目录

BUG 和后门
缓冲区溢出
ROOT KITS
社交工程和非直接攻击
打电话请求密码
伪造 EMAIL
拒绝服务攻击
偏执狂
完整的安全策略
不要采取单独的系统或技术
部署公司范围的强制策略
提供培训
根据需要购置设备
识别安全的商业问题
考虑物理安全
第五章协议层安全
TCP/IP 和网络安全
TCP/IP 协议集和 OSI 参考模型
物理层
网络层
传输层
应用层
第六章 保护资源
安全的实施过程
资源和服务
保护 TCP/IP 服务
THE WEB SERVER
CGI 脚本
保护 IIS
文件传输协议服务器(FTP)
访问控制
简单邮件传输协议(SMTP)
INTERNER 蠕虫
MELISSA 病毒
E-MAIL 和病毒扫描
网络级 E-MAIL 扫描
访问控制方法
配置 SMTP 服务器的验证功能
测试和评估
测试已存在的系统
实施一个新的系统
安全测试软件
第七章　防火墙基础
防火墙技术现状

防火墙的定义和描述
防火墙的任务
实现一个公司的安全策略
创建一个阻塞点
记录 INTERNET 活动
限制网络暴露
防火墙术语
网关
电路级网关
应用级网关
包过滤
代理服务器
网络地址翻译 NAT
堡垒主机
强化操作系统
非军事化区域 DMZ
筛选路由器
阻塞路由器
防火墙默认的配置
包过滤
规则和字段
包过滤的优点和缺点
状态多层检测(STATEFUL MULTI-LAYER INSPECTION)
代理服务器
WEB 代理
电路级网关
优点和缺点
应用级网关
代理服务器的优点
代理服务器(应用级网关)
防火墙的一些高级特性
认证
日志和警报
远程访问和虚拟专用网 VPN
第八章 防火墙体系结构
防火墙策略和目的
建立一个防火墙
设计规则
保持设计的简单性
安排事故计划
堡垒主机的类型
单宿主堡垒主机
双宿主堡垒主机
单目的堡垒主机

审计非法服务,特洛伊木马和蠕虫
结合所有攻击定制审计策略
渗透策略
NETBILS AUTHENTICATION TOOL NAT
IP 欺骗和劫持:实例
TCP/IP 堆栈
SYN FLOOD 攻击
SMURF 和 FRAGGLE 攻击
TEARDROP/TEARDROP2
PING OF DEATH
LAND ATTACK
第四章控制阶段的安全审计
控制阶段
获得 ROOT 的权限
获得信息
审计 UNIX 文件系统
审计 WINDOWS NT
L0PHTCRACK 工具
UNIX 密码安全
SHADOW 密码文件
JOHN THE FIPPPER 和 CRACK
信息重定向
擦除渗透的痕迹
作为跳板攻击其它系统
控制方法
系统缺省设置
合法及非法的服务,守护进程和可装载的模块
NETBUS
审计和控制阶段
第五章入侵监测系统
什么是入侵监测
入侵监测的功能
入侵监测系统的构架
网络级 IDS
主机级 IDS
IDS 规则
网络异常的监测
网络误用监测
执行动作 ACTION
误报
入侵监测系统软件
INTRUDER ALERT
第六章 审计和日志分析
基线的建立

网络安全与防火墙篇

第一章 什么是安全？

引　　言

本书第一章内容主要对于安全的发展以及其重要性作了简明的阐述，并介纠了一些国内外知名的网络安全相关网站，并对于如何建立：有效的安全策略给出了很好的建议，并让人家了解几种安全标准。

本章要点：

- 有关安全的定义
- 解释网络安全的必要性
- 识别哪些资源需要被保护

- 识别常见的几种安全威胁类刑
- 如何建立有效的安全矩阵

媒体经常报道一些有关网络安全威胁的令人震惊的事件：，针对日前流行的 Netscape Navigator 和微软的 IE 浏览器程序对于复杂精密攻击(目标是摧毁电子商务服务器)存在的一些安全问题，因此计算机和网络管理员以及用户都必须应付不断复杂的安全环境。黑客和计算机病毒都是普遍的威胁以至于甚至某个具体的日期都与一个特别的安全问题相关。主要的在线电子商务都被证明是易受攻击的。例如，e-bay 和 Amazon．COM 都是恶性攻击的受害者。攻击事件本身，例如 1988 年的 Robert Moms Internet Worm(蠕虫)都变得具有传奇色彩。

众所周知的黑客包括 kevinMitnick 和 JohnDraper(此人既是大名鼎鼎的 CaptainCrunch)但是更多不知名的黑客在互联网上制造着破坏。尽管下面的新闻故事听上去像是一本侦探小说中的摘录，但它却是上实实在在的发生了。一名被 Pentagon 认为是对美国的安全构成头号威胁， 比 KGB 更具致命性的间谍被证明是一名 16 岁的英国音乐学生黑客(他在他的卧室进行“ 工作 ”)美国参议院武器装备委员会被告之 FBI 害怕一个东欧的间谍集团已经获得了美国最高级的机密，包括美国空军防御系统弹道导弹设计。这名在校生在互联网世界上以“ DatastreamCowboy ”而著称，被罚款 1915 美金，但他解释说“ 这些地方比起英国大学计算机来说但容易进入了 ’现在商界张开双臂欢迎 Internet 去从事商业、通讯和合作。敏感信息和通讯路线的完整则变成了一个非常重要的话题，对于相关的威胁，例如黑客和病毒，迅速作出反应以及消除它是每个网络管理员工作的一部分，

Internet 对于任何一个具有网络连接和 ISP 帐号的人邮是开放的，事实上它本身被没计成了一个开放的网络。因此它本身并没有多少内置的能力使信息安全，从一个安全的角度看，Intemet 是天生不安全的。然而，商界和个人现在都想在 Intemet 上应用一些安全的原则，

在 Internet 发明人当初没有意识到的方式下有效的使用它。对于 Internet 用户一个新的挑战是如何在允许经授权的人在使用它的同时保护敏感信息。

安全是什么?

简单的说在网络环境里的安全指的是一种能够识别和消除不安全因素的能力。安全的一般性定义也必须解决保护公司财产的需要，包括信息和物理设备(例如计算机本身)。安全的想法也涉及到适宜性和从属性概念。负责安全的任何一个人都必须决定谁在具体的设备上进行合适的操作，以及什么时候。当涉及到公司安全的时候什么是适宜的在公司与公司之间是不同的，但是任何一个具有网络的公司都必须具有一个解决适宜性、从属性和物理安全问题的安全政策。 .

这节课将讨论与 Internet 有关的安全问题，伴随着现代的、先进的复杂技术例如局域网(LAN)和广域网、Internet 网 Internet、已经 VPN。安全的想；去和实际操作已经变得比简单巡逻网络边界更加复杂。对于网络来说一个人可以定义安全为一个持续的过程，在这个过程中管理员将确保信息仅仅被授权的用户所共享。

本节课结束时，你将熟悉那些被你公司认为适宜的，用来建立和限制行为的过程和技术。你将集中精神在有关将你公司与互联网相连接的安全的问题上。Internet 连接对于陌生用户连接到外露的资源上极为容易。你必须确保它们只能访问那些你想让他们访问的内容，这节课将学习一些控制用户和黑客访问，如何对事件：做出反应，以及当有人规避那些控制时如使损害最小化的方法。

黑客活动

尽管在“黑客帝国“等影片中，黑客只有浪漫色彩，黑客活动被证明是代价高昂的。根据计算机安全机构和 CERT(计算机紧急事件响应组)黑客活动口见增多，并且越来越具有破坏性。CERT 曾提供下列数据以显示黑客活动的效果。

. 五分之一的互联网站点都经历过安全损害
. 估计每年在美国由安全损害所导致的损失可达到 100 亿美金
。 从去年开始网络入侵已经增加了 50%。

根据由信息安全杂志(www. infosecuritymag. com)进行的一项在 1999 年对 745 名 IT 技术人员的调查显示 52%的被调查者在过去的 12 个月经历过某种攻击、入侵、个人信息的泄露。大多数的攻击不是来自于外部，而是来自于网络内部的职员。被凋查者发现的网络入侵的总的花费超过了 2300 万美金，这个数字还不包括未被报道和未知的事件。

IT 界已经对这样的攻击作出了反应，大多数公司已经创立了安全政策，商界、公司机构、电子商务站点现在使用了防火墙，入侵侦察系统以及跟踪网络活动的程序。然而根据一篇来自信息安全杂志的文章(WWW. infosecuritymag. com 巧 uly99／under,htm)这些措施并不能阻止这样的攻击，原因是：

. 日趋精密的攻击以及以 Internet 为基础的技术的快速发展
. 超负荷的 IT 技术人员和资金的缺乏而不能获得更多的资源
. 没有被充分安全保护的系统大量的快速的部署、

风　险

收集数据是一门并不完美的艺术，被不同的专家收集到的数据真正意味着什么总是引起争议的，http：／／www,anticode. com 这个站点在新兴的黑客中极受欢迎，它是许多提供方便可用的资源给新兴的 Internet 用户的站点之一。它使得用户：

- 获得如何开始黑客活动的相当准确的建议
- 扫描网络以确定那些目标被攻击
- 使用虚假信息攻击 e-mail，数据库，文件：,
- 摧毁和渗透路由器和其他的网络连接设备
- 击败和摧毁认证和加密方法

以及 Web 服务器使其瘫痪

抵御攻击是困难的，除非你知道如何把攻击分类有系统的反击它，但是确保你的系统绝对安全，是不可能的。

百分之百的安全?

连通性就意味村危险，如果你允许合法的用户访问你的计算机或网络就存在着被误用的危险，一种流行的说法是只有与网络无连接并且被关闭的锁在一个安全的地方(钥匙被扔掉)的计算机，才是真正唯一安全的计算机，尽管这种方法使得计算机很安全，但也使得计算机毫无用处。然而，尽管你从来不可能实现绝对安全，但是你可以达到某种水平，使得几乎所有最熟练的和最坚定的黑客不能登陆你的系统。可行的安全策略能够使黑客对你的公司的损害最小化。它们甚至能够抵御最坚定的黑客。对于网络安全，你要经常限制合法用户的网络许可权，以便他们仍旧能够完成他们的任务，但是不能获得更多的访问权限。这个简单的策略的后果是即使黑客能够窃取到一个合法用户的身份并且进入到系统。他将只能获得那个用户访问权限。这样的一个限制措施将抑制任何可能的由那个盗取了用户名字和密码的黑客所引起的损害。

安全即寻求平衡

一个关键的安全原则是使用有效的但是并不会给那些想要真正想要获取信息的合法用户增加负担的方案，寻找出一条实际应用此原则的途径经常是一个困难的寻求平衡举动。使用过于繁杂的安全技术使得合法用户厌烦和规避你的安全协议是非常容易的。黑客时刻准备着和用这样一些看上去无害的行动，因此拥有一个过分繁杂的安全政策将导致比没有安全政策还要低效的安全。你总是需要考虑一下你的安全政策给合法用户带来的影响在很多情况下如果你的用户所感受到的不方便大于所产生的安全上的提高，则你的政策是实际降低了你公司的安全有效性。

建立有效的安全矩阵

尽管一个安全系统的成分和构造在公司之间是不同的，但某些特征是一致的，一个可行的安全矩阵是高度安全的和容易使用的，它实际上也需要一个合情合理的开销。，一个安全矩阵由单个操作系统安全特征、日志服务和其他的装备包括防火墙，入侵检测系统，审查方案构成。

一个安全矩阵是灵活的可发展的，拥有很高级的预警和报告功能，表 1—1 概括了一个有效的安全矩阵系统最主要的几个方面。

特点	描述
允许访问控制	通过只允许合法用户访问来达到你的日的
	最人扩展通信的功能同时最小化黑客访问的可能性 当黑客已经访 6 习到你的资源时尽可能地减小破坏性
容易使用	如果一个安全系统很难使用，员工可能会想办法绕开它 你要保证界面是直观的
合理的花费	你不仅要考虑初始的花费还要考虑以后升级所需要的费用 你还要考虑用于管理所要花的费用：需要多少员工， 达到什么样的水平来成功的实施和维护系统。
灵活性和伸缩性	你的系统要能让你的公司按其想法做一些商业上的事情 你的系统要随着公司的增长而加强
优秀的警报和报告	当一个安全破坏发生时，系统要能快速地通知管理员足够详细的内容要配置系统尽可能正确地对你发出警告。可以通过 Email，计算机屏幕，pager 等等来发出通知。

保 护 资 源

你现在在已经学会了一个安全系统的一般性原则，接下来应该讨论什么资源需要被保护为你的网络构建安全构架的时候，把你的资产划分为 4 个资源组是很有帮助的：

- 终端用户资源(员于使用的 windows98／2000 主机)
- 网络资源(路由器、交换机、电话系统)
- 服务器资源(包括文件；、DNS、Web、FTP 和 e-mail 服务器)
- 信息存储资源(包括人力资源和电子商务数据库)

终端用户资源

确保你已经使得你公司的职员保护他们的工作站，对于你的资源来说并不是所有的损害都来自于带有恶意的用户的操作或黑客攻入你的系统。经常，计算机仅仅是被简单的用户操作失误所损害。例如，很多雇员开没有意识到下载 ActiveX 文件和使用 Java 小程序所涉及的危险，还有很多人当他们离开办公室(甚至很短时间)他们也并不使用屏幕密码保护程序，以防止偷窥用户也常常不知不觉的下载病毒和特洛伊木马(Tr01ans)因此损害了网络的,正常功能。一个特洛伊木马(trojans)是一—个程序或文件,其目的是在于用一个合法的方式进行操作，然而有一个替代的秘密的操作，例如把关键的敏感的公司信息通过 E-mail 发送给黑客。然而,职员通过使得他们的浏览器被设置成对于 ActiveX 和 Java 小程序最大程度的安全设置来提高安全性能,你也可以确信每名员工当从互联网上下载任何东西时都使用病毒检查监测。教育每名使用者早期应用的安全技术很重要的一点是保护本地资源,然而 internet 安全涉及则不仅仅是保护个人资源。

网络资源

网络对于一个公司来说是一个主要的通讯媒介，如果一个黑客获得访问权限或者控制了公司的网络，他将能访问几乎所以的公司数据。必须意识到许多黑客能够仿造任何 IP 协议设备(它拥有一个 IP 地址)，这称之为 IP 欺骗。这种行为允许黑客获得访问权限去进行系统偷窥(systemsnooping)。因为在 TCP／IP 里没有保护是可行的，所以黑客可以充分和用任何不具有专门机制的设备。另外的网络资源包括路由器，同样也易受到攻击和带宽消耗。

服务器资源

Internet 上的 E-mai 和 FTP 服务器都易受到几种类刑攻击，一般的，服务器给网络架构提供存储区域，并且成为枢纽。它们也控制全部的系统安全。黑客试图获得服务器资源的访问不权限，这样他们就能够访问和控制其它资源。

信息存储资源

任何公司最重要的功能是它如何组织和传播信息。一个黑客最终的目标是发现信息并且篡改帮助建立和传输信息的网络和方法黑客。由于多种原闪，黑客想要获得信息，有些是怀有恶意，还行一些是为了进行工业间谍刺探，表 l-2 列举出了一个网络潜在的易受攻击的部分。

重要地点	潜在的威胁
终端用户资源	病毒，木马，Java 小程序可以对本地系统造成危险。
网络资源	IP 欺骗，系统探测，及获得相关信息
服务器资源	非授权侵入，截取服务，木马。服务器资源经常成为最主要的目标
数据库和信息资源	得到商业机密，交易行为，消费者的数据，等等

黑客的分类

流行文化经常把黑客描写成为才华横溢、蔑视权威、未完全成熟的男性。尽管这种描述有时的正确的，但是根据他们的态度和动机来给黑客分类可能是更加实用的。
恶意的举动可能有很多原因，但是这类举动一般是归纳到 3 个大的范畴。当确定你公司的安全的时候，需要考虑的最重要的臆见事是识别出把你的公司作为目标的黑客的类型和预料黑客的态度。这 3 个类别是偶然的破坏者，坚定的破坏者和间谍。

偶然的破坏者

偶然的破坏者有时是一个信息寻求者，但更多的时候是一个另人恐怖的 ”猎手 ”。这种偶然的破坏者拥有超人的智慧，换句话说，偶然的破坏者可以轻松的闯入你的系统但并不一定有任何目的，大多数的黑客都属于这类范畴。仍然能够和用合适的安全应用程序以及特殊的机制来阻止这种侵入，特别的这个安全政策规定了你发现并且对黑客做出反应，可能一些偶然的破坏者是一些能够获得电话线的十几岁的恶作剧者，网络中这样一群黑客的数量是很多的。

坚定的破坏者

坚定的破坏者不管后果和困难要获得你系统的访问权，这种类别的黑客正通过互联网或者一个员工来达到目的。黑客能够获得被专门设计为能够进入你的网络的方法和工具，尽管你拥有有效的设备和清晰的安全政策，这种类型的黑客使用任何方法和决心和意志将最终导致成功。坚定的破坏者经常闯入高度精密的系统以证明他们的实力，一般来说这些黑客并不是毁坏信息而经常是获得公司和网络的信息，仅仅因为他们有这个实力。坚定的破坏者有许多动机，例如为了个人原因而收集信息，一个黑客可能是一个不满的职员，然而也可能是对于大的公司或者政府的怨恨所造成的。一些攻击是黑客想要去除他们认为有争议的或者不满的内容的存在的结果。其他的黑客有着更加独特的动机，有的是为了出名，有的是需要获得一种成就感，还有的是为了证明网络能力，这样的一些动机也许可以解释大多数在过去的几年中发生的页面涂改事件。

间谍

有着非常明确的目标，想要获得信息或者摧毁服务，他们有着很好的资金来源，对于资源几乎不加限制的访问权限，间谍的动机是获取财富和意识形态的信仰。这些黑客为了他们视之为目标的网络访问权限不惜一切代价。对工业间谍感兴趣的大公司和许多政府都经常资助间谍组织，但是一些间谍只是雇佣兵，他只为出价最高的人服务。以后的课程将讨论如何使用防火墙和具体的办法去防御黑客，对于一个坚定的黑客，审查是最有效的武器，依靠合适的审查，你将进可能快的发现和制止一个黑客。对于审查更为详细的讨论将在以后的课程中进行。另外的一个课程将提供一个计划。通过这个计划你将对黑客作出反应并且记录下这个活动，有时与执法部门取得联系是必须的。例如美国联邦调查局(FBI)。

安全标准

在完成关于一些引起安全基础的讨论之后，我们必须注意几种已存在的安全标准。国际标准化组织(ISO)7498-2 安全体系结构文献定义了安全就是最小化资产和资源的漏洞。资产可以指任何事物。漏洞是指任何可以造成破坏；系统或信息的弱点。威胁是指潜在的安全破坏。ISO 进一步把威胁分类为偶然的或故意的，主动的或被动的。偶然威胁是指没有事先预谋的事件，这类的威胁包括天然的灾祸或错误的系统维护。故意的威胁包括非常有经验的攻击者和用特殊的系统知识来破坏计算机或网络上的数据。被动式威胁不修改系统中所包含的信息。

安全服务

ISO 7498-2 文献此外还定义了几种安全服务。表 1-3 作了一些总结。这些服务将在后面的章节中详细介绍。

服务	目的
认证	提供身份的过程。
访问控制	确定一个用户或服务可能用到什么样的系统资源，亦看还是改变。一旦一个用户认证通过，操作系统上的访问控制服务确定此用户将能做些什么。
数据保密性	这个服务保护数据不被未授权的暴露。数据保密性防止被动威胁，包括一些用户想用 packet sniffer 来读取网线上的数据
数据完整性	这个服务通过检查或维护信息的一致性来防止主动的威胁
不可否定性	不可否定性是防止参与交易的全部或部分的抵赖。比如说在网络上，一个人发送了一封 Email 信息或一些数据，如 ping 包或 SYN 包，然后说“ 我并没有发送 ”。不可否定性可以防止这种来自源端的欺骗。

安全机制

根据 ISO 提出的，安全机制是一种技术，一些软件或实施一个或更多安全服务的过程。ISO 把机制分成特殊的和普遍的。一个特殊的安全机制是在同一时间只对一种安全服务上实

施一种技术或软件。加密就是特殊安全机制的一个例子。尽管你可以通过使用加密来保护数据的保密性，数据的完整性和不可否定性，但实施在每种服务时你需要不同的加密技术。一般的安全机制都列出了在同时实施一个或多个安全服务的执行过程。特殊安全机制和一般安全机制不同的另一个要素是一般安全机制不能应用到 OSI 参考模型的任一层上。普通的机制包括：

- 信任的功能性：指任何加强现有机制的执行过程。例如，当你升级你的 TCP／IP 堆栈或运行一些软件来加强你的 Novell，NT,UNIX 系统认证功能时，你使用的就是普遍的机制。
- 事件检测：检查和报告本地或远程发生的事件
- 审计跟踪：任何机制都允许你监视和记录你网络上的活动
- 安全恢复：对一些事件作出反应，包括对于已知漏洞创建短期和长期的解决方案，包括对受危害系统的修复。

额外的安全标准

除了 ISO 7498-2 还存在一些其它政府和工业标准。主要包括

- British Standard 7799：概括了特殊的“ 控制 ”，如系统访问控制和安全策略的使用以及物理安全措施。目的为了帮助管理者和 IT 专家建立程序来保持信息的安全性。
- 公共标准
- 桔皮书(美国)

桔皮书

为了标准化安全的级别，美国政府发表了一系列的标准来定义一般安全的级别。这些标准发表往一系列的书上通常叫做“ 彩虹系列 ”，因为每本的封面的颜色都是不同的。由为重要的是桔皮书。它定义了一系列的标准，从 D 级别开始(最低的级别)一直到 A1(最安全)级。有关这部分内容我们会在操作系统安全篇中详细介绍。

本章小结：

通过本课的学习，相信你已经对于安全的概念有了清晰的认识，并了解关于需要保护资源的分类，并详细介绍建立一个有效的安全矩阵所应具备的属性：对于安全标准的理解有助于我们日后制定完整的符合国际化标准的策略。

问题讨论：

- √ 制定有效的安全矩阵应具备什么属性?
- √ 资源分类的重要性及其优点?
- √ 几种常见的安全标准的定义?

第二章

安全的基本元素

引　言

了解构成安全的一些基本元素，对于我们进一步进行安全方案的制定和实施是至关重要的：你还需要进一步了解一些安全机制来建立你的安全体系结构。这节课将讨论一个连

贯的安全政策的重要性以及审查，加密，认证机制。

本章要点：

- 阐述一个有效的安全策略基本
- 识别用户认证方法的关键
- 解释对于访问控制方法的需要
- 列举出三种在互相网上的主要加密方法
- 解释审计的需要
- 在选择安全设备和软件：时要考虑使用的简易性

安全的基本元素

下图显示了最重要的安全元素，同时它也展示了这些安全元素的构成的等级。

每一个元素都与其它的元素共同产生作用以确保一个机构能够尽可能有效的通信，在金字塔底部的是团体的安全政策，它是任何成功的安全政策的基础。拥有一个安全政策并不能保证你将消除入侵和信息丢火，为了防止上述情况发生，你还必须小心谨慎地审查你的网络，然而，一个安全策略可以为你以后的活动提供一个基础。

管理使用和执行安全政策,审齐用户活动,试图确定安全问题(包括非法的用户操作,一个有关很低补丁水平的系统,或一个网络外部的入侵)管理层和安全管理员将创建一个共同的安全政策，因为这样就为所有的网络活动提供了一个基础。

安全策略

一个安全政策将允许你建立一个有效的安全基础设施，基础设施包括：

- 安全资源，包括信息和实际系统本身
- 所有的雇员都尽可能快的完成工作

安全政策必须为整个机构提供指导方针并且是建立安全系统使用的防御第一线，你必须确保你的安全政策并不与你的公司的目标和实际活动相抵触，因此你必须对于你的资源合理的保护。为了确定资源准确需要多少保护，你必须确定它将遇到多大危险，举一个内部用户工作站很显然比一个 WEB 服务器遇到的危险要小的多，因为后者直接暴露在 Internet 上，为了减少危险，你应该采取以下步骤：

- 为你的系统分类
- 指定危险因数
- 确定每个系统的安全优先级
- 定义可接受和不可接受的活动

- 决定在安全问题上如何教育所有员工
- 确定谁管理你的政策

一旦你确定了危险因素和资源的优先级，你将能确定你将对每一部分资源采取什么样措施，根据资源的情况你将记录你的安全政策。举个例子你可以指定用户工作站必须运行新的防病毒软件和你的外部路由揣在外部端口过滤掉 Telnet,你最重要的资源，例如 E-mail 服务器，将需要最详细和最严格的保护。

系统分类

正如上面所述，第一步是有效地分配安全资源，建确一个合理的安全基础设施，你必须确认然后根据对机构的重要性对系统和数据进行分类。

经常，把系统资源分出三个类别是有必要的：

级别 1：那些对于生意的运行是至关重要的系统，例如，一个电子商务公司可能把它的 WEB 服务器作为级别工的系统，雇员的数据库，用户数据库，E-mai 服务器都认为级别工资源。

级别 2：那些是必须的但对于日常工作不是至关重要的系统，尽管它们不能长时期地不工作，但是一两天不工作不会使公司迫于瘫痪。举个例子，如果员工传呼机号码的数据库两大不能正常工作，这样虽然很不方便，但不会造成致命的问题。

级别 3：只要桌上电脑并不会对级别 1 和级别 2 的系统造成影响，则本地桌上电脑将属于级别 3。

表 2-1 概括了这种分类原则

安全分类级别			
级别	数据	系统	安全
级别 3：日常工作	一些用于操作的数据	一般的系统，在数据丢失或停止时不会导致公司的商业行为正常运转	一般的安全策略和防范
级别 2：较重要	如果数据保护不好的话会使公司产生极大的风险	操作系统或电子商务在线系统，其停止时间最多不能超过 48 小时，这种情况内部服务器不能直接连入到 Internet	一般的安全策略加上特殊的监视，审计和恢复策略

级别 l：最重要	需要高度保护的重要数据，如商业机密和客户资料等	重要任务级的系统，系统停止运行不能超过几个小时，如证书服务器，公网上对外服务的一些服务器等	安全分析及扩展的安全机制，系统级别的审计，监视和安全功能

明智地为系统分类

安全管理员经常犯下这样的错误，即把太多的资源划到级别 l，级别 1 的资源仅仅是那些一也不能产生的问题的资源，例如：E-mail 已经飞快地成为了绝大多数机构中最重要的构成元素，绝大多数网络管理员把它归化为级别 l 资源，因为它们对网络其它部分提供了一个基础。对于用户而言，绝大多数机器都不是级别 1 资源，即使 CEO 的笔记本电脑坏了，但是公司其它的电脑毫无疑问在 CEO 电脑维修期间仍旧正常工作，类似的，一个非电子商务站点并不会把它的 WEB 服务器作为级别 1 资源，你应该小心谨慎地权衡每种情况，举个例子，如果你的公司使用局限网，那么它的 WEB 服务器是多么重要?你应该依据下面的标准来做出判断。

- 机器的流量是多少?
- 机器上的信息的敏感度，服务器是仅仅包括少量的链接和作为“ 神经中枢 ”(即重要的信息在这几进行交换)。
- 根据系统的性质，一些系统天生的比其它系统更加安全。

资源优先级划分

在把公司资源都分类以后,你的安全实施计划中应该包括一个危险优先级列表和一个行动列表，你的应该根据每个系统和它的信息(包括多余系统的可用性等等)的重要性而定。这种优先级列表是重要的，因为当发生事故时，员工将不会被迫去决定什么应该先被抢救，期待他们在那种情况下做出是一种过渡的负担，将损害公司整个的安全，很少的了工厂部门有充足的人手和资源去解决所有级别 1 系统。

你应该从财政状况以及时间上考虑优先级问你自己以下几个问题：

- 我能为这部分资源花费多少钱和时间?
- 哪种级别工资源需要最大的安全?

一个级别 l 的系统含有重要的资源并要慎重考虑，但一个级别 3 的系统也许仅仅需要病毒检查， 一个不切实际的政策将伤害一个公司保护自己的能力，甚至可能伤害公司有效通信的能力。如果你正在从事用信用卡进行电子消费或电子现金交易活动，你需要对在这些系统里用到的数据和服务器进行特别的保护，如果系统被成功的渗透，你的公司将对被盗用的信用卡帐号或其它信息付出代价，更为重要的是你公司的声誉将很难恢复。

指定危险因数

一旦你所有网络资源被分类和优先级化，你必须指定危险因数，危险因数指的是一个黑客攻击某种资源的可能性，你已经定义的某种资源将确定危险因数，当对某种资源确定危险

因数时，需使用这条基本原则，资源越敏感危险因数就越人。举个例子，生产钉书钉的公司有一个 WEB 站点，这个站点的危险因数要远远低于一个生产弹道导弹的公司的站点，安全基础没施是安全政策在执行阶段的体现，它将包括多层次的防御和依据每个系统的分类而确定下来的不同等级的保护。http://www.securtyinfo.com 这个站点对于正准备创建一个安全策略的来说是一个好去处，这个站点描述了政策和技术之间的关系。

定义可接受和不可接受活动

为了对特殊的资源设计安全政策，一个有经验的安全管理员必须区别出可接受和不可接受活动。这样的活动必须根据每类资源而定，你的安全实施计划必须指定可接受的活动和不可接受的活动。对于安全而言，可接受和不可接受的范畴总是有效的，然而，机构组织将根据需要来确定不同的可接受活动，一个对于一家公司是可行的政策可能会对另外一家公司带来灾难性后果，因此，尽管基本原则是一致的，但是个体的实际应用将会是不同的甚至是根本的不同。

可接受的活动

对于每一类资源，可接受的活动将是不同的，假设对于你公司的 WEB 站点可接受的活动包括允许用户仅仅浏览在公文件夹里的 HTML 页的内容和递交请求,你的政策将给予系统管理员额外的权限使他们可以访问 WEB 站点的所有目录，并且进行管理，最后你的安全政策将毫无疑问地给予你公司的 Webmaster(网络管理员)更深的访问权限使得他可接受的活动。

不可接受的活动及实施

对于每一类资源，不可接受的活动也是不同的，当你定义什么是不可接受时，你可以使用两种方式中的一种，你既可以列举出什么是可接受的，这样就建立了一个不可接受的列表或者你清晰地列举出什么是不可接受的，每个方法都有它自己的优点和缺点，如果使用不当，一个可接受活动的列表经常是范围太广，并且实际上常与用户活动产生矛盾阻碍了公司的正常功能，后面一种经常遗漏掉不可接受的活动，使得保护产生了一个裂口，一个法律问题随时产生，如果安全政策遗漏了一个重要的活动或者几个活动的组合，则一个黑客可以找出这个政策的漏洞。因为没有两个商业团体是相同的，所以不可接受活动没有一个清晰的定义，因此经常必然地把不可接受的活动定义为任何没行具体标明为是可接受的活动，然而使用如此一个大的范围制订和实施一个安全基础设施将是很困难的。

因此最好的解决方案是定期定义和列举出不可接受的活动，这样做可能会花费一些时间并且需要经常更新，但是也将能够建立一个有效的政策，扩展一下上面假设的例子，你也许想要除了网络管理员任何人不能修改 HTML 文什的内容，通过例举出这样的活动，你能确保这些活动在你的保护机制里已经被具体地说明，并且你的用户知道了政策。

将策略应用到资源上

一但你已经确认了资源，并且确定了它们的，你必须对你网络里的每一个元素确定一个合适的安全策略，安全策略包括购买防火墙设备和使用加密，每一个设备都需要一个单独的安全评估，你应该对于你最重要的资源实施最全面和先进的安全策略。

列举出你将应用到每个资源上的策略，例如你可能不用在你的路由器上实施包过滤，这个步骤是基础的，但是你应用到你的系统时它将节约大量的时间。

应用安全策略到资源上的一个关键是考虑在每个资源上将花费多少时间和金钱，安全策略将总是最佳性能价格比的，意思是尽可能的全面有效同时尽可能少的花费。

定义教育标准

完成有效的安全的一个最好方法是教给你公司的职员关键的安全原则。举个例子，如果用户知道如何选择好的密码，则对于一个黑客而言将更加困难规避你的密码认证系统。经常这样的一个系统对于站点的安全是至关重要的，管理员需要了解如何在他管理的系统上设立有效的安全，程序员需要知道如何编写软件，以使软件不会为黑客提供后门去刺探网络。通过定义你想要不同的组织知道哪些知识，你将能创建和使用机制去训练他们。表 2-2 显示了你提供给你公司网络的用户不同级别的训练：

级别	知识的需要
用户	要对一些安全威胁和漏洞敏感：要对保护公司的信息和资源引起重视
执行者	需要达到熟悉公司安全知识的级别并做出使用信息安全程序的决策
管理员	开发防止威胁和漏洞的技能来满足系统和资源安全的需要

谁负责管理策略

如果你没有指定哪些人或组织对于维护安全计划的每一部分负责任，则最好的安全也将会很快失败。你的安全政策应当列举出叫哪些部门负责保护哪些系统，如果你没有为资源分类并且专门为系统的各个部分指定责任人，则你的系统将不会达到它所必需的安全。在一些更大的公司，整个一个部门将负责单一的网络安全，大多数的管理资源将被用于审查职员对于政策的遵守情况。

加　密

加密是使某些东西只能是某些特定的接受者可以知道的过程。网络和文件：经常使用加密技术。对于文件而言，加密把容易渎取的源文件变成密文文件。能够政取这种密文的方法是获得密钥(即把原来的源文件加密成密文的东西)。网络是一个开放式系统，加密变的不仅对于 email 文件，而且对于网络通信都很重要。

加密类型

你可能听说过不同的加密文件：方法，包括使用算法，例如 DES，RSA 和 MD5。这些不同方法的每一种都是在网络中用到的三种重要的加密类型的实例。

- 对称加密：使用一个字符串(密钥)去加密数据。同样的密钥用于加密和解密
- 非对称加密：使用一对密钥来加密数据。这对密钥相关有关联，尽管分析公钥和获得私钥是很困难的(几乎是不可能的)，这对密钥一个用于加密，一个用于解密，反之亦然。非对称加密的另外一个名字是公钥加密。
- HASH 加密：更严格的说它是一种算法，使用一个叫 HASH 函数的数学方程式去加密数据。理论上 HASH 函数把信息进行混杂，使得它不可能恢复原状。这种形式的加密将产生一个 HASH 值，这个值带有某种信息，并且具有一个长度固定的表示形式。你将在整个课程中看到这三种加密类型的用法。

有关更详细的加密知识我们会在第三章中重点讲述。

认　证

认证过程试图验证一个用户，系统或系统进程的身份，在这种验证发生时，依据系统管理员制定的参数真止的用户或系统能够获得相应的权限。

如果你使用过 ATM 下或出示过学生 ID 卡，或使用过汽车驾驶执照，则你已经涉及了一种个人认证的形式，如果你曾经使用密码使你的机器登录到网络，则你已经参与了认证，事实上任何使用过家门钥匙或者汽车钥匙的人都用到了用户认证的原则，然而认证也用于整个系统和网络。

认证方法

用户或系统能够通过四种方法来证明他们的身份，对于认证这节课的其余部分将根据这四种方式来讨论具体的程序，你能通过以下四种方法来证明白己的身份。

- What you know?
- What you have?
- Who you are ?
- Where you are?

Whatyou know?

在互联网和计算机领域中最常用的认证方法是密码认证，当你登陆计算机网络时它总是需要你输入密码，这是你应该知道的。计算机把它的认证建立在密码之上，如果你把密码告诉了其他人，则计算机也将给予那个人的访问权限，因为认证是建立在已知密码之上的，这并不是计算机的失误，而是用户本身造成的，当然仅仅屈于一种模式的认证。

Whatyou have?

这种方法稍微先进一些，因为你需要一些物理原理，一个好的例子是一张楼宇通行卡只有在扫描器上划过卡的人才能进入大楼，这里认证是建立在这张卡之上，如果你把这张下借给了别人，那个人也能进入这幢大楼，因此如果你希望为进入大楼创建一个更加精密的认证系统，你可以要求不仅要有通行卡而且要有密码认证。在计算机领域中“ 你拥有什么 ” 方法的一个典型例子是智能卡和数字认证的使用。

智能卡

所有的智能卡都含有一块蕊片，蕊片中包含了一些拥有持卡人的个人信息，驾照信息及医疗信息等等，一块智能卡与标准信用卡大小相等甚至更大，尺寸大小主要取决于内嵌蕊片的功能。有时内嵌蕊片包含只读信息，蕊片比起信用卡背面的磁条卡含有更多的信息，这种类别的智能卡经常只能被开发一次，并且完全依赖于称为智能卡可读器来进行操作，美国快递蓝卡站点，它是专门设计成开发上面所提到的智能卡的市场。所有的智能卡都依赖于一个可渎器(一个电子设备)。ISO 7816 文献包含了用于智能卡的标准，你可以往以下的站点中到有关智能卡的更多内容

智能卡工业协会 WEB 站： www。scia. org

Schlumberger 主页站点 www. slb. com／smartcards.

Visa 站点 www.visa.com/nt/chip/main.html

Who you are?

这种过程通常需要一些物理因素，如基因或其它一些不能复制的个人特征，这种方法也被认为是生物测定学。到目前为止高级生物学认证已经很有经验，并且只在一些高安全环境中实施。现在，上百个公司都开发出较低价格的生物测定解决方案。例如这种方法包括指纹，面部扫描器，视网膜扫描器和语音分析。

Compaq 公司提供了对于标准串口鼠标的指纹扫描器，并附在临视器旁。你可以出问 www.compaq.com/products/optionts/fit/index.html 来找到一些更多相关的内容。

Where you are?

考虑到认证的缺点，这种策略根据你的位置来决定你的身份。例如，UNIX 的 rlogin 和 rsh 程序通过源 IP 地址来验证一个用户，主机或执行过程。反向 DNS 查询不是一个很严谨的认证实施，但它却是相关的因为它至少在允许访问前企图判断传输的源位置。

特殊的认证技术

下面是两种用于加强认证系统的技术。它们结合使用加密技术和额外策略来检查身份。你不需要一定使用像 Kerberos 或一次性密码这样的程序，但是在你的认证手段中使用这样的程序可有效地帮你防止一些恶意破坏。

Kerberos

Kerberos 系统是美国麻省理工学院为 Athena 工程而设计的，为分布式计算环境提供一种对用户双方进行验证的认证方法。Kerberos 是一种被证明为非常安全的双向身份认证技术，其身份认证强调了客户机对服务器的认证，而别的身份认证技术往往只解决了服务器对客户机的认证。Kerberos 有效地防止了来自服务器端身份冒领的欺骗。在讨论认证的过程之前让我们先了解一 · 下几个元素的约定：

K-——--密钥
A---—一身份
C-----—-用户
P------—访问授权服务器
PAC---访问授权服务器签发的授权凭证
S-—--—-应用服务器，如邮件服务器等
{…}Kn ——表示用 Kn 加密人括号中的内容

Kerberos 的认证过程如下：

①用户 C 以明文的形式向向身份认订 I』艮务器 A 发送自己的名字；服务器 A 从安全数据库中杳找到用户 C 的加密密钥 Kc，随机生成下一阶段使用的加密密钥 K1，然后将 K1 和用于以后向服务器 A 证实用户身份的通信凭据{K1。C}Ka 用 Kc 一起加密为{K1,{k1，C}Ka}Kc 传给用户 C。

②用户 c 得到服务器 A 发回的{K1，(k1,C)Ka}Kc 后，使用自己的密钥 Kc 进行解密通信凭据{K1，c}Ka。由于用户 c 知道只有服务器 A 知道 Kc，因此用户 c 可以确认服务器的身份。用户 c 将得到的送给服务器 A， 申请访问授权服务器 P 的通信凭据{K2,C}KP。当身份认证服务器 A 收到用户的请求后，它用自己的私钥 Ka 来解密。由于服务器 A 只有 c 知道 Kc，所以身份认证服务器可以确定这个请求必定是来自 c 的。这样双方就进行了身份认证。接着双方就可以进行下面的操作了。

C->A：{K1，C}Ka,{C,MD-5Checksum，timestamp}K1

A--)C：·.....

我们可以看出，在 C 向 A 的请求信息中包含一个数据签名：{C,MD-5 Checksum，timestamp}K1，该数字签名含有时间戳，只在一段时间内生效。这可以使得攻击者无法篡改原始信息，并且无法进行重传攻击。

不过我们在使用 Kerberos 认证应该注意以下一些问题：

- 用户 C 的加密密钥是整个身份认证过程的核心所在，必须定期更换
- 多数计算机系统没有保存钥匙的安全区域。实际应用中应对保存各用户加密密钥的安全数据库进行严格管理。
- 随机产生的加密密钥应符合安全的规定

一次性密码(OTP)

为了解决固定口令的诸多问题,安全专家提出了一次性口令(OTP：OneTimePassword)的密码体制，以保护关键的计算资源。

OTP 的主要思路是：在登录过程中加入不确定闪素，使每次登录过程中传送的信息都不相同，以提高登录过程安全性。例如：登录密码：MD5(用产名+密码+时间)，系统接收到登录口令后做一个验算即可验证用产的合法性。

访问控制

每个系统都要确保只有它们想要的个体，系统才能够访问，这种机制叫访问控制。一个网络内部的机制确保每个用户和系统只能访问安全策略所允汁的访问。访问控制是发生在认证过程之后。在你经过系统认证后，是通过访问控制机制来控制你在系统中能访问些什么，这种机制能用于赋予或拒绝权限。一个形象的比喻是把访问控制看作是一个公司的大楼。大多公司都有一个议会休息室并且任何人都能进入，这个休息室可以看作是一个 WEB 服务器允许未授权的用户访问其主页。要进入公司真正的办公室，人们需要出示身份徽章。这种形式的安全允许只有经过认证的员工才能访问公司的办公室。在员工进入人楼后，他们的身份卡只能允许他们访问某些办公室。这种机制是一种访问控制，它限制了认证后的用户能访问些什么。

所有的操作系统都支持访问控制。访问控制是保护服务器的基本机制。你必须在服务端上限制哪些用户可以访问服务和守护进程。

访问控制列表(ACL)

现代的信息系统把资源处理成有着某些特征和属性的对象。资源可以是像打印机或磁盘这样的设备，也可以是操作系统，应用程序或内存。计算机上的文件：也是一种资源。与这些资源安全相关的特性就是访问控制列表(ACL)。一人 ACL 是标识个人用户或组的数据库。每个用户或组都被分配一个访问级别，并根据这个数据库所包含的内容定义这些用户或组能够执行什么。一个通过认证的用户仍必须通过 ACL 来取得相应的权限

执行控制列表(ECL)

在访问控制里一个新的概念就是执行控制列表(ECL)，经常用于特殊的应用程序，如 NetscapeNavigator 或微软的 InternetExplorer。一个 ECL 允许操作系统限制一些特定程序的活动。没有商业的操作系统或平台实施一个完全的 ECL 策略。UNIX 系统包含了一些对于 rexec，rlogin 和 rshell 程序的执行控制列表版本。这些程序都使用执行控制列表来确定在主机 A 上的哪些用户可以不登陆的情况下在 B 主机上执行程序。但是这种形

式的执行控制列表只能在远程系统上工作。

执行控制列表的一个好处就是能对于那些恶意的Active X控件程序的破坏起到一定的保护作用。例如，你可以进一步地控制．java小程序。最后，软件商们已开始开发能够执行更多任务的ECL程序，来允许用户自己决定程序的参数。

审计

审计是整个安全计划一个基本特征。多数现在的系统可以以日志文件的形式记录下所有的活动。这些日志可以帮助对你实施的安全进行有效地诊断。通过这些活动的日志，你总是可以判断是否或者怎样一个不允许的活动发生。

被动式和主动式审计

审计包括被动地记录一些活动。在被动审计中，计算机简单地记录一些活动，并不做什么处理，因此，被动式审计不是一个实时的检测，因为必须得查看这些日志然后对其它包含的内容采取措施。被动式审计的原则是需要你前期事先的做些设置。

主动式审计包括主动地响应非法和入侵，这些响应可能包括

- 结束一个登陆会话
- 拒绝——些主机的访问(包括WEB站点，FTP服务器和e-mail服务器)
- 跟踪非法活动的源位置

安全的权衡考虑和缺点

很多时候管理员需要实施安全却在设计阶段没有慎重考虑。安全需要经常也有些缺点，它们可能会是

- 增加了复杂性：你不得不培训用户如何使用你需要的安全机制
- 降低了系统响应时间：认证，审计和加密机制会降低系统性能

本章小结：

有效的安全结果是来自一个坚固的安全策略，在本课中你已学到一个安全策略足是由于不同的技术，服务和机制来一起工作的。我们还学到如何和用一些可靠的技术和规则，如加密，主动式和被动式审汁，存取控制哼结合来达到一个可靠的安全，当然，我们也不要忘记要权衡地考虑安全所带来的一些负面影响。这里要求人家要尽可能的使你的安全实施不要过于复杂。

问题讨论：

√ 安全包含哪些要素

√ 评估风险因素的方法及策略

√ 加密、认证的几种方式及原理(包括两种特殊的认证方式)

第三章

应用加密

引　　言

前面已提到，应用加密是由于多种原因的。加密可以保证数据的保密性，也可用于验证用户，它足在实现网络安全的重要手段之一。在本课中，你将学到如何使用对称加

密，非对称加密和 HASH 加密来建立一个信任关系。
本章要点：

- 列出特定的对称加密，非对称加密和 HASH 加密
- VPN 的原理和实施
- 证书服务器的安装和配置及 SSL 的应用
- 在 WindowsNT 和 Linux一下配置 PGP 及 GPG

加密的优势

加密提供以下四种服务，见表 2-3

服务	解释
数据保密性	这是使用加密的通常的原因。通过小心使用数学方程式，你可以保证只以你打算接收的人才能查看它。
数据完整性	对需要更安全来说数据保密是不够的。数据仍能够被非法破解开修改。一种叫 HASH 的运算方法能确定数据是否被修改过。
认证	数字签名提供认证服务。
不可否定性	数字签名允许用户证明一条信息交换确实发生过。金融组织由其依赖于这种方式的加密，用于电子货币交易。

加密强度

加密文件：一个常被讨论但又经常被误解的方面是加密强度。什么构成了加密的强度?什么是被美国出口法保护的?哪种级别的加密是被不同的安全需要所要求的?如何确定加密的有效强度?

加密强度取决于二个主要因素：

首先是算法的强度，包括几个因素，例如，除了尝试所有可能的密钥组合之外的任何方法都不；能数学的使信息被解密。从我们的角度而言，我们应该使用工业标准的算法，它们已经被加密学专家测试过无数次，任何一个新的或个体的配方将不被信任直到它被商业的认证。

第二个因素是密钥的保密性，一个合乎逻辑但有时被忽略了的方面没有算法能够发挥作用如果密钥受到损害，因此，数据的保密程度直接与密钥的保密程度相关，注意区分密钥和算法，算法不需要保密，被加密的数据是先与密钥共同使用，然后再通过加密算法。

第三个因素是密钥程度，这是最为人所知的一个方面，根据加密和解密的应用程序，密钥的长度是由”位”为单位，在密钥的长度上加上一位则相当于把可能的密钥的总数乘以二倍，简单的说构成一个任意给定长度的密钥的位的可能组合的个数可以被表示为 2 的 n 次方，这几的 n 是一个密钥长度， 因此，一个 40 位密钥长度的配方将是 2 的 40 次方或 1099511627776 种可能的不同的钥，与之形成鲜明对比的是现代计算机的速度。

尽管可能加密的密钥的总数是非常大的，专门的计算机现在可以在不到一天时间内试验许多种密钥的组合，在一九三三年，Michael wiener 研制出一种专门的计算机，专门破译 DES(一种使用 56 一位密钥的算法)。在研制的过程中他发现设计所需要的费用是呈直线则的，考虑到他的结果和 Moore 的法则的因子(此法则指出计算力大约每 18 个月增长一倍)。其实任何密码都能破解而无论它的长度，想像一下这样的密钥和用现代的机器去破解是多么的快速。简单的说，一个人或组织在密钥破解的装备上花的钱越多，则密钥就会被越快的破解，这种断言最近已经得到证实。ElectronicFrontierFoundation 建造的专门的计算机最近在不到三天的时间内破泽了一个 64 位基础的密码。

尽管有相对的缺点，美国政府把使用超过 40 位的密钥的加密规为强加密，这种加密出口相关的法律已经获得通过。美国国内公司想要出口使用强加密的产品，首先要获得美国国务院的许可。例如，PrettyGoodPrivacy(PGP)加密工具的国际版本，虽然这些法律可能会变得日益宽松，但是一些公司和组织将毫无疑问继续遵守它。尽管公司和政府用现代化的计算机可以击败 40 位的加密,但是耗费的成本超过了信息本身的价值。事实』上，决定需要密钥的长度的一个因素是被保护信息的价值。尽管 40 位的密钥对于金融交易来说并不总是合适的，但对于个人用户的需要已经足够了。目前美国出口法对于 40 位密钥长度的限制已取消。

建立信任关系

应用加密指的是在主机之间建立一个信任关系。在最基本的级别上，一个信任关系包括一方加密的信息并只有另一方的合作伙伴可以解密这个文件。这种任务是和用公钥加密来完成的。这种类别的加密要求你建立一个私钥和一个公钥。一旦你已经产生了一对密钥，你可以把公钥发布给任何人。

你可以通过以下两种方法来发布你的公钥：

- 手动：你首先必须和接收方交换公钥，然后用接收方的公钥来加密信息。PGP 和 S／MIME 需要使用这种方法。
- 自动：SSL 和 IPSec 通过一系列的握手可以安全地交换信息(包括私钥)，在本课你将学到有关这方面更多的知识。

下面是在加密中一些术语的简单介绍：

Rounds，Parallelization 和强度加密

Round 是在加密过程中一个离散部分。通常一种算法要经过很多“ 圈 ”的运算。大多的对称加密算法的 rounds 首先对未加密数据的一半进行运算，然后再对另一半处理。然后每一半加密后的数据再重新运算以达到更复杂的结果。对信息分开进行加密使对称加密更快速。有关加密中的 parallelization 是指使用多进程，多处理器或多台机器来破解一种加密算法。你可以通过访问 http：／／www,rsalabs．com／rsalabs／challenges 来学到有关公钥挑战加密机制的更多内容。

强壮的加密是使用一些超过 128 位长度的密钥来实施的。较新的技术可能需要对强壮加密来作新的定义。在 2000 年 1 月，美国政府发布了有关允许出口什么样的强壮加密的产品，这次发布要求所有的新产品在出口前都要经历一次技术检查揭示。美国政府这么做的目的是要跟踪所有使用加密的政时和用户。

对称加密

在对称加密或叫单密钥加密中，只有一个密钥用来加密和解密信息。尽管单密钥加密的一个简单的过程，但是双方都必须完全的相信对方，并都持有这个密钥的备份。但要达到这种信任的级别并不是想像中的那么简单。当双方试图建立信任关系时可能一个安全破坏，已经发生了。首先密钥的传输就是一个重要问题，如果它被截取，那么这个密钥以及相关的重要信息就没有什么安全可言了。

一个有关对称密钥加密的例子如你用来防问你的 ATM 机所使用的密码或登陆到你的的 ISP 密码。对称加密的好处就是快速并且强壮。这种特点允许你加密大量的信息而只需要几秒钟。对称加密的缺点是有关密钥的传播，所有的接收者和查看者都必须持有相同的密钥，因此所有的用户必须寻求一种安全的方法来发送和接收密钥。

但是，如果用户要在公共介质上如互联网来传递信息，他需要一下中方法来传递密钥，当然如果物理的发送和接收密钥是最安全的，但有时这是不可能的。一种解决方法就是通过电子邮件来发送，但这样的信息很容易的被截取到，从而击破了加密的日的。用户不能加密包含密钥的邮件,因为他们必须共享另一个用来加密含有密钥邮件的密钥。这种困境就产生了问题：如果对称密钥用它们自己来加密，那为什么不直接用相同的方法在第一步就使用?一个解决方案就是用非对称加密，我们将在本课的后面提到。

所有类型加密的一个主题就是破解。一种减少使用对称加密所造成的威胁的反措施就是改变密钥的规律性。然而，定期改变密钥经常是困难的，由其是你的公司里有很多用户。另外，黑客可以使用字典程序，password sniffing 来危及对称密钥的安全，或者通过搜翻办公桌，钱包以及公文包。对称加密也很容易被暴力攻击的手段击败。

对称加密算法

有很多特殊的数学算法来实现对称加密。这些算法包括数据加密标准(DES),TRIPLE，DES,RSA 算法的 RC2,RC4,RC5,RC6：MARS，Twofish，以及 Serpent。

数据加密标准

美国的国家技术标准局(NIST)在 1977 年小式地采用了 DES。你可以在 http：／／www,nist. gov 了解更多有关 NIST 的内容。DES 和 TripleDES 已经成为许多公司和组织加密的标准。 在美国联邦执行标准(FIPS)PUB 46-l 中有详细介绍
FIPS 文献是由 NIST 开发的公共标准。Cipher-Block Chaining(CBC)是数据加密标准的一种模式，升在 FIPSPUB 81 里有详细描述 http：／／www,nist. gov／itl／div897／pubs／fip81. htm。美国国家安全机构(NSA)和国家技术标准局(NIST)来维护这些系统。

DES 是一种 block 密文意思是把数据加密成海 64 他的 block。使用相同的密钥来加密和解密。这种标准使用一种叫做“ diffusion and confusion ”的技术。每 64 位的数据义被分成两半，并利用密钥对每一半进行运算(称做一次 round)。DES 行 16 个 rounds，并且对于每个 round 运算所使用密钥的位数是不同的。

DES 的优点是快速并易于实施。DES 已经提出使用了超过 25 年，因此很多硬件和软件都使用 DES 算法。但是，密钥的传播和管理非常困难，因为 DES 依赖于单密钥模式。

TripleDES

普通 DES 使用 56 位长度的密钥，并且被认为应用一般信息上已经足够了。对于一些更敏感的信息，一些用户使用一种叫 triple DES 的技术。这种情况下是，信息首先被使用 56 位的密钥加密，然后用另一个 56 位的密钥译码，最后再用原始的 56 位密钥加密，

这样 TripleDES 使用了有效的 128 位长度的密钥。在／L 种加密的级别中，Triple DES 经常能防止 man-in-the-middle 攻击。普通的 DES 加密速度很快，并且 Triple DES 也要比其它的对称算法速度快。Triple DES 最大的优点就是可以使用已存在的软件和硬件。在 DES 加密算法上已做出大量投资的公司可以轻松的实施 TripleDES。

对称算法由 RSA 安全公司创立

RonRivest，AdiShamir，和 LeonardAdleman 在 1977 年发明了他们的公钥加密系统，并且以他们名字中的第一个字母命名。到现在，他们已经发明了／L 种不同的算法。RSA 算法可用于几种商业的操作系统和程序中，包括 WindowsNT 和 NetscapeNavigator。

RSA 安全公司(www. rsa. com)在加密的领域中广为人知并有卓越的成效。RSA 的技术包括在互联网上利 WWW 上已存在和建议的标准。RSA 的 WEB 站点(http：／／www,rsa. com)含有有关加密和安全技术的一些实用信息。

在商业应用程序中 RC2 利 RC4 是最常用的对称密钥算法。它们使用可变长度的密钥美国最多支持到 128 位。在国际上，RC2 利 RC4 从美国出口密钥限制到 40 位。

RC2 和 RC5

RC2 是由 Ron Rivest 开发的，它是一种 block 模式的密文，就是把信息加密成 64 位的数据。因为它可以使用不同长度的密钥，它的密钥长度可以从零到无限大，并且加密的速度依靠密钥的大小。

RC5 类似于 RC2,也是 block 密文,但是这种算法采用不同的 block 大小和密钥大小。还有住算法中数据所通过的 round 也是不同的。一般建议使用 128 位密钥的 RC5 算法并有 12 到 16 个 rounds。

RC4

是由 Rivest 在 1987 年开发的，是一种流式的密文，就是实时的把信息加密成一个整体。密钥的长度也是可变的：在美国一般密钥长度是 128 位，向外出口时限制到 40 位，因为受到美国出口法的限制。LotusNotes，OracleSecuresQL，CDPD 都使用 RC4 的算法。

RC6

不像其它一些较新的加密算法，RC6 包括整个算法的家族。RC6 系列在 1998 年被提出在 RC5 算法提 Ui 后,经调查发现其在对特殊的 round 上加密时存在于一个理论上的漏洞。RC6 的设计弥补了这种漏洞。

Blowfish and，rwolish

Blowfish 是由 BruceSchneier 开发的一种非常灵活的对称算法，并且在个人的加密领域里是非常有名的并作出了很大的贡献。它使用不同的 round 密文，并且密钥的长度最大可支持到 448 位。

Schneier 现在已创建了一种较新的算法叫 Twofish。这种算法使用 128 位的 block 并且速度要比 Blowfish 快得多。Twofish 支持 28 位，192，和 256 位的密钥。是一种有前途的加密算法并可用于智能卡上。

Skiack and MARS

Skiack 是由美国国家安全机构设计的一种加密程序。MARS 是由 IBM 提出的一种算

法，并且速度要比 DES 还要快，和 Twofish 一样，它主要也要面向工作在智能卡上而没计的。

高级加密标准

一些专家认为 DES 和 TripleDES 不足以满足宣全的需求。在 1997 年 1 月，美国国家技术标准局(NIST)开始对 DES 展开调查的过程。到写这本书的时候，NIST 已经进行了第三轮评估。为了满足其它一些需求，对称加密选择了 AES 必须能建立 128，192，和 256 位长度的密钥，并可支持不同的平台。

非对称加密

非对称加密在加密的过程中使用一对密钥,而不像对称加密只使用一个单独的密钥。一对密钥中一个用于加密，另一个用来解密。如用 A 加密，则用 B 解密，如果用 B 加密，则要用 A 解密。

重要的概念是在这对密钥中一个密钥用来公用，另一个作为私有的密钥：用来向外公布的叫做公钥，另一半需要安全保护的是私钥。非对称加密的一个缺点就是加密的速度非常慢，因为需要强烈的数学运算程序。如果一个用户需要使用非对称加密，那么即使比较少量的信息可以也要花上小时的时间。

非对称加密的另一个名字叫公钥加密。麻省里上学院的数学家们在 1970 年首先开发了非对称密钥(公钥)技术。尽管私钥和公钥都有与数学相关的，但从公钥中确定私钥的值是非常困难的并且也是非常耗时的。在互联网上通信，非对称加密的密钥管理是容易的因为公钥可以任易的传播，私钥必须在用户手中小心保护。

非对称密钥加密元素

三种最常见的非对称密钥加密是 RSA，the Digital Signature Algorithm(DSA)，Diffie-Hellman。DSA 是美国国家技术标准局研发的技术，并且已广为使用。尽管它的功能不同于 RSA，但它并不是一项专利，并且成为 Linux 下公钥加密方法的标准。Diffie-Hellman 是一种安全交换密钥的协议，因此可以看做密钥交换协议。它是一种开放式标准并在安全通信中广泛使用，主要有一点作了改动： 因为 Diffie-Hellman 密钥交换协议的方法易受 mad · in-the · middle 这类攻击，所以 Station-to-station(STS)协议改变了 Diffie · Hellman 协议包括采取相应的认证。

HASH 加密

HASH 加密把一些不同长度的信息转化成杂乱的 128 位的编码里,叫做 HASH 值。HASH 加密用于不想对信息解密或读取。使用这种方法解密在理论上是不可能门，是通过比较两上实体的值是否一样而不用告之其它信息。HASH 加密别一种用途是签名文件。它还可用于当你想让别人检查但不能复制信息的时候。

举个例子，一台自动取款机(ATM)不需要解密一个消费者的个人标识数字(PIN)磁条卡将项客的代码单向地加密成一段 HASH 值，一旦插下时，ATM 机将计算用户 PIN 的 HASH 值并产生一个结果，然后再将这段结果与用户卡上的 HASH 值比较。使用这种方法，PIN 是安全的，即使对于那些维护 ATM 机的人来说。

签名

信息鉴别的方法可以使信息接收者确定：信息发送者的身份以及信息正传送过程中是否被改动过。如果信息的收发双方对该信息的内容及发送端没有争执的话，那么只采用鉴别技术也就足够了。鉴别技术可以保证在信息传送过程中对信息内容的任何改动都可以被检测出来，并且能够正确的鉴别出信息发送方的身份。但是，当信息的收发方对信息的内容及发送端产生争执时，只用鉴别技术就不够了。

收方可以伪造一份信息，从中获得非法和益，并且自称该信息是由发送方发过来的。例如，银行通过通信网络传送一张支票，收方就可以对支票数额进行改动，并且声称他已收到了这张支票。和用前面的鉴别技术丝毫也解决不了这个问题，因为鉴别使用了一个收／发双方共享的秘密密钥，这样才能是发放产生一个鉴别码而接收方又能对该鉴别码进行校验。但是收方也能对他伪造的信息产生一个合法的鉴别码，这给整个系统带来严重的安全问题。

在许多情况下，特别是商业系统中，通常都和用书面文件，来规定契约性的责任，虽然鉴别技术可以完全有效的防止第三者的介入,但是却丝毫不能防上下接收者的伪造。问题的另一方面是发送方可能是不诚实的，由于他发送的信息变得对他很不和，而要逃避责任，那么发送方就可能谎称他从未发过这个信息。在按个争执过程中，第二方也无法分辨那种情况是真实的。

为了解决上述问题，就必须和用另外一种安全技术—-一数字签名。签名必须达到如下效果：在信息通信的过程中，接收方能够对公正的第二方(可以是以方事前统一委托其解决某一问题或某一争执的仲裁者)证明其收到的报文内容是真是的,而且确实是由那个发送方发过来的，同事签名还必须保证发送方式后不；能根据自己的和茄否认他所发送过的报文，而收方也不能根据自己的利益来伪造报文或签名。

对于数字签名的产生过程来说，必须有足够的信息才能对报文和签名进行验证，没有足够的信息就会给伪造或否认报文提供可乘之机．但是收发双方用来产生与校验的签名的信息不能完全相同,因为一旦接收方能够用发送方用来产生签名的相同信息(算法和参数)来证实报文和签名，那么收方同样也能够用它来伪造报文和签名．所以签名产生者与签名证实者之间的相同信息绝对不能太多，如果发送方事后担心接收方否认接收到了他所发送的报文，那么发送方应能够请求获得报文证明，也就是说由接收方对发送方提供收到报文的证据，例如，如果甲方把报文发送给乙方，那么乙方就要向甲方发送一份签了名的报文证明收到了，由于这份报文有乙方的签名，所以，乙方是不能抵赖他所收到的报文的．

随着信息经济和知识经济的迅猛发展，无纸办公彻底改变了过去手下操作的各种不便，显得更安全、更有效、更迅速、更简沾、更方便。数字签名以其独特的优势适应了这种发展，在无纸办公中占有十分重要的地位。例如，对公司内部有下级呈给上级请求批阅的公文在以往只需领导大笔一挥签名盖章，以个人的笔迹来证明其真实性。但手写的文件签名非常容易伪造．除此之外，签名者还可以否认签名，宣称它是伪造的．但在无纸办公年代,计算机网络中传送的电子公文义如何盖章呢?又如何来证明签名的真实性呢?这就是--一数字签名．

数字签名的功能：

- 接收者能够核实发送这对报文的签名
- 发送这事后不能抵赖对报文的签名
- 任何人不能伪造对报文的签名．
- 保证数据的完整性，防止截获者在文件中加入其他信息
- 对数据和信息的来源进行保证，以保证发件人的身份．

- 数字签名有一定的处理速度，能够满足所有的应用需求

HASH 算法

HASH 加密使用复杂的数字算法来实现有效的加密。以下是目前使用的几种标准算法

MD2，MD4，和 MD5

MD2,MD4 和 MD5 是一组基于单向 HASH 功能的算法。这些操作采用一定长度的字节流并产生一个唯一的指纹。这种过程是单向的因为你不可能通过从返同的签名中而产生一一些信息，而且指纹是唯一的因为没有两条信息会有相同的 HASH 值。这些操作可以使用信息摘要算法对 e-mail 信息,证书和其它一些想保证内容完格性的项目产生唯一的单向指纹。通常信息摘要是 128 位长度的。

RonRivest 还开发了信息摘要算术 2(MD2)。MD4 和 MD5 要比 MD2 更快并广为使用。MD4 容易遭到攻击，到少最后几圈的加密曾被成功地攻破过。Rivest 又开发了 MD5，要比 MD4 更强壮开仍使用 128 位的 HASH。

安全 HASH 算法(SHA)

安全 HASH 算法是另一种 HASH 功能的应用。还有著名的安全 HASH 标准(SHS)是由 NIST 和 NSA 开发的并用于美国政府。它可以从任意的长度的字串摘取 160 位的 HASH 值。SHA 在结构上类似于 MD4 和 MD5。尽管它比 MD5 的速度要慢 25%，但它更加安全。它产生的信息摘要比 MD5 要长 25%，因此对于攻击来说是更安全的。

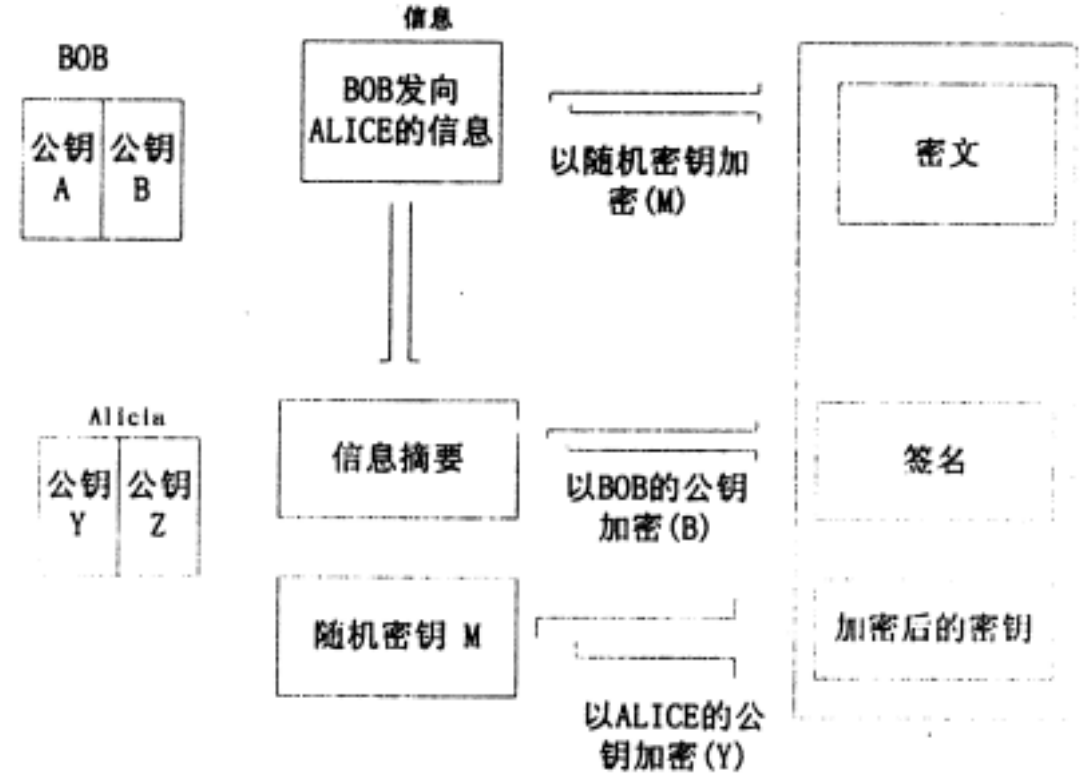
应用加密的执行过程

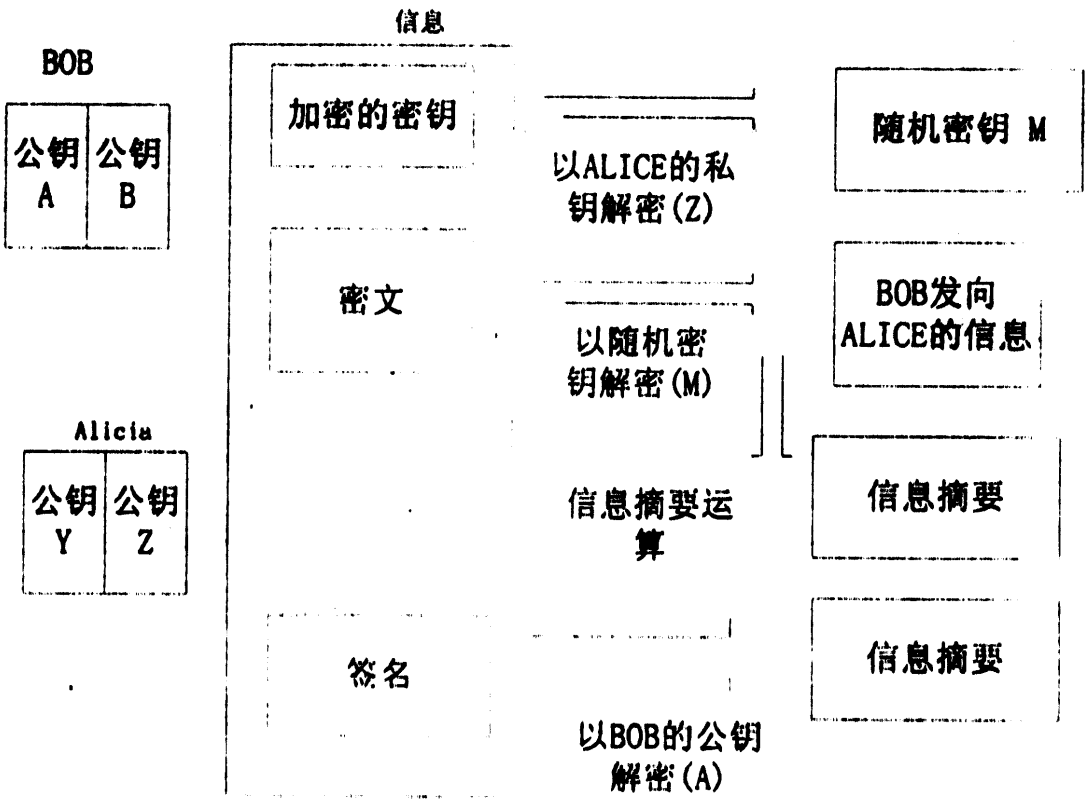
加密的手段可广泛的应用于不同的应用程序中，从 email 客户端到 WEB 服务器到实际的网络当中，如虚拟专用网络(VPN)。很多流行的加密都是综合使用对称，非对称和 HASH 加密的。这种结合的使用增加了每种类型加密的强度，减少了它们的弱点。一些程序像 IIS,PGP，SSL,S-MIME 都结合使用了对称，非对称和 HASH 加密。

电子邮件(E—mail)

E-mail 是很明显的需要加密的程序，由其现在商业用户已经离不开它。用于加密 e-mail 的流行方法就是使用 PGP 或 S-MIME。虽然加密的标准不同，但它们的原则都是一样的。然而，尽管多数加密程序使用不同的对称，非对称，和单向加密以及改变它们对数据加密的顺序，整个过程是相同的。

下面是发送和接收 E-mail 中加密的全部过程，如下面两幅图所示





1. 发送方和接收方在发送 Email 信息之前要得到对方的公钥。
2. 发送方产生一个随机的会话密钥，用于加密 email 信息和附件的。这个密钥是根据

时间的不同以及文件的大小和日期而随机产生的。算法通过使用 DES，TripleDES，Blowfish，RC5 等等。

3. 发送者然后把这个会话密钥和信息进行一次单向加密得到一个 HASH 值。这个值用来保证数据的完整性因为它在传输的过程中不会被改变。在这步通常使用 MD2，MD4，MD5 或 SHAl。MD5 用于 SSL，而 S-MIME 默认使用 SHAl。
4. 发送者用白己的私钥对这个 HASH 值加密。通过使用发送者白己的私钥加密，接收者可以确定信息确实是从这个发送者发过来的。加密后的 HASH 值我们称做信息摘要。
5. 发送者然后用在第二步产生的会话密钥对 e-mail 信息和所有的附件加密。这种加密提供了数据的保密性。
6. 发送者用接收者的公钥对这个会话密钥加密，来确保信息只能被接收者用其自己的私钥解密。这步提供了认证。
7. 然后把加密后的信息和数字摘要发送给接收方。解密的过程正好以相反的顺序执行。

以下部分是使用上述方法来实施特殊的 e-mail 加密的实现。

PrettyGoodPrivacy(PGP)

针对电子邮件和文本文件可能最流行的高技术加密程序就是 PGP,PGP 足成功的出为采用对称加密和非对称加密技术以及 HASH 加密的优点。你可以通过 http：／／www,pgp. Com 来访问 PGP 的主页。

SecureMIME(S-MIME)

这是一个公共的，工业标准方法，特别是应用到 Netscape Communicator's Messenger E-mail 程序上。s—MIME，与 PGP 相比使用有点不同的算法，密钥格式以及密钥服务器。然而它们的原则是——样的就是用确切的步骤来进行加密，解密和签名信息。

加密文件

除了加密 e-mail 信息，你还可以加密整个硬盘的任何部分，为文件创建校验和，建立隐藏加密的驱动器。对于 Windows 平台来说 BestCrypt(www. jetico. corn)是一个很不错的选择。

其它——些流行的用于实施加密文件的产品包括

BlowfishAdvancedCS(hOme。knuut。de／mchahn／sOftware。html。)

Locker(www. 10cker4u. com)

EasyCrypt(www. easycrypt. co. uk)

MD5sum

MD5sum 可以应用到 Windows NT 或 Liunx 上。Linux一下的 md5sum 实用程序可对一个单独的文件建立固定长度的校验和，这个文件可以是任意大小，但是校验和总是保持 128 位的长度。这种校验和是非常有用的，因为它检查一个文档是否被损害。

Web 服务器加密

目前对于加密 WEB 服务器有两种可接受的模式,它们是安全超文本传输协议(Secure HTTP)和安全套接字层(SSL)。这两种协议都允许白发的进行商业交易，因为从 90 代中期互联网上的商务迅猛增长。SecureHTTP 和 SSL 都使用对称加密，非对称加密和单向加密，并使用单向加密的方法对所有的数据包签名。

SecureHTTP

SecureHTTP 使用非对称加密保护在线传输，但同时这个传输是使用对称密钥加密的。大多的浏览器都支持这个协议，包括 NetscapeNavigator 和微软的 InternetExplorer。

安全套接字层(SSL)

SSL 协议允许应用程序在公网上秘密的交换数据，因此防止了窃听，破坏和信息伪造。SSL3．0 是由互联网工程任务组(1ETF)规定的。SSL 允许两个应用程序通过使用数字证书认证后在网络中进行通信。它还使用加密及信息摘要来保证数据的可靠性。SSL 是整附在传输层协议(通常是 TCP／IP 层)之上的。所有的浏览器都支持 SSL，所以应用程序在使用它时不需要特殊的代码。SSL2．0 最早是由 Netscape 公司发明的并在 1995 年成为一项标准，SSL3．0 定义于 1996 年是当前的标准并且所有浏览器都支持它。

在某方面，SSL 可能比其它方法更加安全因为根据开放式系统互联(OSl)模式，它加密的过程是发生在网络的较低层。与 SecureHTTP 相比 SSL 可加密更多的内容，因为 Secure HTTP 只能加密 HTTP 流量，而 SSL 可加密所有的数据包。

网络级协议

仅考虑在文件级别上进行加密是不够的。文件级加密中介在互联网上如何使用加密的方面。网络级协议和算法在网络层上建立一个安全通道，提供私有性，完整性和认证。

虚拟专用网络(VPN)协议

VPN 指的是在公用网络上建立专用网络的技术。之所以称为虚拟网主要是因为整个 VPN 网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台(如 INTERNET，ATM，FRAMERELAY 等)之上的逻辑网络，用户数据在逻辑链路中传输，VPN 具有虚拟的特点：VPN 并不是某个公司专有的封闭线路或者是租用某个网络服务商提供的封闭线路，但同时 VPN 又具有专线的数据传输功能，因为 VPN 能够像专线一样在公共网络上处理自己公司的信息。VPN 可以说是一种网络外包，企业不再追求拥有白己的专有网络，而是将对另外一个公司的访问任务部分或全部外包给一个专业公司去做，这类专业公司的典别代表是电信企业。

VPN 具有以下优点：

(1) 降低成本：企业不必租用长途专线建设专网，不必大量的网络维护人员和设备投资。

(2) 容易扩展：网络路由设备配置简单，无需增加太多的设备，省时省钱。

(3) 完全控制主动权：VPN 上的设施和服务完全掌握在企业手中。比方说，企业可以把拨号访问交给 NSP 去做，由自己负责用户的查验、访问权、网络地址、安全性和网络变化管理等重要工作。VPN 通过采用 ”隧道 ” 技术，并在 Internet 或国际互联网工程工作组(1ETF)制定的 lpsec 标准统一下，在公众网中形成企业的安全、机密、顺畅的专用链路。常见的 VPN 协议有 PPTP 和 IPSec。

PPTP 与 IPSec 在安全性上的比较

PPTP 是由 Microsoft 和 US Robotics 率先推出的。PPTP 在推出之初的目的是用于拨号 VPN，这种协议通过使用户拨号进入本地 ISP 并利用隧道技术按入到企业网络中，增

加了远程接入的可用性。与 IPSec 不同，在 PPTP 用用制定时，其目的并不足用于处理 LAN 到 LAN 隧道的。

PPTP 是 PPP 协议的扩展，后者是一种定义 IP 网络上点到点按入的协议。PPP 被广泛地应用于将拨号用户和宽带用户连接到公共 Internet 或专用企业网络。由于 PPP 在第二层上发挥作用，因此，将 PPP 包封装起来的 PPTP 连接使用户可以发送 IP 之外的数据包，比如 IPX 或 NetBEUI 数据包。另一方面，IPSec 在第三层运行，只能提供 IP 包的隧道传输。

PPTP 中常用加密方式是在 PPP 层定义的。一般来说，PPTP 客户机是 Microsoft 桌面系统，它所使用的加密协议为 MiCROSOFT 点到点加密方案(MPPE)。MPPE 是基于 RSA RC4 标准的，它支持 40 位或 128 位加密算法。虽然这种加密强度可以满足许多应用的需要，但是人们通常认为它不如 IPSec 提供的一些加密算法安全，尤其不能与 IPSec 中的 168 位三重数据加密标准(DES)相比。

保护与服务

与此同时，IPSec 在设计上是为了在受保护的 LAN 之间的 Intemet 上建立一条安全隧道。它用于与远程办公室、其它 LAN 或企业供应商建立连接。例如，大型汽车公司可以使用 IPSec VPN 来安全地通过 Internet 将其供应商连接起来，对 Intemet 上采购订货提供支持。IPSec 还支持远程用户与企业网络之间的连接。同样，Microsoft 在 WindowsNTServer4. 0 的 Routing and AccessServer 中增加了对 PPTP 的 LAN 到 LAN 隧道技术的支持。

从加密强度和数据集成方面来说，IPSec 一般被认为要优于 PPTP。该协议将密钥管理与对 X. 509 认证、信息集成和内容安全性的支持结合在一起。另外，IPSec 中提供的最强密度的 168 位三重 DES 加密算法比 128 位 RC4 加密算法更安全。IPSec 还提供了逐包加密与验证功能，可以防止“ 中间人攻击 ” (man in middle attack)。第三方在使用这种攻击时，将截获到的数据加以篡改，再发送给接收者。

PPTP 之所以不能抵御这种攻击，主要是由于它只对会话进行验证，而不验证单个包。不过，请注意，要想对 PPTP 连接成功地实施“ 中间人人攻击 ”需要进行大量的工作，并需要掌握一定的技术。

对许多企业来说，从 Windows 平台(PPTP 支持们 ndows NT、95 和 98)运行 PPTP 的能力可以使部署和维护 VPN 无缝地进行。而另一些企业则认为 PPTP 不如 IPSec 安全。然而，应当牢记，如果为远程用户部署 VPN 的话，IPSec 需要使用部门在每个桌面系统上加载特殊的客户软件。客户软件的部署和维护是很繁重的任务，必须慎重考虑。从简单性的角度看，PPTP 在部署上非常容易。

公钥体系结构(PKl)

PKI 服务器用来负责管理公钥，证书和签名。为了认证持有者的一对密钥的身份，PKI 还提供撤销密钥的功能如果密钥不再合法。例如，如果一个私钥已被破解或被公布那么它将被宣告无效。PKI 的主要目的是尽快的允许产生证书和撤消它。

PKI 标准

PKI 是基于 X. 509 之上的，是证书格式的标准并提供它们如何被访问。为 PKI 面设计的新的标准已开发出来，在本书出版时，最后的 RFC 文件包括

- RFC2510：说明 PKI 使用的术语和协议

- RFC 2560：提供有磁在线证书状态协议(OCSP)的内容
- RFC 2585：描述 PKI 使用的协议和体系结构
- RFC 2587：说明 LDAP2 是如何用于 PKI 服务器中的
- RFC 2527：解释 PKI 使用目的的信息文档

PKI 术语

- Certificateauthority(CA)：负责发布证书的一组机构。一个 CA 可以把真正的认证委托到一个注册的认证机构(RA)。
- CA certificate：用于在 Internet、Extranet 和 Intranet 上进行身份验证并确保数据交换的安全。公钥证书是以数字方式签名的声明，它将公钥的值与持有相应私钥的主体(个人、设备和服务)的身份绑定在一起。通过在证书上签名，CA 可以核实与证书上公钥相应的私钥为证书所指定的主体所拥有。
- End entity：在主题里列出的终端用户或个人
- Certificate policy statement：CA 根据也已确立的一套标准向申请人颁发证书。CA 在受理证书请求(以及颁发证书、吊销证·书和发布 CRL)时所采用的一套标准被称为 CA 策略。通常，CA 以一种叫做证书惯例声明(Certification Practice Statement，CPS)的文档发布其策略。
- Repository：传播到网络下允许访问证书的一系列东西

本章小结：

下表显示了安全所需考虑的事项，通过本课的学习我们可以在 NT 及 LINUX 下实现 Email 及数据的加密从而达到网络安全的目的，本章 VPN 的原理和实施也是重点

术语	功能
加密	打乱和恢复网络上的数据。防止非授权的欺骗并保证数据的可靠
认证	建立参与者的身份证明，使用认证的规则
密钥	一些单词，短语或文本串来加密和解密信息
对称加密	一种使用一个密钥的加密方法
非对称加密	使用一对密钥加密的方法。用其中一个加密，另一个用来解密
HASH 和签名	使用单向散列算法生成一段 HASH 值以确保唯一性
证书	数字 ID 用一证实参与者的身份。经常也是一段 HASH 代码
防火墙	控制网络进出数据包的系统，网络加密经常发生在这一层

翻

问题讨论：

√ 加密的种类及原理，它们各自的优点和缺点?

√ VPN 原理及实施

√ 证书服务器和 SSL 原理及相关配置
√ 熟练掌握 PGP 和 GPG 的应用

第四章

典型的攻击方式及安全规则

引言

为了进一步讨论安全，你必须理解你有可能遭遇到的攻击的类型，为了进一步防御黑客，你还要了解黑客所采用的技术、工具及程序，所有类型的攻击经常被合在一起使用，一般情况下，攻击被结合起来产生一个具体的后果，例如：一个用户有可能将特洛伊木马程序放置在 WEB 服务器，因为服务器一执行这个程序，黑客将能在服务器上实施拒绝服务攻击，导致机器重启，一旦机器重启，它将载入木马程序。

本章要点：

- 描述典型的安全攻击类型
- 创建一个有效的特殊的解决方案
- 描述有效网络安全通用的方针和规则

前门攻击和暴力攻击

前门和暴力攻击它们都试图击败前面讨论的认证过程。在一个前门攻击中一个黑客伪装成一个合法的用户进入系统，因为一个黑客拥有一个合法用户的所有信息，他(她)就能够很简单地从系统的“前门”正当地进入。

暴力攻击类似于前门攻击，因为一个黑客试图通过作过一个合法用户获得通过。两者的区别是在暴力攻击中一个黑客使用所有的他认为能够击败认证利获得一个合法用户密码的字母、单词、字符。一个暴力攻击是一个并不精密复杂的企图尝试每一样东西包括字典文件，嗅探器和重复的登陆企图。暴力攻击的一个具体例子是，一个黑客试图使用计算机和信息的结合去破解一个密码。在一种情况下一个黑客需要破解一段单一的被用 RC4 算法和非对称密钥加密的信息，为了破解这种算法，一个黑客需要求助于非常精密复杂的方法，它使用 120 个工作站，两个超级计算机利从三个主要的研究中心获得的信息，即使拥有这种配备，它也将花掉八天的时间去破解加密算法，实际上破解加密过程八天已是非常短暂的时间了。 ’

针对一个安全系统进行的暴力攻击需要人量的时间，并且经常是极大的意志力和决心的结果。然而，一些系统非常易于暴露于这种攻击之下，主要因为不适宜的安全设置和策略，暴力攻击经常容易被侦测到，因为它经常使用重复的登陆企图。

字典程序攻击

字典攻击是常见的一种暴力攻击。如果一个潜在的黑客试图通过使用传统的暴力攻击的方法去获得密码的话，他(她)将不得不尝试每种可能的字符，包括大小写，数字，通配符。一个字典攻击通过仅仅使用某种具体的密码来缩小尝试的范围，大多数的用户使用标准单词作为一个密码，一个字典攻击试图通过利用包含单词例表的文件去破解密码。强壮的密码通过结合大小写字母、数字、通配符来击败字典攻击。黑客经常使用程序，例如 For

Unix 版本的 iohntheripper 或 Novell PassCrack 去获得非法通过。这样的攻击就是一种暴力攻击，经常被用来针对网络。然而，黑客也在别的方面上使用字典程序，如一个字典程序能够使得黑客利用多台机器来破解一个 ZIP 文件的密码。

BUG 和后门

一个 BUG 是一个程序中的错误，它产生一个不注意的通道。很多情况下一个运行在服务器的操作系统或程序包含了这些问题，黑客经常了解这些问题并充分利用它们。一个后门是一个在操作系统上或程序上未被记录的通道。程序设计员有时有意识地在操作系统或程序上设置后门以便他们迅速地对产品进行支持，在这种情形下，大多数的后门并不是怀有恶意的。然而，一些系统管理员并没有意识到他们的操作系统中有后门，但是黑客却意识到了。因此，那些本来被用来作为对系统进行迅速支持的后门却变成一个黑客攻击的手段。

缓冲区溢出

目前最流行的一种 BUG 类攻击就是缓冲区溢出。当目标操作系统收到了超过它设计时在某一时间所能接收到的信息量时发生缓冲区溢山。这种多余的数据将使程序的缓存溢出，然后覆盖了实际的程序数据，缓冲区溢出使得目标系统的程序自发的和远程的被修改，经常这种修改的结果是在系统上产生了一个后门，尽管这项攻击的技术要求非常高，但是一旦执行这项攻击的程序被设计出来却是非常简单的，这种简单性对安全专家提山了一个严峻的挑战。

ROOT KITS

Root KIT 是多种 UNIX 系统的一个后门，它在控制阶段被引入，并且产生一个严重的问题，Roo KIT 由一系列的程序构成，这些程序用特洛伊木马取代合法的程序，这种取代叫供给黑客再次进入的后门和特别的分析网络工具，例如 sniffer，除此之外这种被修改的工具能够隐藏他们自己的存在和他们的活动，使得侦察无效。

社交工程和非直接攻击

社交工程是使用计谋和假情报去获得密码和其他敏感信息，研究一个站点的策略其中之一就是尽可能多的了解属于这个组织的个体，因此黑客不断试图寻找更加精妙的方法从他们希望渗透的组织那里获得信息，举个例子：一组高中学生曾经想要进入一个当地的公司的计算机网络，他们拟定了一个表格，调查看上去显得是无害的个人信息，例如所有秘书和行政人员和他们的配偶、孩子的名字，这些从学生转变成的黑客说这种简单的调查是他们社会研究工作的一部分。利用这份表格这些学生能够快速的进入系统，因为网络上的大多数人是使用宠物和他们配偶名字作为密码。另一种社交工程的形式是黑客试图通过混淆一个计算机系统去模拟一个合法用户，或者甚至一个程控机交换员。在某此情形下，一个黑客冒充一个系统经理去打电话给一个公司，在解释了他的帐号被意外锁定了后，他说服公司的某位职员根据他的指示修改了管理员权限，然后黑客所需要做的就是登录那台主机，这时他就拥有了所有管理员权限，一些诱骗人们说出他们的信用卡帐号的诈骗高手经常从事社交工程，这些人使受害者糊里糊涂就泄露了一些敏感信息。这种社交工程的典型目标包括每一个能够获得关于系统信息的人包括秘书，门卫，管理员，甚至安全专家。

打电话请求密码

尽管不像前面讨论的策略那样聪明，简单的打电话寻问密码也经常奏效。在社交工程中那些黑客冒充失去密码的合法雇员，经常通过这种简单的方法重新获得密码。

伪造 Email

使用 telnet 一个黑客可以截取任何一个身份证，发送 Email 给一个用户，这样的 Email 消息是真的，因为它发自于一个合法的用户。在这种情形下这些信息显得是绝对的真实，然而它们是假的，因为黑客通过欺骗 Email 服务器来发送它们。它也是一个黑客如何利用一个缺乏有效认证过程的例子。SMTP 服务器天生就是不安全的，很少有公司花费时间利金钱增添认证过程在它们的 Email 服务器，因此黑客很容易获取任何一个他们想要得到的身份证，然后发送任意多的消息。

黑客利用假的 email 来进行社交工程。为了获得密码了其它敏感信息黑客发送那些看上去来自合法用户的 Email，因为用户经常认为任何一个 Einail 必须来自一个合法的用户。一个冒充系统管理员或经理的黑客就能较为轻松的获得大量的信息，黑客就能实施他们的恶意阴谋。

拒绝服务攻击

在一个拒绝服务攻击中，一个黑客阻止合法用户获得服务。这些服务可以是网络连接，或者任何一个系统提供的服务。一个 DOS 攻击能够让一个黑客试图使一个系统或程序如 FTP 服务器负载。还有，一个黑客可以上传大量的信息给 FTP 服务器，使它的硬盘驱动器塞满，这两种行动都可以使一个没有专门防备的服务器瘫痪，在某些涉及 UNIX 系统情况下，FTP 服务器能够崩溃并且使得黑客能够进入作为服务器的驱动器中。硬件、操作系统和程序特别容易受到负载的影响，允许这些任何一种负载的因素就等于允许非法进入整台系统。

DOS 攻击在 WINDOWS NT 服务器上非常流行，击败一个 UNIX 系统的安全防范是容易的，主要因为它是基于一个假设，所有的用户都是善意和有能力的，在拒绝攻击服务有两种目的：

- 摧毁服务器，使它对于任何人都不能服务。
- 获取黑客止在摧毁的任何一个服务器的身份，黑客的策略，例如欺骗和“man-in-the-middle"攻击，必须使得他们正在欺骗的主机失效，拒绝服务攻击并不能使黑客拒绝个人的身份，但是可以使得这个合法的个人不能被响应。

尽管特殊的安全实施是独特的，但所有的网络都几乎有以下 8 个规则

1. 偏执狂
2. 你必须有一个完整的安全策略
3. 不要采取单独的系统或技术
4. 在公司内强制执行
5. 提供培训
6. 根据需要和放置设备
7. 要关注安全商业发布
8. 考虑物理安全

偏执狂

尽管偏执狂这个词看上去好像是夸人的，如果你不是一个爱怀疑的偏执狂，那么你可能不会尽你最大的努力坚持不懈地跟随你的安全策略。在个人用户标准上，如果你一旦连上了互联网，那么你就有可能成为被攻击的目标。在网络标准上，假设你所设计的安全系统

能够被黑客攻破 ;这种假设将促使你尽可能的在多种级别上采取多种技术来保护你的系统。采取后补机制使当一个黑客攻破了一个区域时，其它区或仍然能够牵制黑客的活动，这种安全机制虽然很简单，但它可以保护你的整个网络。

使用适当的安全规则是为了最大程度地减少威胁。例如，如果你使用适当的访问控制，一个黑客盗取了一个合法用户的身份，那么他也只能访问那个合法用户所能访问到的一些资源。定义一个用户的职责和访问权限是最小化威胁的一个关键。

另一种方法来保证安全是隔离你的系统。如果你把你的FTP文件与你的WEB文件分开，那么渗透到 WEB 安全并不能使你的 FTP 安全受到破坏。在后面的课程里将会学到有关这方面更多的知识。

完整的安全策略

一个安全策略是决定安全的一个基本。如果你没有一个有效的安全策略，你真正的实施是不协调的，并为黑客留下的存取点。黑客经常搜索一个站点是否存在“ 薄弱链接 ”以进行渗透。如果发现这些较弱的链接是操作系统的默认值或 BUG，这些问题的存在是由于系统管理员没有按照基本的步骤来升级操作系统，增加用户或安装一个新的程序。一个全面的安全策略能帮你纠正这些易忽略的问题，并使你的网络和安全保持一致性。Securityinfo。com 主页(http：／／www,securityinfo．com)，提供了非常有用的有关安全规则和发布信息。

要搞清每个部门是如何应用安全策略的。防止每个部门自己制定安全策略，或者自行解释安全策略，因而妨碍格体安全策略应用的效果并且开启新的安全汕洞。再强调一下，确保你公司所有人员包括部门经理都要遵守这些策略。

安全利系统管理员应当紧密监视所有的网络组件 ：。一个站点的安全很容易因为某台主机的保护机制很弱而被破坏。在这里假设一种情况：一个站点的安全管理员仔细地对网络资源的安全进行了没置。一个新的操作系统版本很快发布了出来，研发部门的人得到了该产品的测试版本，他们将该产品安装在用于测试的机器上。某个攻击者扫描该网络并希望入侵系统。攻击者发现网络中只有一台主机的安全性很差。他使用了所有的攻击手段对这台主机进行渗透。安全管理员没有想到攻击会从内部网络发起。攻击者可能会在已经入侵的主机—上安装 Packetsniffer 来捕获管理员的密码。如果能强制所有部门都遵循安全协议的话，上面描述的问题是可以轻易预防的。

不要采取单独的系统或技术

一个成功的安全系统是个矩阵，或者是多种手段、技术和子系统的结合。只要可能，你应使用多种安全规则和技术来保护每个资源。例如，一个仅依赖于认证的网络与结合使用认证、访问控制利加密相比几乎是不安全的。同样，保护你的站点最好在路由器上实施包过滤并在防火墙之后实施用户认证和入侵检测。

使用多种手段和技术来弥补每个单独技术的弱点，从而提高整体安全性。作为你公司的安全开发者，你要在这些可选的基础上来平衡你的安全。所谓的平衡是很重要的因为你可以实施多种方法，但未必达到有效的安全目的。最关键的是要对每种保护方法的弱点进行分析并判断使用这些额外的手段是否能减少你的风险。没有一个完整的产品，技术或解决方案可以完全防护所有的威胁。安全威胁发展和增长的很快。你需要向所有的职员提供资源来很好的达到安全的功能。

在每种设备(如路由器或 WEB 服务器)和每个级别(如操作系统或 Intemet 服务器)使用多种技术，你可以限制一个黑客所造成的破坏。举个例子，你可能利用加密的技术来补充防火墙的不足如用 S-MIME 来安全保护 E-mail。

部署公司范围的强制策略

更多的情况下，公司指定了安全策略然而系统管理员却没有强制执行这些策略。系统利安全管理人员赋予日常用尸 root 或 administrator 的访问权限，他们并没有意识到潜在的问题。管理员知道如何避免对系统的意外损坏和其它类型的破坏，但大多数的普通用户并不知道如何避免这些问题。攻击者会尽量定位这些账号，选择破解它们而不是其它更安全的账号。公司的主管人员还试图绕过安全规范，因为这些规范使他们在想尽快访问信息时显得不方便。在小型的公司中，许多所有者都希望有 root 或 administer 的权限因为他们就是“ 老板 ”一条好的管理规则是在系统中尽可能少的有 root 或管理权限的账号。有些人认为即使是最客气安全控制机制也是在浪费他们的时间，他们会忽略这些策略或者绕过它们。这种天真的和看起来必要的行为会开启安全方面的漏洞,攻击者可以发现并利用这些漏洞。因此，一个公司的安全策略应当使每个人都有责任维护公司的整体的安全。

提供培训

培训是最有效利便捷地实施安全规范的方法之一。在整个公司范围内进行一个小时左右的培训，例如如何正确设置密码，可以极大地增强整体的安全等级。

下面是对三种用户级别进行培训的建议。

终端用户：用户必须被告知在互联网上出现了哪些新的病毒。你可以通过公司的电子邮件信息或会议电话通知。有时，你需要对终端用户进行培训，使他们可以正确使用你需要实施的新工具。

管理员：安全管理员必须跟踪最新的威胁和对策。一个好的建议是让每个安全管理人员跟踪一个课题或领域。例如，一个安全管理员跟踪最新的病毒，另一个人跟踪最新的黑客工具和技巧。

经理：经理需要知道用来保证站点安全的最新工具。一个有用的技巧是给他们演示如何成功地闯入相关的站点

根据需要购置设备

希望购买最新的设备和软件的愿望是很容易实现的，然而，你应当根据实际需求来考虑购买下面是一些应该采取的步骤：

- 根据评估审核的需求来决定
- 结合管理来确定特殊的需求
- 确定一个新的技术如何对最终用户产生影响
- 结合管理来节省资金
- 进行调查来确定在你的公司中实施哪些产品

识别安全的商业问题

安全问题迅速成为商业问题，主要是因为花费。投资者和客户对公司是否尽力确保安全问题非常关心。IT 管理者和公司总裁也对证明他们努力加强网络安全非常重视。这样做有助于节省资金和树立公司正面的形象。

在表 5-1 中列山了在管理安全花费和资源时使用的术语

术语	定义

AmOniZatiOn	会计术语，用来确定过时仪器的价格。折旧还包括软硬件的贬值。
CharZebaCk，	精确确定使用各种网络安全服务花费的能力，这些服务可以 包括：1T 专家实施的工作，包括系统安装，网络施工和安全咨询
	使用防火墙，服务器和其它网络资源
Capacity forecasting	预测带宽需求为未来的用户提供服务。
Trends	识别合法利非法用户的流量，你可以建立这些活动的基线。
Performancemanagement	确定现有网络中系统的工作量。

等待是指在客户端和服务器之间处理请求的时间。安全由于需要额外的加密通常会增加网络等待的时间。安全规范还会在以下方面影响商业运作利用户。

- 增加成本：许多安全解决方案需要非常的的成本。一个站点防火墙的授权费用会有 $20,000．00 或更多。
- 不方便：新的程序和手续可能给用户带来不便，尤其是经常出差和在远程工作的用户。记住，要使最终用户意识到虽然在短期内给他们带来一些不便，但从长远角度看，将会节省他们的时间并加强公司的安全。

考虑物理安全

许多公司和组织应用了复杂的安全软件,却因为主机没有加强物理安全而破坏了整体的系统安全。通常情况下，公司会把防火墙利网络置于公共区域，暴露在外意味着危险。其他的考虑对物理安全来说也很重要。

通常，攻击者会通过物理进入你的系统等非 Internet 手段来开启 Internet 的安全漏洞。这种漏洞可能包括：

- 放置防火墙设备的房间开着
- 员工手动删除信息
- 员工泄露密码和其它信息
- 员工偶而给网络带来了病毒，大多数病毒是用户不小心的行为造成的，例如一些不知情的用户从家中带来了被病毒感染的磁盘。

关于物理安全的问题你应当问自己下列问题：

- 公司安装的防火墙是否被锁在房间中
- 网络主机(例如路由器，Web 服务器，FTP 服务器)是否安全并且被监视？
- 是否有员工独自在重要的区域办公?

增强物理安全的方法包括：

- 用密码锁取代普通锁

- 将服务器放到上锁的房间中
- 安装视频监视设备

一些公司采用了先进的方法来增强物理安全，安装了数字相机并且将其配置成某种“ tripwire ”。每当有人从数字相机前经过，该相机就拍下快照，然后通过电子邮件或其它手段将图像传送给管理人员。这项策略对于增强极为重要的设备的物理安全非常有用。

本章小结：

了解黑客常见的几种攻击方式及原理，增强网络安全意识以避免受到社交工程类的攻击：作为安全人员应该遵循的一些规则。

第五章

协议层安全

引　　言

因为有经验的黑客理解如何通过 TCP／IP 协议堆栈开发使用网络，而且他们知道一个数据包是如何建立和路由的，你也需要很清楚的理解这些论点。安全管理员需要有丰富的 TCP／IP 方面的知识有很多原因。要适当地实施防火墙过滤，安全管理员必须对于 TCP／IP 的 IP 层和 TCP／UDP 层有很深的理解。黑客经常使用 TCP／IP 堆栈中一部分区或来破坏网络安全。在本课中，你会学到有关 TCP／IP 每一层的特点。

本章要点：

- 识别在 TCP／IP 堆栈不同层上的潜在的咸胁
- 对于不同资源的级别划分及保护措施

TCP／IP 和网络安全

互联网和 TCP／IP 的经常是同义的。当 Intemet 首先在 1966 年创建时，创始者远没有对安全问题考虑的太多。Intemet 最初建立的时候叫 ARPAnet，最大的困难并不是安全相关问题而是操作问题。创始者非常关心网络的功能，并不在乎黑客是否能攻破网络。因此 Internet 和 TCP／IP 并没有被设计强烈的安全原则。安全机制经常被修改以适应现有的网络和 TCP／IP，下面的很多信息也许应该被重新审查，但是你需要理解协议，这样你才能够最好的保护你的网络。你也将学到黑客如何利用 TCP／IP 的漏洞进入网络。

TCP／IP 协议集和 OSI 参考模型

国际标准化组织(1SO)创建一个七层网络模刑作为网络通信的标准。这个模型被称为开放式系统互联参考模刑(OSl)。如果你是一个网络管理员或安全管理员，你将对 OSi 参考模刑非常熟悉。TCP／IP 堆栈包括四层。为了更好的理解 TCP／IP，请与 OSl 模犁进行比较。

物理层

物理层由传输在线缆上的电子信号组成。用于信号传输的介质的类型定义了物理层。一些介质是光纤，同轴电缆利双绞线。物理层上的安全保护措施不多。如果一个潜在的黑

客可以访问物理介质，如搭线窃听和 sniffer，他(她)将可以复制所有传送的信息。唯一有效的保护是使用加密，流量添充等。所有这些技术，对于黑客来说利用 sniffer 来获得信息都是很难成功的。

网络拓扑

安全管理员必须了解他们保护的网络的所有布局。黑客最常用的攻击和渗透到网络中的一种方法是在公司内部主机上安装一个 packetsniffer。记住物理定义了介质上的电子信号。局域网使用基带传输，任何线缆上传输的数据将可被任何可以物理连接的人得到。理解你的网络布局可以帮助阻止未知的 sniffer 发生。最普通的网络拓扑结构是星型，总线型，环型，和复合型。

网络层

TCP／IP 堆栈的下一层是 Intemet 层或 IP 层。IP 层主要用于寻址和路由。它并不提供任何错误纠正和流控制的方法。IP 层使用较高效的服务来传送数据报文。所有上层通信，如 TCP，UDP，ICMP，IGMP 都被封装到一个 lP 数据报中。TCP 和 UDP 将分别讨论，但是 ICMP 和 IGMP 被认为仅存在 Intemet 层，因此被当做一个单独的 IP 层协议来对待。在网络层应用的协议在主机到主机的通信中起到了帮助作用。绝大多数安全威胁并不来自了 TCP／IP 堆栈的这一层：然而你必须知道使用了什么协议。

Internet 协议(IP)

IP 地址是一个 32 位的地址，可以往 TCP／IP 网络中说明一台主机的唯一性。你需要知道一个 IP 地址是什么以及 IP 包头包含什么。一个 IP 包头的大小为 20 字节。IP 包头中包含一些信息和控制字段，以及 32 位的源 IP 地址和 32 位的目的 IP 地址。这个字段包括一些信息，如 IP 的版本号，长度，服务类型和其它配置。每一个 IP 数据报文都是单独的信息，从一个主机传递到另一个主机。主机把收到的 IP 数据包整理成一个可使用的形式。这种开放式的构造使得 Ip 层很容易成为黑客的目标。

黑客经常利用一种叫做 IP 欺骗的技术，把源 IP 地址替换成一个错误的 IP 地址。接收主机不能判断源 IP 地址是不正确的，并且一上层协议必须执行一些检查来防止这种欺骗。在这层中经常被发现的另外一种策略是利用源路由 IP 数据包，仅仅被用于一个特殊的路径中传输。这种利用被称做源路由。这种数据包被用于击破安全措施例如防火墙。

使用 IP 欺骗的一种攻击很有名的一种是 SmurI ’攻击。　一个 Smurf 攻击向大量的远程主机发送一系列的 ping 请求命令。黑客把源 IP 地址换成想要攻击目标主机的 IP 地址。所有的远程计算机都响应这些 ping 请求，然后对目标地址进行回复而不是回复给攻击者的 IP 地址用。目标 IP 地址将被大量的 ICMP 包淹没而不能有效的工作。Smurf 攻击是一种拒绝服务攻击。

Internet 控制信息协议(ICMP)

Intemetn 控制信息协议(ICMP)在 IP 层检查错误和其它条件。一个 ICMP 信息是对于 IP 包头的扩展并且也包含了几层。一般的 ICMP 信息是非常有用的。例如，当你 ping 一台主机想看它是否运行时，你就正在产生了一条 ICMP 信息。远程主机将用它自己的 ICMP 信息对 ping 请求作出回应。这种过程在多数网络中不成问题。然而，ICMP 信息能够被用于于攻击远程网络或主机。近来的攻击方法包括 Tribal flood Network(TFN)系列的程序利用 ICMP 来消耗带宽来有效地摧毁站点。一个广为人知的 ICMP 攻击涉及到微软的 TCP／IP 堆栈。一黑客从 ping 请求中产生一个特殊的 ICMP 信息包。运行早期 TCP 堆栈版本的任

何计算机都不能很好的处理改变后的 ICMP 请求而导致崩溃。在 WINNUCK 传发了这种信息后，业界把这种攻击称为 WINNUCK 攻击。到今天，微软的站点对于 ping 并不作出响应，因为微软已经过滤了所有的 ICMP 请求。一些公司现在也在他们的防火墙上过滤了 ICMP 流量。

传输层

传输层控制主机间传输的数据流。传输层存在两个协议，传输控制协议(TCP)和用户数据报协议(UDP)。每个协议都将在后面的课程中深入讨论。你应该熟悉传输层的二个特点，这样你就能够充分使用关键的网络安全方法。TCP 和 UDP 提供的服务是不同的必须从一个安全的观点上区别对待。

传输控制协议(TCP)

TCP 是一个面向连接的仂，议：对于两台计算机的通信，它们必须通过握手过程和信息交换。一旦这些步骤完成，一个连接就建立了。TCP 因此保证了可靠的传输。FTP 是一个著名的基于 TCP 之上的协议。一旦一个连接建立并且数据开始传输时，如果有任何部分的信息在些过程中丢失，TCP 将重新传输。TCP 协议用于多数的互联网服务，HTTP，FTP 及 SMTP。

TCP 握手

当一个连接建立的时候，理解和保护你网络中使用的 TCP 流量的关键是要理解 TCP 握手的过程。你应该不断地检查 TCP 握手，因为它经常被黑客操纵。

TCP 包头

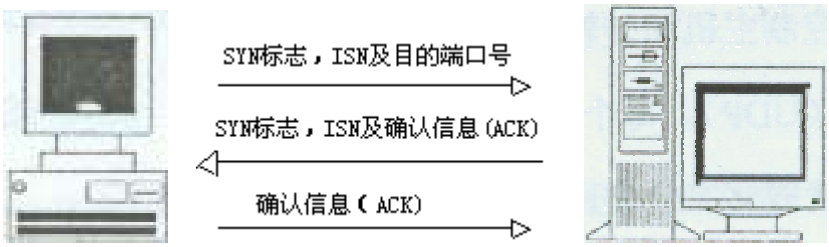
TCP 包头的标记区建立和中断一个基本的 TCP 连接。有三个标计来完成这些过程

- SYN：同步序列号
- FIN：发送端没有更多的数据要传输的信号
- ACK：识别数据包中的确认信息

建立一个 TCP 连接：SYN 和 ACK

建立 TCP 连接，必须要经过三次握手。三次握手由下面几步构成(本例中使用客户机/服务器模式)：

1. 客户端(或请求端)通过激活一个 TCP 包头中的 SYN 标计来执行一个 activeopen。这个 TCP 包头包括：
   用于连接的端口号；序列号字段中的初始序列号(ISN)。这个号是随机产生的
   客户端和服务器传输数据流时用于同步。
2. 服务器通过向客户端发送其自己的 SYN 而执行了一个 passiveopen，包含
   服务器的 ISN；对于客户端的一个确认(ACK)
3. 最后，客户端返回一个 ACK 给服务器。现在客户端和服务器可以通过比特流来传输数据，并且连接建立。如下图显示了整个执行过程



中断一个 TCP 连接：FIN 和 ACK

因为 TCP 连接是全双向的，中断一个 TCP 连接需要四个步骤。全双向意味着数据独立的在两个方向上流动，因此两个连接都必须被关闭，为了正确的关闭 TCP 连接，任何一个主机都必须发送一个 FIN(就是激活 TCP 包头中的 FIN 标记)，当一台主机接受到一个 FIN，它必须终止流动在另一个方向的数据，通过发送一个 FIN 到另一端的应用程序，一个会话结束大多数的应用程序将关闭两个方向上的数据流，然而，仅仅关闭一个方向并且在于关闭的模式中进行操作是可能的。

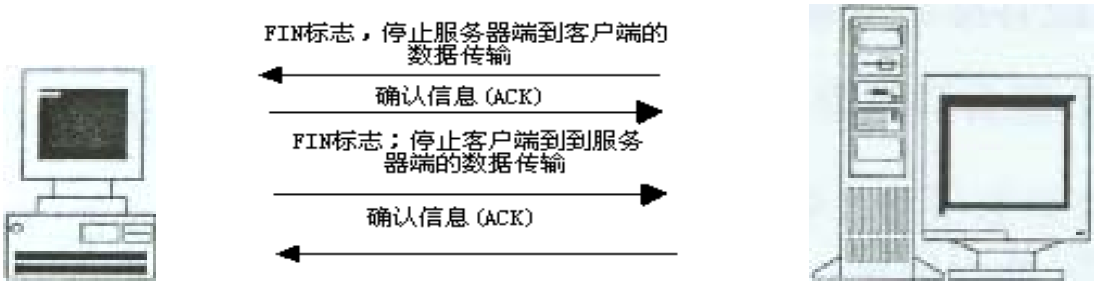
结束一个 TCP 连接的四个基本步骤是

1、服务器通过激活 FIN 标记执行一个 Activeclose(客户端经常结束应用程序，但是服务器将开始 TCP 连接的结束)，这个行动终止了从服务器到客户机的数据流。

2、客户端通过发送一个 ACK 到服务器，执行了一个 passiveclose。

3、客户端也发送它自己的 FIN 给服务器，以终止从客户端到服务器的数据流。

4、最后服务器发送一个 ACK 返回给客户端，TCP 连接被终止了，下图展示了完整的过程。



用户数据报协议(UDP)

UDP是一个非面向连接的协议。它经常用做广播类型的协议，如音频和视频数据流。它更快并更少占用带宽，因为一个UDP连接不被持续保持。这个协议并不能保证信息的仁慈也不能重复被中断的传输，但TCP可以。因此，在音频或视频传输中，几个数据包的丢失将不会有什么影响。

一些其它使用UDP的协议，例如TFTP，它要比FTP简单。如果认证并不被考虑的话也是非常有用的。类似于TFTP的协议需要所有的包都到达，但这些协议仅仅需要确保在应用层上传递和接收。UDP仅很少有安全上的隐患。因为主机发出一个UDP信息并不期望收到一个回复，在这种数据报文里面嵌入一个恶意的活动是很困难的。

端口

TCP和UDP都使用端口的概念。一台运行TCP／1P的机器几乎总是同时有不同的应用程序在运行。它们必须都能够同时通信。例如，一台计算机即可以充当WEB服务器也可以当做FTP或MAlL服务器。需要一种机制使进来的数据包能够指向各自相相应的程序，就像一个海港有

不同的港口或码头能使不同的船只停到相应的位置。早期的开发商给出一个类似的方法去处理信息。

为了使信息能够被正确地引导，每个程序被赋予了特别的TCP或UDP端口号。进入计算机的网络数据包都包含了一个端口号并且被操作系统发送到相应的程序。几十年来，主要的端口号已经标准化了，例如，文件传输协议使用TCP20和21端口号，DNS使用TCP和UDP的53端口号，WEB服务器使用80端口号，SNMP使用UDPl61和162端口号，Email服务器使用TCP25端口号。

TCP和UDP都有65536个可用的端口。Internet Assigned Numbers Authority(IANA)规定前1023,个端口作为well-know端口。well-know端口专门为服务器端的应用程序保留下来，一个服务器应用程序能够使用任何未被限定的端口，及那些大于1023的端口，而不需要向IANA申请。这条信息是非常重要的，因为安全在很大程度上依赖于你控制网络数据包的能力，你必须能够准确地确定这些数据包流向哪些计算机和程序。

应用层

最后一层是应用层，并且是最难保护的一层。因为TCP／IP应用程序几乎是可无限制地执行的，你实际上是没有办法保护所有的应用层上的程序的。但是，所有的应用层上的程序都有一些共性，你知道TCP／IP主要是用于客户机／服务器模式上的，应用层是这种使用的最好例子。例如，用户想要通过Intemet浏览器来访问WEB页面。唯一的限制就是一台主机上可以有多少个端口来通信。因为TCP和UDP端口不一样，大约有130000个应用程序可以用于TCP／IP之上。保护网络上的每一个应用程序是不太可能的，所有只允许一些特殊的应用程序能通过网络进行通信是一个不错的方法。

简单邮件传输协议

SMTP本身有很小的风险，但黑客还是尝试去破坏一个Email服务器。Sendmail是UNIX下的一个守护进程并负责前面段落中所提到的过程。早期版本的sendmail有很多安全方面的问题。通过这些年的努力，Sendmail现在已变得很安全了，现在已能够很放心的去使用了。通常，黑客对SMTP服务器采用不同方式的攻击。举个例子，黑客可能创建一个伪造的Email信息只接发送到你的SMTP服务器，这条信息可以包含一些社会工程的内容。SMTP服务器其它的一些安全风险是拒绝服务攻击。黑客经常向SMTP服务器发送大量的Email信息使得这台服务器不能处理合法用户的Email流量。这种方法有效地导致SMTP服务器不可用，因此对合法的email用户造成了拒绝服务。

大家都知道的SMTP的风险就是发送和接收病毒和特洛伊木马。一个典刑的e-mail信息包含很少的一些基本内容：标题说明了信息从哪里开始，接收者是谁，以及时间利日期。Email信件中标题中的信息很容易被作假。信件的另一个位置是正文部分，含有标准的文本或真正的信息，较新的Email客户端程序可以发送HTML格式的信息。Email信件中标题和正文部分不会包含可执行的代码：因此，病毒和特洛伊木马不会出现在这两个位置中。病毒和木马经常是出现在附件中的。一封Email信件：可以含有各种类型的附件，包括病毒和木马。最佳防御含有恶意附件的方法是购买一台可扫描所有邮件信息的SMTP服务器。另一个预防性的方法是进行用户教育。教育你的e-mail用户病毒利木马是如何通过SMTP传播的以减少它们在网络中的出现。

文件传输协议(FTP)

FTP用来建立TCP／IP连接后发送利接收文件：。FTP由服务器和客户端组成，几乎每一个TCP／IP主机都有内置的FTP客户端，并且大多数的服务器都有一个FTP服务器程序。FTP

用两个端口通信。利用TCP21端口来控制连接的建立，控制连接端口在整个FTP会话中保持开放，用来在客户端和服务器之间发送控制信息和客户端命令。数据连接建立使用一个短暂的临时端口。在客户端和服务器之间传输一个文件时每次都建立一个数据连接。

黑客很少直接使用FTP。因为它仅用于发送和接收文件，因此很难被破坏。然而，黑客所做的是间接地破坏FTP服务器。FTP服务器可能不需要对客户端进行认证：当需要认证时，所有的用户名和密码都是以明文传输的。一种常见的破坏就是寻找允许匿名连接并且有写权限的FTP服务器，然后黑客上传不正确的信息以塞满整个硬盘的空间。这种做法的目的是希望FTP服务器安装在含有操作系统的硬盘上，如果硬盘被黑客用错误的信息塞满，这种负载将会导致操作系统不能正常运行。同样使用的技术包括FTP服务器上的日志文件，黑客添满硬盘，使日志文件没有空间再记录其它事件，这样黑客企图进入操作系统或其它服务而不被日志文件所检查到。

另一种对于FTP服务器的破坏是把一些盗版软件拷贝到服务器上。然后黑客把FTP服务器通知给其他黑客，其他的黑客将上传或下载这些诧版软件。在任何服务器上并没有直接目的的攻击，因为所有的活动看上去都是合法的。然而，黑客已经把这个FTP服务器作为一个存储服务器来达到他们非法活动的目的。

超文本传输协议(HTTP)

HTTP是互联网上最广泛的协议，互联网上大概有一半的流量是HTTP。HTTP使用80端口来控制连接和一个临时端口传输数据，HTTP有两种明显的安全问题，它们是客户端浏览应用程序和HTTP服务器外部应用程序，HTTP客户端使用浏览器访问和接收从服务器端返回的WEB页面。浏览器应用程序用于格式化不同类型的内容。举个例子，如果你下载一个电影文件：需要另一种应用程序来观看这个电影，浏览器需要WEB页面包含这样的电影，并且HTTP通过发送所有的请求页面和相关内容来做出响应。当客户端接收到这个电影文件：必须加载一个类似WindowsMediaPlayer或RealAudioPlayer这样的程序，目前的浏览揩有很多预先配置的浏览应用程序并且功能被修改，除非所有相关问题已经被解决，对用WEB用户的另一个问题是下载有破坏性的activeX控件或JAVAapplets。这些程序在用户的计算机上执行并含有某种类别的代码，包括病毒或特洛伊木马。对于这种破坏的最佳保护方法是教育你的用户，这些程序是干什么用的并警告他们不要下载未被检验过的应用程序。

HTTP服务器也必须要小心保护，HTTP服务器在很多基础上类似FTP服务器。当一个WEB用户请求一个HTTP页面时，HTTP服务器从它自己的硬盘中找到这个页面并发送给客户端，客户端必须合适的格式化这个页面。然而，这些类型的WEB服务器是非常简单的并且不能为用户提供很好的经验，为了扩大和扩展WEB服务器的功能，一些扩展的应用程序可以加入到HTTP服务器中。这些扩展的应用程序包括JAVA，CGI，AST等等。这些程序都有一些安全漏洞，一旦WEB服务器开始执行代码，那么它有可能遭到破坏。这些程序有两种方法来破坏WEB服务器：第一，通过修改当前HTTP服务器的程序如何执行：第二，在HTTP服务器上放置一个特洛伊木马，然后让HTTP服务器执行特洛伊木马。

Telnet

Telnet是用于远程终端访问的并可用来管理UNIX机器。Windows NT默认安装是不提供一个Telnet服务器的，第一个第三方的服务可以很容易地加进去。Telnet是首先考虑有关安全的因为它要求远程用户登陆。但是Telnet是以明文的方式发送所有的用户名和密码的。有经验的黑客可以劫持一个Telnet会话。使用TeLnet的别一个安全问题是什么时候使用这个协议。Telnet应该在你检查整个连接到你的网络上的客户端和服务器时才使用。因此，它不应该应用到互联网上。你还应该在防火墙上过滤掉所有的Telnet流量。有一系列的程序功能类似：它们被称

为r系列，包括rsh和rlogin。当使用r系列程序的时候要考虑和Telnet相同的安全问题。

许多系统管理员已经用SecureShell(SSH)来代替Telnet和UNIX下r系列的应用程序。你可以通过访问．http：／／www,ssh．com来学习更多有关SSH的知识。SSH加密所有传输的内容，还允许通过公钥加密机制来进行认证。

简单网络字管理协议(SNMP)

SNMP允许管理员检查状态并且有时修改SNMP节点的配置。它使用两个组件，即SNMP管理者和SNMP节点。管理者收集所有由SNMP 节点发送的trap，并且直接从这些节点查询信息。SNMP就是安装相关厂商的SNMP客户端软件的没备。SNMP通过UDP的161利162端口传递所有的信息。

有关SNMP的安全是认证是怎么发生的并且数据是怎样传输的。SNMP所提供的唯一认证就是community name。一个community就是由SNMP来验证节点的术语。如果管理者和接点有相同的communityname，将允许所有SNMP查寻。如果一个黑客危及到community name，他(她)将能够查询和修改网络上所有使用SNMP的1y点。另一个安全问题是所有的信息都是以明文传输的。一个黑客用SNMP管理器连接到网络中的任何位置上都可以得到这些信息，包括communityname。SNMP不应该应用到公网上，尤其是互联网上。SNMP是在你公司私有的网络中可用的网络管理解决方案，但是所有的SNMP流量要在防火墙上过滤掉。目前应用SNMP v3版本可能解决上述问题。

域名系统(DNS)

DNS在解析DNS请求时使用UDP的53端口。但是53端口。一次区域传输是以下面两种情况完成的在进行区域传输时使用TCP的

- 一个客户端利用nslookup命令向DNS服务器请求进行区域传输
- 当一个从属域名服务器向主服务器请求得到一个区域文件

黑客可以攻击一个DNS服务器并得到它的区域文件。这种攻击的结果是黑客可以知道这个区域中所有系统的IP地址和计算机名字。

然而你可以保护你的DNS服务器：首先你要把这个服务器放到防火墙后面，然后配置你的防火墙阻止所有的区域传输，第二你可配置你的系统只接受特定主机的区域传输。我们可以利用通知选项来确保只有那些经验证的系统能得到一个区域传输。许多安全服务，包括入侵检测应用程序，扫描器以及,SSH，需要合法的DNS目的是能够正常的运转。反向DNS查寻对于一些应用程序如SSH也是基本要求。

本章小结：

通过本章的学习，达到对于TCP／IP协议有了更深刻的认识，并对TCP／IP的漏洞详细分析，黑客经常也通过这些漏洞进行攻击。对于TCP／IP每一层存在的协议详细剖析以尽可能地确保你的公司发送的都是一些安全的信息。

问题讨论：

／ TCP／IP与OSI相比分为哪四层?且每层都存在什么协议?

／ FTP、TELNET及SNMP等常见协议存在什么样的安全问题?如何解决

第六章

保 护 资 源

引　　言

前面我们已经学到TCP／IP是一个非常强大而且流行的协议，然而，它也有一定的安全隐患，不仅是因为它的流行，还因为它的当初设计是面向资源开放的。任何人都可通过RFC来学到它设计的所有特性。本章我们将讨论对于TCP／IP常见的攻击，包括HTTP、FTP、SMTP等服务器我们怎样有效地防范。

本章要点：

- 使用用WindowsNT C2级安全管理来保护操作系统
- 保护TCP／IP服务，包括HTTP、FTP和SMTP等
- 测试和评估系统及服务的重要性
- 网络扫描器，操作系统附加软件以及日志分析工具。

安全的实施过程

表7—1中的描述会帮助你如何应用你的安全策略

数字	步骤	描述
1	根据需要对资源分类	前面已经学过有关 LevelI，II 和 III 的分类。你还要考虑对网络管理的分类包括对每个系统的详细内容，包括硬件的类型、当前的配置和使用的协议等。优先级和其它一些因素是类别的—部分。
2	定义一个安全策略	你还必须定义和发布你的安全策略。如果公司的安全策略只有你或少数 IT 员知道的话是没有什么价值的。所有的员工都应该知道安全策略是放置到什么位置并且如何应用到他们的工作当中。
3	保护每个资源和服务	这步包括下面所有的活动 . 改变服务器和系统的默认值 . 删除一些无关的服务 . 坚持地监视公共连接，包括 VPN，modembank，由其是 WEB 和 FTP 服务器。 . 确保物理安全 . 锁定注册表项和密码文件：
4	日志，测试和评估	在所有的系统上实行日志记录，并定期有规律地检查这些日志：要配置你的日志文件，使它们不能成为安全威胁。

5	重复执行和保持当前	即使已采取了上述的四个步骤也永远不要假设你已经完成了安全保护。你需要记住当—个新的黑客技术开发出来后你现有的策略可以就会存在缺口。

我们前面已学过有关前两个步骤的知识，这节课的重点是下三步的实施。要明确地对前面所讨论过的有关TCP／IP资源的安全保护。

资源和服务

每个服务都是单独运行的。作为一个安全专家，你必须设计出一种方法使这种独立为你工作，而不是和你做对的。每个单独的服务可能会产生一些问题，因为一旦一个黑客危及到你的系统，可以利用这个服务来攻击另外一个服务。但是你可以使你的服务和操作系统按下面所建议的方法来工作。

保护服务

你可以通过调整不同的权限、服务和技术来保护服务。你还要改变系统的默认值以及删除不必要的服务。

保护配置文件

配置文件可能会成为黑客进一步确定网络内主机情况的工具,还可以进一步确定穿过主机的流量。Packetsniffer可用于捕获配置文件的详细信息。当一块网卡被设置成混杂模式时，黑客可以开始破坏这个网络。对于这种活动可以用不同的有效方法阻止。

协同使用不同的方案和技术

在安全资源里最重要的一个概念就是要协同使用方案和技术，如果一个黑客攻破了一种方案那么还会有另一种来抵抗。还要考虑像HTTP，Telnet，FTP这些服务。每种系统都有它们自己的漏洞，一定要逐个地保护，这些要求包括改变默认的设置。

要按照服务安全策略来定义操作系统的策略。你的系统不要仅依靠安全因素的某一条(如认证，加密，或审计)。举个例子，不要仅依赖于认证的方法，你可以再加上加密和审计的手段来使用你的系统更安全一些。

通过改变默认设置来保护服务

任何有经验的黑客都知道一些流行服务、serveR或计算机的默认设置。因此，你要尽可能地改变这些默认设置。在本课你将学到如何更改这些特殊的默认值。

删除不必要的服务

通常删除不必要的服务会更安全些。很多公司都忽略了这种简单的解决办法，而无意识地为黑客留下了后门。例如，如果你使用WindowsNT上的IlS，那么就不要让service这个服务运行。如果不这么做会引起没必要的风险。简单地说如运行在系统上的OS／2子系统就是不必要的，因为它产生了一个安全突破口。所以你一定要小心对待这些多余的服务。进一步说就是不要运行它们，因为很多黑客查找这些多余的服务。

保护TCP／IP服务

以下更深入地讨论如何更有效地保护Internet服务。多数对于Internet服务访问控制的实施都是通过基本操作系统内定的用户帐号。NT和UNIX都有特殊的系统帐号用来管理服务或守护进程。你要改变默认帐号的名字来增加安全性。在WindowsNT利Intemet服务中，都是通过一个叫"localsystem"的帐号来控制管理的。你应该可以感觉到这个帐号不是普通的帐号，并可以直接用它来登陆，除此之外它还有着管理的优先权限。黑客可以利用这些Internet服务以管理员的权限来执行一段恶意代码。改变用于管理每个Internet服务的帐号可以使管理员更好地控制和审计所有的Internet服务。同样这种做法也适用于UNIX的守护进程。目前互联网上最常见的服务有WEB SERVER：FTP SERVER；SMTP SERVER：DNS等等。

The Web Server

安全保护Web Server的关键是要把操作系统，Web服务器程序，以及服务器硬盘上的文件分离开放置到单独的硬盘分区中。如果一个破坏发生，这种分离将会限制一个黑客对于特殊硬盘或硬盘的一部分上面的活动。另一个关键是不要把操作系统，应用程序文件，用于Web页面的HTML文仆和脚本文件放到同一一块硬盘，要把硬盘分成几个区，然后只把操作系统放到主分区内。　下一步，要把WEB服务器程序(如lis)装到第二个分区上，然后把所有的HTML文件移到另外一个分区上，并把含有HTML内容的分区设置成只读，这是一种防止黑客活动的简单却又有效的方法。这样用户仍然可以查看HTML文件，但是当黑客访问些分区的时候会在很大程度上受到限制。然后你要把脚本文件(如CGI,ISAPI,PERL脚本等)放到另一个分区上。因为这些脚本必须可以被执行，你必须允许这种执行。但是你可能经常在系统上设置不允许对些分区有写入权限。黑客经常试图在含有WEB服务的脚本文件的目录中放置木马程序。当黑客成功地在脚本目录中放置了木马程序后，他仅仅需要在任何的WEB浏览器中执行一个脚本。通过把脚本单独放到一个特殊的硬盘或分区，你可以更轻松地保护操作系统和其它一些服务，防止一些恶意的代码在此目录中执行。利用这种方法，如果一个黑客攻破了服务器上的一部分安全设置，但他(她)仍受限于其它分区的设置，而不能对整个硬盘拥有访问的权限。而且，如果那个分区是只读的，黑客不能向里拷贝文件或改变任何文件。这种方法是关于如何利用安全技术创建一个安全系统、设备和资源的矩阵。

众所周知的Unicode漏洞就是利用了操作系统以及IIS默认安装方式而导致的，如我们可以简单地在浏览器中输入一下列代码即可获得相关信息 http://ip/scripts/..%c0..%af../winnt/system32/cmd.exe?/c+dir+，这样我们就可以看到对方IIS所安装的路径，同样也可以采用这种方法来涂改WEB页面，目前流行的蓝色代码也是利用Unicode的漏洞来造成攻击的，解决的方法其实也很简单，我们只需要把操作系统或IIS默认安装的路径及目录名全部改掉，并删除Scripts日录就可以了，或者可到微软的官方网站上下载相应的补丁程序。

CGI脚本

公共网关接口(CGI)脚本经常会产生安全方面的隐患。一个原因是它们像小型的服务器：它们可以执行命令并向客户端显示信息。黑客可以使用表面上看之良好的脚本，但实际上是为了攻破你的系统而精心及计的。CGI脚本主要有两方面的漏洞：

- 它们有意或无意地泄露主机系统的信息
- 脚本用于处理远程用户的输入，如表单中的内容或搜索索引的命令，可以被欺骗以任意执行系统命令。

把CGI脚本放到它们自己专用的分区是保护你系统的一种方法。其实多数问题都可以通

过小心地编写代码来避免。确保你的CGI程序员在编写这些脚本时倍加小心。要严格测试这些脚本是否含有不期望或不止确的数据。如果你不熟悉Peri或C(或者其它一些用于编写脚本的语言)，去找一些精通这些语言的人。否则，你可能会因为这些不严谨的脚本而导致一个安全破坏。

为了确保CGI脚本的安全，你要注意以下提出的问题：

- 我们是否使用了经过编译的CGl网关而不是那些用Peri或shell编写的脚本?
- 有多少可信的客户端(如远程用户提交表单)可以输入正确信息?
- 我们要对缓冲匡：溢出采取什么样的警惕?有时，一个CGI脚本可能仅计算内存中的1024个字节，但当需要处理更多的数据时，结果是，这个程序。。。经常是shell将会崩溃，并且用户数据覆盖了程序堆栈。从这点可以看出，黑客可以在系统上执行任意代码，且经常是有root权限的。
- 是否有信息直接从客户端(如远程用户)向shelll命令发出消求?这种过程允许用户在数据流中嵌入叫做“ meta characters ”的特殊字符。这些特殊字符可以导致shell崩溃或者产生缓冲区溢出。为了解决这种问题，直接让你的CGI程序员过滤掉这些特殊字符。
- 是否有，有多少CGI脚本可以和shell之间进行交互?

管理员可能要对所有的CGI脚本(也包括其它由公司职员编写的重要的应用程序)单独地进行检查以发现问题。

保护IIs

不像其它的WEB服务器，根据Windows NT操作系统的特性对于IlS服务器要由为小心保护。要遵守WindowsNT磁盘和文件的访问控制以及NT组和用户的权限。因此，如果你使用这台服务器，你必须确保操作系统是安全的。大数常见的黑客技术使黑客能够进入磁盘或正在试图进入。在lis中，你可以使你的操作系统在你不使用台服务器时自动地重新没置权限以进一步增加安全性。举个例子，如果你计划让你的系统在凌晨2点钟的时候重新设置权限，并且如果一个黑客越过你的安全策略而渗透到你系统中的一部分时，自动重新设置权限可能会停止黑客的这种行为。如果你运行lis，你还必须激活所有的审计事件。如果一个攻击发生，lis中的审计将让你判断到底发生了什么，并且可以开始追捕到黑客的访问。如实验7-2显示，建立有效的安全不仅仅是保护操作系统的事，也要通过保护WEB服务本身。

文件传输协议服务器(FTP)

保护你的FTP服务器类似于保护你的WEB服务器。一定要确保把你的用于下载文件的FTP服务器分别单独的分区中。如果可能，一定要尽力把你的FTP用户帐号与用于访问WEB服务揣的帐号分开使用。还有对于每个服务安排单独的操作系统访问控制，这种配置可以防护单独的侵入。如果一个资源受到危及，那么其它的仍然是安全的。

可能一种拒绝服务攻击是塞满你FTP服务器上的硬盘。如果操作系统和FTP存在于同一分区下，那么这种攻击可能会导致系统崩溃。潜在地，一个黑客可能多次地登录服务器，目的是为了填满日志文件导致服务器崩溃。如果你不把你的操作系统，服务器和文件分开的话，黑客可能会很容易地控制它。有时你可能需要对FTP上的公共文件设置成只改访问的权限，但是如果外部用户向你的WED服务器上传文件时，你应该考虑磁盘的空间，如果磁盘已经满了，是因为某些人上传了大量文件，那么整个系统有可能面于崩溃。

访问控制

尽管大多数的FTP服务器只允许对FTP服务下根目录下的文件进行访问，也要确保你的FTP服务器不允许对一些敏感文件的访问。如果你不注意的话，用户可能会取得对你WEB服

务器上的目录的访问权限并且覆盖你的WEB文件，这种问题经常发生。最好的方法是设置为只允许匿名访问，这样所有的人都是只读的权限。

简单邮件传输协议(SMTP)

因为简单邮件传输协议(SMTP)当初的设计并没有考虑安全问题，保护一个E-mail服务器更加困难。较新的SMTP服务器提出了一些安全特性，如反向域名查询来确保E-maiI是否来自一个真正想要发送的人。只要可能一定要使用认证机制。保护E-mail本身的内容，加密是一个关键。前面的课程中我们已经讨论过主要加密的方法以及几种流行的工具，包括在微软服务器上加密方法的特性和公钥加密如PGP。这些方法对于保证通过你的服务器发送的信息是否安全是非常有用的。

Internet蠕虫

Internet蠕虫是一种拒绝服务病毒，在一九八八年十一月二日开始危害了与Internet相连的主机很多大，它是一个非常重要的历史事件，闲为它告沂了安全专家有关TCP／IP心用程序的漏洞。此事件：是由一个利用UNIX下的TCP／IP实施的漏洞编写的程序产生的，这个用C语言编写的程序大约破坏了5000台Internet上的主机，这种病毒以几种主要方法影响基于WEB技术开发的程序。首先，WEB程序语言如JAVA现在已经强制严格检查边界，在JAVA中想写入超过最后512字节是不可能的。其次，操作系统给予系统运行者对于通过网络攻击的过程更多的控制权限。Internet蠕虫间接的影响堡垒主机利与互联网连接的防火墙的体系结构。最近流行的红色代码也是类似的一种蠕虫病毒，其版本2发作会自动开启600个线程来对外扫描并传播，并会安装木马，它是利用微软WindowsIIS服务器的一个安全漏洞进行攻击和传播，已危害全世界数十万台主机。

Melissa病毒

Melissa病毒是由一个新泽西的黑客创建的，与一九八八年的Intemet蠕虫不同，Melissa病毒是利用E-mail客户端应用程序，而不是服务器本身。这种病毒嵌入到微软的WORD文档中。当用户打开此文档时此病毒将会自身复制并传播，这种病毒影响用户的机器，利用E-mail客户的应用程序自动的发送信息并包含己完全受感染的附件，并发送给用户端的地址薄的前五十名联系者。

E·mail和病毒扫描

Intemet蠕虫和Melissa病毒是需要进行有效E-mail扫描的最典型例子，这两种攻击显示了SMTP服务器的一些漏洞。首先E-maiI服务器不检查传送信息中的内容，其次，它们很容易的被大量的请求导致不能响应。商业反病毒程序可以创建一些安全的级别，因为它们可以在用户激活内嵌病毒之前扫描E-mail附件。然后这些程序只能在个人机器上使用。

网络级E-mail扫描

在一些SMTP服务器中，有关新的安全特点是可以基于网络级的自动扫描病毒、尽管E-mail信息本身不会携带病毒，但一个病毒可以通过附件进行发送。高级的SMTP服务器可以通过把Email信息放到一个临时存放区域来扫描其是否携带病毒。这些服务器扫描文件，然后转发适当的Email。经常，这种执行只需要少量的时间，但这种延迟却是非常值得的。你还可以通过你的防火墙来扫描你的Email。然而这种扫描，不管是通过SMTP服务端还是防火墙，

都在某种程度上降低了系统的性能。

访问控制方法

当保护一个Email服务时，你要做到：

- 禁止转发非验证用户的信息。一些SMTP服务器默认情况下是不禁止这种转发的
- 减小Email附件的大小
- 一个帐号可以接收有限的Email数量

配置SMTP服务器的验证功能

配置SMTP验证还是很有必要的，可以有效地防止黑客把你的SMTP服务器当作发送垃圾邮件的中转站以至于你的SMTP服务器超负荷，下面列出有关Sendmail服务器来实现SMTP认证的步骤：

1．首先要—下载sasl库，该函数库提供了安全认证所需函数，·下载地址是(Ftp：／／ftp．andrew．cmu．edu／pub／cyrus-mail／)，版本1．5．21。

2．·下载sendmail(http：／／WWW．sendmail．org)，版本在8．10．0以上的sendmail才支持SMTP认证功能。 ．

3．注意选择客户端电子邮件软件。并不是所有的客户端电子邮件软件都支持SMTP认证功能，几种常见的 版本要求是这样的：

Netscape Messenger的版本要4．6以上

Outlook和Outlook Express要5．0版本以上

Eudora pro的版本要在4．3以上

Foxmail目前还不支持这个功能。

每一种软件的认证方法是不一样的，编译sasl库的时候和配置sendmail略有不同。我就大家最常见的Outlook Express5。0的设置方法介绍如下

二、安装sasl库

1．解压cyrus—sasl—1．5．21．tar．gz到你选定的目录

2．Cd cyrus—sasl—1．5．21

3，／configure—-enable—login--with-pwcheck

Outlook ExpREss使用LOGIN的认证方法，sam库缺省并不支持这种方式，所以要在生成配置文件时特别加入，另外，Outlook的口令验证方式也不是缺省的方式，所以也需要加-----With-pwcheck的选项。

·下面就可以编译利安装sasl库了

make

make install

4．缺省情况厂，所有的库函数安装到／usr／local／1ib日录下但sendmail使用的库函数是在目录／usr/1ib下的，所以需要做一些调整。

Cd／usr／1ib

ln／LISr／local／1ib／sasl／．／sasl -S

cp／usr／local／lib／1ibsa*．

也可以避开这一步，在第3步时候运行configure脚本前，修改其中的缺省路径就可以了。

打开configure文件找到这一行ac_default_prefix=／usr／local(在文件前几行)，改为

ac_default_prefix=／usr就可以了，这样更方便一些。

5．新建目录／var／pwcheck，供pwcheck命令使用，该命令是一个后台程序，负责检查用户的输入口令，以root权限件使用shadow口令文件。

6．在／usr／“ b／sasl目录－下建立文件Sendmail．conf，加入如下
这样sasL库函数的安装就完成了。
二、编译和配置sendmail
1．解压sendmail软件到你希望的目录，进入sendmail－8．10．2日录。
在devtools／Site／目录下创建config．site．m4文仆，加入如下两行文字，把SMTP认证功能编译到sendmail中。
APPENDDEF(‘ confENVDEF ’,’ －DSASL ’)
APPENDDEF(‘ conf sendmaiI_LIBS ’,· －lsasl ’)
2．回到sendmail－8．10．2目录，再进入sendmail日录，开始编译sendmail，
．/build－c(如果不是第一次编译，需要加入－c选项，清除以前的配置)
编译成功后，运行．／Build lnstall安装软件
3．下一步需要改写Sendmail的配置文件。回到上一级日录，再进入cf／cf目录，找到合适的。mc文件：(具体做法参见其他文章，这些不在本文讨论范围中)。按照你的要求适当修改，加入如下几行：
TRUST_AUTH_MECH(‘ LOGIN PLAIN DIGEST—MD5’)
define(’ confAUTH_ECHANISMS ’,‘ LOGIN PLAIN DIGEST-MD5 ’)
dnl define(‘ confDEF_AUTH_INFO ’,’ ／etc／mail/auth／auth－info ’)
FEATURE(’no_default_msa’)
DAEMON_OPTIONS(’ Port ’ 25，Name=MSA，M=Ea ’)
说明：*TRUST_AUTH_ECH ‘ 的作用是使sendmail不管access文件中如何设置，都能relay那些通过LOGIN,PLAIN或DIGEST－MD5方式验证的邮件.
“confAUTH_ECHANISMS”的作用是确定系统的认证方式‘
“confDEF_AUTIt_INFO”的作用是当你的计算机作为客户机时，向另外一台有smtp认证功能的主机进行认证，用户和密码存放在auth－info文件中，在这个例子中并不需要这个功能，所以注释掉了。
4．编译生成／etc／mail／sendmail．cf文件
m4 XXXX．mc>／etc／mail／sendmail．cf，不过记住一定要备份旧的sendmail．cf文件，否则就可能麻烦了。
5．现在基本上可以了，启动sendmail让我们来测试一下吧
sendmail—bd—q20m
运行 ’ 下面命令
telnet localhost 25
ehlo localhost
注意有没有以－下的信息出现．
250—XXXXXXXX
250—XXXXXXX
250—AUTH LOGIN PLAIN DIGEST—MD5
250—XXXXXX
可能会略有不同，不过你选定的认证方式一定要有的。
如果显示没有问题，恭喜你!服务器端的配置你已经成功了。如果没有出现上面的信息，运行
sendmail -0 loglevel=14 -bS
仔细检查问题所在。在结束服务器端的配置之前，我们还要做一件事，运行pwcheck这个daemon程序，这样才能完成用户认证功能。
Pwcheck &

四、Outlook Express 5．0的配置

1．打开你的Outlook Express，修改你的账号属性，在服务器选项，选取我的 smtp服务端需要认证选项，然后进入配置

2．不要选取安全口令认证，sendmail并不支持这个选项。是选取使用pop3同样的口令还是选择另外输入用户和密码，这就看你的爱好和设置了，这不是关键。如果你在服务器上有一个真实账号，不妨选取使用同样的口令，如果没有账号，选用其他的用户口令同样可以。到此SMTP认证的功能已经实现了。

测试和评估

测试你的系统是实施你的安全计划的关键。

测试已存在的系统

- 利用和黑客使用一样的工具，方法和技术来测试你的网络。很多自动测试工具可以帮你减轻负担。
- 参考服务器日志。你必须比较日志来判断有哪些是真正符合你的安全策略的。要注意那些不符合你策略的因素，通过这些信息来改善用户的兼容性。
- 不要自满。不要因为你已经实施了课上所学的安全方法就简单地假设你的系统是安全的。你必须实时地检查系统的安全性。在互联网上，今天可能的安全将会成为以后不安全的问题，因为硬件在改变，操作系统在更新，或者应用程序的BUG。

实施一个新的系统

在实施一个新的系统或测试一个新的安全设置时，要遵循以下的步骤：

- 和对待你正常的系统一样要实施安全策略和配置
- 把新的系统放到不同的子网中
- 同样，尽可能地符合你网络中的情况
- 与已存在的系统一样利用黑客使用的工具，方法利技术对新的系统进行测试

安全测试软件

大多数的安全测试软件可以测试不同面貌的系统的安全。在你的网络中有一些程序是安全的，而其它一些是需要特殊重点保护的。多数简单的工具可以帮助你恢复安全问题所产生的事件，这些工具主要好处是容易操作并且可自动执行，你可以以较小的代价来定期的运行它们。但是这些安全工具的缺点是很快的就过时，因为这些程序无法检测新发现的安全问题，除非你及时的修改和更新它。

系统管理员想测试他们自己的安全系统，并开发能够符合他们解决方案的程序。但是一些用于检测安全系统的程序也可用于破坏行为。这种级别的风险依赖于是否一个黑客或系统管理员使用这种工具。三种主要安全工具的类别是网络扫描器，操作系统附加软件以及日志记录和分析软件。

网络扫描器

网络扫描器使用一个已知安全问题的数据库并测试网络以防护这些信息出现。流行的网络扫描器包括WebTrends安全分析器。附加的应用程序包括Internet安全扫描器(ISS)，在扫描一个特殊的网络主机后，网络扫描器可对安全风险及漏洞进行分类并给出相应的解决方案。

举个例子，WebTrends可以判断资源是处在高，中还是低风险。大多数扫描器会立即识别HTTP，FTP和SMTP服务器是否处在较低的安全风险中。

操作系统附加软件

你可以利用附加软件来扩展多数服务的安全性，例如包括MicrosoftWindowsNTService Pack4，WindowsNT ResourceKit和UNIX守护进程的更新和补丁。微软现在对于WindowsNT已有了ServicePack6。你可以搜索http：//www,microsoft．com中的下载搜索页面来得到它。现在是：http:// www,microsoft.com/downloads/search.asp?

日志和日志分析工具

这些程序允许系统管理员知道在网络中发生了什么活动，如当一个用户登陆或注销，通过mail发送给系统。这种类型的程序可以记录在你本地网络及远程网络之间的活动。

最后一步就是重复使用你所学到的知识，建立你自己新的知识和技术融入到一个更好的安全实施当中去。安全是一个启发式的执行过程。你必须实时的测试来持久的提高你的安全系统。提高安全经常是对你构造或重新构造系统的一个考验。确保持久的安全唯一方法就是通过向应用声音原则来通知系统管理员。

新的网络技术快速地出现，一定要确保与最后的开发商一起进步。还有，你还要定期地访问一些黑客站点，如http：／／www,astalavista．com或http：／／anticode．com来保证你知道有什么样的潜在侵入会发生。

本章小结：

通过本章的学习，理解实施一个有效安全策略的制定及执行过程，掌握了保护WEB,FTP,SMTP等服务的基本技术和方法。

第七章

防活墙基础

引言

防火墙现在已成为各企业网络中实施安全保护的核心，安全管理员的目的是选择性地拒绝进出网络的数据流量，这些工作都是由防火墙来做的。本章我们会讨论网络中一些简单和复杂的防火墙相关知识

本章要点：

- 了解目前防火墙技术的发展现状
- 定义和描述防火墙在公司安全策略中承担的任务
- 定义普通防火墙术语
- 描述包过滤的特性以及电路级网关和应用级网关
- 描述常见几种的防火墙拓扑结构及安全保护级别
- 实施基于包过滤的防火墙部署

防火墙技术现状

自从1986年美国Digital公司在Intemet上安装了全球第一个商用防火墙系统后，提出了防火墙的概念，防火墙技术得到了飞速的发展。目前有几十家公司推出了功能不同的防火墙系统产品。第一代防火墙，又称包过滤防火墙，主要通过对数据包源地址、日的地址、端口号等参数来决定是否允许该数据包通过，对其进转发，但这种防火墙很难抵御IP地址欺骗等攻击，而且审计功能很差。第二代防火墙，也称代理服务器，它用来提供网络服务级的控制，起到外部网络向被保护的内部网络申请服务时中间转接作用，这种方法可以有效地防止对内部网络的直接攻击，安全性较高。第三代防火墙有效地提高了防火墙的安全性，称为状态监控功能防火墙，它可以对每一层的数据包进行检测和监控。随着网络攻击手段和信息安全技术的发展，新一代的功能更强人、安全性更强的防火墙已经问世，这个阶段的防火墙已超出了原来传统意义上防火墙的范畴，已经演变成一个全方位的安全技术集成系统，我们称之为第四代防火墙，它可以抵御目前常见的网络攻击手段，如IP地址欺骗、特洛伊木马攻击、Internet蠕虫、口令探寻攻击、邮件攻击等等。

防火墙的定义和描述

”防火墙”这个术语参考来自己应用在建筑结构里的安全技术。在楼宇里用来起分隔作用的墙，用来隔离不同的公司或房间，尽可能的起防火作用。一旦某个单元起火这种方法保护了其它的居住者。然而，多数防火墙里都有一个重要的门，允许人们进入或离开大楼。因此，虽然防火墙保护了人们的安全，但这个门在提供增强安全性的同时允许必要的访问。

在计算机网络中，一个网络防火墙扮演着防备潜在的恶意的活动的屏障，并可通过一个“门”来允许人们在你的安全网络和开放的不安全的网络之间通信。原来，一个防火墙是由一个单独的机器组成的，放置在你的私有网络和公网之间。近些年来，防火墙机制己发展到不仅仅是"firlwall box"，更多提及到的是堡垒主机。它现在涉及到整个从内部网络到外部网络的区域，由一系列复杂的机器和程序组成。简单来说，今天防火墙的主要概念就是多个组件的应用。到现在你要准备实施你的防火墙，需要知道你的公司需要什么样的服务并且什么样的服务对于内部用户和外部用户都是有效的。

防火墙的任务

防火墙在实施安全的过程中是至关重要的。一个防火墙策略要符合四个目标，而每个目标通常都不是通过一个单独的设备或软件来实现的。大多数情况下防火墙的组件放在一起使用以满足公司安全目的的需求。防火墙要能确保满足以下四个目标

实现一个公司的安全策略

防火墙的主要意图是强制执行你的安全策略。在前面的课程提到过在适当的网络安全中安全策略的重要性。举个例子，也许你的安全策略只需对MAIL服务器的SMTP流量作些限制，那么你要直接在防火墙强制这些策略。

创建一个阻塞点

防火墙在一个公司私有网络和分网问建立一个检查点。这种实现要求所有的流量都要通过这个检查点。一旦这些检查点清楚地建立，防火墙设备就可以监视，过滤利检查所有进来和出去的流量。网络安全产业称这些检查点为阻塞点。通过强制所有进出流量都通过这些检

查点，网络管理员可以集中在较少的方来实现安全目的。如果没有这样一个供监视利控制信息的点，系统或安全管理员则要在大量的地方来进行监测。检查点的另一个名字叫做网络边界。

记录Internet活动

防火墙还能够强制日志记录，并且提供警报功能。通过在防火墙上实现日志服务，安全管理员可以监视所有从外部网或互联网的访问。好的日志策略是实现适当网络安全的有效工具之一。防火墙对于管理员进行日志存档提供了更多的信息。

限制网络暴露

防火墙在你的网络周围创建了一个保护的边界。并且对于公网隐藏了你内部系统的一些信息以增加保密性。当远程节点侦测你的网络时，他们仅仅能看到防火墙。远程设备将不会知道你内部网络的布局以及都有些什么。防火墙提高认证功能和对网络加密来限制网络信息的暴露。通过对所能进来的流量时行源检查，以限制从外部发动的攻击。

防火墙术语

在我们继续讨论防火墙技术前，我们需要对一些重要的术语有一些认识

网关

网关是在两上设备之间提供转发服务的系统。网关的范围可以从互联网应用程序如公共网关接口(CGl)到在两台主机间处理流量的防火墙网关。这个术语是非常常见的而且在本课会用于一个防火墙组件里来在两上不同的网络路由和处理数据。

电路级网关

电路级网关用来监控受信任的客户或服务器与不受信任的主机间的TCP握手信息，这样来决定该会话是否合法，电路级网关是在OSI模刑中会话层上来过滤数据包，这样比包过滤防火墙要高两层。另外，电路级网关还提供一个重要的安全功能：网络地址转移(NAT)将所有公司内部的IP地址映射到一个“ 安全 ”的IP地址，这个地址是由防火墙使用的。有两种方法来实现这种类型的网关，一种是由一台主机充当筛选路由器而另一台充当应用级防火墙。另一种是在第一个防火墙主机和第二个之间建立安全的连接。这种结构的好处是当一次攻；行发生时能提供容错功能。

应用级网关

应用级网关可以工作在OSI七层模型的任一层上，能够检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级网关能够理解应用层上的协议，能够做复杂一些的访问控制，并做精细的注册。通常是在特殊的服务器上安装软件来实现的。

包过滤

包过滤是处理网络上基于packet-by-packet流量的设备。包过滤设备允许或阻止包，典型的实施方法是通过标准的路由器。包过滤是几种不同防火墙的类型之一，在本课后面我们将做详细地讨论。

代理服务器

代理服务器代表内部客户端与外部的服务器通信。代理服务器这个术语通常是指一个应用级的网关，虽然电路级网关也可作为代理服务器的一种。

网络地址翻译(NAT)

网络地址解释是对Intemet隐藏内部地址，防止内部地址公开。这一功能可以克服IP寻址方式的诸多限制，完善内部寻址模式。把未注册IP地址映射成合法地址，就可以对Intemet进行访问。对于NAT的另一个名字是IP地址隐藏。RFCl918概述了地址并且IANA建议使用内部地址机制，以下地址作为保留地址：

10．0．0．0—10．255．255．255

172．16．0．0—172．31．255．255

192．168．0．0—192．168．255．255

如果你选择上述例表中的网络地址，不需要向任何互联网授权机构注册即可使用。使用这些网络地址的一个好处就是在互联网上永远不会被路由。互联网上所有的路由器发现源或目标地址含有这些私有网络ID时都会自动地丢弃。

堡垒主机

堡垒主机是一种被强化的可以防御进攻的计算机，被暴露于因特网之上，作为进入内部网络的一个检查点，以达到把整个网络的安全问题集中在某个主机上解决，从而省时省力，不用考虑其它主机的安全的目的。从堡垒主机的定义我们可以看到，堡垒主机是网络中最容易受到侵害的主机。所以堡垒主机也必须是自身保护最完善的主机。你可以使用单宿主堡垒主机。多数情况—下，一个堡垒主机使用两块网卡，每个网卡连接不同的网络。一块网卡连接你公司的内部网络用来管理、控制和保护，而另一块连接另一个网络，通常是公网也就是Internet。堡垒主机经常配置网关服务。网关服务是一个进程来提供对从公网到私有网络的特殊协议路由，反之亦然。在一个应用级的网关里，你想使用的每一个应用程协议都需要—个进程。因此，你想通过一台堡垒主机来路由Email，Web和FTP服务时，你必须为每—个服务都提供一个守护进程。

强化操作系统

防火墙要求尽可能只配置必需的少量的服务。为了加强操作系统的稳同性，防火墙安装程序要禁止或删除所有不需要的服务。多数的防火墙产品，包括 Axent Raptor(www,axent．com)，CheckPOint(wwxv,checkpoint．com)-和 Network ASSOCiates Gauntlet(www．networkassociates．com)都可以在目前较流行的操作系统上运行。如Axent Raptor防火墙就可以安装在windOWSNT Server4．o，S0laris及HP-Ux操作系统上。理论上来讲，让操作系统只提供最基本的功能，可以使利用系统BUG来攻击的方法非常困难。最后，当你加强你的系统时，还要考虑到除了TCP/IP协议外不要把任何协议绑定到你的外部网卡上。

非军事化区域(DMZ)

DMZ是一个小型网络存在于公司的内部网络和外部网络之间。这个网络由筛选路由器建立，有时是一个阻塞路由器。DMz用来作为一个额外的缓冲区以进一步隔离公网和你的内部私有网络。DMZ另一个名字叫做serviceNetwork，因为它非常方便。这种实施的缺点在于存在于DMZ区域的任何服务器都不会得到防火墙的完全保护。

筛选路由器

筛选路由器的另一个术语就是包过滤路由器并且至少有一个接口是连向公网的，如Internet。它是对进出内部网络的所有信息进行分析，并按照一定的安全策略-----信息过滤规则对进出内部网络的信息进行限制，允许授权信息通过，拒绝非授权信息通过。信息过滤规则是以其所收到的数据包头信息为基础的。采用这种技术的防火墙优点在于速度快、实现方便，但安全性能差，且由于不同操作系统环境下TCP利UDP端口号所代表的应用服务协议类型有所不同，故兼容性差。

阻塞路由器

阻塞路由器(也叫内部路由器)保护内部的网络使之免受Internet利周边网的侵犯。内部路由器为用户的防火墙执行大部分的数据包过滤工作。它允许从内部网络到Internet的有选择的出站服务。这些服务是用户的站点能使用数据包过滤而不是代理服务安全支持利安全提供的服务。内部路由器所允许的在堡垒主机(在周边网上)和用户的内部网之间服务可以不同于内部路由器所允许的在Internet和用户的内部网之间的服务。限制堡垒主机利内部网之间服务的理由是减少由此而导致的受到来自堡垒主机侵袭的机器的数量。

防火墙默认的配置

默认情况下，防火墙可以配置成以下两种情况：

- 拒绝所有的流量，这需要在你的网络中特殊指定能够进入和出去的流量的一些类型
- 允许所有的流量，这种情况需要你特殊指定要拒绝的流量的类型。

可论证地，大多数防火墙默认都是拒绝所有的流量作为安全选项。一旦你安装防火墙后，你需要打开一些必要的端口来使防火墙内的用户在通过验证之后可以访问系统。换句话说，如果你想让你的员工们能够发送和接收Email，你必须在防火墙上设置相应的规则或开启允许POP3和SMTP的进程。

包过滤

包过滤技术(Packet Filter)是防火墙为系统提供安全保障的主要技术，它通过设备对进出网络的数据流进行有选择的控制与操作。包过滤操作通常在选择路由的同时对数据包进行过滤(通常是对从互联网络到内部网络的包进行过滤)。用户可以设定一系列的规则，指定允许哪些类型的数据包可以流入或流出内部网络；哪些类型的数据包的传输应该被扩截。包过滤规则以IP包信息为基础，对IP包的源地址、 IP包的目的地址、封装协议(TCP／UDP／ICMP／IPTunnel)、端口号等进行筛选。包过滤这个操作可以在路由器上进行，也可以在网桥，甚至在一个单独的主机上进行。

包过滤1：作在OIS七层模型的网络层上。包过滤有两个功能，即允许和阻止，如果检查数据包所有的条件：都符合规则，允许功能就进行路由：如果检查到数据包的条件不符合规则，阻止功能将会丢弃所有的包。

规则和字段

包过滤使用规则来确定什么样的数据包允许穿过防火墙。一条规则包含若干个字段。特定的执行包括告诉路由器过滤基于下列字段的IP包的内容：

- 源IP地址
- 目的IP地址

- TCP／UDP源端口
- TCP／UDP目的端口

包过滤对于拒绝一些TCP或UDP应用程序的IP地址进入或离开你的网络是很有效的。举个例子，如果想禁止从IntemetTELNET到你的内部网设备中，你需要建立一条包过滤规则。在前面的课程里我们讨论过TCP／IP是如何工作的，并且知道TELNET是使用TCP的23端口。在包过滤中默认是允许所有都可访问，一条禁止TELNET的包过滤规则应该像表8—1一样

规则号	功能	源 IP 地址	目标 IP 地址	源端口	目标端口	协议
1	Discard	*	*	23	*	TCP
2	Discard	*	*	*	23	TCP

上表例出的信息告诉路由器丢弃所有从TCP23端口出去和进来的数据包。星号说明是特定字段里的任何值。在上面的例子中，如果一个数据包通过这条规则时并且源端口为23，那么它将立刻被丢弃。如果一个数据包通过这条规则时并且目的端口为23时，只有规则中的第二条应用时它才会被丢弃。所有其它的数据包都允许通过。

其它一些Intemet服务在一条规则里需要更多的项目。例如，FTP使用TCP的20利21端口。如果包过滤要禁止所有的数据包直到遇到特殊的允许时，就如下表所示

规则号	功能	源 IP 地址	目标 IP 地址	源端口	目标端口	协议
1	Allow	192. 168. 1. 0	*	*	*	TCP
2	Allow	*	192. 168. 1. 0	20	*	TCP

上表中规则的第一条允许内部网络地址为192．168．10．0的网段内源端口和目的端口为任意的主机初始化一个TCP的会活。第—条允许任意端门为20的远程IP地址可以连接内部网络地址为192．168．10．0的任意端口上。规则的第二条不能限制目标端口是因为主动的FTP客户端是不使用20端口的、当—个主动的FTP客户端发起一个FTP会话时，客户端是使用动态分配的端口号叫做瞬间端口(ephemeralport)。而远程的FTP服务器只探查192.168.10.0这个网络内端口为20的设备。有经验的黑客可以利用这些规则访问你网络内的任何资源。

所以更好的FTP包过滤规则应该像下表一样

规则号	功能	源 IP 地址	目标 IP 地址	源端口	目标端口	协议
1	Allow	192. 168. 1. 0	*	*	21	TCP
2	Block	*	192. 168. 1. 0	20	<1024	TCP
3	Allow	*	192. 168. 1. 0	20	*	TCPACK=I

规则第一条允许网络地址为192．16810．0内的任何主机与目标地址为任意且端口为21建立TCP的会话连接。第二条阻止任何源端口为20的远程IP地址访问内部网络地址为192．168．10．0且端口小于1024的任意主机。第三条允许源端口为20的任意远程主机可以访问192．168．10．0网络内主机任意端口。要记住的是这些规则的应用是按照顺序执行的。第三条看上去好像是矛盾的。如果任何包违反第二条规则，它会被立刻丢弃掉，第三条规则不会执行。但第三条规则仍然需要是因为包过滤对所有进来和出去的流量进行过滤直到遇到特

定的允许规则。

包过滤的优点和缺点

包过滤的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应刚层无关。但其弱点也是明显的：据以过滤判别的只有网络层和传输层的有限信息，因而各种安全要求不可能充分满足：在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大地影响：由于缺少上下文关联信息，不能有效地过滤如UDP、RPC一类的协议：另外，大多数过滤器中缺少审计和报警机制，且管理方式和用户界面较差：对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常是和应用网关配合使用，共同组成防火墙系统。

包过滤最大的缺点就是不能分辨哪些是”好”包哪些是”坏”包，因为只涉及到TCP层，所以与代理型防火墙(应用层网关)相比，它提供安全级别很低：不支持用户认证，包中只有来自哪台主机的信息而不包含来自哪个用户的信息：不提供日志功能。另一个问题就是在限制和允许网络访问时有时需要创建超过100条以上的规则，创建这些规则非常消耗时间。

状态多层检测(statefulmulti-layerinspection)

由CheckPoint提出，状态检测模块分析所有的包通讯层，汲取相关的通信和应用程序的状态信息。状态检测模块能够理解并学习各种协议和应用，以支持各种最新的应用。状态检测模块截获、分析并处理所有试图通过防火墙的数据包，保证网络的高度安全和数据完整。

网络和各种应用的通信状态动态存储、更新到动态状态表中，结合预定义好的规则，实现安全策略。状态多层检测最后一个优点就是允许检查OSI七层模型的所有层以决定是否过滤，而不仅仅是网络层。目前很多公司在它们的包过滤防火墙中都使用状态多层检测。

现在一些流行的包过滤产品有

CheckPoint防火墙(www．checkpoint．com)

Cisco PiX 防火墙(WWW．Cisco．com)

Winrout 防火墙(www．winroute．com)

代理服器

代理技术与包过滤技术完全不同，包过滤技术是在网络层拦截所有的信息流，代理技术是针对每一个特定应刚都有一一个程序。代理是企图在应用层实现防火墙的功能，代理的主要特点是有状态性。代理能提供部分与传输方面的信息，代理也能处理利管理信息。通过代理使得网络管理员实现比包过滤路由器更严格的安全策略。

代理的概念对于防火墙应刚是非常重要的，因为代理把网络IP地址替换成其它的暂时的地址。这种执行对于互联网来说有效地隐藏了真正的网络IP地址，因此保护了整个网络。

代理行几个用处，由于是当黑客开始活动的时候。见左图黑客所做的第一件事就是侦查你的网络上的弱点。通常都是利用端口扫描。为了防止这第一步，你需要尽可能地隐蔽内部系统的配置信息暴露给潜在的攻击者。代

理可以使你隐藏这些信息，并能提供有效的通信。

代理主要有三种基本类型：WEB代理、电路级网关，应用级网关。

WEB代理

WEB代理服务的最人好处就是能提高访问Internet的速度：一旦一个WEB代理服务器配置了足够的缓存，它就可以从这些缓存里对请求提供服务。而WEB代理客户端则可以得到很快速的响应。WEB代理第二个好处是WEB代理使客户端无需正接连接Internet，所以远离成为被攻击的目标。

电路级网关

电路级网关用来监控受信任的客户或服务器与不受信任的主机间的TCP握手信息，这样来决定该会话(session)是否合法。我们知道，要使用TCP协议，首先必须通过三次握手建立TCP连接，然后才开始发送数据。电路级网关通过在TCP握手过程中，检查双方的SYN、ACK和序列数据是否合理逻辑，来判断该请求的会话是否合法。一旦该网关认为会话是合法的，就会为双方建立连接，自此，网关仅复制、传递数据，而不进行过滤。电路级网关通常需要依靠特殊的应用程序来进行复制传递数据的服务。实际上，电路级网关并非作为一个独立的产品存在，它与其他的应用级网关结合在一起，所以有人也把电路级网关门为应用级网关。电路级网关是在OSI模型中会话层上来过滤数据包。也因为如此，它就无法检查应用层级的数据包。最流行的电路级网关是IBM发明的SOCKS网关。很多产品，包括微软的Microsfot ProxyServer就支持SOCKS。

优点和缺点

电路级网关的主要优点就是提供NAT，在使用内部网络地址机制时为网络管理员实现安全提供了很大的灵活性。电路级网关是基于和包过滤防火墙一样的规则。电路级网关提供包过滤提供的所有优点但却没有包过滤的缺点。

缺点为不能很好地区别好包与坏包、易受IP欺骗这类的攻击及复杂性这些都是电路级网关的弱点。电路级网关又一个主要的缺点是需要修改应用程序和执行程序。还有电路级网关要求终端用户通过网关的认证。

应用级网关

应用级网关可以工作在OIS七层模刑的任一层上来检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级网关能够理解应用层上的协议，能够做复杂一些的访问控制，并做精细的注册。但每一种协议需要相应的代理软件，使用时工作量大，效率不如网络级防火墙。常用的应用级防火墙已有了相应的代理服务器， 例如： HTTP、 NNTP、 FTP、Telnet、rlogin、X—Window等，但是，对于新开发的应用，尚没有相应的代理服务，它们将通过网络级防火墙和一般的代理服务。应用级网关有较好的访问控制，是目前最安全的防火墙技术，但实现困难，而且有的应用级网关缺乏“透明度”。在实际使用中，用户在受信任的网络上通过防火墙访问Internet时，经常会发现存在延迟并且必须进行多次登录(Login)才能访问Internet或Intranet。推荐的一些代理防火墙产品有AxentRaptor防火墙(http：／／www,axent．com)和微软MicrosoftProxyServer。

代理服务器的优点

代理服务器的主要优点就是提供NAT的功能，并且对于公网能隐藏你的内部网络也是极为重要的。以下是其它一些额外的好处：

日志和警报：比包过滤和电路级网关提供的日志和警报更全面更坚固。代理服务器与其它两种类刑的防火墙相比分析更的数据包信息，因此几乎可以记录TCP／IP会话的每个部分，从网络桢到应用层。

缓存：因为代理服务器需要对TCP／IP的每一层数据包分析，所以代理服务器经常把这些信息缓存到磁盘上。对所有相同数据的请求会直接从代理服务器的上的硬盘访问而不是远程的服务器，这样可以大大地提高访问速度。代理服务器i可以应用多条规则来配置多久检查一下远程站点的内容更新。 ·

应用程序分析：从前面的讨论中，大家了解了代理服务器可以分析应用程序上的TCP／IP数据流。这里有些这些特性是如何使用的。然而，下列这些特点不是在所有的代理服务器都生效的

- SMTP流量可以用于检查特洛伊木马和病毒
- 可以监视特定的HTTP和NNTP流量来拒绝相关内容
- 特定的域名来拒绝访问整个域

反向代理和代理距阵：使用应用级网关的另外一个好处就是可以提供反向代理服务。这些服务像是单独工作的，除了代理进来的请求。反向代理位于网络防火墙的外边并在Internet上注册作为公司的产品服务器，如WEB服务器或Email服务器。当公共用户访问WEB服务器时实际上访问的是代理服务器，然后由代理服务器于在防火墙内的WEB服务器联系。这样有效防止公共用户直接访问WEB服务器。如果一个黑客企图进入WEB服务器，其实他只能进入代理服务器而已。代理服务器不含有WEB服务器真止的数据，所以进入代理服务器不能得到任何有用的信息。

代理距阵是几个代理服务器配置在一起作为一个使用。代理距阵是代理的聚集并提供负载均衡。当几个反向代理服务器一起使用时，使用整个流量的缓存增加。如果一旦某个代理崩溃还能起到容错的功能。某些代理距阵还可以作为一个单独的单元。举个例子，根据代理服务器在距阵中的配置，在一个上面作的设置需要在所有的代理上做设置。代理距阵还经常任反向代理的环境中使用。当代理距阵用于反向代理解决方案时，公共用户可以同时访问几个WEB服务器。

少量的规则：面向代理的防火墙通常需要比包过滤要少的规则。而且创建这些规则一般只需很少的时间。

代理服务器(应用级网关)

应用级网关的一个缺点是要为TCP／IP应用程序创建过滤。每一个应用程序都要单独配置。很多应用程序都可以在TCP之上使用，防火墙管理员需要对所有的应用程序都很了解并要为每个应用单独配置来创建安全过滤。在某些情况下，需要特定的代理服务器对一个单独的应用程序代理。还有，你还必须配置不同的应用程序和操作系统协同应用级网关工作。

客户端配置

客户端通过代理服务器与远端进行TCP／IP连接时必须使用代理而且指定所有正确的参数。如果内部用户想通过不同的客户端应用程序访问Intemet程序(如浏览器，mail客户端，新闻客户端，FTP客户端及聊天程序等)，第一个应用程序都必须配置使用代理服务器来进行远程访问。经常不是所有的Intemet应用程序都能正确地通过代理服务器访问。

新的应用程序和病毒

当开发出新的应用程序时，这个应用程序的编写要能通过代理服务器访问远程客户端。商业版的代理服务器通常和目前的Intemet程序兼容。然而，当开发出新的应用程序时，你需要联系厂商来升级代理服务器以兼容这个新的应用程序。同样这也需要应用到病毒程序上，在建立你的代理服务当中，可能会配置防止目前多数的病毒。如果防火墙不关心一个新病毒，那可能不知不觉中允许信息穿过代理服务器或从内部客户端出去。如果你的代理服务器用于扫描病毒，那么一定要确保是使用目前最新的病毒防护文件。

速度

因为面向代理的防火墙对于IP包钻研的很深，它们需要更多的系统资源。在非常繁忙的站点上，基于代理的防火墙成为一个累赘，因为它可以导致不期望的延迟。一般推荐使用面问代理的防火墙要使用T—3的速度。

防火墙的一些高级特性

今天多数的防火墙系统组合包过滤，电路级网关和应用级网关的功能。它们检查单独的数据包或整个信息包，然后利用事先订制的规则来强制安全策略。只有那些可按受的数据包才能进出整个网络。当你实施一个防火墙策略时，这三种防火墙类型可能都需要。更高级的防火墙提供额外的功能可以增强你的网络的安全性。尽管不是必需，每个防火墙都应该实施日志记录，哪怕是一些最基本的。

认　证

防火墙是一个合理的放置提供认证方法来避开特定的IP包。你可以要求一个防火墙令牌(firewall token)，或反向查询一个1P地址：反向查询可以检查用户是否真正第来自它所报告的源位置。这种技术有效地反击IP欺骗的攻击：防火墙还允许终端用户认证。应用级网关或代理服务器可以工作在TCP／IP四层的每一层上。多数的代理服务器提供完整的用户帐号数据库。结合使用这些用户帐号数据库和代理服务器门定义的选项来进行认证。代理服务器还可以利用这些帐号数据库来提供更详细的日志：

日志和警报

包过滤或筛选路由器一般在默认情况下为了不降低性能是不进行日志记录的。永远不要认为你的防火墙会自动地对所有活动创建日志。筛选路由器只能记录一些最基本的信息，而电路级网关也只能记录相同的信息但除些之外还包括任何NAT解秆信息。因为你要在防火墙上创建一个阻塞点，潜在的黑客必须要先穿过它：如果你放置全面记录日志的设备并在防火墙本身实现这种技术，那么你有可能捕获剑所有用户的活动包括那些黑客。你可以确切地知道黑客在做些什么并得到这些活动信息代审计。一些防火墙允许你预先配置对不期望的活动做何响应。防火墙两种最普通的活动是中断TCP／IP连接或自动发出警告。相关的警报机制包括可见利可听到的警告。

远程访问和虚拟专用网(VPN)

一些防火墙现在已经提供虚拟专用网络服务(VPN)：VPN址通过公共介质如Internet扩展公司的网络。因为任何访问公共介质的人都要以偷听传输在网络上的数据，因此在VPN下传输的数据都是加密的。VPN把所有加密后数据封装到一个IP包里。因为这个数据包含有有效的IP利TCP信息，可以通过Internet路由出去。

远程访问

VPN不局限于局域网或网络到网络的连接。使用VPN主要的原因是可以往拔号客户端和你的网络间建立安全的连接。WindowsNT通过VPN支持标准的RAS连接。特殊的路由器和(或)防火墙可以配置在Internet上建立VPN：例如，Cisc01720VPN访问路由器允许公司访问Internet并和其他1720 VPN访问路由器活其它兼容设备建立VPN连接。这种特殊的路由器利用专用的VPN协议创建一条隧道。这种专有的技术经常投入到公司的特殊硬件中。

对于VPN的解决方案期待着一种标准化的新型协议。IPSec是这样协议的一种。

本章小结：

正确了解有关防火墙相关的术语对大家进一步的学习是有很大帮助的，本章对些作了详细的介绍，并描述常见的包过滤、代理服务器、VPN的类型及其原理。

问题讨论：

／ 什么是包过滤，其优点和缺点?

／ 代理服务器的分类，各自的优点和缺点?

／ DMZ的功能及划分

／ 防火墙的高级特性有哪些

第八章

防火墙体系结构

引　　言

一个适当的网络安全最重要的特点就是公司的防火墙策略。第一步就是要开发这样一个策略来建立具有合适的硬件和软件配置的防火墙设备。设计和配置一个防火墙一定要很好地适合你公司的需要，你要对一些基本的概念非常熟悉。

本章要点：

- 结合几种不同级的保护来策划一个防火墙系统
- 描述四种类型的防火墙系统设计及它们的安全级别
- 实施一个包过滤防火墙
- 在Linux下使用ipchains来实现包过滤

防火墙策略和目的

一旦你根据需要对所有的资源进行详细记录和分类，然后定义了一个安全策略后，你要准备放置你的资源。资源的放置对于保护你的资产是有着非常大的影响的。防火墙最重要的特点是创建阻塞点。只有少量的物理点允许从Intemet访问你的资源，而且容易控制。Internet站点的安全在很多方面要比内部网络安全容易，因为它允许你创建少数的阻塞点。

通过让进入的信息流进入最小数量的“ 点 ”，你可以浓缩你的保护机制。这种焦点允许你

花最少的努力却获得更多的安全，因为你确切地知道信息流从哪里进入和离开你的系统的。这种更全面更广泛的监视，工具将在阻塞点上配置。在很多方面，放置就是指资源问题，主要是因为如果你对系统没有正确的配置，你就需要更多的硬件来达到需要的保护级别。因为购买和维扩这些设备的代价是非常昂贵的，你必须花些的间来精确地计划如何放置你的资源。

建立一个防火墙

在准备和建立一个防火墙设备时要高度重视。以前，堡垒主机这个术语是指所有打接连入公网的设备。现在，它经常汲及到的是防火墙设备。堡垒主机可以是三种防火墙中的任一种类型：包过滤，电路级网关，应用级网关。

当建设你的堡垒主机时要特别小心。堡垒主机的定义就是可公共访问的设备。当Internet用户企图访问你网络上的资源时，首先进入的机器就是堡垒主机。因为堡垒主机是直接连接到Intemet上的，其上面的所有信息都暴露在公网之上。这种高度地暴露规定了硬件和软件的配置。堡垒主机就好像是在军事基地上的警卫一样。警卫必须检查每个人的身份来确定他们是否可以进入基地及可以访问基地中的什么地方。警卫还经常准备好强制阻止进入。同样地，堡垒主机必须检亦所有进入的流量开强制执行住安全策略里所指定的规则。它们还必须准备好对付从外部来的攻击和可能来自内部的资源。堡垒主机还有日志记录及警报的特性来阻止攻击。有时检测到一个威胁时也会采取行动。

设计规则

当构造防火墙设备时，经常要遵循下面两个主要的概念。第一，保持设计的简单性。第二，要计划好一旦防火墙被渗透应该怎么办。

保持设计的简单性

一个黑客渗透系统最常见的方法就是利用安装在堡垒主机上不注意的组件。建立你的堡垒主机时要尽可能使用较小的组件，无论硬件，还是软件。堡垒主机的建立只需提供防火墙功能。在防火墙主机上不要安装像WEB服务的应用程序服务。要删除堡垒主机上所有不必需的服务或守护进程。在堡垒主机上运行少量的服务给潜在的黑客很少的机会穿过防火墙。

安排事故计划

如果你已设计好你的防火墙性能，只有通过你的防火墙才能允许公共访问你的网络。当设计防火墙时安全管理员要对防火墙主机崩溃或危及的情况作出计划。如果你仅仅是用一个防火墙殴备把内部网络和公网隔离开，那么黑客渗透进你的防火墙后就会对你内部的网络有着完全访问的权限。为了防止这种渗透，要设计几种不同级别的防火墙设备。不要依赖一个单独的防火墙保护准独的网络。如果你的安全受到损害，那你的安全策略要确定该做些什么。采取一些特殊的步骤，包括

- 创建同样的软件备份
- 配置同样的系统并存储到安全的地方
- 确保所有需要安装到防火墙上的软件都容易，这包括你要有恢复磁盘。

堡垒主机的类型

当创建堡垒主机时，要记住，占是在防火墙策略中起什用的。识别堡垒主机的任务可以帮助你决定需要什么和如何配置这些没备。下面将讨论三种常见的堡垒主机类型。这些类型

不是单独存在的，且多数防火墙都属于这三类中的一种。

单宿主堡垒主机

单宿主堡垒主机是有一块网卡的防火墙设备。单宿主堡垒主机通常是用于应用级网关防火墙。外部路由器配置把所有进来的数据发送到堡垒主机上，并且所有内部客户端配置成所有出去的数据都发送到这台堡垒主机上。然后堡垒主机以安全方针作为依据检验这些数据。

这种类型的防火墙主要的缺点就是可以重配置路由器使信息直接进入内部网络，而完全绕过堡垒主机。还有，用户可以重新配置他们的机器绕过堡垒主机把信息直接发送到路由器上。

双宿主堡垒主机

双宿主堡垒主机结构是围绕着至少具有两块网卡的双宿主主机而构成的。双宿主主机内外的网络均可与双宿主主机实施通信，但内外网络之间不可直接通信，内外部网络之间的数据流被双宿主主机完全切断。双宿主主机可以通过代理或让用户直接注册到其上来提供很高程度的网络控制。它采用主机取代路由器执行安全控制功能，故类似于包过滤防火墙。双宿主机即一台配有多个网络接口的主机，它可以用来在内部网络和外部网络之间进行寻址。当一个黑客想要访问你内部设备时，他(她)必须先要攻破双宿主堡垒主机，这有希望让你有足够的时间阻止这种安全侵入和作出反应。

单目的堡垒主机

单目的堡垒主机既可是单堡垒也可是多堡垒主机。经常，根据公司的改变，需要新的应用程序和技术。很多时候这些新的技术不能被测试并成为主要的安全突破口。你要为这些需要创建特定的堡垒主机。在上面安装未测试过的应用程序和服务不要危及到你的防火墙设备。使用单日的堡垒主机允许你强制执行更严格的安全机制。举个例子，你的公司可能决定实施一个新类型的流程序，假设公司的安全策略需要所有进出的流量都要通过一个代理服务器送出，你要为这个表的流程序单独地创建一个新代理服务器。在这个新的代理服务器上，你要实施用户认证和拒绝IP地址。使用这个单独的代理服务器，不要危害到当前的安全配置并且你可以实施更严格的安全机制如认证。

内部堡垒主机

内部堡垒主机是标准的单堡垒或多堡垒主机存在于公司的内部网络中。它们一般用作应用级网关接收所有从外部堡垒主机进来的流量。当外部防火墙设备受到损害时提供额外的安全级别。所有内部网络设备都要配置成通过内部堡垒主机通信，这样当外部堡垒主机受到损害时不会造成影响。

硬件采购问题

管理员在决定什么样的防火墙硬件产品常犯的错误就是购买市场的最大型的最快速的机器。这种想法以为是快速的机器可以较快地处理进出的流量，然而通常这种假设是错误的。

堡垒主机提供的功能并不复杂而且也不需要功能强大的机器。大多数的防火墙实施只需小功率的机器就已足够并能节省资金。堡垒主机可以安装在简单硬件配置之上。堡垒主机运行在的操作系统通常说明了最小硬件的需求。当选择硬件时，可仅使用一些测试过的普通硬件。经常是在一些新的技术在产品环境中被提出并测试时，会发些一些新的安全突破口。

使用较小功率的硬件还有其它几个优点。如果你的防火墙遭到破坏并且黑客在上面安装

了工具或服务以便进一步渗透你的网络，较小功率的计算机可以使这种执行变得缓慢，让你有足够的时间来对付入侵。同样，如果一个黑客发现防火墙是安装到一个超级计算机上，那么它将比标准的计算机更有可能成为对黑客具有吸引力的目标。

购买多快速的处理器和多大的内存将会影响到堡垒主机的任务。举个例子，如果一个堡垒主机要运行一个应用网关服务，就要为这个应用网关实现缓存功能面安装一个人容量的硬盘。所有的堡垒主机都会从相当大容量的内存中获益。虽然不需要快速的处理器来分析进出的流量，但跟踪大量的同步连接是需要更多的内存的。你还必须备份你的堡垒主机：就配置成使用其自己的磁带备份设备。如果你的公司有一个网络备份策略，需要一个帐号和能够从磁带备份服务器上直接访问堡垒主机。这些帐号可以危及到堡垒主机或备份服务器的安全。实行堡垒主机的本地备份可排除这些问题。

操作系统、服务和守护进程

以你计划使用防火墙的类型而定，它可能作为一个应用程序来运行，而不是作为一个物理设备，通常包过滤防火墙是运行在路由器上，你必须使用有它们自己特性的操作系统，使用这种流行的路由器是较好的第一道防线，而且大多数配置过程是在路由器上创建相应的过滤。然而，如果你打算在一台计算机上安装防火墙应用程序，你需要一个操作系统，最关键的问题是你要选择一个你最熟悉的操作系统，如果你是一个Solars管理员你就不能选择Windows NT作为堡垒主机的操作系统，选择一个操作系统可以帮助你减少对于熟悉一个新的防火墙产品需要的时间，这样的选择将减少配置错误的可能性。另一个因素是决定在你公司的网络中一个操作系统上需要哪些服务，如果你的公司需要一个应用程序服务器，能够过滤NNTP，HTPP和SMTT流量，操作系统必须能够使这些服务的使用变得容易。举个例子，你可能精通微软的Windows95,但是Windows95不支持应用程序网关产品，也不支持所有常见的Intemet应用协议。操作系统应该支持多任务和同时多连接。如果你建立一个堡垒主机，但没有一个更喜欢的操作系统，UNIX是一个合理的选择，因为它被使用和被测试了25年，并且被广泛支持，决定使用什么样版本的UNIX也要考虑。要选择一个已经在Intemet上测试过并广泛使用过的版本，不要选择一个新的版本或没有被严格测试过的版本。

你要保证每一个单独的堡垒主机的安全性。举个例子，要安全保护防火墙应用程序，操作系统和其他一些服务，如Telnet，FTT等等。每种系统都有它们自己特殊的漏洞，一定要把它们单独的隔开。当你安装一个操作系统的时候，默认地安装了许多服务或进程。举个例子，大多数版本的UNIX默认情况下都安装Telnet进程。所有不必需的服务都应该禁±下后删除。简单的禁止这些服务不能确保它们以后不会重新允许使用，例如，Windows NT的Scheduler是以管理员权限运行的，由于这个原因许多管理员禁止使用Scheduler服务，然而禁止这个服务并没有删除它，潜在的允许一个黑客访问NT服务器并重新加载这个服务，删除这个服务使得黑客重新安装并使用它们变得非常困难。

你还要尽可能的删除操作系统上的一些应用程序。例如，在一个UNIX系统上你要删除许多用于系统管理的程序，如rm，chmod等等。这些程序允许一个黑客取得root级别的访问，并配置你的防火墙导致非常严重的危害，防火墙设备另一个重要的配置(尤其是应用程序网关)是删除IP路由，如果允许了IP路由，堡垒主机可能会不首先检查数据包是否遵守安全定义，而自动的路由这些数据包。如果你删除了IP路由，堡垒主机必须使用防火墙组件路由或代理进出的流量。删除一些不必要的服务，进程或应用程序是创建一个安全的堡垒主机最基本的步骤。不幸的是这些步骤经常被忽略，删除应用程序看上去好象是多余的，但是记住堡垒主机是黑客进入网络并企图渗透的第一个设备，通过删除所有这些组仆可以使黑客的行动更加困难。

防火墙设计

现在你已经对如何安全地建立防火墙有了很好的认识，下面将学习如何实施一个防火墙策略。设计一个安全防火墙策略的第一步是保证防火墙本身的物理安全性，这一点是很明显的。如果你不把防火墙和产品服务器放到一个安全的位置，任何设备可能都会遭到破坏。整个网络的瘫痪可能是因为一个清洁工在半夜为了省电而关掉了服务器。多数设备允许在物理程序下进行管理或root级访问，举个例子，可以从一张特殊的软盘来引导服务器，或通过一个标准串口连接路由器。这些威胁不能完全从这些设备上删除，这就是需要把设备放到一个安全的物理位置的原因。

四种常见的防火墙设计都提供一个确定的安全级别，一个简单的规则是越敏感的数据就要采取越广泛的防火墙策略，这四种防火墙的实施都是建立一个过滤的距阵和能够执行和保护信息的点。这四种选择是：

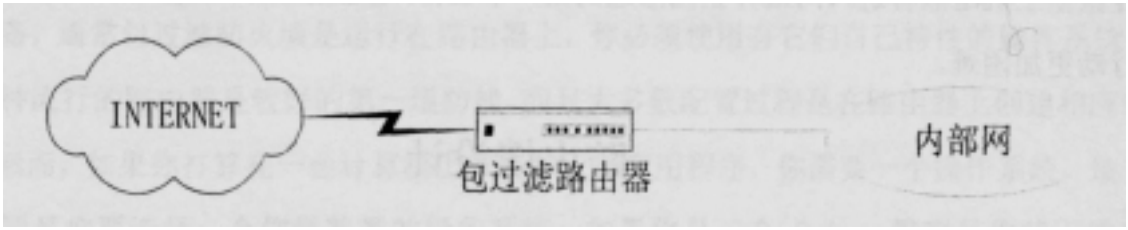
- 筛选路由器
- 单宿主堡垒主机
- 双宿主堡垒主机
- 屏蔽子网

筛选路由器的选择是最简单的，因此也是最常见的，大多数公司至少使用一个筛选路由器作为解决方案，因为所有需要的硬件已经投入使用。用于创建筛选主机防火墙的两个选择是单宿主堡垒主机和双宿主堡垒主机。不管是电路级还是应用级网关的配置都要求所有的流量通过堡垒主机。最后一个常用的方法是筛选子网防火墙，利用额外的包过滤路由器来达到另一个安全的级别。

筛选路由器

筛选路由器被认为是最好的第一道防线。因为筛选路由器就是实施过滤的路由器，所有需要的硬件已放在适当的位置上。你前面学到的筛选路由器可以根据IP地址和TCP以及UDP端口拒绝所有进出的流量。筛选路由器应遵守安全策略，配置路由可接受的数据流量，筛选路由器擅长拒绝IP地址或网络地址范围还有过滤不想要的TCP＼IP应用程序。

如下图9-1显示了包过滤器的图表，它并不昂贵，但仍能提供重要的保护。

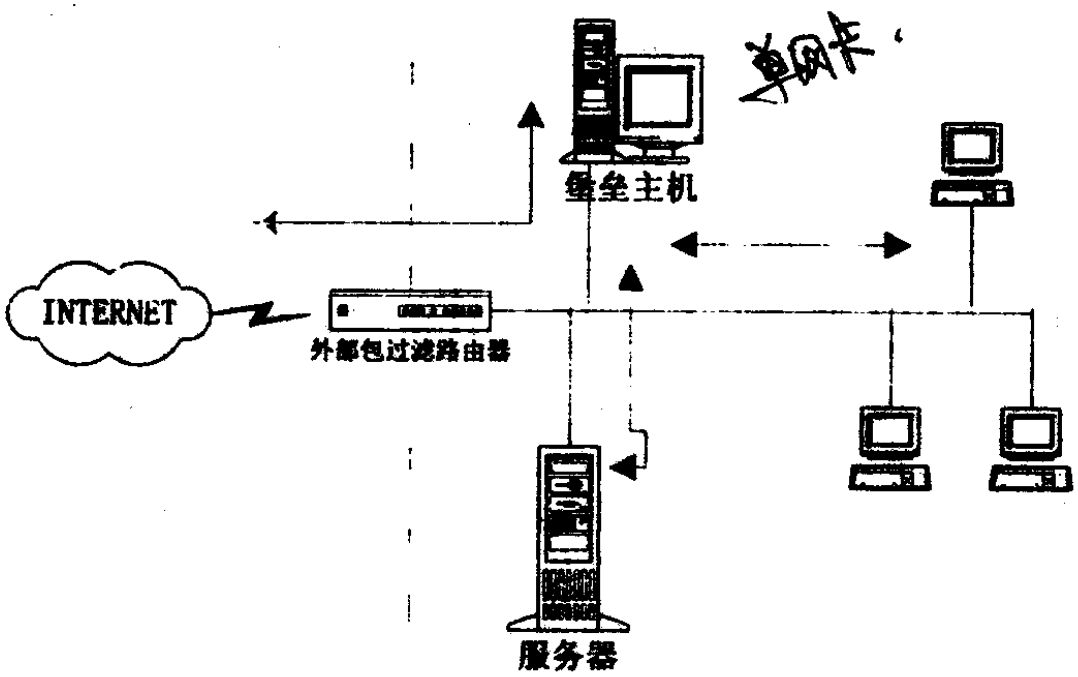


仅使用一个筛选路由器作为解决方案有几个缺点，主要一个就是创建相应的过滤需要对TCP／IP有很丰富的知识要求，筛选路由器仅仅依靠使用这些过滤规则并且一旦有任何错误的配置将会导致不期望的流量通过或拒绝一些可接受的流量。另一个缺点是只有一个单独的设备用来保护你的网络。如果一个黑客可以损害到这个筛选路由器它将能访问你网络中的任何资源。另外，筛选路由器不隐藏你内部网络的配置，任何可能访问筛选路由器的人都能轻松地看到你的网络布局和结构。筛选路由器还没有较好的监视或日志功能。如果一个筛选路由器接收到没被其过滤规则的流量，对这些流量它不能提供什么有用的信息，还有筛选路由器通常没有警报的功能，如果一个安全侵犯发生，对于这种潜在的威胁筛选路由器不能通知安全管理员。

第二种流行的防火墙类型(除了筛选路由器)是使用单宿主堡垒主机的筛选主机防火墙。

单宿主堡垒主机可以配置成电路级网关或应用级网关，当使用这两种类型的任一种作为代理服务器时，堡垒主机可以隐藏内部网络的配置信息。单堡垒主机利用网络地址解释来提供这种功能。使用NAT允许网络管理员利用内部IP地址方案。

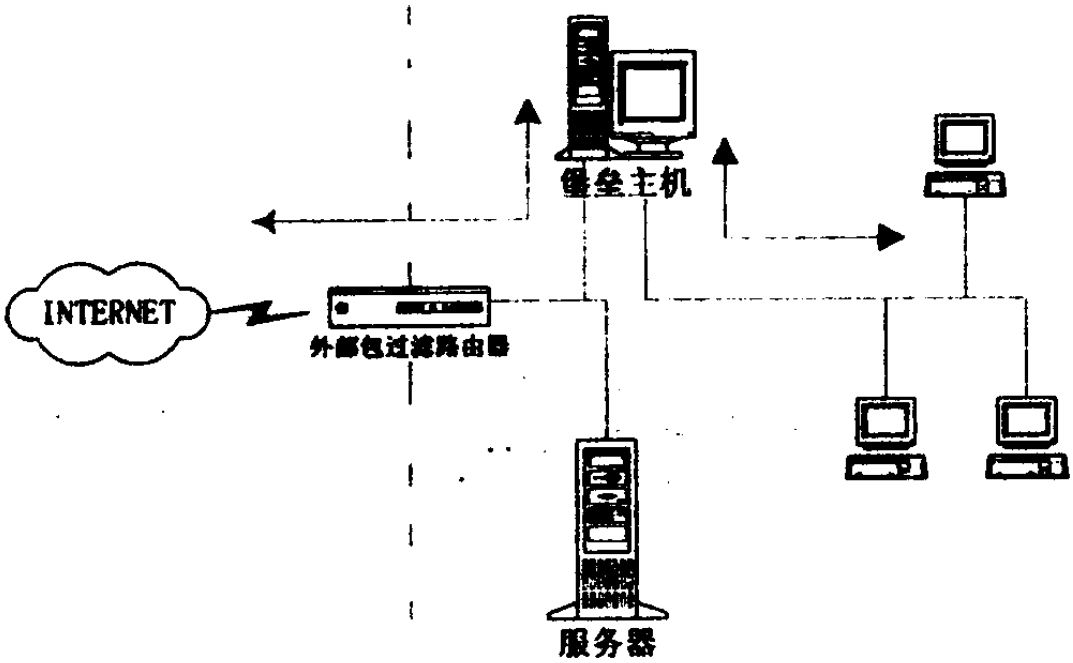
屏蔽主机防火墙是针对所有进出的信息都要经过堡垒主机而设计的。筛选路由器配置成把所有进来的流量路由到堡垒主机上。这种路由允许堡垒主机在把流量代理到内部网络前对所有的流量进行分析。筛选路由器还可以配置路由仅从堡垒主机出去的流量，这种方式配置路由器不允许内部节点重新配置它们的机器绕过堡垒主机。通过仅接受从堡垒主机送出的流量，内部主机必须符合代理服务器所作的限制。堡垒主机配置成拒绝不能接受的流量和代理可按受的流量。单宿主堡垒主机下图所示



这种实施在某些方面要比包过滤防火墙高级。首先，它添加了堡垒主机既可做为电路级网关也可做为应用级网关。还有，堡垒主机本身是由一个安全的设备构成对于一个黑客想要侵入路由器造成足够的难度。现在，黑客不仅必须攻破路由器还要攻破一个不是为了接受登陆请求的隔离的计算机。有了屏蔽主机防火墙，给黑客的破坏带来了加倍地难度。与包过滤比较，这种方法的缺点是增加了成本并降低了性能。因为堡垒主机处理信息时，网络经常需要更多的时间来对用户的请求作出响应。一些类型的堡垒主机还能使用用户访问Intemet变得困难。如果堡垒主机只作为电路级网关，内部主机将不会受到影响。然而，如果堡垒主机服务器作为应用级网关，内部客户端必须被配置成使用应用网关服务。还有，不是所有TCP／IP应用程序都可以通过一个应用级网关工作的。

屏蔽主机防火墙(双宿主堡垒)

这种不同于前面的筛选主机防火墙利用一台双宿主堡垒主机增加了更有效的安全性。如图所示



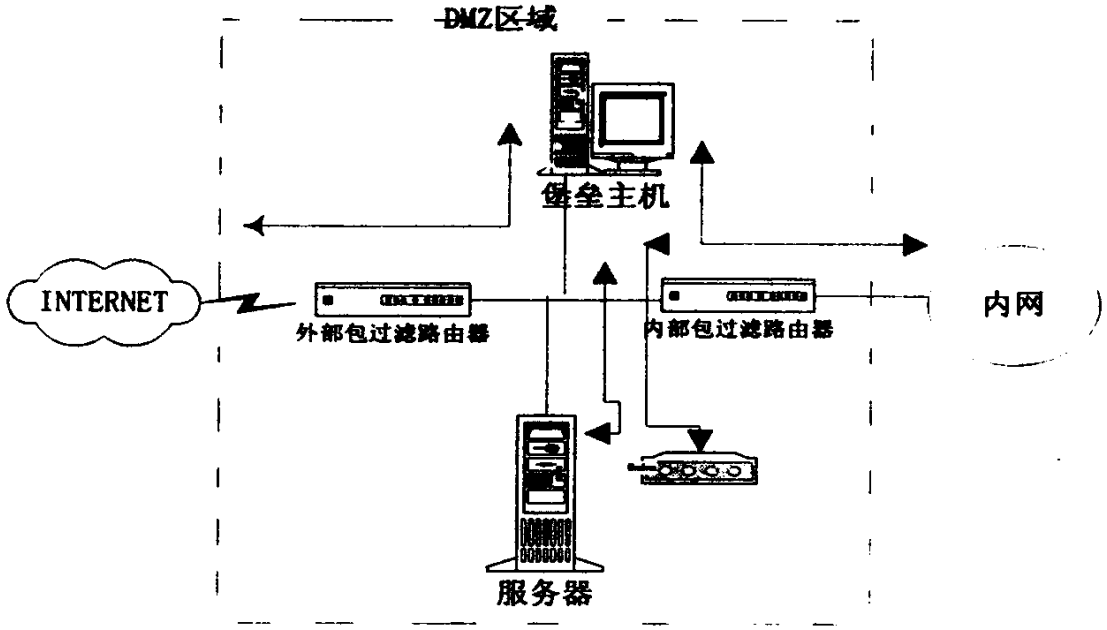
一个双宿主堡垒主机是有一个有着两块网卡的计算机。这种防火墙实施是安全的因为它在你内部网络和外部网络(如Intemet)间创建了一个完全的物理隔断。在单宿主堡垒主机结构上，所有外部的流量直接转发到堡垒主机上执行。然后这种实施，黑客必须攻破堡垒主机利路由器来绕过这种保护机制。

单宿主堡垒主机防火墙的实施仍可能允许黑客来修改路由器而不把数据包转发给堡垒主机，这种活动可能会绕过堡垒主机并且允许黑客直接进入到网络当中。但这种绕过通常不会发生，因为使用单宿主堡垒主机的网络经常配置成把数据包发送到堡垒主机上，而不是直接接发到Internet上。因此一个黑客要绕过单宿主堡垒主机防火墙适当地配置，他(她)必须重新配置整个网络来绕过防火墙。

然而双宿主堡垒主机几乎不会发生这种情况。进而，如果一个黑客可以攻破筛选路由器或双宿主堡垒主机，他(她)可能还不得不渗透其它类型的防火墙实施，这种过程是非常之慢的。双宿主堡垒主机还允许网络管理员实施网络地址解释。

屏蔽子网防火墙

实施防火墙最常见的方法就是屏蔽子网。它在内部网络和外部网络之间建立一个子网，称之为边界网络(PerimeterNetwork)，也称为非军事区DMZ。它是四种防火墙类型中最安全的一种，主要是因为它利用一台既支持电路级网关也支持应用级网关的堡垒主机定义一个非军事区。在这种配置下，所有的公共访问设备，包括modempool和其它类似的资源，被放在这个区域中。DMZ是在Intemet和内部网之间的小型的独立的网络。从下图中可以看出，这种配置使用了外部筛选路由器和内部筛选路由器，而且每个上面都配置成流量通过堡垒主机。



这种布置阻止了任何直接流入子网或DMZ的流量。外部筛选路由器使用标准过滤和拒绝外部对堡垒主机的访问，这种路由器还使用过滤来防止类似IP spoofing的攻击。内部筛选路由器作为第三道防线，利用规则来阻止spoofing和soucerouting，像外部路由器一样，这个路由器拒绝所有不是从堡垒主机进来的流量，并且只向外发送经过堡垒主机的流站。

使用这种方案的主要好处，一个是黑客想要访问你的网络必须攻破这三个单独的设备而不被发现。第一·个好处是内部网对Internet来说是有效地不可见的，因为所有进出的数据包都会直接送到DMZ，而不是你的网络。这样布置使黑客想得到你内部系统的信息几乎不太可能。第二就是，因为路由信息包含网络信息，内部用户不通过堡垒主机则不能访问Internet。任何直接从内部网络发出的数据都不能转发到Internet上，因为在Internet上不存在这样的路由表。这种配置避免了内部用户绕过你的安全机制。在这种情形一下你需要使用一台双宿主堡垒主机，因为路由器确保流量只能通过堡垒主机。

使用中chsins构建Linux-V的防火墙

对一个系统管理员来说，在网络环境里，保护系统与用产免受入侵者的破坏是一件非常重要的事，疏忽的系统管理会给这些入侵者许多攻击的目标。网络上的防火墙能够将你的私有区域网络隔离，并保护你的系统免受外界网络世界的干扰。Ipchains是Linux系统中比较出名的防火墙，它属于一种数据包过滤防火墙。使用ipchains能够达到较好的保护你的系统免受外界网络世界的干扰的效果。

Ipchains的基本设定

首先，要使用Ipchains，你必须先将你的Linux系统核心更改为可支持数据包过滤的版本。你可以检查系统里的／proc／net／ip_fwchains这个文件是否存在，若是有的话，你的系统核心已经支持数据包过滤的功能了。若是没有，请在核心配置文件中加上：

CONFIG _FIREWALL=y

CONFIG _IP_ FIREWALL=y

两个选项后重新编译你的系统核心。

有关lpchains的详细使用设定请参阅后面。这里先说明基本的操作。在用开始系统缺省的情况下会有二个内建的chains：input、output、forward分别处理出入及传送的规则。
lpchains的基本操作如下：
1．建立新的chain：ipchains-N chain
2．删除不要的chain：ipchains-X chain
3．改变chain的polich：ipchains-P chain policy
4少 ¨ i矽1有chain的rule：ipchains-L [chain]
5．删除chain的所有rule：ipchains-F [chain]
6．将chain的计数器归零：ipchains-Z [chain]
以上[chain]若未指定的话就表示所有的chains
更改chains的规则：
1．增加一条新规则：ipchains –A chain
2．删除第一个比对符合的规则：ipchians –D chain
3．删除某个位置号码的规则：ipchains –D chain rulenum
4．在某个位置号码插入一条新的规则：ipchains –I chain [rulenum]
5．更改某个位冒号码的规则：ipchains –R chain [rulenum]
以㈠内位首号码足规则比对的顺宁(优先序)，通常不加代表1(最优先)

Ipchains的详细使用说明

下列是ipchains用来新增及处理数据包比对规则的用法：
ipchains -[ADC] chainrule-specification[options]
ipchains-[RI] chainrulenumrule-specification[options]
—A，--append
增加一条或数条规则在指定的chain最后面。当来源或目的名称对应至数个地址时也会加上每个可能地址。
-D，--delete
从指定的chain开始删除一条或数条规则。可以是规则在chain中的位置号码或者是一条用来比对的规则。
-C，--check
用来测试符合指定规则类型的数据包是否通过系统现在的规则。
下列是关于设定一条规则可用的参数：
-P，protocol[！] protocol
这条规则要检查的协议，可以是tcp，udp，icmp或是a11，也可以代表某个协议的数字或是名称。在协议前加上“！”符号就是做否定的检查。数字0是代表a11。
—S，—source[!]address[／mask][！][port[：port]]
这个参数用来指定数据包的来源，Address可以是网络上的名称或是IP地址。mask就是来源网络的掩码。后面可以加上来源的端口号码(IP数据包)或是ICMP的种类(ICMP数据包)。可以用数字或服务名称表示port或者可以用ipchains-h icmp米察看可以表示的ICMP种类。
—source –port[!] [port[：port]]
用来单独指定来源port
-d，destination[!]address[／mask][!][port[：port]]
目的的地址(设定类似来源)
—-destination-port[!][port[：port]]
用来单独指定目的port

—icmp-type[!]typename
用来单独表示ICMP的种类
-j ,--jump target
用来指定这条规则的目标。也就是比对符合这条规则后要做的事。目标可以是另一个chain(再比对一次)，或一个特别的目标chain。
-i，interface[!]name
用来指出用来接收或送出数据包的网络界面名称。如果不设定本项时，是表示所有的网络界面。如果界面名称后面加上一个“ + ”号，则代表所有由这个名称开头的网络界面。
[!]-f，--fragment
这代表这条规则只会参考到数据包的第二或是更后面的部分，如果该数据包是分割成奸几部分时。由于这就无法分辨出数据包的来源或目的端口，因此只要是规则中有包含指定端口或类刑的，这个数据包都会比对失败。
-b，--bidirectional
双向模式，这个规则会对IP数据包做双向的比对。这就跟直接设两条只有来源和目的的互相对调其余都相同的规则是一样的效果。
-V，--verbose
详细的输出。设定这个参数可让list命令显示网络界面地址，规则选项，选项以及TOS遮码。数据包及人小计数器的内容也会显示，数字后面加“ K ”、“ M ”、“ G ”分别代表1000，1000000及1000000000。其他象新增，插入，或删除等命令也会有比较详细的数据显示出来。
-n，--numeric
数字化输出。象是IP地址或是端口号码都会以数字显示。预设系统会尽量用相关联的名称表示。
-1，· -log
打开核心的数据包记录功能。若是某条规则加上这个选项，只要有比对成功的数据包，核心会用printk()这个函数列出数据包的信息。
-O，--output[maxsize]
拷贝比对成功的数据包到userspace装置。
-m， markmarkvalue
这是用来往userspace中使用防火墙。
这是用来比对成功的数据包上表示一个32位长的指正整数，通常只有要修改核心内部的高手才有可能去用这个选项。
—t，—TOS andrnask xormask
这里设定的遮码值是用来修改IP数据包文件头的TOS栏位用的。当一个数据包比对成功这条规则后，数据包的TOS栏位会跟andmask的值做and运算，然后跟xormask的值做xor运算。TOS会影响系统对数据包的处理状况(象数据包传送的优先顺序等)。
-X，exact
延展数字。使用这个参数时-L命令列出的计数器数字会以正确数字表示(不会用K，M，G等缩写)
[!]-y，--syn
只有带有SYN位设定及ACK和FIN位是清除TCP数据包比对规则成功。这类数据包通常是用来启动一个TCP连线用的。例如若是文件往这类数据包如让网络界面接受，则无法由外部对本机打开一个连线，但是本机可以打开一个对外的连线。
--line-numbers
用来指定这条规则在chain中位置(优先序)

-—no-warnings
关闭所有警告信息
下列是ipchains用来处理规则与chain关心的一些功能
ipchains –D chain rulenum[options]
ipchains-[LFZNX][chain][options]
—D．--delete
从选择的chain中删除一条或多条的规则。这里的rulenum可以是规则的号码或足一条要比对的规则。
—L,--list
列出所选择的chain中的所有规则，如果没有指定chain，则会列出所有chain中的规则。
清除所选择的chain。这跟一条一条删除所有的规则是同样的作用
—Z．--zero
将数据包书及数据包大小计数器归零。
-N．--newchain
新增一个用户定义的chain。
-X．-delete-Chain
删除指定的用户定义的chain。未指定的话，则删除所有用户定义的chain。
以下是ipchains用来设定比较成功后的处理动作的用法：
ipchains –P chain target[options]
-P，-policy
设定chain中比对成功的接着要做的处理。这些处理可以是ACCEPT，DENY，REJECT，MASO，REDIRECT或RETURN这几个特殊的值或是另外一个用户定义的chain。ACCEPT指的是让数据包通过。DENY是丢弃数据包。REJECT跟DENY一样会把数据包丢弃。但是会送一个ICMP信息给来源告知数据包已被丢弃。MASQ是只对传送这个动作和用户定义的chain有效的处理，必须在内核加上CONFIG _IP_MASQUERADE的选项后再编泽才能使用这个选项。使用这个处理，数据包就会被伪装成为由本机所送出的数据包，而且送出以后对方回复的数据包也会被自动反向处理送回本来的机器。REDIRECT只能用在输入及用户定义的chain 中，要使用这个选项，必须先在内核中加上CONFIG _IP_ TRANSPARENT _PROXY这个选项再编译后才能使用。使用这个处理法则，数据包会被转向到本地端的socket，即使这些数据包是要被送到远端去。如果指定要转向的端口是0(预设值)，代表数据包的目的端口就是要转向的端口。如果一个用户定义的chain的检查到了尾端了或是得到的处理是RETURN，则会返回到呼叫这个chain的前一个chain的下一条规则继续比对。如果比对到了内建的chain的尾端或是在内建的chain中得到的是RETURN的处理，则会执行这个预设chain的处理方式。
以·下ipchains的用法是跟IP Masquerade有关的：
ipchains -M[-L，｜-S][options]
-M,--masquerading
这个参数加上-L可以用来查看目前使用masquerading方式的连线。加-S参数可用来调整核心masquerading的参数。
-S,-set tcp tcpfin udp
改变masquerading使用的timeout值。

使用Ipchains架设防火墙的范例及注意事项

住ipchains中，每条规则代表的是数据包所要符合的一组条件，以及当符合这组条件时要做的处理。因此，举个简单的例子，如果说你想拒绝所有从网络地址127．0．0．1(即本机地

址)传过来的属于ICMP这种类型的数据包时，你可以这样做：
$ipchains –A　input –s 127．0．0．1 -p　icmp –j DENY
在这条规则里，数据包要符合的条件就是(1)它要是属于ICMP类型的数据包(2)它要来自127．0．0．1。而符合条件后要做的事就是拒绝(DENY)。
在设定ipchains防火墙时通常只会用到像上面例子的ipchains –A 这样的加入规则的动作，以为一般是在开机时设定好了规则就不会再变动了。如果在使用过程中为了测试或是其他原因，你可能会用到删除规则这个动作。删除规则一般有两种方式，第一种是指定规则号码，像‘ 下例：
$ipchains –D input 1
会从input这组chains中删除编号为1的规则。要查看规则的号码可以用ipchains-L 来查看。
而另一种删除规则的方法，就是键入完整的规则，像下例：
$ipchains-D input –s 127．0．0．1 –p icmp –J DENY
这样就可以删掉上面我们加入的规则。
在TCP类型的连线上我们可能会常常想要限制只让单一方向的连线，比如说想要让自己的机器可以连线到其他的WWW服务器，但不让其他机器连过来。这时就要限制对方的SYN数据包(这种数据包是用来要求打开连线的)，像下例：
$ipchains –A input –p TCP –s 200．200．200．200 –y　-J DENY
就会拒绝从200．200．200．200这台机器过来要求作TCP连线的动作。
底下是更多的例子：
$ipchains –A output -d 200．200．207．0／24 –J REJECT
$ipchains，-A output -d 200．200．208．0／24 –J REJECT
不让我的机器连到200．200．207．*和200．200．208．*这两个网络。
$ipchains –N ppp-out
$ipchains –A output –I ppp0 –J ppp-out
建立一组新的chains，把所有使用ppp0传出的数据包都要比对这组ppp-out里的规则。
$ipchains –A ppp-out -p TCP –d proxy.virtual.net 80 –t ox01 0x10
$ipchains –A ppp-out –p TCP –d 0．0．0．0 telnet –t ox01 0x10
这可以设定连线到proxy.virtual．net的WWW及telnet有最小的延迟。
$ipchains –N ppp-in
$ipchains –A input –I ppp0 –J ppp-in
再建立一组新的chains，把所有使用ppp0传进的数据包都要比对这组ppp-in里的规则。
$ipchains –A ppp-in –s 200．200．200．0／24 –1 –J DENY
所有从200．200．200．0过来的数据包都拒绝并做记录
$ipchains –A input –I LO –J ACCEPT
允许所有从自己机器连到自己机器的连线。
$ipchains –P input DENY
最后拒绝所有从外面来的连线。
需要注意的是规则的顺序很重要，因为数据包是从第一个开始比对起，所以通常我们会先设定准许的连线，然后在最后一个规则设定拒绝所有其他的连线。

本章小结：

本章阐述防火墙策略的制定及目的，堡垒主机的分类及在防火墙拓扑中起到的作用：对于采购硬件设备所应注意的问题，目前防火墙拓扑的设计及在LINUX下熟练使用IPCHAINS来构建防火墙包过滤。

第九章
检测和迷惑黑客

引　　言

早在1997年的11月，黑客就攻进了Yahoo!一著名的搜索引擎站点；尽管这个流行的站点有着非常好的安全性，但仍然被一个叫做Kevinmitnick著名的黑客攻破并在上面留言。当问及到为什么这些黑客可以渗透到这样久经世故的系统中时，Yahoo的安全分析专家这样说：没有任何站点是可以完全阻止黑客的 ”。

本章要点：

- 实施前期的检测
- 迷惑黑客包括他们的活动
- 设置陷井
- 配置Linux下的Tripwire

前期的检测

要考虑到大多数计算机的侵入都是发生在深夜的，前期检测技术经常是唯一的方法来抵制这个时间内潜在的黑客。一个有效的检测策略总是包括审计，但对你的系统来说你必须尽可能的使其简单化来发现问题并自动的解决。

自动安全扫描

你的系统由其在业余时间会成为受攻击的日标。要考虑使用像NTschedule这样的程序(如果你没有删除它)执行一个批处理脚本登陆到当前的连接和使用中的资源，以及完成其它一些安全任务。你可以在业余时间运行这样一个程序，当流量负载较小时，你可以检查黑客的行为避免给你的用户造成不便。

批处理脚本是非常有用的：你可以使用它们来管理和观察很多事情，并完成自动开始初始化响应的任务。相关的介质包括一个简单的NT安全批处理文件，详细记录当前的系统活动并存储到一个文本文件里供以后使用。如果你怀疑某些系统活动，像这样的事件日志是非常有用的。与注视很多而详细日志相比，它们可以产生更多的相关信息。

使用登陆脚本

登陆脚本可以用于几个目的。通常，登陆脚本用于定义用户登陆的环境。登陆脚本是在成功登陆后的基础上才执行的。它们还能用来增强网络的安全性。很多黑客最终都要试图攻破UNIX的root帐号或NT的administrotr帐号以得到超级用户访问的权限。安全管理员可以修改这些登陆脚本让这些帐号来执行不同的审计内容。举个例子，你可以创建一个登陆脚本当root帐号登陆的时候就执行；这样一个脚本将记录企图登陆系统的主机名和IP地址。这些信息可以和以前记录的信息相比较，来识别任何企图用root帐号登陆的活动。使用登陆脚本的方法不局限于超级帐号。黑客有时为了避免触发警报而不是直接试图对超级用户访问。还要考虑对管理服务和进程的特殊帐号使用登陆脚本，通常这些帐号不是作为普通用户帐号登陆的，而是验证操作系统服务和进程的。你要时时刻关注这些特殊帐号像普通帐号一样的登陆。对于这些帐号相关的登陆脚本可以运行内存分页的应用程序，一发现这些帐号企图登陆便警告安全管理员。登陆脚本几乎可以多种不受限制方法使用。一个可以从登陆脚本中的命令行发布或执行任何东西。使用登陆脚本还是一个不昂贵的解决方法因为它的特点接近于各种服务

的操作系统。

自动审计分析

日志文件提供一些非常有用的信息来帮助阻止安全侵入。有关日志最难的部分就是决定对什么来进行记录。一般来说，要记录两件事，成功和非成功活动。你还可以监视不同位置的一些信息，如路由器或特殊的应用程序服务。当决定好需要记录什么时，你可能犯的错误是宁可多记录一些事情而不少记录。日志文件需要定期扫描，而且里面的信息内容经常是巨大的。你可以写个脚本来扫描你的网络并自动分析活动。这种自动执行节省了管理员的时间，减少了管理的费用，并增强了安全性。

Checksum分析

黑客经常攻进计算机后种植特洛伊木马程序或病毒。黑客希望这些文件最终能够被自动执行或重新启动后执行。一个非常普通的技术就是创建一个与操作系统经常使用的文件相同名字的特洛伊木马。你可能需要分析一些重要的运行程序的大小来确保黑客没有篡改它们。一些程序会自动扫描重要文件的数据，时间戳和相关信息。然后跟以前扫描过的值相比较。如果某个文件被修改过或者时间戳与大小都不匹配，那么些文件大概就被木马所替换了。如果发现了木马或病毒，要立即用好的文件替换回来并查出黑客是从哪里侵入系统并种植这个木马的。举个例子，如果黑客利用木马替换了一个不太重要的，但是基本的文件，如vbrun300．dll，并有着和其相同的名字。通过利用checksum分析，你可以看到这些文件不是适当的大小，并能逐步纠正这些问题。

迷惑黑客

除了简单地捕捉到这些活动之外，有很多种方法来迷惑黑客。这样做的一个原因是为了保持你在网络上有足够的时间来发现和跟踪他们。例如，你可以配置一条防火墙规则对于一些黑客的源1P地址直接指向一个假的系统中。许多大型的网络都在他们的网络内创建一个完整的系统实际上全部都是一些假信息目的是为了迷住黑客并使他们一直在线直到抓住他们。从虚假帐号到假文件，拌索到监狱，如果你的公司有一些资源并且是有诱惑力的，你一定要小心的考虑到这些技术。使用这些技术也不是没有风险的，一些公司选择简单的终端连接

假帐号

到现在，你已经知道系统的一些默认选项是黑客最初的目标之一。但是你也同样可以利用这些默认信息直接防范黑客。例如，在NT中系统管理员帐号叫“ administrator ”。在前面的课里，你己学过有关对帐号改名为潜在的黑客入侵增加了很大的难度。现在你可以进一步地创建一个新的叫做administrator的帐号，并赋予给它对系统中的任何对象没有访问权限，同时设置详细的审计和警报，如使用登陆脚本通知你当企图使用这些帐号登陆发生时。

假文件

使用假文件常见的方法是建立一个错误的密码文件。一个错误的密码文件对于迷惑黑客是非常重要的。在这个文件：里，你可以添加错误的名字利密码，使它们看上去似乎合理的，但并不可用。在UNIX系统中，黑客经常使用像CRACK这样的程序来进行暴力攻击。像CRACK这样的程序主要是采取很长的一列密码并逐个地进行加密，这和UNIX加密密码文件的方法是一样的，然后CRACK用这些加密后的结果与密码文件里加密后的密码相比较，如果匹配，那么这个程序已经破解了密码。这种过程可能花几天，甚至几星期，但仍可能会得到很多帐号

的密码。然而，如果你提供了一个假的密码文件，黑客忙于破解这个无价值的文件会花掉大量的时间，重要的是，这使你的系统安全会持续更长的时间。

Ttipwire和automatedchecksums

网络安全中的tripwire主要是基于军事应用程序使用的。Tripwire的想法是当一个潜在的黑客开始渗透你的网络时，他(她)要么陷入你所设置的陷井中，要么会在篡改后留下明确的数据。Tripwire可以做很多事情，如听从安全管理员结束黑客的网络连接，或建立一个对于已发生改变的数据库。Tripwire类似于假文件可用不同的方法来使用。

Tripwire的概念

当用tripwire安排一个陷井时也可能会产生危险，像那种自动地退出网络连接，一定要备加小心地安排。有害的tripwire一定不要被一个内部用户或其它的网络管理员偶然地使用。还有，要考虑防止一个黑客所进行报复产生的副作用。当使用TripwireforUNIX和NT这样的程序时，你要想到入侵者可能会操纵这些文件以至这些改变不会被注意到。因此，要考虑使用只读的磁盘和介质来存储敏感数据。

WindowsNT的性能监视器可以用来跟踪系统。可是你只能用其系统级的特性来设置系统警报。

Jails

Jails是一个你可单独创建的系统且来延迟黑客行动。Jails通常考故意地提供一些错误的信息，为了让管理员有时间检测和抓住这些黑客。Jails还能成为危险的出路包括黑客活动，主要因为一个黑客可能攻破你的jaiI并进入你真正的系统中去。你的安全策略可能允许你创建一个Jails。系统管理员有时建立一个Jail仅仅是为了学习，担心公司以后禁用这种行为。是否建立一个Jail或其它类似装置需要由对这种技术的优点和缺点有完全的理解的管理人员决定的。使用Jails也可能是合理的，由其是在一个特殊的大型网络中。一个执着的黑客准备在渗透你的系统前通过某些站点来作为中继。想知道这些黑客的源位置，你经常需要得到数据包(packet)和物理线路踪迹。要完成这种跟踪，你必须保持黑客始终是在线的。

有才能的黑客在一段时间内使用系统仅几分钟，即使他们正在渗透或正得到控制权时。事实上，大多的黑客经常同时工作在不同的系统之上，并在它们之间切换。这种做法使黑客的活动看起来是断断续续的，而构不成威胁。结果是检测非常困难直到发现怀有恶意的活动为时已晚。

一个好的黑客，像一个好的管理员一样，足偏执狂。有时，抓住黑客唯一的方法是作好前期的准备。这种前期的方法可能包括使黑客绊倒在Tripwire之下如实验10-2；或创建一个Jail，如NetworkAssociate’sCyberCopSting程序。简单地说，你需要尽可能地利用多种安全方法和手段。

惩罚黑客

通常，简单地断开黑客的连接是不够的，因为他们会重新开始。惩罚黑客和迷惑黑客的不同是惩罚黑客扩充了抓住他们之后所为：摆脱了一成不变性。在下一章里关于检测到一个黑客时将采取哪些特殊的步骤是我们的重点。

方法

想办法检测和阻止黑客的活动受限于你的创造力，对黑客手段的知识，以及对你网络的了解。一种方法可能是使用一种WINNUKE版本的脚本程序来阻止一些用你的假帐号登陆的源IP。另一种方法可能是使用Chagen服务。Chsgen服务是一种几乎废弃的用于排错的服务。它不停地发送含有字符的流量直到连接中断。

在一个你想要阻止黑客的机器上，你可以把Chargen配置运行到21端口上(默认是FTP的端口)。当黑客检测到21端口激活时，Chagen将发送不停十亡的字符流量。因为一个Chargen客户端不是设计于可接受如此多的字符，应用程序经常会崩溃。事实上，利用这种反向的Chargen攻击黑客的整个系统是很普通的。

工具

可以利用很多安全工具来检测黑客。有些工具利应用程序我们在前面已讨论过。安全工具可以往黑客攻击时向你发送警报，或试图这么做。安全工具的范围可从简单的包捕获到入侵监测应用程序。有大量可用的工具能根据你预先确定的攻击模式，来帮你检查网络活动，并对这些模式做出反应。响应的范围可以是通过管理员增强防火墙的安全，并关闭连接。这些工具在你的“ 软件库 ”中是不可缺少的。在附录中有一些额外的练习可以帮助你学习更多的有关如何并跟踪黑客的知识。

本章小结：

对于保护你的网络最佳的办法就是要提前知道你的网络中存在什么样的问题，或在攻击还未对你造成后果时及时的发现，本章描述了关于提前检测的方法和迷惑黑客的一些技术手段，并要学会使用Tripwire来定期发现是否受到破坏。

第十章
事 件 响 应

引　　言

前面你已经学过如何牵制和惩罚黑客行为。当一个安全攻击发生时你需要一个计划来和黑客进行周旋，你还要有一个好的策略来说明怎样及何时报告一个问题，并且还要能通知相关组织和人们详细内容，这节课描述了当检测到一个黑客所采取的一些特殊步骤。

本章要点：

- 对一个安全突破作出相应的反应
- 当你的系统遭到攻击确定能帮助你的安全组织
- 向一些安全组织订阅安全方面的信息

提前决定

你不会想在紧急时刻才做订制策略的决定，经调查已再三的证明人们在紧急的情况下才做一些简单的决定，除非事先已存在定义好的、明确的策略。举个例子，AT＆T在1995年发现黑客侵入了它的网络，系统管理员们试图解决这个问题，决定建立一个“ 电子监狱 ”。尽管这种作为看上去很谨慎的帮助公司查出这些渗透者，管理员们还是被严厉的训斥，因为高级管理人员认为他们的解决方案使公司的网络变的危险。

在AT＆T中的矛盾是管理人员和系统管理员之间不能很好的通信，这种矛盾警告了每一个人要有一个相同情况的好的计划，如果你有一个很好的组织，事先做好了策略，那么避免这种情况是很容易的。当考虑如果一个黑客攻击你的网络需要如何做的时候先要决定采取什么步骤，然后记下那些决定。对执行的详细列表进行分类，并把它写入你的策略当中，并确保所有相关的员工都有一份复印件,你的安全计划中要能保证什么时候中断一个黑客的会话，什么时候维持黑客的行为。

不要惊慌

在紧急情况发生或安全攻击中告诉某些人不要惊慌是很容易的，但真正的在那时能做到这一点却是困难的。然而，在事先定义好的策略中你计划中的行动将会告诉你如何去做，允许你清醒的思考和更有效的响应。

记录下所有的事情

系统和服务日志当然是要记录的基本内容，审计日志经常是黑客侵入到系统中所做的假象，然而，如果一个安全攻击发生，你还需要记录下你所采取响应的事件，审计日志仅仅是你需要的一半内容，一个帐号详细内容的例子应该包含什么时间以什么身份进入你的网络或企图进入你的网络等一系列详细内容以判断说明系统可能已经被影响，黑客可能已经侵入，以及黑客采取的特殊的或感兴趣的行为。如果你小心的记录你自己的活动。如果你既小心记录你自己的活动，又学习有关黑客的知识，就会增加避免进一步问题的机会。详细日志允许修正你安全系统中的问题是极为重要的。

分析当前形势

要确定是否一个真正的安全攻击发生。经常一些不适合的用户所做的行为被怀疑成黑客行为，这种行为有可能是工作需要所做的管理。如果一些人做出草率的决定并开始处理事件响应，那么即使是再好的策略也会失败。一旦你发现问题一定要警醒和耐心。

确定攻击的范围

一旦你怀疑一个黑客已经进入你的系统，要分析当前形势你首先采取的过程是黑客是处在第一阶段(侦察)，第二阶段(渗透)，还是第二阶段(控制)。其它一些步骤包括：

判断帐号是否被影响

识别哪些文件被读取，改变，替换

跟踪黑客在你系统中的活动

参考审计日志

判断是否某些权限被重新设置

一个安全组或部门需要判断你系统中危险的范围。再此活动中，系统管理员要停用其它所有活动。举个例子，如果黑客删除了文件，系统管理员仅需要在被改变的硬盘上恢复它们。

停止和牵制黑客活动

和黑客渗透到一个系统后企图控制一样，下一步你需要击破黑客，包括控制他们的活动。你要直接以你的安全策略来阻止黑客的连接包括他们的活动。不过记住这种牵制策略也经常是危险的。不管多健全的策略，都要根据具体的形势而决定。前面的步骤普遍的适用于大多数公司。除停止和牵制活动外，还要执行一个响应计划，要对你的公司的策略和安全突破的

性质作单独的测定。你要小心考虑你所学过有关安全规则的特性。

实施响应计划

多数情况响应就是根据你的策略来做什么事情。这些步骤包括

- 通知管理人员
- 中断连接或建立一个“监狱”(jail)
- 打电话叫警察
- 联系黑客
- 追踪路由和其它活动来进一步映射黑客的行为

通知受影响的个体

如果黑客已经危及到一个合法用户的帐号。你可可能需要直接让那个用户改变他(她)的密码并耐心的检查那台计算机上的文件是否有被替换。

通知服务提供商

通知你的ISP有以一下两个原因：

. 你可以让ISP暂时中断连接使攻击中止
. ISP可以帮你跟踪攻击

通知Internet代理商

在1998年，CERT收到了41871封电子邮件：信息和1001和热线电话报告有关互联网上的安全事件；。CERT全体人员调查了影响18900个站点的3734台计算机。如果你怀疑一个黑客侵入你的系统，你可能需要通知CERT(http：／／www.cert.org)。。

分析和学习

最重要的是你要能从事件响应的过程中学到些东西。为了能最好地分析你的响应，要求提出下面的每个问题：

. 黑客是如何绕过安全策略的?是贿赂内部员工?社交工程?暴力攻击?修改路由表?还是穿过了不严格的防火墙7
. 真正响应的效果是怎样的强度?能够提高什么?以后你要有些什么不同的做法?

最后，记下你所学过的特殊课程，并更新或修改你的安全策略及实施，要重视你在实际经验中所学到的知识。

本章小结：

尽管你采用了多种保护措施，有时侵入事件仍会发生，对于事件响应所处理的态度和方法也是非常重要的，本章在这方面给出很好的建议。

操作系统安全篇

第一章

网络安全基础

引　　言

随着各种操作系统不断地开发，服务器和桌面式计算机已起到了决策的功能性，且经常是发布式的设备通过广域网或局域网相连。连接这些网络可通过多种介质和拓扑，比如以太网、光纤等。尽管这些互联系统最主要的动机是信息和资源共享，但这种连接还是会导致系统及数据被攻击。因为UNIX和NT操作系统已被广泛应用，所以它们更容易成为被攻击的目标。公司的Intranet和互联网易遭受到黑客的攻击，访问数据和应用程序，还有可能导致更严重的损害。因此，一个可靠协调的想法就是需要在任一个工作的组织里都开发一个坚固的安全策略。

本章要点：

- 阐述在UNIX和NT环境下实现安全的需要
- 描述安全方面的工业评估标准，包括ITSEC、TCSEC，and Common Criteria(CC)
- 能够识别确定三种安全级别的准则
- 讨论用于实施安全系统的安全机制，包括特殊和广泛机制
- 描述NT所谓"out-of-the-box"的安全问题
- 识别和描述用于架设NT安全结构的组件
- 讨论一般对于UNIX产生威胁的因素

安全的定义

由国际标准化组织(1SO)早期对安全做的定义，IS07498-2文献定义安全就是最大程度地减少数据和资源被攻击的可能性。ISO进一步地定义厂另一术语＂资产＂，就是存在于任一计算机系统的数据、应用程序和资源。ISO所描述的漏洞是指能够被一些人对那些资产取得访问权限的任何事情。通常，漏洞是指系统的各种弱点，系统安装和操作时所未注意的方面。威胁即是任何能对系统安全造成危害的活动。IS07498-2文献定义对于所有等级的本地和远程系统及应用程序访问的主要安全服务。具体内容见下表

服务	描述
认证	如何确定自己的身份。如利用一个带有密码的用户帐号进行登陆
访问控制	赋予用户对文件和目录的权限
数据保密性	保护系统或主机上的数据不被非认证的用产访问
数据完整性	提供对于类似位于网络中＂劫持＂这种手段的攻击的保护措施
不可否定性	当两个系统交互时，如果一方拒绝承认发生过这种交易，另一方就需要拿出证据来证明交易确实发生过。不可否定性也是提供防止欺骗的安全服务

评估标准

多数政府和组织都不和那些没有经过第三方安全标准证明的公司时行商业交易。安全经常所关心的是地域性，就是不同的工业、组织和国家政府都有不同的手续和标准来提供有效的安全模式。近来更多的努力正企图建立一个全球的ISO安全文献。下面的标准文档不是特殊针对UNIX或NT的，它们是对不同的网络类型提供一个大体上的框架。

欧洲信息技术安全评估标准(丌SEC)文献BS 7799

在欧洲，欧洲信息技术安全评估标准BS 7799对网络威胁提出一个大纲。它定义了计算机管理员需要对之响应的漏洞。BS 7799写于1999年，详细内容如下

- 审计过程
- 对文件系统审计
- 评估风险
- 防护病毒控制
- 适当地管理关于商业新闻及安全发布的信息

想了解更多有关丁ITSEC的信息，请访问http：／／www.Itsec.gov.uk

可信任计算机系统评估标准(TCSEC)

在美国，国家计算机安全中心(NCSC)负声对信仟的计算机产品建立安全标准做出响应。NCSE创建了信任的计算机系统评估标准(TCSEC)，保护局(DOD)标准5200．28，来建立信任等级。这种标准想要打算指出系统潜在的安全特性和安全功能性及有效性的组成。

TCSEC设计了几种安全等级的级别，从A到D。筹级D是指最不安全的计算机。而A级是最高的等级，通常是在用在军用的计算机上。等级C通常是实施在商业环境中，它要求数据的属主必须有能力确定谁能够访问数据，叫做灵活访问控制(DAC)：

TCSEC和ITSEC有些相似。不过ITSEC在讦估时把功能性(F)和效率性(E)分开。TCSEC的C2级绰同于ITSEC的F-C2,E2级。

TCSEC安全等级

安全级别	描述
D	最低的级别。如 MS-DOS 计算机，没有安全性可言
C1	灵活的安全保护。系统不需要区分用户。可提供根本的访问控制。
C2	灵活的访问安全性。系统不仅要识别用户还要考虑唯一性。系统级的保护主要存在于资源、数据、文件和操作上。NT 属于 C2 级的系统
B1	标记安全保护。系统提供更多的保护措施包括各式的安全级别。如 AT&T 的 SYSTEMV 和 UNIXwithMLS 以及 IBMMVS/ESA
B2	结构化保护。支持硬件保护。内容区被虚拟分割并严格保护。如 Trusted XENIX and Honeywell MULTICS
B3	安全域。提出数据隐藏和分层，阻止层之间的交互。如 Honeywell XTS-200

A	校验级设计。需要严格的准确的证明系统不会被危害，而且提供所有低级别的因素。如 HoneywellSCOMP

C2级和F-C2，E2级要求

对于C2和F-C2,E2级分类的关键是一个系统需要具备以下几个主要方面
灵活的访问控制：资源的属主对其访问性有完全的控制
对象再利用：

对象再利用必须由系统来控制。因此，任何时间当一个应用程序或进程在利用一个对象，比如内存，在被另一程序或进程使用的时候，那么内存中以前的内容是不会被新用户所发现的。这种标准要求控制在磁盘、监视器、键楹、鼠标、以及所有附加到系统．上的设备。
标识和认证：

这种标准要求每个用户对于操作系统都有一个唯一的标识符， 并且操作系统能够根据个人标识符跟踪用户所有的活动
审计：

最后一个主要的要求就是计算机管理员械能够审计所有与安全相关事件及个人用户的活动。还有，审计的数据只有计算机管理员才有权限访问。
公共标准(CC)

公共标准是统一不同地区和国家安全标准的标准，如ISO把ITSEC和TCSEC合并到一个标准文献里。这种标准也就是目前的IS015408,ISO公共标准2．1的版本。 公共标准说详细说明和评估了计算机产品和系统的安全方面特征。它是第一个国际公认的IT安全标准，是建立在ITSEC和TCSEC基础上并意于代替它们而成为全球的标准。
公共标准提供两个基本功能：

1. 标准化描述安全必要条件，比如安全需要什么，能满足那些需求的产品和系统，以及对那些产品和系统进行测试和评估。
2. 以可靠的技术基础来对那些产品和系统进行评估

其它重要概念

理解公共标准有三个基础概念。在特定的情形下为了确定合适的安全产品和系统，这些概念被广泛地用于通信和执行过程。
保护文件：由IT管理员、用户、产品开发者及其它产商定义的一套特定安全需要制定的文档
安全目标：由厂商提出一个IT产品和系统能提供怎样的安全而做的声明。包括特殊产品信息，以解释流行产品或系统如何满足保护文件的。
评估目标：要被评估的IT产品或系统。产品必须要通过保护文件和安全目标所例出的特殊安全需求的评估。根据公共标准要求，产品必须要经可信任的第三方机构分析和测试后才能通过。

安全等级

UNIX和NT操作系统提供了很大范围的安全选项。它们允许你在每个系统上定做符合你所需要的安全尺度。通过本书的课程你将会利用多种方法来使的你UNIX或NT系统更加安全。尽管安全的实现是由很细微的工作组成的，不过为了讨论目的，本课把安全等级大致地分成了三类，低、中、高三个级别

安全等级	适用于	实施
低	计算机在一个安全的区域里 计算机不包含和访问敏感信息	操作系统安全未应用 使用防病毒软件 防止计算机遭遇偷窃行为
中	计算机含有或访问公司数据 计算机可被超过一人以上的访问	能够审计 使用文件级权限保护 实施帐号策略 操作系统提供反措施和保护对策
高	计算机含有高度敏感或极有价值的数据 计算机处在一个高风险的位置	操作系统为满足选择性功能被分成最小部分 在操作系统上使用额外的更严格的策略和保护措施

安全机制

安全机制用于来实施安全系统。主要存在两种形式的安全机制，特殊和广泛。

特殊安全机制

某些技术可以实施在不同的级别来提供安全。这些技术是：

- 加密机制，对流动在系统或网络之间的数据加行加密(或在本机的两个进程之间)
- 数字签名机制，与加密极为相似，但另一个好处是检验发送者和内容是可信的，这种交易是由第三方来做的。
- 访问控制机制，简单的检查来确保在完成一个任务或程序时发送方和接收方是通过认证的。比如，网络允许一个有资格的用户在远程登陆的时候访问资源。
- 数据完整性机制，一种确保每片数据的顺序、编号和时间戳的技术。
- 认证机制，就像用户级的这种简单密码验证方法。认证也可以应用到程序中，要求每次访问都要通过验证。
- 数据添充机制，额外的针对网络上进出的数据流，为了防止那些熟悉数据包的大小并以取得访问权限为目的的人对网络进行监视。举例说明，当一个新的登陆会话建立后，在会话开始的时候主要有几个较小的数据包传输和接收。对这些包头进行分析可以提防那些网络监视者捕获下面一些数据包(因为较小的数据包和主字段都存在于包头中)。数据添充可以使所有的数据包看起来都是相同大小的，所以可避免某一个数据包被单独地摘出分析。

广泛安全机制

其它不受限于特殊级别的安全机制，有

- 信任的功能性建立，某些服务或主机在各方面都是安全的而且可以信任。
- 安全标签的应用，指出数据敏感性的级别。举例说明，一个文件可以有附加的标签在读／写特权旁，只允许那些完全符合标签登陆的帐号才能访问。

- 审计跟踪经常在不同级别上使用，监视易受到入侵的活动和安全侵害。比如，UNIX的系统文件日志能够记录企图访问重要帐号的事件。

安全管理

为了协助管理者开发一种方案和策略，可以指定不同范围的安全管理，这些范围有：

- 系统安全管理，从事整个计算机环境和安全的管理。在此范围，策略已事先定义，服务提供商为顾问，选择特殊安全机制。这个部门还要负责审计和恢复的工作以及所有更深入的安全工作。
- 安全服务管理，包括那些实际的安全服务提供商
- 安全机制管理，包括那些负责以下活动的人们

》 数据流量添充
》 产生或分配数字签名
》 加密的密钥
》 数据完粘
》 访问控制

WindOWSNT安全

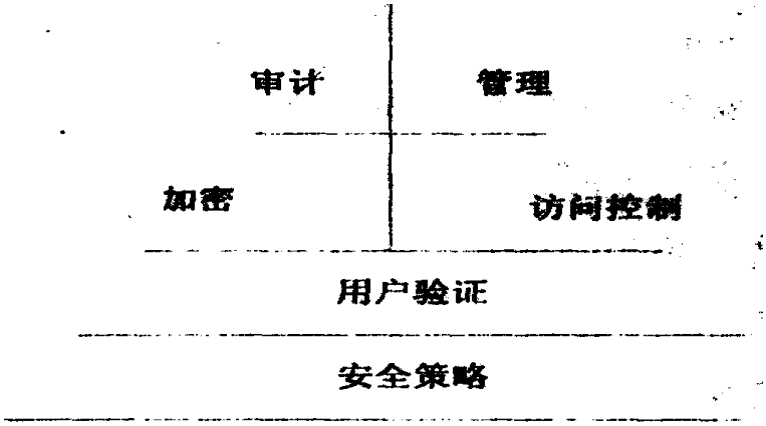
微软的WindowsNT操作系统是专为符合工业或政府安全需要所没计的。但是NT的安全问题一直在发生。流行的站点http：／／www．rootshell,com就列出了能对NT产生危害的攻击手段和过程。几乎每周都会有新的问题出现。在这节课里，您将利用特殊的手段来实践，理解在NT上这些攻击是如何发生的：这些知识将使你防止类似的攻击以最大限度地保证你的计算机安全。

在你能够理解如何修补一些NT漏洞前，你首先要对这些问题有一定的了解。当你重新安装一个NT操作系统后，它是处在一个非常不安全的状态，大多数其它操作系统也是这样。这种不安全的状态最小化了新用户把他(她)们自己的系统锁定的机会；还允许每个组织配置NT的安全性以达到他们的目的。我们将讨论有关NT的安全性，用一些流行的攻击方法和工具来对一个全新安装的NT操作系统(未做任何修补漏洞：工作)进行测试。

任何操作系统的主要漏洞都是由于用户和组、文件系统、策略、系统默认值、Bug，以及审计都处于一种待定的状态。NT还有一个其它操作系统所未具备的且易受攻击的漏洞，即是注册表。NT的注册表必须要安全保护。在下面的练习你将测试这些方面并能注意到它们的漏洞。

WindOWSNT的安全结构

现在你已经基本理解如何着手使你的NT平台更安全，接F来我们再看看NT自己的体系结构。如下图，专业的安全主要有六个要素来达到实施安全的目的以满足特定的系统或公司。WindowsNT操作系统内置就有支持用户验证、访问控制、管理和审计的功能。WindowsNT明确地想通过五种特殊的方法来避免绕过这些安全参数。一个基本的安全定义就是：仅允许合法的用户来做他们想做的事！”



WindowsNT安全组件

下面列出了WindowsNT符合于C2级标准的安全组什

- 灵活的访问控制——一WindowsNT支持C2级标准要求的灵活访问控制，要求包括允许对象的属主能够完全控制谁可以访问这个对象及什么样的访问权限。
- 对象再利用-一一Windows NT很明确地阻下所有的向用程序不可访问被另一应用程序使用所占用资源内的信息(比如内存或磁盆)。这种安全面貌是NT没有能力恢复已往磁盘上删除的文件的主要原因。
- 强制登陆-一-与Windows for Workgroups、Windoxs 95利98不同，WindowsNT用户在能访问任何资源前必须通过登陆来验证他们的身份，这也是另一个原因缺乏这种强制登陆的NT要想达到以前的C2级的标准就必须禁止网络功能。
- 审计-一-因为Windows NT采用单独地机制来控制对任何资源的访问，所以这种机制可以集中地记录下所有的访问活动。
- 控制对象的访问-一-WindowsNT不允许直接访问系统里的资源，这种不许直接访问是允许访问控制的关键。在允许访问之前，用户或应用程序的权限首先被验证。

WindowsNT对象

为了实现其安全特色，WindowsNT设计把系统所有类型的资源处理成特殊的对象。这些对象包括资源本身、机制和需要访问的程序。依照把所有都封装成对象并建立一个单独的机制来使用它们，微软创建单独的方法来对那些对象时行访问控制。基于这种方法学，WindowsNT通常被叫做基于对象的操作系统。

微软安全主要是基于下列对象的规则

. 所有的资源都以对象表示
. 只有WindowsNT能够直接访问那些对象
. 对象包括数据和功能
, 所有的对象在被访问之前都要经过NT的安全子系统验证
. 存在着几种不同类型的对象。每种对象确定了这些对象能够做些什么

在WindowsNT里有一下列主要的对象类别：

. 文件：
, 目录
. 打印机

. 输入输出设备
。 Windows
。 线程
. 进程
. 内存

这种结构的主要目的就是坚固性。这种设计要求所有的访问都要被相同的方法来减少这种安全机制被绕过的机会。

安全的组成部分

WindowsNT安全子系统由五个关键部分组成：安全标准符、访问令牌、安全描述符、访问控制列表、和访问控制条目。利用这些组件的交互作用来控制用户的活动。

安全标识符

安全标识符(SID)是统计上地唯一的数组分配给所有的用户、组、和计算机。统计上的唯一指的是两个数组发生重复的可能性是极为罕见的。每次当一个新用户或组被建立的时候，它们都会接收到一个唯一的SID。每当WindowsNT安装完毕并启动的时候，也会有一个新的SID分配给这台计算机。SID标识了用户、组和计算机的唯一性，不仅仅是在某台特定的电脑上还包括和其它计算机交互的时候。

为了确保SID的唯一性，它们是综合计算机名字，当前时间、以及处理当前用户模式线程所花费CUP的时间所建立起来的。一个SID看上去就像这样：

S—1—5-163499331-18283675290-12989372637-500

SID是WindowsNT安全结构的基础，因些我们将通过本课在不同方面来使用和讨论它们

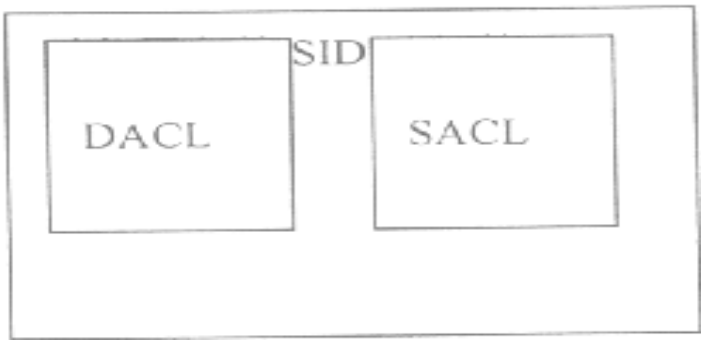
访问令牌

登陆的过程主要目的一部分是在用户被验证之后分配给他们访问令牌。访问令牌是由用户的SID、用户所属于组的SID、用户名、用户所在组的组名构成的。访问令牌就好比用户能够访问计算机资源的入场券 ”。无论何时用户企图进行访问，都要向WindowsN出示访问令牌。Windows NT检查访问令片相倚的对于对象请求访问控制列表。如果用户使用此对象的认错通过，将赋予相关的权限访问。

访问令牌只有在登陆的过程中才会发布，所以一旦对用户的访问权限作了改动的话就要重新登陆后才能收到一个更新后的访问令牌。

安全描述符

WindowsNT内的每个对象都有一个安全描述符作为它们属性的一部分。安全描述符持有对象的安全设置。安全描述符是由对象属主的SID、组SID，灵活访问控制列表以及计算机访问控制列表。如下图



访问控制列表

两种类型的访问控制列表是灵活的和系统的。灵活访问控制列表里记录用户和组以及它们的相关权限，要么允许要么拒绝。灵活访问控制列表列出每个用户和组的特定的权限。系统访问控制列表包含为对象审计的事件。当没有特殊指定访问控制列表的类型时，通常是灵活访问控制列表。如下图。

访问控制条目

每个访问控制条目(ACE)包含用户或组的SID及对对象所持有的权限。对象分配的每个权限都有一个ACE。访问控制条目有二种类型：允许访问或拒绝访问。在访问控制列表里拒绝访问ACE优先于允许访问。当用户认证检查之后，同时搜索相关的拒绝访问ACE或访问控制列表的最后项，不管哪个在前面。因此，不可访问优先于所有其它的权限。

当管理工具列出一个对象的访问权限时，是按照字母顺序由用户开始，然后是组。

安全子系统

现在你已理解用于WindowsNT安全子系统的组件了，接下来我们将讨论在NT下的实际软件来实现安全措施。安全子系统由下列部分组成：

- Winlogon
- 图形化鉴定和认证DLL
- 本地安全授权(LSA)
- 安全支持提供接口(SSPi)
- 认证信息包
- 安全支持提供商
- Netlogon服务
- 安全帐号管理(SAM)

Winlogon，本地安全授权，和Netlogon服务可以在任务管理器里的进程看到。

WinlOgon and GINA

Winlogon主要负责加载GINA DLL并监视安全认证的顺序。GINA DLL为登陆和登陆请求提供接口。GINA DLL被设计成独立的模块并可被更强壮的认证机制所代替。目前有很多强有力的认证设备可以使用，比如利用指纹认证来代替默认的GINA DLL。
Winlogon访问注册表里的＼HKLM＼software＼Microsoft＼windows＼NT\currentversion＼winlogon 键来查看Gina DLL值是否存在。如果此DLL存在，Winlogon加载并使用那个DLL。否则的话WindowsNT就使用默认的DLL,叫MSG!NA．DLL，是NT自带的。
由Winlogon来监视安全认证的顺序并当一个登陆请求发生时通知给GINA。

本地安全授权(LSA)

本地安全授权是一个保护子系统，主要负责下列任务：

. 加载所有的认证包，包括检查存在于注册表中
＼HKLM＼System＼CurrentControlSet＼ControL＼LSA中的Authentication Packages值
. 为用户找回本地组的SID以及用户的权限
. 创建用户的访问令牌
. 管理本地安全服务的服务帐号
. 存储和映射用户权限
. 管理审计策略和设置
. 管理信任关系

安全支持供应商接口(SSPl)

微软的安全支持供应商接口利RFC2743及RFC2744所定义的一般安全服务API极为相似
安全服务提供商API为应用程序和服务要求安全认证连接提供了解决方法。

认证包

认证包的内容提供真正的用户验。认证包检查通过GINA DLL所得到的证书，当用户的证书被检验后，认证包向LSA返回SID，包括用产的访问令牌。

安全支持供应

安全支持供应是安装驱动程序来支持额外的安全机制。WindowsNT默认安装包括以下：

. Msnsspc.dll：微软网络(MSN)挑战／响应认证方法
. Msapsspc.dll：分布式密码认证(DPA)挑战／响应方法，也用于MSN
. Schannel.Dll 利用证书授权机购(如VeriSign)所发布的证书来时行验证。这种认证方法通常是在安全套接字层(SSL)或私有通信技术(PCT)协议连接时所使用。

Netiogon

Netlogon服务必须为认证的传输建立一个安全的通道。为了达到这种效果，要定位一个域控制器来建立安全通道。最后，通过这条安全通道来传递用户的证以再以用户SID及用户权限的形式接收到域控制器的响应。

安全帐号管理(SAM)

安全帐号管理实际上是一个掌管用户和用户证书的数据库。它存储在WindowsNT注册表的一部分。每个域都有不同的SAM，作为两台域服务器复制的一部分。

Unix安全

在UNIX里，等同于WindowsNT注册表的是一个捆绑的文本文件和应用程序运行在内存中。没有像NT一下的Regedt32这样的集中控制程序，因此这方面不是我们讨论有关UNIX结构的重点，通过本门我们将学习UNIX的登陆利密码机制以及文件系统的权限。

一般UNIX的安全漏洞

从很多的媒体报导中都能了解到有关UNIX被扫描及攻击的事件；。在1988年11用2 日由毕业于美国Cornell大学计算机系的RobertT．Morris编写的一个程序偶然地发布到互联网上。按照Morris程序的设计，可以看出在那时互联网上就存在了漏洞及一些安全隐患。此病毒可自复制以损耗CPU及物理内存的资源使它们运行极为缓慢甚至导致系统崩溃。

在今天的UNIX领域里，病毒相对少了许多，可能是因为硬件结构已大不相同，因此想制造病毒是一个艰巨的任务。病毒需要有root的超级权限所以导致UNIX系统更多的危险。为了有效地防止UNIX系统被病毒侵害主要有以下几步：

- 系统级的目录写保护
- 有规律地检验更改时间和对系统执行做校验和
- 在特殊的地方只安装可信任的应用程序
- 确保用户只能执行公用的应用程序，不能包括其它可写的目录
- 不要安装没有经过检验的应用程序

缓冲区溢出

因为不像WindowsNT的注册表那样，UNIX没有集中的目录被HACK，黑客们较关注单独应用程序的缓冲区溢出。你可能知道，所有的应用程序都是在操作系统中的内存里来运行。每一小片内存称做缓冲区。缓冲区是内存中存放数据的地方。在程序试图将数据放到计算机内存中的某一位置，但没有足够空间时会发生缓冲区溢出。
下面对这种技术做一个详细的介绍。

缓冲区是程序运行时计算机内存中的一个连续的块，它保存了给定类型的数据。问题随着动态分配变量而出现。为了不用太多的内存，一个有动态分配变量的程序在程序运行时才决定给他们分配多少内存。如果程序在动态分配缓冲区放入太多的数据会有什么现象?它溢出了，漏到了别的地方。一个缓冲区溢出应用程序使用这个溢出的数据将汇编语言代码放到计算机的内存中，通常是产生root权限的地方。

单单的缓冲区溢出，并不会产生安全问题。只有将溢出送到能够以root权限运行命令的区域才行。这样，一个缓冲区利用程序将能运行的指令放在了有root权限的内存中，从而一旦运行这些指令，就是以root权限控制了计算机。当一个应用程序收到这些意外的信息时，这些信息可能会导致程序自身向外扩展，也就是覆盖或叫溢出，导致缓冲区里是一些错误的信息。一旦溢出发生，很可能使应用程序或系统崩溃并留下一个shell，这个shell通常也是以root权限来访问的。缓冲区溢出的最典刑例子有本地时间进程表的程序Crond。
还有作为FTP服务器的旧版本的Wu-ftpd。Sendmail关于缓冲区溢出也有很少的历史了。

本章小结：

通过本章学习对Windows NT以及UNIX系统的安全面貌有了大体的了解，对于达到某些安全标准如ITSEC，TCSEC，CC的需要。对于NT所谓的"out-of-the-box"有了深刻的认识及相应解决方法。

第二章

帐 号 安 全

引　　言

用户帐号不适当的安全问题是攻击侵入系统的主要手段之一。其实小心的帐号管理员可以避免很多潜在的问题，如选择强同的密码、有效的策略加强通知用户的习惯，分配适当的权限等。所有这些要求一定要符合安全结构的尺度。介于整个过程实施的复杂性，需要多个用户共同来完成，而当维护小的入侵时就不需要麻烦这些所有的用户。

整体的安全策略中本地帐号的安全是非常重要的。这节课，我们将探讨用不同的方法来保护本地帐号的安全。

本章要点：

- 描述帐号安全和密码之间的关系
- 在WindowsNT和UNIX系统的实现安全帐号的技术
- 在NT下实施密码策略的步骤
- 描述UNIX密码安全及密码文件的格式
- 分析UNIX—卜的安全威胁，拒绝帐号访问和监视帐号

密码的重要性

密码是UNIX和WindowsNT安全基础的核心。如果危及到密码，那个基本的安全机制和模式将遭到严重影响。为了选择强固的密码，你需要在帐号策略里设置更多相关的选项。你还要帮助用户选择强壮的密码。　　，

一个强固的密码至于要有下列四方面内容的三种：

. 大写字母
. 小写字母　　.
. 数字
. 非字母数字的字符，如标点符号

强闹的密码还要符合卜列的规则

. 不使用普通的名字或呢称
. 不使用普通的个人信息，如生日日期
. 密码里不含有重复的字母或数字
. 至少使用八个字符

从黑客的思想考虑，避免密码容易被猜出或发现(比如不要写到纸条上放到抽屉里)。

NT下的密码安全

在NT下为了强制使用强壮的密码，你可以更改注册表里的LSA值来实现，叫passfilt．dll，

这个文件可以在WindowsNT的ServicePack2及以后的版本里找到。在LSA键值下需要添加NotifcationPackages字串并把值为passfilt．dll加进去。这串值必须在公司所有的域控制器里都加入。同时你还需要使用passprop．exe这个程序来使passfilt．dll生效。

UNIX下的密码安全

在UNIX中加密后的密码信息是存在一个文件里，通常是／etc／passwd。维护好这个文件：的安全性是非常重要的。在UNIX系统里它的属主是具有最高权限的帐号，即root的。UNIX基本上有两类用户：普通用户和系统特权用户。有时特权用户也被不确切地叫做超级用户。实际上，一个超级用户帐号的标识号是为零。当一个帐号建立的时候，会被分配一个唯一的标识数字(UID)。这个数字分配从0开始，最低的数字(也就是最高的权限)是分配给登陆帐号root的。Root可以执行任何程序，打开任何目录，检查任何文件：，改变系统内任何对象的属性及其它任意的功能。任何对于攻击UNIX系统的黑客最终目的都是取得Root帐号。

Root掌管／etc／passwd文件。此文件可以被所有登陆的用户读取，它包含每一个用户的认证信息。因此，在简单的UNIX系统上任何人都可以复制这个文件的内容并分析哪个字段是包含加密后的密码。然后利用不同的密码一系列的尝试和／etc／passwd加密后的字串进行比较。因此，密码的选择是UNIX系统安全级别中最重要的。

.

WindOWsNT帐号安全

首先，也是最困难的任务就是确保只有必需的帐户被使用而且每个帐号仅有能满足他们完成工作的最小权限。在一个大型的公司里，通常是用一个或多个用户域集中管理所有的用户帐号。域是一个中央集权的帐号数据库可以在分布于公司中间。因此有经验的管理员尽量把用户放到较少的域里面以便于管理。这种限制通常促进公司策略的粘附性。本地组创建本地资源并管理权限。本地资源的机器要被配置成信任集中帐号域。但有时这种设置也是不可行的，因为和远程站点间没有足够的带宽。

有几种技术可以解帐号安全的问题。其中一个主要关心的是确保不再有新的帐号建立或已存在的帐户权限不作改动。另一个简单的方法就是利用netuser和netgroup命令把信息定向到一个文本文件里后进行比照。有规律地运行这些命令并对输出的文本文件中的帐号列表进行比较就能轻易地发现问题。一些内置的工具，比如系统任务进度表程序，可以自动的执行。也可以使用其它一些外部工具比如Peri或diff可以自动地对标准列表和当前的设置进行比照。

帐号重命名

另一个可靠的办法就是对默认的帐号重命名。包括administrator、guest以及其它一些由安装软件时(如IIs)所自动建立的帐号。这些帐号必须好好保护因为它们易受攻击。然而简单地重命名帐号并不能很好地隐藏它们。因为Windows NT必须知道哪一个是管理员帐号，管理员帐号当前的名字是保存在注册表里的。

帐号策略

为了保持用户数据库不被侵犯，你必须强制用户养成良好的习惯在帐号的设置上要能有效地防止黑客使用暴力破解的方法来攻击。这些任务主要是通过WindowsNT上的帐号策略上设置的。帐号策略的设置是通过域用户管理器来实施的，从策略的菜单中选择用户权限，第一项是有关密码的时效，第二项是有关密码长度的限制，以及帐号锁定等机制。

实现强壮的密码

大多数情况下，仅养成使用好密码的习惯是不够的：你还需要使用更强壮的密码来有效阻止类似于字典攻击的暴力破解攻击。我们前面已经讨论，一个强壮的密码至少需要六个字符，不能包括用户名的任何一部分，并且至少要有大小写字母，数字，和通配符等。为了实施强壮的密码你需要在注册表里LSA项加入本课已提过的其它的密码过滤器。在主域控制器或在任一可能会升级为主域控制器的备份域控制器上， 你都需要在注册表

HKLM＼System＼CurrentControlSet＼Control＼LSA中加入PASSFILT的字串。

UNIX帐号安全

在讨论UNIX帐号安全，你首先要理解UNIX密码的安全。这种理解需要检查密码文件的格式。你可以利用—下面的命令来得到几种特殊密码的格式

$man 5 paSSWord

密码文件包括几个字段，在表2-1作了详细解释

字段	用处
登陆名字	用户登陆时所真正使用的名字
加密后的密码	在 UNIX 中，密码是用高强度的 DES 算法来进行加密并保存结果
UID	用户唯一的标识号
GID	用户组的标识号
用户名	用户真正的名字
HOME	默认的主目录
SHELL	默认的程序 SHELL 接口

密码文件在显示的时候是加密的：这种显示叫做Shadow密码，通常创建在／etc／shadow属于root且只有root有权访问。

密码时效

按目前的形势，已有更强大的硬件大大地缩短了利用自动运行的程序来猜测密码的时间。因此在UNIX系统中防止密码被攻击的别一方法就是要经常地改变密码。很多时候，用户却不改变密码。因此一种机制用来强制规律性的更改密码是合乎要求的。这种技术称做密码时效并在很多UNIX系统上有效。

密码时效：LINUX

在LINUX系统上，密码时效是通过chage命令来管理的。

参数	意思

—m	密码可更改的最小天数。如果是零代表任何时候都可以更改密码
-M	密码更改的最大天数
-W	用户密码到期前，提前收到警告信息的天数
-e	帐号到期的日期。过了这天，此帐号将不可用。
-d	上一次更改的日期
-I	停滞时期。如果一个密码已过期这些天，那么此帐号将不可用
-L	例出当前的设置。由非特权用户来确定他们的密码或帐号何时过期

举个例子

%chage-m 2-M 30-W 5　steven

此命令要求用户steven两天内不能更改密码，并且密码最长的存活期为30大，并在密码过期前5大通知他。

记录不成功的登陆企图

所有的UNIX系统都能够记录非成功的登陆企图。在L1NUX中，登陆的失败是由syslog守护进程记录在／var／log／messages文件里。可以用下列命令来查找相关信息

$grep login／var／log／messages

搜索路径(PATH)的重要性

在UNIX里，常使用的命令用来在不同的环境卜查找一组特殊的目录称做PATH。想要运行当前目录包含的命令时是不需要加上一长串路径名的。在UNIX中用户经常使用 ”. ” 来表示当前的目录。如果 ”. ” 作为shell环境变量的一部分时，一个全局目录下的shell脚本或公用命令就有可能被相同目录的伪程序所解释，而这个命令可能包含一段代码，一旦被执行后果可能是较严重的，比如是一个木马程序。在Bourne orKom Shell里搜索路径通常这样来设置：

$PATH=pathnamel：pathname2：pathname3

$export PATH

在C或类似的shell里，以下列命令设置

%setpath：(pathnamel pathname2 pathname3)

在UNIX中像这样的路径可以保存在．profile文件里，可以看到像下面的语句

PATH=／bin：／usr／bin：／sbin：$HOME

Export PATH

因此，如果你经常参考用户主目录下的某个文件时，就创建一个叫"bin"的并把所以的个人的可执行文件放到里面；并要严格注意它们的安全性。假设 ”. ” 路径名存在于用户的shell初始化文件里，并用户不精通有关安全的知识而且不太注意环境变量中路径，那么可以想像他经常使用到的who命令。假设用户已创建了下面的文件：

$touch／tmp／testfile　。

然后，编辑下面的程序并保存为who．c文件

#include<stdio．h>

main()

{

system(“／usr／bin／who")；
system(“／bin／rm／tmp／testfile2>／dev／null ”)；
}
然后对些程序进行编译
$gcc –O　who who．c
并且此用户可能含有这样的profile：
PATH=.：／bin：／usr／bin：／sbin：$HOME
ExpoRT PATH
现在，如果户键入
$who
再去找找你刚刚建立的testfile这个文件，看看发生了什么

限制root登陆

另一增强root帐号安全的方法是限制其在系统上直接登陆。不同版本的UNIX处理此项任务的方法是不同的。
在SUN的Solaris系统上要修改／etc／default／login文件，你需要加入下面一行
CONSOLE=／dev／console

限制

对于多用户环境来说另一个可行的方法是通过限制shell来给外部用户他配权限。一个例子是rksh shell就是KornShell的一个受限制的版本，它允许提供原shell大部分功能除了下面几条
。重定向I／O(如>和>>)受限
。改变目录受限
。环境变量不允许改变
。检查Path名字
这种：方法对于那些用户不注意运行了一个可能导致打开安全访问的程序是非常有用的。

用户空闲时间

为了进一步增加安全性，一些公司鼓励在一些草根级基础上做安全练习。那些并没有时刻注意白己屏幕或者停止使用很长时间的用户很有可能导致其它人访问他们工作站上的保密数据和文件；。在这种环境下应该实施一种策略能够自动注销或中断。屏幕保护是一种可行的方法。或者，公用的应用程序像自动锁动能够监视列：强制中断一个会话。

监视帐号

系统管理员还要经常地监视一些可疑的用户帐号的使用，比如一个正在休假的用户帐号正被使用中，或者用户帐号正运行着不成比例的计算清单资源，比如内存和磁盘的使用率。对于这种任务有一些有用的文件是用户和帐号文件；。Utmp文件就是一个会话信息文件：并被记录。wtmp文件是有关帐号信息的文件：并被记录。它们包括

- 用户名和UID
- 终端线的数量
- 设备号

- 执行ID
- 存在的状态
- 其它的相关的信息

通常可以使用last,who,write,login等这样的命令来得到相关的信息。有时你还能知道会话是来自何处(比如Internet主机地址或网关) ‘

系统事件记录工具

大多数UNIX系统中，syslogd是一个守护进程用来配置监听和记录其它系统利进程的活动。然后把这些记录集中到一个文件里以便日后用类似awk,grep,sed这样的命令来进行分析。Syslog工具有一个配置文件是／etc／syslog．conf。此文件：包含不同重要程度的内容，如信息、警告、紧急、重要。还包括将要发送一个文件的目标接收站如或远端主机。

附加的日志文件位置

本课主要讨论使用／var／admin／Ioginlog。· 下面是一些你需要有规律的进行审计，存在于不同UNIX系统中日志文件：的常见位置：

- ／etc／wtmp：可在Berkerley系统中找到(Solaris利HPboxes)，包含登陆和文件改变的记录
- var／adm／acct或var／adm／pacct：如果允许，用来审计执行过程
- ／usr／etc／accton或／usr/lib／acct：在FREEBSD中刚于跟踪系统执行过程
- ／usr／adm／sulog：在某些系统中用于记录使用su命令的活动
- ／etc／remote：包含UUCP使用的信息。你也可以从／var／spool／uucp／．Admin查到

这些信息有关更多内容我们会在安全审计、攻击和威胁分析篇中详细介绍。

本章小结：

在本课中介绍了帐号安全和密码安全之间的关系，并给出了在NT利UNIX下实现帐号安全的解决方案及具体实施步骤，最后关于UNIX下的安全威胁，可以采取拒绝帐号，监视帐号等方法来解决。

第三章

文 件 系 统 安 全

引　　言

现在你已知道如何实施帐号的安全，并已建立了一个有效的认证机制，接一下来将实施安全中访问控制部分。访问控制必须在两个地方实施，即本地和远程。文件：可以由用户在本地访问或通过网络进行远程访问。本课将对这两种方法逐一进行测试。

本章要点：

- 识别NT本地和远程文件访问控制的权限

- 解释磁盘分区的重要性以及相关安全
- 识别分配和使用共享权限
- 阐明umask和chmod命令的功能
- 描述setuid,setgid,stick刨t的目的以及它们的UID及GID的关系

WindOWsNT文件系统安全

当建立文件的权限时你必须先实现WindowsNT的文件系统(NTFS)，当然你也可以使用FAT格式,但当并不支持文件级的权限。FAT只在那些相对来讲对安全要求较低的情况下使用。即使NTFS也不能认为是能完全地保护文件的，这一点在稍后的实验中你将会看到。一旦已经实施了NTFS的文件系统格式，可通过WindowsNT的资源管理器来直接来管理文件的安全。使用NT资源管理器你可为设置目录或文件的权限。基于文件级的权限你可以分配下面几种：读取(R)，写入(W)，执行(X)，删除(D)，改变(P)，取得所有权(O)。详细请参照下表：

NTFS 权限	基于目录	基于文件
读取(R)	显示目录名，属性，所有者及权限	显示文们：数据，属性，所有者及权限
写入(W)	添加文件和目录,改变一个属性以及显示所有者和权限	．显示所有者和权限：改变文件：的属性：在文件内加入数据
执行(X)	显示属性，可进入目录中的目录，显示所有者利权限	显示文件属性，所有者和权限：如果是可执行文件可运行
删除(D)	可删除目录	可删除文件：
改变权限(P)	改变目录的权限	改变文件的权限
取得所有权(O)	取得目录的所有权	取得文件的所有权

为了简化权限的管理，NT有几种有关权限的标准。通常在分配权限的时候，往往是组合使用权限而不是使用单独的权限，这些权限如下表

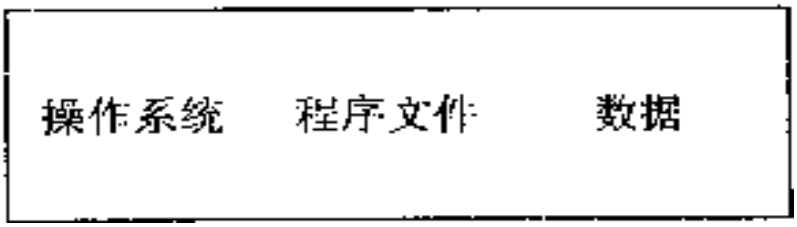
标准权限	基于日录	基于文件：
不可访问	无	无
例出	RX	不适用
读取	RX	RX
添加	WX	不适用

添加和读取	RWS	RX
更改	RWXD	RWXD
完全控制	ALL	ALL

在这些权限的基础上，你可以达到根据需要来访问控制。但是确定什么是你需要的最小权限是困难的。回顾一下第一课我们所讲的一个新建立的NTFS分区默认情况下everyone组对其有完全控制的权限。这种标准是无法接受的，如果你不加选择的删除everyone组或在任何地方都把不可访问的权限赋予给 ’ everyone组，那么有可能会损坏你的NT安装。Everyone组必须可以访问主要的系统目录(比如登陆目录)来使用户能够连接和登陆到服务器上。因为用户在开始登陆的过程中还没有被认证，你必须使用everyone组提供访问以使他们能够被认证。赋予everyone组不可访问其实更危险，因为拒绝访问优先不允许访问，而且所有的用户都是属于everyone组的，这样也就等于完全阻止了对文件系统的访问。
目录的权限分配和文件是一样的，目录的权限影响其目录中新建的文件。换句话说就是任何新建的文件将继承此目录的权限。

磁盘分区

因为操作系统目录的权限是非常严格的，把WindowsNT放置自己单独的分区内是个明智的选择。在这个分区上只安装WindowsNT而不安装应用程序使管理任务简单很多，一个磁盘分区可能会像下图这样。



尽管这种分区需要额外地策划，但它还是很有吸引力特别是简化了对于目录权限的管理。目录可以根据需要分开。如果你在运行一个设备如WEB服务器，你可能会考虑使用HTML，图像和其它一些静态文件：在一个分区上而你的脚本文件则放到另一个分区上。你可以将脚本设置成只可以执行那些静态文件：可允许读取。这种策略的结果就是易于管理文件和目录的权限。

复制和移动文件

最后，你要理解当文件被复制和移动的时候发生了什么。每当一个文件：被复制到一个新的目录里时，这个文件将继承目标目录的权限。当文件移动时，过程是很复杂的。如果一个文件：从一个目录移动到同一分区·下的另一个目录，那么此文件的权限将保留。当文件：在相同的分区内移动时，WindowsNT对于新目录的位置更新目录分配表。当文件：在两个不同的分区间移动时，WindowsNT首先把这个文件复制到新位置，在成功地复制之后，WindowsNTG再删除掉原始的那个文件。一个新文件被建立后，将继承目标目录的权限。

远程文件访问控制

远程的访问一个文件：或目录是通过共享权限来提供的。一个共享就是供远程用户访问文件：的网络访问点。当配置这些共享时，你要设置相应的权限。共享权限的应用类似于在

NTFS上权限的应用。主要的区别是共享权限缺乏精细地权限设置。你只能分配不可访问、读取、更改和完全控制的权限。参照一下表

权限	允许
完全控制	改变文件的权限；在 NTFS 卷上取得文件的所有权： 能够完成所有有更改权限所执行的任务
更改	创建目录和添加文件；更改文件内的数据：更改文件的属性 删除目录和文件；能完成所有有读取权限执行的任务
读取	显示目录和文件名：显示文件：数据和属性：运行应用程序文件： 在目录里可转到另一日录
不可访问	仅能利共享目录建立连接，拒绝访问而且目录里的内容不可见

共享的权限利共享点一定要小心地分配。因为权限仅仅是分配给共享点的，任何共享点下的文件：或目录都足以和共享点本身相同的权限被访问的。

结合使用本地和远程权限

WindowsNT权限的设计是要综合使用NTFS和共享权限。因为WindowsNT的设计是作为一个服务器，用户很少直接访问文件：。当然，共享的安全性对于需要更加安全是远远不够的，因此共享利远程都需要使用。当你结合使用共享和NTFS权限时，两者中最严格的权限优先使用。

UNIX文件系统安全

在UNIX领域里，所有的信息都是储存在文件里，并有一个相关的名字。文件是存储在，目录，但UNIX仍把它看作是文件：。本课的重点是UNIX文件系统是如何处理权限的。

这些权限控制什么样的用户可以访问以及如何访问。文件系统已是强制UNIX系统安全的最基础的方法。

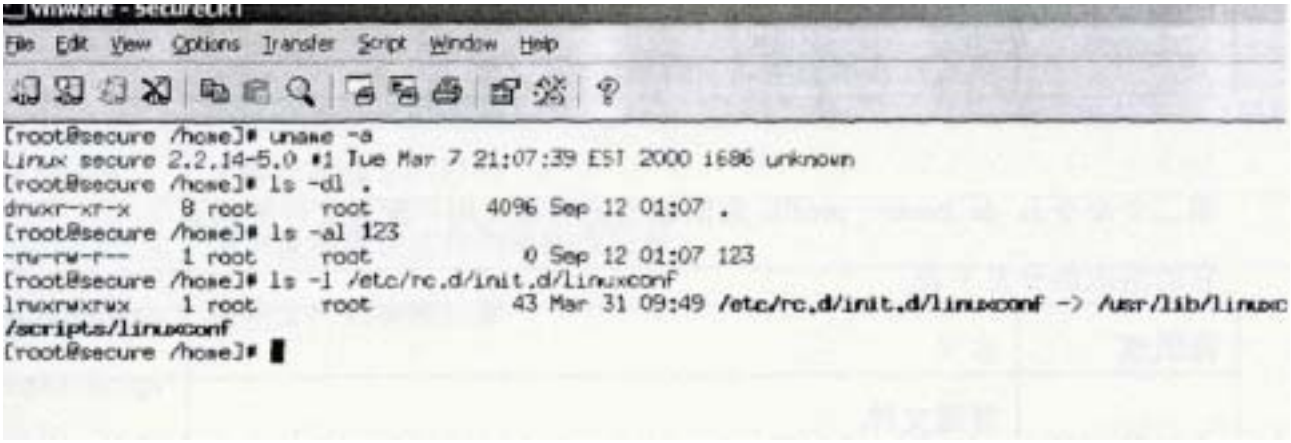
UNIX下的文件格式

UNIX对于文件的读取和写入，是以像树状结构的方式维护的。很多年前，UXNI文件系统就支持长文件名和目录名。所有的文件都有i—节点或连接点；它包含一个文件：所有的统计和后勤信息。一些数据包含：

- 文件类型
- 大小(以字节为单位)
- 参考计数。如果有其它不同名字而实际上是相同的一个文件(叫做链接文件：)
- 拒绝地址列表指示器
- 时间戳。比如文件最后一次访问的时间：文件内容最后一次被修改的时间等
- 安全相关字段：文件属主的UID及GID

● 文件：访问权限或位，也称做Mode bits。

Ls命令是最常用的UNIX命令，刚来查看文件：和目录的权限。如下图显示



第一个命令1s-Id．意思是：

列出当．下的内容通常．是指当前的目录；在本例中，用户自动地登陆到他的主目录中，而命令中的．是作为当前目录的意思

对于命令输出的结果详细说明见下表

输出符号	含义
d	表明目录
r	属主可以读取访问
W	属主有写权限
X	属主对目录有搜索及执行权限
R	属主所在组的用户有读取访问的权限(本例中是 staff 组)
-	属主所在组没有写权限
X	属主所在组对目录有搜索及执行权限
R	其它用户有读取权限(任何人)
-	其它用户没有写权限
X	其它用户对目录有搜索及执行权限
4	参考计数
test	属主的登陆名
Staff	属主用户所属于的组名
512	目录的大小(字节)

Time Stamp	最后一次改变大小的日期
08：41	改变时的时间
	所有这些信息所属于的文件名

第二个命令ls-la．bashrc_profile如图输出的的有关用户配置文件的信息
它的组成部分见下表

范围值	含义
-	普通文件
R	属主有读取访问权限
W	属主有写权限
	属主没有执行权限
R	属主所在组有读取权限
-	属主所在组没有写权限
-	任何组都没有执行的权限
R	其它用户有读取权限(任何人)
-	其它用户有写权限
-	其它用户没有执行的权限
230	文件大小
TimeStamp	文件建立的日期。

第二个命令ls-lal23列出一个普通文件的权限。此文件在这里叫123。1s．俞令通常都是列出其属主和其它用户对此文件有什么样的特殊权限。
第四个命令ls—1／etc／rc．d／init．d／linuxconf主要列出了linux重要配置文件：linuxconf的权限。参照表3-6

文件值	含义
L	链接：文件指向另一个文件
Rwx	属主有完全控制的权限
Rwx	属主所在组有完全控制的权限

RWX	所有其它用户有完全控制的权限
1	参考计数(说明是唯一的文件：)
Root	此文件：真正的所有者
Root	文件：所属的组名
43	文件大小(字节)
Time Stamp	文件首次建立的日期
->	用来说明真正文件的链接或符号
／usr／lib／linuxconf／redhat／scripts／linuxconf	说明文件的物理位置

现在你已经理解了在UNIX下的文件或目录不同模式位所代表的含义，下面我们将用不同的方法来改变它们。

Theumask命令

Umask命令广泛地应用于所有的UNIX系统当中用于设置文件后来的模式位。它还经常 常应用于登陆文件中来设置默认的权限。键入些命令会显示出当前值。要想改变这个值，用户要加不同的参数来改变默认的模式位。

有关模式位的总结见表3—7

模式值(八进制)	八进制模式的含义
7	读取，写入，和执行
6	读取和写入
5	读取牙口执行
4	只读
3	写入和执行
2	写入
1	执行
0	不可访问

通常对普通文件：默认的权限是666(属主、所在组及其它用户有读取和写入的权限)。每个位(八进制值)都分配给文件的三个组成部分(属主、所在组及其它用户)。对于一个可执行的程序默认的权限可能是777(对所有的用户都是有读取、写入和搜索执行的权限)。Umask命令默认的"mask"为022，通常与文件的模式位相AND来改变，比如对一个默认权限为0666的文件：作AND得到最后的模式位为0644，也就是最后文件的权限为属主有读，写权限，所在组利其它用户有只读的权限。

在一个站点中的所有的用户都期望保护他们自己的数据，默认情况＇下，是由其它用户来检查的，所有的用户都应该有一个UMASK值为077。如果用户需要和所在组的用户协同完成项目时，那么umask值为037是最佳的选择。

The chmod命令

Chmod命令是用来操纵文件权限的。这个命令可以以两种方法来应用

. 绝对模式：当使用这种方法时，命令是这样的

chmod 666 filename

这里，权限的模式位已经被绝对地应用到了文件：上。应用到不同组成部分上的权限(如属主，组，其它用户)取决于输出的模式位，请参考表3—4

. 符号模式：当使用这种方法时，命令是这样的

chmod a+rwx filname

这里，对于些文件所有用户的权限都是可以读取、写入及执行。因为这些符号符合利用ls命令所显示出来的描述。

下表总结了所有Chmod命令使用的符号

符号	含义
U	用户或属主
6	组
O	其它
A	所有的用户，组和其它部分
+	增加这些权限
-	去掉这些权限
=	设置权限等于

UID和GID

所有的对象都用灵活的方法来控制描述文件的权限位。这些对象是文件：、可执行程序等。这些信息保存在对象所在文件系统的索引节位置上。每个文件信息节点的主要位置是来设置这些位的。通常情况—下这些位置是16位并且把它作为一个实体来处则。其中九个位用来设置文件的模式(如读取、写入，执行或者无位)。三个附加位用来描述在一个文件：中这些位是如何协同UID利GID来共同工作的。UID是独一无二的，并且表明在系统的／etc／passwd文件：中。GlD也是唯一的，描述在系统／etc／Group文件。

当某用户开始使用系统时，一个程序开始调用，这个程序由内核来跟踪然后分配资源如内存、CPU、I／0等等。为了帮助内核跟踪这些信息，每个程序必须有一个程序标识符(PID)。每一个PID在它的表里都有四个其它数字，两个类似于UID和G1D。另外，也会分配一地特殊的UID和GID，叫做有效UID利GID。这种程序有时需要获得不同于主UID和GID的标识符(比如转为其它用户或增加权限以更改用户密码)。在这种实例中，有效的UID和GID是不同于初始值的。这些有效值是由UNIX内核来评估并分配安全访问的权限。

SETUID、SETGID和粘制位

UNIX允许程序在运行的时候取得其它的UID和GID。当一个程序改变它的UID时叫SUID(set-uidorsetuid)程序：同样，当一个程序改变它的GID时，叫做SGID(set-gid or setgid)程序。当一个程序改变它的UID或GID时就是在设置文件权限的SUID或SGID的权限位。一个程序可以在同时设置这些位。

下表3—9列出了用于改变有效UID或SID的特殊位

权限位	含义
s	当设置文件属主的内容时，标明如果 UNIX 内核执行那么它的有效 UID 将设置成那个属主用户的。
S	说明设置了 setuid，但执行位(x)并未设置　　，
s	当设置文件的组内容时，标明如果 UNIX 内核执行那么它的有效 UID 将设置成那个组。
S	说明设置了 setgid，但组的执行位(x)并未设置
t	在程序终止后，不会立即从 UNIX 中的交换页面区域删除。这个选项已经过时了。现代的 UNIX 系统忽略这个位并且自己来管理内存。
t	当设置在目录上时，一个用户如果对目录下的文件：有写的权限则仅可以删除此目录下的内容。通常，在目录上仅需要有写的权限

在信息节点的16个位上setuid位处于第12个位上，setgid位于第11个位上，粘制位通常处于剩余的10个位上。程序需要利用SUID／SGID的特性获得特殊的权限。举个例子， passwd这个程序，必须写入到系统的密码文件：里，需要以有root权限的身份来执行任务。 因为SUlD／SGID机制临时地赋予给用产更多的权限，所以对系统中所有有这些设置位的应用程序必须监视和检查改变。

本章小结：

通过对文件权限的严格设置是实现系统安全的一个必需步骤，通过本课的学习达到对NT和LINUX的文件权限有了深入的了解，并对权限的分配具体操作灵活使用。

第四章

评 估 风 险

引　　言

为了保护你的计算机系统和网络，必须对潜在的安全威胁提高警惕。如果你理解了安全，你就能很敏感地对你的计算机系统利网络进行风险评估。在本课，你将复习安全威胁和识别在WindowsNT下和UNIX下特殊安全相关的问题。

本章要点：

- 识别普通和特殊的操作系统攻击手段
- 更改WindowsNT系统的默认值以增加安全性
- 扫描一个系统来判断哪些服务在运行并存在安全风险
- 解释UNIX安全的有关因素，包括rlogin命令，NIS和NFS

安全威胁

网络中基本上存在于两种或胁：

。偶然的威胁：主要是由一些天真的用户没有做预先的考虑和计划。举个例子，一个用户可以远程地访问系统并且可能偶然地建立了一个以前用户没有彻底中断的登陆会话。第二个用户就很可能访问到先前用户访问过的一些至关重要的信息。

。有意图的威胁：执行一个有计划的行动。它的范围可能是从一些简单的文件：固定的数据，到整个系统的体系改变来进行恶意的破坏。

有意图的威胁义可以进一步地分为两类：

。被动的威胁：比如在网络中利用sniffer捕获数据包没有警告内容或改变目的地址。数据的合法用户对这种活动一点也不会察觉到。

。主动的威胁：主要是包括修改信息或用于正常运转的数据。一个例子就是如果一个系统接收到错误的IP地址时，它会浪费时间的大连接那个非法主机，从而负面地影响了其它的用户。

攻击的类型

现在你已经了解了威胁的一般分类，你还要能对攻击的类型进行分类，这包括：

Spoofing or masquerade attacks：这种攻击，一个主机(程序或应用程序)伪装成另一个主机或网络上的实体。通过与另一台主机建立信任的关系来进行欺骗性的攻市，并且任何交易都会导致更进一步的危害。

Replay attacks：是指网络数据包在传输过程中有其自己的包头或内容，目的是完成欺骗。内容的伪造是为了避免检查，如checksums等。最终的目的是取得访问权或突破安全。

拒绝服务攻击：拒绝服务攻击是使主机或系统不能正常地运转因为网络上的另一个程序或节点正占用着所有的资源(如快速的请求的flood)。举个例子，对于每个请求发送异乎寻常的高速的数据流导致返回的是错误的网络地址，使主机在网络中的缓

冲区无法工作，因此其它合法的用户也不能使用此服务。

内部攻击：内部攻击是非常常见的而且在很多类型攻击中都会发生。这种方法利用在外部攻击取得非授权的访问然后可以在内部进行活动，有时这是非常容易的，因为安全的措施主要是防止外部的攻击。在应用程序之间窃听信息以及危及现有的控制机制是常用的二种技术。

Trapdoor attacks：在这种trapdoor攻击中，一些命令容易被使用并且激活时，会产生潜在的非授权访问。比如，尽管登陆帐号有着较好的密码保护机制，但一些帐号是用来运行诊断(通常具有很高级别的权限)并可能留下易遭入侵的程序漏洞。虽然入侵者不能利用那个帐号来登陆，但他能观察文件：并看到利用SUID转为root的一些应用程序。执行这些应用程序即可取得较高的权限来进行破坏活动。

特洛伊木马：特洛伊木马是trapdoor攻击的一个变种。它把一些非授权的命令隐藏在一个看似实现普通功能的程序中来产生突破口。

在UNIX中，最常见类型的特洛伊木马类型之一就是root kit，它是代替合法程序的程序，利用email把系统中／etc／shadow文件的内容发送出去，或捕获登陆的序列并通过email发送出去，完成明文密码的拷备。Solaris和Linux更倾向于这种木马的攻击。

击键记录的威胁

一个特殊威胁的类到就是键盘记录程序(keylogger)。键盘记录如果安装到你的网络系统当中，可以造成很大的安全威胁。在无形中记录一下计算机中所有的击键记录并存储在一个文件里，并有可能通过预先设置的E-mail发送出去。下面列出了Keylogger程序的一般特性

- 截收所有的键盘市键记录，鼠标记录，活动窗口标题，静态文本及用户的其它输入
- 悄悄地运行着并且不会影响受害者计算机的性能
- 截取密码和登陆名
- 保存用户名利登陆时间
- 保存访问过的WEB站点的URL
- 对输出的日志文件加密

可以访问http：／／www,keyloggers．com来下载for Windows NT／2000的keylogger程序如果想下载forUNIX或LINUX版本，访问http://www.multimania.com/cdc/keylogger.htm

WindOWSNT的安全风险

WindowsNT像每个其它重要的操作系统一样，包含许多默认的设置和选项，允许更复杂的管理。这些系统默认值可以被有经验的攻击者用来渗透系统。有些默认值不能改变，但有些可以改变。这些改变可以提供足够的安全性。

默认目录

在WindowsNT初始化安装后要考虑很多默认选项的安全性。例如，WindowsNT4．0默认是安装在系统主分区的＼WINNT目录下。使用不同的目录对合法用户不会造成任何影响，但对于那些企图通过类似WEB服务器这样的介质远程访问文件的攻击者来说大大地增加了难度。

默认帐号

在前面的课程里我们曾谈过对帐号改名。对于administrator，Guest和其它一些系统帐号

都应该改名。其它一些帐号，比如IUSER－MACHINENAME是在安装llS后产生的，对其也应该改名。

默认共享

WindowsNT出于管理的目的自动地建立了一些共享。包括CS,DS利系统其它一些根卷。ADMIN$是一个指向＼SYSTEMROOT＼目录的共享。尽管它们仅仅是针对管理而配置的，但仍形成一个没必要的风险，成为攻击者一个常见的日标。你可以通过增加注册表＼HKLM＼System＼CurrentControlSet＼Service＼LanManServer＼Parameters下一个叫AutoShareServer的键值，类型为DWORD并且值为0，来禁止这些管理用的共享。对于-使用Windows NTWorkstation的机器，键值名为AutoShareWks。 ·

系统扫描

黑客在侦查阶段经常使用系统扫描器。扫描程序黑客来识别系统和网络上可能存在的漏洞。扫描程序还可以帮助管理员来发现他们系统上潜在的漏洞。有关扫描详细的内容我们会在安全审计、攻击和威胁分析篇中详细介纠。

UNIX的安全风险

为了能够适当地保护一个UNIX系统，你必须留意那些本来就存在的主要应用程序和命令。’下面列出了一些常见的UNIX安全风险

- rlogin命令
- 网络信息系统(NIS)
- 网络文件：系统(NFS)

Therlogin命令

rlogin命令是从BerkeleyUNIX的品种中演变出来的，适应网络供给及分布式系统访问。rlogin命令可以被设置成不需要输入密码。rlogin命令实际上违反了安全的初衷，因此多数系统上根本就不再支持它。其它一些系统，包括LINUX，支持这些命令的较高的修正版本。

远程系统通过下面两个文件：来检查用户的身份：

。 ／etc／hosts.equiv(有些系统不支持此文件：)

。 远程系统的．rhost文件，在远程用户的主目录下

第一个文件是系统级文件主要由系统或网络管理员来维护。显然地，如果这个文件：的权限被危及，那么几乎任何一个入侵者都能远程地登陆到目标主机上。第二个文件存在于目标系统的主目录里；它的权限也一定要安全地维护。

在一般的rlogin执行过程中，etc／hosts．equiv文件用来检查源系统的主机名，如果出现，则进一步的远程登陆过程继续。如果未出现，那么第二个文件：(．rhosts)将被用来检查源主机的主机名。任何一种方法，可能都要呈现给远程主机要求的登陆名以作为用户的身份。然而，如果系统主机名没呈现，或不匹配．rhost文件里的内容，则rlogin程序将自动地要求输入密码。rlogin的－1选项是很有用的因为不是在每个系统上都能得到同样的或唯－的登陆名。rlogin是工作在TCP层上并使用513端口，可参照／etc／services文件。

Telnet与riogin的比较

在Telnet方案中，典刑的基于TCP／IP网络中简单的客户端服务器模式。而且，Telnet不担当信任远端的目标主机，让两台客户机和服务器通过一般的认证。在二个系统间交换的网

络数据包是不经过加密的。

与rlogin／rlogind方案类似，除了rlogin程序的认证需要信任的模式。所有被信任的用户都可以访问到远程系统。Rcp和rsh是rlogin的相关命令：它们允许在系统间复制文件：或在远程系统上执行命令，它们和rlogin一样使用相同的信任模式。在支持／etc／hosts．equiv文件的系统上，此文件：利用将远程主机的名字写入，来允许任何想登陆主机的用户有着相同的信任关系-一如果登陆是发生在目标主机上。rlogind首先从上至下地检查／etc／hosts．equiv文件：内容，直到发现匹配允许进入系统的主机名字。要hosts．equiv文件里有一些特殊如·下：

novas.com

-@trainlng

+@finance

第一选项说明在“ noyas.com ”主机上的所有用户可以以他们自定义的登陆名来登陆目标主机面不需要密码。noyas因此是受信任的主机。

-@trainning项用于不被信任或不允许登陆目标系统的网络组。相反，+@finance是完全受信任的允许访问的网络组。

有关NIS的安全

网络信息系统(NIS)是在本地网络中创建分布式计算机环境的方法之一。NIS最早由SUN公司发明。它作为一个网络数据库存储着一些重要的配置把网络中的机器绑定到一个单独的可用的实体里。

NFS是跨网络的分布式文件：系统。通过NFS机制，服务器端可以将自己的一部分文件：凋出，让多个客户主机透明地使用服务器上的文件：和目录。客户通过mount这些从服务器端凋出的目录和文件：，就像使用-本机的文件：一样方便。对于客户端的用户来说，当访问这些凋出来的文件：时，几乎不会感到访问这一文件卷与访问其它文件卷有什么区别，或许会感到稍稍有一些延迟而已。

为了理解使用像NIS系统的需要，设想一个UNIX的网络供很多的人使用。对于一个想登陆到网络中不同机器的用户，可能在每台机器上都需要不同的帐号和不同的密码。这种方案是非常笨掘的；用户可能更需要只使用一个单独的，集中管理的网络密码就能登陆到任何一台机器上。NIS的一个主要目的就是提供集中的密码数据库来允许只有一个单独帐号的用户在网络中任一台机器上都有效。

管理一个大型的UNIX网络除了维持一个集中的密码数据库外还有其它一些问题。一个问题就是要维护大量的用于保证系统正常运转的配置文件。不像NIS系统那样，要改变机器上的配置需要管理员登陆到每一台单独的机器上进行一些必要的修改。NIS允许一些相应的配置文件从一个中心区分布，从一个单独的位置作改动时将会通过网络遍及到其它地方。NIS仍然被LINUX,AIX,HP-UX广泛地使用，Sun最近已经把其系统默认使用升级到NIS+。NIS+与NIS非常相像，但有许多新的功能。

NIS的不安全因素

NIS服务天性就是不安全的。这种不安全来自系统运行时多方面原因。　下面讨论一些主要问题。

没有认证的要求

内置的RPC协议不要求主机联系端口映射或其它的RPC服务来验证它们自己。对于这种

缺乏安全的部分解决方法如’下

- 使用wrapper程序来允许你拒绝端口映射访问那些含主要IP地址或域名的主机。
- 在强固的防火墙后使用RPC协议，并信任防火墙内的任何主机
- 使用"secure RPC"来加强RPC。

通过广播联系服务器

使用ypbind通过广播来联系服务器。因此，能够访问本地网络的任何大都能通过ypserv执行和分布假的NIS映射。近来一些ypbind的版本(如由Linux发布的)允许当你启动ypbind时专门指定NIS服务器的IP地址。参考／etc／yp．conf文件：

明文的分布

NIS的映射是以明文的方式分布的。特别是NIS密码的映射可以被任何在网络中使用ypcat程序访问的人读取，因此即使加密后的密码也可以看到。一些NIS的版本允许发布shadow密码映射，略微地改进这些问题。然后，一个包捕获程序(如tcpdump)仍能到这捕到这些shadow映射，揭示加密后的密码。并通过字典程序来破解这些密码。

加密和认证

yppasswdd守护进程即不对事务处理进行加密也不使用任何的验证机制。因此当用户改变密码时，密码会以明文和未加密的形式在网络上传输。

端口映射过程和TCPWrapper

Linux当前的版本加入了增强的端口映射过程，由host．allow利hosts．deny来进行控制。这使得RPC服务被严格限制在特定的网络中。要想允许访问应当在／etc／hosts．a11ow 文件：中加入一行：

Portmap：XXX．XXX．XXX．XXX

XXX．XXX．XXX．XXX表示某网络或主机的IP地址。类似的，在文件：／etc／hosts．deny中增加同样的一行会禁止它们对网络的访问。 。

Securenet 文件

NIS安全性的一个重要的提升是从SunNIS服务器和Linux服务器上的Securenet文件获得的。这个文件：允许你限制哪些网络和子网的主机可以访问NIS服务器。该文件：的形式如下：

#Pound signs denote comment lines

netmask network

在这里用网络地址来表示网络，网络掩码用来比较要求进入的IP地址和列出的网络地址。值得注意的是这里网络掩码是往前面，网络号是在后面；如果地址吻合，则要求被允许。为了使这些步骤更清晰，—下面提供了一个Securenet文件的样例：

```
#
# securenets
#ThiS file defines the access rights tO your
#NIS server for NIS clients．This file contains netmask／network
#A clients IP address needs tO match with at least one Of those
#
#One can use the word“host”  instead Of a netmask Of
#255．255．255．255．Only IP addresses are allowed in This
#file，not hostnames．
```

```
 #
#Always allow access for localhost
 255．0．0，0      127．0．0．0
#This line gives access tO everybody．Please Adjustl
0．0．0．0      0．0．0．0
#ThiS line allows access tO anyone On the 198．168．1．0
#subnetwork
255．255．255．0 198．168．1．0
```

使用Securenets文件可以在一定程度上增强NIS的安全性，但是却不能解决所有的NIS安全问题。

NIS+的不安全因素

SunMicrosystems开发了NIS+来弥补NIS的局限性并提供了更强大的数据库结构。N1S+和NIS的目的相同，都是提供客户端/服务器的结构来共享网络的资源，例如用户的账号。由于NIS+不能运行于Linux或任何除了Solaris的UNIX版本中，所以你无法用试验来说明它。

NIS+与NIS相比有如一下优点：

- 更多的映射：NIS+能够比NIS发布更多的映射，因此NIS+的数据库中可以集中管理更多的系统配置。
- 分层的数据库结构：NIS是一个平面式的数据库，并没有子域的概念。NIS+允许你建立分层的域和子域，这一点更象DNS。这个功能使NIS+能够用于更大的安装。
- 对从属服务器进行增量升级：NIS在数据库更改时必须要把整个的NIS映射分发到从属服务器：NIS+服务器可以只分发改动过的数据。当映射很大时这一功能可以极大地提高效率。
- 存储信息：客户端用存储的信息来定位服务器，而不使用广播
- 在主机和用户级进行合理地验证：NIS+支持NIS主要的概念，NIS+域中每一个实体代表一台主机或一个用户。NIS+提供基于公钥加密的信任状，这可以使一个用户登录到NIS十域中的一台主机并且声明其身份和权限。
- 建立NIS+主要的具有共享权限的组：组也可以分层次。　　，
- 允许和拒绝访问：NIS+在NIS组的级别允许或拒绝对NIS+表中的数据进行访问。访问可以被限制在那些有信任状的主机或用尸。访问还可以对所有大开发，包括没有信任状的机器或刚户。
- 可以设置权限：使用N1S+，密码的映射被组织成任何有信任状的用户和主机可以读取除加密的密码外的所有部分，而加密过的密码只能被root读取。这种方法和在NIS映射中使用shadow密码的效果相同。

NIS+提供如此多的新功能增加了管理的复杂性。大多数的复杂性是由加强安全性引起的。跟踪信任状更是个恶作剧，你可能因为错误的设置而不能登录服务器。

另一个缺点是由于NIS+要提供兼容性引起的。NIS+的fuwq可以允许在NIS兼容的模式下，这样NIS的客户端可以从服务器接收信息。然而，在这种兼容模式·下工作时，所有NIS+增强的安全机制都必须被禁止。总而言之，如果你使用了NIS+所有的功能的话，会比NIS更安全。

NFS的安全问题

网络文件系统(NFS)是在UNIX网络中使用的文件共享协议，它是由SunMicrosystems开发的分布式文件系统。在UNIX环境—下有很多应用程序，包括：

- 分布式宿主目录：如果某个用户的宿主目录位于NFS服务器上输出的文件系统中，然后被网络上其它计算机mount上，则该用户无论登录任何一台计算机都可以访问这些文件；。与NIS网络的密码配合，从用户的角度来看NFS可以使大量的计算机互换。
- 集中管理软件包：一个大的软件包可以安装在NFS服务器上的某个分区内，然后将该分区输出供其它主机使用。管理工作只需在服务器上进行，客户端可以立即使用升级的软件包。
- 节省磁盘空间：可以把很少改动的大文件安装在共享的NFS分区，然后共享给其它计算机。例如，可以把UNIX完整的使用手册安装在输出的NFS上共享给网络上的计算机。

使用NFS会带来两种安全问题。首先是管理的同步问题，包括在各种机器上的用户和组共亨NFS分区，允许或拒绝某些主机利用户访问特定的文件系统。第二个问题更基础，它涉及到NFS系统不适合在有不信任主机的环境中使用的弱点。

用户、组和NFS的关系

当客户端的机器远程mount上服务器的NFS分区，它必须提供该分区上有关文件所有权的用户ID和组信息。例如，主机nfs_server输出了文件：系统／export／home，客户端主机nfs —_client挂接该分区为／home。在nfs_server上目录／export／home／usr的所有者是UID为501的用户，该目录在nfs cLIent上显示为／home／user，所有者是UID501。然而，UID501将由客户端计算机来解释，所以客户端的UID501的用户必须和服务器上UID501的用户相同。组ID也存在同样的问题。

SecureRPC

各种访问控制机制要受到各种各样的限制：在检验身份时没有严格的验证机制。例如，你使用文件／etc／exports来限制对／psycho分区的访问。一台主机声明它是被允许的主机，同样，一个用户也可以声明他上UID为1001的用户而不需要验证其身份。

Secure RPC协议试图在申请NFS资源时增加一种严格的验证机制。它是基于公钥和私钥的加密系统。通常情况下，当客户端要从运行Secure RPC的服务器上获取资源时，客户端和服务器会使用公钥加密来交换“ conversationkey ”。这个conversationkey会将时间戳加密到每个RPC请求中。服务器可以信任从客户端发送来的请求，因为它可以使用conversatiOn key将这些时间戳解密。

NFS安全小结

NFS协议在本质上不安全，归于以—下问题：

- RPC不安全：RPC协议没有内置的验证手段，所以使用NFS的主机不需证明其身份。
- Secure RPC也不安全：Secure RPC使用的公钥方法在原理上是安全的，但是Sun选择的密钥长度太短以至于很容易被破解。
- NFS文件传输时未加密：即使使用了Secure RPC，在网络上传输的大量数据并未加密。象TCPdump这样的程序可以捕获通过NFS挂接所传输的所有文件

基于以上原因，NFS最好使用在处于防火墙保护之下的可以信赖的网络中。

本章小结：

在本课中，我们了解到了UNIX和Windows潜在的一些安全问题。并学习了常见的操作系

统攻击手法，包括keylogger。更改Windows附操作系统的缺省设置来增加安全性，及通过扫描系统来确定正在运行那些服务， 以及它们所处的安全等级。我们还学习了关于UNIX操作系统的命令，如rlogin等。最后讨论NIS和NFS的安全问题。

第五章

降 低 风 险

引　　言

简单的更改一些操作系统的默认设置和一些权限的控制是不足以目前存在的各种攻击方式，在本课我们将进一步学习如何保护NT和UNIX－下所存在的安全隐患。

本章要点：

- 理解操作系统补丁和HotFix的目的和重要性
- 为增强安全性修改WindowsNT的注册表。
- 了解，安装和在UNIX中使用TCPWrapper利MD5。
- 分析WindowsNT中的审计日志。

PatChes和Fixes

许多操作系统和系统软件中存在的漏洞会威胁到操作系统安全。操作系统的厂商定期地为其产品发布这些漏洞的补丁和修复方法。这些patch可以解决操作系统的某些特定的问题，包括安全问题。这些厂商通常会建议除非那些补丁能够解决你系统中的实际问题，否则不要安装他们；厂商的补丁和flx都有相关的文档。系统管理员应当仔细阅读这些文档来确定该补丁或fix是否适合你的网络。下面的章节包含了下载WindowsNT和Linux的patches、fixes和文档的位置。

Microsoft service packs

任何像WindowsNT操作系统这样的复杂程序都必然存在各种各样的漏洞。虽然，大多数的漏洞并不会威胁操作系统，但不幸的是，少数涉及安全风险的漏洞会酿成大祸。微软以service pack的形式来发布主要的操作系统升级。本教程使用Service Pack6a。在发放Service Pack各升级版本之间微软公布的系统修复方法成为Hot Fixes。这些特殊问题的补丁可以解决一些特定的漏洞。微软的Service Pack包括了NT的补丁和热修复。Service Pack位于www．microsofi．com／ntserver，在那里有最新的WindowsNT4．0的ServicePack。

大家知道ServicePack的每一个升级版本都包含了前一版本的内容，但由于微软的疏忽偏偏在Service Pack6的时候忘了加Service Pack5的内容，也就是说Service Pack5所能防止的漏洞ServicePack6却不能，这个问题是严重的，直到最后微软才公布了Service Pack6a。

Red Hat Linux勘误表

由于存在许多种类的UNIX，所以要到适当的站点寻求支持。例如，Linux的用户可以购买RedHat的产品，这样可以获得其厂商的支持。RedHatLinux的勘误表包含了其产品的补丁和fix，它位于如下的网Jll：www．redhat．com／corp／support／erratao

警告：

由于替代了核心的系统文件：，这些补丁通常可以卸载。你需要选择该功能提供的选项。在没有备份文件的情况下，如果补丁不稳定的话，操作系统可能无法回复。

无论补丁的功能如何，你都应当在安装它之前对系统进行完整的备份。如果可能的话把补丁安装到操作系统之前，最好先在试验的环境进行测试。

注册表的安全性

所有配置和控制WindowsNT的数据最终都存在于注册表中。所以，如果注册表不；安全的话，则WindowsNT的安装也不安全。你对操作系统所做的许多改动都会更改注册表。同要保证文件：系统的安全一样，你必须也要保证访问注册表的安全。

到目前为止，大多数的漏洞集中在允许以只读的方式来访问部分注册表。就像NTFS文件系统的缺省权限一样，注册表中许多部分的缺省安全设置对保护系统来说并不足够。像我们已经使用过的RedButton，就是通过远程访问没有实施正确安全保护的注册表来进行攻击的。不幸的是，了解需要保护注册表，知道那些注册表的内容需要得到保护和如何对它们进行保护是截然不同的问题。微软从没有公布过一份完整的文档来解释如何对注册表的各部分进行权限设定。在本课中我们将要试验的大部分设置都经过了在微软之外的研究和测试。

注册表结构

WindowsNT中的注册表是一系列的数据库文件：，主要存储在＼WlNNT＼System32＼Config目录下有些注册表文件：建立和存储在内存中。这些文件的备份也存储在＼WINN％Repair 目录下。你应当应用NTFS权限来保护这些文件：和备份。只有系统的账号才需要访问这些文件。一旦数据库文件：得到了保护，你就需要使用regedt32程序来对注册表本身进行安全的设置。由于regedt32没有已经存在的快捷方式，所以你需要从run菜单中运行它，点开始一运行，输入regedt32。运行regedt32程序后，你会看到注册表的五个主要的组成部分。每个部分是一个子树，这些子树的总体组成了WindowsNT中所有的系统配置。　下表列出了这些子树和它们的用途。

子树	描述
HKEY_LOCAL_MACHINE	包含了所有与本机有关的操作系统配置数据。 在这里存储了像装载哪个设备的驱动等信息。 不论在本机登录的用户是谁，该子树的内容不 变。

HKEY_USERS	包含两个子键： ● ．Default：包含在 CTRL+ALT+DELETE 登录画面显示时操作系统使用缺省设置。 ● 当前用户的安全标示符(SID)
HKEY_ CURRENT_ USER	包含当前用户的交互式的数据。任何曾经登录过本机的用户都有这个子树的副本，并存储在＼WINNT＼Profiles＼username 的目录下，文件名是 NTUser．Dat。如果这里和 HKLM 中的任何 key 相同的话，该子树的值优先。这个子树实际上是指向 HKU＼SID。
HKEY_ CLASSES_ ROOT	包含软件的配置信息，例如文件：扩展名的映射。它实际上指向＼HKLM＼Sofiware＼Classes。
HKEY CURRENT CONFIG	包含了活动的硬件配置的数据。这些数据来自 HKLM 的 SOFTWARE 矛 USYSTEM。

如你所见，大多数的注册表都源自HKLM子树。保护HKLM子树同样重要，因为攻击者会使用在HKLM中的优先权来覆盖那里的设置。

HKLM本身也包含了几个独立的子树，如下表为所示．

子树	描述
Hardware	每次 Windows NT 启动时都重新建立。它包含了连接到计算机的物理设备的信息。
SAM	包含真实的用户账号和密码。SAM 不能直接访问，但可以通过 Windows NT 操作系统的 API 来访问。
Security	包含所有本机的安全信息。与 SAM 子键相同，该项也不能直接被访问。
Software	包含独立于当前用户的程序配置信息。
System	存储计算机中服务和设备的配置信息。

注册表访问控制

一旦确定要保护什么，先选择它，然后从“ 安全 ”菜单中选“ 权限 ”，存在两种主要的安全权限和几种细致的权限。主要的安全权限是读和完全控制。细致的控制权限在下表列出。

权限	描述
查询数值	允许某用户和组从注册项中读取数值
设置数值	允许某用户和组在注册项中没置数值
创建子项	允许某用户和组在给定的注册项中建立子项
计数子项	允许某用户和组识别某注册项的子项。
通知	允许某用户和组从注册表的项中审计通知事件：
创建链接	赋予用户或组在特定项中建立符号连接的权限
删除	允许用户或组删除选定的项
写入 DAC	允许用户或组获得将目录访问控制列表写入注册表项的权限。这是一种有效的更改权限
写入所有者	允许用户或组具有夺取注册表项的拥有权的权限。
读取控制	允许用户或组获得访问选定注册表项的安全信息。

如同设置文件安全，先选择组再选定你希望赋予的权限。

注册表的审核

如同审核文件系统，你需要监视对特定的注册表区域的访问行为，对已经加以保护的注册表区域的审核尤为重要。如果你得知有人试图访问这些注册表项，你实际已经得到了攻击者在收集信息的阶段的报警。在注册表中设置审核同在文件系统中设置审核相同。

再次强凋，对Everyone组的审核通常是个明智的选择。

仔细地选扦审核注册表中的哪些内容是非常重要的。注册表每秒钟被访问成百上千次如果你审核太多的内容，那么系统的负担是巨大的。

禁止和删除WindOWSNT中不必要的服务

在加强像WindowsNT这样比较新的操作系统的安全性时，最艰巨的任务是如何弥补现存服务中大量的安全漏洞。大多数的服务并不包含安全问题。另外，某种特定的应用并不需要WindowsNT所提供的大多数服务。由于WindowsNT被设计成功能强大的网络操作系统，所以它提供的大量的服务。大多数安装的WindowsNT都被配置成提供某种特殊的用途和目的。通过删除不必要的服务，你可以减小潜在的风险。

举个很好的例子，例如Windows NT中包含的OS／2和Posix子系统，包含它们的根本目的是向后兼容。在Windows NT Resource Kit中的C2Config 1 :具可以删除0S／2和Posix子系统。

除了OS／2和Posix子系统外，还有许多服务应当被删除。

有些服务无法在不损坏WindowsNT的前提下轻易删除，因此必须将其禁止。典型的服务是Server服务，由它来处理进入的NetBIOS网络请求。实际上，运行该服务将开启很多不必要的漏洞。通过禁止该服务，你可以使大约三分之二的破坏WindowsNT的工具失效。有时你无法在内部禁止一些服务，因为你必须在提供内部用户连接该服务的同时还要防范外部用户使用它们。这种禁止服务的方法是最低的需求，但是起码比让它们被直接访问到要好。

下表列举了一些你应当对外过滤的常见的Windows NT服务，以及这些服务的监听端口，你可以在路由器或防火墙上过滤掉这些端口。

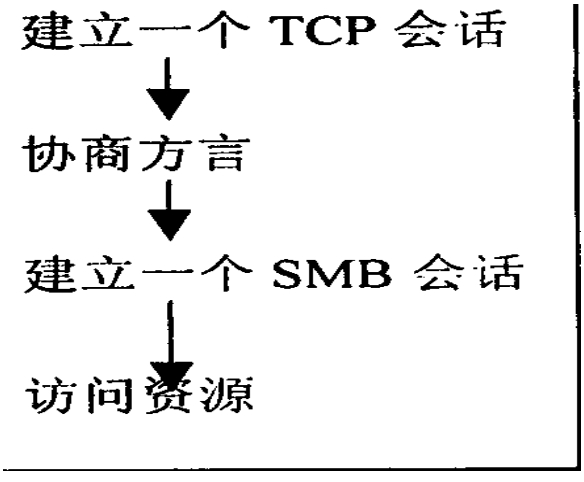
服务	使用的 TCP／IP 端口
DNS 区域传输	TCP 53
MS 网络	UDPl37 和 138：TCPl39
MS RPC	TCP 135：UDP 135
MSRPC(secondary)	UDP 1028
MSSQLServer	TCP 1433
SNMP	TCPl61 和 162：UDP l61 和 162

加强网络连接安全

一旦你禁止或过滤了服务，你需要设法保护网络。你可能还记得要达到C2的安全等级，WindowsNT将不得不禁止网络功能，这是由于WindowsNT使用的网络协议的一些设计上的问题造成的。

WindowsNT的网络是基于ServerMessageBlock(SMB)协议的，该协议是NetBIOS协议的改进版本。幸运的是，大部分或所有网络中现存的问题都可以被更正或补偿。不幸的是，许多问题的解决要付出超过所获得的安全好处的代价。

右图品示下SMB连接过程的概要。



WindowsNT网络使用六种方言，按性能排列分别是：

- PCNetwork Program 1．0　　．
- MicrosoftNetworks 1．03
- LanMan 1．0
- LM 1．2X002
- LanMan 2．1
- WindowsNTLM0．12

协商的过程就是要找到服务器和客户端之间最高版本的SMB。这里最大的问题是验证的强度取决于客户端而非服务器。通过配置客户端只使用最低版本的SMB可以强制使用陈旧的加密。如果在SMB进程中验证失败的话，将发生下列两种情况之一。或者访问被拒绝，或者是更危险的情况，建立了一个空的SMB会话。缺省情况下，这个空会话是Everyone组的身份建立的，因此，所有Everyone组可以访问的资源未授权的用户也可以访问了。

为了防止这个问题，你应当从Everyone组中删除匿名用户。你需要更注册表中HKLM＼System＼CurrentControlSet＼control＼LSA＼RestrictAnonymous的值为1。

如果你的客户端只使用WindowsNTworkstation的话，你还可以禁止LAN Manager的 验证。Windows95／98和WindowsforWorkgroups都使用LANManager验证，所以这也会禁止对那些客户端的访问，因此也不可行。另一个选择是强制服务器来决定使用什么样的客户端验证机制，而不是由客户端来做决定。这项措施也并非十分有效，因为服务器还是会发送所有六种方言给客户端。它主要是防止SMB降级攻击。这种攻击使用了不同的包嗅探器来监听SMB的验证会话。当服务器检测到这个过程，客户端会发送一条信息给服务器，这信息指出只存在低端的明文的验证方式，服务器收到这条信息并以这种方式建立会话。然后客户端以明文方式传送密码，攻击者会将密码捕获并存储下来。

为了控制LANManager验证，你需要改变注册表中HKLM＼System＼CurrentControlSet＼Control＼LSA＼LMCompatibilityLevel项的值。缺省情况十它的值是0，表明不是使用WindowsNT验证就是使用LM验证。如果值为1则表明两种验证方式都可以使用，但需要由服务器而不是客户端来决定方式。若值为2的话，则不；会采用LM的验证方式。

使用SMB的签名是另一种好的选择，它使WindowsNT对所有的包都使用加密的签名来防止l欺骗。这种方式几乎消除了伪造报文的可能性。然而，它会对Windows95／98和WindowsforWorkgroups的客户端的连接产生了不利的影响，因此，在使用前应当对其进行测试。要配置服务器只接收签名的报文，你需要把注册表中HKLM ＼ System ＼ cunentCOntrOlSet ＼ SerVices ＼ LanManServe\Parameters ＼ RequireSecuhtysignature值从0改为1。客户端也必须配置为只生成和相应签名的报文。在客户端，你需要把HKLM ＼ System ＼ CurrentControlSet ＼ Serivces ＼ Rdr ＼ Parameters ＼ RequireSecuritySignatures的值从0改成l。

其它配置的更改

你需要考虑各种其它的改变，大多数的这种改变都是针对WindowsNT的某种发展阶段的攻击所做出的。

加强打印机驱动的安全

WindowsNT的打印驱动以完全控制权限运行在操作系统级别。缺省情况下，任何人都可以在WindowsNT中安装打印机驱动。这种开发是系统容易遭受木马攻击。攻击者可以建立假的打印机驱动而实际上进行了其它的活动，例如，开启后门。

要严格限制只允许管理员组和打印机操作员可以安装打印驱动，　需要在HKLM＼

System＼ctirrentControlSet＼Control＼Print＼Providers＼LanMan Print 中增加类型为REG DWORD的AddPrintDrivers项，开设置其值为l。

隐藏上次登录的用户名

为了预防物理接触计算机的非法用户得知上一次登录系统的合法用户名，应当将HKLM＼Sofiware＼Microsofi＼Windows NTXCurrentVersions＼Windlogon中类型为REG SZ的DontDisplayLastUserName的值没为1。

因为任何可以直接访问计算机的大都可以用许多方法快速地破坏系统,所以上面谈到的方法也并不十分有效。任何可以直接访问网络的人，即使是个普通的用户，也可以轻易得到用户列表。然而，由于这种简单和快速的改动可以减缓潜在攻击者的脚步，所以还是值得一试的。

加强共享系统对象的安全

你可以严格限制象打印机和串口等共享对象只能被管理员使用。由于这种限制可以影响许多程序，所以在应用这种限制时要格外小心。

要实施这种对共享系统对象的访问控制，请在注册表中

HKLM＼System＼currentControlSet＼Control＼Session Manager中增加一个类型为REG—DWORD的名称为ProtectionMode的项，并将其值设成1。

清除系统关机后的页面交换文件

页面交换文件：是在WindowsNT进行工作时用于内存交换的。能够直接物理接触计·算机的人可以重启系统并拷贝该文件：。页面文件中保存着在使用中被交换和写满的重要信息。在HKLM＼System＼CurrentContrioSet＼Control＼Session Manager＼Memory Management中增加类型为REG DWORD名称为ClearPageFileAtShutdown的项，并将其值设成1，你可以让Windows NT在关机时用随机的内容改写整个的页面文件：。

这种清除的工作只发生在正常的关机情况下，所以如果有大可以直接关电源的话，该键值将不起作用。

禁止缓存登录的信任状

WindowsNT通常会缓存本机登录的用户信任状，所以如果域控制器出现问题或无法连接，用户还是可以在本地登录。

这种缓存功能会引起问题。例如，James在午餐后被公司炒了鱿鱼，James在域上的帐号也为防止其收拾个人用品时登录破坏数据而被禁止了，但由于WindowsNT在本地缓存了他的登录信任状，James还是可以返回办公室，将他的计算机从网络上断开，然后登录。当他的计算机无法通过域控制器进行身份验证时就尝试缓存中的信息，这不会因为其在域上的账号被禁止而受影响。James还是可能登录到本机并拷贝或破坏本地的数据。

虽然缓存并没有特别严重的威胁，但是如果你希望禁止Windows NT本地缓有的信任状， 你需要在HKLM＼Microsofi＼WindowsNT＼CurrentVersion＼Winlogon 中增加类刑为REG DWORD名称为CacheLogonsCount的项，开设置其值为0。

加强定时服务的安全

要加强WindowsNT的定时服务需要做一些设置。由于定时服务是以完全控制权限运行程序，所以如果攻击者能够自动运行某些程序的话，例如批处理程序，他们便可以进行许多非法的活动。

首先，HKLM＼System＼CurrentControlSet＼Services＼Schedule的权限应当更改为只允许系统管理员能够访问。这个设置会使只有管理员才可以查看有哪些定时运行的程序。其次，请确保HKLM＼CurrentControiSet＼Contro!＼LSA＼SubmitControl的值被设置成0。这项设置只允许管理员可以向定时服务列表中添加程序。最后，请确保在定时服务列表中要运行的程序使用的是完整路径，而且要执行的文件：被完全锁定。如果不使用完整的路径，WindowsNT会使用系统路径来寻找可执行程序。攻击者可以把木马程序放置在靠前的目录中。如果不进行锁定设置，则潜在的攻击者可以用其它的可执行程序覆盖该文件：。

加强可移动设备的安全

通常，像软驱和光驱等可移动设备被共享后可以夸网络地访问。你可以限制只允许交互式的用户才可以访问到这些可移动设备。这样，除非用户物理登录本机否则无法使用软驱和光驱。要设置这方面的安全性，你需要使用几种不同的注册表项。要控制软盘驱动器，你需要在HKLM＼Sofiware＼Microsofi＼WindowsNTkCurrentVersion＼Windlogon中增加类型为REG SZ名称为AllocateFIoppies的项， 并设置其值为1， 对光驱的设置相似， 不过要设置 AllocateCDRoms项。另一种控制软驱的方法是和用包含在 ·Windows NT Resource Kit中的FloppyLock服务。它严格限制了只有管理员才可以访问该软驱。

禁止和删除UNIX中不必要的服务

大多数的UNIX服务不包含安全问题。然而，UNIX中存在一些众所周知的安全问题，如果你使用像TFTP，SMTP，FTP和Telnet这样的特殊服务的话，你应当对这些服务进行更改。这部分将告沂你如何拒绝访问这些可能破坏安全的服务。

TFTP命令

简单文件传输协议(tftp)命令用于不要密码的文件：传输，它会带来安全风险。它允许用户不需登录就可以从任何系统接收文件：并且拥有读写的权限。该协议最早应用无盘工作站，X终端和类似的需要从网络上的服务器接收所有文件的设备。在旧版本的TFTP和类似的程序中存在一些安全漏洞。大多数的站点或者禁止该服务，或是安装了加强安全的版本。

在这些安全的版本中，已经知道的安全漏洞被修复了，只有在提供X终端连接时才需要运行TFTP。

Sendmail和SMTP守护进程

UNIX操作系统中的sendmail守护进程通常使用简单邮件传输协议(SMTP)。由于该守护进程必须对各种用户的邮箱中的电子邮件进行读写，所以它一般以root的权限运行。通过sendmail程序获得访问权限是破坏UNIX操作系统安全的通常手段。

在sendmail的早期版本中，调试工具和选项在系统内部编码为可执行程序。在后来的版本中将它们明确地禁止或删除了。因为SMTP使用25端口(或直接使用名称)，你可以迅速识别常见的sendmail漏洞是否已经补上

拒绝入站访问

由于／etc／inetd．conf是集中管理进入网络访问的文件：，所以这个文件必须以安全的目的进行控制。如果该文件被恶意的用户访问到，则任何事情都有可能发生，通常是程序被恶意的版本所替代，安装后门程序等等。

因此，你必须经常检查或监视这个文件并且确保其只能被root编辑。一些工具和软件包

可以帮助加强inetd．conf文件的安全，有选择性地启动和禁止基于inetd的服务。

类似地，你可以通过建立／etc／fipusers文件有选择地拒绝FTP请求的进入。这个文件中包含一些不受欢迎的FTP用户的列表。

拒绝出站访问

如果主机被设置成不支持出站访问Internet服务，那些提供客户端服务的命令如Telnet，FTP等应当被禁止这些可以在常见的UNIX目录中，如／bin、／sbin、／usr／bsd、／usr／ucb等目录中找到，实际存放目录的位置会随不同的操作平台和版本而不同，但它们总位于系统范围内通常可以访问到的目录。

TCPWrapper

TCPWrapper如同它的名字所表示的，象＂外套＂一样保护着基于TCP的服务和程序。因此TCPWrapper中的各个部分都在记录和监视着远程客户端用户和服务器端的程序或守护进程之间的联系。由于日志是由各个服务程序负责记录的，所以如果发生了安全问题，你应当能够从日志文件中找到入侵发生的原因。

因此，TCPWrapper是一些服务器程序的集合，充当标准的服务程序的角色，并且提供 了一些选项和记录日志的功能。

- telnetd
- fipd
- rlogind
- talkd
- fingerd

TCPWrapper运行于一些UNIX操作平台，并且可以被看成是应用网关的设置工具。远程或外部客户端运行Telnet程序来连接提供Telnetd程序的服务器。该程序深知Telnet特殊的．工作模式。在建立连接的初期，它们在TCP层建立段segment，然后通过IP层在客户端和服务器主机之间发送IP包datagram。IP包的头部包含着源和目标的IP地址和其它一些信息。TCP段中包含着由服务器程序处理的真实的数据。这种工作模式被所有TCPWrapper的程序所使用。

TCPWrapper程序将其它层置于inet守护进程(inetd)和单独的TCP服务进程(如in．telnetd)之间。回忆一下，当inet守护进程检测到在某个端口上有入站连接时，它会查询配置文件来确定应当启动那种服务进程来处理该连接。’在运行TCPWrapper的系统上，inetd配置文件总会启动称为tcpd的程序。当tcpd运行时，它会检查访问权限，记录连接日志，在端口上启动正确的服务进程。由于．TCPWrapper程序并不向远程客户端发送任何关于自身的信息，所以它们不会对远程显示任何标志，而远程会认为在同标准的服务器程序进行通信。当前TCPWrapper程序在所有类型的UNIX操作系统中广泛地应用着。它们提供了基本的网络安全等级。

对TCPWrapper包的访问控制有两个文件来管理， 它们是／etc／hosts．allow和／etc／hosts．deny。这两个文件包含了server：client形式的规则。如果客户端向服务器发送了连接的请求，并且在／etc／hosts．allow中有该server：client的匹配对的话，则连接被允许。但是如果该匹配对出现在／etc／hosts．deny中的话，则连接被禁止。缺省情况下，未列出的连接对是允许的。如果／etc／hosts．allow或／etc／hosts．deny文件丢失的话，则相应的访问总是被允许

警告：建立这两个文件时要格外地小心，由于它们按顺序执行。一旦先检查到的规则满足的话，后面的规则将被忽略。这样一来，有可能不受欢迎的主机可以进入网络，而合法的

主机却被这种机制排除在外。

文件内容的格式或语法是：

- 列出网络或守护进程，然后是冒号“ ：”，接着是客户端主机名称，然后和冒号“ ：”和解释器脚本名称。这些解释器脚本缺省是／dev／null。
- 空行或使规则的排列更清楚。
- 如果某一条规则很长，为了可读性，应当在下一行使用“ ＼ ”符号。
- 可以使用标准的UNIX符号，例如“ * ”通配符表示匹配所有。下列符号也用来增强规则的易读性。

》 ALL

》 LOCAL

》 UNKNOWN

TCPWrapper的其它功能包括对远程主机进行验证并且显示banner信息。在主机地址欺骗过程中，远程客户端向服务器发送数据包，在包头中通常包含远程客户端的地址(称为源地址)，服务器的IP地址(称为目标地址)，和一对表示服务的端口号。恶意的远程客户端程序会更改源地址来欺骗服务器。如果安装了带DPARANOID标志TCPWrapper软件包，它会在允许连接前对远程客户端的源地址的合法性进行检查。

TCPWrapper使用DNS解析IP地址来检查该主机的地址是否合法。由于入站的数据包含有源地址，TCPWrapper会向DNS服务器反向解析IP地址成DNS名。然后再把该DNS名用另一台DNS服务器解析成IP地址，通过比较前后两次的IP地址可以判断远程客户端是否进行了IP欺骗。如果前后的IP不符的话，TCPWrapper通常会拒绝该客户端，拒绝其访问任何服务，并且记录到日志中。TCPWrapper通常会在允许或拒绝服务前显示banner来解释某些网络连接失败的原因。

Tcpd提供访问控制，除主程序之外，TCPWrapper还有如 · 下程序

- Tcpdchk，用于在安装后对设置的检查
- Tcpdmatch，用于测试对入站客户端请求如何反应的设置
- Safe-finger，为防止远程主机使用finger漏洞而设的陷阱
- Try-from，用于测试主机和名称解析

信息摘要5(MD5)

MD5是用于对个别文件进行安全性检查的工具，它可以检测任何对文件：的更改和破坏。MD5可以把任意长度的文件做成128位的数字摘要。任何两个不同的文件不可能有相同的信息摘要。MD5算法还用于数字签名的程序，像RSA这样的加密是先将大的文件：作数字摘要，然后用私钥对其作签名。

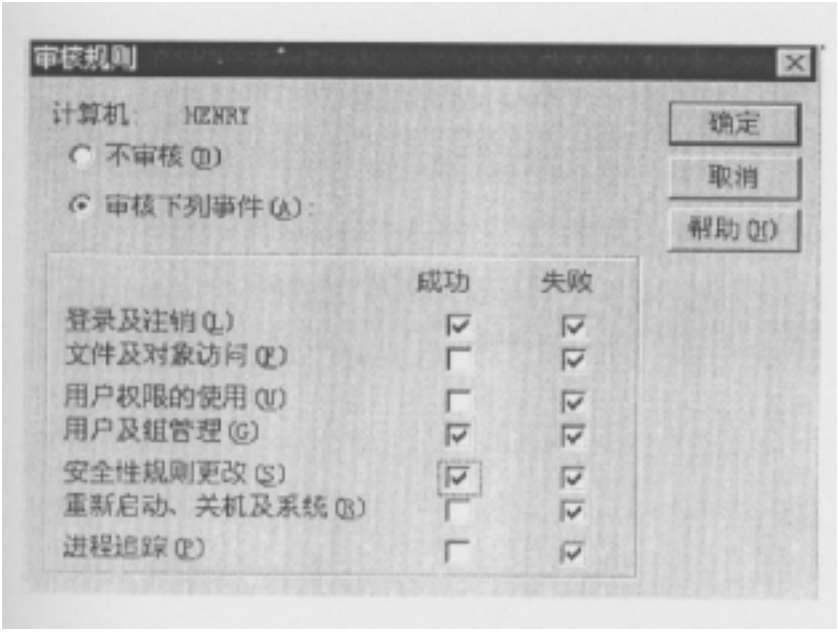
要获得更多关于MD5的信息，请访问 ’ 下面的站点：

ftp：／／fip．rsa．com／pub／md5．doc．

WindOWSNT中的日志记录

加强系统安全的下一步是开启审核。在WindowsNT中对特定活动的跟踪都记录在安全事件日志中。你已经接触过注册表的审核。在这一部分中将讨论审核。由于没有完全安全的事情，所以审核是确定在计算机系统中发生过什么情况的有力工具。在WindowsNT中有许多地方允许你进行审核。你应当通过域用户管理器来审核各种用户的行为。确定审核哪些事件 需要花费一些心思。如果审核的内容过多，将会给系统增加不必要的负担并降低操作系统

的效率。如果审核的内容太少，将会忽略一些问题。通常的折中方案如左图所示：



在上面的图中审核了所有的失败，通常它们表示发生了问题。这些信息有助于确定哪些账号被破坏了。用户和组的管理审核包括跟踪象添加用户的行为。你还应当跟踪成功地重新启动，关机和其它系统活动。攻击者可以使用各种技巧，例如安装嗅探器需要操作系统的重新启动，一些莫名其妙的重新启动应当引起怀疑。

一旦你开启了系统审核，你还应当审核文件和目录。这种功能需要NTFS文件：系统的支持，FAT不支持审核。跟踪系统文件对审核文件和目录来说非常重要。从WindowsNT资源管理器中通过文件属性来设置文件的审核，选择文件权限。缺省情况一下，所有文件和目录的审核都是关闭的。

审核是基于成功和失败两种情况的。成功是用于记录哪些用户正常地访问了文件，而失败则指出哪些人在没有正确的权限情况下试图访问文件。这有可能是攻击造成的结果，但也有可能是文件系统权限设置得不正确所导致的。一旦审核被开启，简单地查看信息是不够的。

如果你不对收集到的信息进行监视，那么这种审核是无效的。应当有规律地使用事件查看器来分析审核的信息。

本章小结：

在本课中，学习了如何降低WindowsNT和UNIX操作系统的潜在风险，了解了操作系统的补丁和fix的目的和重要性。为了增强安全性，你还更改了WindowsNT的注册表，然后是禁止和删除服务。在UNIX下你安装和使用了TCPWrapper和MD5，并且分析了WindowsNT下的审核日志。

安全审计，攻击和威胁分析篇

第一章

安 全 审 计

引　　言

在本课中你将学习实施成功的安全审计的主要步骤。你还将学到更多的作为一名审计人员如何定义自己的角色、从不同的角度实施工作，以及明确安全审计的原则。这些原则包括风险评估、实施审计的策略和提出相关安全建议的方法。

本章要点：

- 明确安全审计人员的主要职责
- 列出安全审计的原则
- 评估网络风险的要素
- 描述安全审计的过程

安全审计人员的需要

安全审计人员是进行风险评估的个体。作为一名审计人员，你的职责是通过对网络风险进行评估，从而提出有效的安全解决方案。换句话说你要在不影响职员日常工作的前提下尽量保证网络的安全。一个合格的审计人员应从两个角度来分析网络：

(1)从黑客的角度进行思考，寻找现有网络的漏洞，对网络资源加以保护；

(2)从雇员和管理者的角度进行思考，寻找最佳途径既可保障安全又不影响商业运作效率。

安全审计人员的工作

安全审计人员采用两种方式来达到一个高的安全等级。首先他们帮助网络管理人员制定一致性的安全策略。任何一个管理规范的网络都制定了一系列的安全策略。容易出现的问题是网管和安全专家所制定的可靠的安全策略只有用户在抵制它。其次是进行风险评估。下面列出一些风险评估的内容：

- 明确你所审计的企业的性质
- 阅读一份书面的安全策略
- 评价已经存在的管理和控制体系
- 实施安全审计(也称风险分析)
- 将系统按安全等级进行分类，包括数据库、Web服务器、路由器和账号数据库
- 提交一份审计报告

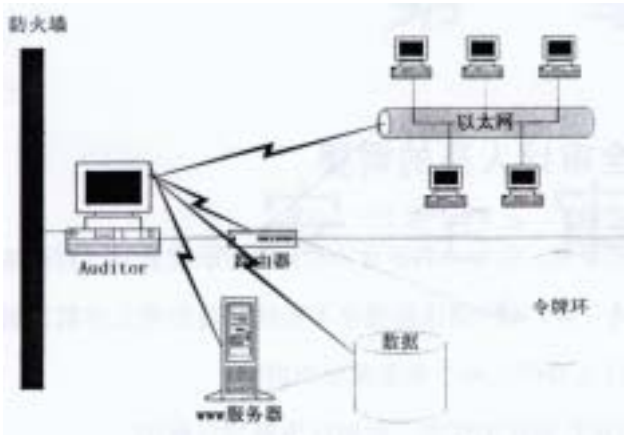
在学习特定的审计方法之前，你应该了解作为一名审计人员如何从两个角度看待网络。

审计人员的职责和前瞻性

作为一名审计人员，你应该至少从两个角度来对待网络：从安全管理者的角度和从顾问的角度考虑：

从安全管理者的角度考虑

作为一个安全管理者，你知道网络是如何配置的而且你想要探测到潜在的安全漏洞。因为已经得知了网络的拓扑、服务器配置和应用的操作系统和协议，所以此时你更像一个得知内情的黑客。这种审计角色需要你从防火墙内部进行监测，关注内部网络的服务器和主机是否有异常情况；如图所示



此外，有时一名安全管理者还要从防火墙外部进行渗透看是否能穿透防火墙进而控制网络主机，此时更关注防火墙的规则没置是否有漏洞。这种角度需要你能够对防火墙进行分析并且了解防火墙配置的一些问题。

提示：作为一名审计人员，你会发现很多系统管理员把敏感的设备放在防火墙外面。举例来说，许多管理员为了省事把Web，DNS和FTP服务器放在防火墙外部，要对这种情况加以关注并建议把它们至于防火墙内部。

从安全顾问的角度

作为顾问会实施许多安全管理者的工作，你将在防火墙内外进行测试，这时你将从两个角度进行操作：从黑客的角度和从不知情的审计者的角度。审计人员最初不了解网络的拓扑结构、服务、协议和操作的情况，此时从一个不了解内情的黑客角度来侦查、渗透和试图控制网络，这类审计人员通常被称为“ ethical hacker ”或“ white hat hacker ”，IBM ·ethical hacking division和AxentTigerTeam提供了这类审计的工具。

第二种类刑的审计人员从一个内部知情人的角度来评估网络安全。如果从这个角度来操作，你将首先与IT经理和其他相关的雇员接触。你将实施现场分析，了解所有网络的资源。 当你从这种角度来操作时，你实际是以第三方的身份评估现有网络的安全情况。

多数情况下，审计人员会合并这两种角度来提供更深层次的审计。在本教程中，你将学习如何从防火墙内外来进行审计工作。在学习和讨论这些概念时，请思考一个安全管理者或安全审计人员如何实施这些方法。

内部威胁分析

大多数人对黑客的认识更倾向于一个匿名者从外部试图渗透进网络内部。近些年来，从防火墙内部进行攻击造成了更大的损失。有时攻击来自不满的雇员，有时来自对安全策略不了解的雇员。工业间谍也是一个不容忽视的问题。

提示：黑客也使用很多你在本课程中使用的工具。当然，安全审计工具同样可用于非法的途径。例如，安全管理人员和黑客都使用NMAP和SATAN程序来扫描网络。

风险评估

风险评估是指定位网络资源和明确攻击发生的可能性。一些专家指出风险评估是一种“ 差距分析 ”，因为风险评估经常显示出安全策略和实际发生攻击之间的差距。下面将讨论在风险评估过程中将采用的步骤：

仔细检查书面的安全策略

只有对企业的性质有所了解，才能有效地对网络和资源进行审计。而了解企业性质的最好途径是先阅读网络安全的策略。没有一份书面的、公布于众的安全策略，网络也不会具备有效的安全。安全专家把书面的安全策略比喻成“ roadmap ”或“ framework ”，因为它使网络在扩大规模中仍能保持安全。作为审计人员，你应该仔细阅读安全策略并检验雇员对策略的执行情况。

有效的安全策略是简单的。虽然只有一个目标，即增强网络和主机安全，但一个企业的安全策略可能由好几个子文档组成。一些文档定义了标准用户和网络策略，包括可按受的Internet使用，可支持的软件：安装等等。Procedure文档更加详细地列举出如何对非授权的网络使用进行防范，对黑客进行入侵检测和其它细节等等。一份设计的文档列出网络拓扑和协议情况，以及公司如何计划实施网络边缘和内部安全设备。

对资源进行分析、分类和排序

找到网络中最重要的资源，黑客经常袭击不重要的系统，希望以它们为平台来攻击其它更有价值的网络资源。 下表列出了一些你在进行风险分析时应考虑的问题。

问题	回答
什么是受攻击的目标?	如果目标是一般用户的操作系统，则风险是低的。但如果是大力资源系统的话，则风险是高的。
出现问题的严重性?	一旦出现问题，后果有多严重?是会影响企业还是影响个别的系统?通常，你需要对损失的时间和金钱进行评估。
发生攻击的可能性?	攻击发生的可能性到底有多大?是不太可能发生还是非常有可能发生。

通常遭受攻击的资源

因为数据分布在不同的操作系统上，如Web服务器和数据库服务器，从而导致了它们不安全。这种分布性还开启了其它安全漏洞。从技术的角度，还需要对资源进行分类。

攻击热点	潜在威胁

网络资源	● 路由器和交换机 ● 防火墙 ● 网络主机
服务器资源	● 安全账号数据库 ● 信息数据库 ● SMTP 服务器 ● HTTP 服务器 ● FTP 服务器

根据类别对资源排序通常是个明智的策略。在许多情况一下，你还要考虑到一些特定的主机与公司组织结构的关系。对资源按优先级进行排序通常需要你对公司组织结构进行考虑，因为一个部门的数据库可能比另一个部门的数据库更重要。举例来说，每个部门都有自己的数据库，但人力资源、账号和研发部门的数据比其它部门的更重要。

考虑商业需求

为你的企业需求定制安全策略。我们还应当考虑一些特殊的部门和个体，尽量说服他们采用你的解决方案。除非你的策略考虑到他们的需求并提高了他们的工作效率，否则他们不会支持你的提议。再次强调你应当提高各部门的工作效率并使他们的数据更安全。

评估已有的边界和内部安全

首先你需要了解现时的安全情况，这一过程包括对公司边界和内部安全情况的收集，还有控制管理的构架、日志、访问控制机制和其它情况。边界安全指网络间区分彼此的能力。防火墙是定义安全边界的第一道屏障。流行的防火墙产品包括CheckPointFireWall-1，AxcentRaptor，和CyberGuardGuardianFirewall。

内部安全是指网络管理员监测和打击未授权的网络活动的能力。内部安全通常被忽视。但1999CSI／FBI关于计算机犯罪和安全调查表明很多企业已经把来自内部的威胁列为头等考虑的问题。在本课程中你会实施一些有效的内部网络安全产品，包括Axcent NetRecon，IntruderAlert ， EnterpriseSecurityManager ， eTrustIntrusionDetection,InternetSecuritySystems InternetScanner，NetworkAssociatesCyberCopScanner和其它的一些产品。

作为审计人员，你应该确保你所维护的网络能够从下列外部攻击中尽快恢复。

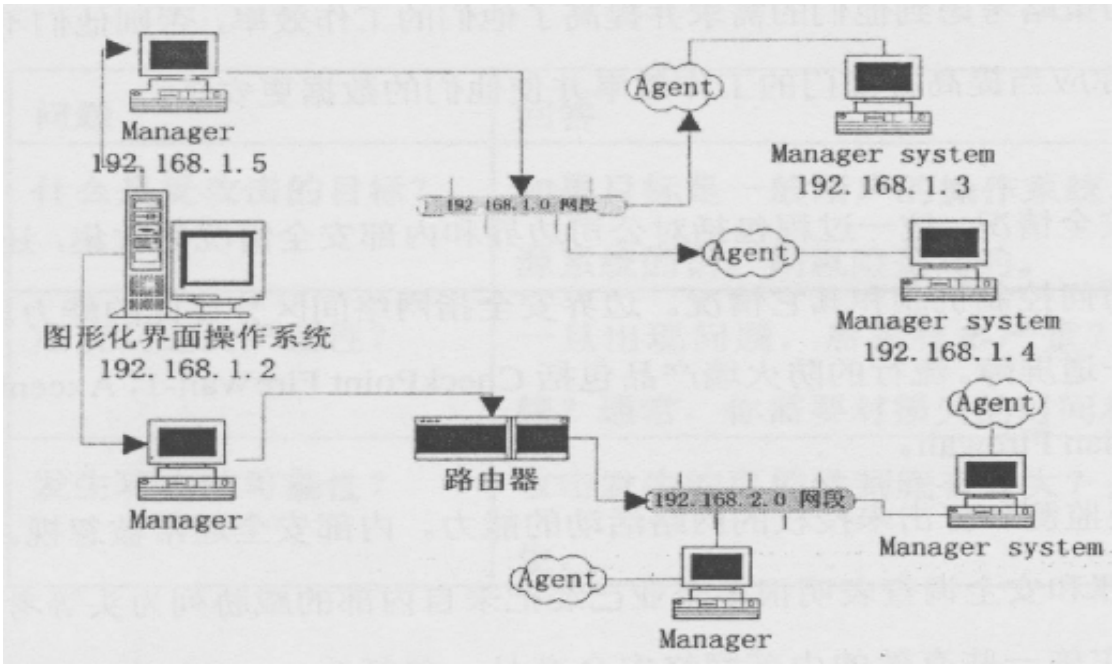
- 消耗带宽式攻击：攻击者发送大量欺骗性数据占用网络带宽，达到拒绝服务的目的。
- 错误的防火墙规则设置：错误的代理服务和包过滤规则的设置是网络安全极大的隐患
- 将系统至于防火墙之外：尽可能将网络资源至于防火墙内部

使用已有的管理和控制结构

网络管理人员选择不同的方式来管理网络安全。有时一个网络已经使用了一些网络安全产品。这时，你必须了解它们的工作情况。大多的情况下，你需要提出合理的安全解决方案。基于网络的管理产品将软件安装在一台服务器上，由它来向网络提出杏询。提出查询要求的：主机为管理者，管理者扫描网络上所有可疑的活动。

在这种结构一下，网络中每台计算机都被动地相应查询。基于网络的安全产品有eTrust IntrusionDetection(www．cai．com．)，NetworkFlightRecorder(．www．nfr．com．)和Axent NET PrOwler (www．axent．com)。

这种结构的优点是网络中的主机并不知道被监视。你不需要在被管理的主机上安装软件；这种结构的缺点是在交换环境下需要做特殊的设置，因为交换环境一下主机间的联系是一对一的。而且，基于网络的扫描软件通常不能跨路由。



基于主机的安全管理结构使用标准的三层管理体系，如上图所示： 第一层是简单的图形用户界面，功能是同管理者通信和显示信息。第二层是管理者，它向代理发出查询请求，从代理处收集信息并将这些信息提交给图形用户界面。第三层是安装在每台主机上的代理。

这种结构更复杂，因为你需要在每个要管理的主机上都安装软件；代理必须首先向管理者注册，之后管理者才能直接向代理发出查询请求。这种结构可以更准确的反映网络活动的情况。SNMP代理通常以这种方式接受管理，InternetSecuritySystems，Axent和其它一些厂商出售相关的产品。基于主机的扫描器在交换环境下工作得很出色，若路由器没有过滤掉管理者使用的端口则对代理的查询还可跨路由。

综上所述，两种管理结构各有优劣，适合不同的管理任务。你可以建议对已有的管理结构应用另一种策略，你还可以建议公司实施附加的管理策略。

风险评估阶段

在实施审计的时候，你将尝试采取一些黑客的行为：试图侦查、渗透和控制网络系统。这三个步骤是作为一名黑客和安全审计人员进行的重要阶段，我们将采刚一些分析手段以增强网络的安全性，经过分析进而提交报告是黑客和审计人员主要的不同点。

侦查阶段 .

在侦查阶段，你将扫描和测试系统的有效安全性。对网络进行侦查意味着要定位出网络资源的具体情况，包括IP地址、开放端口、网络拓扑等。这种分析工作通常需要大量的时间，

我们可以使用自动运行的扫描程序。

实施分析要求对系统逐个检测， 下面列出一些通常的检测项目：

- 已知的服务漏洞
- 缺省安装
- 不安全的网络管理
- 弱口令
- 不正确的服务配置
- 网络拓扑的缺陷
- 信息泄漏
- 未授权的设备和服务
- 可管理的设备
- 未授权的服务
- 加密机制
- 额外的用户权限
- 已知的软件版本漏洞

当一台主机(如HFTP服务器，路由器，或操作系统)提供了多于必须的信息时称为信息泄漏。缺省情况下，许多FTP和HTTP服务器都泄漏了黑客可以和用的信息。直到现在，各种网络还是要发布一些有关自身的敏感信息，包括网络管理员的姓名，DNS服务器，网络状态等等。

渗透阶段

渗透意味着你能绕过安全控制机制，如登录账号和密。你还可以通过使加密机制无效从而破坏数据的机密性和完整性。你还可以是网络拒绝提供服务。

在这个审计阶段，你将检查各种系统的漏洞，并试图使下列元素无效：

- 加密
- 密码
- 访问列表

在本课程中，你将学习到更多的渗透网络和主机的方法。

控制阶段

控制意味着可以随心所欲的管理网络和主机。审计人员从不试图控制网络主机，只是通过演示他可以控制网络主机来证明现有网络存在的问题。你将发现，控制表明一个黑客可以控制网络资源，创建账号，修改日志，行使管理员的权限。在你提交报告时，你必须提出如何防止黑客获得网络和主机的控制权的建议。

本章小结：

作为审计人员，你必须学会从黑客的视角来审视网络，还必须了解公司雇员和管理者的想法。在本课中，我们了解了审计人员在网络风险评估中特殊的角色以及如何同最终用户保持一致性，还讨论了审计过程中应用的策略和软件。在 · 下一课中，你将学习到在侦查特定的网络和主机漏洞过程中使用的程序。

第二章

侦 查 手 段 和 工 具

引　言

如你先前所知，黑客和安全审计人员采取的第一步都是侦查网络。在本课中，你将接触一些网络侦查工具和方法。

本章要点：

- 描述侦查过程
- 识别特殊的侦查方法
- 安装和配置基于网络和基于主机的侦查软件
- 实施网络级和主机级的安全扫描
- 配置和实施企业级的网络漏洞扫描器

安全扫描

安全扫描以各种各样的方式进行。你将和用Ping和端口扫描程序来侦查网络，你当然也可以使用客户端／服务器程序，如Telnet和SNMP等，来侦查网络泄漏的有用信息。你应当和用一些工具来了解网络。有些工：具很简单，便于安装和使用。有时，审计人员和黑客和用程序语言如Peri。C，C抖和Java自己编制一些工具，这是因为他们找不到现成的针对某种漏洞的工具。

另外一些工具功能更全面而且在使用前需要认真地配置。专门从事网络管理和安全的公司出售这些工具。你将在本课中学习使用这些工具。好的网络级和主机级扫描器会试图监听和隔离进出网络和主机的所有会话包。在学习这些“ Hacker-in-a-box ”的解决方案前，你应 当先接触一些当前黑客常常使用的技巧。

Whois命令

Whois(类似于finger)是一种internet的目录服务，whois提供了在Internet上一台主机或某个域的所有者的信息，如管理员的姓名、通信地址、电话号码和Email地址等信息，这些信息是在官方网站whois server上注册的，如保存在InternlC的数据库内。Whois命令通常是安全审计人员了解网络情况的开始。一旦你得到了Whois记录，从查询的结果还可得知 primary和secondary域名服务器的信息。

nSlOOkUp

使用DNS的排错]工具nsiookup，你可以和用从whois查询到的信息侦查更多的网络情况。例如，使用nslookup命令把你的主机伪装成secondaryDNS服务器，如果成功便可以要求从主DNS服务器进行区域传送。要是传送成功的话，你将获得大量有用信息，包括：

- 使用此DNS服务器做域名解析到所有主机名和IP地址的映射情况
- 公司使用的网络和子网情况
- 主机在网络中的用途。许多公司使用带有描述性的主机名，像mail．companya,com，www．companyb．com和print．companyc．com。

使用nslookup实现区域传送的过程

(1)使用whois命令查询目标网络，例如在Linux提示符下输入whoiswebmaster,com．cn
(2)你会得到目标网络的primary和slaveDNS服务器的信息。例如，假设主DNS服务器的名字是ns．webmaster,com．CB
(3)使用交互查询方式，缺省情况一下nslookup会使用缺省的DNS服务器作域名解析。键入命令serverns．webmaster,com．CB定位目标网络的DNS服务器；
(4)列出目标网络DNS服务器的内容，如1swebmaster,com．cn。此时DNS服务器会把数据传送给你，当然，管理员可以禁JkDNS服务器进行区域传送，目前很多公司将DNS服务器至于防火墙的保护之下并严格设定了只能向某些主机进行区域传送。

一旦你从区域传送中获得了有用信息，你便可以对每台主机实施端口扫描以确定它们提供了那些服务。如果你不能实现区域传送，你还可以借助ping和端口扫描工具，当然还有traceroute。

host

Host命令是UNIX提供的有关Internet域名查询的命令，可实现主机名到IP地址的映射，反之亦然。用host命令可实现以一F功能：

- 实现区域传送
- 获得名称解析信息
- 得知域中邮件服务器的信息

参数叫可显示更多的信息，参数-1实现区域传送，参数-t允许你亦询特定的DNSi~录。例如，要查询ciwcertified．com域的邮件服务器的记录，你需要键入命令：

host -t mxciwcertified．com　你可以参考UNIX命令帮助获得更多信息。

TraceroUte(tracert)

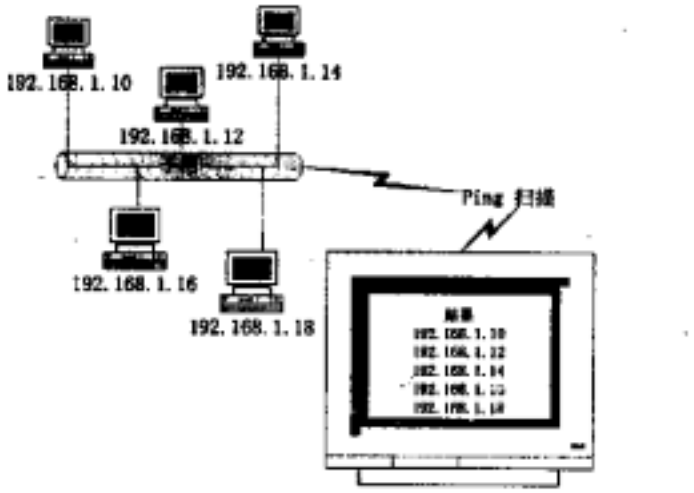
Traceroute用于路由追踪，如判断从你的主机到目标主机经过哪些路由器、跳计数、响应时间如何、是否有路由器当掉等。大多数操作系统，包括UNIX，Novell和WindowsNT，若配置了TCP／IP协议的话都会有自己版本的traceroute程序。当然我们也可以使用其它一些第三方的路由追踪软件：，在后面我们会接触到这些工具。

使用traceroute，你可以推测出网络的物理布局，包括该网络连接Internet所使刚的路由器。traceroute还可以判断出响应较慢的节点和数据包在路由过程中的跳计数。

PIng扫描作用及工具

Ping一个公司的Web服务器可帮助你获得该公司所使用的IP地址范围。一旦你得知了HTTP服务器的IP地址，你可以使用Ping扫描工具Ping该子网的所有IP地址，这可以帮助你得到该网络的地址图。

如一下图所示，你可以使用ping扫描工具侦查出网络的物理拓扑情况。



Ping扫描程序将自动扫描你所指定的IP地址范围。WS_PingProPack工具包中集成有Ping扫描程序，单独的Ping工具有许多，Rhin09Pinger是比较流行的程序。

端口扫描

端口扫描与ping扫描相似，不同的是端口扫描不仅可以返间IP地址，还可以发现目标系统上活动的UDP和TCP端口。如图所示是一次端口扫描所侦杏到的服务的情况。

在本例中，地址192．168．1．10正在运行SMTP和Telnet服务，地址192．168．1．12正在运行FTP服务，主机192．168．1．14木运行任何可辨别的服务，而主机]92．168．1．16运行着SMTP服务。最后一台主机属于Microsoft网络，因为该网络使用UDPl37和TCPl38、139端口。

端口扫描软件

端口扫描器是黑客最常使用的工具。一些单独使用的端口扫描I具象Port Scannerl．1，定义好IP地址范围和端口后便可开始实施扫描。还有许多单独使用的端口扫描器，如UItraScan等。像Ping扫描器，许多工具也集成了端口扫描器。NetScan、PingPro和其它一些程序包集成了尽可能多的相关程序。你将发现许多企业级的网络产品也将ping和端口扫描集成起来。

网络侦查和服务器侦查程序

如图2-9所示，使用简单的程序如PingPro，你可以侦查出Microsoft的网络上开启的端口。Ping Pro的工作是通过监测远程过程调用服务所使用的TCP、UDPl35端口，和Microsoft网络会话所使用的UDPl37，138，和139端口来实现的。其它的网络扫描工具允许你监测UNIX，Novell，AppleTalk的网络。虽然Ping Pro只能工作在其安装的特定子网，但还有更多更复杂的工具，这些工具的设计者把它们设计成为可以识别更多的网络和服务类型的程序。

例如，NMAP是UNIX下的扫描工具，它可以识别不同操作系统在处理TCP／IP协议上细微的差别。你可以从Http：／／www．insecure,org获得该程序。其它类似的程序还包括checkos,queso和SATAN。

堆栈指纹

许多本课中介绍的程序都和用堆栈指纹技术，这种技术允许你和用TCP／IP来识别不同的操作系统和服务。因为大多数的系统管理员注意到信息的泄露而且屏蔽了系统标志，所以应用堆栈指纹的技术十分必要。但是，各个厂商和系统处理TCP／IP协议的特征是管理员所

难以更改的。许多审计人员和黑客记录·下这些TCP／IP应用的细微差别，并针对各种系统构建了堆栈指纹表。

要想了解操作系统间处理TCP／IP协议的差异需要向这些系统的IP和端口发送各种特殊的包。根据这些系统对包的回应的差别，你可以推断出操作系统的种类。例如，你可以向主机发送FIN包(或任何不含有ACK或SYN标志的包)，你会从下列操作系统获得用心：

- MicrosoftWindowsNT，98,95,和3．1l
- FreeBSD
- CISCO
- HP／UX

大多数其它系统不会回应。虽然你只不过缩小了一点范围，但这至少开始了你对目标系统的了解。如果你向目标系统发送的报文头有未定义标志的TCP包的话，2．0．35版本以前的LINUX系统会在回应中加入这个未定义的标志。这种特定的行为使你可以判断出目标主机上是否运行该种LINUX操作系统。

下列是堆栈指纹程序和用的部分特征，许多操作系统对它们的处理方式不同：

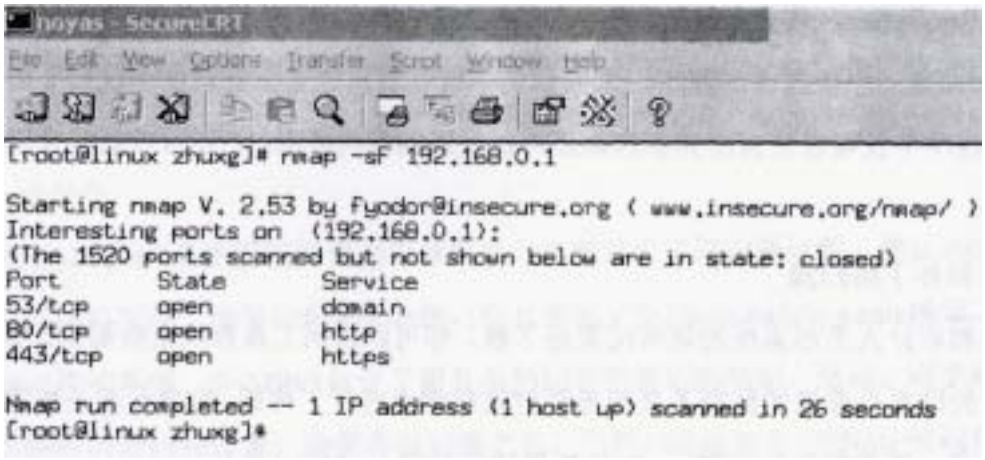
- ICMP错误信息抑制
- 服务类型值(TOS)
- TCP／IP选项
- 对SYNFLOOD的抵抗力
- TCP初始窗口：只要TCP开始进行三次握手，总是先发出一个SYN包。像NMAP这样的 程序会发出一个SYN包欺骗操作系统作回应。堆栈指纹程序可以从回应报文的格式中推论出目标操作系统的一些情况。

NMAP

NMAP由于功能强大、不断升级和免费的原因十分流行。它对网络的侦查十分有效是基于两个原因。首先，它具有非常灵活的TCP／IP堆栈指纹引擎，NMAP的制作人FYODOR不断升级该引擎是它能够尽可能多的进行猜测。NMAP可以准确地扫描服务器操作系统(包括Novell，UNIX，Linux，NT)，路由器(包括CISCO，3COM和HP)，还有一些拨号设备。其次，它可以穿透网络边缘的安全设备，例如防火墙。 ·

NMAP穿透防火墙的一种方法是和用碎片扫描技术(fragment scans)，你可以发送隐秘的FIN包(-sF)，Xmas tree包(-sX)或NULL包(-sN)。这些选项允许你将TCP查询分割成片断从而绕过防火墙规则。这种策略对很多流行的防火墙产品都很有效。

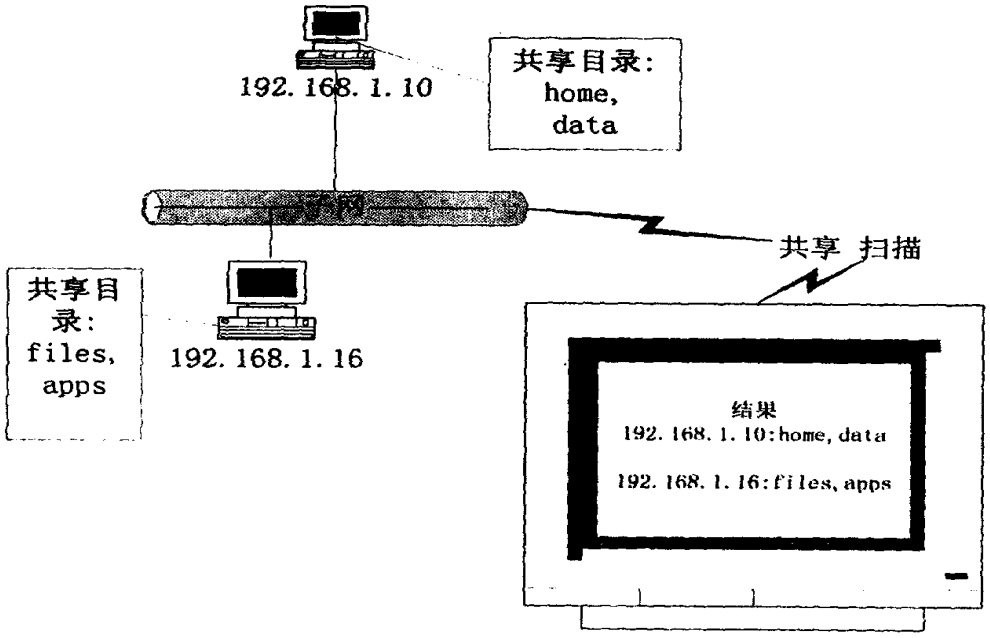
·下图所示是一份扫描结果



当前NMAP只能运行在UNIX操作系统上。操作系统类型包括Linux的所有版本，Free BSD 2．2．6—30，HP／UX，和Solaris。在linux的X-Windows上还提供图形界面。最好的掌握NMAP的方法是学习使用它。使用nmap—h命令可以显示帮助信息，当然，你也可以用man nmap命令查看它的使用手册。

共享扫描

你可以扫描网络中绝大多数的内容，包括正在使用的共享。这种扫描过程提供了重要的侦查和和用各种资源和文件的方法。如下图所示是共享扫描的工作示意图。



共享扫描软件

Ping Pro提供了允许审计人员扫描Windows网络共享的功能。它只能侦查出共享名称，但不会入侵共享。例如，Microsoft网络和用TCPl39端口建立共享。更具侵略性的侦查软件有知名的RedButton，许多Intemet站点都免费提供下载。

RedButton是一个很古老的程序，大多数的系统管理员和安全管理员都找到了防范它的方法。这个程序不仅可以侦查出共享名称还可以发现相应的密码。它还可以获得管理员的账号名称。

缺省配置和补丁级扫描

黑客和审计人员对系统的缺省配置很了解。你可以编制工具查找这些弱点。实际上，本课中讨论的许多企业级的侦查工具都是针对这些弱点进行工作的。安全专家还知道操作系统工作的细节，根据服务补丁和hot fix的数量进行升级。

使用Telnet

TeLnet是远程登录系统进行管理的程序。缺省情况一下telnet使用23端口。当然，你还可以利用Telnet客户端程序连接到其它端口。

例如，你可以Telnet至HTTP端口。在连接一段时间内若没有任何动作，服务器会因为无法识别这次连接而自动切断。但是你通常可以从HTTP服务器上得到一些信息。例如，可以

得知服务厂商的信息，版本(如ApacheWebServerl．36或IlS4．0)等等。虽然信息不是很多，但你至少能从报错信息中推断出服务器类刑。如下图所示你与服务器连接被终止，但在Web服务器报错信息中仍可以看出HTTP服务器版本。你还可以用Telnet连接上系统再使用SYST命令，许多TCP／IP堆栈会泄漏一些重要的信息。

使用SNMP

简单网络管理协议(SNMP)允许你从网络主机上查询相关的数据。例如，你可以收集TCP／IP方面的信息，还有在路由器、工作站和其它网络组件上运行的服务情况。SNMP由网络管理系统(NMS)和代理Agent组成。NMS通常安装在一台工作站上，再将代理安装在任何需要接受管理和配置的主机上。

当前存在三个版本的SNMP。SNMPvl最普通但也最不安全。原因有两个，首先，它使用弱的校验机制。只是靠communityname作验证，而communityname只是很短的字符串。其次，SNMP用明文发送community name，易于被sniffer捕获。而且，许多网络管理员使用缺省的“ public ”作communityname。任何黑客都会首先尝试用“ public ”来访问SNMP。

SetRequest命令

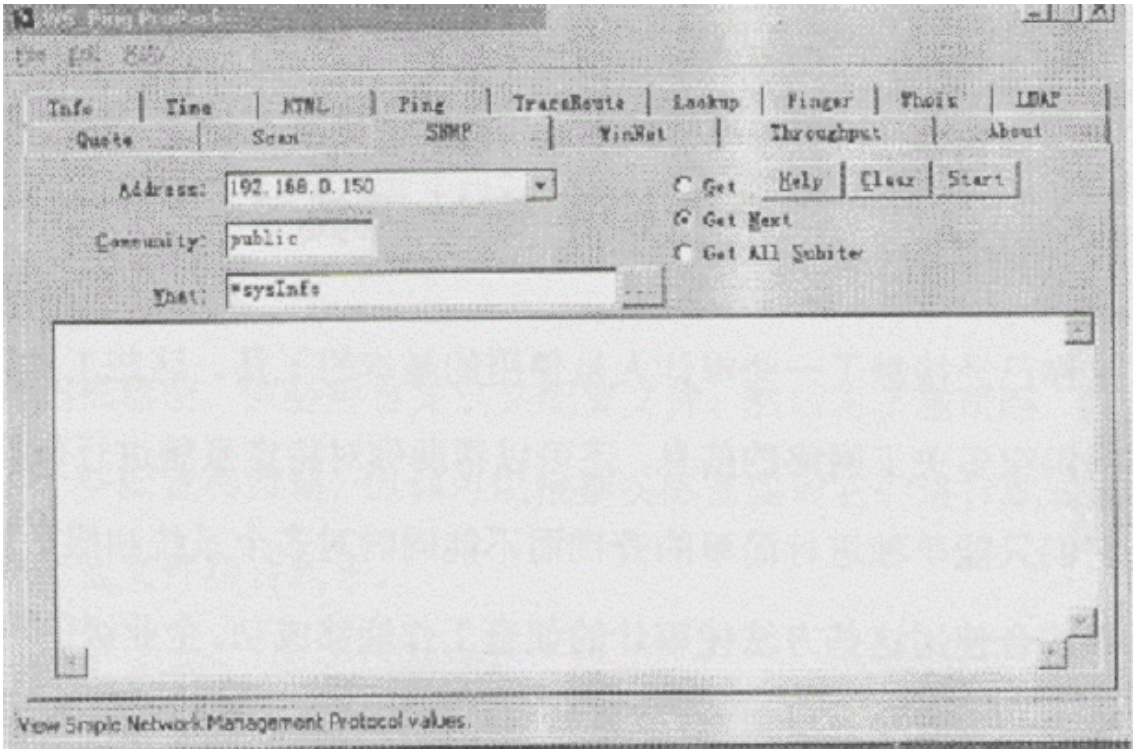
你还可以和用SNMP重新配置接口或服务。这包括设置路由跳计数，停止和启动服务，停止和启用接口等等。如果你使用SNMPvl而且黑客又得到community name的话，他就可以侦查和控制你的系统。SNMPv3包含了更复杂的加密和验证的机制。然而，许多网络管理员由于使用缺省的密码和设置，给黑客以可乘之机。当然，经过加密的SNMP密码仍然可以被捕获和暴力攻击。

SNMP软件

许多厂商出售SNMP管理软件，常见的SNMP软件有：

- HP的OpenView
- WindowsNTResourceKit中的SNMPUTIL
- 各种各样的网络附加：工具包，如PingProPack等

虽然象HP的OpenView程序是工业的标准，你还可以使用功能稍差的程序象PingPro来获取网络的情况。如图显示了PingPro中的SNMP模块。



TCP／IP服务

大多数的SMTP和POP3服务仍然以明文方式发送密码，这增大了Man-in-the-middle攻击成功的可能性。而且，LDAP、FTP、SMTP，尤其是HTTP服务非常容易遭受缓冲区溢出的攻击。

附加的TCP/IP服务

LDAP服务容易引起问题，不仅因为该服务所泄漏的信息而且经常遭受缓冲区溢出的攻击。E-mail程序如MicrosoftOutlook，Eudora和NetscapeCommunicator也包含LDAP客户端软件。而且，象Ping Pro和NetScan等管理工具运行你进行更复杂的查询。TFTP的问题是没有验证机制。黑客喜欢对其进行拒绝服务攻击，对系统提出了严峻的考验。

简单TCPflP服务

像Finger和TFTP等简单TCP／IP服务所泄漏的信息容易被黑客和用进行社会工程和其他类型的攻击。LDAP，FTP和SMTP服务经常出现安全问题有很多原因。首先这些服务容易泄漏太多自己配置的信息。

Finger

Finger服务使你考验获取远程服务器上的用户信息。使用Finger，你可以得到：

- 用户名
- 服务器名
- E-mail账号
- 用户当前是否在线
- 用户登录时间

- 用户的crond任务　　。

企业级的审计工具

进行到这里你已经接触了一些审计人员使用的基本的工具。这些工具便于安装和使用。它们可以为你提供很多关于网络的信息，还可以帮助你对特定系统进行风险评估。前面讨论程序的缺点是它们只能单独进行简单的查询而不能同时对多个系统和服务实施侦查。一个好的审计人员需要综合使用这些方法使审计的侦查工作能够成功。企业级的审计程序用以其人之道还制其人之身的方式来对付黑客，通过对网络进行综合的攻击使你可以实时地检测到网络的漏洞，并加以改进。

绝大多数的网络探测器都支持TCP／IP，而且许多还支持其它协议包括IPX／SPX，NetBEUI和AppleTaik。你已经对侦查数据库有所了解，在这一部分，你将更多地接触如何配置和更新侦查数据库。你还将学习网络扫描器的一些特性。

通常，网络扫描器程序无法跨子网。当然你可以在每个子网中都安装一个。然而，有些扫描器(如WebTrends Security Analyzer Enterprise Edition和ISS Internet Scanner Enterprise Edition)是可以跨子网的。

在你用扫描器扫描网络之前，你必须先配置它使其能够识别网络上的主机。有时，扫描器可以自动识别，但其它时候你必须手动配置它。每个程序都有它自身的配置方法，但配置原则是相同的。所有的商业扫描器都支持TCP／IP。许多还支持象IPX／SPX，NetBEUI，AppleTalk，DECnet和其它协议。你应当根据你的网络中应用的协议情况来购买不同的版本。许多版本的扫描器只支持特定的操作系统，因此你必须在购买前考虑到其使用的平台。以前，网络扫描器、探测器和入侵监测系统都是在UNIX系统下工作得更出色。但是随着Windows NT更加成熟，许多功能强大的产品也出现了。

扫描等级

大多数的企业级的扫描器允许你选择安全扫描的等级。一次轻级别的扫描通常会扫描众所周知的端口(从0到1023)和常见的安全漏洞，包括弱口令，低的补丁等级和额外的服务。如果你扫描一个小型的子网大概需要花费30分钟。中级和严格级别的扫描根据网络的速度和运行扫描程序的主机CPU的时钟速度快慢等因素通常会花费几天的时间。

定义严格级别的扫描策略会让扫描器对目标网络发起连续的攻击。如果你设置了规则让扫描器扫描所有的65,535个端口，还要检测口令强度以及细致地分析从管理账户到UNIX子系统的每项服务的话，工作量是相当大的。这种扫描不仅费时，而且会极大地加重网络的负担。个别主机将无法承受这种扫描。

配置文件和策略

在使用任何扫描器前，你必须首先定义配置文件，然后再实施策略。绝大多数的扫描程序事先都定义了一些配置和策略，但你可以根据实际需要对它们进行编辑和增加。需要注意的是要将策略和配置文件：结合起来。

报告功能

企业级的扫描程序具有细致的报告功能。可以用很多种格式输出信息，包括：

- 简单的ASCII文本
- HTML字处理文本格式，如RTF，或一些专和格式，例如MicrosoftWord(DOC)或Corel

WordPerfect(WPD)。

- 电子表格形式，例如MicrosoftExcel。
- 图形格式，包括幻灯片，例如MicrosoftPowerPoint

报告风险等级

大多数的网络扫描器将风险分成低、中、高三个等级。你将接触到各种扫描器是如何汇报它们的扫描结果的。即使得出你的网络只有低的安全问题，你也不应该沾沾自喜。一名优秀的黑客可以从很小的缺陷入手给系统造成致命的破坏。

Axeet NetRecon

NetRecon是最先为Windows NT网络设计的网络扫描产品之一。NetRecon象其它扫描器一样可以发现网络中的各种元素，处理本课中讨论的各种问题，包括密码检查。NetRecon可以比较准确的模拟各种攻击。NetRecon的界面由三个窗格组成。对象窗口允许你查看每个扫描对象，通过单击可以展开目录结构。通过扫描网络，图形窗口显示低、中、高的风险等级。状态栏显示扫描的进程。你可以对网络进行深度扫描，当然这种扫描会耗费大量的时间。例如，广泛的扫描会花费两天的时间。

漏洞数据库和对象列表

在NetRecon中以一些漏洞列表作为侦查数据库，你可以将这个列表理解为攻击指纹，但是这个名词通常被用于入侵检测系统程序中。如果你持有NetRecon的授权，便可以从Axent的Web站点(http：／／www.axent.com．)升级这个漏洞列表。通过Reprots view Vulnerability Descriptions菜单，可以查看相关漏洞的描述。
下面列出NetRecon~以扫描出的系统漏：

- Finger服务漏洞
- GameOver(远程管理访问攻击)
- 未授权注销禁止
- 服务漏洞，包括SMTP、DNS、FTP、HTTP、SOCKS代理和低的sendmail补丁等级。

大多数网络扫描器，如NetRecon，包含了事先定义好的对象列表。通过选择Reprots，VIew ObiectiveDescriptions，你可以查看在NetRecon中已经配置好的当前对象列表。

Network Associates CyberCop Scanner

CyberCopScanner是NetworkAssociates的产品，该公司的产品还包括SnifferBasic(前身是NetXRay)和其它网络管理软件。象NetRecon一样，CyberCop Scanner是一个主机级别的审计程序。与Axent的产品一样，CyberCop也把各种漏洞分类为低、中、高三个等级。
附录B中是一份CyberCop Scanner生成的报告样例。

技术提示：CyberCop Monitor不是网络扫描器，它是入侵监测系统程序，能够对黑客活动进行监视，提供报警功能，还能惩罚黑客。你将在本教程中学习一些入侵检测系统程序。

Web Trends Security Analyzer

该软件以前叫Asmodeus Security Scanner，WebTrends的产品在UNIX和NT系统一下都经过很好的测试。Security Analyzer的优点之一是与UNIX搭配使用多年，操作界面也简单易用。在主界面上选择Poiicy，然后edit，这时SecurityAnalyzer的选项窗口将出现。你可以选择扫描的强度，或编辑已有的策略、建立新的策略。如果你点击Host Selection标签，便可以选择子网内主机的范围。

Internet Security Systems的扫描产品

Internet Security Systems是最早生产扫描程序的公司。在本课中你将学习Internet扫描器和系统扫描器。它们都是ISS设计来提供跨操作平台的安全工具包。

ISS Internet Scanner

这款扫描器工作于UNIX和NT平台，象AxentNetRecon、WebTrends Security Analyzer和其它扫描器一样可以扫描远程主机。

Ineternet Scanner有三个模块：intranet，firewall和Web服务器。程序的策略是希望将网络活动分类，并针对每种活动提供一种扫描方案。这个特点由于你可以直接扫描更重要和经常遭受攻击的系统而变得十分有效。你也可以在三个模块中定义你自己的扫描参数。

下列是InternetScanner中部分扫描的项目：

- PHP3缓冲区溢出
- Teardrop和Teardrop2攻击
- 跨网络的协议分析仪(包括tcpdump和Sniffer Basic)
- 搜索一些FTP服务类别，包括WarFTP
- SNMP和RMON检测
- Whois检测
- SAMBA溢出
- 增强的SMS支持
- 增强的NT功能，仗它与UNIX一样有效

ISS Security Scanner

Security Scanner是基于主机的扫描程序。它可以深入挖掘系统的情况。由于是基于主机的扫描程序，所以能更深入地扫描系统内部。这一功能在检查象数据库、FTP和Web服务等特定的系统时显得十分有用。这种程序应该只运行在考虑到有黑客活动的高风险的系统上。

其它扫描程序厂商

其它提供扫描和检测漏洞的产品包括：

- Security DynamicsKaneSecurity Analyst(http：／／www,securitydynamics．com．)
- NetectHackerShield(http：／／www．netect．com．)

社会工程

我们已经接触了一些侦查程序，其中有的工具非常灵活和全面。但是，通过人为你侦查网络情况更方便。一名优秀的审计人员会从大力资源角度来获取网络信息。虽然你可以用社会工程对网络进行渗透和控制，但用这种方法来侦查网络也同样有效。作为安全管理人员你不应低估社会工程的威胁。作为安全审计人员，你也不应在侦查工具和技巧中漏掉社会工程。

电话访问

审计人员试图以人为突破口。在从Nslookup获得有关信息后和用电话骗取更多的有用信息。通过这种方法，你可以获得更多的信息，甚至骗取他大给你访问网络主机的权限。

E-mail诈骗

虽然欺骗性的邮件本身是无效的，但你可以伪装成工程技术人员骗取别人回复你的信件，泄漏有价值的信息。

教育

作为安全管理人员，避免员工成为侦查工具的最好方法是对他们进行教育。通过提高员工对设备的认识和增强他们的责任感，可以使他们变得更难于被黑客控制。

获得信息

作为安全审计人员，你可以把信息分成网络级别和主机级别的信息。

网络级别的信息

下表中列出了你需要获得的有价值的网络级别的信息。

信息	描述
网络拓扑	安全审计人员首先应当搞清楚网络的类别(以太网，令牌环等等)，IP 地址范围，子网和其它网络信息。配线架的位置也很重要。作为安全管理大员，你的目标是和用防火墙、代理服务器等设备保护这些信息。
路由器和交换机	掌握路由器和交换机的种类对分析网络安全十分重要，你可以是路由器泄漏信息。
防火墙种类	大多数的网络都有防火墙。如果你能够访问防火墙，便可以侦查它并寻找相应的漏洞。
IP 服务	最基本的服务包括 DHCP，BOOTP，WINS，SAMBA，和 DNS。DNS 服务特别容易遭受缓冲区溢出的攻击。
Modem 池	也许最流行的绕过防火墙做法是通过 modem 连接再附以 Man-in-the-middle 攻击和包捕获。War dialer 是在 Internet 上寻找网络连接的重要的审计工具。

主机级别的信息

下表列举了一些更有价值的主机级别的信息

信息	描述
活动端口	你应该了解服务器上有那些端口是活动的。HTTP 和 FTP 服务是最容易遭受端口扫描的服务，而且黑客会进一步实施缓冲区溢出攻击。
数据库	数据库类型(例如 Oracle,MicrosoftSQLServer 和 IBMDB2)，物理位置和应用协议都很有价值。
服务器	服务器类型是非常有价值的信息。一旦你确定了服务器的种类是 Microsoft 或 UNIX，便可以有针对性的和用系统的缺省设置和补丁侦查登录账户名称，弱口令和低的补丁等级。

近年来，许多成功的黑客都和用了大量的业余时间。他们阅读了大量的文献，研究系统的缺省设置和内置的漏洞。无论你是安全管理大员还是安全审计大员，都应该尽可能地多掌握产品的情况。

例如，通过研究TCP／IP的RFC文件：，你可以获知各个厂商如何应用TCP／IP协议。在StudentCD中的RFC目录中有RFCl700文章，其中描述了TCP和UDP端口的划分情况。这种文献是你和黑客都可以免费得到的关于协议、操作系统和硬件信息的资料。

合法和非法的网络工具

黑客会尝试使用任何工具，不论它有多复杂。而且，黑客工具和审计工具并没有本质上的区别。在本课中讨论的一些工具，如AxentNetRecon，通过广播主机名进行查询。这些信息可以帮助系统管理员和安全管理大员明确需要扫描那些资源。无论如何，这些程序并不仅限于系统管理员的正当使用。

黑客可以使用本课中讨论的任何工具。使用企业级的扫描：工具通常会占用大量的带宽，并不是隐蔽的侦查工具。因此，任何系统管理员，安全审计人员或黑客都乐于使用网络级的扫描程序即使冒不是引起注意就是使整个网络瘫痪的风险。

本章小结：

侦查是安全审计中非常重要的一个环节,在这节课里面我们学习使用不同的技术和工具来对网络进行扫描、获得相应信息和潜在的漏洞。要求学员能够熟练掌握Pinger、PingPro、NMAP、Netrecon和ISS Internet Scanner等工具的原理工具体应用。

第三章

服务器渗透和攻击技术审计

引　　言

一旦黑客定位了你的网络，他通常会选定一个目标进行渗透。通常这个目标会是安全漏洞最多或是他拥有最多攻击工具的主机。非法入侵系统的方法有很多，你应当对这些方法引起注意。

本章要点：

- 知道那些对象容易遭受攻击
- 讨论渗透策略和手法
- 列举潜在的物理、操作系统和TCP／IP堆栈攻击
- 识别和分析暴力攻击、社会工程和拒绝服务攻击
- 实施反渗透和攻击的方法

常见攻击类型和特征

攻击特征是攻击的特定指纹。入侵监测系统和网络扫描器就是根据这些特征来识别和防范攻击的。下面简要回顾一些特定地攻击渗透网络和主机的方法。

常见的攻击方法

你也许知道许多常见的攻击方法，下面列出了一些：

- 字典攻击：黑客和用一些自动执行的程序猜测用户命和密码，审计这类攻击通常需要做全面的日志记录和入侵监测系统(1DS)。
- Man-in-thc-middle攻击：黑客从合法的传输过程中嗅探到密码和信息。防范这类攻击的有效方法是应用强壮的加密。
- 劫持攻击：在双方进行会话时被第三方(黑客)入侵，黑客黑掉其中一方，并冒充他继续与另一方进行会话。虽然不是个完全的解决方案，但强的验证方法将有助于防范这种攻击。
- 病毒攻击：病毒是能够自我复制和传播的小程序，消耗系统资源。在审计过程中，你应当安装最新的反病毒程序，并对用户进行防病毒教育。
- 非法服务：非法服务是任何未经同意便运行在你的操作系统上的进程或服务。你会在接下来的课程中学到这种攻击。
- 拒绝服务攻击：利用各种程序(包括病毒和包发生器)使系统崩溃或消耗带宽。

容易遭受攻击的目标

最常遭受攻击的目标包括路由器、数据库、Web和FTP服务器，和与协议相关的服务，如DNS、WINS和SMB。本课将讨论这些通常遭受攻击的目标。

路由器

连接公网的路由器由于被暴露在外，通常成为被攻击的对象。许多路由器为便于管理使用SNMP协议，尤其是SNMPvl，成为潜在的问题。许多网络管理员未关闭或加密Telnet会话，若明文传输的口令被截取，黑客就可以重新配置路由器，这种配置包括关闭接口，重新配置

路由跳计数等等。物理安全同样值得考虑。必须保证路由器不能被外人物理接触到进行终端会话。

过滤Telnet

为了避免未授权的路由器访问，你应和用防火墙过滤掉路由器外网的telnet端口和SNMP[161，162]端口

技术提示：许多网络管理员习惯于在配置完路由器后将Telnet服务禁止掉，因为路由器并不需要过多的维护工作。如果需要额外的配置，你可以建立物理连接。

路由器和消耗带宽攻击

最近对Yahoo、e-Bay等电子商务网站的攻击表明迅速重新配置路由器的重要性。这些攻击是由下列分布式拒绝服务攻击工具发起的：

- Tribal Flood Network(TFN)
- Tribal Flood Network(TFN2k)
- Stacheldraht(TFN的一个变种)
- Trinoo(这类攻击工具中最早为人所知的)

因为许多公司都由ISP提供服务，所以他们并不能直接访问路由器。在你对系统进行审计时，要确保网络对这类消耗带宽式攻击的反映速度。你将在后面的课程中学习如何利用路由器防范拒绝服务攻击。

数据库

黑客最想得到的是公司或部门的数据库。现在公司普遍将重要数据存储在关系刑或面向对象的数据库中，这些信息包括：

- 雇员数据，如个人信息和薪金情况。
- 市场和销售情况。
- 重要的研发信息。
- 货运情况。

黑客可以识别并攻击数据库。每种数据库都有它的特征。如SQLServer使用1433／1434端口，你应该确保防火墙能够对该种数据库进行保护。你会发现，很少有站点应用这种保护，尤其在网络内部。

服务器安全

WEB和FTP这两种服务器通常置于DMZ，无法得到防火墙的完全保护，所以也特别容易遭到攻击。Web和FTP服务通常存在的问题包括：

- 用户通过公网发送未加密的信息：
- 操作系统和服务存在众所周知的漏洞导致拒绝服务攻击或破坏系统：
- 旧有操作系统中以root权限初始运行的服务，一旦被黑客破坏，入侵者便可以在产生的命令解释器中运行任意的代码。

Web页面涂改

近来，未经授权对Web服务器进行攻击并涂改缺省主页的攻击活动越来越多。许多企业、政府和公司都遭受过类似的攻击。有时这种攻击是出于政治目的。大多数情况一下Web页面的涂改意味着存在这入侵的漏洞。这些攻击通常包括Man-in-the-middle攻击(使用包嗅探器)

和和用缓冲区溢出。有时，还包括劫持攻击和拒绝服务攻击。

邮件服务

广泛使用的SMTP、POP3和IMAP一般用明文方式进行通信。这种服务可以通过加密进行验证但是在实际应用中通信的效率不高。由于大多数人对多种服务使用相同的密码，攻击者可以和用嗅探器得到用户名和密码，再和用它攻击其它的资源，例如WindowsNT服务器。这种攻击不仅仅是针对NT系统。许多不同的服务共享用户名和密码。你已经知道一个薄弱环节可以破坏整个的网络。FTP和SMTP服务通常成为这些薄弱的环节。

与邮件：服务相关的问题包括：

- 和用字典和暴力攻击POP3的login shell：
- 在一些版本中sendmaii存在缓冲区溢出和其它漏洞：
- 和用E-mail的转发功能转发大量的垃圾信件：

名称服务

攻击者通常把攻击焦点集中在DNS服务上。由于DNS使用UDP，而UDP连接义经常被各种防火墙规则所过滤，所以许多系统管理员发现将DNS服务器至于防火墙之后很困难。因此，DNS服务器经常暴露在外，使它成为攻击的目标。DNS攻击包括：

- 未授权的区域传输；
- DNS毒药，这种攻击是指黑客在主DNS服务器向辅DNS服务器进行区域传输时插入错误的DNS信息，一旦成功，攻击者便可以使辅DNS服务器提供错误的名称到IP地址的解析信息：
- 拒绝服务攻击；

其它的一些名称服务也会成为攻击的目标，如下所示：

- WINS，“ Coke ”通过拒绝服务攻击来攻击没有打补丁的NT系统。
- SMB 服务 (包括 Windows 的 SMB 和 UNIX 的 Samba) 这些服务易遭受 Man-in-the-middle攻击，被捕获的数据包会被类似LOphtCrack这样的程序破解。
- NFS和NIS服务。这些服务通常会遭受Man-in-the-middle方式的攻击。

在审计各种各样的服务时，请考虑升级提供这些服务的进程。

审计系统BUG

作为安全管理者和审计人员，你需要对由操作系统产生的漏洞和可以和用的软件做到心中有数。早先版本的MicrosoftllS允许用户在地址栏中运行命令，这造成了IlS主要的安全 问题。其实，最好的修补安全漏洞的方法是升级相关的软件：。为了做到这些，你必须广泛地 阅读和与其他从事安全工作的大进行交流，这样，你才能跟上最新的发展。这些：工作会帮助 你了解更多的操作系统上的特定问题。

虽然大多数的厂商都为其产品的问题发布了修补方法，但你必须充分理解补上了哪些漏洞。如果操作系统或程序很复杂，这些修补可能在补上旧问题的同时又开启了新的漏洞。因此，你需要在实施升级前进行测试。这些测试：下作包括在隔离的网段中验证它是否符合你的需求。当然也需要参照值得信赖的网络刊物和专家的观点。

审计Trap Door和Root Kit

Root kit是用木马替代合法程序。TrapDoor是系统上的bug，当执行合法程序时却产生

了非预期的结果。如老版本的UNIX sendmail，在执行debug命令时允许用户以root权限执 行脚本代码，一个收到严格权限控制的用户可以很轻易的添加用户账产。

虽然root kit通常出现在UNIX系统中，但攻击者也可以通过看起来合法的程序在WindowsNT中置入后门。象NetBus,BackOrifice和MastersOfParadise等后门程序可以使攻击者渗透并控制系统。木马可以由这些程序产生。如果攻击者够狡猾，他可以使这些木马程序避开一些病毒检测程序，当然用最新升级的病毒检测程序还是可以发现它们的踪迹。在对系统进行审计时，你可以通过校验分析和扫描开放端口的方式来检测是否存在root kit等问题。

审计和后门程序

通常，在服务器上运行的操作系统和程序都存在代码上的漏洞。例如，最近的商业Web浏览器就发现了许多安全问题。攻击者通常知道这些漏洞并加以和用。就象你已经知道的RedButton，它和用了Windows NT的漏洞使攻击者可以得知缺省的管理员账号，即使账号的名称已经更改。后门(backdoor)也指在操作系统或程序中未记录的入口。程序设计人员为了便于快速进行产品支持有意在系统或程序中留下入口。不同于bug，这种后门是由设计者有意留’下的。例如，像Quake和Doom这样的程序含有后门入口允许未授权的用户进入游戏安装的系统。虽然看来任何系统管理员都不会允许类似的程序安装在网络服务器上，但这种情况还是时有发生。

从后门程序的危害性，我们可以得出结论，在没有首先阅读资料和向值得信赖的同事咨询之前不要相信任何新的服务或程序。在你进行审计时，请花费一些时间仔细记录任何你不了解它的由来和历史的程序。

审计拒绝服务攻击

WindowsNT易遭受拒绝服务攻击，主要是由于这种操作系统比较流行并且没有受到严格的检验。针对NT服务的攻击如此频繁的原因可以归结为：发展势头迅猛但存在许多漏洞。在审计WindowsNT网络时，一定要花时间来验证系统能否经受这种攻击的考验。打补丁是一种解决方法。当然，如果能将服务器置于防火墙的保护之下或应用入侵监测系统的话就更好了。通常很容易入侵UNIX操作系统，主要因为它被设计来供那些技术精湛而且心理健康的人使用。在审计UNIX系统时，要注意Finger服务，它特别容易造成缓冲区溢出。

缓冲区溢出

缓冲区溢出是指在程序重写内存块时出现的问题。所有程序都需要内存空间和缓冲区来运行。如果有正确的权限，操作系统可以为程序分配空间。C和C++等编程语言容易造成缓冲区溢出，主要因为它们不先检查是否有存在的内存块就直接调用系统内存。一个低质量的程序会不经检查就重写被其它程序占用的内存，而造成程序或整个系统死掉，而留一下的shell有较高的权限，易被黑客和用运行任意代码。

据统计，缓冲区溢出是当前最紧迫的安全问题。要获得关于缓冲区溢出的更多信息，请访问Http：／／www-4．ibm．com／sofiware／developer／library／overflows／index．heml．

防范拒绝服务攻击

你可以通过以下方法来减小拒绝服务攻击的危害：

- 加强操作系统的补不一等级。
- 如果有雇员建立特定的程序，请特别留意代码的产生过程。

- 只使用稳定版本的服务和程序。

审计非法服务，特洛伊木马和蠕虫

非法服务开启一个秘密的端口，提供未经许可的服务，常见的非法服务包括：

- NetBus
- BackOrifice和BackOrifice2000
- Girlfriend
- 冰河2．X
- 秘密的建立共享的程序

许多程序将不同的非法服务联合起来。例如，BackOrifice2000允许你将HTTP服务配置在任意端口。你可以通过扫描开放端口来审计这类服务，确保你了解为什么这些端口是开放的。如果你不知道这些端口的用途，用包嗅探器和其它程序来了解它的用途。

技术提示：不要混淆非法服务和木马。木马程序通常包含非法服务，而且，木马程序还可以包含击键记录程序，蠕虫或病毒。

特洛伊木马

特洛伊木马是在执行看似正常的程序时还同时运行了未被察觉的有破坏性的程序。木马通常能够将重要的信息传送给攻市者。攻击者可以把任意数量的程序植入木马。例如，他们在一个合法的程序中安放root kit或控制程序。还有一些通常的策略是使用程序来捕获密码和口令的hash值。类似的程序可以通过E-mail把信息发送到任何地方。

审计木马

扫描开放端门是审计木马攻击的途径之一。如果你无法说明一个开放端口用途，你也许就检测到一个问题。所以，尽量在你的系统上只安装有限的软件：包，同时跟踪这些程序和服务的漏洞。许多TCP／IP程序动态地使用端口，因此，你不应将所有未知的端口都视为安全漏洞。在建立好网络基线后，你便可以确定哪些端口可能存在问题了。

蠕虫

Melissa病毒向我们展示了TCP／IP网络是如何容易遭受蠕虫攻击的。在你审计系统时，通常需要配置防火墙来排除特殊的活动。防火墙规则的设置超出了本术的范围。但是，作为审计人员，你应当对建议在防火墙上过滤那些从不信任的网络来的数据包和端口有所准备。蠕虫靠特定的软件传播。例如，在2000年三月发现的Win32／Melting．worm蠕虫只能攻击运行Microsoft Outlook程序的Windows操作系统。这种蠕虫可以自行传播，瘫痪任何种类的Windows系统而且使它持续地运行不稳定。

结合所有攻击定制审计策略

攻击者有两个共同的特点。首先，他们将好几种不同的方法和策略集中到一次攻击中。其次，他们在一次攻击中和用好几种系统。综合应用攻击策略可以增强攻击的成功率。同时和用好几种系统使他们更不容易被捕获。

例如，在实施IP欺骗时，攻击者通常会先实施拒绝服务攻击以确保被攻击特征；会建立任何连接。大多数使用Man-in-the-middle的攻击者会先捕获SMB的密码，再使用LOphtCrack这样的程序进行暴力破解攻击。

渗透策略

你已经了解到那些网络设备和服务是通常遭受攻击的目标和黑客活动的攻击特征。现在，请参考下列的一些场景。它们将有助于你在审计过程中关注那些设备和服务。请记住，将这些攻击策略结合起来的攻击是最容易成功的。

物理接触

如果攻击者能够物理接触操作系统，他们便可以通过安装和执行程序来使验证机制无效。例如，攻击者可以重启系统，和用其它启动盘控制系统。由于一种文件：系统可以被另一种所破坏；，所以你可以使用启动盘获得有价值的信息，例如有管理权限的账号。

物理攻击的简单例子包括通过重新启动系统来破坏；Windows95或98的屏幕锁定功能。更简单的物理攻击是该系统根本就没有进行屏幕锁定。

操作系统策略

近来，美国白宫的Web站点(http：／／www,whitehouse．gov)被一个缺乏经验的攻击者黑掉。攻击者侦查出该Web服务器(WWWl．whitehouse．gov)运行的操作系统是Solaris 7。虽然Solaris7被成为艺术级的操作系统，但管理员并没有改变系统的缺省设置。虽然该站点的管理员设置了tripwire，但攻击者还是使用phf／ufsrestore命令访问了Web服务器。

较弱的密码策略

上面白宫网站被黑的例子可能是由于该系统管理员使用FTP来升级服务器。虽然使用FTP来更新网站并没有错，但大多数FTP会话使用明文传输密码。很明显，该系统管理员并没有意识到这种安全隐患。又由于大多数系统管理员在不同的服务上使用相同的密码，这使攻击者能够获得系统的访问权。更基本的，你可以保证／etc／passwd文件的安全。

NetBIOS Authentication Tool(NAT)

当攻击者以WindowsNT为目标时，他们通常会使用NetBIOSAuthenticationTool(NAT)来测试弱的口令。这个程序可以实施字典攻击。当然它也有命令行界面，这种界面的攻击痕迹很小。而且命令行界面的程序也很好安装和使用。在使用NAT时，你必须指定三个文本文件：和IP地址的范围。当然，你也可以指定一个地址。NAT使用两个文本文件来实施攻击而第三个来存储攻击结果。第一个文本文件包含一个用户列表，第二个文件中是你输入的猜测密码。

当使／H命令行版本时，语法格式为：

nat -U username．Txt -ppasswordlist．Txt –O outputfile．tXt

即使服务恭设置了密码的过期策略和锁定，攻击者还是可以和用NAT反复尝试登录来骚扰管理员。通过简单地锁定所有已知的账号，攻击者会极大地影响服务器的访问，这也是·一些系统管理员不强行锁定账号的原因。

较弱的系统策略

到此为止，你已经学习了一些外部攻击。然而，对于-管理员来说最紧迫的是大多数公司都存在不好的安全策略。如果安全策略很弱或干脆没有安全策略，通常会导致弱的密码和系统策略。通常，公司并不采取简单的预防措施，比如需要非空的或有最小长度要求的密码。忽略这些限制会给攻击者留下很大的活动空间。

审计文件系统漏洞

不论你的操作系统采取何种文件系统(FAT，NTFS或NFS)，每种系统都有它的缺陷。

例如，缺省情况下NTFS在文件夹和共享创建之初everyone组可完全控制。由于它是操作系统的组成部分(WindowsNT)，因此也成为许多攻击的目标。NFS文件系统可以共享被远程系统挂接，因此这也是攻击者入侵系统的途径之一。

IP欺骗和劫持：实例

IP欺骗是使验证无效的攻击手段之一，也是如何组合攻击策略攻击网络的典型实例。IP欺骗和用了Intemet开放式的网络设计和传统的建立在UNIX操作系统之间信任关系。主要的问题是使用TCP／iP协议的主机假设所有从合法IP地址发来的数据包都是有效的。攻击者可以利用这一缺陷，通过程序来发送虚假的IP包，从而建立TCP连接，攻击者可以使一个系统看起来象另一个系统。 .

许多UNIX操作系统通过rhosts和rlogin在非信任的网络上(如Internet)建立信任的连接。这种传统的技术是流行的管理工具并减轻了管理负担。通常，这种系统由于把UNIX的验证机制和IP地址使用相结合从而提供了适当的安全。然而，这种验证机制是如此的独立于IP地址不会被伪造的假设，以至于很容易被击破。

Non-blind spoofing和Blind spoofing

Non-blind spoofing是指攻击者在同一物理网段上操纵连接。Blind spoofing是指攻击者在不同的物理网段操纵连接。后者在实施上更困难，但也时常发生。

进行IP欺骗的攻击者需要一些程序，包括：

- 一个包嗅探器
- 一个能够同时终止TCP连接、产生另一个TCP连接、进行IP伪装的程序

IP欺骗涉及了三台主机。像先前分析的那样，使用验证的服务器必须信任和它建立连接的主机。如果缺乏天生的安全特性，欺骗是非常容易的。

思·下列的场景，有三台主机分别是A,B和C。A使用TCPSYN连接与合法用户B初始一个连接。但是B并没有真正参与到这次连接中，因为C已经对B实施了拒绝服务攻击。所以，虽然A认为是在与B对话，但实际上是与C对话。IP欺骗实际上组合了几种攻击手法包括对系统实施了拒绝服务攻击，还包括和用验证技术。

作为审计人员，你不应该说服管理员终止这种信任关系，相反，你应当建议使用防火墙规则来检测有问题的包。

TCP／IP堆栈

为了成功地审计系统，你需要理解每种攻击的特征。

SYN flood攻击

这种拒绝服务攻击和用了TCP建立连接时三方握手的弱点。攻击者可以建立很多半开连接。在这个过程中，当服务器要跟攻击者建立连接时，攻击者却终止了连接。攻击者再建立其它的连接然后再终止，直到目标服务器打开成百上千的半开连接。SYNflood是最常见的攻击Web服务器的攻击手段。

Smurf和Fraggle攻击

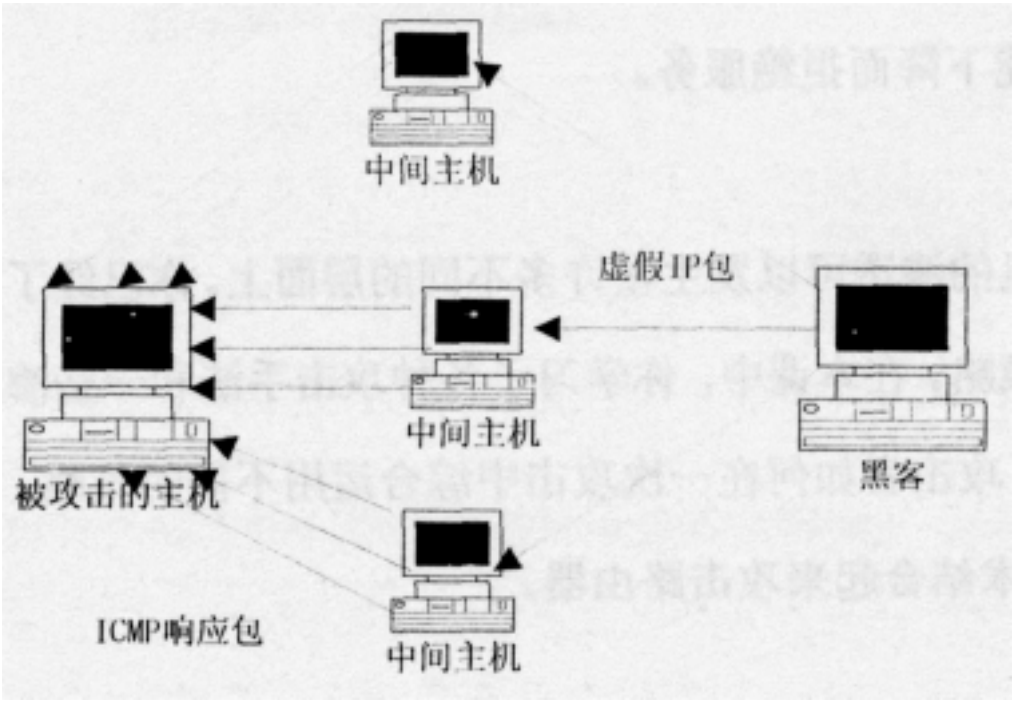
Smurf攻击是和用Ping程序中使用的ICMP协议。攻击者首先制造出源地址是受攻击主机的IP地址的包。下一步，攻击者将这些包发送给不知情的第三方，使它们成为帮凶。如果攻击者发送足够的ICMP包，回应会超过受攻主机的承受能力。实际上Smurf攻击是一种IP欺

骗式的攻击，将导致拒绝服务攻击的结果。

Fraggle攻击与Smurf攻击类似，只是和用UDP协议。虽然标准的端口是7，但是大多数使用Fraggle攻击的程序允许你指定其它的端口。

最好的防止你受到Smurf和Fraggle攻击的方法是在防火墙上过滤掉ICMP报文，或者在服务器上禁止Ping。当然，这要付出加大连通性测试难度的代价。

如图所示smurf攻击原理



Smurf,Fraggle,和广播地址

广播地址是指那些结尾是255或0的地址。有些路由器回应广播IP地址。广播地址可以被合法地用于排错工具。你可以向整个子网发送Ping包看哪些地址回应。当然，这些地址也会被Smuff和Fraggle攻击所和用，一个广播地址会有上百台主机参与攻击。

作为审计人员，你应当建议在路由器上禁止网络中的直接广播地址。访问http：／／netscan．org你可以获得更多有关直接广·播和Smuff与Fraggle攻击的信息。

Teardrop／Teardrop2

Teardrop类的攻击和用UDP包重组时重叠偏移的漏洞。例如，Sendmail使用ident服务 来验证用户访问服务的尝试。你可以从RFCl413文件了解更多的identity协议。

Linux和WindowsNT以及95／98更容易遭受这些攻击。Teardrop是一种拒绝服务攻击，会导致蓝屏死机，并显示STOPOxOOOOOOOA错误。虽然大多数操作系统打了防止这种攻击的补丁，但Teardrop仍然会耗费处理器的资源和主机带宽。Teardrop和Teardrop2的关键区别是后者使用20个字节的数据填充，而且欺骗了包的长度，允许新的攻击者绕过特定的服务补丁”和hotfix。

技术提示：Teardrop攻击通常被称为Boink攻击，而Teardrop2攻击被称为Bonk攻击。

Ping of death

这种攻击通过发送大于65536字节的ICMP包使操作系统崩溃。通常不可能发送大于65536个字节的ICMP包，但可以把报文分割成片段，然后在目标主机上重组。最终会导致

被攻击目标缓冲区溢出。

Land attack

这种攻击是指攻击者发送IP和端口(source和destination)相同的包，导致被攻击目标由于系统崩溃或性能下降而拒绝服务。

本章小结：

对网络和主机的渗透可以发生在许多不同的层面上。你已经了解到包括获得服务器的访问权在内的一些策略。在本课中，你学习了各种攻击手法和一些渗透攻击网络主机的程序和方法。你还学习了攻击者如何在一次攻击中综合运用不同的策略。例如，攻击者将拒绝服务攻击和IP欺骗技术结合起来攻击路由器。

第四章

控制阶段的安全审计

引　　言

前面我们已经学习了有关网络侦查和渗透的手段。作为审计人员，你同样有责任提醒你的客户，攻击者可以在服务器和网络上建立控制。为了有效地做到这一点，你必须熟悉那些能够成功获得网络控制权的规则、工具和手段。审查典型的控制手段将有助于你发现并汇报这种弱点和漏洞。

本章要点：

- 了解控制过程
- 识别控制手段
- 掌握记录控制过程和手段的方法

控制阶段

一旦攻击者成功地渗透进你的系统，他会立即试图控制它。在这一阶段的目标包括：

- 获得root的权限
- 收集信息
- 开启新的安全漏洞
- 擦除渗透痕迹
- 攻击其他系统

如果攻击者成功地进行到这一阶段，通常就很难被发觉了，应该在渗透阶段阻上下他们的攻击行为。

获得root的权限

攻击者最终目的是获得root的权限。Root权限是终极的前门，因为它有权建立更多的

账号，操纵服务和持续控制系统。攻击者会采用许多不同的策略来获得这一权限，包括前门课程中讨论的各种手段。像BackOrifice(只对Windows95／98有效)和NetBus、冰河等非法服务是众所周知的允许攻击者获得并保持root权限的工具。UNIX操作系统更容易出现trap door和缓冲区溢出的问题。

非法服务和trap door允许攻击者使用合法的账号来升级访问权限。如果攻击者获得了合法的用户账号，他就很容易升级和获工具有管理权限的账号。攻击者和用账号来做的不仅仅是访问系统。

创建额外账号

为了减小从系统中被清除的几率，攻击者通常会在获得root权限后创建额外的账号。使用几种不同的账号攻击者便可以进行异常的活动，将被察觉的可能性降到最低。即使被察觉，攻击者也可以凭借多个账号进入系统。例如一些大刑的公司被渗透得很彻底以至于弄不清哪些账号是合法的哪些不是。攻击者的目的是造成这种不确定性。

使用批处理文件是创建额外账号的一种手段。例如，你可以在Windows记事本中建立有关文本文件。你可以给它起任何的文件名，但要用．bat做文件的扩展名。这个特殊的批处理文件使用netuser命令在WindowsNT中增加账号。如果愿意的话，你还可以给这些账号增加密码。注意在命令的最后加上／add字符串。在批处理文件中还可将新增的账号加入了管理员组中。如果该组不存在，批处理文件会建立它。你也可以增加没有密码的管理员账号。在UNIX和Novell操作系统中同样存在类似的问题。

技术提示：要想使用NetBus进行控制，登录用户必须拥有更新密码的权限(例如，更新WindowsNTSAM数据库)，然而，如果当前用户工具备这样的权限，你可以和用scheduling服务，或者把批处理程序放在＼winnt＼profilesXAdministrator＼Start MenuXPrograms＼Startup目录中。这样，当管理员登录时该文件自动运行。

审计这种控制手段的方法是查看哪些没有填写完整的用户账号。例如，上面的批处理文件并没有在域用户管理器中加入任何描述性的语句。

获得信息

一旦攻击者获得root的权限，他将立即扫描服务器的存储信息。例如，在人力资源数据库中的文件：，支付账目数据库和属于上层管理的终端用户系统。在进行这一阶段的。控制活动时，攻击者在脑海中已经有明确的目标。这一阶段的信息获取比侦查阶段的工具有针对性，该信息只会导致重要的文件和信息的泄漏。这将允许攻击者控制系统。

攻击者获得信息的一种方法是操纵远程用户的Web浏览器。大多数的公司并没有考虑到从HTTP流量带来的威胁，然而，Web浏览器会带来很严重的安全问题。这种问题包括Cross-frame browsing bug和Windows spoofing以及Unicode等。浏览器容易发生缓冲区溢出的问题，允许攻击者对运行浏览器的主机实施拒绝服务攻击。一旦攻击者能够在局部使系统崩溃，他们便可以运行脚本程序来渗透和控制系统。

Cross-frame browsing bug允许怀有恶意的Web站点的制作者创建可以从用户计算机上获得信息的Web页面。这种情况出现在4．x和5．x版本的Netscape和Microsoft浏览器上，这种基于浏览器的问题只会发生在攻击者已经知道文件和目录的存储位置时。这种限制看起来不严重，但实际上并非如此。其实，任何攻击者都清楚地知道缺省情况下UNIX操作系统的重要文件存放在(＼etc)目录下，Windows NT的文件在(＼winnt)目录下，IIS在 (＼inetpub＼wwwroot)目录下等等。

大多数的攻击者都知道操作系统存放文件的缺省位置。如果部门的管理者使用Windows98操作系统和MicrosoftWord，Excel或Access，他很可能使用＼deskto＼MyDocuments

目录。攻击者同样知道＼windows~tart＼menu＼programs＼startup目录的重要性。攻击者可能不知道谁在使用操作系统或文件和目录的布局情况。通过猜测电子表格，数据库和字处理程序缺省存储文件的情况，攻击者可以轻易地获得信息。

虽然攻击者无法通过浏览器控制系统，但这是建立控制的第一步。和用Cross-frame browsingbug获得的信息要比从网络侦查和渗透阶段获得的信息更详细。通过阅读文件：的内容，攻击者会从服务器上获得足够的信息，要想阻止这种攻击手段，系统管理员必须从根本上重新配置服务器。

审计UNIX文件系统

Root kit充斥在互联网上，很难察觉并清除它们。从本质上来说， Root kit是一种木马。大多数的Root kit用各种各样的侦查和记录密码的程序替代了合法的1s，su和ps程序。审计这类程序的最好方法是检查象1s，su和ps等命令在执行时是否正常。大多数替代Root kit的程序运行异常，或者有不同的的文件大小。在审计UNIX系统时，要特别注意这些奇怪的现象。下表1列出了常见的UNIX文件的存放位置。

文件名	存放位置
／	根目录
／sbin	管理命令
／bin	用户命令：通常符号连接至／usr／bin
／usr	大部分操作系统
／usr／bin	大部分系统命令
／usr／iocal	本地安装的软件包
／usr／include	包含文件（用于软件开发）
／usr／src	源代码
／usr／iocal／src	本地安装的软件包的源代码
／usr／sbin	管理命令的另一个存放位置
／var	数据(日志文件，假脱机文件：)
／vr／log	日志文件
／export	被共享的文件系统

／home	用户主目录
／opt	可选的软件
／tmp	临时文件
／proc	虚拟的文件系统，用来访问内核变量

审计WindowsNT

下列出了在WindowsNT中通常文件的存放位置

文件名	位置
＼winnt	系统文件目录：包含 regedit. exe 和注册表日志
＼winnt＼system32	包含许多子目录，包括 config(存放 security.log，event.log 和 application.log 文件)
＼winnt＼system32＼config	包含 SAM 和 SAM. LOG 文件，NT 注册表还包含密码值
＼inetpub	缺省情况下，包含 IIS4. 0 的文件，包括＼ftproot，＼wwwroot
＼programfiles	服务器上运行的大多数程序的安装目录
＼winnt＼profiles	存放与所有用户相关的信息，包括管理配置文件

L0phtCrack工具

L0phtCrack被认为是对系统攻击和防御的有效工具。它对于进行目录攻击和暴力攻击十分有效。它对于破解没有使用像!@#￥%／＼&*()等特殊字符的密码非常迅速。L0phtCrack可以从http：／／www,lOpht,com上获得。

L0pht使用文字列表对密码进行字典攻击，如果字典攻击失败，它会继续使用暴力攻击。这种组合可以快速获得密码。L0pht可以在各种各样的情况＇下工作。你可以指定IP地址来攻击WindowsNT系统。然而，这种方式需要首先登录到目标机器。L0pht还可以对SAM数据库文件进行攻击。管理员从＼winnt\ repair目录拷贝出SAM账号数据库。第三中方式是配置运行LOpht的计算机嗅探到密码。LOpht可以监听网络上传输的包含密码的会话包，然后对其进行字典攻击。这种方式使用L0pht需要在类似WindowsNT这样的操作系统之上，并且你还需要物理地处于传输密码的两个操作系统之间。

UNIX密码安全

UNIX下的密码文件通常存放于／etc／passwd，它保存着可读驭的账号信息。所有的数据 (除加密的密码数据)都存储在这。因为必须把UID号与用户名相互转换，而且确定用户的宿主目录所以这个文件是必要的。

／etc／passwd文件是冒号分隔的文本文件，文件的每一行都以下列的格式来描述一个用户的： usemame：x：UID：GID：FullName：HomeDirectory：Shell

例如，参考下列记录：

test：x：501：501：testuserJames：／home／test：／bin／bash

上面记录描述了一个用户名是test．UID号是501，GID号是501，全名是testuser james，宿主目录是／home／test，和登录shell是／bin／bash的用户。Password文件：必须能够被所有用户读取，但是不能被除root外的任何用户写入：而且／etc目录只能被root写入。

shadow密码文件

老版本的UNIX操作系统如SunOS，在／etc／passwd文件：中还包含经过加密的用户登录密码。加密的密码被存储在前面例子中的x位置(在用户名和UID中)。因为密码以加密方式存储，所以它不能直接被读取。但是，如果有加密的密码，一个攻击者可以从字典中读取字串和用相同的加密算法进行加密，再将运算的结果和密码文件中的进行比较。由于用户一般容易选择较弱的密码，所以这种基于字典的攻击经常能够破坏；系统。

为了防范基于字典的攻击，UNIX操作系统采用了shadow密码的技术。加密的密码从／etc／passwd文件移植到第二个文件中，(／etc／shadow文件：或类似的文件：)。这个文件：只有root可读。由于不能被别的用户读取，所以加密的密码通常的用户不可见，也就避免了上面讨论的字典攻击。

各种操作系统的shadow文件：的名称并不相同，如下表所示

操作系统	Shadow 密码文件
AIX	／etc／security／passwd
Linux，Solaris	／etc／shadow
HP-UX(v. 9)	／. security／etc／passwd
HP-UX(v.10)	A different approach,using a protected password database

除了加密密码外，shadow密码文件还可以包含密码过期的信息。这一信息用来迫使用户在一定情况下改变密码。我们将会在稍后来讨论shadow文件的概念。

命令passwd将加密的密码插入／etc／shadow文件：中。Root可以运行带用户名参数的passwd命令为任何用户设置密码。例如，为user用户更改密码，使用—下列语法命令：

host#passwd user

Password：[mdden]

Pe-type：(hidden)

JohntheRipper和Crack

JohntheRipper和Crack是在基于UNIX的操作系统上常见的暴力破解密码的程序。这两个工具被用来设计从UNIX上获取密码。所有版本的UNIX操作系统都将用户账号数据库存放在／etc／passwd或／etc／shadow文件中。这些文件在所有UNIX系统中存放在相同的位置。为了使UNIX正常运行，每个用户都必须有读取该文件的权限。

JohntheRipper和Crack是最常见的从shadow和passwd文件中获得密码的程序。这些两个工具将所有的密码组合与passwd或shadow文件：中加密的结果进行比较。一旦发现有吻合的结果就说明找到了密码。

在你审计UNIX操作系统时，请注意类似的问题。虽然许多扫描程序，如NetRecon和ISS Internet Scanner可以模仿这种-工具类刑，许多安全专家还是使用像L0pht和John the Ripper来实施审计厂作。

信息重定向

一旦攻击者控制了系统，他便可以进行程序和端口转向。端口转向成功后，他们可以操控连接并获得有价值的信息。例如，有些攻击者会禁止像FTP的服务，然后把FTP的端口指向另一台计算机。那台计算机会收到所有原来那台主机的连接和文件：。

相似的攻击目标还包括重定向SMTP端口，它也允许攻击者获得重要的信息。例如，攻击者可以获得所有使用SMTP来传送E-mail账号的电子商务服务器的信息。即使这些传输被加密，攻击者还是可以获得这些传输的信息并用字典攻击这些信息。

创建新的访问点

你已经知道了攻击者会试图通过控制和建立新的账号来创建尽可能多的前门。通过安装额外的软件和更改系统参数，攻击者还可以开启后门。像优秀的系统管理员，黑客通常习惯于某种攻击策略，所以你必须注意攻击者的控制手段。安装后门的另一个通常方法是在操作系统中安置木马。

端口转向

攻击者通常使用多个Telnet或FTP会话来隐藏他们的行为，这种连接的链条会花费更多的时间来追踪。端口转向是一种有效的攻击策略，因为很难准确追踪通过端口转向连接的攻击者。

自动添加账号和木马

通常，一个负责任的系统管理员会定期扫描用户的账号数据库，查看是否有权限的变更，新添加的账号和任何有关系统策略更改的可疑行为。然而，攻击者会和用老的账号登录系统。即使管理员定期核查用户的账号数据库，攻击者还可以和用定时服务等自动执行的程序来添加账号。通过定时服务来添加新的账号和重新设置权限，攻击者可以骗过最挑剔的管理员。其它添加账号的方法包括使用像NctBv．s或BackOrifice 2000这样的程序来完全绕过安全账号数据库。你将在稍后学习这些程序。

擦除渗透的痕迹

如果实施了审核，你会记录下足够的黑客活动的证据。通常，攻击者反复尝试登录系统的记录很容易被发现。销毁这些记录的最好的方法是找到操作系统的日志存放位置。通过破坏这些日志文件，攻击者可以骗过系统管理员和安全审计人员。

这些日志文件包括：

- Web服务器
- 防火墙
- SMTP,HTTP和FTP服务器
- 数据库

日志文件：类型包括：

- 事件：日志
- 应用程序日志
- 安全日志

作为跳板攻击其它系统

通常,攻击者渗透你的操作系统的目的是通过它来渗透到网络上其它的操作系统。例如，NASA服务器是攻击者通常的攻击目标，不仅因为他们想要获取该服务器上的信息，更主要的是许多组织都和该服务器有信任的连接关系，比如DepartmentofDefense。

因此，许多情况下，攻击者希望攻击其它的系统。为了防止类似的情况发生，美国政府要求那些直接连到政府部门的公司必须按照Rainbow Series的标准来实施管理。从1970年开始，该系列标准帮助系统确定谁可以安全的连接。这个系列中最长被使用的是Department Of DefenseTrusted Computer System Evaluation Criteria，该文件被成为OrangeBook。例如，C2标准是由OrangeBook衍生出来并被用来实施可以信任的安全等级。这个等级是C2管理服务(C2Config．exe)在MicrosoftNT的服务补丁基础上提供的。

控制方法

新的控制方法层出不穷，原因有以下几个。首先是因为系统的升级不可避免的会开启新的安全漏洞，二是少数黑客极有天赋，他们不断开发出新的工具。大多数的UNIX操作系统都有C语言的编译器，攻击者可以建立和修改程序。这一部分讨论一些允许你控制系统的代表性程序。

系统缺省设置

缺省设置是指计算机软硬件 ‘ Out-of-the-box ”的配置，便于厂商技术支持，也可能是因为缺乏时间或忽略 · 了配置。攻击者和用这些缺省设置来完全控制系统。虽然改变系统的缺省设置非常容易，但许多管理员却忽视了这种改变。其实，改变缺省设置可以极大地增强操作系统的安全性。

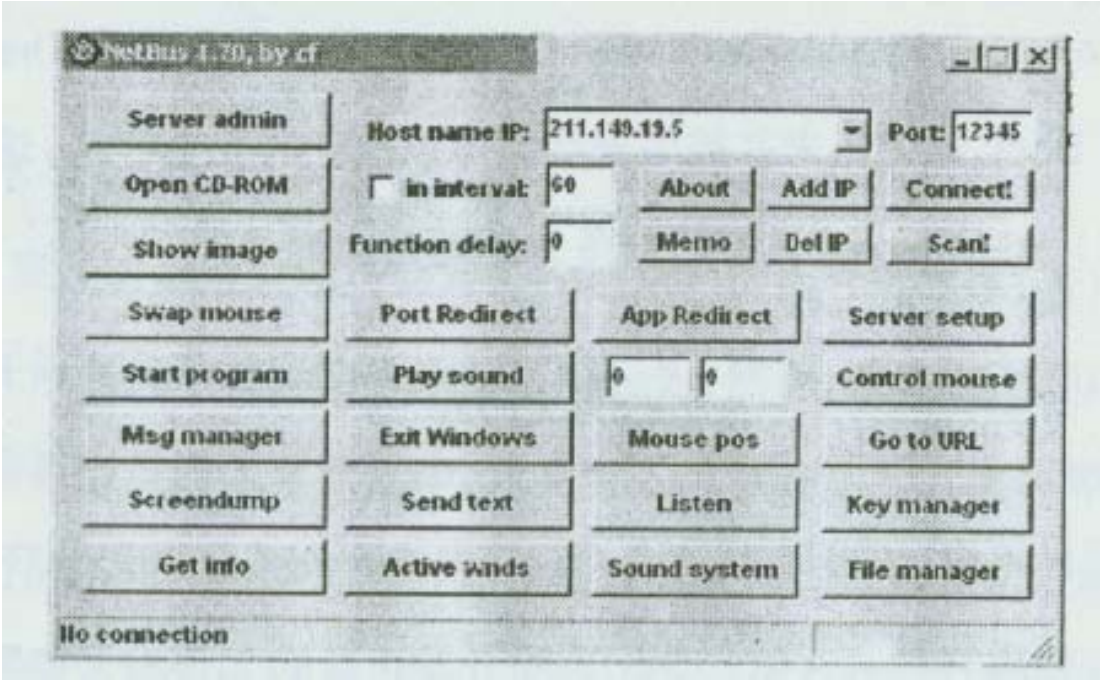
合法及非法的服务，守护进程和可装载的模块

WindowsNT运行服务，UNIX运行守护进程，Novell操作系统运行可装载的模块。这些守护进程可以被用来破坏操作系统的安全架构。例如，Windows NT的定时服务以完全控制的权限来执行。如果用户开启了定时服务，他就有可能运行其它的服务，(例如，域用户管理器)，从而使用户更容易控制系统。

攻击者可以建立破坏安全的守护进程。有些可以捕获密码，并通过邮件：发送给远方攻击者。另外，像rootHt可以绕过安全账号数据库，进而完全控制系统。有两个众所周知的I工具NetBus和BackOrifice。虽然，它们已不再是最前卫的工具了，但这种控制思想仍然延续着。

NetBus ·

在一九九六年三月发布的NetBus被用于控制Windows95／98和NT操作系统。最初的版本是1．5版，后来有了1．6和1．7版的升级。NetBus可以破坏；操作系统中已经存在的安全构架。它允许远程用户以当前登录用户的权限来控制系统(例如，添加，删除和复制文件)，如下图是NetBusl．7的界面。



NetBus2．0版的程序功能更强，它需要额外的配置，记录大量的日志，所以目标太大，通过这个版本已用做远程管理的工作。所有版本的NetBus都允许设置密码，通过密码攻击者可以把你排除在操作系统的管理者之外。

一旦NetBus被安装在你的操作系统上，非授权的用户便可以：

- 运行程序
- 强迫重启系统
- 注销用户
- 控制Web浏览器，包括指向特定的URL
- 捕捉击键记录(仅在WindowsNT—下有效)
- 重定向端口和程序
- 获得关于当前版本的信息
- 上传，下载和删除文件：
- 控制，升级和定制服务器
- 管理密码保护
- 显示，终止远程系统上的程序

NetBus传输

NetBus使用TCP建立会话。缺省情况下，服务器使用12345端口。12631也是一个通常使用的监听端口，当然服务器可以配置用任意端口监听。因此，如果攻击者自己定制了服务器的话，跟踪NetBus的活动将变得很困难。然而，NetBus服务器也使用12346端口来建立初始

连接，不经过编译程序无法改变这个端口。作为审计人员，你可以通过捕获包来检查这个端口。客户端动态地产生端口，给扫描类似的端口带来很大的困难。
许多类似的程序使用固定的端口，你可以扫描整个的网络监测可疑的活动。

配置信息

下列表格提供了从1．6到2．0版的NetBus的文件大小，这些数据有助于你来确定是否有木马存在。NetBusl．6版中的文件

文件	描述	大小(kB)
NetBus. exe	客户端	567,296
Patch. exe	服务器	472,576
Keyhook. dll	附加的服务器文件	54,784

NetBus1．7中文件的大小

文件：	描述	大小(kB)
NetBus. exe	客户端	599,552
Patch. exe	服务器	494,592
Keyhook. dll	附加的服务器文件：	54. 784

NetBus2．0使用了许多附加的文件，使该程序更容易被检测和删除

文件	描述	大小(kB)
NetBus. exe	客户端	1,24l,600
Patch. exe	服务器	624,640
NBHelp. d11	程序扩展	7l，680

技术提示：请注意这些程序可以被改成其它的文件名。

注册表项

NetBusl．x版的程序使用下列的注册表项，在每次系统启动时在内存中运行服务器：
HKEY—LOCAlMACHINE＼SOFTWARELMicrosofi＼Windows＼CurrentVersion＼Run＼
注册表中的键值和server的名称相同，所以请寻找任何可疑的表项。Patch．exe是最常用

的名字。如果攻击者对服务器采用了密码保护，则密码将以明文的方式存储在·下面的注册表键值中：

HKEY—CURRENT USER＼Patch＼Settings＼ServerPwd

对于某些版本的NetBus，下列键值是用来启动程序的：

HKEY — LOCAlMACHINE ＼ SOFTWARE ＼ Microsofi ＼ Windows ＼ CurrentVersion ＼ RunServices

技术提示：任何优秀的病毒扫描器都会捕获大多数的NetBus，虽然有些版本的NetBus通过改变特征码来避开病毒扫描器，你还是可以下载McAfee或No~on反病毒软件：来解决这一问题。研究NetBus控制的过程是要学习非法服务是如何控制系统的。

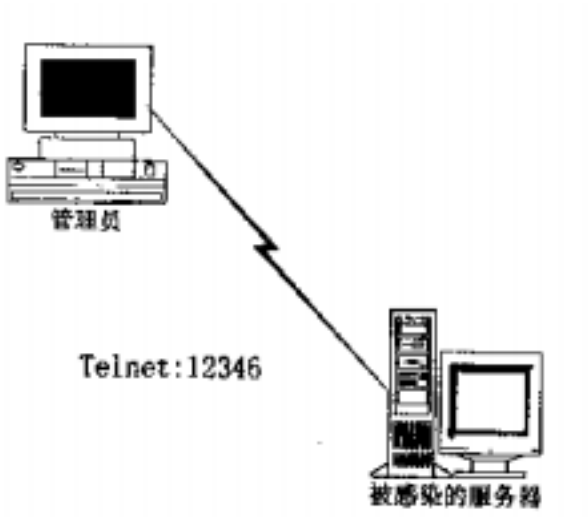
检测NetBus

首先，你可以考虑使用象TCPDUMP或NetXRay等包嗅探器，检查缺省的12345端口或12346端口。即使应用了入侵监测系统，你还是应当定期的运行包嗅探器，这有助于确定可疑的活动。

使用netstat，你可以键入—下列命令：

Netstat -an或Netstat -p udp

你也可以使用Telnet来连接NetBus。通过连接12345或12346端口，你可以简单地确定系统是否中了NetBus，如下图所示。



如果服务在运行而你试图连接12346端口的话，将被提示连接遗失。如果服务没有运行的话，连接会失败。有时，服务器图标会显示为火炬，火炬图标说明是1．6版的NetBus。1．7版的图标我们会在本课的实验中看到。有些版本的程序图标显示为MicrosoftInternetExplorer的频道形状。如果用户知道这些图标的含义，将有助于问题的解决。

当前的NetBus2．0版不象一个黑客工具而更象一个“合法”的程序。但是，考虑到该程序的历史，你应当对它也引起高度的重视。和用流行的图标生成和编辑工具，你可以任意改变NetBus图标的显示形式。使用像SaranWrap和SilkRope这样的程序，你可以使程序显示为任何的程序。类似的程序可以使用户以为安装了合法的程序，而实际上却安装了木马程序。

清除NetBus

高质量的反病毒程序可以检测并清除NetBus。如果NetBus服务器正在运行，操作系统

由于把NetBus看成系统的一部分所以不会让你从Windows资源管理器中删除它。然而，你可以使用Telnet来删除NetBus服务。Telnet到12345端口，再输入下列命令：

RemoveServer；1；

请确保输入上面的命令，使用相同的大写字母和分号。你也许要重复这个命令。通常，如果连接中断说明NetBus服务被删除了。你可以重启系统；再使用telnet来确定该服务是否被清除。

如果有密码保护，会先提示你需要密码。如果确实如此而你又无法猜到密码，你可以运行LOphtCrack，或者用DOS启动并手动删除该服务揣。Telnet到服务揣并输入下列命令可以得知该程序的安装信息。

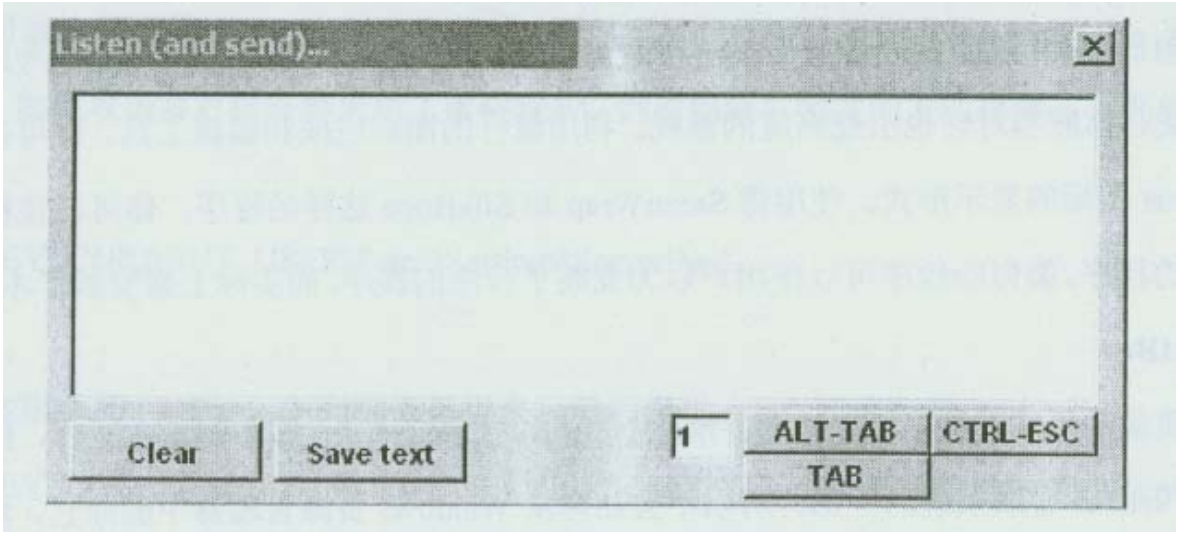
Getlnfo；0；

该命令将告知你文件的位置,重启后是否自动运行,以及有多少客户端连接到服务器。另一种清除NetBus的方法是使用其客户端，点击清除服务器按钮。如果攻击者采用了密码保护的话可能会要求你输入密码。你也可以搜寻前面讨论的文件：。虽然服务器可以被重命名，但是到2．0版Keyhook．d11文件名一直保持不变。2．0版使用NBHelp．d11做文件：名。绝大多数的反病毒程序，如NortonAntivirus等，可以检测出所有版本的NetBus，然而，能够检测NetBus并不能意味着可以检测其它类似的非法程序。因此，你还需要检查注册表。

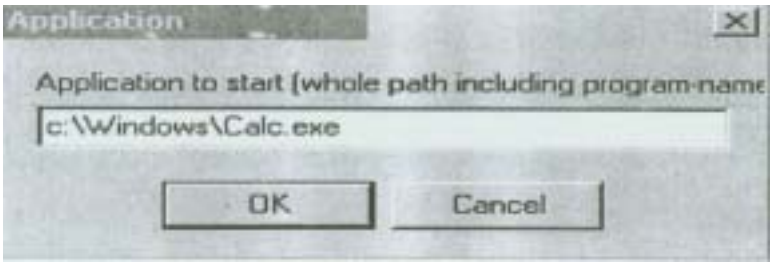
警告：你可以·下载许多检查NetBus的程序。然而，你需要从值得信赖的站点上下载，如Norton反病毒程序的制造商。其它的声称可以清除NetBus木马的程序可能会在你的操作系统上植入新的木马。

NetBus命令

点击Listen按钮会打开监听和发送窗口，如下图所示。



如果连接是激活的，你可以利用该窗口来捕获键盘输入信息。点击FileManager按钮允许你从远程主机上传和下载文件。Show Files按钮允许你扫描硬盘，而Download，Upload和Delete按钮更是不言自明了。点击KeyManager的按钮，你可以使键撤有效或无效。StartProgram 按钮允许你允许任何程序，包括批处理和其它应用程序。任何攻击者都可以如下图所示输入应用程序的位置。



PortRedirect按钮允许你把本机的某一端口流量转到另一端口，甚至转到其它主机的端口。AppRedirect按钮允许你将某一程序的运行指定到特定的端口，从而可以远程使用Teinet进行控制。除了必须有个用户登录服务器外，该命令不需要依赖任何本地的用户的干涉。

BackOrifice和BackOrifice2000

BackOrifice是另一个允许用户得到操作系统控制权的黑客工具。BackOrifice只能攻击Windows95和98系统。BackOrifice2000可以工作在所有Windows操作系统中。这个程序不会对UNIX系统造成直接的威胁，但是会极大地危害Windows系统。入侵者和用BackOrifice2000来攻击Windows操作系统，从而可以获得危害UNIX和Novell系统的信息。任何连接到BackOrifice服务器的大都可以获得操纵网络连接的信息。这一工具使攻击者和用可信任的系统获得非授权的访问成为可能。你可以从许多站点获取BackOrifice和BackOrifice2000，包括packerstorm,securify.com。

BackOrifice和BackOrifice2000使用和NetBus相同的客户端朋艮务器系统的构架。客户端可以是UNIX，Windows95／98和WindowsNT操作系统。

如果未被检测到，BackOrifice和BackOrifice2000允许攻击者：

- 获取系统信息，包括当前用户，CPU种类，Windows版本号，内存使用，挂接磁盘的种类(包括网络磁盘映射)，和所有驱动的信息。
- 收集用户名和密码(包括屏幕锁定密码)和用户缓存的密码(如拨号连接，Web和网络访问)。
- 获得文件的完全访问权限，包括运行程序和进程的权限；写入注册表的权限；列出可访问网络资源的权限；列出、建立和删除网络连接的权限；列出所有共享的资源和密码；建立和删除共享。
- 实施端口和程序的重定向，包括通过TCP远程Telnet来运行程序。
- 通过HTTP从浏览器上传和下载文件。

缺省设置：

服务器缺省在UDP的31337端口进行监听。当然，你可以配置服务器在任何的非保留端口进行监听。BackOriffice还提供了HTTP服务，你可以将它配置在任何的非保留端口，如8080。BackOrifice2000允许你将传输的数据加密并且可以使用任何端口。

缺省情况下，客户端使用UDPl049端口。当服务器提供HTTP服务时，客户端可以使用1056端口进行连接。然而，攻击者可以在命令行使用带参数p的命令来改变端口。这使得在网络上追踪BackOrifice的工作变得很困难。不像NetBus，BackOrifice加密所有客户端到服务器的会话信息。

精选命令

下表列出了你在BackOrifice命令行可以执行的命令。在学习过程中，请注意中了

BackOrifice和BackOrifice2000的Windows98客户端是很容易给UNIX,Novell和NT服务器带来危害的。

命令	描述
Dir,md,rd	列出，建立和删除目录
Shareadd／sharelist／sharedel	建立，列出和删除共享
Copy／delete／find	拷贝，删除和搜索文件
View	列出文本文件内容
Httpon／httpoff	启动和停止 HTTP 服务，必须指定端口号。
Keylog start／end	开始和终止键盘记录
Netconnect netlist／Netdisconnect	将服务器系统连接到网络资源；列出网络接口，域和服务器；断开连接
Rediradd／redirlist	将 TCP 连接和 UDP 包重定向到其它的 IP
Regmakekey／regdelkey	建立和删除注册表中的键值
Passes	列出系统的所有密码，包括所有适配器(如拨号适配器)和网络连接，以及屏幕锁定
Reboot	重新启动系统
Tcpsend	从 TCP 连接发送和接受文件：；同标准的 TFTP 服务器一样，客户端连接服务器机器，发送文件然后立即断开。
Quit	推出程序

审计和控制阶段

审计人员应当很好地和用扫描程序，日志文件和其它工具。然而，你必须懂得什么是可疑的流量。这些流量可能是象未授权的NMAP，SATAN，NetBus和BackOrifice2000等发出的数据包，或者是一些你从未听说过的程序。

审计人员和攻击者最主要的不同点是审计人员从不真正进入控制阶段。在这一阶段，请注意记录你在使用协议分析仪和其它工具时发现的问题。存在许多报告潜在控制问题的方法，每种都可以证明你能够获得系统的控制权。这些方法包括：

- 列出通过自动执行的扫描程序(如NetRecon，ISS Internet Scanner或eTrust Intrusion Detection)获得的信息。
- 产生流量记录在日志中，记录时间，用日志来证明你的活动。
- 显示捕获的报文，这些包包括断开号，IP地址和其它信息。
- 显示你渗透的屏幕快照。

在本课中会有一些实验呈现给你一些控制系统的方法。这些信息只是用来说明目的，你不应当在审计或其它时候应用这些控制方法。

本章小结：

在本课中，我们学到了有关控制阶段的一些特殊步骤和方法，审计这些事件是困难的，需要我们熟悉每种黑客所采用的手法和工具，一些木马程序像netbus即使不是最新的工具，但了解它的原理对我们是有很大帮助的。

第五章

入 侵 监 测 系 统

引　　言

我们已经接触了手工和自动运行的扫描程序。这些：工具在审计过程中是非常有用的。你还使用了包嗅探器，这是另一个确定网络中存在哪些活动类型的工具。入侵监测系统会在两方面引起你的注意。首先，这种保护网络的形式变得越来越流行。你需要了解网络当前的结构来确定配置是否合适。第二，你可能在推荐这种产品，因此，你必须知道如何为特殊的网络情况推荐这种产品。

在测试过程中你可以使用多种类型的工具。这些工具在整个的审计过程中是必不可少的。它们会帮助你在枯燥乏味的分析过程中节省时间。

本章要点：

- 入侵监测系统的作用及原理
- 区分入侵监测系统和自动扫描程序
- 在入侵监测系统中使用的元素，包括manager和agent
- 入侵检测软件的应用

什么是入侵监测

入侵监测系统处于防火墙之后对网络活动进行实时检测。许多情况下，由于可以记录和

禁止网络活动，所以入侵监测系统是防火墙的延续。它们可以和你的防火墙和路由器配合：工作。例如，你的IDS可以重新配置来禁止从防火墙外部进入的恶意流量。你应当理解入侵监测系统是独立于防火墙工作的。

入侵监测系统IDS与系统扫描器systemscanner不同。系统扫描器是根据攻击特征数据库来扫描系统漏洞的，它更关注配置上的漏洞而不是当前进出你的主机的流量。在遭受攻击的主机上，即使正在运行着扫描程序，也无法识别这种攻击。

IDS扫描当前网络的活动，监视和记录网络的流量，根据定义好的规则来过滤从主机网卡到网线上的流量，提供实时报警。网络扫描器检测主机上先前设置的漏洞，而IDS监视和记录网络流量。如果在同一台主机上运行IDS和扫描器的话，配置合理的IDS会发出许多报警。

入侵监测的功能

大多数的IDS程序可以提供关于网络流量非常详尽的分析。它们可以监视任何定义好的流量。大多数的程序对FTP，HTTP和Telnet流量都有缺省的设置，还有其它的流量像NetBus，本地和远程登录失败等等。你也可以自己定制策略。下面讨论一些更常见的检测技巧。

网络流量管理

像ComputerAssociates ’eTrust Intrusion Detection(以前是SessionWall)，Axent Intruder Alert和ISSRealSecure等IDS程序允许你记录，报告和禁止几乎所有形式的网络访问。你还可以用这些程序来监视某一台主机的网络流量，eTrustIntrusionDetection可以读取这台主机上用户最后访问的Web页。

如果你定义了策略和规则，便可以获得FTP，SMTP，Telnet和任何其它的流量。这种规则有助于你追查该连接和确定网络上发生过什么，现在正在发生什么。这些程序在你需要确定网络中策略实施的一致性情况时是非常有效的工具。

虽然IDS是安全管理大员或审计人员非常有价值的工具，但公司的雇员同样可以安装像eTrustIntrusionDetection或IntrudeAlert这样的程序来访问重要的信息。攻击者不仅可以读取未加密的邮件，还可以嗅探密码和收集重要的协议方面的信息。所以，你首要的工作是要检查在网络中是否有类似的程序在运行。

系统扫描，Jails和IDS

在本教程的早些时候，你学习到如何应用不同的策略来加强有效的安全。这项任务需要在网络中不同的部分实施控制，从操作系统到扫描器、IDS程序和防火墙。你已经使用过系统扫描器，许多安全专家将这些程序和IDS结合起来。系统完整性检查，广泛地记录日志，黑客“ 监狱 ”和引诱程序都是可以同IDS前后配合的有效工具。

追踪 ·

IDS所能做到的不仅仅是记录事件，它还可以确定事件发生的位置，这是许多安全专家购买IDS的主要原因。通过追踪来源，你可以更多的了解攻击者。这些经验不仅可以帮你记录 ’ 下攻击过程，同时也有助于确定解决方案。

入侵监测系统的必要性

防火墙看起来好像可以满足系统管理员的一切需求。然而，随着基于雇员的攻击行为和产品自身问题的增多，IDS由于能够在防火墙内部监测非法的活动止变得越来越必要。新的技术同样给防火墙带来了严重的威胁。例如，VPN可穿透防火墙，所以需要IDS在防火墙后

提供安全保障。虽然VPN本身很安全，但有可能通过VPN进行通信的其中一方被root kit或NetBus所控制，而这种破坏行为是防火墙无法抵御的。基于以上两点原因，IDS已经成为安全策略的重要组成部分。

我们还需要注意的是，攻击者可以实施攻击使IDS过载，其结果可能是IDS系统成为拒绝服务攻击的参与者。而且，攻击者会尽量调整攻击手法，从而使IDS无法追踪网络上的活动。

入侵监测系统的构架

有两种构架的IDS可供选择，每种都有它的适用环境。虽然主机级的ID工具有更强的功能而且可以提供更详尽的信息，但它并不总是最佳选择。

网络级IDS

你可以使用网络级的产品，象eTrustIntrusionDetection只需一次安装。程序(或服务)会扫描整个网段中所有传输的信息来确定网络中实时的活动。网络级IDS程序同时充当管理者和代理的身份，安装IDS的主机完成所有的工作，网络只是接受被动的查询。

优点和缺点

这种入侵监测系统很容易安装和实施；通常只需要将程序在主机上安装一次。网络级的IDS尤其适合阻止扫描和拒绝服务攻击。但是，这种IDS构架在交换和ATM环境下工作得不好。而且，它对处理升级非法账号，破坏策略和篡改日志也并不特别有效。在扫描大型网络时会使主机的性能急剧下降。所以，对于大型复杂的网络，你需要主机级的IDS。

主机级IDS

像前面所讲的，主机级的IDS结构使用一个管理者和数个代理。管理者向代理发送查询请求，代理向管理者汇报网络中主机传输信息的情况。代理和管理者之间直接通信，解决了复杂网络中的许多问题。

技术提示：在应用任何主机级IDS之前，你需要在一个隔离的网段进行测试。这种测试可以帮助你确定这种Manager-to-agent的通信是否安全，以及对网络带宽的影响。

管理者Managers

管理者定义管理代理的规则和策略。管理者安装在一台经过特殊配置过的主机上，对网络中的代理进行查询。有的管理工具有图形界面而其它的IDS产品只是以守护进程的形式来运行管理者，然后使用其它程序来管理它们。

物理安全对充当管理者的主机来说至关重要。如果攻击者可以获得硬盘的访问权，他便可以获得重要的信息。此外，除非必需管理者的系统也不应被网络用户访问到，这种限制包括Intemet访问。

安装管理者的操作系统应该尽可能的安全和没有漏洞。有些厂商要求你使用特定类刑的操作系统来安装管理者。例如，ISSReaL Secure要求你安装在WindowsNTWorkstation而不是WindowsNTServer．这是由于在NTWorkstation上更容易对操作系统进行精简。

特殊的考虑

每种IDS厂商对他们的产品都有特殊的考虑。通常这些考虑是针对操作系统的特殊设置的。例如，许多厂商要求你将代理安装在使用静态IP地址的主机上。因此，你也许需要配置DHCP和WINS服务器来配合管理者。这种特殊的考虑在一定程度上解释了为什么大多数IDS

程序用一个管理者来管理数台主机。另外，安装管理者会降低系统的性能。而且，在同一网段中安装过多的管理者会占用过多的带宽。 另外，许多IDS产品在快于10MB的网络中工作起来会有问题。通常IDS的厂商要求你不要将管理者安装在使用NFS或NFS+的UNIX操作系统上，因为这种文件：系统允许远程访问，管理者会使它们缺乏稳定和不安全。

除非特殊情况，你不应将IDS的管理者安装在装了双网卡或多网卡的用做路由器的主机上，或者安装在防火墙上。例如，WindowsNTPDC或BDC也不是安装大多数IDS管理者的理想系统，不仅因为管理者会影响登录，而且PDC或BDC所必须的服务会产生trapdoor 和系统错误。

管理者和代理的比例

管理者和代理的比例数字会因生产厂商和版本的不同而不同。例如，Axent Intruder Alert建议在UNIX或NT的网络上不要使用超过100个代理，NetWare网络中每个管理者不应使用超过50个代理。然而，你需要建立基线来确定IDS结构的理想配置。理想配置是指IDS可以在不影响正常地网络操作的前提下实时监测网络入侵。

代理

自于代理负责监视网络安全，所以大多数的1DS允许你将代理安装在任何可以接受配g的主机上。当你在考虑产品时，你应当确保它可以和网络上的主机配合工作。大多数的产品在UNIX,NT和Novell网络环境中可以出色的工作。有些厂商也生产在特殊网络环境下工作的代理，例如DECnet，mainframes等等。无论如何，你应当通过测试来选择最适合你的网络的产品。所有的代理都工作在混杂模式，并且捕捉网络上传递的信息包。

理想的代理布局

请考虑将代理安装在像数据库，Web服务器，DNS服务器和文件：服务器等重要的资源上。像eTrust Intrusion Detection这样的基于扫描的IDS程序也许更适合在某些特定的时段扫描个别的主机。这个工具能够确保你在占用最小带宽的前提下监视网络活动。

下列是部分适合放置代理资源的列表：

- 账号、大力资源和研发数据库
- 局域网和广域网的骨干，包括路由器和交换机
- 临时工作人员的主机
- SMTP，HTTP和FTP服务器
- Modem池服务器和交换机、路由器、集线器
- 文件服务器

许多新的网络连接设备限制了IDS扫描。

管理者和代理的通信

在你学习如何为网络挑选产品时，需要明确管理者和代理的通信方式。大多数的IDS 程序要求你首先和管理者通信，然后管理者会查询代理。

通常，· 管理者和代理在通信时使用一种公钥加密。例如，Axent的产品使用400位长Diffie-Helman加密。标准的SSL会话使用128位的加密。比较这两种标准，你可以发现大多数的IDS厂商都采用安全的通信。

有些老的主机级的产品采用明文或经过非常弱地加密的会话。这种功能工具讽刺意味，由于明文传输易遭受叫acking和Man-in-the-middle攻击，这样会严重地破坏你监测和保护网络安全。

有些管理者可以和其它管理者通信。这种管理者之间的通信可以节省带宽并减轻你的管理负担。通过使用组织结构有可能避免这种通信。例如，AxentIntruderAlert(1TA)使用被称作domain的层次结构来组织代理。

审计管理者和代理的通信

作为审计人员，你应该对用户名和密码进行核实，而不应保留缺省设置。同时，你还要确保通信要经过加密和尽可能的安全。

IDS规则

就像应用防火墙，你必须为IDS建立规则。大多数的IDS程序都有预先定义好的规则。你最好编辑已有的规则并且增加新的规则来为网络提供最佳的保护。通常建立的规则有两大类：网络异常和网络误用。企业级的IDS通常可以实施上百条规则。

不同厂商在使用审计的术语时有所差别。例如，eTrustIntrusionDetection用“ rules ”来讨论安全审计的规则，而IntruderAlert却使用“ poiicies ”。你将会了解到IntruderAlert使用“ policies ”时意味更深远，它允许你为个别策略建立规则。因此，在理解各个厂商的产品时，不要被术语所迷惑。

网络异常的监测

IDS程序会报告协议级别的异常情况。如果配置正确的话，它可以提示你有关NetBus，Teardrop或Smurf攻击。例如，如果存在过多的SYN连接，IDS程序会向你报警。

网络误用监测

网络误用包括非工作目的的Web浏览，安装未授权的服务(如WARFTP服务)，和玩儿游戏(如Doom或Quake)。你可以对其进行日志记录，阻塞流量或主动地制止。例如，你可以和用程序实施反击或设置“ dummy ”系统或网络进行诱导。

网络误用是物理的，操作系统的或远程攻击的结果。物理攻击包括偷取硬椭或物理操纵机器来获取信息。操作系统攻击指经过验证的用户试图获得root的访问权限。远程攻击指攻击者通过网络来攻击设备。

执行动作Action

在大多数的IDS程序中，你可以为规则赋予动作。在你定义规则时，通常必须考虑将规则实施到网络上的时机和方式。一项规则的其它元素包括：

- 需要保护的主机。你可以指定某台主机或某一范围内的主机。
- 需要做日志记录的和禁止的主机。你可以指定某台主机或某一范围内的主机。
- 实施策略的时间段
- 事件的描述
- 对发生的事件如何反应，包括：

》 重新配置防火墙
》 阻塞特定的TCP连接
》 日志记录机制
》 邮件：，传真，电话提示
》 启动其它程序来阻止攻击
》 SNMP陷阱

IDS程序要求你先建立规则，进而赋予动作。你可以自己定义规则。然而，大多数的IDS

厂商已经设想了许多场景。这并不意味着你不需要建立自己的规则或编辑已经存在的规则来确保它们符合你的需求。

误报

如同实施防火墙，IDS也需要仔细地设置。否则，你将收到并不实际存在的攻击和问题 的报告。误报“ falsepositive ”就是指这种不准确的报告。

然而，完全忽略误报是不明智的。IDS程序有时候会检测到一些非法的网络活动，即使 并没有对这些活动定义规则。例如，许多IDS系统会报告说存在过多的与NetBus和某些 UNIX的rootkit相关的SYN连接。虽然你需要对误报引起重视，但你还必须培养识别何时 忽略误报何时认真对待它们的能力。网络级的IDS更容易发生误报情况，尤其在它们被配 置成检测对某些主机的攻击时，例如NetBus，密码攻击等等。

入侵监测系统软件

突出的1DS厂商包括Axent，ISS和Platinum Technology。在你选择产品时，请充分考虑哪一款产品更适合你的公司。有些产工具有优秀的图形界面，很容易使用。其它产品可能工具有扩展性。下列是部分厂商列表：

- Axent Intruder Alert(http：／／www,axent．com／)
- Cisco NetRanger(http：／／www,cisco．com／)
- ISS RealSecure(http：／／www．iss．net／)
- Computer Associates ’eTrustIntrusionDetection(formerlySessionWall 3)
- Computer Misuse Detection System(．http：／／www．cmds．net／)
- Network FlightR ecorder(．http：／／www,nfr．com)
- Network Associates ’CyberCop Monitor(http：／／www,networkassociates．com．)

Intruder A1ert

IntruderAlen(ITA)是使用管理者／lq理结构的功能强大的产品。管理者和代理可以运行于UNIX，NT和Novell网络中。ITA的第一个优点是它可以在许多网络环境中应用。由于公司很少只应用单一厂商的产品，所以你选择的IDS应该可以适用于尽可能多的厂商的产品。

ITA的第二个优点是其分布式的管理结构。ITA软件包由两个服务和三个应用程序组成：

- ITA　Manager(充当服务，守护进程或Novell的可装载的模块)
- ITA　Agent(充当服务，守护进程或Novell的可装载的模块)
- ITA　Admin(用来配置代理的应用程序)
- ITA　Vlew(用于查询代理的程序)
- ITA　Setup(从管理者域中添加和删除代理的程序)

在本部分，你将体验这种分布式的结构如何提供容错和可扩展性。

ITA的构成元素

IntruderAIert的管理者和代理都以Windows服务，UNIX守护进程或Novell可装载模块的形式运行。因为它们由ITAAdmin或ITAView来控制，所以本身并没有内置图形或命令行接口。

所有的管理者和代理都有特别的名字，你使用这些名字来连接管理者。然后管理者允许你管理代理。像先前所说的，管理者和代理之间的连接使用400位的公钥加密。IntruderAIen将代理置于成为“ 域 ”的逻辑组中。你可以根据操作系统种类、服务器种类或系统功能建立

自己的域。你还可以为一个管理者添加多个代理。ITA的域不同于DNS或WindowsNT域。

ITAAdmin和ITAView

只有通过ITAAdmin和1TA View才能够操纵管理者和代理。ITAAdmin允许你来配置IDS结构。而且，你可以使用ITAAdmin来管理多个管理者和代理。在连接成功后，你可以为特定的代理建立或编辑安全策略。只有与管理者连接好，你才可以配置代理。连接好管理者后，你可以在任何注册过的代理上管理策略。

ITA View是你获得由代理捕获和发送的信息的工具。一旦你在ITA Admin中建立了策略，你便可以使用ITAView来查找网络上发生的任何问题。

支持ITAAdmin和ITAView的平台

你可以在一些操作平台上安装ITA．Admin和ITAView，包括Solaris，Novell，NT和各种UNIX操作系统。这样，你可以在分布式的环境中应用管理者和代理。

ITA代理的安装

ITA的Setup程序只能自安装了代理和管理者的系统上运行。使用此程序，你可以停止和启动本地的管理者和代理。你可以用它来向远程的管理者注册本地代理或从远程管理者数据库中清除本地代理。

你可以改变上图所示的结构。例如，你可以为ITA的管理者主机增加或删除代理，或者将代理注册到其它的管理者。你还可以根据需要将代理配置成可以同多个管理者通信。当前，ITA还不支持管理者之间的通信。

将代理组织成域的形式可以减轻你的管理负担。例如，你可以根据所在的操作系统类型来组织代理，还可以根据地理，商业目的和安全优先等等来组织代理。无论你如何将代理分类，你都应当仔细的进行计划并记录下来。作为审计人员，如果你的客户公司存在规划和记录得不够好的结构，你应当采取补救的措施。

连接到管理者

在操作代理之前，你必须连接注册过的管理者。当第一次启动ITAAdmin时，你没有可供选择的管理者。要为ITAAdmin配置管理者，选中并右键点击管理者图标。然后输入管理者名字，用户名和密码。ITAAdmin将在下次启动程序时记住该管理者的名字。在连接管理者后，你可以管理任何在该管理者注册的代理。为了管理代理，点击管理者的名称，然后查看应用的策略，你可以建立，编辑和应用监测入侵行为和实施反应的策略。

ITA连通性

现在，ITA只允许你连接使用FQDN命名的设备(通过NetBios或DNS服务)。在TCP／IP网络中，ITA通过TCP通信。缺省的管理端口是5051。缺省的代理端口是5052。你可以更改这些缺省端口。在IPX／SPX网络中，SPX是最常被使用的协议。

你可以通过网络使用ITAAdmin和ITAView连接任何代理。由于ITA使用名称解析而不是IP地妇L，所以你需要一些名称解析的方案，你不能仅仅使用IP地力L正如你所猜测的，使用DNS系统解析IP地址是不够的，你还必须保证能够进行反向DNS解析。

没有运行DNS，NetBIOS(例如WINS)解决方案的WindowsNT操作系统也可以工作。如果你的TCP／IP网络不支持DNS或NetBIOS命名，则必须使用HOSTS或LMHOSTS文件：。ITA支持IPX／SPX，你可以将用于连接的文本文件：包含进来。

如果在代理寻找管理者时存在问题，你应当确定该服务是否正在运行。你还需要实施端

口扫描来确定它们是否在网络中声明白身的存在。如果你运行了DNS但不具备反向解析的功能，则管理者和代理并不能识别对方，即使它们工作在同一操作系统中。

ITA和防火墙

防火墙会产生其它的连接问题。如果你试图连接处于防火墙保护下的代理，通常会因为防火墙只允许某些流量通过而失败。为了解决上述问题，请为该连接定义防火墙规则。

定义策略和建立规则

一旦你定义了策略，便可以开始使用它。你可以观看在PolicyLibrarytree · 厂的策略。然而，这个列表只是提供了潜在的策略。如果你希望更改工作中的代理，则点击活动的管理者图标然后是从PolicyLibrarytree起源的策略。

ITA View分三次列出一些或全部的策略。不要对这种重复感到迷惑：程序列出了活动的策略和任何你可能使用策略，还列出至少两个域的策略：缺省的所有代理和缺省的NT。第三个tree列出了你可能增添到缺省域中的策略。当然，你可以重命名这些缺省的域，也可以增加新的域。第四个tree列出了事先定义好的策略，你可以剪切并粘贴到策略库中，并激活它们。在观看ActivePoliciestree时你无法看到特殊的规则短语和条款。你可以在Policies tree的管理者名称(如Studentl0)下看到这些信息。

规则的建立

同eTrustIntrusionDetection一样，ITA的规则也包含一些子元素。这些对确定ITA监测哪些网络和主机以及采取哪些行为有所帮助。所有ITA的策略都包含三个部分：选择、忽略和动作。

如果你希望确定一种特别的活动，例如NetBus连接或Land攻击，则Select元素来定义。ITA针对你定义好的规则来实施特殊的行为。一旦你使用一个Select段并定义了事件：，ITA就知道这个事件：了。

然而，ITA并不知道针对这个事件采取什么行动。Ignore段就是用来满足这个需要的。ITA将忽略任何你放在Ignore段中的条款，即使你已经定义过了。在Action段中的条款将决定ITA对你所定义的事件采取什么行为。如果你把相同的事件：同时置于Ignore和Actionm中的话，ITA不会对该事件：采取行动。通常，Ignore段被用来处理误报。ITA规则使用Boolean逻辑。如果Select段被激活或为真，ITA将杳看任何的Ignore和Action段。例如，在Action段中规定ITA将事件：记录到日志文件中，而且Ignore段中没有覆盖这条逻辑的话，ITA将采用在Action段中定义的规则。

对规则排序 ·

你可以决定每条规则的重要性顺序。每条规则可工具有0到100的值。0到33的值表示这条规则是个警告，34到66表示为中等程度的安全问题，而67到100表示已经发生了严重的安全问题。ITA并不会自己将这些新的规则进行排序，你需要投入事件正确地对它们排列优先级顺序。

Indirect，Filter和Disable三个复选框对定义规则来说并不是必须的。这些只是ITA在应用规则时进行附加控制的。Indirect选项只允许当其它ITA规则引用时才运行，Filter选项将被其它规则检测到的事件删除掉，Disable在ITA检测时删除掉整个的规则。

进行查询

你可以使用ITA View进行查询。从ITA View的主界面，单击New按钮你可以定义并进行

查询。DefineNewFilter对话框允许你连接管理者，然后直接从管理者向代理进行查询。从这里，你可以存储或装入事先定义好的能够帮助你快速了解某台主机安全状况的查洵(例如filters)由于这个程序独立于ITAAdmin运行，你必须重新登录管理者。这项要求加强了安全性，而且保证了一个程序的崩溃并不会影响到管理和查询代理。

在连接好代理后，你可以开始进行查询。你的查询受限于你在ITA View中建立和激活的规则。你还可以根据优先级来进行查询。或者使用查询文本框，或者从管理者对象窗口向查询列表窗口拖拽查询项，然后选择Go。在查询对话框中的内容将覆盖在查询列表窗口的输入内容。

购买IDS注意事项

在选择产品时，请注意下列问题，见表

要点	问题
产品支持	谁你们公司所在区域的联系人?他们什么时候工作?什么是你的申报策略?他们什么时候可以进行支持?支持的花费是多少?有没有免费支持号码?
产品培训	提供什么形式的培训?培训包括在产品中吗?花费有多少?
升级策略	管理者和代理升级的频率有多快?升级需要花费吗?第一年的升级是免费的吗?如何通知进行升级?有没有对升级的建议过程?
公司声誉	有哪些公司使用你们的产品?能否让我同使用过你们公司产品的系统管理员接触来了解情况?
IDS 功能	在 IDS 饱和前能处理的流量?如何通知我这些问题?
产品的可扩展性	策略能够制定到什么复杂程度?该 IDS 可以处理多少种攻击特征和策略?策略能够细致到什么程度?我可以自己制定策略吗?产品研发的时间有多长?
网络支持	哪种网络系统该 IDS 系统支持得最好?在 UNIX,Novell 和 NT 中各有什么缺点?你的产品缺省情况下能检查出什么 sendmaii 漏洞?可以支持那种工作系统或设备(如路由器)。
加密	管理者和代理是否使用公钥加密?使用哪种公钥?

有些IDS厂商不希望泄漏他们的产品的细节。然而，你要弄清楚是该公司不愿意泄漏这些重要信息，还是根本就没搞懂这些产品。

建立基线是你在审计过程中应当采取的第一步。在建立基线时，先在网络活动的峰值期间运行IDS一段很短的时间。下面的连续将告诉你更多的关于整个网络活动的情况。掌握这些信息是唯一能够确定你所运行的网络是否“正常”的标准。确定在员工工作期间发生了哪种类型的活动。这些情况有助于你捕获那些有工业间谍或其它安全伤害的雇员行为。另外可以在晚间运行IDS，因为这是攻击者从外界进行攻击的最常见时段。

本章小结：

在本课中，我们学习了什么是入侵监测系统。你还使用了ComputerAssociate的eTrustIntrusionDetection和AxentIntruderAlert。你使用了网络级和主机级的扫描器来了解IDS结构。你了解了管理者和代理的用途和如何设置它们。你还了解到在购买IDS产品时要考虑那些问题，以及用IDS进行审计时要注意的基本问题。例如，你了解到应当检查IDS文档的情况和实施的是否正确。最后，你了解了如何检查非法服务。

第六章

审 计 和 日 志 分 析

引　　言

在审计过程中，你需要投入大量的时间分析日志文件。在本课中，你将学习对利用一些工具对重要资源进行审计。也许分析日志文件：是安全审计中至关重要而工具有挑战性的方面。区分合法用户和非法用户十分困难。不论你进了多大的努力以保障网络的安全，你必须假设黑客会在某些时刻入侵系统。你需要能够确定何时产生缺陷以及如何产生缺陷的值得信赖的方法。日志分析为你提供了这两种服务。

日志记录的分寸不易把握。如果记录得太多，则有用信息不易查找。如果记录得太少，则不能收集足够的信息。实际上你也许会得出相反的结论，例如由于网络负载的增加而导致系统的运行效率有所下降。

本章要点

- 为用户的活动建立基线
- 进行日志分析
- 过滤NT和Unux工作系统的事件日志
- 审计用户登录，系统重启和一些特殊资源的使用

基线的建立

建立基线是进行日志分析的开始。基线是网络活动的参考标准。通过一段长时间(通常一个月或更多)对日志的仔细分析，你可以建立一条基线。在建立基线的过程中，应根据用户的活动倾向对日志进行检查。从广泛地观察入手，分析网络活动的大致倾向，尤其注意极轻和极重的网络活动时期。大多数公司网络活动最频繁的时间段出现在清晨上班，午饭期间和·下班时期。然而活动图样会有所不同。

防火墙和路由器日志

在分析防火墙和路由器日志时，集中完成下列任务：

- 识别源和目的接口
- 找到源主机和目的主机
- 跟踪使用迹象：在每个接口上观察能够显示从外部进行过扫描的迹象。这种迹象表明有人在试图勾勒网络的拓扑结构。
- 协议的使用：搜寻与Internet直接相关的应用，包括HTTP流量，RealPlayer，MP3流量，ICQ，InstantMessenger,和IRC流量。此外，还要搜寻ICMP，TCP和UDP连接。
- 搜索可疑端口的连接：例如12345(NetBus缺省端口)和31337端口(BackOrifice2000的缺省端口。

操作系统日志

一旦你在通过熟悉网络活动的基础上建立好基线后，便可疑更细致地分析它了。建立基线的最终目的是为比较和衡量未来的网络活动建好标准。落在在这个标准之外的活动都应受到仔细的检查。

记录UNIX系统日志

Syslogd是记录Linux和UNIX系统日志的服务。你可以通过编辑／etc／syslog．conf文件配置该服务。在UNIX工作系统中有好几个本地工具用来帮助你对已经发生过的活动进行分析，这些：工具包括：

- last：扫描／var／!og／lastlog文件并报告各种信息，包括用户登录、注销和远程位置，系统关闭和重启，还有处理登录的服务信息(如Telnet,FTP等等)
- lastb：提供尝试登录失败的信息
- lastlog：提供关于所有用户最后一次登录的信息，还有哪些用户从未登录。

还有一些常见的日志如下：

access-log	纪录HTTP／web的传输
acet／pacct	纪录用户命令
aculog	纪录MODEM的活动
btmp	纪录失败的纪录
lastlog	纪录最近／L次成功登录的事件和最后一次不成功的登录
messages	从syslog中记录信息(有的链接到syslog文件：)
sudolog	纪录使用sudo发出的命令
sulog	纪录使用su命令的使用
syslog	从syslog中记录信息(通常链接到messages文件：)
utmp	纪录当前登录的每个用户
wtmp	一个用户每次登录进入和退出时间的永久纪录
xferlog	纪录FTP会话

记录NT系统日志

事件察看器是WindowsNT本地日志记录的工具。你可以用它来控制事件日志服务。通过开始—程序-一管理工具-—事件：察看器的途径可以启动事件察看器。

WindowsNT将日志记录分为三个类别：

- 系统日志：记录服务的启动和失败，系统关闭和重启。
- 安全日志：记录用户登录，用户权限的使用和变更，对象的访问。
- 程序日志：记录与工作系统有关的程序的运行的情况。

在NT中开启审计功能

在WindowsNT中你需要分别设置审核功能来捕捉事件。在域用户管理器中设置系统和域级别的规则。进入域用户管理器中，选择规则审核，再选取你想审核的事件。如果你要审核目录和文件级别的事件，首先需要在域用户管理器中开启相应的审核功能，然后通过Windows资源管乐器激活相应的你想审核的资源。

虽然系统间的事件检查有所不同，但你至少需要检查表6-1中列举的事件。这些事件：从ServicePack4后有效。· 下表列出了一些WindowsNT中的重要事件。

事例号	描述
529	登录失败(在安全日志中)
6005	WindowsNT 重新启动(在系统日志中)
6006	正常关机(在系统日志中)
6007	因权限不够而不正常的关柳，请求(在系统日志中)
6008	称为“不正常关机”事件：，当 NT 被不正常关机时，该信息被记录下来。注意：有些工具(包括 sysprep. exe 和 shutdown. exe)会使 NT 记录这些信息。应仔细研究这些信息。
6009	记录工作系统的版本号，修建号，补丁号和系统处理器的信息。(在系统日志中)

在这一部分中讨论的事件：不是错误信息。不要混淆系统事件和错误信息。WindowsNT错误信息代码在下列URL地址有相关的列表：
http://msdn.microsoft.com/library/psdk/psdkref/errlist_9usz.htm

确定WindowsNT的补丁等级

你可以从事倒：察看器中找到系统的补丁等级。用winver工具更方便。你可以在开始运行中使用该工具，键入命令winver。

在WindowsNT中确定系统启动时间

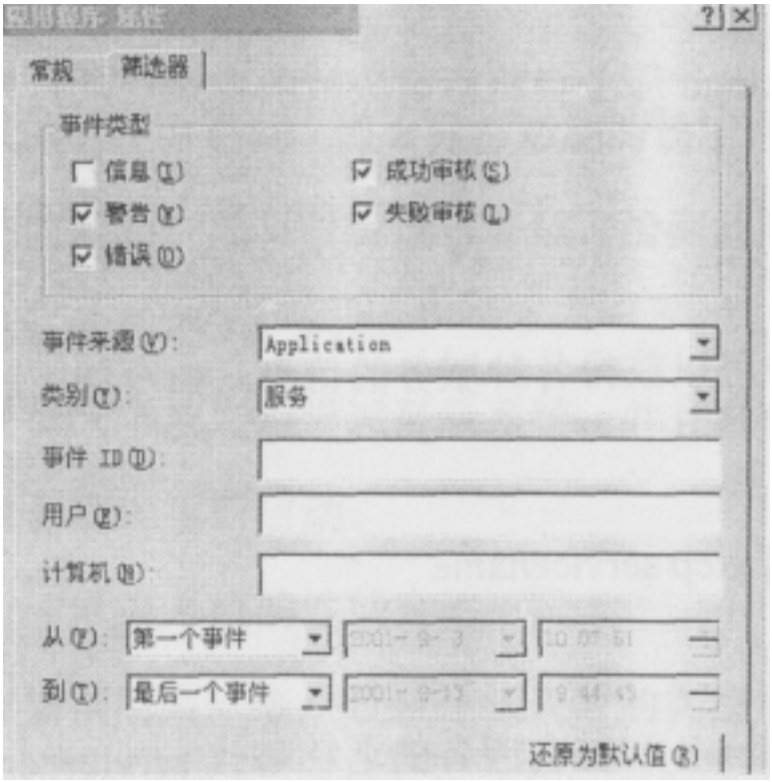
系统的关机和重启通常为黑客所为。你需要快速确定系统启动了多长时间。虽然你可以从事件：察看器中找到该事件，当然还可以使用uptime．exe：工具，该工具可从下列URL地址获得：http：／／www,microsofi．com／TechNet／winnt／Winntas／tools／uptime．asp

日志过滤

日志记录文件会变得很大。你必须知道如何有效地审查这些信息。下面将讨论如何对NT、Linux和第三方软件的日志进行审计。

在WindowsNT中过滤日志

如同任何高性能的工作系统，NT允许你对事件日志进行过滤， 日志过滤的功能十分强大。以为只显示符合过滤条件的事件，所以使用时要十分谨慎，否则在你设置范围之外的非法活动不会显示出来。这是各种安全工具(包括防火墙和入侵监测系统)的通病。
如下图所示：



在Linux中过滤日志

使用不带参数的·last和lastlog命令会提供太多的信息。 下面是定制信息的一些方法：

- last-X：只显示与系统关闭和重启有关的事件：:
- last -x reboot：显示所以系统重启事件；
- last -x shutdown：显示所以系统关闭事件；
- last -a：将所有主机信息列在最后一列；
- last -d：显示所有远程登录信息；
- last -n：允许你定义用last命令显示多少行信息。例如，last—n 2显示最后的两条信息。

你可以合并命令。例如，last -ad将显示远程登录的IP和主机明，如果可能还会将IP转换为DNS名。你可以将last命令与lgrep结合起来缩小查找范围。例如，last –x 丨grep丨Wed丨grep ftp将只显示发生在星期二的有关FTP的事件：。

Lastlog

Lastlog命令会读取／var／lo砂Iastlog文件。Lastlog命令有一些参数，下列是最常用的情形：

- Lastlog –t number_of_days：显示指定天数内的记录。例如，lastlog –t 2将列出最近两天内的登录情况。
- Lastlog –u login-name：显示指定用户的最后一次登录记录。

使用Lastb命令

lastb命令会读取／var／Log／btmp文件。通常此文件并不存在，但可以使用下列命令创建它：

host#touch／var／log／btmp

一旦你创建了该文件，syslogd服务会将所有失败的登录信息写入该文件：。Lastb和last命令的参数相同。

其它命令和文件

从／var／log／messages文件：中可以获得各种服务的信息，命令如·下所示：

host#cat／var／log／messageslgrepservicename

你可以用Telnet,FTP，sendmail和其它服务的名称替代servicename。还可以用head命令察看messages文件中前十条记录，或使用tail命令察看后十条记录。你还可以察看／var／log／secure文件：。下列命令列出telnet连接记录：

host#cat／var／log／securelgreptelnet

你可以用其它关键词替换telnet，如FTP,除root外的用户名，rlogin和finger。

最后，你可以使用uptime命令察看Linux工作系统启动的时间。

[test@studentl james]#uptime

5：40pmup4days，22：59，2 users，loadaverage：0．00,0．00,0．00

[tests@studentl james]#

操作系统附件和第三方日志记录工具

你不应该只依赖系统本身的日志记录工具，还可以使用象EnterpriseReportingServer和WebTrends for Firewalls and VPNs这样的工作系统附件。要获得更多信息，你可以访问www．webtrends．com，你会得到许多技术细节。

像Evinci．com(www．evinci．com)等公司开发的“ SWATteams ”可以监视和记录任何入侵、拒绝服务攻击等可疑的活动。第三方日志记录工具的有点是黑客很难篡改日志记录文件：，而且对事件的反应速度很快。缺点是需要额外费用和人员培训。

可疑的活动

一旦你能够确定系统的正常活动，那么异常活动的识别也就容易了。高明的黑客会试图把他的活动伪装成合法的活动。如果没有建立基线，检测危险的活动是很困难的。

“ 可疑的活动 ”有很多种形式：例如：

- 一个用户两周以来每天半夜二点尝试登录系统，并且没有登录成功。
- 主服务器每天早晨自动地重新启动。
- 在一天中的特定时间段内系统的性能突然＇下降。

第一种情况是黑客尝试用某一账户登录系统失败的典刑示例，在攻击的初始阶段，黑客出于谨慎的原因不想引起账号锁定。由于是发生在异常的时段工具有重复的特性，你应该

对内部进行认真的核查。

往第二种情形中，服务器在异常时段内的重新启动应引起重视。许多只安装后需要操作系统(如WindowsNT)重新启动才能使用。通常，高明的黑客会等待工作系统合法的重启，但有时他们会因为缺乏耐心而直接使用工作系统命令或拒绝服务攻击使目标服务器重新启动，从而开始使用黑客工具。

第三种情形可以由许多种原因造成。轻度的系统性能一下降通常不会引起报警。但是，这也可能是由于黑客在大规模攻击前的准备工作所引起的或是拒绝服务攻击的前期。投入时间为你的系统建立基线非常必要,因为你可以对照基线的情况来决定是否采取调查行动。

可疑活动的例子丰富多样。在调查取证时，应特别核查＇下列迹象：

- 异常时段内的合法活动或任何不在基线范围内的用户举动。
- 任何失败。尤其是登录失败，文件访问失败和用户权限使用失败。
- 任何主要的系统活动，如关机和重启。这种情形包括物理系统和软件系统如服务和进程。
- 磁盘空间的快速丢失和塞满。

最后强调，任何在基线之外的活动都是可疑的。虽然这些工作初始看来使大生畏，但久而久之会变得简单。

其它类型日志

路由器、防火墙和工作系统并不是唯一需要做日志记录的系统。其它需工作日志记录的系统如下：·

- 入侵监测系统
- 拨号连接
- ISDN和flamerelay连接
- 雇员访问日志

日志存储

你已经知道黑客如何定位审计日志工作为一名审计人员，你需要确保日志记录的安全性。建议如下：

- 将日志文件存储在不同机器上。
- 将日志文件复制到可擦写的CD-ROM上
- 定时备份日志文件

有些公司将日志直接打印下来，这种方式可工作为复制到可擦写的CD-ROM上的补充，因为电子形式的日志比打印下来的文本更便于搜索。

审计和系统性能下降

对系统的审核需要更多的系统资源，此外还会加重网络流量。如果你使用慢速连接的网络，应用象Axent'sEnterpriseSecurityManage和其它一些软件会引起网络性能急剧地下降。

虽然SNMP被设计用来减小网络管理的流量，但请注意用来监视SNMP的软件：(包括HP的OpenView)会影响服务器的性能。包捕获程序(如tcpdump，Sniffer Basic等)同样会显著地影响运行它们的系统的性能。

本章小结：

在本课中，你学习了在实施安全审计过程中分析防火墙、路由器、工作系统和入侵检测系统日志文件的重要性。你还学习了如何为你的系统的正常活动建立基线，如何识别日志

记录中的可疑活动。你还练习使用了一些自动执行的扫描工具(包括入侵检测系统扫描稚序和防火墙)来建立安全基线。

第七章
审 计 结 果

本章要点：

- 对特定的网络问题提供解决方案
- 建立评估报告工具有前瞻性的检测服务
- 精简工作系统
- 安装工作系统附件：，如个人防火墙
- 实施本地安全审计
- 用SSH替代Telnet，rlogin和rsh

建议审计执行过程

我们已经学习使用了一些实施有效安全审计的工具。现在还剩’下最后一步：提交细致的书面建议。建议应从三个角度来提出：

- 为了能够确定安全策略和实施情况的差距，建议采用特定方法继续进行有效的审计。
- 抵御和清除病毒，蠕虫和木马，修补系统漏洞。
- 建议改善和增强如下内容：

》 重新配置路由器
》 添加和重新配置防火墙规则
》 升级工作系统补丁类型
》 升级旧有的和不安全的服务和TCP／IP堆栈
》 加强网络审核
》 自动实施和集中管理网络内部和边界安全
》 增加入侵检测产品
》 增强物理安全
》 加强反病毒扫描
》 加强用户级别的加密
》 删除不必要的用户账户，程序和服务

下表列出了对上图中每一个类别的改善建议

分类	改善
防火墙	● 保证包过滤和防火墙规则的正确设置和有效 ● 扫描 DMZ 区域内的有问题的主机

入侵监测	● 升级入侵监测系统规则 ’ ● 识别需要监测的新内容
主机和个大安全	● 实施用户级别的加密 ● 在单个客户端上安装“个人防火墙”来锁定端口和减小风险
强制实施策略	● 安装监视软件，如 Axent 的企业级安全管理器 ● 对物理安全进行有规律的审计

建立审计报告

在本书的附录中A提供了一份审计报告样例，你的报告自然应该与它不同，但这份样例对报告的格式及结构提出了建议。文档中将报告问题和提出建议。

在安全审计报告中应包含以下元素：

- 总体评价现在的安全等级：你应该给出低、中或高的结论，包括你监视的网络设备的简要评价(例如，大型机，路由器，NT系统，UNIX系统等等)
- 对偶然的、有经验的和专家级的黑客入侵系统做出时间上的估计。
- 简要总结出你的最重要的建议。
- 详细列举你在审计过程中的步骤：此时可以提及一些在侦查、渗透和控制阶段你发现的有趣问题。
- 对各种网络元素提出建议，包括路由器，端口，服务，登录账户，物理安全等等。
- 讨论物理安全：许多网络对重要设备的摆放都不注意。例如，有的公司把文件服务器置于接待台的桌子后，一旦接待人员离开，则服务器便暴露在网络攻击之下。有一次，安全审计人员抱着机器离开，安全守卫还帮了忙。
- 安全审计领域内使用的术语。

最后，记着递交你的审计报告。因为安全审计涉及了商业和技术行为，所以应该把你的报告递交给两方面的负责人。如果你采用电子邮件的方式递交报告，最好对报告进行数字签名和加密。

增强一致性

你不仅需要指出问题所在，还要排除问题。· 下面列工作为审计大员你应提出哪些建议。这些步骤总结了你在本课程中学到的安全规则。

持续审计和加强安全的步骤

下列是你对所有希望继续进行有效审计的公司建议采取的步骤。

》 定义安全策略。

》 建立对特定任务负责的内部组织。

》 对网络资源进行分类。

》 为雇员建立安全指导。

》 确保个大和网络系统的物理安全。

》 保障网络主机的服务和工作系统安全。

》 加强访问控制机制。
》 建立和维护系统。
》 确保网络满足商业目标。
》 保持安全策略的一致性。
》 重复的过程。

以上都是保证安全的基本步骤。许多国际性的公司要求符合这些需求。无论你提出了哪些方面的建议，你至少应该遵循某一种国际性的安全标准。

安全审计和安全标准

至少有三个国际安全标准可以供你在书写报告时进行参考。每种标准都可以帮助你使用正确的语言进行表达，更重要的是使你关注客户的商业需求。许多网络工作者认为这些标准没有必要，在处理更多的实际问题时很难将这些抽象的概念铭记在心。最后，将概念转变为实践是困难的。

然而，因为许多公司要求遵循这些标准，所以它们也变得越来越重要。例如，许多政府在同公司进行商业工作时要求符合BS7799标准。

IS0 7498—2

国际标准组织(ISO)建立了7498系列标准来帮助网络实施标准化。其中第二个文件7498-2描述了如何确保站点安全和实施有效的审计计划。文件的标题是《Information Processing Systems,Open System Interconnection,Basic Reference Model,Part 2：security Architecture》，它是第一篇论述如何系统地达到网络安全的文章。你可以从www．iso．ch．获得更多的ISO标准的信息。

英国标准7799(BS 7799)

BS 7799文档的标题是《A code Of Practice For lnformation Security Management》，论述了如何确保网络系统安全。1999年的版本有两个部分。BS 7799-1讨论了确保网络安全所采取的步骤。BS 7799-2讨论了在实施信息安全管理系统(1SMS)时应采取的步骤。虽然BS 7799是英国的标准，但由于它可以帮助网络专家设计实施计划并提交结果，所以很多非英国的公司也接受这一标准。BS 7799系列与ISO 9000系列的文档有关。这些标准保证了公司之间安全的工作。

实施信息安全管理系统(ISMS)的目的是确保公司使用的信息尽可能的安全。因此，需要考虑能够帮助在你的公司中建立、管理和传送信息的每个要素。这些要素包括电话联系，文件：系统(文本和电子格式)，网络传输等。所以，定义ISMS的任务变得很艰巨，你需要记录和分类建立信息的任何组成部分，包括铅笔、邮票、邮件等等。所幸的是，你可以定义一个范围，它可以使你只关注哪些对你的网络影响最大的内容。

在完善ISMS是，应遵循以下步骤：

》 定义安全策略。 .
》 为你的信息安全管理系统(ISMS)定义范围。
》 风险评估。
》 对已知的风险进行排序和管理。

你已经在本课中学习了每个步骤，当然，你需要将学到的技能与BS 7799和IS07498-2标准结合起来。这些标准会使工作为一名审计大员工具有可信度。

在BS 7799和ISO 7498-2文档中讨论的许多步骤可以帮助你实施在前面提到的目标。这些标准建议你采取如—下步骤：

》 发布安全策略。
》 公布负责大名单。
》 培训公司大员的信息安全意识。
》 定义汇报事件：的程序。
》 建立有效的反病毒保护措施。
》 确保实施的策略与公司商业目标的一致性。
》 制定规范以确保雇员不会为了完成任务而破坏软件许可规则。
》 物理上确保对网络工作记录的安全。
》 建立系统来保护公司数据的安全。
》 实施能够衡量规定的安全策略与实际遵守情况的等级的机制和过程。

Common Criteria(CC)

Common Criteria提供了有助于你选择和发展网络安全解决方案的全球统一标准。ISO为了统一区域和国家间的安全标准指定了CommonCriteria，因此，CC与IS09000系列相似都是用来提供可以证明的过程。虽然CC的目的是统一ITSEC和TCSEC，但它们还是用来取代“ OrangeBook ”标准。在编写本：日时，CommonCriteria被称为ISO国际标准15408(IS 15408)。Common Criteria2．1等同于IS l5408。

该文件由三个部分组成：

- 第一部分：定义了如何创建安全目标和需求，还提供了一个术语的概述。
- 第二部分：定义了如何建立能够使商业通信更安全的需求列表。列举了如何将这些需求组织成classes(抽象的需求，例如验证和加密)，families · (更特别的需求，例如用户和过程验证)，和components(使用Kerberos进行验证，和一次性口令)。
- 第三部分：提出了如何建立能够达到公司安全需求的“ 保险内容 ”的过程。还讨论了七个日益广泛使用的严格的Evaluation Assurance Levels(EAL)。

这三部分的内容描述得很细致和复杂。然而工作为审计大员你只需要理解这些条款的基本内容。许多IT专家使用它们来：

》 第一公司需要的特殊殴置。
》 提供了审计大员和IT专家在商!眶和技术交流中常用的术语。
》 定义了为更新网络或特殊产品而建立特殊过程的需求。 .
》 需要由软件和硬件厂商声明的证明能力。

下表描述了与安全审计大员有关的概念和术语。

术语	描述
Protection Profile(PP)	需要的网络服务和元素的详细列表，报括安全目标。
Security objectives	列出如何提出特别的弱点的书面叙述。这是一种总体的陈述。安全需求比目标陈述更具体。
Security Target(ST)	由生产厂商提供的描述安全工具的用处的一组声明。与安全目标和安全需求不同。安全需求是由厂商实施在软硬件上的，而安全目标只是由 IT 部门和网络审计人员定义的目标。

Target Of Evaluation(TOE)	你将要审计的某个工作系统，网络，分布式的程序或软件：。使用安全目标和安全对象，你可以确定系统是否满足了目标以及对象是否达到了声明的功能。
Packages	任何允许 IT 专家达到安全目标和要求的可以重复使用的内容。例如七个 EAL。你可以合并这些 Package 来确保额外的安全。
Evaluation Assurance Level (EAL)	七个事先定义好的 packages,用来帮助 IT 专家评价规划的和已经存在的网络和系统。

EvaluationAssuranceLevel

Evaluation assurance levels(EAL)提供了描述和预测特别的工作系统和网络的安全行为的通用的方法。等级数越高，则要求得越严格。EAL 1需要由TOE厂商做出声明的证明，EAL 7需要你核实和记录下实施过程的每一个步骤。你应该注意到当EAL的等级升高时，两项要求也会变得更严格。

- 设计的证明：EAL 1只要求检查产品的文件，而EAL 7要求对系统进行完全的记录完整的独立的分析。
- 抵御攻击的能力：EAL 1需要产品至少声明能够提供对攻击的有效防范；而EAL 7需要工作系统能够抵御复杂的破坏数据机密性和拒绝服务式的攻击。

EAL 类别	描述
EAL 1	功能上的测试：分析产品的声明，和实施 TOE 的基本测试。 ·
EAL 2	结构上的测试：需要选择 TOE 的重要元素来经受具有权威资格的测试，例如程序开发者。
EAL3	系统的测试和检查：进行测试的要求非常严格，在有限的基础上，操作系统的所有元素都必须独立地检验。
EAL4	系统地设计，测试和回顾：这一级别的保证是允许已经完成的程序和以前实施的系统进行更改的最高保证。这一级别还需要操作系统通过抵御低级别的攻击的测试。
EAL5	半正式的设计和测试：操作系统必须可以经受适度的，比较复杂的攻击。

EAL6	半正式地验证设计和测试：与 EAL5 相同，但是需要第三方的 TOE 设计核 实。
EAL7	操作系统必须经完整地回顾和被证明能够抵御灵活的攻击。正式地设计和测试：确保发展的过程有组织，由第三方记录所有的过程。例如，所有通信都必须被记录下来。

你可以从，http：／／csrc．nist．gov／c／index．html．了解CommonCriteria

增强路由器安全

简单地增强路由器安全的方法包括：

- 严格控制路由器的物理访问。
- 获得最新的工作系统升级(包括NT系统做路由，和专门的路由器工作系统，例如Cisco IOS)
- 确保路由器不受拒绝服务攻击的影响。
- 确保路由器不成为拒绝服务攻击的不知情的帮凶。

下表提供了一些建议来确保第三、四项的要求

过程	描述
入口和出口过滤	配置你的路由器只路由那些具有合法的内部 IP 地址的数据包离开。你的路由器应当丢弃任何不具有合法的内部 IP 地址的包。这个设置有助于网络不成为发送虚假 IP 包的源头。
	然后，配置路由器丢弃所有源于表 7 月 5 日的 IP 地址包 ● 要获得更多的信息请查看 IntemetDraftierf-grip-isp-07(1SP 的安全展望)
禁止广播过滤	许多拒绝服务攻击，包括 Smuff 攻击，都是攻击者和用路由器在配置上允许直接广播的漏洞。最简单的确定路由器是否配置成回应这些地址的方法是 ping 该网络地址(例如 192．168．4．0)或该网络广播地址(例如 192．168．4．255)

在入口和出口过滤中应当考虑的IP地址

分类	地址

HistoricalLowEndBroadcast	0. 0. 0. 0／8
Limitedbroadcast	255. 255. 255. 255／32
RFCl918 私有网络	10. 0. 0. 0／8
RFCl918 私有网络	172. 16. 0. 0／12
RFCl918 私有网络	192. 168. 0. 0／16
本机回环地址	127. 0. 0. 0／8
连接本地网络	169. 254. 0. 0／16
D 类地址	224. 0. 0. 0／4
E 类保留地址	240. 0. 0. 0／5
未分配地址	248. 0. 0. 0／5

想获取更多的信息，访问下列网址http：／／www,sans．org／dosstep／index．hem

提前检测

提前检测是指你使用黑客的策略和手法来对付他们，而不是简单地停止攻击。一个有效的检测策略通常包括审计，但你必须同时使它能够简单地检测系统问题和自动提供解决方案。

扫描检测和jails

有些入侵监测程序，例如NetworkAssociates’Sting，允许你建立虚假账号甚至是虚假的网络来引起攻击者的兴趣。这种目标使攻击者把时间花费在不存在的资源上，另外提醒网络管理员网络中存在可疑的活动。

反击的系统通常包括建立一台服务工作为目标。它们可以包括下列内容：

- 混杂模式扫描
- 虚假的数据库
- 虚假的账号文件
- 虚假文件：
- 虚假的管理员账号
- 自动将攻击者引入虚假网络中的防火墙配置
- 报警或惩罚黑客行为的Tripwire账号
- 物理线路追踪(试图确定黑客使用的端口或电话线路)
- 数据包追踪(试图了解包的起源)

检测工作在混杂模式的网卡

你可以实施远程扫描来确定一块网卡是否]工作在混杂模式。象AntiSniff这样的程序使

用三种主要的方法来检测网卡是否工作于混杂模式：

》 检测网卡电子方面的变化来确定网卡的工作模式。

》 发送各种包(ARP请求，ICMP包，DNS请求，TCP SYN floods，等等)。如果从某台主机返回的包等待了一段不正常的时间，而且没有被主机处理过的迹象，则程序便推断出该主机的网卡可能出于混杂模式。

》 将错误的ICMP请求包含在无效的以太网地址头中。所有没有：工作在混杂模式的系统将忽略这些请求，而那些回复错误的ICMP请求的主机将有可能出于混杂模式。

像AntiSniff这样的程序通过推论来判断网卡是否』工作在混杂模式。由于这些程序只是根据有限的数据来下结论，所以容易出现误报。通常明智的做法是定时进行混杂模式检测的扫描。例如，LOpht包含其自身的调度。使用WindwosNTScheduler或UNIX的cron程序，你可以自动实施所有扫描。想获得更多的有关如何检测网卡的混杂模式的信息，请访问LOpht站点www．iOpht．com／antisniff／。L0pht还提供的UNIX版本的AntiSniff。然而你需要编泽它，

并且只能运行在FreeBSD和Solaris工作系统下。

主机审计解决方案

在审计主机时，你会发现由于每台主机都是针对不同的商业目的，所以你也需要提供不同的解决方案。你可以建议下列的审计方案。

- 实施本机审计：虽然你希望能补充象last和时间查看器这样的本机审计工具，，但本机审计程序通常是审计过程好的出发点。
- 安装监视软件，例如Axent'sEnterprise Security Manager(ESM)：这种软件通报中央控制系统那些系统低于规定策略的限度之下。例如，这种监视程序可以设置成提醒你哪些系统的密码有效期设置得过低。
- 清除安装工作中的临时文件 :自动安装程序通常在临时文件中留下重要的数据包括密码
- 修复和清理被损坏的系统 :你可以清除非法的服务像NetBus,TribalFlood和BackOrificeo
- 替代服务：例如，你可以用SSH服务来替代Telnet，SSH使用公钥加密来保证登录会话的安全。
- 安装工作系统附件，例如个人防火墙和加密服务。

清除“ 感染 ”

反病毒软件可以扫描出众所周知的非法服务，木马，病毒和蠕虫。然而，你应当能够排除至今还未检测到的问题。为了检测和清除感染，你可以：

- 使用TCP／IP排错的工具，例如ne~tat
- 使用Teinet连接怀疑的端口
- 升级和运行反病毒程序

个人防火墙软件

虽然称为个大防火墙，但这类软件提供了两个主要的功能。

- 端口阻塞
- 连接追踪

你还可以拒绝特定的IP地址。这些程序并不是真的防火墙。而且；大多数的个大防火墙软件并不适合做服务器的安全解决方案。

流行的软件

流行的防火墙软件包括：

- Networklce's Blacklce和Black，Ice Defender(www．networkice．com)
- McAffee'sConSeal(www.signal9.com)
- ZoneLabs ’ ZoneAlarm(www,zonelabs．com)

虽然大多数的个大防火墙产品是针对客户端系统的，但Networklce(．www．networkice．com)同样也适合对高性能的产品提供支持。它们是ICEcap和Blacklce。后者是主机级的入侵监测软件：的代表。

IPSec和加密

许多公司越来越重视内部的攻击。为了解决这种问题，你可以建议应用IPSec和个人加密。PGP程序是简单地应用IPSec来帮助建立有效的局域网和广域网级别的VPN解决方案的实例，从www．pgp．com上可以获得该软件：。

个人加密产品包括象BestCrypt这样的程序(www．bestcrypt．com)。这些软件有助于公司确保文件， 目录甚至是整个硬盘的保密性。这些工作系统的附件可以帮助确保数据的机密。

加密和安全策略的一致性

其实，有些公司不希望使用个人加密，因为不希望员工加密的文件：连管理者和IT人员也解不开。因此，如果你建议了这种解决方案，你需要准备建立Key escrow系统来统一管理加密和解密。

审计可以建立在多种级别上。例如，如果你在WindowsPrimaryDomainController(PDC)实施了审计，则该策略将应用于整个域。审计还可以发生在工作系统级别。例如，你可以象前面课程中所学的审计登录失败和系统关闭。最后，你可以在资源级别实施审计，这些资源包括文件和目录。

修补系统漏洞

审计人员的：工作就是发现系统漏洞并修补它们。工作系统的hotfixes和servicepacks是修补系统漏洞的主要手段。你可以升级TCP／IP堆栈，或者，甚至应用Ipv6。

NI中的TCP序列

知道ServicePack5出现之前，windowsNT使用的TCP序列机制是很容易被预测的。虽然序列号可以从随机的数值开始，但是随后接收的包会在序列上加一。攻击者通常会和用这种可以预测的序列数，因为这允许他们进行劫持攻击。虽然由SP5提供的序列机制也没有像Linux和UNIX工作系统中的复杂，但仍然建议安装最新的Service Pack 6a版本，

Ipv6

虽然Ipv6无法实施在每种场合，但它迅速成为一种选择。IPv6使用了加密和验证机制，现在主流的工作系统如WindowsNT，Linux 6．1和Solaris都支持IPv6。在本书工作的时候，选择IPv工作为唯一的协议会限制访问Internet，但是在某些情况下对隔离的局域网使刚IPv6会达到更高的安全效果。

IPv6提供了下列的安全特性：

- 加强的验证机制(通过验证扩展头)减小了被spoofing和叫acking攻击的可能性。
- 数据加密(通过EncryptedSecurityPayload扩展头)减小了被嗅探攻击的可能性。

想获得关于IPv6的更多信息，请访问http：／／www,ipv6．org。这个站点包含了最新的有关IPv6发展的信息，所有与协议相关的RFC文件，和所有支持IPv6的工作系统和程序。

升级和替代服务

通常你需要升级和替代已经存在的服务。在进行更改时，请考虑下列的步骤：

- 研究新的产品。问问自己它是否适合你的网络和商业情况。
- 确定需要多少时间来实施这些变化。
- 在把它们应用到产品之前彻底地进行测试。
- 要考虑到这些升级和替代会影响其它服务。大多数的网络主机之间是相互影响的。这些新的服务会引起这些问题吗?
- 确定是否需要对最终用户进行培训。

Secure Shell(SSH)

Telnet,rlogin和rsh非常有用。它们允许你远程工作服务器就象在本地工作一样。Rexec程序允许你不用提供密码就可以从远程在服务器上运行命令。然而，这些服务都是以明文的方式传输信息。Secure Shell(SSH)是最常见的替代这些服务的方法。在本文工作时，SSH2是最新的版本。

SSH提供的安全服务

SSH提供两项基本的服务：

- 数据保密：由于服务器首先发送它的公钥给客户端，所以数据通道是加密的。然后客户端使用服务器的公钥对所有信息加密。当服务器收到加密的信息后，使用自己的私钥对信息进行解密。
- 验证：仗用上面谈到的公钥，两个用尸交换彼此的公钥然后使用公钥进行验证。这种机制的好处是在网络上不会传输用户名和密码的信息。

你需要理解SSH首先加密了数据通道，然后运行各种各样的验证方法。缺省情况下，Secure Shell使用22端口，允许你使用公钥进行加密。SSH2使用DSA数字签名算法，这种算法与RSA公钥加密相似，但是没有专和。当然，SSH2可以使用RSA算法。

在SSH中的加密和验证

加密的过程从服务器自动把公钥发送给客户端开始。然后客户端使用公钥加密信息，服务器用自己的私钥对信息解密。随后系统间的所有传输都要加密。

验证

缺省情况一下， SSH会首先尝试用公钥进行验证。这些公钥存储在每个用户的$HOME／.ssh2目录一下。例如，如果在你的RedHatLinux 6.1工作系统一下有一个名叫james的用户。则所有的密钥(包括james的公钥和私钥)都存储在、home巧ames／．ssh2目录下。请注意这是个隐藏目录。

如果这些密钥或识别和验证的文件并不存在，则SSH将使用标准的存放在／etc／passwd和／etc／shadow数据库中的用户名和密码。这种方式的缺点是在网络中传输了用户名和密码。虽然密码信息是加密的，但是在公网上传送密码肯定是不安全的。

SSH2内容

最初SSH是被发展来使UNIX系统之间的连接更安全的。然而，许多Windows的客户端允许你在连接UNIX工作系统时使用SSH。一下表提供了UNIX和NTSSH2的有关内容

内容	描述
／usr／Iocal／bin／ssh2	LinuxSSH2 客户端
SSH Secure Shell 客户端	许多的 Windows · 下 SSH 客户端之—…。 F-Secure 支持 Windows 和 Macintosh 系统
／usr／local／bin／ssh-keygen2	为每个用户生成密钥对
／usr／Iocal／bin／scp2	客户端允许你使用由 SSH 加密的通道来远程执行命令
／usr／Iocal／sbin／sshd2	SSH2 守护进程
／usr／Iocal／bin／ssh-agent2	允阡你将公钥存储在内存中。只要你已经建立了信任关系，则登录时不需要密码。
／usr／!ocal／bin／sfip-server2	运行 sshd2 的 secure FTP 服务器。某些 Windows 客户端可以使用 secure FTP 服务器
／usr／iocal／bin／sfTp2	Secure FTP 客户端

你可以从各种途径获得SSH，包括www．ssh．org，www．ssh．com，和rufus．w3．org。要获得更多有关SSH2的信息，你可以阅读随文档附带的README文件，或者阅读FAQ (http：／／www,ssh．org／faq．html)你可以从各种RPM站点获得各种版本的SSH(例如rufus．w3．org和www．datafellows．com)。

在使用客户端/服务器产品时，你必须首先配置服务器和客户端彼此通信。要做到这一点，需用安装和建立信任关系。在Linux下，安装服务器的同时也安装了客户端。然后，你可以生成和交换公钥。服务器的配置过程包括生成公钥和私钥。这些密钥会自动在SSH握手阶段进行传输。你必须输入下列命令来启动SSH2服务：

／usr／local／sbin／sshd2

你可以编辑／etc／rc.local文件使ssh2d每次都自动启动。对于Red Hat Linux工作系统，你只需要在该文件最后加上／usr／local／sbin／sshd2一行即可。

使用SSH登录

使用SSH登录，你需用使用—下列命令格式：　　．

／usr／local／bin／ssh2 –L usemame hostname

例如，使用用户名test登录系统noyas，你需用键入‘下列命令

·　　／usr／local／bin／ssh2 –1 test noyas

与SSH1兼容

如果你有已经运行SSH1的系统，则按照文件名是SSH2．QUICKSTART的指导来工作

就行了。按照下列步骤进行将保证你的SSHl客户端可以使用SSH2。

SSH和验证：建立用户之间的信任关系

交换公钥的方法是最安全的SSH验证手段。在SSHfuwuq可以使用公钥加密进行验证之前，每个用户必须正确地建立信任关系。通常，这意味着每个用户必须交换公钥。 下列是建立允许验证的密钥对的过程。这个过程假设两个用户希望使用公钥验证的SSH验证方式。请记住，SSH服务器自动加密数据通道。客户端只提供公钥进行验证。每个用户需要按照下面的过程进行设置。

1、使用／usr／Iocal／bin／ssh-keygen2程序生成密钥对。象上面谈到的，Ssh-keygen2程序自动在每个用户主目录下的．ssh2目录中生成密钥对。

2、改变目录到你的主目录下的．ssh2目录中。然后重命名公钥和私钥文件。如果你使用标准的1024位加密，该文件缺省的名称是id dsa 1024 a和id—dsa 1024_a．pub。你可以自由地分发结尾是．pub的文件，然而，不是以．pub结尾的文件必须保密。其实，你应当确保该文件：只能被你读取。你还应当重命名这些文件：并跟踪它们。例如，如果你的用户名是test，并且系统名为noyas的话，你可以将他的公钥和私钥分别重命名为test．noyas和test．noyas．pub

3、 然后建立名为identification和authorization的两个文件。文件Identification内有你自己的私钥的名称，文件authorization内有你允许进入你的系统的所有用户的公钥的名称。你可以在该文件中输入任何你想输入的公钥名称。

4、在文件identification中输入私钥的名称。正确的格式是：Idkey test．noyas

5、同伴之间交换公钥。请记住，私钥要自己保管好。

6、在你收到其他人的公钥后，请确保把这些文件存放在．ssh2目录下。然后，你必须在文件authorization中输入同伴的公钥名称。语法是：Keykeyname．pub。每一项占一行。如果你在文件：authorization中输入Sandi和Jacob的公钥，你的文倒：authorization将如下所示：

key sandi．pub

key jacob．pub

7． 一旦你和至少一个同伴进行完以上的步骤，则用户间便可以使用公钥加密来进行SSH2验证了。

技术提示：为了使这些步骤能够正常工作，必须运行sshd2的守护进程。请记住，sshd2守护进程通过自动传送公钥到所有申请的客户端来进行加密。每个用户负责建立彼此的信任关系来进行验证。你还应该保证DNS能够正常提供解析工作。

本章小结

在本课中，你学习了如何分析安全审计的结果来证明存在漏洞以及提出建议来弥补它们。你实施了几种增强网络安全的解决方案，包括个人防火墙，本机审计和SSH。你现在已已经具备了知识和技能来解决在审计的侦查阶段发现的问题。