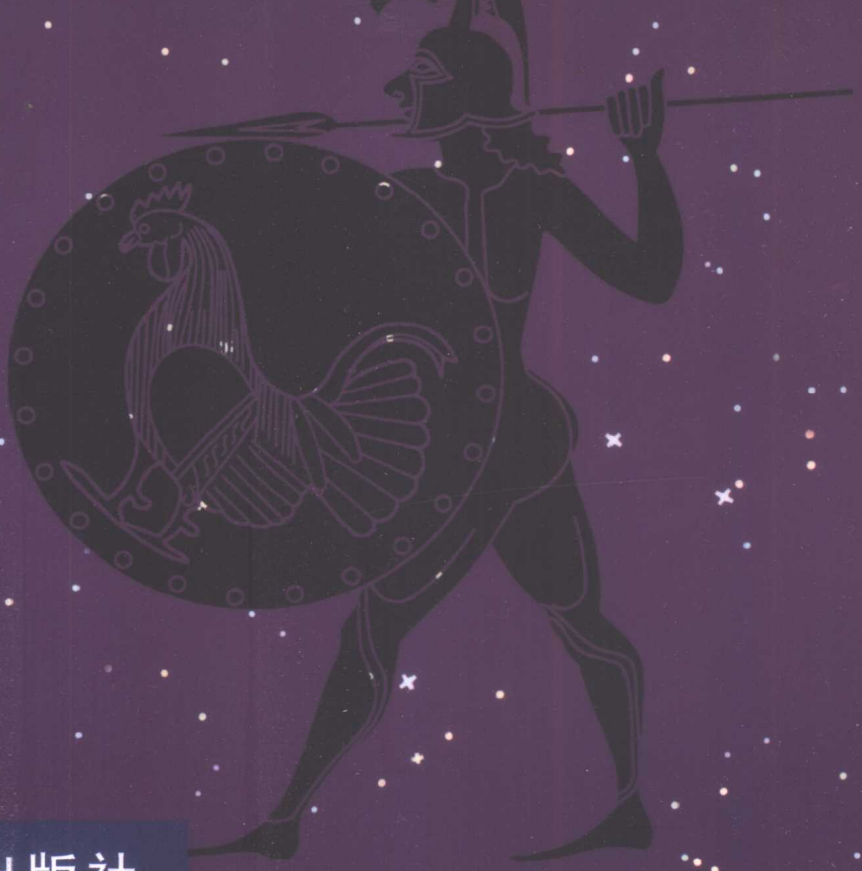
flying

防守反击

黑客攻击手段分析与防范

余伟建 严忠军
卢科霞 王 凌 编著

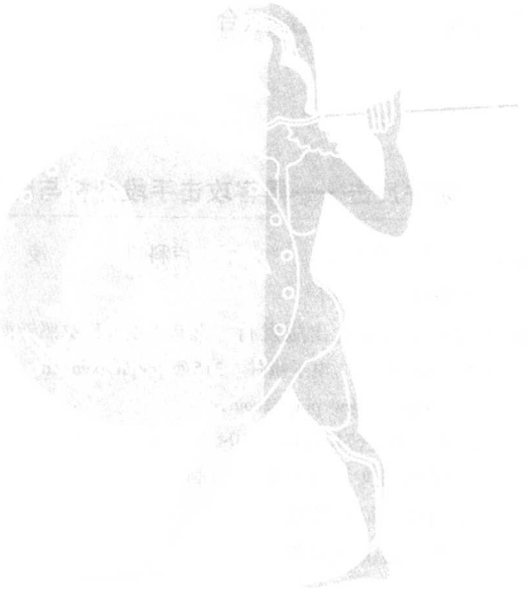


人民邮电出版社
www.pptph.com.cn

防守反击

黑客攻击手段分析与防范

余伟建 严忠军
卢科霞 王 凌 编著



人民邮电出版社

图书在版编目（CIP）数据

防守反击：黑客攻击手段分析与防范 / 余伟建，卢科霞，严忠军编著.
—北京：人民邮电出版社，2001.8
ISBN 7-115-09589-2

Ⅰ．防…　Ⅱ．①余… ②卢… ③严…　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（2001）第 053932 号

内容提要

本书全面介绍了网络安全和黑客防范技术。为了能够防范黑客，本书首先分析网络上的各种攻击手段，然后针对不同的攻击方法给出了相应的防范策略。全书共分为 12 章，包括特洛伊木马、网络炸弹、网络监听与 Sniffer、扫描器、密码破解、Web 攻防、拒绝服务攻击、欺骗攻击、常见的系统漏洞和计算机病毒等方面的内容。

本书除了介绍相关理论以外，同时还对一些相关软件的使用方法进行了详细说明，重要的部分还从源程序代码进行分析，让读者了解黑客整个的攻击过程，从而加强读者的防范意识、提高读者 “反黑” 的技术水平。

本书内容丰富，通俗易懂，深入浅出，适合于那些想加强自己系统的安全性和对黑客防范技术感兴趣的读者阅读。

防守反击——黑客攻击手段分析与防范

◆编　　著　余伟建　严忠军　卢科霞　王　凌
责任编辑　张立科
◆ 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@ pptph.com.cn
网址　http://www.pptph.com.cn
读者热线:010-67129212　010-67129211(传真)
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本:787 × 1092　1/16
印张:17.75
字数:426 千字　　2001 年 8 月第 1 版
印数:1 - 5 000 册　　2001 年 8 月北京第 1 次印刷

ISBN 7-115-09589-2/TP·2429

定价:25.00 元

关于本书

随着计算机网络飞速发展，享受着互联网带来的便利与新的生活方式的人们却不得不面对来自网络安全方面的威胁。在信息爆炸的 21 世纪，Internet 的应用更加广泛，而大多数的网民却不了解自己的系统以及 Internet 所固有的缺陷，相信任何一位网民或企业都不希望自己的重要信息或者资料被泄漏或被窃取。

Internet 已经将世界连成一个整体，上网的人越来越多，但是由于 Internet 本身设计的缺陷及其开放性，使它很容易受到黑客攻击。目前市场上有许多关于网络安全方面的书籍，而绝大多数书籍局限于理论的介绍与分析，读者看后不知所云。针对这一情况，本书详尽地分析讲解了一些黑客攻击的例子和攻击工具。我们写这本书的真正目的绝对不是想要教人去做黑客，而是本着“知己知彼，百战不殆”的思想让大家去“认识黑客、了解黑客、防范黑客”。

本书的目的在于让人们更清楚地了解来自网络的安全威胁，了解黑客以及黑客的攻击手段，让读者学会怎样在互联网上保护自己的权益不受侵害。

全书共分 12 章，第 1 章介绍一些关于黑客文化和黑客技术的背景知识，从第 2 章到第 12 章分别介绍了各种黑客的基本攻击手段（如特洛伊木马、拒绝服务、IP 欺骗）以及相关的攻击软件（像冰河木马、网络刺客、NetXRay、扫描器）并对各种攻击手段给出相应的防范措施；同时还介绍了各种系统存在的漏洞以及修补措施、密码破解、病毒源码分析以及各种防病毒软件等方面的知识。

每一章都采用如下的思路来介绍：首先介绍每一种攻击方法的基本概念、背景知识以及带来的危害，然后介绍实现攻击的相关软件，再讲解攻击的源代码程序的编写方法，有了上面的知识，最后我们介绍了相应的防范措施。

本书具有如下特色：

通俗性：力求避开一些晦涩的专业词语，用一些通俗易懂的语言，提起读者的兴趣。

多层次性：适合不同类型的读者，书中的黑客攻击背景方面的知识适合那些想了解黑客的人。黑客软件的应用适合那些初入门会上网对黑客技术有兴趣的人，关于黑客源代码的编写方面的内容适合高层编程人员做进一步的研究之用。

实用性：书中对于各种黑客的攻击手段都有相应的防范措施。本书的重点在于“防”！对读者防范各种黑客攻击很有实际的意义。

相信广大读者在读了本书以后，一定会受益匪浅。祝大家一切顺利！

编者

2001 年 8 月

目　录

第 1 章　黑客文化和黑客技术概述

全球信息高速公路的建设，Internet/Intranet 的发展，将对整个社会的科学与技术、经济与文化带来巨大的推动和冲击，同时也给我们带来了许多挑战。Internet/Intranet 信息安全是一个综合的系统工程，需要我们在网络安全技术方面的研究和应用领域做长期的攻关和规划。

在 Internet/Intranet 的大量应用中，Internet/Intranet 安全面临着重大的挑战。事实上，资源共享和信息安全历来是一对矛盾。近年来，随着 Internet/Intranet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的信息安全问题也日益突出。据美国 FBI 统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机入侵事件。

一般认为，计算机网络系统的安全威胁主要来自于黑客攻击。黑客攻击早在主机终端的时代就已经出现了，随着 Internet 的发展，现代黑客则从以系统为主的攻击转变为以网络为主的攻击。新的手法包括：通过网络监听获取网上用户的账号和密码；监听密钥分配过程，攻击密钥管理服务器，得到密钥或者认证码，从而取得合法资格；利用 UNIX 操作系统提供的守护进程缺省账户进行攻击，如 Telnet Daemon、FTP Daemon 和 RPC Daemon 等；利用 Finger 命令收集信息，提高自己的攻击能力；利用 Send mail，采用 Debug、Wizard 和 Pipe 等进行攻击；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等。目前，已知的黑客攻击手段多达 500 余种！

攻击的结果可以造成 Internet 瘫痪或者引起 Internet 商业的经济损失。人们面临的计算机网络系统的安全威胁日益严重，因而，我们非常有必要分析黑客，从而在“知己知彼”的基础上提高我们对黑客的认识，进而采取相应的措施，以达到“百战不殆”的效果。

1.1　黑客文化

1.1.1　Hacker 与 Cracker

Hacker，国内一般译为“黑客”或“骇客”。Hacker 至少包含这样的含义：必须是技术上的行家，必须是热衷于解决问题、克服限制的人，他们对任何操作系统神秘而深奥的工作方式由衷地感兴趣。Hacker 通常是些程序员。他们同时掌握操作系统和编程语言方面的高级知识。他们能发现系统中所存在的安全漏洞以及导致那些漏洞的原因。Hacker 们不停地探索新的知识，自由地共享他们的发现。他们从来没有、也永远不会存心破坏数据。

以下是在世界范围内得到广泛认可的 Hacker 行为准则：

（1）不恶意破坏任何的系统，这样做只会给自己带来麻烦，恶意破坏他人的软件或系统将导致法律刑责。

（2）不修改任何系统文件，如果只是为了要进入系统而修改它，那么请在达到目的后将

它改回原状。

（3）不要轻易地将要攻击的站点告诉不信任的朋友。

（4）不要在 BBS 上或者电话中谈论自己所做的有关攻击的事情。

（5）在发表文章的时候不要使用真名。

（6）正在入侵的时候，不要随意离开计算机。

（7）不要侵入或破坏政府机关的主机。

（8）将笔记放在安全的地方。

（9）想要成为“Hacker”就要真正地去攻击并且读遍所有有关系统安全或系统漏洞的文件。

（10）侵入计算机中的账号不得清除或修改。

（11）不得修改系统档案，如果为了隐藏自己的侵入而作的修改则不在此限，但仍须维持原来系统的安全性，不得因得到系统的控制权而将门户大开。

（12）不将已破解的账号与他人分享。

Cracker 是指那些强行闯入远端系统或者以某种目的干扰远端系统完整性的人。Cracker 通过获取未授权的访问权限，破坏重要的数据，拒绝合法的用户服务或只是使他们的目标产生一些小问题。Cracker 是很容易被区分的，这是因为他们的行为具有恶意性。

由此可以看出，真正给系统或网络构成威胁的是 Cracker，通常所说的黑客应该是指 Cracker。因此要防范的也应该是 Cracker。

1.1.2 对黑客技术的思考

黑客技术，简单地说，是对计算机系统和网络的缺陷和漏洞的发现，以及针对这些缺陷实施攻击的技术。这里说的缺陷，包括软件缺陷、硬件缺陷、网络协议缺陷、管理缺陷和人为的失误等。很显然，黑客技术对网络具有破坏能力。近段时间，一个很普通的黑客攻击手段把世界上一些顶级的大网站轮流考验了一遍，结果证明即使是如 YaHoo 这样具有雄厚的技术支持的高性能商业网站，黑客都可以给他们带来经济损失。这在一定程度上损害了人们对 Internet 和电子商务的信心，也引起了人们对黑客的密切关注和对黑客技术的思考。

在这里要讨论的一个主要问题是：研究黑客技术对国家是否有利？

1. 黑客技术属于科学技术的范畴

黑客技术是 Internet 上的一个客观存在，对此无须讳言。和国防科学技术一样，黑客技术既有攻击性，也有防护的作用。黑客技术不断地促使计算机和网络产品供应商改善他们的产品，对整个 Internet 的发展一直起着推动作用。就像不能因为原子弹具有强大的破坏力而否认制造原子弹是高科技一样，也不能因为黑客技术具有对网络的破坏力而将其摒弃于科学技术的大门之外。发现并实现黑客技术通常要求这个人对计算机和网络非常精通，发现并证实一个计算机系统漏洞可能需要做大量测试、分析大量代码和长时间的程序编写，这和一个科学家在实验室中埋头苦干没有太大的区别。发现者不同于那些在网上寻找并使用别人已经写好的黑客软件的人。这个区别就好像武器发明者和使用者的区别。一个国家可以立法禁止民间组织和个人拥有枪枝，但是，却不能禁止个人拥有黑客技术。

2. 辨证地看待黑客技术

黑客技术的作用是双面的。和一切科学技术一样，黑客技术的好坏取决于使用它的人。

计算机系统和网络漏洞的不断发现促使产品开发商修补产品的安全缺陷，同时也使他们在设计时更加注意安全。研究过黑客技术的管理员会把他的系统和网络配置得更安全。如果没有那些公布重大漏洞发现并提出修补建议的黑客，Internet 不可能像今天这样让人们受益，也不会有今天这么强壮（相对于以前而言）。利用黑客技术从事非法破坏活动为自己谋取私利，理所当然是遭人唾弃的行为。这种人不是把精力放在对系统缺陷的发现、研究与修补上，而是出于某种目的设法入侵系统，窃取资料、盗用权限和实施破坏活动。

3. 黑客技术和网络安全不可分

可以说黑客技术的存在导致了网络安全行业的产生。一个典型的产品安全公告产生的过程是这样的（这里的例子讲述了微软公司的一个漏洞）：一个黑客在测试一个程序时，发现存在有不正常的现象，于是他开始对这个程序进行分析。经过应用程序分析、反编译和跟踪测试等多种技术手段，黑客发现该程序的确存在漏洞，于是针对该漏洞编写了一个能获取系统最高控制权的攻击程序，证实该漏洞的确存在。随后，这位黑客向微软公司写信通知其漏洞细节，并附上了攻击程序，要求微软公司修补该漏洞。微软公司开始对此不予答复。无奈，黑客在其网站上对世人公布了该漏洞，并提供攻击程序下载给访问者测试。顿时很多 Internet 上的网络安全论坛上都谈论此事。这时微软公司马上对该漏洞进行分析，随后在其安全版块上公布有关的安全公告，并提供解决方案和补丁程序下载。

对于这种情况，恶意黑客（Cracker）会利用微软公司的安全公告公布的漏洞去破坏系统，而网络安全专家会根据安全公告提醒用户修补系统。网络安全产品开发商则会根据该漏洞的情况开发相应的检测程序，而网络安全服务商则会为用户检测该漏洞并提供解决方案。

4. Internet 网络的脆弱性

Internet 的基础是 TCP/IP 协议、网络设备和具有联网能力的操作系统。TCP/IP 协议簇有一些先天的设计漏洞，很多即使到最新的版本仍然存在。有的漏洞是和 Internet 的开放特性有关的，可以说是无法修补的。最近发生的对各顶级网站的攻击方式就是利用 Internet 的开放特性和 TCP/IP 协议的漏洞。

网络设备（如路由器）担负着 Internet 上最复杂繁重的吞吐和路由工作，功能强大而且复杂，以目前的技术而论，没有可能完全避免漏洞。以占市场份额 70%以上的 Cisco 产品而论，其已知的漏洞有 30 多条。

各种操作系统也存在先天缺陷和由于不断增加新功能带来的漏洞。UNIX 操作系统就是一个很好的例子。UNIX 的历史可以追溯到 20 世纪 60 年代。大多数 UNIX 操作系统的源代码都是公开的，近 30 多年来，各种各样的人不断地为 UNIX 开发操作系统和应用程序，这种协作方式是松散的，早期这些程序多是以学生完成课题的方式或由研究室的软件开发者突击完成的，这种协作开发软件构成了 UNIX 的框架，这个框架当初没有经过严密的论证，直到今天，商业 UNIX 操作系统如 Solaris 和 SCOUNIX 都还是构建在这个基础之上的，除非重新改变设计思想，推翻 30 年来的 UNIX 系统基础，否则以后还必须遵循这个标准。这种情况导致了 UNIX 系统存在很多致命的漏洞。最新的版本虽然改进了以往发现的安全问题，但是随着新功能的增加，又给系统带来了新的漏洞，很多软件开发人员只为完成系统的功能而工作，用户日新月异的需求和硬件的飞速发展，使生产商不可能也没有时间对每一个新产品做全面的安全测试，虽然一些正式的软件工业标准有利于改善这种局面，但即使生产商按照这些工业标准开发测试，也难以保证十全十美，因为源代码公开的特性，使黑客有足够的条件来分

析软件中可能存在的漏洞。

5. 对黑客技术的研究严重不足

如果从整个社会的文明现状来看，黑客技术并非尖端科技，充其量只能说是 Internet 领域的基础课题。其实黑客技术并不神秘，但计算机产品供应商对其一直讳莫如深，黑客技术的发展从局部来说让产品供应商不安，这造成整个计算机行业对黑客技术的重视不够，从而导致当今黑客组织和黑客技术研究都呈无政府状态。从长远的角度看，黑客对产品的测试和修补建议将促进产品的安全性，对客户和供应商都是有利的。现在世界上也许还没有哪一个国家真正投入人力和物力研究黑客技术，所以造成目前的 Internet 基础仍然很薄弱，对于一个黑客来说，要制造一个令媒体关注的新闻是一件很容易的事情。这也是网络安全令世人担忧的原因之一。

6. 网络安全公司需要黑客

从事网络安全技术服务的公司，如果没有研究开发黑客技术的水平，或者没有发现客户系统潜在隐患的能力，其服务质量是没有办法保证的。目前国际上很多从事网络安全业务的公司纷纷雇请黑客从事网络安全检测与产品开发，甚至一些政府部门也不惜重金招纳黑客为其服务。因为网络安全的防范对象是恶意黑客，所以必须有了解攻击手段的黑客参与，才能更全面地防范黑客攻击。合格的网络安全专家必须具有黑客的能力，不了解黑客技术的网络安全专家是不可想象的。

7. 国家的黑客技术发展有利于国家安全

Internet 的开放互连的特征决定黑客技术可以跨国攻击，它既可以用于攻击，也可以用于防御。用兵之道，必须攻防兼备。所以未来信息战的胜负有赖于一个国家的整体黑客技术水平，这是不需要讳言的。

黑客技术的发现，对有关的软件开发商和信息产业是“短痛”，从长远的角度看却是有利的。而从信息国防安全的高度而言，黑客技术的发展更有利于国防建设的大局。它的客观存在性决定了如果我们不去了解和研究它，则会受制于它。在信息技术越来越发达的今天，我们需要开发自己的网络安全产品来为信息产业保驾护航，更需要本领高强的黑客参与网络安全产品的研究开发和测试，这样产品的质量才上得去。

8. 现代国家的重要部门的网络无法完全和 Internet 脱离

网络化的趋势不可避免，任何行业都需要网络通信。纵观处于应用阶段的网络技术和硬件，可以发现走在最前面的依然是 Internet。所以 TCP/IP 网络互连技术被广泛地用于各行各业。有关部门认识到 Internet 的安全脆弱性，采取了一定的措施，例如使重要部门的网络在物理上与 Internet 完全脱离。这是比较有效的。但网络安全是一个整体的概念，只要能接触重要部门网络的人没有完全与 Internet 脱离，就不能说该网络与 Internet 已经完全脱离。比如一个重要部门的系统管理员经常上网的个人计算机上就可能有他所在重要部门的机密资料，通过顺藤摸瓜的方法，黑客可以获取更多他们想要的信息。黑客还可能通过电话、无线电和卫星信号传输的方式对重要部门的网络进行渗透。

9. 未来信息战的可能性是存在的

当今社会的信息化程度越来越高，计算机和网络与人们的生活的关系越来越紧密。一个现代化国家的社会信息网络如果遭到毁灭性打击，足以使人们的生活倒退几十年。这种战争比较文明，不会造成人员伤亡，但破坏力绝不比一场常规战争小。相对于传统的战争和能造

成地球毁灭的核战争而言，信息战的可能性也许更大。在网络更加发达的未来社会，除了高能量电磁波的攻击外，信息对抗战的主力将是黑客。

诚然，网络的基础设施是计算机，而不是单片机，黑客的攻击是基于代码的数据流攻击而不是强大的电流攻击，美国政府能勉强应付棘手的 DoS（拒绝服务，具体内容参见第 8 章）攻击，而且就算网络在攻击下瘫痪，也能在数小时内恢复。可是，真正的黑客和网络安全专家应该能意识到，真正有组织的大规模的信息战还没有到来。

个人的力量是有限的，再高明的黑客也不足以对付一个国家和社会。真正的威胁来自于政府组织的全方位攻击，这种攻击不仅仅局限于代码和数据流攻击，还包括信息渗透、机密资料连环破解和人工的物理接触。从整体上来说，全世界的网络都存在着被人忽视的管理漏洞，机密的资料和控制指令总会有渠道泄露出去。

真正的信息战没有到来以前，谁也估计不到破坏会到什么程度。这取决于国家之间的攻守准备。要打赢这场战争，除了对网络安全技术要有足够准备外，其他方面的人力和物质准备可能不会比一场局部的常规战争少。

10. 国内网络安全的投入和培训不足

据估计，国内电子商务站点的网络管理人员至少有 90% 以上没有受过正规的网络安全培训。这几年中国的 Internet 处于发展建设阶段，大部分的 ISP（Internet 服务提供商）和其他从事信息产业的公司都没有精力在网络安全方面进行必要的人力和物力投入，很多重要站点的管理员都是 Internet 的新手。一些操作系统如 UNIX，它们在那些有经验的系统管理员的配置下尚且有缺陷，在这些新手手中更是漏洞百出。很多服务器有 3 种以上的漏洞可以使入侵者获取系统的最高控制权。

一些公司对网络安全问题非常轻视。他们认为服务器上没有重要数据，也没有资金往来，如果有人入侵他们的系统，最多是窜改一下首页而已，谈不上大的危害。但他们可能没有意识到，如果恶意黑客入侵他们的计算机后，利用这台服务器的身份对其他有重要资源的服务器作案，造成第三方的损失后，公司可能成为该案的“替罪羊”。

11. 发展有中国特色的网络安全/黑客技术是强网之路

不可否认，在计算机领域上我们的技术整体上比西方发达国家落后。Internet 基础协议是开放的，UNIX 系统的代码基本上是开放的，操作系统开放源代码是必然的趋势。硬件是别人的。但软件可以是自己的。在计算机领域，我国的软件技术明显优于硬件。黑客技术不是一个非常底层的领域，其开放性尤其明显。对系统极具破坏力的攻击程序代码和脚本在 Internet 上不难得到，相对于获得商业软件产品的源代码来说，黑客程序的源代码更容易设法获取。黑客技术是起源于开放的 UNIX 环境，在 Internet 上得到繁荣的发展。

很多国家都制定了未来信息战的方略，作为一个爱好和平的国家，我们的信息战方略应该是以防御为主的。但我们不可能不研究那些攻击性极强的高深黑客技术，正如虽然我们不想使用核武器，但不得不去研制它一样。去年，俄罗斯黑客成功地对美国五角大楼的计算机系统实行了渗透，并窃取了一些机密资料。有迹象显示，俄罗斯黑客还可能入侵了最高机密的计算机系统，据新闻周刊（NEWSWEEK）的报导，俄罗斯黑客使用的入侵手段是“不可能检测到的”。对于美国这种对计算机依赖程度很高的国家而言，俄罗斯黑客的这种手段是很具威慑力的。

12. 付出一定代价是必要的。早付出比晚付出好

对于计算机病毒，包括国人在内的计算机用户都为它付出了沉重的代价。无数重要的数据被病毒吞噬消失得无影无踪。但多年来经过与计算机病毒的斗争，我国对病毒的研究和反病毒技术已经走在了世界的前列。坏事来得早比来得晚好。在和平年代，我们有充足的时间应付不利的事件，经历的风浪越多，将更使我们有足够的经验应付恶劣环境下的突发事件。

如果平时我们没有对付高明的黑客攻击的经验，很难相信我们有能力去打一场未来可能发生的信息战争。

13. 对网络安全进行立法

立法应该着重于保护用户的利益，而不应该鼓励缺乏网络保安措施的系统运行于 Internet 上。过分严格的法律保障将使人们忽略自己保护系统的责任，用户应该对具有明显漏洞的系统负责，比如一个重要用户没有设置密码，那么管理员和用户对由此带来的安全威胁和经济损失应该承担主要的责任。法律打击的对象应该是那些利用黑客研究成果从事破坏活动的人（这些人往往是没有能力发现黑客技术的）。

Internet 对我们的工作和生活将会越来越重要，全世界对这个巨大的信息宝藏正进行不断的发掘和利用，人们在获得巨大利益的同时，也面临着各种各样的威胁，网络安全威胁带来的损害与人们对网络的依赖程度成正比。我国对黑客技术的认识和对网络安全的研究正处于起步阶段，在我们进行现代化建设的时代，网络安全越来越成为关系国计民生的大事，它需要全社会的重视，让我们用勇于探索，大胆创新的精神来精心研发网络安全产品和维护我们的网络安全，为中国信息产业保驾护航!

1.2 国内黑客网站与 2000 年黑客事件回顾

随着 Internet 网的发展，国内的黑客网站也有一些，下面列出的是一些比较有代表性的黑客网站及其主要内容。

（1）绿色兵团——提供网络安全信息及服务。

（2）中国黑客网页大联盟——中国黑客网站链接。

（3）仙剑黑客乐园——黑客入门、黑文精粹、工具下载。

（4）黑客圣殿——提供黑客攻防软件，提高网虫和一些系统管理员的安全意识。

（5）蓝客学堂——全面的安全工具，安全文献。

（6）黑客俱乐部——黑客新闻、信息、资料，还有黑客工具中心。

（7）Dark Sun——黑客组织，提供黑客软件、黑客教程、黑客新闻。

（8）安全地带——安全资料、安全软件、黑客相关、安全通道。

（9）飞弹基地黑客总站——经典黑客工具、软件下载。

（10）红色力量——一个非政府性网络安全组织，研究并讨论网络安全与反黑客技术。

（11）黑白网络——黑客工具下载、后门制作方法等。

进入 2000 年以来，风起云涌的全球网络在经历着前所未有的购并整合的同时，还要时刻面对病毒侵蚀、黑客狂攻的冲击，这使原本不够成熟的网络环境蒙上了一层束缚之雾，给前途无量却荆棘丛生的网络发展之路平添了不少障碍。下面的几个事件足以反映出黑客的破坏

力，也促使人们冷静地反思网络安全的重要性。

2 月初，YaHoo!、亚马逊网上书店、美国有线新闻网（CNN）、拍卖网站 eBay 及刚上市的超市网站 Buy.com 等美国 8 家大型网站遭到黑客不同程度的攻击。据悉，此次造成的经济损失可能在 12 亿美元以上，其中受害公司在 3 天内损失的市值高达 10 亿多美元，营销和广告收入损失达 1 亿美元以上。受影响的公司及其 Internet 合作伙伴为了更新安全设施，将要另外花费 1～2 亿美元。此外，这次袭击还将给受害公司的品牌、合作关系以及未来的客户造成损害。

2 月 8 日和 13 日这两天，新浪网的 E-mail 系统遭到黑客袭击，导致用户无法收发邮件的时间最长达 17 个小时。在黑客攻击之后，人们发现遗留下来的信件是平时的 10 倍之多。据估计，此次黑客发来的信至少是平时新浪网所收信件的 100 倍以上。

2 月 14 日，中国选择网在上海热线机房的主机服务器遭受黑客大约 8 次袭击，正在参加“夜话”聊天的网友受害不少。

3 月，被称为网上最大中文书店的当当网站声称：近来，黑客对当当网站进行了长达数周的恶意攻击，不仅删除该网站的一些图书信息，还使网站出现长达数小时无法运行的现象。

在 3 月某日的凌晨，美国历史最悠久和最权威的民意调查机构——盖洛普的网站遭黑客窜改，人们花了大约 6 个小时进行修复。据悉，美国总统选举工作人员和新闻工作者非常依赖盖洛普网站的调查结果，如果黑客窜改了数据，可能导致盖洛普发出令传媒误以为真的报告。

3 月某日晚，白宫网站主页上飘扬的美国国旗竟变成了骷髅头的海盗旗；在美国总统克林顿与副总统戈尔的合影中，戈尔成了独眼龙。

4 月 26 日，我国有不下 10 万台计算机与 CIH 病毒“同归于尽”。在北京，该日上午 9 点各公司正式上班之前，已有近千台计算机被 CIH 病毒破坏。

5 月 4 日，一种被称为“爱虫”的新型计算机病毒席卷了亚洲、欧洲和美洲等地区。全世界约有 100 多万台计算机遭到侵袭，因计算机系统瘫痪或关闭造成的经济损失达 100 亿美元。“爱虫”病毒的大规模袭击令各地政府与企业的计算机系统招架不及，陷于瘫痪。

6 月，一种名为“新欢”的病毒开始传入我国。它是一种存于电子邮件附件中的病毒，可导致网络瘫痪。据悉，天津一家外企的计算机曾被其袭击。国内其他一些大城市也出现了案例，多数袭击发生在与国外联系密切的外资企业。