信息安全概论 课程实验（实践）指导书

《信息安全概论》课程组 编著

上海海洋大学海洋智能信息实验教学示范中心

目 录

实验一 密码学基本实验

3DES、AES、RSA 加/解密实验

一、实验目的

1、学习 3DES 密码算法原理，学习 3DES 密码算法编程实现

2、学习 AES 密码算法的原理，学习 AES 密码算法的编程实现

3、学习 RSA 密码算法的原理，学习 RSA 密码算法的编程实现

二、实验环境

Windows7

工具：C:\tools\密码学课程\01 密码学算法\04 分组密码\023des 密码算法

工具：C:\tools\密码学课程\01 密码学算法\04 分组密码\03aes 密码算法

工具：C:\tools\密码学课程\01 密码学算法\05 公钥密码\01rsa 密码算法

三、实验内容

1、3DES 加密/解密

2、AES 加密/解密

3、RSA 加密/解密

四、实验步骤

1、3DES 加密/解密

1.1 运行程序，即可得到 3DES 加密算法的结果。如图 1-1 所示

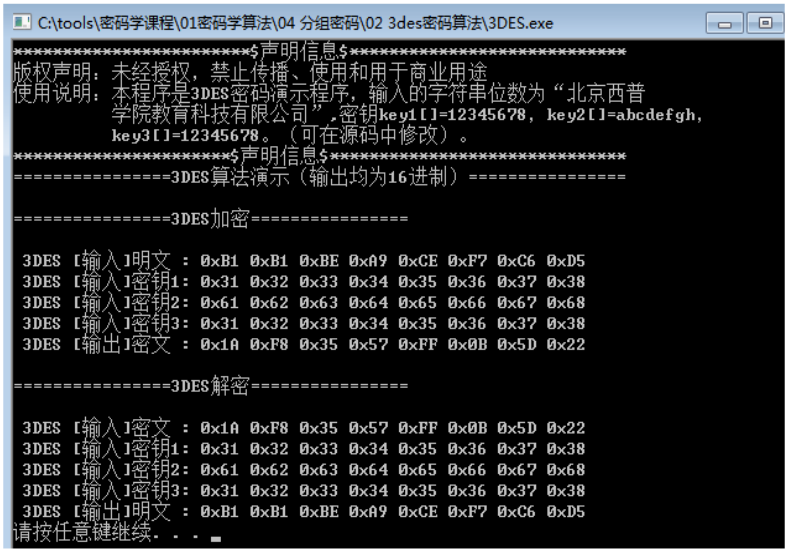


图 1-1

2、AES 加密/解密

2.1 字符串加解密

2.1.1 运行文件【AES.exe】，程序运行界面。如图 2-1 所示

图 2-1

2.1.2 在第一个框格中输入【helloworld】，点击【字符串加密】，即可在第一个框格中输入密文。如图 2-2 所示

图 2-2

2.1.3 将得到的密文字符串拷贝到第二个框格中。如图 2-3 所示

图 2-3

2.1.4 点击【字符串解密】，即可得到明文。如图 2-4 所示

图 2-4

2.2 文件文件加解密

2.2.1 新建 xipu.txt，其文件内容如下。如图 2-5 所示

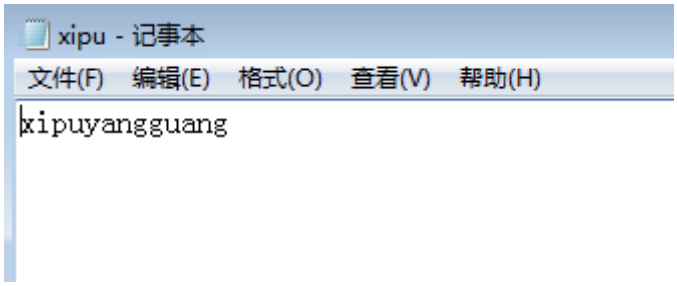


图 2-5

2.2.2 点击【浏览】，选择要加密的文件【xipu.txt】。如图 2-6 所示

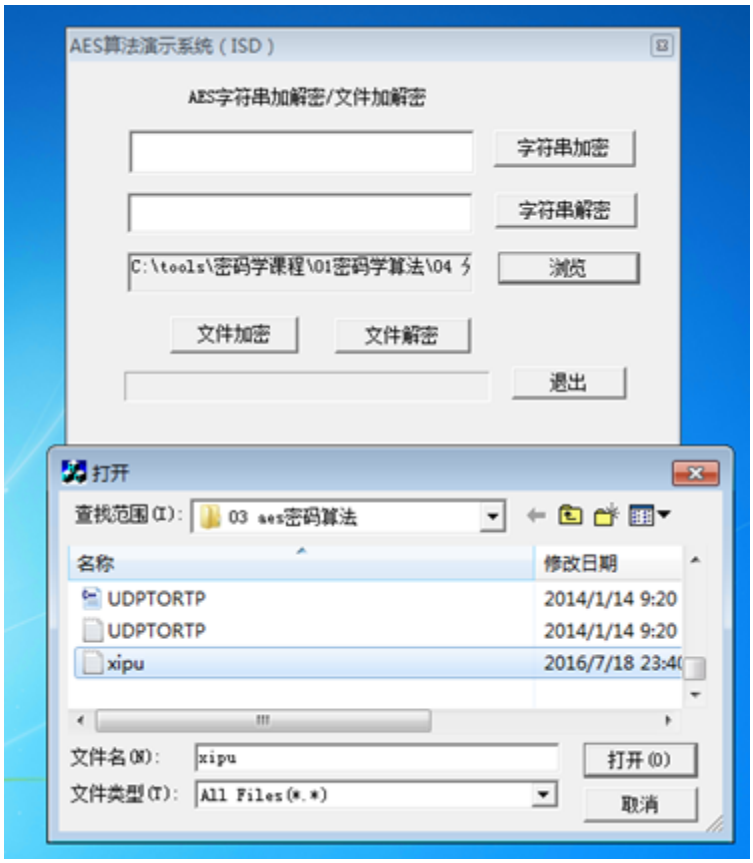


图 2-6

2.2.3 点击【文件加密】，会提示加密成功，并生成一个以【.en】，为后缀名的文件。如图 2-7 所示

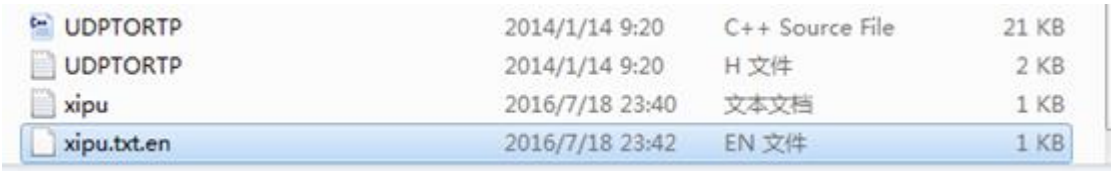


图 2-7

2.2.4 点击【浏览】，选择加密后的文件，点击【文件解密】，即可生成一个以【.de】为后缀名的文件。如图 2-8 所示

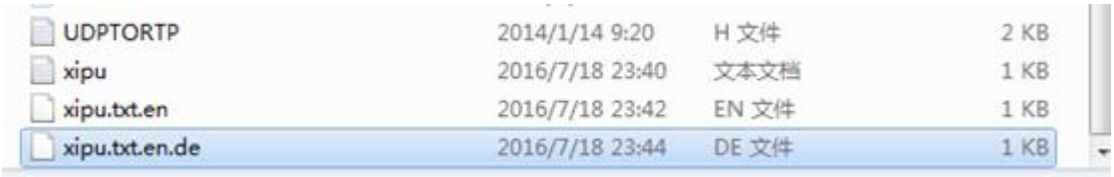


图 2-8

2.2.5 用记事本打开文件【.de】，即可查看被解密的明文文件。如图 2-9 所示

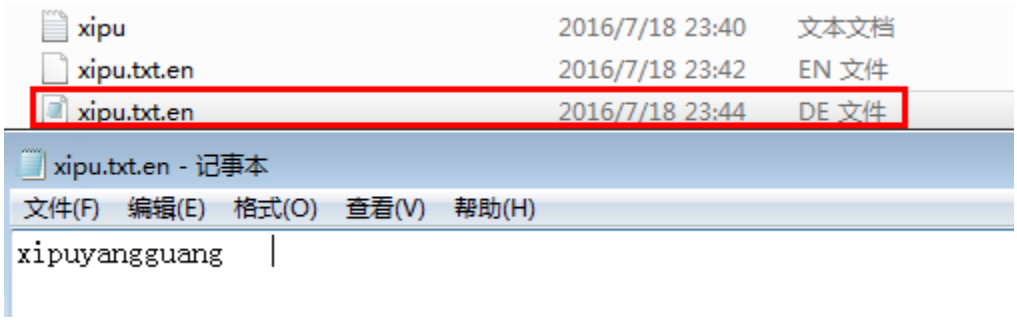


图 2-9

3、RSA 加密/解密

3.1 运行 rsa.exe 程序，结果如下。如图 3-1 所示

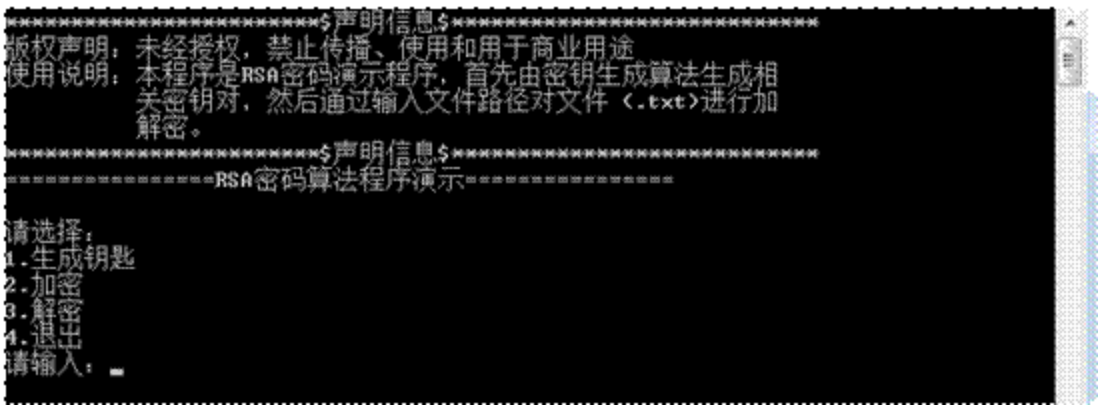


图 3-1

3.2 输入 1，输入存放公钥和私钥的文件名，即可在程序同级目录下生成相应文件。如图 3-2 所示

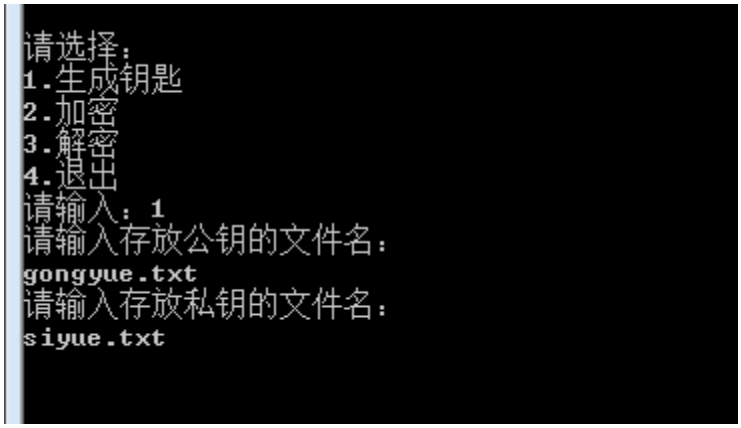


图 3-2

3.3 选择 2，输入存放公钥的文件名和需要加密的文件【hello.txt】（若无该文件，可先行在软件目录下创建，内容为 helloWorld!）和需要输出的文件名【enhello.txt】。如图 3-3 所示

图 3-3

3.4 对比明文文件内容和密文文件内容。如图 3-4 所示

图 3-4

3.5 解密文件，进行类似的操作即可。

实验二 哈希算法及破解实验

MD5 算法、SHA-1 算法、RainbowCrack 彩虹表破解密码 hash、暴力破解 MD5crack

一、实验目的

1、学习 MD5 算法的原理，学习 MD 算法的编程实现

2、学习 SHA-1 密码算法的原理，学习 SHA-1 密码算法的编程实现

3、使用彩虹表破解散列值 b0baee9d279d34fa1dfd71aadb908c3f

4、掌握 MD5 破解的方法、过程和原理，增强对 MD5 算法安全性的认识

二、实验环境

Windows7

工具：C:\tools\密码学课程\01 密码学算法\06hash 算法\02md5 算法

工具：C:\tools\密码学课程\01 密码学算法\06hash 算法\03sha-1 算法

Kali

C:\实验工具集\05_日常应用安全

三、实验内容

1、通过 MD5 算法，输入明文得到消息摘要值

2、通过 SHA-1 算法，直接输出明文消息的摘要值

3、RainbowCrack 破解 hash 值

4、暴力破解 MD5crack

四、实验步骤

1、通过 MD5 算法，输入明文得到消息摘要值

1.1、运行程序，输入明文，即可得到摘要值。如图 1-1 所示

图 1-1

2、通过 SHA-1 算法，直接输出明文消息的摘要值

2.1、运行程序，结果如下。如图 2-1 所示

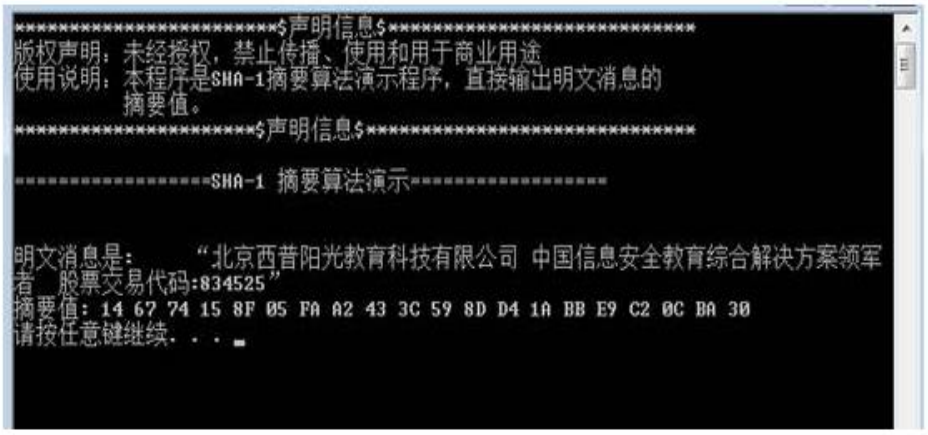


图 2-1

3、RainbowCrack 破解 hash 值

3.1、点击左边打开终端。如图 3-1 所示

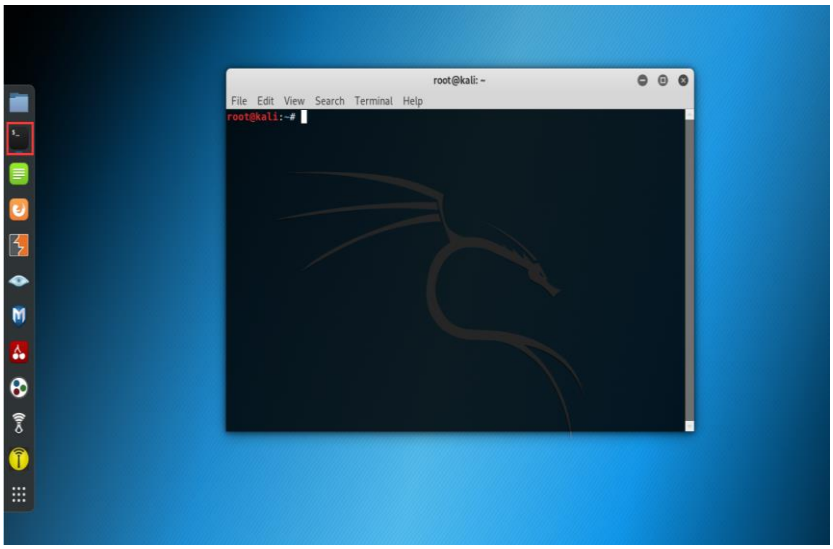


图 3-1

3.2、在终端输入命令 rcrack 命令，显示命令格式信息。如图 3-2 所示

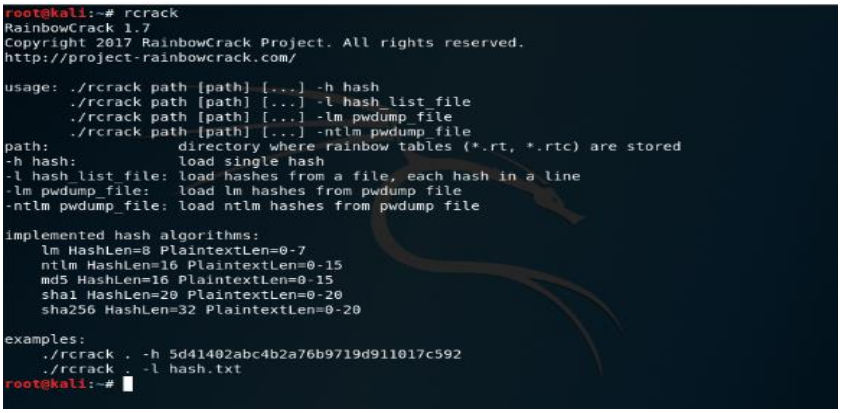


图 3-2

3.3、在终端中输入 rtgen，显示参数格式。如图 3-3 所示

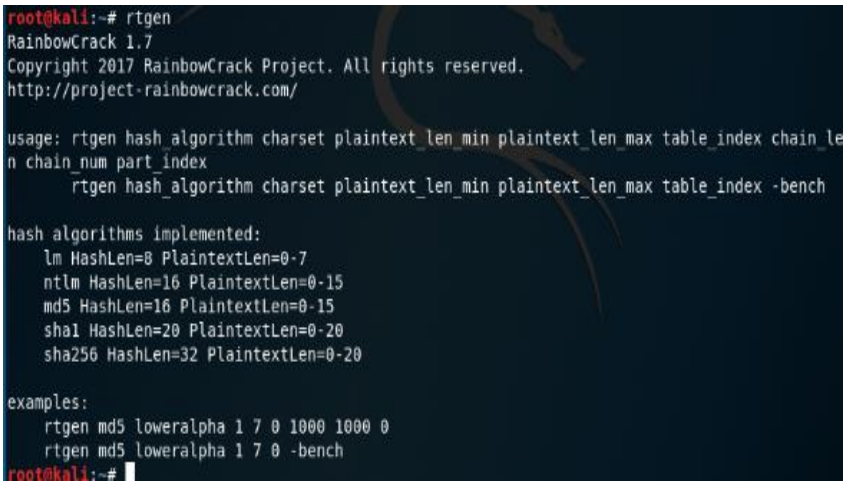


图 3-3

3.4、利用 rtgen 命令创建一个的彩虹表，在终端中输入 cd /usr/share/rainbowcrack 切换目录，输入 rtgen md5 numeric 5 5 0 100 2000 0 生成彩虹表。如图 3-4 所示

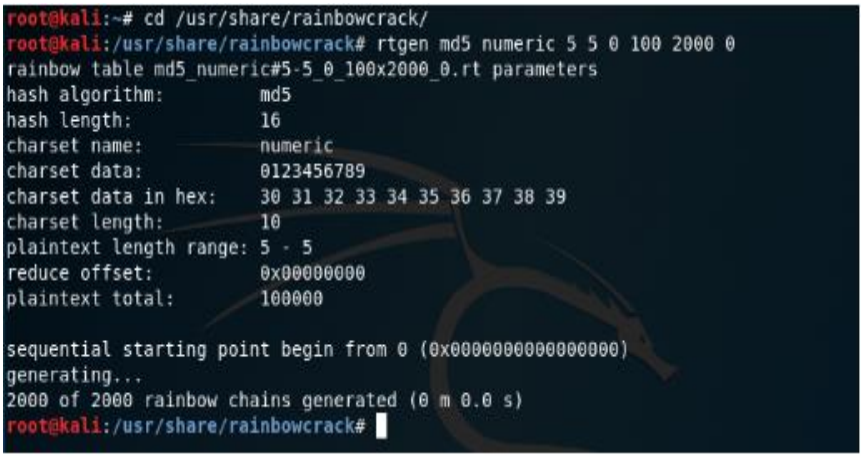


图 3-4

3.5、利用 rtsort 命令排序生成的字典，加快彩虹表的查找速度。在终端中输入 rtsort .。如图 3-5 所示

图 3-5

3.6、在终端输入 echo -n 11111 | openssl md5 生成 hash，最后使用 rcrack 命令破解散列值在终端中输入 rcrack . -h b0baee9d279d34fa1dfd71aadb908c3f，可以看到破解成功。如图 3-6 所示

```
root@kali:/usr/share/rainbowcrack# echo -n 11111 | openssl md5
(stdin)= b0baee9d279d34fa1dfd71aadb908c3f
root@kali:/usr/share/rainbowcrack# rcrack . -h b0baee9d279d34fa1dfd71aadb908c3f
1 rainbow tables found
memory available: 2542505164 bytes
memory for rainbow chain traverse: 1600 bytes per hash, 1600 bytes for 1 hashes
memory for rainbow table buffer: 2 x 32016 bytes
disk: ./md5_numeric#5-5_0_100x2000_0.rt: 32000 bytes read
disk: finished reading all files
plaintext of b0baee9d279d34fa1dfd71aadb908c3f is 11111

statistics
--------------------------------------------------------------
plaintext found:                            1 of 1
total time:                                 0.00 s
time of chain traverse:                     0.00 s
time of alarm check:                        0.00 s
time of disk read:                          0.00 s
hash & reduce calculation of chain traverse: 4900
hash & reduce calculation of alarm check:    1903
number of alarm:                            64
performance of chain traverse:              2.45 million/s
performance of alarm check:                 1.90 million/s

result
--------------------------------------------------------------
b0baee9d279d34fa1dfd71aadb908c3f  11111  hex:3131313131
root@kali:/usr/share/rainbowcrack#
```

图 3-6

4、暴力破解 MD5crack

4.1、获得 MD5 密文

4.1.1 打开 C:\实验工具集\05_日常应用安全\第 4 节暴力破解-MD5crack\目录下的 MD5Maker.exe，在软件界面中输入“123456”生成 MD5 散列值。如图 4-1 所示

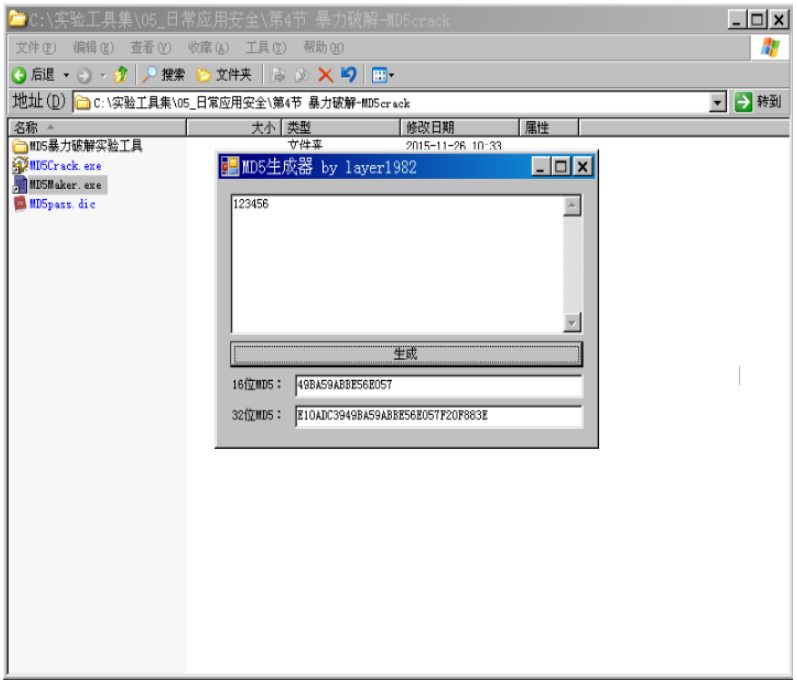


图 4-1

4.2、破解已知的简单 MD5 值

4.2.1、打开 C:\实验工具集\05_日常应用安全\第 4 节 暴力破解-MD5crack\目录下的 MD5Crack.exe，将上文生成的 32 位 MD5 散列值复制到输入框中。如图 4-2 所示

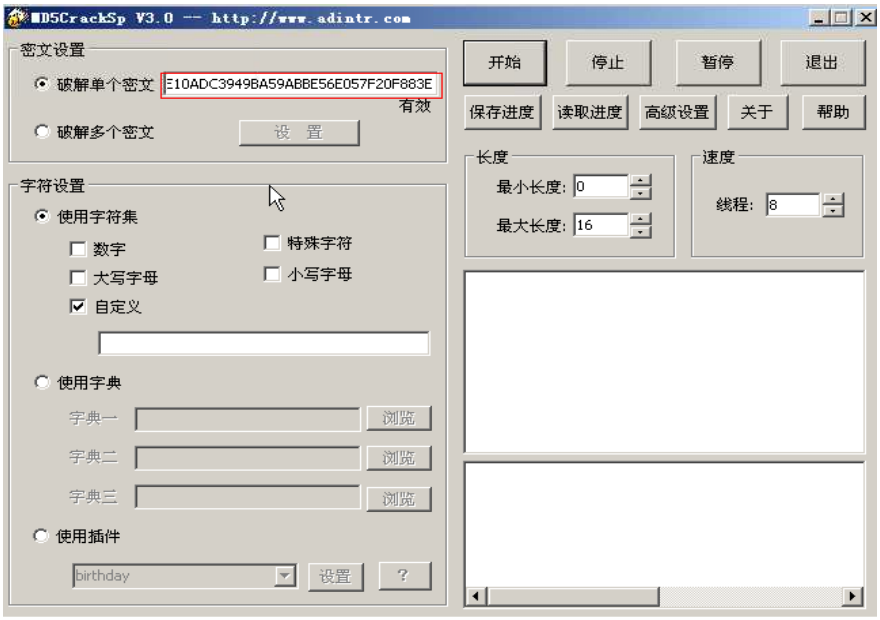


图 4-2

4.2.2、选取适当的字符集，点击“开始”进行破解；破解完成后提示所用时间。如图 4-3 所示

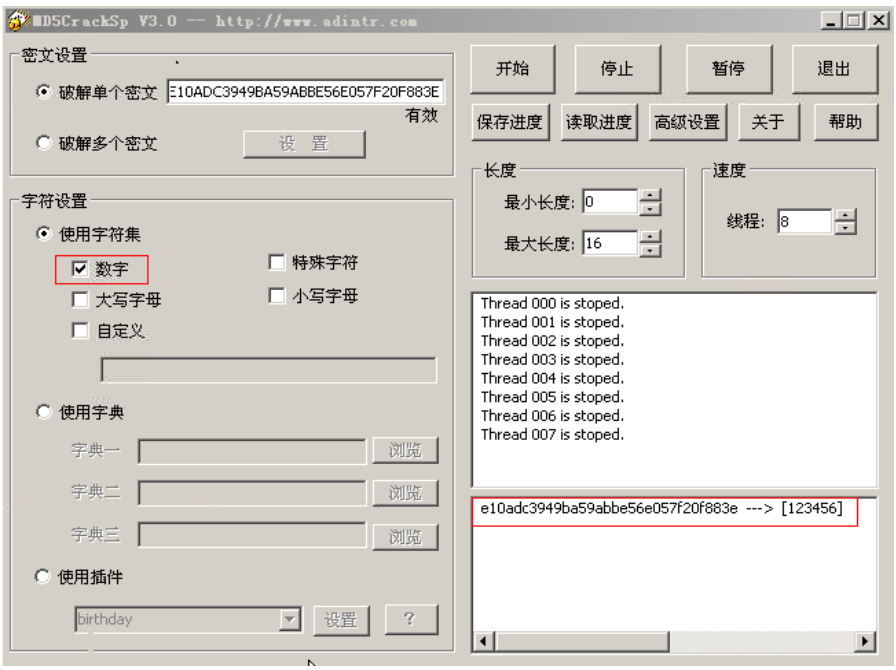


图 4-3

4.2.3、点击“确定”即看到现暴力破解出的明文。如图 4-4 所示

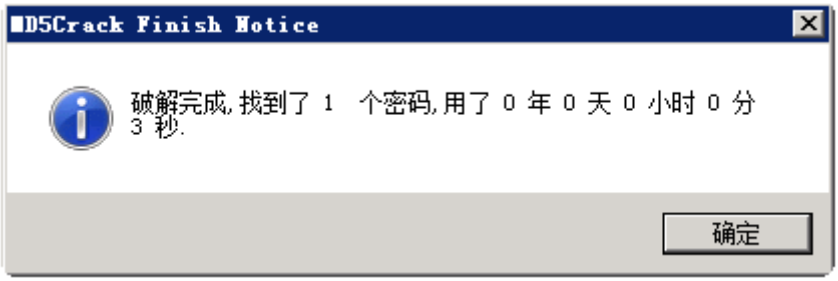


图 4-4

4.3、.破解已知的较复杂 MD5 值

4.3.1、用 MD5 生成器生成较为复杂的明文 MD5 值，例如：aaaaaa，复制密文到破解软件中，并配置破解参数。如图 4-5 所示

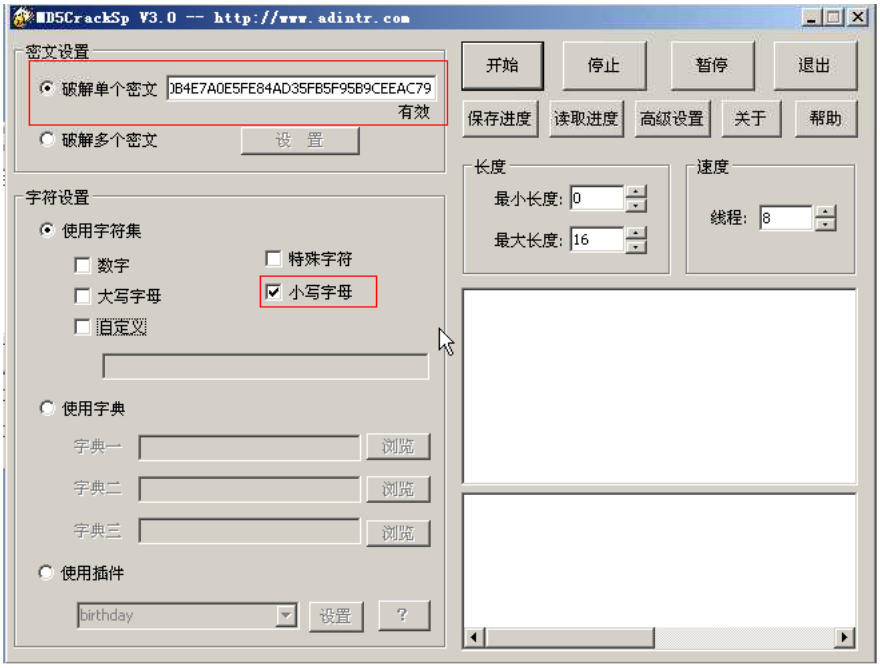


图 4-5

4.3.2、点击“开始”即可进行暴力破解。如图 4-6 所示

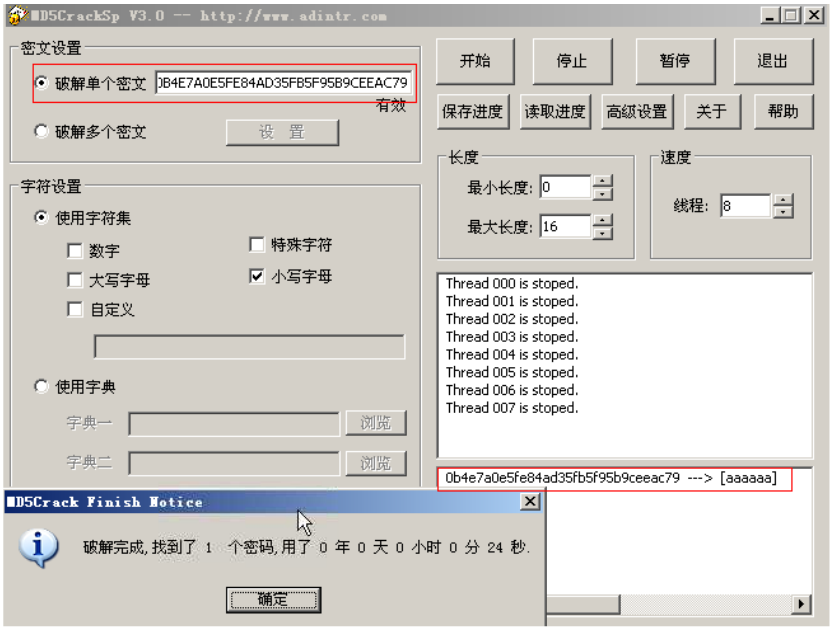


图 4-6

4.3.3、再次选取长度更长或者密码与数字混合的明文的 MD5 值进行破解。不难看出，当对明文未知的情况下，明文长度，字符集的选择都影响 MD5 值的暴力破解。

实验三 抓包获取 FTP 用户名和密码实验

FTPScan 和 Wireshark 抓包/远程破解 FTP 用户名和密码

一、实验目的

1、了解 FTPScan 破解工具，学习 FTPScan 扫描破解过程

2、练习 wireshark 的抓包过程。查看数据包中的信息。

二、实验环境

目标机：http://192.168.1.3

工具目录：C:\实验工具集\05_日常应用安全

操作系统：WindowsSever2008R2　　CentOS6.5

三、实验内容

1、字典扫描破解

2、打开 wireshark 抓取数据包，筛选 ftp 数据包并查看封包列表中的信息。

四、实验步骤

1、字典扫描破解

1.1、启动 FTPScan

1.1.1、打开 C:\实验工具集\05_日常应用安全\第一节 FTPscan 远程破解 ftp 用户名与密码\FTPScan 目录。如图 1-1 所示

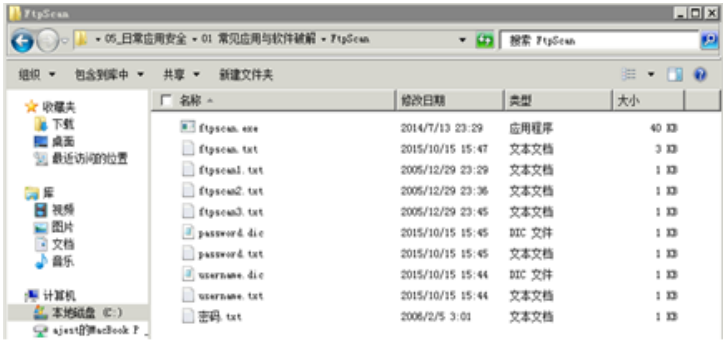


图 1-1

1.1.2、打开 cmd 命令行，进入到 FTPScan 目录，命令 cd C:\实验工具集\05_日常应用安全\第 1 节 FTPscan 远程破解 ftp 用户名与密码\FtpScan。如图 1-2 所示

图 1-2

1.1.3、输入 dir 命令，即可查看该目录下的文件。如图 1-3 所示

图 1-3

1.2、进行扫描

1.2.1、在命令行输入 ftpscan，即可进入到 ftpscan 的命令行界面，页面会显示语法信息。如图 1-4 所示

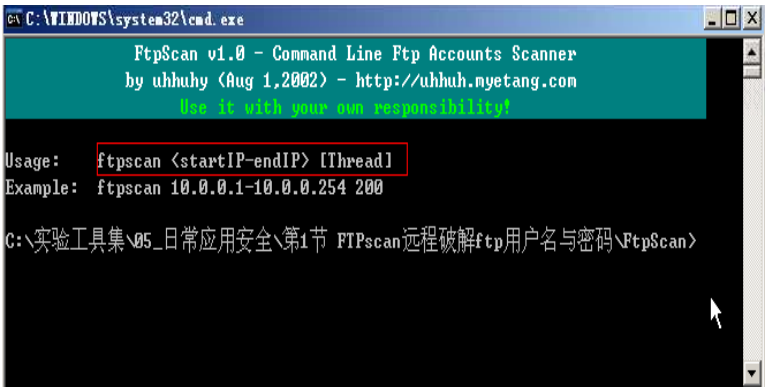


图 1-4

1.2.2、在界面中输入 ftpscan 192.168.1.3，即可进行扫描。如图 1-5 所示

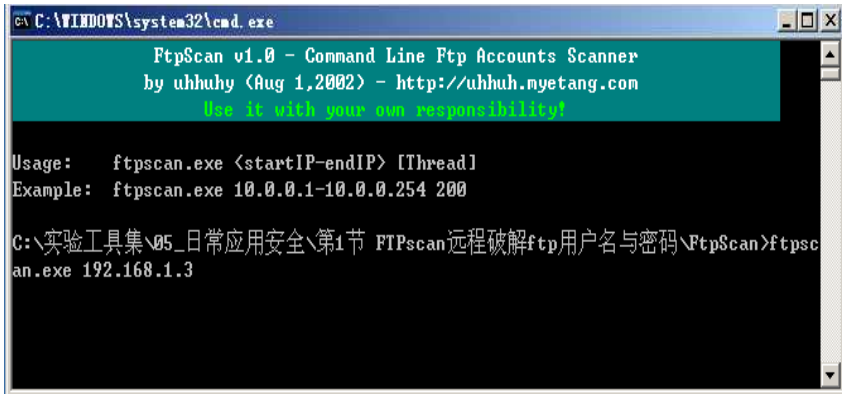


图 1-5

1.2.3、扫描结果，绿色的代码即为目标主机 FTP 服务器的用户名【administrator】和密码【Simplexue123】。如图 6 所示

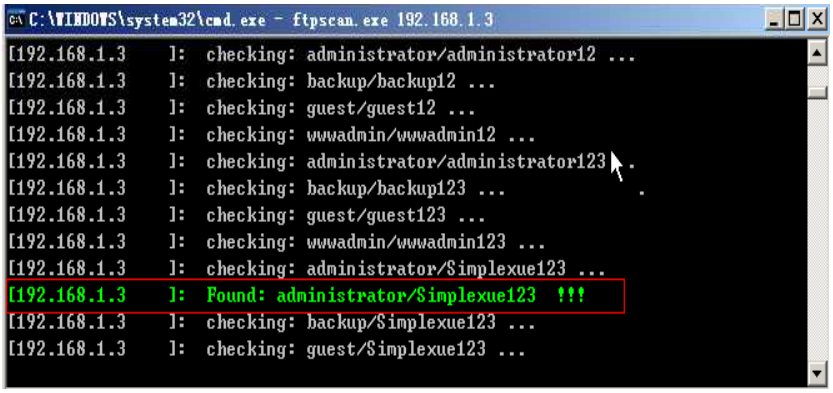


图 1-6

1.3、连接 FTP 服务器

1.3.1、打开资源管理器，在地址中输入 ftp://192.168.1.3。如图 1-7 所示

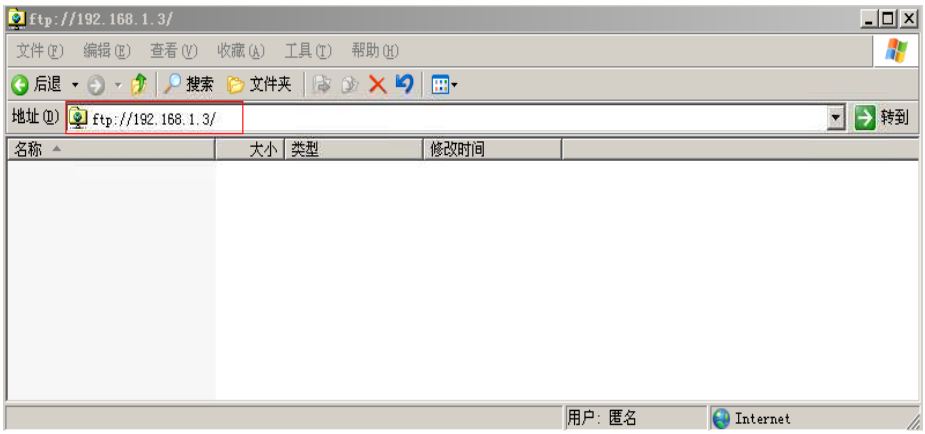


图 1-7

1.3.2、敲击回车，输入用户名【administrator】和密码【Simplexue123】。如图 1-8 所示

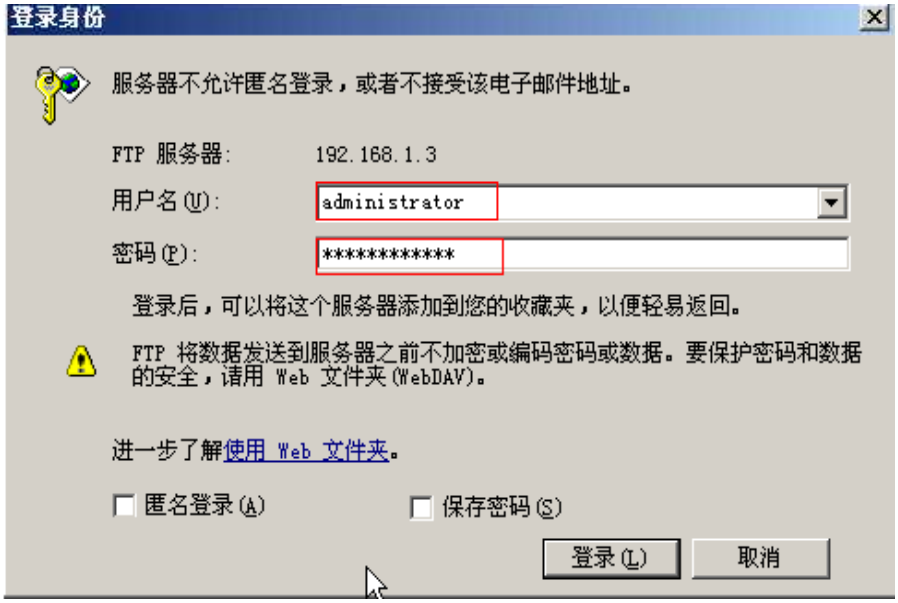


图 1-8

1.3.3、登录成功后，即可看到一个文件夹，说明 FTP 密码破解成功。如图 1-9 所示

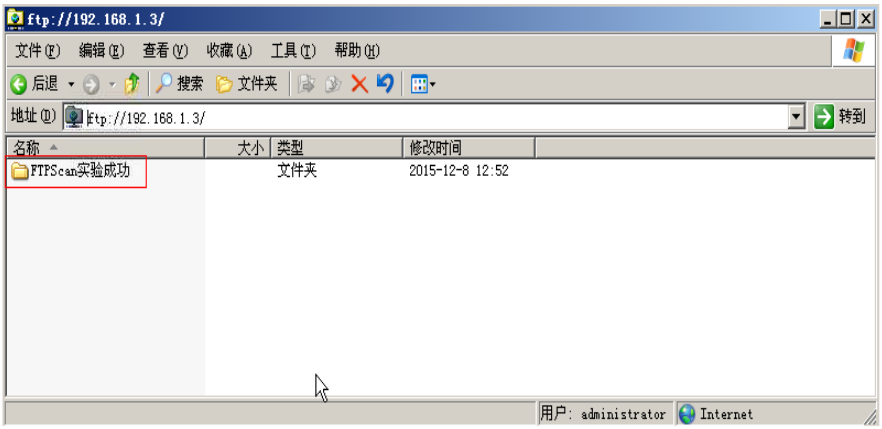


图 1-9

2、打开 wireshark 抓取数据包，筛选 ftp 数据包并查看封包列表中的信息。

2.1、抓取 ftp 数据包

2.1.1、双击桌面上的“wireshark”图标。如图 2-1 所示

图 2-1

2.1.2、弹出 wireshark 的主界面，双击“本地连接”，等待跳转至自动抓取数据包的界面。如图 2-2 所示

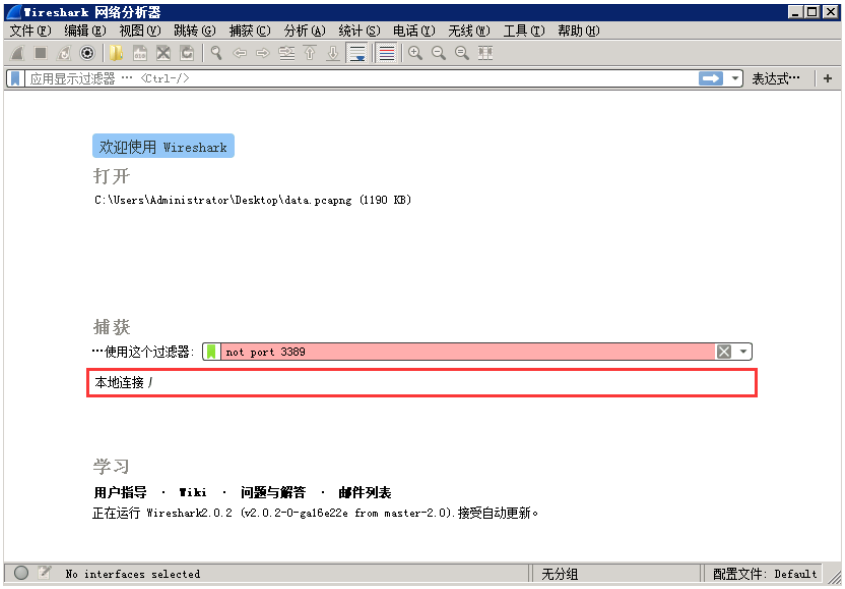


图 2-2

2.1.3、Wireshark 以本地连接为接口开始自动抓取数据包。如图 2-3 所示

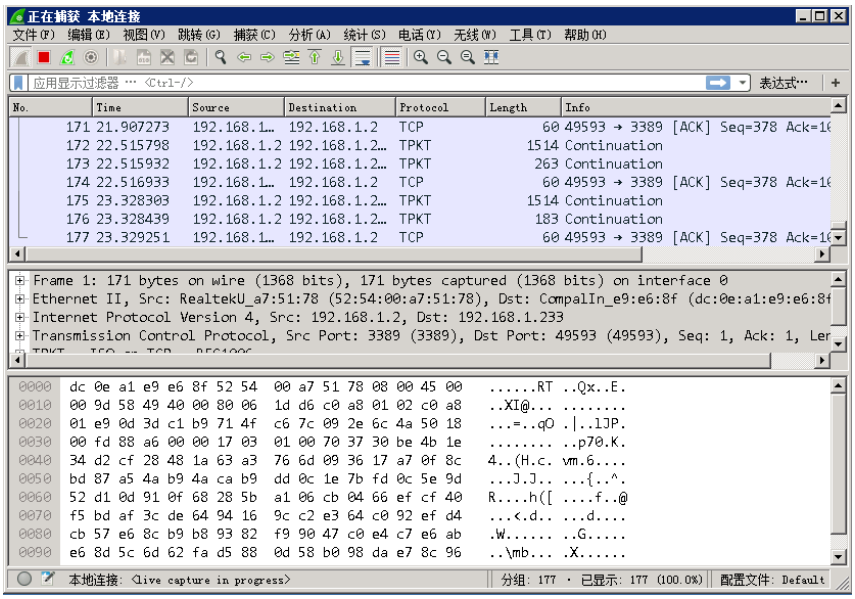


图 2-3

2.1.4、在桌面双击打开“计算机”，在地址栏输入 ftp://192.168.1.3 并回车。如图 2-4 所示

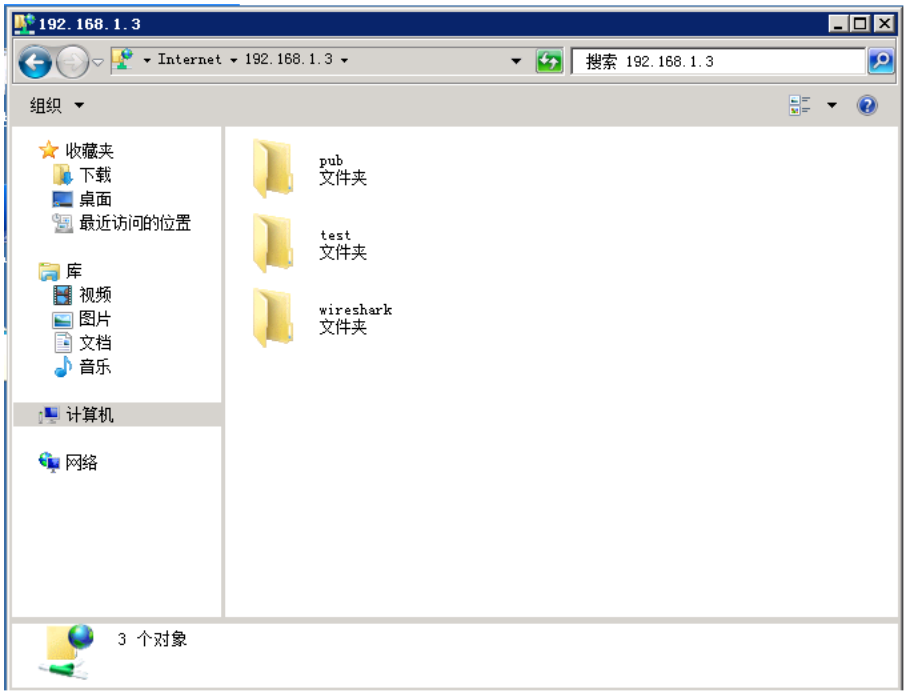


图 2-4

2.1.5、右键单击空白处，选择登录。如图 2-5 所示

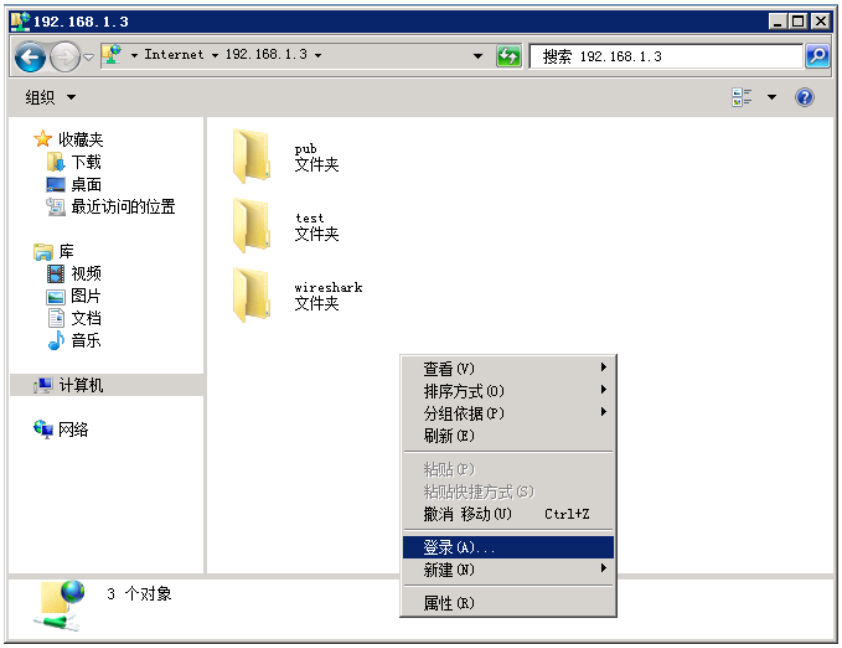


图 2-5

2.1.6、在弹出的登录对话框中输入，用户名和密码（用户名为：wireshark，密码为 Simplexue123），并进行登录。如图 2-6 所示

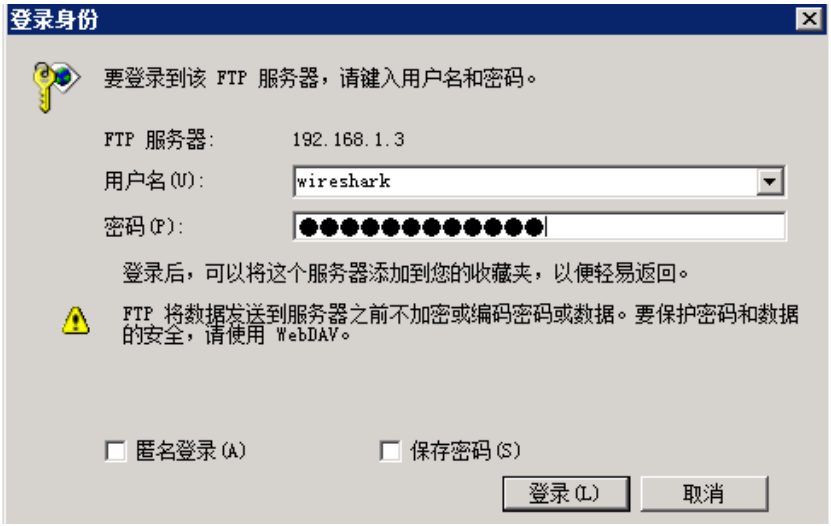


图 2-6

2.1.7、成功登陆后，返回 wireshark 主界面。单击红色的停止抓包按钮。如图 2-7 所示

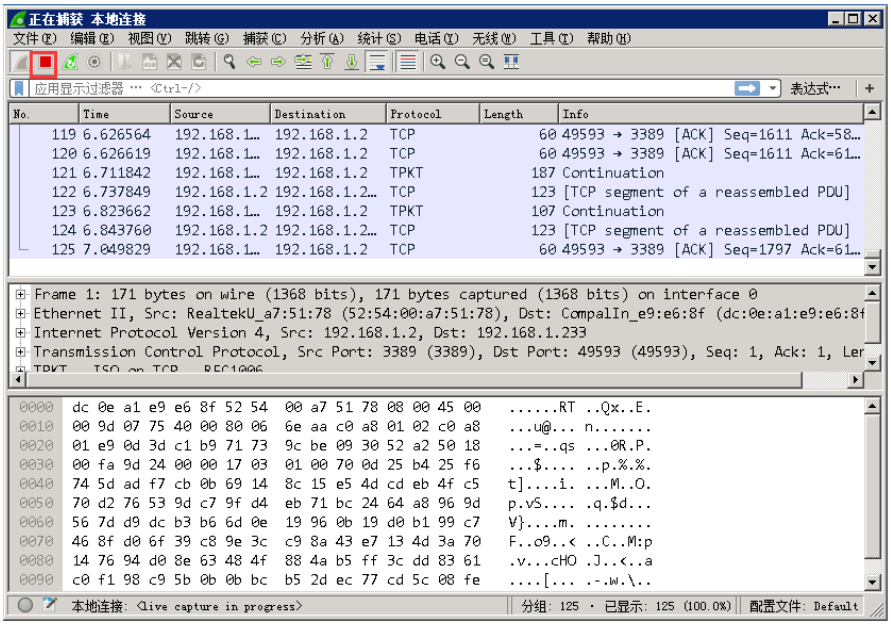


图 2-7

2.1.8、在过滤器中输入“ftp”并回车，查看所有的 ftp 协议数据包。如图 2-8 所示

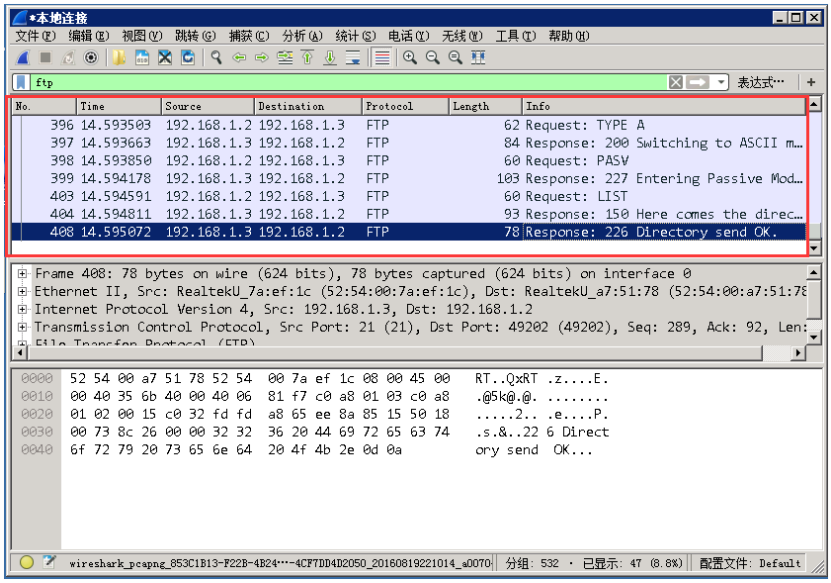


图 2-8

2.1.9、单击“调整分组列表以适应内容”按钮会自动跳转封包列表字段的大小。如图 2-9 所示

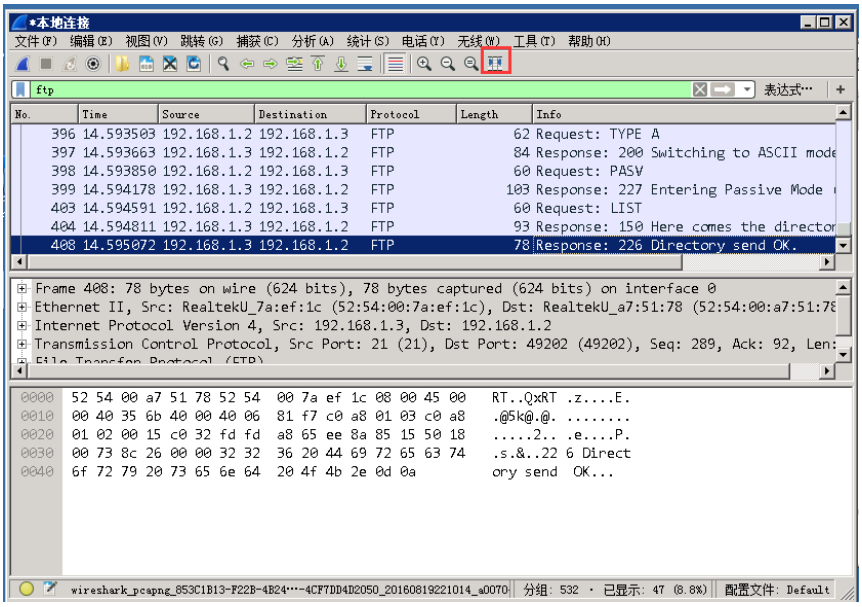


图 2-9

2.1.10、查看封包列表中的信息。寻找关于 USER 和 PASS 的信息，进行查看。如图 2-10 所示

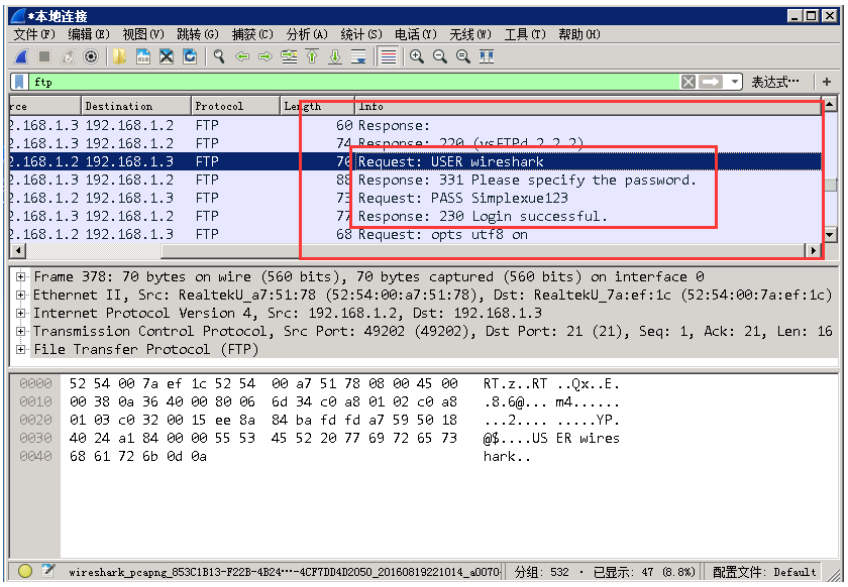


图 2-10

2.1.11、查看得出，当 USER 的值为“wireshark”，PASS 的值为“Simplexue123”的 request 得到的 response 为 successful。那么说明 ftp 的用户名为 wireshark 密码为 Simplexue123

实验四 CA 证书实验

基于数字证书的安全电子邮件、搭建 CA 发布 HTTPS 站点

一、实验目的

1、学习数字证书，学习数字证书签发安全电子

2、学习 CA 的搭建，学习 HTTPS 站点的发布

二、实验环境

Windows Server2008　　Windows XP

Windows2008

三、实验内容

1、掌握免费个人数字证书申请、安装、导入和导出、OutlookExpress 的配置、使用数字证书签发安全电子邮件的流程

2、搭建 CA 实现发布 https 站点

四、实验步骤

1、掌握免费个人数字证书申请、安装、导入和导出、OutlookExpress 的配置、使用数字证书签发安全电子邮件的流程

1.1、数字证书的申请安装操作

1.1.1、申请证书

开启并登录 WindowsXP 虚拟机，打开 IE 浏览器，输入证书申请地址：http://192.168.1.3/certsrv，（192.168.1.3 为 Windows Server 2008 服务器的 IP 地址）。如图 1-1 所示

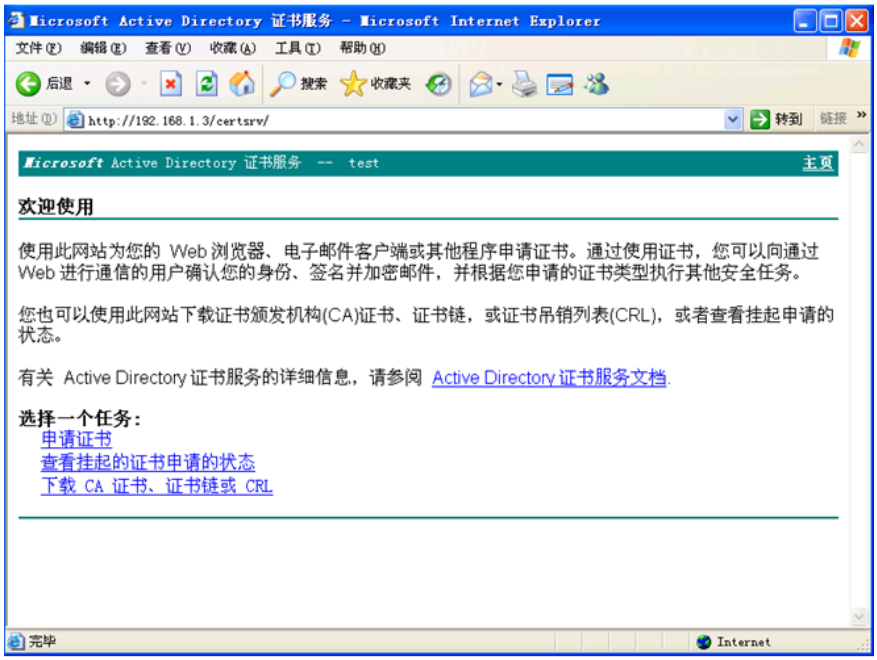


图 1-1

选择申请证书->电子邮件保护证书。如图 1-2 所示

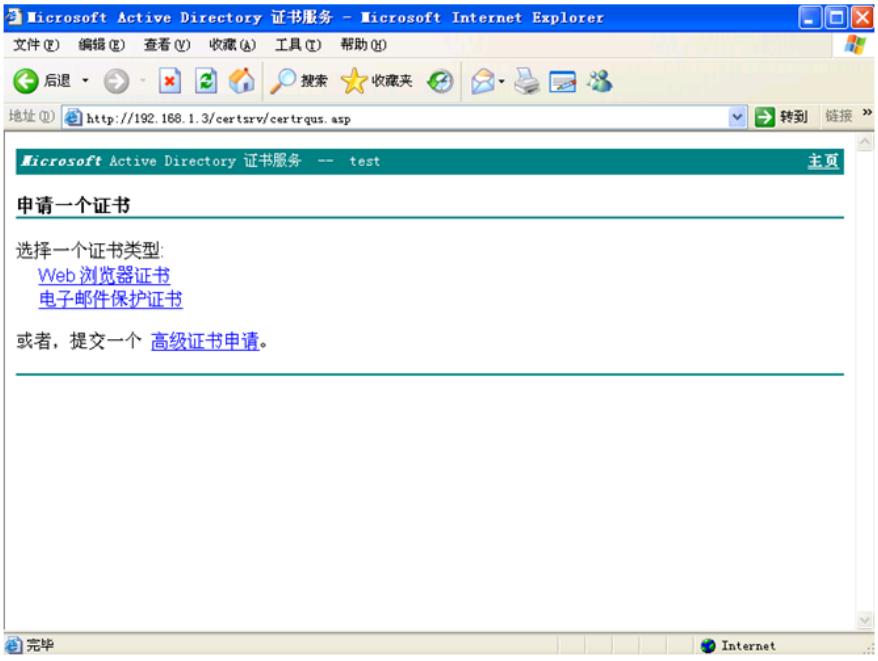


图 1-2

填写用户的基本信息包括名称（要求使用用户真实姓名）、公司、部门、城市、省份、国家地区、电子邮箱（要求邮件系统能够支持邮件客户端工具，不能填写错误，否则会影响安全电子邮件的使用）、更多选项——加密服务提供程序

（可以选择“Microsoft Strong Cryptgraphic Provider”）、关闭强私钥保护，申请格式选择 CMC。单击提交。如图 1-3 所示

图 1-3

单击是。如图 1-4 所示

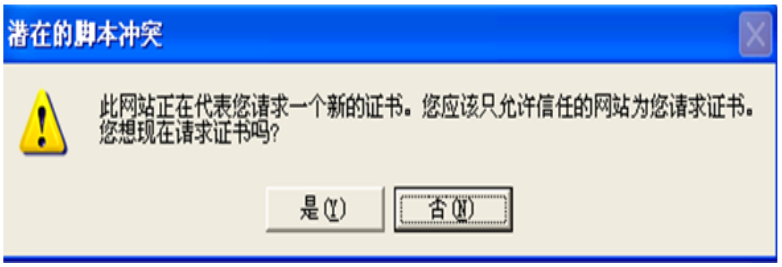


图 1-4

证书申请成功。如图 1-5 所示

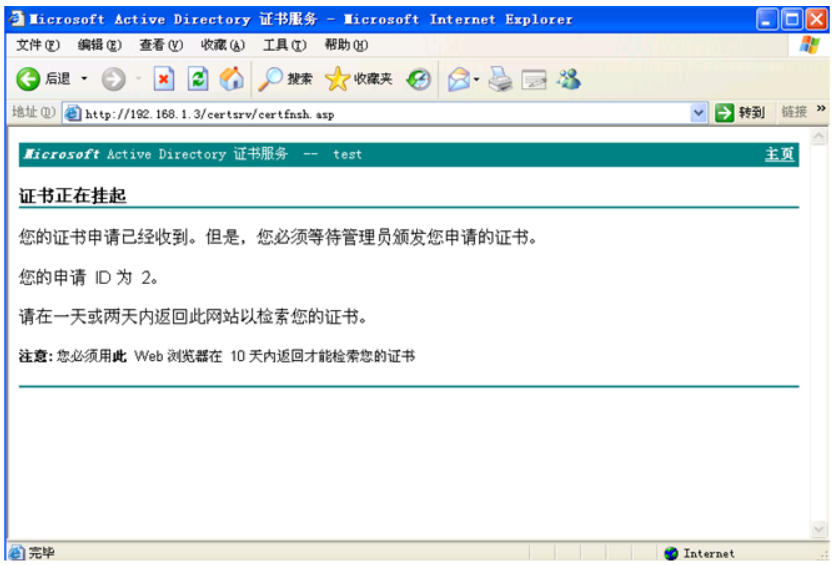


图 1-5

1.1.2、颁发证书

在 Windows Server 2008 管理工具中打开证书颁发机构，单击挂起的申请，可以看到刚刚申请的证书，右键该证书，选择所有任务—>颁发。如图 1-6 所示

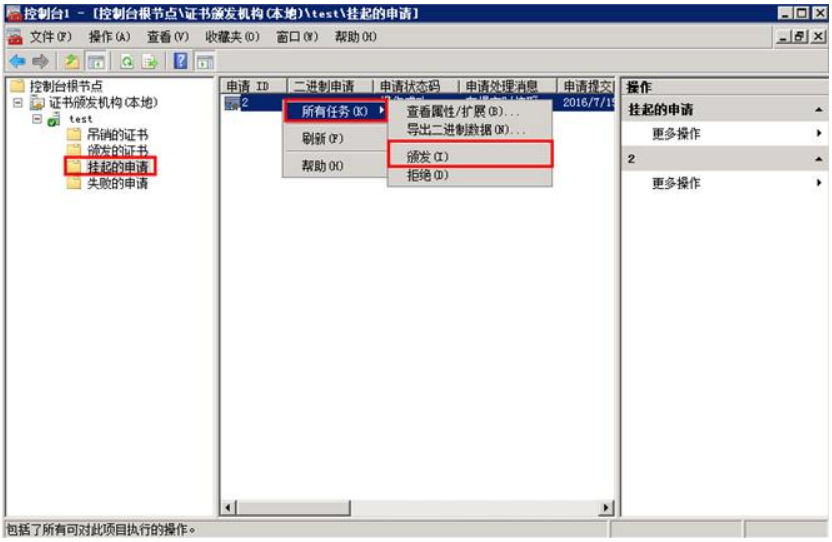


图 1-6

1.1.3、安装数字证书

在 WindowsXP 虚拟机的 IE 浏览器中输入 http://192.168.1.3/certsrv，单击查看挂起的证书申请的状态。如图 1-7 所示

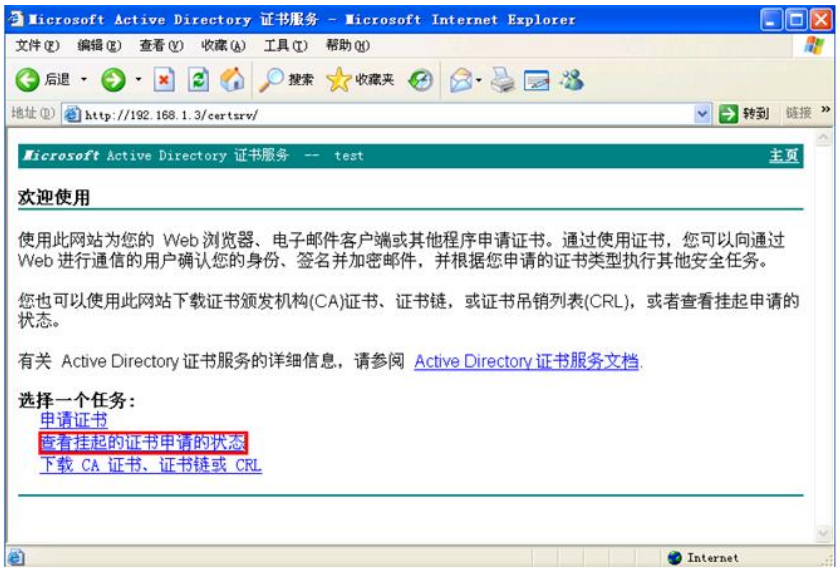


图 1-7

单击电子邮件保护证书。如图 1-8 所示

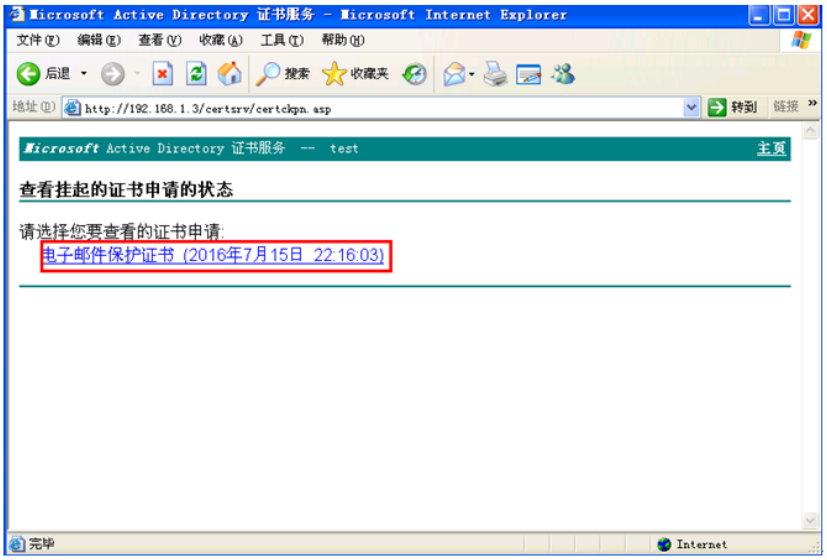


图 1-8

单击安装此证书。如图 1-9 所示

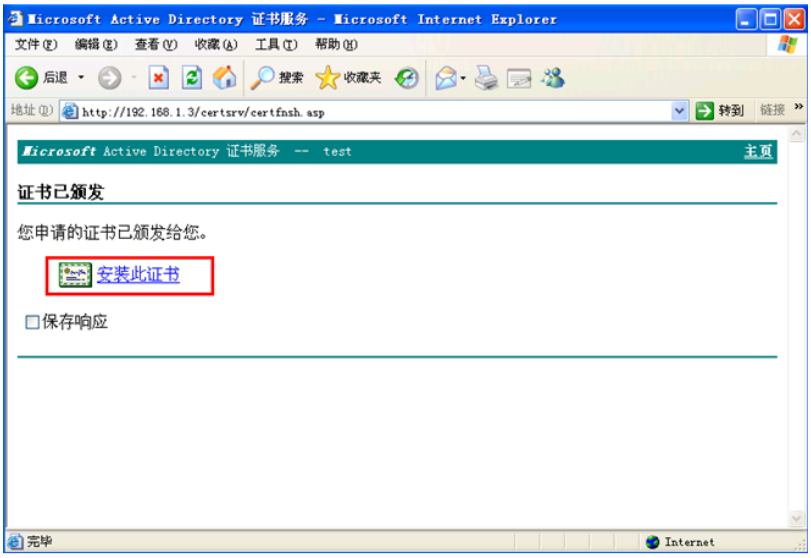


图 1-9

单击是。如图 10 所示

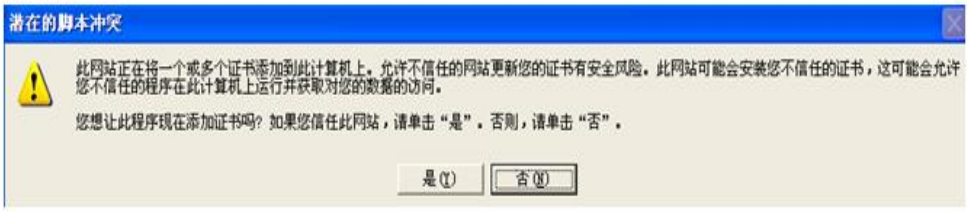


图 1-10

弹出安全警告，单击是。如图 1-11 所示

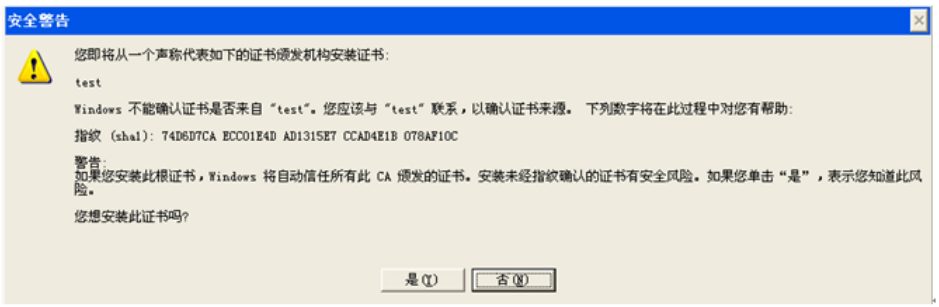


图 1-11

证书成功安装。如图 1-12 所示

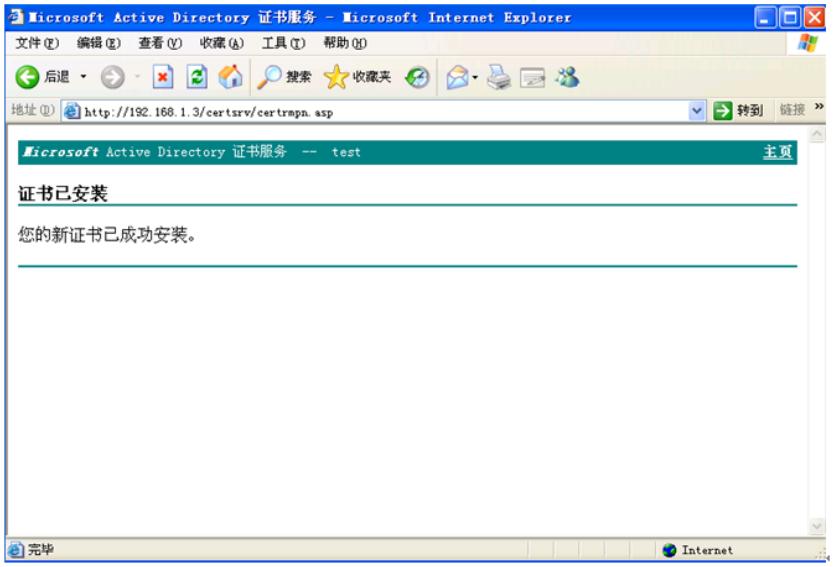


图 1-12

1.1.4、数字证书的查看

在 Windows XP 虚拟机的 IE 浏览器的菜单栏工具->Internet 选项->内容->证书中，可以看到证书已经被安装地成功。双击证书查看证书内容。如图 1-13 所示

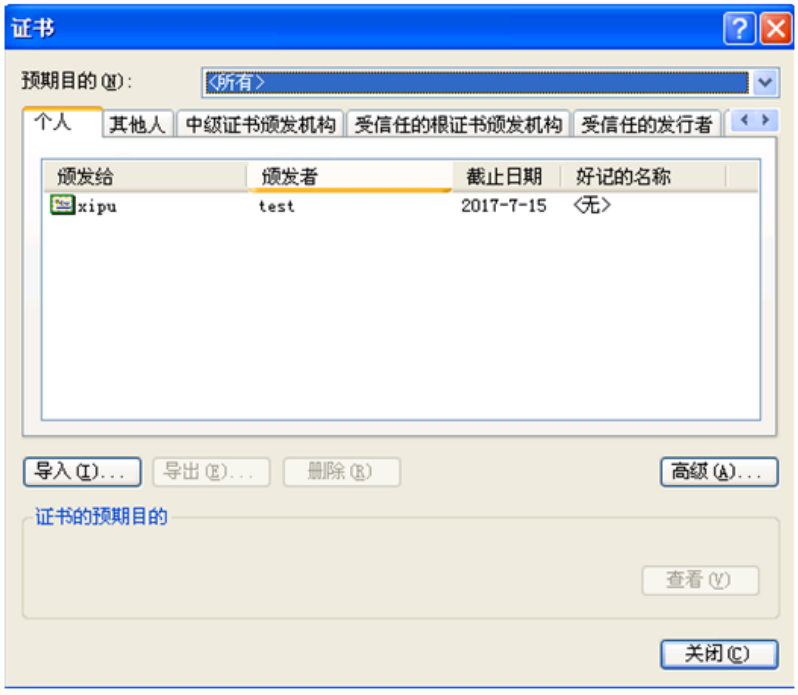


图 1-13

1.2、数字证书的导出和导入操作指导

为了保护数字证书及私钥的安全，需要进行证书及私钥的备份工作。如果需要在

不同的电脑上使用同一张数字证书或者重新安装电脑系统，就需要重新安装根证书、导入个人证书及私钥。具体步骤如下：

1.2.1、备份证书和私钥的操作步骤

打开 WindowsXPIE 浏览器，工具->Internet 选项->内容->证书。如图 1-14 所示

图 1-14

选择一个数字证书，点击“导出”按钮，此时会弹出证书导出向导。如图 1-15 所示

图 1-15

点击“下一步”，可以选择是否将秘钥和证书一起导出。如图 1-16 所示

图 1-16

因导出的证书按文件存放，故选择导出文件的格式。如图 1-17 所示

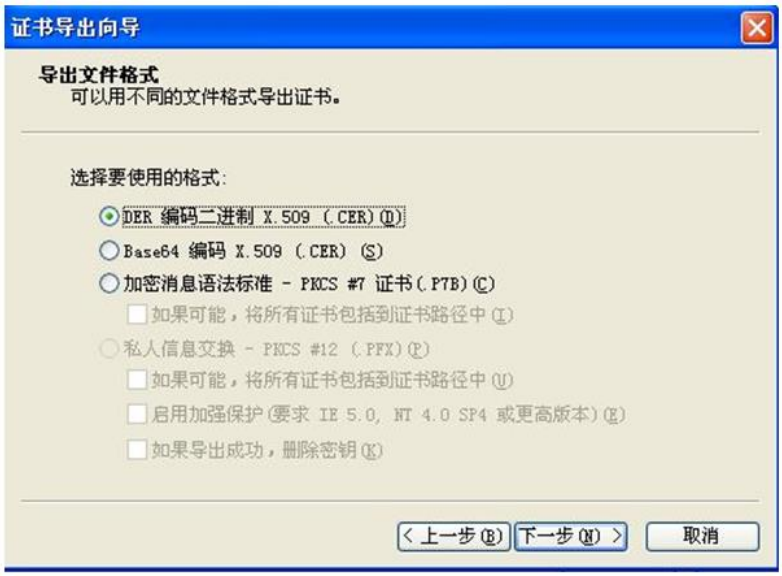


图 1-17

指定证书导出后文件的文件名和路径。如图 1-18 所示

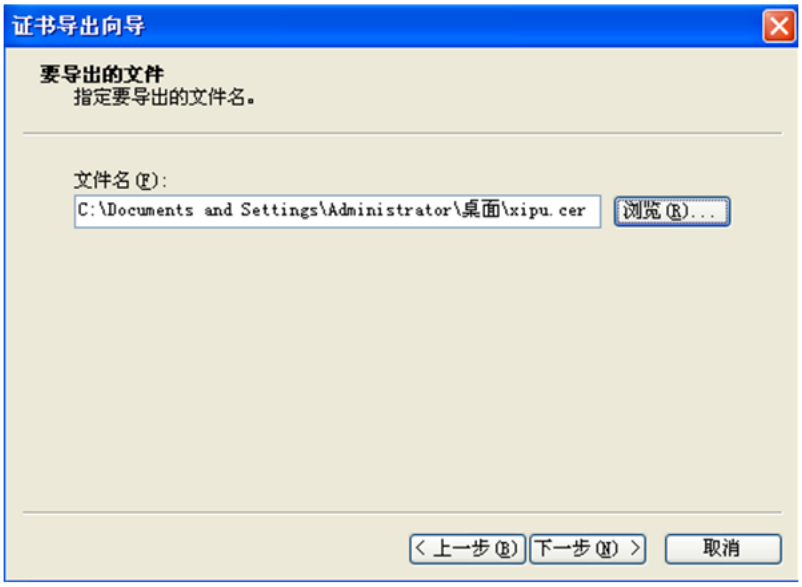


图 1-18

此时显示前面你所选择的所有设置，如果觉得完全正确则点击“完成”，如有错误则点击“上一步”。如图 1-19 所示

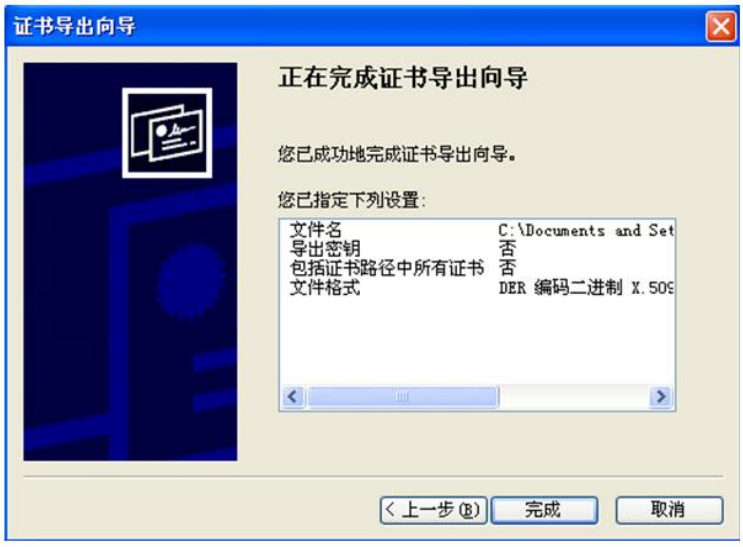


图 1-19

1.2.2、导入证书及私钥的操作步骤

打开 Windows XP IE 浏览器，工具->Internet 选项->内容->证书。或者，开始->设置->控制面板->Internet 选项->内容->证书。如图 1-20 所示

图 1-20

点击“导入”按钮，此时会弹出证书导入向导。如图 1-21 所示

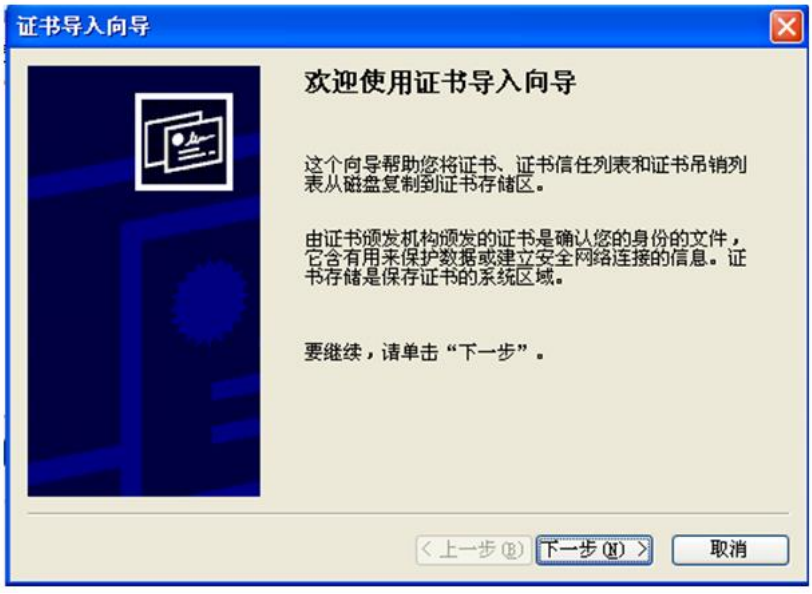


图 1-21

点击“下一步”，根据向导提示选择导入证书的文件名和路径。如图 1-22 所示

图 1-21

选择导入证书的存储区，可以由系统自动选择也可以由用户指定，系统默认该证书是用户自己的证书而存入“个人证书”之中，而如果你要导入对方的证书（这主要发生在你要利用对方证书给对方发送加密邮件的时候），则应该自己指定位置并选择“其他人”。如图 1-23 所示

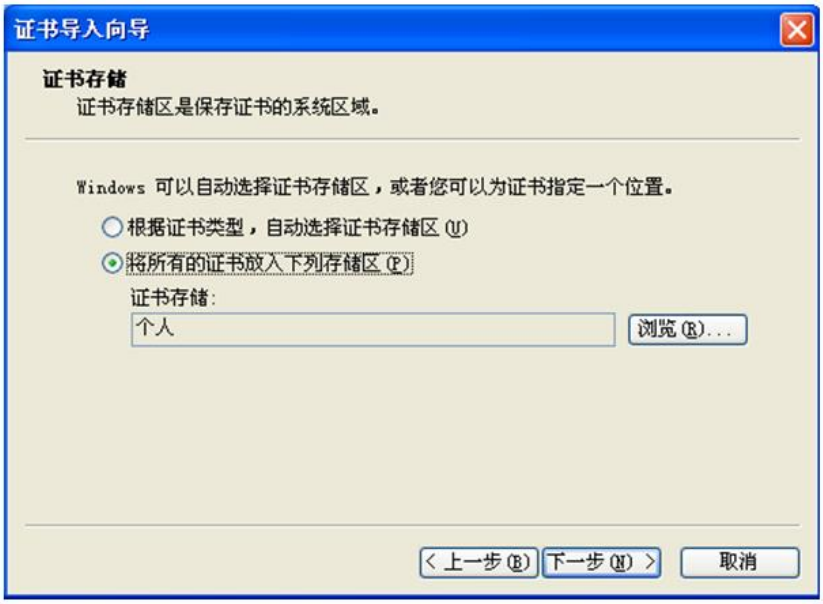


图 1-23

此时显示前面你所选择的所有设置，如果觉得完全正确则点击“完成”，如有错误

则点击“上一步”。如图 1-24 所示

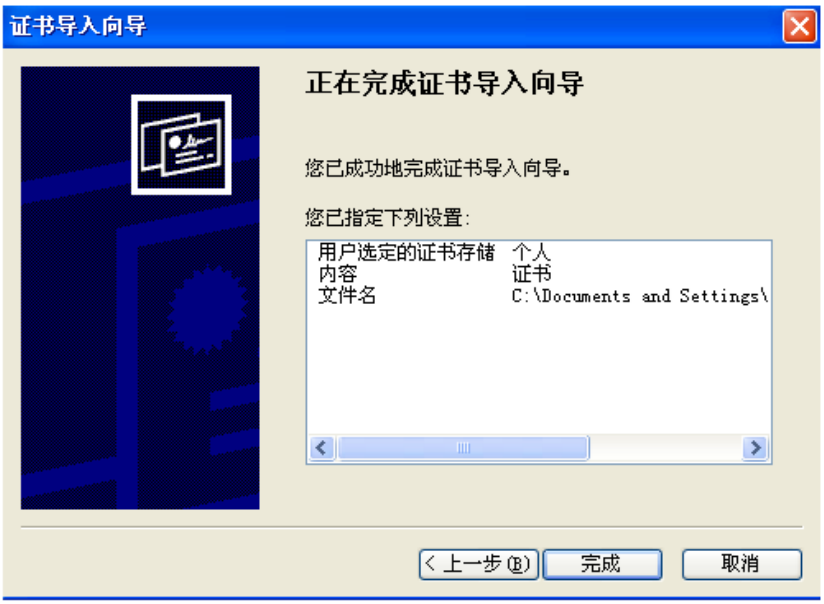


图 1-24

1.3、利用数字证书对电子邮件进行数字签名和加密

使用 OutlookExpress 可以对电子邮件进行加密和数字签名。对电子邮件进行签名需要一个属于你自己的数字证书，而要对电子邮件进行加密则需要拥有对方的数字证书。

1.3.1、配置 Outlook，建立你自己的账号

在 Windows XP 上单击开始->程序->Outlook Express，单击菜单上的“工具”->“账户”。如图 1-25 所示

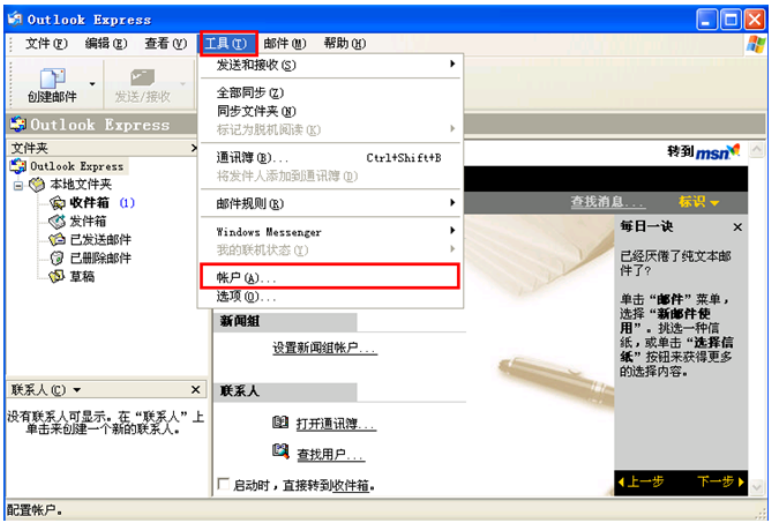


图 1-25

点击“添加”->“邮件”。如图 1-26 所示

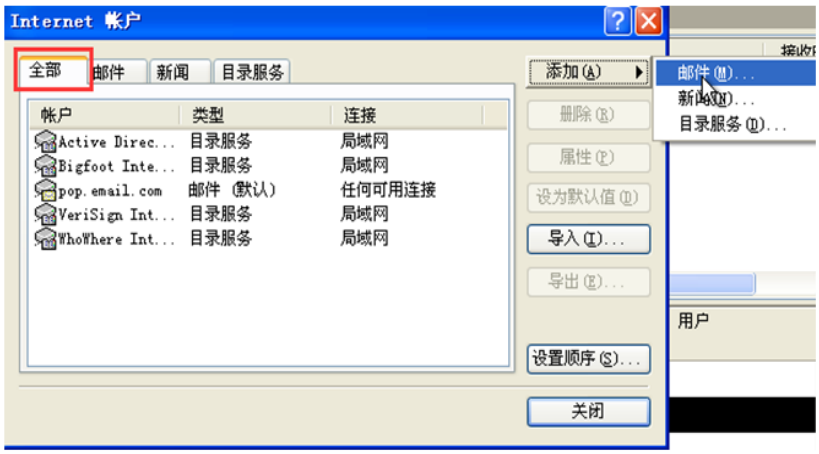


图 1-26

输入显示名称。如图 1-27 所示

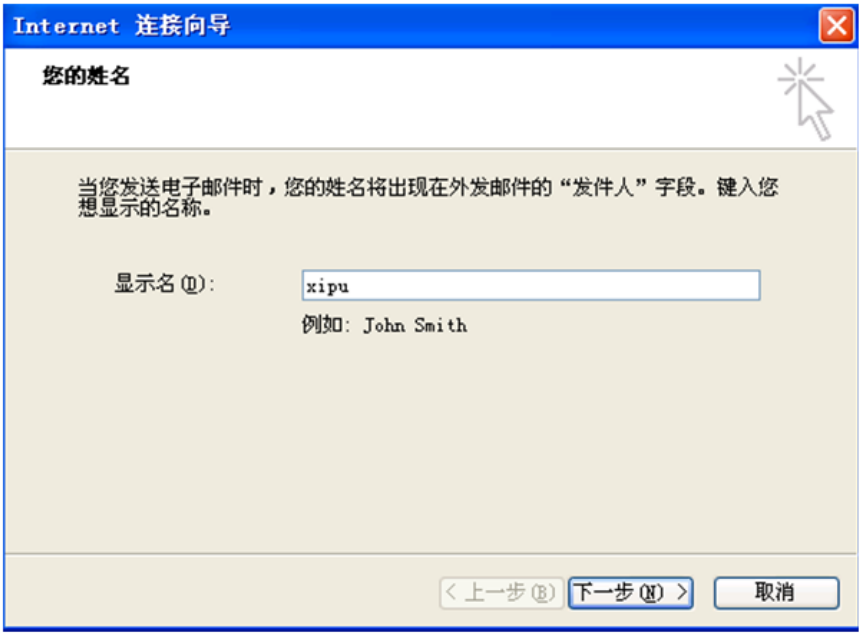


图 1-27

输入电子邮件地址。如图 1-28 所示

图 1-28

设置接收邮件服务器和发送邮件服务器。如图 1-29 所示

图 1-29

输入电子邮箱的帐户名称和登录密码。如图 1-30 所示

图 1-30

单击“下一步”，单击完成，邮件设置成功。如图 1-31 所示

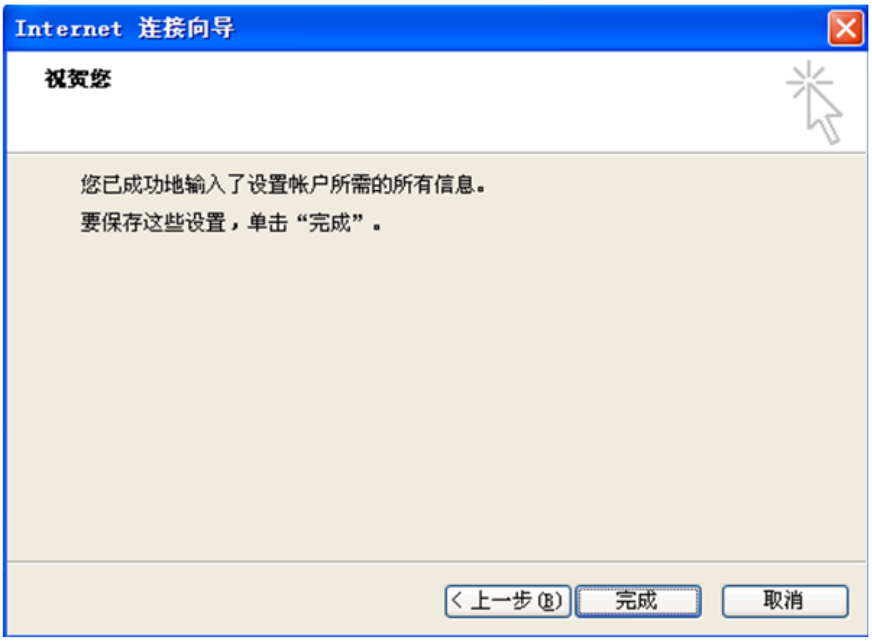


图 1-31

在 Outlook Express 中，单击“工具”菜单中的“帐户”。如图 1-32 所示

图 1-32

选取“邮件”选项卡选中用于发送安全邮件的帐号，然后单击“属性”。在属性设置窗口中，选择“服务器”选项卡，勾选“我的服务器要求身份验证”。如图 1-33 所示

图 1-33

选取安全选项卡，选择签名证书和加密证书及算法。如图 1-34 所示

（注意：如果此处证书列表为空，可在 IE 浏览器单击工具 àInternet 选项 à 内容 à 高级，勾选安全电子邮件）

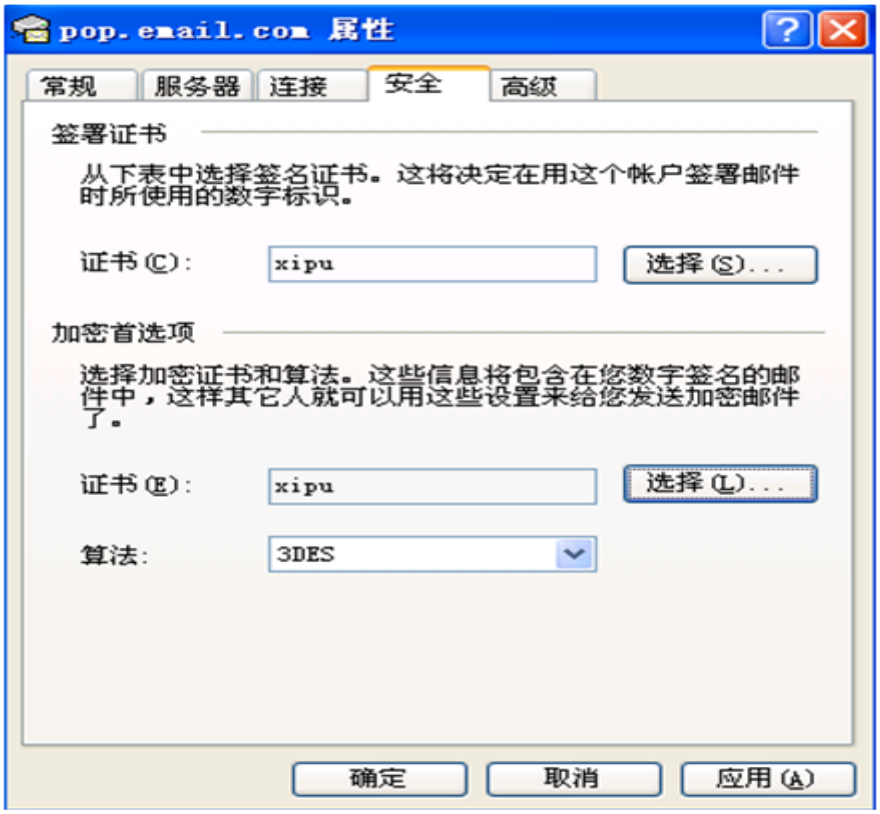


图 1-34

在弹出的“选择默认帐户数字标识”窗口中，选择要使用的数字证书。单击“确定”按钮，完成证书设置。其他补充设置。如图 1-35 所示

图 1-35

如果你希望在服务器上保留邮件副本，则在帐户属性中，单击“高级”选项卡。勾选“在服务器上保留邮件副本”。此时下边设置细则的勾选项由禁止（灰色）变为可选（黑色）。

1.3.2、使用 Outlook 发送附数字签名的电子邮件（此步骤只做说明不操作）

单击 Outlook Express 窗口中的“新邮件”按钮，撰写新邮件内容，填写好收件人邮箱地址和邮件主题。选取“工具”菜单中的“数字签名”项或工具条上的“签名”按钮，在邮件收件人的右侧会出现一个红色的“签名”标牌。如图 1-36 所示

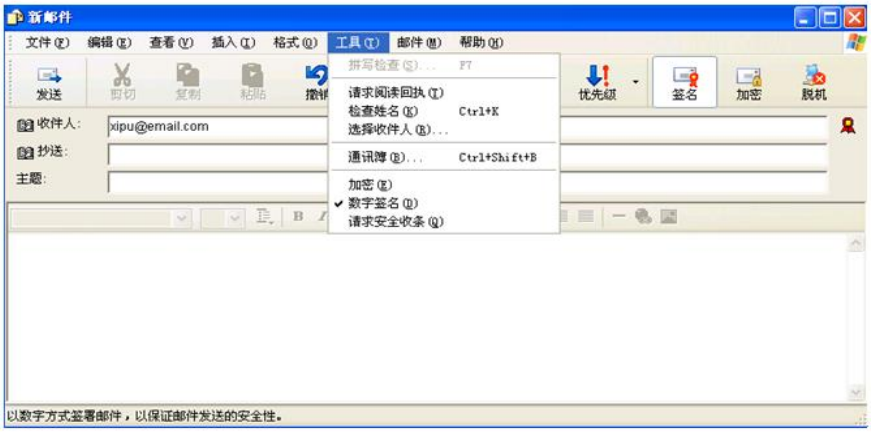


图 1-36

点击新邮件窗口左边的“发送”按钮。发出带签名的电子邮件。

当收件人收到并打开有数字签名的邮件时，将看到“数字签名邮件”的提示信息（用户可以设置下次不提示该信息），按“继续”按钮后，才可阅读到该邮件的内容。若邮件在传输过程中被他人篡改或发信人的数字证书有问题，页面将出现“安全警告”提示。在收件箱中，当邮件未阅读或签名未检查时，签名证书标志出现在未拆封信封图标（在发件人姓名前）的右侧；当双击邮件进行安全检查后，证书标志出现在已拆封的信封图标的左侧。

1.3.3、使用 Outlook 发送加密的电子邮件

要发送加密电子邮件，你需要有收件人的数字证书。获得收件人数字证书的方法可以是让对方给你发送带有其数字签名的邮件。将该邮件打开后，在会右边看到对方的证书标志。单击该标识，找到“安全”项，单击“查看证书”按钮，可以查看“发件人证书”；单击“添加到通讯簿”按钮，在通讯簿中保存发件人的加密首选项，这样对方数字证书就被添加到你的通讯簿中。有了对方的数字证书，你就可以向对方发送加密邮件了。

在 Outlook Express6 中撰写新邮件或者回复已经收到的邮件，写好邮件内容后，选取“工具”菜单中的“加密”项或单击工具栏上的“加密”按钮，邮件的右侧将会出现一个蓝色的锁型加密标识。该邮件也可以同时使用发件人的数字签名。如图 1-37 所示

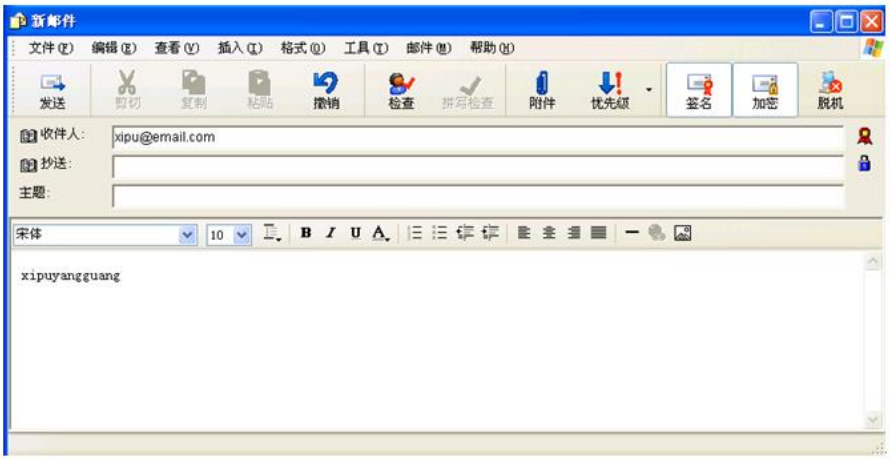


图 1-37

当收件人收到并打开已加密过的邮件时，将看到”加密邮件”的提示信息，按“继续”按钮后，可阅读到该邮件的内容。当收到加密邮件时，完全有理由确认邮件没有被其他任何人阅读或篡改过，因为只有在收件人自己的计算机上安装了正确的数字证书，Outlook Express 才能自动解密电子邮件；否则，邮件内容将无法显示。

2、搭建 CA 实现发布 https 站点

2.1、CA 的搭建

2.1.1、点击【开始|管理工具|服务器管理器】，打开服务器管理器。如图 2-1 所示

图 2-1

2.1.2、点击【角色】，然后点击【添加角色】。如图 2-2 所示

图 2-2

2.1.3、进入到【添加角色向导】，点击【下一步】。如图 2-3 所示

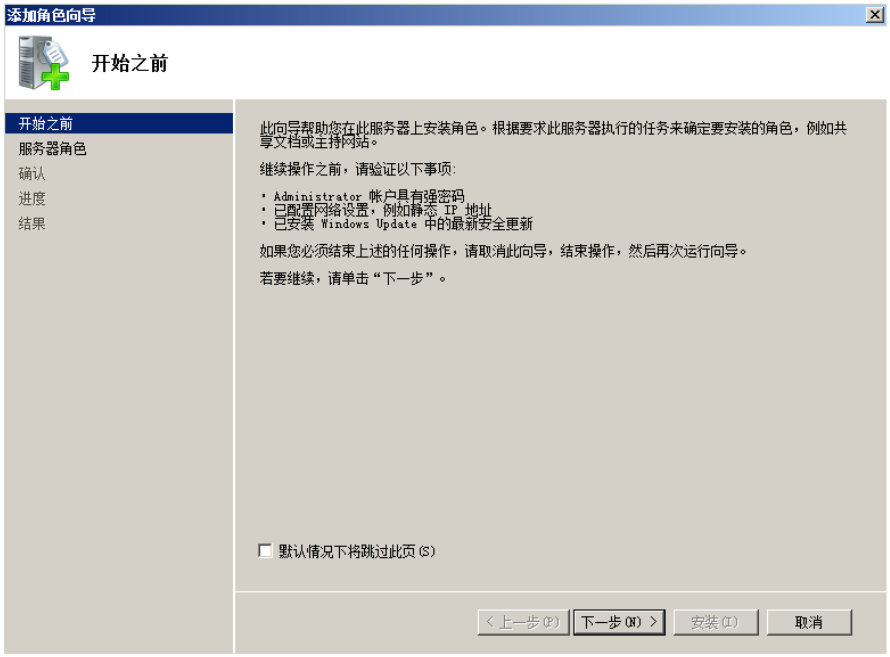


图 2-3

2.1.4、勾选【Active Directory 证书服务】，点击【下一步】。如图 2-4 所示

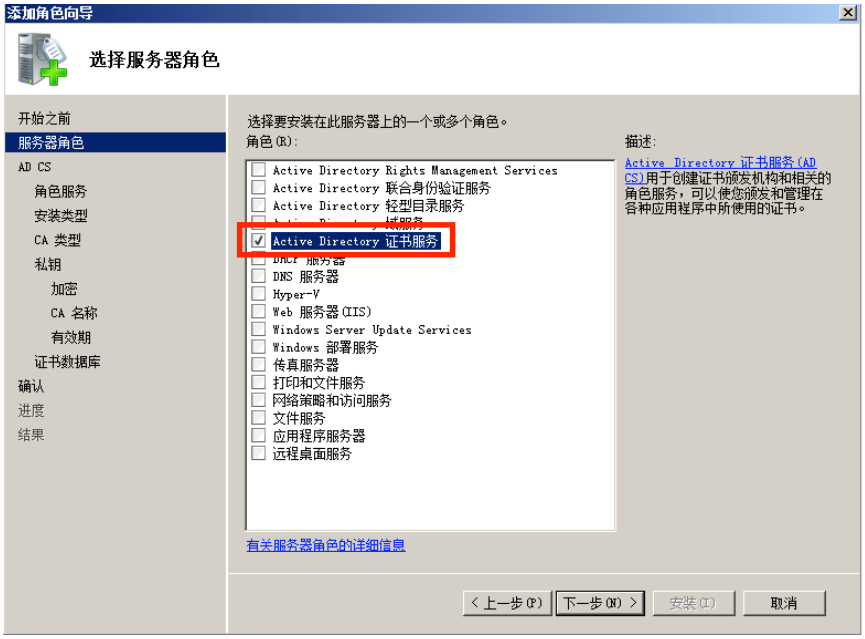


图 2-4

2.1.5、显示出 Active Directory 证书服务简介，点击【下一步】。如图 2-5 所示

图 2-5

2.1.6、勾选（默认）【证书颁发机构】，勾选【证书颁发机构 web 注册】，直接点击【添加所需的角色服务】。如图 2-6 所示

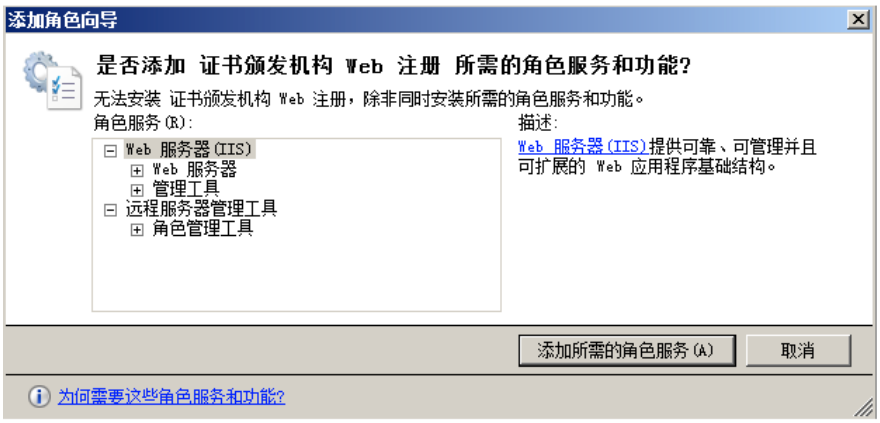


图 2-6

2.1.7、选择两项服务之后，点击【下一步】即可。如图 2-7 所示

图 2-7

2.1.8、指定安装类型，默认即可，点击【下一步】。如图 2-8 所示

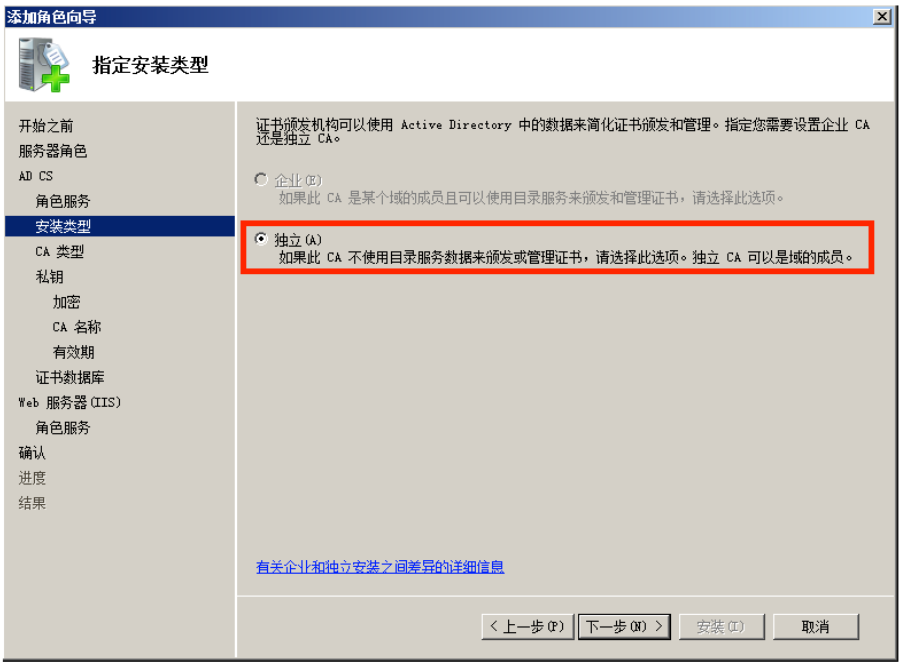


图 2-8

2.1.9、选择【根 CA】，点击【下一步】。如图 2-9 所示

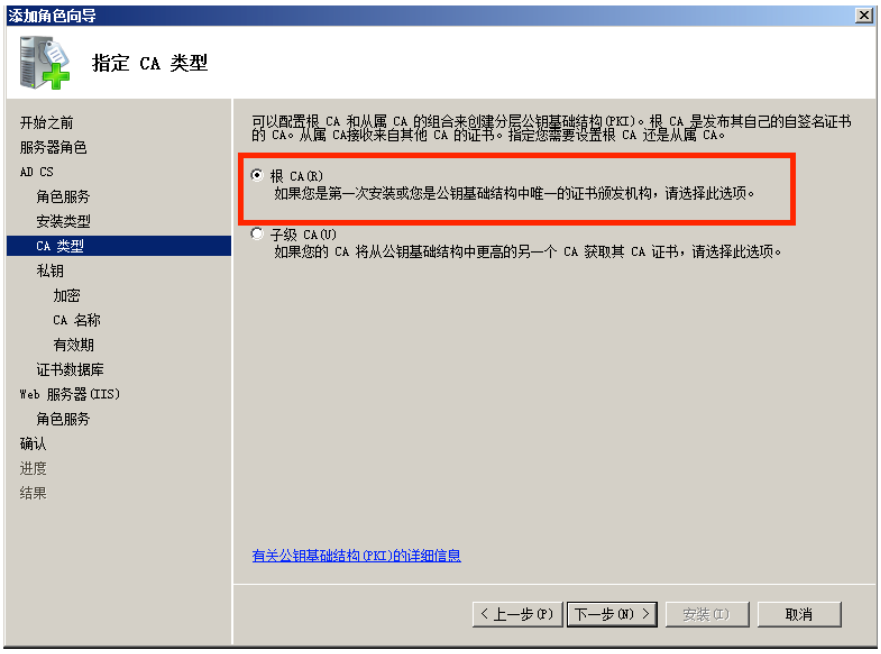


图 2-9

2.1.10、选择【新建私钥】，点击【下一步】，如图 2-10 所示

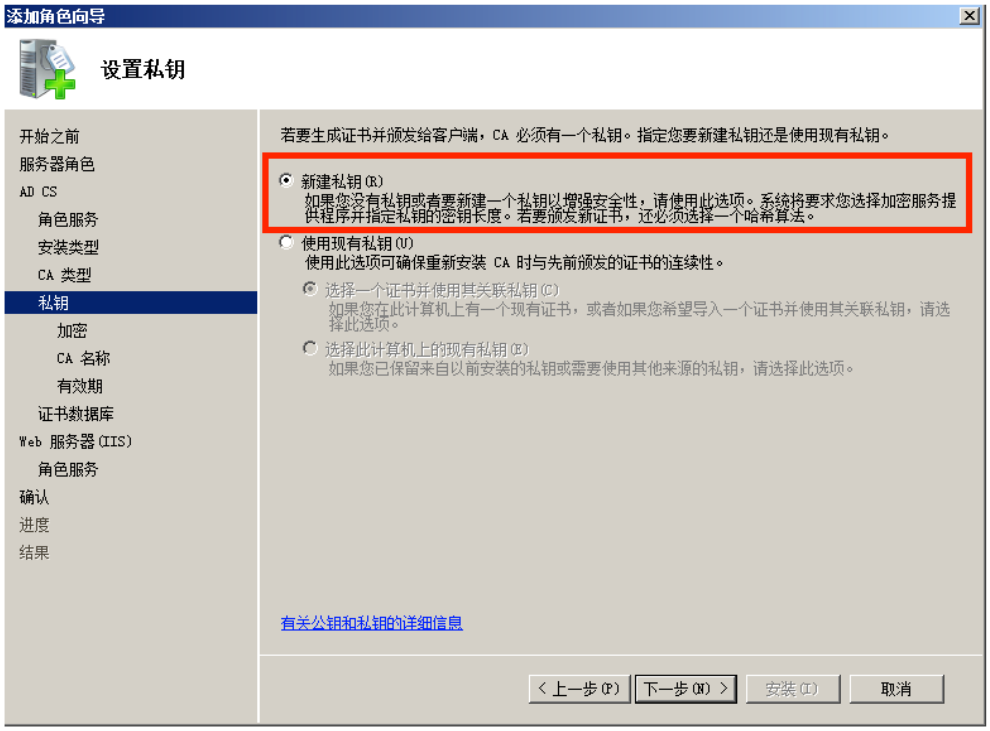


图 2-10

2.1.11、进入到 CA 配置加密页面，默认即可，点击【下一步】。如图 2-11 所示

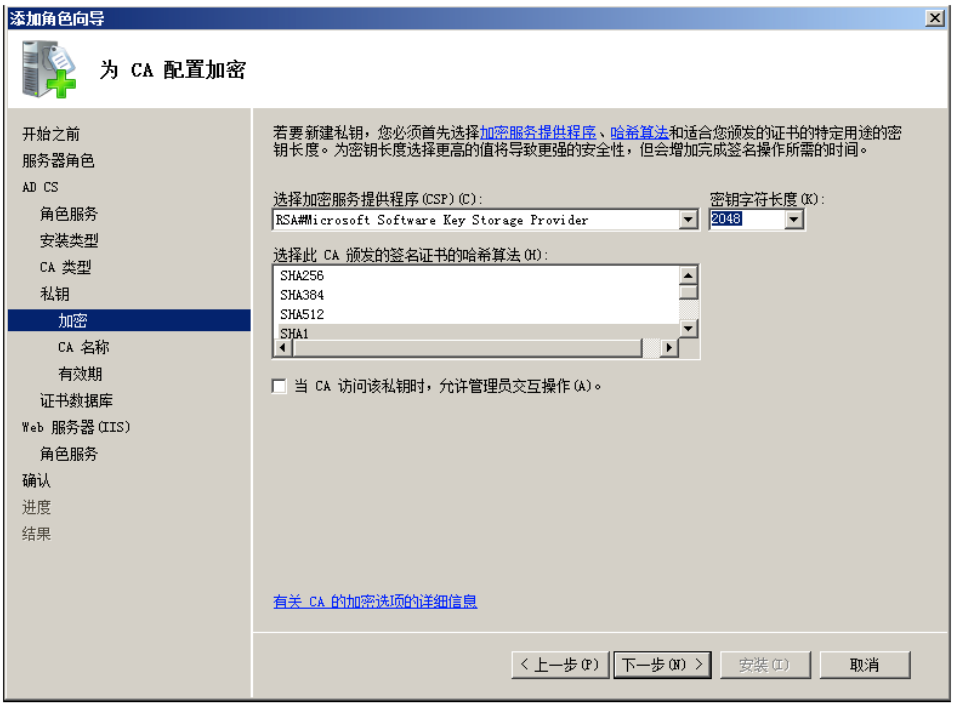


图 2-11

2.1.12、输入 CA 的名字【shiyanbar】，点击【下一步】。如图 2-12 所示

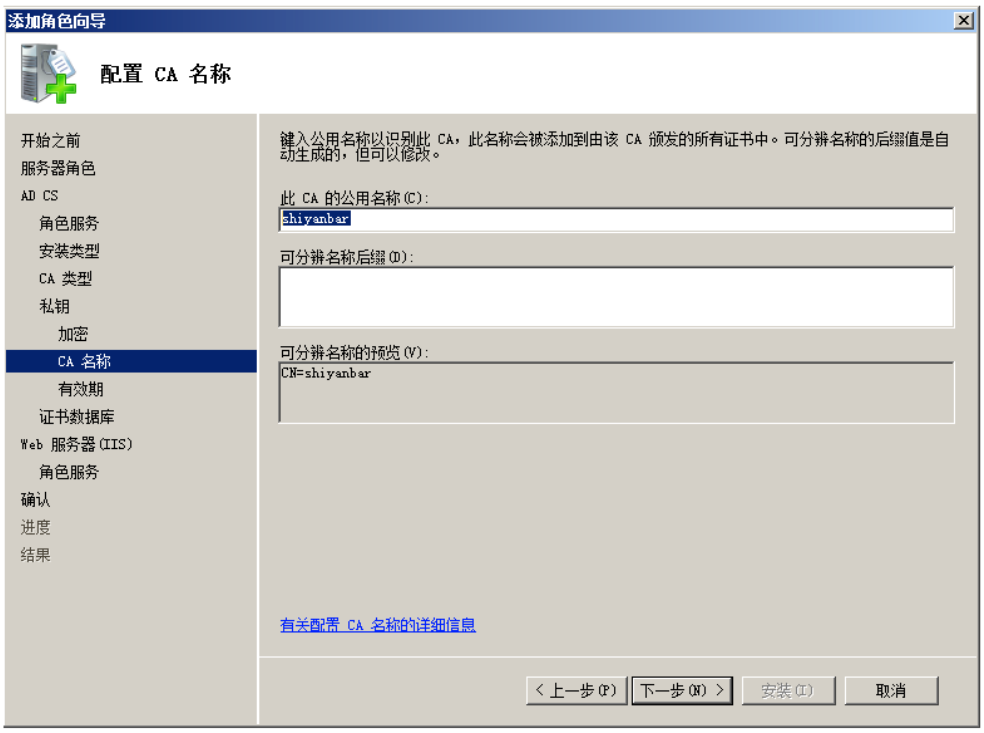


图 2-12

2.1.13、设置证书的有效期，默认即可，点击【下一步】。如图 2-13 所示

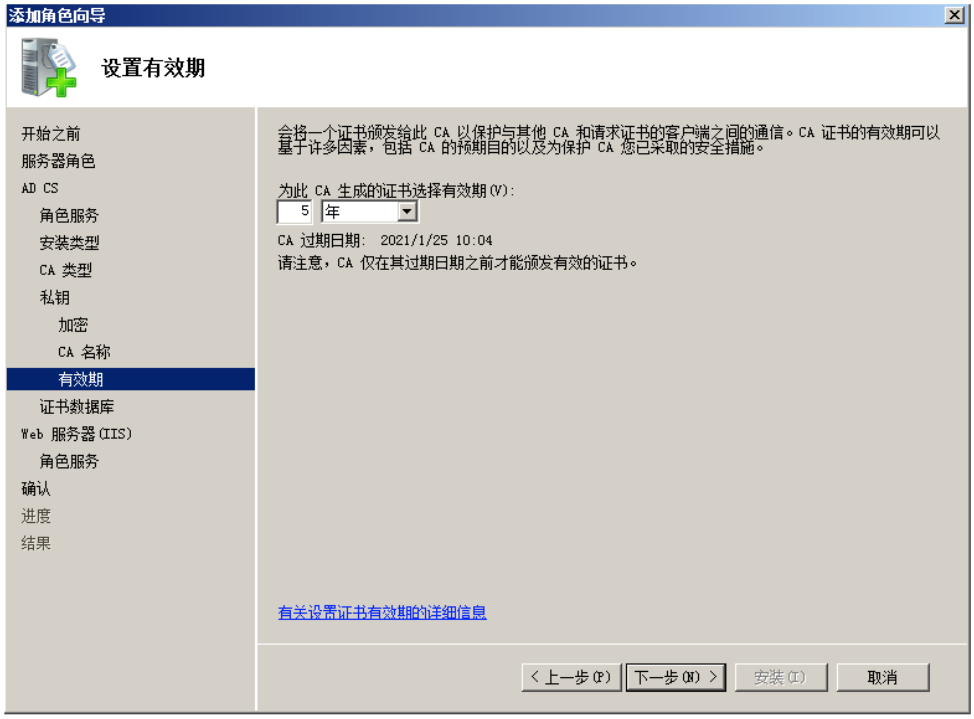


图 2-13

2.1.14、配置证书数据库，默认即可，点击【下一步】。如图 2-14 所示

图 2-14

2.1.15、进入到 Web 服务器（IIS）配置，点击【下一步】。如图 2-15 所示

图 2-15

2.1.16、根据需要勾选必要的服务，点击【下一步】。如图 2-16 所示

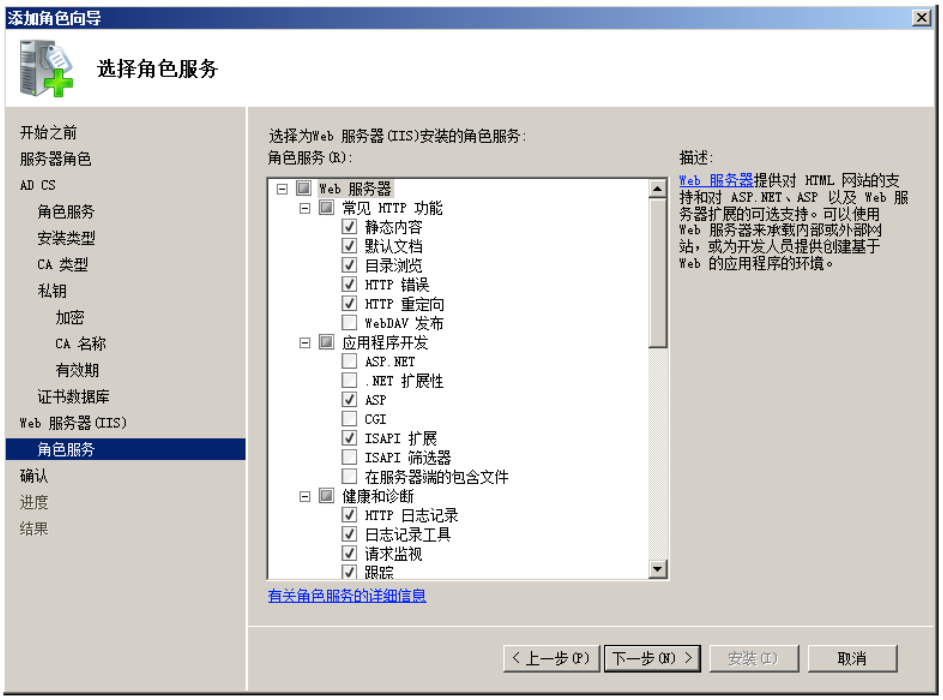


图 2-16

2.1.17、点击【安装】，即可进行安装。如图 2-17 所示

图 2-17

2.1.18、提示安装成功，点击【关闭】即可。如图 2-18 所示

图 2-18

2.1.19、打开 IE 浏览器，【工具|Internet 选项|安全|受信任的站点】，将地址【http://192.168.1.3】添加到可信站点中。如图 2-19 所示

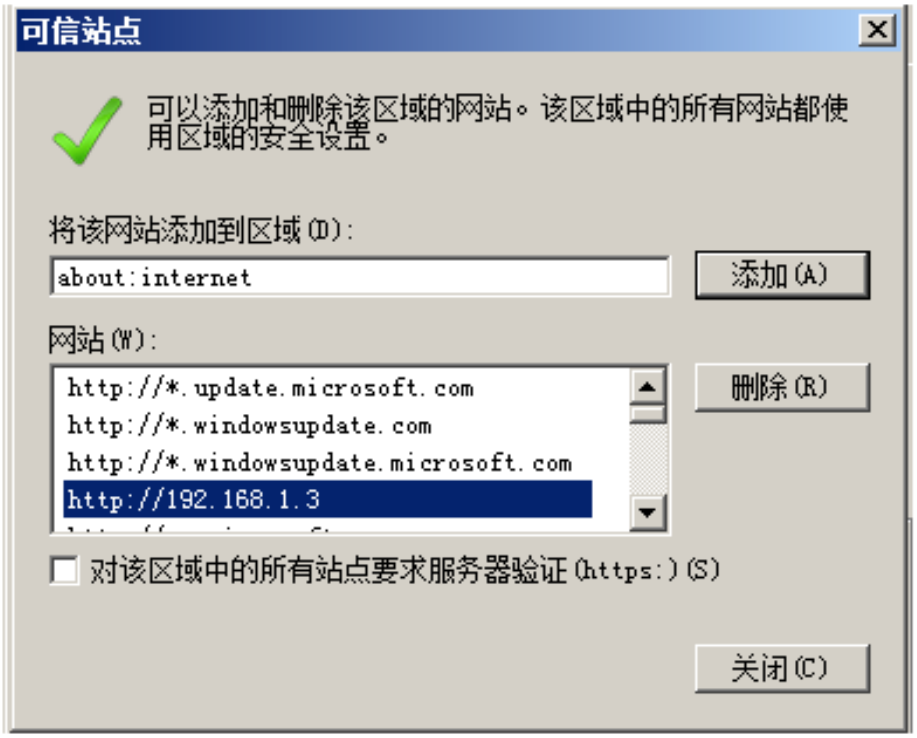


图 2-19

2.1.20、在 IE 浏览器中输入地址【http://localhost/certsrv】，即可使用证书服务了。如图 2-20 所示

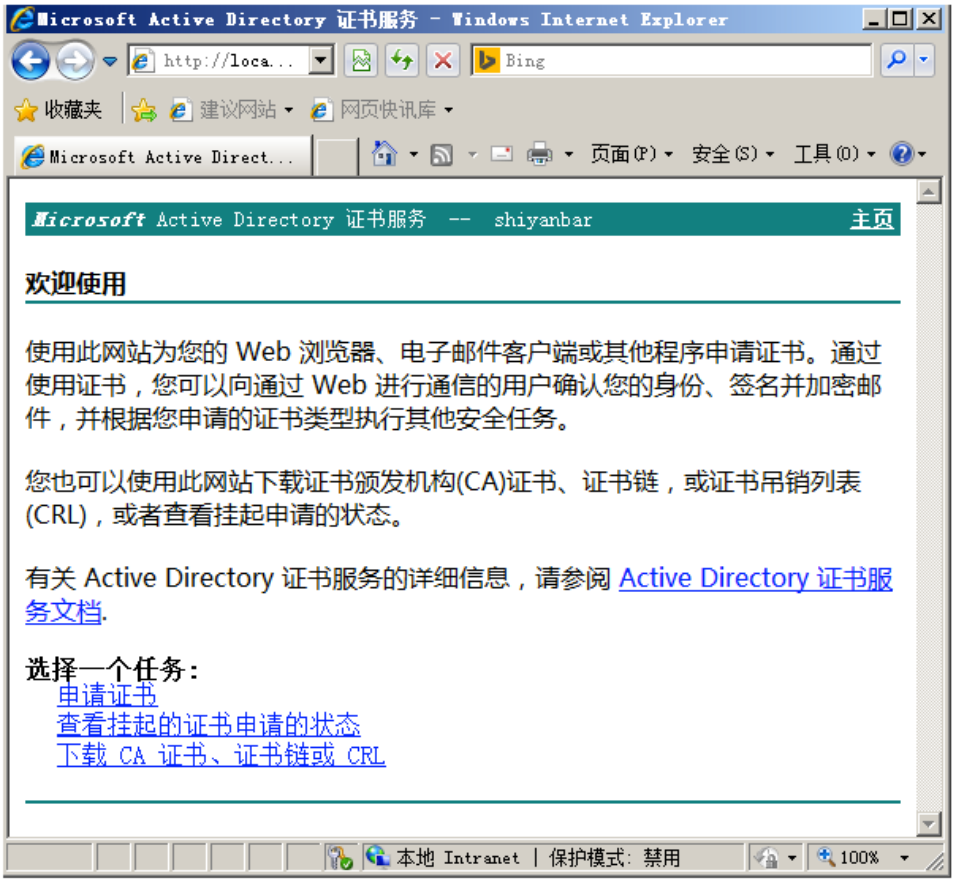


图 2-20

2.2、服务器证书的申请与颁发

2.2.1、 点击【开始|管理工具|IIS】。如图 2-21 所示

图 2-21

2.2.2、点击【服务器证书】，出现服务器证书页面。如图 2-22 所示

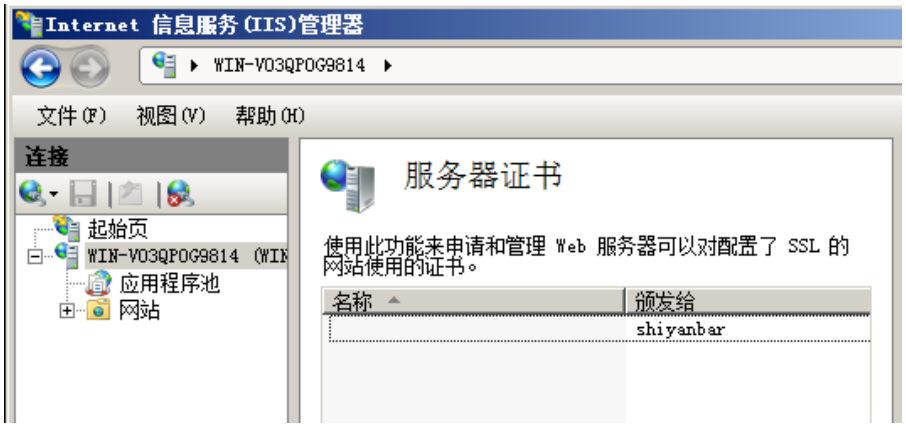


图 2-22

2.2.3、在右侧操作栏中，点击【创建证书申请】，弹出申请证书页面，填写关信息，点击【下一步】。如图 2-23 所示

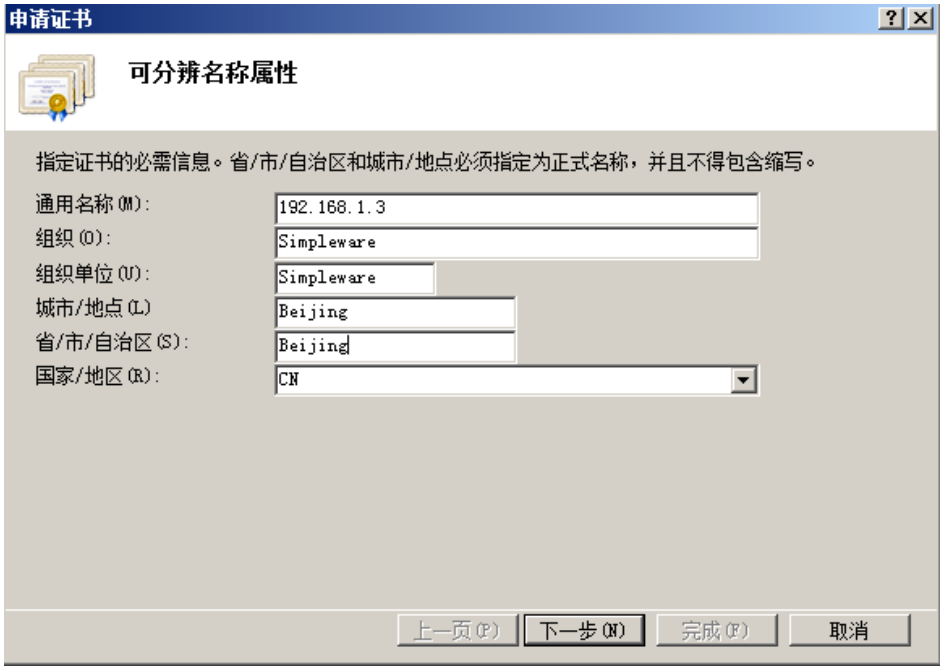


图 2-23

2.2.4、 选择加密服务提供程序，默认即可，点击【下一步】如图 2-24 所示

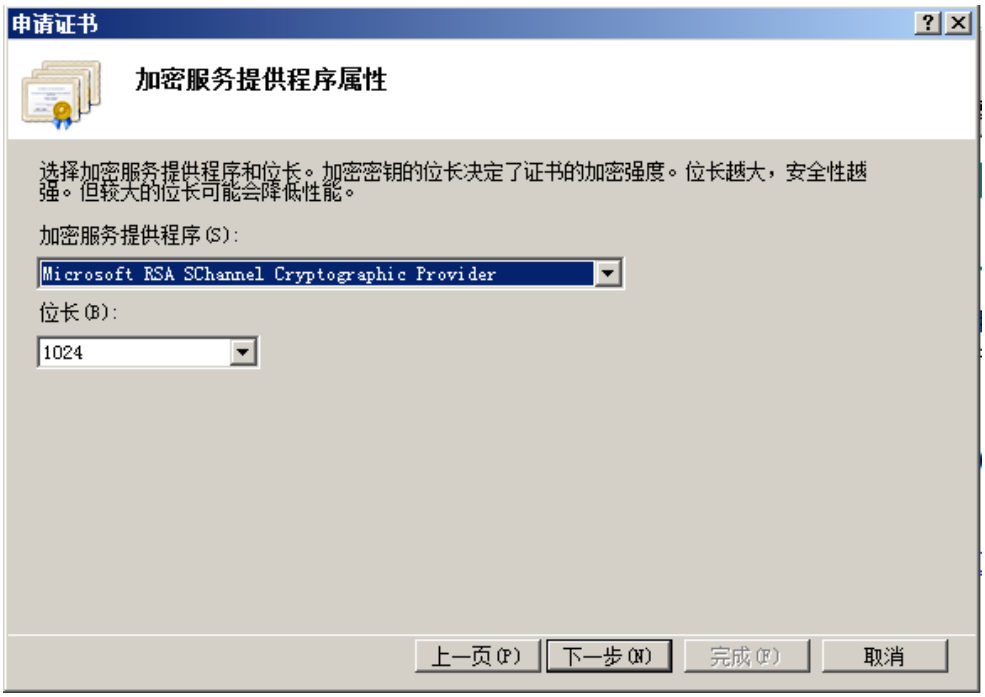


图 2-24

2.2.5、为申请的证书指定一个文件名，点击【完成】。（文件 shiyanbar_https.txt 需要手动创建）如图 2-25 所示

图 2-25

2.2.6、使用 IE 浏览器访问站点【http://192.168.1.3/certsrv】，如图 2-26 所示

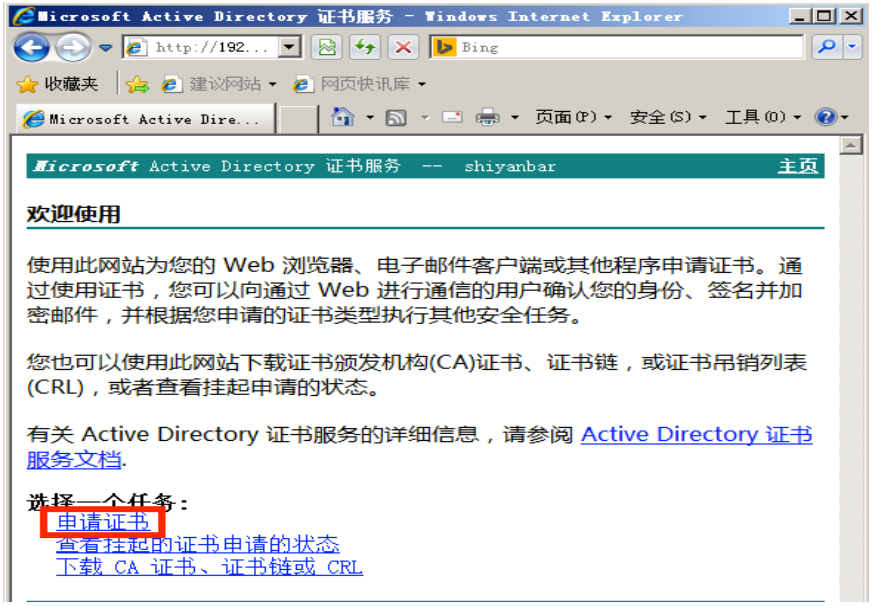


图 2-26

2.2.7、 点击【申请证书】，继续点击【高级证书申请】(若直接转到如图 28 界面，则跳过本步骤)。点击第二项【使用 bas64 编码的 CMC……】。如图 2-27 所示

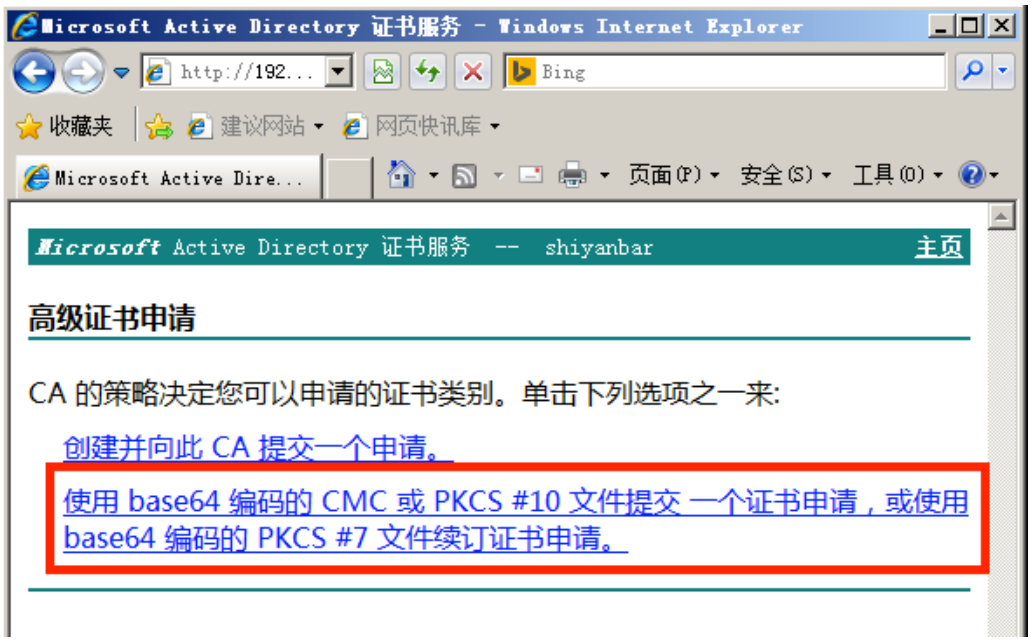


图 2-27

2.2.8、将之前保存的密钥文档文件找到并打开，将里面的文本信息复制并粘贴到“Base-64 编码的证书申请”文本框中；确定文本内容无误后，点击【提交】。如图 2-28 所示

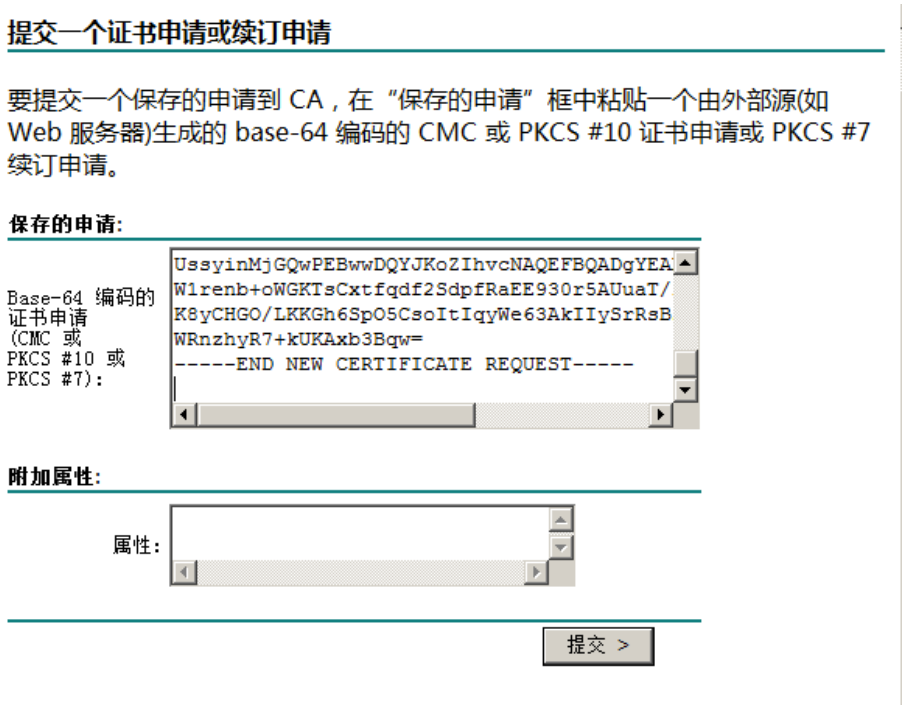


图 2-28

2.2.9、 此时可以看到提交信息，申请已经提交给了服务器，关闭 IE。如图 2-29 所示

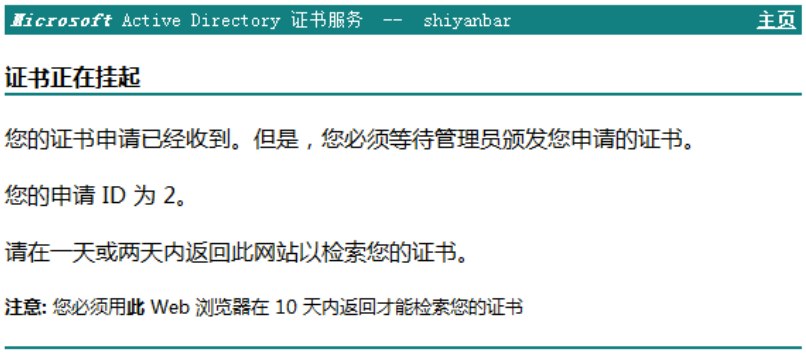


图 2-29

2.2.10、 打开证书服务器处理用户刚才提交的证书申请；点击【开始|运行】，输入：certsrv.msc，然后回车就会打开证书服务功能界面，找到【挂起的申请】位置，可以看到之前提交的证书申请。如图 2-30 所示

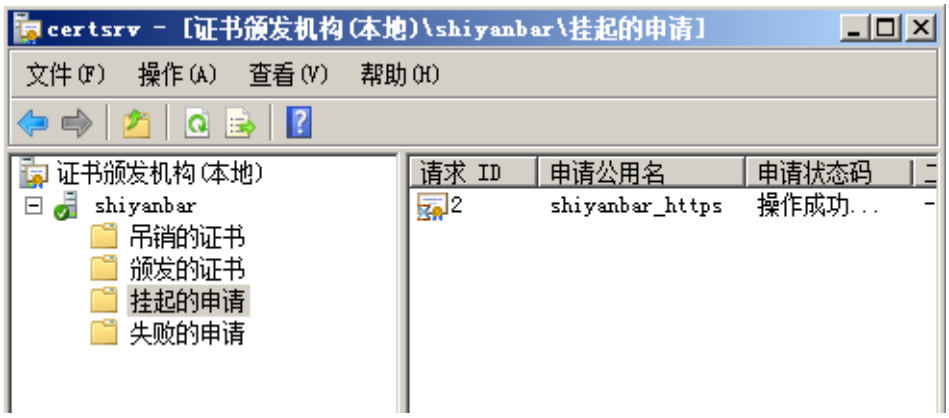


图 2-30

2.2.11、 右键点击记录【所有任务|颁发】，记录从界面中消失，点击【颁发的证书】，看到有一条记录，即说明证书申请和颁发成功。如图 2-31 所示

图 2-31

2.3、服务器证书的下载与安装

2.3.1、 打开 IE 浏览器，输入地址【http://192.168.1.3/certsrv】，点击【查看挂起的证书申请的状态】，之后会进入“查看挂起的证书申请的状态”页面，点击【保存的申请证书】。如图 2-32 所示

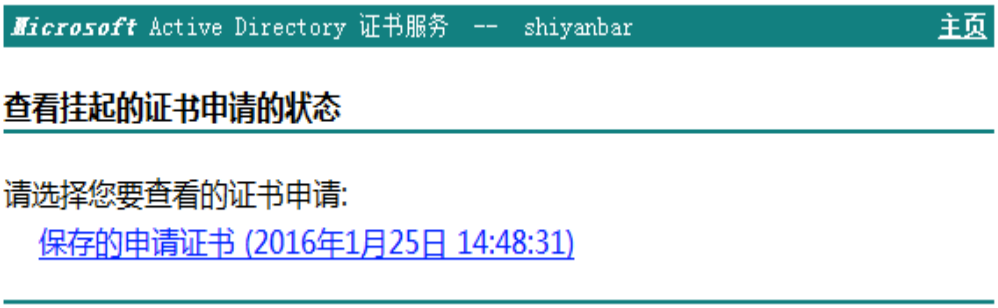


图 2-32

2.3.2、 点选【Base64 编码】，点击【下载证书】，并且将下载的证书保存。如图 2-33 所示

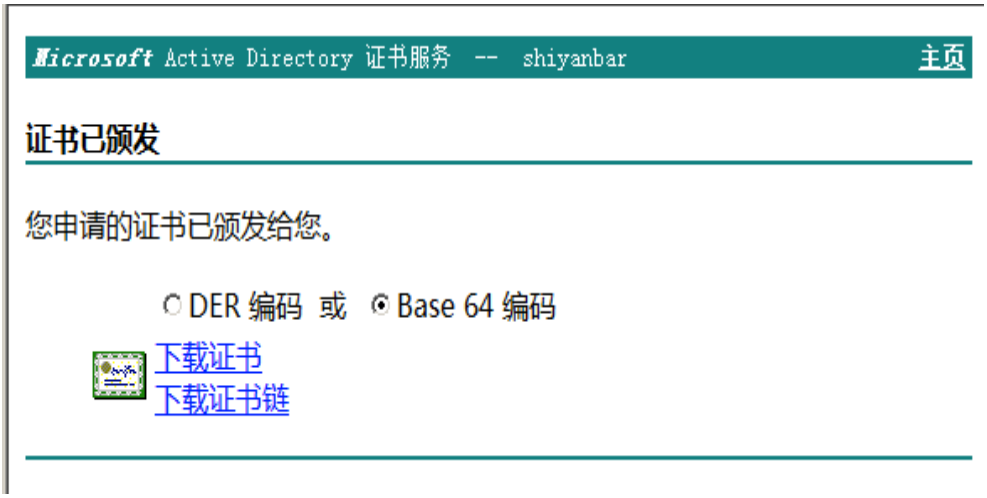


图 2-33

2.3.3、 打开 IIS 管理器，点击【服务器证书|完成证书申请】。选择刚才保存的证书。输入【shiyanbar_https】,点击确定。如图 2-34 所示

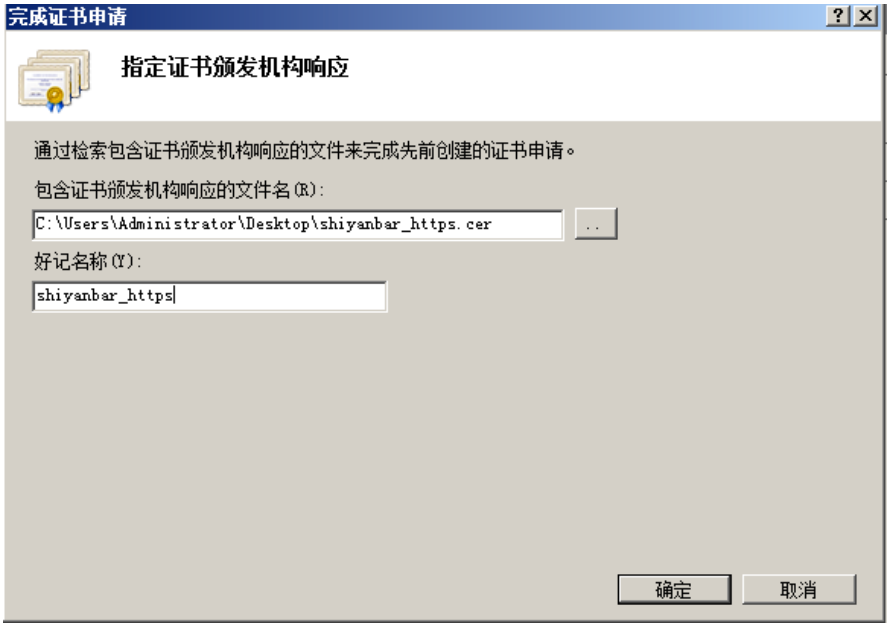


图 2-34

2.3.4、 完成上述操作之后，可以看到刚刚安装好的服务器证书。如图 2-35 所示

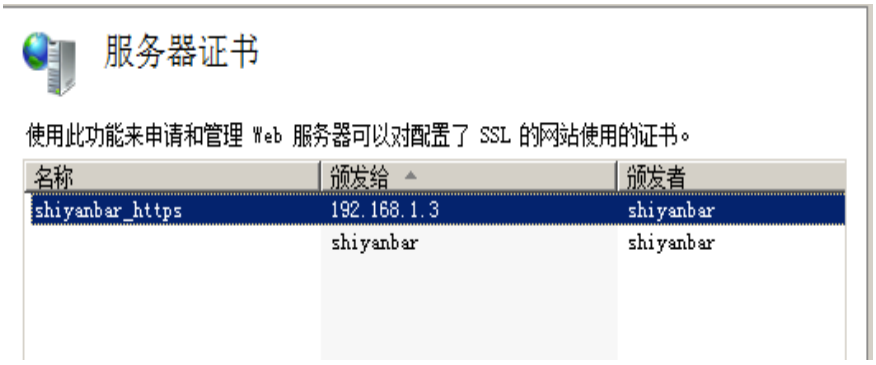


图 2-35

2.4、发布 HTTPS 协议

2.4.1、打开默认网站站点。如图 36 所示

图 2-36

2.4.2、 点击【绑定】->【添加】，将类型改为【https】，点击【SSL 证书】为【shiyanbar_https】,点击【确定】即可。如图 2-37 所示

图 2-37

2.4.3、 网站绑定窗口会出现两个记录。如图 2-38 所示

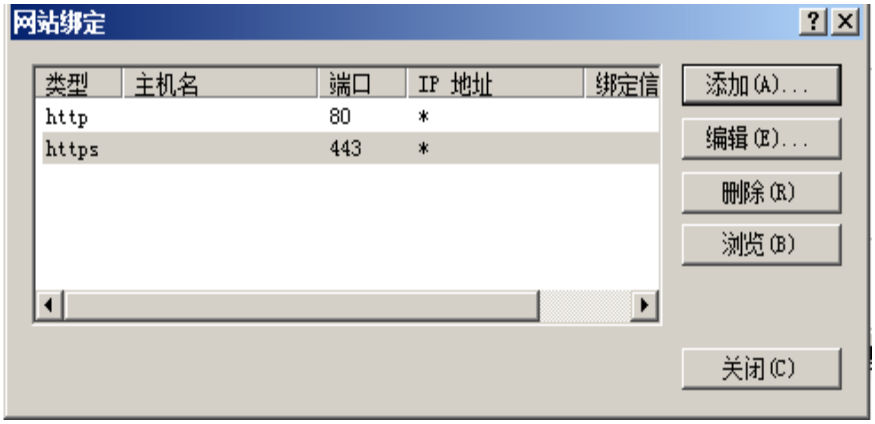


图 2-38

2.4.4、进入到默认站点的 SSL 设置，点击【应用】。如图 2-39 所示

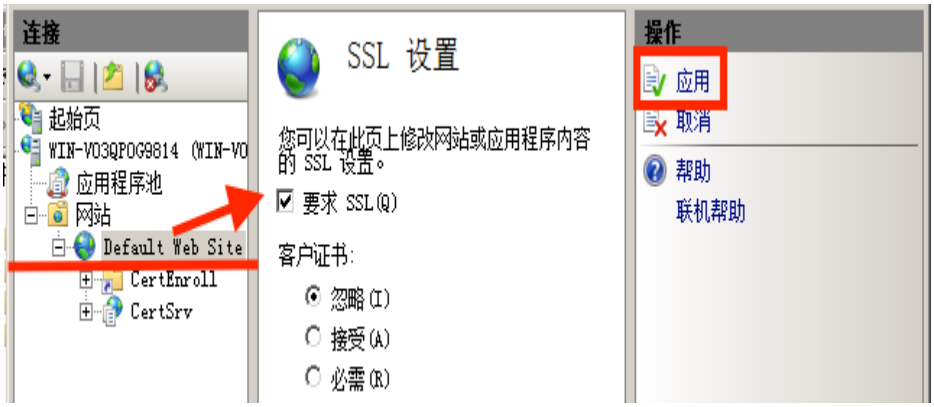


图 2-39

2.4.5、 在 IE 浏览器输入【http://192.168.1.3】。如图 2-40 所示

图 2-40

2.4.6、 在浏览器输入【https://192.168.1.3】。如图 2-41 所示

图 2-41

实验五 端口扫描与入侵检测实验

最强端口扫描器 nmap/nmap 端口扫描、入侵行为检测实验、入侵检测规则编写。

一、实验目的

利用 nmap 命令探测出目标系统开放的端口和服务类型

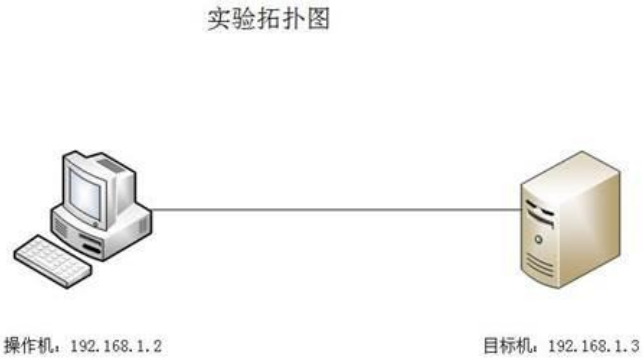
了解扫描工具 nmap

掌握网络入侵检测模式的使用方法

掌握编写规则的应用

二、实验环境

1.



2.目标机：192.168.1.3

工具目录：C:\实验工具集\02_主机安全\01_信息收集

3.CentOS 7

主机登录名：root 密码：Simplexue123

Windows 7

主机登录名：administrator 密码：Simplexue123

三、实验内容

利用 nmap 命令探测出目标系统开放的端口和服务类型

了解 nmap 端口扫描

掌握网络入侵检测模式的使用方法

入侵检测规则编写

四、实验步骤

1.利用 nmap 命令探测出目标系统开放的端口和服务类型

1.1 利用工具扫描目标主机

1.1.1 点击右边打开终端，如图 1-1

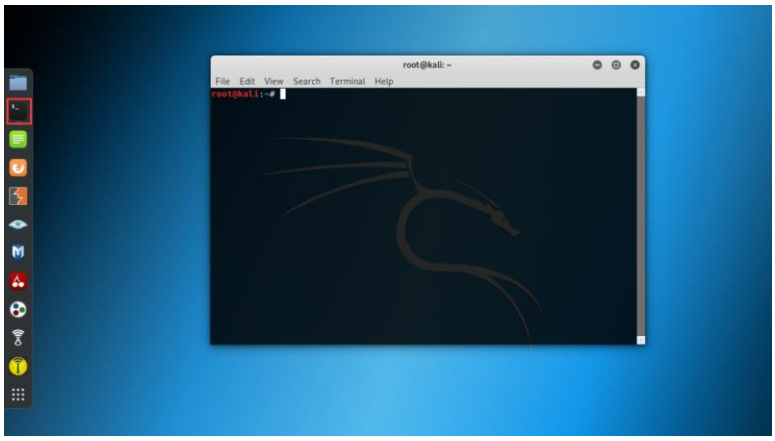


图 1-1

1.1.2 在终端中输入命令 nmap 192.168.1.3，对目标主机进行端口扫描。如图 1-2 所示

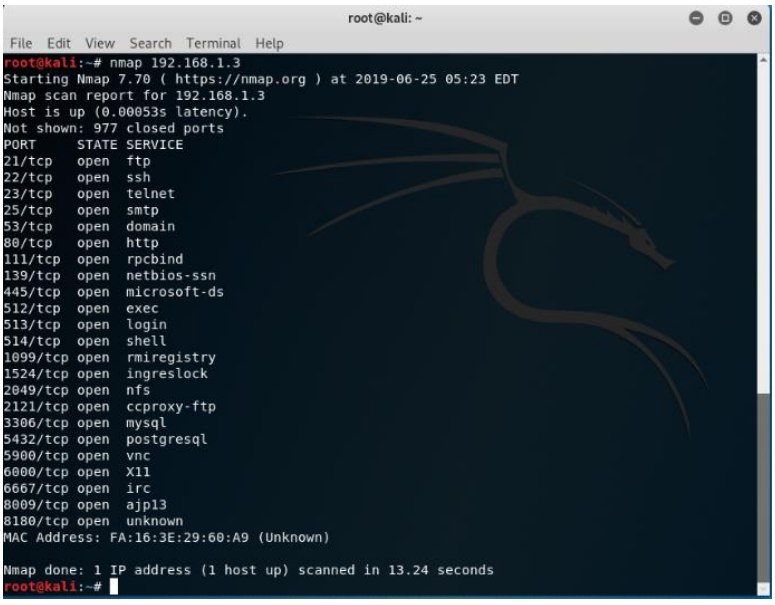


图 1-2

1.1.3 在终端中输入命令 nmap -sT 192.168.1.3，使用-sT 来实现 tcp 全连接扫描，与目标端口进行三次握手，尝试建立连接，如果建立连接成功，则说明端口开放，但是扫描速度慢。如图 1-3 所示

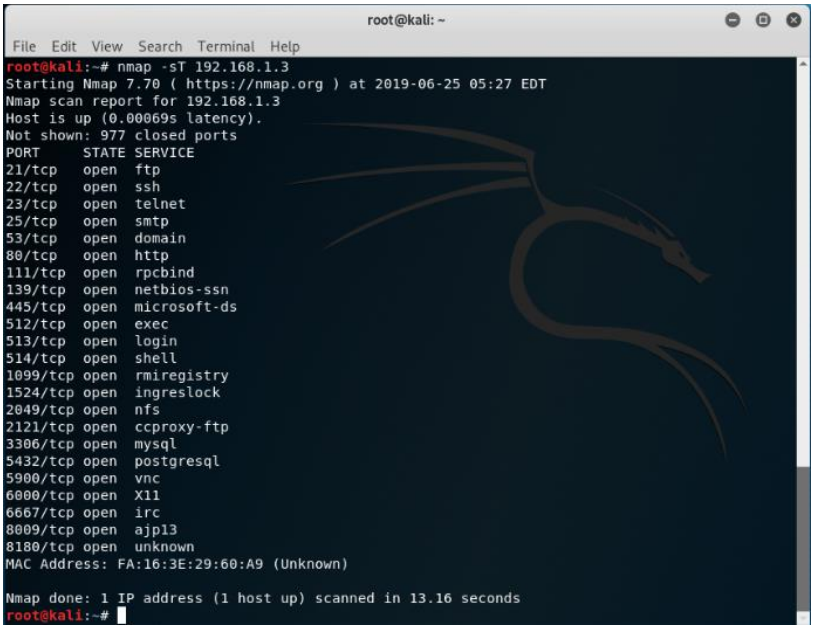


图 1-3

1.1.4 在终端中输入命令 nmap -sS 192.168.1.3，使用 SYN 扫描（-sS），该选项也称为“半开连接”或者“SYNstealth”。nmap 发送 syn 包后等待回应，如果接收 SYS/ACK 包说明端口开放，如果收到 RST 包，说明端口关闭；如果没有回应或者回应 icmp 不可达错误消息，则说明端口被过滤。如图 1-4 所示

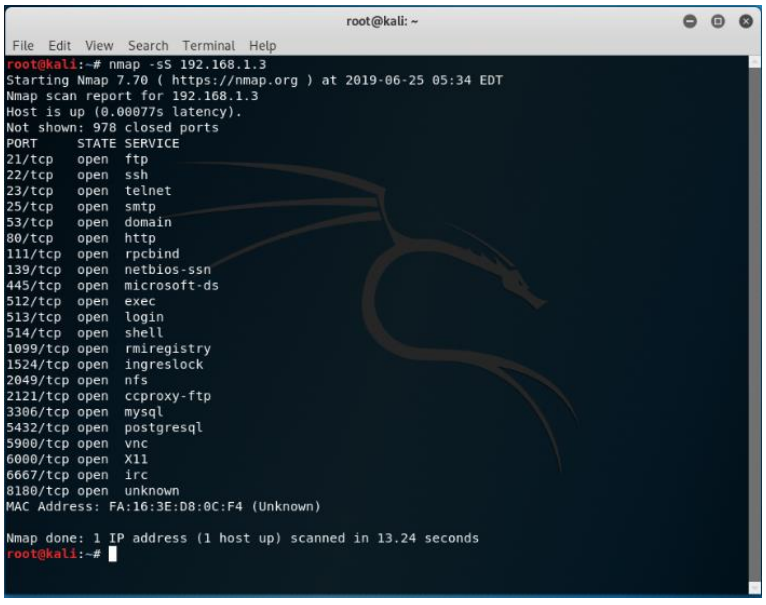


图 1-4

1.1.5 在终端中输入命令 nmap -sN -p 21,22,80,1433,3306,3389 192.168.1.3，参数-sN，即 NULL 扫描，不会设置任何控制位，参数-p 选项针对特定的端口进行扫描。如图 1-5 所示

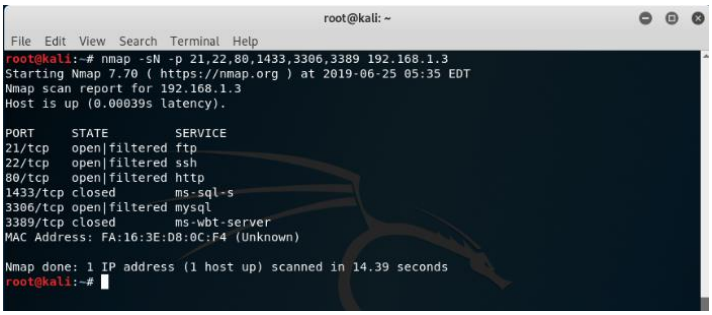


图 1-5

1.1.6 在终端中输入命令 nmap -sV 192.168.1.3，参数-sV 探测服务版本。如图 1-6 所示

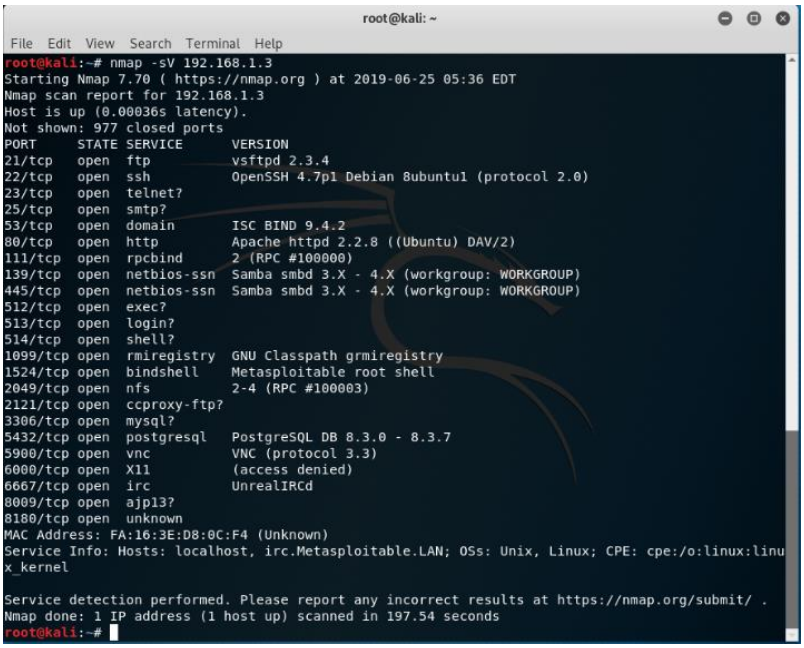


图 1-6

1.1.7 在终端中输入命令 nmap -sN -p 21,22,80,1433,3306,3389 192.168.1.3 -oX dk.html，参数-oX 在当前目录下生成 dk.html 文件，用于保存扫描信息。如图 1-7 所示

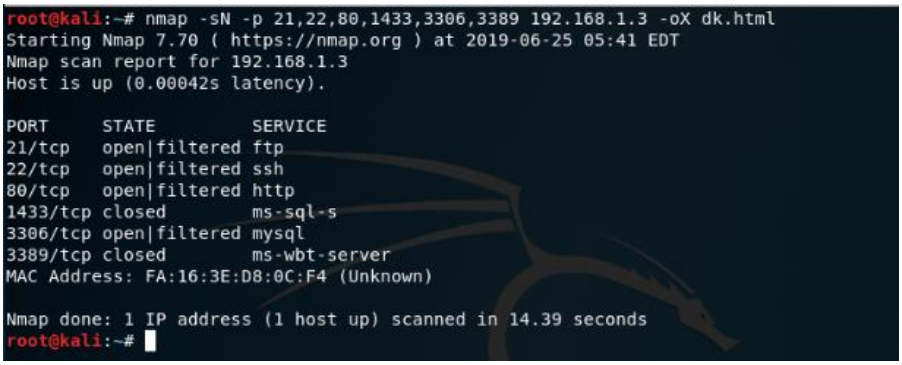


图 1-7

1.1.8 在终端中输入 cat dk.html,查看扫描信息。如图 1-8 所示

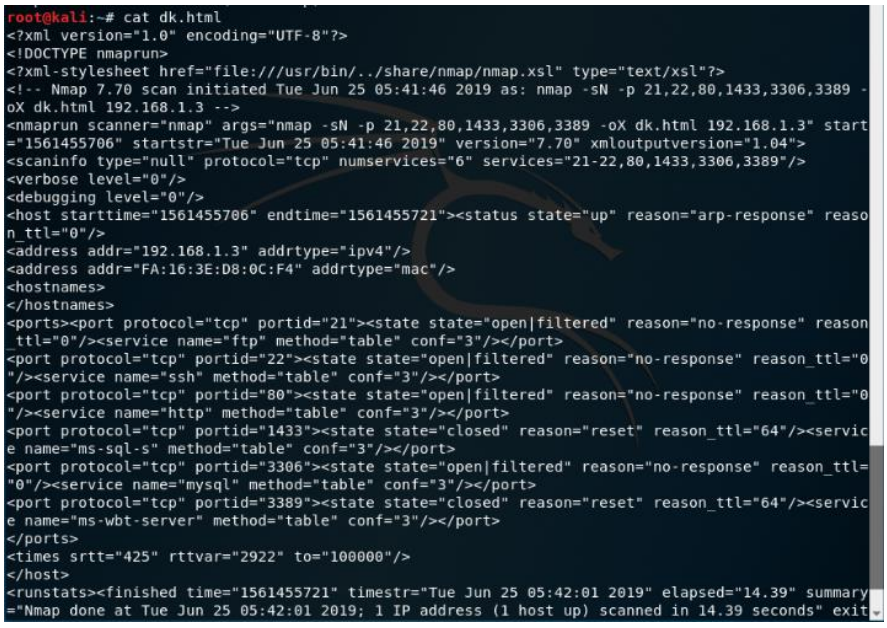


图 1-8

2.nmap 端口扫描

2.1 ZenmapGUI

2.1.1 操作机 192.168.1.2：在”C:\实验工具集\02 主机安全\01 信息收集\第 2 节 Nmap 端口扫描”中找到 NMap，并打开 Zenmap GUI。如图 2-1 所示

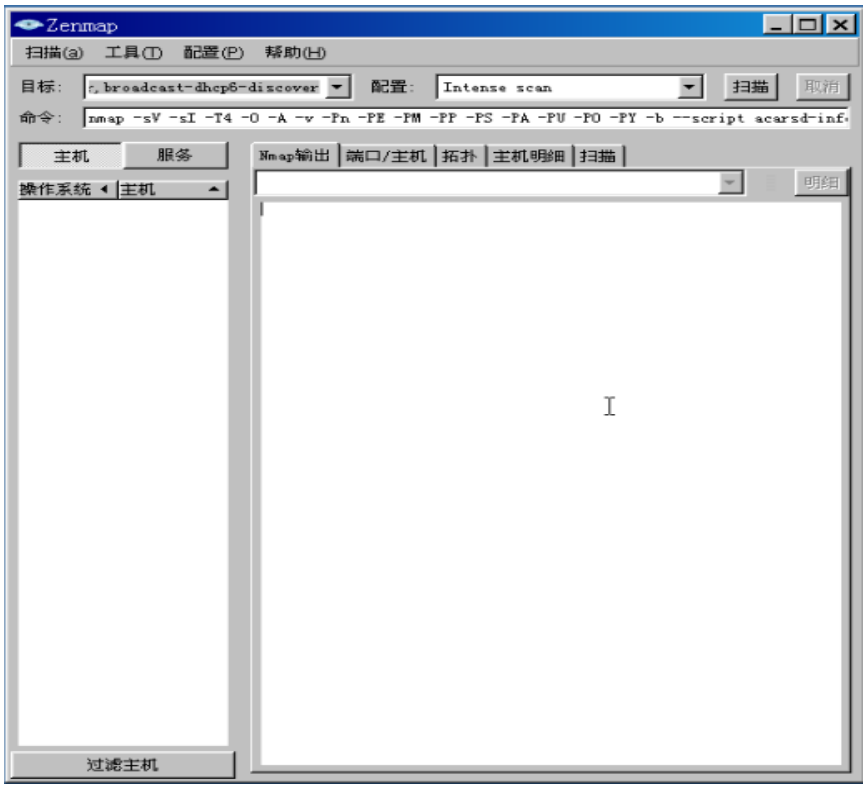


图 2-1

2.1.2 点击菜单栏中的【扫描】，点击【新建窗口】，即可创建新的扫描窗口，并输入 192.168.1.3。如图 2-2 所示

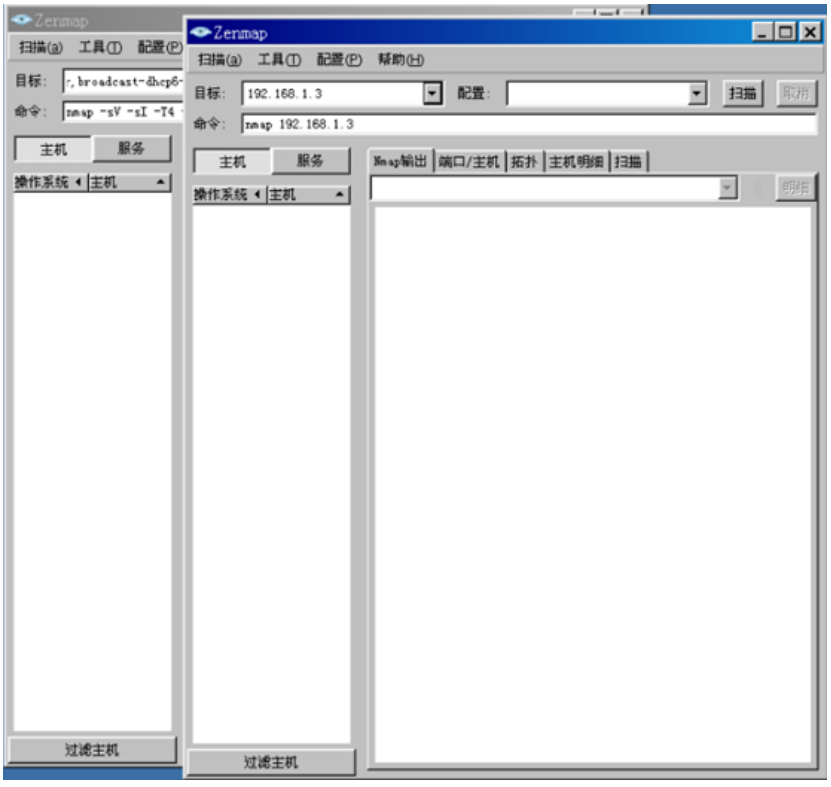


图 2-2

2.1.3 在 配置框格中，点击右侧小三角号，即可选择扫描方式，在此处可以选择【Regular scan】。如图 2-3 所示

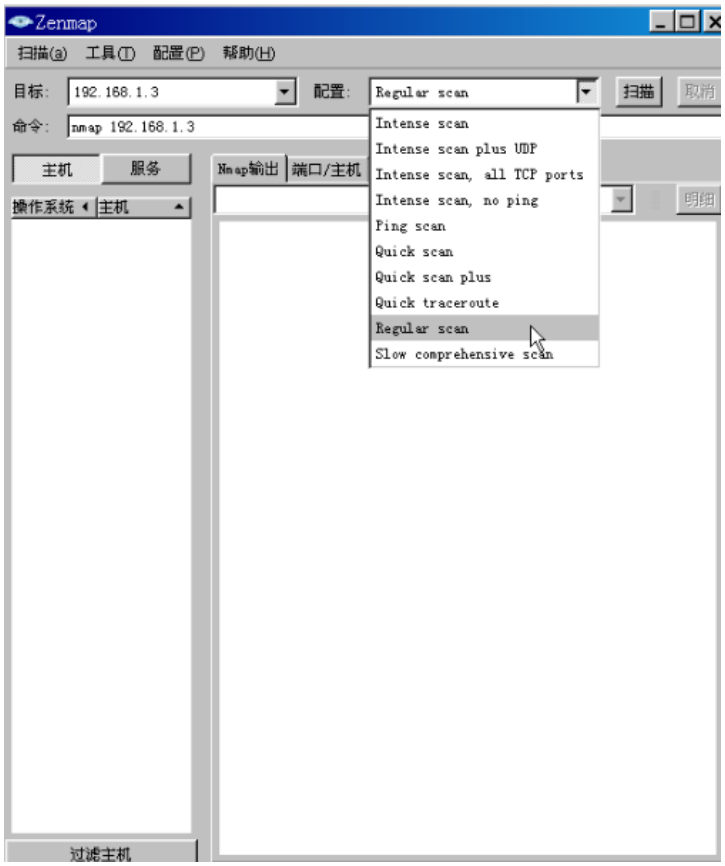


图 2-3

2.1.4 点击右侧【扫描】按钮即可进行扫描。如图 2-4 所示

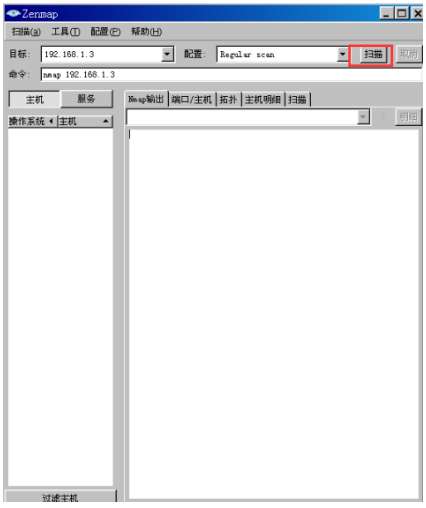


图 2-4

2.1.5 经过一段时间之后，即可得到扫描结果。如图 2-5 所示

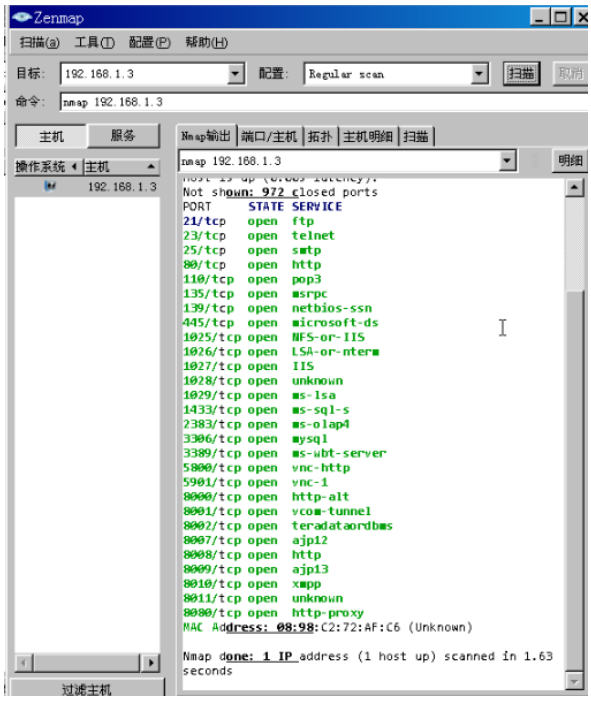


图 2-5

2.1.6 点击【服务】和【端口/主机】即可查看目标主机开启的服务所对应的窗口。如图 2-6 所示

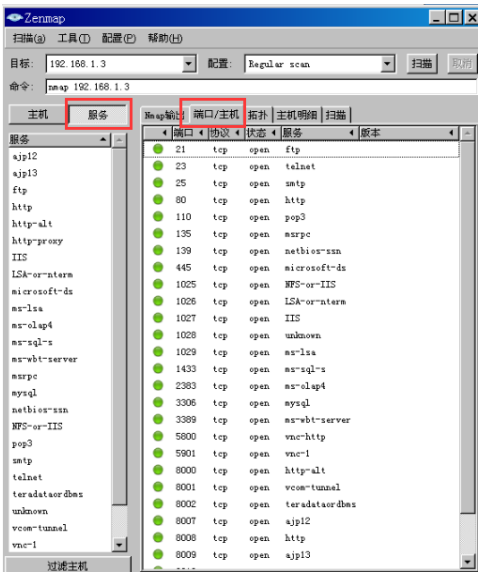


图 2-6

2.2 命令行模式

2.2.1 操作机 192.168.1.2：打开 cmd，输入命令【nmap】即可得到命令帮助信息。

如图 2-7 所示

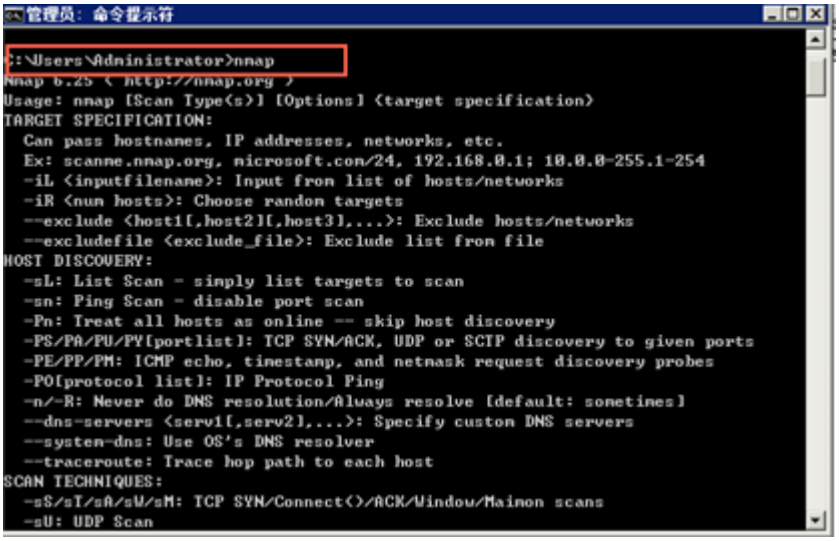


图 2-7

2.2.2 在命令行下输入命令【nmap 192.168.1.3】，进行 RegularScan。如图 2-8 所示

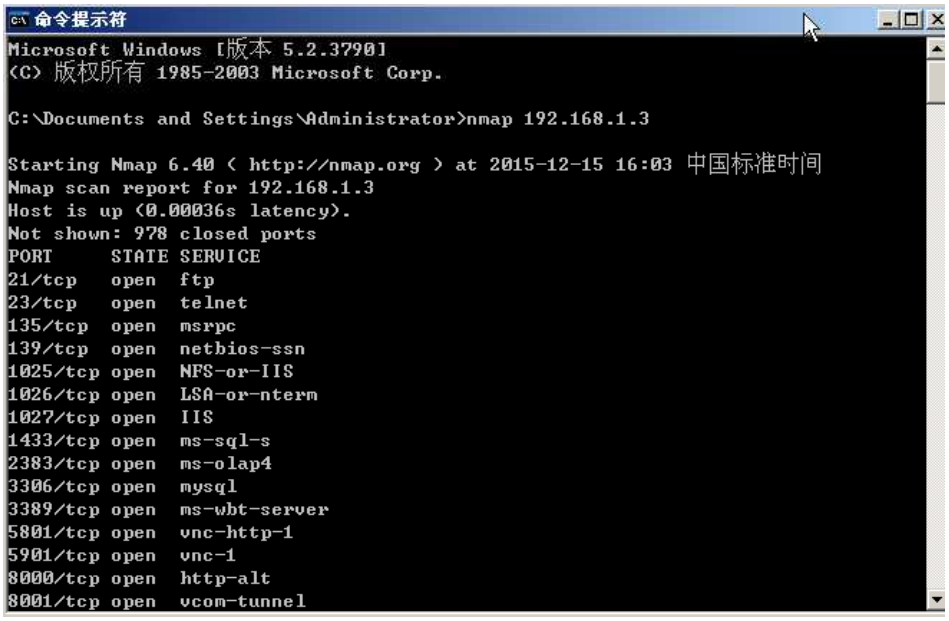


图 2-8

2.2.3 在命令行下输入命令【nmap -p 21,22,80,3389 192.168.1.3】，对指定的 21，22，80，3389 端口进行扫描。如图 2-9 所示

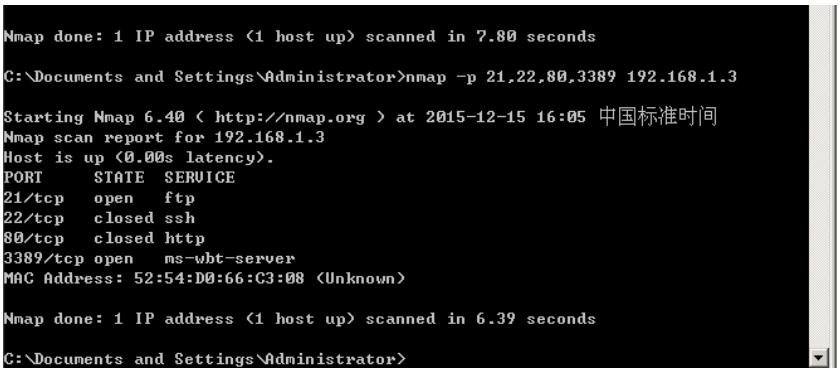


图 2-9

2.2.4 在命令行输入【nmap -sT 192.168.1.3】，对目标主机进行全连接扫描。全连接扫描完成完整的三次握手过程，稳定可靠但容易被日志记录。此种方法花费时间可能较长。如图 2-10 所示

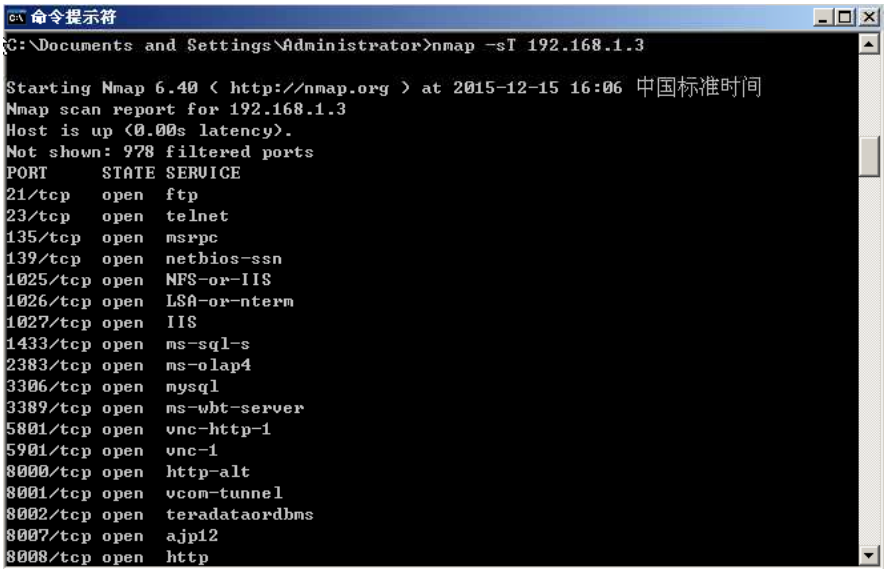


图 2-10

2.2.5 在命令行输入【nmap -sS 192.168.1.3】，对目标主机进行半开连接扫描。扫描器向目标主机发送 SYN 包测试主机是否监听某个端口而不进行全连接。此种方法比全连接扫描方式隐蔽。如图 2-11 所示

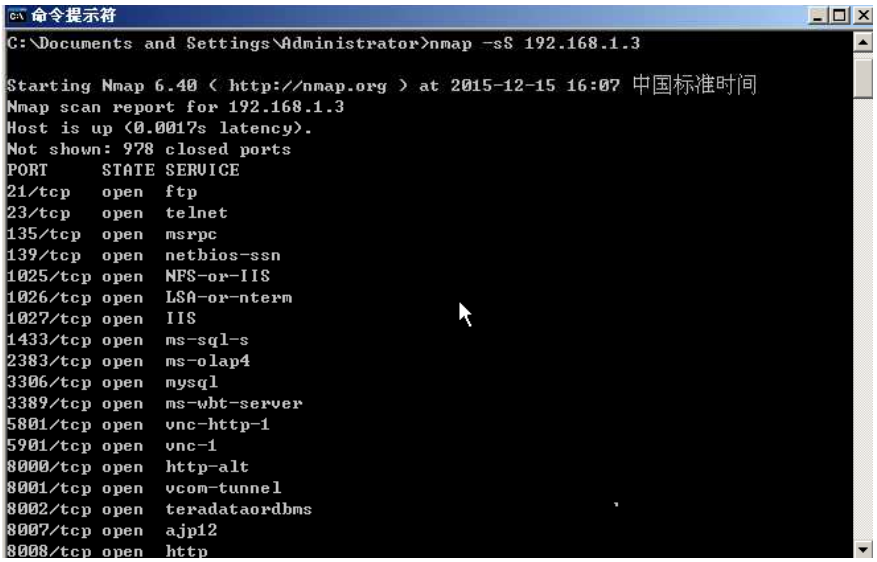


图 2-11

2.2.6 输入命令【nmap -sV 192.168.1.3】，用以显示 banner 信息。如图 2-12 所示

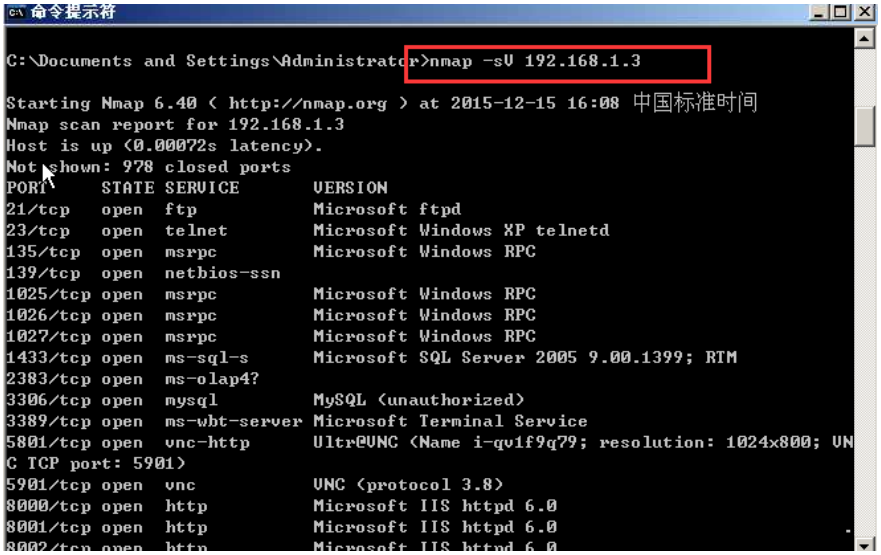


图 2-12

2.2.7 输入命令【nmap -oX 1.xml 192.168.1.3】，即将扫描结果以 xml 的形式输出，文件名为【1.xml】。如图 2-13 所示

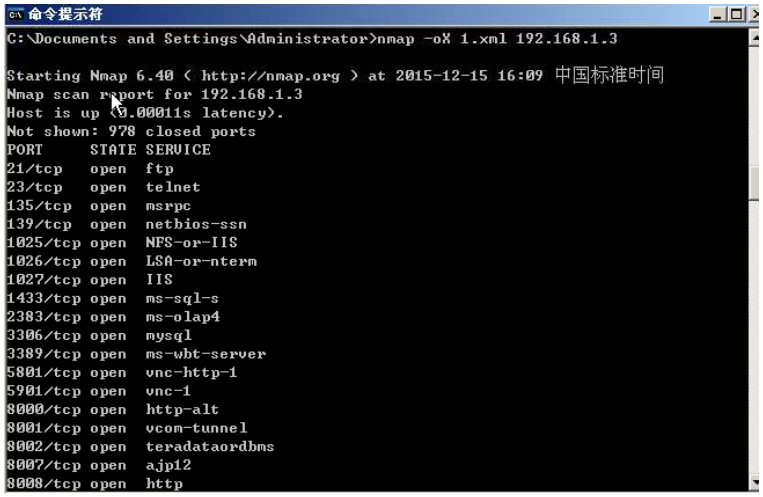


图 2-13

2.2.8 保存文档的位置在【C:\Documents and settings\Administrator】，双击保存好的【1.xml】文件，即可查看结果。如图 2-14 所示

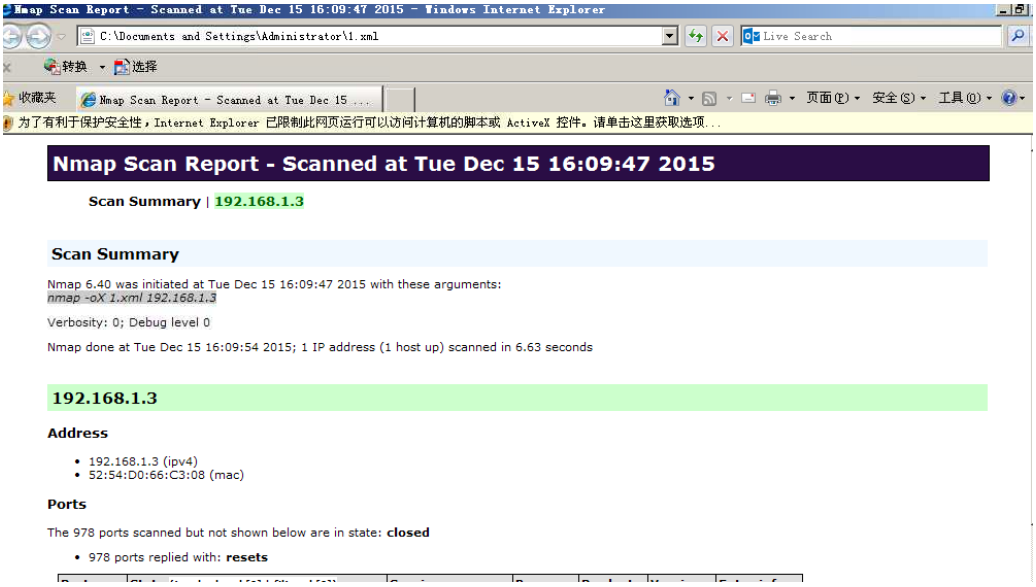


图 2-14

2.2.9 在命令行界面，nmap 命令也可以组合使用，具体命令说明请参考命令【nmap】的结果，具体组合方式请同学们自行尝试。

3.入侵行为检测实验

3.1.1 入侵检测模式简单介绍：

- 网络入侵检测模式（Network Intrusion Detection Mode）需要载入规则库才能工作。在入侵模式下，Snort 并不记录所有捕获的包，而是将包与规则

对比，仅当包与某个规则匹配的时候，才会记录日志或产生报警。如果包并不与任何一个规则匹配，那么它将会被悄悄丢弃，并不做任何记录。运行 Snort 的入侵检测模式的时候，通常会在命令行指定一个配置文件。

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。

- 命令参数介绍：

  -c：这是最常用的选项，用来指定配置文件 snort.conf 的位置。如果执行该选项，Snort 就会去指定路径寻找 snort.conf 文件。例如，如果 snort.conf 文件在/etc 目录中，我们要用命令行选项“-c /etc/snort.conf”来启动 Snort。

  -h：设置本地网络，如 192.168.1.0/24。

  -d：显示包的应用层数据。

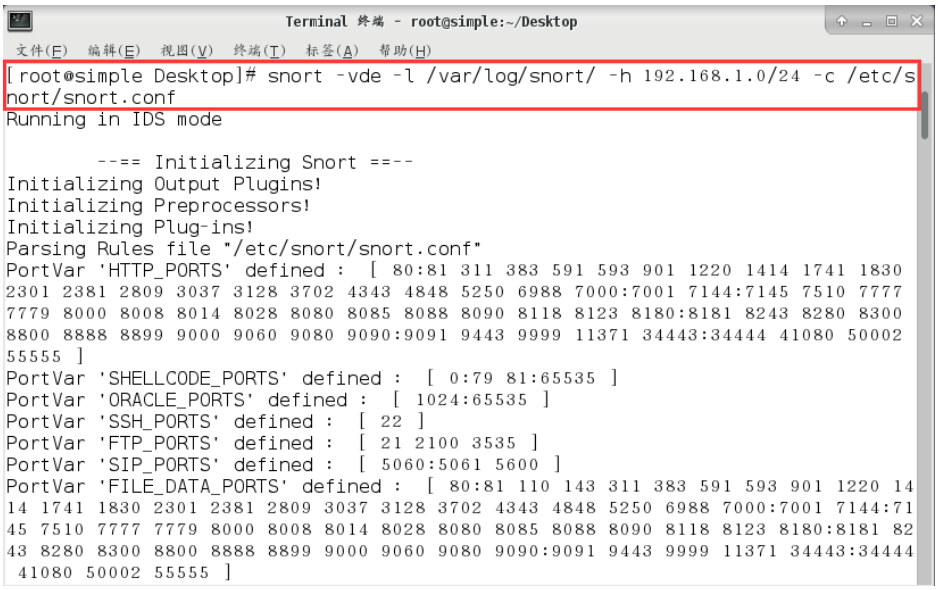
  -s：使 snort 把报警消息发送到 syslog，默认的设备是 LOG_AUTHPRIV 和 LOG_ALERT。可以修改 snort.conf 文件修改其配置。

  -A：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。

3.1.2 打开地址为 192.168.1.2 的主机 init 5 进入桌面模式，输入命令 snort -vde -l /var/log/snort –h 192.168.1.0/24 –c /etc/snort/snort.conf。启动 snort，将数据包输出到/var/log/snort 目录下。ctrl+c 结束掉该进程。

“-h 192.168.1.0/24”参数作用为只对本地网络进行日志分析。

“-c /etc/snort/snort.conf”参数作用为加载/etc/snort/snort.conf 该配置文件。如下图 3-1 所示



- 图 3-1

3.1.3 使用 cat 命令查看 snort.conf 文件。命令为 cat /etc/snort/snort.conf。该文件中包含了许多入侵检测的规则文件。如下图 3-2 所示

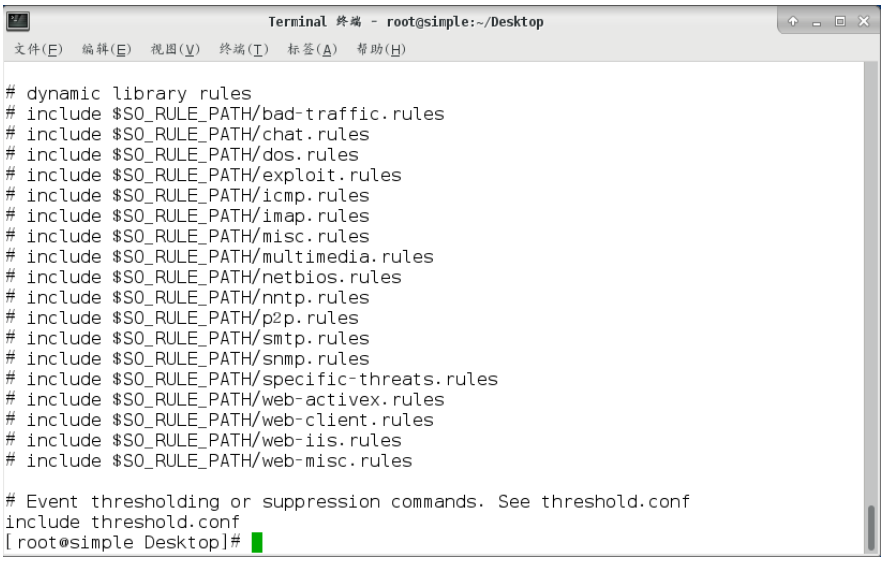


图 3-2

3.1.4 “-l”参数可以指定日志文件存放的位置。如果在“-l”参数后没有指定具体位置。系统自动将日志保存在/var/log/snort 目录下。首先 ls 查看/var/log/snort 下的日志文件，有日志文件将其删除，命令为 rm –rf snort.log.*。如下图 3-3 所示

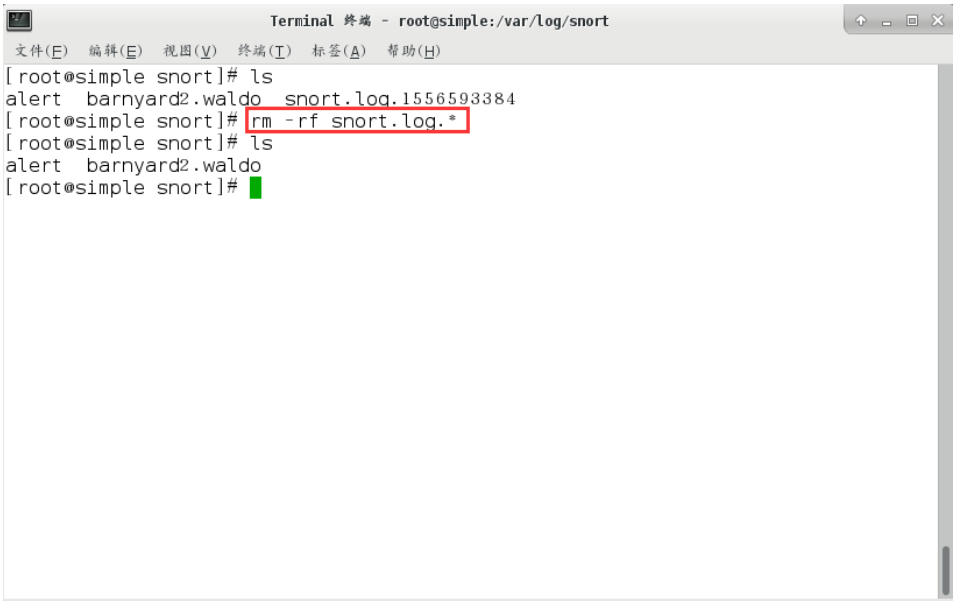


图 3-3

3.1.5 执行命令 snort –c /etc/snort/snort.conf。如下图 3-4 所示

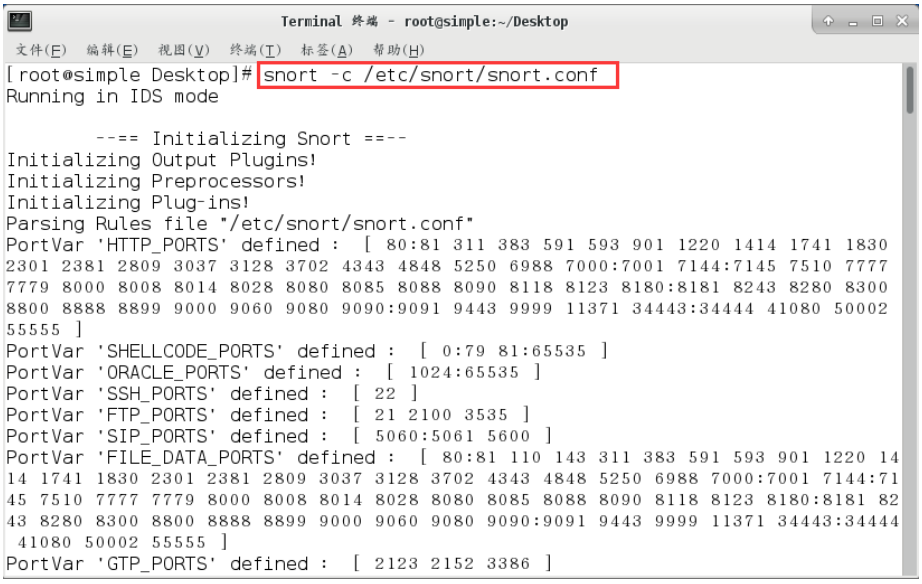


图 3-4

3.1.6 使用 ctrl+c 组合键结束掉该进程，进入/var/log/snort 的目录，使用“ls”命令查看该目录下的文件。发现以“snort.log.”命令的日志文件，已经再次生成。如下图 3-5 所示

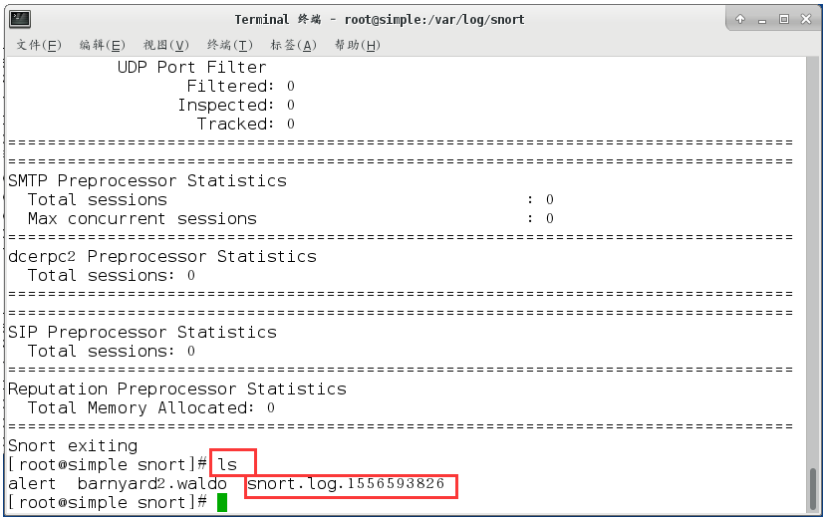


图 3-5

3.1.7 切换目录为“/home”,查看该目录下的文件。并没有“snort.log.”开头的文件。如下图 3-6 所示

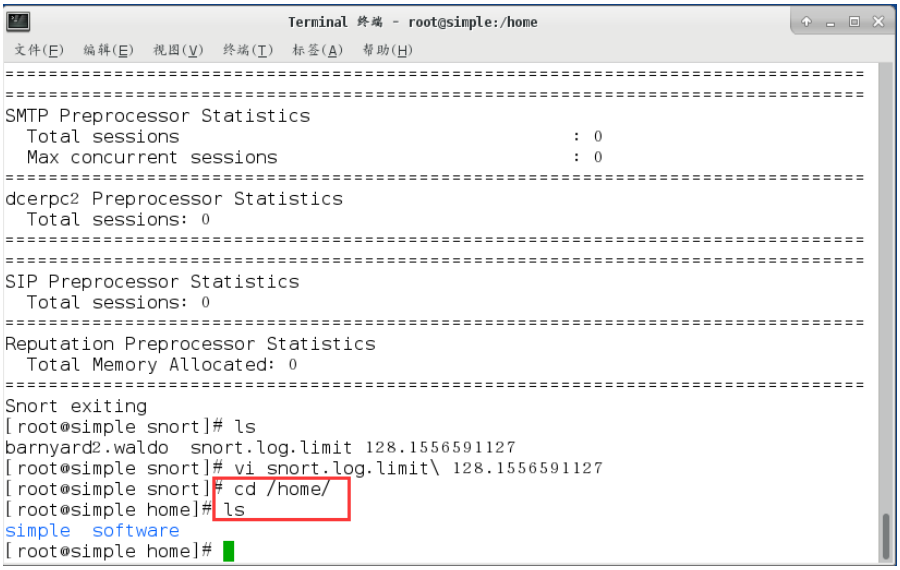


图 3-6

3.1.8 执行命令 snort –l /home/ –c /etc/snort/snort.conf。如下图 3-7 所示

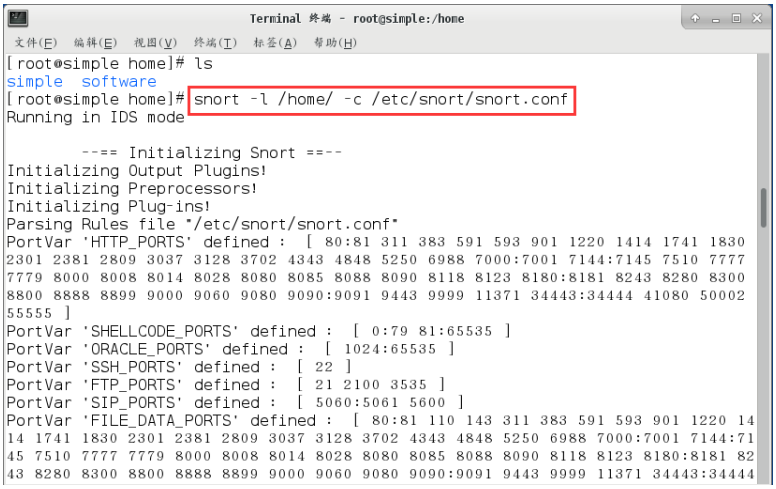


图 3-7

3.1.9 使用 ctrl+c 的组合键结束掉 snort 的进程。将目录切换到“/home”目录下。使用“ls -l”命令查看“/home”下的文件。在 home 目录下输出日志文件成功（注意：如果没有看到相关日志文件，可重新打开一个新终端进行查看）。如下图 3-8 所示

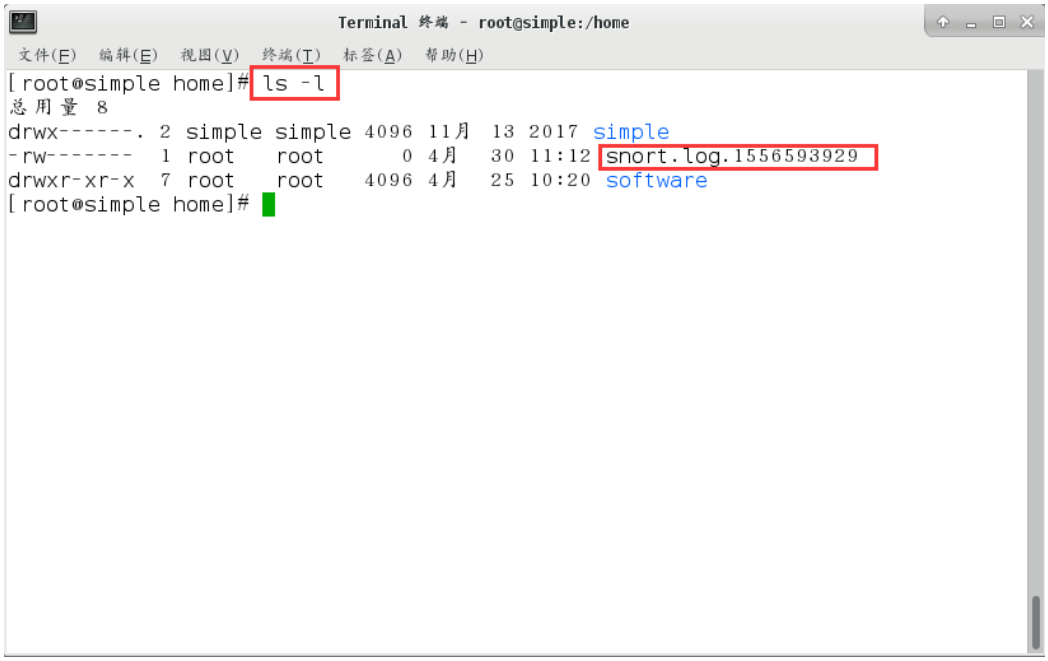


图 3-8

3.2. 入侵检测输出插件的四种模式

3.2.1 输出插件的作用是将报警数据输出到显示器或转储到文件。所以对于 Snort 而言输出插件就是系统的主要瓶颈，Snort 本身能对封包进行快速读取和分析处理，但是试图将其显示输出，或者存储到数据库中时却有些力不从心。如何将

Snort 日志记录到一个指定文件呢？我们通过执行命令（假设/var/log/snort/yourfile 文件存在）来记录。这里我们对 4 个输出插件进行简单介绍。在入侵检测模式中 alert-mode 有 fast、full、unsock 和 none 四种模式。

fast：是一种快速简单的输出插件，之所以快是因为它只记录 timestamp（时间戳）、signature(特征)、source IP、destinationIP、source port、destination port、TCP flags 和 Protocol。

full：对每个产生警报的 IP 将其解码后的包记录下来。与 fast 不同的是，它记录地更全面。这也是它的预设告警模式。

unsock：这个插件的作用是建立一个 UNIX 域管道并向它发送警报。当然其它进程也可对该管道进行监听，目的是实时接收 Snort 警报数据。注意一点这个功能和 Windows 系统无法配合使用。

none：这个插件作用是关闭警报。

3.2.2 这里只需要掌握-A 参数后面跟的四个参数的含义，了解这四个参数只是让 Snort 能以不同的方式报警。以 fast 为例进行简单操作，执行命令 snort -A fast。如下图 3-9 所示

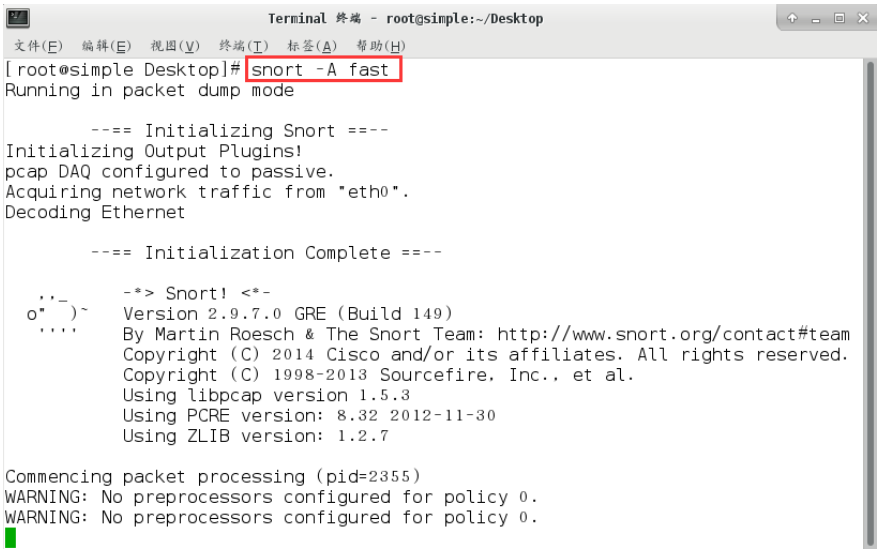


图 3-9

3.2.3 在虚拟机 192.168.1.3 上 ping 访问 192.168.1.2，执行命令 ping 192.168.1.2。如下图 3-10 所示

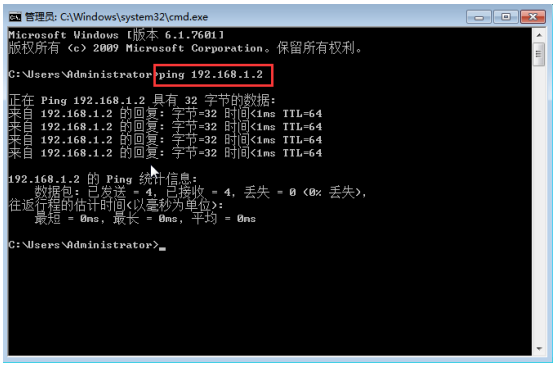


图 3-10

3.2.4 ping 访问后回到 192.168.1.2 查看记录输出的数据包，Ctrl+C 可结束程序。如下图 3-11 所示

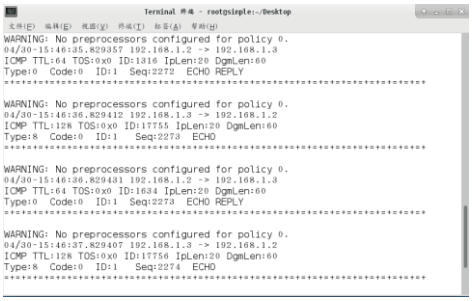


图 3-11

4.入侵检测规则编写

4.1full 报警模式下，ping 访问记录警告

4.1.1 打开 192.168.1.2 主机，init 5 进入桌面模式。打开终端，输入命令 snort –c /etc/snort/snort.conf –A full。如下图 4-1 所示

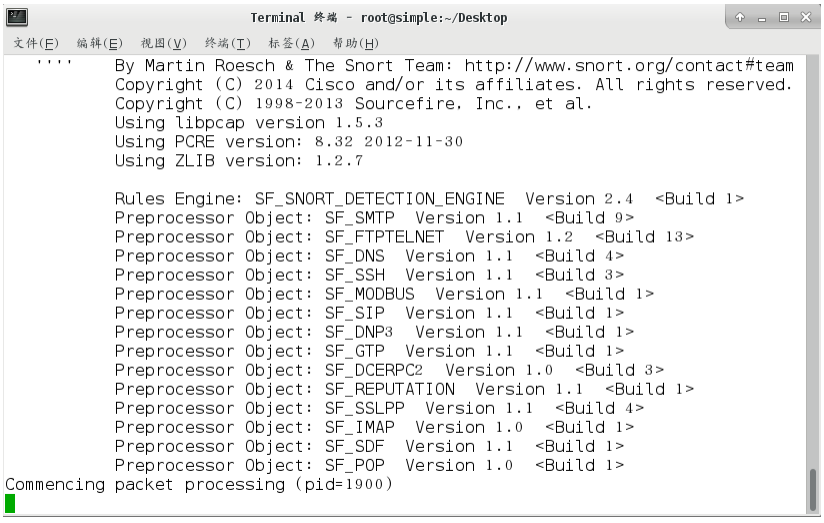


图 4-1

4.1.2 新打开一个终端执行命令 cd /var/log/snort 切换路径，ls 查看路径下文件。如下图 4-2 所示

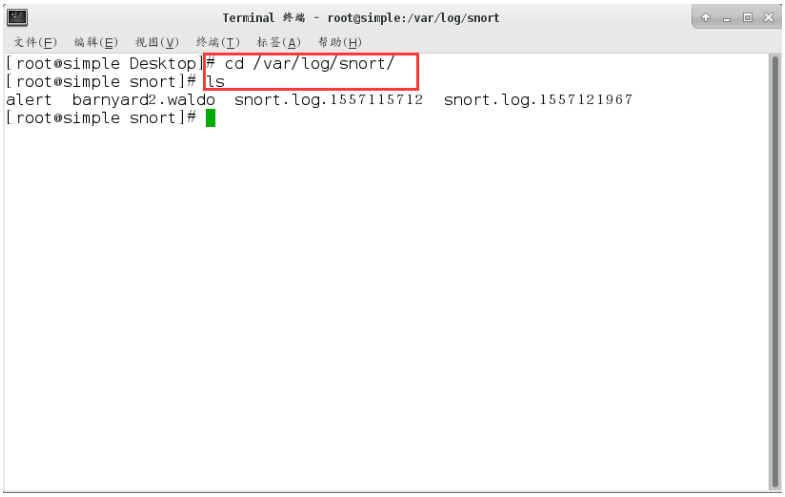


图 4-2

4.1.3 使用 cat 命令查看 alert 文件的内容，发现内容不为空(具体内容以实际环境为准)。alert 文件中的内容就是在 full 报警模式下，配置规则进行验证所产生的警告记录。如下图 4-3 所示

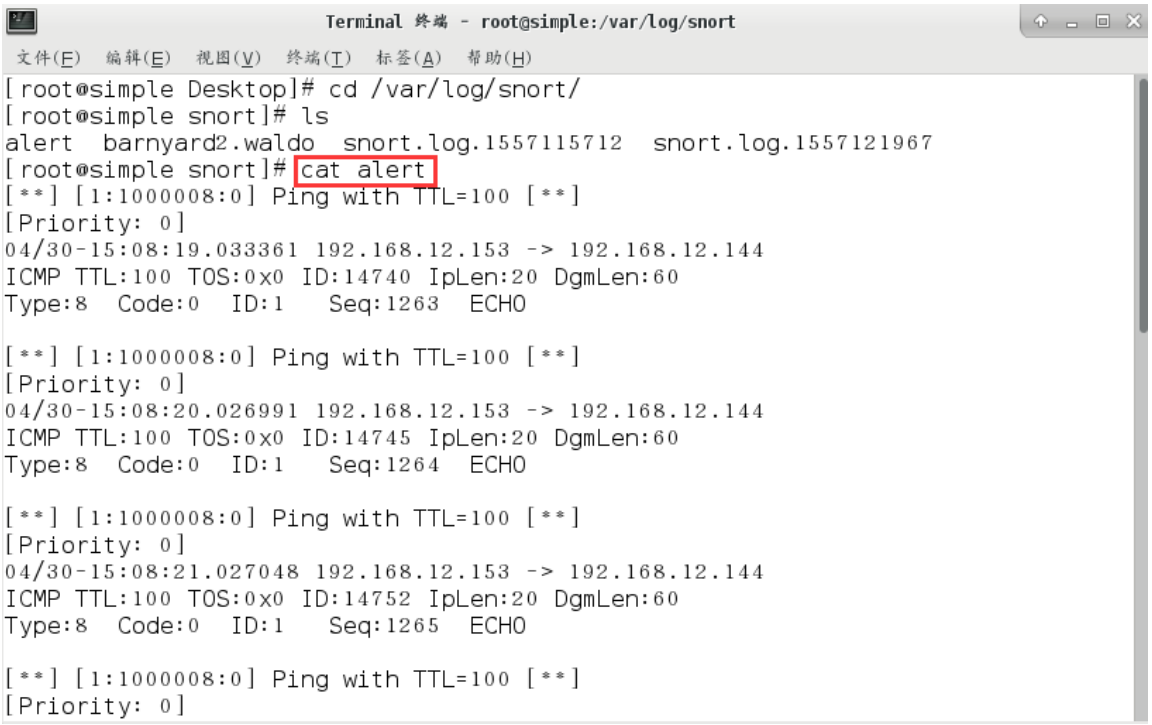


图 4-3

4.1.4 使用 vim 命令编辑”/etc/snort/rules/local.rules”规则配置文件。如下图 4-4 所

示

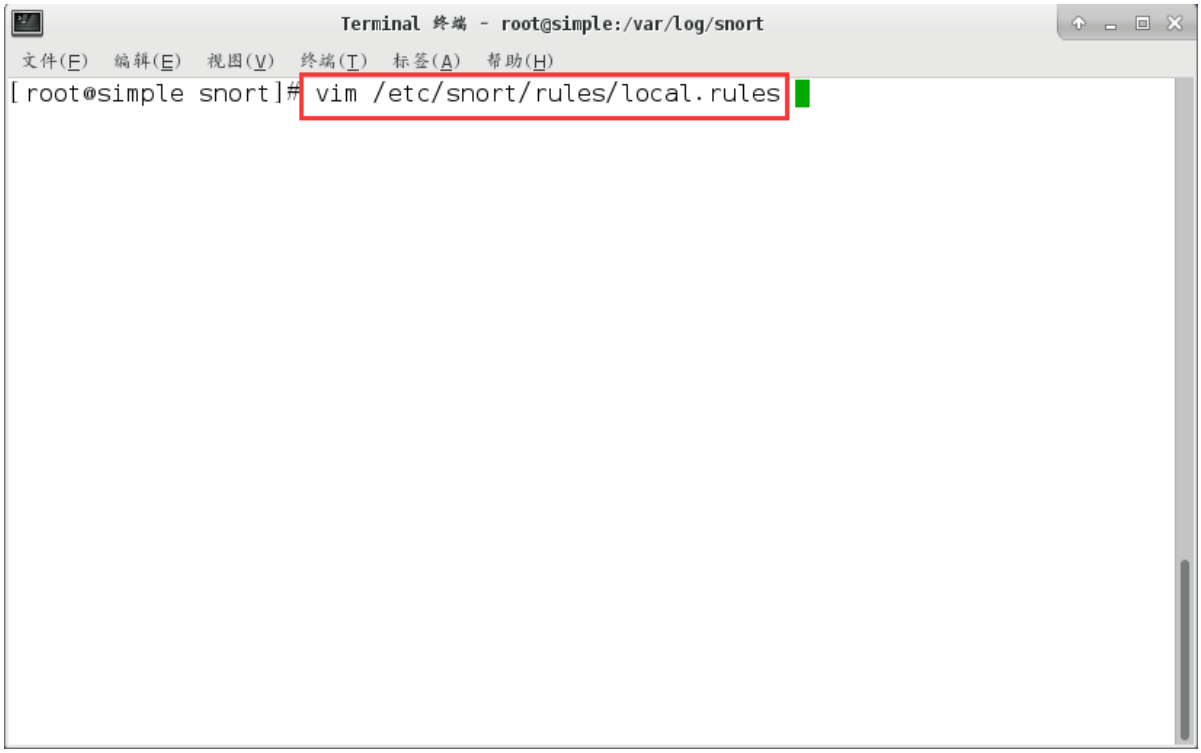


图 4-4

4.1.5 在 local.rules 文件的尾部增加 snort 规则。规则为 alert icmp any any -> any any (msg:"Ping with TTL=100";ttl:100; sid:1000008;)，将 ttl 值为 1000 的 ping 访问数据包以规则 id 为 1000008 记录警告信息。配置后保存退出。如下图 4-5 所示

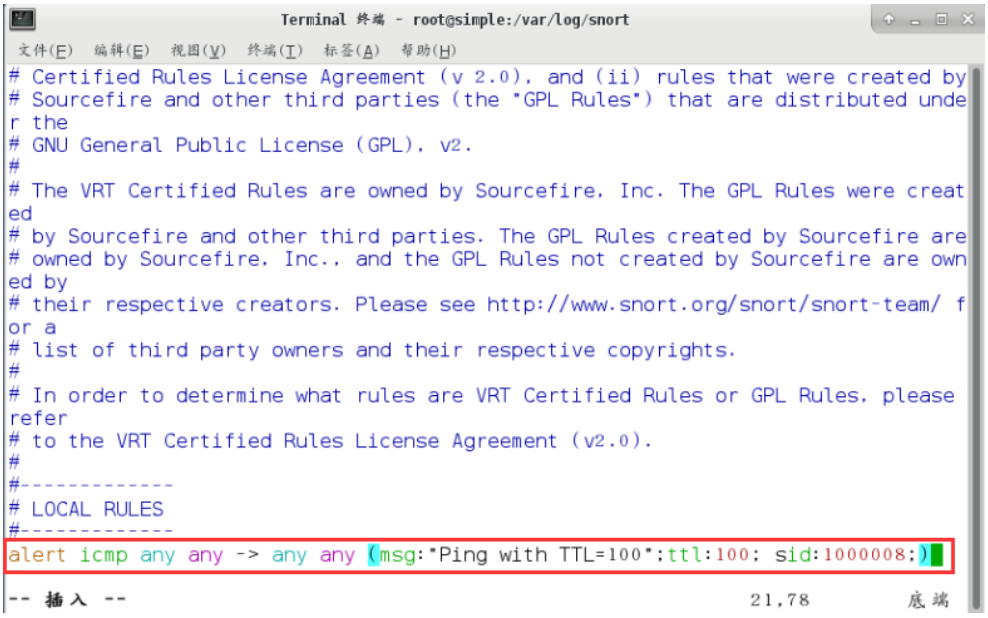


图 4-5

4.1.6 切换到地址为 192.168.1.3 的主机，打开 cmd 命令窗口。执行命令 ping –n

1000 –i 100 192.168.1.2。-n 可以指定 ECHO 数据包数，-i 可以指定生存时间字段值。这里-n 可以随意指定，-i 必须指定为 100，要与上面规则配置相同。如下图 4-6 所示

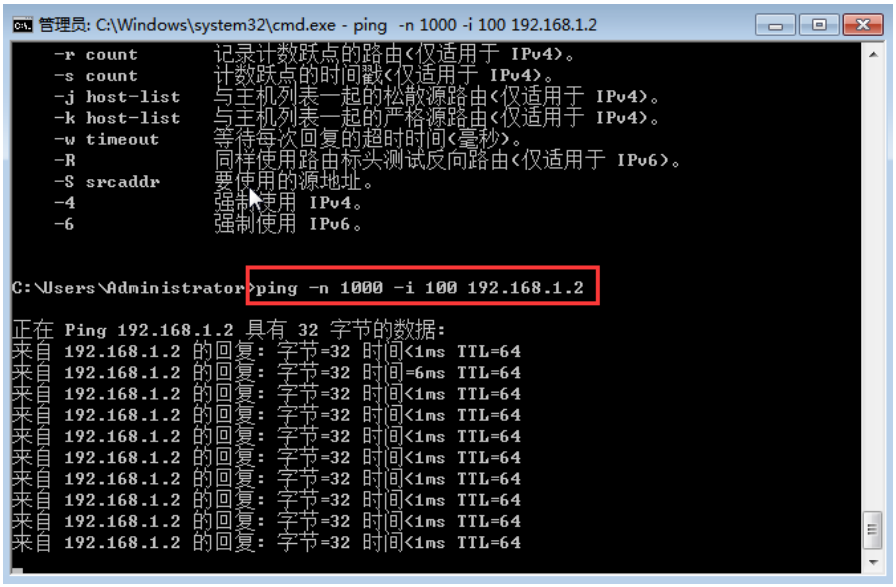


图 4-6

4.1.7 切换到地址为 192.168.1.2 的主机。使用 ctrl+c 组合键结束掉 snort 的进程。如下图 4-7 所示

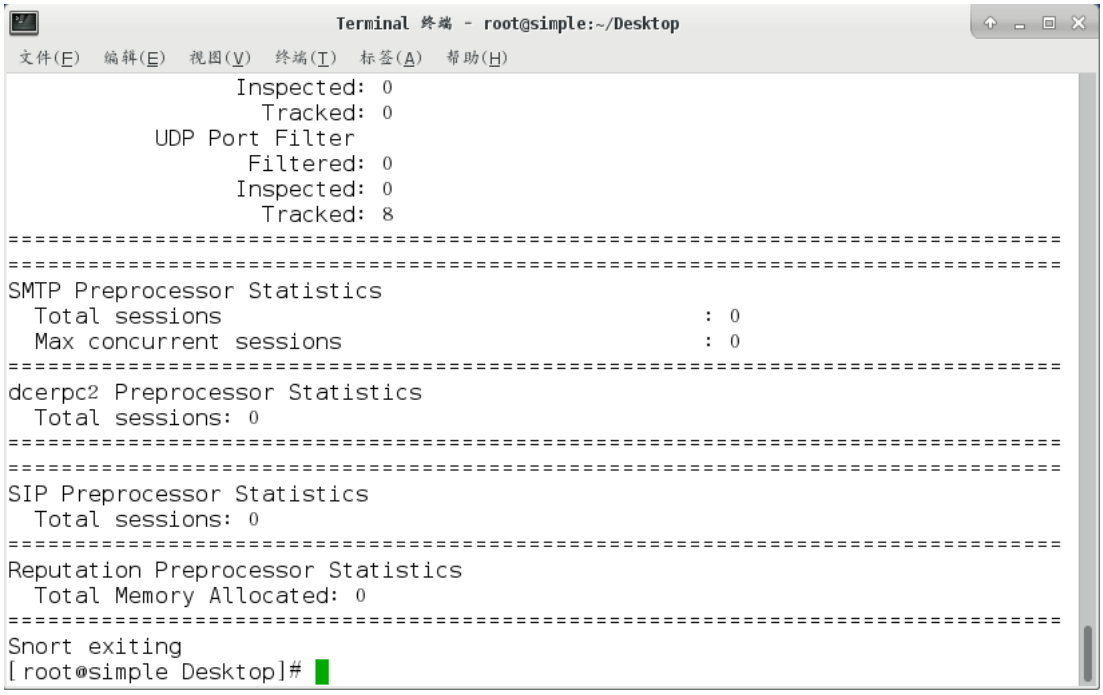


图 4-7

4.1.8 使用命令 cd /var/log/snort 切换至路径，使用命令 cat alert 查看 alert 文件内容。如下图 4-8 所示

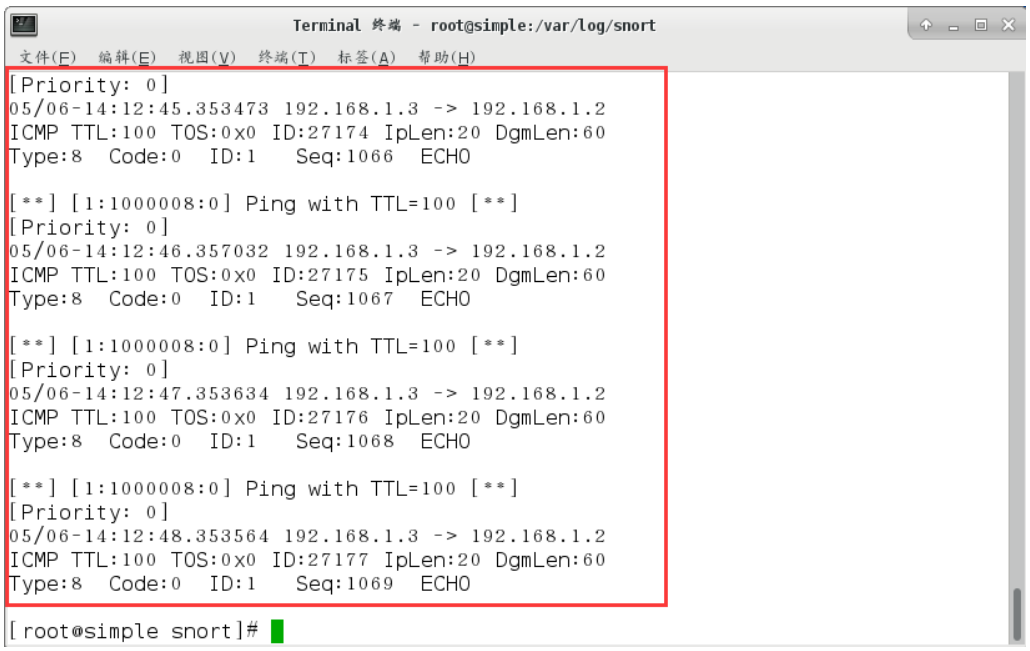


图 4-8

4.1.9 alert 中的数据包内容，包含了 sid（规则编号），报警信息等，就是上面规则中的设置信息。如下图 4-9 所示

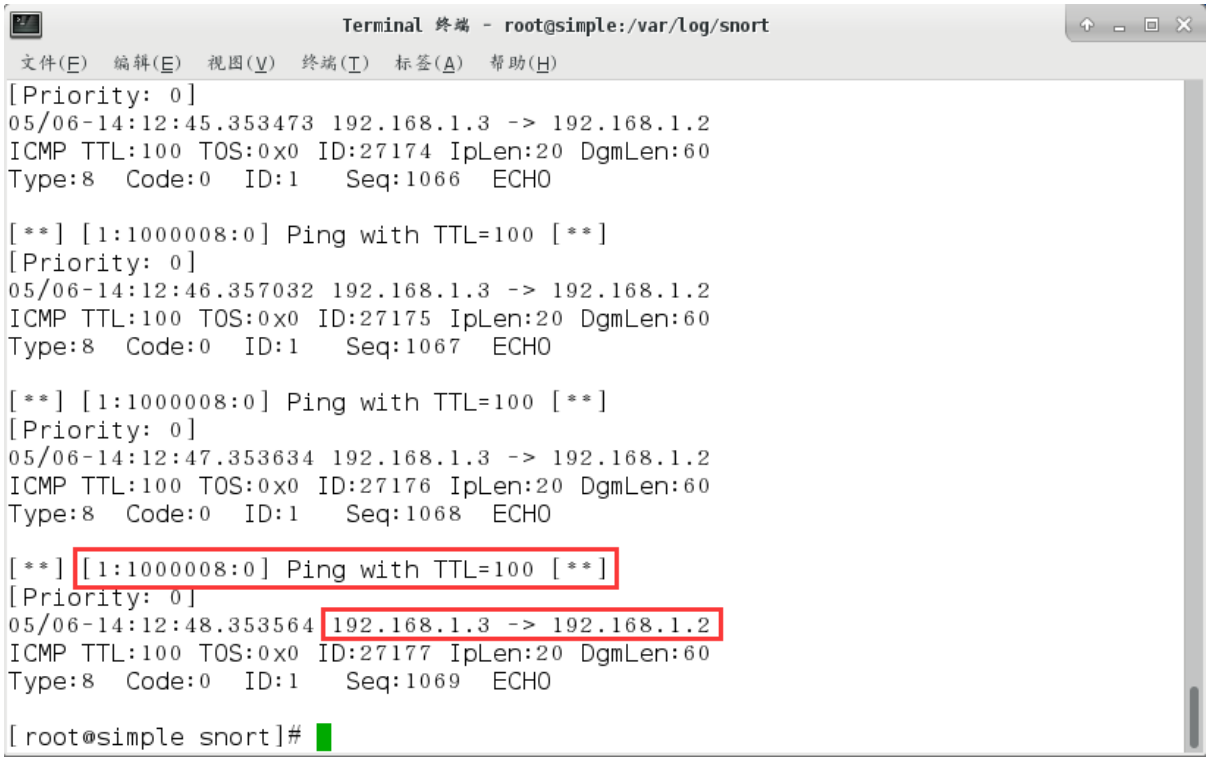


图 4-9

4.2. full 报警模式下，nmap 扫描端口记录警告

4.2.1 在进行 snort 检测之前，先查看 nmap 端口扫描获取的数据包的 tcp 标志位。

打开 centos 终端，输入命令 wireshark 打开抓包工具 wireshark，选择 eth0 网卡后点击 Start 开始抓包。如下图 4-10 所示

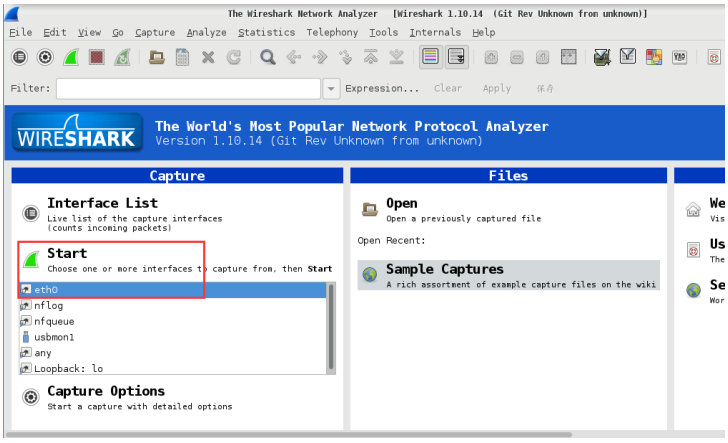


图 4-10

4.2.2 在 Windows 上打开软件 Nmap，在目标处输入 IP 地址 192.168.1.2，点击扫描，开始 nmap 扫描，扫描结束。如下图 4-11 所示

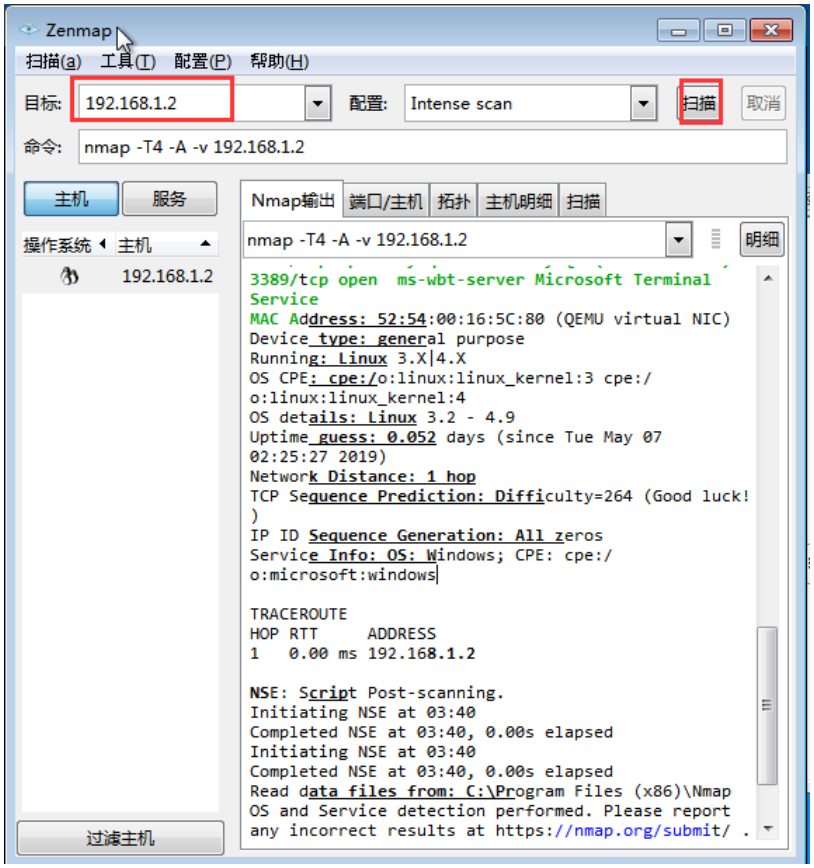


图 4-11

4.2.3 回到 centos 查看抓包信息。在 wireshark 的 filter 栏输入“tcp”后回车，再点击下面数据包列表的“destination”查看本机发往 Windows 的数据包。分析其特征，

一个明显的特征是包的 tcp 标志位几乎都是“RST”“ACK”（下面规则配置中就可以用 flags:RA 进行配置）。如下图 4-12 所示

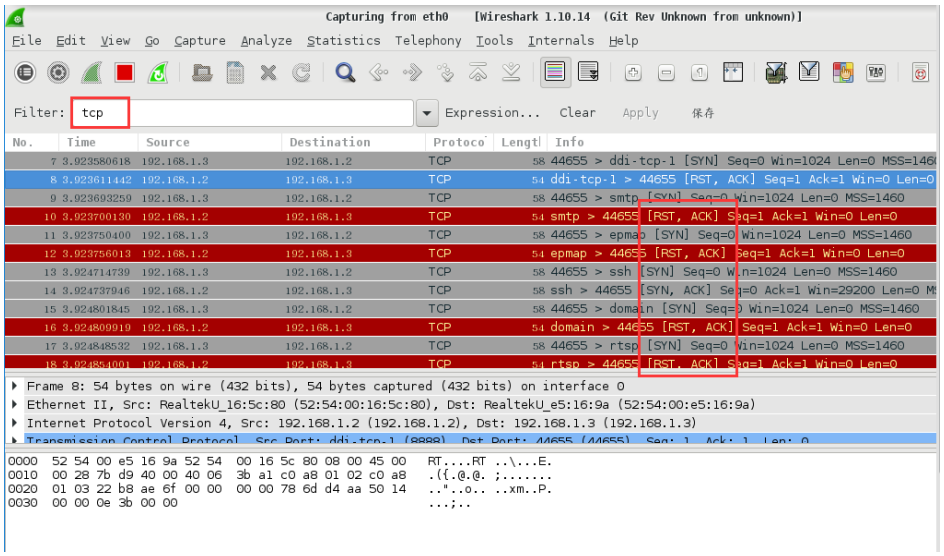


图 4-12

4.2.4 通过上面的分析配置规则。vi /etc/snort/rules/local.rules 编辑配置文件，将上面配置的规则删除。添加配置规则 alert tcp any any ->any any (msg:"Nmap Scan";flags:RA; sid:1000016;),设置 nmap 扫描端口记录警告，添加规则后:wq 保存退出。如下图 4-13 所示

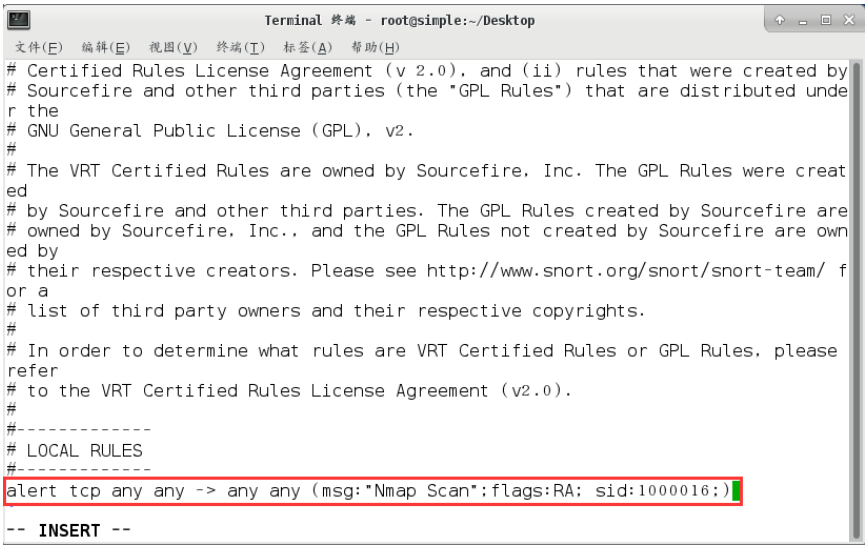


图 4-13

4.2.5 执行命令 snort –c /etc/snort/snort.conf –A full，开启 snort。如下图 4-14 所示

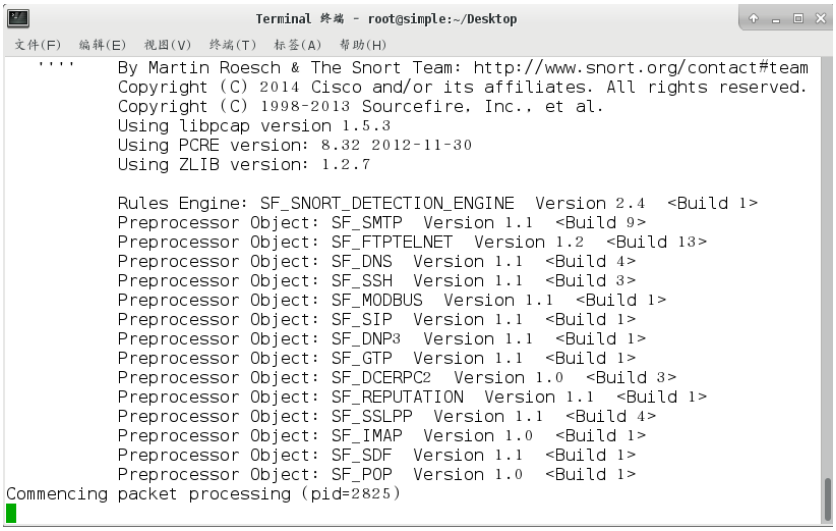


图 4-14

4.2.6 切换至 Windows 打开 zenmap，对 centos 虚拟机进行 nmap 端口扫描，输入命令 nmap -T4 -A -v 192.168.1.2 完成扫描。如下图 4-15 所示

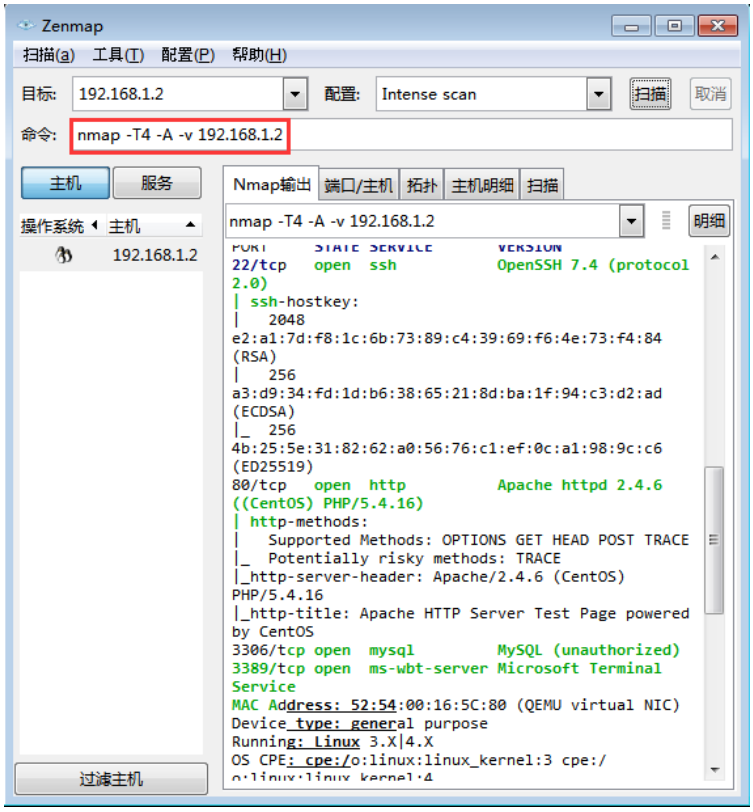


图 4-15

4.2.7 完成扫描后回到 centos，Ctrl+C 结束 snort 进程，显示数据包统计信息。如下图 4-16 所示

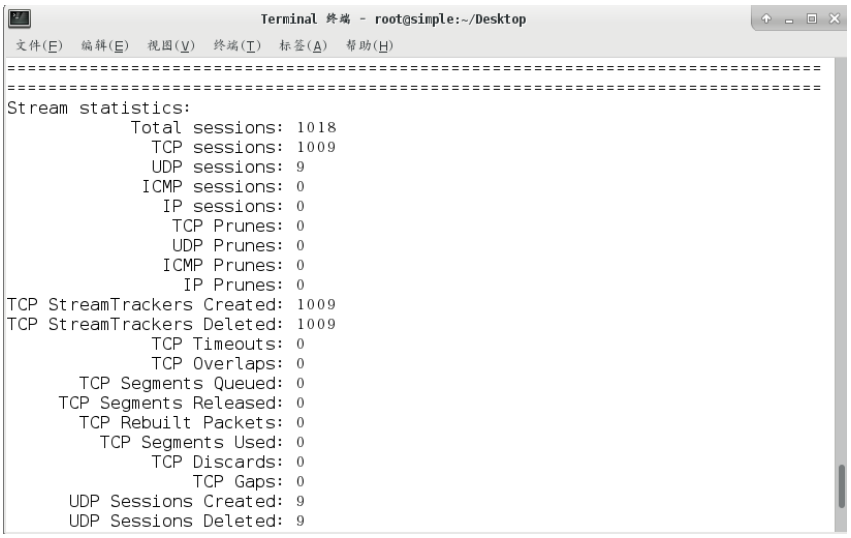


图 4-16

4.2.8 执行命令 cd /var/log/snort 切换路径，执行命令 cat alert，查看 alert 文件记录的警告信息内容，可以看到编号及名称都与上面的规则配置相符合。如下图 4-17 所示

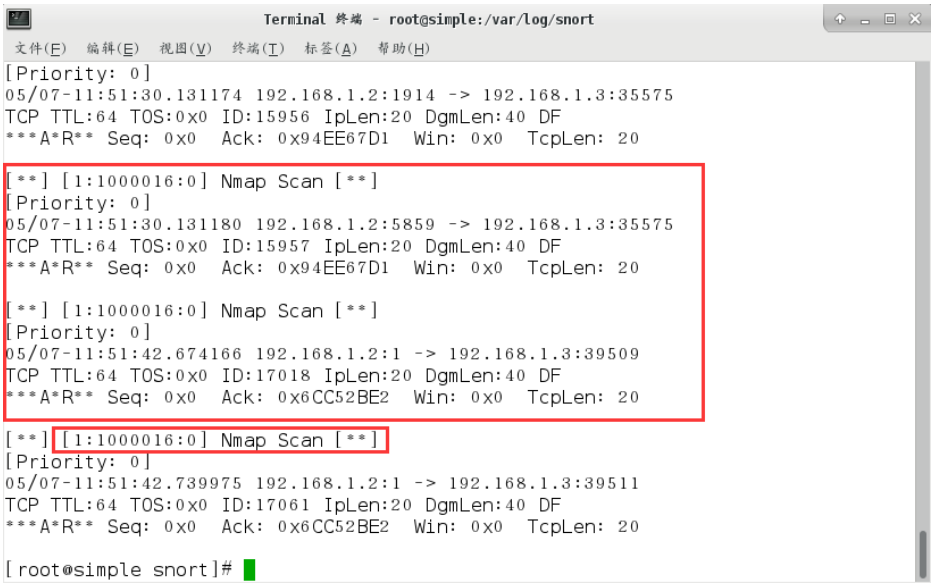


图 4-17

实验六 病毒与恶意代码实验

脚本病毒修改 IE 默认主页、禁止设置任务栏和开始、病毒木马清除工具 Wsyscheck

一、实验目的

1、掌握脚本病毒的原理，了解脚本病毒的攻击过程，了解典型的脚本病毒的破坏结果，掌握典型脚本病毒的清除方法。

2、熟悉 Wsyscheck 工具各项功能的使用。

二、实验环境

Windows 2003，计算机病毒实验工具 ProcessMonitor

Wsyscheck

三、实验内容

1、脚本病毒修改 IE 默认主页

2、禁止设置任务栏和开始

3、病毒木马清除工具 Wsyscheck

四、实验步骤

1. 脚本病毒修改 IE 默认主页

1.1 脚本病毒代码分析和查看

1.1.1 打开桌面上 tools\Virus 文件夹下的 MainUI.exe，在界面左侧的实验列表中选择脚本病毒实验，单击“初始化病毒工具”。如图 1-1 所示

图 1-1

1.1.2 提示初始化完毕。如图 1-2 所示

图 1-2

1.1.3 在界面实验实施下的功能选择区选择修改 IE 默认页，在界面右侧将会看到该脚本病毒的全部代码。通过相关的注释我们可以了解病毒的运行机制。如图 1-3 所示

图 1-3

1.1.4 若想对脚本病毒代码进行编辑，可以在界面右侧的编辑区对代码直接进行编辑，单击“保存脚本”即可对编辑后的脚本进行保存，点击“重置脚本”将恢复最初的脚本代码。

1.2 禁止“运行”菜单

1.2.1 打开桌面上 tools\ProcessMonitor 文件夹下的 Procmon.exe，这里我们只对注册表进行监控（若弹出提示，单击 Agree 即可）。如图 1-4 所示

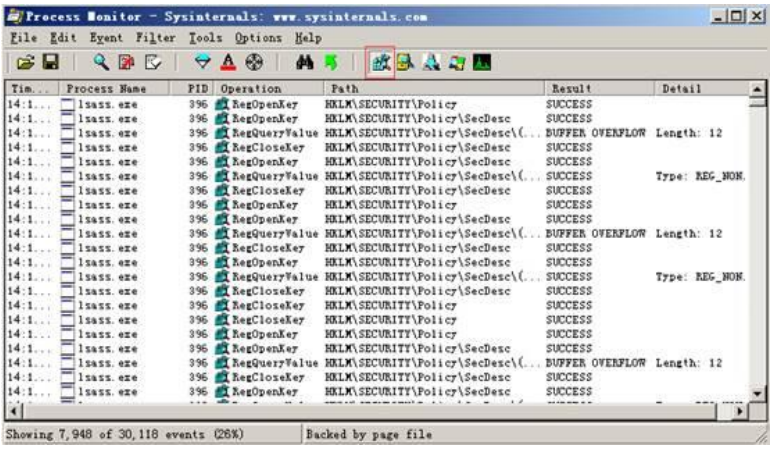


图 1-4

1.2.2 未进行脚本前，打开 IE 浏览器，单击工具，选择 Internet 选项，可以看到在常规选项卡下主页的地址，并且可以进行设置。如图 1-5 所示

图 1-5

1.2.3 单击执行脚本，开始进行实验，运行脚本病毒代码。如图 1-6 所示

图 1-6

1.2.4 在 ProcessMonitor 中，可以监控到运行该病毒脚本时对注册表进行的操作。如图 1-7 所示

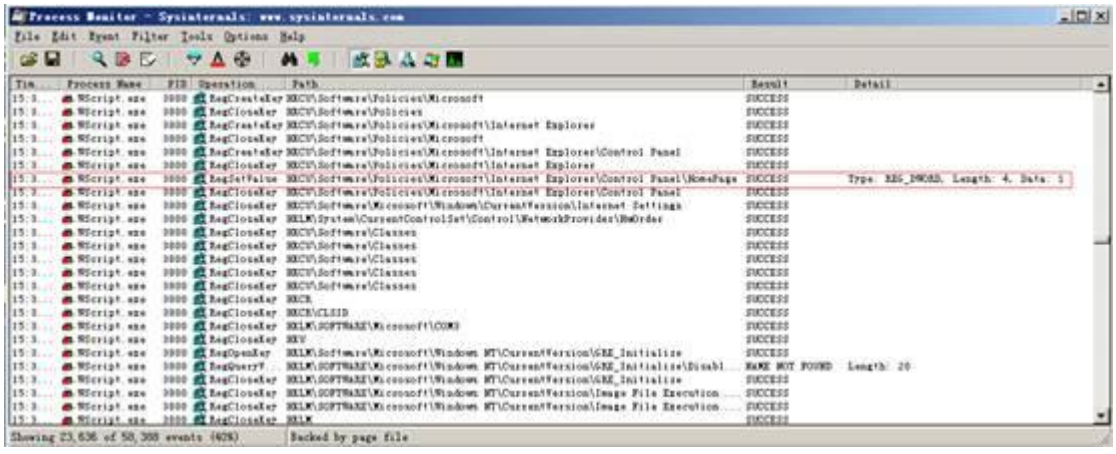


图 1-7

1.2.5 按 Win+R 组合键或者单击开始，单击打开运行，输入 regedit，回车，打开注册表，在

HKCU\Software\Policies\Microsoft\InternetExplorer\ControlPanel 下，可以看到新建了

HomePage，且其键值为 1。如图 1-8 所示

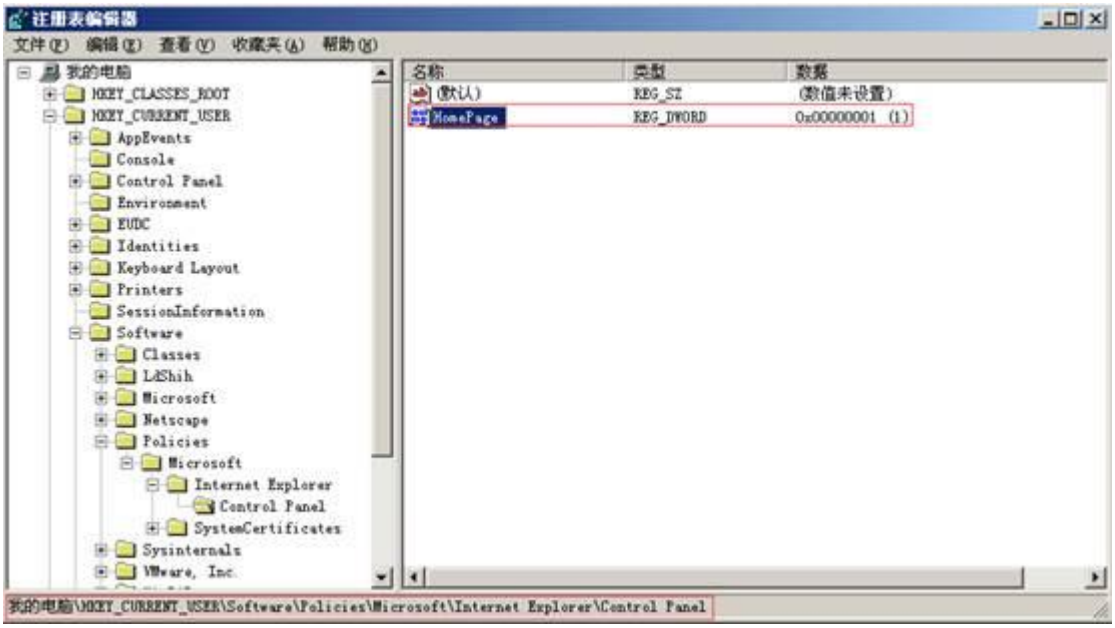


图 1-8

1.2.6 重新打开 Internet 选项，可以看到此时不能再对主页进行修改。如图 1-9 所示

图 1-9

1.2.7 单击恢复设置，开始恢复实验，运行恢复代码。如图 1-10 所示

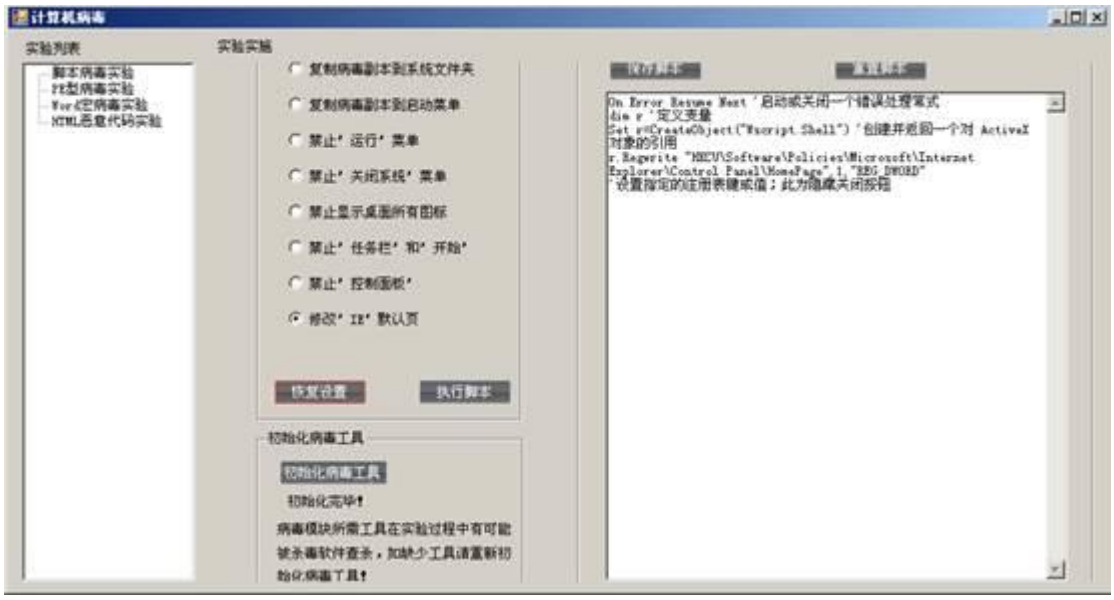


图 1-10

1.2.8 此时注册表的相应键值由 1 改为 0。如图 1-11 所示

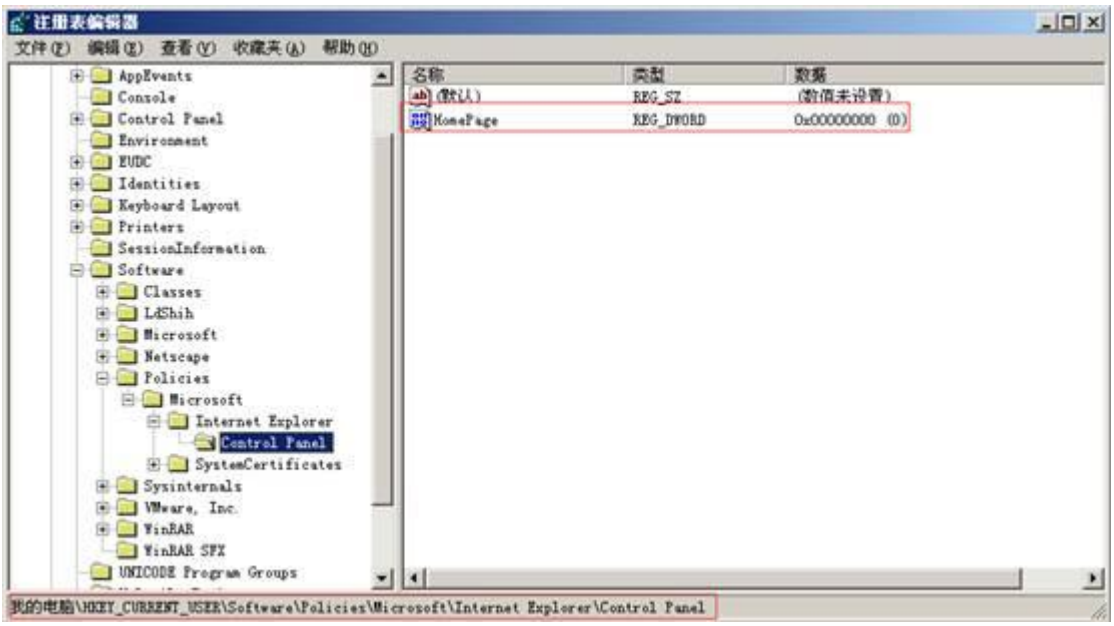


图 1-11

1.2.9 查看 Internet 选项，此时可以继续编辑主页了。如图 1-12 所示

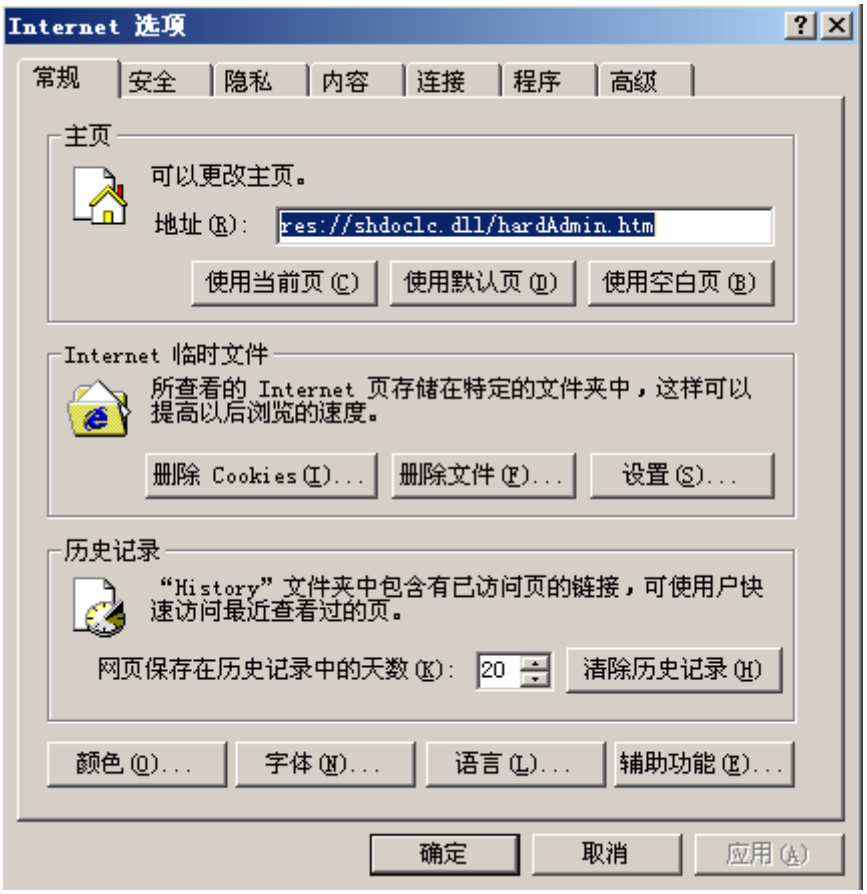


图 1-12

2.禁止设置任务栏和开始

2.1 脚本病毒代码分析和查看

2.1.1 打开桌面上 tools\Virus 文件夹下的 MainUI.exe，在界面左侧的实验列表中选择脚本病毒实验，单击“初始化病毒工具”。如图 2-1 所示

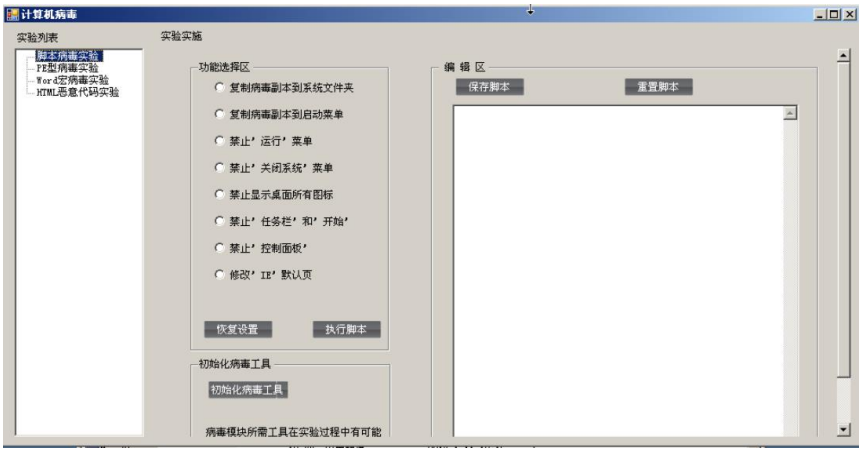


图 2-1

2.1.2 提示初始化完毕。如图 2-2 所示

图 2-2

2.1.3 在界面实验实施下的功能选择区选择禁止‘任务栏’和‘开始’，在界面右侧将会看到该脚本病毒的全部代码。通过相关的注释我们可以了解病毒的运行机制。如图 2-3 所示

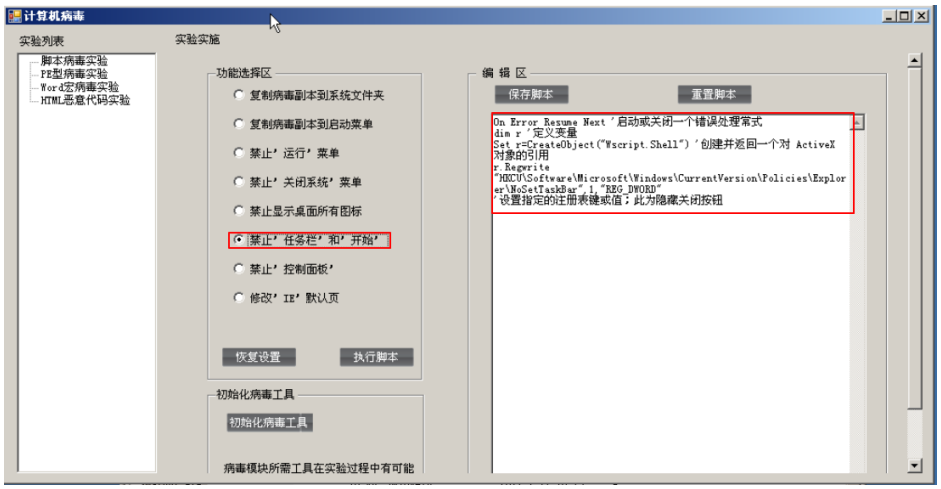


图 2-3

1.1.4 若想对脚本病毒代码进行编辑，可以在界面右侧的编辑区对代码直接进行编辑，单击“保存脚本”即可对编辑后的脚本进行保存，点击“重置脚本”将恢复最初的脚本代码。

2.2.禁止设置任务栏和开始菜单

2.2.1 打开桌面上 tools\ProcessMonitor 文件夹下的 Procmon.exe，这里我们只对注册表进行监控（若弹出提示，单击 Agree 即可）。如图 2-4 所示

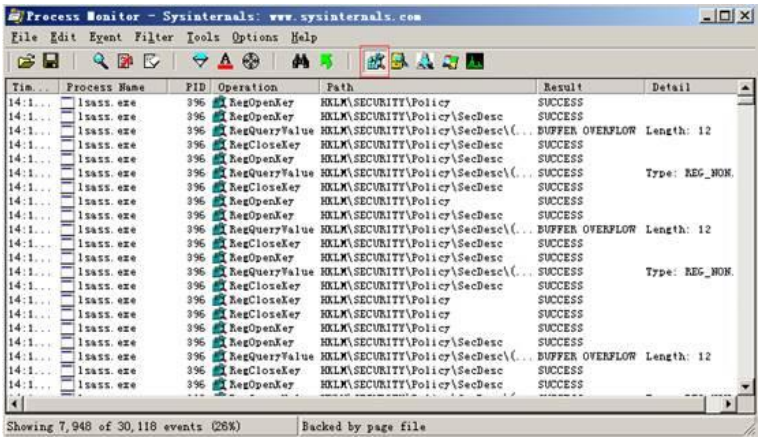


图 2-4

2.2.2 单击执行脚本，开始进行实验，运行脚本病毒代码。如图 2-5 所示

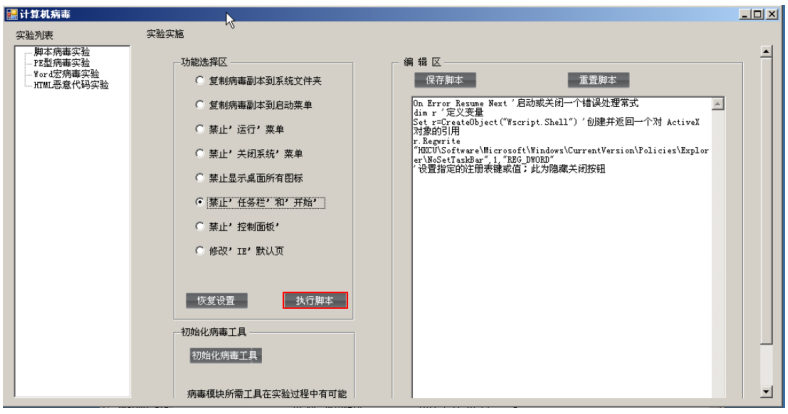


图 2-5

2.2.3 在 ProcessMonitor 中，可以监控到运行该病毒脚本时对注册表进行的操作。如图 2-6 所示

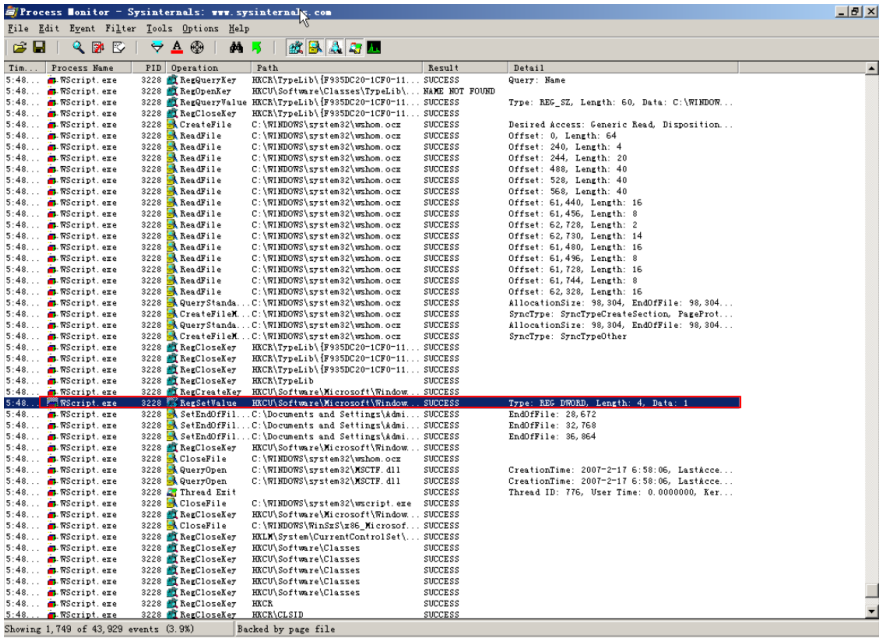


图 2-6

2.2.4 按 Win+R 组合键或者单击开始，单击打开运行，输入 regedit，回车，打开注册表，在 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 下，可以看到新建了 NoSetTaskBar，且其键值为 1。如图 2-7 所示

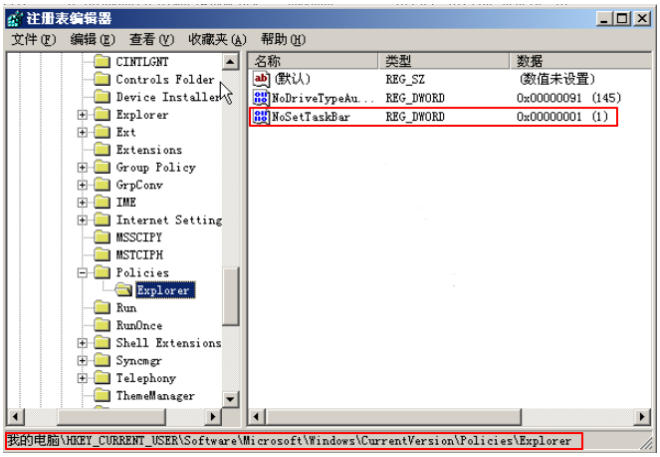


图 2-7

2.2.5 在任务栏单击右键选择属性，提示限制，即禁止了设置任务栏和开始菜单。如图 2-8、图 2-9 所示

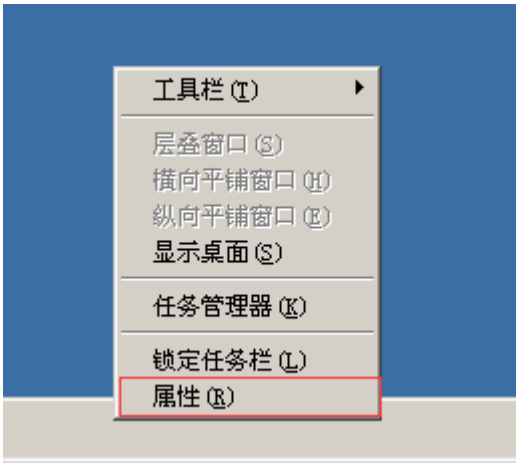


图 2-8

图 2-9

2.2.6 单击恢复设置，开始恢复实验，运行恢复代码。如图 2-10 所示

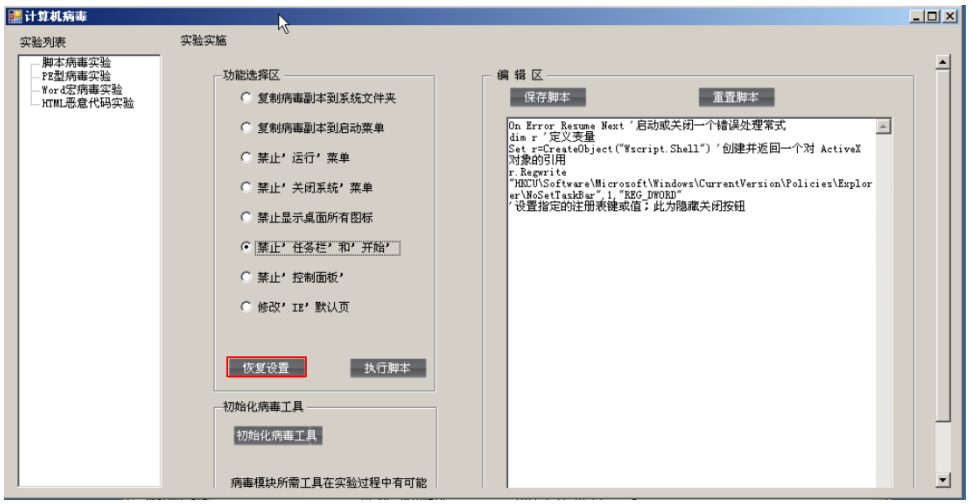


图 2-10

2.2.7 同时相应的注册表项的键值也由 1 改为 0。如图 2-11 所示

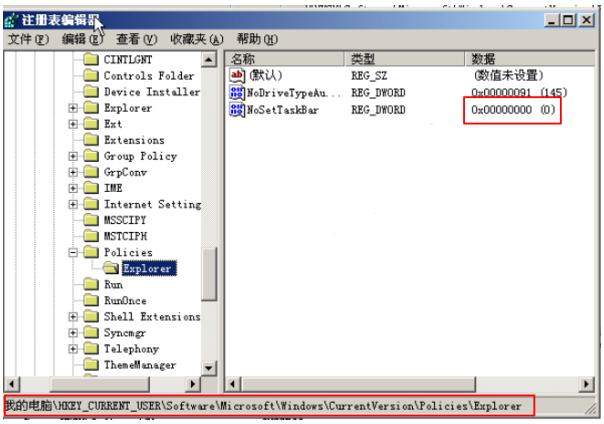


图 2-11

2.2.8 注销或者重启电脑（密码 Simplexue123），发现能重新使用任务栏的属性功能。如图 2-12 所示

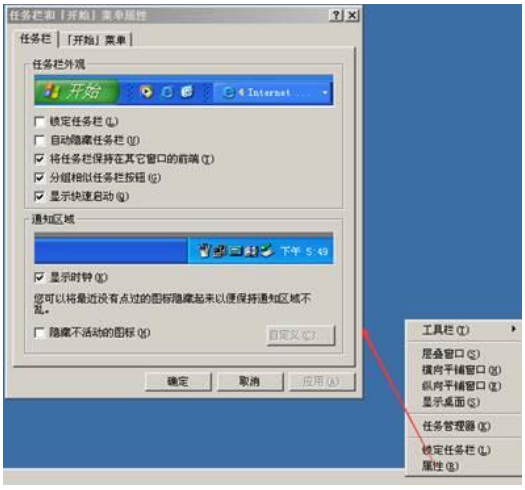


图 2-12

3.病毒木马清除工具 Wsyscheck

3.1Wsyscheck 的使用

3.1.1 打开桌面上 tools\Wsyscheck 文件夹下的 Wsyscheck.exe，其运行界面如下。如图 3-1 所示

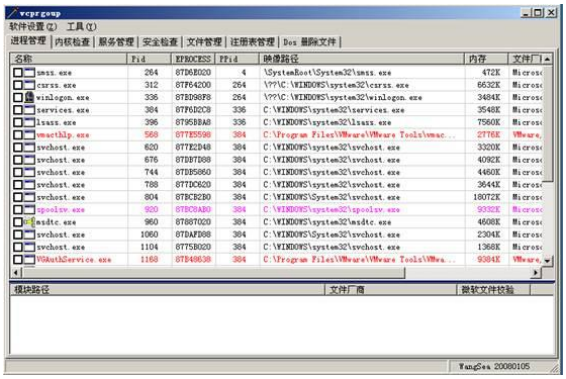


图 3-1

3.1.2 单击软件设置菜单，可以进行软件的相关设置。例如单击“校验微软文件签名”后变为灰色，同时运行界面中多了一列“微软文件校验”。如图 3-2、图 3-3 所示

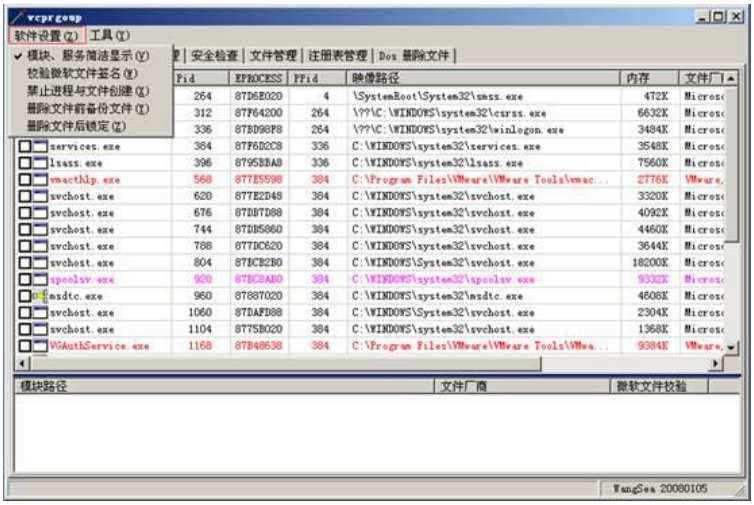


图 3-2

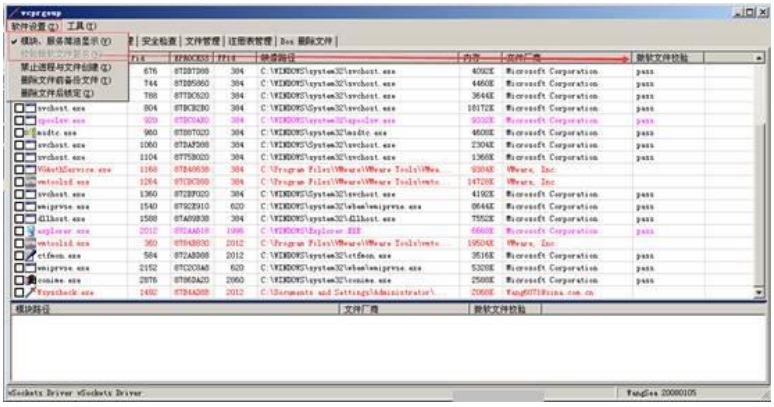


图 3-3

3.1.3 如果确定木马文件,可选择结束进程并删除文件,这样的话 Wsyscheck 会将其

结束并删除文件。但有时因为木马有关联进程未同时结束，会重新加载木马文件。这时我们可以选择“软件设置”下的“删除文件后锁定”。这时当结束进程并删除文件后 Wsyscheck 将创建 0 字节的锁定文件防止木马再生。

3.1.4 单击工具菜单，可以使用相关的工具执行相应的功能。如图 3-4 所示

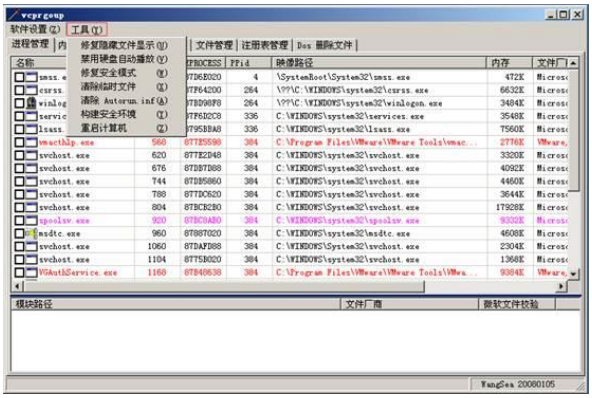


图 3-4

3.1.5 其中，在工具菜单下，

1) 清除临时文件：删除 %TEMP%,%windir%\Temp 及%windir%\DownloadedProgramFiles 下的所有文件。

2)禁用硬盘自动播放：本功能还包括磁盘无法双击打开故障。注意，某些故障修复后可能需要注销或重启才能生效。

3)修复安全模式：某些木马会破坏安全模式的键值导致无法进入安全模式，本功能先备份当前安全模式键值再恢复默认的安全模式键值。

3.1.6 在进程选项卡下，显示了系统的所有进程，并用不同的颜色进行标识。其中，红色表示非微软进程，紫红色表示虽然进程是微软进程，但其模块中有非微软的文件。其右键菜单如下。如图 3-5 所示

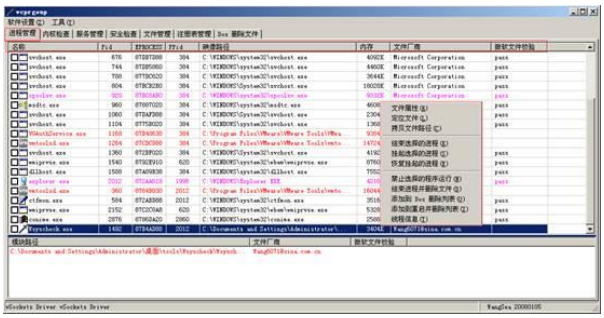


图 3-5

3.1.7 其中，“禁止程序运行”这个功能就是流行的 IFEO 劫持功能，我们可以使用它来屏蔽一些结束后又自动重新启动的程序。通过禁用它的执行来清理文件。解除禁用的程序用“安全检查”页的“禁用程序管理”功能，所以在木马使用 IFEO 劫持后也可以“禁用程序管理”中恢复被劫持的程序。

3.1.8 进程管理界面下方列出了选中进程的模块。其右键菜单如下。如图 3-6 所示

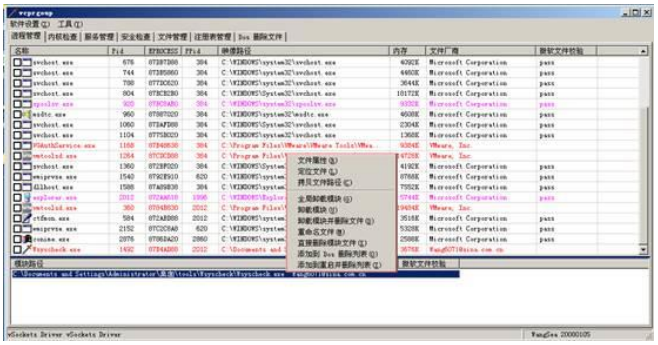


图 3-6

3.1.9 在内核检查模块选项卡下，包含 4 个子功能，其中 SSDT 检查子功能界面如下，其列表包含六列，发现木马修改了 SSDT 表时先恢复 SSDT，再做注册表删除等操作。其右键菜单如下。其它子功能可自行查看。如图 3-7 所示

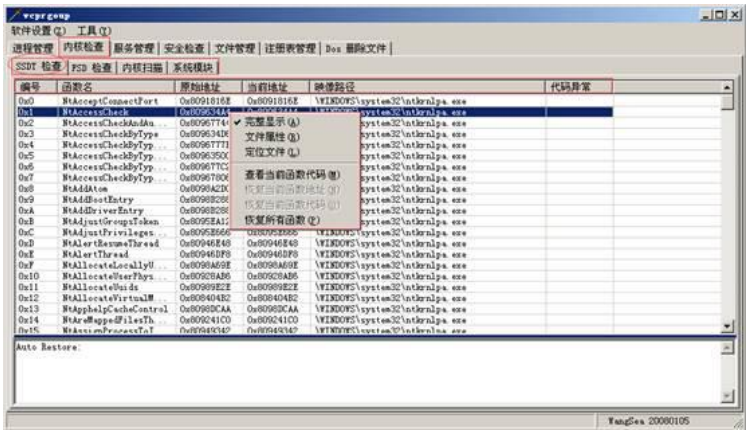


图 3-7

3.1.10 在服务管理选项卡下，显示了系统的所有服务，其列表包含八列，其中，红色表示该服务不是微软服务,且该服务非.sys 驱动（最常见的是.exe 与.dll 的服务，木马大多使用这种方式）。其右键菜单如下。如图 3-8 所示

图 3-8

1.1.11 在服务管理选项卡下，使用“检查键值保护”后，蓝色显示的是有键值保护的随系统启动的驱动程序。它们有可能是杀软的自我保护，也有可能是木马的键值保护。在取消了软件设置中的“模块、服务简洁显示”后，查看第三方服务可以点击标题条“文件厂商”排序，结合使用“启动类型”、“修改日期”排序更容易观察到新增的木马服务。

3.1.12 在安全检查选项卡下，有六个子功能。常规检查子功能主要检查 Host、WinSock、禁用程序和重要键值变动 4 个方面。如图 3-9 所示

图 3-9

3.1.13 活动文件子功能列表包含五列，红色显示的是常规启动项的内容。其右键菜单如下。如图 3-10 所示

图 3-10

3.1.14 IE 安全子功能列表包含五列，可对 ActiveX 控件进行注册和反注册，其右键菜单如下。如图 3-11 所示

图 3-11

3.1.15 端口状态子功能罗列了系统所有打开的端口。如图 3-12 所示

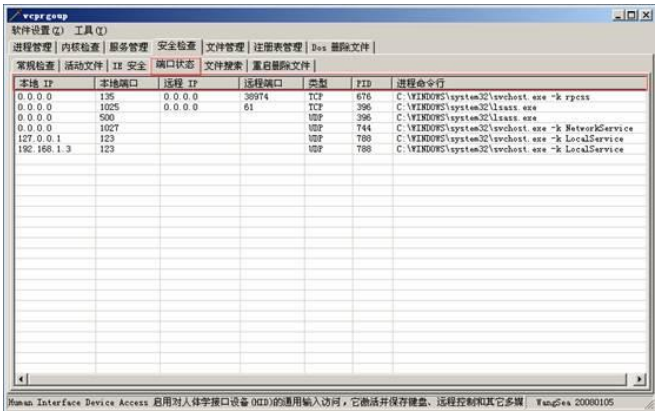


图 3-12

3.1.16 文件搜索字功能可对文件进行搜索。选中搜索结果后单击右键选择“保存列表”导出搜索结果列表 1，在 PE 启动后再执行一次得到结果 2，将结果 1 与结果 2 相比较，可以用来对付某些 Wsyscheck 检测不出深度隐藏的 RootKit。如图 3-13 所示

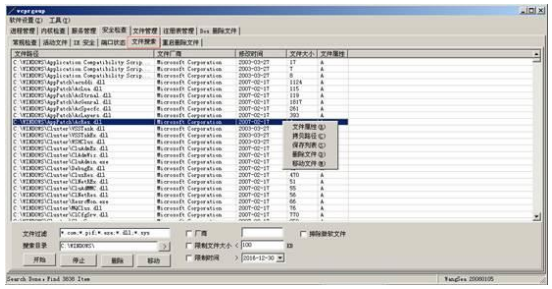


图 3-13

3.1.17 重启删除文件子功能如下。如图 3-14 所示

图 3-14

3.1.18 在文件管理选项卡下，可对磁盘上的文件夹和文件进行相关操作。如图 3-15 所示

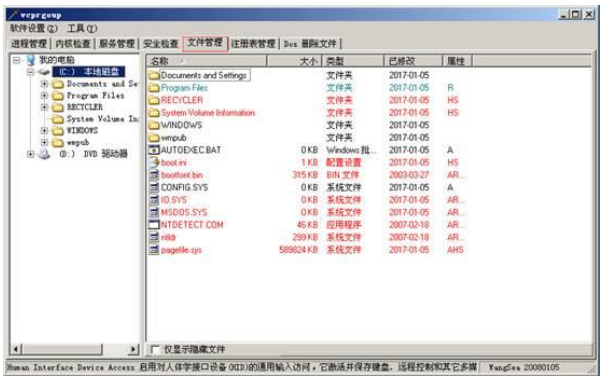


图 3-15

3.1.19 左边列表主要是对文件夹的操作，其右键菜单如下。如图 3-16 所示

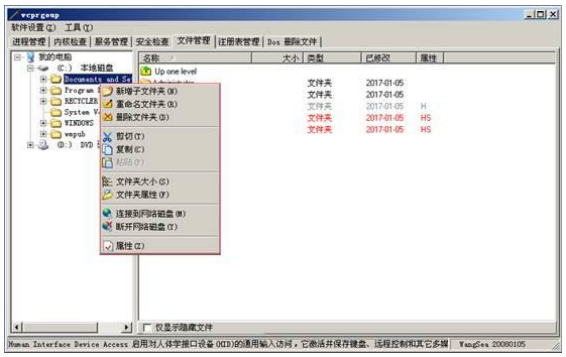


图 3-16

3.1.20 右边列表主要是对文件的操作，其中“删除”操作是删除文件到回收站，支持畸形目录下的文件删除。应注意的是如果文件本身在回收站内，请使用直接删除功能。或者使用剪切功能将它复制到另一个地方。否则你可能看到回收站内的文件删除了这个又添加了那个。其右键菜单如下。如图 3-17 所示

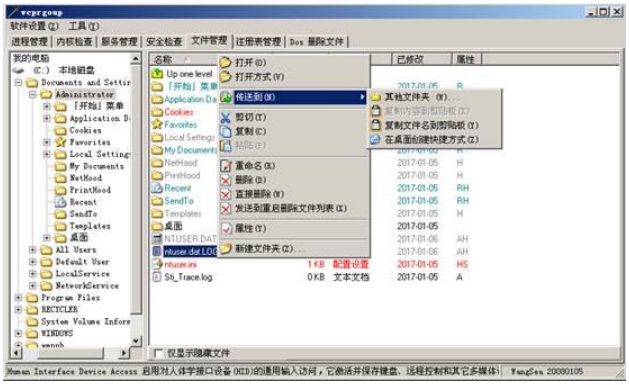


图 3-17

3.1.21 在注册表选项卡下。左边列表主要是对注册表项的操作，其右键菜单如下。如图 3-18 所示

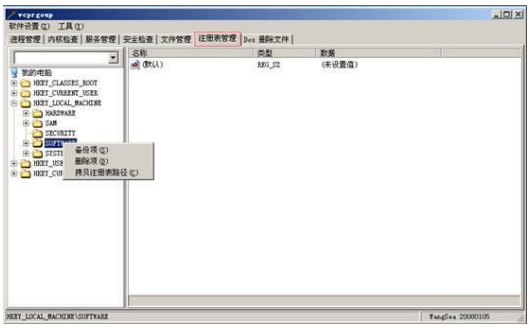


图 3-18

3.1.22 右边列表主要是对注册表键值的操作，其右键菜单如下。如图 3-19 所示

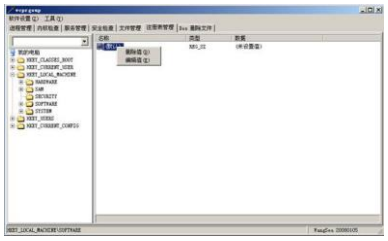


图 3-19

3.1.23 此外，还可以只用下面的方法快速定位到某些指定的常用注册表路径。如图 3-20 所示

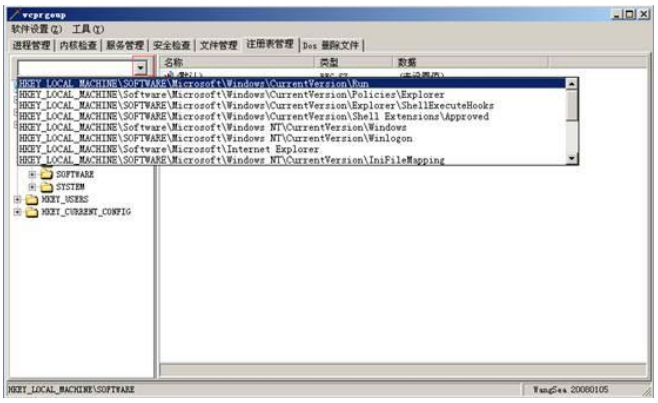


图 3-20

3.1.24 在 Dos 删除文件选项卡下，可以单击添加待删除文件按钮来添加想要删除的文件，再选中文件后单击执行 Dos 删除按钮来对选中的文件进行 Dos 删除。如图 3-21 所示

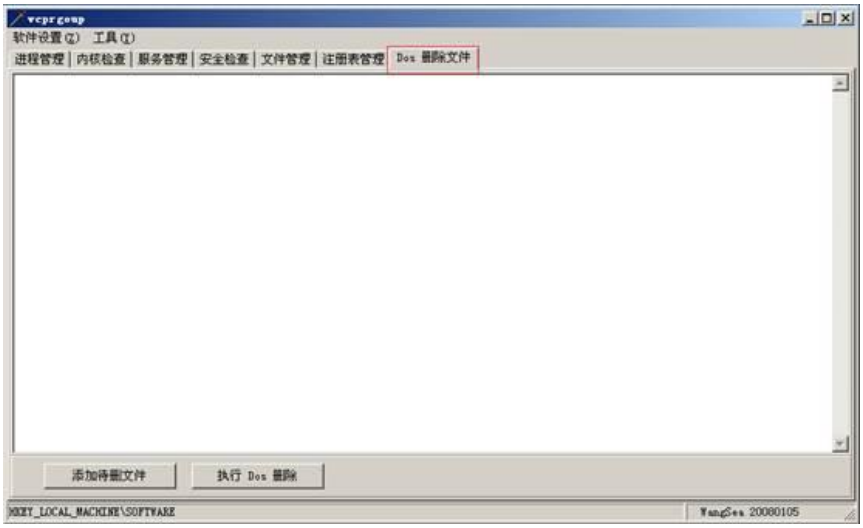


图 3-21

3.1.25 通常使用 Wsyscheck 清理木马的简单方法如下：

1)勾选“软件设置”下的“删除文件后锁定”以阻止文件再生。

2)批量选择病毒进程，使用“结束进程并删除文件”。

3)插入到进程中的模块多不可怕，全局钩子在各进程中通常都是相同的，处理进程的模块即可。建议采用“直接删除模块文件”，本功能执行后看不到变化，但文件其实已经删除。不建议使用“卸载模块”功能（为保险也可以与“重启删除”联用），原因是卸载系统进程中的模块时有可能造成系统重启而前功尽弃。

4)执行工具中的“清理临时文件”、“清除 Autorun.inf”。

5)安全检查中可以修复的修复一下。不强求，重启后再执行二次清理。

6)重启机器，大部份的病毒应该可以搞定了。此时再次检查，发现还有少量的顽固病毒才使用“禁用”“线程”“卸载”“重启删除”“Dos 删除”等方法。

7)清理完后切换到文件搜索页，限制文件大小为 50K 左右，去除“排除微软文件的勾”搜索最近一周的新增的文件，从中选出病毒尸体文件删除。

实验七 远程控制与 VPN 实验

Windows 下 IPC 管道的建立和远程控制、Windows 下 SSL_VPN 实验

一、实验目的

1、Windows 下 IPC 管道的建立和远程控制

(1) 了解 IPC$漏洞原理

(2) 掌握 IPC$漏洞攻击方法

(3) 掌握 PsExec 工具的使用

(4) 掌握远程控制工具上兴软件的使用

2、Windows 下 SSL_VPN 实验

掌握 SSLvpn 搭建。

二、实验环境

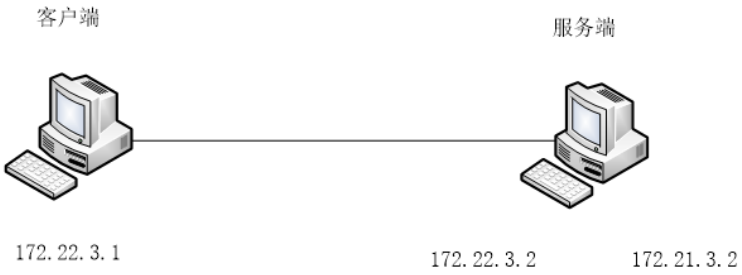
1、Windows 下 IPC 管道的建立和远程控制

实验拓扑图

工具目录:C:\实验工具集\06_网络与无线安全\01_典型协议攻击

靶机帐号:administrator 密码：Simplexue123

2、Windows 下 SSL_VPN 实验



三、实验内容

1、Windows 下 IPC 管道的建立和远程控制

(1) 打开被攻击机即目标主机的 IPC$默认共享

(2) 利用 net 命令与远程主机建立 IPC$连接

(3) 利用工具 PSEXEC 实施攻击

2、Windows 下 SSL_VPN 实验

(1) 配置 SSLVPN 服务端。

(2) 配置客户端进行连接。

四、实验步骤

1、Windows 下 IPC 管道的建立和远程控制

1.1 打开被攻击机即目标主机的 IPC$默认共享

1.1.1 启动实验台，以实验台为被攻击机即目标主机。打开命令行模式，进行利用 IPC$漏洞攻击，首先要保证被攻击机 IPC$默认共享已经打开。在实验台中可用 net share 命令开启 IPC$共享，同时查看 IPC$共享。如图 1 所示

```
C:\Users\Administrator>net share C$=C:
C$ 共享成功。


C:\Users\Administrator>net share

共享名       资源                            注解

-------------------------------------------------------------------------------
IPC$                                         远程 IPC
C$           C:\                             默认共享
命令成功完成。
```

图 1-1

1.2.利用 net 命令与远程主机建立 IPC$连接

1.2.1 首先设置远程主机的账户密码。

```
net use \\远程主机 ip "密码" /user:"用户名"     #与目标主机建立 IPC$连接通道
net use z: \\远程主机 IP\c$     #将目标主机的 C 盘影射为本地 Z 盘
copy C:\a.txt \\远程主机 ip\C$     #拷贝本地文件 C:\a.txt 到目标主机（注意盘符要大写，a.txt 后添加一个空格）
```

1.2.2 在 cmd 命令行模式下输入命令 net use \\192.168.1.3\ipc$ "Simplexue123"

/user:"administrator"与目标主机建立 IPC$连接。如图 2 所示

图 1-2

1.2.3 在命令行下利用 cd 进入软件目录`C:\实验工具集\06_网络与无线安全\01_典型协议攻击\第 4 节 Windows 下 IPC$管道的建立和远程控制`,利用 copy 命令向服务器复制 a.txt 文件。

如图 3 所示

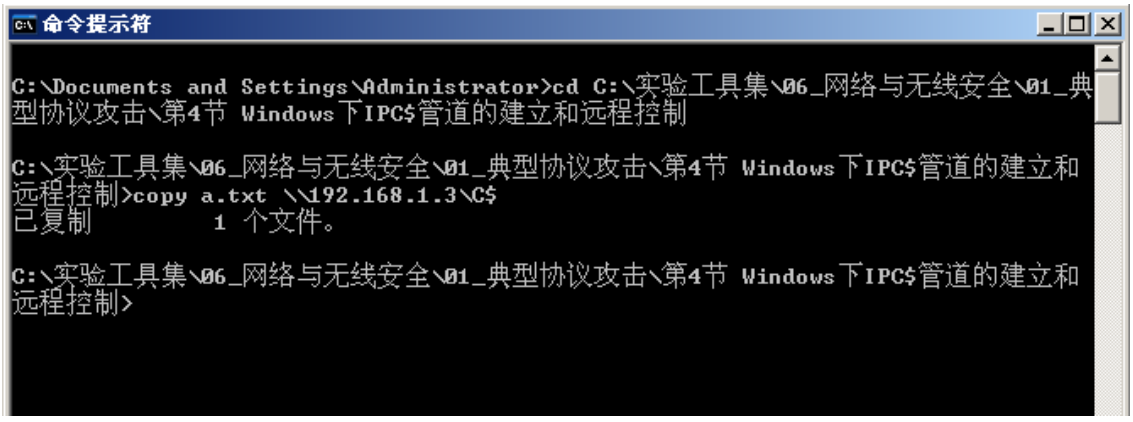


图 1-3

1.2.4 将对方的 C 盘映射为本地的 Z 盘,则可以像操纵本地硬盘一样对目标主机 C 盘进行操作。如图 4 所示

图 1-4

1.3 利用工具 PSEXEC 实施攻击

1.3.1 利用 PsExec 工具获得对方的 Shell，命令如下：PsExec \\远程主机 ip -u 用户名 -p 密码 cmd.exe；这里的-u 和-p 参数分别指定远程主机的用户名和密码，cmd.exe 是远程主机的命令行程序。如图 5 所示

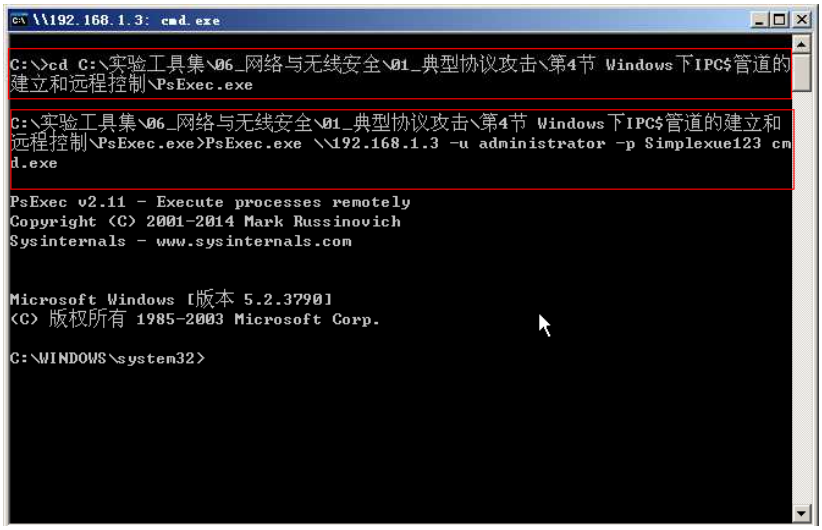


图 1-5

1.3.2 通过下图可以看到 ipconfig 命令已经在远程主机上执行了，获得的是对方主机的 IP 地址 192.168.1.3。如图 6 所示

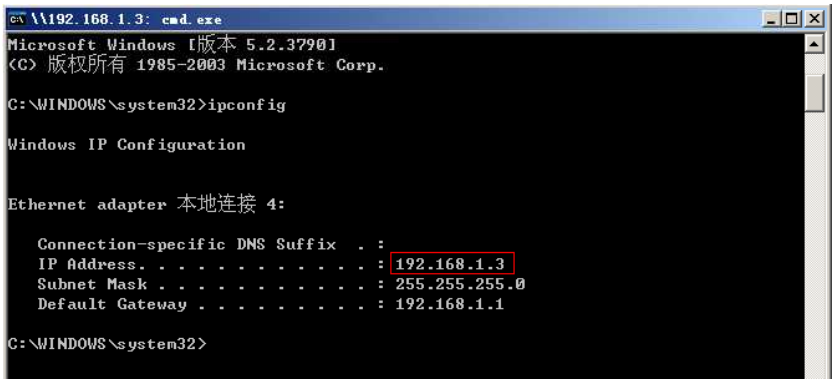


图 1-6

2、Windows 下 SSL_VPN 实验

2.1 客户端安装

2.2.1 在客户端（其 IP 地址为 172.22.3.1）上，双击桌面上的

“openvpn-install-2.3.10-I601-x86_64”进行安装，默认安装即可。如图 2-1 所示

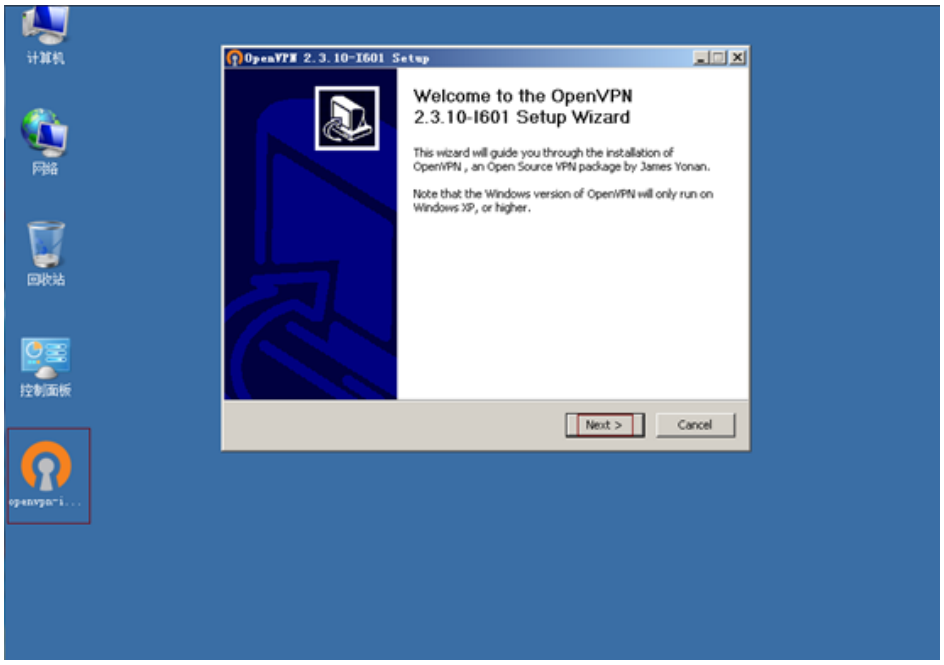


图 2-1

2.2 在安装过程中会弹出如下提示，选中”始终信任来自 OpenVPNTechnologies,INC 的软件”，

单击“安装”按钮，后面继续默认安装即可。如图 2-2 所示

图 2-2

2.2.服务器端软件安装

2.2.1 在服务端（其 IP 地址为 172.22.3.2）上，双击桌面上的“openvpn-install-2.3.10-I601-x86_64”进行安装，选中软件所有功能，然后单击“Next”安装。如图 2-3 所示

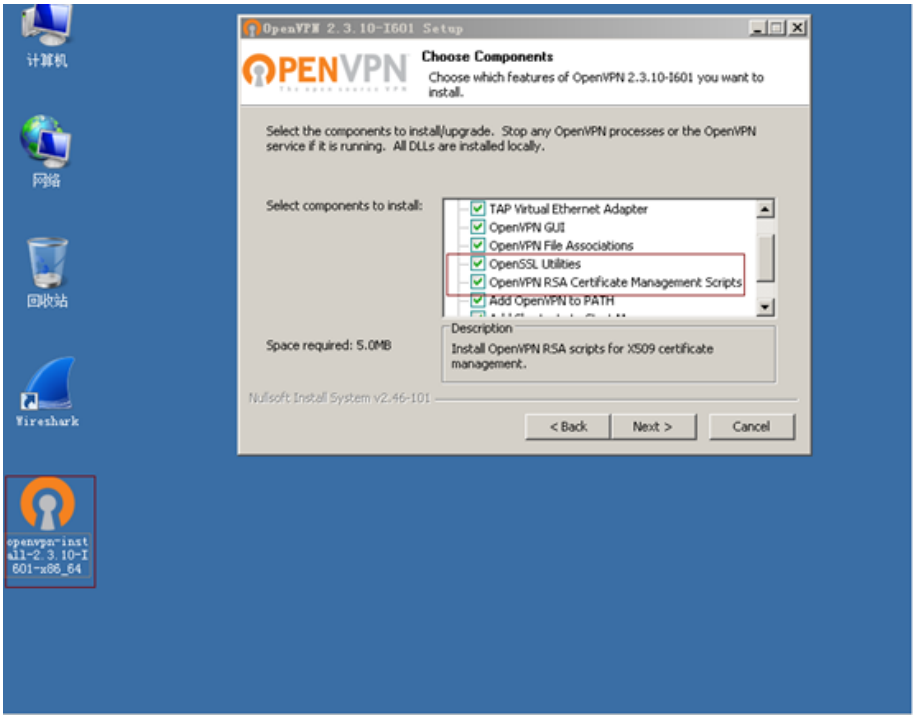


图 2-3

2.2.2 在安装过程中会弹出如下提示，选中”始终信任来自 OpenVPN Technologies, INC 的软件”，单击“安装”按钮，后面继续默认安装即可。如图 2-4 所示

图 2-4

2.2.3 复制一份目录 C:\ProgramFiles\OpenVPN\easy-rsa 下的 vars.bat.sample 文件，重命名为 vars.bat，右键该文件，选择编辑。如图 2-5 所示

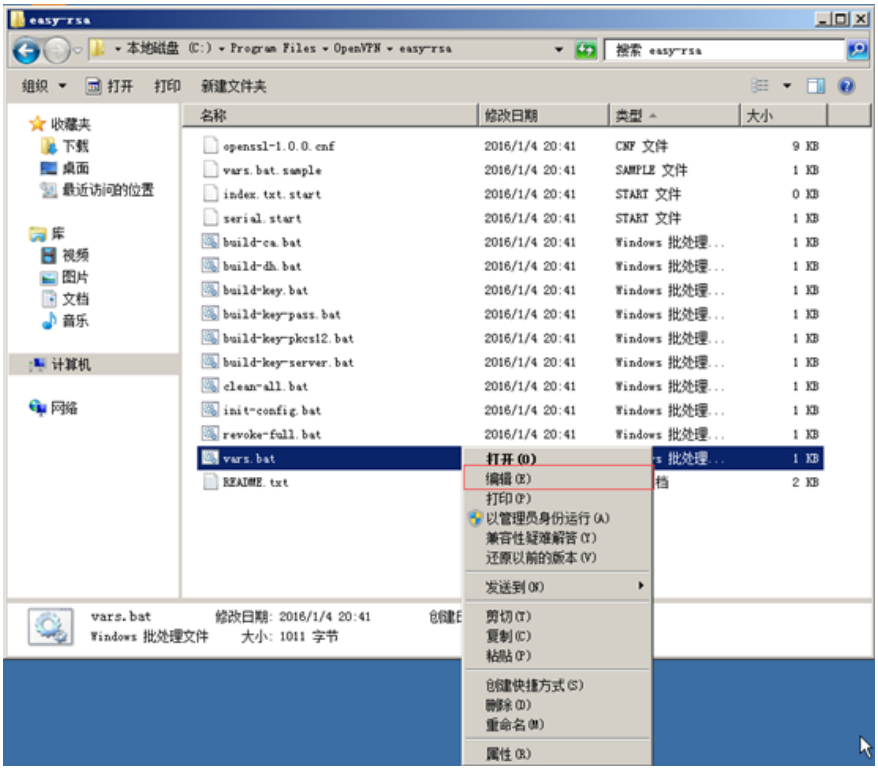


图 2-5

2.2.4 修改配置文件的参数

```
1.  set KEY_COUNTRY=CN
2.  set KEY_PROVINCE=BJ
3.  set KEY_CITY=BeiJing
4.  set KEY_ORG=xipu
5.  set KEY_EMAIL=xipu@host.domain
```

保存并关闭文件。如图 2-6 所示

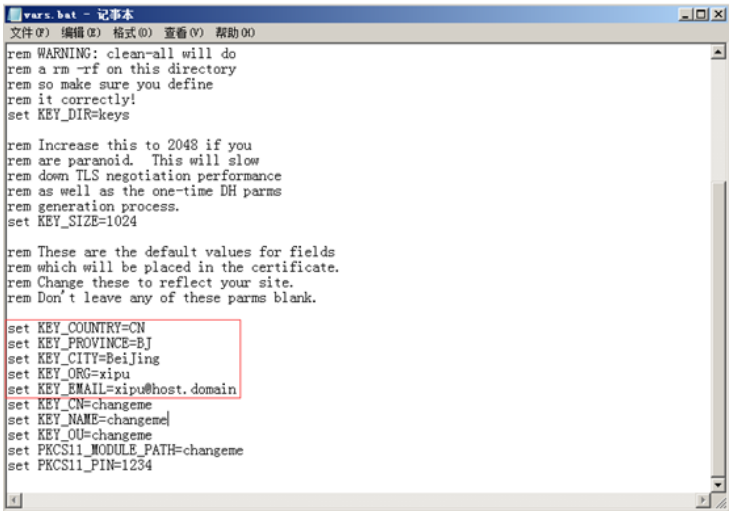


图 2-6

2.2.5 单击“开始”->”运行”->输入 cmd 命令。如图 2-7 所示

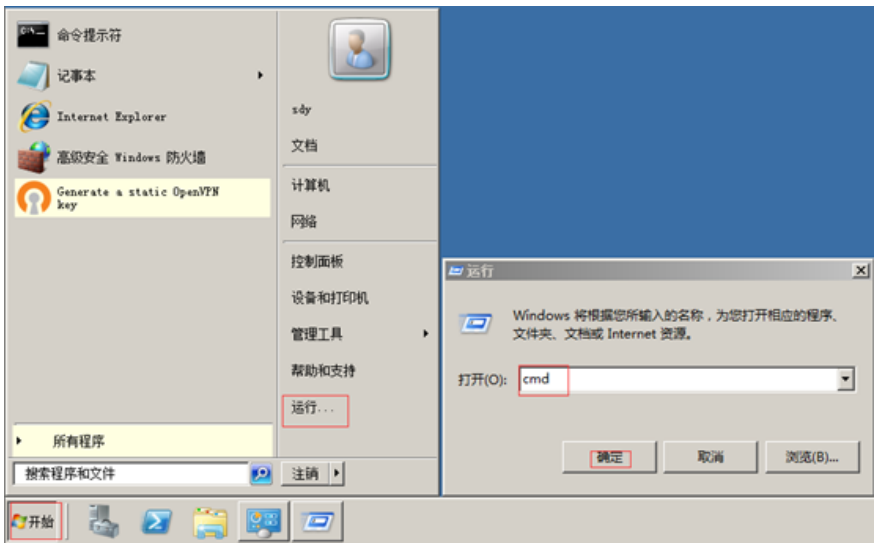


图 2-7

2.2.6 在命令行下输入 `cd C:\ProgramFiles\openvpn\easy-rsa`。如图 2-8 所示

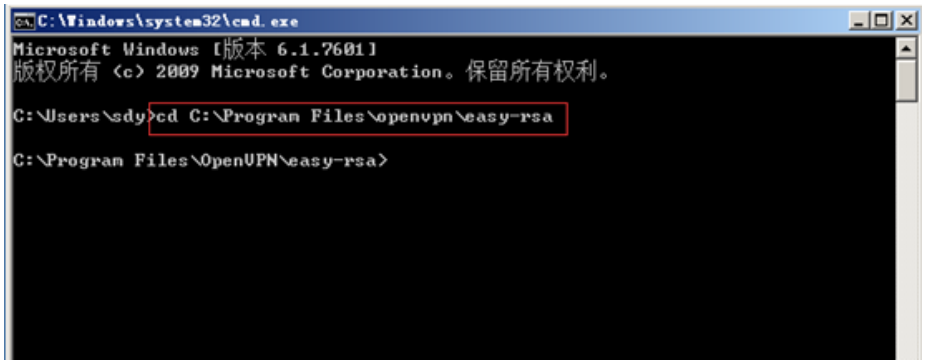


图 2-8

2.2.7 输入命令“vars”，设置相应的局部环境变量。如图 2-9 所示

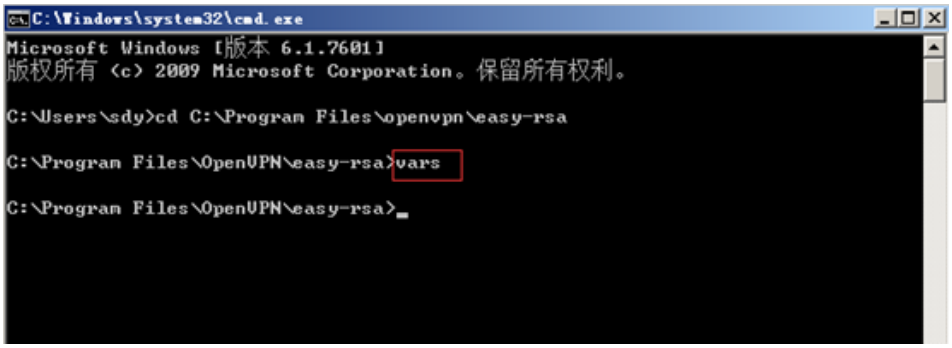


图 2-9

2.2.8 输入命令“clean-all”，清理操作。如图 2-10 所示

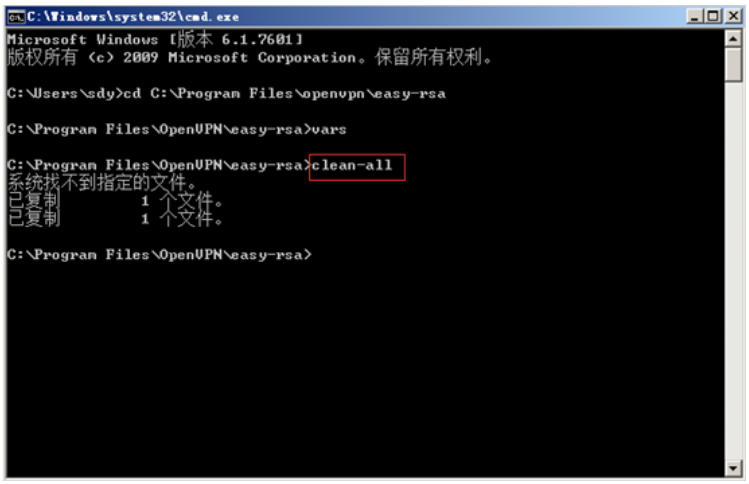


图 2-10

2.3.生成 CA

2.3.1 继续在服务端的 cmd 上输入命令“vars”。如图 2-11 所示

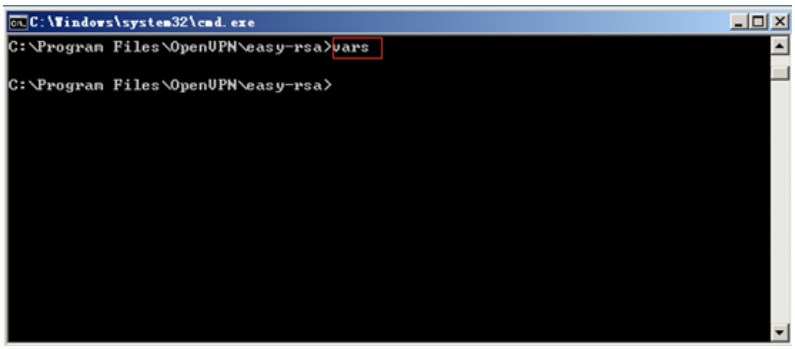


图 2-11

2.3.2 输入命令 build-ca,填写参数，创建 CA 根证书（保持默认参数也可以）。如图 2-12 所示

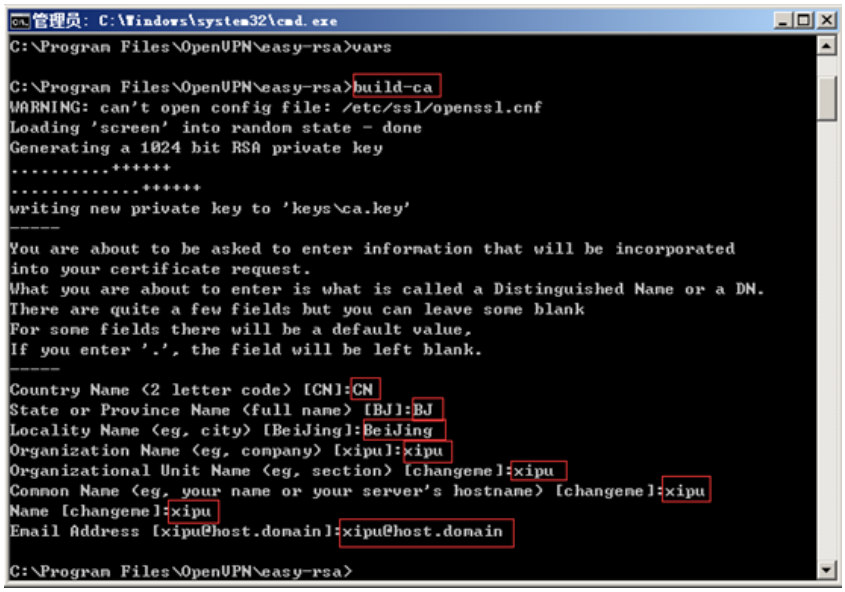


图 2-12

2.4.生成 dh1024.pem 文件

2.4.1 继续在服务端的 cmd 上输入命令 vars。如图 2-13 所示

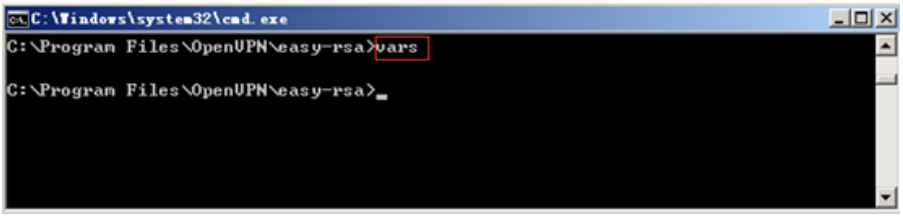


图 2-13

2.4.2 输入命令 build-dh。如图 2-14 所示

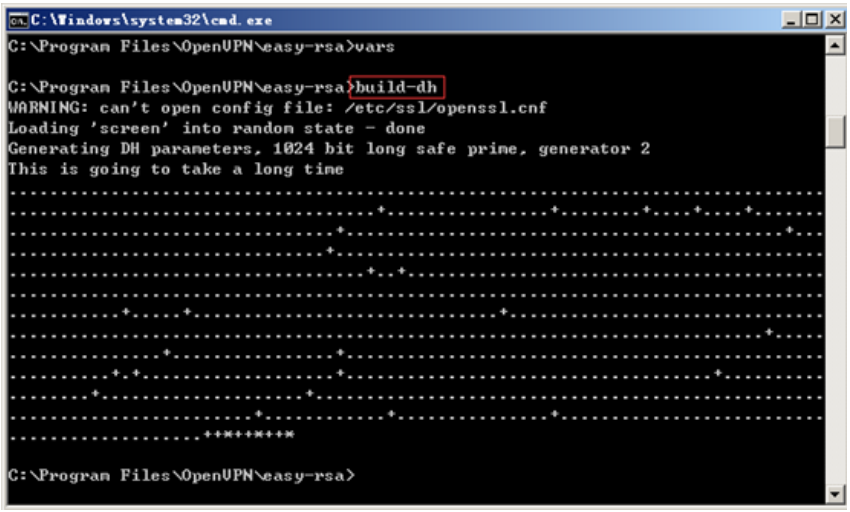


图 2-14

2.5.生成服务端正书

2.5.1 继续在服务端的 cmd 上输入命令 vars。如图 2-15 所示

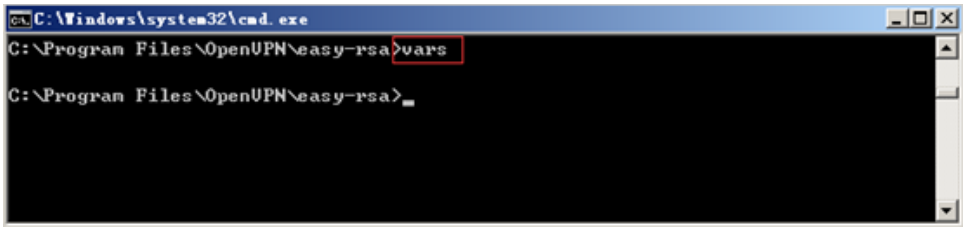


图 2-15

2.5.2 输入命令 build-key-server xipuserver，填写参数，创建服务端证书。如图 2-16 所示

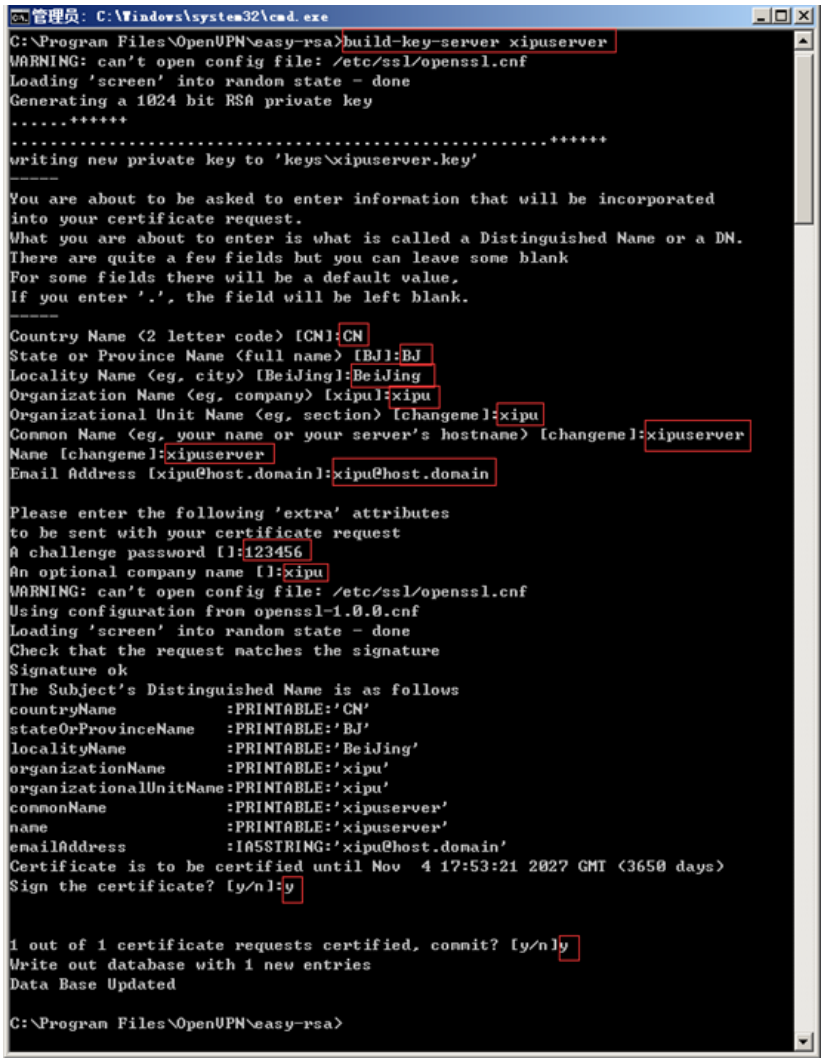


图 2-16

2.6.生成客户端证书

2.6.1 继续在服务端的 cmd 上输入命令 vars。如图 2-17 所示

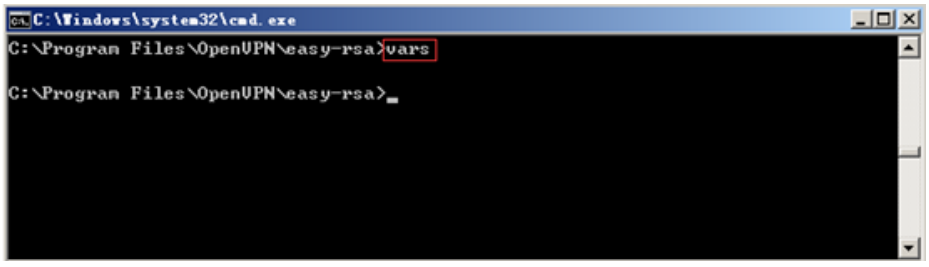


图 2-17

2.6.2 输入命令 build-key xipuclient，生成客户端证书。如图 2-18 所示

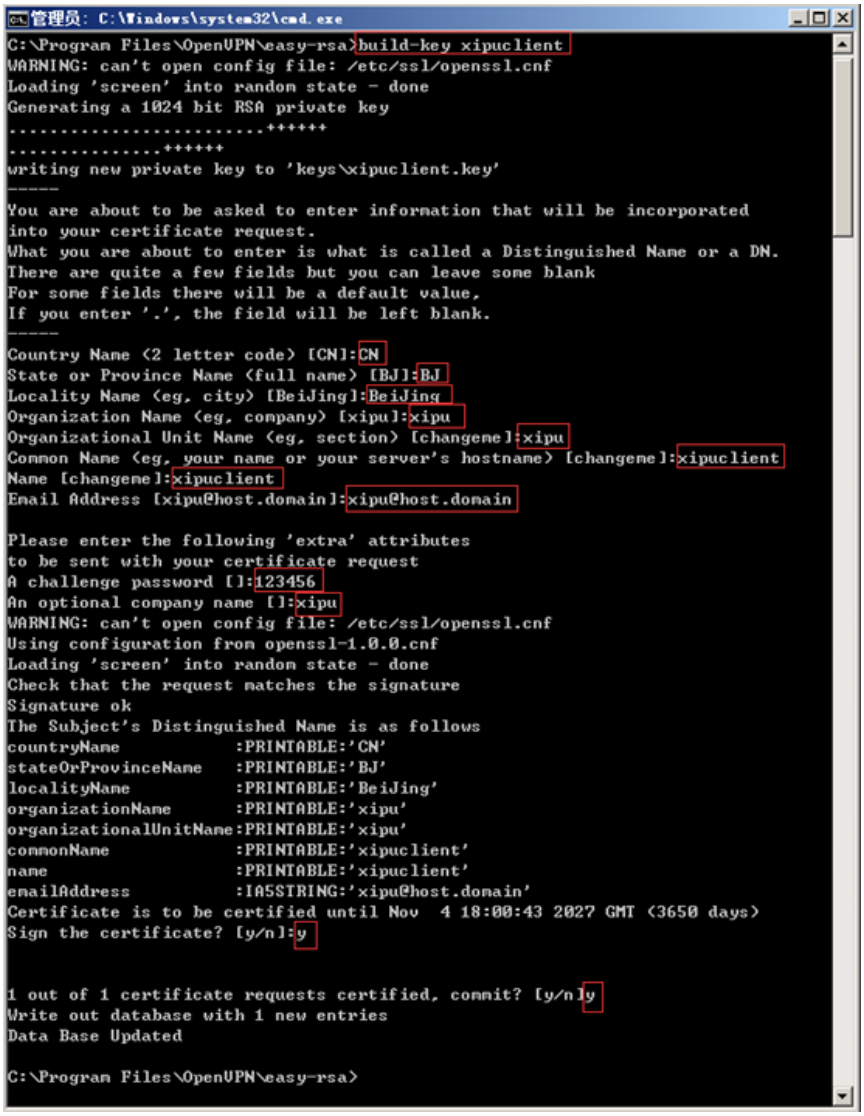


图 2-18

2.7.修改服务端配置文件参数

2.7.1 在服务端上，进入 C:\ProgramFiles\OpenVPN\sample-config 目录，右键 server.ovpn 文件，选择打开，修改服务端配置参数。如图 2-19 所示

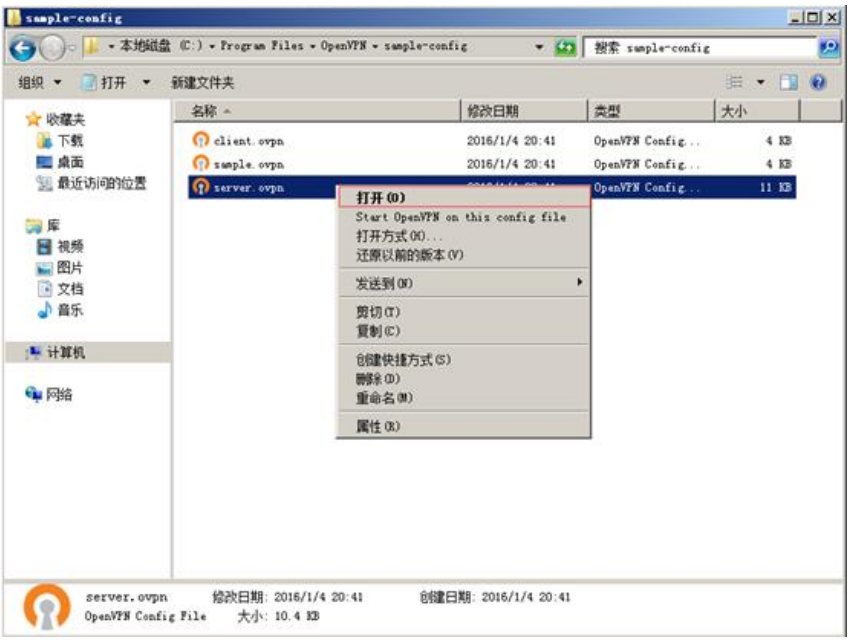


图 2-19

7.2 下面代码为配置文件中需要修改的地方，其他保持默认，修改完后保存即可。如图 2-20 所示。

```
1.  certxipuserver.crt #服务端证书
2.  keyxipuserver.key#服务端 key
3.  dhdh1024.pem #迪菲亚证书
4.  server10.10.10.0255.255.255.0 #给虚拟局域网分配的网段
```

图 2-20

2.7.3 将修改后的 server.ovpn 文件复制到目录 `C:\ProgramFiles\OpenVPN\config` 下，把 `C:\ProgramFiles\OpenVPN\easy-rsa\keys` 目录中的“ca.crt、ca.key、dh1024.pem、xipuserver.crt、xipuserver.csr、xipuserver.key”复制到 `C:\ProgramFiles\OpenVPN\config` 目录下。如图 2-21 所示

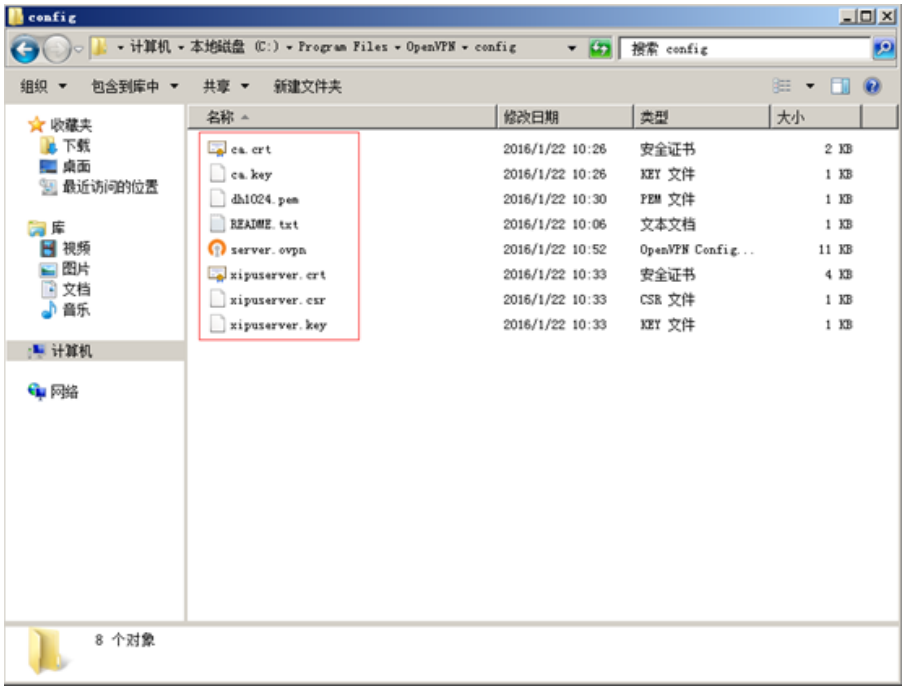


图 2-21

2.7.4 双击桌面上的 OpenVPNGUI 图标，启动软件。如图 2-22 所示

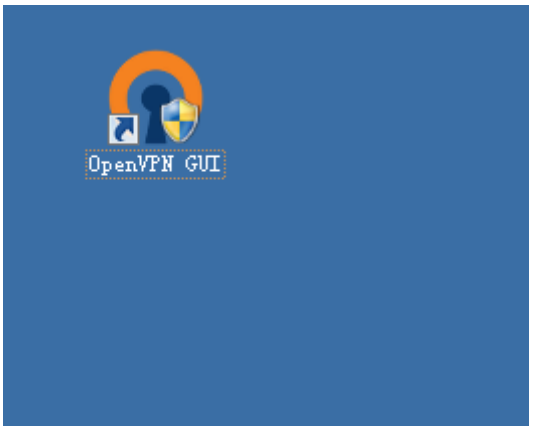


图 2-22

2.7.5 在任务栏，右键 openvpn 图标，选择“Connect”即可。如图 2-23 所示

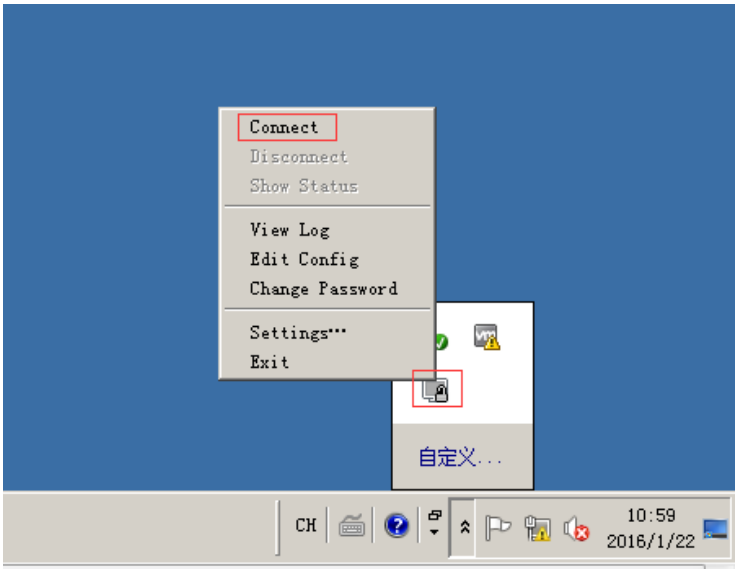


图 2-23

2.7.6 图标变绿色，表示连接成功。如图 2-24 所示

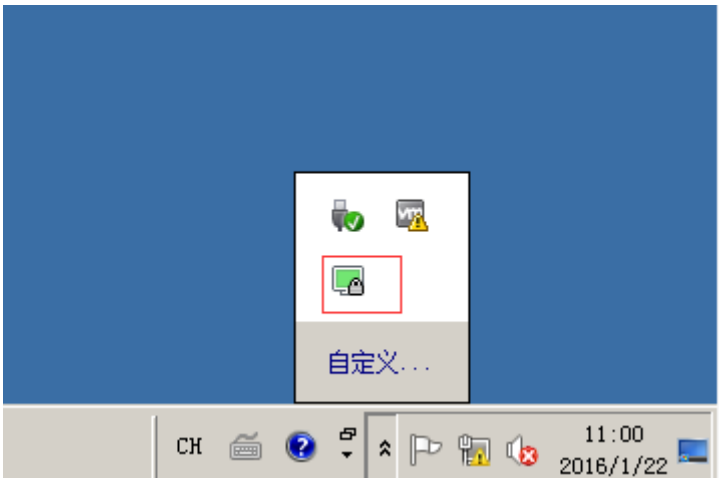


图 2-24

2.7.7 重新打开一个 cmd，输入命令 ipconfig，可以看到服务端 VPN 网卡 IP 地址分配为 10.10.10.1。如图 2-25 所示

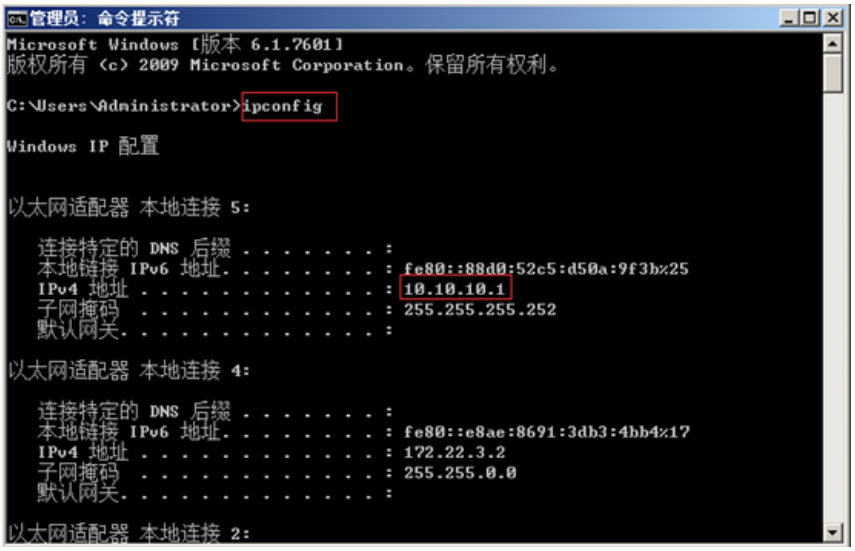


图 2-25

2.8.客户端配置文件操作

2.8.1 在客户端上，进入 C:\ProgramFiles\OpenVPN\sample-config 目录，右键 client.ovpn 文件，选择打开，修改客户端配置参数。如图 2-26 所示

图 2-26

2.8.2 修改客户端文件，参数按照下面进行更改。保存后关闭文件。将修改后的 client.ovpn 文件复制到目录 C:\ProgramFiles\OpenVPN\config 下。

remote 172.22.3.2 1194 #VPN 服务端的 IP 地址和端口 cert xipuclient.crt#服务端证书 key xipuclient.key#服务端 key 如图 2-27、2-28 所示

图 2-27

图 2-28

2.9.复制服务端配置文件到客户端机器上

2.9.1 在客户端上，单击“开始”->”运行”->”mstsc”。如图 2-29 所示

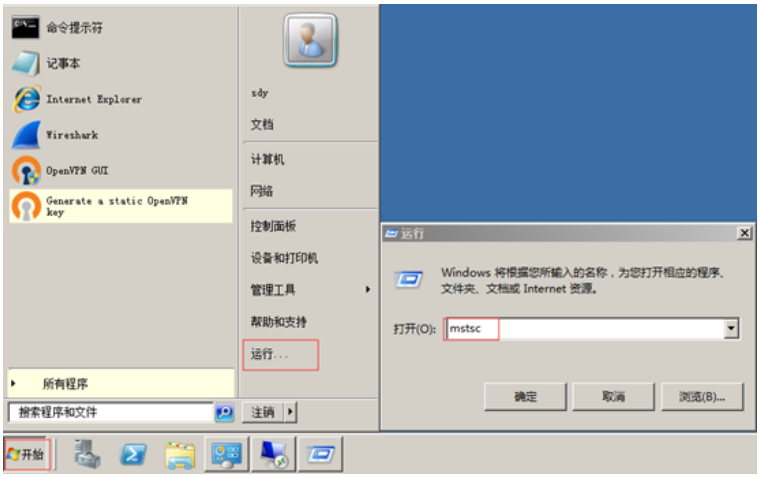


图 2-29

2.9.2 在弹出的对话框输入服务器 IP 地址 172.22.3.2、账号 administrator 和密码 Simplexue123，远程连接服务器，拷贝客户端文件。如图 2-30 所示

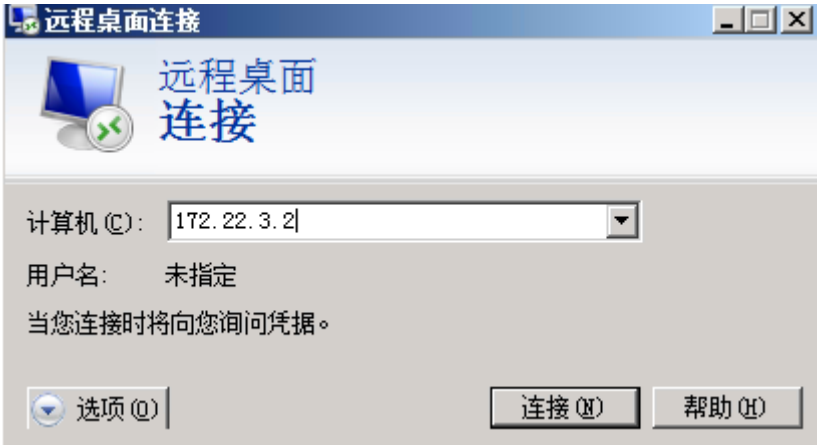


图 2-30

2.9.3 把服务端“C:\ProgramFiles\OpenVPN\easy-rsa\keys”目录中的“ca.crt、ca.key、xipuclient.crt、xipuclient.csr、xipuclient.key”复制到客户端“C:\ProgramFiles\OpenVPN\config”目录下。如图 2-31 所示

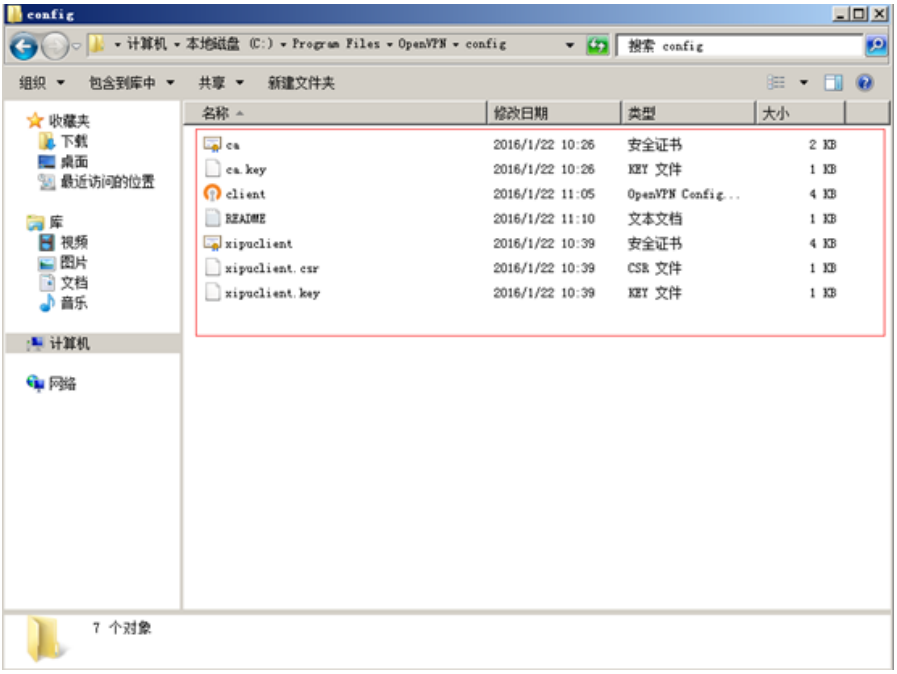


图 2-31

2.9.4 双击客户端桌面上的 OopenVPNGUI 图标，启动软件。如图 2-32 所示

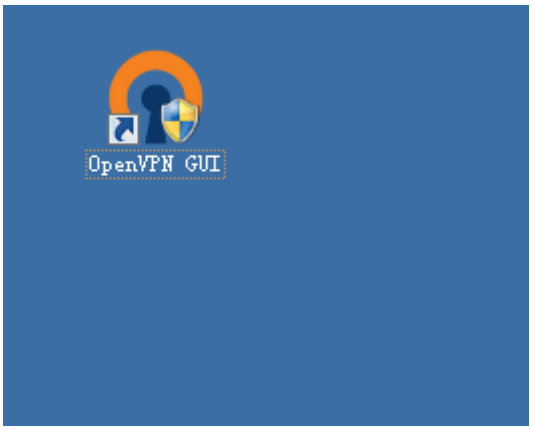


图 2-32

2.9.5 在任务栏，右键 openvpn 图标，选择“Connect”即可。如图 2-33 所示

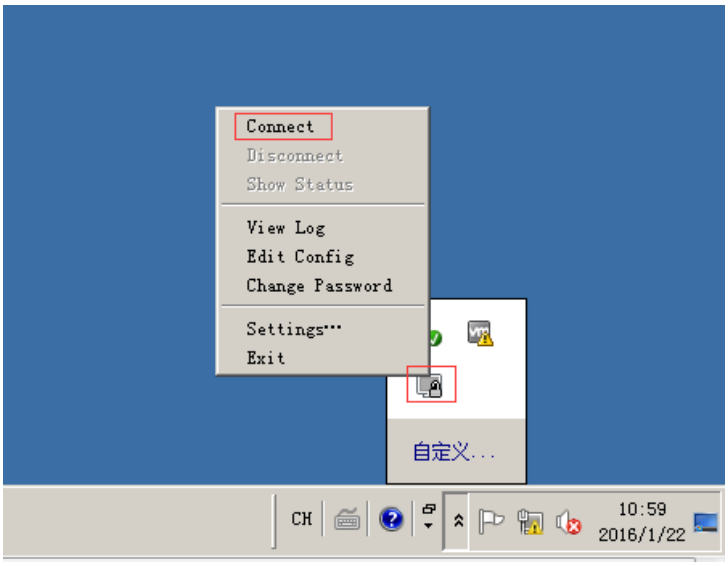


图 2-33

2.9.6 图标变绿色，表示连接成功。如图 2-34 所示

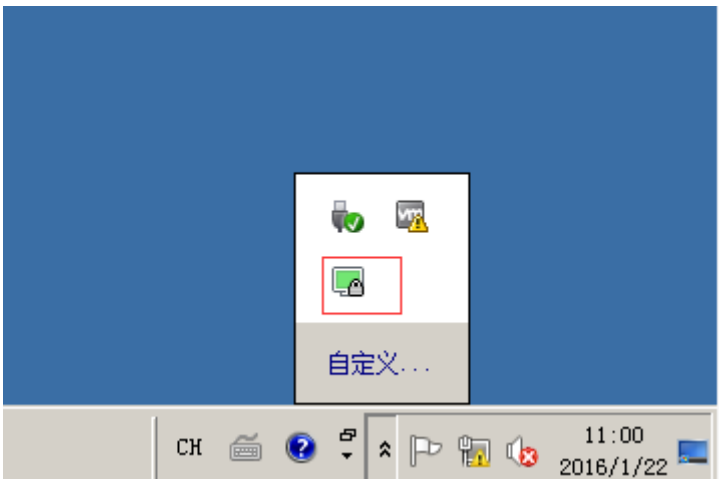


图 2-34

2.9.7 打开 cmd，输入命令 ipconfig，可以看到客户端 VPN 网卡 IP 地址 1 为 10.10.10.6。如图 2-35 所示

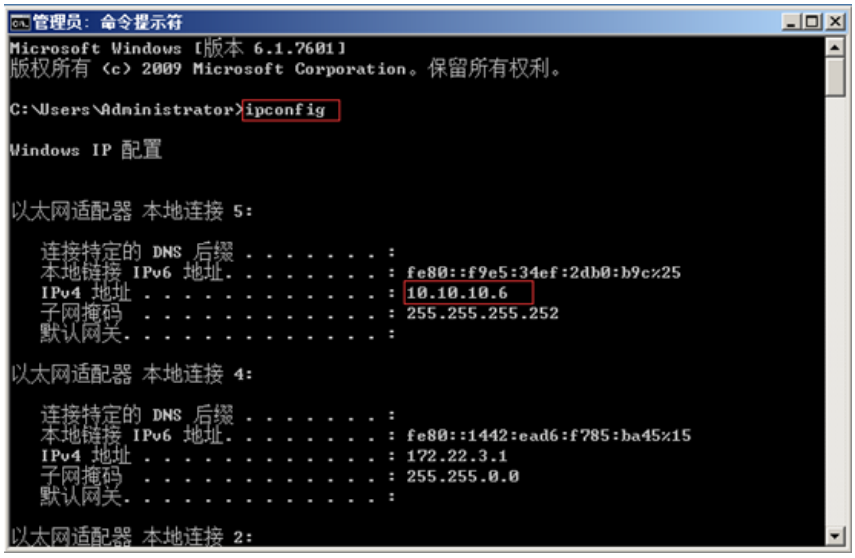


图 2-35

2.10.验证加密性

2.10.1 在服务端上为了使 wireshark 能够显示 VPN 网卡，需要进行下面几步的操作。

单击开始—>控制面板—>硬件—>设备和打印机处的设备管理器，打开设备管理器。单击查看—>显示隐藏的设备。如图 2-36 所示

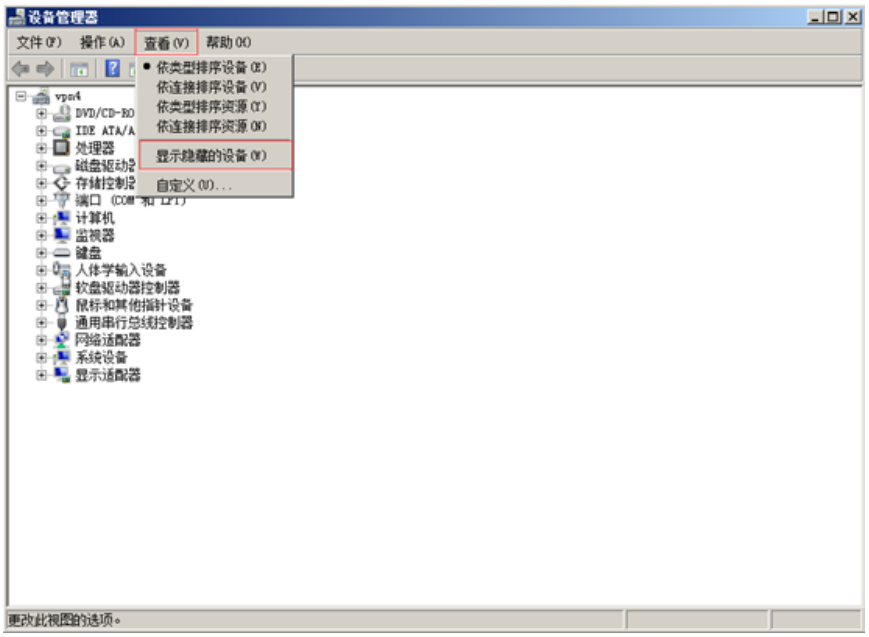


图 2-36

右键非即插即用驱动程序下的 NetGroupPacketFilterDriver，选择属性。如图 2-37 所示

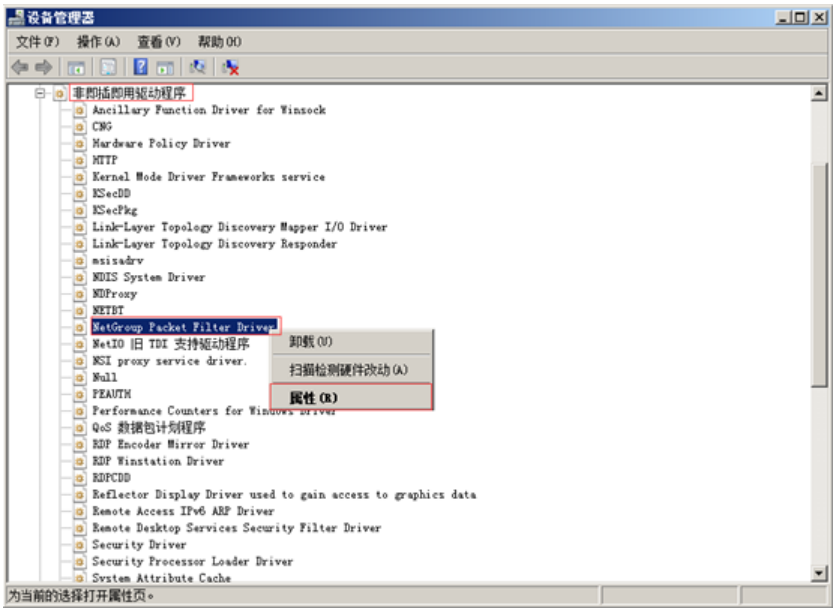


图 2-37

切换到驱动程序选项卡，将启动类型改为系统，单击确定。如图 2-38 所示

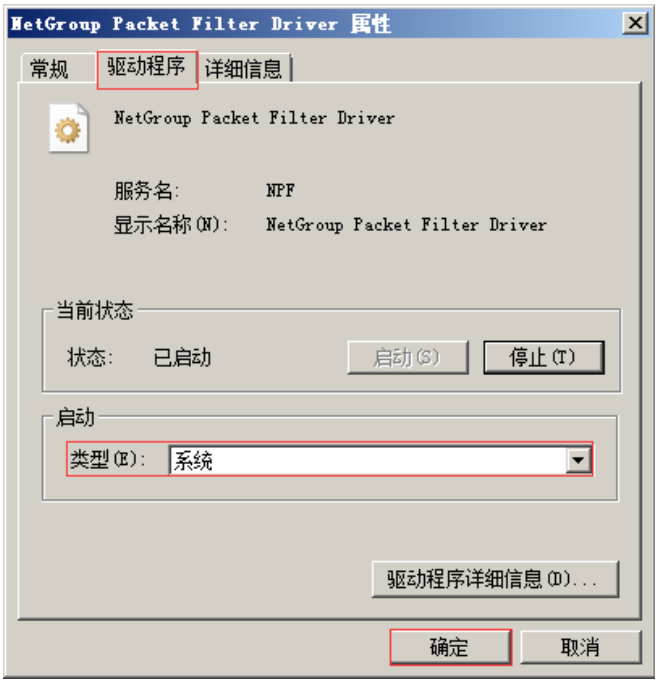


图 2-38

打开 cmd，输入命令 netstopnpf 和 netstartnpf，重启 npf 服务。如图 44 所示

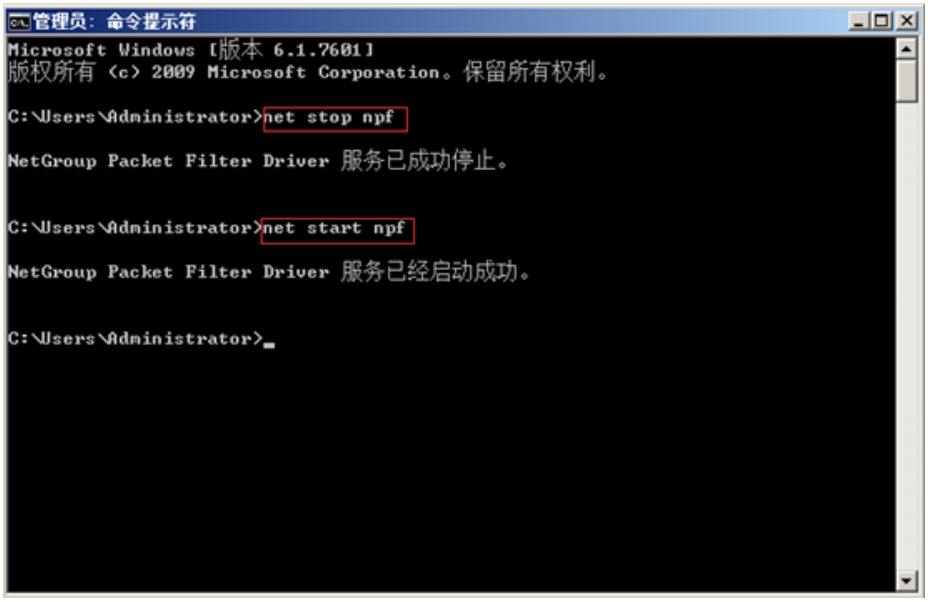


图 2-39

输入命令 ipconfig，可以看到 10.10.10.1 所在的网卡为本地连接 5，172.22.3.2 所在的网卡为本地连接 4。如图 2-40 所示

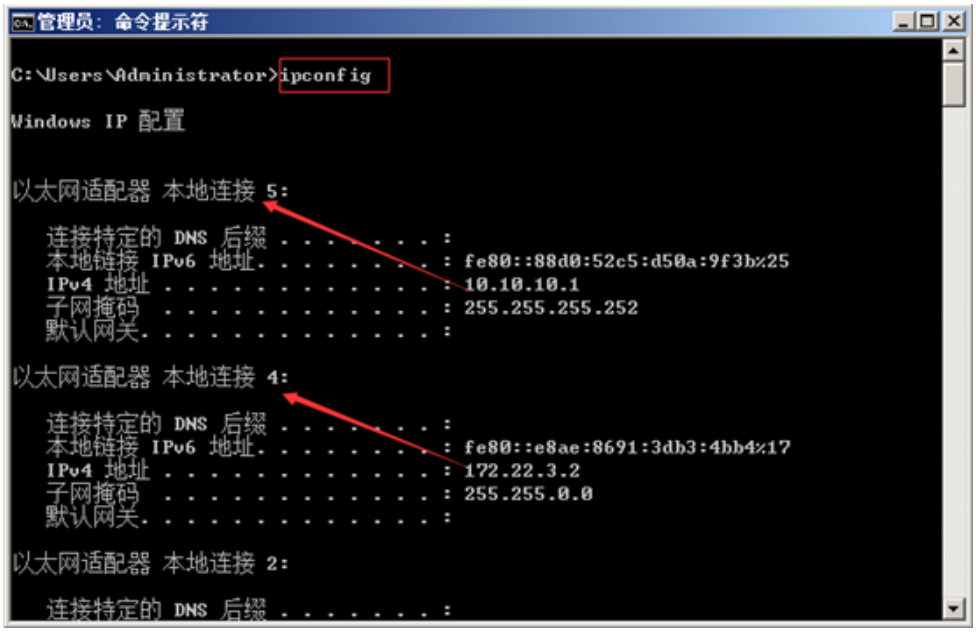


图 2-40

2.10.2 在客户端打开两个命令行窗口,分别输入命令 ping 172.22.3.2 -t 和 ping 10.10.10.1 -t。如图 2-41、2-42 所示

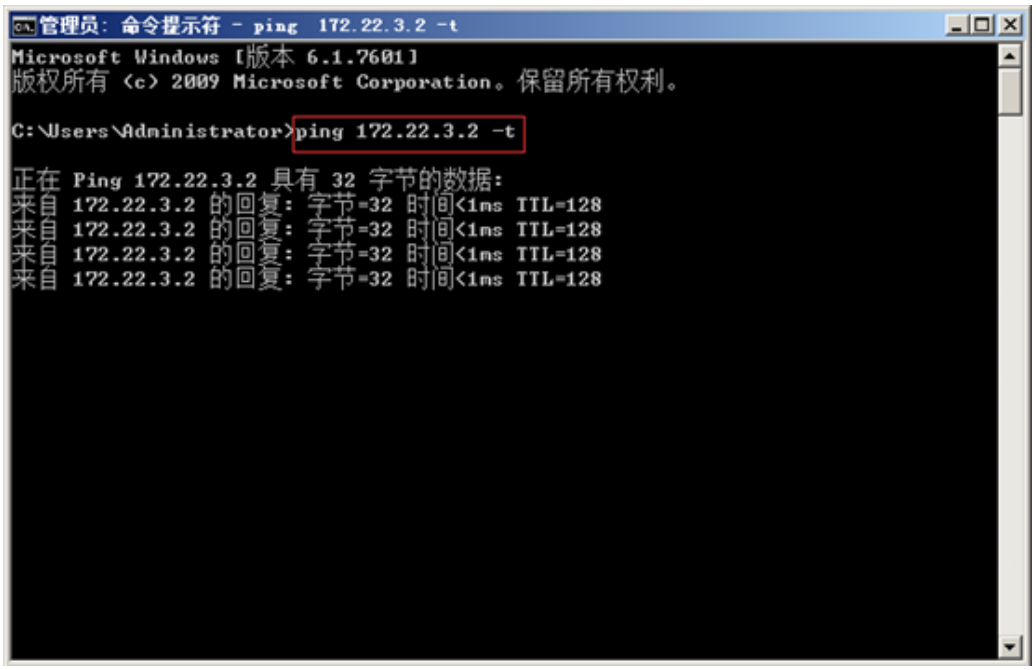


图 2-41

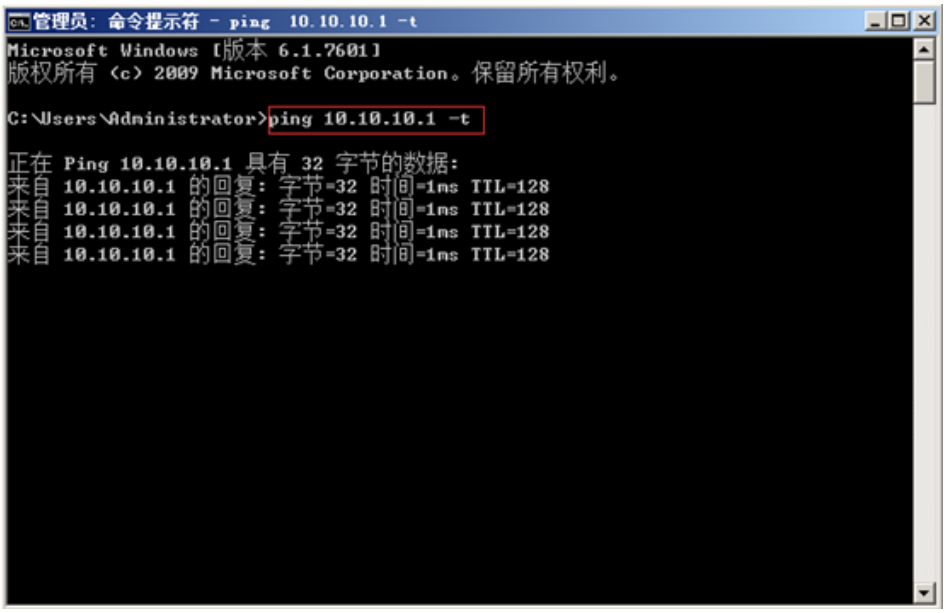


图 2-42

2.10.3 双击桌面上的 wireshark 图标，选择本地连接 4，单击开始捕获分组按钮。如图 2-43 所示

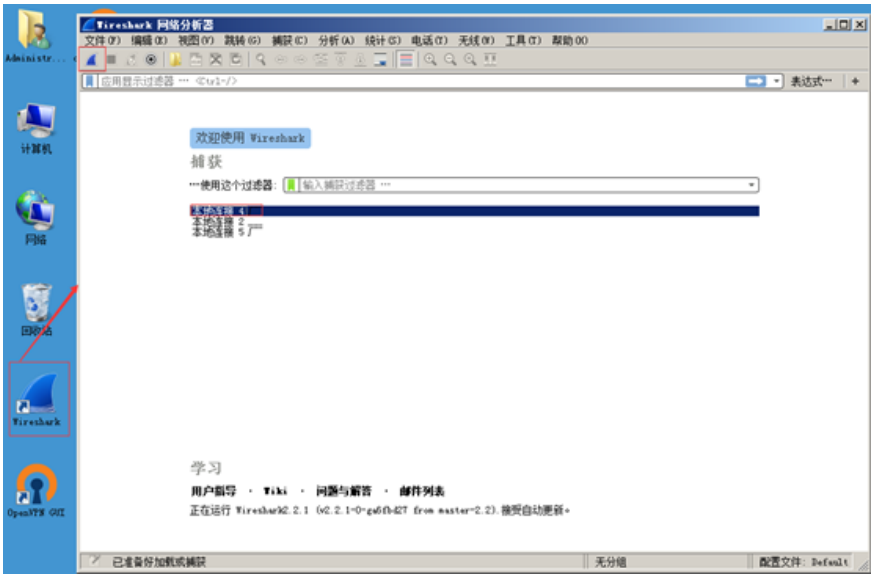


图 2-43

2.10.4 抓取 172.22.3.2 所在网卡本地连接 4 的数据包。如图 2-44 所示

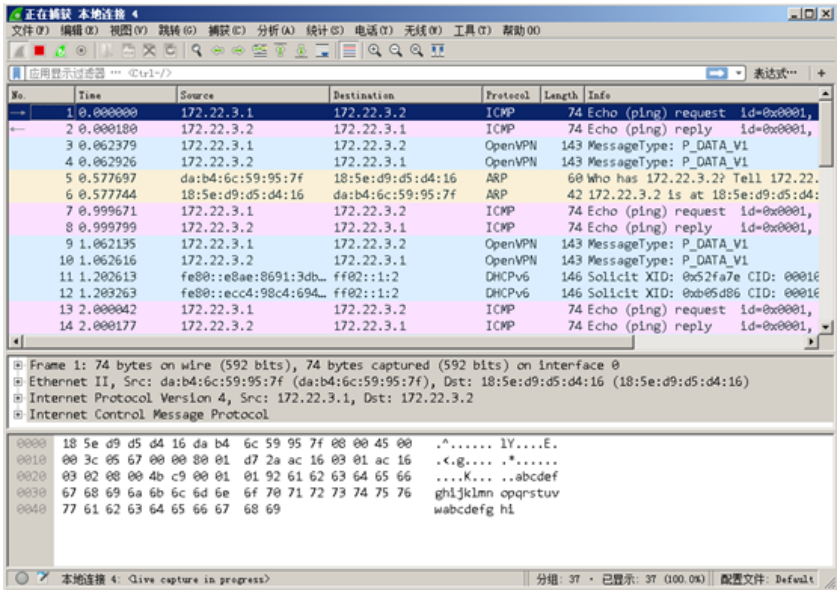


图 2-44

2.10.5 关闭并重新打开 wireshark，选择本地连接 5，单击开始捕获分组按钮。如图 2-45 所示

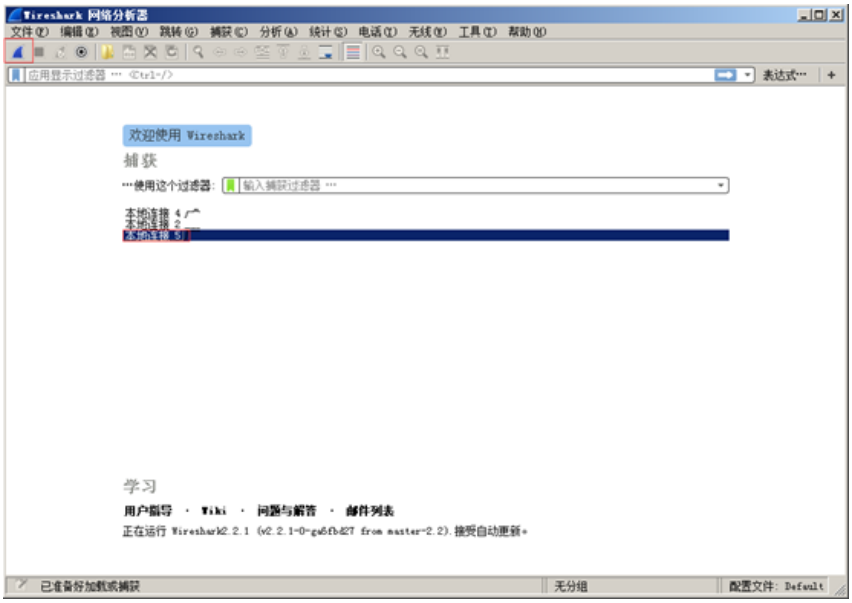


图 2-45

2.10.6 抓取 10.10.10.1 所在网卡本地连接 5 的数据包。如图 2-46 所示

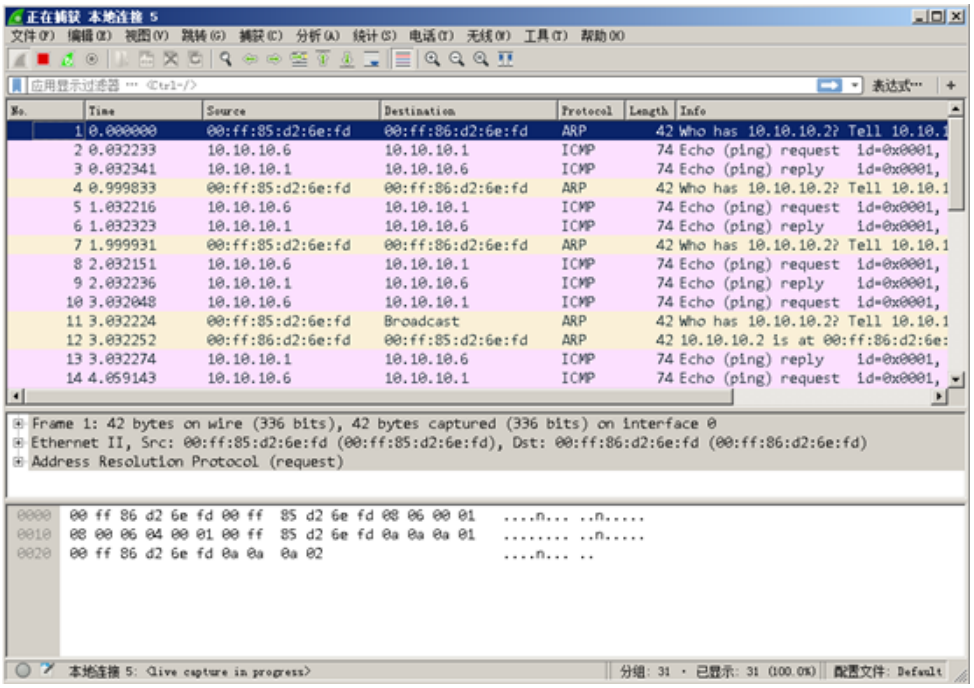

正在捕获 本地连接 5
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式…
No. Time Source Destination Protocol Length Info
1 0.000000 00:ff:85:d2:6e:fd 00:ff:86:d2:6e:fd ARP 42 Who has 10.10.10.2? Tell 10.10.1
2 0.032233 10.10.10.6 10.10.10.1 ICMP 74 Echo (ping) request id=0x0001,
3 0.032341 10.10.10.1 10.10.10.6 ICMP 74 Echo (ping) reply id=0x0001,
4 0.999833 00:ff:85:d2:6e:fd 00:ff:86:d2:6e:fd ARP 42 Who has 10.10.10.2? Tell 10.10.1
5 1.032216 10.10.10.6 10.10.10.1 ICMP 74 Echo (ping) request id=0x0001,
6 1.032323 10.10.10.1 10.10.10.6 ICMP 74 Echo (ping) reply id=0x0001,
7 1.999931 00:ff:85:d2:6e:fd 00:ff:86:d2:6e:fd ARP 42 Who has 10.10.10.2? Tell 10.10.1
8 2.032151 10.10.10.6 10.10.10.1 ICMP 74 Echo (ping) request id=0x0001,
9 2.032236 10.10.10.1 10.10.10.6 ICMP 74 Echo (ping) reply id=0x0001,
10 3.032048 10.10.10.6 10.10.10.1 ICMP 74 Echo (ping) request id=0x0001,
11 3.032224 00:ff:85:d2:6e:fd Broadcast ARP 42 Who has 10.10.10.2? Tell 10.10.1
12 3.032252 00:ff:86:d2:6e:fd 00:ff:85:d2:6e:fd ARP 42 10.10.10.2 is at 00:ff:86:d2:6e:
13 3.032274 10.10.10.1 10.10.10.6 ICMP 74 Echo (ping) reply id=0x0001,
14 4.059143 10.10.10.6 10.10.10.1 ICMP 74 Echo (ping) request id=0x0001,
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: 00:ff:85:d2:6e:fd (00:ff:85:d2:6e:fd), Dst: 00:ff:86:d2:6e:fd (00:ff:86:d2:6e:fd)
Address Resolution Protocol (request)
0000 00 ff 86 d2 6e fd 00 ff 85 d2 6e fd 08 06 00 01 ....n... ..n.....
0010 08 00 06 04 00 01 00 ff 85 d2 6e fd 0a 0a 0a 01 ....n.....
0020 00 ff 86 d2 6e fd 0a 0a 0a 02 ....n... ..
本地连接 5: <live capture in progress>
分组: 31 · 已显示: 31 (100.0%)
配置文件: Default

图 2-46

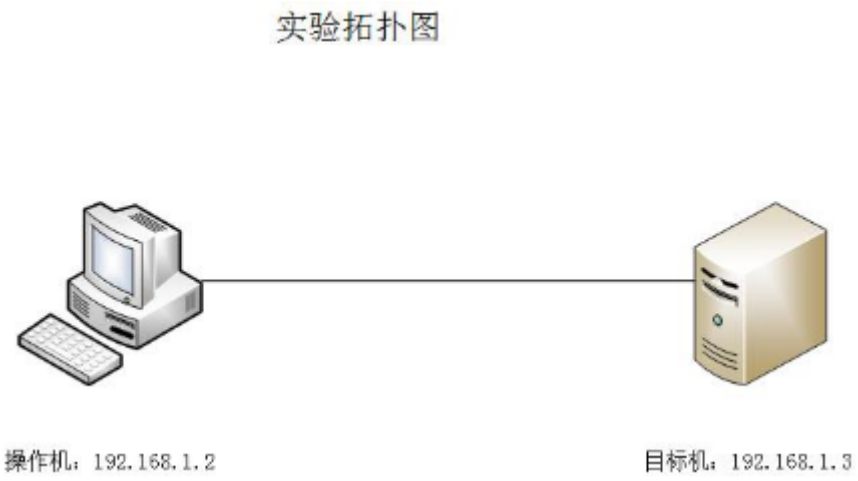
实验八 SQL 注入 access 数据库实验

一、实验目的

1、理解 SQL 注入的原理

2、学习手工注入的过程

二、实验环境



目标机：192.168.1.3

工具: C:\实验工具集\01*WEB 安全\02* 注入技术实验工具

三、实验内容

1、找到有注入漏洞的目标网站

2、猜解表名

3、猜解列名

4、猜测字段内容

四、实验步骤

步骤 1、找到有注入漏洞的目标网站

1.1 目标站点：【http:// 192.168.1.3:8008】,随便选择一个链接

【http://192.168.1.3:8008/onews.asp?id=45】。如图 1-1 所示

图 1-1

1.2 测试链接，在链接末尾添加【’】。如图 1-2 所示

图 1-2

1.3 在链接末尾添加【 and 1=1】。如图 1-3 所示

图 1-3

1.4 在链接末尾添加【and 1=2】，返回页面显示该网站存在注入漏洞。如图 1-4 所示

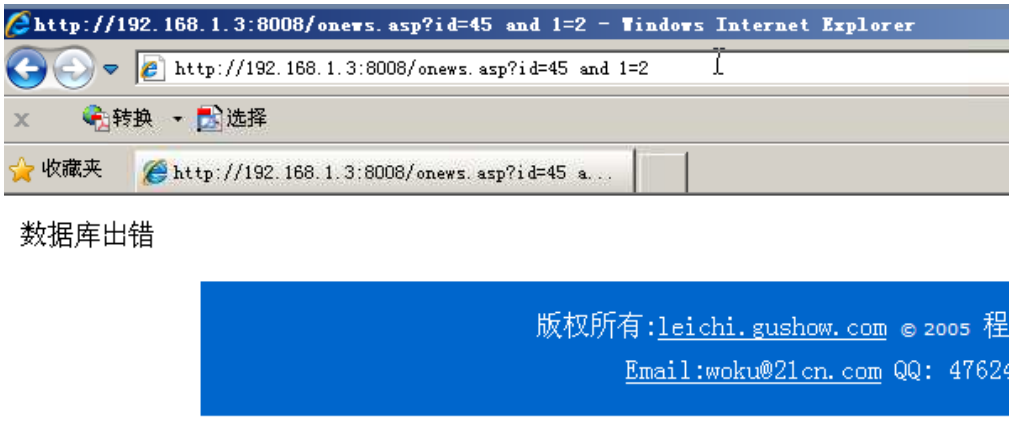


图 1-4

步骤 2、猜解表名

2.1 在链接末尾添加语句【and exists(select * from admin)】，页面正常显示，说明存在表名【admin】。如图 1-5 所示

图 1-5

步骤 3、猜解列名

3.1 在连接末尾添加语句【and exists(select admin from admin)】，页面显示正常，即在表中存在 admin 列。如图 1-6 所示

图 1-6

3.2 同样的方法，在链接末尾添加【and exists(select password from admin)】，页面显示正常，说明存在列 password。如图 1-7 所示

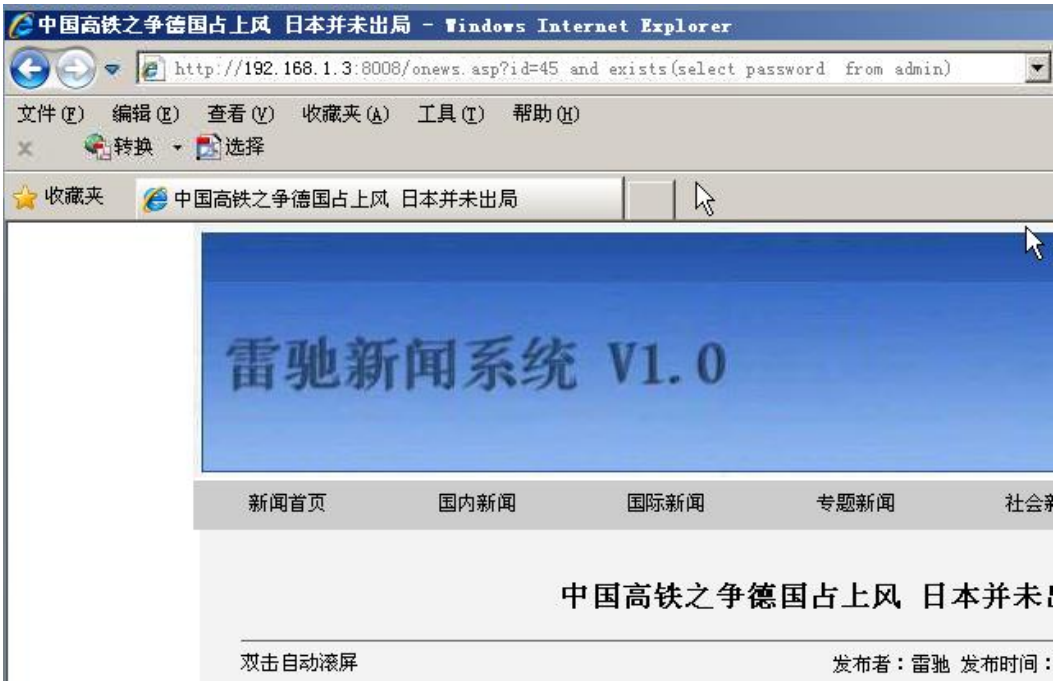


图 1-7

步骤 4、猜测字段内容

4.1 猜测字段的长度，在连接末尾输入语句【and (select top 1 len (admin) from admin)>1】，页面显示正常，数字依次加 1，进行测试，如【and (select top 1 len (admin) from admin)>5】，说明字段长度为 5。如图 1-8 所示

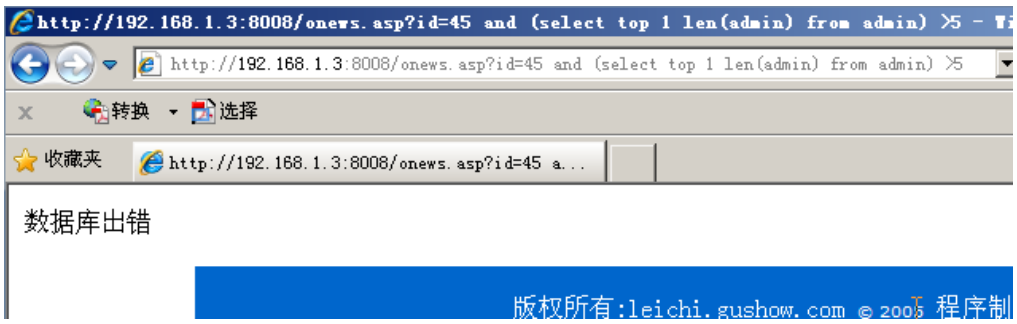


图 1-8

4.2 同样的方法，在链接末尾添加连接【and (select top 1 asc(mid(admin,1,1)) from admin)>97】，可猜解出第一条记录的第一位字符的 ASCII 码为 97，对应 a。如图 1-9 所示

图 1-9

4.3 同样的方法可以得到 admin 字段内容为【admin】，password 字段内容为【bfpms】。

实验九 备选实验

隐写技术、word 文档中隐藏数据、密钥穷举、利用 arp 协议缺陷实现中间人攻击

一、实验目的

1、隐写技术

(1) 了解隐写技术的分类

(2) 了解隐写技术的基本原理

2、word 文档中隐藏数据

掌握在 word 文档中隐藏数据的方法

3、密钥穷举

密钥穷举、字典、查表攻击

4、利用 arp 协议缺陷实现中间人攻击

利用 arp 协议缺陷实现中间人攻击获取网络中传输的明文密码。利用中间人攻击实现 DNS 欺骗攻击。

二、实验环境

1、隐写技术

Windows Server 2008

相关文件地址：C:\Users\Administrator\Desktop\hidden\隐写技术

2、word 文档中隐藏数据

Windows Server 2008

3、密钥穷举

Windows7

工具：C:\tools\密码学课程\02 密码学分析\lab1

4、利用 arp 协议缺陷实现中间人攻击

3 台 Win2003，

靶机 ip 分别为 192.168.1.3，192.168.1.4，攻击机为 192.168.1.2

192.168.1.4 搭建了 ftp 服务器，账户为：administrator，密码为 Simplexue123。

192.168.1.4 配置了 dns 服务。

软件：cain

三、实验内容

1、隐写技术

(1)插入方法

(2)修改方法

2、word 文档中隐藏数据

隐藏数据

3、密钥穷举

(1)DES 加密

(2)穷举攻击

(3)字典攻击

(4)查找攻击

4、利用 arp 协议缺陷实现中间人攻击

(1)利用 cain 进行 arp 欺骗

(2)利用 cain 抓取 ftp 密码

(3)利用 cain 进行 dns 欺骗

四、实验步骤

1、隐写技术

1.1.插入方法

1.1.1 追加插入法，在文件末尾附加数据是数字隐写术里最常用、最简单的方法，在前面的实验中，我们使用了 Windows 系统的 copy 命令将压缩文件追加进了图片，图片没有遭到损坏。我们来对具体情况进行分析，用 WinHex 工具打开文件 1.jpg。如图 1-1 所示

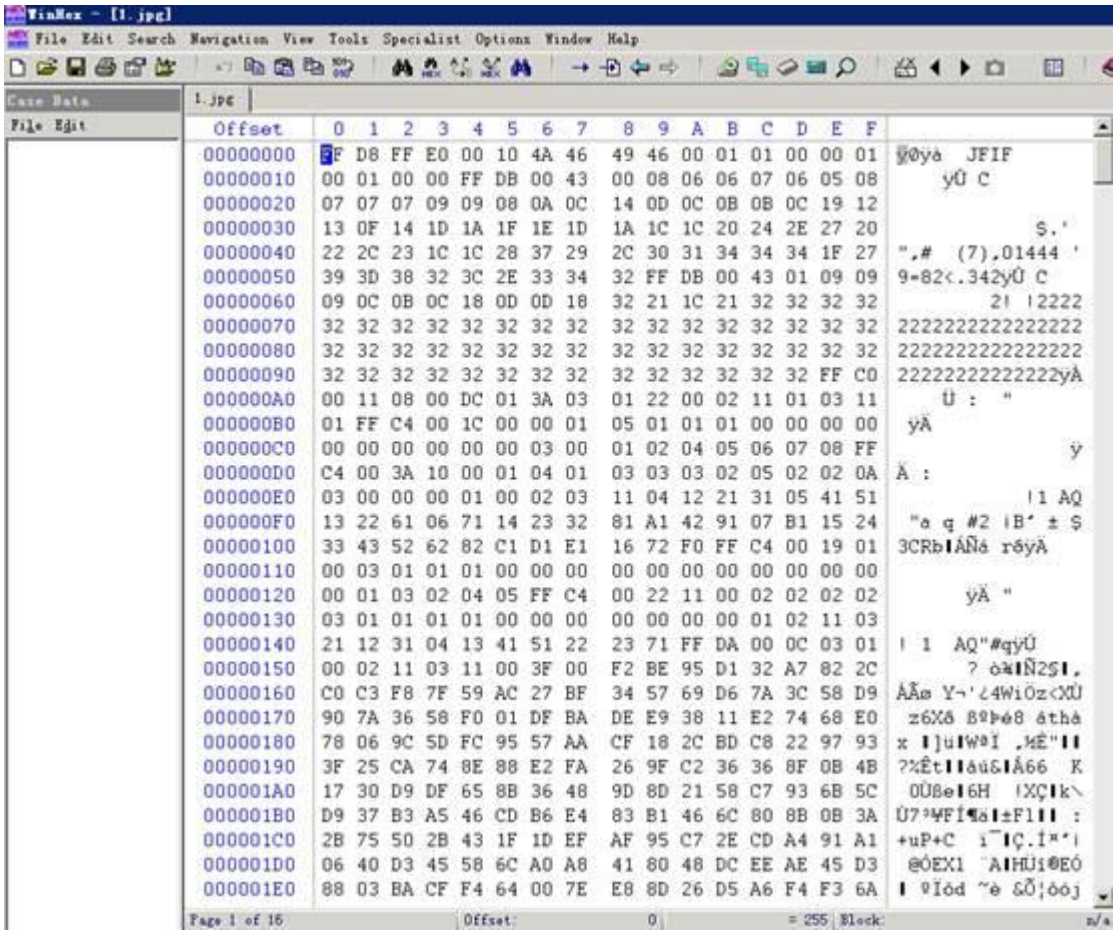


图 1-1

1.1.2 在程序界面中，左侧 Offset 一栏显示的是计数器和偏移量，中间一栏则是十六进制表示的文件数据，右侧一栏是以 ASCII 码格式表示的文件数据。在十六进制最底部可以看到 jpg 文件以“0xFF 0xD9”结尾。如图 1-2 所示

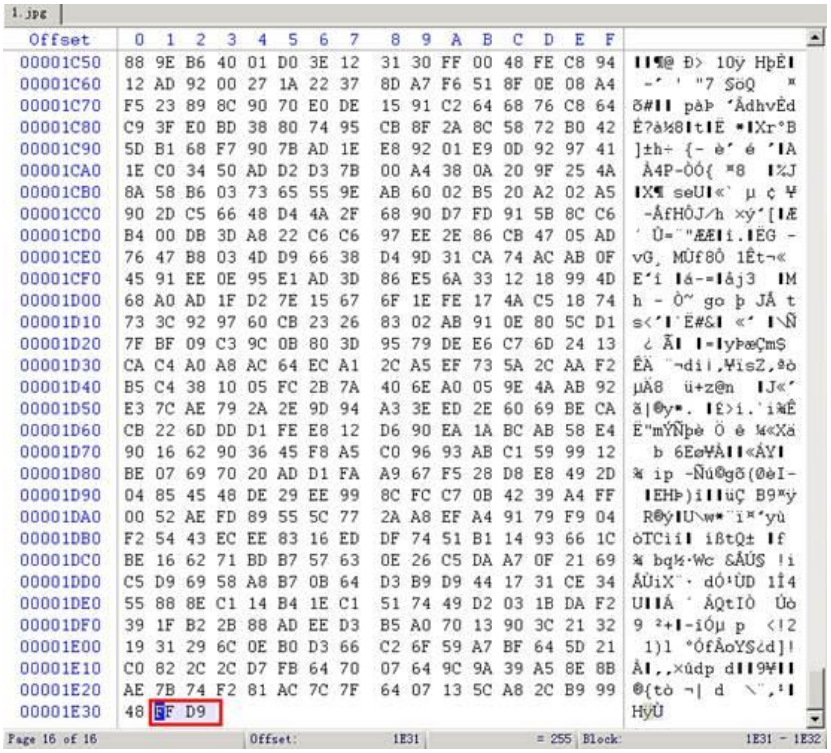


图 1-2

1.1.3 现在我们打开 2.jpg 查看其尾部数据，可以发现在文件结束符之后仍旧有一部分数据，相应的，ASCII 码部分的字样体现出了图中被追加的内容。如图 1-3 所示

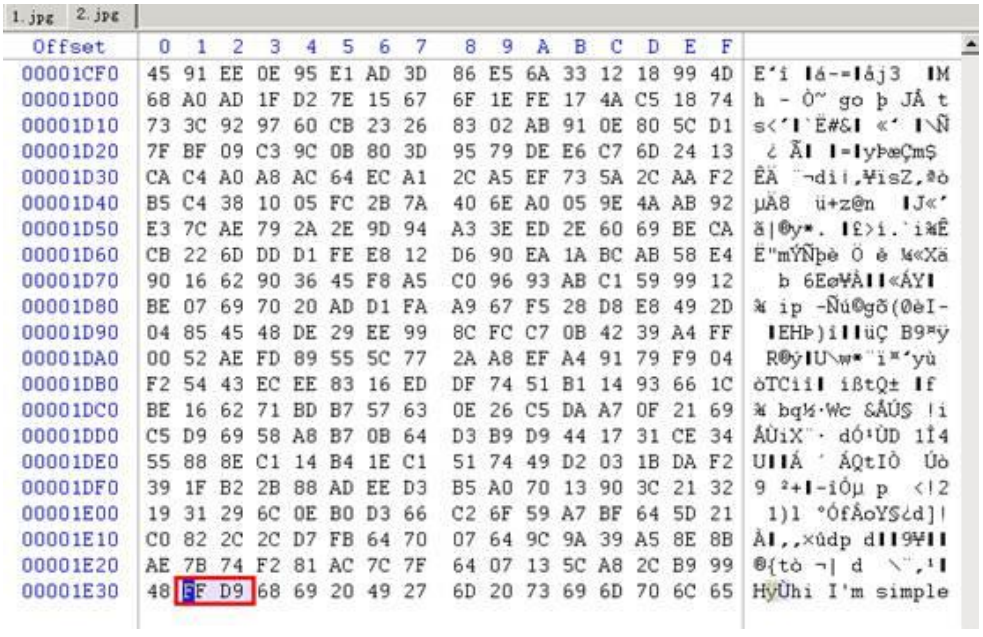


图 1-3

1.1.4 前置插入法，任何可以插入批注内容的文件都可能被插入数据而丝毫不影响视觉效果，例如，JPEG 文件最多可以在其中插入 65533 个字节的批注信息。JPEG 文件被文件标识符

分成不同的区域，每个标识符都以 0xFF 开头，这些标识符标识着文件的布局、格式和其他详细信息。批注区是数据隐藏的绝好位置，在 APP0 标识符的作用下，解码器（图像浏览器）无法识别的元数据都被忽略掉了。标识符详细信息如图 1-4 所示

标识符	值（十六进制）	大小（字节）	详细信息
SOI	FF D8	2	图像起始位置
APP0	FF E0	2	App标识符（文件详细信息）
SOF0	FF C0	2	框架起始位置（宽度、高度等）
SOS	FF DA	2	扫描起始位置
EOI	FF D9	2	图像结束位置/文件结束符（EOF）

图 1-4

1.2.修改方法

1.2.1 LSB，最低有效位修改法，利用的是 24 位调色板，调色板中有红、绿、蓝三原色。在一个图像的 24 位调色板中，每 8 位表示一个原色，也就是说红、绿、蓝分别有 256 个色调。在 LSB 修改法中，8 位颜色值的最后一位（最低有效位）由 1 改为 0，由 0 改为 1，或者保持不变，每个字节的最低有效位的组合表示插入的隐藏内容，如果是文本信息的话，这些最低有效位重新组合后，每 8 位代表一个 ASCII 字符。如图 1-5 所示

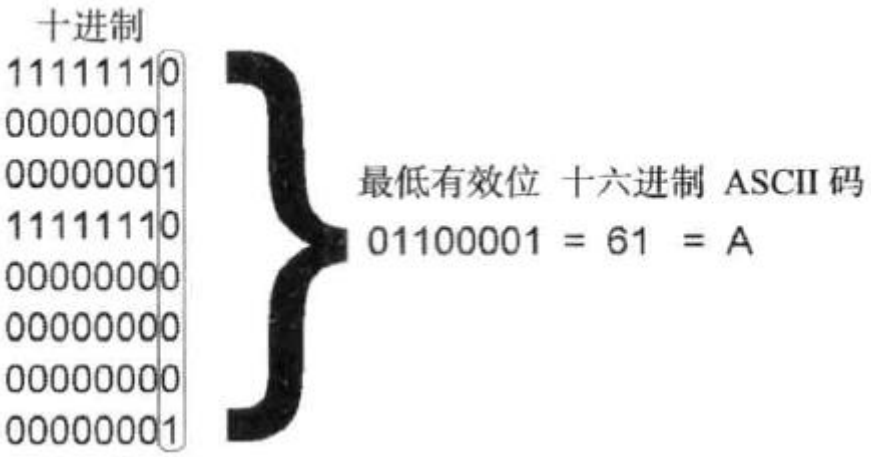


图 1-5

2.2 LSB 修改方法适用于 24 位的图像文件，例如 JPEG 文件和 24 位的 BMP 文件。

2、word 文档中隐藏数据

2.1.隐藏数据

2.1.1 在桌面打开 word 输入三行内容，以便进行对比。如图 2-1 所示

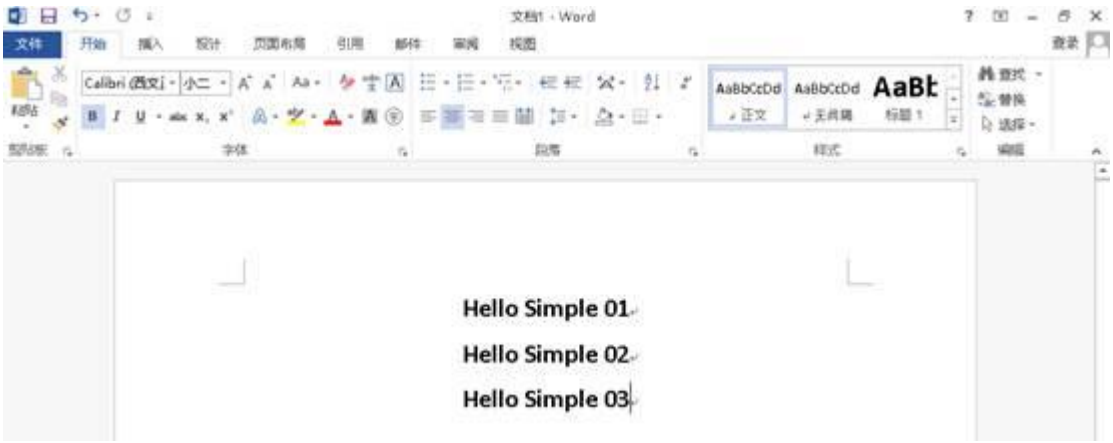


图 2-1

2.1.2 选中第二行的内容，右键单击选择“字体”，在弹出的设置界面的“效果”一栏会有一个复选框为“隐藏”，选中。如图 2-2 所示

图 2-2

2.1.3 点击“确定”，选中内容消失。如图 2-3 所示

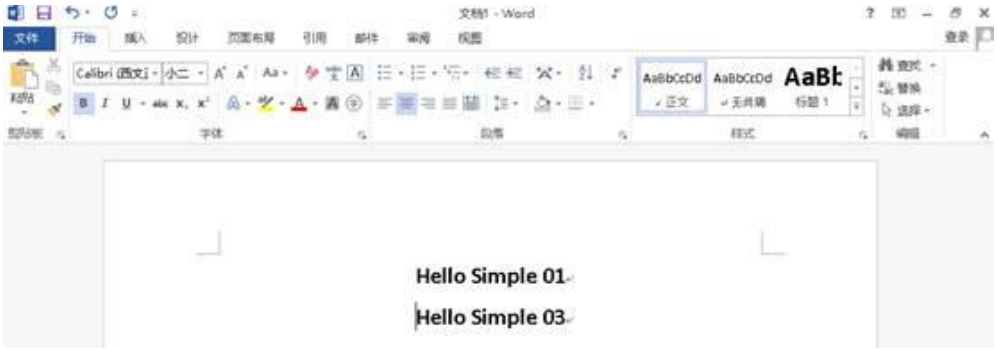


图 2-3

2.1.4 默认情况下，隐藏文本是不会被打印出来的，如果其他用户想知道文件中是否包含隐藏文本，可以单击“文件”->“选项”->“显示”，选中“隐藏文字”复选框（选中下方打印选项中的“打印隐藏文字”同样可以将隐藏内容打印出来）。如图 2-4 所示

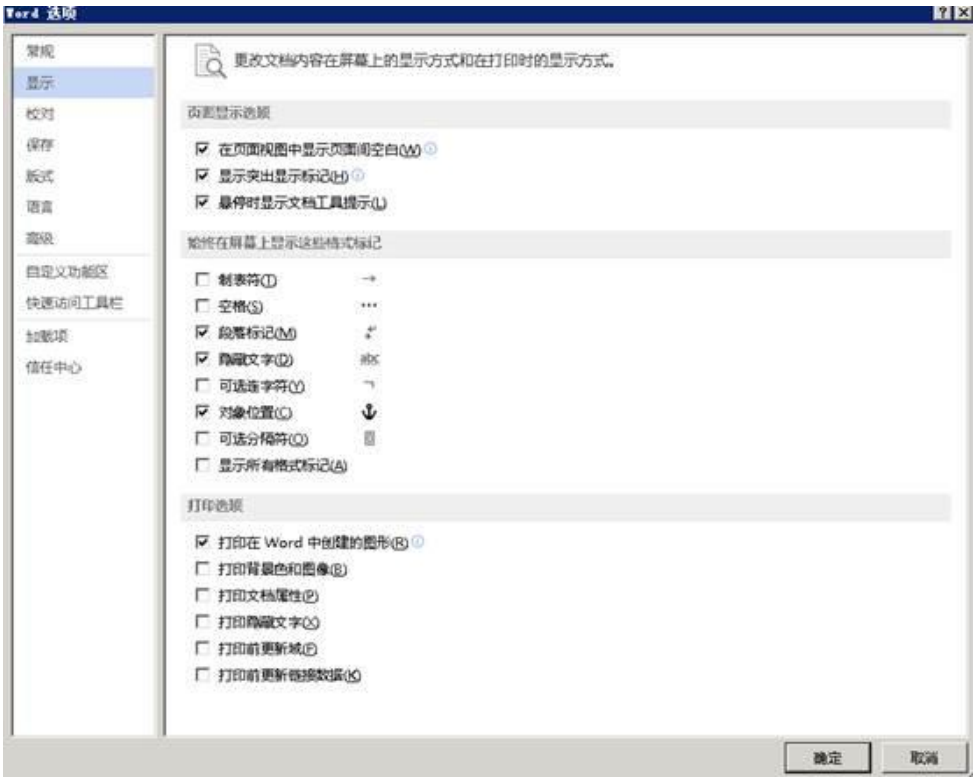


图 2-4

2.1.5 点击“确定”查看效果。如图 2-5 所示

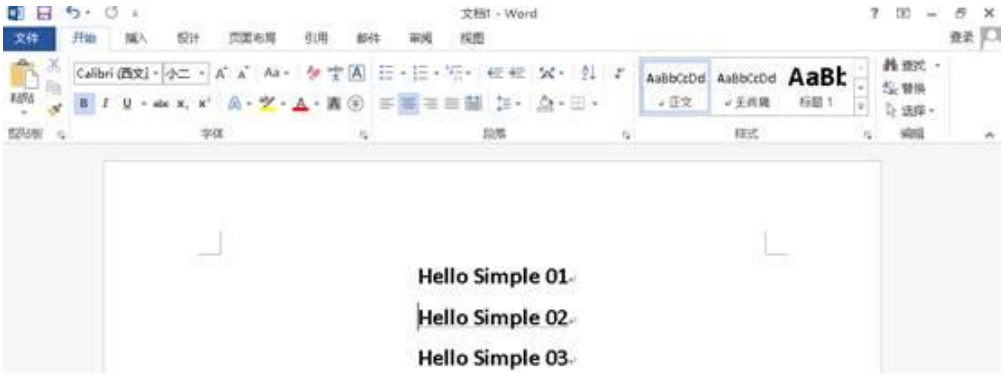


图 2-5

2.1.6 此外，还有一种方式可以发现文档中的隐藏文字。首先保存文件，点击“文件”->“信息”->“检查文档”。如图 2-6 所示

图 2-6

2.1.7 点击“检查文档”，在文档检查器中选中需要检测的内容。如图 2-7 所示

图 2-7

2.1.8 开始检查，发现内容。在最下面即可发现文档中具有隐藏文字，我们可以将其删除或用上述的方法来将它显示出来。如图 2-8 所示

图 2-8

2.1.9 还有一种隐藏方式便是，如果是在白色背景下使用白色字体，文档检查器是无法检查出来隐藏文字的，但是这种方式可以通过选定字段的方式发现。其他的隐藏位置诸如文档属性的摘要部分，自定义标签下。如图 2-9 所示

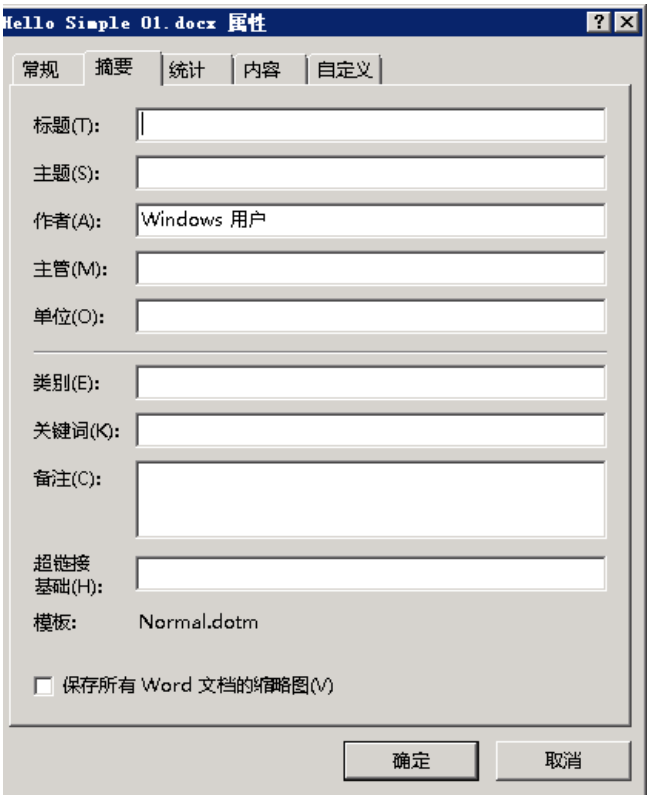


图 2-9

2.1.10 在自定义标签中添加的内容是不会显示在属性的主视图中的,必须打开该标签才可以看到此类高级属性

3、密钥穷举

3.1、DES 加密

3.1.1 编辑框

输入密钥：输入用于加密的十六进制密钥（16 位）

输入明文：输入明文串

对应密文：DES 加密后的密文，十六进制（16 位）

3.1.2 按钮

加密：DES 加密

导出明文：导出明文文件 cleartext.txt 到程序所在文件路径

导出密文：导出密文文件 cipher.txt 到程序所在文件路径

3.1.3 操作流程

输入密钥-输入明文-点击加密-得到密文-导出明文-导出密文

运行【CryptographyLab.exe】打开界面。如图 3-1 所示

图 3-1

DES 加密。输入 16 位密钥：1234567af1234567，输入明文：nihao，点击加密，可得到密文：df73fb877256e45d。如图 3-2 所示

图 3-2

点击导出明文和导出密文，在程序所在目录生成 ciphertext.txt 和 cleartext.txt，分别用于存放明文和密文。如图 3-3 所示

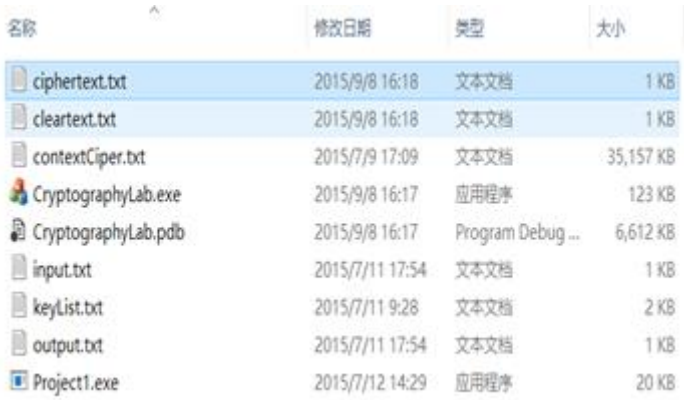


图 3-3

3.2、穷举攻击

3.2.1 编辑框

导入明文：从之前 DES 加密导出的明文文件中导入明文

导入密文：从之前 DES 加密导出的密文文件中导入密文

密钥范围：从低到高，十六进制，16 位

对应密钥：穷举攻击破解出的密钥，十六进制，16 位

3.2.2 按钮

导入明文

导入密文

开始破解

显示密钥

3.2.3 操作流程

导入明文-导入密文-输入密钥范围-开始破解-得到密钥

流程如下所示：

重新打开 CryptographyLab.exe，选择穷举攻击，点击导入明文，导入密文，分别从 ciphertext.txt 和 cleartext.txt 文件中导入明文和密文，输入密钥范围 1234567af1234565 和 1234567af1234569。如图 3-4 所示

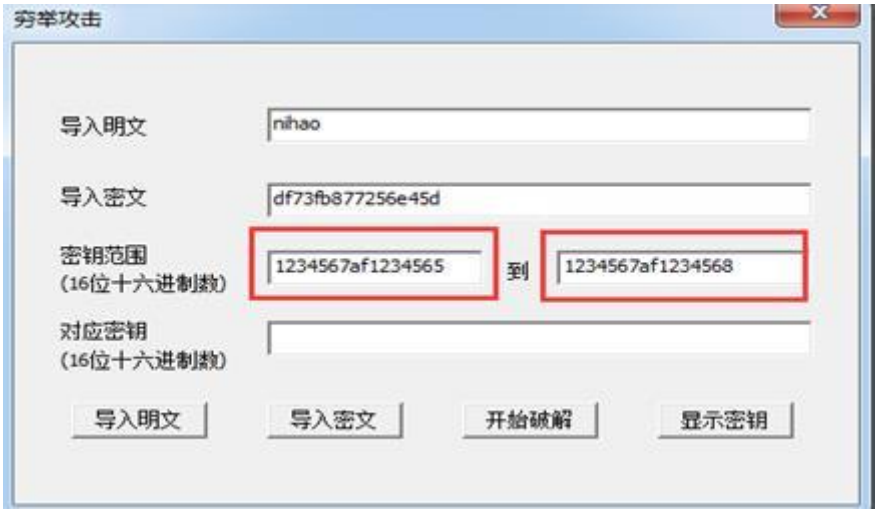


图 3-4

点击开始破解，相关输入数据存入程序目录下 input.txt 文件，弹出运行界面展示破解过程。如图 3-5 所示

图 3-5

运行完后，将找到的密钥存入 output.txt，回到穷举攻击界面，点击显示密钥按钮，将密钥显示出来。如图 3-6 所示

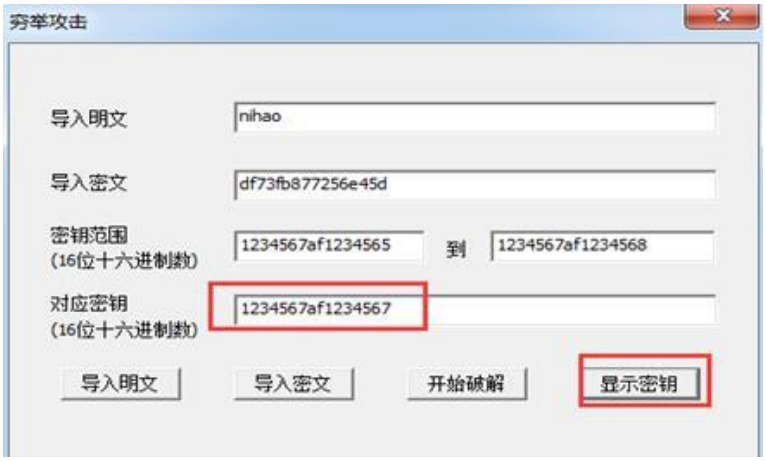


图 3-6

3.3、字典攻击

3.3.1 编辑框

输入对数：输入密文明文对数，最大为 100000

输入密钥：输入固定的密钥，十六进制，16 位

密文明文对：每页显示 5 对

输入密文：从密文明文对中选择密文

对应明文：查找到的明文，十六进制，16 位

3.3.2 按钮

修改：修改密文明文对数

生成明文密文对文件：生成的 contextCiper.txt 存放到程序所在文件路径

上一页

下一页

字典攻击

3.3.3 操作流程

输入对数-输入密钥-生成明文密文对文件-输入密文-点击字典攻击-得到对应明文

重新打开 CryptographyLab.exe，选择字典攻击，输入对数 50，点击修改。如图 3-7 所示

图 3-7

输入密钥 1234567af1234567，点击生成明文密文对文件，生成 50 对明密文对。如图 3-8 所示

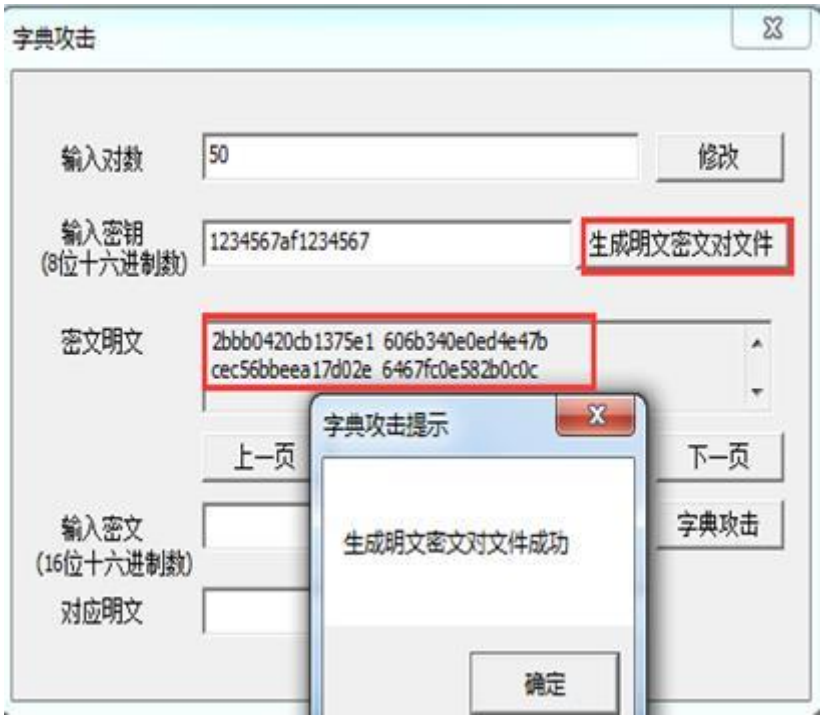


图 3-8

从生成的密文明文对中选一个密文，比如输入密文 2bbb0420cb1375e1，点击字典攻击，则找到对应明文 606b340e0ed4e47b。如图 3-9 所示

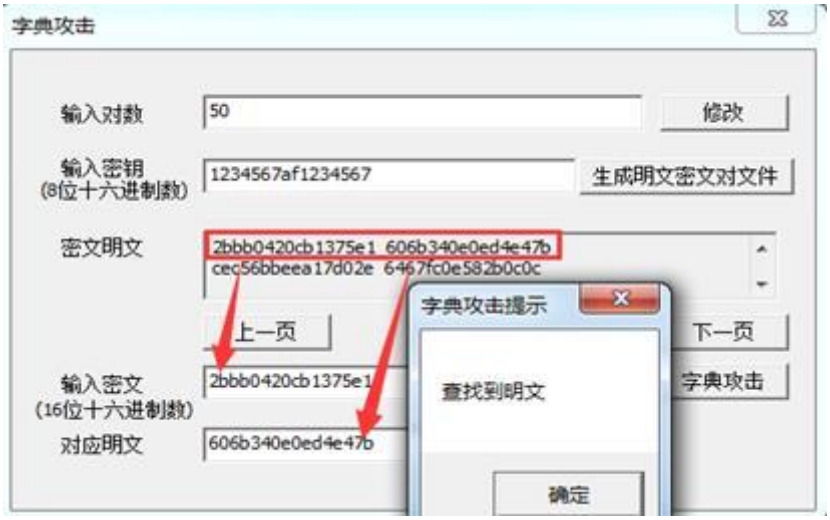


图 3-9

3.4、查找攻击

3.4.1 编辑框

输入对数：输入密文明文对数，最大为 100000

输入明文：输入明文串

密钥密文对：生成随机的密钥密文对

输入密文：从密钥密文对中选择密文

对应密钥：查找到的密钥，十六进制，16 位

3.4.2 按钮

修改：修改密钥密文对数

生成对照表：生成密钥密文对照表，存放到程序所在文件路径 keyList.txt

上一页

下一页

查找攻击：开始进行查找攻击

3.4.3 操作流程

输入对数-输入明文-生成密钥密文对-输入密文-点击查找攻击-得到对应密钥

重新打开 CryptographyLab.exe,选择查找攻击，输入对数 30，点击修改。如图 3-10 所示

图 3-10

输入明文 12345678，点击生成对照表。如图 3-11 所示

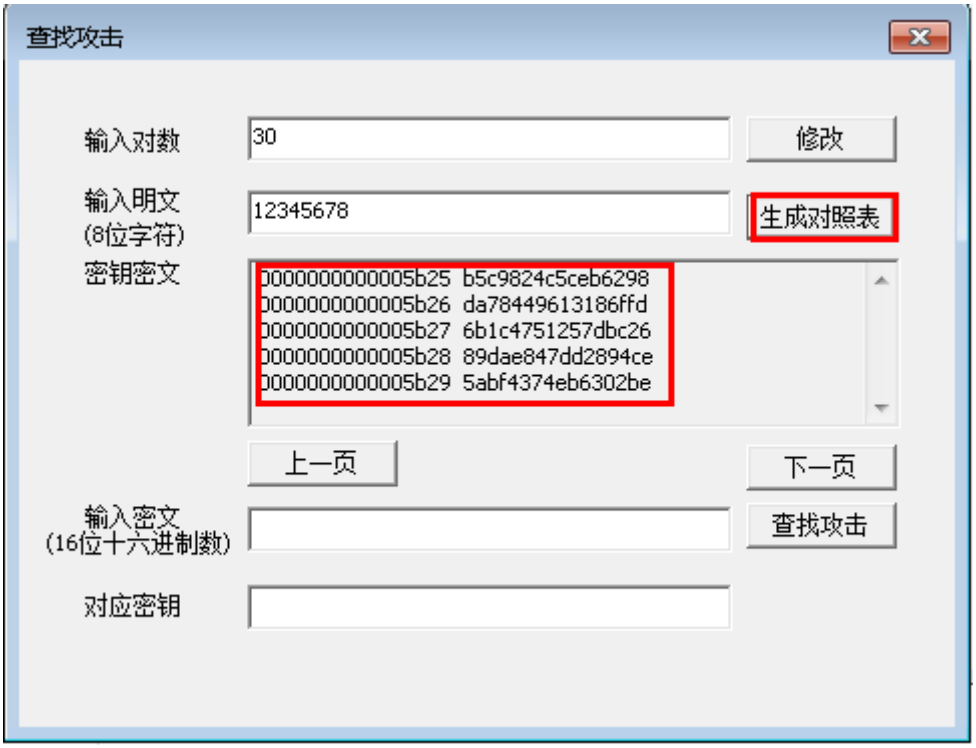


图 3-11

输入密文 b5c9824c5ceb6298，点击查找攻击，成功找到密钥 0000000000005b25。如图 3-12 所示

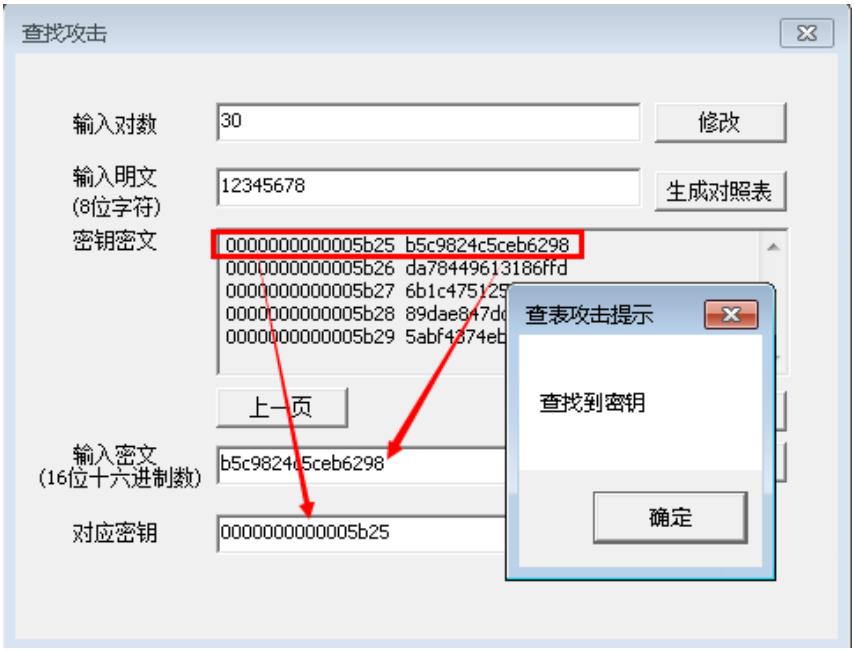


图 3-12

4、利用 arp 协议缺陷实现中间人攻击

4.1.利用 cain 进行 arp 欺骗

4.1.1 切换到 ip 为 192.168.1.2 的服务器中，选择单击桌面【tools】目录下的【利用 arp 协议缺陷实现中间人嗅探网络明文】文件中的【cain4.9\cain\cain.exe】，启动 cain 软件，会有一些提示，可以忽略这些提示。如图 4-1 所示

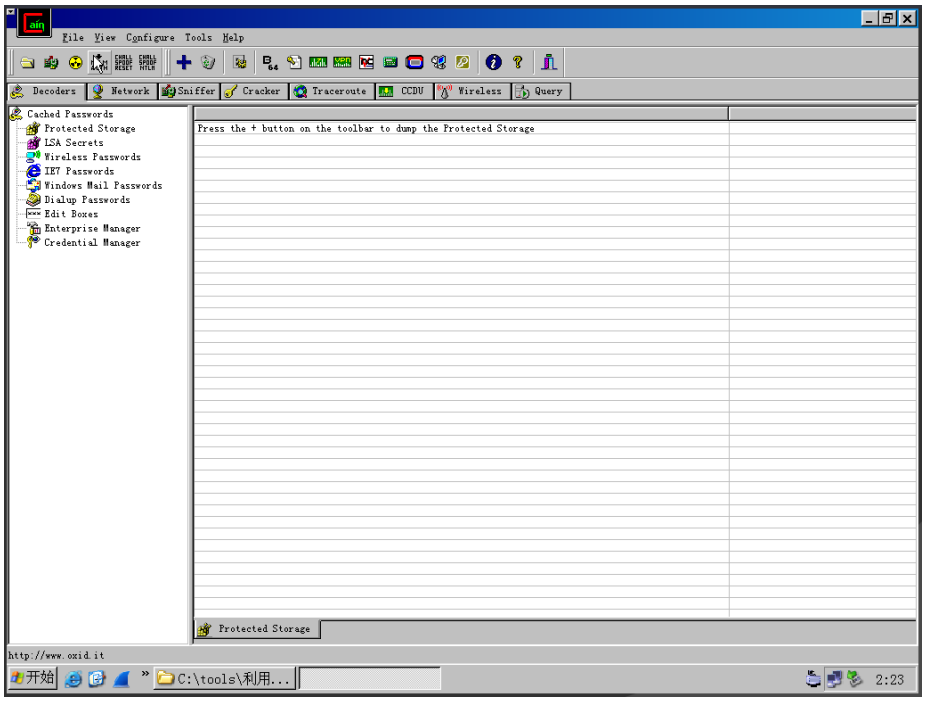


图 4-1

4.1.2 单击菜单栏中的“configure”，选择 192.168.1.2 网卡，单击“确定”按钮。如图 4-2 所示

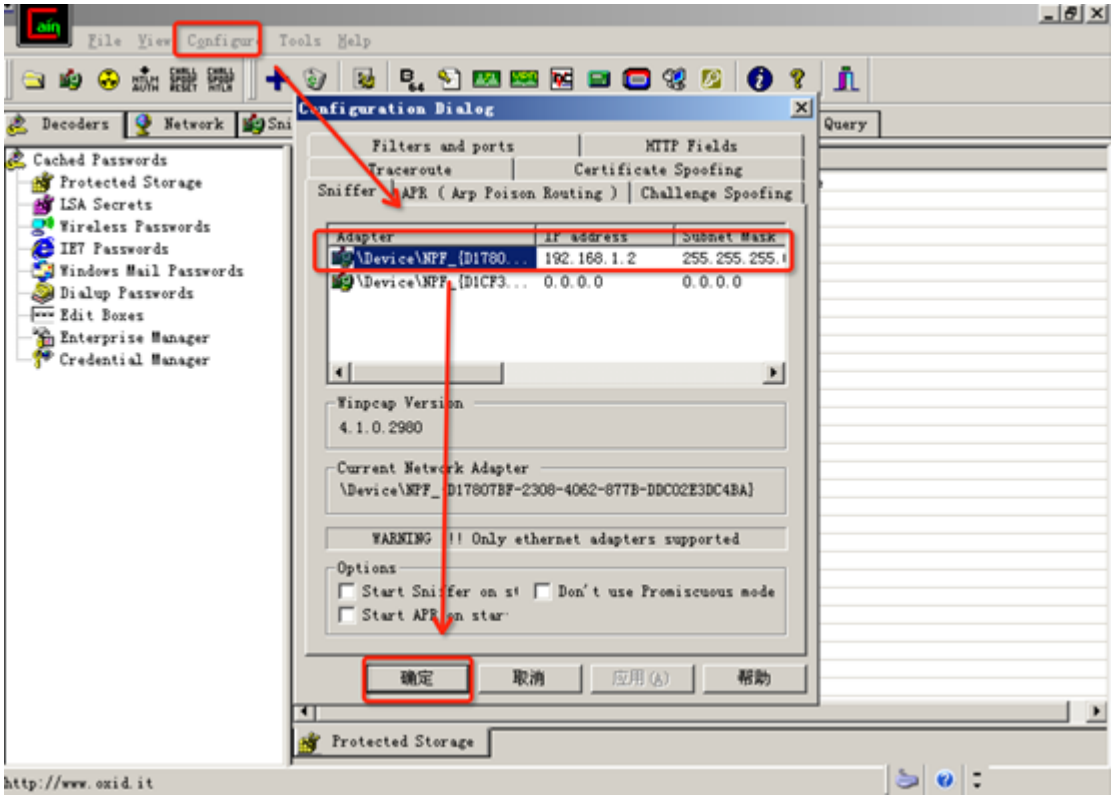


图 4-2

4.1.3 选择好网卡之后，单击 start/stopsniffer 光标开启 sniffer 功能，进入 sniffer 选项卡，选择下方的 hosts 选项，单击空白处，选择 scanmacaddress，进入扫描。如图 4-3 所示

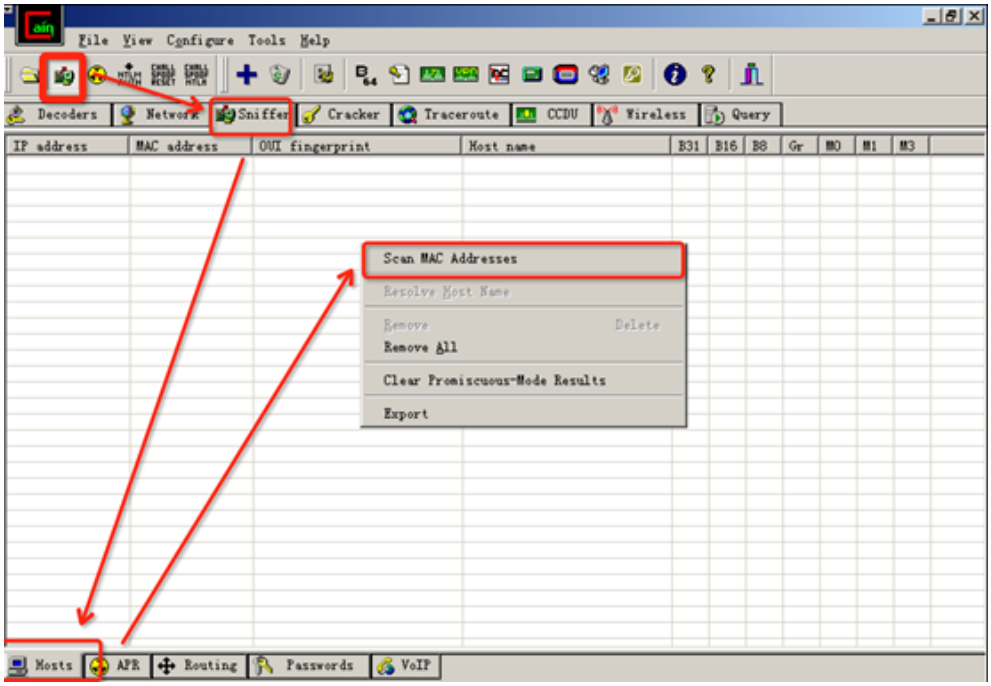


图 4-3

4.1.4 选择了 scanmacaddress 后，选择扫描的网段，选择 allhostsinmysubnet。单击 ok，进行扫描。如图 4-4 所示

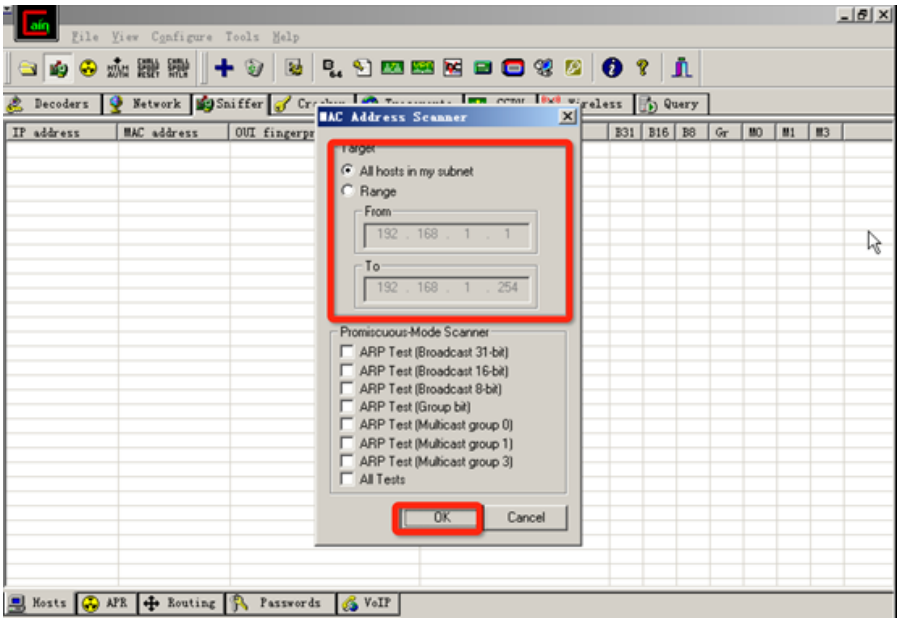


图 4-4

4.1.5 将本网段除了本机外的其他机器全部扫描出来了。可以看到 192.168.1.4 和 192.168.1.3 两个 ip 地址。如果扫出其他 ip 地址，将其删除。只留下（192.168.1.3）和（192.168.1.4）两个 ip 及其 mac 地址。如图 4-5 所示

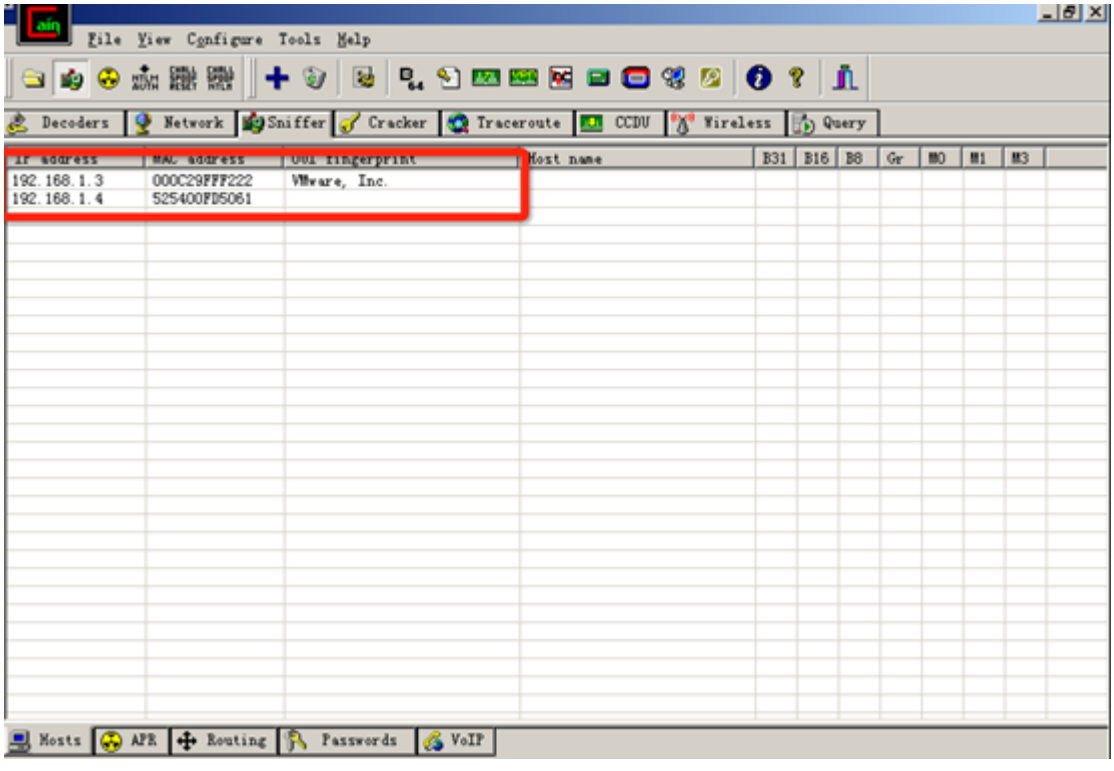


图 4-5

4.1.6 单击左下角“APR”标签，然后单击软件空白处，激活菜工具栏中的“+”按钮，然后单击“+”按钮。如图 32 所示

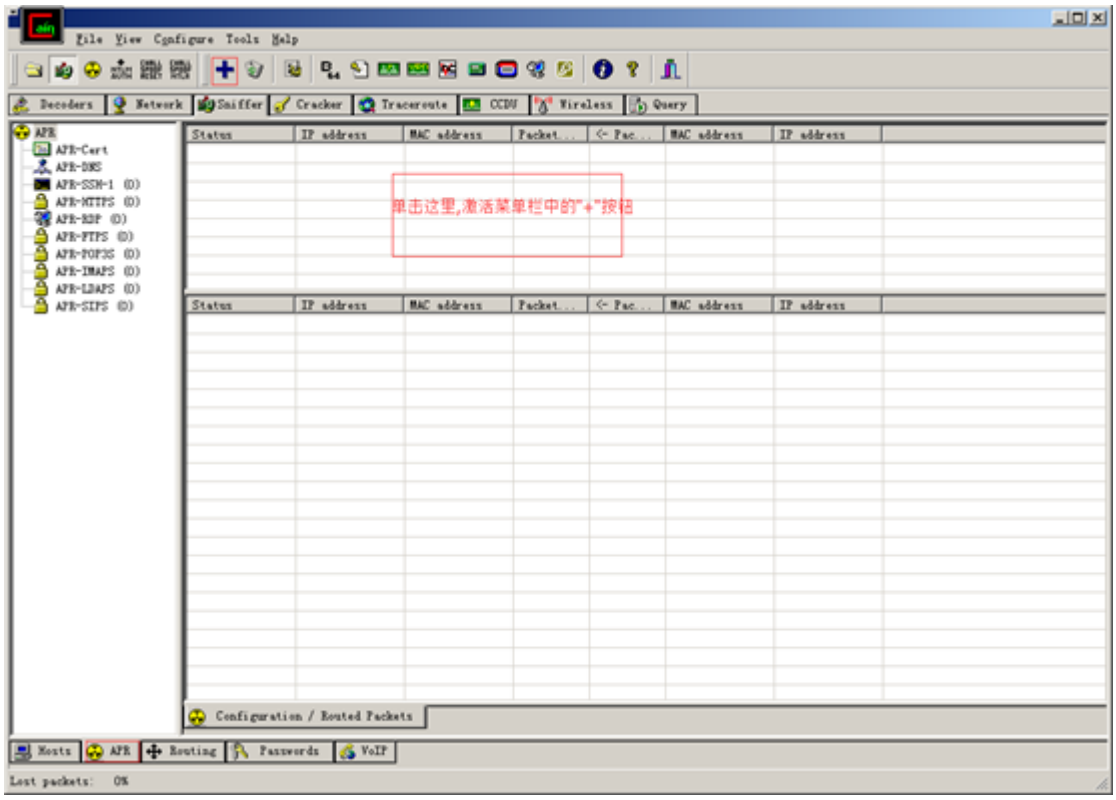


图 4-6

4.1.7 扫描出 mac 地址后，选择下方的 arp 选项，进入 arp 选项页面。单击（+）添加目标地址 192.168.1.4，选中 192.168.1.4 条目。单击 ok。如图 4-7 所示

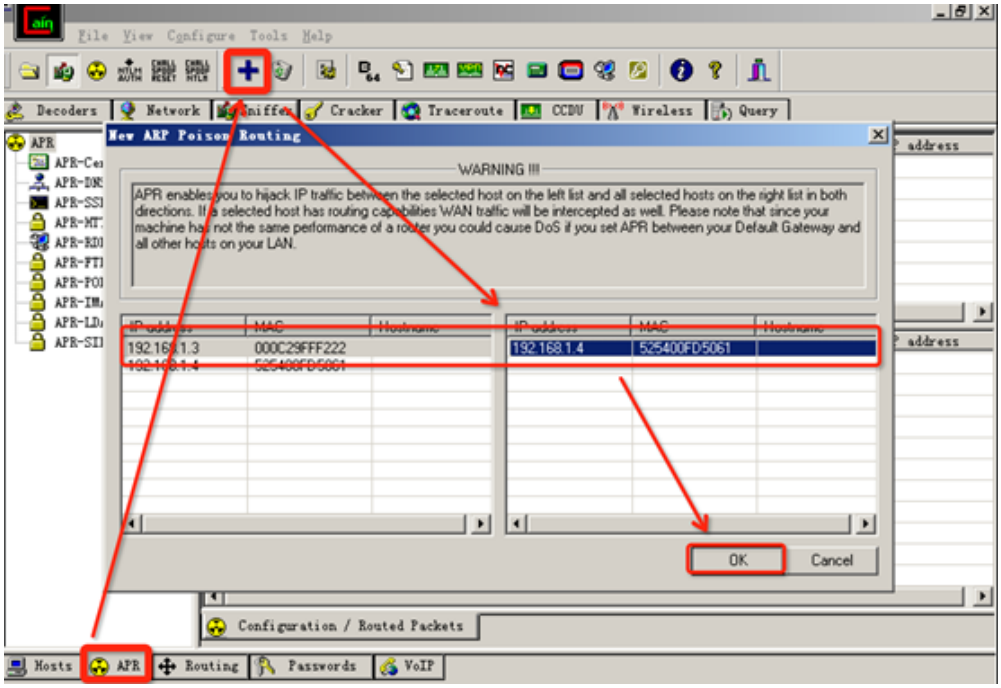


图 4-7

4.1.8 在 cmd 命令行模式下，使用 arp-a 命令查看本地缓冲中的项目。分别在（192.168.1.3）和（192.168.1.4）两台机器上查看。如果没有出现，有些条目没有出现，可以切换到对应的系统使用 ping 命令去 ping 对方的 ip 地址。再使用 arp-a 就可以了。同时由于 mac 地址是唯一的。实验中的 mac 地址与文档中的截图中 mac 地址不一致，是正常的。如图 4-8、图 4-9 所示

```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.3 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.1.2           52-54-00-b9-b8-62     dynamic
  192.168.1.4           52-54-00-fd-50-61     dynamic
```

图 4-8

```
C:\Documents and Settings\Administrator>arp -a

Interface: 192.168.1.4 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.1.2           52-54-00-b9-b8-62     dynamic
  192.168.1.3           00-0c-29-ff-f2-22     dynamic
```

图 4-9

4.1.9 选择好目标后，单击（start/stopapr）按钮开启 arp。如图 4-10 所示

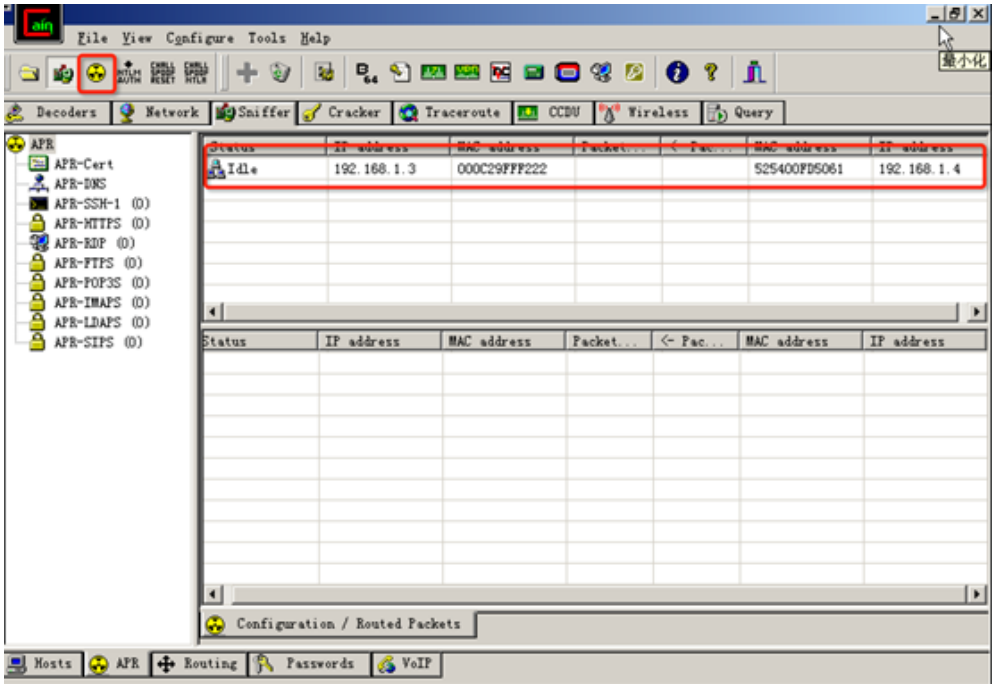


图 4-10

4.1.10 开启 arp 后，再分别进入 192.168.1.3 和 192.168.1.4 的 cmd 中，使用 arp-a 命令查看。发现查看到的 192.168.1.3 和 192.168.1.4 的 MAC 地址发生了改变，其 MAC 地址变得与 192.168.1.2 的 MAC 地址一样，说明 arp 欺骗已经成功。如图 4-11、图 4-12 所示

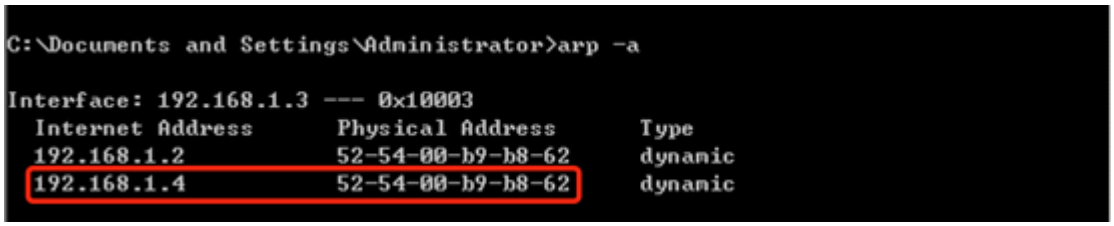


图 4-11

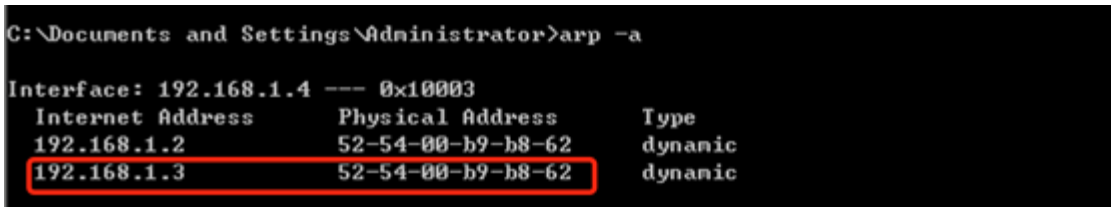


图 4-12

4.2.利用 cain 抓取 ftp 密码

4.2.1 切换到（192.168.1.3）系统中，使用资源管理器连接在 192.168.1.4 上搭建的 ftp 服务器（打开任意一个文件夹，在地址栏输入 ftp://192.168.1.4）。输入正确的账户名密码（administrator/Simplexue123），单击登录。如图 4-13 所示

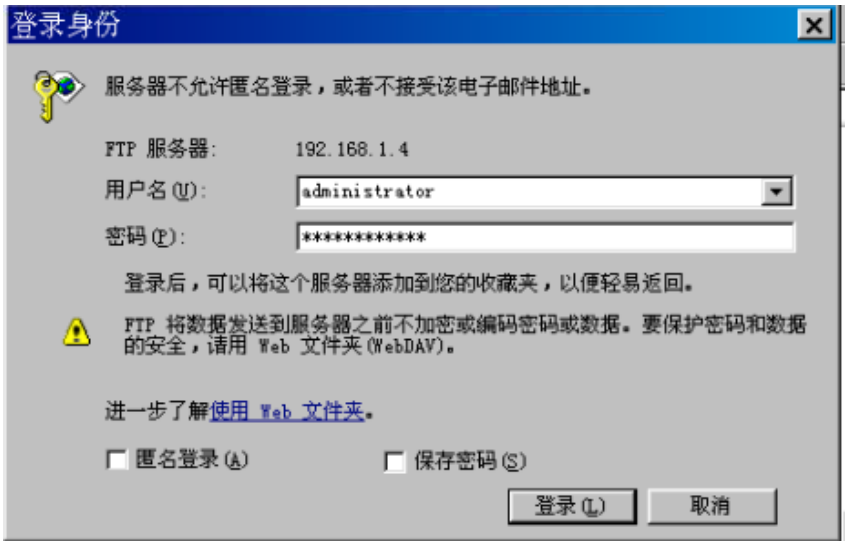


图 4-13

4.2.2 输入正确的用户名密码之后，即可进入 ftp 服务器中。再次切换到（192.168.1.2）系统中。选择 cain 下方的 passwords 选项页面。选择左侧的 FTP 选项。即可看到刚刚在进入 ftp 时输入的 ftp 账户名和密码。如图 4-14 所示

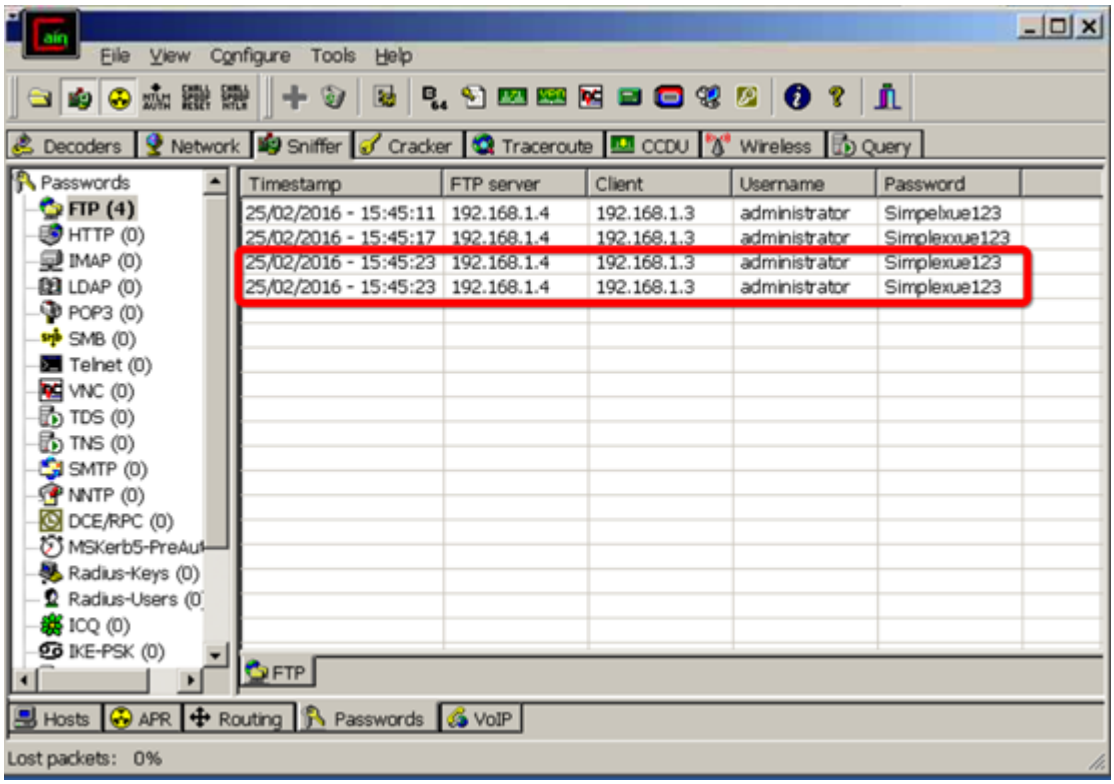


图 4-14

4.3.利用 cain 进行 dns 欺骗

3.1 在 192.168.1.4 中搭建了 dns 服务器。添加了纪录 www.shiyanbar.com，对应的解析 ip 为 192.168.100.100(此步骤已经完成，可跳过)。如图 4-15 所示

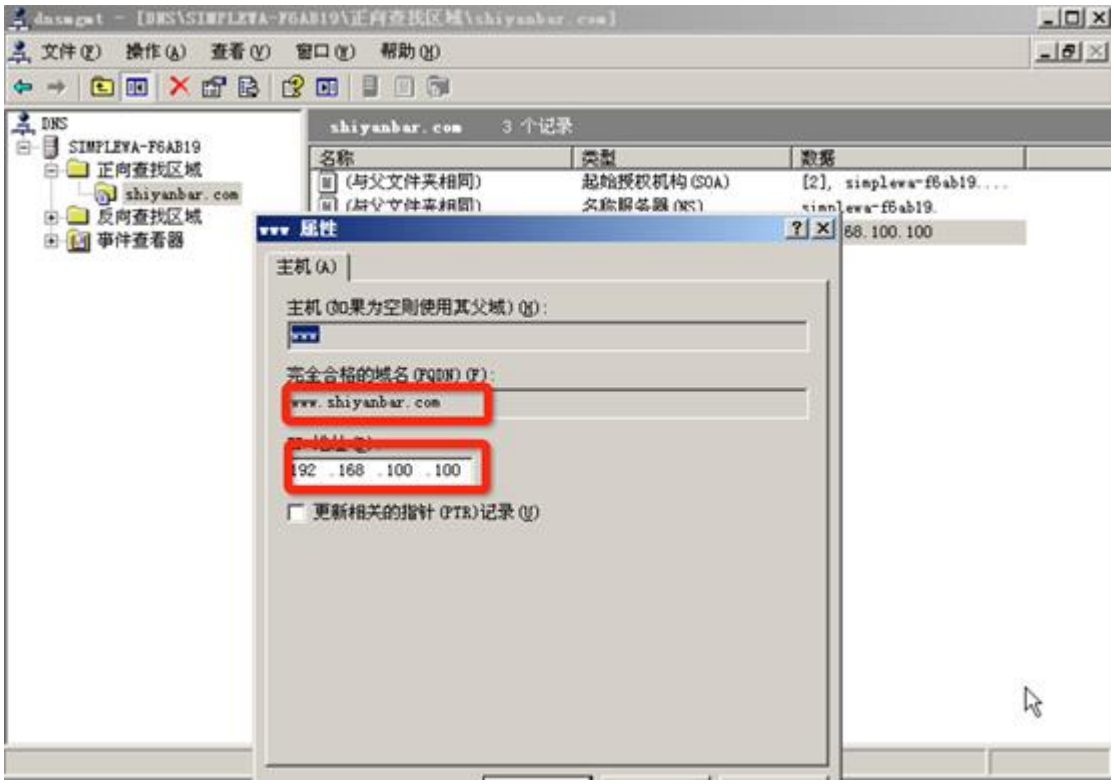


图 4-15

4.3.2 由于环境限制，需要自行指定 dns。在 192.168.1.3 和 192.168.1.4 上都需要进行指定。

将 dns 地址指向 192.168.1.4（若是弹出窗口警告选择“否”即可）。如图 4-16 所示

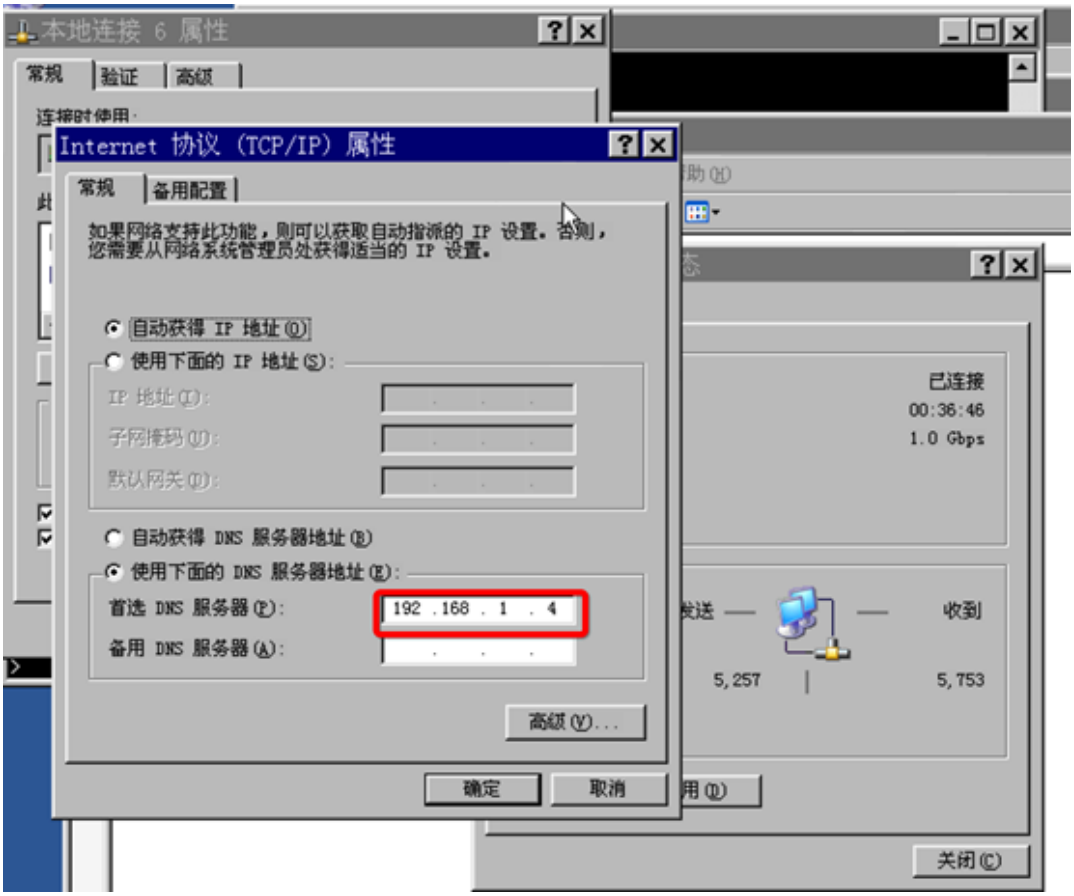


图 4-16

4.3.3 首先切换到 192.168.1.2 中进入 cain，单击（start/stoparp）按钮关闭 arp。在切换到 192.168.1.3 中，进入 cmd 命令行使用 nslookup 查询。如图 4-17 所示

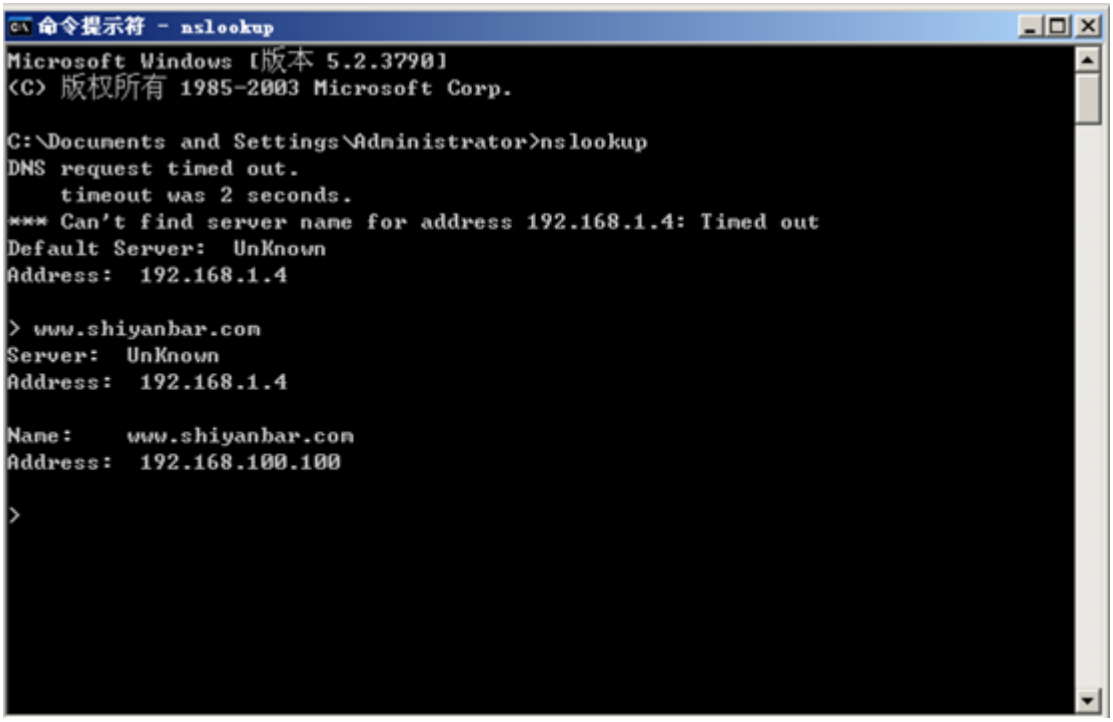


图 4-17

从上图可以看出，成功的解析出的域名所对应的 ip 地址为 192.168.100.100。

4.3.4 切换到 192.168.1.2 中，进入 cain 软件中，选择下方的 apr 页面，选择左侧的 APR-DNS 选项。在单击上方的（+）添加一个目标，将网址解析的 ip 改为 1.1.1.1，单击 ok。单击（start/stopapr）按钮开启 arp。如图 4-18 所示

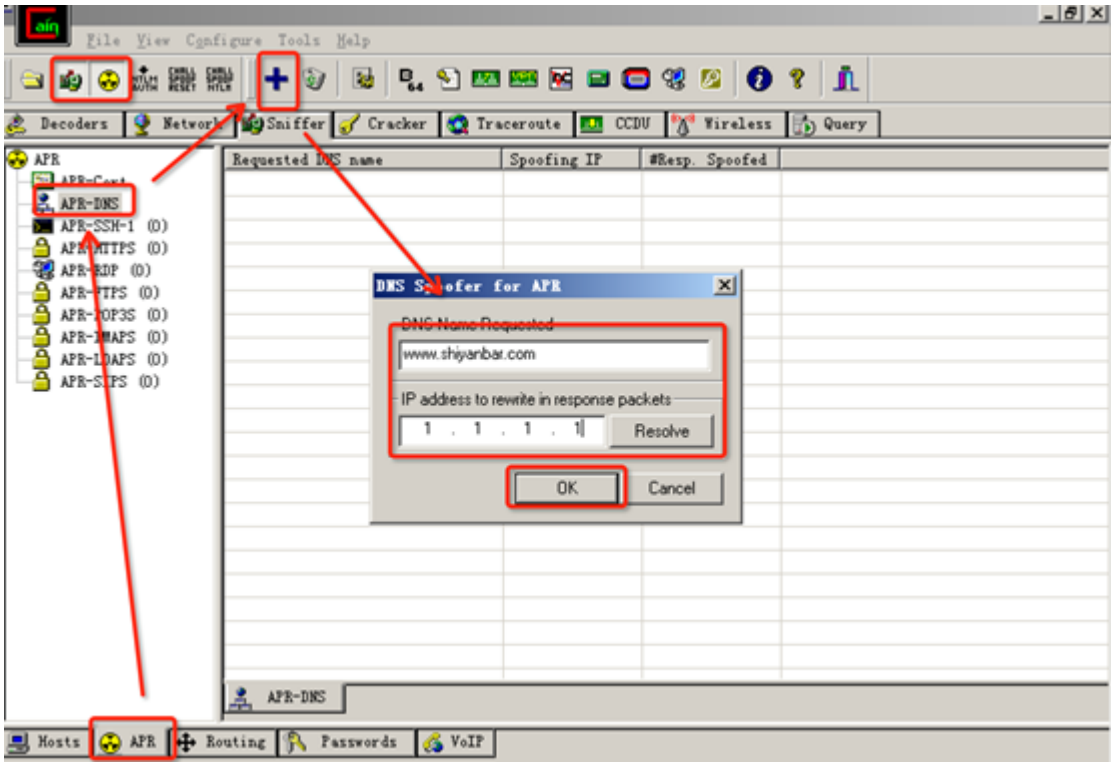


图 4-18

4.3.5 单击 ok 后页面可以看到刚刚设置的解析。如图 4-19 所示

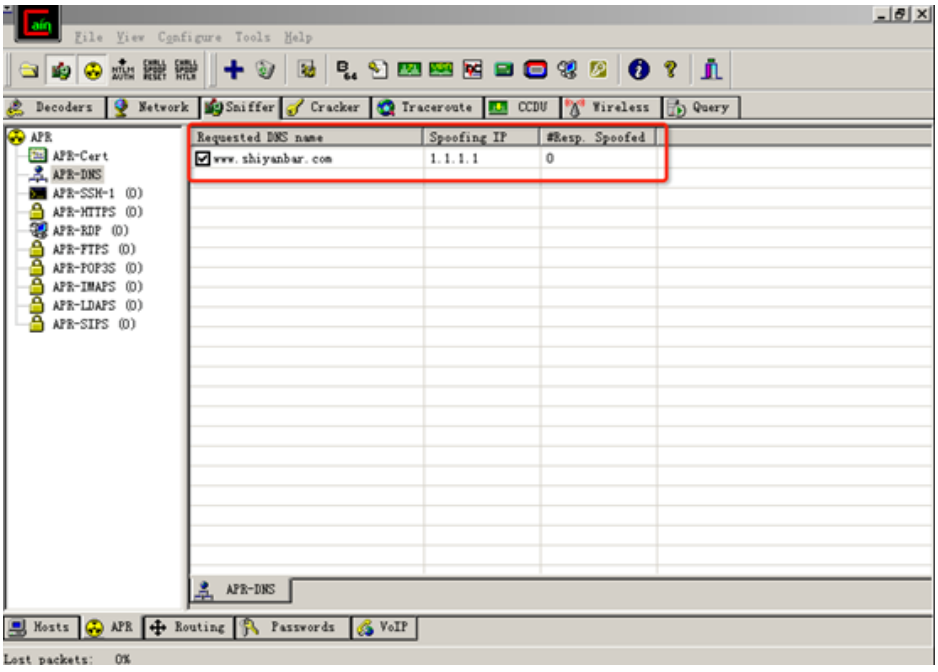


图 4-19

4.3.6 切换到 192.168.1.3 的 cmd 命令行模式中，再次查询。如图 4-20 所示

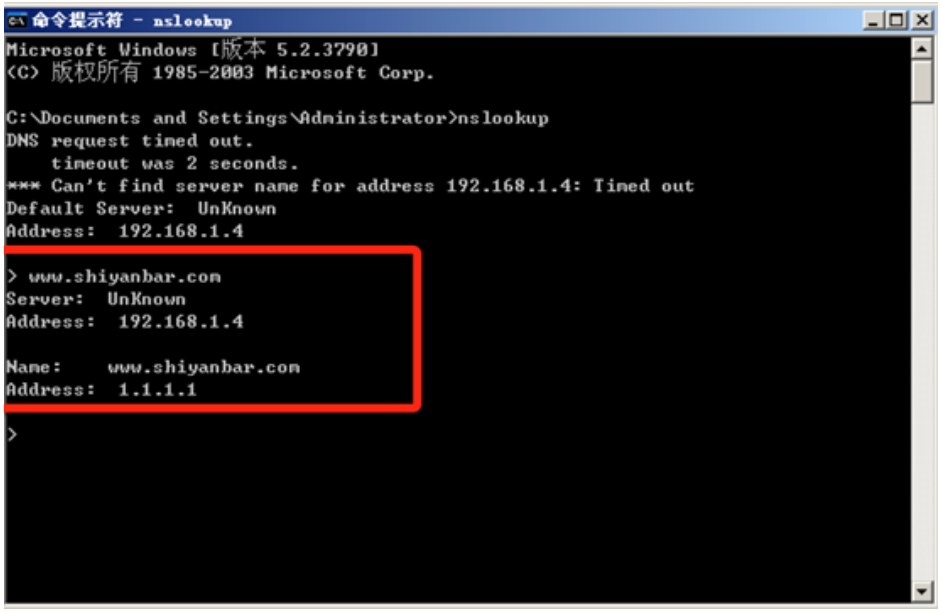


图 4-20

4.3.7 从图 19 中可以看出，www.shiyanbar.com 的 dns 解析已经被改变成为设定的 1.1.1.1，成功地做到了 dns 欺骗。

附录：学生实验报告要求

实验报告参考模板如下：

实验报告封面

实验报告

题目： _____

学　院：信息学院

专　业：

班　级：

学　号：

姓　名：

年　　月　　日

一、实验目的

标题一、实验目的（宋体四号加粗）

正文（正文 宋体小四，1.5 倍行距）

二、实验环境

三、实验内容

四、实验步骤

（图文方式叙述）

五、实验结果及分析

（遇到的问题与解决）

六、实验体会