Hackers Beware

黑客
——攻击透析与防范

[美] Eric Cole 著
苏雷 等译

New Riders
電子工業出版社
Publishing House of Electronics Industry
www.phei.com.cn

黑　客

——攻击透析与防范

Hackers Beware

[美] Eric Cole　著

苏　雷　等译

電子工業出版社
Publishing House of Electronics Industry
北京 · Beijing

内 容 简 介

本书全面、系统地介绍了关于网络安全技术的知识和相关问题。书中主要介绍了能够成功保护网络系统免受攻击的方法，并且对各种攻击的机理进行了全面的论述。本书的突出特点：全面跟踪了当前黑客攻击的关键技术和方法，针对不同对象和情况，提出了不同的防范策略，具有很强的实用性和时效性。本书结构合理、内容翔实，有助于训练安全方面的专门人才，使他们能够更好地对各种威胁做出正确的反应，使防范工作做在攻击者的前面。本书还可以为网络管理员、系统管理员在预防黑客方面提供有效的安全防范与管理策略。

图书在版编目（CIP）数据

黑客——攻击透析与防范/（美）科尔（Cole, E.）著；苏雷等译. -北京：电子工业出版社，2002.1
书名原文：Hackers Beware
ISBN 7-5053-7435-4

I. 黑... II. ①科... ②苏... 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097835号

书　　名：黑客——攻击透析与防范
原 书 名：Hackers Beware
著　　者：[美] Eric Cole
译　　者：苏　雷　等
责任编辑：谭海平　杜　萌
排版制作：今日电子公司制作部
印 刷 者：北京天竺颖华印刷厂
出版发行：电子工业出版社　www.phei.com.cn
　　北京市海淀区万寿路173信箱　邮编：100036
经　　销：各地新华书店
开　　本：787 × 1092　1/16　　印张：37　字数：923千字
版　　次：2002年1月第1版　　2002年1月第1次印刷
书　　号：ISBN 7-5053-7435-4
　　TP·4287
定　　价：59.00元
著作权合同登记号　图字：01-2001-1463

前　言

网络安全是一个流行的话题，有关这方面的书籍几乎不用介绍。大约十年以前，大多数人并不知道什么是Internet或电子邮件，再早一些时候，大多数家庭和办公室也没有计算机，一些人甚至在怀疑计算机与网络的用处。但是世界变化得太快了，当在写这篇简介的时候，感觉到网络世界的繁荣景象，就像是在迪斯尼世界中一样。十年前我们认为是科幻小说里才会有的东西现在不仅已变成了现实，而且已深入到了我们的生活之中。现在真正是计算机网络的时代了！

从功能的角度来讲，孤立的计算机是非常安全的。如果在家中放一台没有接入网络的计算机，那就不需要什么安全措施。可是现实中人们通过Internet把他们的计算机连接了起来，我们在互相信任的基础上建立了这个网。这里仅存在一个问题：人们之间并非完全互相信任。然而，在很多情况下，我们给所有用户完全的信息存取权。基于这一点，我们来追溯一下事情的起因。这其实是由于过去人们只关注于技术与功能，而并不担心安全问题，但事实上当前的安全问题已非常严重。

我还记得十年前在安全部门工作时的情景：人们都不愿搭理我，到处都给我白眼看。为什么会这样？因为人们还没有认识到安全工作的重要性，而是认为安全工作纯粹是在为根本不存在的威胁而浪费金钱。在那时，其他的技术和安全技术比起来，可以很容易地比较它们的效益。比如，扩展网络或安装新服务器可以加快访问速度、增加计算效率、提供更大的存储空间等。而安全技术却没有这些直接效益，它有的只是间接效益：数据和信息得到安全保障。一般情况下，在没有受到损失之前，人们是不会真正认识到安全的重要性的。只有当攻击者侵入了系统并盗走一千万美元的时候，人们才开始重视安全问题。想想看，如果他们一开始就在安全上投入的话，能省多少钱呢！

在越来越多的单位遭受损失的情况下，越来越多的单位认识到提前对安全投资的重要性。汽车保险就是这样，人们在买车的同时也买下了保险，只是为了防备万一车祸发生所带来的损失。我认识一些三十多年都没有发生过车祸的人，但是他们仍然购买保险。这是因为购买汽车保险可以降低出车祸时的损失，这已在人们心中形成了一种共识。同样的道理也适用于网络安全。不管您的公司是从事什么行当的，规模有多大，投资网络安全都是明智之举。

没有系统是安全的。任何接入Internet的系统都受到探测并有可能遭到侵入。我们可以做一些简单的实验来验证一下。可以用家中的直接接入或拨号接入Internet的计算机来做这个实验。购买或者从网上下载防火墙，这类软件工具有好几种，但Zone Alarm是一个免费版本，它可以从www.zonelabs.com下载。将这个防火墙安装在计算机系统上，接入Internet，48小时后会有吃惊的发现。通常在不到两天的时间内，系统会被探测到数次并可能被侵入。举个例子，当从Internet服务提供商（ISP）那里索要到一个IP后，接入网络，在不到30分钟的时间里就受到了5次探测。如果是家用计算机，没有域名，不受到太多关注，但还是被探测并受到攻击。对于公司而言，一定会受到更多攻击的。如果没有良好的防范措施，就会被非法攻入并遭受损失。

有一些公司曾对我说过，他们的系统从来都没有受到过攻击。这些话肯定是不对的。事实上，应该是他们从来都没有检测到攻击。眼不见心不烦并不能解决问题，清楚并能针对自己系

统进行恰当的防范措施是非常关键的。本书就是要介绍黑客们在干什么以及他们所用的工具和技术。通过本书，可以从准确的角度对系统做出更好的防范。

应该明确，成功的防范必须建立在对攻击充分了解的基础之上，这正是本书的目的：介绍黑客攻击与破坏的技术、方法以及工具，让人们利用这些知识建立更安全的网络。安全防范不是一句空话，必须了解威胁是什么。在这个领域只有知识是最有力量的。

本书就是介绍黑客攻击的内幕以及如何防范黑客的关键。保护网络安全是一次没有终点的旅行，但就我的经验来看，它也是一次非常令人愉快而且回报相当大的旅行。快让我们开始在网络安全世界中的美妙旅途吧！

第1章 简 介

无论现在工作在何种领域，都不可能没有注意到Internet对当今社会造成的巨大冲击。它为人们展现了一个原来只在梦境中出现的机遇和市场。

对于Interent而言，就像任何一种其他的新技术一样，它都是有利弊两个方面。积极的方面是它提供了巨大的机遇，消极的一面是它给许多公司造成了安全上的隐患。然而真正意识到这种潜在危险的公司却很少。这就像坐进一辆以每小时80公里速度行驶的崭新的车里，却发现工程师并没有为它安装上刹车装置。如果这种情况真的发生了，而且有很多人买了这种车的话，那么由于车辆内部没有安装刹车装置而给交通运输带来的危险是难以想像的。同样的事情也会发生在Internet上。虽然现在很多公司已经在网络设备上进行了数百万的投资，同时也已经意识到安全问题很重要，但是他们的网络公司还是非常脆弱和易受攻击的。

本书的重点就是强调没有任何方法可以完全地维护公司的网络安全，除非对所面对的危险有非常清醒的认识。只有深入了解了攻击是怎么回事，黑客是怎么样攻击一台机器的，一个公司才能给自己正确定位从而使公司得到更好保护。如果为了防范某种攻击而保护一个站点，而你对这种危险毫无所知或者并不知道它是如何工作的，显然，你就不能防范这种攻击。了解黑客能够对用户系统做些什么和这种攻击在网络上的表现形式，就有能力去构建一个安全的系统。

虽然这本书讨论了如何攻击他人系统的技巧和一些常见工具的使用，但是这并不意味着它是一本教你如何进行攻击的手册。它只是用来帮助公司关闭易于遭受攻击的薄弱之处和保护计算机免受攻击。我只是想提醒大家注意到那些可供使用的工具以及应用它们是如何的简单。而且我想向大家展示一个公司要构建一个安全的系统应该做些什么。

1.1 进行攻击的黄金时期

无论从哪个方面来看，这都是一个进行攻击的黄金时期。总的来说，这是一个成为黑客的大好时代。因为很多的系统都很容易受到攻击，它们中的大多数的安全性都很差，攻击者可以轻易选择进行攻击的机器。更令人担心的是，大多数公司都没有足够的信息和资源去跟踪那些攻击者，所以即使那些攻击者被检测到，抓到他们的机会也是微乎其微的。没有人会监管Internet，受知识和经验所限，黑客往往占有优势。现在不仅是一个成为黑客的好时机，而且也是一个成为计算机安全专家的好时机。在这个领域有许多工作和挑战等待着我们。

最近一个广为人知的遭受攻击的例子发生在2000年2月。几个大的网站在很短的时间内遭受了攻击。攻击的类型是分布式拒绝服务攻击，它使得合法的用户无法到达公司站点。我们将在第6章详细讨论这种攻击的细节问题。从商业角度来看，它对遭受攻击的公司造成了巨大的损失。对于一个网上书店来说，这种攻击将会导致大量收入的流失，公司不仅失去了生意，而且失去了众多的顾客。

让我们先看个例子。如果一位意图通过在线购物的顾客在上午10点登录一个公司站点，浏

览器显示“Web Site Unavailable”（站点不可到达）的信息，他可能会在10:45再次重新试着登录，当他在11点又一次登录还是得到“Web Site Unavailable”的信息时，显然，他将会到另外一个竞争对手那里购买这种商品。在网络上有很多的竞争者，如果顾客在短时间不能登录一个站点的话，他很快就会放弃转而去找另外一个站点。

具有讽刺意味的是，很多公司是如此的害怕“2000年问题”而为此投入了巨资。从某些方面来看，它更像是一种浪费，因为这个问题被过高地估计，并且媒体也过分地渲染了它的危险性。更加严重的是，这些公司仍然没有考虑到安全问题。到目前为止，他们还不想进行这个方面的投资。

公司站点非常容易受到攻击，是由各种各样的原因所造成的，首当其冲的是缺乏安全意识。大多数公司到目前为止还没有意识到它们所面临的危险。本书的目的之一就是提醒大家意识到这个问题，并且能够使用一些已有的工具对自己的站点进行保护。无知是致命的，知识就是力量。如果一名持枪歹徒闯入你家，而你没有任何武器，你就不能保护好自己。换而言之，如果你自己拥有武器并且了解入侵者使用的武器的缺点，你就会占据上风。这就是本书的目的所在，教给IT人员一些攻击者经常使用的工具和技巧，使他们能够更好地武装自己。

1.2 问题的严重程度

要将所有被攻击过的站点名罗列出来，即使用不了整本书，也可能会需要好几页的篇幅。本节将会给出一些曾经遭受过攻击的站点的例子来表明我们现在面临的问题是多么的严重。

下面的例子，直接来自于Internet。它们涵盖了商业网站、政府网站、国内的网站、国际网站、娱乐性网站和公益性网站。它们之中没有一个是安全的，没有一个逃脱了被攻击的命运。任何公司都有可能遭受到攻击，只要接入了Internet，不管它在哪里，它是干什么的。下面是一些曾经遭受到攻击的站点的列表：

- U.S. Department of Commerce（美国贸易部）
- Church of Christ（基督教会）
- Unicef（联合国儿童基金会）
- Valujet
- NASA（美国国家航空及太空总署）
- United States Air Force（美国国家空军）
- CIA（美国中央情报局）
- Malaysian Government（马来西亚政府）
- Greenpeace（国际绿色和平组织）
- Tucows
- Philippine IRS（菲律宾国税局）
- Star Wars
- Six Flags
- Cartoon Network（卡通网）
- University of Texas（得克萨斯大学）

- NY Times（纽约时报）
- Dominos
- Comdex
- Motorola（摩托罗拉）
- FOX（福克斯公司）

这些站点中的大多数都被黑客进入并且内容也被更改。这种攻击方式同时也被称之为网页涂改攻击（web graffiti attacks）。显然，遭受到这种攻击的网站的性能会受到很大影响。这种攻击会以一种隐性的方式获取系统的信息，所以受攻击者很难发现。如果在Internet上搜索有关于黑客的站点或者相似的站点时，可以看到很多与涂改攻击有关的内容。值得注意的是，其中的一些内容对于任何人来说都是具有攻击性的。

下面是一个主要的搜索引擎所搜索到的黑客网站。当用户试图连接到此URL时，将会得到如下的信息，而不是一个正常的站点页面。

```
P4NTZ/H4GiS -WORLD DOM1N4T1ON '97

FOR the cast month ,anyone who has viewed this page & used their search
engine,
now has logic bomb/worm implanted deep within their computer.

The worm part of this 'virus,'(in layman's terms)spreads itself across
internal networks that the infected machine is on.

Binary programs are also infected.

On Christens Day,1997,the logic bomb part of this 'virus,' will become
active,
Wreaking havoc upon the entire planet's networks.

The virus can be stopped.

But not by mortals.
```

大多数人只会把它当作是一个玩笑，但是它仍然会造成某些人的恐惧和迷惑。这种攻击的类型提出了一个令人感兴趣的话题："如果……会怎么样？"如果一个著名的网站感染上了这种病毒的话会怎么样呢？大家可以设想一下它的后果。

1.2.1 总的趋势

因为本书的目的是告诉大家如何防范黑客和攻击者，所以先了解一下有关Internet网络安全方面的现状是非常重要的。根据经验，Internet是攻击者们的天堂。首先，攻击者可以轻易地进入任何想要进入的系统，并且他们因此而被抓住的可能性很小。更令人担心的是，越来越多复杂的攻击方法被完善地组织在一起，使得即使是普通人都可以在任何时间运行这些工具对系统进行攻击。如今，即使是很幼稚的攻击者都可以如同资深的黑客一样轻松地进入到一些站点。

Internet发展的速度是如此之快，以至于对于网络安全的问题始终没有得到应有的重视。但是很普遍的是，我们大部分人还对此熟视无睹，事情只会变得越来越糟糕。网络攻击者始终占有优势，并且这种优势还会持续一段时间直到那些公司开始加强自己的系统。目前对于这些系统存在隐患的公司来说，最好的办法就是切断同Internet的联系直到他们的系统变得安全起来。但是显然没有人会这样做。

另一件使得安全问题变得更加严峻的是公司是如何构建他们的网络的。在过去，每个公司的网络和系统都是不同的。在20世纪80年代后期，公司雇佣程序员来定制他们的应用程序和系统，所以如果攻击者想要进入网络的话，必须对用户的网络环境有相当深入的了解。他从一个公司所获取的信息对于他试图攻击另外一个公司网络系统来说，是毫无用处的，因为此时的系统是各不相同的。而现在，几乎每个公司都使用相同的设备和软件。如果一个攻击者对Cisco、Microsoft和UNIX有很深的了解，他就能够进入到Internet上的任何一个系统。因为这个网络是如此的相似，软件和硬件都已经被标准化，攻击者的工作量已经减轻了很多。

有人会认为这也使得维护系统安全的工作变得更加容易，因为当我们学会了如何去维护一个系统安全以后，我们便可以轻易地与其他人共同分享这些知识。这个问题可以从两个方面说起。首先，由于某些原因，网络上的一些不规范者希望能够共享这些经验，而一些遵守规范的人却不愿意共享。其次，即使是操作系统和应用程序是相同的，它们在配置上也是完全不同的。从攻击者的观点来看，这些不同之处在安全保护方面是至关重要的。这是因为即使服务器A上运行的是Windows NT系统，并且运行良好，但这并不意味着能够克隆服务器A上的配置到服务器B上，因为它们的配置在很大程度上是大相径庭的。

为了更好地理解这个问题，我们来关注一下安全缺口这个问题。大约在一年以前，一个黑客小组对多个银行系统进行了“测试”，他们发现其中一个系统极其容易受到攻击。于是，在数个小时之内，他们从这家银行提取了1000万美元存入到了一个私人的户头上。由于这家银行的安全性是如此之差，这些攻击者能够抹去他们所留下的蛛丝马迹，使得安全专家很难发现他们的线索。他们仅仅留下是谁负责了这次行动的信息。这些黑客并没有直接通过自己的计算机进行攻击，而是绕过其他的几个站点进行了攻击。这使得想抓住他们变得更加困难。

既然攻击者知道逃脱的机会非常大，他们就变得更加自信而且越来越想证明自己不会被抓住或者被起诉。为了减少被关注的程度，攻击者常常会在进行攻击不久以后，打电话给该银行的总裁为自己的行为进行辩解，他们从容地走进银行家的办公室解释他们是谁，他们已经干了些什么。这些攻击者为总裁提供了两种解决问题的方案。一是银行可以因此而起诉他们，但是他们会否认所做的和所说的一切，包括他们之间的这次谈话。这些黑客声称他们干得非常干净利索，没有留下任何的痕迹可以证明他们曾经进行过攻击，因此银行方面也无法把他们绳之以法。而且，他们将会通知所有的电台、电视台、新闻报纸，这家银行曾经被攻击过，以及从这家银行偷取金钱是如何容易。那么银行将会因名誉受损而损失更多的存款和顾客。这些攻击者所提供给银行的另一种选择是，银行以维护安全的名义付给他们500万美元，而他们会将其余的500万美元归还给银行。

试着猜想一下银行总裁将会做出什么样的选择呢？在几分钟之内，他签署了一份文件，然后得到了剩余的500万美元。

可能会觉得这很难以理解，但是事实上这是真的。攻击者经常占据了上风，而被攻击者总

是处于他们的控制之下。在这个例子中，总裁作出了一个明智的决定，使得银行的损失减少到了最低程度。如果银行坚持要起诉的话，它不但不会得到那1000万美元，还会因为在公众当中的声誉受损而受到更大的损失。每个公司都应该意识到，除非他们实施了非常安全的措施，否则的话，攻击者能够轻易地攻击他们的网络系统从而更进一步控制整个公司。

1. 系统非常容易被入侵

目前那些进行攻击的人们都具有很广的知识面和技巧经验。一个极端是那些没有什么经验但是有很多空余时间的初学者，另一个极端是那些拥有一定经验的比较熟练的黑客。非常不幸的是，许多公司网络的安全性能非常差，以至于进入它们的系统并不需要高深的知识。他们下载一些可执行文件或者是一些脚本，运行它们就会得到一些提示或者是系统管理员才拥有的账号。普通用户只要了解了操作系统的基本特性，如登录，就能使用鼠标和键盘对系统进行攻击。

很多家庭为了防范小偷而采取了基本的保护措施，而不是因为他们具有很高的安全意识。老练的攻击者能够进入任何房间。但是由于这样的人相对来说比较少，所以能够提供防范低级别的功能就会为系统安全带来很大的好处。这就是为什么很多人为他们的门窗加上了锁，并且有的还安装上了报警系统。在Internet上，那些初级的攻击者的水平只到达了如果他们知道哪个地方没有装上锁的话他们就可以进入的程度。但是很多公司还处于一百年以前的原始状态：所有的门都没有上锁，甚至是很多入口连一扇门都没有。这个问题现在非常严重。甚至在每个公司都认识到网络上大部分都是这种低级别的攻击者，并且会因此而采取措施防范这些攻击时，这个问题仍然存在。只要这些站点还是和Internet互联的话，他们就不会有百分之百的安全感，但是希望通过本书将这个程度提高到百分之九十。当今，只有不到百分之五十的公司对自己的安全性能是放心的。为了确保企业的安全，必须改变以前对Internet的一些不正确的想法。

2. 攻击工具容易获得，也容易使用

不仅仅是系统容易受到攻击，而且那些能够自动进行攻击的工具也非常容易从网上获得。即使是一个非常不成熟的攻击者，都可以从网上下载一些工具进行非常专业的攻击。这种获取工具的便利性可以将任何一个能够接触Internet的用户转变成一个可能进行攻击的黑客。如果用户能够操作一台计算机，就可以在自己还不知觉的情况下，使用一些非常复杂的工具对系统造成破坏。

（1）Internet混乱无序的本性

另外一个问题是任何接入到Internet的用户都可以毫不费力地在当地、国家内部和国际的任何一个区域浏览，一不小心在IP地址中误输入了一个数字就会连接到一个可能是远在天边的计算机。

当连接上非本国的计算机的时候，要跟踪这种连接就必须得到国际间的互相合作。由于这种连接到世界各地的计算机网络是非常容易操作的，攻击者们就可以在对目标进行攻击之前，通过在几个不同国家的计算机之间的绕行来隐藏他们的线索。通常情况下，通过选择那些还没有发生联系的国家进行攻击可以减少自己被成功追踪的可能性。

举个例子，如果一名攻击者想连接一台位于加利福尼亚的计算机，他可以直接和它相连接，这只需要几秒钟的时间，但这使得别人能够很容易追踪到他的踪迹。或者用另外一种方法，他可以首先花费几分钟连上一台位于英国的计算机，然后再连入一台位于俄罗斯的机器，再到法

国，接着到中东、以色列、远东，最后到达加利福尼亚。在这种情况下，想要沿原路返回追踪到攻击者踪迹的机会是渺茫的。首先，这会花费很多的时间，其次，这需要各个方面的通力合作，而这往往是难以做到的。

（2）大量的资源

Internet不仅使得攻击者能够更加容易攻击系统或者进行犯罪活动，它也能够教会人们怎么去做这些事情。攻击者不仅可以访问那些被攻击过的系统，而且可以很容易地从网上得到那些教导他们如何进入系统的资料和技巧。如果攻击者想攻击一个自己并不熟悉的特殊的操作系统，可以花几个月的时间对它进行研究或者在几分钟之内从网上得到所需要的东西。由于在网上已经有了许多前人做过的工作和留下的资源，这使得攻击者所要做的工作变得更加轻松。

（3）没有人会监管网络

目前，由于没有人对网络进行监管，当问题出现时就没有清楚的界线去界定哪些人负责调查，发生了哪些犯罪行为。大多数国家正在试图建立一个常规的法律并把它应用于Internet上。在某些情况下可以适用，但有些情况又不太适用。即使网络中存在监视网络的实体，这也非常困难，因为那些犯罪活动是在网络的虚拟世界里发生的。在现实生活中，如果超速的话是很容易被发现的。而在Internet上，由于是在虚拟的空间里犯罪，这很难被追查或者被起诉。

3. 公司不会做出报道

另外一个主要的焦点问题是关于攻击的报道很少，我们将这个现象称之为“冰山效应”。因为当从表面上看这个问题时，会觉得整个Internet还处于上升时期，问题不是很大，但是如果从深层次去看这个问题时，就会发现有个大问题。那些攻击行为没有得到报道的主要原因有两个：无知和不良的社会影响。

（1）无知

首先，公司没有意识到他们遭受了攻击。这是主要的因素，这会对公司造成更大的损失。即使公司不能预防攻击，如果它能够定时地进行监测，也能够尽量减少自己的损失。不能够进行监测，不仅仅会对本公司造成很大的问题，而且会对其他的公司站点带来很大的危害，因为在Internet上一个站点可以作为对另一个站点进行攻击的平台或者是跳板。

这是在保护自己的站点免受拒绝服务攻击时所必须考虑的一个重要问题。当公司站点已经安装了防止拒绝服务攻击软件，并不能表明这个站点已经是万事无忧了。想要自己的站点免受攻击的话，还必须考虑要确保Internet上其他的站点不能被用来作为攻击的跳板或者平台。至关重要的是：要保证自己的站点不受攻击必须确保Internet上的每一个站点都做了恰当的工作。

（2）不良的社会影响

第二个原因是担心会造成不好的社会影响。大多数情况下，当公司报道一个安全漏洞时，就立刻会成为社会的热点。试着想像一下如果《华盛顿邮报》的头版头条是：某家银行被黑损失2000万美元。我们会立刻把在这家银行的存款取出而转移到另外一家银行。大部分银行都很清楚如果他们向外界透露遭受到攻击的话，他们就会损失更多的资金。所以与其这样，还不如不向外界公开，而用日常的工作经费来弥补这部分损失。并且，大多数的安全问题还没有得到解决，所以为什么要告诉外界呢？遭受更多的批评也不能挽回损失。这就是问题的关键所在，

他们不但会损失惨重，而且在社会上的名声也会受影响。基于这些原因，大多数公司都不愿意向外界透露他们的安全漏洞。

1.2.2 为什么问题变得如此严重

当Internet日益在商业上应用越来越广泛时，每个公司都在寻求从中获取利益。决策者也在紧紧地抓住这个可以使他们受益的机会。每个人都只看到了它的正面，几乎没有人看到它消极的一面。很少有人会回头考虑如此迅速地转入Internet带给他们自己和顾客的巨大风险。对于任何一个问题，忽略它的时间越长，遭受损失的可能性就越大。现在这个问题还会变得越来越糟，公司除非修复这个问题，或者从这场竞争中退出，否则别无选择。接下来让我们看看这个问题是怎样逐步发展得越来越严重的。

1. 2000年问题

世界上几乎没有哪一个公司会对2000年问题无动于衷的。由于媒体不遗余力地对2000年问题大力宣传，许多公司将全部精力和资源都投入到了2000年问题的解决当中，而忽略了其他的问题。某些公司将2000年问题视为公司生死存亡的惟一问题加以考虑。这些公司都没有意识到在解决2000年问题的过程中，他们都忽略甚至还增加了在其他方面的安全隐患问题。

不幸的是，在接下来的一年里，一些公司才注意到由于急于解决2000年问题而造成的其他一些副作用。他们在解决2000年问题过程中所采用的一些方法与一些众所周知的保证安全性的方法有所抵触。

首先，大多数公司聘请了外部的顾问人员来修复2000年问题。因为所有的公司都急于解决2000年问题，他们很少对那些顾问公司进行背景检查，以至于由谁对他们的系统进行操作都毫不知情。更为糟糕的是，许多公司让解决这一问题的人们以系统管理员的身份完全访问所有的系统。与此同时，由于他们自身也非常繁忙，所以不能对这些顾问公司的操作人员进行有效的监督。在通常的情况下，公司都不会这样做的，但是在2000年问题的名义下，这样做就显得很正常了。如果他们在公司系统留下了一个后门的话，他们就可以从系统中得到所需要的任何东西，而公司对此是毫无办法。

第二，由于时间关系，大部分为系统提供的补丁和更新文件没有得到很好的测试和确认，这就意味着有某些非法的程序或者是病毒会隐藏在这些文件当中，从而进入到机器内部。现在，2000年问题已经时过境迁了，大多数公司都相信自己的系统已经不会再受到2000年问题的干扰，然而几乎没有人了解在他们系统内部运行的到底是什么东西。

正如前面所述，当系统中有一个后门供以后的攻击者使用的话，就没有一个很好的方法去保护自己的系统。如果一名攻击者留下了一个后门，他或许并不会立即使用它，而有可能是在一年以后再来利用。即使公司检测到了攻击，它也不可能追寻到一年以前就已经留下的后门。看看现在的公司对安全问题的处理方法和忽视的程度，我们就可以想像在未来的几个月或几年内将会有相当多的问题有待解决。在忽略了一件事太长的时间以后，当重新想处理它，就会发现事情变得越来越糟。

由于以下的这些原因，公司对于安全问题很难理解：

- 安全问题每时每刻都在发生。

- 它还会继续发生。
- 当公司意识到安全问题时，可能已经太迟了。

公司比较喜欢解决2000年问题是因为它有一个时间界限，因为它有补救的方法，过了千禧年之夜以后，这种威胁就会解除。而如今我们现在所面临的安全问题与我们以前所遇见的所有问题都不一样，很少有人能够真正了解它。它就在我们谈论它的同时发生，没有时间期限，也没有解决这个问题的简单、直接的方法。再过20年，当前企业的现状会发生很大的改变。那些现在对安全问题提前预防的公司就会走在前头，而不重视安全问题的公司则不可避免地落在了后面。不幸的是，坏事总会来临的。

2. 对现有系统修复的花费很高并且效率不高

好消息是有越来越多的公司开始意识到安全问题，并且严肃认真地考虑它。坏消息是现在为时已经有一些晚了，安全问题正变得越来越严重。这其中有几个原因，但是最大的原因是我们忽视这个问题太久了，要修复这个问题还需要花费很大的功夫。

大多数人都将安全问题认为是后面要做的事。他们首先构造网络，然后安装上防火墙或者是其他安全措施。越来越多的攻击事件证明这种安全模型已经越来越落伍了。

如果在建筑行业中应用这种模型的话，将会发生下面的情形。总工程师将会仔细研究房屋的结构，设计好建造房屋的计划。他先建造屋顶、边墙、清水墙，然后粉刷和铺地板。接着电工会敲开侧墙将电线布好，再重新砌上清水墙、重新粉刷，然后水管工人将会把所有的水管道铺好。可以看出来，建造房屋是不会按照这种方法的。因为它极其没有效率，过于浪费，而且最终产品质量也不过关。然而，由于某些原因，人们仍然会按照这种方法来构建自己的网络系统。安全问题不能在事后考虑，我们必须在设计网络结构的开始就周全考虑安全性问题。

3. 安全会带来的无限好处

另一个关于安全性的问题是，当一个公司决定对安全性问题进行投资，那么它将会从中得到无穷无尽的好处。如果对一个新的主干网进行投资，就会发现网络的速度有了很大提高。如果投资新服务器，就会发现它的性能有了更大的提高。如果对安全性能进行投资，就会大大减少侵入站点的可能性，只是管理层不能从中得到直接的、可以估算的利益。

这种想法当然是很自然的，因为大多数公司从来就没有想到他们的系统是不安全的，他们对为什么要花费额外的资金对安全功能进行投资而感到迷惑不解。他们的理由是在过去的一年里他们的系统从来没有出现过问题，为什么要对一个以前从来没有考虑的问题（并且也没有发生过任何问题）进行投资来减少风险呢？

正如大家所知，这是一个安全意识的问题。所有的公司都应该意识到现在没有检测到任何安全漏洞并不表明自己的系统就一点问题都没有。除非所有的公司都开始对安全问题进行研究，并且对安全问题与网络进行综合考虑，否则发生在2000年2月的分布式拒绝服务攻击就会经常发生。以前，我曾经有机会为一个大型电信公司的内部安全问题做一些工作。开始的时候，那个公司已经意识到一些安全性问题有待解决，但是他们并不想为此花费很多的钱。经过长时间的讨论后，这家公司才决定从预算中拨出一定的经费以建立安全机制。经过几年的运行后，没有发现任何安全问题，于是公司就决定将安全机制的这部分预算削减。他们声称，既然没有任何安全漏洞的话，就完全没有必要在安全性问题上花费更多的钱了。

这种逻辑经常出现，但是在很多方面这都是错误的。就如同说：已经住了十年的屋子一直没有破漏，为什么现在需要为屋顶进行另外的投资呢？在这个例子中，很显然由于屋顶的存在所以房子内部没有被淋，因此对屋顶的投资是必要的。

看起来似乎如此简单，但一谈到安全问题，大多公司都不会遵照这种逻辑。而对安全进行投资的真正原因是：如果公司的安全问题并不是很普遍，所做的安全投资才起了作用。而且，由于现在的网络安全环境变得越来越恶化，还必须为此耗费更多的资源。最重要的是，由于许多公司对安全性问题已经忽视了很久，远远落后于要求，所以他们就需要投入更多的资源来追赶，甚至是超越这段距离。只有当公司意识到安全问题是他们不得不付出努力解决的问题时，这种发生危险的可能性才能减小。

1.3 公司正在做什么

几乎在阅读每一份国际性的新闻报纸的时候都会看到有关于安全问题的消息。值得指出的是，即使所有的人都在谈论安全问题和对安全问题缺乏认识，大多数的公司还是不愿意把自己的安全漏洞问题报道出来。这有两个原因：首先，公司不愿意因为报道自己的安全问题而造成负面的社会影响；其次，实际上大多数公司并不知道漏洞是何时产生的。如果入侵者获得了进入系统的权限，破坏了一些敏感的信息，但是并没有造成服务的中断的话，公司检测到入侵的可能性将会很小。许多公司只在服务发生了中断时，才检测到遭受了攻击。

这种情况是经常发生的，比如说：公司A作为某个市场的最初进入者获取了大量的利润。通过网络漏洞，它的竞争者得到了这个信息，并且出售同样的商品，那么原来公司A准备获得4000万美元的利润就会因此降低到3000万美元。在这个例子中，除非公司A拥有安全的网络系统，否则它怎么能将所有这些损失完全归过于一个小的网络安全故障上面呢？最终，这个损失将会推到别的因素上面，而不是真正的原因。

当看到这本书上的例子的时候，读者当中的某些人可能会觉得这些事情离我们太遥远而显得荒谬可笑。但是这些例子却真实地反映了目前大多数公司安全问题的现状，这种事情发生得太多了。公司对于它们所遭受的攻击毫无准备，只有在事情发生以后才采取办法解决。在目前发生的大多数安全性问题中没有准备是一个很大的因素。

1.3.1 零忍耐

一些人认为除非公司对黑客们采取强硬的手段和惩罚，否则的话公司将永远处于被攻击的位置。这听起来有一些道理，但是问题是大多数公司总裁都将主要的精力放在了发展公司业务和获取更多的利润上面。因此，对黑客采取强硬的手段并不是永远都适用的。如果公司已经做好了应付当前威胁的准备和有了一定的自我保障能力的话，它们就可以还击。但是，现在的公司一谈到安全方面的问题时，它们就束手无策，除了投降就是退出这个领域。下面就是一个公司无法总是采用强硬的手段来对付黑客的例子。

鲍勃，高级网络管理员，在一家迅速发展的公司即将得到提升的机会。但是经过公司决策层的激烈讨论后，鲍勃不但没有得到这个晋升的机会，还要无偿地干别的工作，并且没有一个

工作头衔。出于难以理解和愤怒，鲍勃在某一周末来到了工作室，将所有的共享文件和最后三周的备份文件都设了密码，并且设定只有他本人才有阅读公司这些数据的惟一权限。这就意味着没有鲍勃的密码，任何人都无法阅读这些数据。那些可以用的文件都是一个月以前的，这意味着这些资料的用处很小。鲍勃走进主控信息中心说除非给他提升的机会和一些补偿，否则的话，所有的数据都不能恢复。

这家公司对这种行为采取了严厉的措施，他们不仅仅拒绝了鲍勃的要求，而且启动了正常的司法程序来起诉鲍勃。最终得到的好消息是经过了漫长的法庭调查和高昂的费用，他们成功起诉了鲍勃，坏消息是由于公司丢失了所有资料，他们的很多项目只能重新进行，这不可避免失去了一部分顾客。这家公司由于这个事情耽误了整整8个月的时间。在某些情况下，采取强硬的手段是能够凑效的，但是由于这种手段潜在的危害，做出这种决定对于公司来说是不明智的。从大的方面来看，它常常关系到公司是不是还准备在商业领域呆下去的问题。

正如你所看到的，当公司的系统安全性能很差时，没有任何磋商的办法。不解决它，只会使事情变得越来越糟。

1.3.2 侥幸的安全意识

很多公司存有一种侥幸的安全观点：因为没有人知道我们的网络，并且，也没有人真正打我们公司的主意，所以为什么需要这种安全投资呢？没人会想进入我的系统。随着站点越来越容易被入侵，这种观点也越来越靠不住。不同领域不同形式的公司都曾经被入侵过。很多公司已经认识到对于安全问题来说，无知是致命的。

如果确信你的公司是如此的不引人注目，那些攻击者因此而不会攻击你的站点的话，那这是自欺欺人。我曾经通过获取一些IP地址注册过一些小的测试性的站点，并且为它们申请了一个主域名。在建立这个站点不到两天的时间里，我就被扫描了几十次，并且还有一部分人试着入侵我的系统。

这显示了Internet上两个重要的事实：第一，对于一个攻击者来说，没有小站点的概念，所有的站点对于他们来说都是一样的；第二，攻击者在扫描整个网络，当有新的机器连入到Internet上时，他们就会追踪这台机器，并且猜想这个新加入的站点是不是没有很完善的安全措施——毕竟，这才是那些人们最关注的事情。换句话说，如果正在建立一个新的站点，在没有配置好所有的安全机制之前请不要将它连入到Internet，否则将会受到莫名其妙的攻击。

1.3.3 试着修复已经建立起来的系统

很多人认为安全是后面才要考虑的问题。他们首先建立起一个网络，然后建立一个防火墙或者是做一些安全措施。随着攻击变得越来越普遍，这种模型也变得不再有效。

如果一个站点已经在网上存在了一段时期而没有正确的安全设置，那么这家公司就更应该感到担心。因为当想测试一个站点是不是安全的时候，我们必须假定它是不安全的。在大多数情况下，它使得我们必须花费更多的金钱和时间去保存数据和重新建立系统，而不是简简单单地为这个系统打上补丁。

1.3.4 过于重视或者极不重视

一个主要的错误是：人们对于安全问题要么漠不关心，要么太过于重视。如果一个公司觉得自己不能达到最高级别的安全性能时，就完全放弃而毫不设置安全措施。每个公司都必须认识到有一些安全措施总比没有强。只要他们开始考虑这个问题，他们最终总会使得自己的站点变得非常安全。并且在很多情况下，只要付出很少的努力就可以解决很多的安全漏洞问题。所以，只要提供了一定安全级别的保护，就能大大提高系统免受攻击的可能性。

1.4 公司现在应该做些什么

各种各样的公司为了它们的生意而去迎接Internet，但是它们只是仅仅从纯功能的角度来看待它。这些使用了 Internet 某些功能的应用是不是真的像我们预期的那样给我们的工作带来好处呢？提出这个问题是解决问题的很好的开始，但是公司的决策者们必须逐步改变他们的想法，同时应该将安全因素考虑进去。安全就是这样一种事物，如果到需要它的时候再去考虑的话，可能已经为时太晚了。就等同于没有电话，但在需要它的时候才想要一部电话一样。如果等到出现紧急情况需要叫一辆救护车时，再去想办法弄到一部电话已经太晚了。我们需要准备一部电话来以防不时之需。那个时候就可以简单地通过电话叫一辆救护车而不用做其他额外的工作了。配置安全机制是至关重要的，这样即使出现漏洞，也可以采取相应的行动，使得破坏的影响减到最小。

为了理解应该设置什么样的机制，我们首先来看看有关于安全性的几个原则和它们是如何处理目前的问题的。

1.4.1 预防和检测投资

为了使得站点变得安全，人们必须对这个问题有两点认识：预防和监测。很多公司将焦点集中到预防上而忽视了监测这个问题。比如说，大约有百分之九十的公司已经安装了防火墙，它是用来解决预防问题的。然而，这个问题是有两重性的：第一，公司不能预防所有的信息，所以一些可能是攻击性的程序会随之进入到系统；第二，公司所设置的大多数预防机制既没有被设计好也没有被配置好，这意味着它只能提供很少的预防功能。

贯穿于本书的一个主题是预防是可选的，而监测则是必需的。一个公司如果想建立一个不受外界攻击的站点，显然这是不切实际的，不可能建立起一个能够防范所有攻击的站点。在那些攻击行为不可能被防范的时候，公司需要建立起一个能够在攻击者还没有来得及对网络进行破坏之前就能够监测到这种行为的防范措施。

我就遇到过很多那些安装了一排又一排防火墙但是可以被绕过的站点。当问他们何以如此时，他们说由于很多人经常抱怨防火墙堵塞了信息的流通，所以决定给他们一个单独的通道。如果这不是自相矛盾的话，我实在是想不出来怎么说好。公司建立防火墙是为了阻止未经授权的信息的流入，但是当雇员们抱怨防火墙所做的工作时，就给他们一个另外的通道，这就为攻击者提供了一个缺乏抵抗力的通道。如果入侵者有两条路径进入一个站点，一条是通过防火墙，另外一条是绕过防火墙，他会选择哪一条呢？

即使是公司拥有很好的预防机制，当然大多数公司都做不到这一点，能够实时监测到攻击才是关键。

1. 首先关闭最大的漏洞

当攻击者准备攻击一个站点时，他常常会选择一条没有阻力的道路。因此，公司详细了解它所有的弱点并且不把全部精力投入到某一个区域是非常重要的。我看过很多公司将自己的全部精力投入到如何去配置一个防火墙来保护自己的网络，这种情况是非常普遍的。这些公司忘记了它们的拨号系统是没有经过授权的绕过了防火墙。黑客当然不会花费大量的力气去攻破防火墙，而放弃能够绕过防火墙的由拨号系统进入的方法。

公司通常必须了解自己的薄弱环节，并修复它。一旦修复了最薄弱的环节，次薄弱的环节将会变成最薄弱的环节，再接着修复它。对于系统的安全而言，总是有需要修复的地方。只有当公司了解了自己网络系统的安全状况和有一个减小系统风险的计划，它才能解决这些问题。

系统安全专家的最终目标是找出系统最薄弱的环节，并且在还没有遭到攻击之前修复好它。最终结果是修复好了大部分的薄弱之处以至想要攻击系统的人无从下手为止。请注意，除了极少数情况，不可能修复好每一个安全漏洞。举个例子，与Internet连接就是一个易受攻击之处，当然每个公司都知道这样做的好处大于坏处。安全措施的最大目标就是减少和减轻系统遭受攻击的风险，并且使得攻击者不容易轻易地进入，或者能够在他成功地进入系统之前监测到他的行动。

2. 提高安全级别来防止业余和偶然的攻击者

大多数人认为那些攻击者只使用最复杂、最先进和最好的工具进行攻击。因此，如果能够防范这种类型的攻击的话，就已经到了一个很高的水平。然而，如果一个黑客能够在10分钟之内学会使用一种简单的工具就可以攻击你的系统，你认为他会再去花费10天的时间来学习一种很复杂的工具来破坏你的系统吗？

我经常为一些公司是否应该在安全问题上投入大量的资金进行一些评估工作，但是我常常发现他们忽视了一些小节问题。在一次评估中，一个公司几乎打上了所有的最先进的补丁，安装了好几重防火墙和入侵监测系统，并且对所有的账号进行了权限的设置。通过查号台，我知道了公司的拨号号码，但是无法猜出任何人的密码。最后，我试着使用guest这个账号并且没有密码，居然我进入了系统。一个拥有如此完善安全系统的公司怎么会存在这样明显的一个漏洞呢？不幸的是，这种情况会经常发生，因为这些公司对安全问题是如此紧张，以至于他们遗忘了那些只需要几秒钟就可以修复的错误。

1.4.2 给予监测技术更多的关注

公司不能够坐以待毙。问题发现得越早，就越能够减少公司所遭受的损失。如果能够及时监测到攻击行为，也许只需花两个小时就能解决问题而不必使系统关闭。如果监测一个攻击行为用了两个星期的话，就可能需要好几天的工作并且系统还要被关闭一段时间。问题只会随着时间增长而增多。

当连入了Internet之后，无论安全系统是多么的完善，总会有攻击者能够侵入系统。解决问题的策略就是尽可能地预防攻击和监测别人正在对你的系统干些什么。很多安全专家都说惟