晋城职业技术学院
JINCHENG INSTITUTE OF TECHNOLOGY
信息工程系

基础实训项目

佐证材料

2021年11月

目　录

模块一 网络安全基础

职业能力要求

专业能力：掌握网络安全行业的基本情况，了解网络安全行业的新技术；培养良好的职业道德

学习目标

- 了解网络安全的重要性；
- 掌握网络安全的定义；
- 了解信息安全的发展历程；
- 了解网络安全常见的防护技术。

1.1 基本概念

网络安全从其说就是网络上的信息安全，涉及的领域很广。网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因为偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常的运行，网络服务不中断。包括以下含义：

一，网络运行系统安全

二，网络上系统信息的安全

三，网络上信息传播的安全，即信息传播后果的安全

四，网络上信息内容的安全。

1.2 主要特性

1.保密性

信息不泄露给非授权用户、实体或过程，或供其利用的特性。

2.完整性

数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性

3.可用性

可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击

4.可控性

对信息的传播及内容具有控制能力。

5.可审查性

即出现安全问题时提供依据与手段

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的内部业务处理、办公自动化等发展到基于复杂的内部网（Intranet）、企业外部网（Extranet）、全球互联网（Internet）的企业级计算机处理系统和世界范围内的信息共享和业务处理。在系统处理能力提高的同时，系统的连接能力也在不断的提高。但在连接能力信息、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、应用系统安全和网络管理的安全等。

因此计算机安全问题，应该像每家每户的防火防盗问题一样，做到防范于未然。甚至不会想到你自己也会成为目标的时候，威胁就已经出现了，一旦发生，常常措手不及，造成极大的损失。

1.3 网络安全现状

随着计算机技术的飞速发展，信息网络已经成为社会发展的重要保证。有很多是敏感信息，甚至是国家机密。所以难免会吸引来自世界各地的各种人为攻击

（例如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等）。同时，网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。

1.国外

2012 年 02 月 04 日，黑客集团 Anonymous 公布了一份来自 1 月 17 日美国 FBI 和英国伦敦警察厅的工作通话录音，时长 17 分钟，主要内容是双方讨论如何寻找证据和逮捕 Anonymous 等黑帽子黑客的方式，而其中涉及未成年黑客得敏感内容被遮盖。

目前 FBI 已经确认了该通话录音得真实性，安全研究人员已经开始着手解决电话会议系统得漏洞问题。

2012 年 02 月 13 日，据称一系列政府网站均遭到了 Anonymous 组织的攻击，而其中 CIA 官网周五被黑长达 9 小时。这一组织之前曾拦截了伦敦警察与 FBI 之间的一次机密电话会谈，并随后上传于网络。

2. 国内

2010 年，Google 发布公告称将考虑退出中国市场，而公告中称：造成此决定的重要原因是因为 Google 被黑客攻击。

2011 年 12 月 21 日，国内知名程序员网站 CSDN 遭到黑客攻击，大量用户数据库被公布在互联网上，600 多万个明文的注册邮箱被迫“裸奔”。

2011 年 12 月 29 日下午消息，继 CSDN、天涯社区用户数据泄露后，互联网行业一片人心惶惶，而在用户数据最为重要的电商领域，也不断传出存在漏洞、用户泄露的消息，漏洞报告平台乌云昨日发布漏洞报告称，支付宝用户大量泄露，被用于网络营销，泄露总量达 1500 万～2500 万之多，泄露时间不明，里面只有支付用户的账号，没有密码。目前已经被卷入的企业有京东(微博)商城、支付宝(微博)和当当(微博)网，其中京东及 支付宝否认信息泄露，而当当则表示已经向当地公安报案。

1.4 网络（信息）安全涉及的内容

1.物理安全

网络的物理安全是整个网络系统安全的前提。在校园网工程建设中，由于网络系统属于弱电工程，耐压值很低。因此，在网络工程的设计和施工中，必须优

先考虑保护人和网络设备不受电、火灾和雷击的侵害；考虑布线系统与照明电线、动力电线、通信线路、暖气管道及冷热空气管道之间的距离；考虑布线系统和绝缘线、裸体线以及接地与焊接的安全；必须建设防雷系统，防雷系统不仅考虑建筑物防雷，还必须考虑计算机及其他弱电耐压设备的防雷。总体来说物理安全的风险主要有，地震、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获；高可用性的硬件；双机多冗余的设计；机房环境及报警系统、安全意识等，因此要注意这些安全隐患，同时还要尽量避免网络的物理安全风险。

2.网络结构

网络拓扑结构设计也直接影响到网络系统的安全性。假如在外部和内部网络进行通信时，内部网络的机器安全就会受到威胁，同时也影响在同一网络上的许多其他系统。透过网络传播，还会影响到连上 Internet/Intranet 的其他的网络；影响所及，还可能涉及法律、金融等安全敏感领域。因此，我们在设计时有必要将公开服务器（WEB、DNS、EMAIL 等）和外网及内部其它业务网络进行必要的隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其它的请求服务在到达主机之前就应该遭到拒绝。

3.系统安全

所谓系统的安全是指整个网络操作系统和网络硬件平台是否可靠且值得信任。恐怕没有绝对安全的操作系统可以选择，无论是 Microsoft 的 Windows NT 或者其它任何商用 UNIX 操作系统，其开发厂商必然有其 Back-Door。因此，我们可以得出如下结论：没有完全安全的操作系统。不同的用户应从不同的方面对其网络作详尽的分析，选择安全性尽可能高的操作系统。因此不但要选用尽可能可靠的操作系统和硬件平台，并对操作系统进行安全配置。而且，必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

4 应用安全

应用系统的安全跟具体的应用有关，它涉及面广。应用系统的安全是动态的、不断变化的。应用的安全性也涉及到信息的安全性，它包括很多方面。

应用的安全涉及方面很多，以 Internet 上应用最为广泛的 E-mail 系统来说，其解决方案有 sendmail、Netscape Messaging Server、SoftwareCom Post.Office、Lotus Notes、Exchange Server、SUN CIMS 等不下二十多种。其安全手段涉及 LDAP、DES、RSA 等各种方式。应用系统是不断发展且应用类型是不断增加的。在应用系统的安全性上，主要考虑尽可能建立安全的系统平台，而且通过专业的安全工具不断发现漏洞，修补漏洞，提高系统的安全性。

信息的安全性涉及到机密信息泄露、未经授权的访问、 破坏信息完整性、假冒、破坏系统的可用性等。在某些网络系统中，涉及到很多机密信息，如果一些重要信息遭到窃取或破坏，它的经济、社会影响和政治影响将是很严重的。因此，对用户使用计算机必须进行身份认证，对于重要信息的通讯必须授权，传输必须加密。采用多层次的访问控制与权限控制手段，实现对数据的安全保护；采用加密技术，保证网上传输的信息（包括管理员口令与帐户、上传信息等）的机密性与完整性。

5 管理安全

管理是网络中安全最最重要的部分。责权不明，安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。当网络出现攻击行为或网络受到其它一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。

建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是制定健全的管理制度和严格管理相结合。保障网络的安全运行，使其成为一个具有良好的安全性、可扩充性和易管理性的信息网络便成为了首要任务。一旦上述的安全隐患成为事实，所造成的对整个网络的损失都是难以估计的。因此，网络的安全建设是校园网建设过程中重要的一环。

1.5 安全措施

1.安全技术手段

物理措施：例如，保护网络关键设备(如交换机、大型计算机等)，制定严格的网络安全规章制度，采取防辐射、防火以及安装不间断电源（UPS）等措施。

访问控制：对用户访问网络资源的权限进行严格的认证和控制。例如，进行用户身份认证，对口令加密、更新和鉴别，设置用户访问目录和文件的权限，控制网络设备配置的权限等等。

数据加密：加密是保护数据安全的重要手段。加密的作用是保障信息被人截获后不能读懂其含义。防止计算机网络病毒，安装网络防病毒系统。

网络隔离：网络隔离有两种方式，一种是采用隔离卡来实现的，一种是采用网络安全隔离网闸实现的。

隔离卡主要用于对单台机器的隔离，网闸主要用于对于整个网络的隔离。这两者的区别可参见参考资料。

其他措施：其他措施包括信息过滤、容错、数据镜像、数据备份和审计等。围绕网络安全问题提出了许多解决办法，例如数据加密技术和防火墙技术等。数据加密是对网络中传输的数据进行加密，到达目的地后再解密还原为原始数据，目的是防止非法用户截获后盗用信息。防火墙技术是通过对网络的隔离和限制访问等方法来控制网络的访问权限。

2.安全防范意识

拥有网络安全意识是保证网络安全的重要前提。许多网络安全事件的发生都和缺乏安全防范意识有关。

3.主机安全检查

要保证网络安全，进行网络安全建设，第一步首先要全面了解系统，评估系统安全性，认识到自己的风险所在，从而迅速、准确得解决内网安全问题。由安天实验室自主研发的国内首款创新型自动主机安全检查工具，彻底颠覆传统系统保密检查和系统风险评测工具操作的繁冗性，一键操作即可对内网计算机进行全面的安全保密检查及精准的安全等级判定，并对评测系统进行强有力的分析处置和修复。

模块二 常用系统攻击方法

职业能力要求

熟悉 TCP/IP。

了解黑客攻击的常用手段和方法。

学习目标

- 掌握扫描器使用的方法，能够通过扫描器写出系统漏洞报告。
- 了解网络监听的原理，掌握防御网络监听的方法。
- 了解拒绝服务攻击的原理，掌握防御拒绝服务攻击的方法。

2.1.扫描器的使用

2.1.1 X-Scan 简介

X-Scan 是中国著名的综合扫描器之一，它是免费的而且不需要安装的绿色软件、界面支持中文和英文两种语言、包括图形界面和命令行方式（X-Scan 3.3 以后取消命令行方式）。X-Scan 主要由国内著名的民间黑客组织“安全焦点”（http://www.xfocus.net）完成，从 2000 年的内部测试版 X-Scan V0.2 到目前的最新版本 X-Scan 3.3-cn 都凝聚了国内众多黑客的努力。X-Scan 把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述、漏洞溢出程序，方便网管测试、修补漏洞。

X-Scan 采用多线程方式对指定 IP 地址段(或单机)进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式，扫描内容包括：远程操作系统类型及版本，标准端口状态及端口 BANNER 信息，CGI 漏洞，IIS 漏洞，RPC 漏洞，SQL-SERVER、FTP-SERVER、SMTP-SERVER、POP3-SERVER、NT-SERVER 弱口令用户，NT 服务器 NETBIOS 信息等。扫描结果保存在/log/目录中，index_*.htm 为扫描结果索引文件。

2.1.2 X-Scan 安装与使用

一 实验目的：

1.了解目前系统存在的典型漏洞；

2.学会使用网络扫描和漏洞扫描工具

二．实验步骤

1，运行‘xscan_gui.exe’；如图 2-1 所示

图 2-1 运行文件

2，运行 x-scan 之后随即加载漏洞检测样本；如图 2-2 所示。

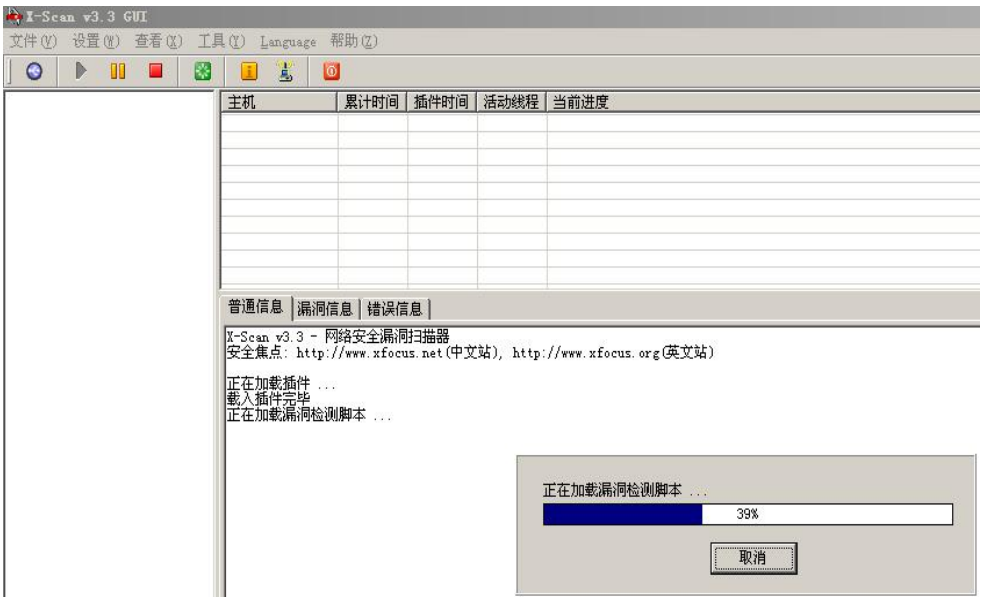


图 2-2 加载漏洞检测样本

3，设置扫描参数；如图 2-3 所示。

图 2-3 设置扫描参数

4，扫描参数界面需要制定 IP 范围，这里可以是一个 IP 地址，可以是 IP 地址范围，可以是一个 URL 网址；如图 2-4 所示。

图 2-4 设置扫描 ip 地址范围

5，点开‘全局设置’前面的‘+’号；展开后会有 4 个模块，分别是“扫描模块”、“并发扫描”、“扫描报告”、“其他设置”。如图 2-5 所示。

图 2-5 全局设置

6，点击“扫描模块”在右边的边框中会显示相应的参数选项，如果我们是扫描少数几台计算机的话可以全选，如果扫描的主机比较多的话，我们要有目标的去扫描，只扫描主机开放的特定服务就可以，这样会提高扫描的效率。如图 2-6 所示。

图 2-6 设定扫描的服务

7，选择“并发扫描”，可以设置要扫描的最大并发主机数，和最大的并发线程数。如图 2-7 所示。

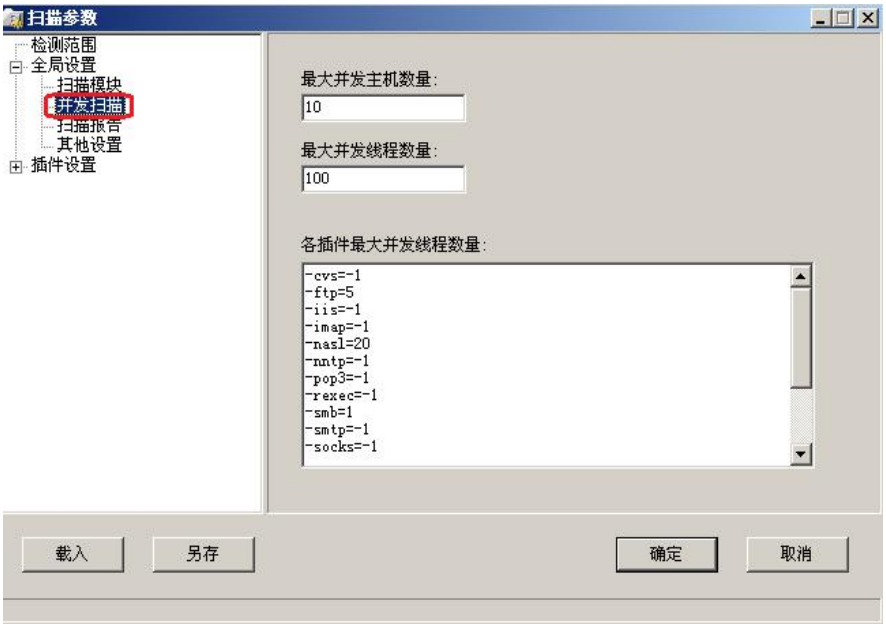


图 2-7 设置并发扫描

8，选择‘扫描报告’，点击后会显示在右边的窗格中，它会生成一个检测IP 或域名的报告文件，同时报告的文件类型可以有 3 种选择，分别是 HTML、TXT、XML。如图 2-8 所示。

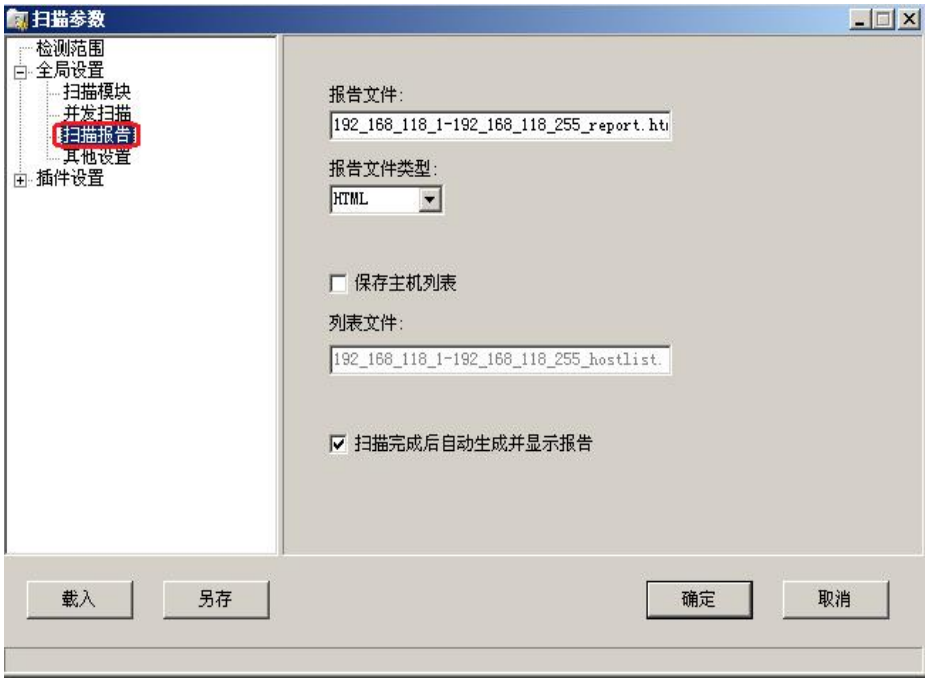


图 2-8 设置报告文件格式

9，选择‘其他设置’，有 2 种条件扫描：（1）‘跳过没有响应的主机’，（2）‘无条件扫描’。如果设置了‘跳过没有响应的主机’，对方禁止了 PING 或防火墙设置使对方没有响应的话，X-SCAN 会自动跳过，自动检测下一台主机。如果用‘无条件扫描’的话，X-SCAN 会对目标进行详细检测，这样结果会比较详细也会更加准确。但扫描时间会更长（有时候会发现扫描的结果只有自己的主机，这是可以选‘无条件扫描’就能看到别的主机的信息了）。‘跳过没有检测到开放端口的主机’和‘使用 NMAP 判断远程操作系统’这两项需要勾选，‘显示详细进度’项可以根据自己的实际情况选择（可选）。如图 2-9 所示。

10，在‘端口相关设置’中可以自定义一些需要检测的端口。检测方式“TCP”、“SYN”两种，TCP 方式容易被对方发现，准确性要高一些，SYN 则相反。如图 2-10 所示。

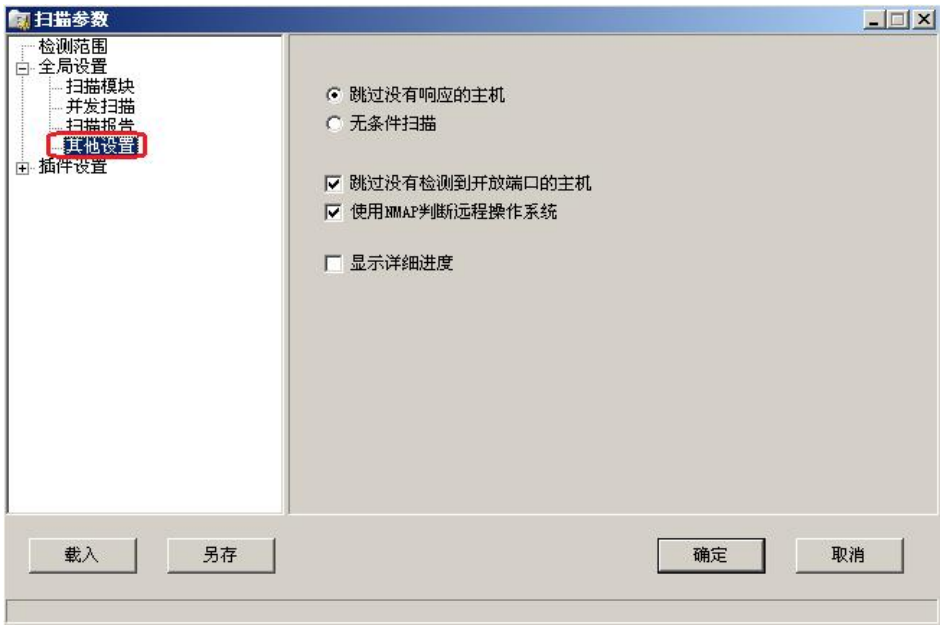


图 2-9 其他属性设置

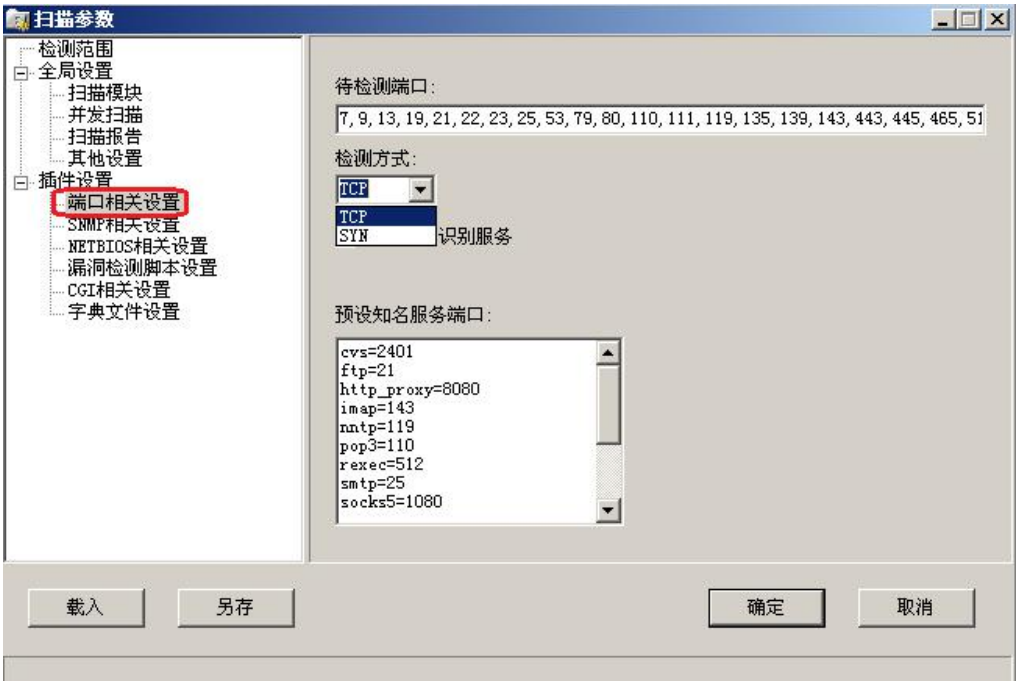


图 2-10 扫描端口设置

11，‘SNMP 相关设置’用来针对 SNMP 信息的一些检测设置，在监测主机数量不多的时候可以全选；如图 2-11 所示。

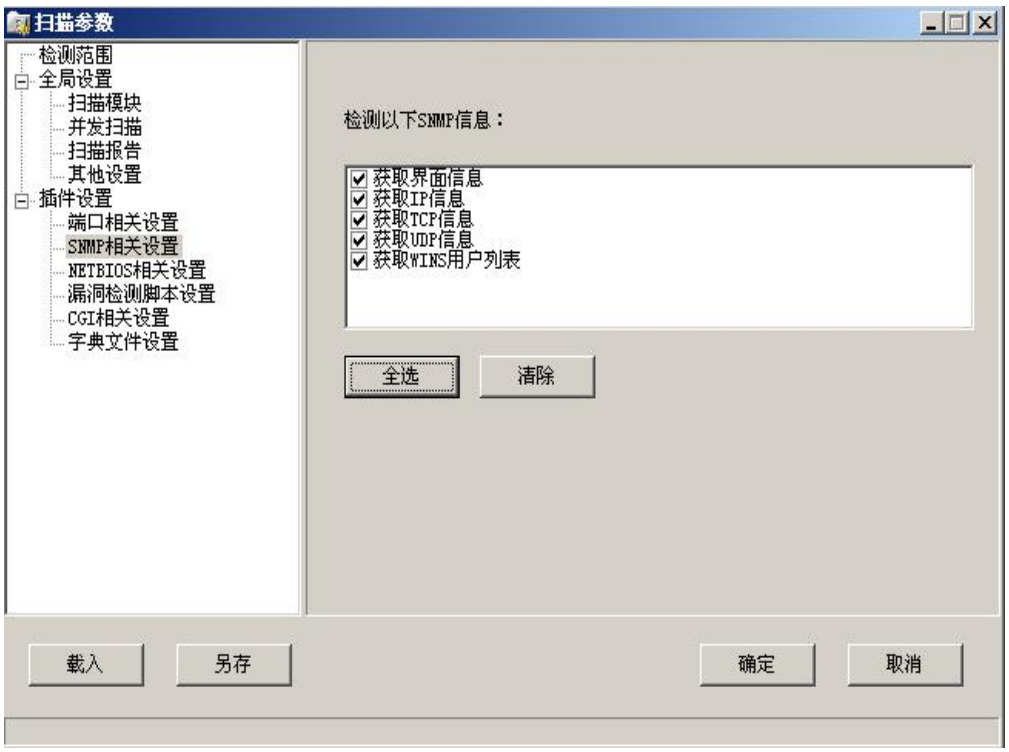


图 2-11 SNMP 检测设置

12，“NETBIOS 相关设置”是针对 WINDOWS 系统的 NETBIOS 信息的检测设置，包括的项目有很多种，根据实际需要进行选择。如图 2-12 所示。

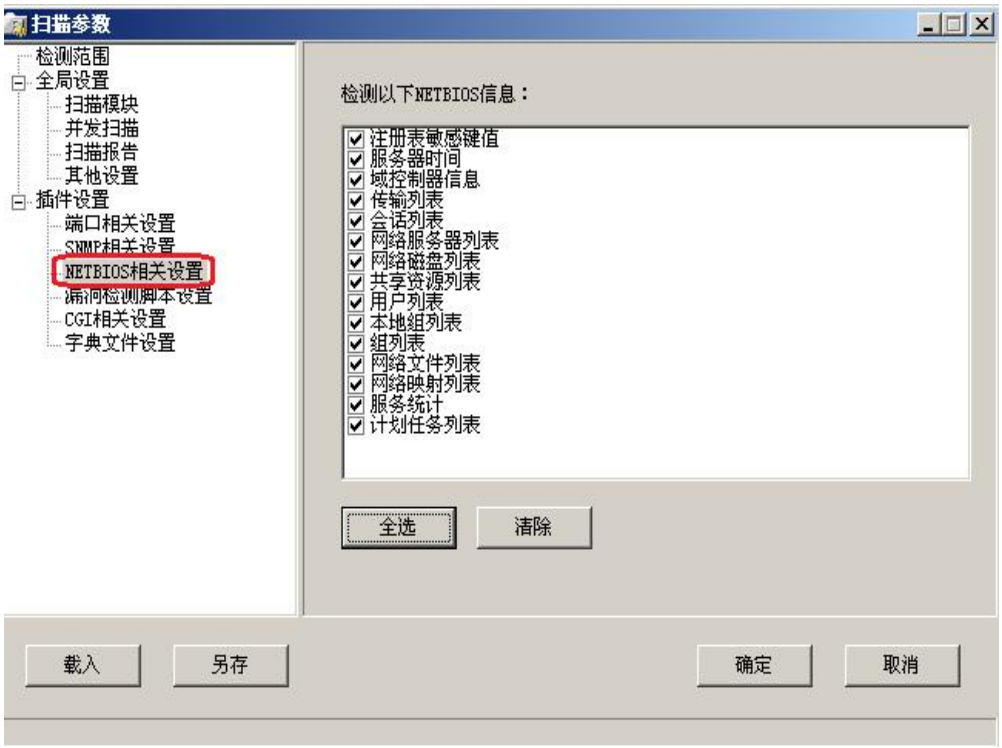


图 2-12 NETBIOS 信息的检测设置

13，如需同时检测很多主机的话，要根据实际情况选择特定的漏洞检测脚本。如图 2-13 所示。

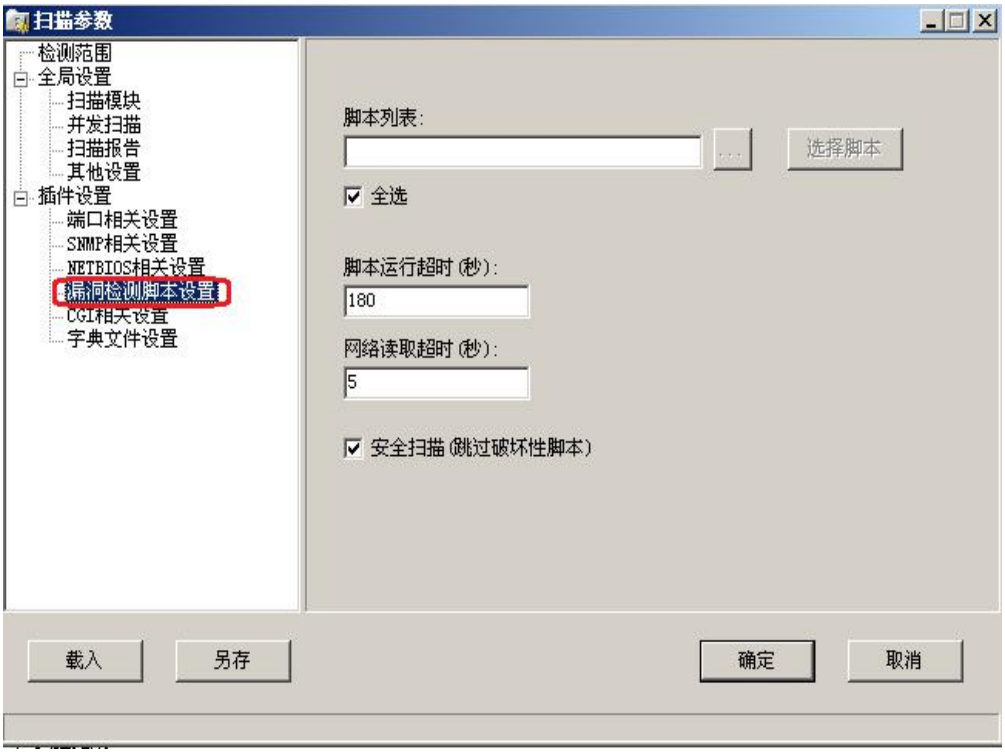


图 2-13 选择漏洞检测脚本

14，‘CGI 相关设置’，默认就可以。如图 2-14 所示。

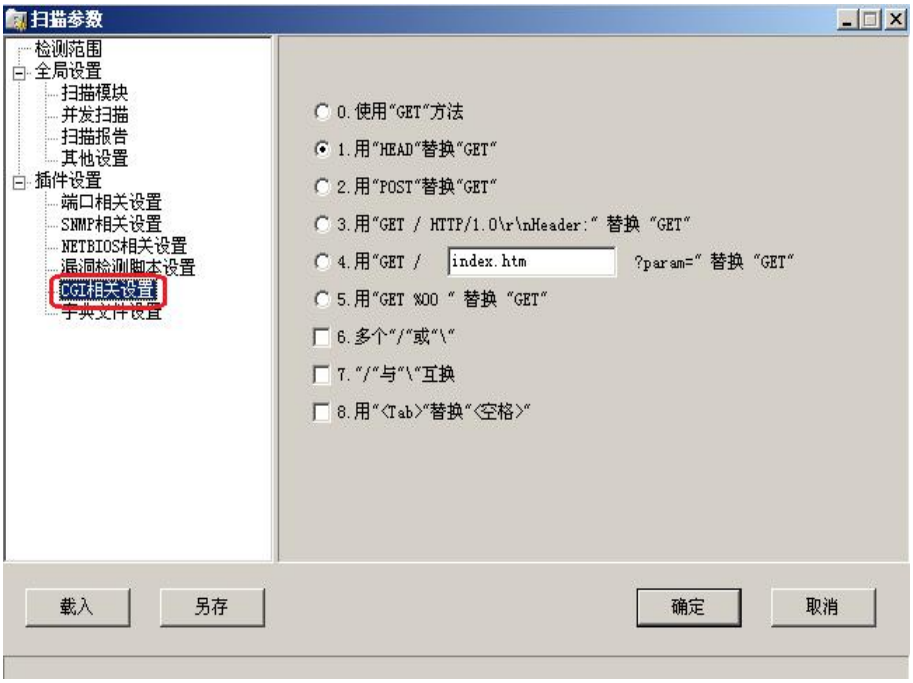


图 2-14 CGI 相关设置

15，‘字典文件设置’是 X-SCAN 自带的一些用于破解远程账号所用的字典文件，这些字典都是简单或系统默认的账号等。我们可以选择自己的字典或手工对默认字典进行修改。默认字典存放在“DAT”文件夹中。字典文件越大，探测时间越长，此处无需设置。如图 2-15 所示。

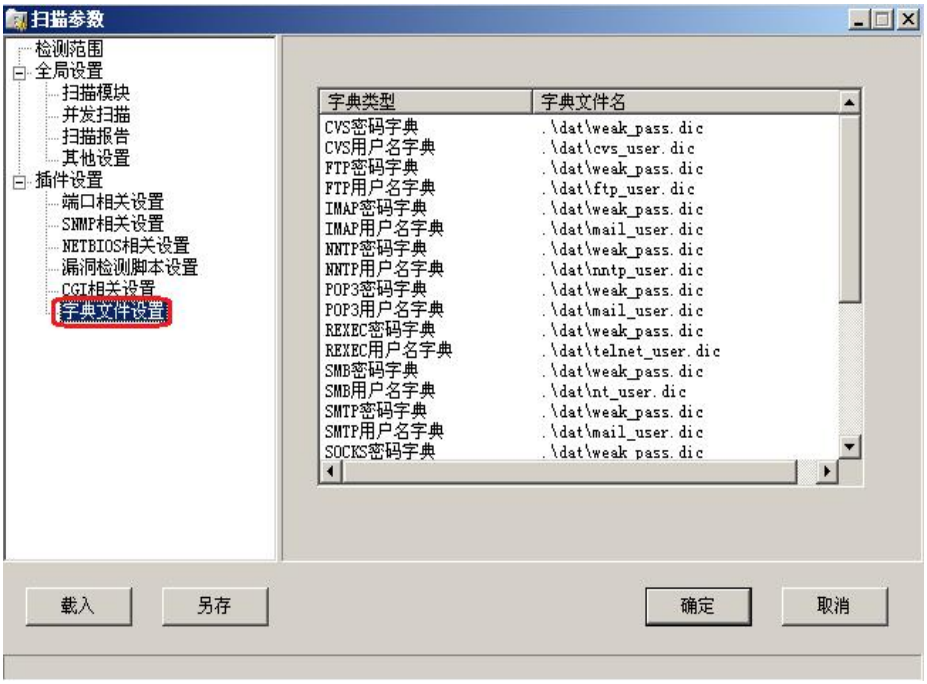


图 2-15 字典文件设置

16，在‘全局设置’和‘插件设置’2 个模块设置好以后，点‘确定’保存设置，然后点击‘开始扫描’就可以了。X-SCAN 会对对方主机进行详细的检测。如果扫描过程中出现错误的话会在“错误信息”中看到。如图 2-16 所示。

图 2-16 开始扫描

17，扫描过程中。如图 2-17 所示。

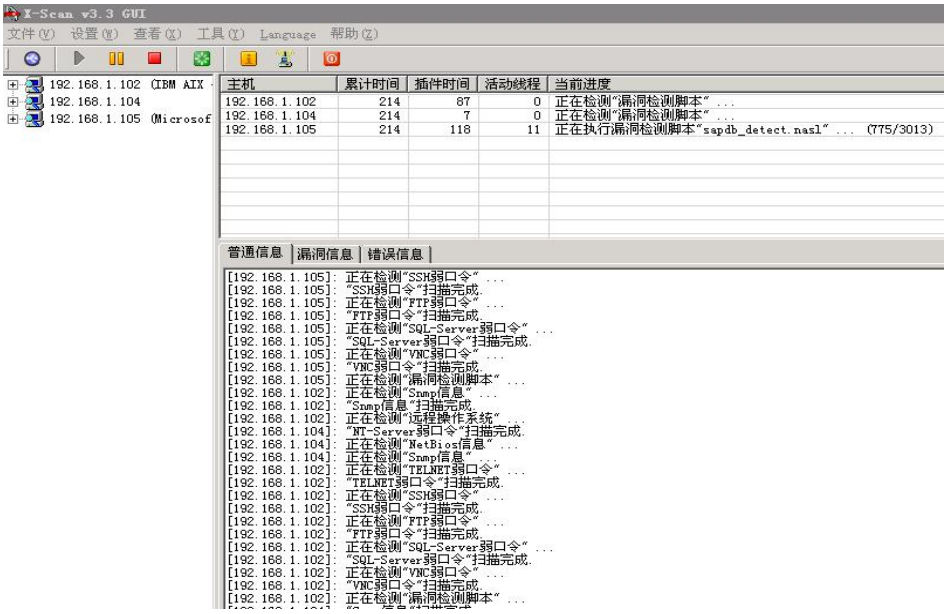


图 2-17 扫描过程

18，扫描结束以后会自动弹出检测报告，包括漏洞的风险级别和详细的信息，以便我们对对方主机进行详细的分析。如图 2-18 所示。

图 2-18 检测报告

19，以下为本实验抓图参考：如图 2-19 所示。

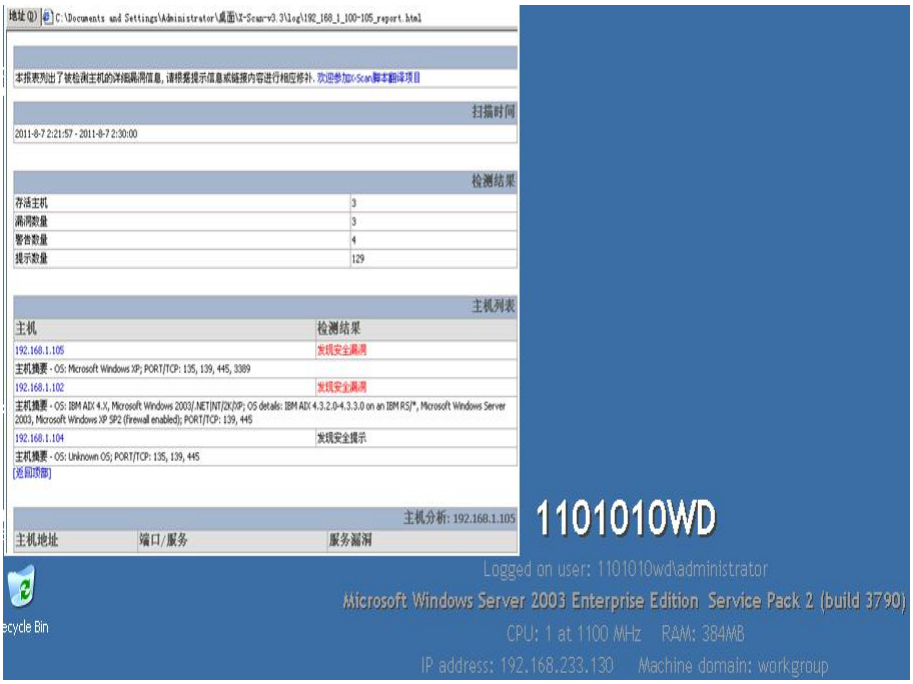


图 2-19 抓图

实验总结：

经过这个课时的实践，我们在对网络安全工具 SuperScan 的应用----收集远程网络主机和寻找自己网络中的漏洞有了一定的了解，特别是 SuperScan 中的“Scan”和“Windows Enumeration”两项，我们可以利用它们寻找网络上其它客户机的 TCP/IP 参数。

2.2 网络监听工具

2.2.1 网络监听的意义及工具

网络监听是一种监视网络状态、数据流程以及网络上信息传输的管理工具，它可以将网络界面设定成监听模式，并且可以截获网络上所传输的信息。也就是说，当黑客登录网络主机并取得超级用户权限后，若要登录其它主机，使用网络监听便可以有效地截获网络上的数据，这是黑客使用最好的方法。但是网络监听只能应用于连接同一网段的主机，通常被用来获取用户密码等。

Wireshark 是一个网络封包分析软件。其主要功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。其使用目的包括：网络管理员检测网络问题，网络完全工程师检查资讯安全相关问题，开发者为新的通讯协定出错，普通使用者学习网络协议的相关知识。

值得注意的是，Wireshark 并不是入侵检测软件。对于网络上的异常流量行为，Wireshark 不会产生警示或是任何提示。然而，仔细分析 Wireshark 撷取的封包能够帮助使用者对于网络行为有更清楚的了解。Wireshark 不会对网络封包产生内容的修改，它只会反映目前流通的封包资讯。Wireshark 本身也不会送出封包至网络上。

2.2.1 Wireshark 网络监听实验

一．实验目的与要求

1、初步掌握 Wieshark 的使用方法，熟悉其基本配置。

2、通过对 Wieshark 抓包实例进行分析，进一步加深对各类常用网络协议的理解。

3、学习和掌握如何利用 Wireark 进行网络安全监测与分析。

虚拟主机为 windows xp，物理主机为 win7　Wieshark 软件

二．实验步骤

1、安装 Wireshark

（1）双击文件夹中的可执行文件，如图 2-20 所示。

图 2-20 Wireshark 的可执行文件

(2)该对话框时一个安装提示，如果之前没有安装过该文件，则点击下一步，如图 2-21 所示。

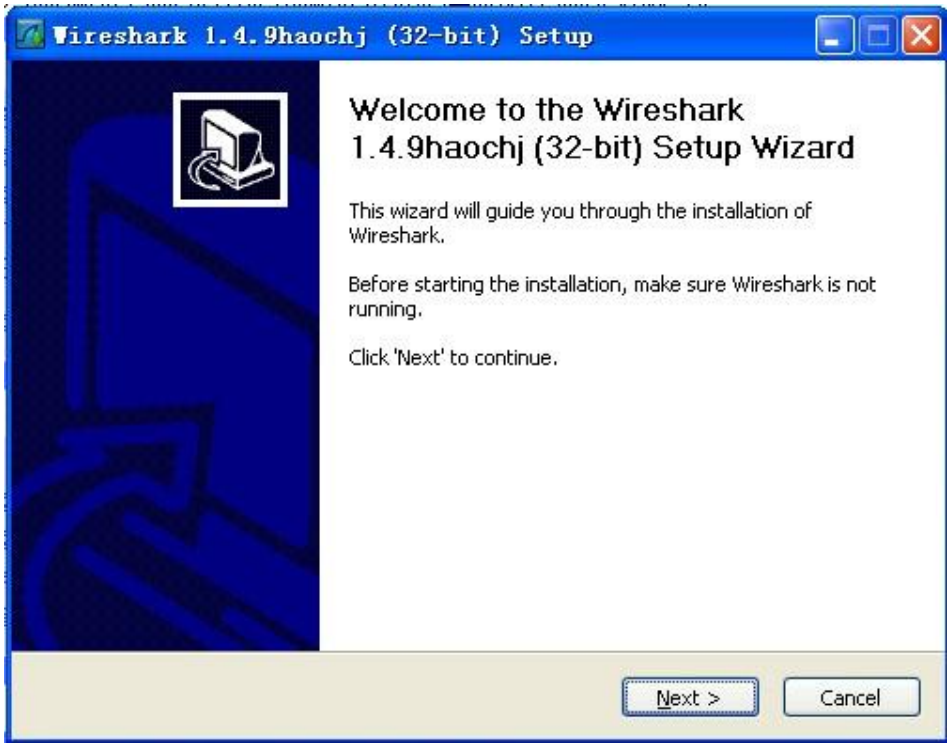
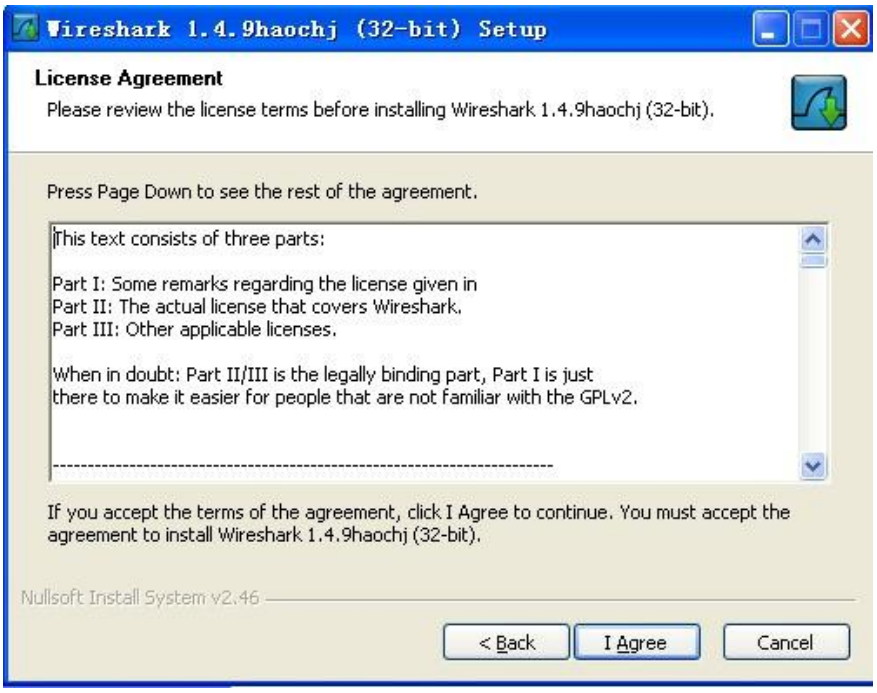


图 2-21 确认对话框

（3）图 2-22 所示是一个关于该软件的许可证说明，可以忽略，点击下一步。



2-22 Wireshark 的许可说明

（4）在图 2-23 中罗列出来的是一些可选安装组件，可根据实际需要选择安装

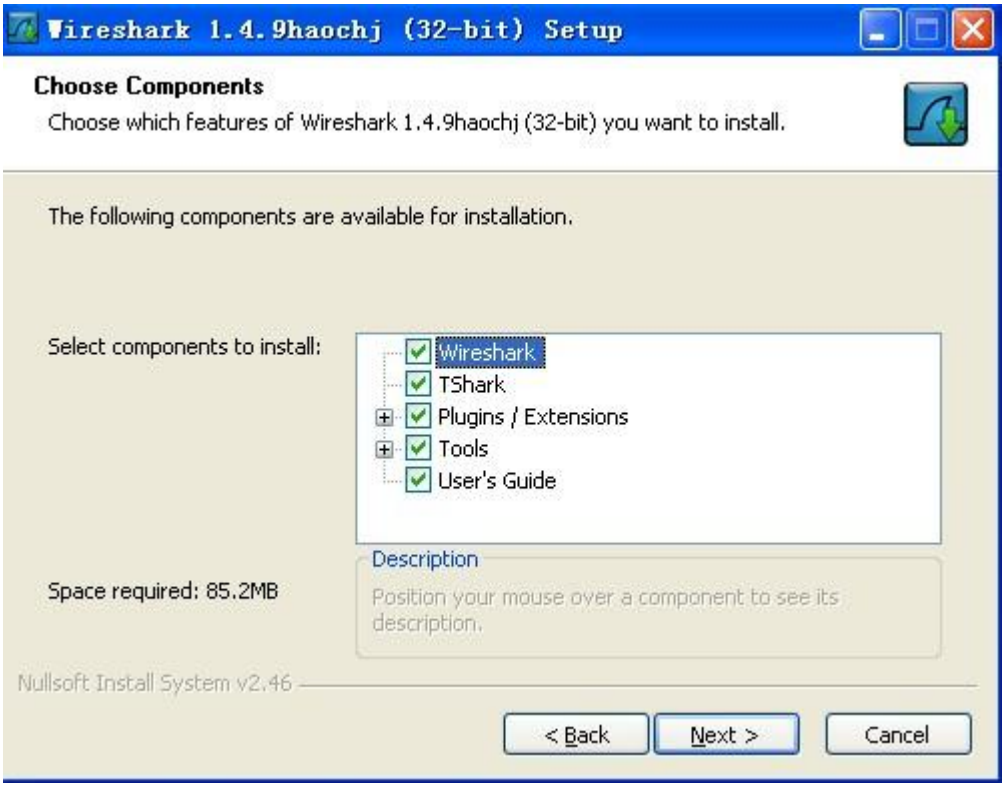


图 2-23 选择安装组件

（5）以下是关于该软件的图标创建位置和支持的文件拓展，图标部分可根据实际情况选择，然后点击下一步，如图 2-24 所示。

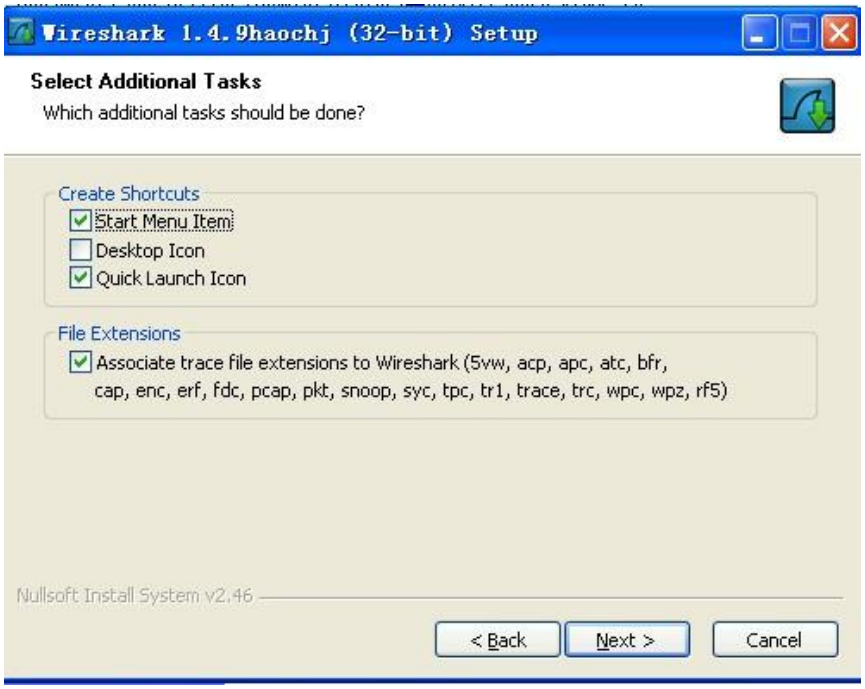


图 2-24 快捷方式

（6）程序的安装位置，这里选择默认，点击下一步。如图 2-25 所示。

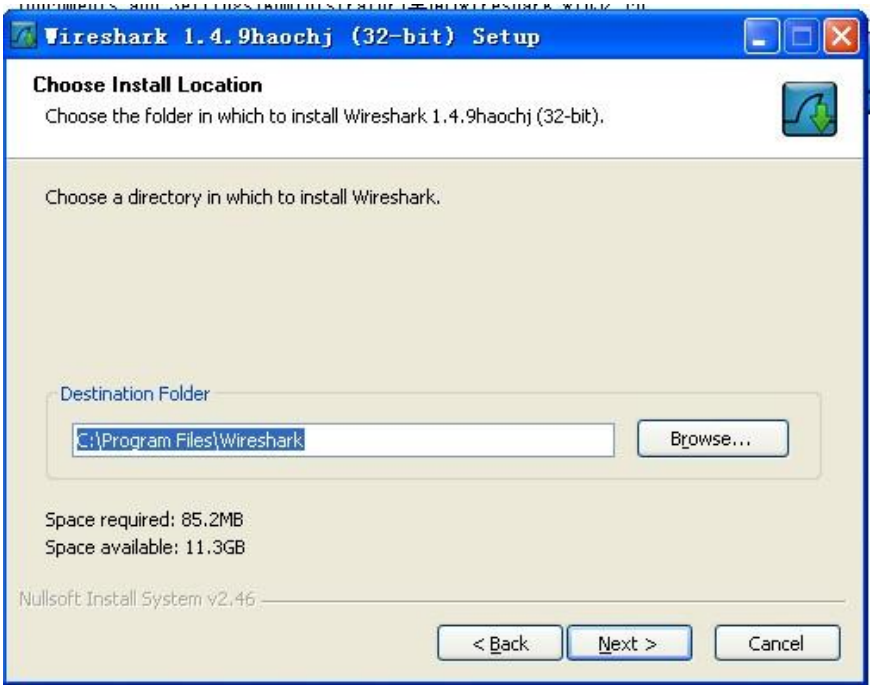


图 2-25 程序安装位置

（7）安装 WinPcap 插件，在这一步必须勾选安装，不然无法进行以下的实验。如图 2-26 所示。

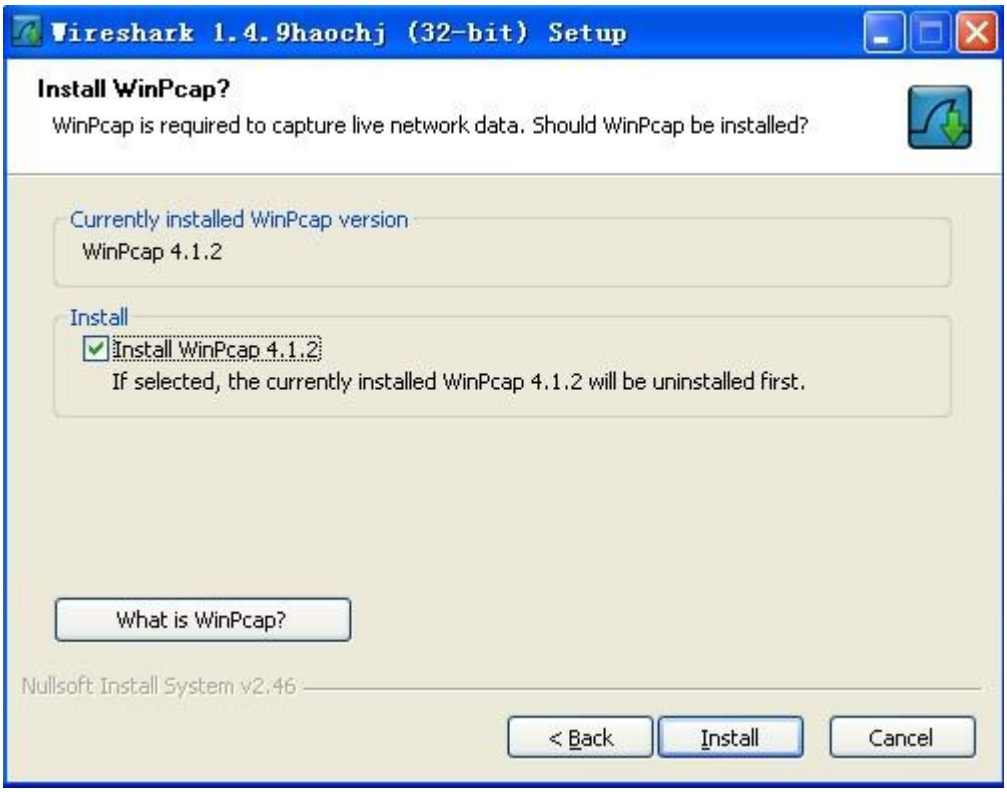


图 2-25 勾选 WinPcap 插件

（8）下面开始进入 WinPcaP 插件的安装过程，点击下一步，如图 2-26 所示。

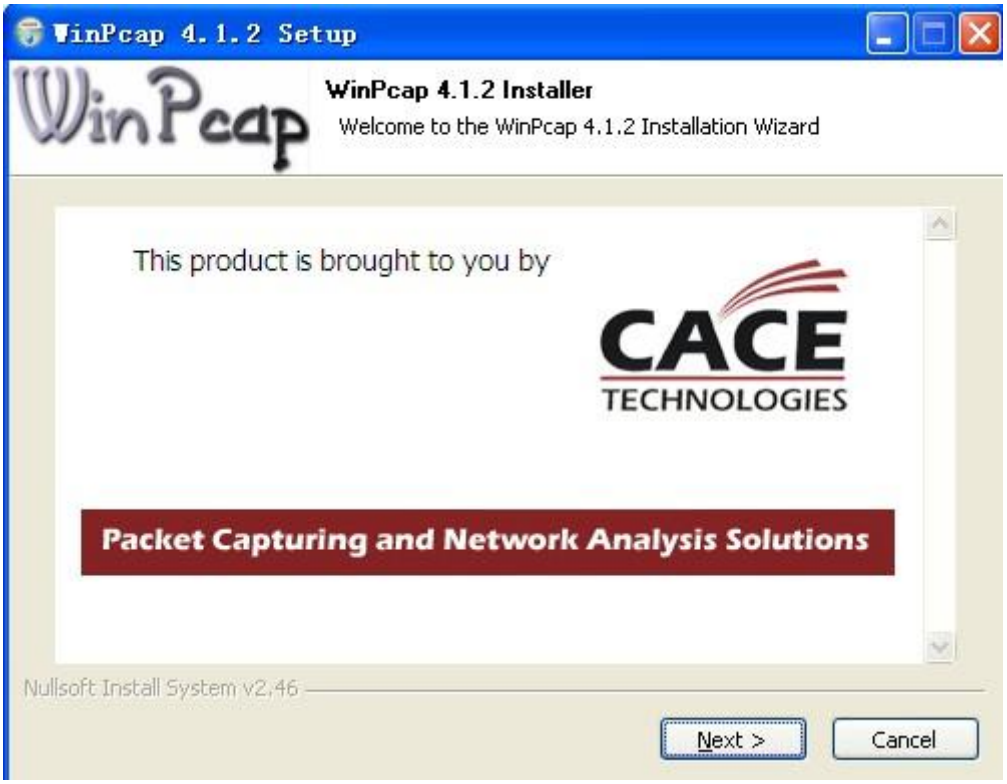


图 2-26 安装 WinPcaP

（9）这一步是对 WincaP 插件的介绍，可以不用理会，继续下一步。

图 2-27 WinPcaP 介绍

（10）WinPcaP 的许可协议，点击“I Agren”，如图 2-28 所示。

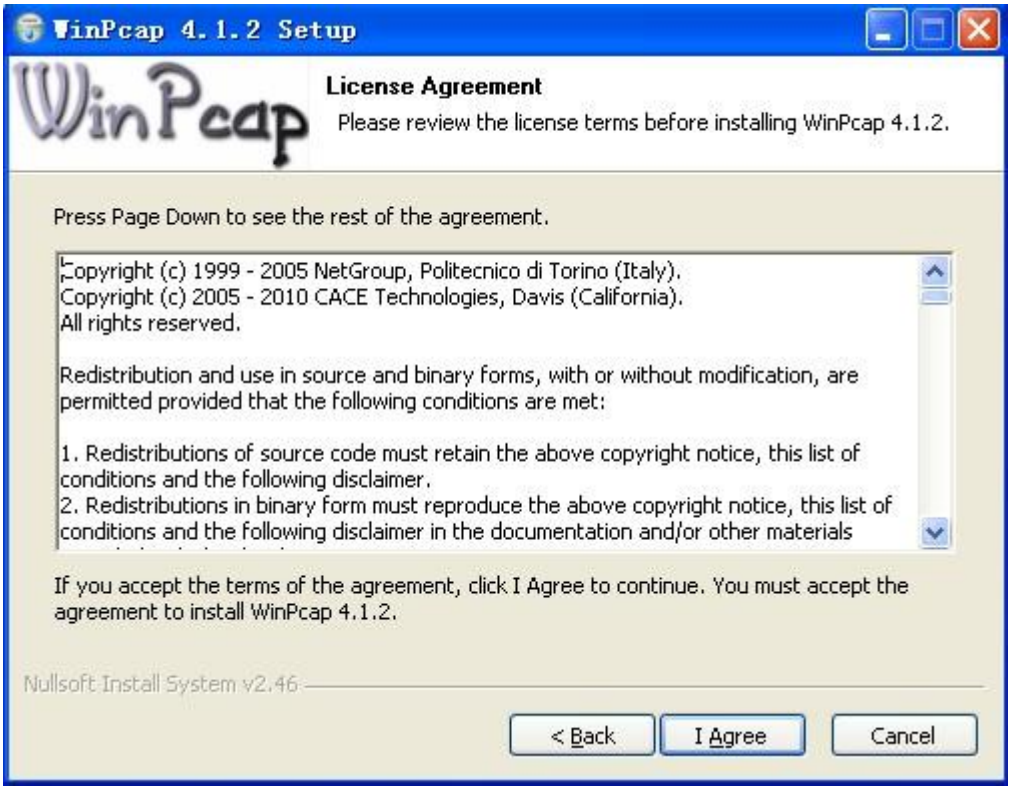


图 2-28 许可协议

（10）在系统引导时自动启动该插件，默认选择，点击“Install”，如图2-29 所示。

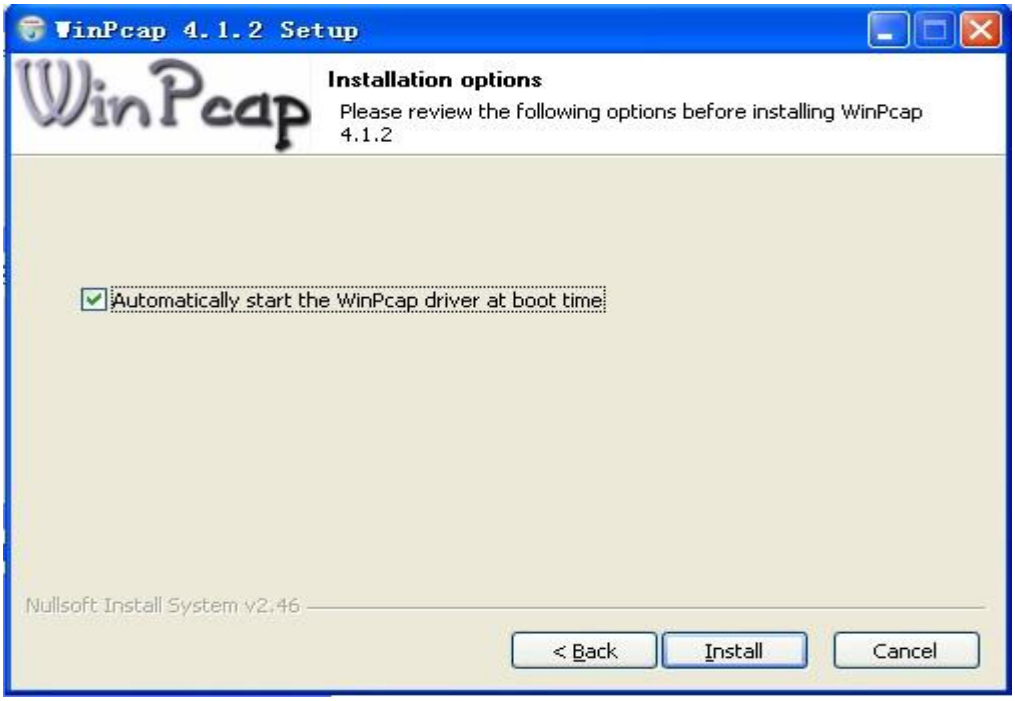


图 2-29 WinPcaP 的自动启动

（11）经过了那么多步，终于到尽头了。直接点“Finish”，结束 WinPcaP 的安装。

图 2-30 WinPcaP 安装结束

（12）插件安装完了，点击下一步，如图 2-31 所示。

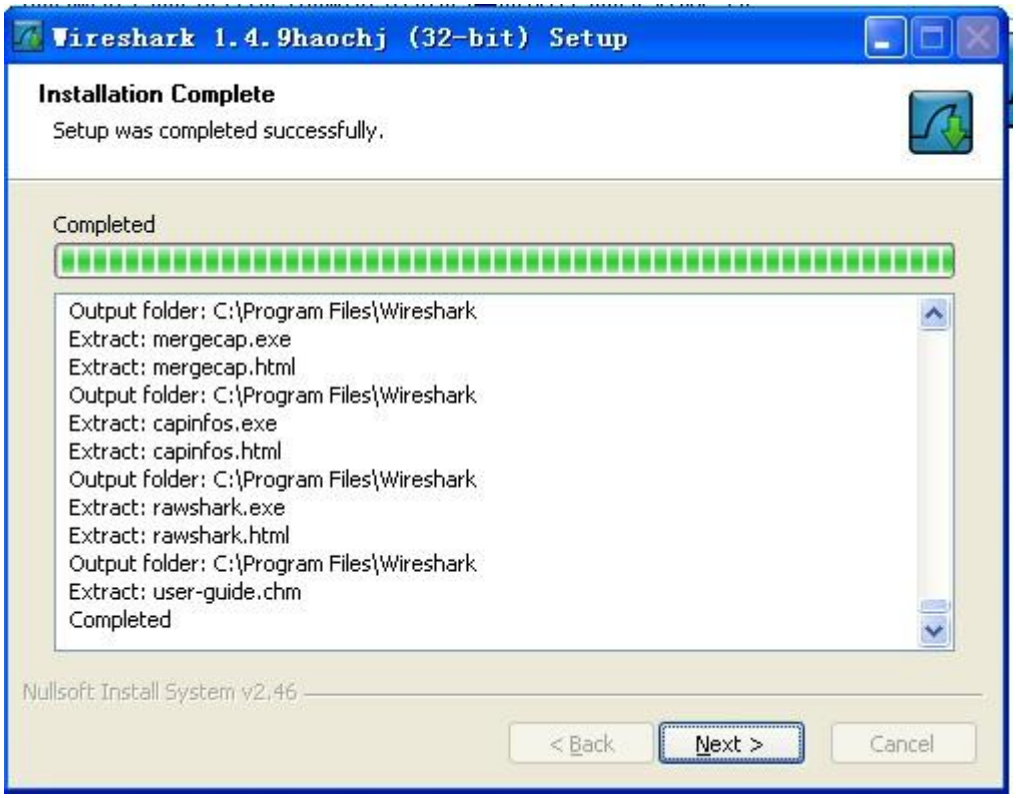


图 2-31 Wireshark 安装结束

（13）Wireshark 安装的最后一步，勾选“Run Wireshark……”，点击“Finish”

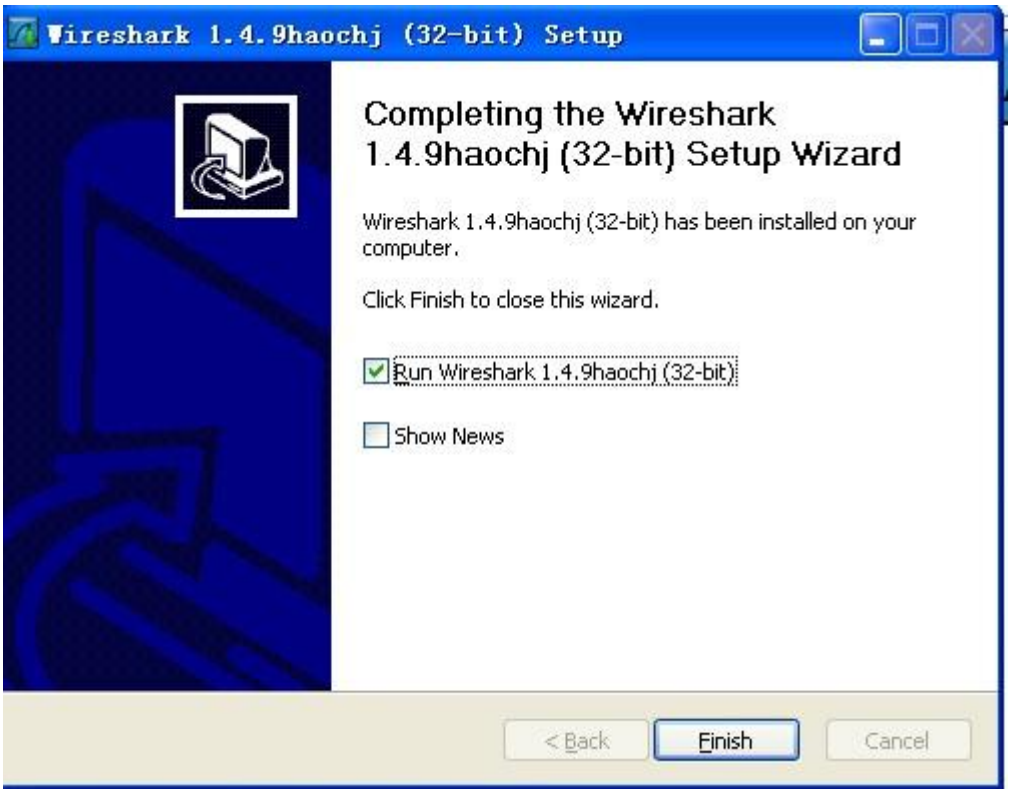


图 2-32 Wireshark 成功安装

2、Wireshark 的基本操作

（1）在 ip 为 192.168.0.4 的虚拟主机上双击安装好的 Wireshark 可执行文件“Wireshake.exe”，弹出 Wireshark 操作界面。

（2）在菜单栏点击“抓包”，在选项中单击“抓包参数选择”。如图 2-33 所示。

图 2-33 选择抓包参数选择

（3）在这里可以看到，有两块活动网卡，因为后面要利用选择的网卡来作为发送和接收分组的网络接口。所以桥接类型连接的网卡便是我们最佳选择。

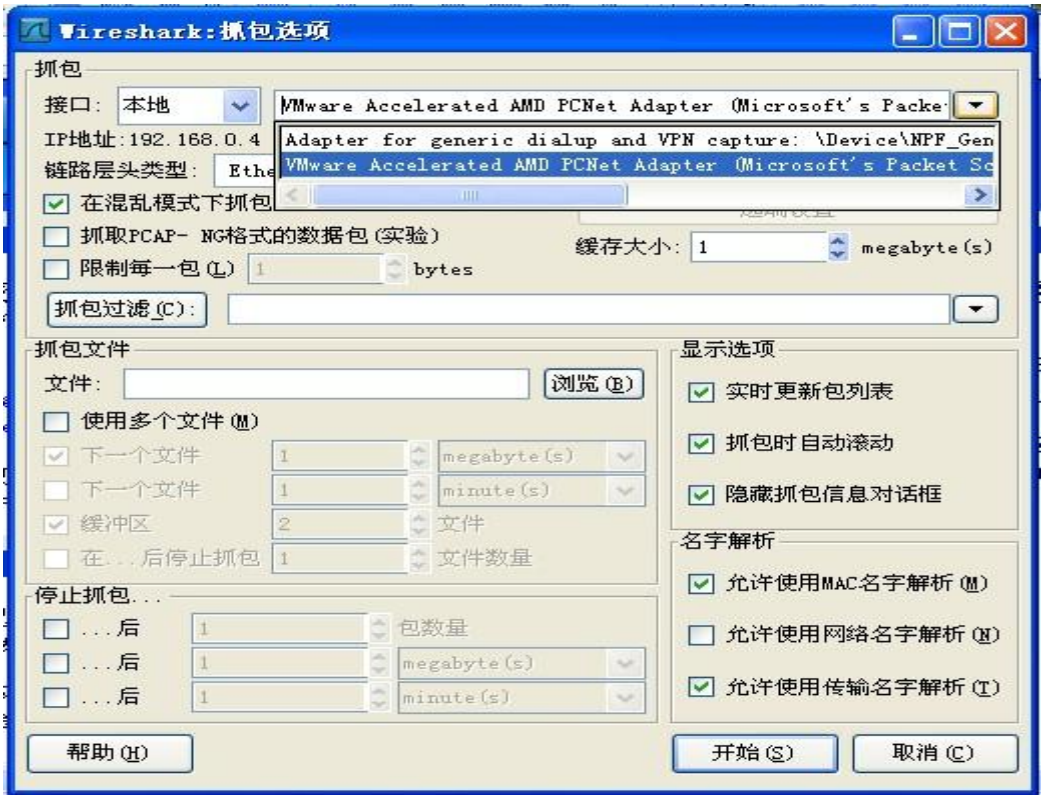


图 2-34 监听网卡选择

我们在物理主机的命令提示符窗口中“ping 192。168.0.4”，当 ping 结束后,点击工具栏中的第四个按钮，结束正在运行的抓包,如图 2-35 所示。

图 2-35 输入过滤条件

(4)先来测试一下软件是否能正常运行，在抓包过滤条件中输入 icmp，点击右下角的“开始”，如下图所示。

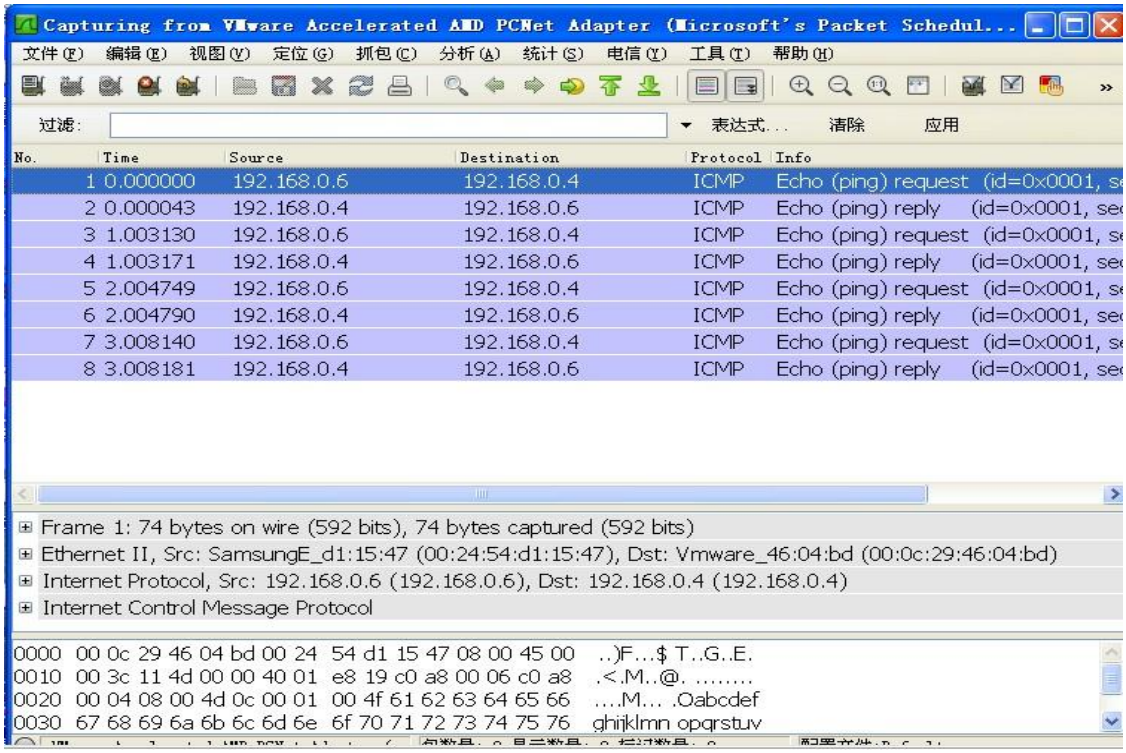


图 2-36 针对 icmp 的抓包

我们在物理主机的命令提示符窗口中“ping 192。168.0.4”，当 ping 结束后,点击工具栏中的第四个按钮，结束正在运行的抓包,如图 2-37 所示。

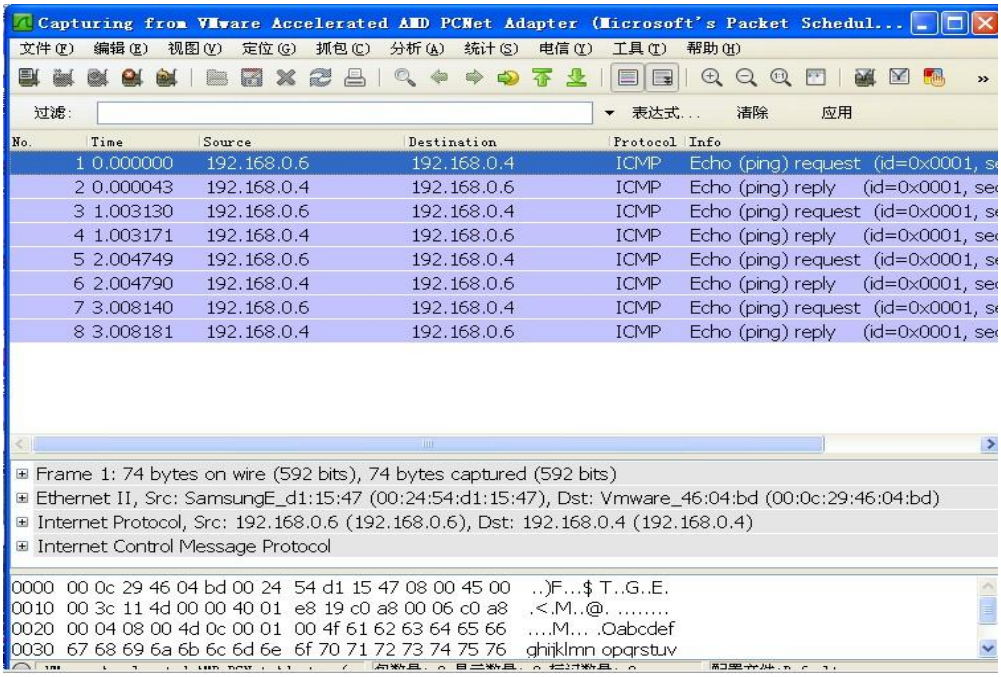


图 2-37 针对 icmp 的抓包

从图中可以看到，当 ping 命令结束时，一共抓到 8 个数据包，单数都是物理主机发送向虚拟机主机的的 ICMP Echo Request 包，双数是由虚拟主机发向物理主机的 ICMP Echo Reply 包，是对前者的数据包的响应。

（5）更改过滤条件，输入如图所示的的条件进行点击“开始”进行抓包，

图 2-38 抓获网络浏览的报文

打开浏览器，访问 www.baidu.com,软件就开始抓包，下图就是一段时间后抓的包。

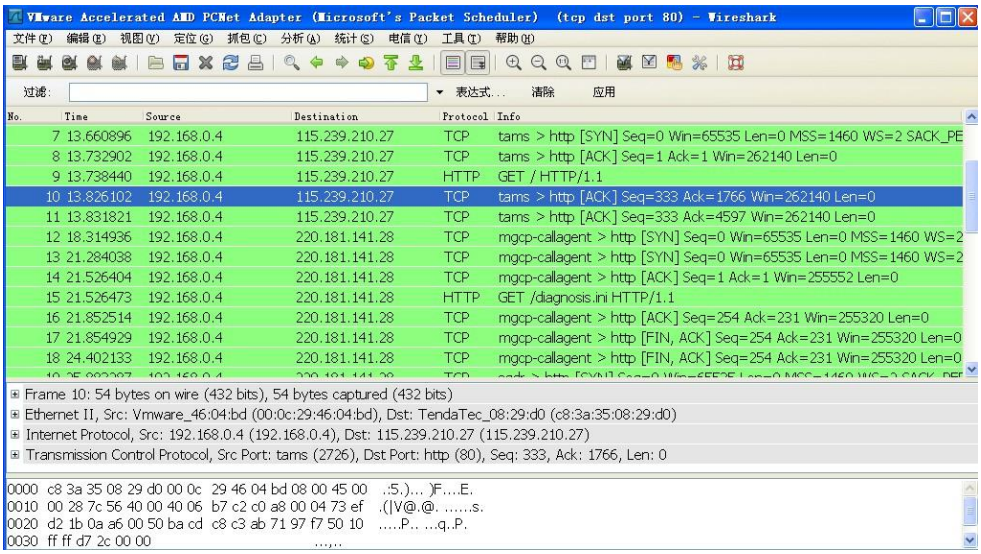


图 2-39 浏览 WEB 抓到的包

从数据包列表中可以看到，从虚拟机主机访问的目标地址不止一个，而在不同的时间使用的协议也不相同。

虚拟主机要和百度上的服务器连接，虚拟主机就要先发送一个 SYN 标记的包，告诉服务器建立连接（如数据包 7）。服务器端收到 SYN 标记的数据包后，就会发一个对 SYN 包的确认包 ACK 给客户机（即虚拟主机）表示对第一个 SYN 包的确认，并继续握手操作（如数据包 8）。虚机主机收到 ACK 标记的确认包，又发送一个 ACK 标记的确认包给服务器，通知 A 连接已建立（如数据包 10），通过三次握手，一个 TCP 连接完成。

而绿色部分下面的窗口表示的是选定的某个数据包的层次结构和协议分析。最下面窗口是数据包的 16 进制数据的具体内容，也即是数据包在物理层上传递的数据。

3、在数据包中单词代表的意思

No.列标识出 Ethereal 捕获的数据包序号

Time 表示在什么时间捕获到该数据包

Source 和 Destination 标识出数据包的源地址和目的地址

Protol 表明该数据包使用的协议

Info 是在列表中大概列出该数据包的信息

Frame 代表数据帧

4、常用的过滤条件

a. ether host 00:e5:g9:00:00:03

捕获 MAC 地址为 00:e5:g9:00:00:03 网络设备通信的所有报文

b. host 192.168.11.22

捕获 IP 地址为 192.168.11.22 网络设备通信的所有报文

c. tcp port 80

捕获网络 web 浏览的所有报文

d. host 192.168.0.8 and not tcp port 80

捕获 192.168.0.8 除了 http 外的所有通信数据报文

e. tcp

捕获所有 TCP 协议的数据包

f. tcp port 23

捕获 TCP 端口号是 23 的数据包，不管是源端口还是目的端口

……

2.2.3 总结

通过本实验，掌握 Wieshark 的基本配置和使用方法，同时也对数据传输的过程和协议有了更深的了解。比如建立连接要通过三次握手，软件和网站使用的协议也各不相同。

Wieshark 是我们学习和了解网络的有用的软件之一，特别是用用来分析数据包。在本次试验过程有遇到过问题也有收获经验：使用 wireshark 时，通过精确定位过滤来捕获自己想要的包，这样捕获的包比较直观有用且数据包较小。为了大量数据包对笔记本网卡冲太大导致死机可以在抓包时注意及时的点击关闭正在进行的抓包。

2.3 拒绝服务攻击演示实验

2.3.1 拒绝服务攻击

拒绝服务攻击即攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一。其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。拒绝服务攻击问题也一直得不到合理的解决，究其原因是因为这是由于网络协议本身的安全缺陷造成的，从而拒绝服务攻击也成为了攻击者的终极手法。攻击者进行拒绝服务攻击，实际上让服务器实现两种效果：一是迫使服务器的缓冲区满，不接收新的请求；二是使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接

拒绝服务攻击使系统瘫痪，或明显的降低系统的性能，因为过量使用资源而致使其他合法用户无法 访问。大部分操作系统、路由器和网络组件都容易受 DoS 攻击。SYN Flood 是当前最流行的 DoS（拒绝 服务攻击）与 DDoS（分布式拒绝服务攻击）的方式之一，这是一种利用 TCP 协议缺陷，发送大量伪造 的 TCP 连接请求，从而使得被攻击方资源耗尽（CPU 满负荷或内存不足）的攻击方式。 介绍这种攻击的基本原理要从 TCP 连接建立的过程开始。建立 TCP 连接的标准过程是这样的： 首先，请求端（客户端）发送一个包含 SYN 标志的 TCP 分组，此同步报文会指明客户端使用的端口以及 TCP 连接的初始序号；第二步，服务器在收到客户端的 SYN 分组后，将返回一个 SYN/ACK 分组， 表示客户端的请求被接受。第三步，客户端也返回一个确认分组 ACK 给服务器端，到此一个 TCP 连接 完成。以上的连接过程在 TCP 协议中被称为三次握手（Three-way Handshake）。问题就出在 TCP 连接 的三次握手中，假设一个用户向服务器发送了 SYN 分组后突然死机或掉线，那么服务器在发出 SYN/ACK 应答后是无法收到客户端的 ACK 分组的（第三次握手无法完成），这种情况被称为半开 TCP 连接状态。此时服务器端一般会重试（再次发送 SYN/ACK 给客户端）并等待一段时间后丢弃这个半开 TCP 连接，这段时间的长度我们称 SYNTimeout，一般来说这个时间是分钟的数量级（大约为 30 秒-2 分 钟）；一个用户出现异常导致服务器的一个线程等待 1 分钟并不是什么很大的问题，但如果有一个恶意 的攻击者大量模拟这种情

况，服务器端将为了维护一个非常大的半开连接列表而消耗非常多的资源——数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断对这 个列表中的 IP 进行 SYN/ACK 的重试。实际上如果服务器的 TCP/IP 栈不够强大，最后的结果往往是堆 栈溢出崩溃。即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无 暇理睬客户的正常请求（毕竟客户端的正常请求比率非常之小），此时从正常客户的角度看来，服务器 失去响应，这种情况我们称作：服务器端受到了 SYN Flood 攻击。

2.3.2 拒绝服务攻击演示实验

一．实验目的：

学习 DoS（Denial of Service）攻击的基本概念理解拒绝服务攻击原理，掌握一种利用该原理攻击 Web 服务器的程序设计方法

二．实验内容： 1．拟定网站攻击方案 2．编写一个程序，完成以下功能：创建操作窗口，显示窗口 确定 WWW 服务器的 IP 地址并显示在屏幕上 按方案对网站进行拒绝服务攻击 对攻击结果进行测试，将测试结果显示在屏幕上

三．实验器材（设备、元器件）： 个人计算机 、SYNflood 的相关工具，(如 syn.exe) 该工具具备有一定的危险性，建议在虚拟环境中演示。

【注意事项】 在虚拟机环境下进行，如配置虚拟机。在非生产网络下，关闭相关防火墙（如天网、系统自带防火墙） 两台机器一组，相互测试。

四．实验步骤

1、合作者甲： 登录到 Windows2000 server，打开命令行提示窗口，运新 netstat -a 命令，该命令显示了所有当前的连接，可以注意到 netstat -a 所返回的记录是比较少的，因为这时还没有开始 SYN Flood 攻击

2、合作者乙： 通过命令行，切换到 syn.exe，输入以下格式命令：C:\syn.exe 被攻击 IP 被攻击端口 源 Ip 源端口 发送的包数量 循环次数 间隔时间

3、合作者乙：输入命令后，攻击开始，按下 ctrl+C 可以停止攻击程序

4、合作者甲：再次运行 netstat -a 命令，查看遭受 SYNflood 攻击之后的

结果： 可以看到系统收到了大量的从某个 ip 和端口发出的 SYN 包，导致与系统的半开连接数量急剧上升，系统资源增加。

5、两人相互交换实验。

6、有条件的话，开启本机的防火墙软件，再次尝试 synflood 攻击，查看结果是否有所不同

实验数据及结果分析： 在受攻击的实验主机上安装了一个 Web 服务器 Apache 攻击前，用 IE 浏览器访问该 Web 服务器，可以正常访问 进行攻击时，再访问该 Web 服务器，已经不可以访问

模块三 数据加密技术

职业能力要求

正确分析实际使用中遇到的常用数据加密安全问题。

熟练使用常用的数据加密软件。

学习目标

- 掌握密码学的有关概念。
- 理解对称加密算法和公开密钥算法的基本思想以及两者的区别。
- 掌握 PGP 加密系统的工作原理、密码的生成和管理。

3.1 概述

3.1.1 密码学的概念

密码学是研究编制密码和破译密码的技术科学。研究密码变化的客观规律，应用于编制密码以保守通信秘密的，称为编码学；应用于破译密码以获取通信情报的，称为破译学，总称密码学。

密码学是研究如何隐密地传递信息的学科。在现代特别指对信息以及其传输的数学性研究，常被认为是数学和计算机科学的分支，和信息论也密切相关。著名的密码学者 Ron Rivest 解释道:“密码学是关于如何在敌人存在的环境中通讯”，自工程学的角度，这相当于密码学与纯数学的异同。密码学是信息安全等相关议题，如认证、访问控制的核心。密码学的首要目的是隐藏信息的涵义，并不是隐藏信息的存在。密码学也促进了计算机科学，特别是在于电脑与网络安全所使用的技术，如访问控制与信息的机密性。密码学已被应用在日常生活：包括自动柜员机的芯片卡、电脑使用者存取密码、电子商务等等。

3.1.2 密码学的发展

密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果，特别是

各国政府现用的密码编制及破译手段都具有高度的机密性。

进行明密变换的法则，称为密码的体制。指示这种变换的参数，称为密钥。它们是密码编制的重要组成部分。密码体制的基本类型可以分为四种：错乱－－按照规定的图形和线路，改变明文字母或数码等的位置成为密文；代替－－用一个或多个代替表将明文字母或数码等代替为密文；密本－－用预先编定的字母或数字密码组，代替一定的词组单词等变明文为密文；加乱－－用有限元素组成的一串序列作为乱数，按规定的算法，同明文序列相结合变成密文。以上四种密码体制，既可单独使用，也可混合使用 ，以编制出各种复杂度很高的实用密码。

20 世纪 70 年代以来，一些学者提出了公开密钥体制，即运用单向函数的数学原理，以实现加、脱密密钥的分离。加密密钥是公开的，脱密密钥是保密的。这种新的密码体制，引起了密码学界的广泛注意和探讨。

利用文字和密码的规律，在一定条件下，采取各种技术手段，通过对截取密文的分析，以求得明文，还原密码编制，即破译密码。破译不同强度的密码，对条件的要求也不相同，甚至很不相同。

3.2 加密、解密与数字签名

加密是通过特定算法和密钥，将明文（初始普通文本）转换为密文（密码文本）。解密是加密的相反过程，是使用密钥将密文恢复至明文。加密解密算法其实就是一种数学函数，用来完成加密和解密运算。而密钥是由数字、字符组成，用它来实现对明文的加密或对密文的解密。数字加密的安全性取决于加密算法的强度和密钥的保密性。加密的用途是保障隐私，避免资料外泄给第三方，即使对方取得该信息，也不能阅读已加密的资料。如图 3-1 所示。

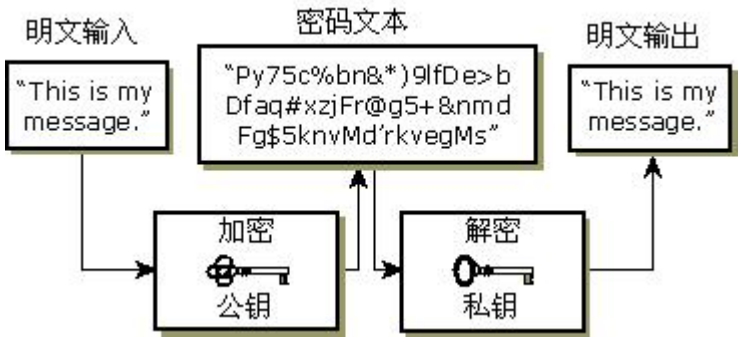


图 3-1 加密解密过程

在 OSI 参考模型中，除了会话层以外，其他各层均可以进行一定程度的加密，但习惯上通常在高层进行加密。加密有两种方式：传统加密和公开密钥加密。

3.2.1 传统加密

发送方和接收方用同一把密钥分别进行加密和解密的方式称为传统加密。传统加密也称作单密钥的对称加密。这种加密技术的优点是加密速度快、数学运算量小，但密钥的管理有一定的难度。如图 3-2 所示。

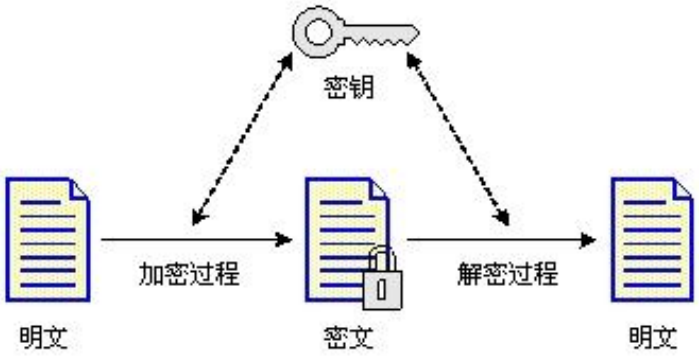


图 3-2 传统加密过程

传统加密可以大致分为字符级加密、比特级加密和 DES 等几种方式。

（1）字符级加密

字符级加密是以字符为加密对象。通常有替换密码和变位密码两种方式。在替换密码中，每个或每组字符由另一个或另一组伪装字符所替换。最古老的一种密码是凯撒密码，在这种方法中，每个字母将移动 4 个字符，例如将 a 替换为 E、将 b 替换为 F、将 z 替换为 D，4 就是这种加密算法的密钥，当然每次移动的字符可以随意。这种方法比较简单，很容易被破译。后来出现了一种单字符和多字符替换的改进算法，就是把明文中的一个或多个字符换成另一个或多个字符。替换密码会保持明文的字符顺序，只是将明文隐藏起来。而变位密码是对明文字符作重新排序，但不隐藏它们，变位密码要比替换密码更加安全一些。

（2）比特级加密

比特级加密是以比特为加密对象。首先将数据划分为比特块，然后通过编码/译码、替代、置换、乘积、异或、移位等数字运算方式进行加密。比特级加密采用的基本思想与字符级加密相同，仍为替换与变位。与字符级加密相比，比特级加密算法更复杂，一般较难破译。

（3）DES

典型的传统加密算法有 DES、DES3、RDES、IDEA、Safer、CAST-128 等，其中应用较为广泛的是美国数据加密标准 DES。DES 算法由 IBM 研制，广泛应用于许多需要安全加密的场合，如 Unix 的密码算法就是以 DES 算法为基础的。DES 是一种用 56 位密钥来加密 64 位数据的方法，综合运用了置换、代替、代数等多种加密技术，把明文分成 64 位比特的块，使用 64 位密钥（实际密钥长度为 56 位，另有 8 位的奇偶校验位），迭代深度达到 16。

3.2.2 公开密钥加密

如果在加密和解密时，发送方和接收方式使用的不是同一把密钥，而是相互关联的一对密钥，这种加密方式称之为公开密钥加密。公开密钥加密也称为双密钥的不对称加密，需要使用一对密钥，其中用来加密数据的密钥称为公钥，通常存储在密钥数据库中，供公共使用；用来解密的密钥称为私钥，私钥具有保密性。典型的公开密钥加密算法有 RSA、DSA、PGP 和 PEM 等，其中 PGP 和 PEM 广泛应用于电子邮件加密系统。如图 3-3 所示。

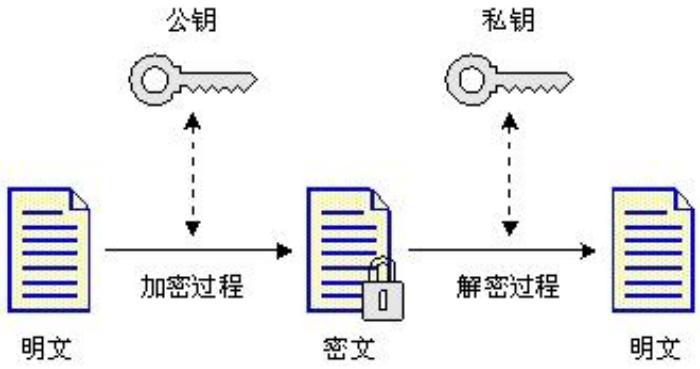


图 3-3 公开密钥加密解密过程

公开密钥加密算法应满足三点要求：

- 由已知的公钥 Kp 不可能推导出私钥 Ks 的体制。
- 发送方用公钥 Kp 对明文 P 加密后，在接收方能用私钥 Ks 解密，即可恢复出明文。可用 DKs（EKp（P））=P 表示，其中 E 表示加密算法，D 表示解密算法。
- 由一段明文不可能破译出密钥以及加密算法。

考虑网络环境下各种应用的具体要求以及算法的安全强度、密钥分配和加密的速度等方面的因素，通常是将传统密钥算法和公开密钥算法结合起来，这样可以充分发挥两种加密方法的优点，即公开密钥系统的高安全性和传统密钥系统的足够快的加解密速度。

3.2.3. 数字签名

使用公开密钥加密的最大好处在于公开密钥加密能够实现数字签名。数字签名是认证方法中的一种。认证就是验证数据发送方的身份，发送方用自己的私钥通过签名算法对原始信息进行数字签名运算，并将运算结果即数字签名一同发给接收方。接收方可以用发送方的公钥及收到的数字签名来校验收到的信息是否是由发送方发出，是否经过其他人的修改。

上述的数字签名方法是把整个明文都进行加密，在实际应用中由于加密很慢，所以经常希望能够发送签名的明文文件而不要求加密整个报文。现在经常使用一种叫做“报文摘要”的数字签名方法。这种方案基于单向散列函数的思想，该函数从一段很长的明文中计算出一个固定长度的比特串，通常使用哈希函数。哈希函数是一种单向的函数，即一个特定的输入将运算出一个与之对应的特定的输出，且无论输入信息的长短，都可以得到一个固定长度散列函数。这个固定长度的散列函数叫做报文摘要。这时明文和自身签名私钥加密的数字摘要组合成数字签名。如图 3-4 所示。

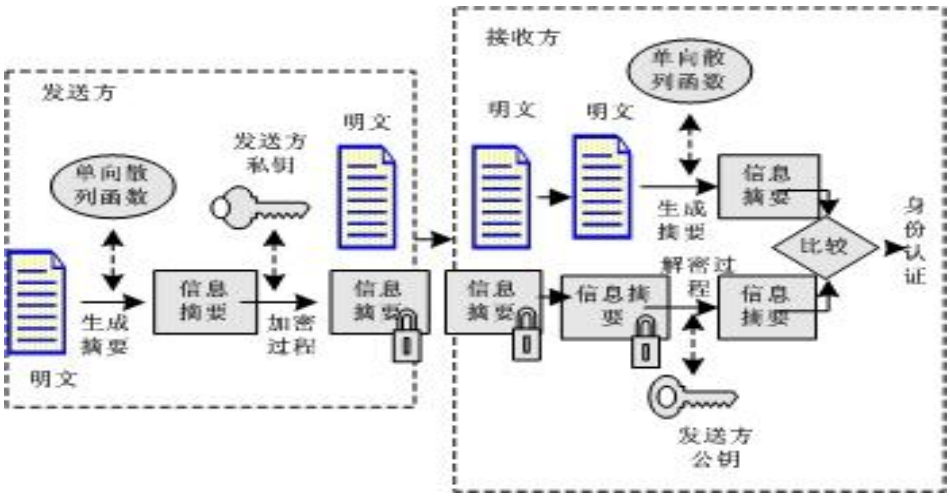


图 3-4 数字签名工作工程

3.3 PGP 加密工具的使用

3.3.1 PGP 加密和解密

PGP（Pretty Good Privacy）是一种在信息安全传输领域首选的加密软件，采用了非对称的“公钥”和“私钥”加密体系。由于美国对信息加密产品有严格的法律约束，因此限制了 PGP 的一些发展和普及，现在该软件的主要使用对象为情报机构、政府机构、信息安全工作者（例如较有水平的安全专家和有一定资历的黑客）。PGP 最初的设计主要是用于邮件加密，如今已经发展到了可以加密整个硬盘、分区、文件、文件夹、集成邮件软件进行邮件加密，甚至可以对 ICQ 的聊天信息实时加密。

1. PGP 相关的加密解密方法

PGP 是基于 RSA 公钥加密体系的，RSA 算法是一种基于大数不可能质因数分解假设的公钥体系。简单地说就是找两个很大的质数，一个公开即公钥，另一个不告诉任何人，即私钥，这两个密钥是互补的，就是说用公钥加密的密文可以用私钥解密，反过来也一样。

假设甲要寄信给乙，他们互相知道对方的公钥。甲就用乙的公钥加密邮件寄出，乙收到邮件后就可以用自己的私钥解密出甲的原文。由于没别人知道乙的私钥，所以即使是甲本人也无法解密那封信，这就解决了信件保密的问题。另一方面由于每个人都知道乙的公钥，他们都可以给乙发信，那么乙就无法确信是不是甲的来信。这时候就需要用数字签名来认证。

PGP 采用 MD5 单向散列算法，产生一个 128 位的二进制数作为“报文摘要”。甲用自己的私钥将 128 位的特征值加密，附加在邮件后，再用乙的公钥将整个邮件加密。当乙收到这份密文后，乙用自己的私钥将邮件解密，得到甲的原文和签名，乙的 PGP 也从原文计算出一个 128 位的特征值来和用甲的公钥解密签名所得到的数比较，如果符合就说明这份邮件确实是甲寄来的。这样两个安全性要求都得到了满足。

PGP 还可以只签名而不加密整个邮件，这适用于公开发表声明时，声明人为了证实自己的身份，可以用自己的私钥签名。这样就可以让收件人能确认发信人的身份，也可以防止发信人抵赖自己的声明。这一点在商业领域有很大的应用前

途，它可以防止发信人抵赖和信件被途中篡改。

2. PGP 相关的密钥管理机制

PGP 中的每个公钥和私钥都伴随着一个密钥证书。它一般包含以下内容：

密钥内容（用长达百位的大数字表示的密钥）；

密钥类型（表示该密钥为公钥还是私钥）；

密钥长度（密钥的长度，以二进制位表示）；

密钥编号（用以唯一标识该密钥）；

创建时间；

用户标识（密钥创建人的信息，如姓名、电子邮件等）；

密钥指纹（为 128 位的数字，是密钥内容的提要表示密钥唯一的特征）；

中介人签名（中介人的数字签名，声明该密钥及其所有者的真实性，包括中介人的密钥编号和标识信息）。

PGP 把公钥和私钥存放在密钥环（KEYR）文件中，PGP 提供有效的算法查找用户需要的密钥。

PGP 在很多地方需要用到口令，口令主要起到保护私钥的作用。由于私钥太长且无规律，所以难以记忆，PGP 把它用口令加密后存入密钥环，这样用户就可以用易记的口令间接使用私钥。PGP 的每个私钥都由一个相应的口令加密，需要用户输入口令的地方主要有：

需要解开受到的加密信息时，PGP 需要用户输入口令，取出私钥解密信息；

当用户需要为文件或信息签字时，用户输入口令，取出私钥加密；

对磁盘上的文件进行传统加密时，需要用户输入口令。

3.3.2 PGP 的使用

重启后，进入系统时会自动启动 PGPtray.exe，这个程序是用来控制和调用 PGP 的全部组件的，如果认为没有必要每次启动的时候都加载它，可以这样取消它的启动：“开始”→“程序”→“启动”，删除其快捷方式即可。

1. 创建和保存密钥对

（1）PGP 安装完成后，可以单击“开始”→“程序”→“PGP”→“PGPkeys”，弹出 PGP 密钥管理窗口。如图 3-5 所示。

图 3-5 密钥管理窗口

（2）单击工具栏最左边的“生成新密钥对”图标，弹出 PGP 密钥生成向导对话框。需要说明的是，在软件首次安装并注册完毕后，会直接产生密钥生成向导。如图 3-6 所示。

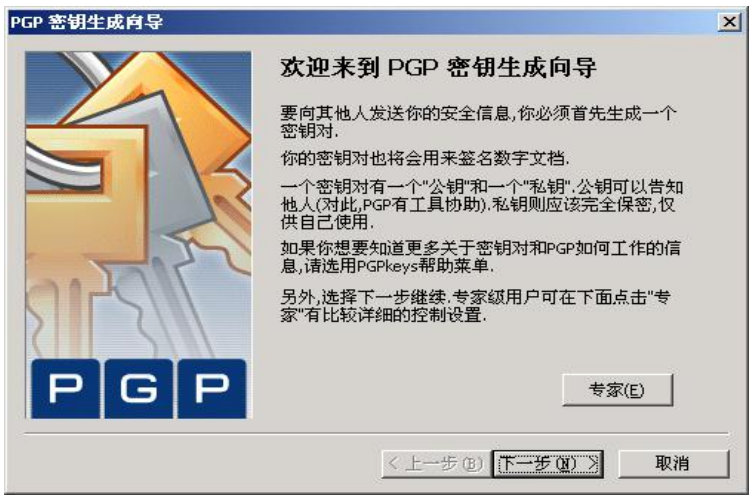


图 3-6 密钥生成向导

（3）单击“下一步”按钮，在分配姓名和电子信箱对话框中，填入用户名和邮件地址。如图 3-7 所示。

图 3-7 填写信息

（4）单击“下一步”按钮，输入保护私钥的 PIN 码，这样可以使私钥更加安全。为了更好的保护私钥，密码至少要输入 8 个字符，并且应该包含非字母字符。如图 3-8 所示。

图 3-8 输入私钥的 PIN 码

（5）单击“下一步”按钮，密钥开始生成。如图 3-9 所示。

（6）单击“下一步”按钮，PGP 密钥产生向导成功完成。如图 3-10 所

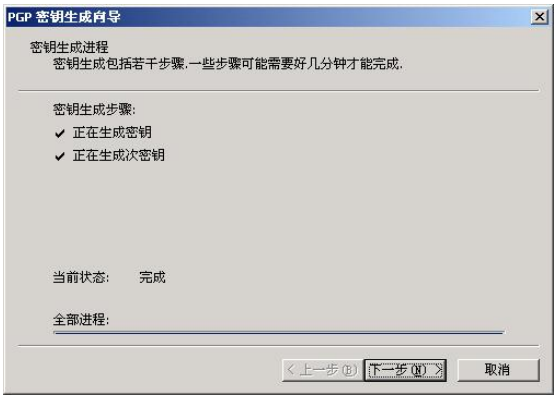


图 3-9 生成密钥

图 3-10 向导完成

（7）单击“完成”按钮，回到密钥管理窗口。如图 30-11 所示。

图 3-11 密钥管理窗口

（8）在关闭 PGP 密钥管理窗口时，系统弹出提示对话框，提示将密钥文件进行备份。如图 3-12 所示。

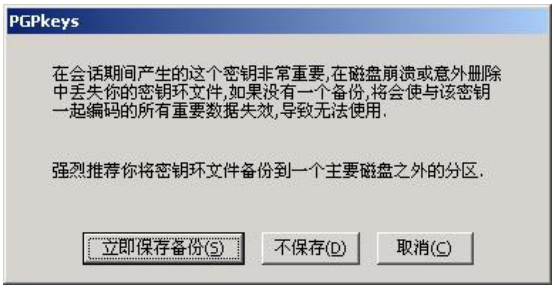


图 3-12 密钥备份

（9）单击“立即保存备份”按钮，首先保存公钥文件“pubring.pkr”。如图 3-13 所示。

图 3-13 保存公钥文件

（10）单击“保存”按钮，再保存私钥文件“secring.skr”。如图 3-14 所示。

图 3-14 保存私钥文件

2. 使用 PGP 加密解密文件

（1）使用 PGP 加密一个文件

打开资源管理器，找到要加密的文件，右击需要加密的文件名，在弹出的快捷菜单中选择“PGP” →“加密”项。如图 3-15 所示。

图 3-15 文件加密

在弹出的 PGP 外壳窗口中，确认加密文件阅读者，即接收人。如图 3-16 所示。

图 3-16 输入接收者

单击“确定”按钮，出现原文件的以“.pgp”为后缀名的加密文件。如图 3-17 所示。

图 3-17 加密文件

（2）使用 PGP 解密一个文件

当需要对 PGP 加密的文件进行解密时，双击该加密的文件，弹出一个对话框，需要输入用户私钥字段。如图 3-18 所示。

图 3-18 输入用户私钥

输入正确的口令后，单击“确定”按钮，开始文件解码，并弹出对话框，要求输入解密后的文件要存储的路径和文件名，输入后单击“保存”按钮，然后就可以打开保存后的已解密的文件了。如图 3-19 所示。

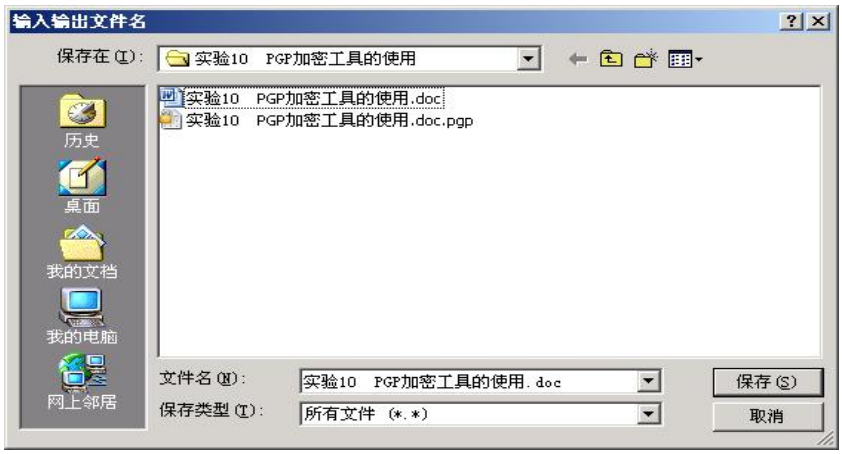


图 3-19 解密成功

（3）使用 PGP 销毁加密文件

右击要销毁的加密文件，在弹出的快捷菜单中选择“PGP”→“粉碎”项，弹出安全删除加密文件确认对话框，单击“是”按钮，销毁加密文件。如图 3-20 所示。

图 3-20 销毁文件

3. 使用 PGP 进行签名和验证

（1）使用 PGP 对一个文件进行签名

打开资源管理器，选择一个需要签名的文件，右击弹出快捷菜单，打开 PGP 菜单项的子菜单，选择“签名”项，先弹出 PGP Shell 密钥选择对话框，确认加密文件阅读者即接收人，单击“确定”按钮后，弹出 PGP Shell 输入密码对话框，用户可以在签名密钥文本框选择签名人，因为签名要使用签名人的私钥，所以需要在为以上密钥输入密码文本框中，输入保护私钥的口令。如图 3-21 所示。

图 3-21 签名输入私钥

单击“OK”按钮，在资源管理器中出现后缀为“.sig”的签名文件。如图3-22所示。

图 3-22 生成签名文件

（2）使用PGP对一个文件进行验证

右击已签名的文件，在弹出的快捷菜单中选择“PGP”→“校验签名”项，即可核对签名人的身份。如图3-23所示。

图 3-23 校验签名

（3）测试修改签名文件

修改文件名，然后双击签名文件，会弹出选择被签名的文件。找到被签名的文件，单击“打开”按钮，会显示签名错误。如图3-24所示。

图 3-24 测试校验签名文件

从以上操作可知，对文件进行签名，可以表示签名人对该文件的真实性和完整性负责。

4. 使用PGP加解密一封邮件

（1）使用PGP加密一封邮件

使用Microsoft Outlook写一封邮件。如图3-25所示。

图 3-25 Outlook 写信

先选中邮件内容，选择复制，然后，右击系统托盘中的“PGPtray”图标，在快捷菜单中选择“剪贴板”→“加密”，对邮件进行加密。弹出公钥选择对话框。如图 3-26 所示。

图 3-26 公钥选择

PGP 开始加密剪贴板中的内容，加密完毕后，在 Microsoft Outlook 邮件内容处，粘贴剪贴板中加密过的内容，将该邮件发出。如图 3-27 所示。

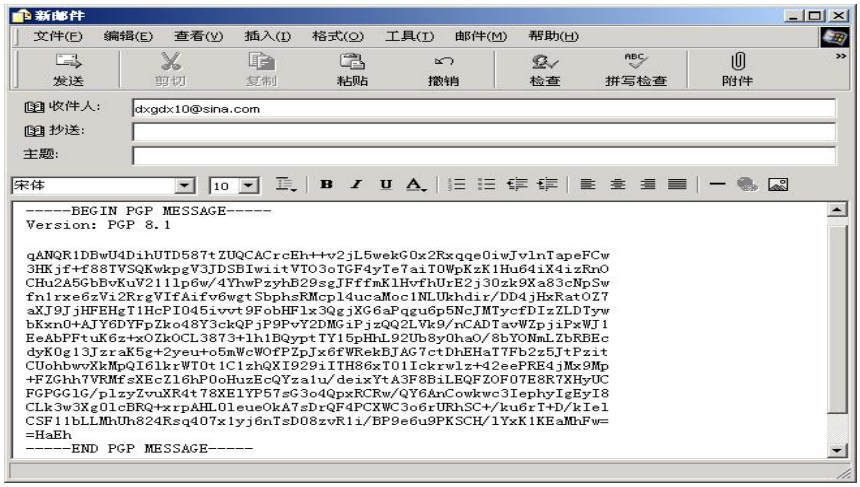


图 3-27 发出加密文件

（2）使用 PGP 解密一封邮件

对方收到经过 PGP 加密的邮件，先选中邮件文本中“-----BEGIN PGP MESSAGE-----”到“-----END PGP MESSAGE-----”的内容，选择复制，然后，右击系统托盘中的“PGPtray”图标，在快捷菜单中选择“剪贴板”→“解密&校验”，对邮件进行解密，此时弹出输入私钥密码窗口。如图 3-28 所示。

图 3-28 输入解密私钥

解密成功，如图 3-29 所示。

图 3-29 解密成功

5.练习：

在你的计算机上构建 FTP 服务器，在 FTP 服务器上共享一个 Word 文档，要求和你同网段的计算机都可以访问该 FTP 服务器并下载该 word 文档，但只有某个确定的用户才能正确读取该文档中的内容。验证你的设置。

在你的计算机上构建 FTP 服务器，在 FTP 服务器上共享一个 Word 文档，要求所有用户都可以访问该 FTP 服务器并下载该 word 文档，并确保该文档在共享和传输过程中不会被篡改。验证你的设置。

使用 Foxmail Server 在你的计算机上搭建邮件服务器，在另外两台计算机上分别向该邮件服务器申请帐户，要求 2 个帐户在另外两台计算机上只能使用 Outlook Express 相互收发邮件，并保证邮件的内容不会被其他人窃取。验证你的设置。

模块四 操作系统安全

职业能力要求

熟练使用 Windows 系统平台下各种应用系统。

能根据实际需要正确地进行 Windows 操作系统的安全设置。

掌握虚拟机内 windows 系统的安装与使用。

学习目标

- 操作系统的用户安全设置
- 操作系统的密码安全设置
- 操作系统的系统安全设置
- 操作系统的服务安全设置
- 操作系统的注册表安全设置

4.1 操作系统的安全问题

操作系统是计算机资源的直接管理者，它和硬件打交道并为用户提供接口，是计算机 软件的基础和核心。在网络环境中，网络的安全很大程度上依赖于网络操作系统的安全性。没有网络操作系统的安全性，就没有主机系统和网络系统的安全性。因此操作系统的安全是整个计算机系统安全的基础，其安全问题日益引起人们的高度重视。作为用户使用计算机和网络资源的中间界面，操作系统发挥着重要的作用。因此，操作系统本身的安全就成了安全防护的头等大事。操作系统安全防护研究通常包括以下几方面内容。

(1).操作系统本身提供的安全功能和安全服务，现代的操作系统本身往往要提供一定 的访问控制、认证与授权等方面的安全服务，如何对操作系统本身的安全性能进行研究和 开发使之符合选定的环境和需求。

(2).对各种常见的操作系统，采取什么样的配置措施使之能够正确应付各种入侵。

(3).如何保证操作系统本身所提供的网络服务得到安全配置。

4.1.1 操作系统安全概念

一般意义上，如果说一个计算机系统是安全的，那么是指该系统能够控制外部对系统 信息的访问。也就是说，只有经过授权的用户或代表该用户运行的进程才能读、写、创建 或删除信息。

操作系统内的活动都可以认为是主体对计算机系统内部所有客体的一系列操作。操作 系统中任何存有数据的东西都是客体，包括文件程序、内存、目录、队列、管道、进程间 报文、I/O 设备和物理介质等。能访问或使用客体活动的实体称为主体，一般说，用户或者 代表用户进行操作的进程都是主体。主体对客体的访问策略是通过可信计算基(TCB)来实现 的。可信计算基是系统安全的基础，正是基于该 TCB，通过安全策略的实施控制主体对空 体的存取，达到对客体的保护。

安全策略描述的是人们如何存取文件或其他信息。当安全策略被抽象成安全模型后， 人们可以通过形式货摊方法证明该模型是安全的。被证明了的模型成为人们设计系统安全 部分的坐标。安全模型精确定义了安全状态的概念访问的基本模型和保证主体对客体访问 的特殊规则。

一般所说的操作系统的安全通常包含两方面意思：一方面是操作系统在设计时通过权限访问控制、信息加密性保护、完整性鉴定等机制实现的安全；另一方面则是操作系统在使用中，通过一系列的配置，保证操作系统避免由于实现时的缺陷或是应用环境因素产生的不安全因素。只有在这两方面同时努力，才能够大可能地建立安全的操作系统。

4.1.2 计算机操作系统安全评估

计算机系统安全性评估标准是一种技术性法规。在信息安全这一特殊领域，如果没有这一标准，那么与此相关的立法、执法就会有失偏颇，终会给国家的信息安全带来严重 后果。由于信息安全产品和系统的安全评价事关国家的安全利益，因此许多国家都在充分 借鉴国际标准的前提下，积极制定本国的计算机安全评价认证标准。

美国可信计算机安全评估标准(TCSEC)是计算机系统安全评估的第一个正式

标准，具 有划时代的意义。TCSEC 将计算机系统的安全划分为 4 个等级、8 个级别。这里仅给出等级划分的基本特征以满足本章后续内容之需要。

(1) D 类安全等级：D 类安全等级只包括 D1 一个安全类别，安全等级 低。D1 系统只为文件和用户提供安全保护。 普通的形式是本地操作系统，或者是一个完全没有保护的网络。

(2) C 类安全等级：该类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C4 两类。C1 系统通过将用户和数据分开来达到安全的目的。C4 系统比 C1 系统加强了可调的审慎控制。在连接到网络上时，C4 系统的用户分别对各自的行为负责，通过登录过程、安全事件和资源隔离来增强这种控制。

(3) B 类安全等级：B 类安全等级分为 B1、B4、B3 三类。B 类系统具有强制性保护功能，强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。

(4) A 类安全等级：A 系统的安全级别 高。目前 A 类安全等级只包含 A1 一个安全类 别。其显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析 后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足：系统管理员必 须从开发者那里接收到一个安全策略的正式模型；所有的安装操作都必须由系统管理员进 行；系统管理员进行的每一步安装操作都必须有正式文档。

4.1.3 国内的安全操作系统评估

为了适应信息安全发展的需要，借鉴国际上的一系列有关标准,我国也制定了计算机信息系统等级划分准则。我国将操作系统分成 5 个级别，分别是用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级。

1.自主访问控制

计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制 (如访问控制列表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息，并控制访问权限扩散。自主访问

控制机制根据用户指定的用户只 允许由授权用户指定对客体的访问权。

2.身份鉴别

计算机信息系统可信计算基初始执行时，首先要求用户标识自己的身份，并使用保护 机制(如口令)来鉴别用户的身份；阻止非授权用户访问用户身份鉴别数据。通过为用户提 供唯一标识，计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统 可信基还具备将身份标识与该用户所有可审计行为相关联的能力。

3.数据完整性

计算机信息系统可信计算基通过自主和强制完整性策略，阻止非授权用户修改或破坏 敏感信息。在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

4.客体重用

在计算机输出信息系统可信计算基的空闲存储客体空间中，对客体初始指定、分配再分配一个主体之前，撤销该客体所含信息的所有授权。当主体获得对一个已释放的客体的 访问权时，当前主体不能获得原主体活动所产生的任何信息。

5.审计

计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它的访问或破坏活动。可信计算基能记录在案下述事件：使用身份鉴别机制；将客体引入用户地址空间(如打开文件、程序初始化)；删除客体；由操作员、系统管理员或(和)系统安全管理员实施的动作以及其他与系统安全有关的事件。对于每一事件，其审计记录包括：事件的日期和时间、用户事件类型、事件是否成功。对于身份鉴别事件，审计记录包含来源(如终端标识符)；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名。对不能由计算机信息系统可信计算基独立辨别的审计事件，审计机 制提供审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算 基独立分辨的审计记录。

6.强制访问控制

计算机信息系统可信计算基对所有主体及其所控制的客体(例如，进程、文件、段、设备)实施强制访问控制，为这些主体及客体指定敏感标记，这些标记

是等级分类和非等级类 别的组合，它们是实施强制访问控制的事实依据。计算机信息系统可信计算基支持两种或 两种以上成分组成的安全级。计算机信息系统可信计算基控制的所有主体对客体的访问应 满足：仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类，且主体安全级 非等级类别包含了客体安全级中的非等级类别，主体才能写一个客体。计算机信息系统可信计算基使用身份和鉴别数据，鉴别用户的身份，并保证用户创建的计算机信息系统可信 计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

7.标记

计算机信息系统可信计算基应维护与主体及其控制的存储客体(例如，进程、文件、段、 设备)相关的敏感标记，这些标记是实施强制访问的基础。为了输入未加安全标记的数据， 计算机信息系统可信基向授权用户要求并接受这些数据的安全级别，且可由计算机信息系 统可信计算基审计。

8.隐蔽信道分析

系统开发者应彻底隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道 的 大带宽。

9.可信路径

当连接用户时(例如，注册、更改主体安全级)，计算机信息系统可信计算基提供它与 用户之间的可信通道路径。可信路径上的通信能由该用户或计算机信息系统激活，且在逻 辑上与其他路径上的通信相隔离，并能正确地加以区分。

10.可信恢复

计算机信息系统可信计算基提供过程和机制，保证计算机信息系统失效或中断后，可 以进行不损害任何安全保护性能的恢复。

该规定中，级别从低到高，每一级都将实现上一级的所有功能，并且有所增加。第 1 级是用户自主保护级，在该级中，计算机信息系统可信计算基通过隔离用户与数据，使用户具备自主安全保护能力。通常所说的安全操作系统，其 低级别即是第 3 级，日常所见的操作系统，则以第 1 级和第 4 级为主。4 级以上的操作系统，与前 3 级有着很大的区别。4 级和 5 级操作系统必须建立于一个明确定义的形式化安全策略模型之上。此外，还需要考虑隐蔽通道。在第 4 级结构化保护级中，要求将第 3 级系统中的自主和强制访问控制扩展到所有主体与客体。

第 5 级访问验证保护级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问，访问监控器本身必须是抗篡改的、足够小且能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到小。支持安全管理员职能；提供审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。这种系统具有高的抗渗透能力。

4.1.4 操作系统的安全配置

操作系统安全配置主要是指操作系统访问控制权限的恰当设置、系统的及时更新以及 对于攻击的防范。所谓操作系统访问控制权限的恰当设置是指利用操作系统的访问控制功 能，为用户和文件系统建立恰当的访问权限控制。由于目前流行的操作系统绝大多数是用户自主级访问控制，因此对于用户和重要文件的访问权限控制是否得当，直接影响系统的安全稳定和信息的完整保密。不同的系统，其安全设置通常有所区别。

随着利用操作系统安全缺陷进行攻击的方法的不断出现，操作系统和 TCP/IP 缺陷逐渐 成为系统安全防护的一个重要内容。在不影响正常的系统功能和网络功能的基础上，进行 安全防范。

随时更新操作系统，是系统安全管理的一个重要方面。及时地更新系统，会使整个系 统的安全性能、稳定性能、易用性能得到大幅度提高。

4.1.5 操作系统的安全漏洞

可以说，几乎所有的操作系统都不是十全十美的，总存在安全漏洞。比如在 Windows NT 中，安全账户管理(SAM)数据库可以被以下用户复制：Administrator 账户、Administrator 组的所有成员、备份操作员、服务器操作员以及所有具有备份特权的人员。SAM 数据库的 一个备份拷贝能够被某些工具所利用来破解口令。

我们是否可以放心地使用 Windows XP? 微软在 Windows XP 的安全性方面做了许多工作，增加了许多新的安全功能，例如，Internet 连接防火墙，支持多用户的加密文件系统，改进的访问控制，对智能卡的支持等。Windows XP 到

底有多安全，它是否是一种安全的操作系统呢？Windows XP 提供了自主访问控制保护,并具有审计主体责任和它们的初始动作的能力。从操作系统的等级来看，Windows XP 仍然是 C 级操作系统，即是一个安全等级比较低的操作系统。

另一方面，操作系统作为软件存在的许多漏洞使黑客有机可乘。例如，Windows XP 发布后，与之有关的漏洞有：通用即插即用(UPnP)拒绝服务漏洞、GDI 拒绝服务漏洞、终 端服务 IP 地址欺骗漏洞。UPnP 拒绝服务漏洞的是这样的：UPnP 服务使计算机能够发现和 使用基本的网络设备。而 Windows Me 和 Windows XP 自带 UPnP 服务不能正确地处理某 种类型的无效请求，因此产生了一个安全漏洞。该漏洞含有一个内存泄漏问题，Windows XP 系统每次接收到这样的一个请求时，就会有一小部分系统内存无法使用，如果这种情况重 复发生，就会耗尽系统资源，使性能降低，甚至完全终止。

实际上，根据目前的软件设计水平和开发工具，要想绝对避免软件漏洞是不可能的。 操作系统作为一种系统软件，在设计和开发过程中造成这样或那样的缺陷，埋下一些隐患， 使黑客有机可乘，也可以理解。可以说，软件质量决定了软件的安全性。

4.2 操作系统安全配置实验

一、实验目的

1、掌握 Windows 系统的安全机制，了解安全策略的主要内容和用途，掌握操作系统安全策略的设置方法。

2、掌握 Windows 下审核策略的设置方法，了解审核策略的制定准则。掌握查看器查看审核日志和审核事件的一般方法。

3、了解 Windows 的 NTFS 文件系统提供的对本地文件的安全保护功能，掌握其使用方法。

二、实验环境

一台装有 Windows 2003 操作系统的计算机。

三、实验内容：

1、系统安全配置

2、系统安全审核

3、NTFS 文件系统安全应用

四、实验项目及步骤：

（一）系统安全配置实验

【实验原理】

操作系统的安全配置是整个操作系统安全策略的核心，其目的是从系统根源构成安全防护体系，通过用户和密码管理、共享设置、端口过滤、本地安全策略、外部工具使用等手段形成一套有效的系统安全策略。Windows 系统安装的默认配置是不安全的，因此，在系统投入使用之前，应该进行一些设置，以便使系统更安全。

通过本地安全策略可以控制：访问计算机的用户用户名；授权用户使用计算机上的哪些资源；是否在事件日志中记录用户或组的操作。其中与系统身份谁密切相关的密码策略用于管理域账户或本地用户账户。

【实验步骤】

（1）设置密码策略。在【本地安全策略】窗口中，选择【安设设置】|【账户策略】|【密码策略】，如图 4-1 所示。

图 4-1 本地安全策略

（2）设置密码复杂性。双击窗口右侧【密码必须符合复杂性要求】，弹出如图 4-2 所示对话框。

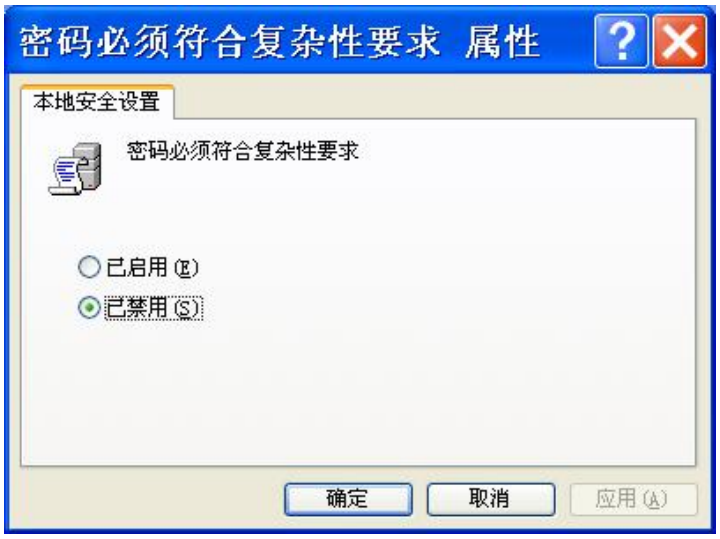


图 4-2 密码复杂性

对密码复杂性要求策略进行修改，该安全设置确定密码是否符合复杂性要求。如启用该策略，则密码必须符合以下最低要求：

不得明显包含用户账户名或用户全名的一部分；

长度至少为六个字符；

至少包含以下四种字符中的三种：英文大写字母(A~Z)；英文小写字母(a~z)；10 个基本数字（0~9)； 非字母字符（如，!$#%)。

密码策略设置后，在更改或创建密码时，会强制执行复杂性要求。

（3）修改密码长度。双击右侧【密码长度最小值】，弹出如图 4-3 所示对话框。

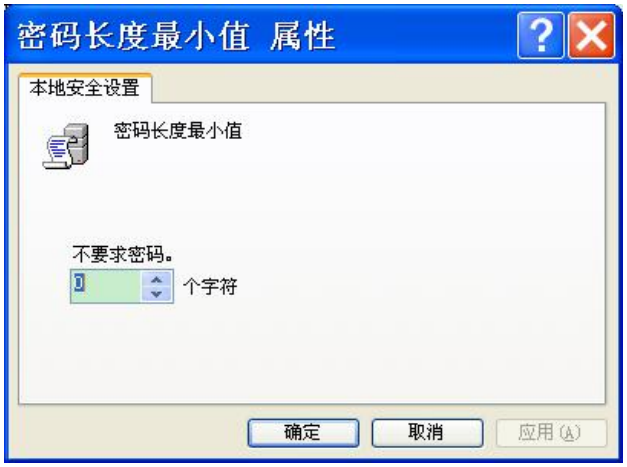


图 4-3 设置密码最小值

（4）修改密码最长存留期。双击右侧【密码最长存留期】，弹出如图 4-4 所示对话框。该安全设置确定系统要求用户更改密码之前可以使用该密码的时间。

可将密码的过程天数设置在 1~999 天之间，或将天数设置为为 0，可指定密码永不过期。如果密码最长使用期限在 1~999 之间，则密码最短使用期限必须小于密码最长使用期限。如果密码最长使用期限设置为 0，则密码最短使用期限可以是 1~998 天天之间的任何值。使用密码每隔 30~90 天过期一次是最佳安全操作。通过对密码的最长有效期进行修改，保证用户的密码到达有效期后必须更换密码。

图 4-4 密码最长存留期

（5）修改密码最短存留期限。方法同上。

（6）设置强制密码历史。双击右侧【强制密码历史】，弹出如图 4-5 所示对话框。为防止用户重新使用旧密码，该安全设置确定归纳法要个用户账户相关的密码的数量，该值必须为 0~24 之间的一个数值。该策略通过确保旧密码不能继续使用，从而能够增强安全性。

图 4-5 强制密码历史

（7）为域中所有用户使用可还原的加密来存储密码。双击右侧【为域中所有用户使用可还原的加密来存储密码】，弹出如图 4-6 所示对话框。该安全设置确定操作系统是否使用可还原的加密来存储密码。如果应用程序使用了要求知道用户密码才能进行身份验证的协议，则该策略可为它提供支持。

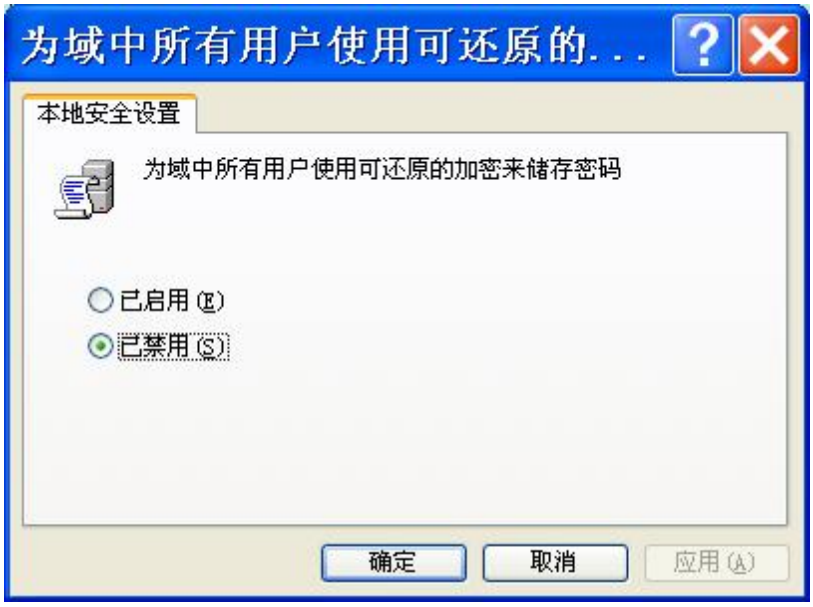


图 4-6 存储密码

（二）系统安全审核实验

【实验原理】

审核策略用于确定计算机的安全性事件日志记录了哪些安全事件。能够审核的事件类型包括：对文件和文件夹的访问、登录以及退出登录、关闭以及重新启动计算机、对用户和组的改动。对审核事件的成功或者事件的或者两者都审核。跟踪成功事件可以决定用户对特定文件或者打印机访问，能够利用该信息计划资源。跟踪失败事件以寻找可能出现的安全破坏。 安全审核的内容应该包括：

（1）审核账户登录事件。该审核用于确定是否对用户在计算机上登录或注销的每个实例进行审核。如果定义了该策略设置，则可指定是否审核成功、失败或根本不审核此事件类型。成功审核会在账户登录尝试成功时生成一个审核项，可用来确定哪个人成功登录到哪台计算机。失败审核会在账户登录尝试失败时生成一个审核项，该审核项对于入侵检测十分有用，但此设置可能导致拒绝服务状态，因为攻击者可以生成数百万次登录失败，并将安全事件日志填满。

（2）审核账户管理。该设置用于确定是否对计算机上的每个账户管理事件

进行审核。账户管理事件的示例包括：创建、修改或删除用户账户或组；重命名、禁用或启用用户账户；设置或修改密码。在响应安全事件时，组织可以对创建、更改或删除账户的人员进行跟踪，这一点非常重要。

（3）审核登录事件。该设置用于确定是否对用户在记录审核事件的计算机上登录、注销或建立网络连接的每个实例进行审核。账户登录事件是在账户所在的位置生成的，而登录事件是在登录尝试发生的位置生成的。成功审核会在账户登录尝试成功时生成一个审核项，该审核项的信息对于记账以及事件发生后的辩论十分有用，可用来确定哪个人成功登录到哪台计算机。失败审核会在账户登录尝试失败时生成一个审核项，该审核项对于入侵检测十分有用，但此设置可能会导致拒绝服务状态。

（4）审核策略更改。该设置用于确定是否对更改用户权限分配策略、审核策略或信任策略的每个事件进行审核。如果定义了此策略设置，则可指定是否审核成功、审核失败或根本不审核此事件类型。成功审核会在成功更改用户权限分配策略、审核策略或信任策略时生成一个审核项，该同的信息对于记账以及事件发生后的辩论十分有用，可用来确定谁在域或单个计算机上成功修改了策略。失败审核会在对用户权限分配策略、审核策略或信任策略的更改失败时生成一个审核项。

（5）审核特权使用。该审核设置用于确定是否对用户行使权限的每个实例进行审核。如果定义了此策略设置，则可指定是否审核成功、失败此事件类型。启用这些设置以后，生成的事件数量将十分庞大，并且验证以进行分类。只有在已经计划好如何使用所生成的信息时，才应启用这些设置。

（6）审核过程追踪。该审核设置用于确定是否审核事件的详细跟踪信息，如程序激活、进程退出、句柄复制和间接对象访问等。启用该审核将生成大量事件，因此通常都城将其设置为无审核。

（7）审核系统事件。该审核设置用于确定在用户重新启动或关闭计算机时，或者影响系统安全或安全事件发生时，是否进行审核。同时启用系统事件的失败审核和成功审核，也仅记录极少数事件，并且所有这些事件都非常重要，因此建议在组织中的所有计算机上启用这些设置。

审核的结果一般都保存到系统的日志中，可以使用事件查看器查看安全日志

文件的内容，以及在日志文件中特定的事件。事件查看器有三种日志可以查看，应用程序日志包括程序的错误、警告和信息；安全日志包括被审核事件的成功或者失败信息，这是设置审核策略的结果；系统日志包括 Windows 产生的错误、警告和信息。

【实验步骤】

1、设置审核策略。

（1）打开【本地安全设置】窗口。单击【控制面板】|【管理工具】|【本地安全策略】|【本地策略】|【审核策略】，弹出如图 4-7 所示的窗口。

图 4-7 本地安全设置

（2）设置相关策略。双击右侧相关的策略，在弹出的对话框中选中要设置的审核操作，如图 4-8 所示。然后单击【确定】按钮，完成设置。

图 4-8 设置相关策略

2、审核对特定文件或文件夹的访问。

（1）打开【属性】对话框。右击 Windows 文件夹，在弹出对话框中、选择【属性】，弹出【属性】对话框。

（2）单击【安全】选项卡，在弹出的对话框中单击【高级】按钮，在弹出的对话框中单【审核】|【添加】，弹出如图 4-9 所示对话框。

图 4-9 审核文件夹的访问

（3）在【输入要选择的对象名称】文本框中，输入要审核的用户账户名，然后单击【确定】，弹出如图 4-10 所示对话框。

图 4-10 输入对象名称

（3）对要审核的事件进行编辑。选中要审核的事件对应的复选框，定义完成后单击【确定】按钮。

3、使用事件查看器。

（1）打开【事件查看器】窗口。单击【开始】|【程序】|【管理工具】，单击【事件查看器】|【安全性】，弹出如图 4-11 所示的窗口。

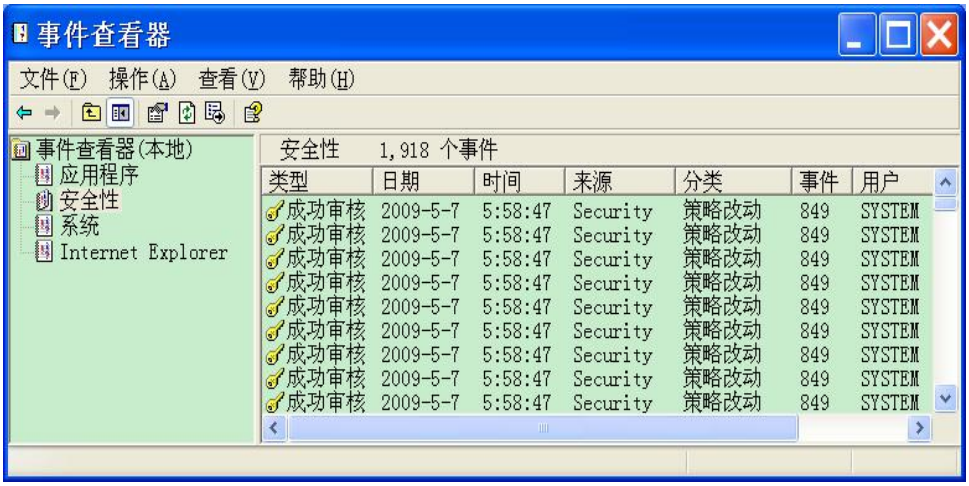


图 4-11 事件查看器

（2）查看日志的详细信息。双击相应的日志事件。

（3）查看并筛选事件。默认的事件查看器会显示所有的事件，为了更改日志中显示的内容，可以使用菜单【查看】|【筛选】命令来查找被审核的事件，或者使用菜单【查看】|【查找】命令来搜索特定的事件，如图 4-12 所示。

图 4-12 筛选事件

（三）NTFS 文件系统安全应用实验

【实验步骤】

1、数据保密性实验，设置只允许有访问权的用户打开设置属性的文件夹。

（1）以 administrator 账号登录到 Windows 2003 Server。

（2）建立文件夹。打开我的电脑，在 D 盘建立一个文件夹（如 user），在 user 中建立一个 user1 文件夹。为了保护这个文件夹不被其他用户使用，设置 user1 安全属性。

（3）设置访问权限。右击 user1，单击【属性】，在弹出的对话框中单击【安全】选项卡，如图 4-13 所示。

图 4-13 设置访问权限

单击【高级】，在弹出的对话框中取消【允许父项的继承权限传播到该对象和所有子对象，包括哪些在此明确定义的项目】复选框中的勾，弹出如图 4-14 所示对话框。输入本地主机的 IP 地址，输入远程电脑的 IP 地址。单击【下一步】

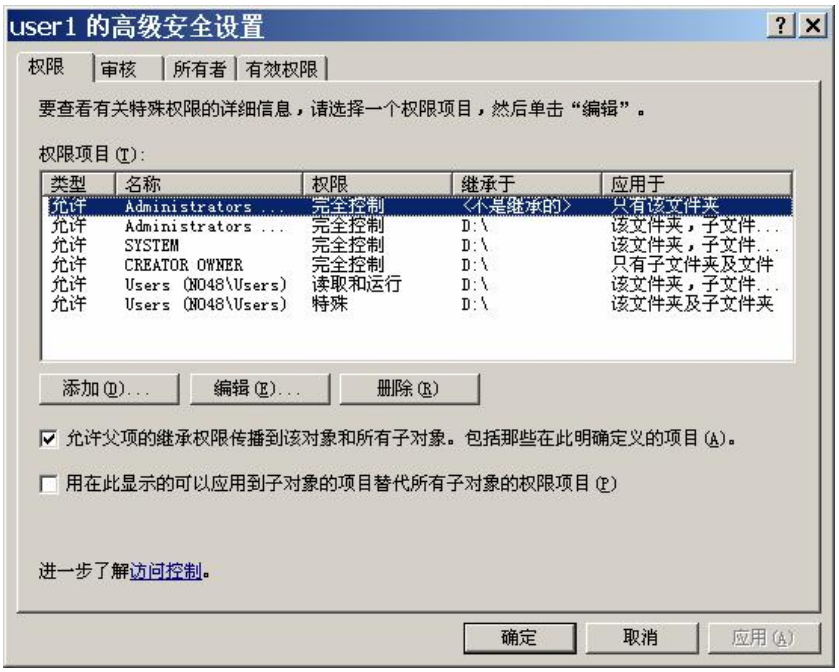


图 4-14 高级安全设置

单击【复制】按钮，返回【user1 的高级安全设置】对话框，单击【添加】按钮，弹出【选择用户或组】对话框。输入允许使用该文件夹的用户的用户名（如 zxl），如图 3-16 所示。

图 4-16 输入用户名

单击【确定】按钮，弹出【user1 的权限项目】对话框，单击【允许】列下的【完全控制】复选框，单击【确定】按钮。单击【允许】列下的【完全控制】复选框，单击【确定】按钮，关闭所有窗口。此时只允许 zxl 访问该文件夹。

（四）服务安全配置

【实验步骤】

（1） 关闭不必要的端口

关闭端口意味着减少功能，在安全和功能上面需要做一些抉择。如果服务器安装在防火墙的后面，风险就会少些。但是，永远不要认为你可以高枕无忧了。用端口扫描器扫描系统已开放的端口，确定系统开放的哪些服务可能引起黑客入侵。在系统目录中的 system32\drivers\etc\services 文件中有知名端口和服务的对照表可供参考， 如图 4-17 所示。

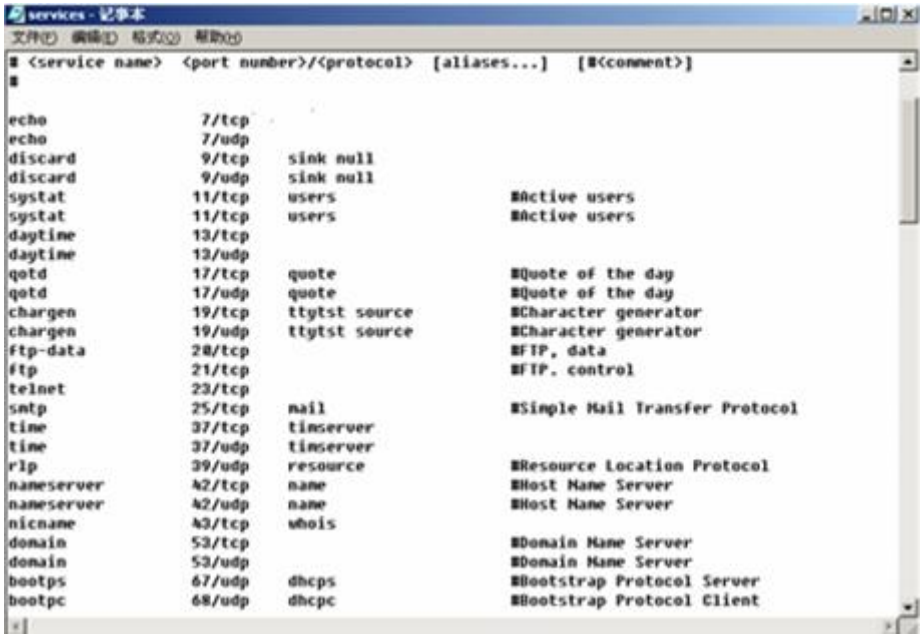


图 4-17 端口和服务对照表

具体方法为：右击“网上邻居”图标，执行“属性”命令，在出现的窗口中右击“本 地连接”执行“属性”命令，在弹出对话框中选中“Internet 协议(TCP/IP)”项，单击“属 性”按钮，再在弹出的对话框中单击“高级”按钮，弹出“高级 TCP/IP 设置”对话框，打 开“选项”选项卡选中“TCP/IP 筛选”项，单击“属性”按钮，弹出“TCP/IP 筛选”对话 框，添加需要的 TCP、UDP 协议即可，如图 4-18 所示。

设置完毕的端口界面如图 4-19 所示。

（2）设置安全记录的访问权限

安全记录在默认情况下是没有保护的，把它设置成只有 Administrator 和系统账户才有权访问，如图 4-20 所示。

图 4-18 设置 IP 的高级属性

图 4-19 设置 TCP/IP 筛选

图 4-20 设置安全记录的访问权限

（3）把敏感文件存放在另外的文件服务器中

虽然现在服务器的硬盘容量都很大，但是还是应该考虑是否有必要把一些重要的用户数据(文件、数据表、项目文件等)存放在另外一个安全的服务器中，并且经常备份。

4） 禁止建立空链接

默认情况下，任何用户都可通过空链接连上服务器，进而枚举出账号，猜测密码。可以通过修改注册表来禁止建立空链接：

即把 LOCAL_MACHINE\SYSTEM\CurrentControl Set\ Control\Lsa 下的 restrictanonymous 的值改成 1 即可，如图 4-21 所示。

此外，安全和应用在很多时候是矛盾的。因此，你需要在其中找到平衡点，如果安全 原则妨碍了系统应用，那么这个安全原则也不是一个好的原则。

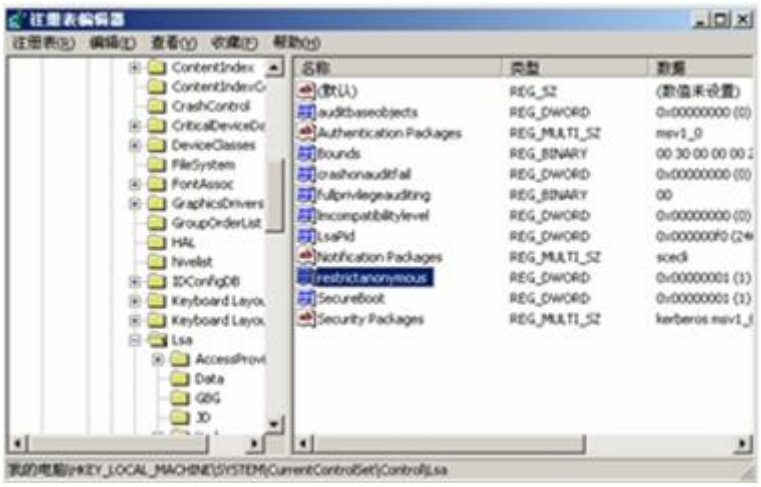


图 4-21 修改注册表

（5）关闭不必要的服务

Windows 2000 终端服务和 IIS 服务等都可能给系统带来漏洞。为了能够在远程方便地 管理服务器，很多计算机的终端服务都是开启的，如果开启了，要确认已经正确配置了终 端服务。有些恶意的程序也能以服务方式悄悄地运行服务器上的终端服务。要留意服务上 开启的所有服务并每天检查。

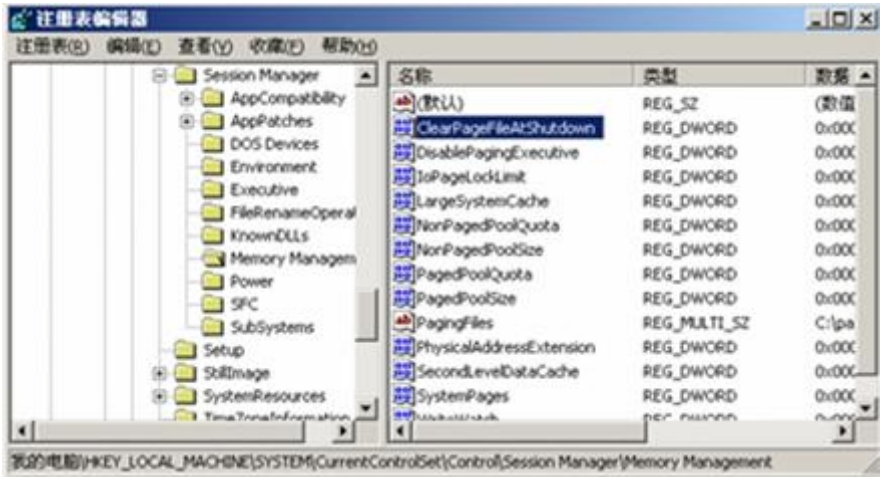
（五）注册表配置

（1）关机时清除文件提供事件的自动发布到订阅 COM 组件页面文件也就是高度文件，是 Windows 2000 用来存储没有装入内存的程序和数据文件 部分的隐藏文件。 某些第三方的程序可以把一些没有加密的密码存在内存中，页面文件中可能含有另外一些敏感资料 ，因此要在关机的时候清除页面文件 。

这可以编辑注册表修改主键 HKEY_LOCAL_MACHINE 下的子键 SYSTEM\CurrentControlSet\Control\Control\SessionManage/Memory Management，把 ClearPageFileAtShutdown 的值设置成 1，如图 4-22 所示。

（2） 关闭 DirectDraw

C2 级安全标准对视频和内存有一定要求。关闭 DirectDraw 可能对一些需要用到 Directx 的程序有影响(比如游戏)，但是对于绝大多数的商业站点是没有影响的。这可以编辑注册表修改主键 HKEY_LOCAL_MACHINE 下的子键 SYSTEM\Current ControlSet\Control\GraphicsDrivers\DCI，将 Timeout 键值设置成 0，如图 4-23 所示。



4-22 修改注册表

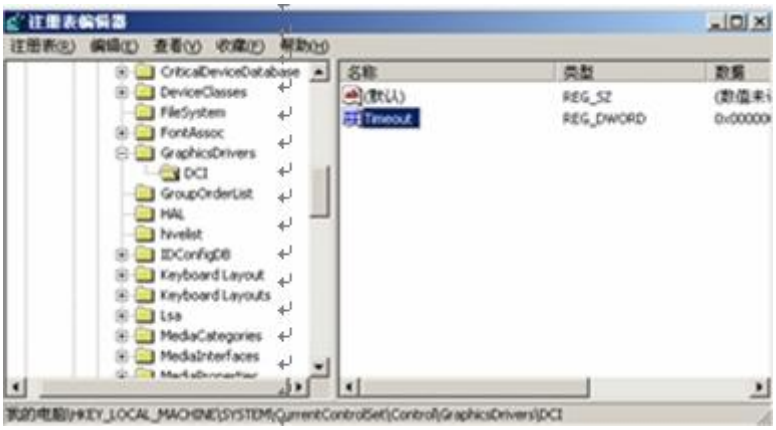


图 4-23 修改注册表

3) 禁止判断主机类型

可利用 TTL(Time to Live,生存时间)值鉴别操作系统的类型,通过 Ping 指令能判断目 标主机类型。许多入侵者首先会 Ping 一个主机，因为攻击某一台计算机需要判断对方的操作系统是 Windows 还是 UNIX。如果 TTL 是 128，就可以认为操作系统是 Windows 2000，如图 4-24 所示。

从图中可以看出，TTL 值是 128，说明该主机的操作系统是 Windows 2000。表 2-7 给 出了一些常见的操作系统的 TTL 对照值修改 TTL 的值后入侵者就无法入侵计算机了。比如将操作系统的 TTL 值改为 100，修 改主键 HKEY_LOCAL_MACHINE 下的子键 SYSTEM\CurrentControlSet\Services\Tcpip \Parameters，新建一个双字节项，如图 4-25 所示。

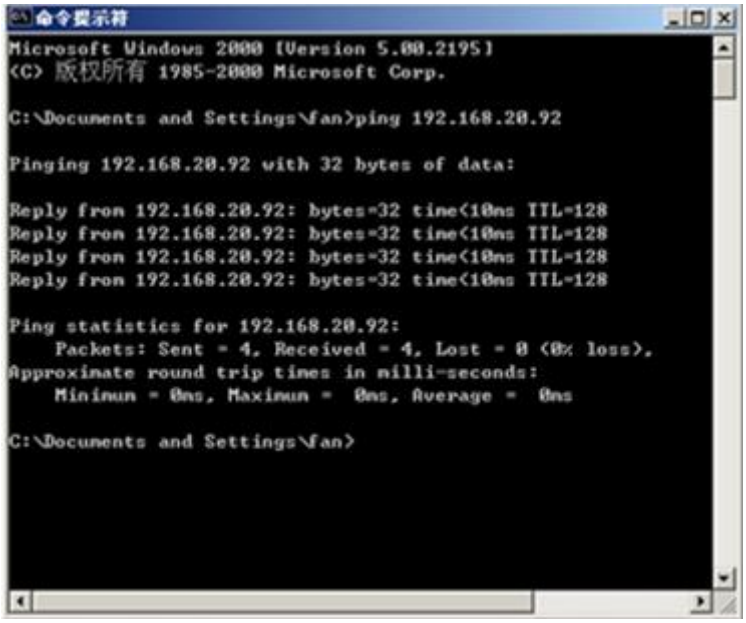


图 4-24 查看操作系统 TTL 值

在键的名称中输入 defaultTTL，然后双击该键名，选中“十六进制”单选按钮，在“数 值数据”文本框中输入 100，如图 4-26 所示。

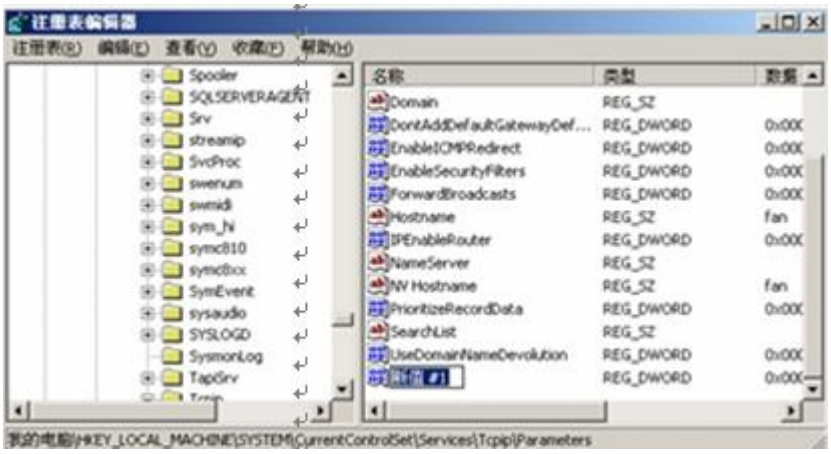


图 4-25 添加双字节项

图 4-26 修改双字节项参数

设置完毕后应重新启动计算机，再次使用 Ping 指令，发现 TTL 的值已经被修改为 100， 如图 4-27 所示。

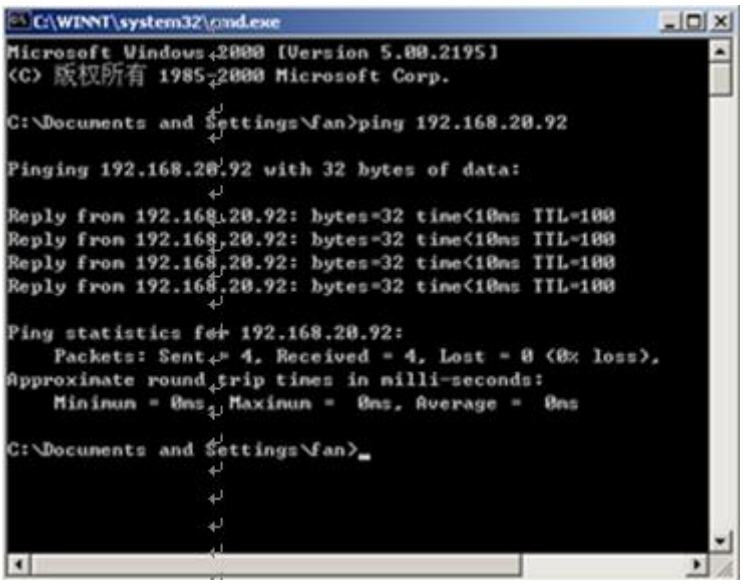


图 4-27 查看操作系统 TTL 值

（六）数据恢复软件

（1）当数据被病毒或者入侵者破坏后，可以利用数据恢复软件找回部分被删除的数据， 在恢复软件中比较著名的有 FinalData。该软件功能强大，可以恢复被误删除和丢失的文件、 目录等。该软件的主界面如图 4-28 所示

图 4-28 FinalData 软件主界面图

图 4-29 选择文件菜单

（2）例如，原来 D 盘上有一些数据文件，现在被黑客删除了，单击“文件”菜单，如图 4-29 所示。

（3）执行“打开”命令，出现当前系统的分区情况，可以选择需要恢复数据的分区， 在这里选择 D 盘，如图 4-30 所示。

(4)选择分区后，软件对指定的分区的数据和目录进行扫描，如图 4-31 所示。

图 4-30 选择分区

图 4-31 软件扫描分区

(5) 扫描完成后，选择查找的扇区范围。如图 4-32 所示。

(6) 扫描的结果是在窗口左侧按目录、文件等进行分类。单击后内容出现在窗口右侧 中，图 4-32 和图 4-34 所示是已经被删除的目录和曾经被删除的文件。

图 4-32 选择查找扇区

图 4-32 查看删除的目录

图 4-33 查看删除的文件

(7) 选中某个文件或者文件夹，右击它则弹出快捷菜单，然后执行“恢复”命令，就 可恢复被删除的文件或文件夹了，如图 4-34 所示。

(8) 该软件操作简单，使用方便，功能强大，可以帮助用户恢复数据。

图 4-34 删除文件的恢复

本模块主要分两部分介绍了网络操作系统的安全问题。第一部分首先介绍了网络操作系 统的有关知识，并分析了国内和国外安全操作系统的评估标准。第二部分主要介绍了 Windows 2000 的安全配置，分为用户安全设置、密码安全设置、系统安全设置、服务安全设置、注册表配置 5 个方面共 35 项，如果每一条都能得到很好的实施，则该计算机无论是 在局域网还是广域网，即使没有网络防火墙，也是比较安全的了。

练习：

1．如何关闭不需要的端口和服务？

2．完成本章所有的配置操作。

3．以报告的形式编写 Windows 2000 配置方案。

4.3.虚拟机 VMware 的安装和使用

实验目的：

了解虚拟机的功能、作用和基本配置。

掌握虚拟机内 windows 系统的安装与使用。

实验内容：

Windows Server 2003 安装。

虚拟机软件的安装。

操作系统 widow server 2003 的安装与配置。

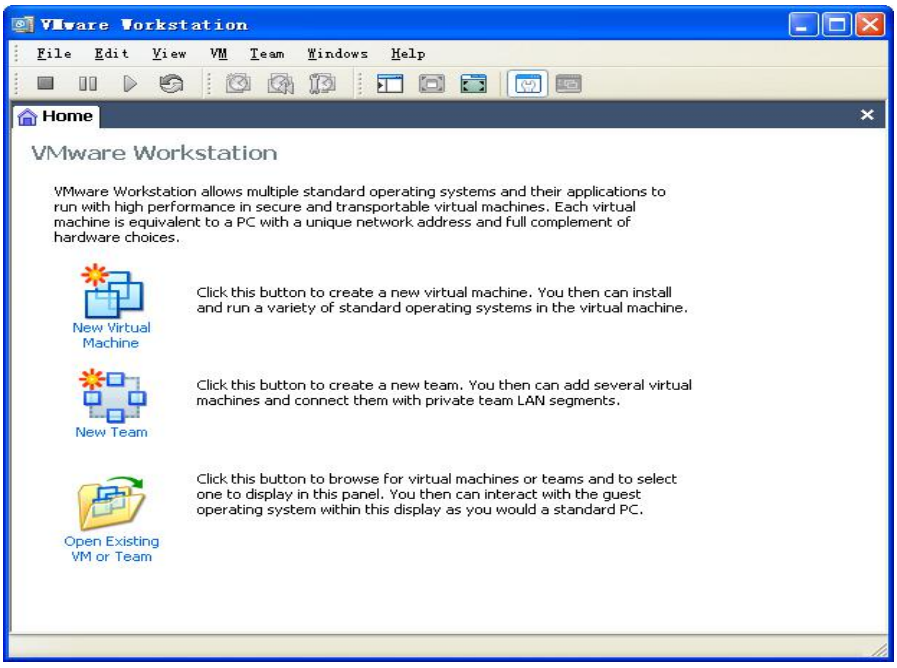
虚拟机与真实机文件共享。

随着互联网的迅速发展，黑客攻击手段日益多样化，作为网络管理人员，及时应对各种威胁以应对黑客的攻击，因此，掌握全面的信息安全技术成为网络管理人员的基本技能。由于条件等诸多限制，目前大多的攻击、防范技术都是在模拟系统中进行的，因此，有必要掌握虚拟系统的安装、配置及使用。本节主要给大家讲授和练习虚拟机的安装和使用。

实验步骤：

1、配置一台虚拟机

（1）在下界面中选择第一项创建新的虚拟机，弹出对话框，如图 4-44 所



示。

图 4-44 新建虚拟机

（2）点下一步即可，如图图 4-44 所示。

图 4-44 新建虚拟机

（3）下界面中需选择第二项自定义，因为很多功能需要我们自己设定，如图 4-45 所示。

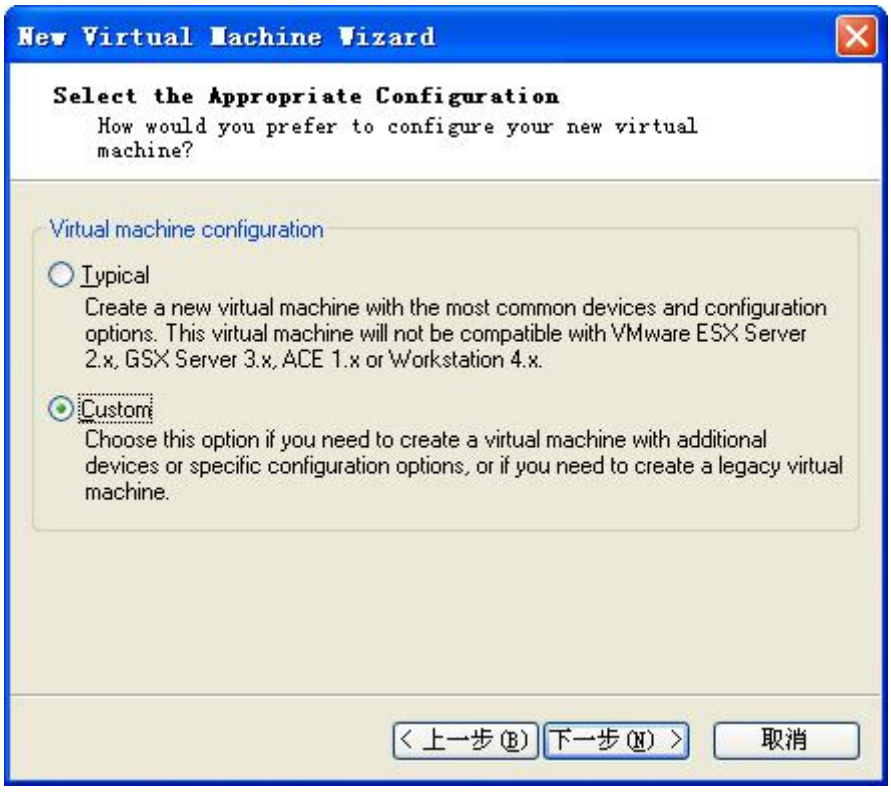


图 4-45 选择虚拟机类型

（4）下界面中选择第一项，如图 4-46 所示。

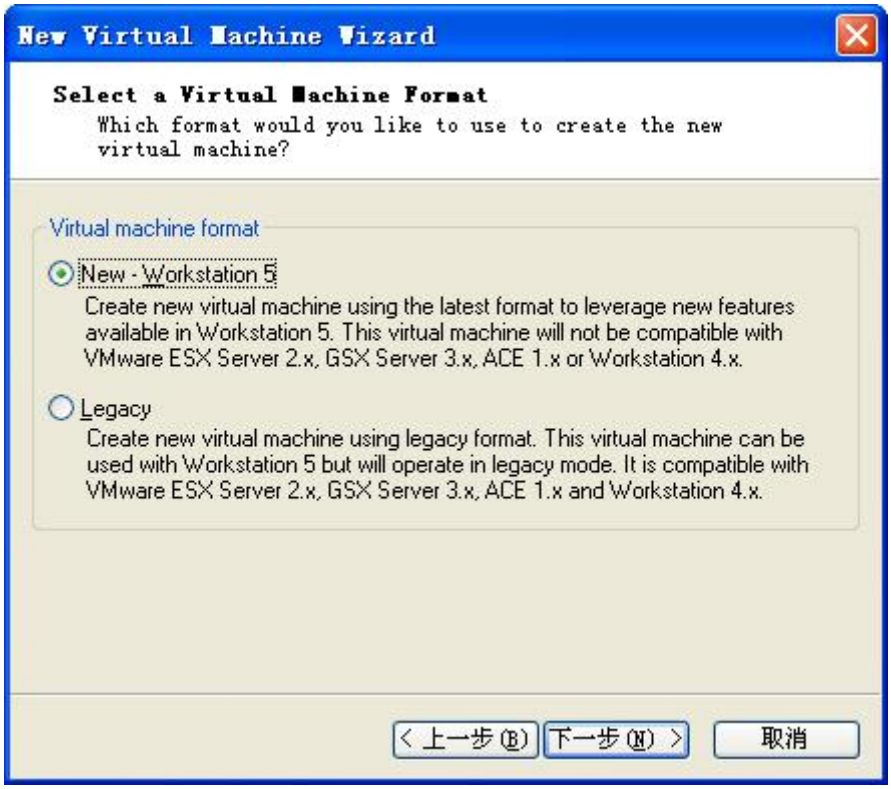


图 4-46 选择虚拟机格式

（5）操作系统选择：操作系统为 Microsoft Windows，版本为 Windows Server 2003 Enterprise Edition，如图 4-47 所示。

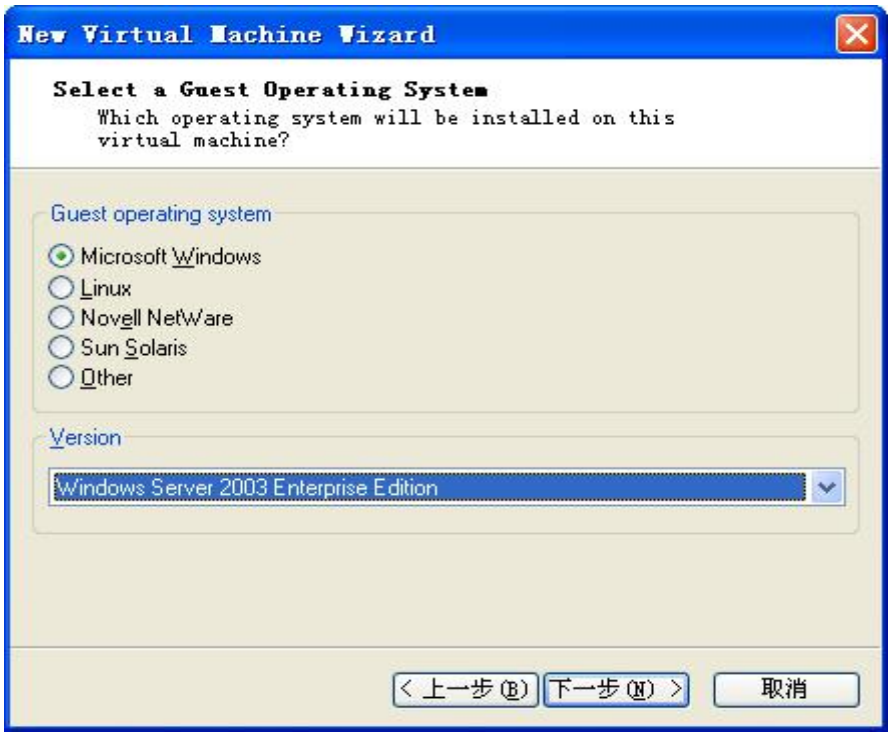


图 4-47 选择虚拟机格式

（6）指定虚拟机存放的位置，最好是自己指定存放位置，如图 4-48 所示。

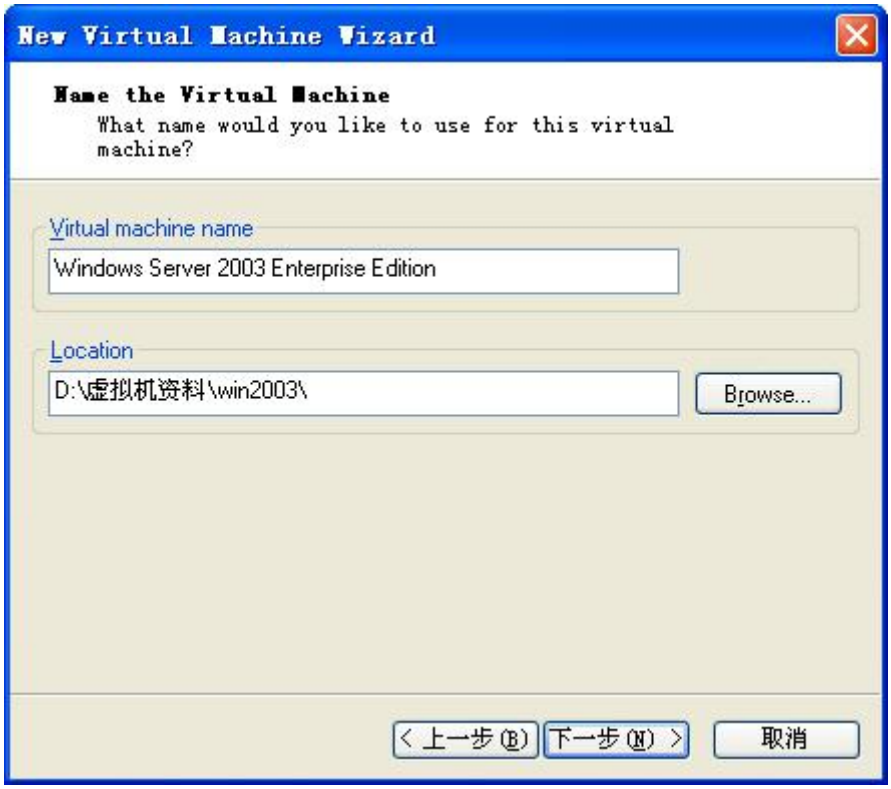


图 4-48 安装位置

（7）指定处理器个数，是否为双核，如图 4-49 所示。

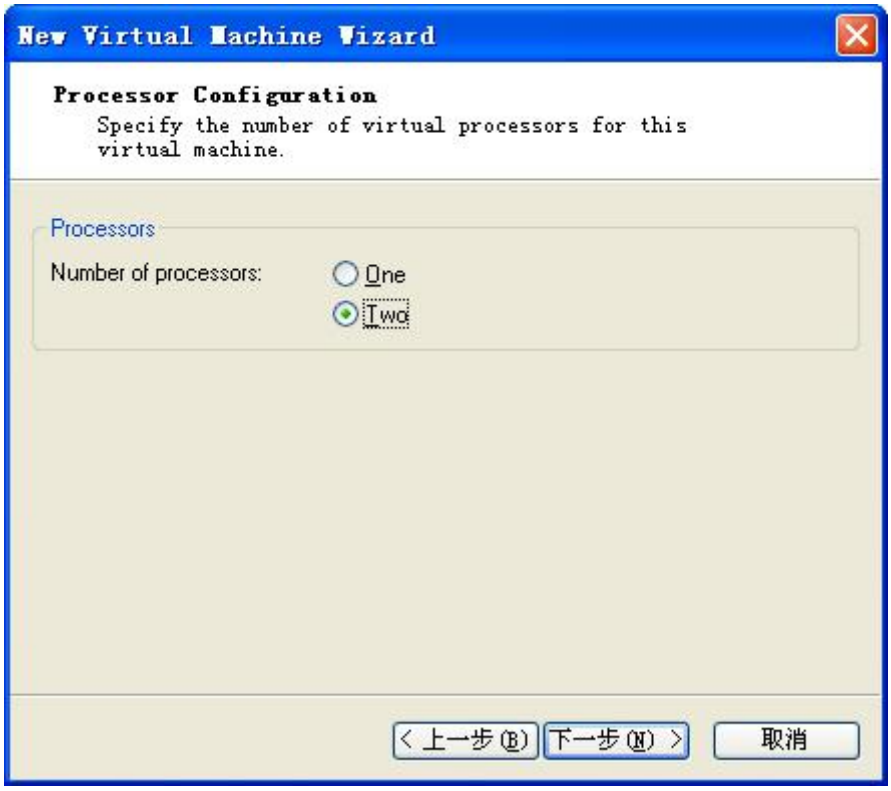


图 4-49 指定处理机个数

（8）指定虚拟机的内存大小，一般为电脑物理内存的一半，如图 4-50 所示。

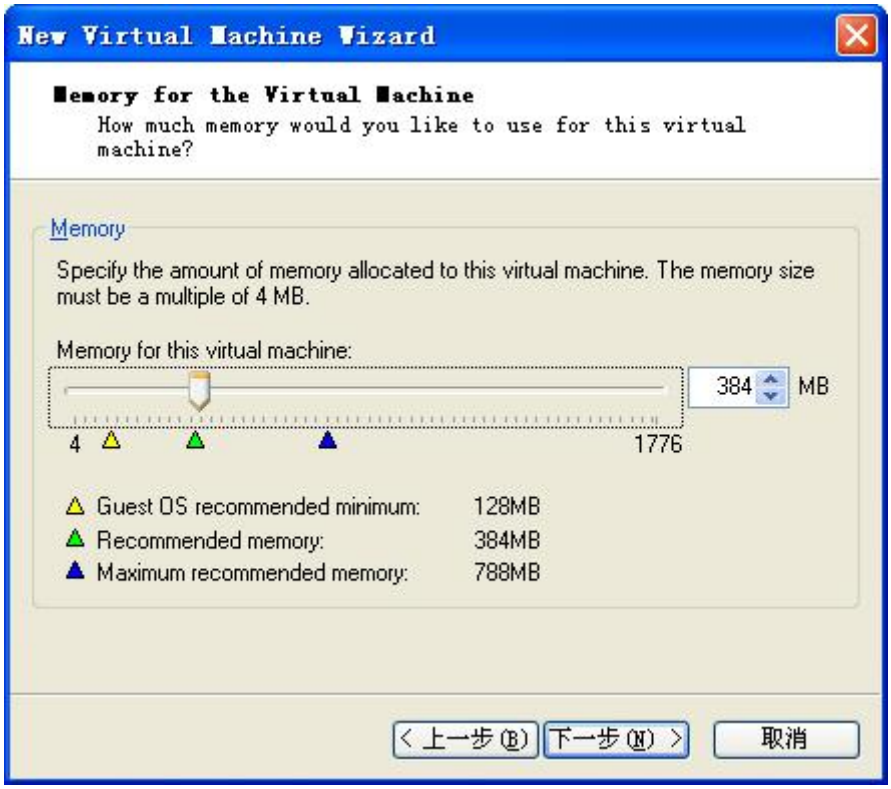


图 4-50 设置内存大小

（9）指定网络连接方式，如图 4-51 所示。

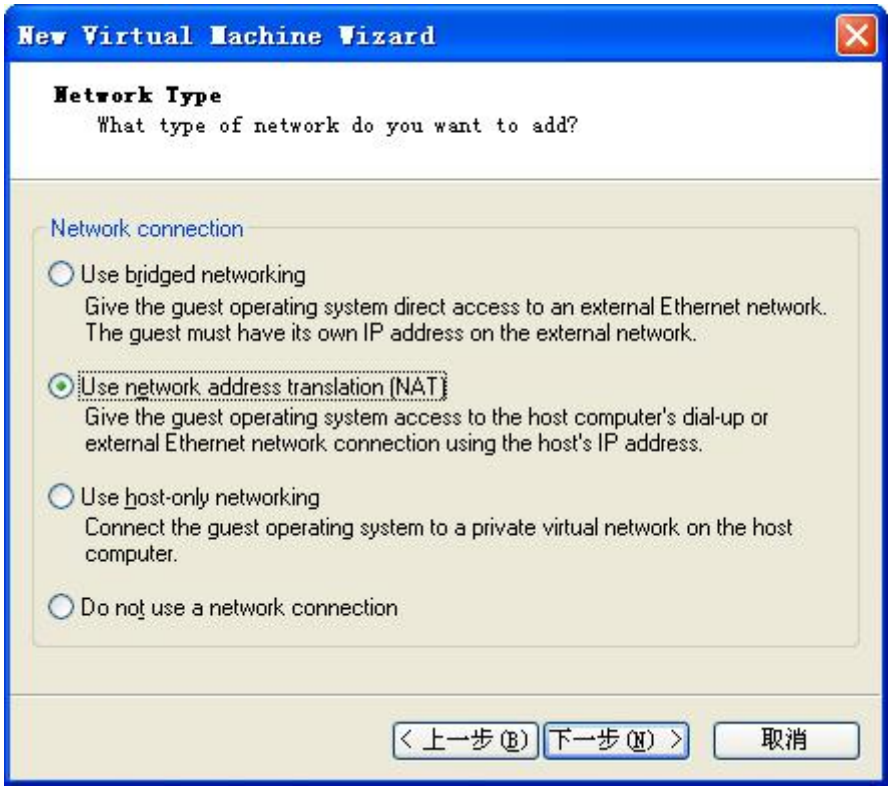


图 4-51 设置网络连接方式

（10）选择 I/O 类型，默认选项即可，如图 4-52 所示。

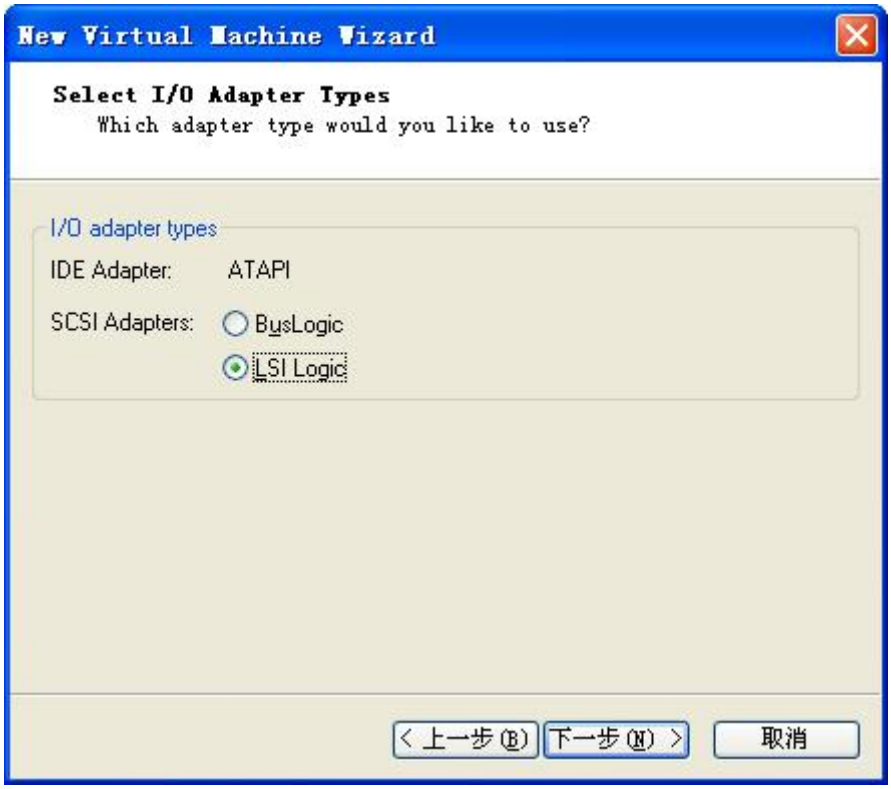


图 4-52 选择 I/O 类型

（11）选择硬盘，选择第一项“创建新的虚拟硬盘”，如图 4-53 所示。

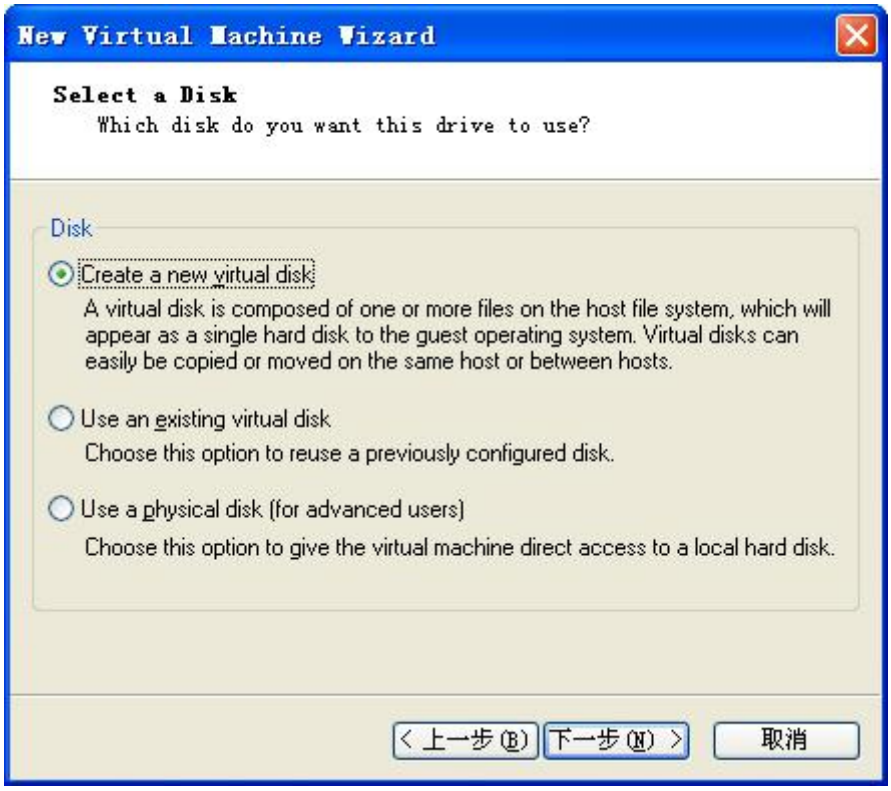


图 4-53 创建新的虚拟硬盘

（12）选择硬盘类型，默认选项即可，如图 4-54 所示。

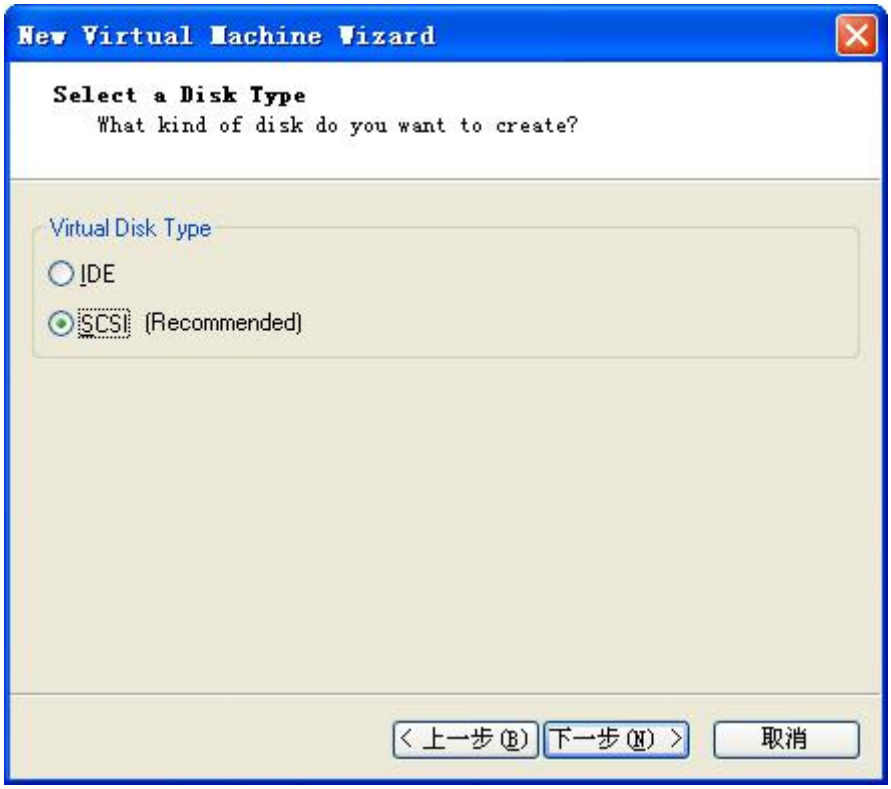


图 4-54 选择硬盘类型

（13）指定虚拟机的硬盘大小，如图 4-55 所示。

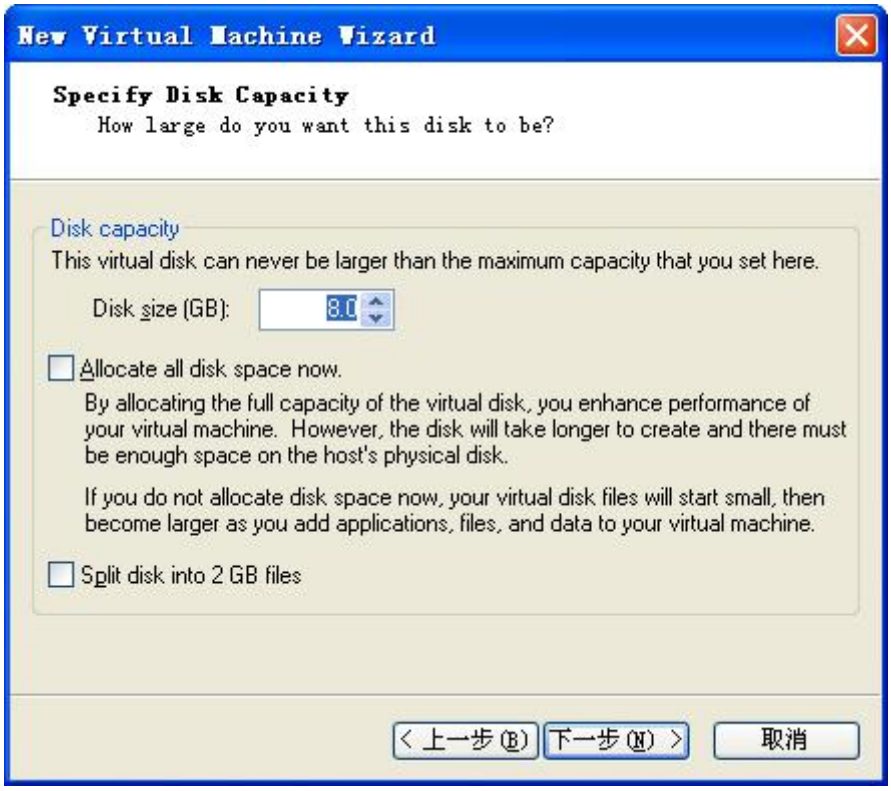


图 4-55 设置硬盘大小

（14）指定虚拟机的文件名，如图 4-56 所示。

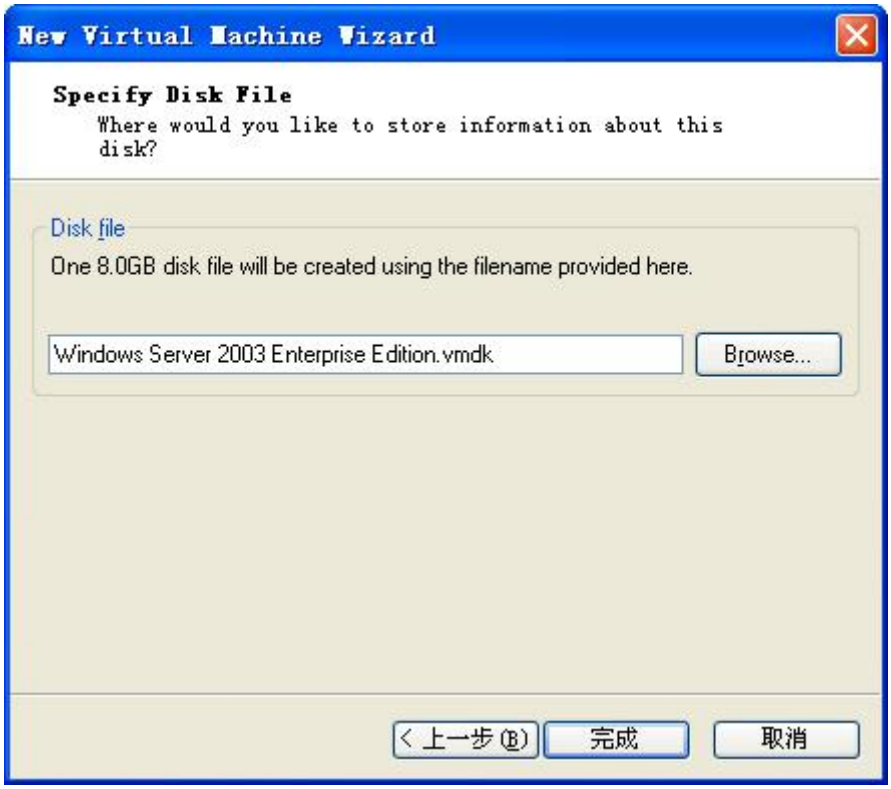


图 4-56 设置虚拟机文件名

（15）如果用镜像包安装系统，则需要设置光驱。如图 4-57 所示。

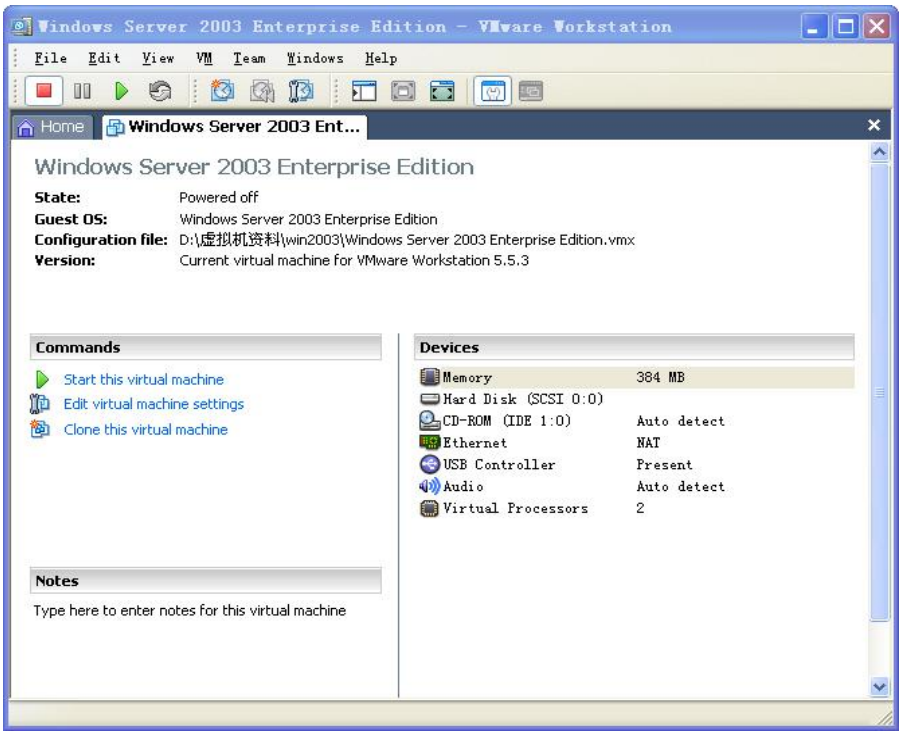


图 4-57 设置光驱

（16）指定镜像包的位置，如图 4-58 所示。

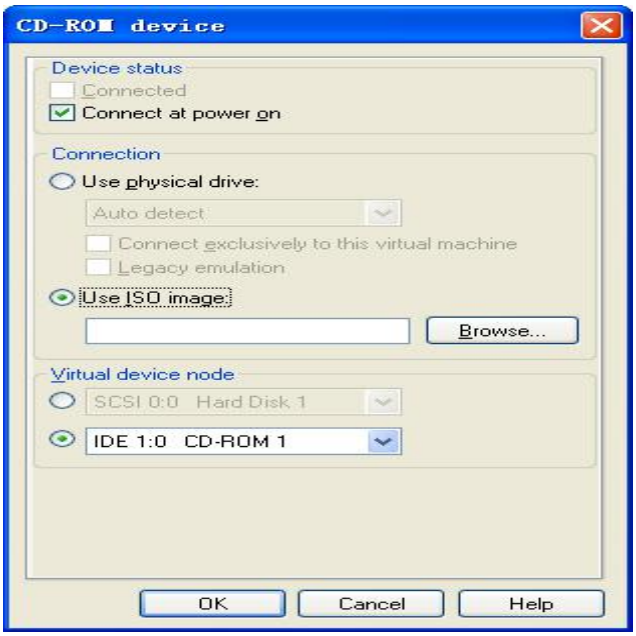


图 4-58 指定镜像包位置

3、在虚拟机上安装 win2003 Server 系统

（1）从光盘启动

根据下面提示进行安装设置，如图 4-59 所示。

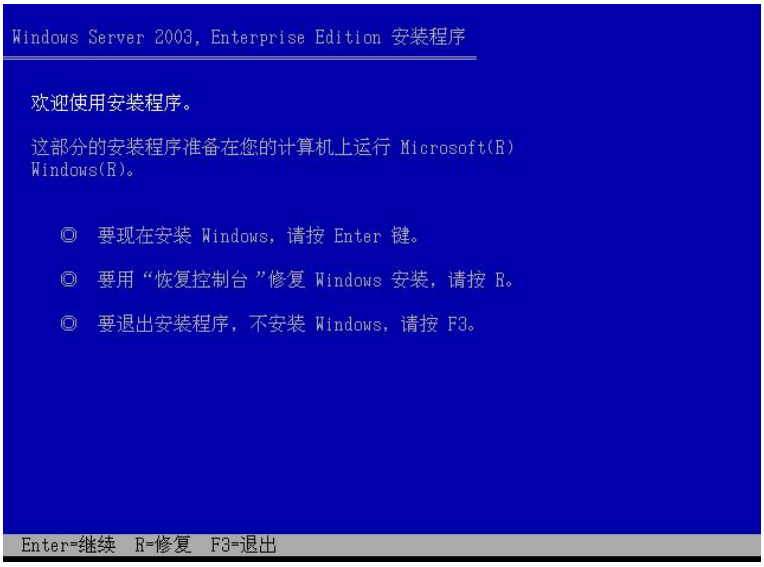


图 4-59 安全系统向导

（2）创建磁盘分区，如图 4-60 所示。

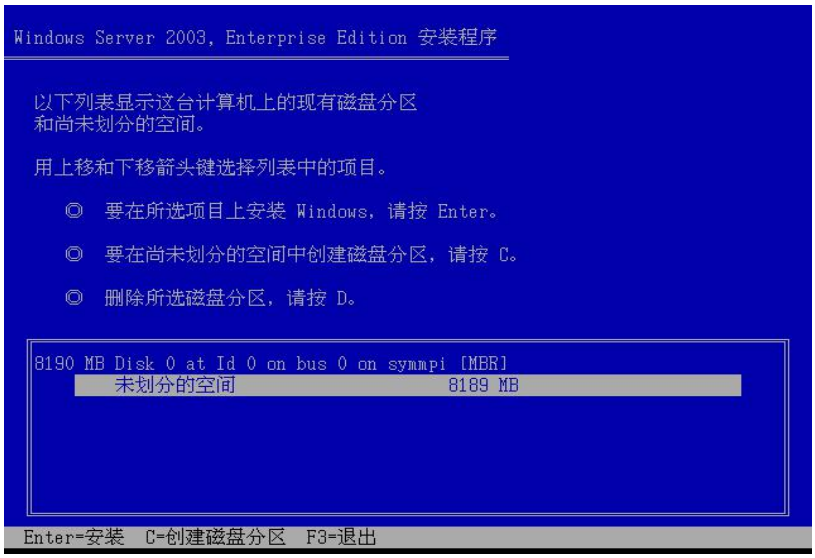


图 4-60 创建分区

（3）格式化磁盘分区，如图 4-61 所示。

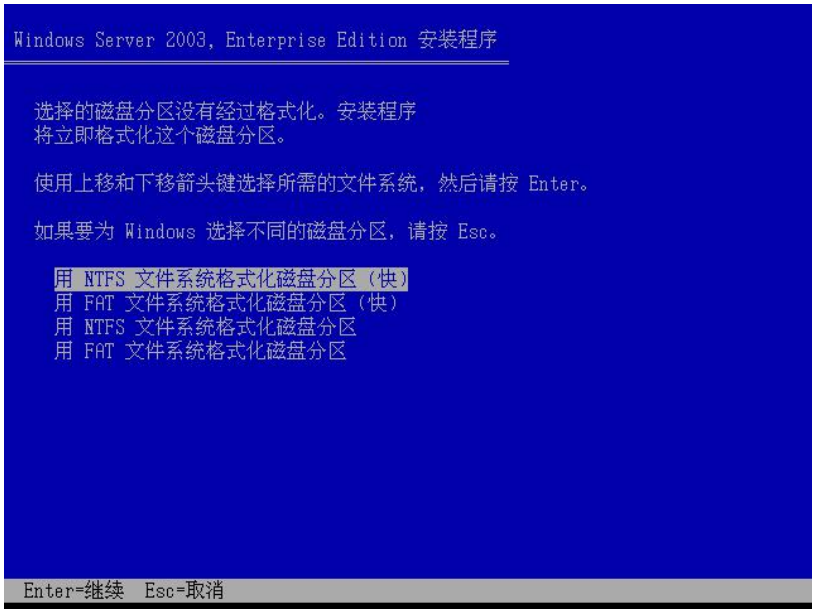


图 4-61 选择格式化方式

（4）复制文件并重新启动。

（5）进入图形界面安装，设置各种格式。

（7）输入姓名和单位。如图 4-62 所示。

图 4-62 设置姓名、单位

（8）输入产品密钥（JCGMJ-TC669-KCBG7-HB8X2-FXG7M），如图 4-63 所示。

图 4-63 输入产品密钥

（9） 选择授权模式：这里我们一般选择每服务器模式。如图 4-64 所示。

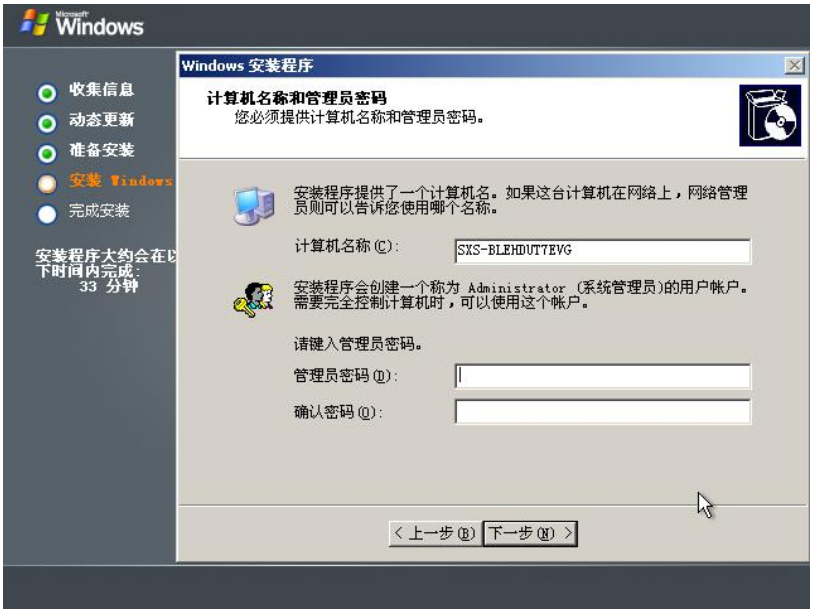
注意：

a．每服务器模式限制同时访问本机的客户机数量，每设备模式不限制，但要求每台客户机都要购买“客户访问许可证”；

b．每服务器模式适合在只有一台服务器的网络中使用，每设备模式适合于有多台服务器的网络中使用。

图 4-64 选择授权模式

（10）输入计算机名和管理员密码。 如图 4-65 所示。



练习：

1．利用虚拟机安装 linux 操作系统和 windows 系统。

2．调试虚拟机使两个系统互通。

模块五 网络设备的配置与安全管理

职业能力要求

理解网络设备的安全机制。

掌握交换机、路由器的基本安全配置。

学习目标

- 理解 VLAN 原理，并熟练配置。
- 熟悉生成树协议的配置。
- 掌握 ACL 不同的实现方法。
- 路由器 RIP、OSPF 协议配置。
- 掌握路由配置及 CHAP 认证的配置方法。

5.1 VLAN 综合实训

5.1.1 VLAN 有关知识

VLAN（Virtual Local Area Network）的中文名为"虚拟局域网"。VLAN 是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术。这一新兴技术主要应用于交换机和路由器中，但主流应用还是在交换机之中。VLAN 是一个在物理网络上根据用途，工作组、应用等来逻辑划分的局域网络，是一个广播域，与用户的物理位置没有关系。VLAN 中的网络用户是通过 LAN 交换机来通信的。一个 VLAN 中的成员看不到另一个 VLAN 中的成员。

5.1.1 VLAN 的配置

一. 实训目的

1. 了解 VLAN 原理；
2. 熟练掌握二层交换机 VLAN 的划分方法；
3. 了解如何验证 VLAN 的划分。

4. 了解 IEEE802.1q 的实现方法，掌握跨二层交换机相同 VLAN 间通信的调试方法；

5. 了解交换机接口的 trunk 模式和 access 模式；

二. 应用环境

教学楼有三两层，分别是一年级、二年级，三年及，每个楼层都有一台交换机满足老师上网需求；每个年级都有语文教研组和数学教研组；三个年级的语文教研组的计算机可以互相访问；三个年级的数学教研组的计算机可以互相访问；一年级与二年级的语文教研组可以 互相访问，但是与三年级的语文教研组不可以相互访问，语文教研组和数学教研组之间不可 以自由访问；通过划分 VLAN 使得语文教研组和数学教研组之间不可以自由访问；使用 802.1Q 进行 跨交换机的 VLAN。

三、实训设备 (神州设备)

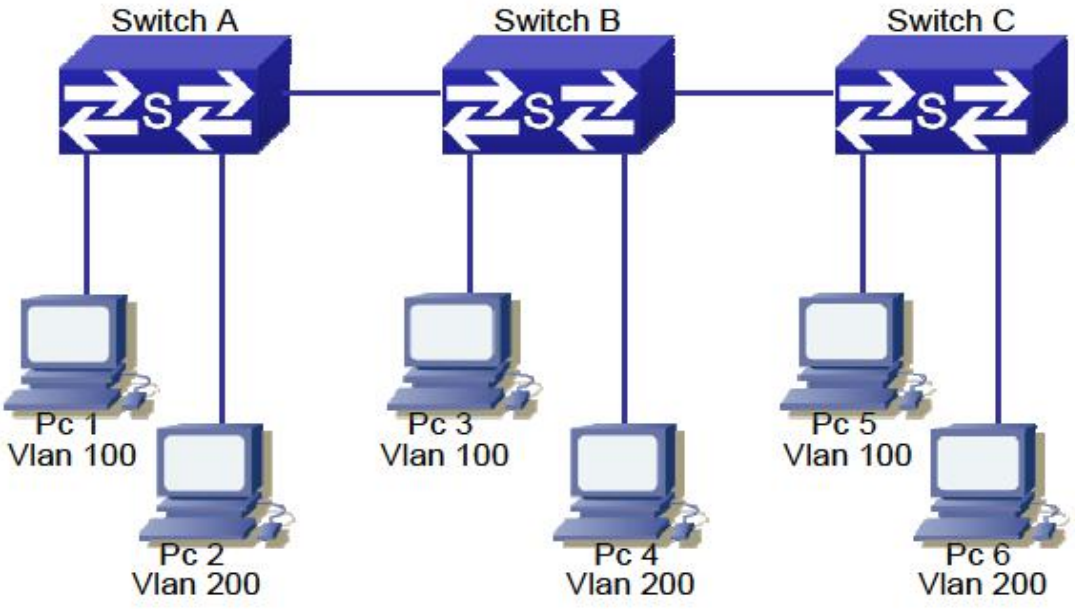
1. DCRS-5650 交换机 2 台（SoftWare version is DCRS-5650-28_5.2.1.0）

2. PC 机 2 台

3. Console 线 1 根

4. 直通网线 2 根

四、实训拓扑



五、 实训要求

在交换机 A、交换机 B 和交换机 C 上分别划分两个基于端口的 VLAN：VLAN100，VLAN200。对应关系如表 5-1 所示。

表 5-1 VLAN、端口对应表

VLAN	端口成员
100	1~8
200	9~16
Trunk 口	24

使得交换机之间 VLAN100 的成员能够互相访问，交换机 A、交换机 B 与交换机 C 的 VLAN200 的成员不能够互相访问；VLAN100 和 VLAN200 成员之间不能互相访问，交换机 B 与交换机 C 之间不允许设置 TRUNK。

PC1 和 PC2 的网络设置如表 5-2 所示。

表 5-2 设备 ip 地址设置

设备	IP 地址	Mask
PC1	192.168.1.31	255.255.255.192
PC3	192.168.1.32	255.255.255.192
PC5	192.168.1.33	255.255.255.192
PC2	192.168.2.101	255.255.255.224
PC4	192.168.2.102	255.255.255.224
PC6	192.168.2.103	255.255.255.224
交换机 A	192.168.1.1	255.255.255.0
交换机 B	192.168.1.2	255.255.255.0
交换机 C	192.168.1.3	255.255.255.0

PC1、PC3 与 PC3 分别接在不同交换机 VLAN100 的成员端口 1~8 上，三台 PC 互相可 以 ping 通；PC2、PC4 与 PC6 分别接在不同交换机 VLAN 的成员端口 9~16 上，三台 PC 互 相不可以 ping 通；PC1、3、5 和 PC2、4、6 互相 ping 不通。

若实训结果和理论相符，则本实训完成。

六、实训步骤

第一步：交换机恢复出厂设置

```
switch#set  default
switch#write
switch#reload
```

第二步：给交换机设置标示符和管理 IP。

交换机 A：

switch(Config)#hostname switchA

switchA(Config)#interface vlan 1

switchA(Config-If-Vlan1)#ip address 192.168.1.1 255.255.255.0 switchA(Config-If-Vlan1)#no shutdown

switchA(Config-If-Vlan1)#exit

switchA(Config)#

交换机 B：

switch(Config)#hostname switchB

switchB(Config)#interface vlan 1

switchB(Config-If-Vlan1)#ip address 192.168.1.2 255.255.255.0 switchB(Config-If-Vlan1)#no shutdown

switchB(Config-If-Vlan1)#exit

switchB(Config)#

交换机 C：

switch(Config)#hostname switchC

switchC(Config)#interface vlan 1

switchC(Config-If-Vlan1)#ip address 192.168.1.3 255.255.255.0 switchC(Config-If-Vlan1)#no shutdown

switchC(Config-If-Vlan1)#exit

switchC(Config)#

第三步：在交换机中创建 vlan100 和 vlan200，并添加端口。

交换机 A：

switchA(Config)#vlan 100

switchA(Config-Vlan100)#

switchA(Config-Vlan100)#switchport interface ethernet 0/0/1-8

switchA(Config-Vlan100)#exit

switchA(Config)#vlan 200

switchA(Config-Vlan200)#switchport interface ethernet 0/0/9-16
switchA(Config-Vlan200)#exit

switchA(Config)#

验证配置：

switchA#show vlan

VLAN Name Type Media Ports

default Static ENET Ethernet0/0/17 Ethernet0/0/18

Ethernet0/0/19 Ethernet0/0/20

Ethernet0/0/21 Ethernet0/0/22

Ethernet0/0/23 Ethernet0/0/24

Ethernet0/0/25 Ethernet0/0/26

Ethernet0/0/27 Ethernet0/0/28

100 VLAN0100 Static ENET Ethernet0/0/1 Ethernet0/0/2

Ethernet0/0/3 Ethernet0/0/4

Ethernet0/0/5 Ethernet0/0/6

Ethernet0/0/7 Ethernet0/0/8

200 VLAN0200 Static ENET Ethernet0/0/9 Ethernet0/0/10

Ethernet0/0/11 Ethernet0/0/12

Ethernet0/0/13 Ethernet0/0/14

Ethernet0/0/15 Ethernet0/0/16

switchA#

switchA(Config)#vlan 100
switchA(Config-Vlan100)#

switchA(Config-Vlan100)#switchport interface ethernet 0/0/1-8；
23 switchA(Config-Vlan100)#exit

switchA(Config)#vlan 200

switchA(Config-Vlan200)#switchport interface ethernet 0/0/9-16
switchA(Config-Vlan200)#exit

switchA(Config)#

验证配置。

24 口已经出现在 vlan1、vlan100 和 vlan200 中，并且 24 口不是一个普通端口，是 tagged 端口。

交换机 B：

switchB(Config)#interface ethernet 0/0/24

switchB(Config-Ethernet0/0/24)#switchport mode trunk

Set the port Ethernet0/0/24 mode TRUNK successfully

switchB(Config-Ethernet0/0/24)#switchport trunk allowed vlan 100 set the port Ethernet0/0/24 allowed vlan successfully

switchB(Config-Ethernet0/0/24)#exit

switchB(Config)# interface ethernet 0/0/23

switchB(Config-If-Ethernet0/0/23)#switchport access vlan 100 Set the port Ethernet0/0/23 access vlan 100 successfully

第五步：验证实训。按下表验证：

动作	结果
PC1 ping PC2	不通
PC1 ping PC3	通
PC1 ping PC4	不通
PC1 ping PC5	通
PC1 ping PC6	不通
PC2 ping PC3	不通
PC2 ping PC4	不通
PC2 ping PC5	不通
PC2 ping PC6	不通
PC3 ping PC4	不通
PC3 ping PC5	通
PC3 ping PC6	不通
PC4 ping PC5	不通
PC4 ping PC6	不通
PC5 ping PC6	不通

5.2 使用生成树协议避免环路产生

一、实训目的

(1) 了解生成树协议的作用；

(2) 熟悉生成树协议的配置。

二、应用环境

采用生成树协议可以避免环路。生成树协议的根本目的是将一个存在物理环路的交换网络变成一个没有环路的逻辑树形网络。IEEE802.1d 协议通过在交换机上运行一套复杂的算法 STA（spanning-tree algorithm），使冗余端口置于“阻断状态”，使得接入网络的计算机在与其他计算机通讯时，只有一条链路生效，而当这个链路出现故障无法使用时，IEEE802.1d 协议会重新计算网络链路，将处于“阻断状态”的端口重新打开，从而既保障了网络正常运转，又保证了冗余能力。

本实训使用 DCS-3926s 系列交换机作为演示设备，其软件版本为：DCS-3926S_6.1.12.0，实际使用中由于软件版本不同，功能和配置方法将有可能存在差异，请关注相应版本的使用说明发布。

三、实训设备

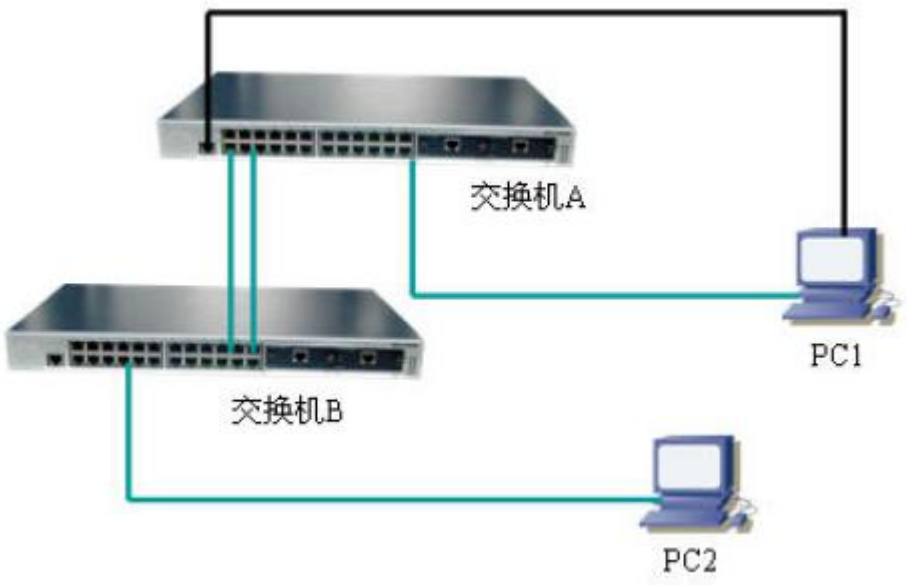
(1) DCS 二层交换机 2 台

(2) PC 机 2 台

(3) Console 线 1-2 根

(4) 直通网线 4-8 根

四、实训拓扑



五、实训要求

IP 地址设置：

设备IP	Mask	子网掩码
交换机A	10.1.157.100	255.255.255.0
交换机B	10.1.157.101	255.255.255.0
PC1	10.1.157.113	255.255.255.0
PC2	10.1.157.114	255.255.255.0

网线连接：

交换机A	e0/0/2	交换机B	e0/0/3
交换机A	e0/0/1	交换机B	e0/0/4

PC1 交换机 A e0/0/24，PC2 交换机 B e0/0/23

六、实训步骤

第一步：连接实训要求中除阴影部分之外的所有部分。

第二步：恢复出厂设置之后，做初始配置（可选）

交换机 A：

```
switch#config
switch(Config)#hostname switchA
switchA(Config)#interface vlan 1
switchA(Config-If-Vlan1)#ip address 10.1.157.100 255.255.255.0
switchA(Config-If-Vlan1)#no shutdown
switchA(Config-If-Vlan1)#exit
switchA(Config)#
```

交换机 B：

```
switch#config
switch (Config)# hostname switchB
switchB(Config)# interface vlan 1
switchB(Config-If-Vlan1)# ip address 10.1.157.101 255.255.255.0
switchB(Config-If-Vlan1)# no shutdown
switchB(Config-If-Vlan1)# exit
switchB(Config)#
```

第三步：确认两台交换机中的生成树协议关闭

```
switch(Config)#no spanning-tree
```

MSTP has already been disabled. //此句表明当前设备中并未启动生成树协议

switch(Config)#

验证配置：

switch#show span

Global MSTP is disabled

switch#

第四步：使用“PC1 ping PC2 –t ”观察现象

(1) 在交换机 B 端口 4 与交换机 A 的端口 2 先未连接时，Ping 结果如何？写在下方：

(2) 插上交换机 B 端口 4 的网线，观察现象，写在下方：

九、课后练习

在交换机中使用 show mac-address-table 命令察看对 PC1 和 PC2 地址的学习是否由于环路的存在而变得不再稳定？

十、共同思考

MSTP 是何含义？

5.3 标准 ACL 实训

一、 实训目的

1、了解什么是标准的 ACl；

2、了解标准 ACL 不同的实现方法；

二、 应用环境

ACL (Access Control Lists)是交换机实现的一种数据包过滤机制，通过允许或拒绝特定的数据包进出网络，交换机可以对网络访问进行控制，有效保证网络的安全运行。用户可以基于报文中的特定信息制定一组规则（rule），每条规则都描述了对匹配一定信息的数据包所采取的动作：允许通过（permit）或拒绝通过（deny）。用户可以把这些规则应用到特定交换机端口的入口或出口方向，这样特定端口上特定方向的数据流就必须依照指定的 ACL 规则进出交换机。通

过 ACL，可以限制某个 IP 地址的 PC 或者某些网段的 PC 的上网活动。用于网络管理。

三、 实训设备

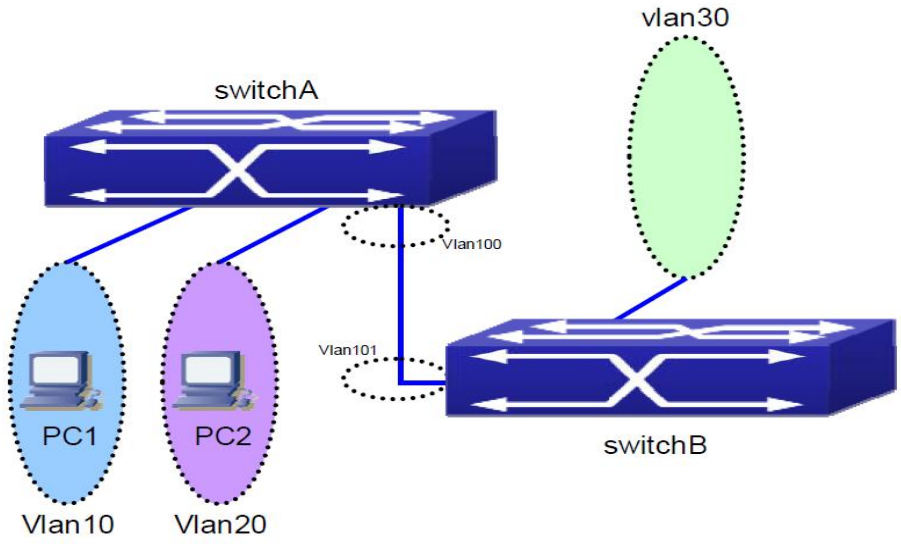
1. DCRS-5656 交换机 2 台（SoftWare version is DCRS-5650-28_5.2.1.0）

2. PC 机 2 台

3. Console 线 1-2 根

4. 直通网线若干

四、 实训拓扑



五、 实训要求(路由配置前实训)

1、在交换机 A 和交换机 B 上分别划分基于端口的 VLAN：

交换机	VLAN	端口成员
交换机 A	10	1~8
	20	9~16
	100	24
交换机 B	30	1~8
	101	24

2、交换机 A 和 B 通过的 24 口级联。

3、配置交换机 A 和 B 各 VLAN 虚拟接口的 IP 地址分别如下表所示：

VLAN10	VLAN20	VLAN30	VLAN100	VLAN101
192.168.10.1	192.168.20.1	192.168.30.1	192.168.100.1	192.168.100.2

4、PC1-PC2 的网络设置为：

设备	IP 地址	gateway	Mask
PC1	192.168.10.101	192.168.10.1	255.255.255.0
PC2	192.168.20.101	192.168.20.1	255.255.255.0

5、验证：

PC1 和 PC2 都通过交换机 A 连接到交换机 B

1、不配置 ACL，两台 PC 都可以 ping 通 VLAN 30；

2、配置 ACL 后，PC1 和 PC2 的 IP ping 不通 VLAN 30，更改了 IP 地址后才可以。

若实训结果和理论相符，则本实训完成。

六、 实训步骤

第一步：交换机全部恢复出厂设置，配置交换机的 VLAN 信息

交换机 A：

DCRS-5656-A#conf

DCRS-5656-A(Config)#vlan 10

DCRS-5656-A(Config-Vlan10)#switchport interface ethernet 0/0/1-8

Set the port Ethernet0/0/1 access vlan 10 successfully

Set the port Ethernet0/0/2 access vlan 10 successfully

Set the port Ethernet0/0/3 access vlan 10 successfully

Set the port Ethernet0/0/4 access vlan 10 successfully

Set the port Ethernet0/0/5 access vlan 10 successfully

Set the port Ethernet0/0/6 access vlan 10 successfully

Set the port Ethernet0/0/7 access vlan 10 successfully

Set the port Ethernet0/0/8 access vlan 10 successfully

DCRS-5656-A(Config-Vlan10)#exit

DCRS-5656-A(Config)#vlan 20

DCRS-5656-A(Config-Vlan20)#switchport interface ethernet 0/0/9-16

Set the port Ethernet0/0/9 access vlan 20 successfully

Set the port Ethernet0/0/10 access vlan 20 successfully

Set the port Ethernet0/0/11 access vlan 20 successfully

Set the port Ethernet0/0/12 access vlan 20 successfully

Set the port Ethernet0/0/13 access vlan 20 successfully

Set the port Ethernet0/0/14 access vlan 20 successfully

Set the port Ethernet0/0/15 access vlan 20 successfully

Set the port Ethernet0/0/16 access vlan 20 successfully

DCRS-5656-A(Config-Vlan20)#exit

DCRS-5656-A(Config)#vlan 100

DCRS-5656-A(Config-Vlan100)#switchport interface ethernet 0/0/24

Set the port Ethernet0/0/24 access vlan 100 successfully

DCRS-5656-A(Config-Vlan100)#exit

DCRS-5656-A(Config)#

交换机 B：

DCRS-5656-B(Config)#vlan 30

DCRS-5656-B(Config-Vlan30)#switchport interface ethernet 0/0/1-8

Set the port Ethernet0/0/1 access vlan 30 successfully

Set the port Ethernet0/0/2 access vlan 30 successfully

Set the port Ethernet0/0/3 access vlan 30 successfully

Set the port Ethernet0/0/4 access vlan 30 successfully

Set the port Ethernet0/0/5 access vlan 30 successfully

Set the port Ethernet0/0/6 access vlan 30 successfully

Set the port Ethernet0/0/7 access vlan 30 successfully

Set the port Ethernet0/0/8 access vlan 30 successfully

DCRS-5656-B(Config-Vlan30)#exit

DCRS-5656-B(Config)#vlan 40

DCRS-5656-B(Config-Vlan40)#switchport interface ethernet 0/0/9-16

Set the port Ethernet0/0/9 access vlan 40 successfully

Set the port Ethernet0/0/10 access vlan 40 successfully

Set the port Ethernet0/0/11 access vlan 40 successfully

Set the port Ethernet0/0/12 access vlan 40 successfully

Set the port Ethernet0/0/13 access vlan 40 successfully

Set the port Ethernet0/0/14 access vlan 40 successfully

Set the port Ethernet0/0/15 access vlan 40 successfully

Set the port Ethernet0/0/16 access vlan 40 successfully

DCRS-5656-B(Config-Vlan40)#exit

DCRS-5656-B(Config)#vlan 101

DCRS-5656-B(Config-Vlan101)#switchport interface ethernet 0/0/24

Set the port Ethernet0/0/24 access vlan 101 successfully

DCRS-5656-B(Config-Vlan101)#exit

DCRS-5656-B(Config)#

第二步：配置交换机各 vlan 虚接口的 IP 地址

交换机 A：

DCRS-5656-A(Config)#int vlan 10

DCRS-5656-A(Config-If-Vlan10)#ip address 192.168.10.1 255.255.255.0

DCRS-5656-A(Config-If-Vlan10)#no shut

DCRS-5656-A(Config-If-Vlan10)#exit

DCRS-5656-A(Config)#int vlan 20

DCRS-5656-A(Config-If-Vlan20)#ip address 192.168.20.1 255.255.255.0

DCRS-5656-A(Config-If-Vlan20)#no shut

DCRS-5656-A(Config-If-Vlan20)#exit

DCRS-5656-A(Config)#int vlan 100

DCRS-5656-A(Config-If-Vlan100)#ip address 192.168.100.1
255.255.255.0

DCRS-5656-A(Config-If-Vlan100)#no shut

DCRS-5656-A(Config-If-Vlan100)#

DCRS-5656-A(Config-If-Vlan100)#exit

DCRS-5656-A(Config)#

交换机 B：

DCRS-5656-B(Config)#int vlan 30

DCRS-5656-B(Config-If-Vlan30)#ip address 192.168.30.1 255.255.255.0

DCRS-5656-B(Config-If-Vlan30)#no shut

DCRS-5656-B(Config-If-Vlan30)#exit

DCRS-5656-B(Config)#int vlan 101

DCRS-5656-B(Config-If-Vlan101)#ip address 192.168.100.2 255.255.255.0

DCRS-5656-B(Config-If-Vlan101)#exit

DCRS-5656-B(Config)#

第三步：配置静态路由

交换机 A：

DCRS-5650-A(Config)#ip route 0.0.0.0 0.0.0.0 192.168.100.2

验证配置：

DCRS-5650-A#show ip route

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default

Gateway of last resort is 192.168.100.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 192.168.100.2, Vlan100

C 127.0.0.0/8 is directly connected, Loopback

C 192.168.10.0/24 is directly connected, Vlan10

C 192.168.20.0/24 is directly connected, Vlan10

C 192.168.100.0/24 is directly connected, Vlan100

交换机 B：

DCRS-5650-B(Config)#ip route 0.0.0.0 0.0.0.0 192.168.100.1

第四步：在 VLAN 30 端口上配置端口的环回测试功能，保证 VLAN 30 可以 ping 通。

交换机 B：

DCRS-5656-B(Config)# interface ethernet 0/0/1 (任意一个 vlan 30 内的接口均可)

DCRS-5656-B(Config-If-Ethernet0/0/1)#loopback

DCRS-5656-B(Config-If-Ethernet0/0/1)#no shut

DCRS-5656-B(Config-If-Ethernet0/0/1)#exit

第五步：不配置 ACL 验证实训。

验证 PC1 和 PC2 之间是否可以 ping 通 VLAN 30 的虚接口 ip 地址

第六步：配置配置访问控制列表

方法 1：配置命名标准 IP 访问列表

DCRS-5656-A(Config)#ip access-list standard test

DCRS-5656-A(Config-Std-Nacl-test)#deny 192.168.10.101 0.0.0.255

DCRS-5656-A(Config-Std-Nacl-test)#deny host-source 192.168.20.101

DCRS-5656-A(Config-Std-Nacl-test)#exit

DCRS-5656-A(Config)#

验证配置：

DCRS-5656-A#show access-lists

ip access-list standard test(used 1 time(s))

deny 192.168.10.101 0.0.0.255

deny host-source 192.168.20.101

方法 2: 配置数字标准 IP 访问列表

DCRS-5656-A(Config)#access-list 11 deny 192.168.10.101 0.0.0.255

DCRS-5656-A(Config)#access-list 11 deny 192.168.20.101 0.0.0.0

第七步：配置访问控制列表功能开启，默认动作为全部开启

DCRS-5656-A(Config)#firewall enable

DCRS-5656-A(Config)#firewall default permit

DCRS-5656-A(Config)#

验证配置：

DCRS-5656-A#show firewall

Fire wall is enabled.

Firewall default rule is to permit any ip packet.

DCRS-5656-A#

第七步：绑定 ACL 到各端口

DCRS-5656-A(Config)#interface ethernet 0/0/1

DCRS-5656-A(Config-Ethernet0/0/1)#ip access-group 11 in

DCRS-5656-A(Config-Ethernet0/0/1)#exit

DCRS-5656-A(Config)#interface ethernet 0/0/9

DCRS-5656-A(Config-Ethernet0/0/9)#ip access-group 11 in

DCRS-5656-A(Config-Ethernet0/0/9)#exit

验证配置：

DCRS-5656-A#show access-group

interface name:Ethernet0/0/9

IP Ingress access-list used is 11, traffic-statistics Disable.

interface name:Ethernet0/0/1

IP Ingress access-list used is 11, traffic-statistics Disable.

第八步：验证实训。

PC	端口	Ping	结果	原因
PC1：192.168.10.101	0/0/1	192.168.30.1	不通	
PC1：192.168.10.12	0/0/1	192.168.30.1	通	
PC2：192.168.20.101	0/0/9	192.168.30.1	不通	
PC2：192.168.20.12	0/0/9	192.168.30.1	通	

七、 注意事项和排错

1、对 ACL 中的表项的检查是自上而下的，只要匹配一条表项，对此 ACL 的检查就马上结束。

2、端口特定方向上没有绑定 ACL 或没有任何 ACL 表项匹配时，才会使用默认规则。

3、firewall default 命令只对所有端口入口的 IP 数据包有效，对其它类型的包无效。

4、一个端口可以绑定一条入口 ACL。

5.4 路由器多区域 OSPF 配置

实训目的

1、掌握多区域 OSPF 的配置；

2、理解 OSPF 区域的意义。

应用环境

区域的概念是 OSPF 优于 RIP 的重要部分，他可以有效的提高路由的效率，缩减部分路由器的 OSPF 路由条目，降低路由收敛的复杂度，在区域边界上，实现路由的汇总、过滤、控制，大大提高了网络的稳定性。

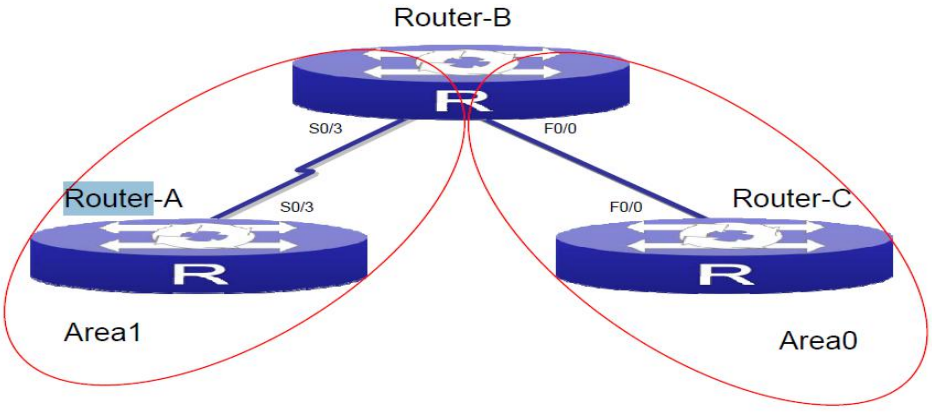
实训设备

1、DCR-2611 三台（Version 1.3.3G (MIDDLE)）

2、CR-V35FC 一根

3、CR-V35MT 一根

实训拓扑



实训要求

Router-A		Router-B		Router-C	
		Serial0/3	172.16.24.2/24	F0/0	172.16.25.2/24
Serial0/3	172.16.24.1/24	F0/0	172.16.25.1/24		
Loopback 0	10.10.10.1/24	Loopback 0	10.10.11.1/24	Loopback 0	10.10.12.1/24

1、按照拓扑图连接网络；

2、按照要求配置路由器各接口地址

实训步骤

第一步：按照上表配置路由器名称、接口的 IP 地址，保证所有接口全部是 up 状态，测试连

通性。

略

第二步：将 Router-A、B 相应接口加入 area0。

Router－A:

Router-A_config#router ospf 1

Router-A_config_ospf_1#network 172.16.24.0 255.255.255.0 area 0

Router－B:

Router-B_config#router ospf 1

Router-B_config_ospf_1#network 172.16.24.0 255.255.255.0 area 0

第三步：将 Router-B、C 相应接口加入 area1。

Router－B:

Router-B_config#router ospf 1

Router-B_config_ospf_1#network 172.16.25.0 255.255.255.0 area 1

Router－C:

Router-C_config#router ospf 1

Router-C_config_ospf_1# network 172.16.25.0 255.255.255.0 area 1

第四步：查看 RA、RC 上的 OSPF 路由表。

Router－A:

Router－A#show ip route

Codes: C － connected, S － static, R － RIP, B － BGP, BC － BGP connected

D － DEIGRP, DEX － external DEIGRP, O － OSPF, OIA － OSPF inter area

ON1 － OSPF NSSA external type 1, ON2 － OSPF NSSA external type 2

OE1 － OSPF external type 1, OE2 － OSPF external type 2

DHCP － DHCP type

VRF ID: 0

C 10.10.10.0/24 is directly connected, Loopback0

C 172.16.24.0/24 is directly connected, Serial0/2

O IA 172.16.25.0/24 [110,1601] via 172.16.24.2(on Serial0/2)！提示学习到的是 OIA 区域间路由，OIA 的路由是通过 LSA3 来传播

Router‐C:

Router‐C# show ip route

Codes: C ‐ connected, S ‐ static, R ‐ RIP, B ‐ BGP, BC ‐ BGP connected

D ‐ DEIGRP, DEX ‐ external DEIGRP, O ‐ OSPF, OIA ‐ OSPF inter area

ON1 ‐ OSPF NSSA external type 1, ON2 ‐ OSPF NSSA external type 2

OE1 ‐ OSPF external type 1, OE2 ‐ OSPF external type 2

DHCP ‐ DHCP type

VRF ID: 0

C 10.10.12.0/24 is directly connected, Loopback0

O IA 172.16.24.0/24 [110,1601] via 172.16.25.1(on FastEthernet0/0)

C 172.16.25.0/24 is directly connected, FastEthernet0/0！提示学习到的是 OIA 区域间路由，OIA 的路由是通过 LSA3 来传播

注意事项和排错

1、区域的划分在接口上进行；

2、作为骨干区域的 area0 必须存在；

3、area 0 只有一个是最好的，当有多个的话就是骨干区域分裂。

5.5 路由器串口 PPP-CHAP 配置

一、实训目的

(1) 掌握 CHAP 验证配置

(2) 理解验证过程

二、应用环境

基于安全的考虑，需要路由器双方经过验证后才能建立连接。

本实训使用 DCR-1702 路由器作为演示设备，软件版本为：1.3.2E/1.3.3A，实际使用中由于设备和软件版本不同，功能和配置方法将有可能存在差异，请关注相应版本的使用说明发布。

三、实训设备

(1) DCR 路由器 2 台

(2) CR-V35MT 1 条

(3) CR-V35FC 1 条

四、实训拓扑

五、实训要求

Router-A		Router-B	
接口	IP地址	接口	IP地址
S1/1 DCE	192.168.1.1	S1/0 DTE	192.168.1.2
帐号	密码	帐号	密码
RouterA	digitalchina	RouterB	digitalchina

六、实训步骤

第一步 Router-A 的配置如果软件为 **1.3.3A** 及其之后的版本，参考如下配置序列。

Router>***enable*** //进入特权模式

Router ***#config*** //进入全局配置模式

Router _config***#hostname Router-A*** //修改机器名

Router-A_config# ***aaa authentication ppp test local***

//定义一个名为 test，使用本地数据进行验证的 aaa 验证方法

Router-A_config***#username RouterB password digitalchina*** //设置帐号密码

Router-A_config***#interface s1/0*** //进入接口模式

Router-A_config_s1/0***#ip address 192.168.1.1 255.255.255.0*** //配置 IP 地址

Router-A_config_s1/0***#encapsulation PPP*** //封装 PPP 协议

Router-A_config_s1/0# ***ppp authentication chap test*** //设置验证方式

Router-A_config_s1/0***#ppp chap hostname RouterA*** //设置发送给对方验证的帐号

Router-A_config_s1/0***#physical-layer speed 64000*** //配置 DCE 时钟频率

Router-A_config_s1/0***#no shutdown***

Router-A_config_s1/0***#^Z*** //按 ctrl + z 进入特权模式

以下配置序列适用于软件版本为 **1.3.3A** 之前的设备

Router***>enable*** //进入特权模式

Router ***#config*** //进入全局配置模式

Router _config***#hostname Router-A*** //修改机器名

Router-A_config***#username RouterB password digitalchina*** //设置帐号密码

Router-A_config***#interface s1/1*** //进入接口模式

Router-A_config_s1/0***#ip address 192.168.1.1 255.255.255.0*** //配置 IP 地址

Router-A_config_s1/1***#encapsulation PPP*** //封装 PPP 协议

Router-A_config_s1/0***#ppp authentication chap*** //设置验证方式

Router-A_config_s1/0#***ppp chap hostname RouterA*** //设置发送给对方验证的帐号

Router-A_config_s1/0#***physical-layer speed 64000*** //配置 DCE 时钟频率

Router-A_config_s1/0#***no shutdown***

Router-A_config_s1/0#***^Z*** //按 ctrl + z 进入特权模式

第二步：查看配置

Router-A#***show interface s1/1*** //查看接口状态

Serial1/0 is up, line protocol is down // 对端没有配置， 所以协议是 DOWN

Mode=Sync DCE Speed=64000 //查看 DCE

DTR=UP,DSR=UP,RTS=UP,CTS=DOWN,DCD=UP

Interface address is 192.168.1.1/24 //查看 IP 地址

MTU 1500 bytes, BW 64 kbit, DLY 2000 usec

Encapsulation prototol PPP, link check interval is 10 sec //查看封装协议

Octets Received0, Octets Sent 0

Frames Received 0, Frames Sent 0, Link-check Frames Received0

Link-check Frames Sent 89, LoopBack times 0

Frames Discarded 0, Unknown Protocols Frames Received 0, Sent failuile 0

Link-check Timeout 0, Queue Error 0, Link Error 0,

60 second input rate 0 bits/sec, 0 packets/sec!

60 second output rate 0 bits/sec, 0 packets/sec!

0 packets input, 0 bytes, 8 unused_rx, 0 no buffer

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

8 packets output, 192 bytes, 0 unused_tx, 0 underruns

error:

0 clock, 0 grace

PowerQUICC SCC specific errors:

0 recv allocb mblk fail 0 recv no buffer

0 transmitter queue full 0 transmitter hwqueue_full

第三步：Router-B 的配置

如果软件为 **1.3.3A** 及其之后的版本，参考如下配置序列。

Router>***enable*** //进入特权模式

Router ***#confi***g //进入全局配置模式

Router _config***#hostname Router-B*** //修改机器名

Router-B_config***#aaa authentication ppp test local***

//定义一个名为 test，使用本地数据进行验证的 aaa 验证方法

Router-B_config***#username RouterA password digitalchina*** !设置帐号密码

Router-B_config***#interface s1/0*** //进入接口模式

Router-B_config_s1/0***#ip address 192.168.1.2 255.255.255.0*** //配置 IP 地址

Router-B_config_s1/0***#encapsulation PPP*** //封装 PPP 协议

Router-B_config_s1/0***#ppp authentication chap test*** //设置验证方式

Router-B_config_s1/0***#ppp chap hostname RouterB*** //设置发送给对方验证的帐号

Router-B_config_s1/0***#shutdown***

Router-B_config_s1/0***#no shutdown***

Router-B_config_s1/0***#^Z*** //按 ctrl + z 进入特权模式

以下配置序列适用于软件版本为 **1.3.3A** 之前的设备

Router>***enable*** //进入特权模式

Router ***#config*** //进入全局配置模式

Router _config***#hostname Router-B*** //修改机器名

Router-B_config***#username RouterA password digitalchina*** !设置帐号密码

Router-B_config***#interface s1/0*** //进入接口模式

Router-B_config_s1/0#***ip address 192.168.1.2 255.255.255.0*** //配置 IP 地址

Router-B_config_s1/1#***encapsulation PPP*** //封装 PPP 协议

Router-B_config_s1/0#***ppp authentication chap*** //设置验证方式

Router-B_config_s1/0#***ppp chap hostname RouterB*** //设置发送给对方验证的帐号

Router-B_config_s1/0#***no shutdown***

Router-B_config_s1/0#***^Z*** //按 ctrl + z 进入特权模式

第四步：查看配置

Router-A#***show interface s1/0*** //查看接口状态

Serial1/0 is up, line protocol is up //接口和协议都是 up

Mode=Sync DTE //查看 DTE

DTR=UP,DSR=UP,RTS=UP,CTS=DOWN,DCD=UP

Interface address is 192.168.1.2/24 //查看 IP 地址

MTU 1500 bytes, BW 64 kbit, DLY 2000 usec

Encapsulation prototol PPP, link check interval is 10 sec //查看封装协议

Octets Received0, Octets Sent 0

Frames Received 0, Frames Sent 0, Link-check Frames Received0

Link-check Frames Sent 89, LoopBack times 0

Frames Discarded 0, Unknown Protocols Frames Received 0, Sent failuile 0

Link-check Timeout 0, Queue Error 0, Link Error 0,

60 second input rate 0 bits/sec, 0 packets/sec!

60 second output rate 0 bits/sec, 0 packets/sec!

0 packets input, 0 bytes, 8 unused_rx, 0 no buffer

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

8 packets output, 192 bytes, 0 unused_tx, 0 underruns

error:

0 clock, 0 grace

PowerQUICC SCC specific errors:

0 recv allocb mblk fail 0 recv no buffer

0 transmitter queue full 0 transmitter hwqueue_full

第五步：测试连通性

Router-A#***ping 192.168.1.2***

PING 192.168.1.2 (192.168.1.2): 56 data bytes

!!!!!

--- 192.168.1.2 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 20/22/30 ms

七、注意事项和排错

(1) 双方密码一定要一致，发送的帐号要和对方帐号数据库中的帐号对应

(2) 不要忘记配置 DCE 的时钟频率

模块六 防火墙技术

职业能力要求

1 掌握防火墙 的工作原理，理解网络地址转换原理

2 理解 Web 认证、VPN 技术。

学习目标

- 掌握 SNAT、DNAT 的配置
- 掌握防火墙 Web 认证配置
- 掌握防火墙 IPSEC VPN 配置掌握

6.1 网络地址转换

6.1.1 防火墙 SNAT 配置

一、实训目的

考虑到公网地址的有限，不能每台 PC 都配置公网地址访问外网。通过少量公网 IP 地址来满足多数私网 ip 上网，以缓解 IP 地址枯竭的速度。

二、应用环境

用于公司内部私网地址较多，运营商只分配给一个或者几个公网地址。在这种条件下，这几个公网地址需要满足几十乃至几百几千人同时上网，需要配置源 NAT

三、实训设备

(1) 防火墙设备 1 台

(2) 局域网交换机 n 台

(3) 网络线 n 条

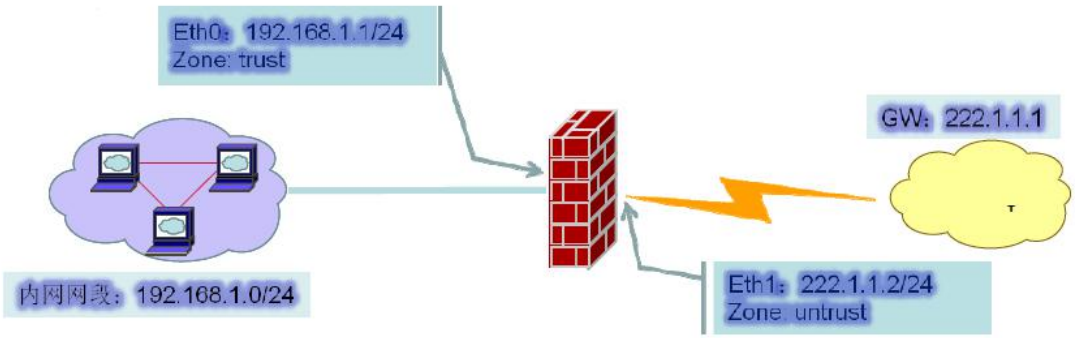
(4) PC 机 n 台

四、实训拓扑

五、实训要求

配置防火墙使内网 192.168.1.0/24 网段可以访问 Internet。

I



六、实训步骤

第一步 配置接口

首先通过防火墙默认 eth0 接口地址 192.168.1.1 登录到防火墙界面进行接口的配置。

通过 WebUI 登录防火墙界面。如图 6-2 所示。

图 6-2 web 界面登陆防火墙

输入缺省用户名 admin，密码 admin 后单击登录按钮，配置外网接口地址。本实训更改为 222.1.1.2。如图 6-3 所示

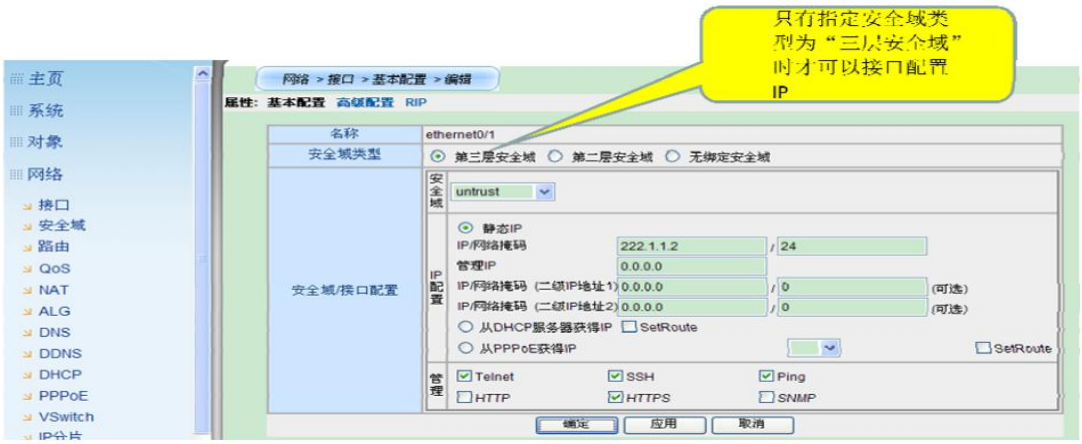


图 6-3 首先指定第三层安全域

第二步 添加路由

添加到外网的缺省路由，在目的路由中新建路由条目添加下一跳地址。如图 6-4 所示。

图 6-4 添加下一跳路由

第三步 添加 **SNAT** 策略

在网络/NAT/SNAT 中添加源 NAT 策略。如图 6-5 所示。

图 6-5 源 NAT 策略示意

第四步 添加安全策略

在安全/策略中，选择好源安全域和目的安全域后，新建策略。如图 2-6 所示。

图 6-6 安全策略方向选择

关于 SNAT，我们只需要建立一条内网口安全域到外网口安全域放行的一条策略就可以保证内网能够访问到外网。如果是需要对于策略中各个选项有更多的配置要求可以单击高级配置进行编辑。如图 6-7 和 6-8 所示。

图 6-7 高级策略的选择

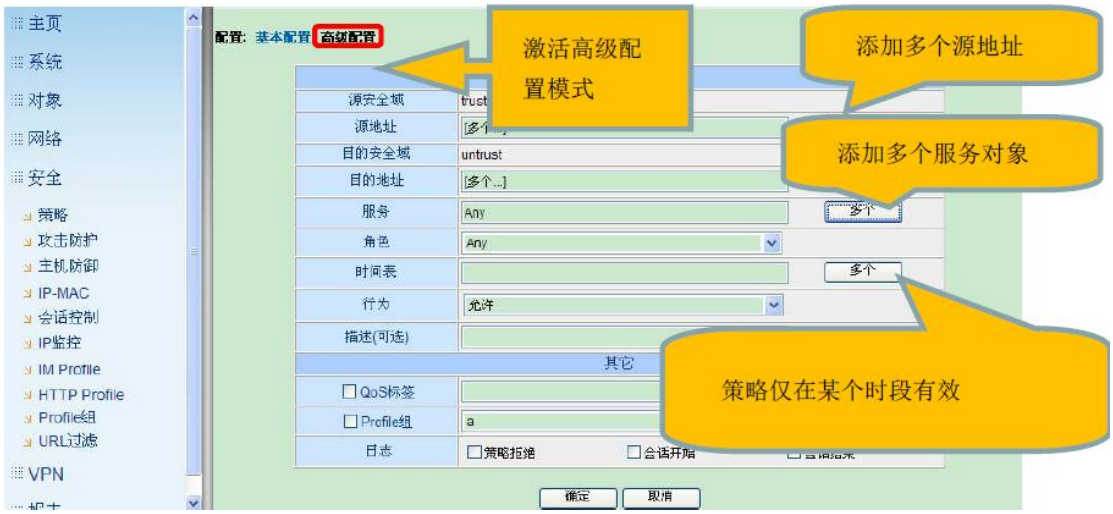


图 6-8 高级策略的编辑

七、实训相关知识

(1)防火墙的接口名称在防火墙中， WAN 接口是防火墙用来连接外网的接口。LAN 接口是外网接口，DMZ 接口用来连接服务器，其他防火墙的接口对应关系在面板上可以找到。

(2)192.168.1.1/24 表示 IP 地址为 192.168.1.1，子网掩码为 24 位，即 255.255.255.0

(3) SNAT 源地址转换,它的作用是将 ip 数据包的源地址转换成另外一个地址。内部地址要访问公网上的服务时（如 web 访问），内部地址会主动发起连接，由防火墙上的网关对内部地址做地址转换，将内部地址的私有 IP 转换为公网的公有 IP，防火墙网关的这个地址转换称为 SNAT，主要用于内部共享 IP 访问外部。

八、共同思考

如果是配置 SNAT 后，只允许在内网用户早 9:00 到晚 18:00 浏览网页，其他时间不做任何限制，如何来实现

九、课后练习

防火墙内网口处接一台神州数码三层交换机 5950，三层交换机上设置了几个网段都可以通过防火墙来访问外网。

6.1.2 防火墙 DNAT 配置

一、实训目的

防火墙上配置了 SNAT 后，内部用户在访问外网时都隐藏了私网地址，如果防火墙内部有一台服务器需要对外网用户开放，此时就必须在防火墙上配置 DNAT，将数据包在防火墙做目的地址转换，让外网用户访问到该服务器。

二、应用环境

由于公网地址有限，一般在申请线路时，运营商分配给我们的只有一个或几个公网地址。但是内部服务器设置成私网地址后，需要将私网地址映射到公网。外网用户才可以通过映射后的公网地址访问到服务器。映射包括两种：一种为端口映射，只是映射需要的服务器端口；一种为 IP 映射，将私网地址和公网地址做一对一的映射。

三、实训设备

(1) 防火墙设备 1 台

(2) Console 线 1 条

(3) 网络线 n 条

(4) 网络交换机 n 台

(5) PC 机 n 台，服务器器 n 台

四、实训拓扑

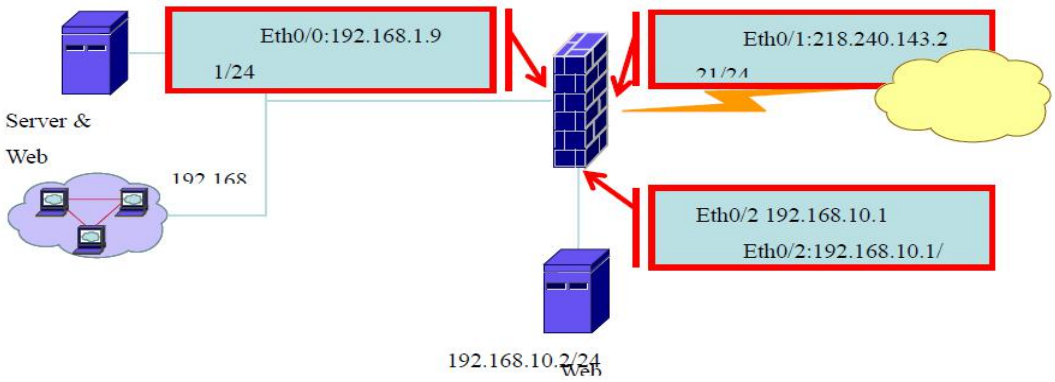


图 6-9 目的 NAT 拓扑示意

五、实训要求

使用外网口 IP 为内网 FTP Server 及 WEB ServerB 做端口映射，并允许外网用户访问该 Server 的 FTP 和 WEB 服务，其中 Web 服务对外映射的端口为 TCP8000。

允许内网用户通过域名访问 WEB ServerB(即通过合法 IP 访问）。

使用合法 IP 218.240.143.220 为 Web ServerA 做 IP 映射，允许内外网用户对该 Server 的 Web 访问。

六、实训步骤

任务一：外网口 **IP** 为内网 **FTP Server** 及 **WEB ServerB** 做端口映射并允许外网用户访问该 **Server** 的 **FTP** 和 **WEB** 服务，其中 **Web** 服务对外映射的端口为 **TCP8000**。

（一）配置准备工作

1、设置地址簿，在对象/地址簿中设置服务器地址，如图 2-10 所示。

图 6-10 添加 IP 地址对象

设置服务簿，防火墙出厂自带一些预定义服务，但是如果我们需要的服务在预定义中不包含时，需要在对象/服务簿中手工定义。如图 6-11 所示。

图 6-11 服务对象添加

（二）创建目的 **NAT**

配置目的 NAT,为 trust 区域 server 映射 FTP(TCP21)和 HTTP(TCP80)端口，如图 6-12 所示。

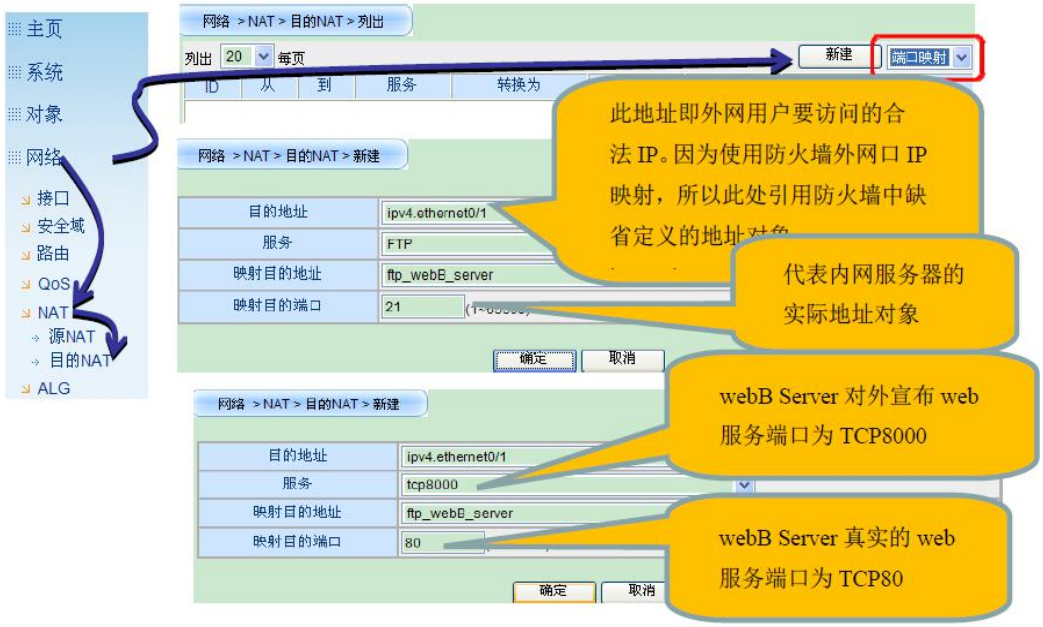


图 6-12 创建目的 NAT 条目

（三）放行安全策略

创建安全策略，允许 untrust 区域用户访问 trust 区域 server 的 FTP 和 web 应用。如图 6-13 所示。

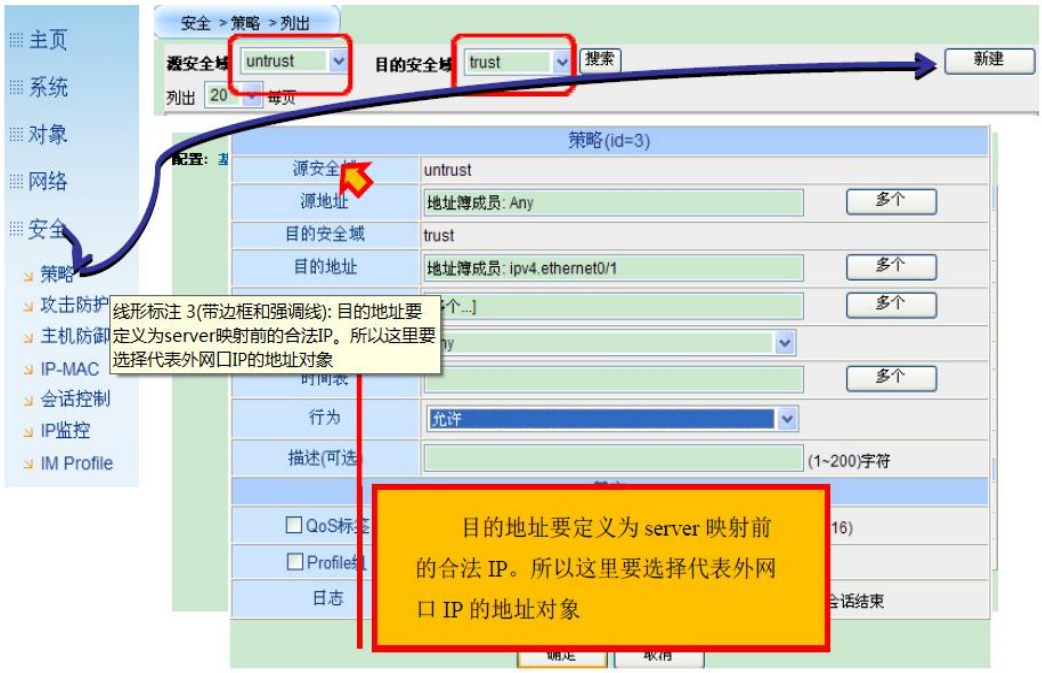


图 6-13 配合目的 NAT 的安全策略配置

任务二：允许内网用户通过域名访问 WEB ServerB(即通过合法 IP 访问）。

实现这一任务所需要做的就是在之前的配置基础上，增加 Trust -> Trust 的安全策略，如图 6-14 所示。

图 6-14 安全策略配置

七、实训相关知识

(1)DMZ “隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的 问题，而设立的一个非安全系统与 安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、

FTP 服务器和论坛等。另一方面，通过这样一个 DMZ 区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。

(2)DMZ 访问控制策略 ①内网可以访问外网②内网可以访问 DMZ ③外网不能访问内网 ④外网可以访问 DMZ ⑤DMZ 不能访问内网 ⑥DMZ 不能访问外网。

(3) DNAT 目的地址转换的作用是将一组本地内部的地址映射到一组全球地 址 ，通俗点来讲，就是对数据包的源地址和目的地址进行修改， 并且保存修改前后的映射关系，根据需要进行还原操作。

(4)多对一的地址转换有什么限制？

为了解决 IP 地址不足的问题，神州数码防火墙允许许多内部的机器对应到一个合法的 NIC IP 地址，使得这些内部机器可同时用一个合法 NIC IP 连上因特网。但是从因特网无法初始一个连接到内部多对一的机器，因为防火墙不知道因特网传来的连接传给哪一部机器。如果内部有服务器对外提供服务则需要一对一的地址转换。

八、共同思考

内网有一台 ftp 服务器，使用防火墙外网口地址将其映射到外网，映射端口为 1221。请思考该功能如何实现?

九、课后练习

请在内网架设一台 Web 服务器，使防火墙将该服务器映射到公网，映射端口为 8888。使内、外网用户可以通过公网地址的 8888 端口访问该服务器。

6.2 防火墙 Web 认证配置

一、网络拓扑

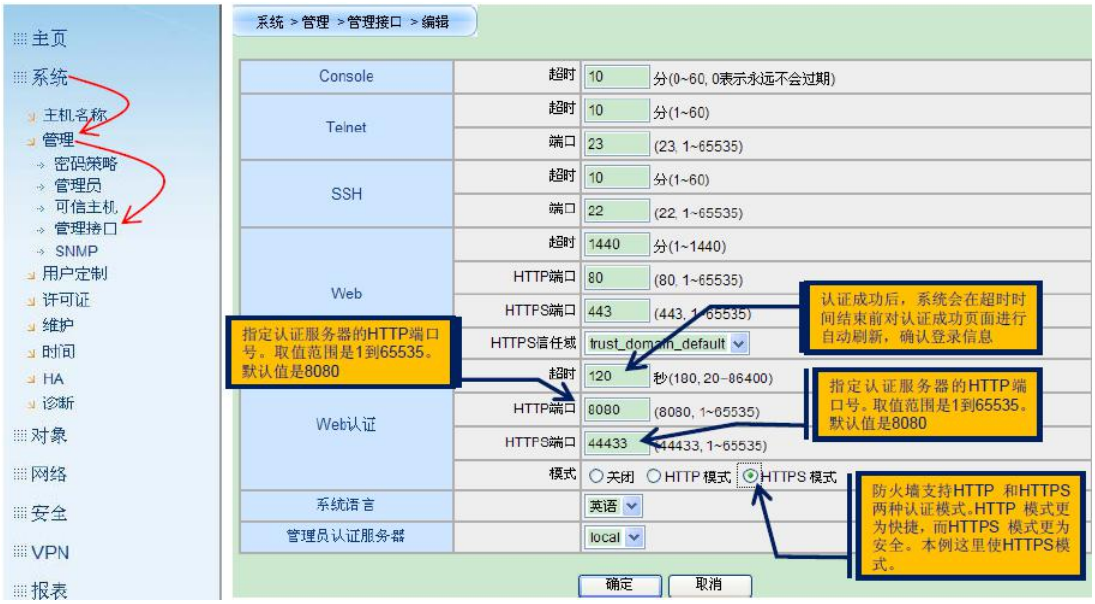
二、需求描述

内网用户首次访问 Internet 时需要通过 WEB 认证才能上网。且内网用户划分为两个用户组 usergroup1 和 usergroup2,其中 usergroup1 组中的用户在通过认证后仅能浏览 web 页面，usergroup2 组中的用户通过认证后仅能使用使用 ftp。

三、配置步骤

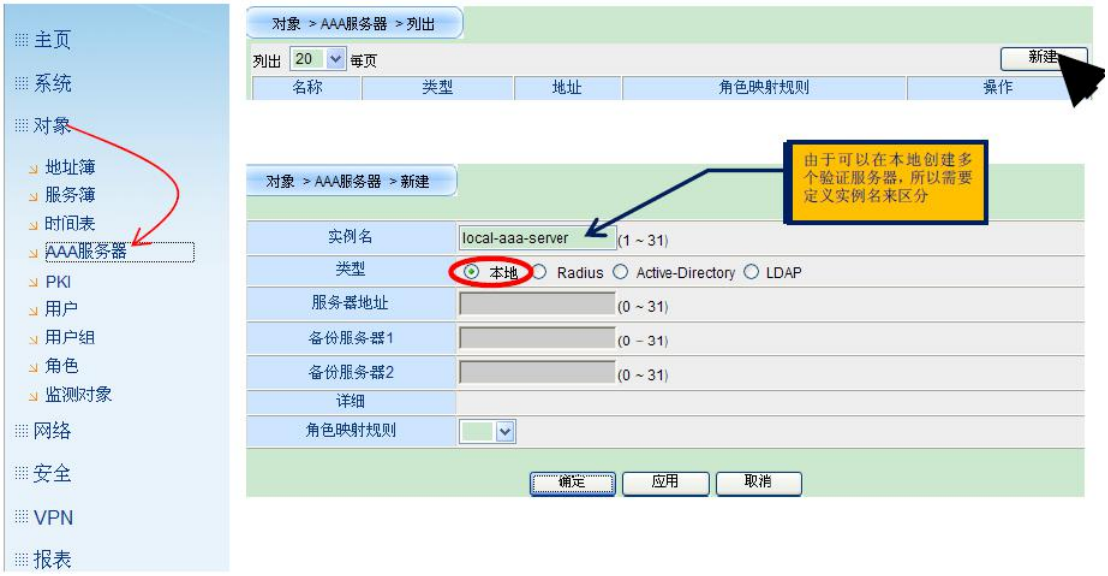
第一步：开启 **web** 认证功能

防火墙 Web 认证功能默认是关闭状态，需要手工在系统/管理/管理接口中将其开启，Web 认证有 http 和 https 两种模式。



第二步：创建 **AAA** 认证服务器

在开启防火墙认证功能后，需要在对象/AAA 服务器中设置一个认证服务器，防火墙能够支持本地认证、Radius 认证、Active-Directory 和 LDAP 认证。在本实验中我们使用防火墙的本地认证，在此我们选择认证类型为本地



第三步：创建用户及用户组，并将用户划归不同用户组

既然要做认证，需要在防火墙的对象/用户组中设置用户组，在本实验中我们设置了 usergroup1 和 usergroup2 两个用户组

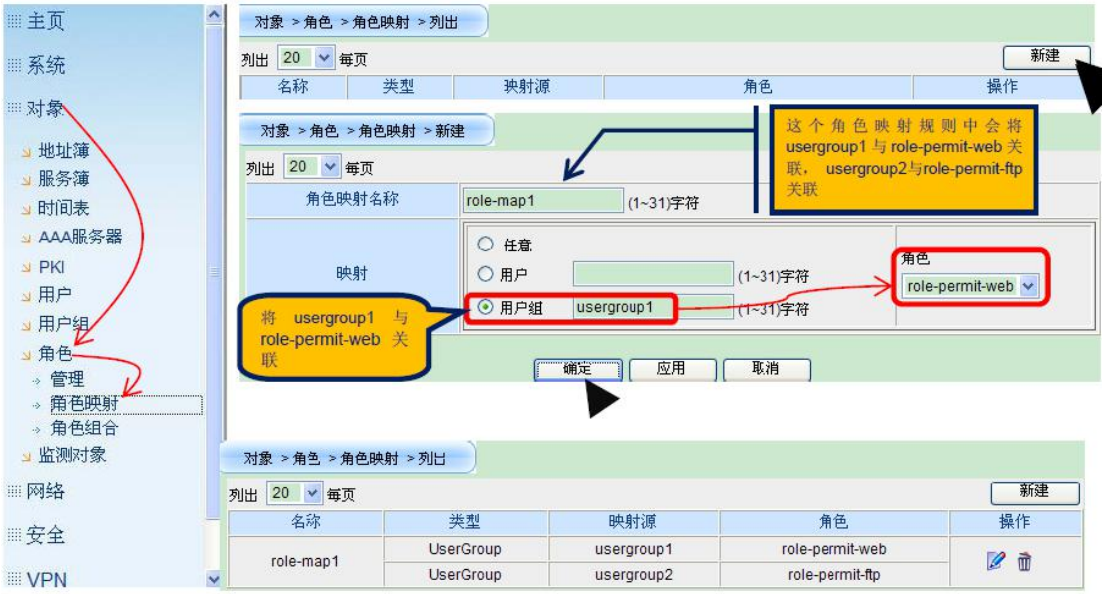
然后在对象/用户首先在在本地服务器中选择之创建好的 local-aaa-server 认证服务器，在该服务器下创建 user1 用户，并将该用户设置到 usergroup1 用户组中，同样的方法创建 user2 用户，并将 user2 用户设置到 usergroup2 组中

第四步：创建角色

创建好用户和用户组后，下面在对象/角色/管理中设置两个角色，名称分别为 role-permit-web 和 role-permit-ftp

第五步：创建角色映射规则，将用户组与角色相对应

在对象/角色/角色映射中，将用户组和角色设置角色映射关系名称为 role-map1，将 usergroup1 用户组和 role-permit-web 做好对应关系，同样的方法将 usergroup2 和 role-permit-ftp 做好对应关系。

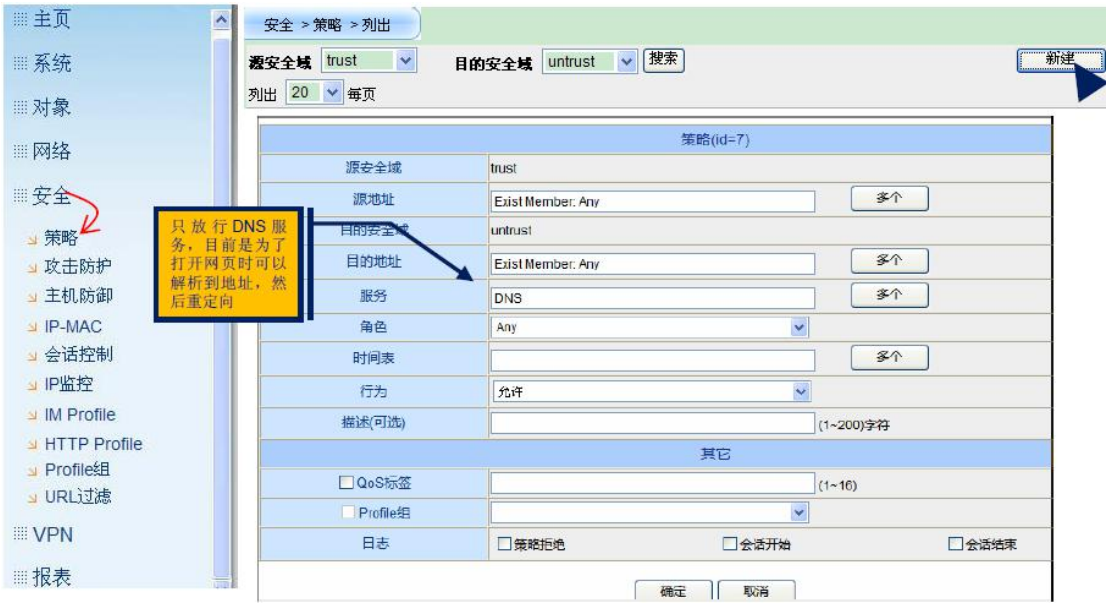


第六步：将角色映射规则与 **AAA** 服务器绑定

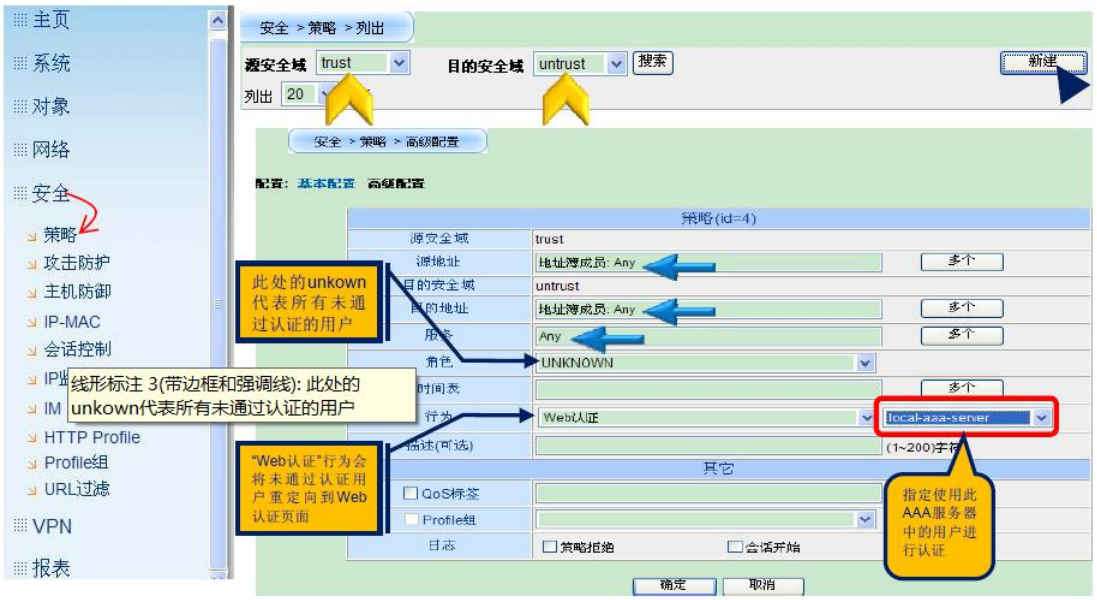
在对象/AAA 服务器中，将角色映射关系 role-map1 绑定到创建的 AAA 服务器 loca-aaa-server 中

第七步：创建安全策略不同角色的用户放行不同服务

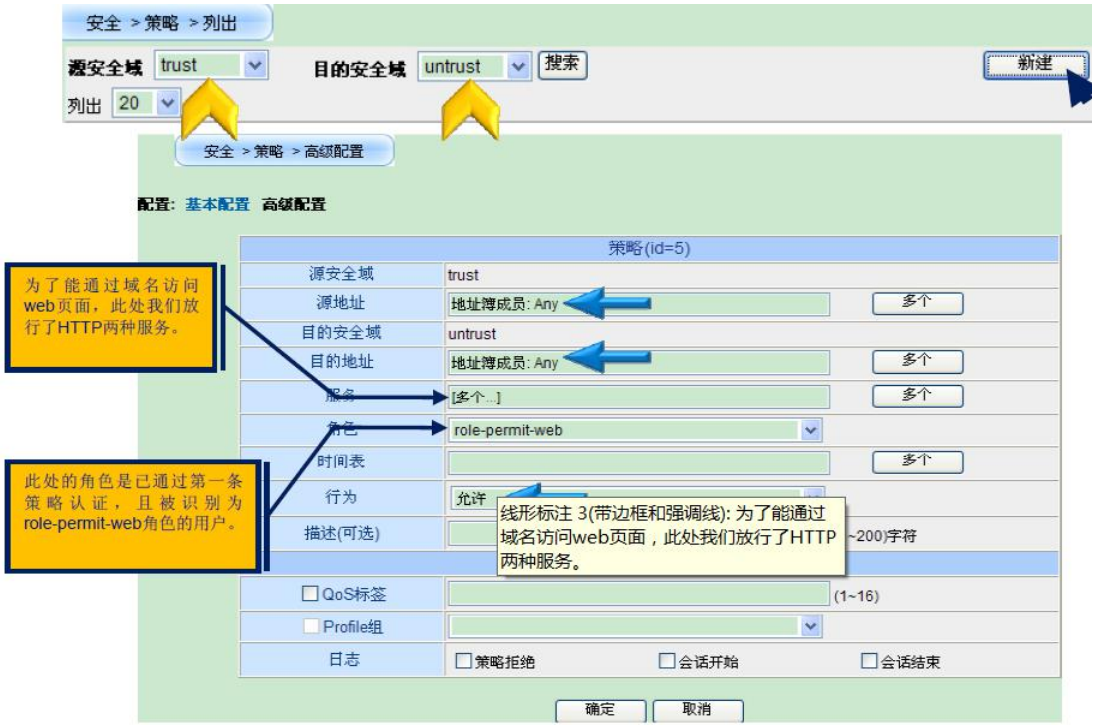
在安全/策略中设置内网到外网的安全策略，首先在该方向安全策略的第一条设置一个方形 DNS 服务的策略，放行该策略的目的是当我们在 IE 栏中输入某个网站名后，客户端 PC 能够正常对该网站做出解析，然后可以从定向到认证页面



在内网到外网的安全策略的第二条我们针对未通过认证的用户 UNKNOWN，设置认证的策略，认证服务器选择创建的 local-aaa-server。



在内网到外网的第三条安全策略中，我们针对认证过的用户放行相应的服务，针对角色 role-permit-web 我们只放行 http 服务

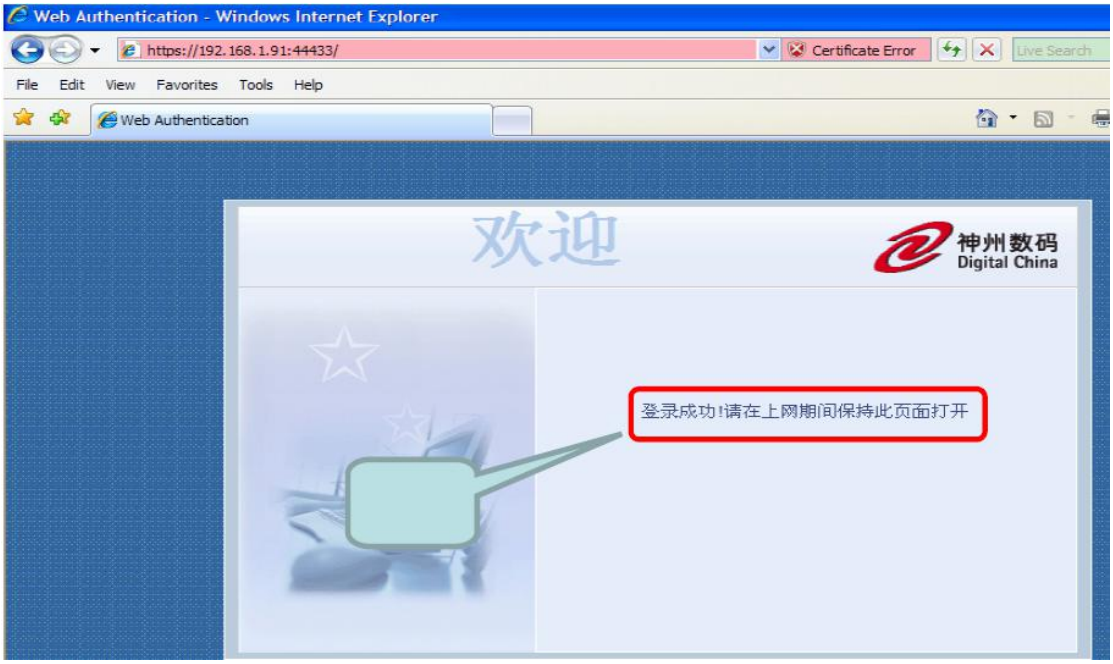


针对通过认证后的用户，属于 role-permit-ftp 角色的只放行 ftp 服务

最后我们看下在安全/策略中我们设置了几条策略，在这里我们设置了四条策略，第一条策略我们只放行 DNS 服务，第二条策略我们针对未通过认证的用户设置认证的安全策略，第三条策略和第四条策略我们针对不同角色用户放行不同的服务项。

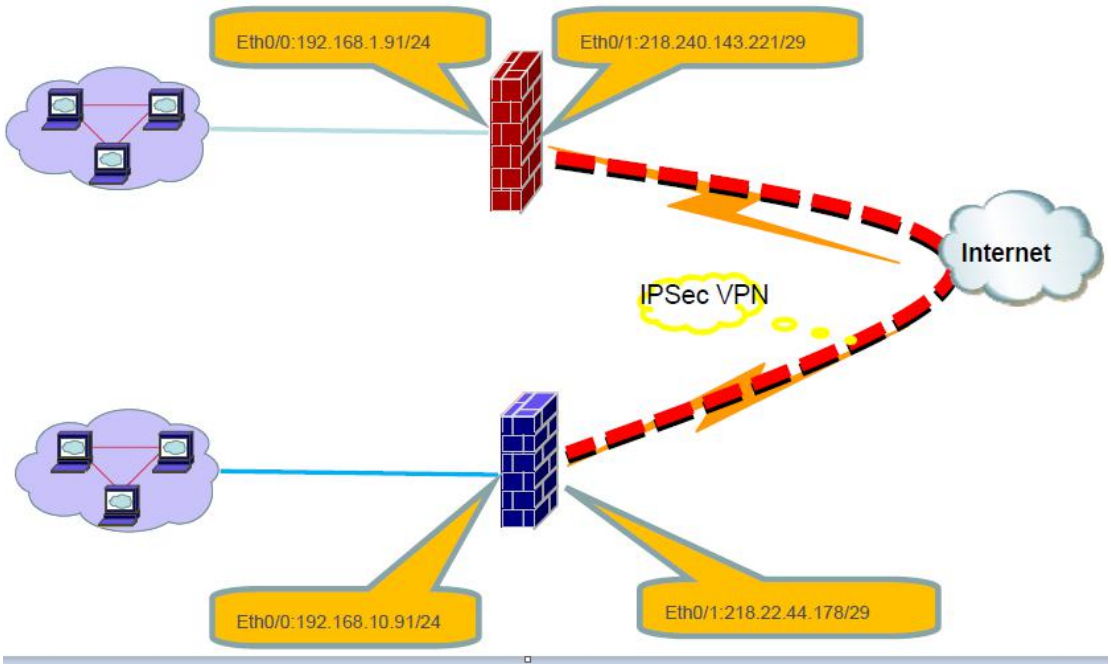
第八步：用户验证

内网用户打开 IE 后输入某网站后可以看到页面马上重定向到认证页面，我们输入 user2 的用户名和密码认证通过后，当我们访问某 ftp 时可以访问成功，当我们访问 web 界面时看到未能打开网页



6.3 防火墙 IPSEC VPN 配置

一、网络拓扑



注：该案例假设防火墙已完成了基本的上网配置

二、需求描述

防火墙 FW-A 和 FW-B 都具有合法的静态 IP 地址，其中防火墙 FW-A 的内部保护子网为 192.168.1.0/24，防火墙 FW-B 的内部保护子网为 192.168.10.0/24。要求在 FW-A 与 FW-B 之间创建 IPSec VPN，使两端的保护子网能通过 VPN 隧道互相访问。

三、配置步骤

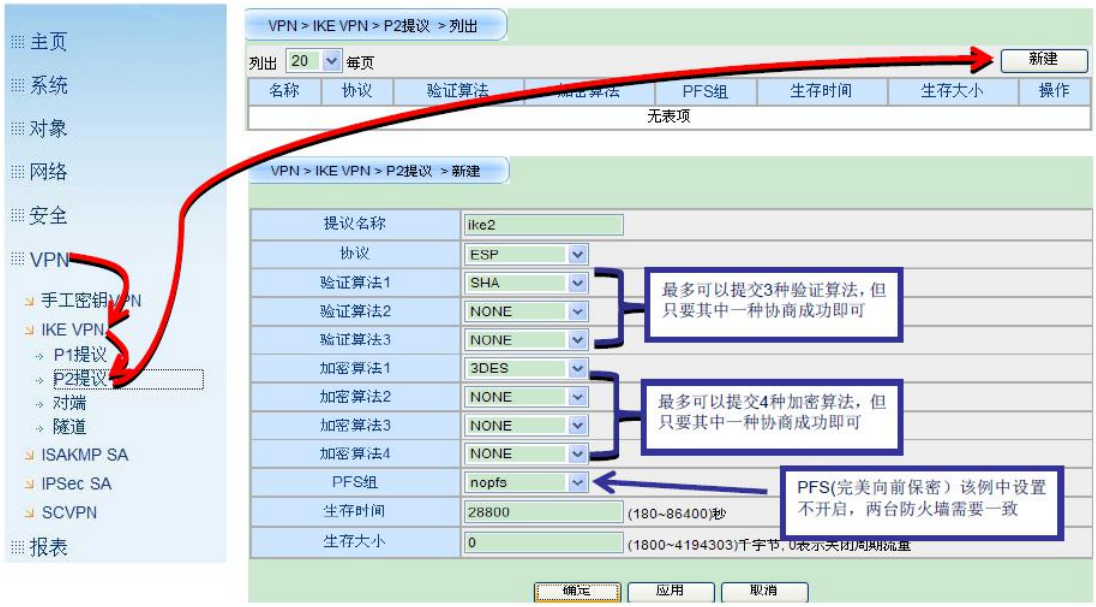
首先看下 **FW-A** 防火墙的配置

第一步：创建 **IKE** 第一阶段提议

在 VPN/IKE VPN/P1 提议中定义 IKE 第一阶段的协商内容，两台防火墙的 IKE 第一阶段协商内容需要一致。

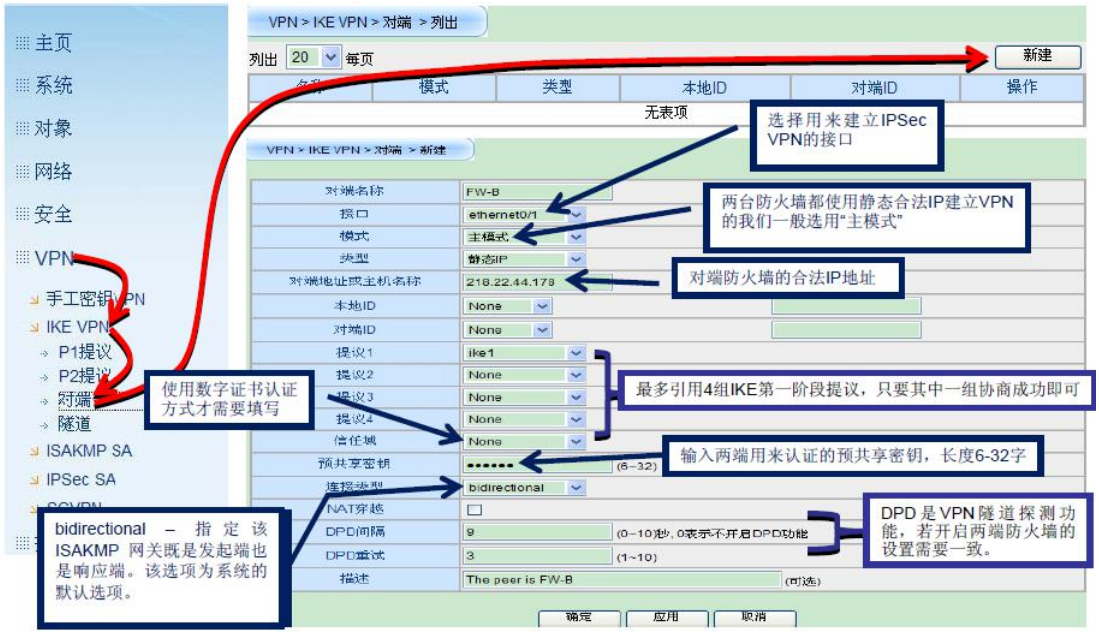
第二步：创建 **IKE** 第二阶段提议

在 VPN/IKE VPN/P2 提议中定义 IKE 第二阶段的协商内容，两台防火墙的第二阶段协商内容需要一致。



第三步：创建对等体（**peer**）

在 VPN/IKE VPN/对端中创建“对等体”对象，并定义对等体的相关参数

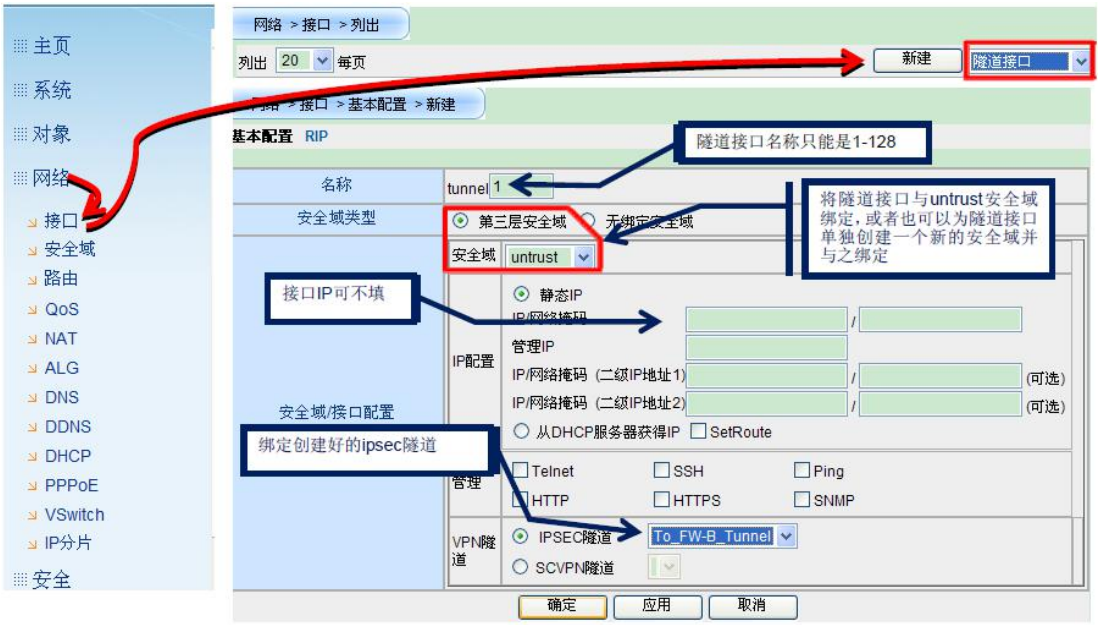


第四步：创建隧道

在 VPN/IKE VPN/隧道中创建到防火墙 FW-B 的 VPN 隧道，并定义相关参数。

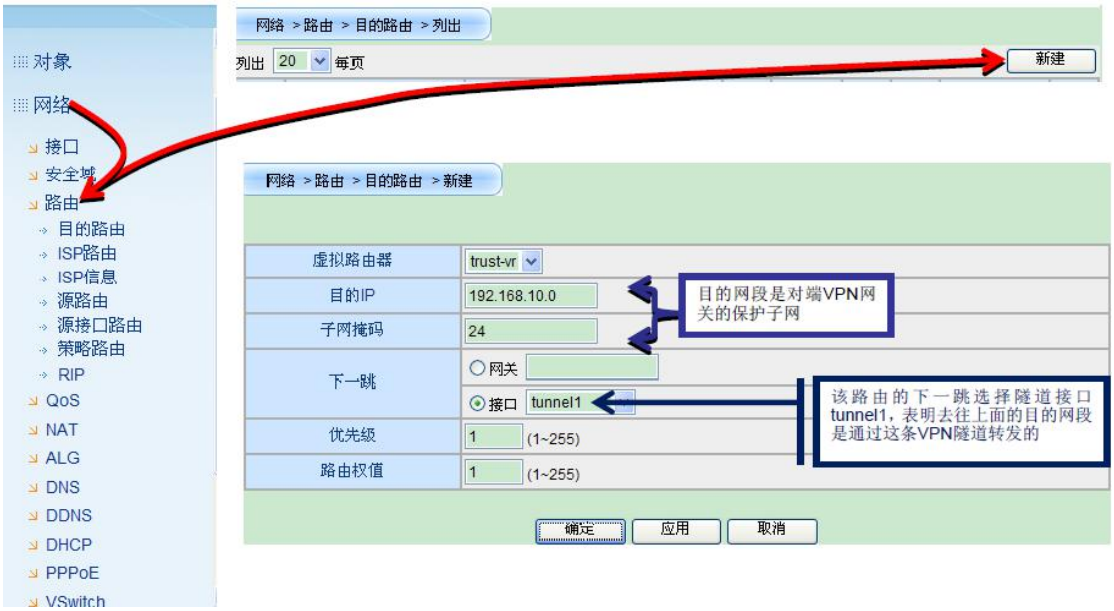
第五步：创建隧道接口并与 **ipsec** 绑定

在网络/接口中新建隧道接口指定安全域并引用 IPSEC 隧道



第六步：添加隧道路由

在网络/路由/目的路由中新建一条路由，目的地址是对端加密保护子网，网关为创建的 tunnel 口



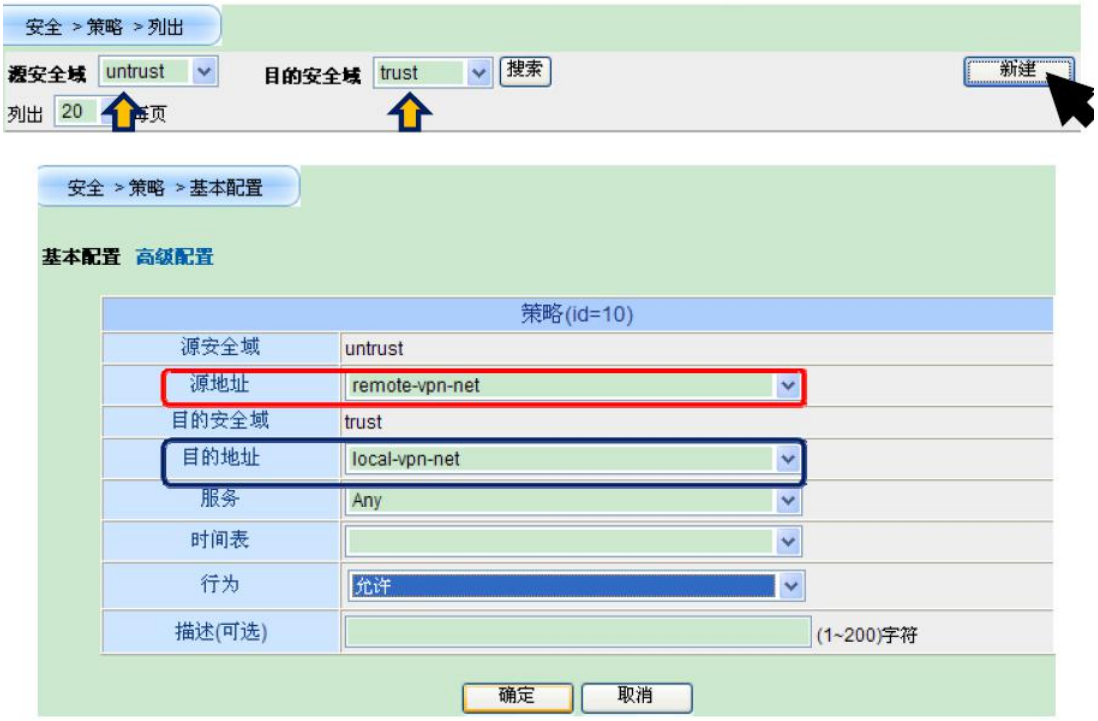
第七步：添加安全策略

在创建安全策略前首先要创建本地网段和对端网段的地址簿

创建完成两个地址簿后，在安全/策略中新建策略

允许本地 VPN 保护子网访问对端 VPN 保护子网

允许对端 VPN 保护子网访问本地 VPN 保护子网



关于 FW-B 防火墙的配置步骤与 FW-A 相同，不同的是某些步骤中的参数设置

创建 IKE 第一阶段提议

创建 IKE 第二阶段提议

创建对等体（peer）

创建隧道

创建隧道接

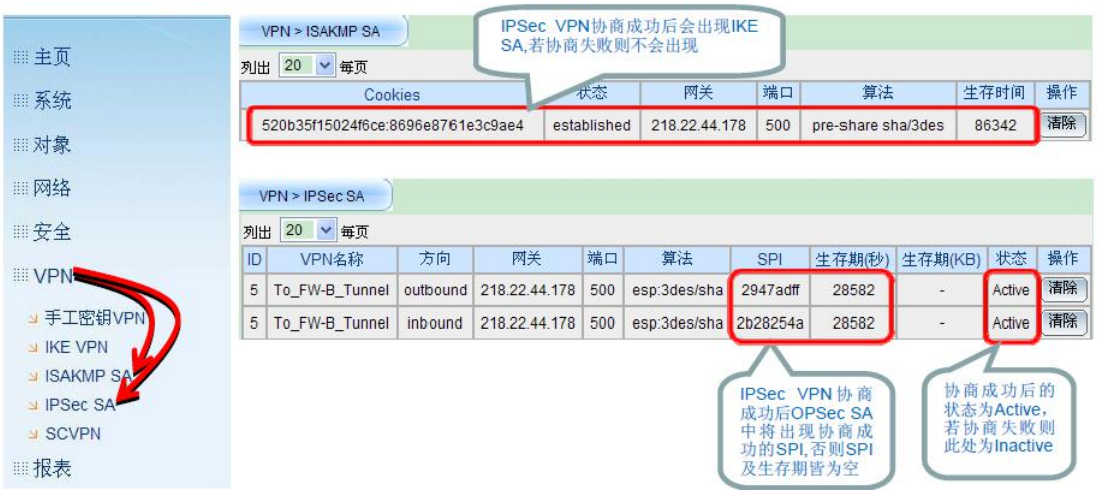
添加隧道路由

添加安全策略

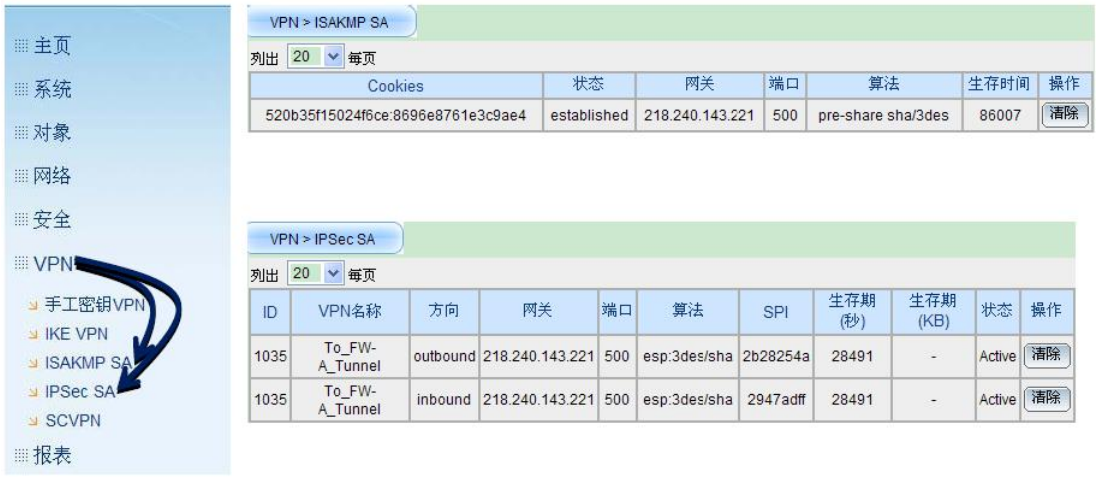
以上为 FW-B 配置的七个步骤不在重复。

第八步：验证测试

查看防火墙 FW-A 上的 IPSEC VPN 状态



查看防火墙 FW-A 上的 IPSec VPN 状态



模块七 综合实训

7.1 实验设计

为了模拟实际网络环境，实训利用实验室有关设备搭建实验环境，并在此环境下准本做进一步的功防实验。

7.1.1 网络拓扑

本实验设计拓扑图如图 7-1 所示。

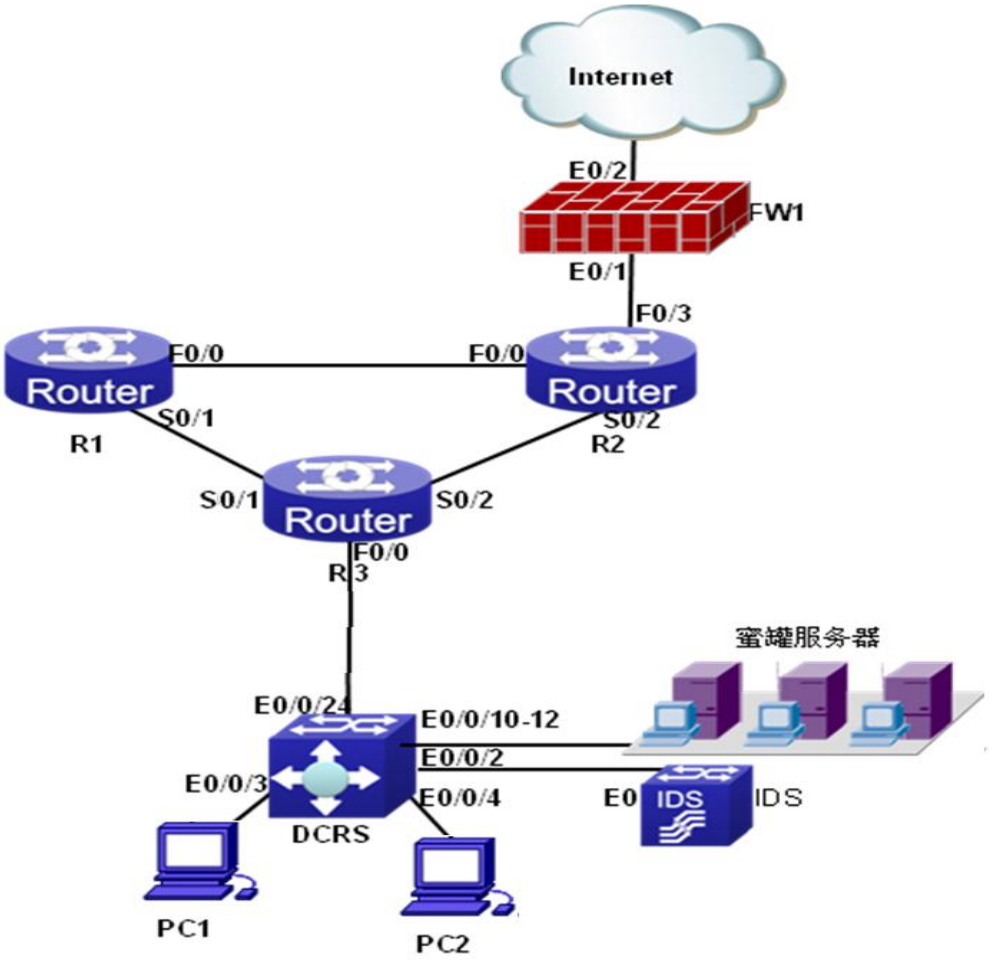


图 7.1 实验拓扑图

7.1.2 实验环境准备

1 设备要求

要完成图 7-1 所示拓扑图的网络环境的搭建，需以下设备支持。（以下以神舟数码网络公司的设备为例）

1）3 台路由器 DCR-2659

2）1 台三层交换机 DCRS-5950-28T

3）1 台防火墙 DCFW-1800S-H-V2

4）1 台入侵检测 DCNIDS-1800-M3

5）1 台蜜罐服务器 DCST-6000

6）2 台 PC 电脑

2. IP 地址规划

IP 地址规划如表 7-1 所示。

7.1.3 实验要求

(1).在 R1 与 R3 之间配置 PPP 协议，启用 PAP 封装。

(2).在 R1 与 R2 之间为以太链路

(3).在 R2 与 R3 之间配置 PPP 协议，启用 CHAP 封装。

(4).R1-R2-R3-DCRS 之间配置 RIPv2 路由协议。

(5)在 FW2 上设置 R1-R2-R3 所组成的外网网络可以访问蜜罐服务器。

(6)在 PC1 上安装 IDS 控制器，设置 IDS 记录所有内网收发数据。

(7)将所有的 PC 的 MAC 地址与端口进行绑定。

(8)在 DCRS 上配置 PC1 不允许访问蜜罐服务器。

(9)在 DCRS 上设置 PC2 能够 ping 通 PC1，但是 PC1 不能 Ping 通 PC2.

表 7-1 地址规划表

路由器 R1	
S0/1	10.0.0.1/8

F0/0	20.0.0.1/8	
路由器 R2		
S0/2	30.0.0.1/8	
F0/0	20.0.0.1/8	
F0/3	201.1.1.1/24	
路由器 R3		
S0/1	10.0.0.2/8	
S0/2	30.0.0.2/8	
F0/0	40.0.0.1/8	
防火墙 FW1		
E0/1	201.1.1.2/24	
E0/2	221.12.1.1/24	
三层交换机 DCRS		
E0/0/24	VLAN40	40.0.0.2/8
E0/0/10-12	VLAN10	192.168.1.1/24
E0/0/2	VLAN20	192.168.10.1/24
E0/0/3	VLAN5	192.168.20.1/24
E0/0/4	VLAN6	192.168.30.1/24
入侵检测 IDS		
E0	192.168.10.2/24	
蜜罐服务器		
E2	192.168.1.2/24	
E3	192.168.1.3/24	
E4	192.168.1.4/24	
PC1	192.168.20.2/24	
PC2	192.168.30.2/24	

7.2 实验主要设备

7.2.1 堡垒服务器

安全堡垒服务器系统（简称 DCSS），全称为 DigitalChina Secure SandBox，是神州数码网络公司专为网络安全攻防实验室研发的产品，是进行网络安全攻击和防御的模拟平台，锻炼学生动态网络安全维护的能力。其名取材于军事术语“沙盘”，这意味着安全堡垒服务器系统可以通过模拟实战演练战术和技术完成网络安全攻防教学。

提供多系统平台的教学：安全堡垒服务器系统系统为计算机及网络安全教育提供多系统平台的教学课件，在教学、培训过程中，根据需要可以启动基于不同操作系统平台的教学课件，满足所有教学环境的需求。

多种模式的攻防课件：安全堡垒服务器系统系统为计算机及网络安全教育提供多模式的安全攻防实验课件，能够进行各种安全威胁的攻防操作，针对不同的攻击防御模式，提供多种实验课件选择。

全程自主操作的攻防演练：安全堡垒服务器系统系统的全部课件均是将安全理论与实际环境和动手操作相结合的实验课程，所有的学习过程中，都需要通过实际动手进行实验操作，完成课件要求的安全威胁攻击以及针对该攻击的安全防御措施。通过不同的实验课程让学员亲身体验计算机及网络安全的攻防全过程，让学生从枯燥的理论学习中解脱出来，可以极大的提升学生学习网络安全知识的积极性，并帮助学生在未来的就业和职业发展奠定扎实、实用的技术基础和经验。

真实的攻防环境：目标主机、操作系统、漏洞均是真实存在的，入侵、防护过程完全真实。并非像一些实验系统只能模拟输出既定的结果，贴近实际。

模块化可独立部署或融合部署：可单独接入终端机器进行安全实验，更可配合神州数码 DCFW 防火墙、UTM 统一威胁管理系统、IDS 入侵检测系统、DCSM 内网安全管理系统、神州数码交换机、路由器、接入认证系统等基础安全及网络实验室模块组合成为真实攻防的全局环境中。

本实验使用的 1 台蜜罐服务器 DCST-6000

7.2.2 防火墙

防火墙(Firewall)是当今使用最为广泛的安全设备，防火墙历经几代发展，现今为非常成熟的硬件体系结构，具有专门的 Console 口，专门的区域接口。串行部署于 TCP/IP 网络中。将网络一般划分为内、外服务器区三个区域，对各区域实施安全策略以保护重要网络。本实验使用 DCFW-1800E-V2 防火墙，软件版本为：DCFOS-2.0R4。

7.2.3 IDS 入侵检测系统

网络变得日益复杂且更加开放，对 Internet 的依赖也更强，因此各公司感到网络越来越不安全了。通常，我们用一台防火墙来限制来自 Internet 的数据流进入我们的网络。但是防火墙并不是没有缺陷的，利用 IP 蒙骗技术和 IP 碎片技术，黑客们已经展示了他们穿过当今市场上大部分防火墙的本领。防火墙可以限制来自 Internet 的数据流进入我们的网络，但是对于来自防火墙内部的攻击却无能为

力。

因此，需要一种独立于常规安全机制的安全解决方案——一种能够破获并中途拦截那些能够攻破网络第一道防线的攻击。这种解决方案就是“入侵检测系统”。利用“入侵检测系统”连续监视网络通讯情况，寻找已知的攻击模式，当它检测到一个未授权活动时，软件会以预定方式自动进行响应，报告攻击、记录该事件或是断开未授权连接。

本实验使用的设备即 DCNIDS-1800 M/M2/G/G2，它是基于网络的实时入侵检测及响应系统，基于网络的入侵检测系统有许多仅依靠基于主机的入侵检测法无法提供的功能。实际上，许多客户最初使用入侵检测系统时，都配置了基于网络的入侵检测，因为它成本较低并且反应速度快。

DCNIDS-1800 M/M2/G/G2 是自动的、实时的网络入侵检测和响应系统，它采用了新一代的入侵检测技术，包括基于状态的应用层协议分析技术、开放灵活的行为描述代码、安全的嵌入式操作系统、先进的体系架构、丰富完善的各种功能，配合高性能专用硬件设备，是最先进的网络实时入侵检测系统。它以不引人注目的方式最大限度地、全天候地监控和分析企业网络的安全问题。捕获安全事件，给予适当的响应，阻止非法的入侵行为，保护企业的信息组件。

7.3 网络搭建

7.3.1 路由器、交换机 IP 地址配置

(1).路由器 R1 的 IP 地址配置

Router>enable //进入特权模式

Router #config //进入全局配置模式

Router_config#hostname Router-A　//重命名

Router-A_config#interface f0/0 //进入接口模式

Router-A_config_f0/0#ip address 20.0.0.1 255.0.0.0 //　设置 f0/0 的 IP　地址

Router-A_config_f0/0#no shutdown

Router-A_config_f0/0#^Z

Router-A#show interface f0/0 //验证

FastEthernet0/0 is up, line protocol is up //接口和协议都必须 up

Router-A_config#interface s0/1 //进入接口模式

Router-A_config_s0/1#ip address 10.0.0.1 255.0.0.0 // 设置 s0/1 的 IP 地址

Router-A_config_s0/1#no shutdown

(2). 路由器 R2 的 IP 地址配置

Router>enable //进入特权模式

Router #config //进入全局配置模式

Router_config#hostname Router-B //重命名

Router-B_config#interface f0/0 //进入接口模式

Router-B_config_f0/0#ip address 20.0.0.1 255.0.0.0 // 设置 f0/0 的 IP 地址

Router-B_config_f0/0#no shutdown

Router-B_config_f0/0#exit

Router-B_config#interface f0/3 //进入接口模式

Router-B_config_f0/3#ip address 201.1.1.1 255.255.255.0 // 设置 f0/3 的 IP 地址

Router-B_config_f0/3#no shutdown

Router-B_config_f0/3#exit

Router-B_config#interface s0/2 //进入接口模式

Router-B_config_s0/2#ip address 30.0.0.1 255.0.0.0 // 设置 s0/2 的 IP 地址

Router-B_config_s0/2#no shutdown

Router-B_config_s0/2#exit

(3). 路由器 R3 的 IP 地址配置

Router>enable //进入特权模式

Router #config //进入全局配置模式

Router_config#hostname Router-C //重命名

Router-C_config#interface f0/0 //进入接口模式

Router-C_config_f0/0#ip address 40.0.0.1 255.0.0.0 // 设置 f0/0 的 IP 地址

Router-C_config_f0/0#no shutdown

Router-C_config_f0/0#exit

Router-C_config#interface s0/1 //进入接口模式

Router-C_config_s0/1#ip address 10.0.0.2 255.0.0.0 // 设置 s0/1 的 IP 地址

Router-C_config_s0/1#no shutdown

Router-C_config_f0/3#exit

Router-C_config#interface s0/2 //进入接口模式

Router-C_config_s0/2#ip address 30.0.0.2 255.0.0.0 // 设置 s0/2 的 IP 地址

Router-C_config_s0/2#no shutdown

Router-C_config_s0/2#exit

(4).三层交换机 DCRS 的 IP 地址设置、端口划分

switch#***set default***

switch#***write***

switch#***reload***

switch (Config)# ***vlan 40***

switch (Config-Vlan40)#

switch (Config-Vlan40)#switchport interface ethernet 0/0/24

switch (Config-Vlan40)#exit

switch(Config)#***interface vlan 40***

switch (Config-If-Vlan40)#***ip address 40.0.0.2 255.0.0.0***

switch (Config-If-Vlan40)#***no shutdown***

switch (Config-If-Vlan40)#***exit***

switch (Config)# ***vlan 10***

switch (Config-Vlan10)#

switch (Config-Vlan10)#switchport interface ethernet 0/0/10-12

switch (Config-Vlan10)#exit

switch(Config)#***interface vlan 10***

switch (Config-If-Vlan10)#***ip address 192.168.1.1 255.255.255.0***

switch (Config-If-Vlan10)#***no shutdown***

switch (Config-If-Vlan10)#***exit***

switch (Config)# ***vlan 20***

switch (Config-Vlan20)#

switch (Config-Vlan20)#switchport interface ethernet 0/0/2

switch (Config-Vlan20)#exit

switch(Config)#***interface vlan 20***

switch (Config-If-Vlan20)#***ip address 192.168.10.1 255.255.255.0***

switch (Config-If-Vlan20)#***no shutdown***

switch (Config-If-Vlan20)#***exit***

switch (Config)# ***vlan 5***

switch (Config-Vlan5)#

switch (Config-Vlan5)#switchport interface ethernet 0/0/3

switch (Config-Vlan5)#exit

switch(Config)#***interface vlan 5***

switch (Config-If-Vlan5)#***ip address 192.168.20.1 255.255.255.0***

switch (Config-If-Vlan5)#***no shutdown***

switch (Config-If-Vlan5)#***exit***

switch (Config)# ***vlan 6***

switch (Config-Vlan6)#

switch (Config-Vlan6)#switchport interface ethernet 0/0/4

switch (Config-Vlan6)#exit

switch(Config)#***interface vlan 6***

switch (Config-If-Vlan6)#***ip address 192.168.30.1 255.255.255.0***

switch (Config-If-Vlan6)#***no shutdown***

switch (Config-If-Vlan6)#***exit***

7.3.2 配置路由器、交换机之间的的多种协议

(1) R1 与 R3 之间配置 PPP 协议，启用 PAP 封装

Router-A_config#***aaa authentication ppp test local***
Router-A_config#***username RouterC password digitalchinaB*** //设置帐号密码
Router-A_config#***interface s0/1*** //进入接口模式
Router-A_config_s0/1#***ip address 10.0.0.1 255.0.0.0*** //配置 IP 地址（已配）
Router-A_config_s0/1#***encapsulation PPP*** //封装 PPP 协议
Router-A_config_s0/1#***ppp authentication pap test*** //设置验证方式
Router-A_config_s0/1#***ppp pap sent-username RouterA password digitalchinaA***
//设置发送给对方验证的帐号密码

Router-A_config_s0/1#***physical-layer speed 64000*** //配置 DCE 时钟频率

Router-A_config_s0/1#***no shutdown***

Router-C_config#aaa authentication ppp test local

Router-C_config#username RouterA password digitalchinaA !设置帐号密码

Router-C_config#interface s0/1 //进入接口模式

Router-C_config_s0/1#ip address 192.168.1.2 255.255.255.0 //配置 IP 地址

Router-C_config_s0/1#encapsulation PPP //封装 PPP 协议

Router-C_config_s0/1#ppp authentication pap test //设置验证方式

Router-C_config_s0/1#ppp pap sent-username RouterC password digitalchinaC //设置发送给对方验证的帐号密码

Router-C_config_s0/1#shutdown

Router-C_config_s0/1#no shutdown //查看配置，测试连通性。

(2). 在 R2 与 R3 之间配置 PPP 协议，启用 CHAP 封装

Router-B_config# aaa authentication ppp test local

//定义一个名为 test，使用本地数据进行验证的 aaa 验证方法

Router-B_config#username RouterC password digitalchina //设置帐号密码路由

Router-B_config#interface s1/0 //进入接口模式

Router-B_config_s1/0#ip address 30.0.0.1 255.0.0.0 //配置 IP 地址（已配置）

Router-B_config_s1/0#encapsulation PPP //封装 PPP 协议

Router-B_config_s1/0# ppp authentication chap test //设置验证方式

Router-B_config_s1/0#ppp chap hostname RouterB //设置发送给对方验证的帐号

Router-B_config_s1/0#physical-layer speed 64000 //配置 DCE 时钟频率

Router-B_config_s1/0#no shutdown

Router-B_config_s1/0#^Z //按 ctrl + z 进入特权模式

Router-C_config#aaa authentication ppp test local

//定义一个名为 test，使用本地数据进行验证的 aaa 验证方法

Router-C_config#username RouterB password digitalchina !设置帐号密码

Router-C_config#interface s1/0 //进入接口模式

Router-C_config_s1/0#ip address 192.168.1.2 255.255.255.0 //配置 IP 地址

Router-C_config_s1/0#encapsulation PPP //封装 PPP 协议

Router-C_config_s1/0#ppp authentication chap test //设置验证方式

Router-C_config_s1/0#ppp chap hostname RouterC //设置发送给对方验证的帐号

Router-C_config_s1/0#shutdown

Router-C_config_s1/0#no shutdown

Router-C_config_s1/0#^Z //按 ctrl + z 进入特权模式

查看配置，测试连通性。

(3). R1-R2-R3-DCRS 之间配置 RIPv2 路由协议

Router-A_config#router rip //启动 RIP 协议

Router-A_config_rip#network 10.0.0.0 //宣告网段

Router-A_config_rip#network 20.0.0.0

Router-A_config_rip#^Z

Router-B_config#router rip

Router-B_config_rip#network 20.0.0.0

Router-B_config_rip#network 30.0.0.0

Router-B_config_rip#^Z

Router-C_config#router rip

Router-C_config_rip#network ***20.0.0.0***

Router-C_config_rip#network ***30.0.0.0***

Router-C_config_rip#network ***40.0.0.0***

Router-C_config_rip#^Z

switch (Config)#router rip

switch (config-router)#network vlan 40

switch (config-router)#exit

7.3.3 配置 PC

在 PC1 上安装 IDS 控制器，设置 IDS 记录所有内网收发数据

(1).配置 PC1 的 IP 地址：192.168.20.2，子网掩码：255.255.255.0。

(2). **SQL Server** 数据库安装过程

- 点击安装程序。

- 出现欢迎窗口。如图 7-2 所示。

图 7-2 欢迎窗口

- 单击下一步，出现计算机名称的窗口，选择本地计算机。
- 单击下一步，出现安装选择窗口，选择‘创建新的 SQL Server 实例，或安装“客户端工具”’ 。如图 7-3 所示。

图 7-3 安装选择窗口

- 单击下一步，出现用户信息窗口。输入姓名和公司名称。
- .单击“下一步”出现许可协议窗口。请仔细阅读许可协议。单击“是”，继续进行安装。
- 单击“是”，出现安装定义窗口，选择“服务器和客户端工具”。
- 单击“下一步”，选择“默认”。
- 单击“下一步”，出现安装类型窗口，选择“典型”并且指定目标文件夹。如图 7-4 所示。.

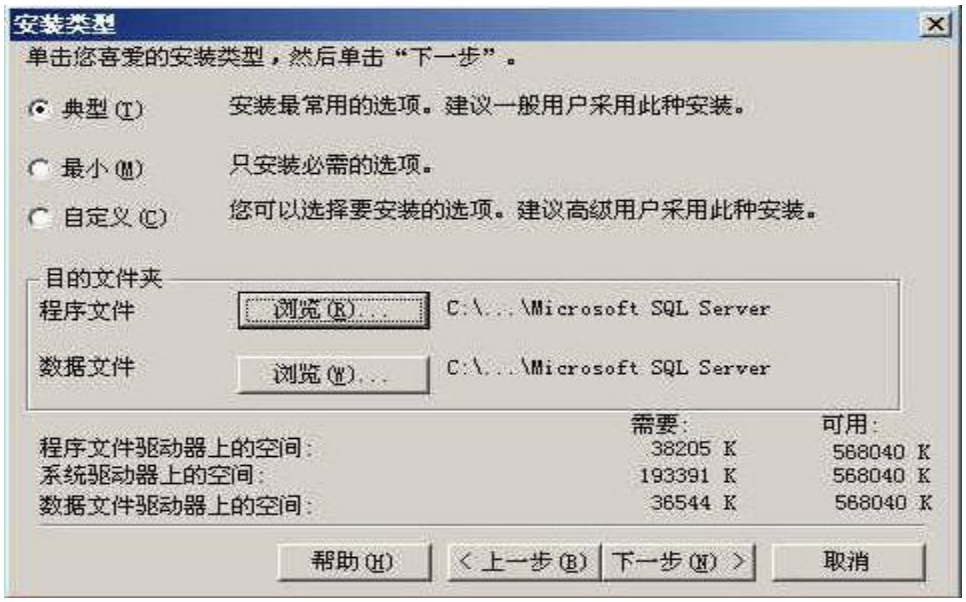


图 7-4 安装类型窗口

- . 单击“下一步”，出现服务帐户窗口，选择“使用本地系统帐户”。
- . 单击“下一步”，出现身份验证模式窗口，选择混合模式，输入登录密码。
- . 单击“下一步”，提示安装程序已拥有足够信息。
- . 单击“下一步”，选择许可模式。
- . 单击“继续”，提示“现在将开始安装 Microsoft Data Access Components 2.6”
- .安装完毕

(3). 安装 **LogServer**

LogServer 从某种意义上说是一个数据库管理器。它包含 LogServer 服务和 DB（数据库）两部分。为了便于用户操作， LogServer 数据库管理器被集成在 console（控制台）上，用户可以通过 console 直接管理 LogServer。

1）将 DCNIDS-1800 M/M2/M3/G/G2/G3 产品光盘插入光盘驱动器，安装程

序自动启动。在安装向导中选择安装 LogServer 组件。

2.） 安装程序正在解压缩文件。

3）.出现“欢迎”窗口。

4）选择安装路径，建议选择安装程序默认的安装路径，点击“下一步”。

5）安装完成，出现“数据服务初始化配置”窗口（也可以通过点击“开始—程序—入侵检测系统—入侵检测系统（网络）—DCNIDS-1800M/M2/M3/G/G2/G3 数据服务安装”进入此窗口，这里要输入正确的服务器地址 192.168.20.2，以及其它信息。

6）输入配置信息后，点击“测试”，配置正确会提示“数据库测试连接成功!”

(4).安装事件收集器

一个大型分布式应用中，用户希望能够通过单个控制台完全管理多个传感器，允许从一个中央点分发安全策略，或者把多个传感器上的数据合并到一个报告中去。用户可以通过安装一个事件收集器来实现集中管理传感器及其数据。事件收集器还可以控制传感器的启动和停止，收集传感器日志信息，并且把相应的策略发送传感器，以及管理用户权限、提供对用户操作的审计功能。

安装过程略

(5).安装许可密钥

密钥文件定义了 DCNIDS-1800 M/M2/M3/G/G2/G3 的认证信息及用户信息。它包含了所授权的产品、升级服务时限、许可证到期日期（只限 Demo key）以及用户注册信息。因此必须拥有许可密钥，DCNIDS-1800 M/M2/M3/G/G2/G3 才能正常工作。如果没有密钥，DCNIDS-1800M/M2/M3/G/G2/G3 既不能分析网络上的活动，也不能分析计算机系统上的活动。

接收到密钥文件之后，必须安装许可密钥，否则系统不能启动。安装许可密要之前必须先安装好事件收集器，因为许可密钥将安装在事件收集器的安装目录中 License 目录下。安装步骤略。

(6) 安装控制台

控制台是图形用户界面（GUI），通过控制台可以完成如下工作：配置和管理所有的传感器并接收事件报警；配置和管理对于不同安全事件的响应方式；配置和管理 LogServer；生成并查看关于安全事件、系统事件和审计事件的统计报告。

(7)启动应用服务

应用服务包括“事件收集服务”、“安全事件响应服务”和“IDS 数据管理

服务”，只有服务启动后，系统才能正常工作。

(8)配置管理控制台

第一次登录系统后需要配置系统平台。首先登录系统，进入组件管理窗口。在组件结构图中添加组件（第一次配置时需要添加传感器组件）。然后选中组件，在属性窗口中配置组件属性，包括配置传感器、LogServer 的属性。可以通过查看组件显示图标判断组件的状态（连通或断开）。

1）添加传感器

2）添加 LogServer

3）配置 LogServer

(9). 配置策略

策略是一个文件，其中包含称为“安全事件签名”的一列项目，这些项目确定了传感器所能监测的内容。签名是网络传感器用来检测一个事件或一系列事件的内部代码，这些事件有可能表明网络受到了攻击，也可能提供安全方面的信息。

7.3.4 配置交换机端口镜像

Switch(Config)#monitor session 1 source interface ethernet 0/0/3 both

Switc (Config)#monitor session 1 destination interface ethernet 0/0/2

Switch(Config)#monitor session 1 source interface ethernet 0/0/4 both

Switc (Config)#monitor session 1 destination interface ethernet 0/0/2

Switch(Config)#monitor session 1 source interface ethernet 0/0/10 both

Switc (Config)#monitor session 1 destination interface ethernet 0/0/2

Switch(Config)#monitor session 1 source interface ethernet 0/0/11 both

Switc (Config)#monitor session 1 destination interface ethernet 0/0/2

Switch(Config)#monitor session 1 source interface ethernet 0/0/12 both

Switc (Config)#monitor session 1 destination interface ethernet 0/0/2

(MAC 地址与端口绑定)

配置文件如下：

Switch(Config)#mac-address-table static address 00-a0-c1-57-ff vlan5 interface Ethernet 0/0/3 //00-a0-c1-57-ff 为 PC1 的 MAC 地址

Switch(Config)#mac-address-table static address a2-c2-1b-32-ff vlan6 interface Ethernet 0/0/4 // a2-c2-1b-32-ff 为 PC2 的 MAC 地址

7.3.5 交换机端口访问配置

(1). PC1 不允许访问蜜罐服务器

ACL (Access Control Lists)是交换机实现的一种数据包过滤机制，通过允许或拒绝特定的数据包进出网络，交换机可以对网络访问进行控制，有效保证网络的安全运行。用户可以基于报文中的特定信息制定一组规则（rule），每条规则都描述了对匹配一定信息的数据包所采取的动作：允许通过（permit）或拒绝通过（deny）。用户可以把这些规则应用到特定交换机端口的入口或出口方向，这样特定端口上特定方向的数据流就必须依照指定的 ACL 规则进出交换机。通过 ACL，可以限制某个 IP 地址的 PC 或者某些网段的 PC 的上网活动。用于网络管理。配置过程如下：

Switch(Config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1

Switch (Config)# access-list 11 deny 192.168.20.2 0.0.0.255

Switch (Config)# firewall enable

Switch (Config)# firewall default permit

Switch (Config)# interface ethernet 0/0/3

Switch (Config-Ethernet0/0/3)#ip access-group 11 in

Switch (Config-Ethernet0/0/3)#exit

(2). 在 DCRS 上设置 PC2 能够 ping 通 PC1，但是 PC1 不能 Ping 通 PC2.

Switch(Config)#ip access-list extended test2

Switch(Config-Ext-Nacl-test2)#deny icmp 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255 // 拒绝 192.168.20.0/24 ping 数据

Switch (Config-Ext-Nacl-test2)#exit

Switch (Config)#firewall enable// 配置访问控制列表功能开启

Switch (Config)#firewall default permit //默认动作为全部允许通过

Switch (Config)#interface ethernet 0/0/3 //绑定 ACL 到端口

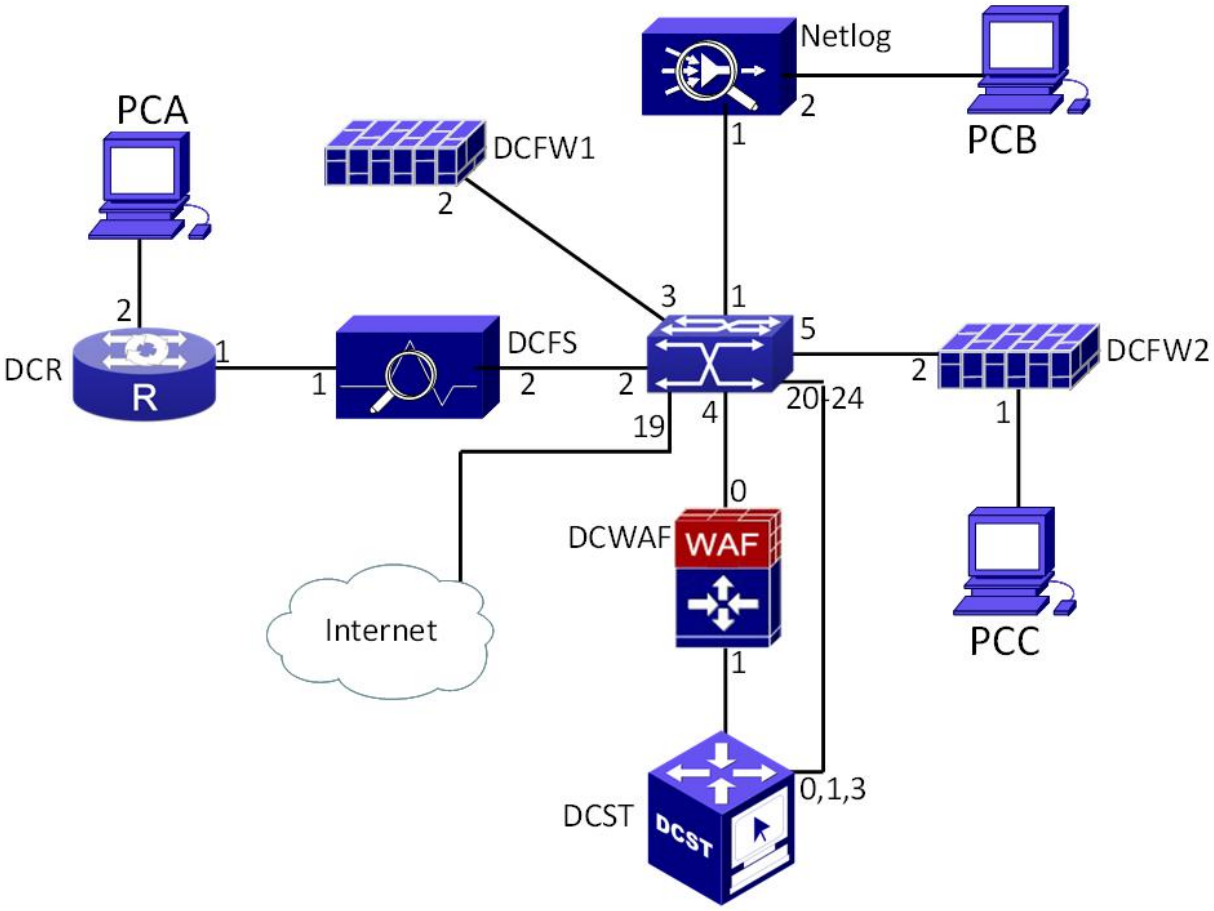
Switch (Config-Ethernet0/0/3)# ip access-group test2 in

7.4 综合实训二

第一部分：网络搭建

（注意：第一部分提交所有设备配置文件，并存放到“提交专用 U 盘”中的“网络设备配置文件”目录下）

1、拓扑结构图



图中 DCRS 的 4、19-24 接口；DCWAF 的 0、1 接口；DCST 的 0-4 接口已经连接完毕，不需要学生进行连接，比赛途中不得其进行改动，不得使 DCST 重启、关机、断电，否则扣除考试 50%分值。

2、IP 地址规划

地址表中的 X 代表本组组编号。

如：一组组编号为 6，DCR 的 1 接口 ip 地址为：192.6.0.1

DCR	1 接口	192.X.0.1/24
	2 接口	192.X.1.1/24
WAF	0 接口（透明模式）	192.X.2.1/24（管理地址）
	1 接口（透明模式）	192.X.2.1/24（管理地址）
DCFS	1 接口	192.X.0.100/24（管理地址）
	2 接口	192.X.0.100/24（管理地址）
NetLog	1 接口	192.X.4.100/24（管理地址）
	2 接口	192.X.4.100/24（管理地址）
DCFW1	2 接口	192.X.3.2/24
DCFW2	1 接口	192.X.7.2/24
	2 接口	192.X.6.1/24
DCRS	1 接口	Vlan 10: 192.X.4.2/24
	2 接口	Vlan 20: 192.X.0.2/24
	3 接口	Vlan 30: 192.X.3.1/24
	5 接口	Vlan 40: 192.X.6.2/24
	4 接口；20-24 接口	Vlan 50: 192.X.2.2/24
	19 接口	Vlan 60:111.0.0.X/24
PCA		192.X.1.2/24
PCB		192.X.4.1/24
PCC		192.X.7.1/24
PCC		192.X.7.1/24

3、赛题内容：

DCFW、DCWAF、DCFS、DCBI-Netlog 设备需要根据题号将配置过程与验证结果进行截图，并提供相应说明，录入设备相对应的文档中，要求在文档中注明截图所属题号。

1) 根据题目地址列表正确配置设备接口信息。

2) PCA 想要与 PCC 相互访问，需要通过加密的隧道传输数据，现在要求在 DCR 与 DCFW2 上配置 IPsecVPN，以保证数据的安全性。

3) 通过网络内的流量管理网关，在晚 16:00-23:00 之间 PCA 的 P2P 流量限制为 10M

4) 同时限制 PCa 的会话数为 100 条。

5) 网络有上网行为管理设备，通过其监控 PCB 的 BT 下载信息。

6) 在监控 PCB 的同时，还要监控 PCA 的 http 上传与下载。

7) 当 PCA 想要访问 PCC 时，需要通过 web 认证，在 DCFW2 上进行设置。

8) PC**B** 用户不会配置 IP 地址，所以在 DCFW1 上配置 DHCP 服务，为 PCB 分配 IP 地址。

9) 公司有一台网站服务器（DCST），为了保护其不受到伤害，在 web 应用防火墙上配置禁止外界扫描。

10) 同时针对网络爬虫进行相应的配置。

11) 全网运行 OSPF，使其能够相互通信。

第二部分 系统加固

1 加固系统

1) 要求设置交互式登陆不需要按 CTRL+ALT+DEL（6%）

截图说明：

2) 要求用户设置安全策略，不允许 SAM 帐户的匿名枚举

截图说明：

3) 要求用户设置安全策略，不允许 SAM 帐户的和共享的匿名枚举

截图说明：

4) 停止并禁用 Task Schedule 服务

截图说明：

5) 停止并禁用 Remote Registry 服务

截图说明：

6) 停止并禁用 Print spooler 服务

截图说明：

7) 开启审核对象访问，成功与失败

截图说明：

8) 开启审核目录服务访问，成功与失败

截图说明：

9) 开启审核特权使用，成功与失败

截图说明：

10) 开启审核系统事件，成功与失败

截图说明：

2 加固 WEB 服务(40%)

1) 对站点根文件夹启用审核功能

截图说明：

2) 优化网站根目录的访问权限

截图说明：

3) 设置 IIS 记录日志字段内容，包括:日期、时间、客户端 IP、服务器 IP、服务器端口、方法

截图说明：

4) 设置 IIS 日志格式为 MICROSOFT IIS 日志格式

第三部分：安全评估

作为一名成熟的安全工程师，在工作过程中发现你所控制的服务器问题非常大，为了能够让上级重视这个问题，你必须向上级反映。你现在需要完成三件事：

1、对整个网络系统的安全性进行评估，并根据模板填写电子版《审计报告》。

2、通过审计过程，设计并填写电子版的《整改方案》。

3、通过前 2 个步骤，填写最终的电子版《评估报告》。