙　杨绍全　编著

西安电子科技大学出版社

2004

内 容 简 介

本书系统地阐述了网络对抗的基本原理和关键技术，主要内容有：目标网络和主机的信息获取、侦察以及截获技术，安全漏洞的挖掘和利用，UNIX 和 Windows 系统的入侵技术，网络协议攻击和分布式攻击技术，Web 攻击技术，恶意代码技术，安全设备和无线网络的对抗技术。

本书取材新颖，概念清晰，可作为信息对抗、通信、电子或计算机相关专业的教材，也可作为相关领域的研究人员和专业技术人员的参考书。

图书在版编目(CIP)**数据**

网络对抗原理／胡建伟等编著. —西安：西安电子科技大学出版社，2004.6

（现代电子信息工程理论与技术丛书）

ISBN 7 – 5606 – 1379 – 9

Ⅰ. 网… Ⅱ. 胡… 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**(2004)**第** 022348 **号**

策　　划　臧延新

责任编辑　潘恩祥　臧延新

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　　**邮编**　710071

http: //www.xduph.com　　E-mail: xdupfxb@pub.xaonline.com

经　　销　新华书店

印刷单位　陕西华沐印刷科技有限责任公司

版　　次　2004 年 6 月第 1 版　2004 年 6 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　**印张**　28.875

字　　数　684 千字

印　　数　1～4 000 册

定　　价　42.00 元

ISBN 7–5606–1379–9/TP・0733

XDUP 1650001−1

前　言

未来高技术战争是以通信网络为基础的信息化战争，谁能占据信息网络的控制权，夺取信息优势，谁就能赢得战争。谁的信息网络系统容易遭受破坏，失去信息优势，谁就会输掉战争。随着网络化、信息化时代的到来，网络正在扮演着越来越重要的角色，对网络的渗透、攻击和防护能力将直接影响一个国家的信息作战能力。

为适应这种形势，教育部于 2000 年新增了信息对抗技术专业。本书就是为配合新专业的建设而编写的。

本书比较系统地阐述了网络对抗的基本内容和关键技术，着重讲述了基本概念和基本技能。在内容编排上，力求由浅入深、循序渐进，分系统进行叙述。

全书共有 6 个部分、18 章，第一部分给出了网络对抗的定义、层次和关键技术以及意义。第二部分讨论了各种目标网络和目标主机的信息获取、侦察技术。第三部分对一些关键漏洞的产生机理和利用方法进行了研究。第四部分专门针对具体的系统所采用的对抗技术进行叙述。第五部分重点阐述了各种恶意代码攻击，如病毒、特洛伊木马和后门等等。第六部分重点介绍了无线局域网和网络安全设备的对抗技术。

本书作为信息对抗技术专业本科生和研究生的教材，参考教学时数为 50～60 学时，实验需另外安排。

本书的第二、三部分由汤建龙编写，其余章节由胡建伟编写，全书由胡建伟统稿，杨绍全审定。

本书在编写过程当中得到了西安电子科技大学电子对抗研究所众多同事的支持和帮助，在此深表谢意。书中不足之处，恳请广大读者批评指正。

编著者

2004 年 1 月

序

西安电子科技大学出版社一直把视角的焦点放在电子信息领域的最新发展和对于生产的应用方面。针对当前新经济时代，信息化水平已成为衡量我国现代化程度和综合国力的主要标志，现在出版“现代电子信息工程理论与技术丛书”，显然是一个十分恰当的时机。这套丛书的主要对象是从事电子信息领域研究和开发的科技工作者、工程师、在读的研究生，以及希望了解该领域发展的各类相关人员。因此本套丛书的重点不在于艰深的理论探讨，而是力求理论联系实际，揭示新应用，发展新领域。总之，我们希望通过这套丛书能帮助读者对电子信息领域的总体、全貌和发展趋势有所了解。

西安电子科技大学出版社一直以电子信息领域的热心读者作为自己的服务对象。这套丛书的好与坏，起的作用大与小都要靠每一位读者来检验。因此在成立编委会和着手编辑这套丛书的时候，我们对读者的对象、读者的需求和读者的兴趣做了多方面的设想。为了使多方面的读者都有所收获，我们力求把每本书每个章节都做到简单明了、深入浅出；每本书都是读者了解电子信息领域的忠实“导游”；每本书都是作者与读者交换思想和促膝谈心的最佳机会。

西安电子科技大学出版社一直有着广泛且相对联系紧密的作者群，他们大多是熟悉电子信息领域发展的一线专家，其中不乏是该领域的知名学者、教授，正是由于这么一个群体，使我们有信心把这套丛书的学术水平和实用价值提到一个新的水平。

尽管如此，这套丛书的编撰还是新的尝试，作者和编辑们缺乏经验，加之本领域发展十分迅速，使我们难于全面把握。衷心希望每一位读者都作为这套丛书的实践检验者，你们的每一条意见，将是丛书提高的重要依据。

丛书编委会

现代电子信息工程理论与技术丛书编委会

目　　录

第一部分　网络对抗综述及信息获取技术

第二部分 代码漏洞利用

第三部分 网 络 攻 击

第四部分 系 统 攻 击

第五部分 恶意代码技术

第六分部 高 级 技 术

第一部分
网络对抗综述及信息获取技术

第 1 章　网络对抗综述

当今世界，计算机网络的触角已伸向了地球的各个角落，渗入到每个领域，它正在对人们的生活和工作方式产生着前所未有的影响，日渐成为人们生活中不可缺少的组成部分。同时，计算机网络信息安全已成为影响国家和人民利益的一大命脉。美国未来学家认为：人们的工作方式就是他们发动战争的方式。全球的这种网络化趋势决定了人们为了政治、军事、经济和文化的利益必然会在计算机网络领域展开异常激烈的“对抗”。

(1) 军网和民网走向融合。为减少投入、共享信息、增加迂回路由，军网和民网相互连接起来。虽然这在一定程度上会对军网的安全性带来影响，但从总体上讲，系统的整体效能有了较大的提高。因此，各国军事网络只有极少数核心部分完全独立，其余网络通过各种方式与民网相连。美军有 95%的网络与民用网络相连，军民网络相互融合的趋势已不可逆转。

(2) 战略、战役、战术网络走向融合。未来局部战争，战略、战役、战术界限模糊，使得战场网、战役网和战略网的区分更加困难，战略性信息、战役性信息和战术性信息在集成化网络环境中有序流动，呈现出紧密互联、相互融合的特点。一体化将是网络发展的必然归宿。

而事实上，网络世界从它开始形成之日起就不太平，或明或暗、或隐或现的网络对抗一直伴随着网络发展的整个过程。

1.1　网络对抗实例

(1) 1979 年，美国少年米尼克成功打入“北美防空指挥中心电脑系统”，偷看了美国瞄准苏联所有核弹头的绝密数据资料。

(2) 1990 年的海湾战争，美军首次把网络攻击手段应用于实战。早在战前，美军就在伊拉克进口的一批计算机散件中预置了带病毒芯片。战争开始不久，伊拉克整个防空指挥控制网络即遭受病毒感染，组织指挥陷入混乱，几乎丧失了防空作战能力。

(3) 1995 年 9 月 18 日，一名年轻的美空军上尉利用一台普通计算机在众目睽睽之下拨号进入互联网，几分钟内便进入美海军在大西洋舰队的指挥系统，在舰队司令懵然不知的情况下，轻而易举地控制了该舰队的军舰，一下子成为了这个舰队的“秘密司令”。这并非是天方夜谭，而是美国“联合勇士”演习的精彩片断，这也就是未来网络战的一种作战景象。

(4) 1999 年 2 月，据英国《星期日商报》报道，英国航空航天部在对其包括通信卫星在内的所有通讯情报设施进行的检测中，忽然发现“天网”系统 4 颗军事卫星中的一颗卫星，不是拒绝接收信号，就是反应迟钝。当天，英国航空航天部就组织专家“会诊”。这时，忽然来了一封电子邮件，声称一个黑客团体已经控制了“天网”卫星，一个由电脑专家、密码专家和航空航天专家组成的黑客团体，在两周前修改了这颗卫星的正常程序，切断了它和航空航天部的联系，改变了卫星飞行轨道。他们扬言，英国政府必须支付赎金，才能收回卫星的控制权，否则他们就要把这颗卫星变成废铁。

(5) 1999 年 4 月，美国《新闻周刊》透露，克林顿批准了由美中情局实施的绝密计划：利用电脑黑客，通过入侵南联盟总统米洛舍维奇及其他领导人的外国银行账户来颠覆这个政府。

(6) 1999 年 3 月，南联盟及俄罗斯计算机高手成功地侵入美国白宫网站，使该网站当天无法工作。4 月 4 日，贝尔格莱德黑客使用“宏”病毒对北约进行攻击，使其通信一度陷入瘫痪。美国海军陆战队带有作战信息的邮件服务器，几乎全被“梅丽莎”病毒阻塞。美军“尼米兹”号航空母舰的指挥控制系统，也因黑客袭击而被迫中断 3 个多小时。从军事的角度来审视这些事件，或许可以认为，对一个国家进行战略打击，点击鼠标比抠动扳机更有效。

(7) 2000 年 2 月，美国著名的几大网站雅虎、亚马逊、CNN 等相继遭到不明身份的“黑客”分布式拒绝服务攻击，导致网站瘫痪、服务中断，引起了各国政府和企业界的极大关注。仅就雅虎网站被袭击的情况来看，攻击者共调用了约 3500 台计算机同时向雅虎发送信息，发送量达 10 亿兆位每秒，远远超出了其信息处理能力，完全堵塞了网络系统，致使雅虎被迫中断服务达数小时。

和平时期发生的网络攻击事件，损失的是商业利益和对人们私人空间的侵害，可如果网络攻击行为的主体是一个国家对另一个国家、一个作战集团对另一个作战集团的行动，那么所造成的后果将不堪设想。网络战争已经成为一种特殊形式的战争。因此，为了在日益尖锐的网络对抗中掌握主动权，各国政府、军队都在加紧网络安全建设，特别在网络对抗中的关键技术研究方面更是投入了重要力量。

1.2 网络对抗定义

网络对抗，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，围绕信息侦察、信息干扰、信息欺骗、信息攻(反)击，为争夺信息优势而进行的活动的总称。

网络对抗的目的是获取和保持信息网络优势，掌握并确保网络空间的制信息权。主要包括保障己方网络信息系统安全及瓦解、破坏敌方网络信息系统的方法手段等。网络对抗

以敌方的战略目标作为首要进攻对象，如军队的 C^4ISR 系统、国家的决策指挥枢纽系统、通信中枢系统等等。大体上，网络对抗涉及到网络侦察、网络攻击和网络防护三个方面的关键技术。

1.3　网络对抗的关键技术

1.3.1　网络侦察

在信息网络对抗中，充分利用信息网络系统，采取多种措施，全方位、有重点地拦截对方信息网络上所传输的信息流，是确保对抗主动权的关键环节。

信息网络上传输的信息，特别是作战指挥控制信息，是传输方尽力保护的资源，也是对方企图全力截获的信息流。通过全面拦截网上的信息，可全面了解敌情，为确定后续采用的对抗措施奠定基础。

网络信息侦察可分为主动式网络信息侦察和被动式网络信息侦察技术。

主动式的网络信息侦察包括各种踩点、扫描技术。被动式的网络信息侦察包括无线电窃听、网络数据嗅探等。在实施网络侦察过程当中，应尽量隐蔽自己的身份，重点截流信息网络的指令信息、协调信息和反馈信息，借助军事专家、情报专家和计算机专家的力量，综合利用各种信息处理技术，最大化地提高信息侦察的效益。

1.3.2　网络攻击

网络攻击作为一种全新的作战手段，其实质就是指利用敌方信息系统自身存在的安全漏洞和其电子设备的易损性，通过使用网络命令和专用软件，进入敌方网络系统，或使用强电磁脉冲武器摧毁其硬件设施的攻击。目的是通过网络攻击形成网络优势，进而夺取制网络权，对目标信息网络的关键主机、节点、网络，通过实施信息攻击，达到破坏对方网络系统的目的。

信息网络通常是由中心控制单元、节点和有线及无线信道组成的多层次、多结构、连接复杂的信息网络体系。破坏信息网络体系，就会从总体上削弱对方运用信息网络的效果。

网络攻击的手段非常多，包括电磁干扰目标网络正常运作，利用各种黑客技术进行网络入侵、信息欺骗和干扰，传播感染病毒，使目标网络拒绝服务等等。这些网络攻击的目的都是围绕制信息权展开的。

1.3.3　网络防护

网络攻击，作为一种对未来战争胜负具有重大影响的全新作战手段，作为具有战略威慑力的信息战利剑，在一定程度上改变了弱守强攻的传统战争法则，为劣势一方开辟了以劣胜优的新途径。同时也是一把双刃剑，它要求人们在重点研究发展网络攻击手段和战法，不断提高网络攻击能力的同时，还应不断增强信息系统的安全防御能力，形成以攻为主，攻防兼备的网络战能力。

网络防护是指为保护己方计算机网络和设备的正常工作、信息数据的安全而采取的措施和行动。网络攻击和网络防护是矛与盾的关系，由于网络攻击的手段是多样的、发展变

化的，因此在建立网络安全防护体系时，必须走管理和技术相结合的道路。网络安全防护涉及面很宽，从技术层面上讲主要包括防火墙技术、入侵检测技术、病毒防护技术、密码技术、身份认证技术、(信源、信道)欺骗技术等。

1.4 网络对抗的特点

网络对抗有以下一些特点：

(1) 没有国界。在网络空间中，距离的概念将消失，网络战场疆域不定。网络作战，其作战范围瞬息万变，网络所能覆盖的都是可能的作战地域，而所有网络都是可能的作战目标。传统作战改变作战方向需要长时间的兵力机动，而网上作战，只需点击鼠标即可完成作战地域、作战方向、作战目标和作战兵力的改变，前一个进攻节点与后一个进攻节点在地域上也许近在咫尺，也许相距万里。

(2) 没有痕迹。网络行动踏雪无痕。网络对抗不见刀光剑影，炮火阵阵、车轮滚滚，施放病毒、窃取数据、引爆网络炸弹都在瞬间完成，可以说是来无影，去无踪。网络作战行动速度快，时间短，敌方还没有来得及发现，网络行动就已经完成。网络行动经常以正常的信息交流形式出现，无迹可查、无影可随，具有很大的欺骗性和隐蔽性，难以一一检测和监视，也很难提前预设针对性强的应对措施。

(3) 作战效果难以评估。网战效果难以预测，同样一次网络攻击行动，可能对敌丝毫无损，也可能修改窃取其数据，阻断其网络通道，使敌遭受惨重损失，甚至可能完全瘫痪其指挥控制系统，导致其社会混乱，经济崩溃，达到不进行火力战而屈人的目的。俄罗斯已将网络攻击确定为大规模毁灭性武器，美军也有人认为网络攻击属于大规模毁灭性武器。

(4) 鼠标点击就是扣动扳机。网络对抗主要有两种形式，一是进行网上技术和信息支援，提供网络最新进攻技术和手段，或者提供敌对网络的信息情报等；二是在网络部队指挥员的统一组织下，直接参与网络作战。它改变了传统作战之前人力和物力集中的方式，而是技能和智能的汇集，通过网上点击鼠标的方式实现。这种形式的改变，意味着战前行动将由人力密集型向知识密集型转化。

(5) 人民战争。未来的网络作战并非是单靠军人利用计算机对敌军事信息系统进行的攻击，而是“所有具备网络攻击能力的人”，对敌交通、金融、贸易、军事等各个领域的全面攻击，以达到制止战争的目的。正因为信息技术的军民通用性和计算机网络的相互关联性，使得网络作战力量趋于大众化，不管是国家还是个人，不管是军人还是平民，只要具备网络攻击能力，都可以在计算机网络战中一展身手。

1.5 网络对抗的层次[8]

第一个层次，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、网络节点以及通信信道。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。

第二个层次，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。敌对双方通过运用强大的物理能量干扰、压制或嵌入对方的信息网络、乃至像热武器一样直接摧毁敌方的信息系统(如高能射频枪、脉冲变压器弹等)；另一方面又通过运用探测物理能量的技术手段对计算机辐射信号进行采集与分析，获取秘密信息。这一层次计算机安全的对策主要是做好计算机设施的防电磁泄露、抗电磁脉冲干扰，在重要部位安装干扰器、建设屏蔽机房等。

第三个层次，逻辑层次的计算机网络对抗：即运用逻辑手段破坏敌方的网络系统，保护己方的网络系统的对抗。这个概念接近于美国人讲的 Cyberspace Warfare，包括计算机病毒对抗、黑客对抗、密码对抗、软件对抗，芯片陷阱等多种形式。它与计算机网络在物理能量领域的对抗的区别表现在：

(1) 在逻辑的对抗中获得制信息权的决定因素是逻辑的而不是物理能量的，取决于对信息系统本身的技术掌握水平，是知识和智力的较量，而不是电磁能量强弱的较量。

(2) 计算机网络空间(Cyberspace)成为战场，消除了地理空间的界限，使得对抗双方的前方、后方、前沿、纵深的概念变得模糊，进攻和防御的界限很难划分。

(3) 虽然它基本上属于对系统的软破坏，但信息的泄露、篡改、丢失乃至网络的瘫痪同样会带来致命的后果。有时它也能引起对系统的硬破坏。

(4) 由于计算机系统本质上的脆弱性，为了对付内行的系统入侵者，信息系统安全的核心手段应该是逻辑的(如访问控制、加密等)，而不是物理的(如机房进出入制度等)，即通过对系统软硬件的逻辑结构设计从技术体制上保证信息的安全。

网络技术惊人的发展速度和网络日益扩大的覆盖面，使逻辑意义上的网络对抗将不仅局限在军事领域，而且会成为波及整个社会大系统的全面抗衡和较量，具有突发性、隐蔽性、随机性、波及性和全方位性。

第四个层次，超逻辑层次(也可叫做超技术层次)的计算机网络对抗：即网络空间中面向信息的超逻辑形式的对抗。网络对抗并不总是表现为技术的、逻辑的对抗形式，如国内外敌对势力利用计算机网络进行反动宣传、传播谣言、蛊惑人心，进行情报窃取和情报欺骗，针对敌方军民进行心理战等。这些都已经超出了网络的技术设计的范畴，属于对网络的管理、监察和控制的问题。利用黑客技术篡改股市数据以及对股市数据的完整性保护属于逻辑的对抗，而直接发表虚假信息欺骗大众则属于超逻辑的对抗。后一种意义上的网络对抗瞄准了人性的弱点，运用政治的、经济的、人文的、法制的、舆论的、攻心的等各种手段，打击对方的意志、意念和认知系统，往往以伪装、欺诈、谣言、诽谤、恐吓等形式出现。

超逻辑层次的对抗与逻辑层次的对抗的主要区别是：它把信息看作为难以用形式化语言描述的、不可分析的对象，其概念更加接近于信息的本质内涵，类似于历史上对信息战概念的传统理解，其战例和作战理论古已有之，并且在运用了现代网络技术后其形式已变得更加丰富多彩。虽然这一层次的对抗也要使用大量高科技，但它本质上是对技术的超越，其关键因素是策划创意的艺术，而不是具体的技术。后者是逻辑上可递归的，本质上可计算的；前者则是对逻辑的超越，本质上不存在可行的求解算法，否则敌方的作战意图、社会政治动向就可以准确地算出来了。显然后者属于更高层次的信息类型。

以上四种网络对抗的概念既有本质上的内在联系，又有各自不同的展开空间：第一个