- 从扫描到嗅探，从渗透到注入，全面揭开黑客攻防谜底
- 既包括个人用户防范知识，也有针对Web、局域网和无线网安全问题的解决方案，读者随查随用
- 资深计算机安全专家汇聚多年经验精心编著

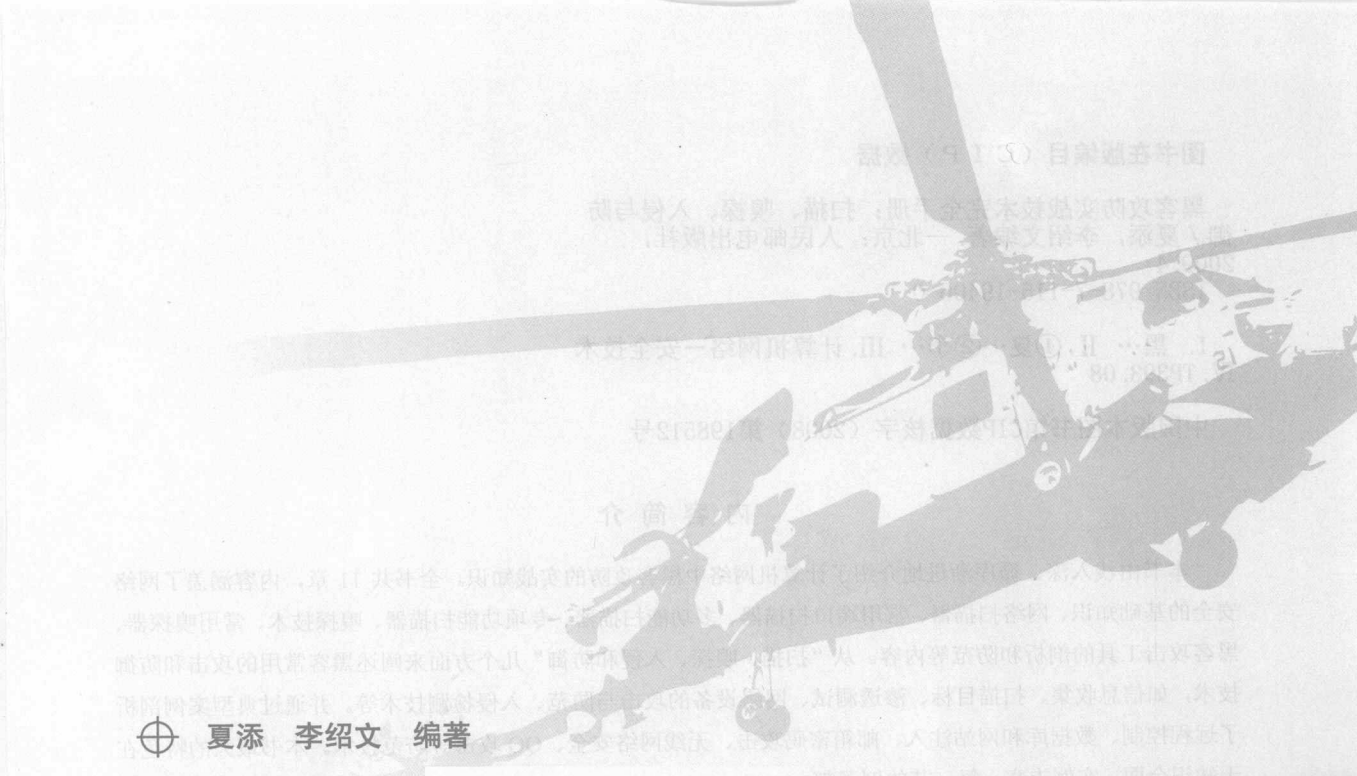
黑客攻防

实战技术完全手册

扫描、嗅探、入侵与防御

夏添　李绍文　编著

人民邮电出版社
POSTS & TELECOM PRESS



夏添　李绍文　编著

黑客攻防

扫描、嗅探、入侵与防御

人民邮电出版社
北京

图书在版编目（CIP）数据

黑客攻防实战技术完全手册：扫描、嗅探、入侵与防御／夏添，李绍文编著. —北京：人民邮电出版社，2009.4
ISBN 978-7-115-19406-0

Ⅰ. 黑… Ⅱ. ①夏…②李… 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（2008）第198512号

内 容 简 介

本书由浅入深、循序渐进地介绍了计算机网络中黑客攻防的实战知识。全书共 11 章，内容涵盖了网络安全的基础知识、网络扫描器、常用端口扫描器、多功能扫描器、专项功能扫描器、嗅探技术、常用嗅探器、黑客攻击工具的剖析和防范等内容。从“扫描、嗅探、入侵和防御”几个方面来阐述黑客常用的攻击和防御技术，如信息收集、扫描目标、渗透测试、网络设备的攻击与防范、入侵检测技术等。并通过典型案例剖析了远程控制、数据库和网站注入、邮箱密码攻击、无线网络安全、QQ 攻击等防范技术。本书最大的特色在于知识全面、实例丰富，每一节的例子都是经过精挑细选，具有很强的针对性，读者可以通过亲手实践来掌握防范黑客的基本要领和技巧。

本书适合于初、中级用户学习网络安全知识时阅读，同时也可作为高级安全工程师的参考资料。

黑客攻防实战技术完全手册：扫描、嗅探、入侵与防御

◆ 编　　著　夏　添　李绍文
责任编辑　张　涛

◆ 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
北京鸿佳印刷厂印刷

◆ 开本：787×1092　1/16
印张：21.75
字数：520 千字　　2009 年 4 月第 1 版
印数：1–4 000 册　　2009 年 4 月北京第 1 次印刷

ISBN 978-7-115-19406-0/TP

定价：39.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前言

如果有一天，一个未曾谋面的陌生人在 QQ 或 MSN 上告诉您说：“您的计算机的密码是×××，您的 QQ 和邮箱密码是×××，您的×××文件……”您一定会在气愤的同时感到非常惊讶，并且非常佩服对方非同寻常的能力。可是您的密码未曾告诉过任何人，也没有把文件给任何人看过，为什么对方就可以掌握自己存储在计算机中的隐私资料呢？其实这就是黑客攻击。类似的网络攻击或入侵方面的例子很多，这已成为了每一位网民的必修课，为了揭开这些谜底，帮助读者保护自己计算机信息的安全，我们特意撰写了本书。

本书特色

- 内容丰富，实例经典

本书追求理论与实践的结合，用浅显的语言讲述精心设计的经典实例，将黑客攻防的基本理论和实战技巧融入到范例当中，全面覆盖黑客攻防的各个角落。

- 实例众多，讲解通俗

为了贴近实战，作者都结合更多的案例讲解每一个知识点，这些实例都是真实案例的提炼和总结。并且攻防的每一步都通过图解形式给出，通俗易懂、详略得当。

- 知识面宽，重点突出

本书涉及的内容众多，有基本的黑客攻防实战技巧，也有深入的黑客攻防技术；既有个人用户的防范知识，也有针对 Internet、局域网、无线网的攻防知识，是真正成为防范高手的晋级知识。每章讲解都遵循“学习目标→攻防原理剖析→实战防范技术与技巧→案例总结”这种读者易于学习和实践的方式进行，达到了既授之以鱼，又授之以渔的目的。

本书内容

我们计算机上一般都装有杀毒和防火墙等安全软件，看似已经打造得铜墙铁壁了，但为什么突然我们的数据或密码就被改变了呢？陌生人是如何知道自己的计算机的 IP 地址的呢？又是如何知道自己的计算机存在漏洞呢？网络服务器怎么被入侵的呢？所有这些疑问都将通过本书得到详细的答案。

本书主要内容是从“扫描、嗅探、入侵和防御”几个方面来阐述黑客常用的攻击和防御技术，这几种技术都是目前在黑客的攻防中使用率最高的。第 1 章～第 2 章介绍网络安全的基础知识以及扫描器分类及原理；第 3 章～第 5 章介绍黑客收集信息的方式以及大型扫描器的使用方法；从第 6 章开始逐步过渡到嗅探攻击技术，其中第 6 章～第 7 章介绍基于嗅探的被动攻击方式以及攻击工具的原理；第 8 章～第 11 章为读者介绍目前主流的木马以及攻击工

具的原理及防范，读者在阅读和学习本书介绍的技术和实战案例时，按照章节顺序阅读就可以达到防范黑客攻击的最佳效果。

读者对象

本书以清晰明朗的写作思路，图文并茂的讲解形式，由浅入深地引导读者学习黑客常用的攻击和防御方法。本书适合于初、中级用户学习网络安全知识时阅读，同时也可作为高级安全工程师的参考资料。

本书由夏添、李绍文编著，在编写过程中，张博、王洪、叶凤云、教青、陈芳、管西京、柯华坤、王大平、林丁报、张英男、张鹏、温才燚、刘冉、李新峰、李连闯、范洪彬、裴要强等提供了很大帮助，在此，对他们表示衷心的感谢。由于时间仓促，加上编者水平有限，书中难免存在一些不足和错误之处，恳请广大读者批评指正，联系邮箱为：zhangtao@ptpress.com.cn。

需要声明的是，本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任，本书的目的在于普及网络安全知识，增强人们防范病毒及木马攻击的能力，提高防范技术水平。

编者

目录

第1章 网络安全概述

随着网络的不断发展，全球信息化已成为人类发展的必然趋势。但由于计算机网络具有开放性、互连性等特征，致使 Internet 用户易受到黑客（hacker）等不法人员的攻击，使得网上信息的安全性和保密性已成为一个至关重要的问题。

随着人们越来越依赖于计算机进行工作，网络安全也越来越受到人们的关注，在世界各个国家的网络不断受到黑客攻击的同时，信息安全技术也得到了突飞猛进的发展。面对信息安全的严峻形势，在网络安全成为普遍问题的情况下，如何保护自己的主机免受黑客的侵犯，已成为每一位网络用户的首要任务。因此，对网络安全有一个较全面的了解显得尤为重要。

1.1 网络安全的定义与所受威胁

1.1.1 网络安全定义

一般来说，网络安全是指保护网络系统中的软件、硬件及信息资源，使之免受偶然或恶意的破坏、篡改和泄露，确保网络系统的正常运行、网络服务不中断。

对用户而言，网络安全的总体目标是确保系统的可持续运行和数据的安全性。

而从广义来讲，网络安全包括硬件资源和信息资源的安全性。

网络安全需要保护的 5 个方面为。

- **可用性**。可用性是指得到授权的实体在需要时可以得到所需要的网络资源和服务。
- **机密性**。机密性是指网络中的信息不被非授权实体（包括用户和进程等）获取与使用。
- **完整性**。完整性是指网络信息的真实可信性，即网络中的信息不会被偶然或者蓄意地进行删除、修改、伪造、插入等破坏，确保已授权用户得到的信息是真实的。
- **可靠性**。可靠性是指系统在规定的条件下和规定的时间内，完成规定功能的概率。
- **不可抵赖性**。不可抵赖性也称为不可否认性。是指通信的双方在通信过程中，对于自己所发送或接收的消息不可抵赖。

1.1.2 网络安全威胁

目前对网络安全威胁分类主要有 3 种方式：一种是对安全威胁的实施者即攻击者进行分类，一种是根据网络安全威胁的行为方式进行分类，另一种是根据安全威胁的技术类型不同进行分类。

1．根据网络攻击者进行分类

著名的网络安全研究学者 John D. Howard 博士认为，网络系统的攻击者有黑客、间谍、恐怖主义者、公司职员、职业犯罪者、破坏者共 6 类，不同类型的攻击者其攻击目的不同。

对于黑客最流行的说法是黑客源于网络共享精神，在几十年前美国国防部刚刚开始 ARPANET 实验的时候，由一些程序设计专家和网络名人组成了具有共享性质的文化群体，这些成员为自己创造了“hacker”这个名词。

黑客专注于发明新技术，而与黑客相对应的骇客（cracker）的定义是指那些专注于搞破坏活动的无聊分子。他们利用网络中现有的技术和软件，乐于表现自己的能力、喜欢看到被破坏者无可奈何的苦笑。黑客们对骇客不屑一顾，他们认为这些人懒惰、不负责任，并且不够光明正大。懒惰表现为只知道将别人的数据、成果据为己有，而不做丝毫贡献；不负责任是指对网络的恶意攻击。人们普遍认为黑客和骇客的区别是，他们是否对新技术的发展有贡献、是否对他人进行恶意的攻击。

本书所说的黑客是指所有对网络节点实施攻击的个人，包括 John D.Howard 博士所说的网络系统的攻击者中的黑客、公司职员、职业犯罪者、破坏者。

我国对网络安全威胁根据攻击者进行分类的另一种方式是，根据攻击来源分为外部攻击、内部攻击和行为滥用攻击。攻击者来自该计算机系统的外部时称作外部攻击；当攻击者就是那些有权使用计算机，但无权访问某些特定的数据、程序或资源的人企图越权使用系统资源时则视为内部攻击，包括假冒者（即那些使用其他合法用户的身份和口令的人）、秘密使用者；特权滥用者也是计算机系统资源的合法用户，表现为有意或无意地滥用他们的特权。

2．根据网络攻击行为方式进行分类

我国最常见的一种攻击类型分类方式为主动攻击和被动攻击两种。

被动方式是指，利用 Internet 可交互的特点，在网络上发布或向用户推出一些含有恶意代码的网页、软件、电子邮件；当用户浏览网页、运行软件、打开电子邮件时，恶意代码在用户计算机中将发挥作用，破坏系统或者安装后门，使用户对计算机失去控制，或者利用被攻击计算机显示出来的信息对其进行全面的分析，从而获得足够的信息。被动攻击方式主要有：搭线窃听，无线截获，用程序和病毒截获信息，流量分析，通信模式、数据模式和数据分析。被动攻击成功与否主要取决于攻击目标的安全意识，如果攻击目标对外来信息特别注意，被动攻击很难取得成功。

主动方式是指，通过网络主动发送违规请求，令目标系统失去响应或者获得目标系统的控制权限，从而达到进一步破坏的目的。因为被动攻击成功的可能性比较小，黑客的攻击大多数都采用主动攻击方式。随着用户安全意识的不断提高，主动攻击成功的可能性也在不断减少，所以被动攻击中通过电子邮件进行攻击的方式得到了更多的应用，这一攻击方式黑客将其称为“社工”。

3．根据网络攻击技术进行分类

美国的 CERT（Computer Emergency Response Team）组织号称是计算机应急分队，是由美国联邦政府资助的专门研究计算机及网络安全的组织，能随时提供最新发现的计算机及网络安全问题，并提供一些解决方法。该组织将攻击分成以下几种类型：

缓冲区溢出、文件非安全处理、参数检查不完全、非安全程序特征、特洛伊木马、弱认

证或加密、配置错误、程序实现错误。

可以看出，该分类方式的优点是能够容易地识别攻击方法的技术特征，缺点是很多攻击方法不能包含在其中。

4．微软公司对安全威胁来源的分类

微软公司对恶意软件的传播方式进行了分析，将安全威胁的来源分为了如下 12 种。

- **电子邮件**。许多恶意软件攻击都选择电子邮件作为传输机制。
- **网页仿冒**。网页仿冒攻击会尝试诱使他人泄露其个人详细信息，如信用卡号或其他财务或个人信息。虽然这些攻击很少用于传播恶意软件，但可能会造成信息泄露，因此它们仍属主要的安全问题。
- **可移动媒体**。此类威胁包括软盘、CD-ROM 或 DVD-ROM 光盘、Zip 驱动器、USB 驱动器和内存卡（媒体），如数码照相机和移动设备中使用的内存卡。
- **Internet 下载**。恶意软件可能会从 Internet 网站（如社交网站）直接被下载。
- **即时消息**。多数即时消息程序允许用户与其联系人列表中的成员共享文件，这就为恶意软件提供了一条传播途径。此外，这些程序也是许多恶意软件攻击的直接目标。
- **对等（P2P）网络**。要启用文件共享，用户首先要安装 P2P 程序的客户端组件并使用已批准的网络端口（如端口 80）。在 Internet 上很容易下载众多的 P2P 程序。
- **文件共享**。在将计算机配置为允许通过网络共享文件时，也为恶意代码的传播提供了另一种传输机制。
- **恶意网站**。恶意网站开发人员可利用网站的功能尝试散布恶意软件或不良材料。
- **远程攻击**。恶意软件可能会试图利用服务或应用程序中特定的弱点进行自我复制。Internet 蠕虫病毒经常使用这种伎俩。
- **网络扫描**。恶意软件编写者利用这一机制来扫描网络，寻找有开放端口的易受攻击的计算机或随机选择 IP 地址进行攻击。
- **词典式攻击**。恶意软件编写者逐个尝试词典中的每个词来猜测用户密码，直到成功为止。

1.2 网络安全漏洞

无论是何种类型的网络威胁，都或多或少与网络安全漏洞有关。通俗来讲，漏洞是指受限制的计算机、组件、应用程序或其他联机资源无意中留下的不受保护的入口点。有人曾对漏洞给出了一个更为通俗的定义：能够被利用来干“原本以为”不能干的事，并且是和安全相关的缺陷。

漏洞的一般定义为：在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

从漏洞的定义可以看出，漏洞既有软件上的漏洞，也有硬件上的漏洞。由于黑客很难利用硬件漏洞，只有最顶尖级的少数黑客才有能力较好地利用硬件漏洞，因此，常说的漏洞一般均指软件漏洞。因人为原因，漏洞在程序编写过程中几乎是不可避免的，据对几百万行 C

语言编写的软件源代码进行统计，每 1 000 行代码中将存在 5～10 个漏洞可以被利用。

漏洞的利用与时间、运行环境和用户存在不可分割的联系，因此，网络安全漏洞也有多种分类方式。

1.2.1 根据漏洞发现时间分类

根据漏洞的发现时间可以将漏洞分为已公布漏洞和 0day。

已公布漏洞指厂商已经发布补丁或临时修补方法的漏洞。如果网络管理员足够尽职尽责，经常关注漏洞及补丁的发布情况，并针对自己维护的网络进行防护，使得已公布漏洞较难发挥其作用。但对于多数网络，管理员没有足够精力或者没有意识到进行补丁的安装，这就为黑客提供了可乘之机。

0day 指未公开和虽已公开但厂商还未来得及发布修补方法的漏洞。这种漏洞一般在私下交易，虽然流传不广，但应用具有更强的针对性，危害更大。

1.2.2 根据漏洞成因分类

虽然根据漏洞的成因分类存在不够完善的地方，如研究的角度不同，同一漏洞可能存在不同的成因，但这一分类方式得到了多数网络安全人员的认可，大致可以分为以下 10 种类型。

字符输入检查、边界条件检查、特殊环境和条件检查、设计方案漏洞、大量打开端口、软件运行权限设置不当、配置错误、竞争条件错误、软件的默认安装、远程管理软件权限限制不够。

1.2.3 根据漏洞严重程度分类

微软公司将漏洞按严重程度粗略的定义为 3 种，分别为：严重等级、中等等级和低等级，如下表所示。

微软对漏洞的分类表

计算机类型	严 重 等 级	中 等 等 级	低 等 级
Internet 服务器	网站毁坏、拒绝服务（DoS）或完全控制	很难利用、异常配置或暂时性影响	有限的影响，例如脚本泄漏
内部服务器	特权提升、数据泄漏或修改。很难审核	可审查的数据泄漏、修改或 DoS	无目标的或碎片数据盗取或修改、有限的 DoS
客户端系统	不经用户许可运行随意代码；远程特权提升	本地特权提升、无目标的数据泄漏或 DoS、使用操作利用	有限的或碎片数据偷窃或修改、恶意网站攻击

1.2.4 按漏洞造成的威胁分类

国内著名的安全公司绿盟科技公司对漏洞分为如下 6 种类型：

远程进入系统、本地越权访问、拒绝服务攻击、嵌入恶意代码、Web 数据接口、其他

类型。

1.3 安全漏洞的检测和修补

有人针对当前信息安全可能出现的问题给出了一个信息安全公式：信息安全 = 先进技术+防患意识+完美流程 + 严格的制度 + 优秀的执行团队 + 法律保障。由此可见，技术在信息安全中只占其中一部分，更多的问题来源于人的因素，防患意识是其中的重要环节，而防患意识落实到现实中就是进行漏洞的检测和修补。

1.3.1 安全漏洞的检测

对于一个结构复杂的网络来说，进行维护和检测是一件相当烦琐的事情，对于位于 Internet 中的计算机，多数被攻击的背后凶手是掌握在黑客手中的已公布或未公布的漏洞。漏洞的成因既有设置上的漏洞，也有用户使用中的缺陷，手动进行检测几乎是不可能完成的工作，多数借助于漏洞检测工具。

一般来说，漏洞检测是模拟黑客的行为，对系统设置进行攻击测试，以帮助管理人员在黑客攻击系统之前，找出网络中存在的漏洞。这样的工具可以远程评估网络的安全级别，并生成评估报告，提供相应的整改措施。

目前，市场中漏洞检测根据不同的技术、不同的监听模式、不同的特征、不同的报告方法，可以分为多种类型，但总的来说，漏洞检测扫描器多数采用基于特征的匹配技术，与基于误用检测技术的入侵检测系统相类似。扫描器首先通过请求/应答，或通过执行攻击脚本，来搜集目标主机上的信息，然后在获取的信息中寻找漏洞特征库定义的安全漏洞，如果有，则认为安全漏洞存在。可以看到，能否发现安全漏洞很大程度上取决于漏洞特征的定义。

每个系统都有漏洞，攻击者掌握的漏洞远比防护人员知道得多，多数情况下，发现一个未知漏洞，远比利用一个未知漏洞要难得多。因此，漏洞扫描器所搜集的漏洞中绝大多数为已经公布的漏洞，只有很少部分为漏洞扫描器公司所发现的漏洞。

每台漏洞扫描器所搜集的漏洞数量多少不一，漏洞库的数量决定了扫描器的检测范围，因此衡量漏洞扫描器的重要标准是能否最大限度地包含所有相关漏洞。黑客与网络管理人员的较量在很大程度上是在比较谁的漏洞扫描器包含的内容更多。

对于商业化的漏洞扫描工具，一般价格较为昂贵，并且这样的扫描工具并不是对所有的 IP 地址都可以扫描。商业化的扫描工具授权有以下几种方式。

- 按 IP 地址授权。扫描工具价格取决于要扫描的 IP 地址数量。
- 按服务器授权。按服务器/工作站的数量计算扫描器的价格。
- 按管理员授权。这种授权方式较为简单，受到用户的广泛欢迎。

对于黑客来说，通常使用的是一种网络中免费或破解的漏洞扫描器。虽然这样的扫描器更新不太及时，但黑客手中常常掌握私下流传的各种 0day 漏洞，正是这些 0day 的广泛流传，使得黑客获取了可持续攻击的动力。

1.3.2 安全漏洞的修补

对于一个互联网中的节点，无论采取何种安全措施，第一步都应该是修补漏洞，如果不能及时修补漏洞，毫无疑问，您将受到黑客的入侵。对用户来说，要修补所有漏洞却是非常烦琐的事情，但也并非是不可能完成的事情，这就需要有章可循。

通常漏洞修补的第一步是进行漏洞扫描，对于 Windows 操作系统用户而言，可以用微软公司提供的 MBSA 或另一款免费软件安全卫士 360 来完成。MBSA 是 Microsoft Baseline Security Analyzer(Microsoft 准安全分析器)的缩写，可以在 http://www.microsoft.com/technet/security/tools/mbsahome.mspx 下载，目前最新版本是 2.1beta 版。安全卫士 360 的本机漏洞扫描功能将在第 5 章进行介绍。另外还有一款非常著名的漏洞扫描工具 HfNetChk。

HfNetChk 的工作过程是：首先检查补丁对应的注册表键值在计算机中是否存在；如果存在，HfNetChk 进一步检查该补丁的相关文件是否存在；如果存在，HfNetChk 开始对比每个文件的版本号和校验和数值是否与 XML 数据库中的对应内容相一致；如果又相同，那么就认为该补丁已经正确安装。否则，如果上述任何一次检查出现失败，就认为该补丁没有安装。

HfNetChk 工作时需要一个 XML 数据库文件，这个文件中包含了不同产品对应的 hotfixes 信息，它们是 Security bulletin 的名字、标题以及有关产品安全 hotfixes 的详细资料。这些详细资料包括如下内容：每个 hotfix 程序包中的文件名及其版本号和文件的校验和数值（checksums）、hotfix 程序包安装时创建的注册表项目、补丁程序间的接替信息、Microsoft 知识库（Microsoft Knowledge Base）中相关文章的序号等。

依据 XML 数据库文件的内容，就规定了 HfNetChk 判断一个补丁是否已经安装到计算机的标准，它们是：补丁安装后所建立的注册表键值、安装的补丁文件版本号和每个文件的校验和数值。

默认配置下，HfNetChk 将 XML 数据库中的文件资料和注册表键值与检测计算机中的文件和注册表键值进行对比，如果其中之一发生了不匹配现象，就会认为相应的补丁程序没有被安装，“Patch NOT Found”以及 Microsoft 知识库中相关文章的序号等信息将向用户显示。

对于微软公司的产品来说，多数已经提供了自动更新功能，这是安全防护中的一大进步。对于多数非微软公司的软件产品，则没有如此人性化。如果没有提供自动更新功能，在安装之后要安装所有补丁是非常麻烦的，甚至，有的漏洞并不一定存在相应的补丁，如 UNIX 操作系统，会在 BugTraq 邮件列表上（参见 http://www.securityfocus.com）发布安全补丁的通知信息。用户需要将补丁集自己整理，如何合理利用网络中的漏洞和补丁资源是网管员们需要深入考虑的问题。

1.4 网络监听

无论网络攻击者还是安全防护人员，网络监听都是一种经常采用的技术手段。网络管理人员通过网络监听可以获得进出网络的每一个数据包，既包括网络中用户正常使用的数据，也包括黑客软件所产生的数据，因此网络管理人员通过网络监听可以分析不法行为，而黑客

通过网络监听则可以获得想要的数据，如用户登录的密码等信息。通过网络监听进行攻击是黑客攻击过程中非常有效的方法之一。

要理解黑客如何进行网络监听，首先需要明白网络监听的原理。

1.4.1 网络监听的原理

在继续进行讲解之前需要先理解以下几个概念。

1．混杂模式

一台计算机要进行网络数据传输，必须安装网卡和网卡驱动程序，为便于区别，每块网卡都有一个在世界上独一无二的48位地址，称为MAC地址，除此外，要进行数据传输，还需要绑定一个32位的IP地址。网卡一般有几种工作模式，如unicast（单播）、broadcast（广播）、multicast（组播）和promiscuous（混杂模式）。unicast是指网卡在工作时接收目的地址是本机硬件地址的数据帧。broadcast是指接收所有类型为广播报文的数据帧。multicast是指接收特定的组播报文。promiscuous则是通常说的混杂模式，是指对报文中的目的硬件地址不加任何检查，全部接收的工作模式。

一般情况下，操作系统会把网卡设为广播模式，在广播模式下，网卡可以接收所有类型为广播报文的数据帧——例如ARP寻址。此外，它会忽略目标地址并非自己MAC地址的报文，即只接收发往自身的数据报文、广播和组播报文，这才是网卡的正常工作模式。而混杂模式是网络监听的根源，混杂模式下网卡对报文中的目标MAC地址不加任何检查而全部接收，这样就造成了无论什么数据，只要是路过的都会被网卡接收的局面。由网卡各种工作状态的定义可以看出，如果网络监听的目的不仅仅是本机数据，则混杂模式是进行网络监听的一个必要条件。

2．嗅探器（Sniffer）

一般情况下，网卡的工作模式由操作系统设置，并没有公开地让用户进行设置的界面。而嗅探器的出现打破了这一僵局，使用户拥有了设置网卡工作模式的权力。

ISS为嗅探器进行定义是：Sniffer是利用计算机的接口截获目的地为其他计算机发送的数据报文的一种工具。Sniffer的正当用途是网络管理员通过在网关进行嗅探，从而进行网络流量分析和数据分析，以便精确地判断网络中每台计算机可能存在的传输问题。

不同的嗅探器工作原理基本相同，但工作能力差别较大，有的嗅探器只能分析少数几种协议，有的却能分析几百种之多，比较著名的嗅探器有IRIS、Ethereal等，其中Ethereal为开源产品。

3．共享式网络

共享式网络的特征是通过网络的每一个数据包都被发送至每一台主机，最常见的共享式网络为使用Hub（集线器）构成的网络。

一般将使用交换机组成的网络称为交换式网络，交换式网络通过交换机构造“MAC-端口”映射表，数据包传送时，只会被送往特定的端口上，通过映射表，也只发送到特定的MAC地址。

据统计数据显示，采用全双工模式的交换式以太网最大传输速度约可以达到共享式以太网的4倍。

在一个网络中，网络监听效果最好的位置是网关、路由器、防火墙等设备，对于黑客来

说，由于网关等设备较难突破，网络监听一般在网络中的某台主机上进行。而对于网络管理人员一般在网关上进行网络监听。

如果一个网络是共享式网络，且将主机的网卡工作模式设置为混杂模式，则可以利用嗅探器在这台主机上监听到网络中传输的每一个数据包。因为网络中数据流量通常较大，黑客关心的是数据中包含的用户名和口令，黑客所用的嗅探器一般具有从数据中将口令筛选出来的功能。

在 UNIX 操作系统下，要将网卡设为混杂模式，需要向网络接口（Interface）发送 I/O 控制命令，而这些 I/O 控制命令，需要超级用户权限。在 Windows 系列操作系统下，这种限制较小，只要能够运行监听软件，就可以将网卡设置为混杂模式。

在交换式网络下进行嗅探，由于网卡只能接收特定端口的数据，需要采用其他技术将正常发往被监听计算机的数据“转移”到本机上来，目前较为成熟的技术为 ARP 欺骗和 DNS 欺骗等。

网络监听只能获得同一个局域网的数据，而不能监听到本网络之外的信息。

历史上最著名的嗅探事件发生在 1994 年，当时，黑客通过在骨干设备上安装网络监听软件，嗅探到 10 万个美军的有效用户名和口令，这在 Internet 中引起轰动。

1.4.2 网络监听的检测和预防

攻与防共存，当网络监听有了成熟技术的同时，对网络监听的检测技术也在不断发展，虽然还达不到非常成熟，但也有了很多可用的检测方法。对可能存在网络监听的检测一般有下面几种方法。

1．Ping 检测

如果怀疑某台计算机在进行监听，则可以通过向该计算机发送正确的 IP 地址和错误的 MAC 地址的 Ping 方法进行检测，如果看到返回，则基本可以判断该计算机处于混杂模式，在进行网络监听。

2．发送大量数据包

如果怀疑某台计算机在进行监听，可以向网络发送大量的垃圾数据包，因为网络监听软件要对接收到的每一个数据包进行分析，在数据量很大时，反映时间会变慢，这时通过对比分析，可以找出处于监听状态的计算机的幕后黑手。

3．使用反监听软件

要检测网络监听，可以使用反监听工具，如 antisniffer 等进行检测。

4．ARP 数据包检测

除 Ping 包检测外，还可以利用 ARP 数据包进行检测，这也是一种常用的检测方法，与 Ping 检测类似。

除对怀疑进行网络监听的计算机进行检测外，应对网络监听最好的办法是做到防患于未然，有以下几种方法可以采用：

- 采用交换式网络。
- 采用 ARP 欺骗检测。
- 进行数据加密。
- 运行反监听工具。