

《信息安全技术》实验指导

作者：TX

2021年 2月 18日

<http://tang.chat>

目录

1 数据加密解密技术	1
1.1 实验名称	1
1.2 实验目的	1
1.3 实验原理	1
1.4 实验材料	1
1.5 实验步骤	1
1.6 实验记录	2
1.6.1 安装openssl密码工具软件	2
1.6.2 创建测试文件	3
1.6.3 使用AES算法加密测试文件	4
1.6.4 使用AES算法解密测试文件	5
1.6.5 使用RSA算法生成公钥私钥	5
1.6.6 使用RSA公钥加密测试文件	7
1.6.7 使用RSA私钥解密测试文件	8
1.7 问题回答	9
2 网络监听嗅探技术	11
2.1 实验名称	11
2.2 实验目的	11
2.3 实验原理	11
2.4 实验材料	11
2.5 实验步骤	11
2.6 实验记录	12
2.6.1 安装Wireshark	12
2.6.2 使用Wireshark分析ICMP协议	14
2.7 问题回答	17
3 入侵检测监控技术	19
3.1 实验名称	19
3.2 实验目的	19

3.3	实验原理	19
3.4	实验材料	19
3.5	实验步骤	19
3.6	实验记录	20
3.6.1	安装Snort	20
3.6.2	使用Snort嗅探模式	21
3.6.3	使用Snort日志模式	25
3.6.4	使用Snort入侵检测模式	26
3.7	问题回答	28
4	系统安全配置技术	29
4.1	实验名称	29
4.2	实验目的	29
4.3	实验原理	29
4.4	实验材料	29
4.5	实验步骤	29
4.6	实验记录	30
4.6.1	Windows安全基线文档	30
4.6.2	本地组策略编辑器	30
4.6.3	配置策略	31
4.7	问题回答	42
5	数据备份恢复技术	43
5.1	实验名称	43
5.2	实验目的	43
5.3	实验原理	43
5.4	实验材料	43
5.5	实验步骤	43
5.6	实验记录	44
5.6.1	安装Rsync	44
5.6.2	使用Rsync	44
5.7	问题回答	51
6	软件破解保护技术	53
6.1	实验名称	53
6.2	实验目的	53
6.3	实验原理	53
6.4	实验材料	53
6.5	实验步骤	54

6.6 实验记录	54
6.6.1 准备测试环境	54
6.6.2 使用PEiD分析测试程序	56
6.6.3 使用UPX脱壳测试程序	56
6.6.4 使用Ollydbg调试测试程序	58
6.7 问题回答	61
参考文献	63

<http://tang.chat>

§ 1

数据加密解密技术

1.1 实验名称

数据加密解密技术

1.2 实验目的

1. 了解对称密码体制、非对称密码体制概念和原理;
2. 熟悉常见加密解密方法特性;
3. 掌握加密解密工具的使用方法。

1.3 实验原理

从密钥生成和使用策略上，密码体制主要分为对称密码体制和非对称密码体制。对称密码体制加密和解密过程中使用相同的密钥，非对称密码体制则使用不同的密钥。

1.4 实验材料

1. 运行Windows XP或更高版本操作系统的PC机一台;
2. OpenSSLv1.1.0i或更高版本软件压缩包。

1.5 实验步骤

1. 安装openssl密码工具软件
2. 创建测试文件
3. 使用AES算法加密测试文件
4. 使用AES算法解密测试文件
5. 使用RSA算法生成公钥私钥

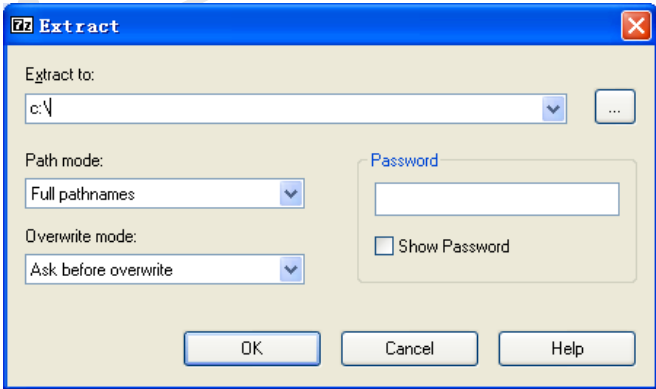
- 6. 使用RSA公钥加密测试文件
- 7. 使用RSA私钥解密测试文件

1.6 实验记录

1.6.1 安装openssl密码工具软件

将openssl压缩包释放到C:
，如图1-1所示。

图 1-1: openssl下载



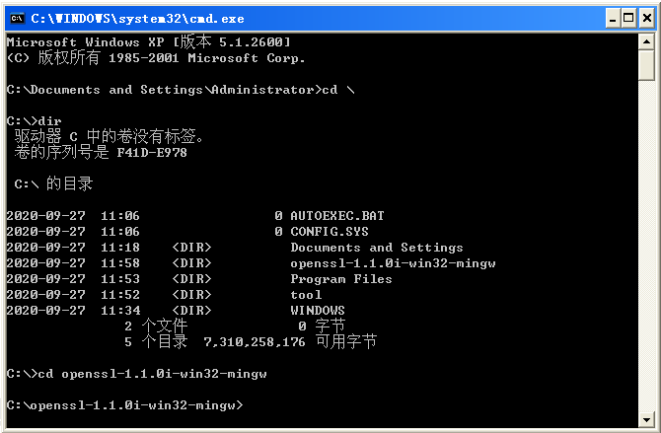
运行“cmd”程序，进入命令行，如图1-2所示。

图 1-2: 进入命令行



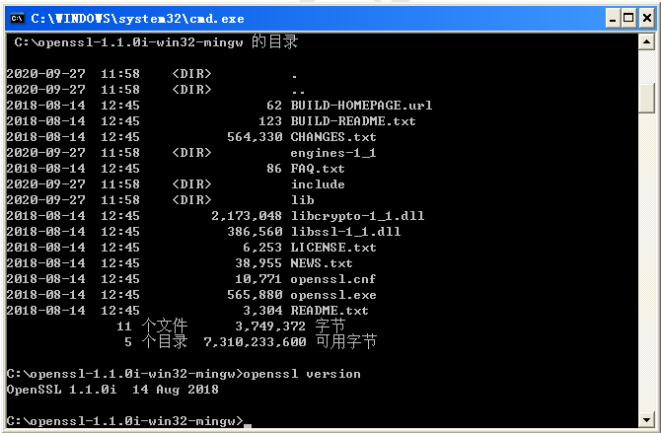
使用“cd”命令进入openssl目录，如图1-3所示。

图 1-3: 进入openssl目录



使用“openssl version”命令查看openssl版本，如图1-4所示。

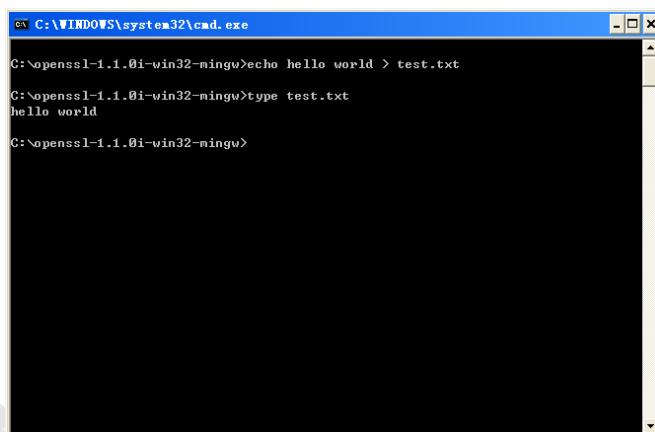
图 1-4: openssl版本



1.6.2 创建测试文件

使用“echo”命令创建测试文件“test.txt”，使用“type”命令查看文件内容，如图1-5所示。

图 1-5: 创建并查看测试文件

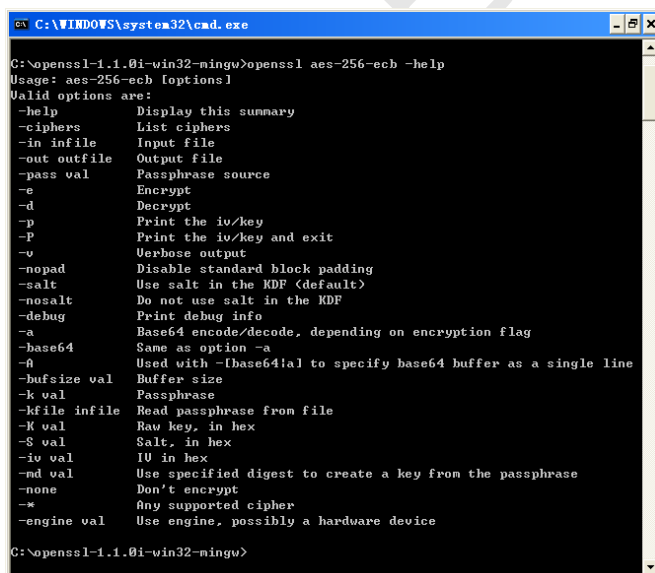


```
C:\WINDOWS\system32\cmd.exe
C:\openssl-1.1.0i-win32-mingw>echo hello world > test.txt
C:\openssl-1.1.0i-win32-mingw>type test.txt
hello world
C:\openssl-1.1.0i-win32-mingw>
```

1.6.3 使用AES算法加密测试文件

使用“openssl aes-256-ecb”命令的“-help”选项查看256位AES电子密码本模式相关帮助文档，学习相关参数，如图1-6所示。

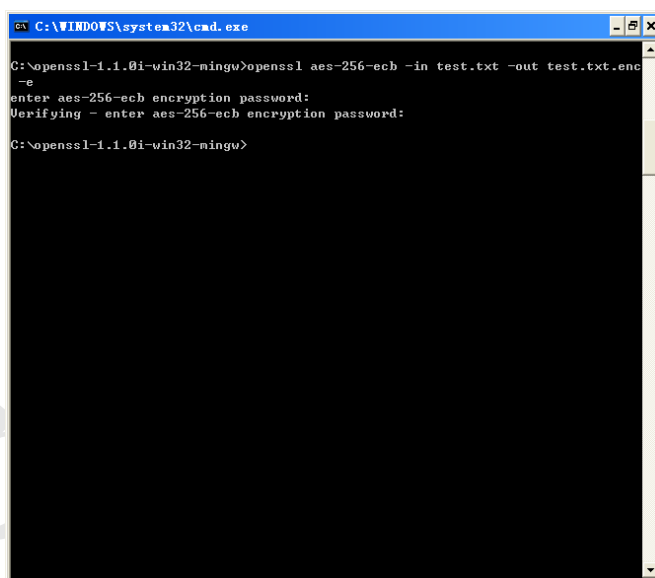
图 1-6: 查看AES帮助文档



```
C:\WINDOWS\system32\cmd.exe
C:\openssl-1.1.0i-win32-mingw>openssl aes-256-ecb -help
Usage: aes-256-ecb [options]
Valid options are:
  -help           Display this summary
  -ciphers         List ciphers
  -in infile       Input file
  -out outfile     Output file
  -pass val       Passphrase source
  -e              Encrypt
  -d              Decrypt
  -p              Print the iv/key
  -P              Print the iv/key and exit
  -v              Verbose output
  -nopad          Disable standard block padding
  -salt           Use salt in the KDF (default)
  -nosalt         Do not use salt in the KDF
  -debug          Print debug info
  -a              Base64 encode/decode, depending on encryption flag
  -base64         Same as option -a
  -A              Used with -[base64]al to specify base64 buffer as a single line
  -bufsize val    Buffer size
  -k val          Passphrase
  -kfile infile   Read passphrase from file
  -K val          Raw key, in hex
  -S val          Salt, in hex
  -iv val         IV in hex
  -md val         Use specified digest to create a key from the passphrase
  -none           Don't encrypt
  -*             Any supported cipher
  -engine val     Use engine, possibly a hardware device
C:\openssl-1.1.0i-win32-mingw>
```

使用“openssl aes-256-ecb”命令的“-e”等选项加密测试文件得到密文“test.txt.enc”，查看密文内容，如图1-7所示。

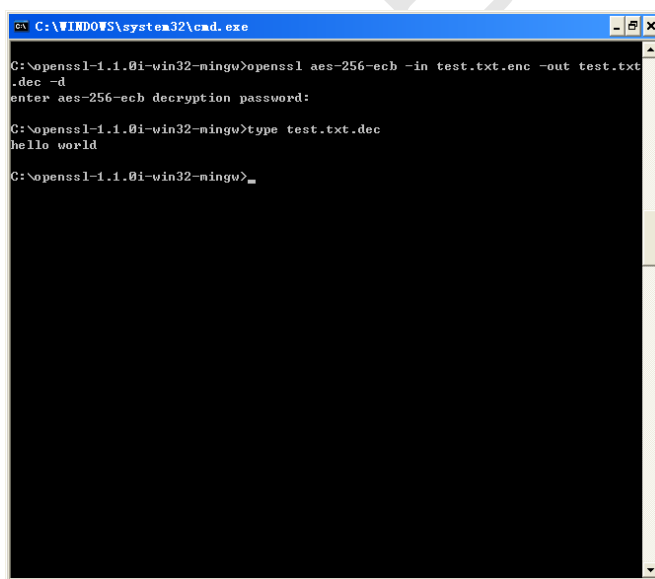
图 1-7: 使用AES加密明文



1.6.4 使用AES算法解密测试文件

查看如图1-6所示AES帮助文档，学习解密文件方法，使用“openssl aes-256-ecb”命令的“-d”等选项解密密文得到明文“test.txt.dec”，查看明文内容，如图1-8所示。

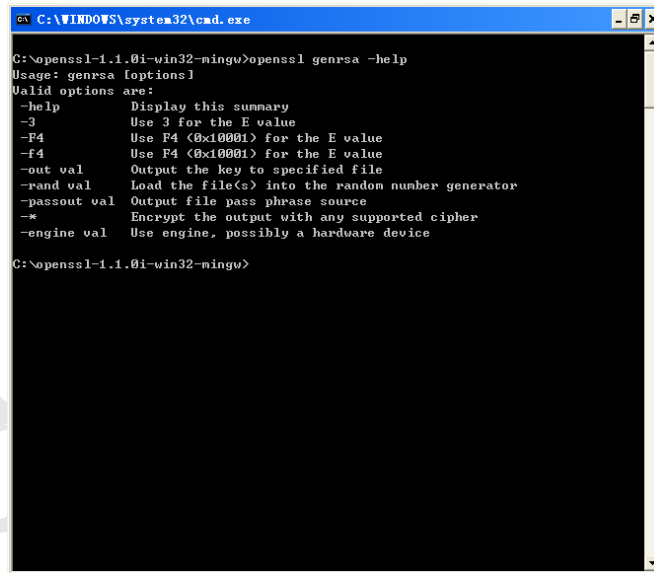
图 1-8: 使用AES解密密文



1.6.5 使用RSA算法生成公钥私钥

使用“openssl genrsa”命令的“-help”选项查看生成私钥帮助文档，如图1-9所示。

图 1-9: 查看生成私钥帮助文档



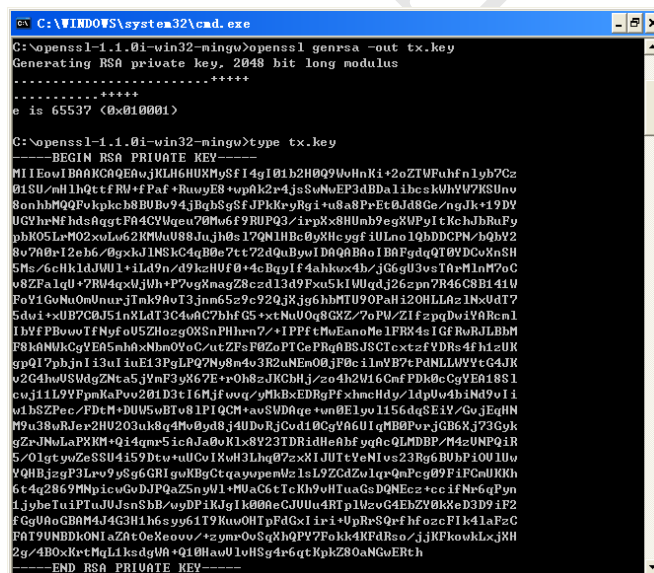
```
C:\WINDOWS\system32\cmd.exe

C:\openssl-1.1.0i-win32-mingw>openssl genrsa -help
Usage: genrsa [options]
Valid options are:
  -help      Display this summary
  -3         Use 3 for the E value
  -F4        Use F4 (0x10001) for the E value
  -f4        Use F4 (0x10001) for the E value
  -out val   Output the key to specified file
  -rand val  Load the file(s) into the random number generator
  -passout val Output file pass phrase source
  -*        Encrypt the output with any supported cipher
  -engine val Use engine, possibly a hardware device

C:\openssl-1.1.0i-win32-mingw>
```

使用“openssl genrsa”命令的“-out”选项生成私钥文件“tx.key”，如图1-10所示。

图 1-10: 生成私钥文件



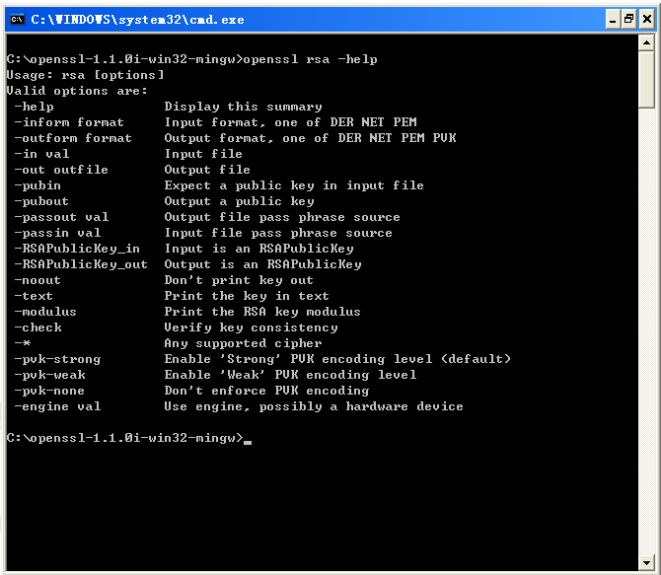
```
C:\WINDOWS\system32\cmd.exe

C:\openssl-1.1.0i-win32-mingw>openssl genrsa -out tx.key
Generating RSA private key, 2048 bit long modulus
+++++
e is 65537 (0x010001)

C:\openssl-1.1.0i-win32-mingw>type tx.key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwjkLH6HUXMySfI4gI01b2H0Q9W0HnKi+2oZTWfuhfalyb7Cz
01SU/nH1hQtTFRM+FPaf+RuwyE8+upak2r4jsSvNoEP3dBDalibcskWhYU7KSUnv
8onhhMQQFokpkcb8BUBo94jBqbSgSfJPkKryRgi+u8a8PrEt0Jd8Ge/ngJk+19DY
UGVhrNFhds8qgtF84CYWqeu70Mw6f9RUPQ3/irpX8HUmbyegXWPYItKchJbRuFy
pbK05LrMO2x0Lw62RMuU88JuJh0s17QNIHBc0yXhcygf iULno1QbDDCPN/bQbY2
8v7a0r12eb6/0gXkL1NSKc4qB0e7tt72dQaBywIDAQABAoIBAfgdQI0YDCvXnSH
SMz/6cHkldJvU1+1Ld9n/d9kzNUF0+4cBqyIf4ahkwx4b/jG6gU3vs1ArHlnM7oC
v8ZFalgU+7RM4qxJvJh+P7ogXmagZ8czd13d9FxsKiU0qdj26zpn7R46C8B141V
FoY1GoNuOmUnurjTmk9AoT3jnm65z9c92QjXjg6hbMTU9OPaH120HLLA21MxUDT7
Sdwi+XUB7C0J51nLd13C4uA7bhfGS+xtNuU0q8GXZ/7oPU/Z1fzpqDu1YARcm1
lMyFPBuwTFNyfoU5ZhozgOXSnPHhrn7/+1PPftMvEanoMe1FR84s1GfRwRJLBm
P8kAMUKCgYEa5nhaXNmoOYoCoutZF8Z0PT0ePRqBJSCTCctcfYDRs4fMzUK
gpQ17pbJn113u1iuE13PgLPQ7My8n4o3R2oUNEm00jR9c1LwP2FAMLLMPPvCgJK
U2C4h0USWdgZnta5Jvnt3yK67E+0h8zJKOMhjz04h2W4ChtFDD0eCgYEAgS1
cu11L9YFpmKaPoo201D3t1Gh1fouqQmBxEDR3PE+AmcHdy71d0u4b1M9o11
v1NSZPzc+FDH+0UW5+DT+01P1QCH+e0U0Aqg+non0E1yo1156dgSE14/cojEoHN
M9c38uRjSp2HU203u8k8q4Mo0yda8jdUoRjCvdi9CgYAGU1uMBBPv+jGBXj23Cpk
gZcJm0LaPXNM+Q14qm5+5aJ80K1+8V23TDRI8hAhfyg0c9LWDBP+M4zUNPQIR
5/01gtv0Z0SSU4459Deo+uU0Co1Xw13Lh072xXI1JUTtYvNiua23Rg6BUhP4OU1u
vQHRjzqP3Lw9y8g6GRIg0kBgCtqayupemLz1L9ZCdZv1q0mPcg09FicCmUKQh
6tdq2869MNPicv0uDJR0Z5n9u1+M0aC6tTcKh9uHTuaGdQNEcz+eifNw6qPyn
1jybeTuiPTuJenSbL4aypDKj1k000aCJUu4dRTp1MzovC4EhZy0kx6D3D9IF2
fCgU0aGBAM4J4C2H1h6zyg61T9Ku0H1PfGxLi+UvR8S0qfhf0zeF1k41aF2C
FAT9UNBDDkONIzZat0eXeeov+zyym0uSgKhqPN7Fokk4KFDao/jjKfKoukLxjXN
2g/4B0xKrtMq1LksgdU0+Q10HauU1oHSg4r6qtKpkZ80aNGuERth
-----END RSA PRIVATE KEY-----
```

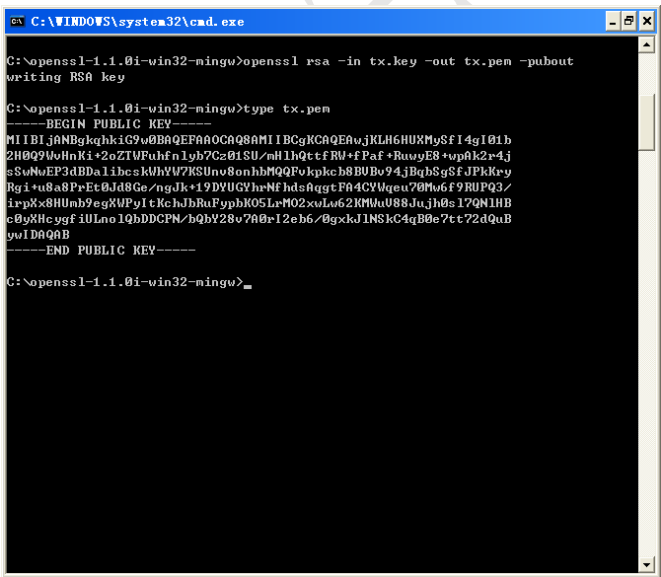
使用“openssl rsa”命令的“-help”选项查看密钥管理帮助文档，如图1-11所示。

图 1-11: 查看密钥管理帮助文档



使用“openssl rsa”命令的“-pubout”等选项从私钥文件“tx.key”中导出公钥文件“tx.pem”，如图1-12所示。

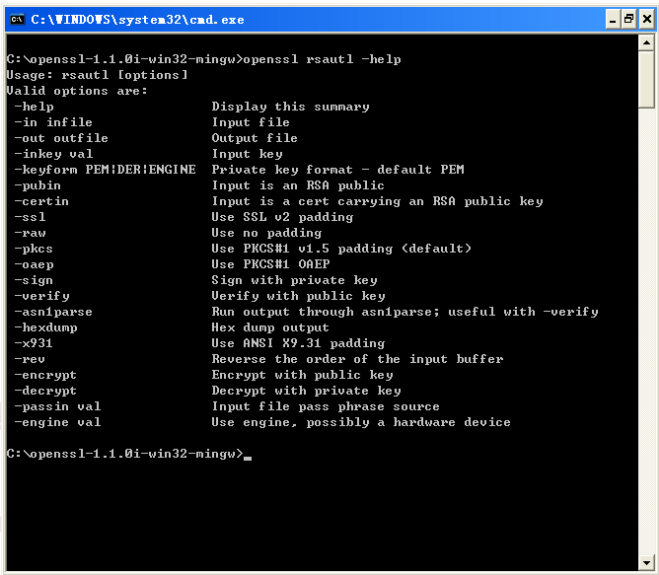
图 1-12: 导出公钥文件



1.6.6 使用RSA公钥加密测试文件

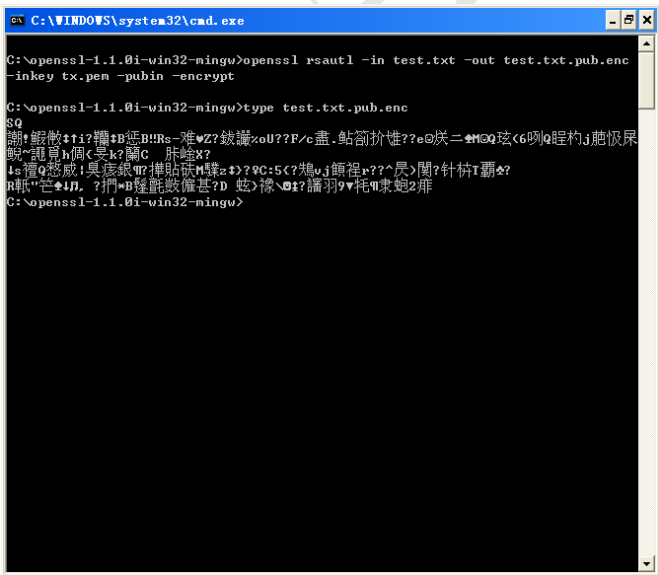
使用“openssl rsautl”命令的“-help”选项查看非对称加密工具帮助，学习加密文件方法，如图1-13所示。

图 1-13: 查看RSA工具帮助



使用“openssl rsautl”命令的“-encrypt”和“-pubin”等选项通过公钥文件加密测试文件明文，得到密文“test.txt.pub.enc”，如图1-14所示。

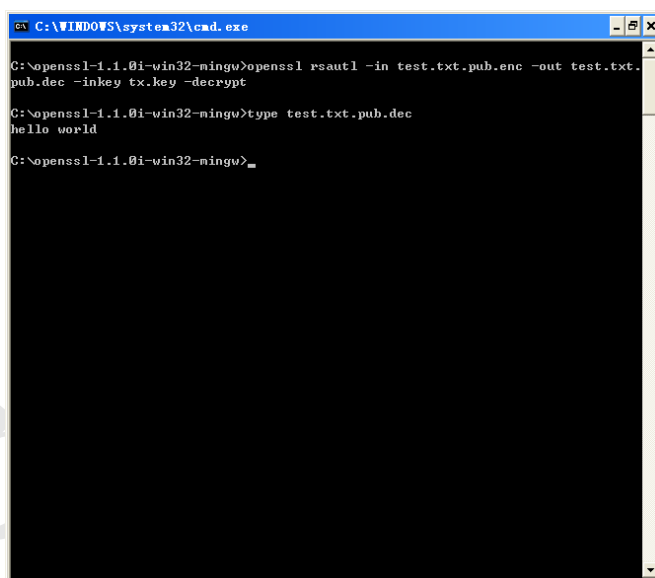
图 1-14: 使用公钥文件加密明文



1.6.7 使用RSA私钥解密测试文件

查看如图1-13所示RSA工具帮助，学习解密文件方法，使用“openssl rsautl”命令的“-decrypt”选项通过私钥文件解密密文，得到明文“test.txt.pub.dec”，如图1-15所示。

图 1-15: 使用私钥文件解密密文



```
C:\WINDOWS\system32\cmd.exe
C:\openssl-1.1.0i-win32-mingw>openssl rsautl -in test.txt.pub.enc -out test.txt.
pub.dec -inkey tx.key -decrypt
C:\openssl-1.1.0i-win32-mingw>type test.txt.pub.dec
hello world
C:\openssl-1.1.0i-win32-mingw>_
```

1.7 问题回答

简述对称密码体制和非对称密码体制的优缺点。

<http://tang.chat>

§ 2

网络监听嗅探技术

2.1 实验名称

网络监听嗅探技术

2.2 实验目的

1. 了解网络监听嗅探的原理;
2. 熟悉常见网络协议的传输过程;
3. 掌握网络监听嗅探工具的使用方法。

2.3 实验原理

通过将网卡设置为混杂模式 (Promiscuous Mode)，计算机可以接收目的地址和本机不相同的数据包。

2.4 实验材料

1. 运行Windows XP或更高版本操作系统的PC机一台;
2. Wireshark v1.10.14或更高版本软件安装程序。

2.5 实验步骤

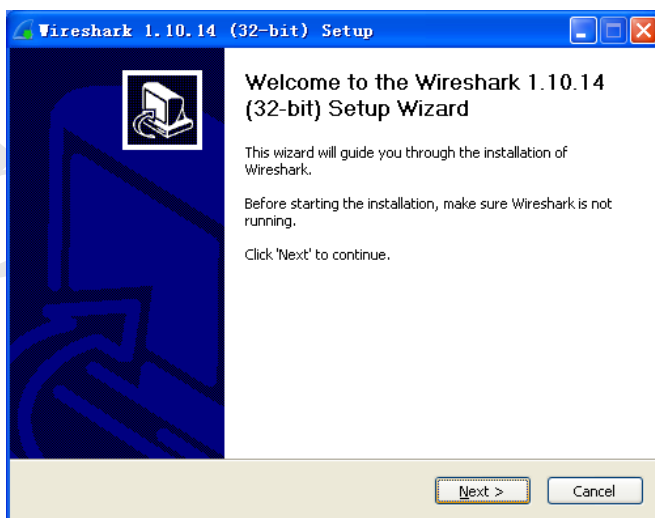
1. 安装Wireshark
2. 使用Wireshark分析ICMP协议

2.6 实验记录

2.6.1 安装Wireshark

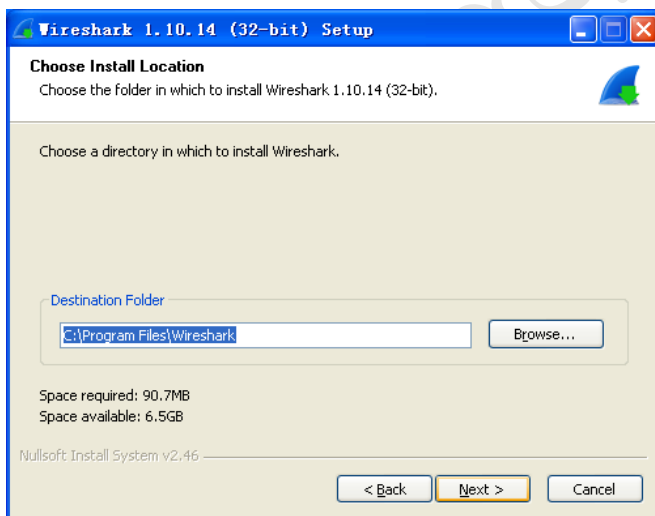
运行Wireshark软件安装程序，进入“安装向导”界面，如图2-1所示。

图 2-1: Wireshark“安装向导”界面



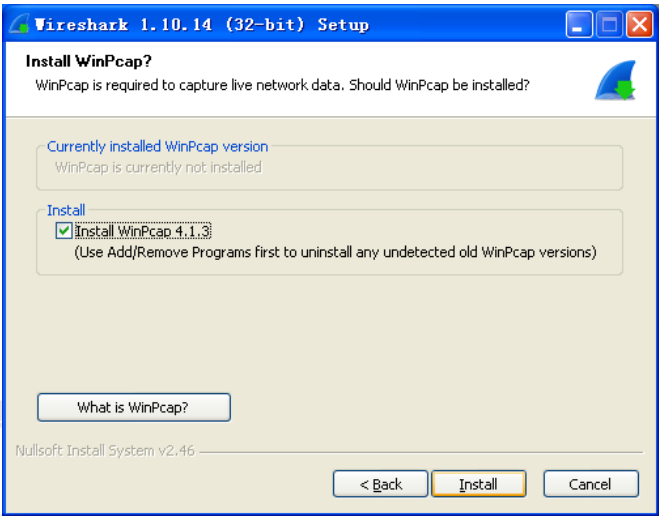
进入“选择安装路径”界面可以自定义安装路径，如图2-2所示。

图 2-2: Wireshark“选择安装路径”界面



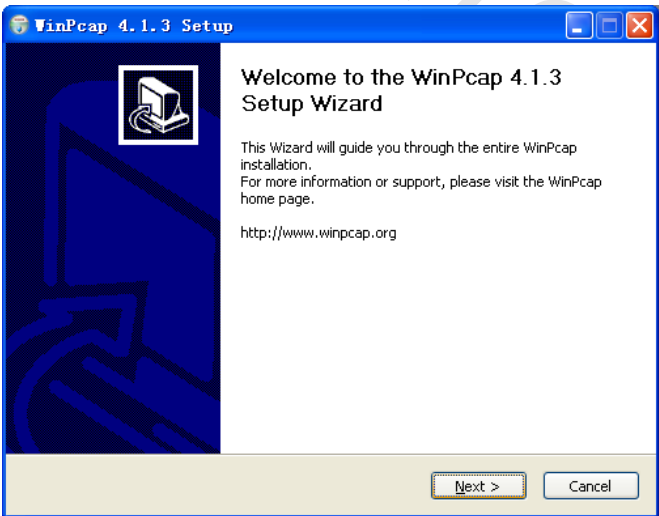
进入“选择安装WinPcap”界面，WinPcap为Wireshark提供了启用混杂模式、抓包分析等核心功能，如图2-3所示。

图 2-3: Wireshark“选择安装WinPcap”界面



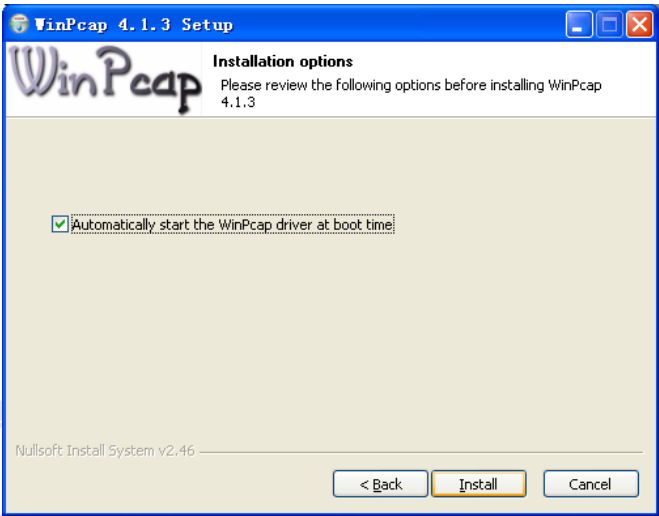
进入WinPcap“安装向导”界面，如图2-4所示。

图 2-4: WinPcap“安装向导”界面



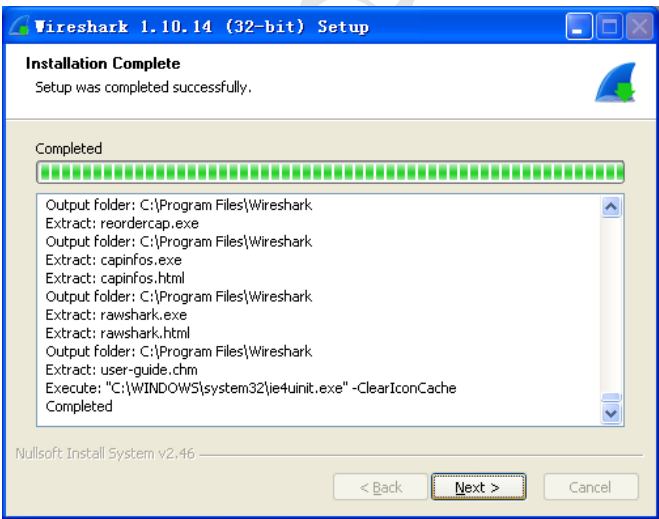
进入WinPcap“安装选项”界面，默认在计算机启动时自动运行WinPcap服务，如图2-5所示。

图 2-5: WinPcap“安装选项”界面



WinPcap安装完成，进入Wireshark“安装完成”界面，如图2-6所示。

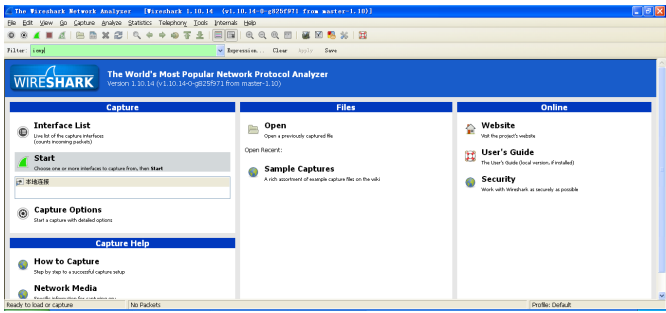
图 2-6: WinPcap“安装完成”界面



2.6.2 使用Wireshark分析ICMP协议

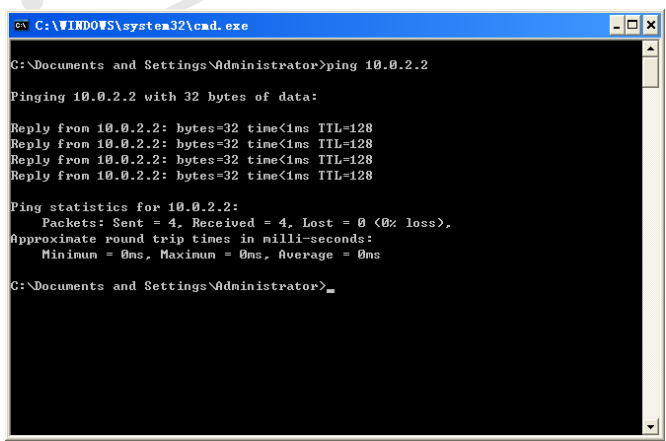
运行wireshark，在“filter”工具栏位置填入“ICMP”，在“Capture”面板的“接口列表”中选中需要监听数据的网络接口，然后单击“Start”按钮开始监听ICMP协议数据，如图2-7所示。

图 2-7: 监听ICMP协议数据



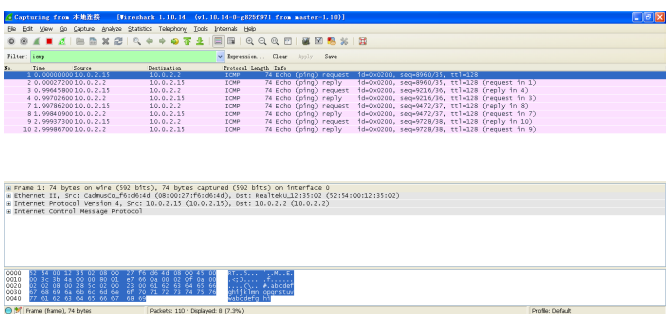
使用“ping”命令探测本地网关或其他计算机IP地址，如图2-8所示。

图 2-8: 使用“ping”命令



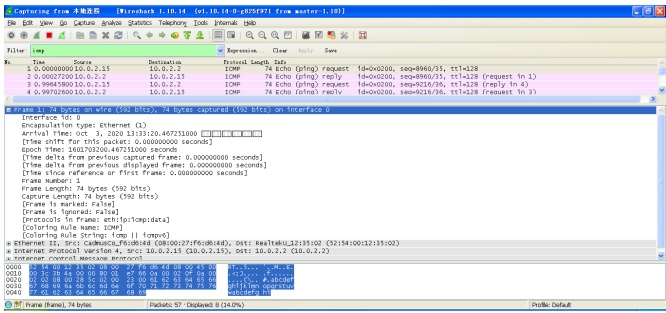
此时，wireshark已抓取到“ping”命令产生的4条ICMP协议请求数据包和4条回应包，如图2-9所示。

图 2-9: 抓取“ping”命令ICMP协议数据包



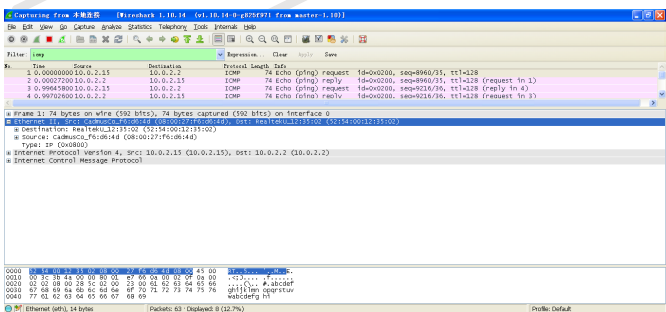
选择其中一条ICMP协议请求数据包，可以看出该数据包共74字节，如图2-10所示。

图 2-10: 查看ICMP协议请求数据包



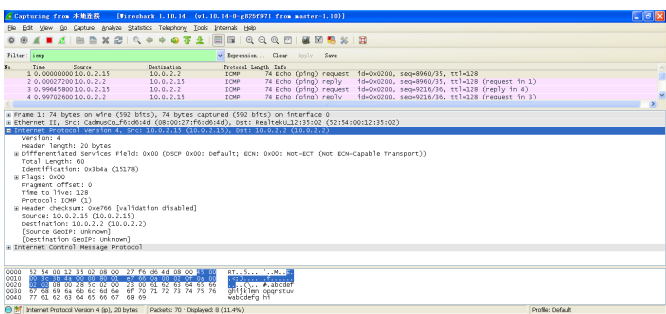
数据链路层采用了Ethernet II协议，共占14个字节，包含了6个字节的目标MAC地址、6个字节的来源MAC地址、2个字节的网络层协议类型（0x0800代表为IP协议），如图2-11所示。

图 2-11: 查看ICMP协议请求数据包的数据链路层数据



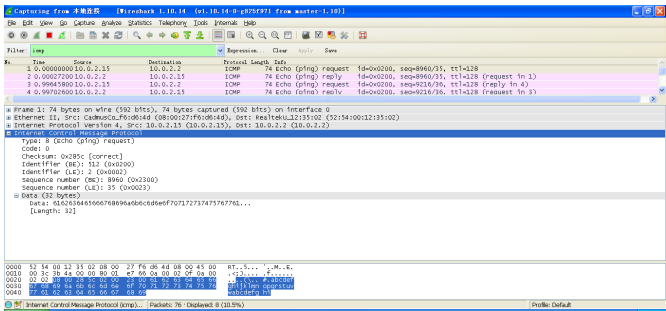
网络层采用了IPv4协议，包含了20个字节的头部数据，如图2-12所示。

图 2-12: 查看ICMP协议请求数据包的网络层数据



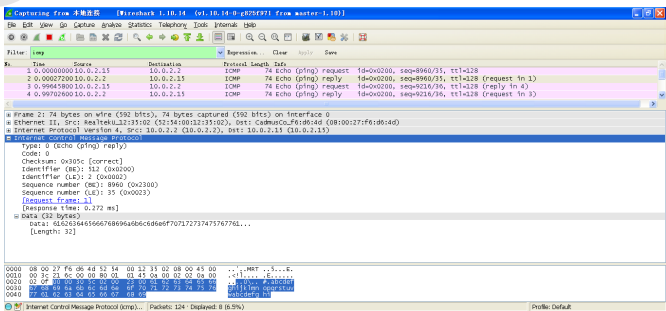
ICMP协议格式的数据，包含了8个字节的头部数据和32个字节的的应用层数据，如图2-13所示。

图 2-13: 查看ICMP协议请求数据包的ICMP头和应用层数据



选择请求数据包对应的响应数据包，查看其ICMP头和应用层数据，如图2-14所示。

图 2-14: 查看ICMP协议响应数据包的ICMP头和应用层数据



2.7 问题回答

简述TCP/IP协议四层协议和OSI七层协议之间的联系。

<http://tang.chat>

§ 3

入侵检测监控技术

3.1 实验名称

入侵检测监控技术

3.2 实验目的

1. 了解入侵检测系统的工作原理;
2. 掌握入侵检测系统的使用方法。

3.3 实验原理

入侵检测系统 (Intrusion Detection System, IDS) 是一种软件或硬件系统, 它监控主机或网络是否存在恶意活动或违反策略行为, 若存在则报告给管理员或使用安全信息和事件管理系统 (Security Information and Event Management, SIEM) 集中收集相关信息。

3.4 实验材料

1. 运行Windows 7或更高版本操作系统的PC机一台;
2. 已安装Wireshark v1.10.14或更高版本。
3. Snort v2.9.8.3或更高版本安装程序。

3.5 实验步骤

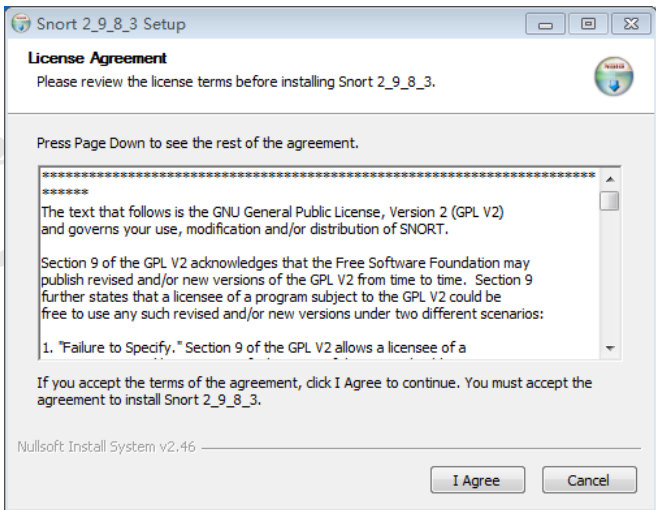
1. 安装Snort
2. 使用Snort嗅探模式
3. 使用Snort日志模式
4. 使用Snort网络入侵检测模式

3.6 实验记录

3.6.1 安装Snort

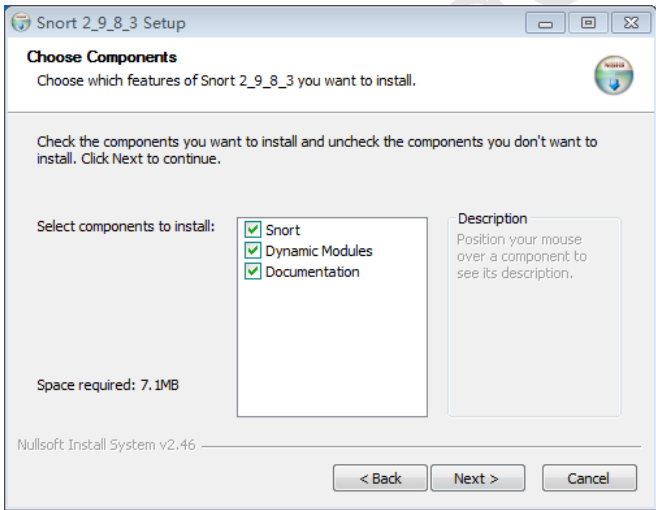
运行Snort安装程序，进入“许可协议”界面，如图3-1所示。

图 3-1: Snort“许可协议”界面



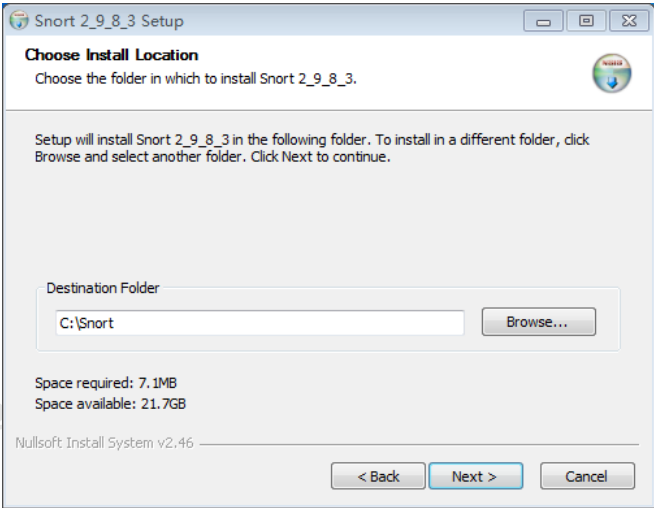
进入“选择组件”界面可以选择是否安装Snort主体程序、动态模块、文档，如图3-2所示。

图 3-2: Snort“选择组件”界面



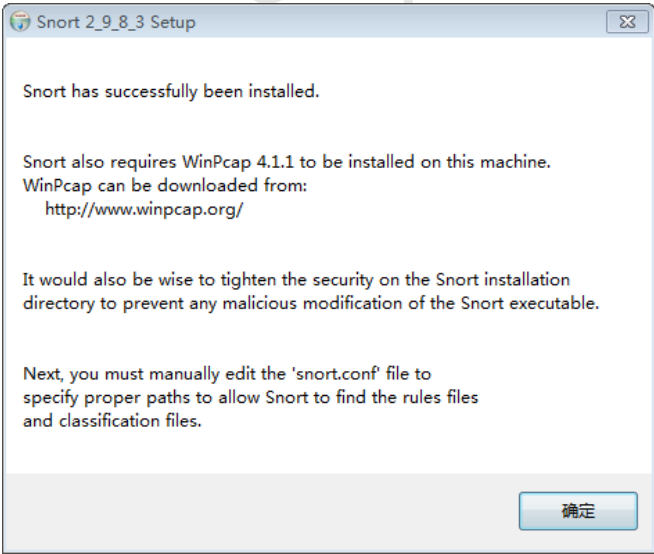
进入“选择安装位置”界面可以选择Snort安装位置，使用默认设置将Snort安装至“C:”，如图3-3所示。

图 3-3: Snort“选择安装位置”界面



安装完毕后，单击“Close”按钮，弹出窗口提示需要安装WinPcap支持和置Snort，如图3-4所示。

图 3-4: 提示安装WinPcap和配置Snort



3.6.2 使用Snort嗅探模式

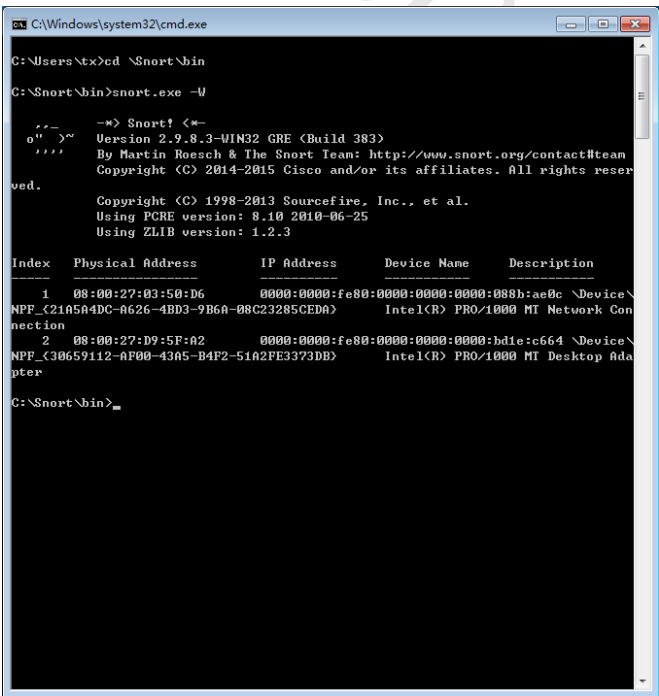
使用Snort之前，先确定需要监控的主机或网络地址。打开新的命令窗口，使用“ipconfig/all”命令列出包括MAC和IP地址在内的本机所有网卡信息，如图3-5所示。

图 3-5: 列出所有网卡信息



进入Snort安装位置下的“bin”目录，使用“Snort -W”命令列出有效网络接口，如图3-6所示。

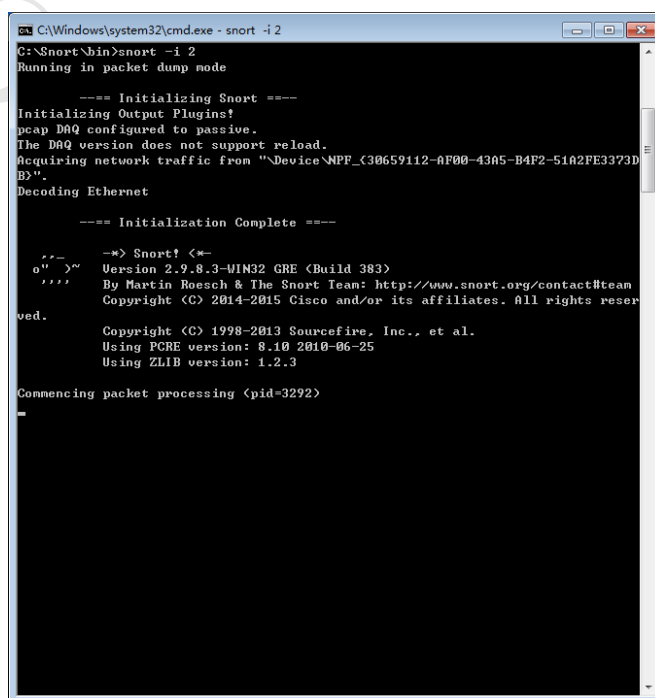
图 3-6: 使用Snort列出有效网络接口



比较图3-5和图3-6，确定嗅探MAC地址为“08-00-27-D9-5F-A2”的网络接口，其索引值（Index）为2，IP地址

为“10.0.2.15”、子网掩码为“255.255.255.0”、网关为“10.0.2.2”。使用“Snort -i 2”命令嗅探该网络接口，如图3-7所示。

图 3-7: 使用Snort嗅探指定网络接口



```
C:\Windows\system32\cmd.exe - snort -i 2
C:\Snort\bin>snort -i 2
Running in packet dump mode

---- Initializing Snort ----
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{30659112-AF00-43A5-B4F2-51A2FE3373D}\{B}
Decoding Ethernet

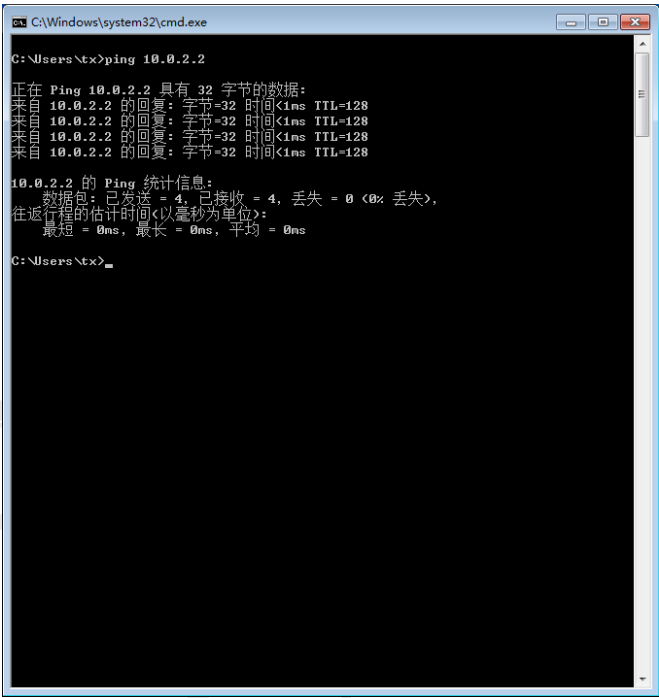
---- Initialization Complete ----

---> Snort! <---
Version 2.9.8.3-WIN32 GRE <Build 383>
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

Commencing packet processing (pid=3292)
```

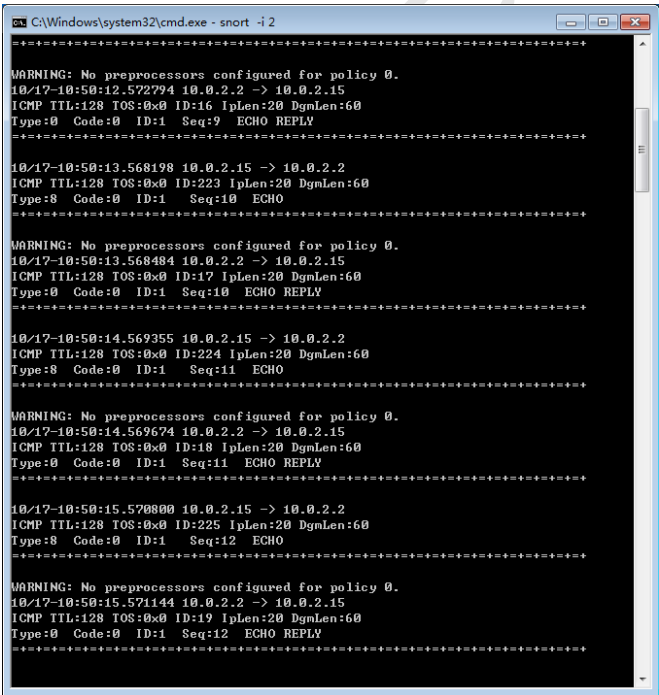
打开新的命令窗口，使用“ping 10.0.2.2”命令探测网关或相同子网IP地址，如图3-8所示。

图 3-8: 使用“ping”命令探测网关



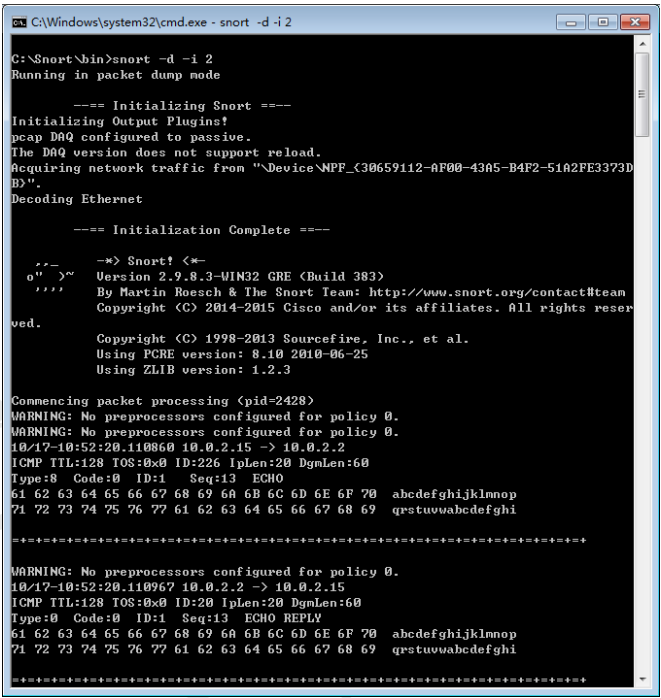
此时，Snort已嗅探到“ping”命令产生的4条ICMP协议请求数据包和4条回应包，如图3-9所示。

图 3-9: 嗅探“ping”命令



使用“snort -d -i 2”命令可以额外显示应用层数据，如图3-10所示。

图 3-10: 嗅探“ping”命令应用层数据

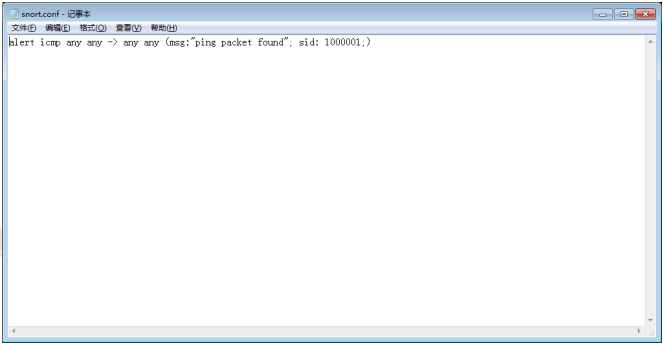


3.6.3 使用Snort日志模式

使用“snort -dev -i 2 -l ../log”命令可以将嗅探到的信息存入到“../log”目录中，即当前目录父目录下的log目录，如图3-11所示。

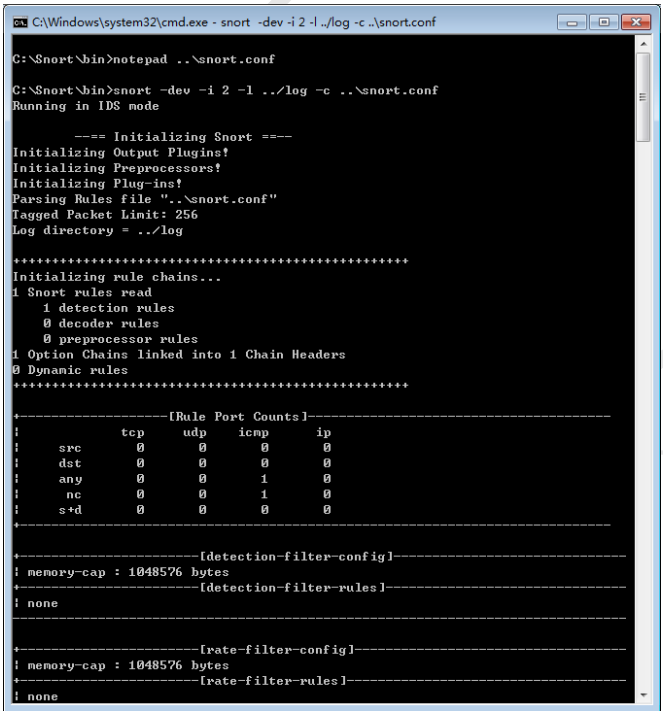
snort.conf”在“C:\snort”中创建并编辑“snort.conf”配置文件，输入一条规则“alert icmp any any -i any any (msg: ”ping packet found”); sid: 1000001;)”，如图3-13所示。

图 3-13: 创建Snort配置文件



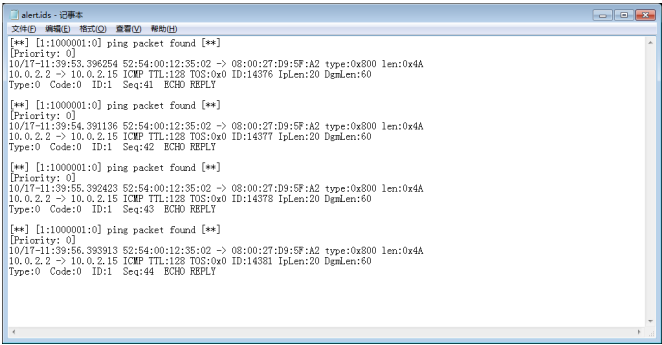
使用“snort ../snort.conf”命令进行入侵检测，如图3-14所示。

图 3-14: 使用Snort入侵检测



如图3-8所示再次使用“ping”命令访问网关，使用notepad打开“C:\snort\log\alert.ids”警告日志文件，如图3-15所示。

图 3-15: 查看警告日志文件



3.7 问题回答

编写规则实现监控标准HTTP协议。

§ 4

系统安全配置技术

4.1 实验名称

系统安全配置技术

4.2 实验目的

1. 了解Windows操作系统安全基线相关概念;
2. 熟悉Windows操作系统安全基线配置选项;
3. 掌握Windows操作系统安全基线配置方法;
4. 熟悉组策略编辑器的使用方法;

4.3 实验原理

不同的组织安全威胁类型可能截然不同，组织为了保证应用和设备安全定义的安全标准叫做安全基线（Security Baselines）。微软公司将来自公司内部、合作伙伴和客户专业知识综合在一起，提供了Windows操作系统安全基线来缓解针对Windows操作系统的威胁。

4.4 实验材料

1. 运行Windows 7或更高版本操作系统的PC机一台。
2. Windows安全合规性工具包（Microsoft Compliance Toolkit）v1.0。

4.5 实验步骤

1. Windows安全基线文档
2. 本地组策略编辑器
3. 配置策略

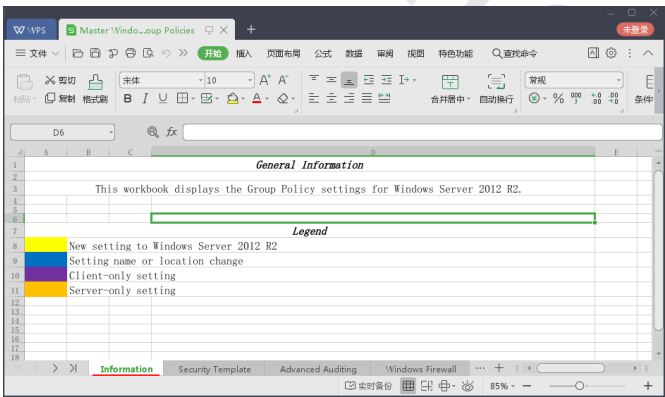
- (a) 配置账户策略
- (b) 配置本地策略
- (c) 配置高级安全Windows防火墙策略
- (d) 配置高级审核策略

4.6 实验记录

4.6.1 Windows安全基线文档

将Windows安全例行性工具包解压至目录“C:\”，选择“Windows Server 2012 R2 Security Baseline.zip”文件解压至当前目录，进入Document目录下，打开“Master Windows Server 2012 R2 Group Policies.xlsx”文件。该文档为Windows Server 2012 R2组策略安全基线文档，包含“基本信息”、“安全模板”、“高级审核”、“Windows防火墙”、“计算机”、“用户”、“IE计算机”、“IE用户”5张表，如图4-1所示。

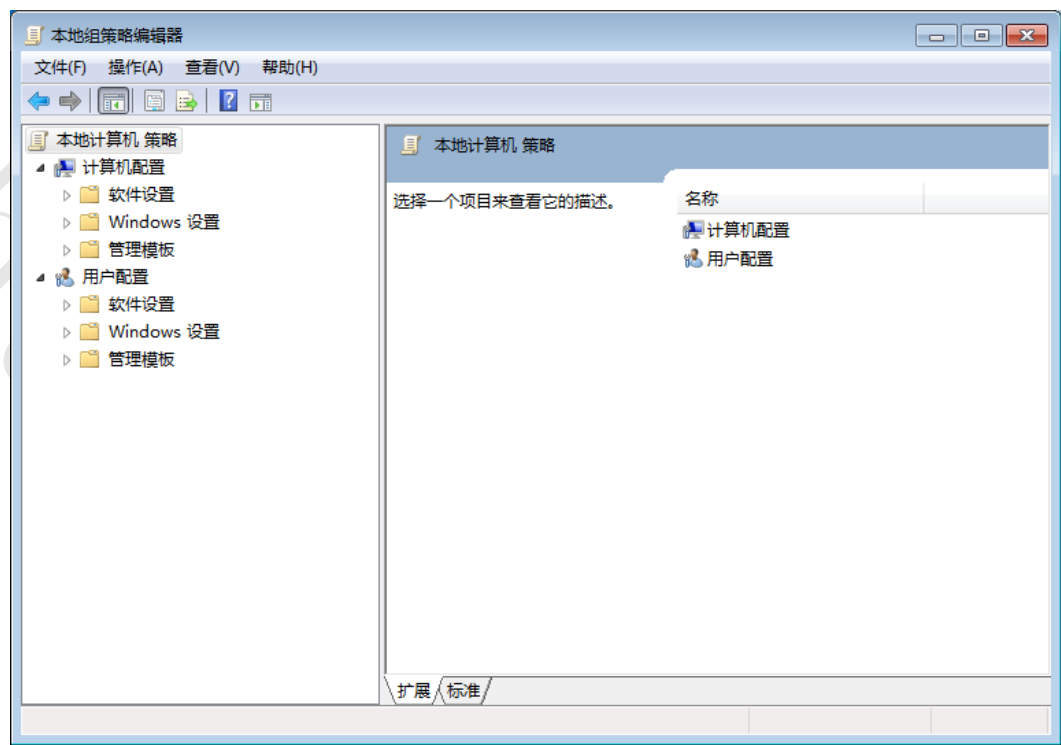
图 4-1: 组策略安全基线文档



4.6.2 本地组策略编辑器

使用“gpedit.msc”命令运行本地组策略编辑器，通过该工具可以配置图4-1中所示文件中给出的策略选项，如图4-2所示。

图 4-2: 本地组策略编辑器

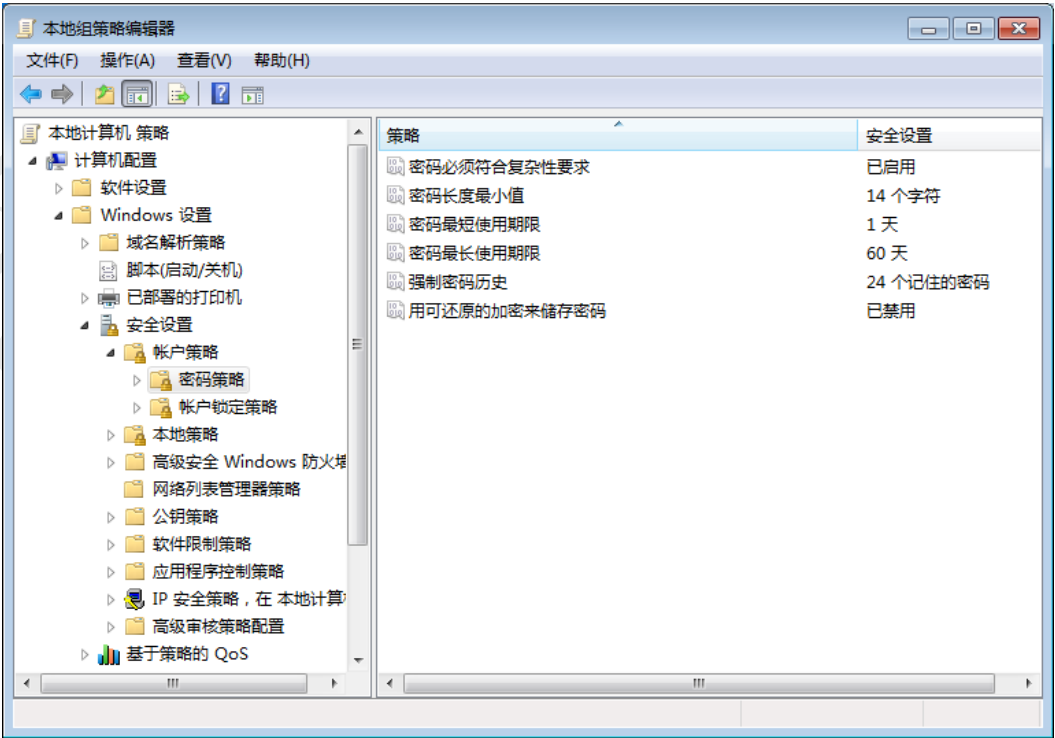


4.6.3 配置策略

配置账户策略

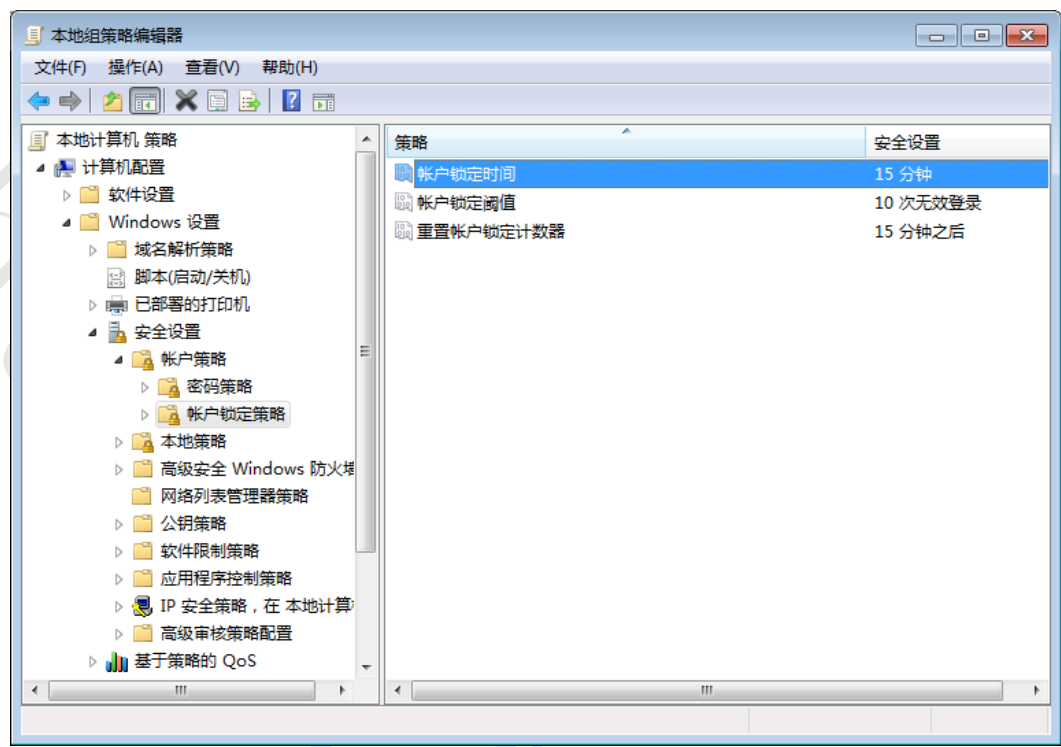
在本地组策略编辑器中，选择“计算机配置”-“Windows设置”-“安全设置“，在“账户策略”下选择“密码策略”，启用“密码必须符合复杂性要求”，设置“密码长度最小值”为14个字符，设置“密码最短使用期限”为1天，设置“密码最长使用期限”为60天，设置“强制密码历史”为“24个记住的密码”，禁用“用可还原的加密来储存密码”，如图4-3所示。

图 4-3: 密码策略



在“账户策略”下选择“账户锁定策略”，设置“账户锁定时间”为“15分钟”，设置“账户锁定阈值”为“10次无效登录”，设置“重置账户锁定计数器”为“15分钟之后”，如图4-4所示。

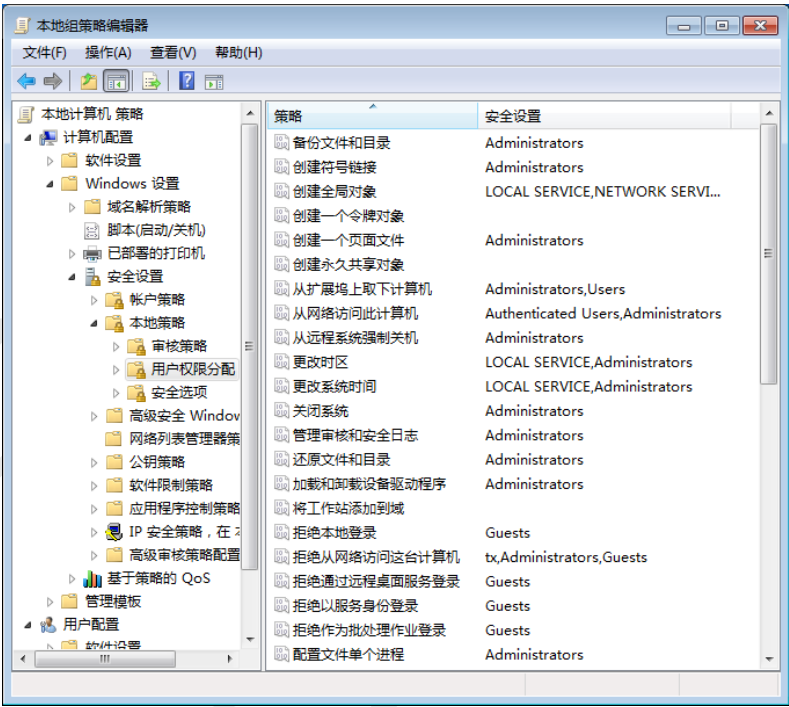
图 4-4: 账户锁定策略



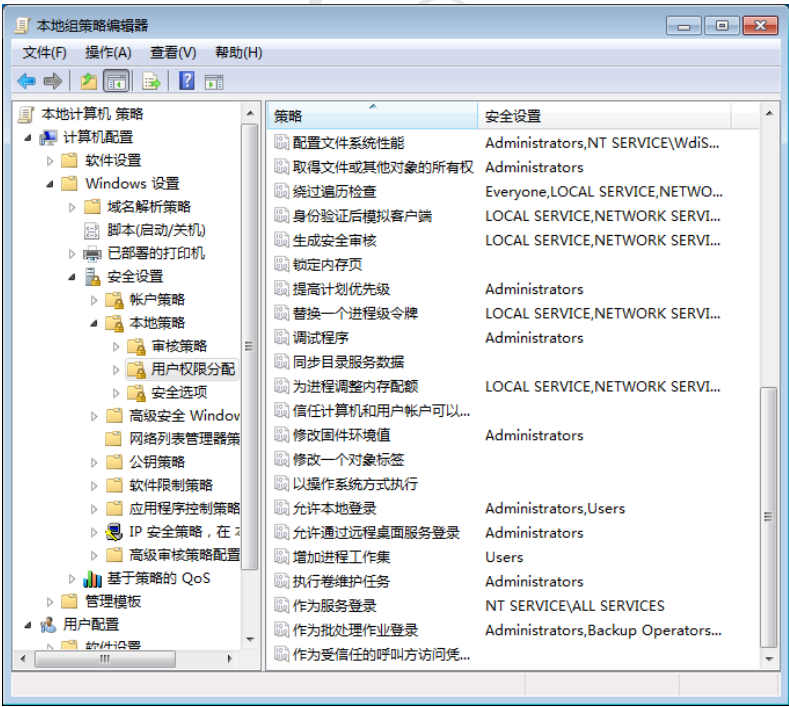
配置本地策略

在“本地策略”下选择“用户权限分配”，设置“备份文件和目录”、“还原文件和目录”、“关闭系统”为“Administrators”用户组，设置“从网络访问此计算机”为“Administrators”用户组和“Authenticated Users”用户组，设置“拒绝本地登录”、“拒绝通过远程桌面服务登录”、“拒绝以服务身份登录”、“拒绝作为批处理作业登录”为“Guests”用户组，设置“拒绝从网络访问这台计算机”为“Administrators”用户组、“Guests”用户组以及计算机本地用户，设置“允许本地登录”为“Administrators”用户组和“Users”用户组，设置“允许通过远程桌面服务登录”为“Administrators”用户组，如图4-5所示。

图 4-5: 用户权限分配策略



(a)

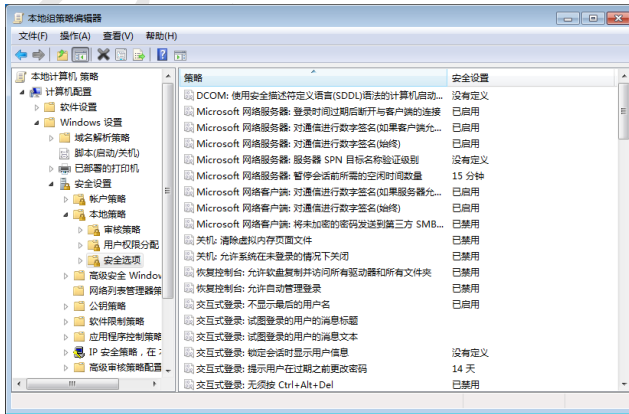


(b)

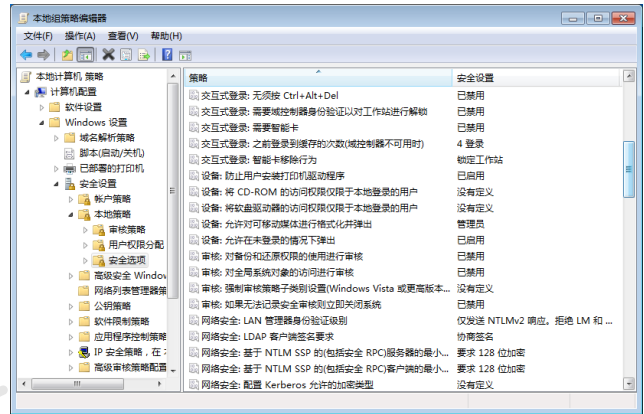
在“本地策略”下选择“安全选项”，禁用“关机：允许系统在未登录的情况下关闭”，启用“交互式登录：不显示最后的用户名”，禁用“交互式登录：无须按Ctrl+Alt+Delete”，设置“网络安全：LAN管理器身份验证级别”为“仅

发送NTLMv2响应。拒绝LM和NTLM”，启用“网络安全：在超过登录后强制注销”，启用“网络安全：不允许SAM账户和共享的匿名枚举”，设置“用户账户控制：标准用户的提升提示行为”为“自动拒绝提升请求”，建议通过设置“账户：重命名来宾账户”和“账户：重命名系统管理员账户”来重命名Guest和Administrator账户名称，如图4-6所示。

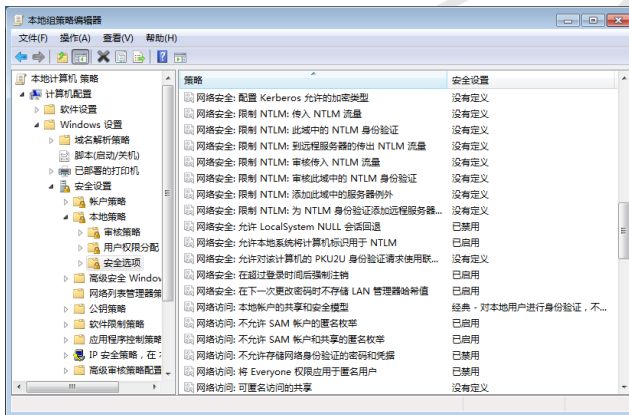
图 4-6: 安全选项策略



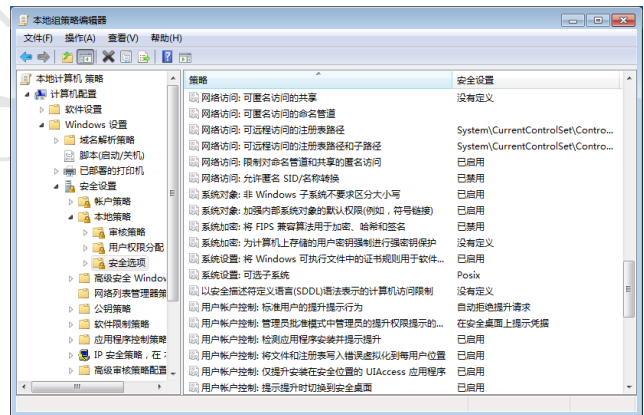
(a)



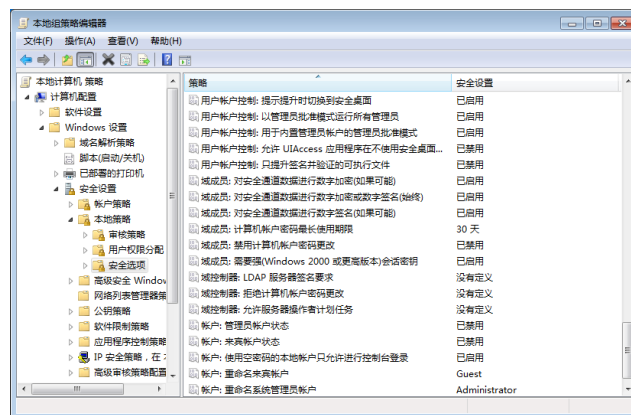
(b)



(c)



(d)

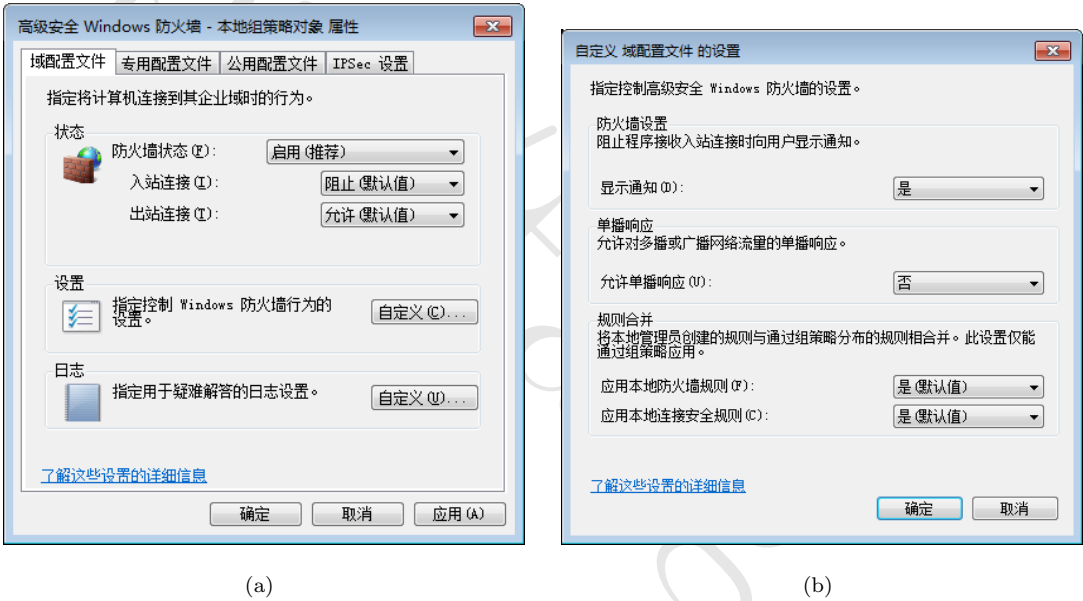


(e)

配置高级安全Windows防火墙策略

在“高级安全Windows防火墙”下选择“Windows防火墙属性”，可以对Windows防火墙的“域配置文件”、“专用配置文件”、“公用配置文件”分别设置策略，可以启用“防火墙状态”，设置“入站连接”为“阻止”，设置“出站连接”为“允许”，在“自定义”设置中可以设置“显示通知”为“是”，设置“允许单播响应”为“否”，设置“应用本地防火墙规则”、“应用本地连接安全规则”为“是”，如图4-7所示。

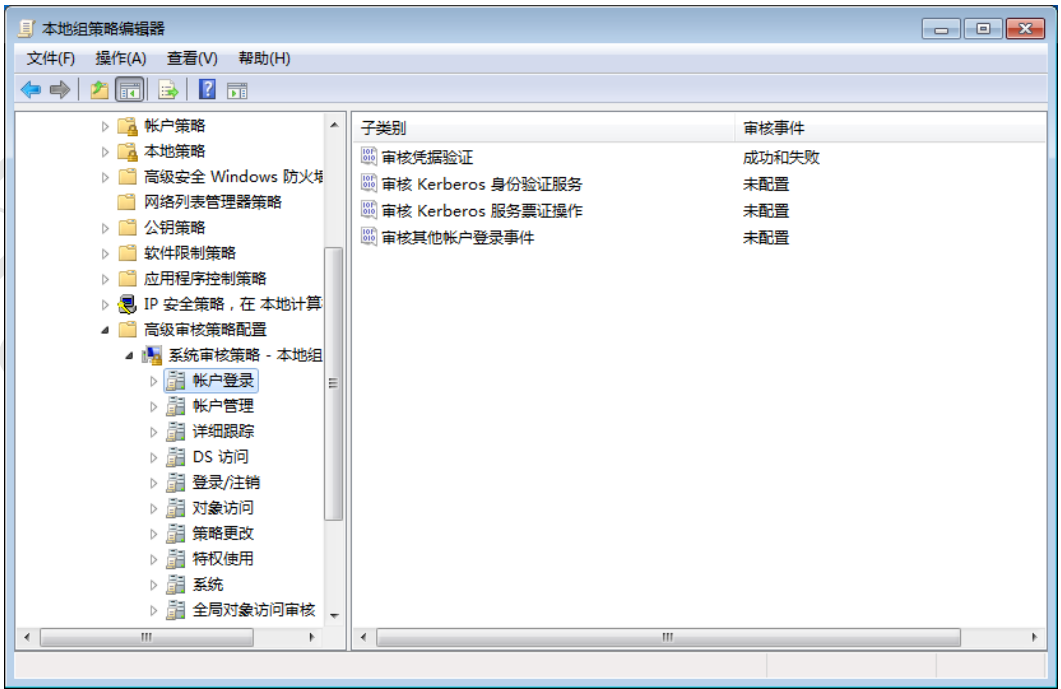
图 4-7: 高级安全Windows防火墙策略



配置高级审核策略

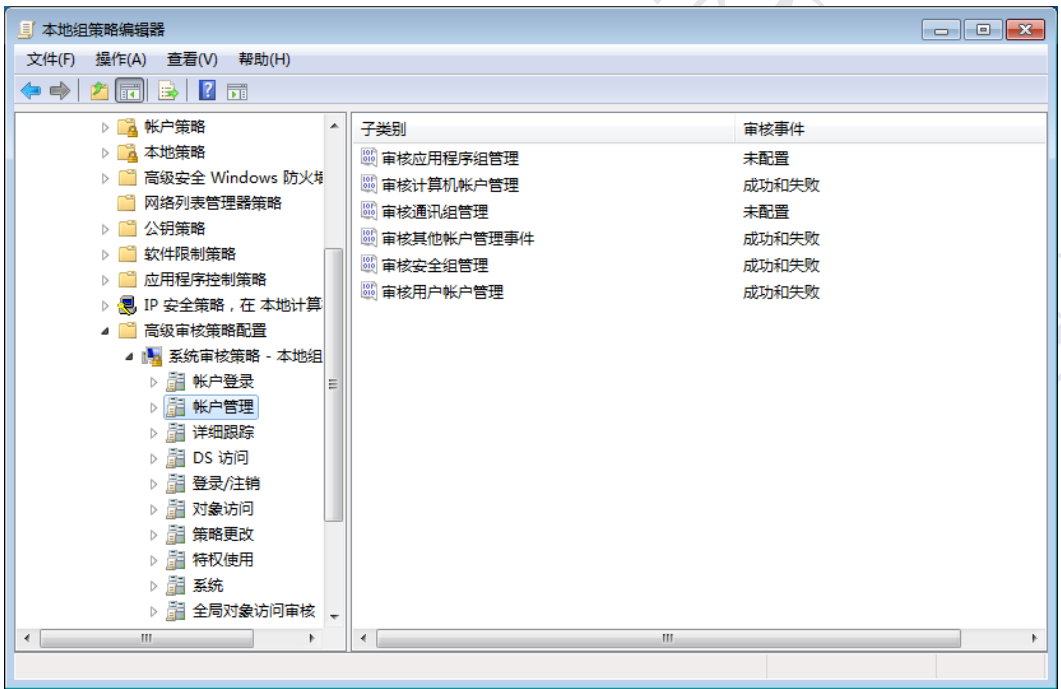
在“高级审核策略配置”下选择“系统审核策略”，继续选择“账户登录”策略，设置“审核凭据验证”为“成功和失败”，如图4-8所示。

图 4-8: 账户登录策略



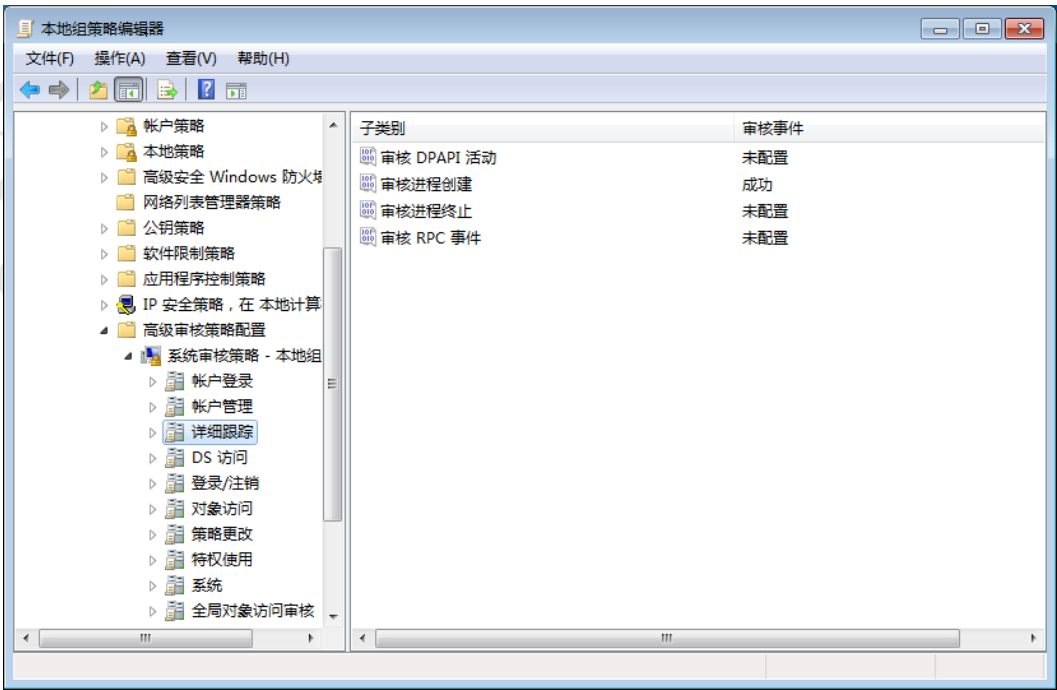
选择“账户管理”策略，设置“审核计算机账户管理”、“审核其他账户管理事件”、“审核安全组管理”、“审核用户管理”为“成功和失败”，如图4-9所示。

图 4-9: 账户管理策略



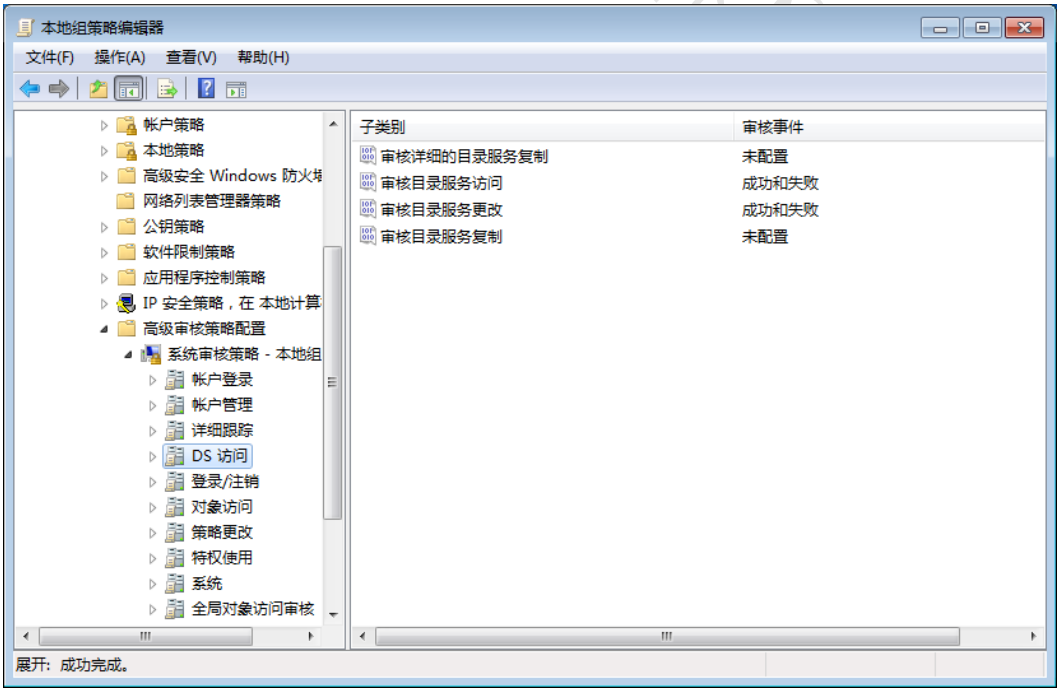
选择“详细跟踪”策略，设置“审核进程创建”为“成功”，如图4-10所示。

图 4-10: 详细跟踪策略



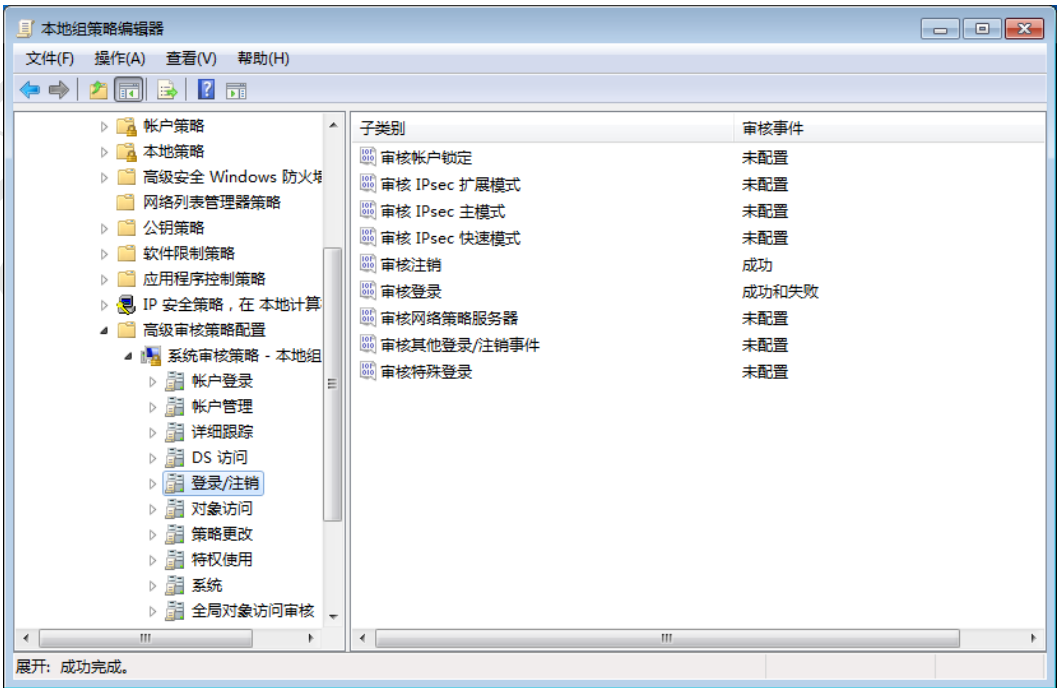
选择“DS访问”策略，设置“审核目录服务访问”、“审核目录服务更改”为“成功和失败”，如图4-11所示。

图 4-11: DS访问策略



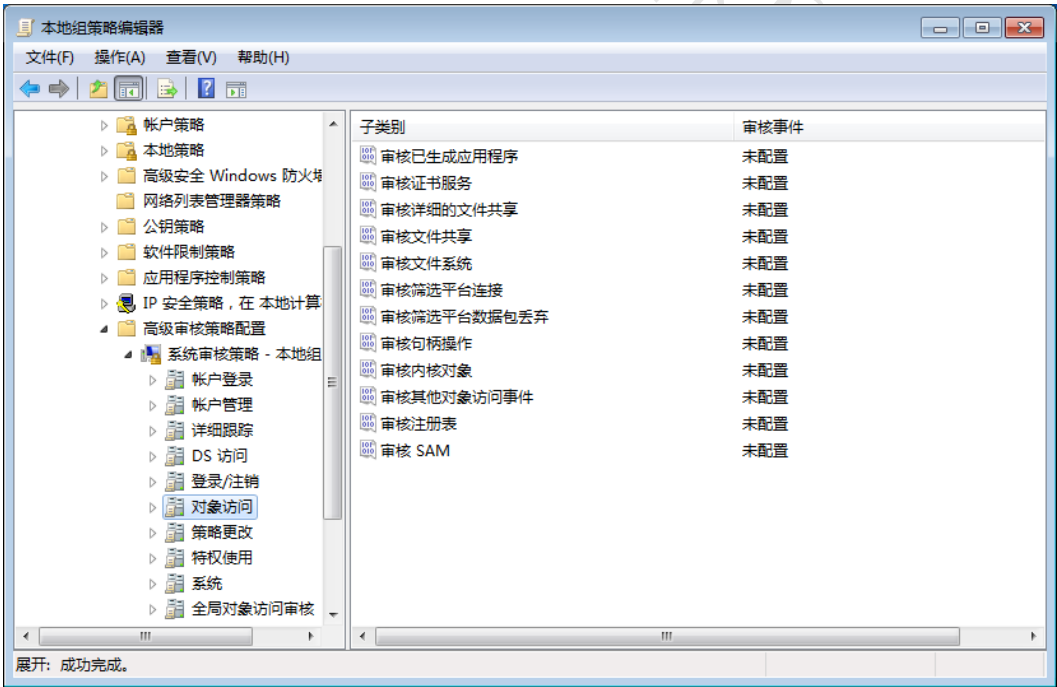
选择“登录注销”策略，设置“审核注销”、“审核登录”为“成功和失败”，如图4-12所示。

图 4-12: 登录注销策略



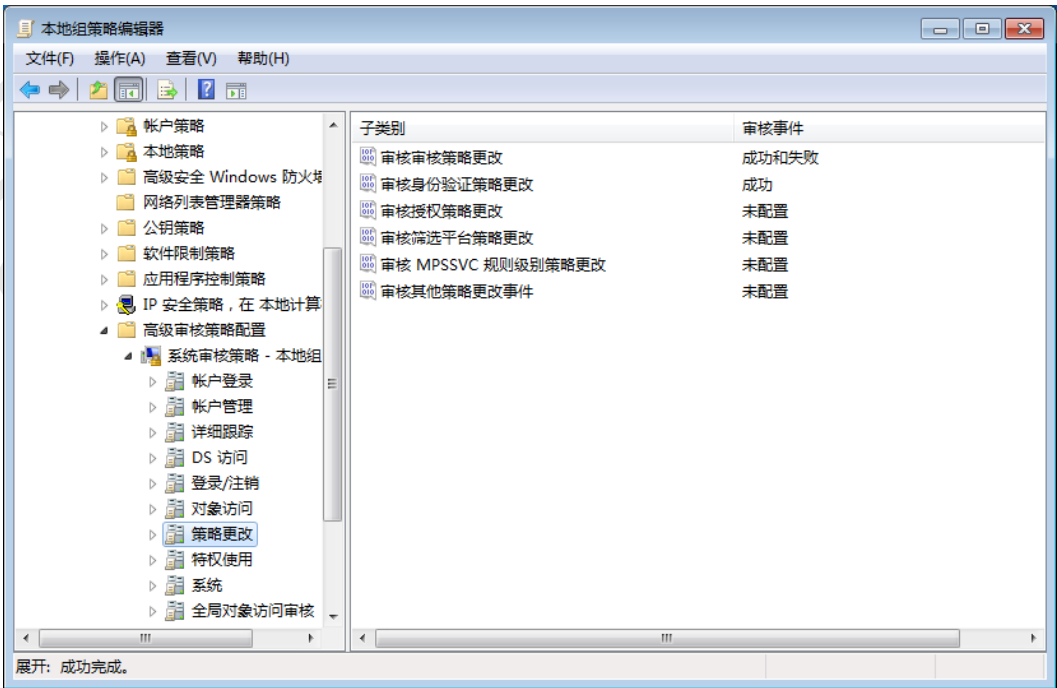
选择“对象访问”策略，设置“审核文件共享”为“成功和失败”，如图4-13所示。

图 4-13: 对象访问策略



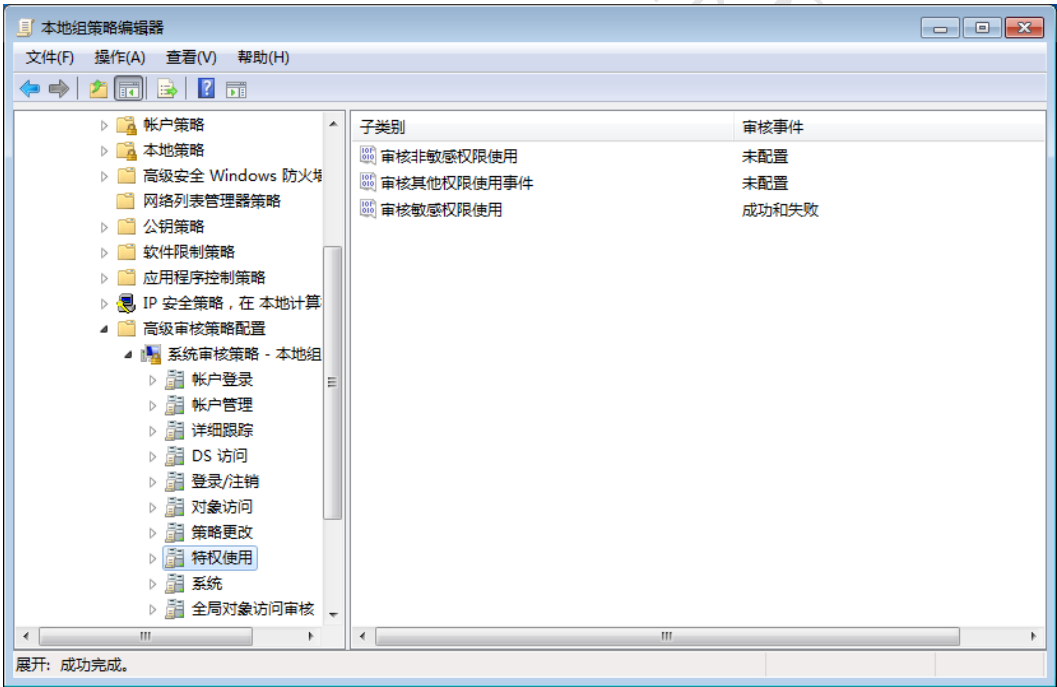
选择“策略更改”策略，设置“审核审核策略更改”、“审核身份验证策略更改”为“成功和失败”，如图4-14所示。

图 4-14: “策略更改”审核策略



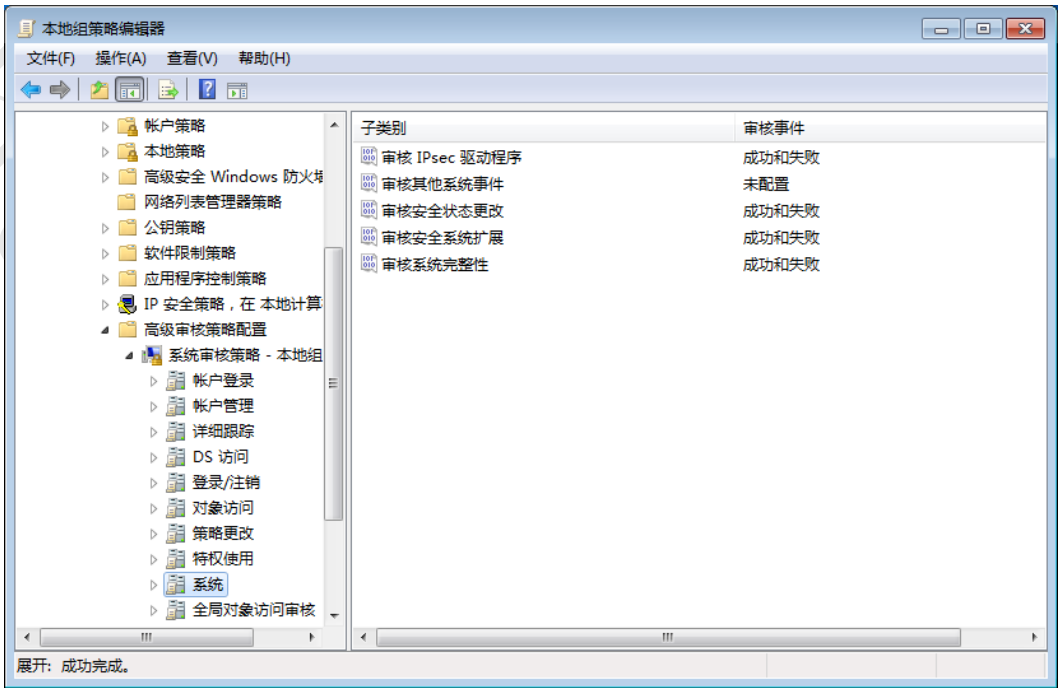
选择“特权使用”策略，设置“审核敏感权限使用”为“成功和失败”，如图4-15所示。

图 4-15: 特权使用策略



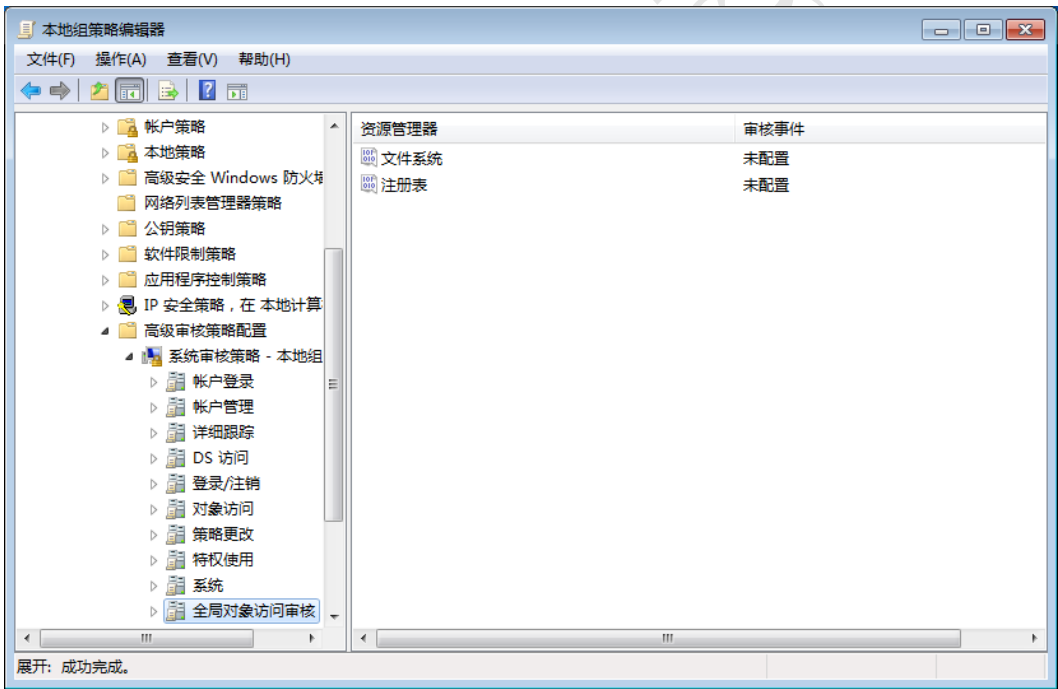
选择“系统”策略，设置“审核IPsec驱动程序”、“审核安全状态改变”、“审核安全系统扩展”、“审核系统完整性”为“成功和失败”，如图4-16所示。

图 4-16: 系统策略



选择“全局对象访问”策略，可以通过设置“文件系统”和“注册表”进行相关全局对象访问审核，如图4-17所示。

图 4-17: 全局对象策略



4.7 问题回答

如何使用组策略取消Windows系统提供的最近访问文件列表功能？

<http://tang.chat>

§ 5

数据备份恢复技术

5.1 实验名称

数据备份恢复技术

5.2 实验目的

1. 了解数据备份的意义;
2. 理解冷备份、热备份、在线备份、离线备份等相关概念;
3. 理解完全备份、增量备份、差异备份的原理;
4. 掌握备份工具的使用方法。

5.3 实验原理

信息安全技术中，备份指计算机存储数据的拷贝，当数据丢失时可以通过备份恢复原有数据，它提供了一种简单的数据灾难恢复方法。

5.4 实验材料

1. 运行Windows 7或更高版本操作系统的PC机一台。
2. Rsync v3.1.3软件压缩包。

5.5 实验步骤

1. 安装rsync
2. 使用rsync
 - (a) 准备测试环境

(b) 测试完全备份

(c) 测试差异备份

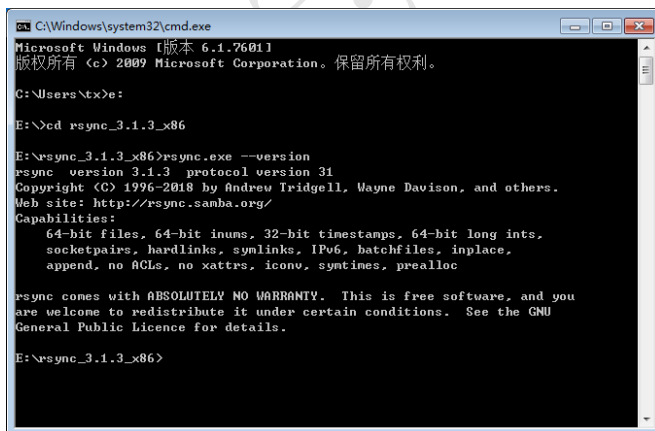
(d) 测试增量备份

5.6 实验记录

5.6.1 安装Rsync

将“rsync_3.1.3_x86.zip”文件解压至目录“E:\”，打开命令行窗口并进入该目录，执行“rsync --version”命令查看rsync版本，如图5-1所示。

图 5-1: 查看rsync版本



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\tx>E:
E:\>cd rsync_3.1.3_x86
E:\rsync_3.1.3_x86>rsync.exe --version
rsync Version 3.1.3 protocol version 31
Copyright (C) 1996-2018 by Andrew Tridgell, Wayne Davison, and others.
Web site: http://rsync.samba.org/
Capabilities:
  64-bit files, 64-bit inums, 32-bit timestamps, 64-bit long ints,
  socketpairs, hardlinks, symlinks, IPv6, batchfiles, inplace,
  append, no ACLs, no xattrs, iconv, symlinks, prealloc

rsync comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. See the GNU
General Public Licence for details.

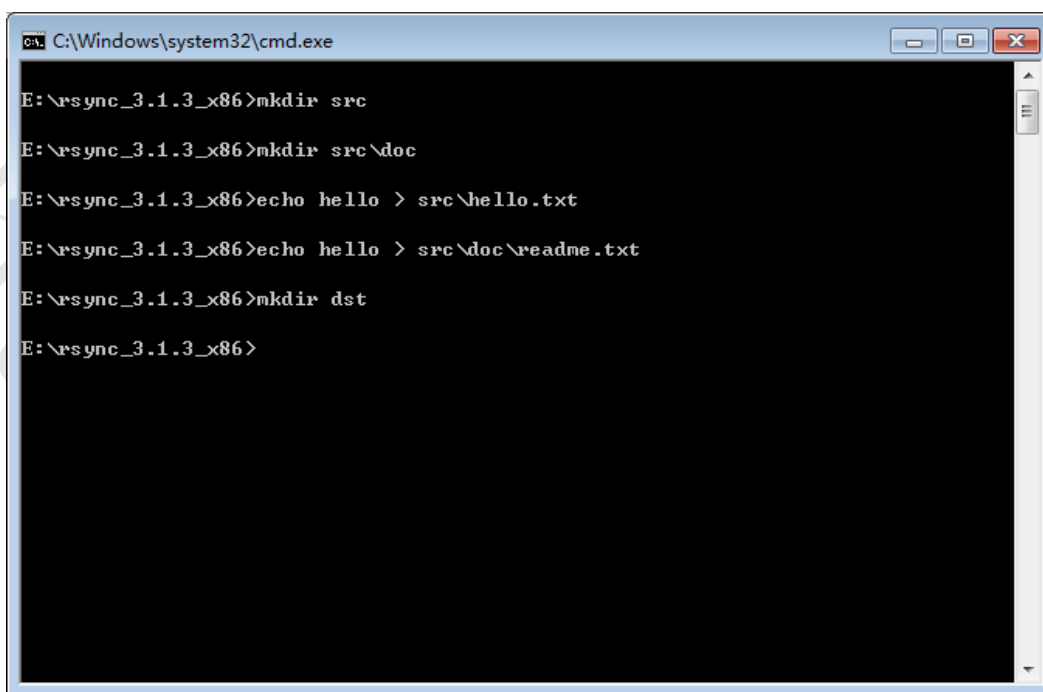
E:\rsync_3.1.3_x86>
```

5.6.2 使用Rsync

准备测试环境

使用DOS命令创建src、dst目录，并在src目录下创建hello.txt文件、doc子目录，以及doc子目录下的readme.txt文件，接着查看是否创建成功，如图5-2、5-3所示。

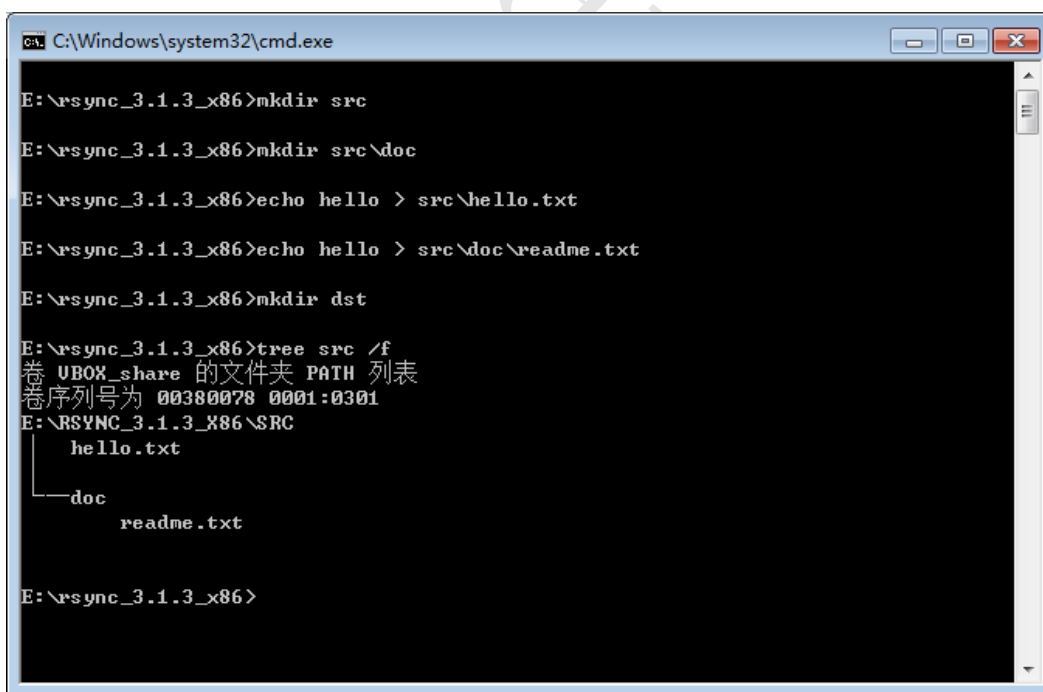
图 5-2: 创建测试环境



```
C:\Windows\system32\cmd.exe

E:\rsync_3.1.3_x86>mkdir src
E:\rsync_3.1.3_x86>mkdir src\doc
E:\rsync_3.1.3_x86>echo hello > src\hello.txt
E:\rsync_3.1.3_x86>echo hello > src\doc\readme.txt
E:\rsync_3.1.3_x86>mkdir dst
E:\rsync_3.1.3_x86>
```

图 5-3: 查看测试环境



```
C:\Windows\system32\cmd.exe

E:\rsync_3.1.3_x86>mkdir src
E:\rsync_3.1.3_x86>mkdir src\doc
E:\rsync_3.1.3_x86>echo hello > src\hello.txt
E:\rsync_3.1.3_x86>echo hello > src\doc\readme.txt
E:\rsync_3.1.3_x86>mkdir dst
E:\rsync_3.1.3_x86>tree src /f
卷 UBOX_share 的文件夹 PATH 列表
卷序列号为 00380078 0001:0301
E:\RSYNC_3.1.3_X86\SRC
|   hello.txt
|___doc
|       readme.txt

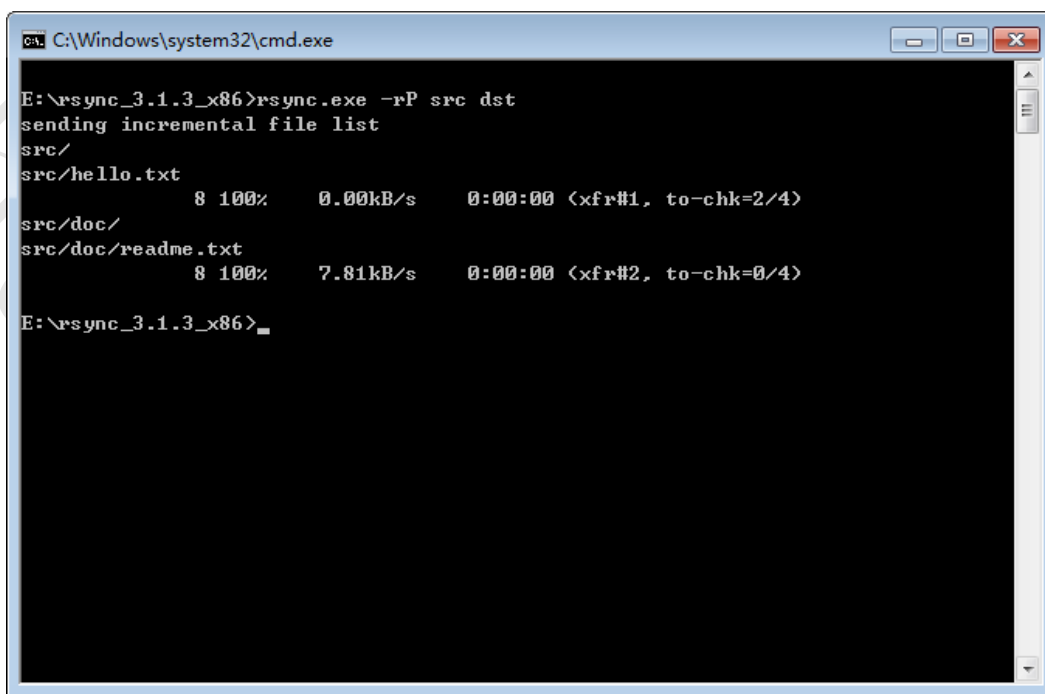
E:\rsync_3.1.3_x86>
```

测试完全备份

使用“rsync -rP src dst”命令将src目录完全备份至dst目录下，其中“-r”选项代表递归处理src目录及其包含的所

有文件和子目录，“-P”选项代表显示备份进程，如图5-4所示。

图 5-4: 完全备份



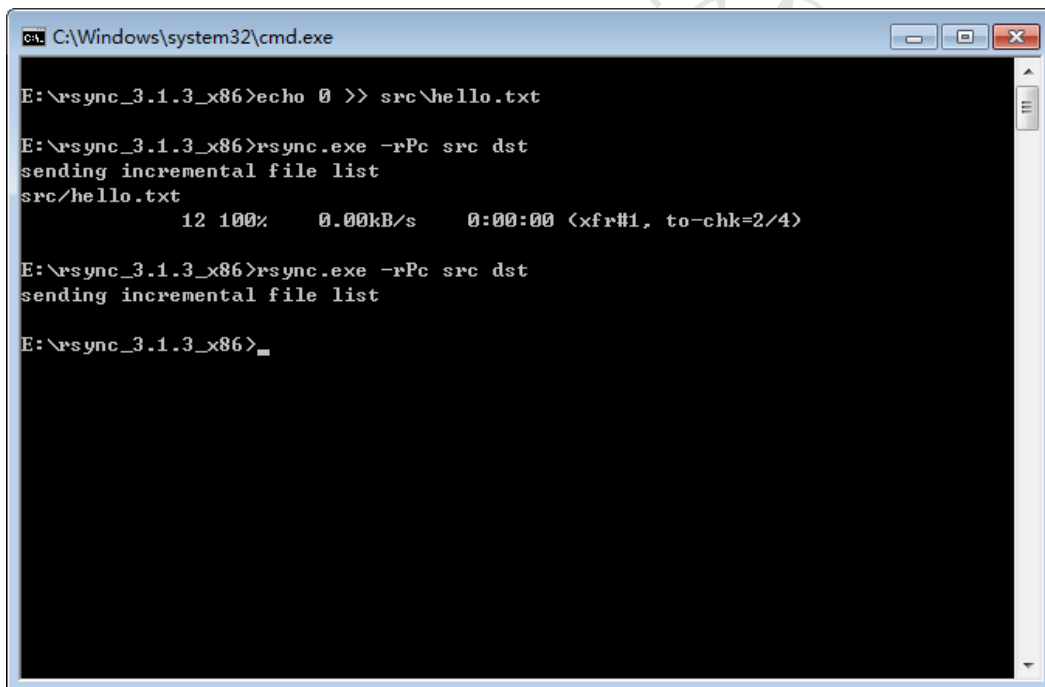
```
C:\Windows\system32\cmd.exe

E:\rsync_3.1.3_x86>rsync.exe -rP src dst
sending incremental file list
src/
src/hello.txt
      8 100%   0.00kB/s   0:00:00 <xfr#1, to-chk=2/4>
src/doc/
src/doc/readme.txt
      8 100%   7.81kB/s   0:00:00 <xfr#2, to-chk=0/4>

E:\rsync_3.1.3_x86>_
```

修改src目录下的hello.txt文件，在如图5-4所示命令选项基础上使用“-c”选项以校验和算法对文件进行校验判断文件是否改动，仅备份改动后的文件，如图5-5所示。

图 5-5: 备份改动文件



```
C:\Windows\system32\cmd.exe

E:\rsync_3.1.3_x86>echo 0 >> src\hello.txt


E:\rsync_3.1.3_x86>rsync.exe -rPc src dst
sending incremental file list
src/hello.txt
     12 100%   0.00kB/s   0:00:00 <xfr#1, to-chk=2/4>

E:\rsync_3.1.3_x86>rsync.exe -rPc src dst
sending incremental file list

E:\rsync_3.1.3_x86>_
```

继续修改src目录下的hello.txt文件，在如图5-5所示命令选项基础上使用“-b”选项判断dst目录相应位置下是否已经存在同名目标文件，若存在则通过修改目标文件名称的方式备份目标文件，从而确保不会覆盖已经存在的目标文件，如图5-6所示。

图 5-6: 备份改动文件和目标文件



```
C:\Windows\system32\cmd.exe

E:\rsync_3.1.3_x86>echo 1 >> src\hello.txt

E:\rsync_3.1.3_x86>rsync.exe -rPcb src dst
sending incremental file list
src/hello.txt
      16 100%   0.00kB/s   0:00:00 (xfr#1, to-chk=2/4)

E:\rsync_3.1.3_x86>dir dst\src\
驱动器 E 中的卷是 UBOX_share
卷的序列号是 0001-0301

E:\rsync_3.1.3_x86>dir dst\src 的目录
2020/10/29  16:30                12 hello.txt~
2020/10/29  16:37                16 hello.txt
2020/10/29  16:28             <DIR>          doc
               2 个文件              4,124 字节
               1 个目录      6,506,328,064 可用字节

E:\rsync_3.1.3_x86>
```

继续修改src目录下的hello.txt文件，在如图5-6所示命令选项基础上使用“-suffix=.20201029.tx”选项为目标文件名称添加指定格式后缀，如图5-7所示。

图 5-7: 添加指定格式后缀

```
C:\Windows\system32\cmd.exe

E:\rsync_3.1.3_x86>echo 2 >> src\hello.txt

E:\rsync_3.1.3_x86>rsync.exe -rPcb --suffix=.20201029.tx src dst
sending incremental file list
src/hello.txt
 20 100%  0.00kB/s  0:00:00 (xfr#1, to-chk=2/4)

E:\rsync_3.1.3_x86>dir dst\src
驱动器 E 中的卷是 UBOX_share
卷的序列号是 0001-0301

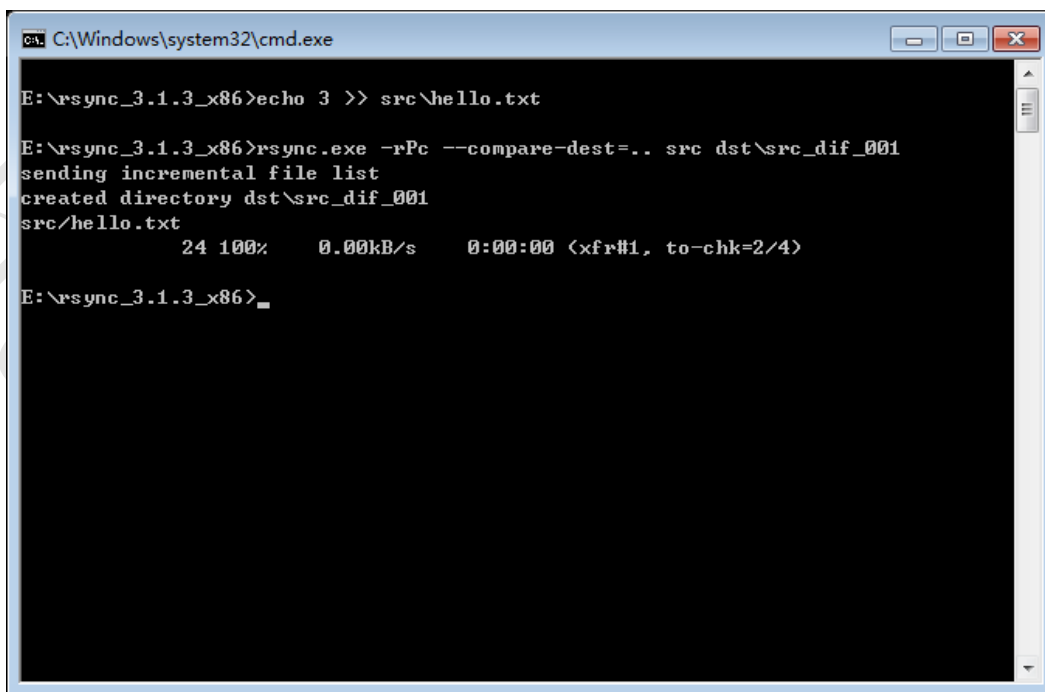
E:\rsync_3.1.3_x86\dst\src 的目录
2020/10/29  16:37                16 hello.txt.20201029.tx
2020/10/29  16:30                12 hello.txt~
2020/10/29  16:41                20 hello.txt
2020/10/29  16:28                <DIR>          doc
               3 个文件             4,144 字节
               1 个目录      6,506,315,776 可用字节

E:\rsync_3.1.3_x86>
```

测试差异备份

继续修改src目录下的hello.txt文件，在如图5-5所示命令选项基础上使用“-compare-dest=..”选项比较上一次完全备份目录和来源目录之间的文件差异并备份至目标目录，这里的“..”是指目标目录（即dst\src_dif_001）的父目录，如图5-8所示。

图 5-8: 差异备份



```
C:\Windows\system32\cmd.exe

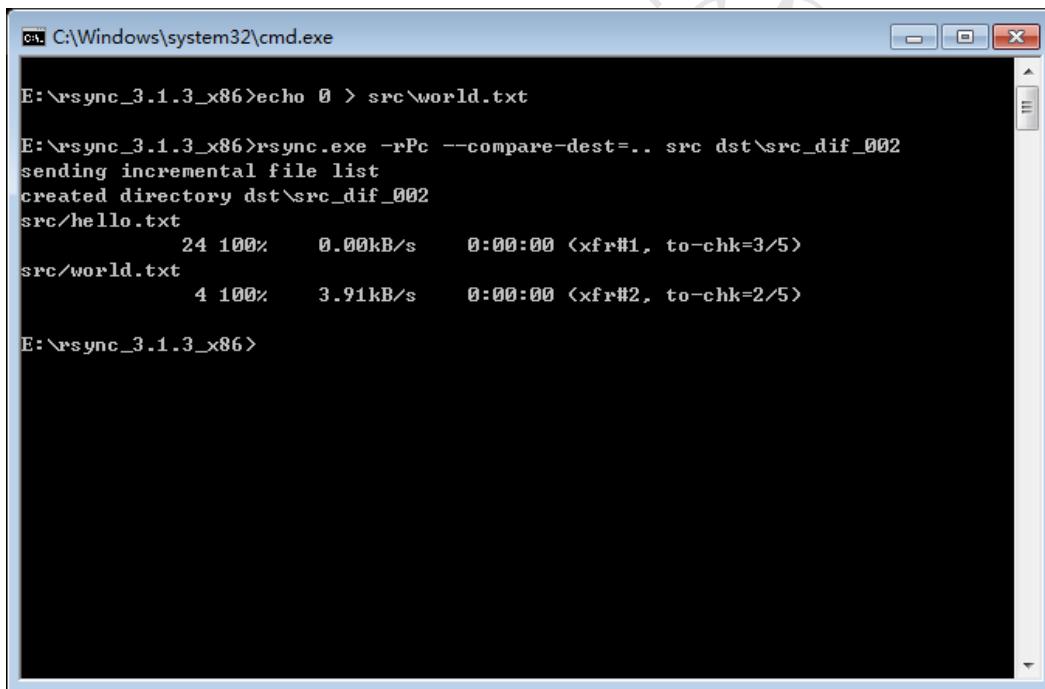
E:\rsync_3.1.3_x86>echo 3 >> src\hello.txt

E:\rsync_3.1.3_x86>rsync.exe -rPc --compare-dest=.. src dst\src_dif_001
sending incremental file list
created directory dst\src_dif_001
src/hello.txt
      24 100%   0.00kB/s   0:00:00 <xfr#1, to-chk=2/4>

E:\rsync_3.1.3_x86>
```

在src目录下创建world.txt文件，继续使用进行差异备份，如图5-9所示。

图 5-9: 继续进行差异备份



```
C:\Windows\system32\cmd.exe

E:\rsync_3.1.3_x86>echo 0 > src\world.txt

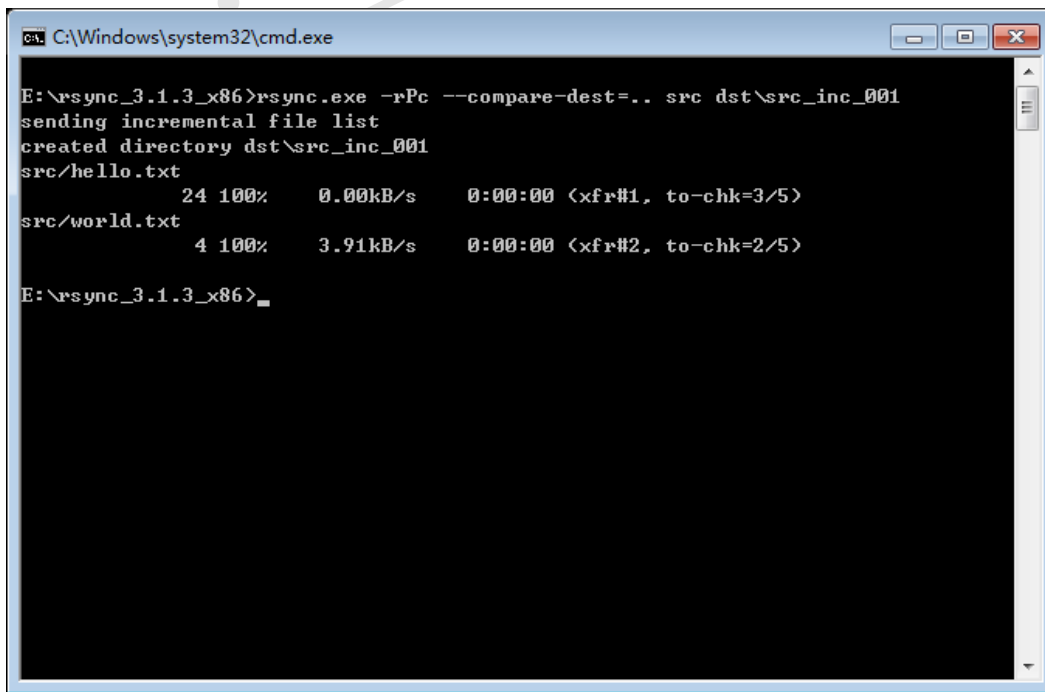
E:\rsync_3.1.3_x86>rsync.exe -rPc --compare-dest=.. src dst\src_dif_002
sending incremental file list
created directory dst\src_dif_002
src/hello.txt
      24 100%   0.00kB/s   0:00:00 <xfr#1, to-chk=3/5>
src/world.txt
       4 100%  3.91kB/s   0:00:00 <xfr#2, to-chk=2/5>

E:\rsync_3.1.3_x86>
```

测试增量备份

使用“--compare-dest=..”选项比较上一次备份目录和来源目录之间更改的文件并备份至目标目录，这里的“..”是指目标目录（即dst\src_inc_001）的父目录，如图5-10所示。

图 5-10: 增量备份



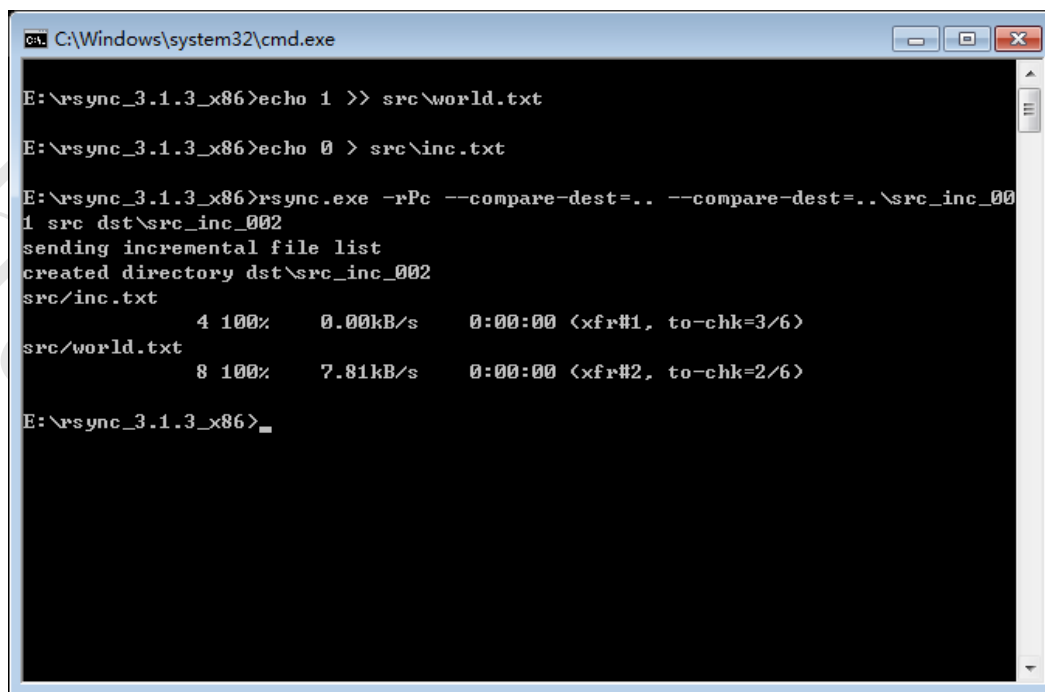
```
C:\Windows\system32\cmd.exe

E:\rsync_3.1.3_x86>rsync.exe -rPc --compare-dest=.. src dst\src_inc_001
sending incremental file list
created directory dst\src_inc_001
src/hello.txt
      24 100%   0.00kB/s   0:00:00 <xfr#1, to-chk=3/5>
src/world.txt
       4 100%   3.91kB/s   0:00:00 <xfr#2, to-chk=2/5>

E:\rsync_3.1.3_x86>
```

修改“world.txt”文件并添加“inc.txt”文件，使用“--compare-dest=..\src_inc_001”选项比较上一次备份目录（即src_inc_001目录）和来源目录之间更改的文件并备份至目标目录，如图5-11所示。

图 5-11: 继续增量备份



```
ca. C:\Windows\system32\cmd.exe

E:\rsync_3.1.3_x86>echo 1 >> src\world.txt

E:\rsync_3.1.3_x86>echo 0 > src\inc.txt

E:\rsync_3.1.3_x86>rsync.exe -rPc --compare-dest=.. --compare-dest=..\src_inc_00
1 src dst\src_inc_002
sending incremental file list
created directory dst\src_inc_002
src/inc.txt
      4 100%   0.00kB/s   0:00:00 (xfr#1, to-chk=3/6)
src/world.txt
      8 100%   7.81kB/s   0:00:00 (xfr#2, to-chk=2/6)

E:\rsync_3.1.3_x86>_
```

5.7 问题回答

比较增量备份和差异备份之间的区别和优缺点。

<http://tang.chat>

§ 6

软件破解保护技术

6.1 实验名称

软件破解保护技术

6.2 实验目的

1. 了解软件保护的重要性;
2. 了解常见的软件破解过程;
3. 理解Windows可执行文件结构;
4. 掌握软件加壳脱壳技术;
5. 掌握软件动态调试技术。

6.3 实验原理

常见软件破解过程会先分析目标程序文件结构，然后使用脱壳技术去除目标程序外部的保护程序，接着使用静态或动态分析技术研究程序代码逻辑，从而找到破解办法。

6.4 实验材料

1. 运行Windows 7或更高版本操作系统的PC机一台。
2. tx_win.trial.exe测试程序;
3. PEiD v0.95软件压缩包;
4. UPX v3.96软件压缩包;
5. OllyDBG v1.10软件压缩包。

6.5 实验步骤

1. 准备测试环境
2. 使用PEiD分析测试程序
3. 使用UPX脱壳测试程序
4. 使用OllyDBG调试测试程序

6.6 实验记录

6.6.1 准备测试环境

准备“tx_win.trial.exe”测试程序，其执行结果如图6-1所示。

图 6-1: 准备测试程序



分别解压“PEiD-0.95-20081103.zip”、“upx-3.96-win32.zip”、“odbg110.zip”等文件，如图6-2、6-3、6-4所示。

图 6-2: 解压PEiD

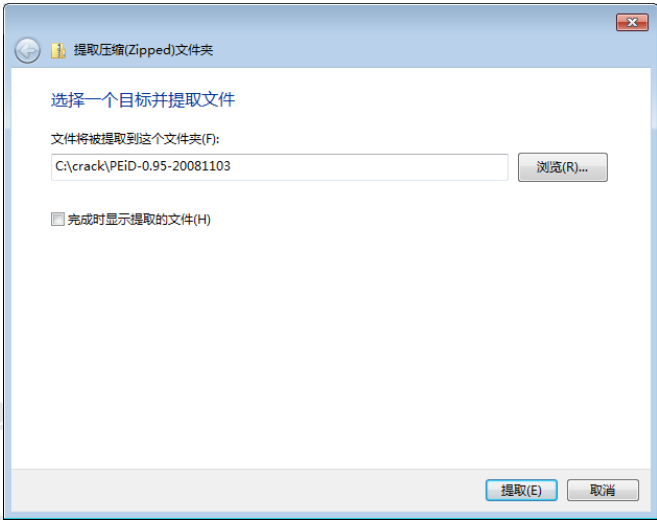


图 6-3: 解压UPX

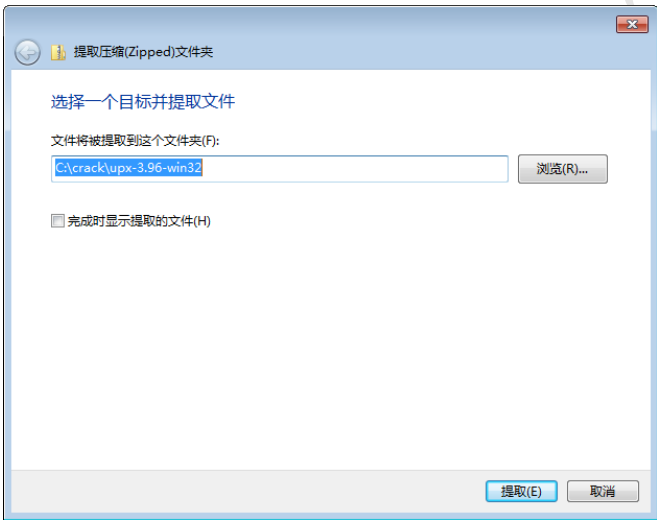
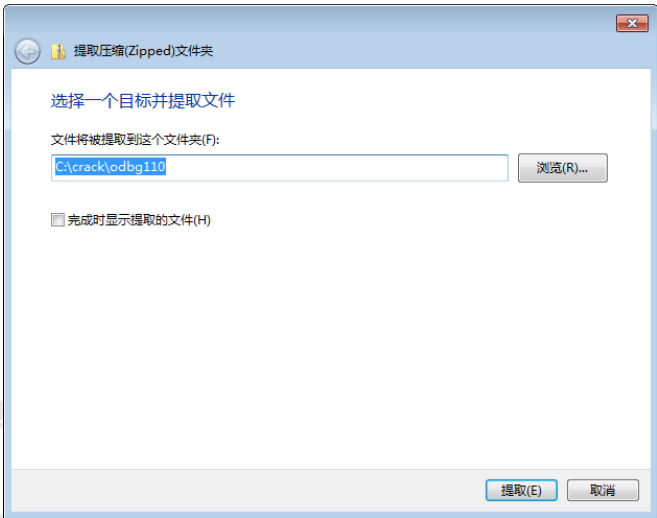


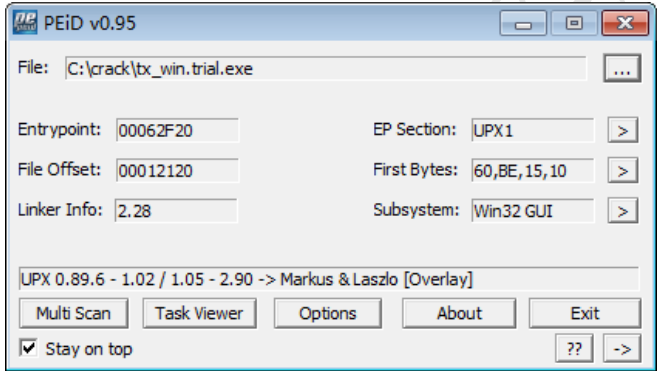
图 6-4: 解压Ollydbg



6.6.2 使用PEiD分析测试程序

使用PEiD加载并分析测试程序，可以观察到“Overlay”附近存在UPX壳相关信息提示，如图6-5所示。

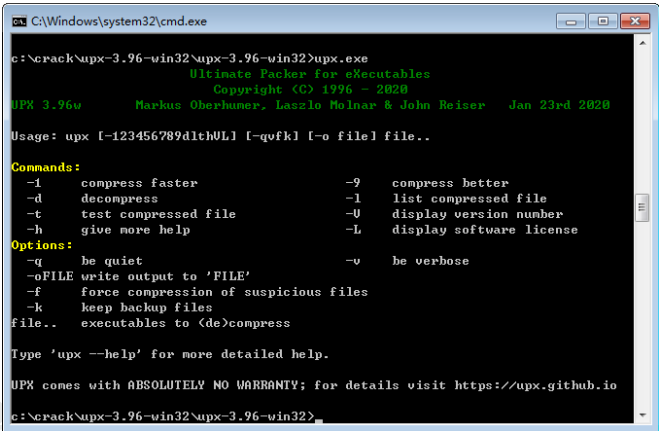
图 6-5: 使用PEiD分析测试程序



6.6.3 使用UPX脱壳测试程序

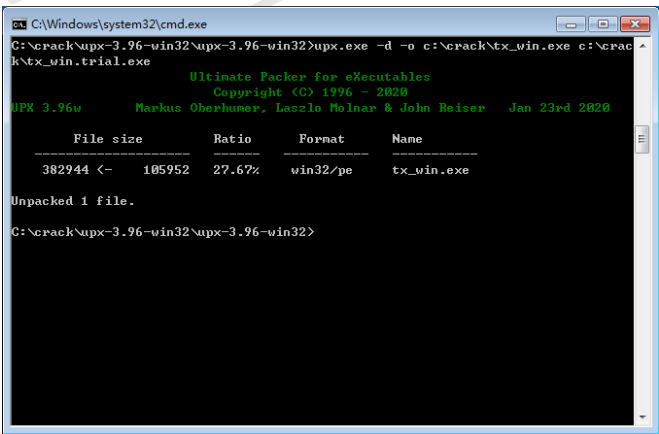
打开命令行窗口，进入UPX解压目录，使用“upx.exe”命令查看命令帮助，如图6-6所示。

图 6-6: 查看UPX命令帮助



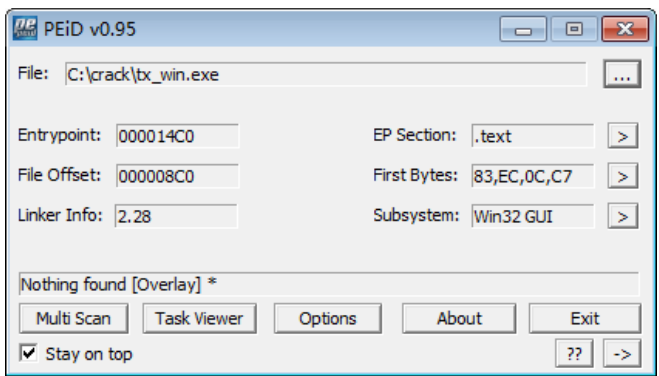
使用“-d”选项解压缩测试程序，并重新命名为“tx_win.exe”，如图6-7所示。

图 6-7: 使用UPX脱壳测试程序



使用PEiD加载并分析“tx_win.exe”，可以观察到“Overlay”附近提示没有加壳，如图6-8所示。

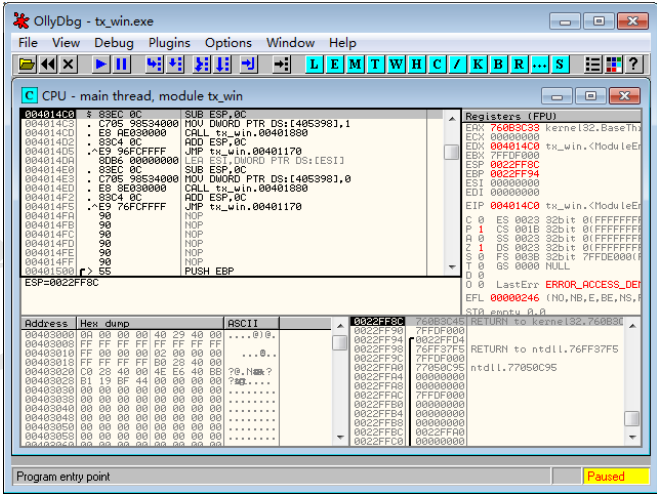
图 6-8: 使用PEiD分析脱壳测试程序



6.6.4 使用Ollydbg调试测试程序

进入Ollydbg解压目录，执行Ollydbg程序并打开“tx_win.exe”程序，如图6-9所示。

图 6-9: 打开脱壳测试程序



使用鼠标右键单击代码区别，弹出右键菜单，选择“Search for”-“All referenced text strings”选项搜索并显示参考文本列表，如图6-10、6-11所示。

图 6-10: 搜索参考文本列表

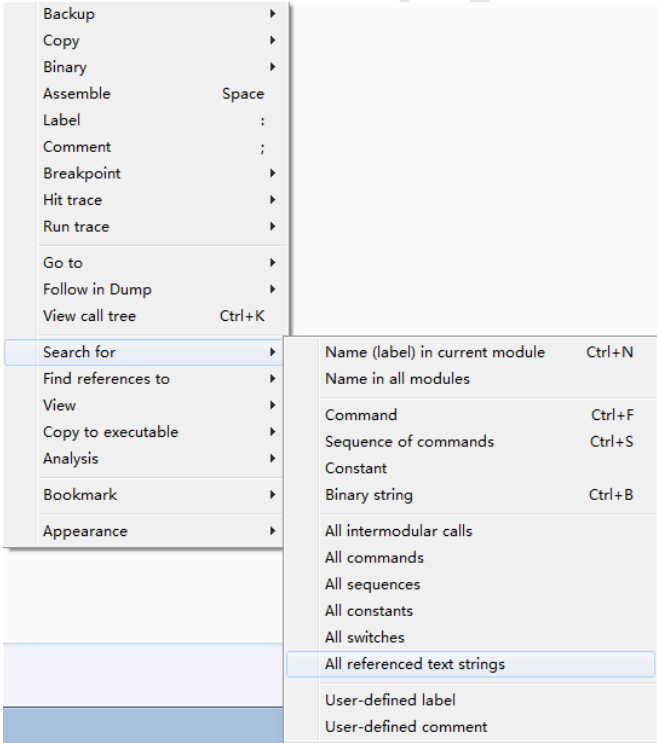
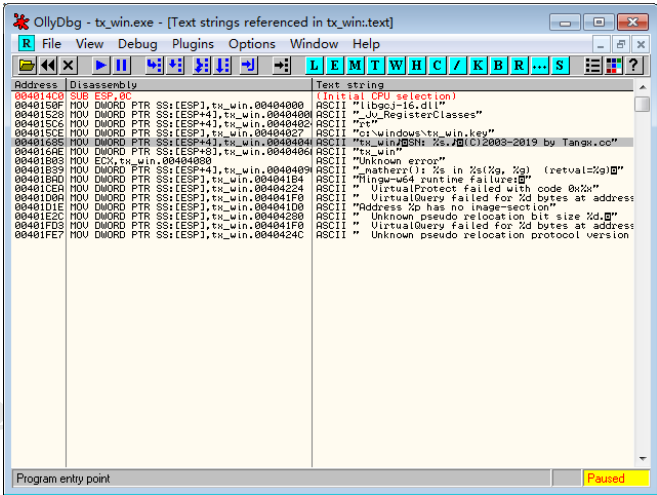


图 6-11: 显示参考文本列表

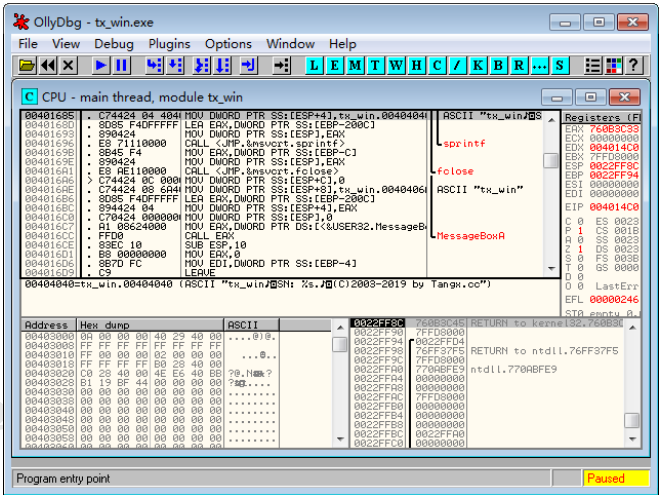


使用鼠标右键单击“tx_win\r\nSN:.....”文本，弹出右键菜单，选择“Follow in Disassembler”选项跟随到汇编程序中参考文本所在位置，如图6-12、6-13所示。

图 6-12: 跟随参考文本位置

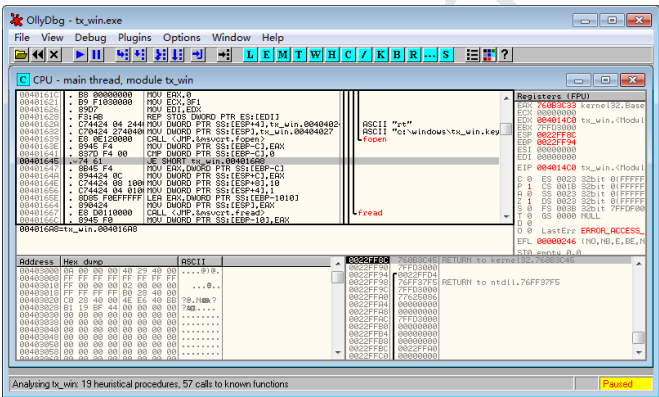
Follow in Disassembler	Enter
Search for text	
Search next	Ctrl+L
Toggle breakpoint	F2
Conditional breakpoint	Shift+F2
Conditional log breakpoint	Shift+F4
Set breakpoint on every command	
Set log breakpoint on every command	
Copy to clipboard	▶
Appearance	▶

图 6-13: 显示参考文本位置



通过对程序进行分析，判断测试程序的序列号存储于“C:\windows\tx_win.key”文件中，如果不存在则提示为试用版，如图6-14所示。

图 6-14: 分析脱壳测试程序



创建“C:\windows\tx_win.key”文件，重新执行测试文件，如图6-15、6-16所示。

图 6-15: 创建相关注册文件

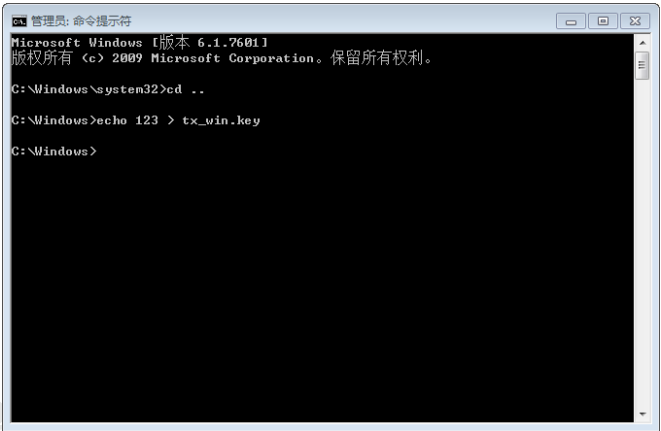
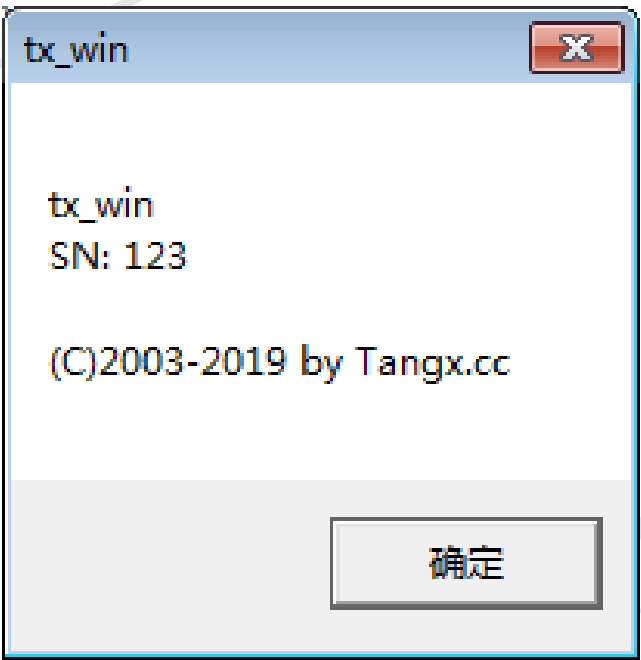


图 6-16: 重新执行测试文件



6.7 问题回答

列出3种以上常见软件保护技术并简述各自的优缺点。

<http://tang.chat>

参考文献

- [1] 火狐浏览器
<http://ftp.mozilla.org/pub/firefox/releases/52.9.0esr/win32/zh-CN/>
- [2] OpenSSL第三方网站列表
<https://wiki.openssl.org/index.php/Binaries>
- [3] OpenSSL (mingw) 版下载
<https://bintray.com/vszakats/generic/openssl>
- [4] Wireshark官方网站
<https://wireshark.org>
- [5] WinPcap官方网站
<https://winpcap.org>
- [6] Npcap官方网站
<https://nmap.org/npcap>
- [7] 入侵检测系统维基百科
http://en.wikipedia.org/wiki/Intrusion_detection_system
- [8] Snort官方网站
<https://www.snort.org>
- [9] Windows安全基线指南
<https://docs.microsoft.com/zh-cn/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines>
- [10] Windows安全基线工具箱
<https://www.microsoft.com/en-us/download/details.aspx?id=55319>
- [11] RSYNC备份同步工具
<https://rsync.samba.org/>

[12] PEiD官方网站

<https://www.aldeid.com/wiki/PEiD>

[13] UPX官方网站

<https://upx.github.io>

[14] OllyDBG官方网站

<http://www.ollydbg.de>