教职工政治学习参考资料

（2023 年第 4 期）

苏州大学党委宣传部编

2023 年 4 月 24 日

教职工政治学习参考资料

（2023 年第 4 期）

苏州大学党委宣传部编　　2023 年 4 月 24 日

● 学习内容

网络安全专题学习

● 参考资料

苏州大学2023年
网络安全培训

目 录

Contents

01 本次培训的目的是什么？

培训目的

1.提高大家安全意识，注重敏感信息保护

（1）个人隐私

（2）工作机密

2.养成良好的安全习惯

（1）电脑使用

（2）服务器管理

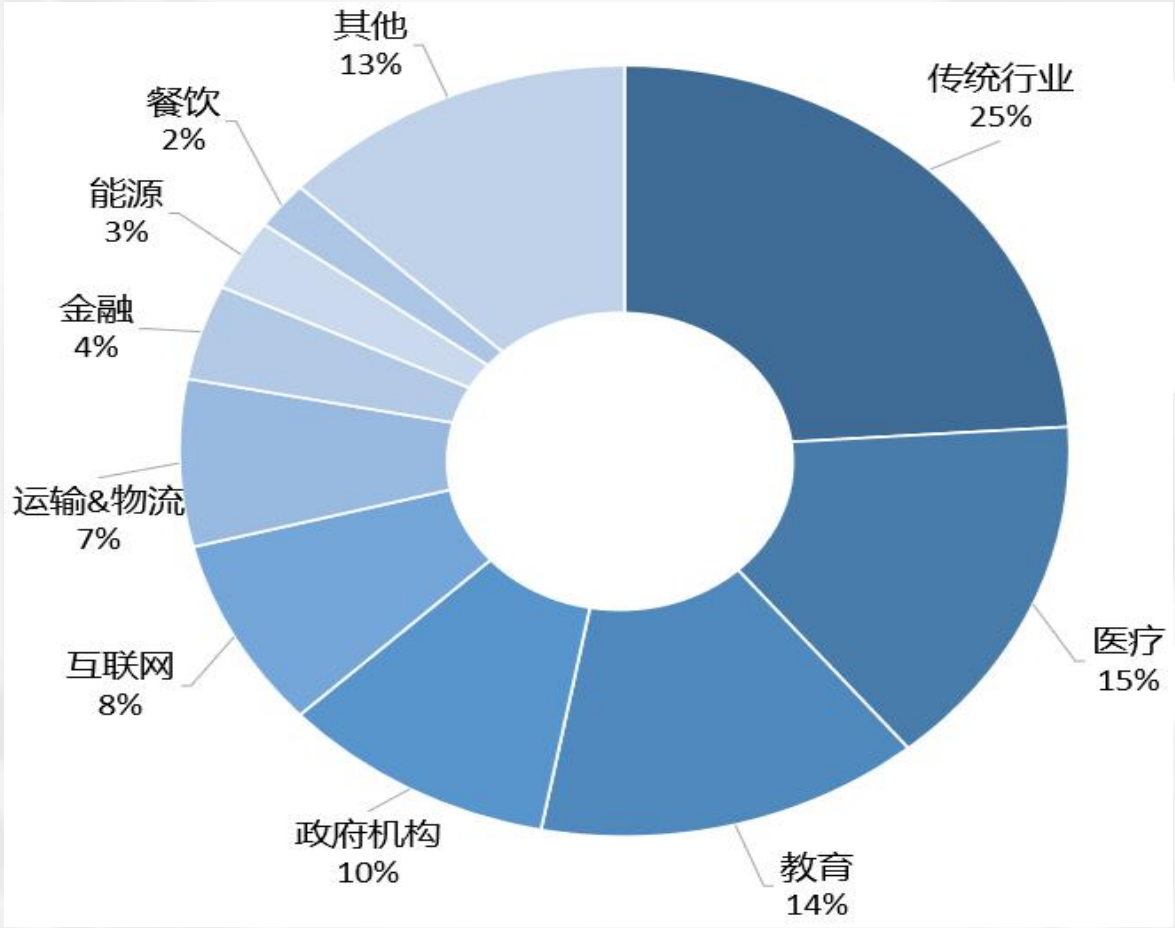
02 如何安全的管理学校服务器?

2022年10月全国勒索攻击地域分布

本月国内遭受勒索病毒攻击的地区分布图如下所示，数字经济发达地区仍是攻击的主要对象，与上个月相比，无较大波动。

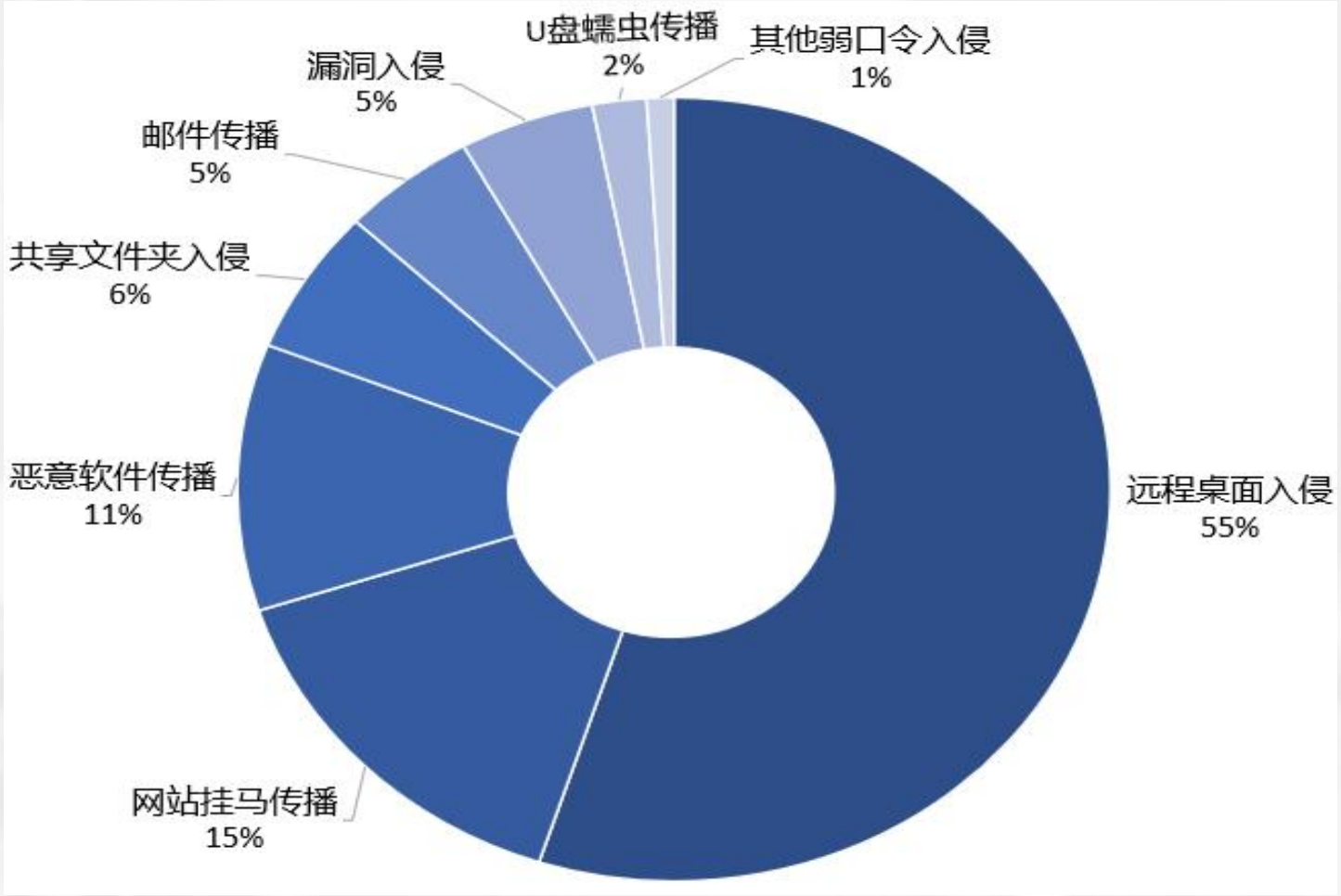
2022年10月勒索病毒影响行业分布

从行业划分来看，数据价值较高的传统行业、医疗、教育、政府机构遭受攻击较为严重。



勒索病毒传播方式

右图为勒索病毒传播的各种方式的占比情况。根据统计可以看出，可以看出勒索病毒的主要攻击方式依然以**远程桌面入侵**为主，其次为通过海量的**垃圾邮件**传播，或利用网站挂马和高危漏洞等方式传播，整体攻击方式呈现**多元化**的特征。



勒索病毒原理与危害

① 病毒进入内网

漏洞
邮件
程序木马
网页挂马
存储设备带入
office组件的病毒感染
人工投毒

② 内网扩散

永恒之蓝
双脉冲星
永恒之冠
永恒浪漫
永恒王者
永恒协作
等等

③ 病毒运行

通过脚本文件进行Http请求
通过脚本文件下载文件
读取远程服务器文件
收集计算机信息
进程遍历文件
调用加密算法运行加密进程

勒索病毒防护建议

10月中旬，辽宁某企业遭到勒索病毒攻击

河南某企业遭遇Phobos勒索软件攻击，导致数十台服务器沦陷

国内某企业反馈其遭遇LockBit 3.0勒索病毒攻击

勒索病毒防护建议

- 及时给办公终端和服务器打补丁，修复漏洞，包括操作系统以及第三方应用的补丁，防止攻击者通过漏洞入侵系统；
- 尽量关闭不必要的端口，如139、445、3389等端口。如果不使用，可直接关闭高危端口，降低被漏洞攻击的风险；
- 不对外提供服务的设备不要暴露于公网之上，对外提供服务的系统，应保持较低权限；
- 用户应采用高强度且无规律的密码来登录办公系统或服务器，要求包括数字、大小写字母、符号，且长度至少为8位的密码，并定期更换口令；
- 数据备份保护，对关键数据和业务系统做备份，如离线备份，异地备份，云备份等， 避免因为数据丢失、被加密等造成业务停摆，甚至被迫向攻击者妥协。
- 敏感数据隔离，对敏感业务及其相关数据做好网络隔离。避免双重勒索病毒在入侵后轻易窃取到敏感数据，对公司业务和机密信息造成重大威胁
- 尽量关闭不必要的文件共享
- 提高安全运维人员职业素养，定期进行木马病毒查杀。

今天，
你对外开放**高危端口**了吗？

高危端口

常见的高危端口如下：

端口号	对应服务（默认）
21	FTP
22	SSH
23	TELNET
139、445	SMB
3306	MYSQL
3389	RDP
省略。。	

高危端口列表

参考文章：https://www.cnblogs.com/blacksunny/articles/11735284.html

高危端口—真实案例admin/admin

你的密码，
真的足够**复杂**吗？

账号安全—密码规律

手机号：18888888888
姓名缩写+出生日期：ZW19871001
姓名缩写+出生日期+特殊符号：ZD_20031223

普通人，正常使用的密码，

一般不会超过3个！

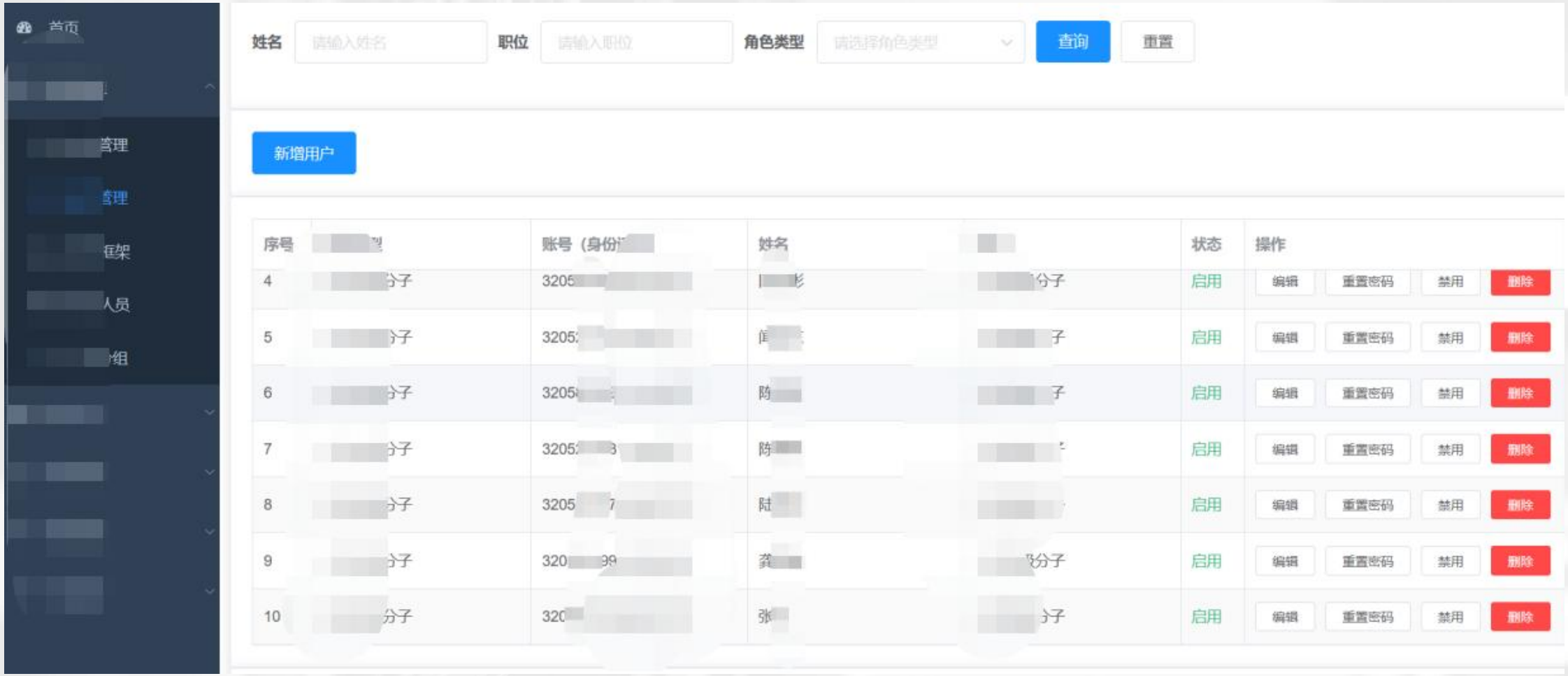
账号安全

1.密码长度大于8位
2.内含大小写字母以及特殊符号
3.无明显规律（一般人想不到、只有自己知道的规律）

示例（假设我生日是3月3日）：
WwwYyyXxx3}6

含义：
字母名字缩写*3，且开头都大写
生日第二个3用相似的特殊符号代替
末尾再加个随机数，数字是3+3=6

web系统弱口令—真实案例



你真的了解，手中的网络**资产**吗？

资产清单

紧急通知！Apache服务爆出最新远程代码执行漏洞，请尽快将装有该服务的系统打上补丁！

完了！我完全不知道哪个服务器开启了Apache服务！

资产清单—包含内容

系统名称：XXX新人报道系统
IP地址：192.168.12.23
url地址：http://xxx.com
开放端口：22，80
运行服务：ssh，nginx

(以上是最基本的资产清单)

下面还可以根据学校具体情况额外增加

开发语言：PHP
数据库：Mysql
框架：ThinkPHP
负责人：XXX

(省略若干……)

资产清单—真实案例

	A	B	C	D	E	F
1	资产名称	host	url	ip	port	service
2	农业 中心		http:/	2	110	
3	能源 中心		http:/	2		
4	汽车 室	http:/	http://qcs cn	20		
5	校史	http://	http://xsg	20		
6	分析	http:// n	http://fxc cn	20		
7	党风 实信息平台	http:// n	http://jdl cn	20		3
8	网络	http://	http://top	20		
9	职工 理系统	http://z	http://zgt	20		
10	材料 实验室仪器预约系统	http://c .cn	http://cls du.cn/link	20		
11	apps	http://a	http://app	20	09	
12	计算 心	http://c	http://cc n	20	8000	t
13	计算 _8000	http://c 3000	http://cc n:8000	20	3000	
14	城市	http://ci .cn	http://ci du.cn	20	81	icecap
15	城市 0	http://ci .cn:8080	http://ci du.cn:8080	20	81	cap
16	财务	http://c	http://c	20	443	
17	财务	http://c 8080	http://c :8080	20	443	http, pop3, t
18	大学 管理系统	http://c	http://c	20		, pop3
19	大学 教育中心	http://s n	http://s cn	20		, pop3
20	档案 理系统	http://c n	http://d cn	20	3009	p13
21	成绩	http:// n/page/fyxt	http://d cn/page/fyxt/fyxtl	20	3009	13
22	实验 系统	http://	http://c	20		
23	实验 系统_8080	http:// 8080	http:// :8080	20		v
24	IBM	http:// cn	http:// . cn	20	060, 910	known, CardWeb-IO, jetdir
25	IBM	http:// u. cn	http:// du. cn	20	060, 910	
26	金智 台	http://	http:/ n	20	060, 910	dir
27	离校	http://	http:/	20	060, 910	dir
28	IBM	http://	http:/ n	20	060, 910	ir
29	金智	http://	http:/ n	20	060, 910	ir
30	电子	http:// n	http:/ cn	20		
31	新中 对系统	http://	http:/ cn	20	900, 850	, pop3, msrpc, microsoft-ds, ms-wbt-server, vnc, fm
32	金龙 通网站查询子系统	http:// n	http:/ d. u. cn	20		http, pop3
33	能源 验教学示范中心	http:// s n	http:/ b . cn	20		
34	工业	http:// du	http:/	20		
35	房地	http:/ du.	http://1	20		-sql-s
36	食品 中心	http:/ ujs n	http://f cn	20	0 , 9010	ing, sdr
37	食品	http: js. :8090	http://fc :8090/	20	0 9010	, sdr
38	食品 设备使用预	http s. /yysys	http://fc /yysys/index.h	20	9010	. sdr
39	华三	http	http://h3	17	800, 8	sunwebadm
40	华三 080	http 080	http://h3c :8080	172	800, 8	sunwebadm

你真的
保护敏感信息/文件了吗?

哪些属于敏感信息/文件?

用户隐私相关:
真实信息
身份证号
手机号
家庭住址
账号密码
银行卡号
社保卡号
(…省略若干)

服务器相关:
测试文件
配置文件
网站源码
说明文件
注释内容（包含敏感信息）
(…省略若干)

保护敏感信息/文件

那我们应该如何做才能规避这个问题?

1.只要涉及到用户隐私的内容，都进行模糊化处理。禁止网站/系统公开用户隐私信息。

2.定期检查服务器是否存在未删除的测试文件、网站源码压缩包、不需要展示的说明文件。

3.督促开发厂商，禁止在注释中遗留敏感信息。如开发人员为了方便，将测试账号密码写在注释中，**不仅方便了自己，也方便了攻击者。**

4.配置文件所在目录，一定要设置访问权限。禁止无关人员进行访问。

保护敏感信息/文件—真实案例

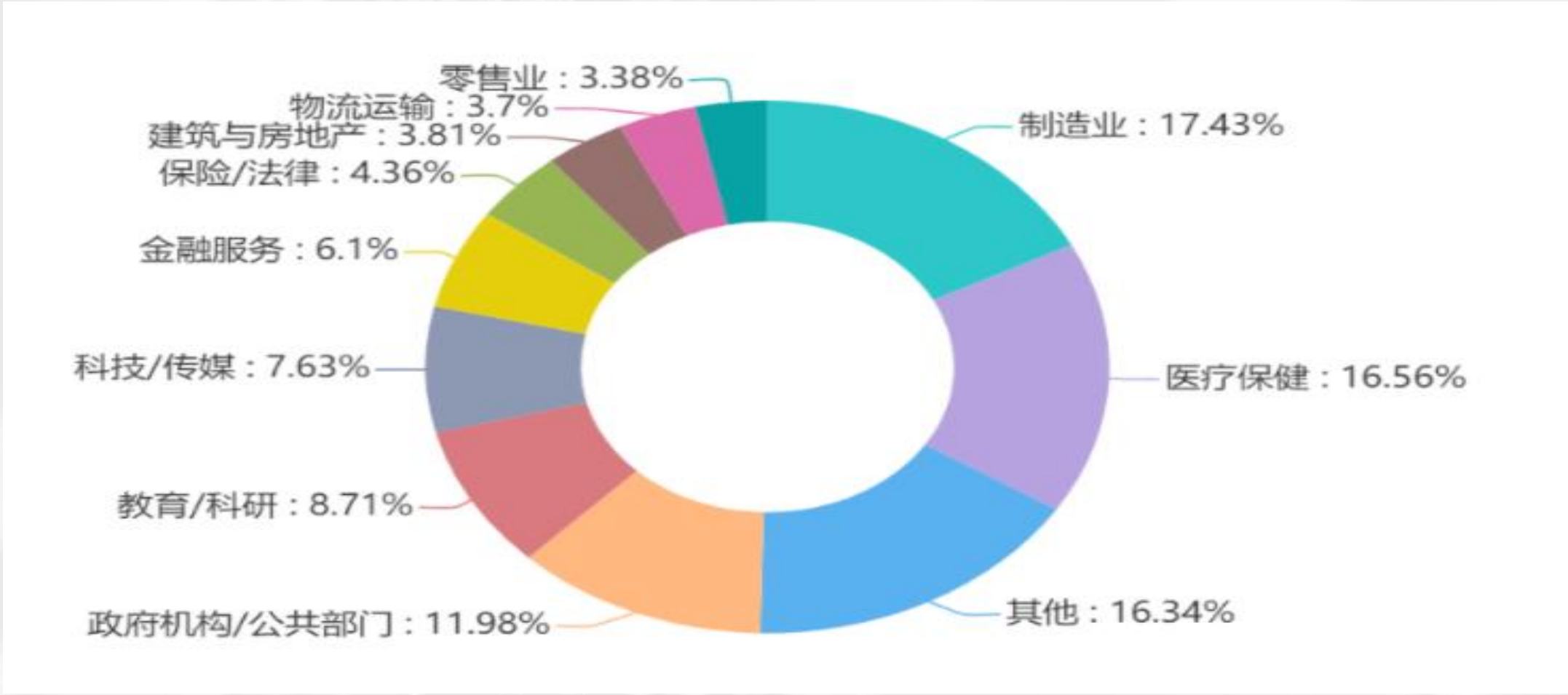
此工作簿已引用其他表格数据，是否更新工作簿以同步最新数据？ 更新

D22

	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
2	单位负责人签名：									学院（部）（公章）：											
3	最高学历取得时间	毕业学校	所学专业	最高学位	最高学位取得时间	毕业学校	所学专业	申报系列	现聘岗位	拟申报职务	职务级别	现职称	现职称取得时间	本专业工作年限	基本合格、不合格年度	岗前培训通过时间	身份证号码	申报人联系电话	2021年外审结果	是否使用去年外审结果	送审专业
4																	987 00			否	
5	2011/	大学		硕士	2011/06			实验技术	岗				2014/07	11	无	2011/12	988 20	13	无	否	免疫学
6	2013	大学		硕士	2013/06			实验技术	实验技术岗				2016/08	8	无	2014/12	986 55	13	无	否	免疫学
7	201	大学		博士	2016/06			实验技术	实验技术岗				2012/07	13	无	2010/12	984 26	180		否	基础医学
8	2013	理工学		硕士	2013/03			实验技术	实验技术岗				2016/08	9	无	2014/12	985 0	137 3	无		外科学
9	2013	大学		硕士	2013/06			实验技术	实验技术岗				2016/08	5		2014/12	36	1886 2			
10	200	大学		硕士	2006/06			服务管理型	实验技术岗				2014/12	10		2013/12	0	156	3/5	否	高分子化学与物理
11	201	大学		硕士	2013/06			实验技术	实验技术				2016/08	9	无	2013/1		188			

你有定期备份服务器的习惯吗？

2021年上半年全球受勒索软件影响的行业



定期备份—真实案例

【紧急通知】关于近日大量学校电脑感染勒索病毒的提醒公告

来源：　　发布日期：2017-05-13

全校师生员工：

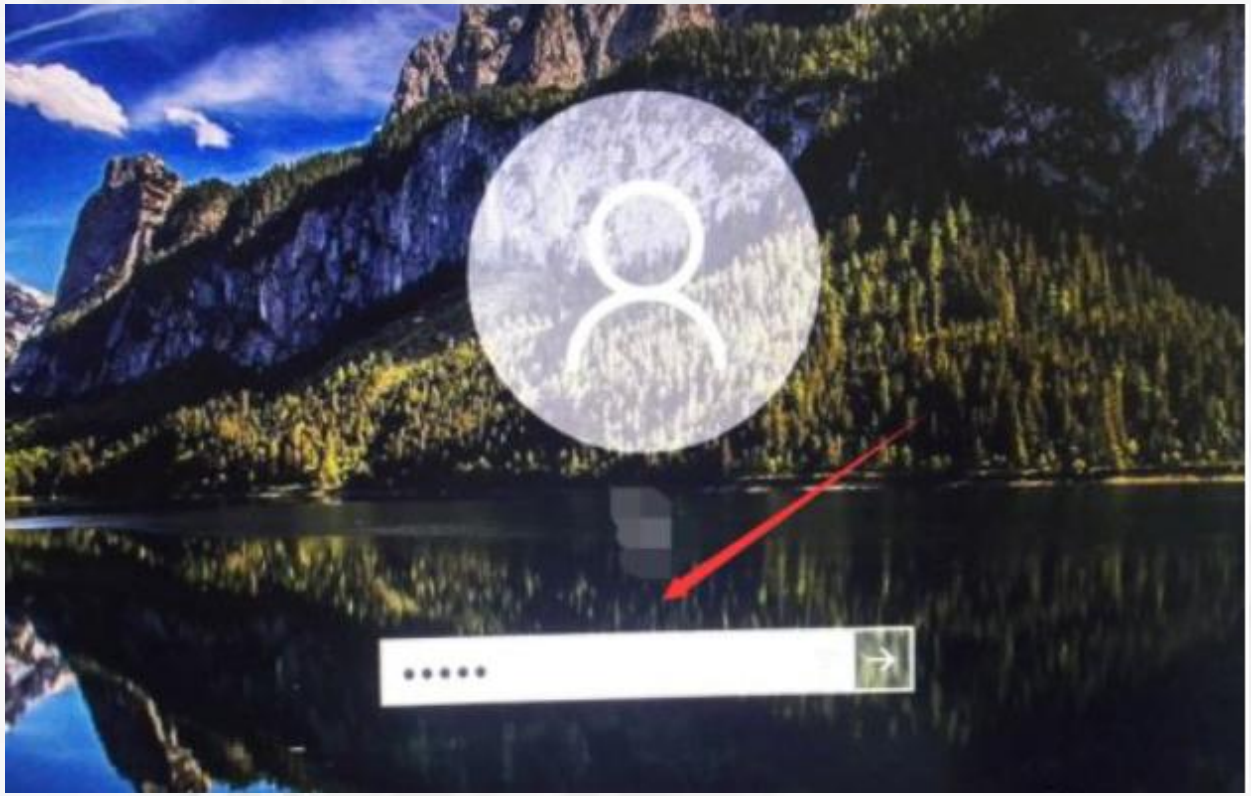
近日，全球爆发电脑勒索病毒，中国多所大学校园网被攻击，重要文件被病毒加密，加密使用了高强度的加密算法难以破解，被攻击者只有支付高额赎金才能解密恢复文件，对学习资料和个人数据造成严重损失。如图所示

北京理工大学提醒勒索病毒的通告：https://www.bit.edu.cn/tzgg17/wlfw/a139971.htm

03 如何安全的使用工作电脑?

（1）电脑锁屏

一定要设置复杂的锁屏密码，并开启自动锁屏！



锁屏设置教程：
https://jingyan.baidu.com/article/c74d6000b49b160f6a595de8.html

（2）不要随意插U盘

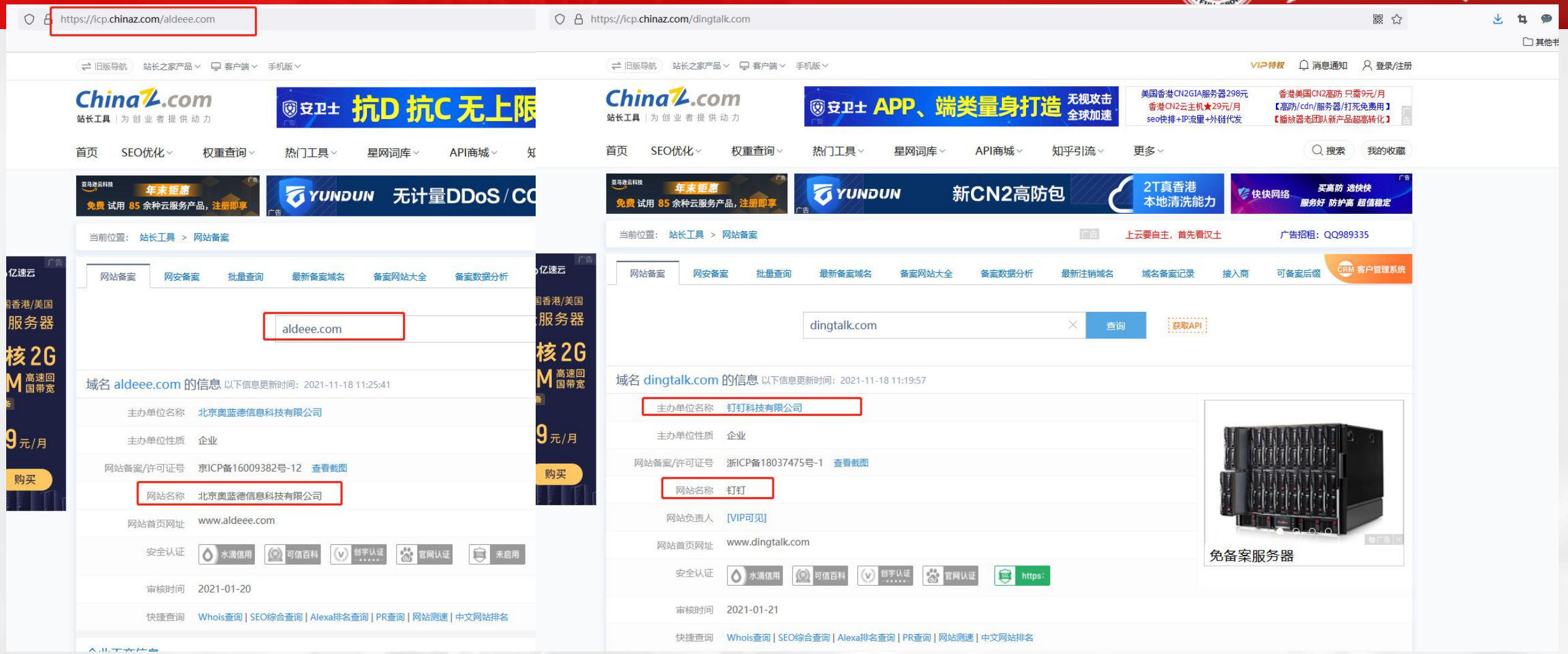
（3）开启防火墙以及防护软件

下载地址：http://sd.suda.edu.cn

（4）不用盗版破解软件


soft3.aldeee.com/pcsoftware/ltrj/762086.html
1.看域名
米云下载
请输入软件名称
搜 索
首页
图形图像
办公软件
视频软件
钉钉最新电脑版
钉钉最新电脑版
2.看界面
大小：212MB
语言：简体中文
版本：官方版 v6.0.0.11902
更新时间：21-06-25
立即下载
精品推荐
我的世界官方最新版
明日之后官方最新版
QQ游戏大厅最新版
王者荣耀官方最新版
和平精英官方最新版
腾讯手游助手官方版
精品软件
植物大战僵尸 21-06-25
QQ游戏大厅 21-06-25
War3 冰封王座 21-08-17
搜狗输入法 21-06-25
好评软件
红色警戒2共和国之 21-08-03
360压缩 21-06-25
鲁大师 21-09-29
谷歌浏览器 21-06-25
热搜推荐
搜狐视频 33.47MB / 21-06-25 点击下载
泡泡加速器 11.6 MB / 21-06-25 点击下载

（4）不用盗版破解软件—备案查询



备案查询网站：https://icp.chinaz.com/

（5）工作电脑定期备份


Ooops, your files have been encrypted!
Chinese (simpl
我的电脑出了什么问题？
您的一些重要文件被我加密保存了。
照片、图片、文档、压缩包、音频、视频文件、exe文件等，几乎所有类型的文件都被加密了，因此不能正常打开。
这和一般文件损坏有本质上的区别。您大可在网上找找恢复文件的方法，我敢保证，没有我们的解密服务，就算老天爷来了也不能恢复这些文档。
有没有恢复这些文档的方法？
当然有可恢复的方法。只能通过我们的解密服务才能恢复。我以人格担保，能够提供安全有效的恢复服务。
但这是收费的，也不能无限期的推迟。
请点击 <Decrypt> 按钮，就可以免费恢复一些文档。请您放心，我是绝不会骗你的。
但想要恢复全部文档，需要付款点费用。
是否随时都可以固定金额付款，就会恢复的吗，当然不是，推迟付款时间越长对你不利。
最好3天之内付款费用，过了三天费用就会翻倍。
还有，一个礼拜之内未付款，将会永远恢复不了。
对了，忘了告诉你，对半年以上没钱付款的穷人，会有活动免费恢复，能否轮
Payment will be raised on
5/16/2017 02:26:59
Time Left
02:22:35:15
Your files will be lost on
5/20/2017 02:26:59
Time Left
06:22:35:15

（6）卖电脑前清除所有数据

回收旧手机、旧电脑…

（7）接收邮件要注意

一、冒充公司领导语气要求提供账号密码；

二、冒充邮箱服务商客服（如邮箱管理员、服务中心、service等）提示邮箱异常、容量升级、安全警告、功能升级等系统消息，输入账号密码；

三、以假乱真，假冒退信、将钓鱼邮件伪装成退信邮件，让收件人输入账号密码解除退信；

四、利用附件内容引导收件人下载中毒；

五、伪装成外贸询盘邮件；

（8）接收邮件要注意—案例

搜狐员工遭遇工资补助诈骗

一份微信群聊记录显示，22年5月18日，搜狐全体员工收到一封来自“搜狐财务部”名为《5月份员工工资补助通知》的邮件，有员工按照附件要求扫码，并填写了银行账号等信息，不但没有等到补助，工资卡内的余额被划走。

5月25日11时，搜狐公司CEO张朝阳发表微博称，事情并没有大家想象的那么严重，主要是一名搜狐员工的内部邮箱密码被盗，盗贼冒充财务部发信给员工。技术部门发现后紧急处理，总体资金损失总额少于5万元。该事件并不涉及搜狐对外的公共服务邮箱xyz@sohu.com。

22年5月25日下午，搜狐在微博发布声明称，5月18日凌晨，搜狐部分员工邮箱收到诈骗邮件。经调查，实为某员工使用邮件时被意外钓鱼导致密码泄露，进而被冒充财务部盗发邮件。事发后，公司IT及安全部门第一时间做了紧急处理并向公安机关报案。据统计，共有24名员工被骗取4万余元人民币。

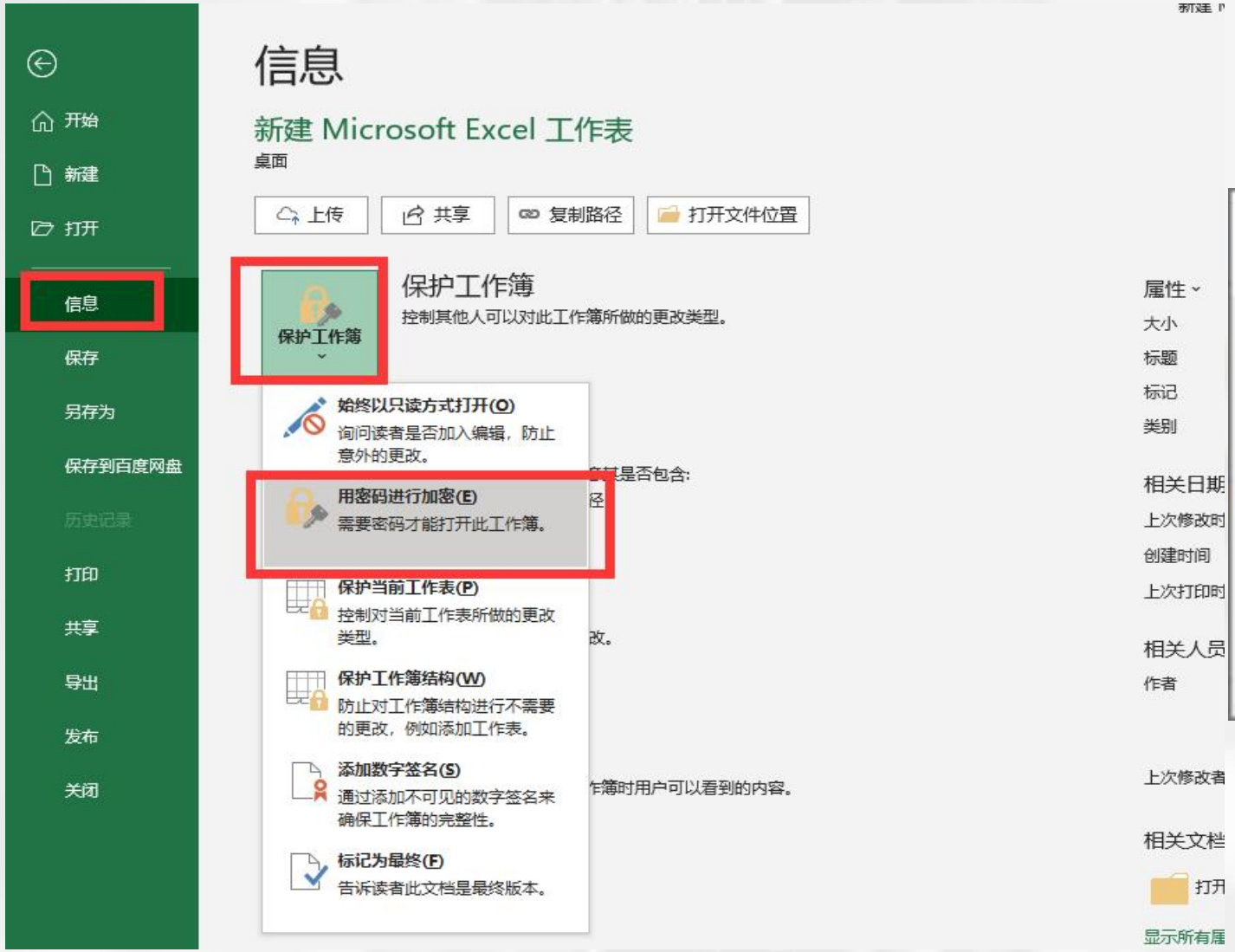
（9）接收邮件要注意—防范技巧

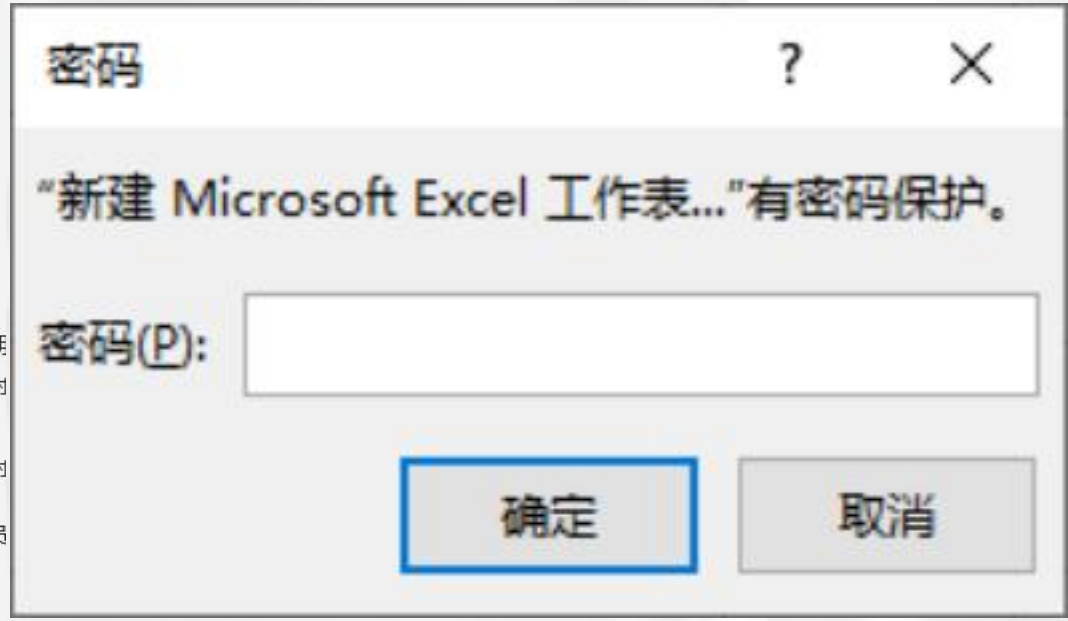
1.每次收到邮件时，仔细观察发件人地址。发现不正常时，可以和旧邮件做比对。

2.当遇到重要事情的邮件时，可以电话联系当事人，或向知道详情的相关人员询问情况。

3.在不清楚详情前，不要随便点击、下载、运行邮件附件。

（10）敏感文件要加密


开始
新建
打开
信息
保存
另存为
保存到百度网盘
历史记录
打印
共享
导出
发布
关闭
信息
新建 Microsoft Excel 工作表
桌面
上传
共享
复制路径
打开文件位置
保护工作簿
控制其他人可以对此工作簿所做的更改类型。
保护工作簿
始终以只读方式打开(O)
询问读者是否加入编辑，防止意外的更改。
用密码进行加密(E)
需要密码才能打开此工作簿。
保护当前工作表(P)
控制对当前工作表所做的更改类型。
保护工作簿结构(W)
防止对工作簿结构进行不需要的更改，例如添加工作表。
添加数字签名(S)
通过添加不可见的数字签名来确保工作簿的完整性。
标记为最终(F)
告诉读者此文档是最终版本。
属性
大小
标题
标记
类别
相关日期
上次修改时
创建时间
上次打印时
相关人员
作者
上次修改者
相关文档
打开
显示所有属


密码
"新建 Microsoft Excel 工作表..."有密码保护。
密码(P):
确定
取消

04 环境安全

走进工位

- 一些工作用到的书籍
- 一个打开的笔记本
- 一个U盘
- 一些发票
- 一些报表文件

这些物品会存在哪些潜在的安全隐患呢?

这里我们就要涉及到本次培训的一个概念:

工作环境与物理安全

u盘安全

没有收好的U盘是第一个值得注意的点，U盘是我们工作中极其方便的数据存储工具。正是由于它的方便易用，常常成为各种信息安全事件高发地。

从这两个方面考虑：

第一，U盘内的资料有可能泄露，如果有重要的文件那么后果很严重

第二，U盘内是否被别人植入病毒或木马？

u盘安全-案例

震网病毒（Stuxnet）在2010年7月开始爆发。它**突破工业专用局域网的物理限制**，利用WinCC系统的2个漏洞，对其开展攻击。

它是第一个直接破坏现实世界中工业基础设施的恶意代码。伊朗政府已经确认该国的布什尔核电站遭到Stuxnet的攻击。

这个案例中使用了可移动存储设备作为传播病毒的工具，对完全物理隔绝的网络系统发起**“摆渡”攻击**，所以U盘就成为了攻击者与受害者之间的**桥梁**。

纸面介质安全

除了一些电子设备会涉及到信息安全，还有一些传统的纸面介质也需要大家防范：

1. 禁止随意放置或丢弃含有敏感信息的纸质文件
2. 不要把密码或者密码提示书写在桌子上
3. 处理离开座位时，应将贵重物品、含有机密信息的资料锁入柜中，并对使用的计算机进行锁屏
4. 应将复印或打印的资料及时取走
5. 禁止在公共场合谈论敏感信息

总结

1.遇事多想想进行某个操作后可能遇到的安全风险有哪些呢?

2.换位思考，如果我作为攻击者，我能猜到“我”的密码规律吗?

3.看到个人信息，多思考该信息泄露到诈骗分子手中后，信息主人会被怎么针对?

多观察，多思考，多防范

谢谢观看

Thanks for watching

你了解你的电脑吗

——保护个人电脑安全

目录

1 Windows基本知识

1.1windows版本

客户端版　win7/win10
服务器版　windows server

1.2运行平台

PC服务器
平板电脑
手机
…

目录

2 Windows数据安全

2.1为什么要保护数据安全

- 数据是入侵者的终极目标
- 保护数据的底层安全，对数据进行加密是一切安全的基础。因为我们需要保护的就是数据安全，很多时候操作系统帮我们做了很多，但仍旧是有漏洞。

2.2数据安全的威胁

- 电源故障
- 驱动器损坏
- 人为操作失误
- 黑客入侵和病毒
- 信息窃取
- 自然灾害

2 Windows数据安全

2.3 数据安全的防护

- 数据本身的安全
  - 依据可靠的加密算法与安全体系
- 数据存储的安全
  - 采用现代信息存储手段对数据进行主动防护
- 数据处理的安全
  - 防止硬件故障和误操作导致正在处理的数据损坏或丢失
  - 防止数据在处理过程中的信息泄露

2 Windows数据安全

2.4数据本身的安全-加密

2.4.1EFS加密

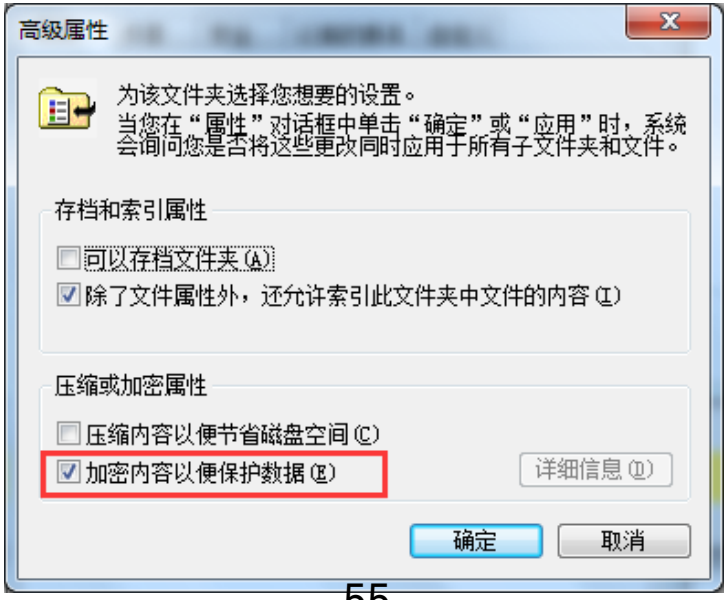
- EFS（Encrypting File System，加密文件系统）是从Windows 2000/XP系统开始，系统所特有的一个实用功能，对于NTFS卷上的文件和数据，都可以直接被操作系统加密保存，在很大程度上提高了数据的安全性。

2 Windows数据安全

2.4.1 EFS加密

EFS加密过程

在文件高级属性里勾选加密内容以便保护数据，加密文件。

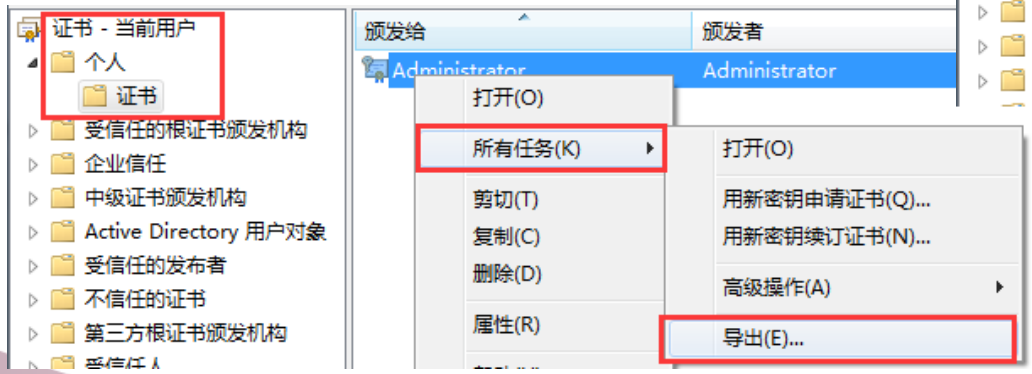


2 Windows数据安全

2.4.1 EFS加密

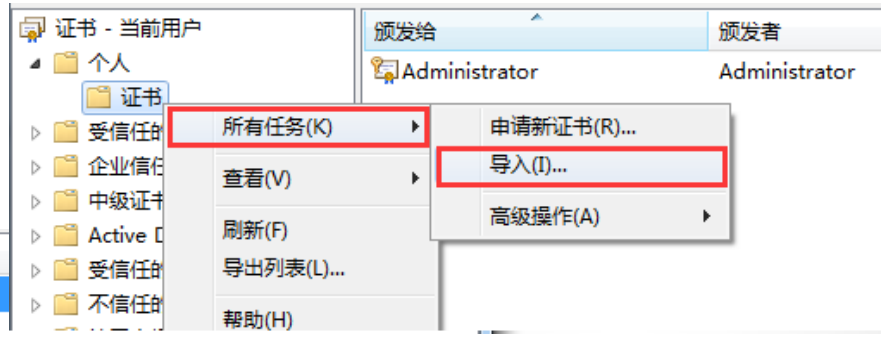
EFS证书管理

打开证书管理器(certmgr.msc)导出用户的证书（公钥/私钥），点击导出，生成一个pfx后缀文件，并妥善保管好此证书



EFS证书管理

当需要解密文件时，打开证书管理器(certmgr.msc)导入证书，即可解密。



2 Windows数据安全

2.4 数据本身的安全-加密

2.4.2 Bitlocker加密

Bitlocker加密，最早是出现于vista系统中， win10系统中有一个自带的bitlocker驱动器加密功能，能够同时支持FAT和NTFS两种格式，用来加密保护用户数据，可以加密电脑的整个系统分区，也可以加密可移动的便携存储设备，如U盘和移动硬盘等。

2 Windows数据安全

2.4.2 Bitlocker加密

Bitlocker加密过程

启用Bitlocker加密

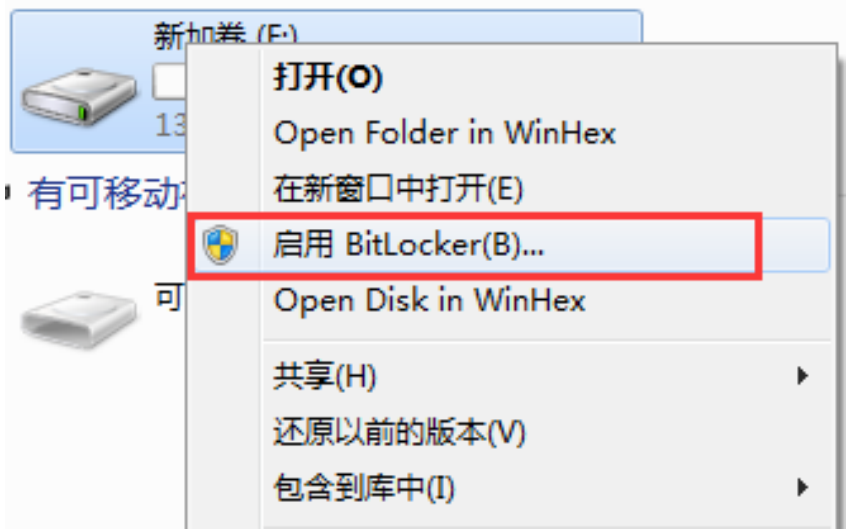
1、在服务器管理器中添加Bitlocker加密功能

2 Windows数据安全

2.4.2 Bitlocker加密

Bitlocker加密过程

启用Bitlocker加密
2、加密驱动器

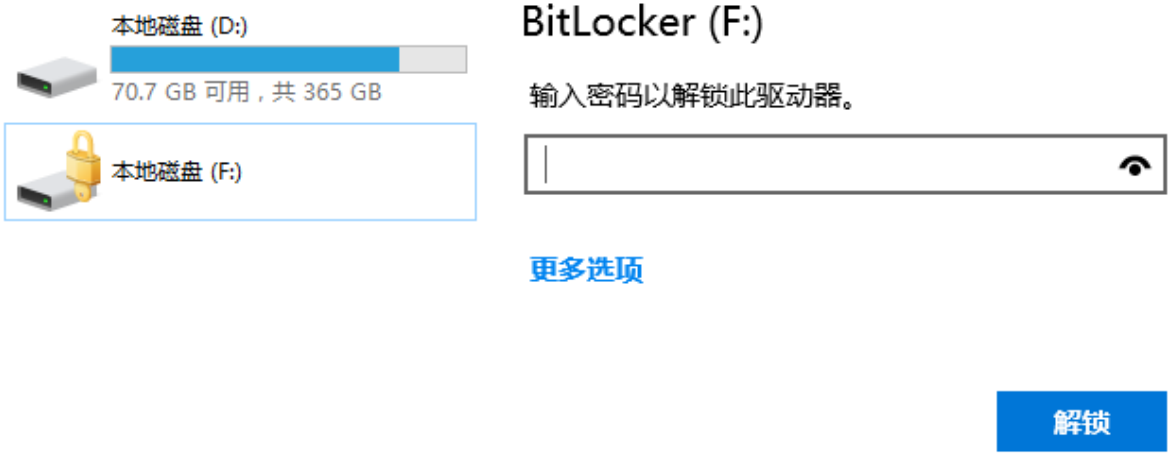


2 Windows数据安全

2.4.2 Bitlocker加密

Bitlocker加密过程

启用Bitlocker加密
3、解密驱动器

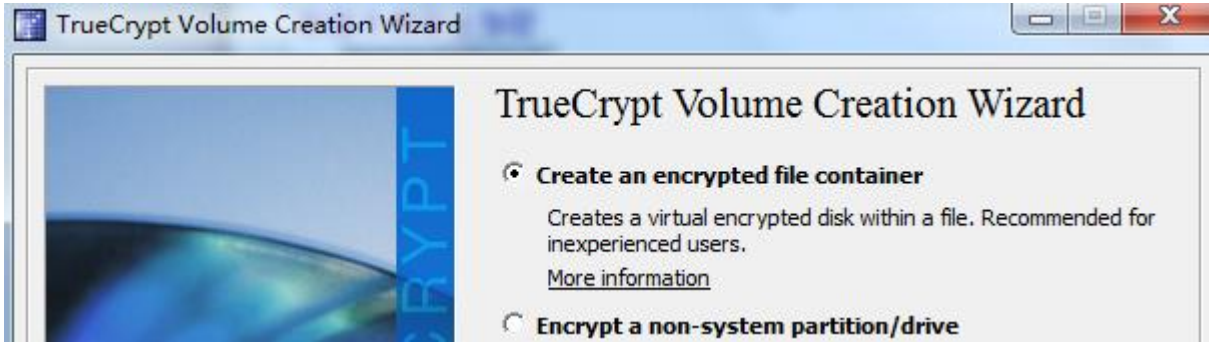


2 Windows数据安全

2.4 数据本身的安全-加密

2.4.3 第三方加密软件

TrueCrypt是一款免费开源的加密软件，同时支持Windows Vista,7/XP, Mac OS X, Linux 等操作系统



2 Windows数据安全

2.4 数据本身的安全-加密

2.4.4 解密软件

PasswarekitEnterprise
PasswareKitEnterprise是一款功能强大的密码破解软件，适用于破解office、rar、TrueCrypt等密码

2 Windows数据安全

2.5 数据存储的安全

2.5.1数据备份

备份管理包括备份的可计划性，自动化操作，历史记录的保存或日志记录，数据备份分为：全备份、增量备份以及差异备份

2.5.2 异地容灾

在各单位的IT系统中，必然有核心部分，通常称之为生产中心，往往给生产中心配备一个备份中心，备份中心是远程的，当火灾、地震等灾难发生时，以保护数据不会丢失。

2 Windows数据安全

2.6 数据处理的安全

2.6.1 关键数据

关键数据备份
关键数据加密

2.6.2 细化用户访问权限

2.6.3 敏感数据防泄漏

目录

3 账户与权限安全

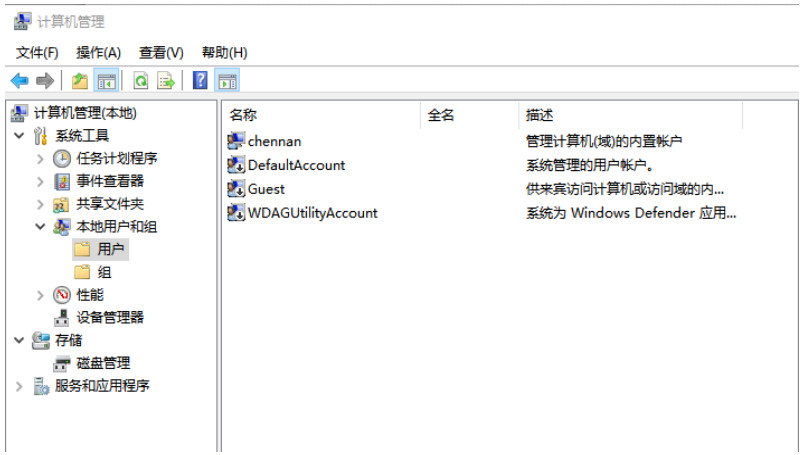
3.1 常见账户和组

用户的构成：用户名+密码+权限。

与使用者相关联的账户

Administrator：默认管理员账户(是Windows系统中权限最高的账户)

Guest：来宾账户(给访客使用的，默认禁用)

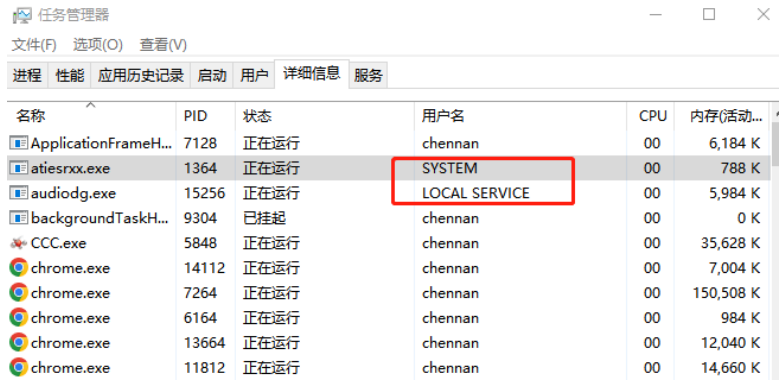


与Windows组件关联的账户

SYSTEM：本地系统账户，为Windows核心组件访问文件提供权限(拥有高于Administrator的权限)

Local Service：本地服务，一部分服务提供访问系统权限(权限非常低)

Network Service：网络服务，一部分网络提供访问系统的权限(权限非常低)



3 账户与权限安全

3.1 常见账户和组

组是一些账户的集合，为“组”设置权限后，隶属于该组的账户默认具有这些权限，方便管理。

组的分类

需要人为添加成员的组

Administrators：管理员组(可以将账户加入改组，让用户具有管理员权限)

Guests：来宾组

Power Users：Windows Server 2008以上系统为向下兼容保留的组(不再使用)

Users：普通用户组，新用户默认为Users组

动态包含成员的组

INTERACTIVE：默认包含本地登录的账户

Authenticated Users：包含了通过验证的用户，不包含来宾用户

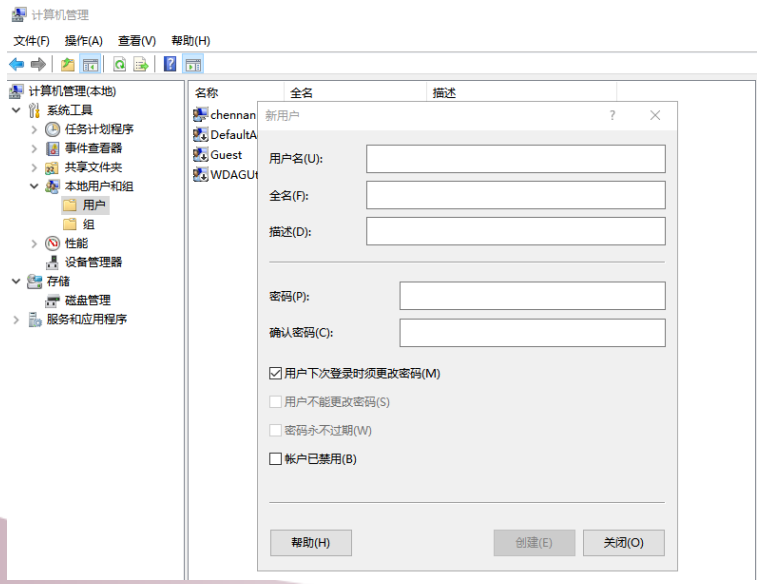
Everyone：所有账户(设置开放权限时使用)

3 账户与权限安全

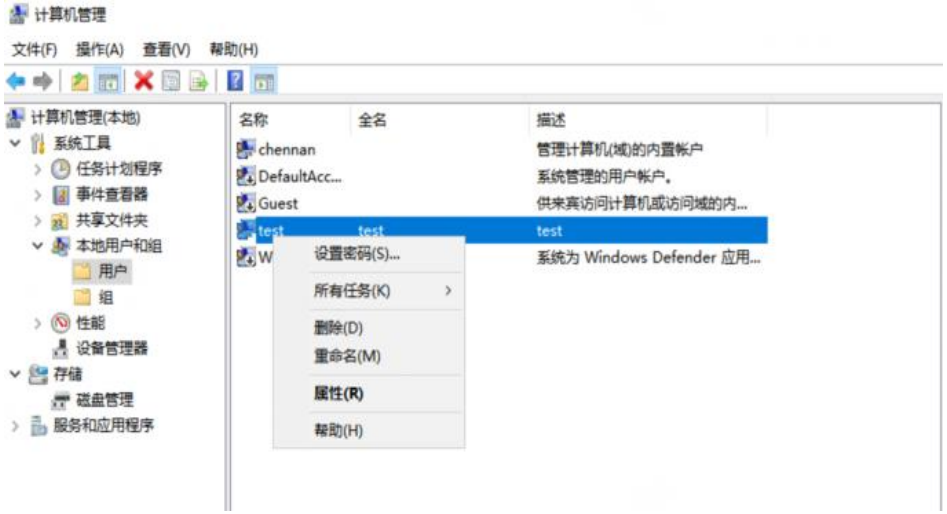
3.2 用户的管理

新建用户

“此电脑”右键选择管理 -> 本地用户和组 -> 用户 -> 右键选择"新用户"



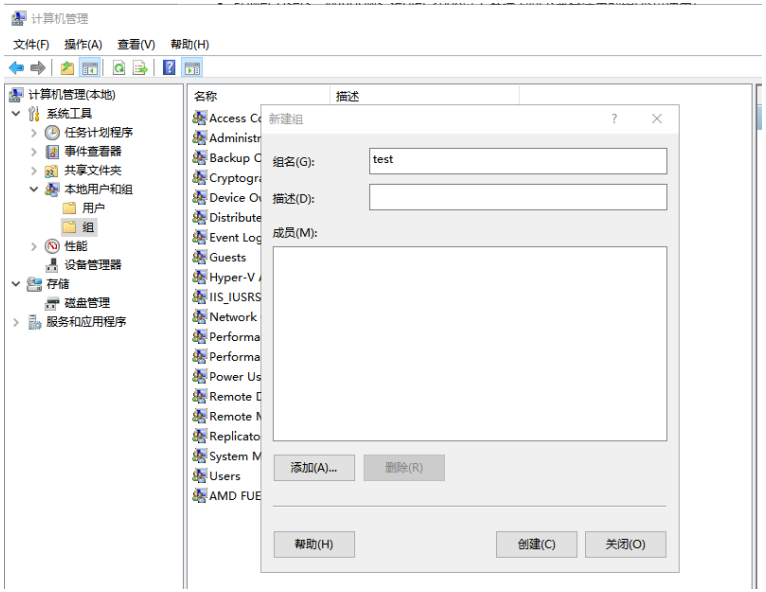
删除用户、重设密码



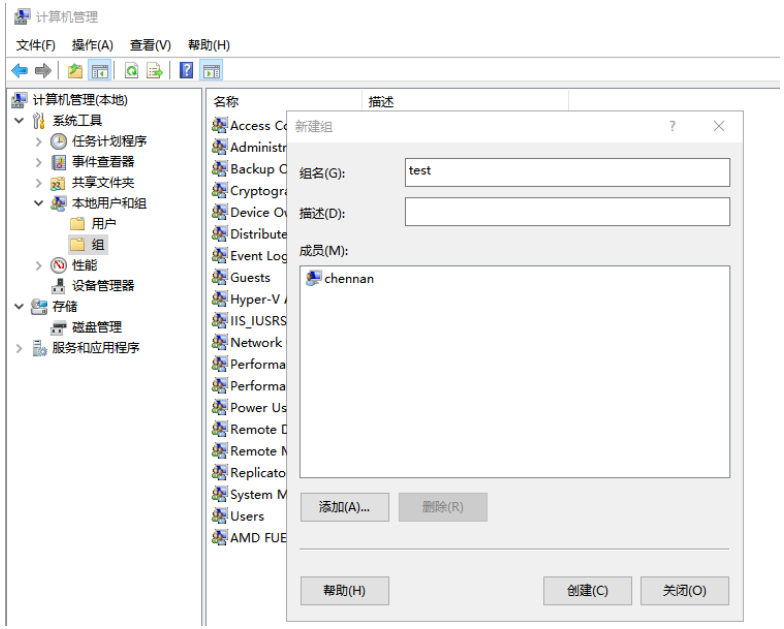
3 账户与权限安全

3.3 用户组的管理

新建用户组



添加test组中的成员



3 账户与权限安全

3.4 windows用户权限基础

Windows的访问控制列表(Access Control List)：访问权限决定着某个用户可以访问的文件和目录 对于每一个文件和文件夹，由安全描述符(SD)规定了安全数据、安全描述符决定安全设置是否对当前目录有效，或者它可以被传递给其他文件和目录。

当一个用户试图访问一个文件或者文件夹的时候，NTFS 文件系统会检查用户使用的帐户或者账户所属的组是否在此文件或文件夹的访问控制列表（ACL）中。如果存在，则进一步检查访问控制项 ACE，然后根据控制项中的权限来判断用户最终的权限。

3 账户与权限安全

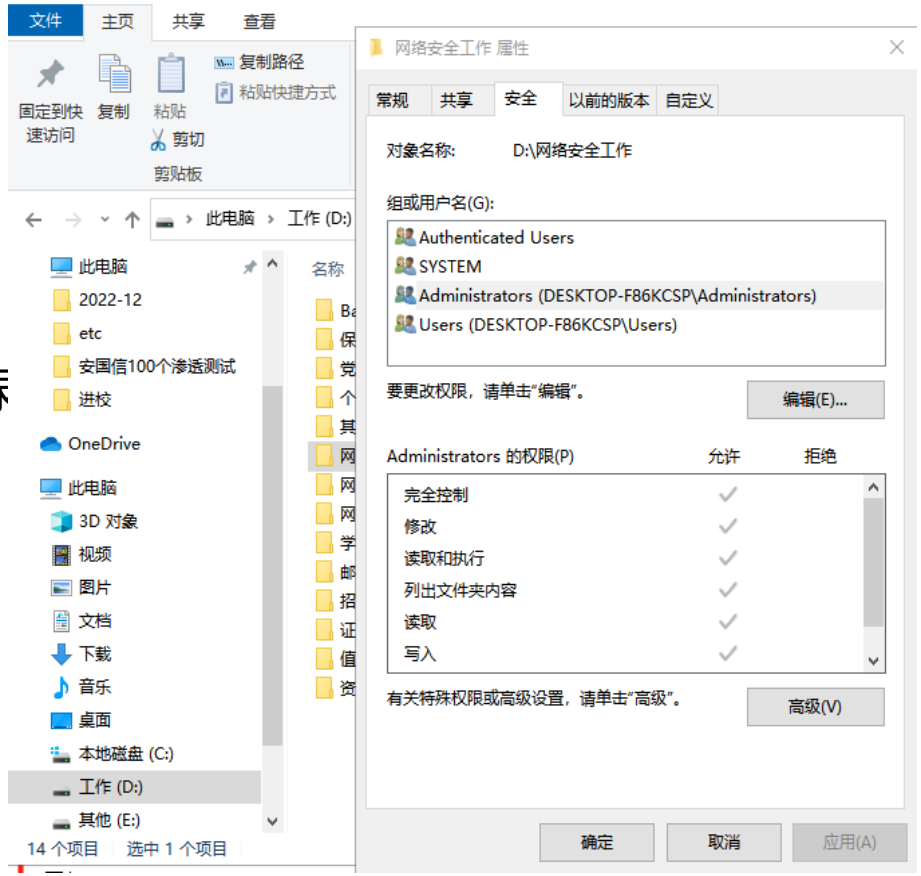
3.4 windows用户权限基础

3.4.1权限高级应用

NTFS文件系统下的权限

完全控制、修改、读取和运行、列出目录

读取、写入



3 账户与权限安全

3.4 windows用户权限基础

3.4.1权限高级应用

文件特殊权限

在高级权限里存在：遍历文件夹/执行文件、列出文件夹/读取数据、读取属性、读取扩展属性、同步等14个高级权限

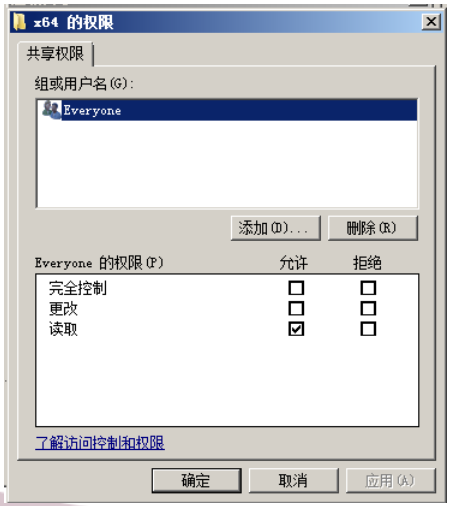
3 账户与权限安全

3.4 windows用户权限基础

3.4.1权限高级应用

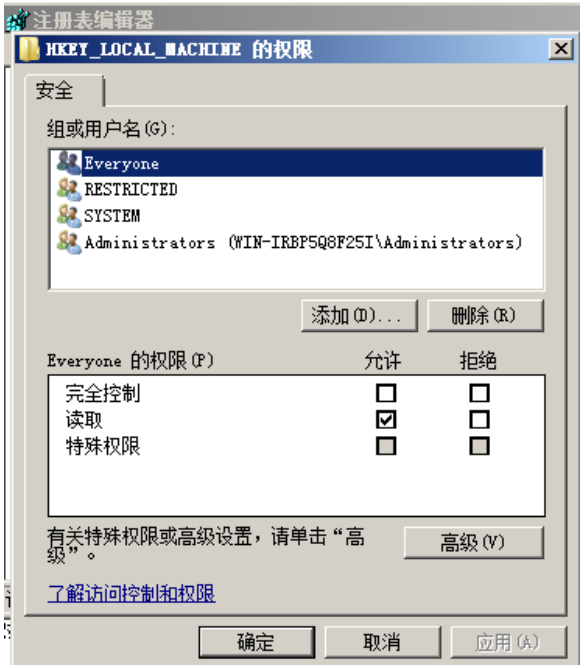
共享权限

完全控制、更改、读取



注册表权限

完全控制、读取、特殊权限



3 账户与权限安全

3.4 windows用户权限基础

3.4.2 权限利用

IPC漏洞利用

IPC$是共享资源的一种,是win9.x系统之后出现的系统默认共享，使用137、138、139、445端口

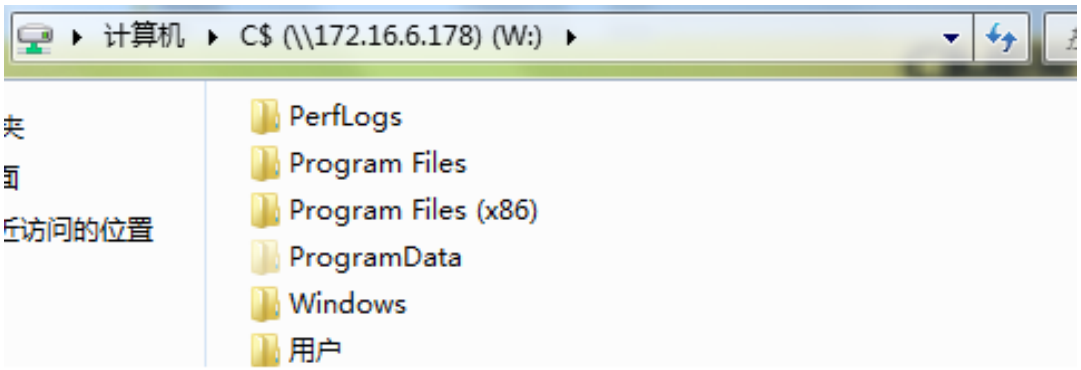
```
C:\Users\Administrator>net share

共享名       资源                            注解

-------------------------------------------------------------------------------
C$           C:\                             默认共享
D$           D:\                             默认共享
E$           E:\                             默认共享
F$           F:\                             默认共享
IPC$                                         远程 IPC
ADMIN$       C:\Windows                      远程管理
命令成功完成。
```

3 账户与权限安全

3.4 windows用户权限基础

3.4.2 权限利用

IPC漏洞利用
扫描目标主机是否开放139、445端口
通过139、445端口爆破系统用户名密码
挂载目标磁盘：net use w: \\ip\c$ password /user:username



3 账户与权限安全

3.4 windows用户权限基础

3.4.2 权限利用

防范IPC$入侵

扫描目标主机是否开放139、445端口

通过139、445端口爆破系统用户名密码

挂载目标磁盘：net use w: \\ip\c$ password /user:username

server版:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

把AutoShareServer（DWORD）的键值改为:00000000。

pro版:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

把AutoShareWks（DWORD）的键值改为:00000000。

- 禁用Server服务
- 使用防火墙过滤139、445等端口
- 设置复杂的密码，防止IPC$穷举密码

3 账户与权限安全

3.5 账户安全防范措施

3.5.1 windows用户口令加固

禁用Guest账户

更改密码复杂度设置

定期对口令进行修改

登录失败次数限制

更改管理员用户默认名称

设置陷阱账户

不显示最后的用户名

设置syskey双重密码

3 账户与权限安全

3.6 权限安全防范措施

配置“用户权限分配”策略

组策略编辑器--计算机配置--Windows设置—安全设置--本地策略—用户权限分配

远程桌面登录用户配置

从网络访问计算机用户配置

配置文件访问权限设置

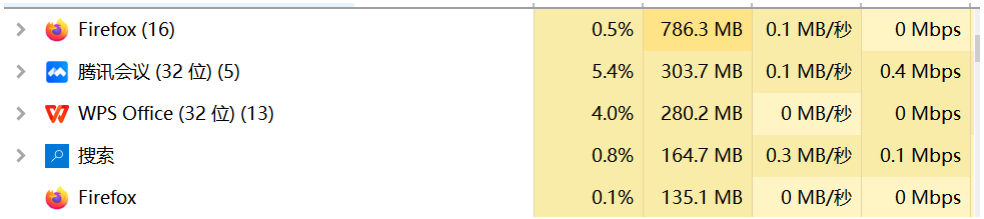
系统盘的权限设置

重要文件的权限设置

目录

4 进程与服务安全

4.1 基本概念



进程

进程是正在运行的程序的实例

程序

程序是一组指令的集合

线程

线程是进程的一部分

线程是比进程更小的处理模块。进程和线程都是由操作系统所包含的程序运行的基本单元

服务

服务是指执行指定系统功能的程序、例程或进程，以便支持其他程序。服务和进程并不是一一对应的。

4 进程与服务安全

4.2 系统进程

4.2.1 系统常见进程

smss

csrss

winlogin

lsass

services

svchost

explorer

映像名称	用户名	CPU	内存(专...	描述
svchost.exe	NETWORK SE...	00	1,008 K	Windows 服务主进程
svchost.exe	SYSTEM	00	11,636 K	Windows 服务主进程
smss.exe	SYSTEM	00	228 K	Windows 会话管理器
wininit.exe	SYSTEM	00	872 K	Windows 启动应用程序
WUDFHost.exe	LOCAL SERVICE	00	1,144 K	Windows 驱动程序基础 - 用
taskhost.exe	Administrator	00	1,916 K	Windows 任务的主机进程
taskmgr.exe	Administrator	04	2,040 K	Windows 任务管理器
audiodg.exe	LOCAL SERVICE	00	10,720 K	Windows 音频设备图形隔离
explorer.exe	Administrator	00	30,740 K	Windows 资源管理器
WmiPrvSE.exe	SYSTEM	00	1,388 K	WMI Provider Host
WmiPrvSE.exe	NETWORK SE...	00	3,556 K	WMI Provider Host
lsm.exe	SYSTEM	00	944 K	本地会话管理器服务
System Idle Pr...	SYSTEM	95	12 K	处理器空闲时间百分比
services.exe	SYSTEM	00	4,028 K	服务和控制器应用程序
spoolsv.exe	SYSTEM	00	3,184 K	后台处理程序子系统应用程序

4 进程与服务安全

4.2 系统进程

4.2.2 重要进程防护

重要进程的存放位置

异常进程的发现

病毒进程的查杀

异常文件删除

映像名称	用户名	CPU	内存(专...	映像路径名称
svchost.exe	NETWORK ...	00	4,616 K	C:\Windows\System32\svchost.exe
svchost.exe	LOCAL SE...	00	5,140 K	C:\Windows\System32\svchost.exe
svchost.exe	LOCAL SE...	00	3,124 K	C:\Windows\System32\svchost.exe
svchost.exe	LOCAL SE...	00	880 K	C:\Windows\System32\svchost.exe
svchost.exe	NETWORK ...	00	1,048 K	C:\Windows\System32\svchost.exe
svchost.exe	SYSTEM	00	2,684 K	C:\Windows\System32\svchost.exe
System	SYSTEM	00	292 K	C:\Windows\system32\ntoskrnl.exe
System Idl...	SYSTEM	98	12 K	
taskhost.exe	Administ...	00	1,916 K	C:\Windows\System32\taskhost.exe

4 进程与服务安全

4.3 系统服务

4.3.1 常见服务

Computer Browser：维护网络上计算机的更新列表，并将列表提供给计算机指定浏览。
Server：支持此计算机通过网络的文件、打印、和命名管道共享。
Workstation：创建和维护到远程服务的客户端网络连接

名称	描述	状态	启动类型	登录为
Security Center	WSCSVC(Windows 安全中心)服务监视并报告计...	已启动	自动(延迟...	本地服务
Server	支持此计算机通过网络的文件、打印、和命名管道...	已启动	自动	本地系统
Shell Hardware Detection	为自动播放硬件事件提供通知。	已启动	自动	本地系统
Smart Card	管理此计算机对智能卡的取读访问。如果此服务被...		手动	本地服务
Smart Card Removal Policy	允许系统配置为移除智能卡时锁定用户桌面		手动	本地系统
SNMP Trap	接收本地或远程简单网络管理协议 (SNMP) 代理...		手动	本地服务
Software Protection	启用 Windows 和 Windows 应用程序的数字许可...		自动(延迟...	网络服务

4 进程与服务安全

4.3 系统服务

4.3.2 服务配置

根据服务的描述以及业务的需求，确定是否使用此服务

对于安装应用程序同步安装的服务，如无必要，应将其关闭。

根据实际情况禁止或者设置成手动启动的方式处理非必要的服务

例：Computer Browser 、Task scheduler 、Remote Registry、Remote Desktop Help Session Manager

4 进程与服务安全

4.4 端口安全

4.4.1 端口分类

按协议划分：TCP端口、UDP端口

常见的TCP端口

80：超文本传送协议HTTP使用80端口，用于实现Web服务和网页浏览

21：文件传输协议FTP使用21端口，用于实现文件的上传和下载

25：简单邮件传送协议SMTP使用端口，用于发送电子邮件

常见的UDP端口

53：域名解析服务DNS使用端口，用于实现将域名解析为IP地址。

161：简单网络管理协议SNMP使用端口，用于实现对网络设备的远程管理和监视。

4 进程与服务安全

4.4 端口安全

4.4.1 端口分类

按端口号划分：公认端口、注册端口、动态或私有端口

公认端口：从0-1023，它们紧密绑定于一些服务。通常这些端口的通讯明确表明了某种服务的协议。例如：80端口实际上总是HTTP通讯。

注册端口：从1024到49151。它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其它目的。例如：许多系统处理动态端口从1024左右开始。

动态和/或私有端口：从49152到65535。理论上，不应为服务分配这些端口。实际上，机器通常从1024起分配动态端口。但也有例外：SUN的RPC端口从32768开始 。

4 进程与服务安全

4.4 端口安全

4.4.2 端口查看

netstat命令，netstat命令的语法格式：

netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]

常见参数说明

-a：显示所有连接和侦听端口。

-n：以数字形式显示地址和端口号。

-o： 显示拥有的与每个连接关联的进程 ID。

-p proto ：显示 proto 指定的协议的连接；proto 可以是下列任何一个: TCP、UDP、TCPv6 或 UDPv6。 如果与 -s 选项一起用来显示每个协议的统计，proto 可以是下列任何一个: IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP或 UDPv6。

4 进程与服务安全

4.4 端口安全

4.4.2 端口关闭

关闭不需要的服务

关闭80口：关掉WWW服务

关闭21端口：关闭FTP服务

启用防火墙对特定端口进行屏蔽

启用IP安全策略对特定端口进行屏蔽

目录

5 日志安全

5.1 windows日志安全概述

Windows操作系统都设计有各种各样的日志文件，如应用程序日志，安全日志、系统日志、FTP日志、WWW日志、DNS服务器日志等等，这些根据你的系统开启的服务的不同而有所不同。我们在系统上进行一些操作时，这些日志文件通常会记录下我们操作的一些相关内容，这些内容对系统安全工作人员相当有用。比如说有人对系统进行了IPC探测，系统就会在安全日志里迅速地记下探测者探测时所用的IP、时间、用户名等，用FTP探测后，就会在FTP日志中记下IP、时间、探测所用的用户名等。

5 日志安全

5.2 操作系统日志配置

日志文件存放路径

Windows Server 2008：%systemroot%\system32\winevt\logs*.evtx

日志文件在注册表中的位置：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog

修改日志文件默认存放路径

Windows Server 2008在事件查看器中通过属性—常规—日志路径，来修改日志文件的位置。

5 日志安全

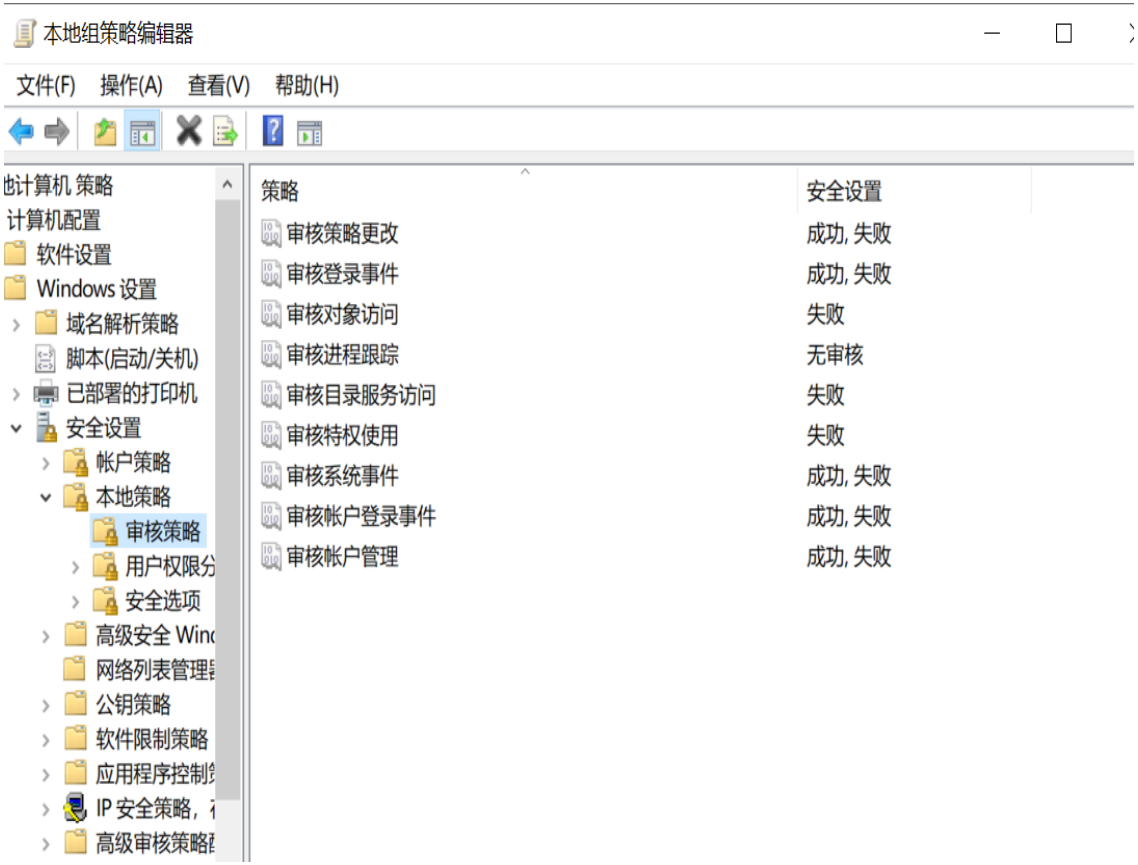
5.2 操作系统日志配置

修改日志文件默认大小以及达到事件日志最大大小时的动作

5 日志安全

5.2 操作系统日志配置

启用审核策略



5 日志安全

5.3 操作系统日志分析

事件ID分析

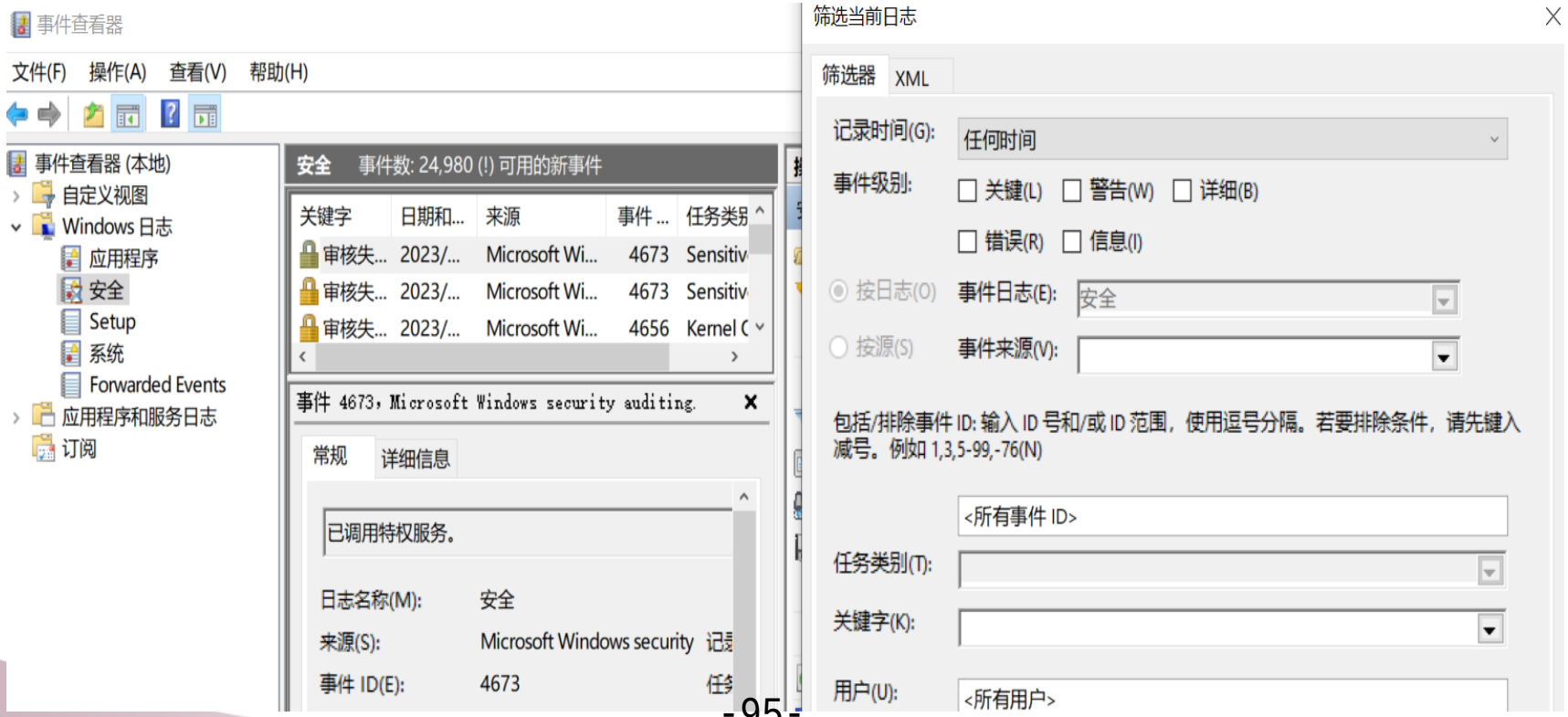
重点检查的ID事件

Win 2003事件 ID	Win 2008事件ID	事件类型	描述
512, 513, 514, 515, 516, 518, 519, 520	4608, 4609, 4610, 4611, 4612, 4614, 4615, 4616	系统事件	本地系统进程，例如系统启动，关闭和系统时间的改变。
528, 540	4624	成功用户登录	所有用户登录事件
529, 530, 531, 532, 533, 534, 535, 536, 537 539	4625	登录失败	所有用户登录失败事件
538	4634	用户成功退出	所有用户退出事件
624, 625, 626, 627, 628, 629, 630, 642, 644	4720, 4722, 4723, 4724, 4725, 4726, 4738, 4740	用户帐号改变	用户帐号的改变，像用户帐号创建，删除，改变密码等等
(631 to 641) and (643, 645 to 666)	4727 to 4737, 4739 to 4762	用户组改变	对一个用户组的所有改变，例如添加或移除一个全局组或本地组，从全局组或本地添加或移除成员等等

5 日志安全

5.3 操作系统日志分析

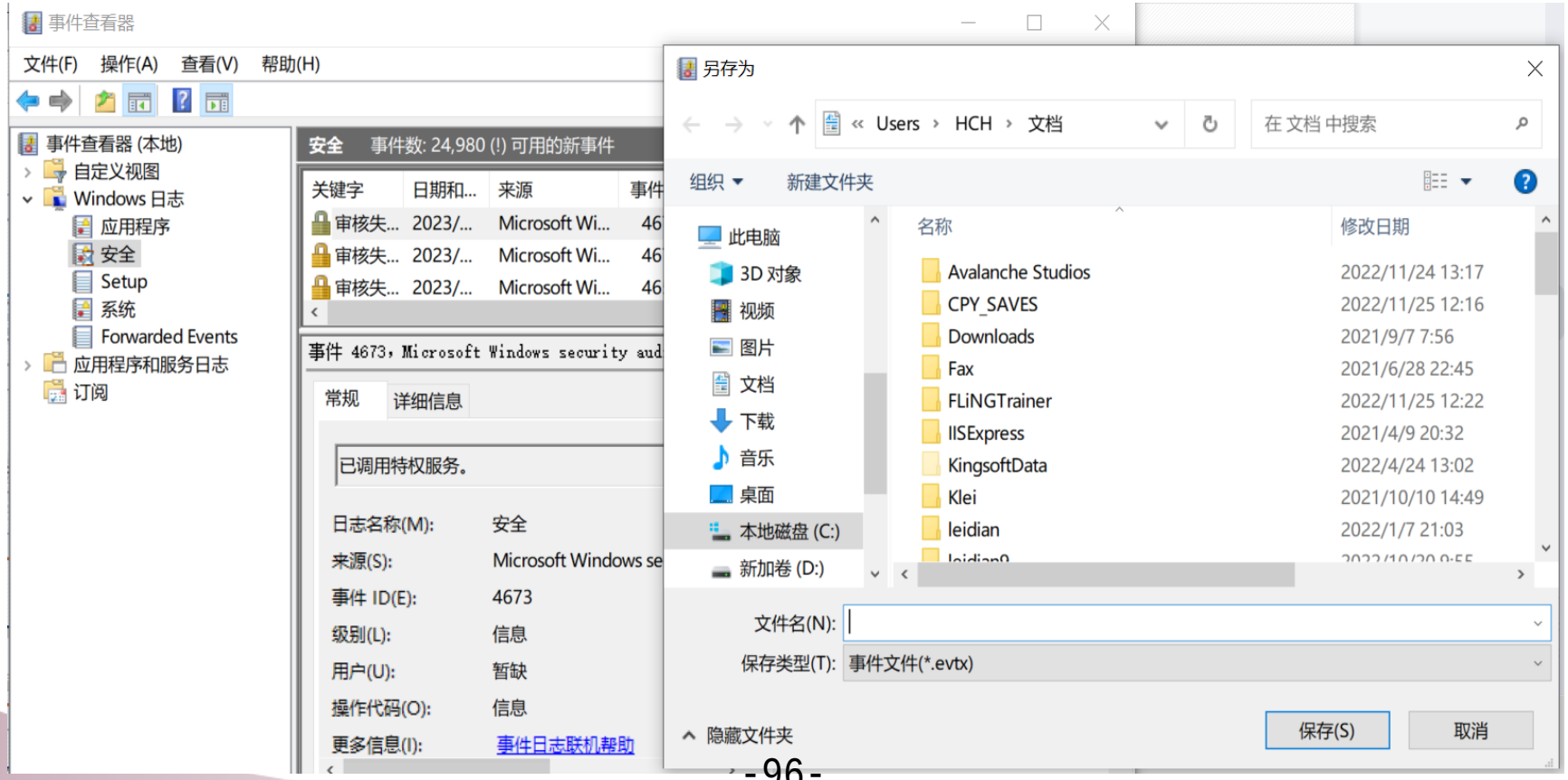
日志筛选



5 日志安全

5.3 操作系统日志分析

日志导出

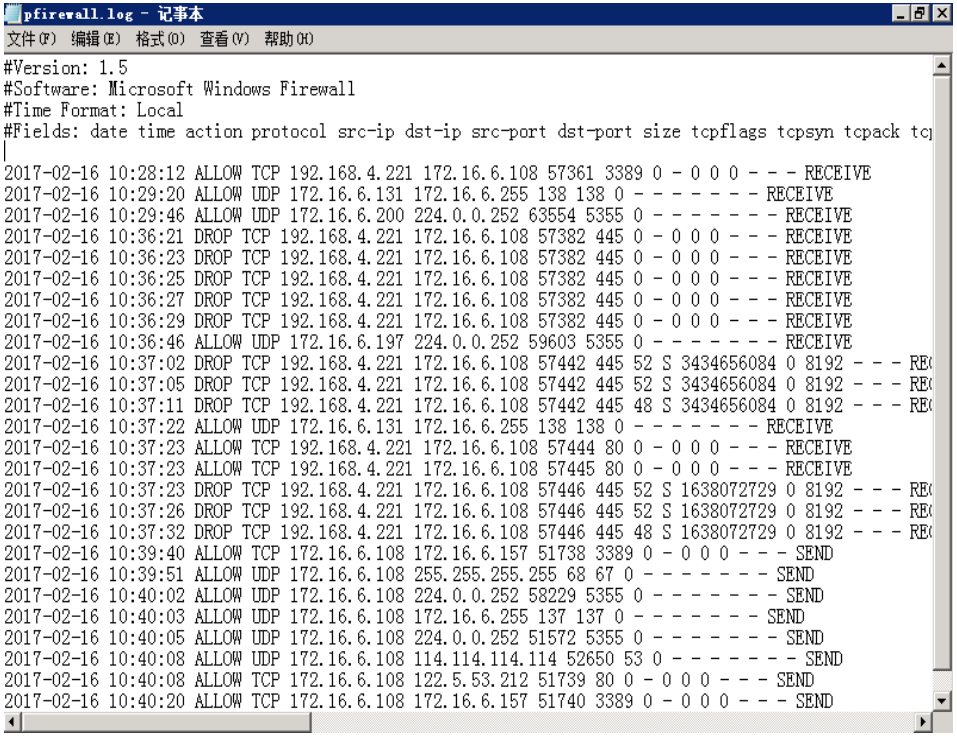


5 日志安全

5.4 防火墙日志分析

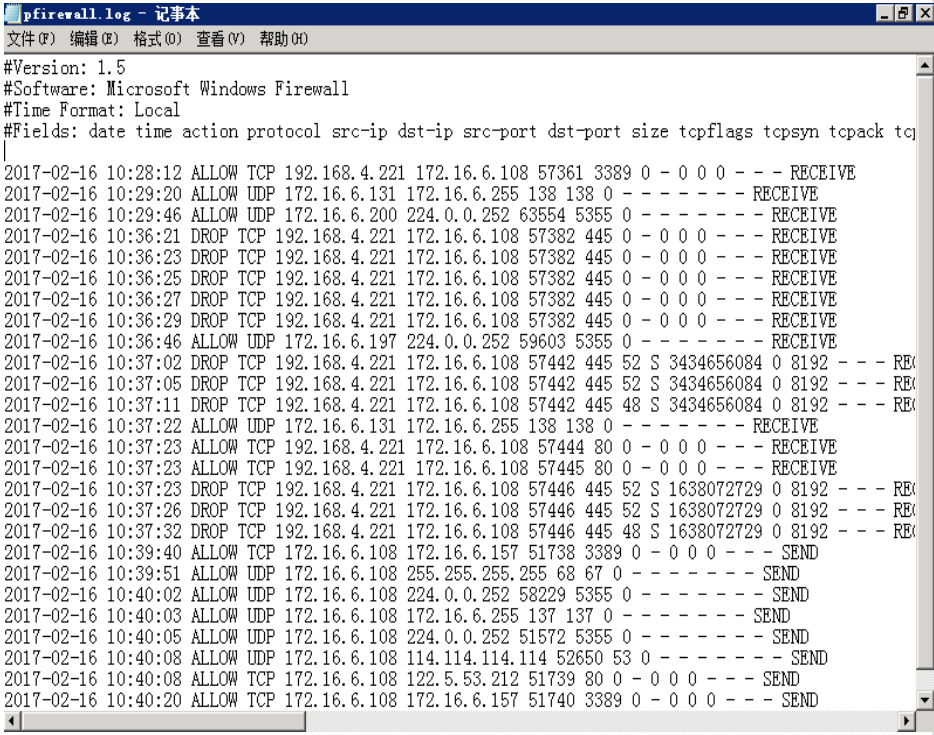
防火墙日志的存放路径

C:\Windows\System32\LogFiles\Firewall



5 日志安全

5.4 防火墙日志分析



2017-02-16 为该条日志记录产生的日期

10:28:12 为该条日志记录产生的时间

ALLOW 为防火墙的动作

TCP 为协议

192.168.4.221 为发起连接的源IP地址

172.16.6.108 为连接的目标IP地址

57361 为发起连接的源端口号

3389 为连接的目标端口号

RECEIVE 表示接收到的数据包。如果是SEND，则表示是发出去的数据包。

5 日志安全

5.5 IIS日志分析

认识IIS日志

IIS日志主要用于记录用户和搜索引擎蜘蛛对网站的访问行为。

IIS日志文件默认的存放位置

Windows Server 2008 iis日志路径：C:\inetpub\logs\LogFiles

IIS日志可以记录用户访问站点的时间、用户的ip、用户访问的页面和动作（get、post）、用户使用的浏览器，并且显示日志返回代码。

IIS日志返回代码含义

2XX 成功

3XX 重定向

4XX 客户端请求错误

5XX 服务器出错……

5 日志安全

5.5 IIS日志分析

IIS日志实例

```
#Software: Microsoft Internet Information Services 7.5
#Version: 1.0
#Date: 2016-03-22 02:58:58
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status
2016-03-22 02:59:21 172.16.0.9 GET / - 80 - 172.16.0.1 Mozilla/5.0+(Windows+NT+6.1;+rv:45.0)+Gecko/20100101+Firefox/45.0 200 0 0 109
2016-03-22 02:59:21 172.16.0.9 GET /welcome.png - 80 - 172.16.0.1 Mozilla/5.0+(Windows+NT+6.1;+rv:45.0)+Gecko/20100101+Firefox/45.0 200
2016-03-22 02:59:21 172.16.0.9 GET /favicon.ico - 80 - 172.16.0.1 Mozilla/5.0+(Windows+NT+6.1;+rv:45.0)+Gecko/20100101+Firefox/45.0 404
2016-03-22 02:59:21 172.16.0.9 GET /favicon.ico - 80 - 172.16.0.1 Mozilla/5.0+(Windows+NT+6.1;+rv:45.0)+Gecko/20100101+Firefox/45.0 404
2016-03-22 03:06:07 172.16.0.9 GET /index.html - 80 - 172.16.0.1 Mozilla/5.0+(Windows+NT+6.1;+rv:45.0)+Gecko/20100101+Firefox/45.0 404 0
2016-03-22 03:06:33 172.16.0.9 GET /index.htm - 80 - 172.16.0.1 Mozilla/5.0+(Windows+NT+6.1;+rv:45.0)+Gecko/20100101+Firefox/45.0 404 0
2016-03-22 03:07:13 172.16.0.9 GET /index.htm - 80 - 172.16.0.1 Mozilla/5.0+(Windows+NT+6.1;+rv:45.0)+Gecko/20100101+Firefox/45.0 200 0
```

访问日期 访问时间 服务器IP 请求方式 请求页面 端口 客户端IP 客户端浏览器信息 返回状态

5 日志安全

5.6 系统日志清除

一个入侵系统成功后的黑客第一件事便是清除日志，如果以图形界面远程控制对方机器或是从终端登录进入，删除日志不是一件困难的事

使用小葵日志清理，帮助清除日志

5 日志安全

5.7 日志安全防护措施

修改windows日志的大小配置

修改日志文件的存放目录

设置日志访问权限

使用第三方软件进行日志的异地备份

NTSyslog--将Windows系统日志转换成syslog消息，然后发送到远程syslog服务器。

3Csyslog--日志服务器，负责接收从客户端发来的日志。

定期检查系统日志，及时发现异常

目录

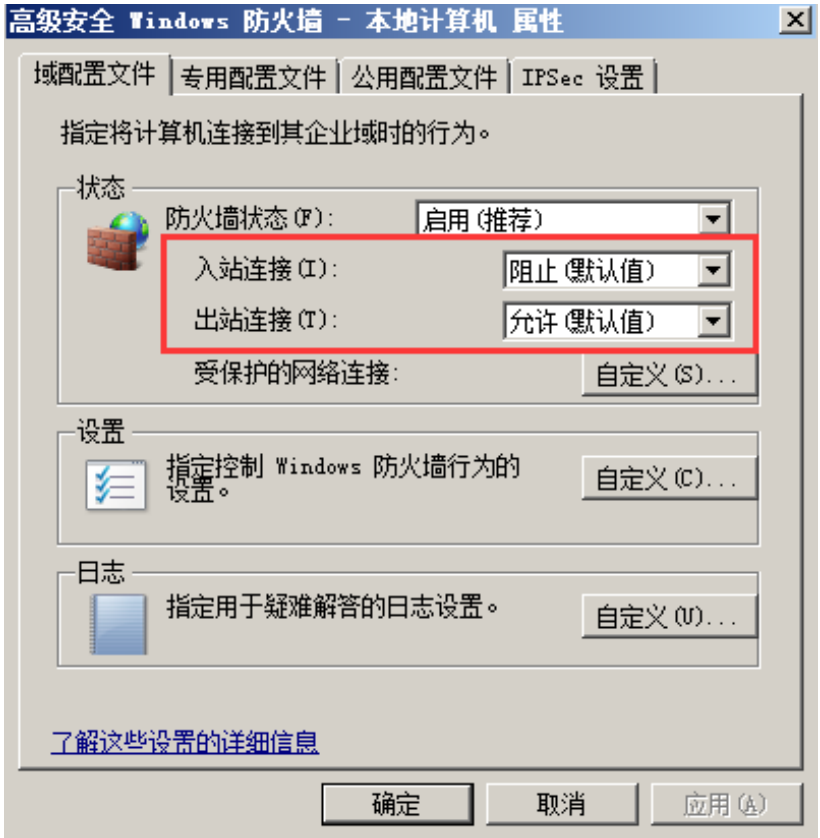
6 windows防火墙

6.1 Windows防火墙概述

系统防火墙功能

防火墙如同锁住了您家中的前门—它可以帮助阻止入侵者（在此情况下为黑客或恶意软件）进入。

仅就防火墙功能而言，默认情况下Windows防火墙只阻截所有传入的未经允许的流量，对主动请求传出的流量不作理会。



6 windows防火墙

6.2 Windows防火墙基本设置

开启、关闭防火墙

6 windows防火墙

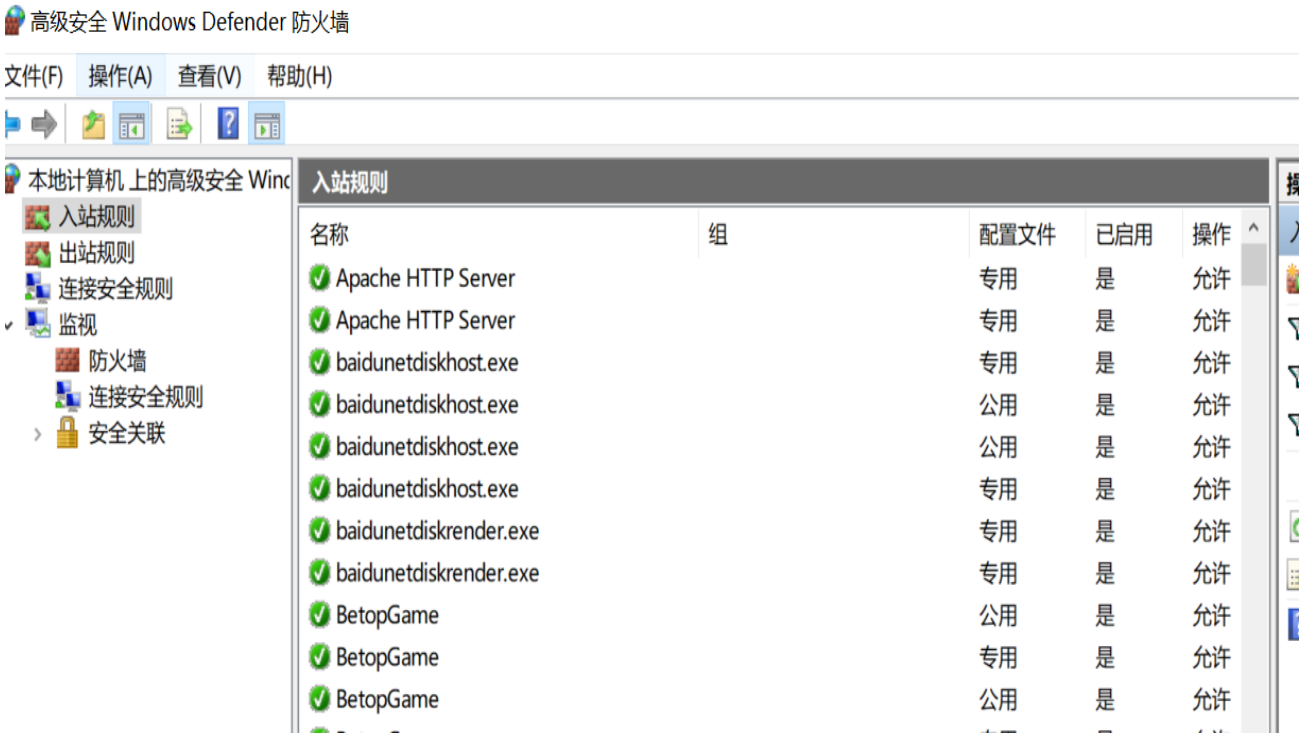
6.2 Windows防火墙基本设置

添加白名单

6 windows防火墙

6.3 Windows防火墙高级设置

高级设置



6 windows防火墙

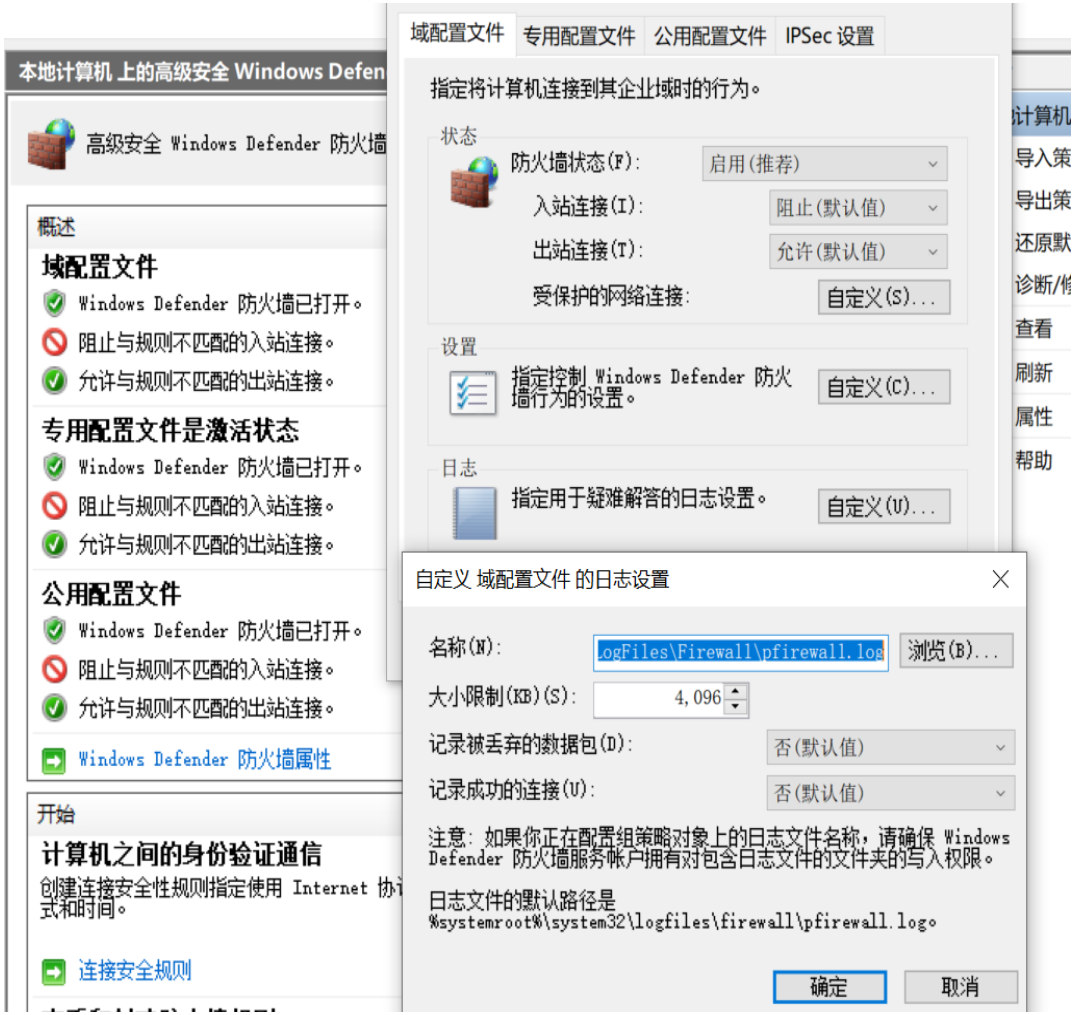
6.3 Windows防火墙高级设置

编辑规则属性

6 windows防火墙

6.3 Windows防火墙高级设置

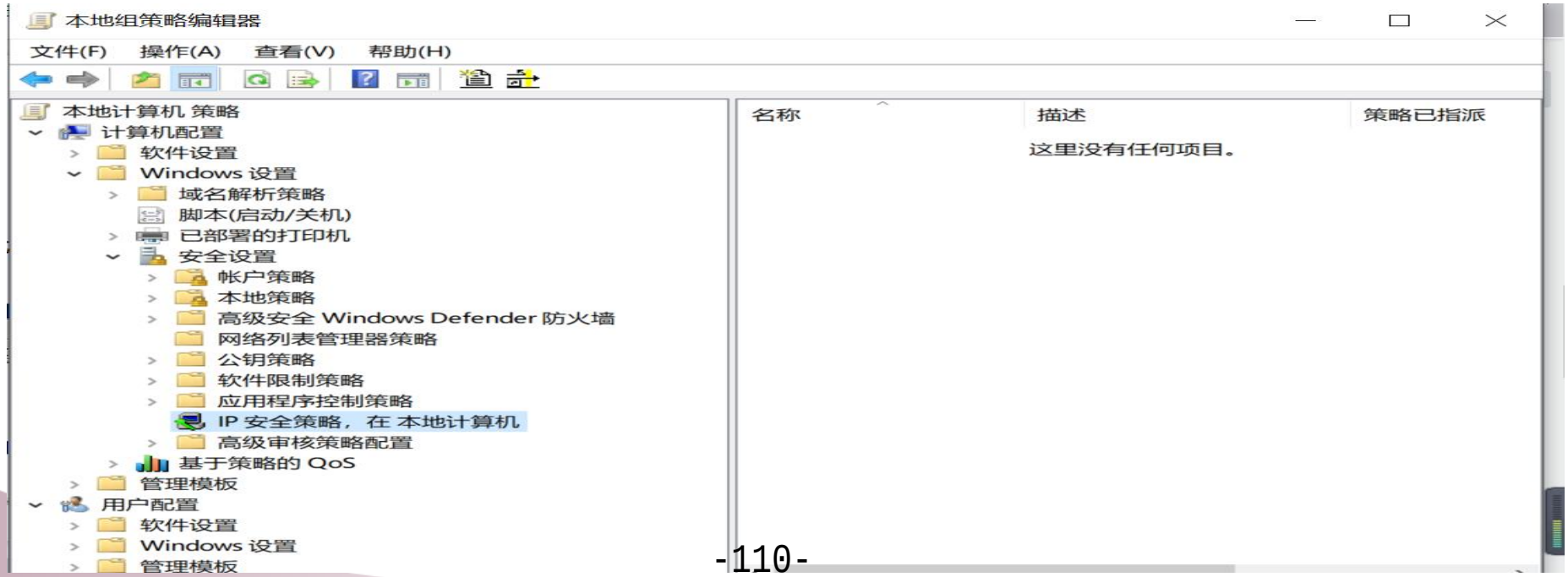
防火墙日志配置



6 windows防火墙

6.4 IP安全策略配置

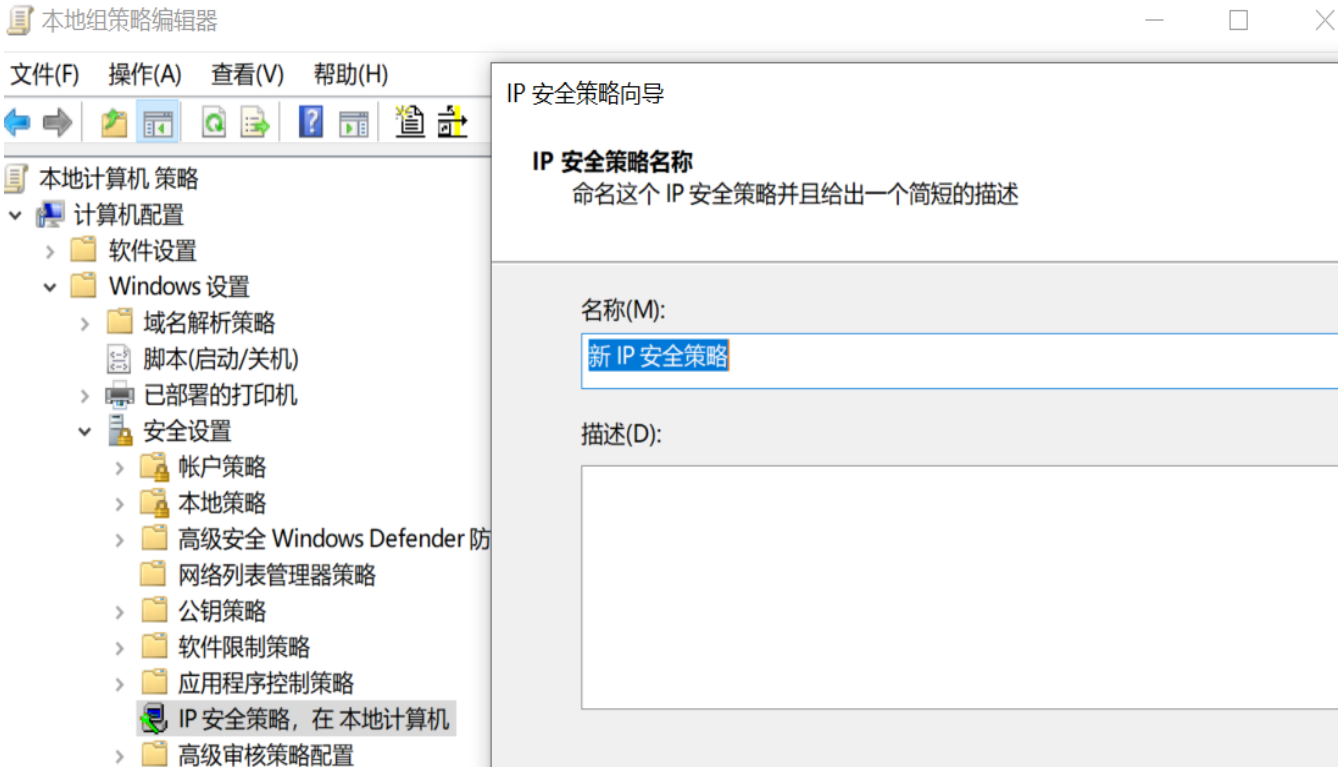
系统自带的IP安全策略，其功能并不比一些免费的防火墙差，可以关闭或开启端口，可以封掉指定的IP地址，还可以封掉指定的域名。



6 windows防火墙

6.4 IP安全策略配置

创建IP安全策略



6 windows防火墙

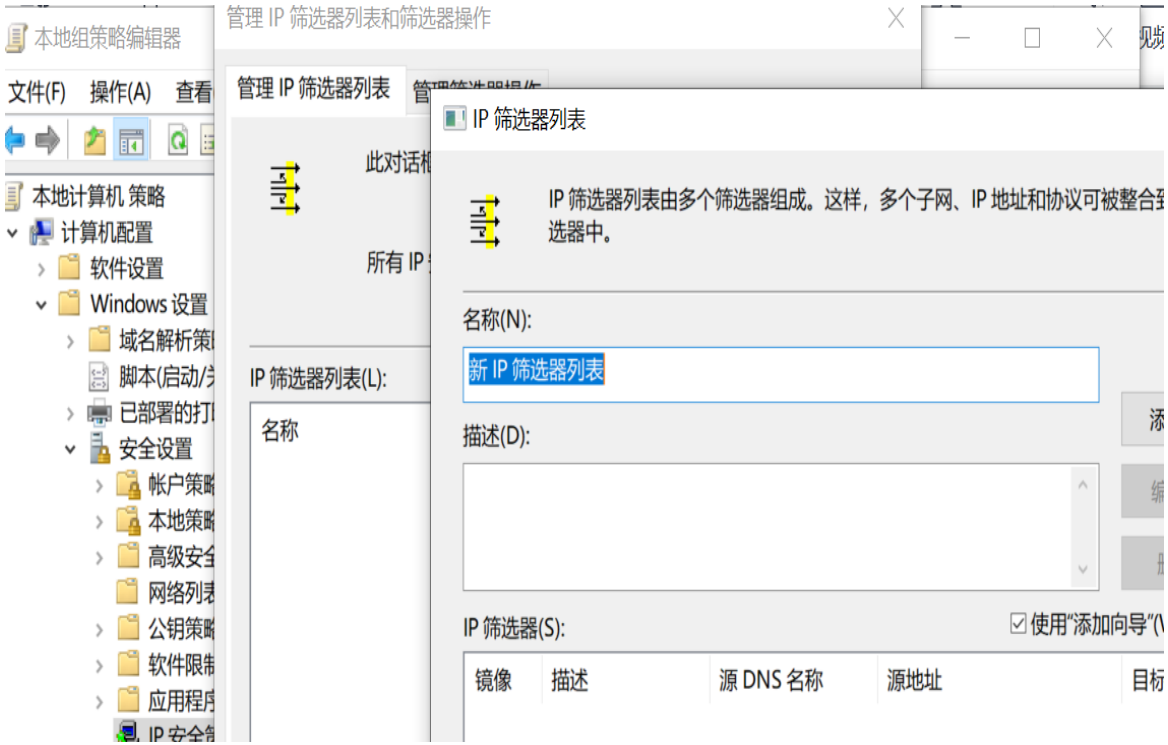
6.4 IP安全策略配置

编辑策略属性，添加IP筛选器

6 windows防火墙

6.4 IP安全策略配置

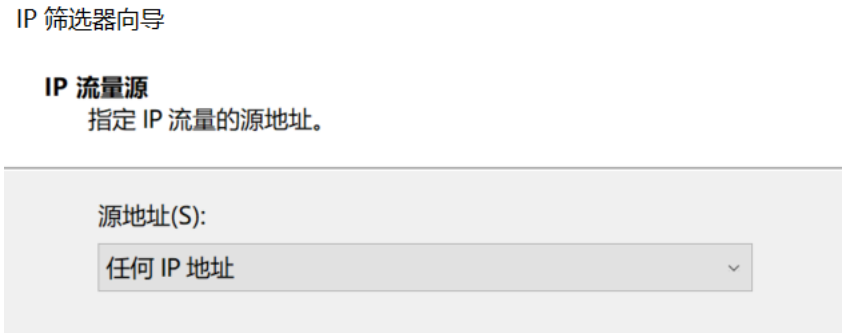
设置筛选器名称并添加

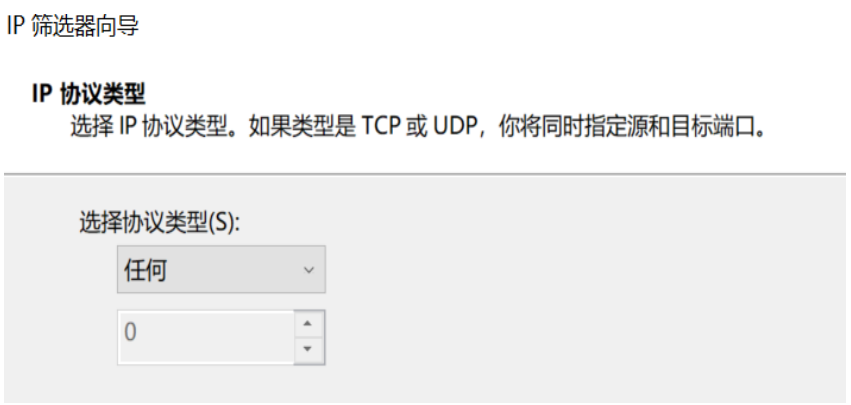


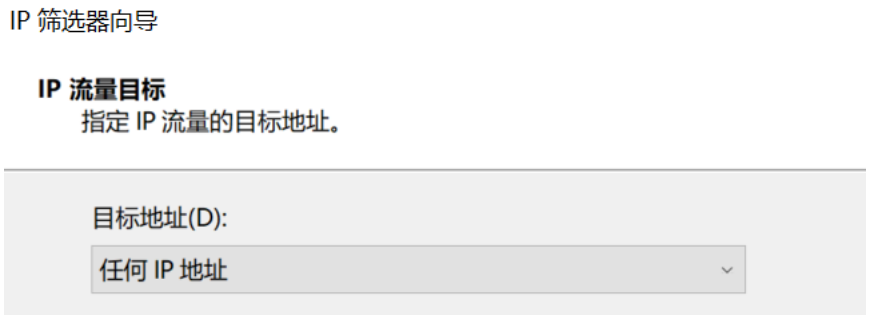
6 windows防火墙

6.4 IP安全策略配置

编辑筛选器属性，添加地址与协议。



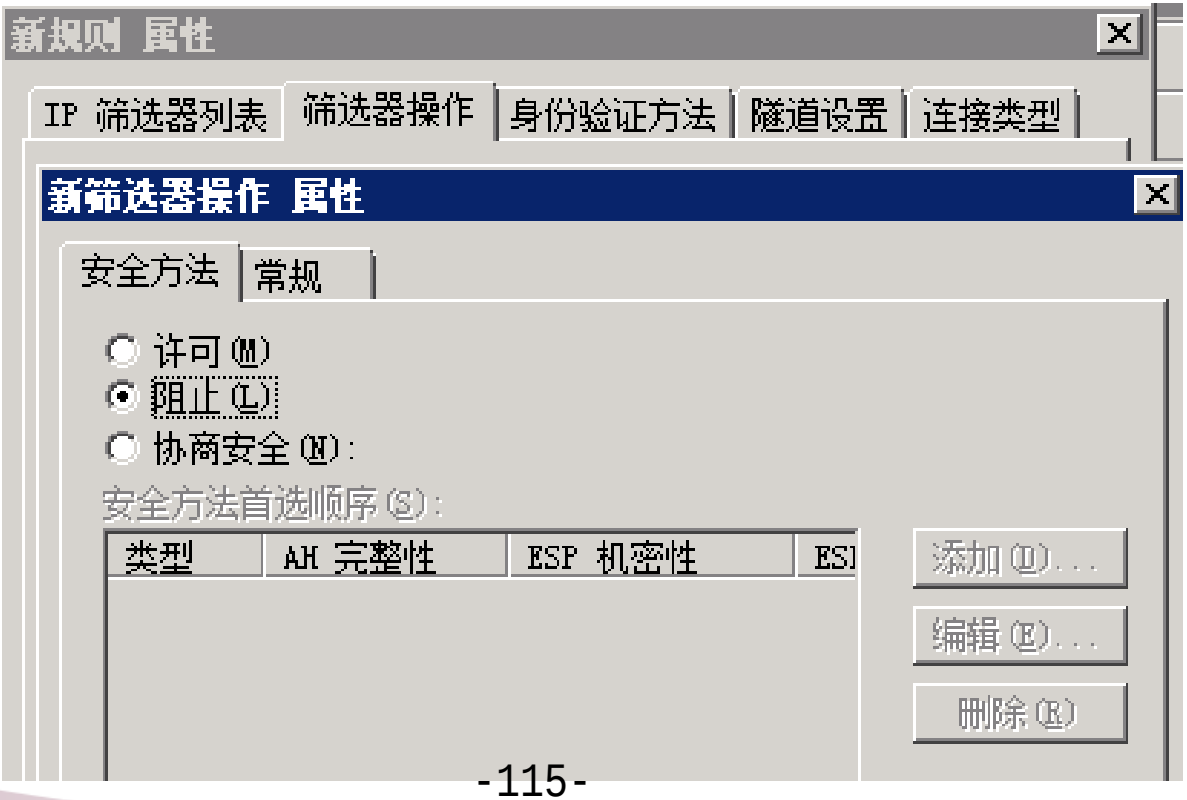




6 windows防火墙

6.4 IP安全策略配置

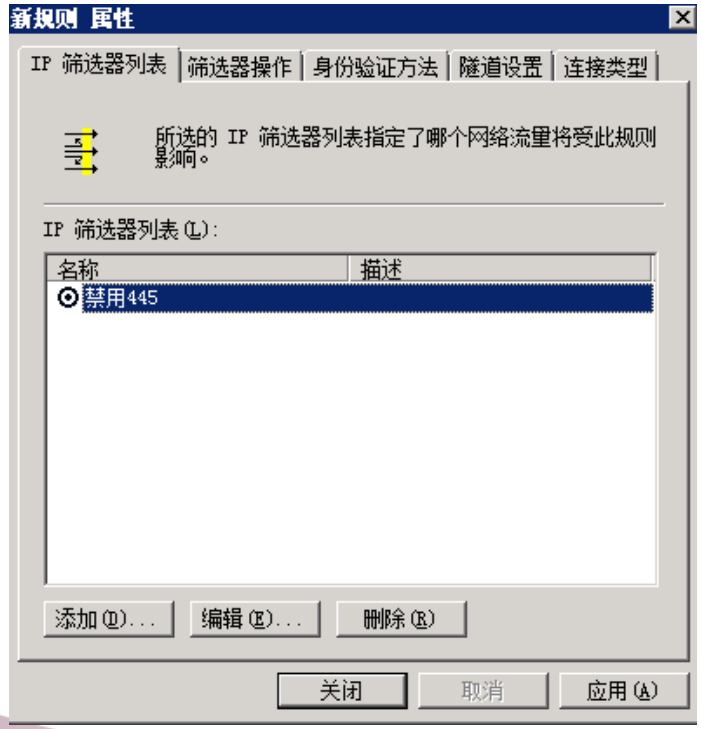
编辑筛选器操作，添加新筛选器操作

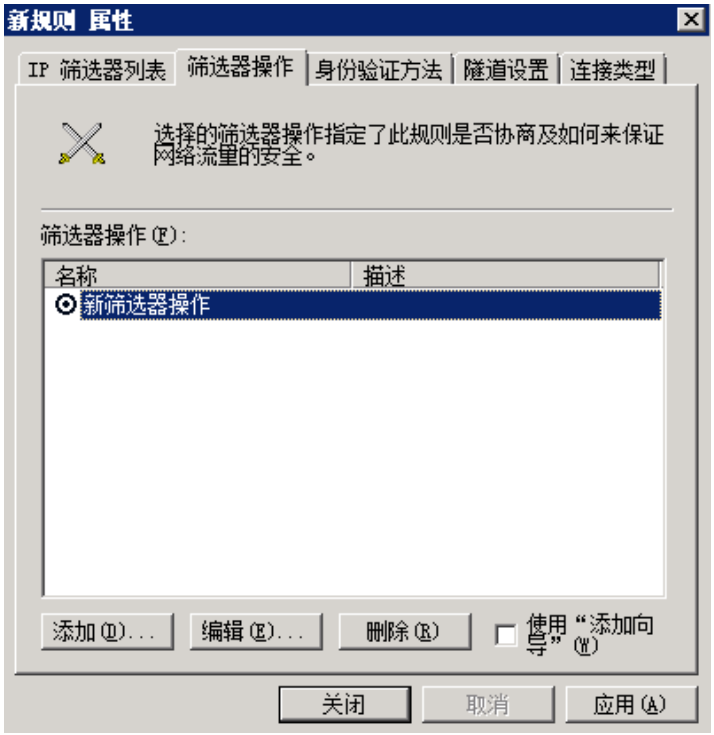


6 windows防火墙

6.4 IP安全策略配置

启用新建的IP筛选器和筛选器操作

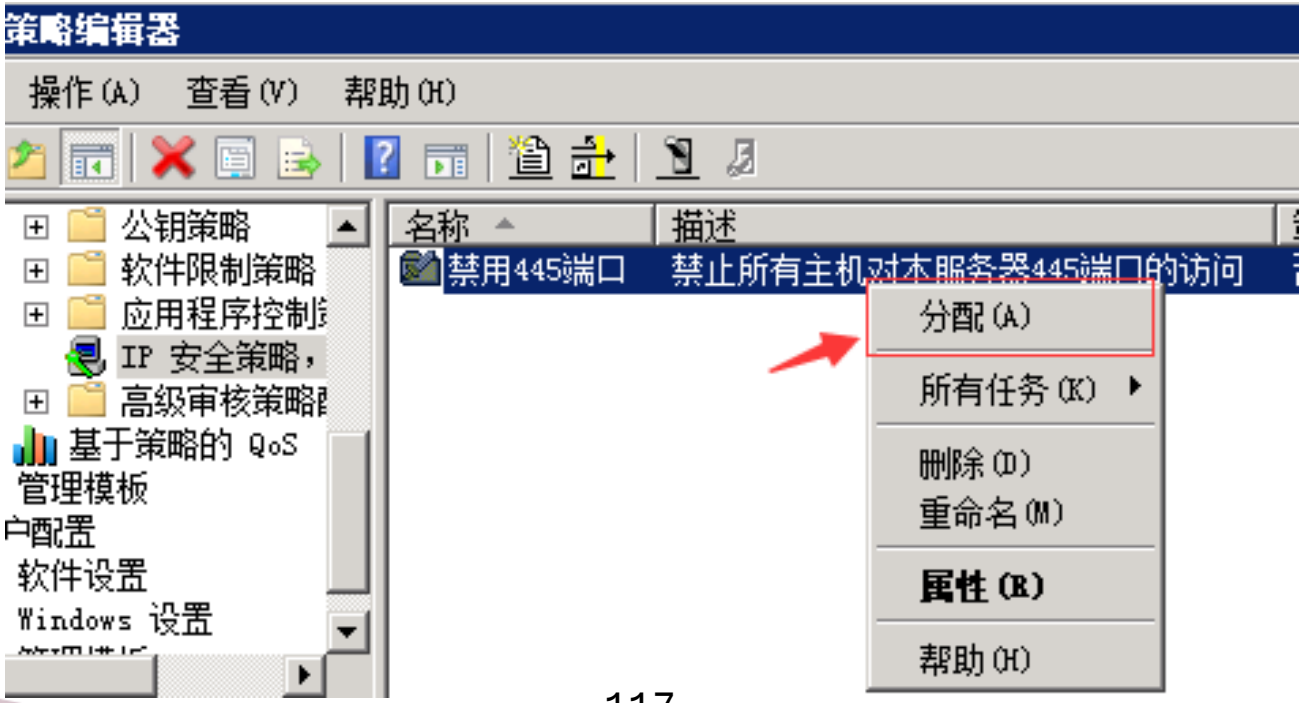




6 windows防火墙

6.4 IP安全策略配置

指派、分配IP策略



目录

7 组策略和注册表安全设置

7.1 组策略和注册表的基本概念

组策略（Group Policy）是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过使用组策略可以设置各种软件、计算机和用户策略。gpedit.msc

7 组策略和注册表安全设置

7.2 组策略安全配置

密码策略配置：

密码必须符合复杂性要求

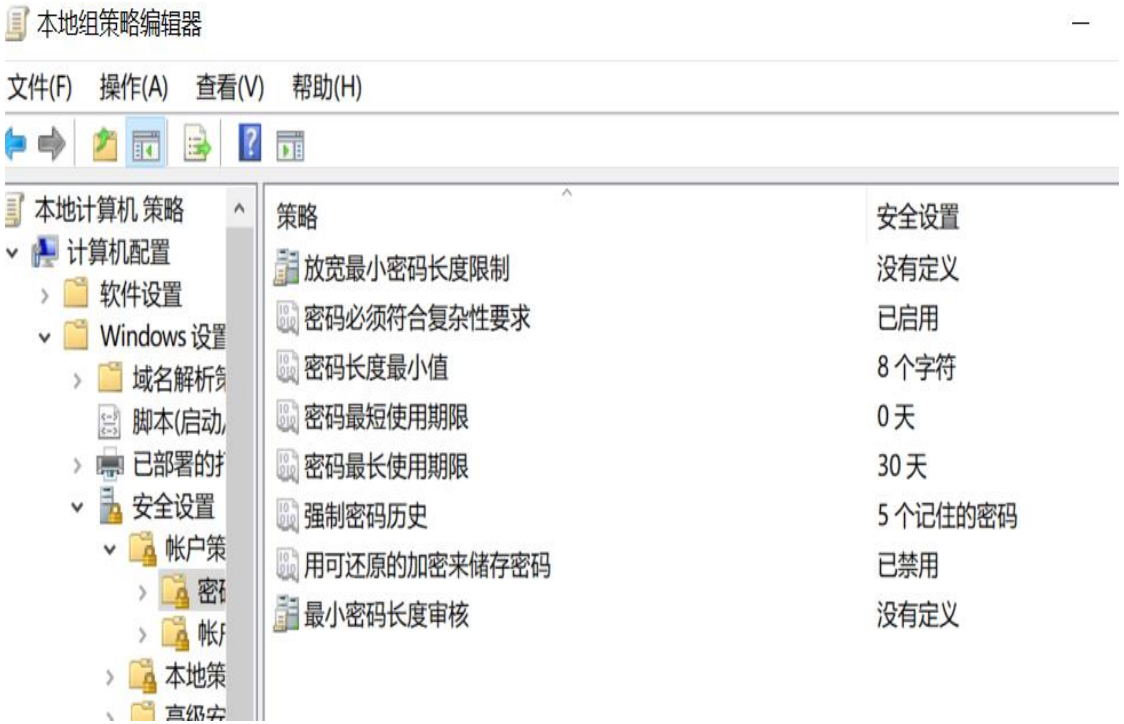
密码长度最小值

密码最短使用期限

密码最长使用期限

强制密码历史

用可还原的加密来储存密码



7 组策略和注册表安全设置

7.2 组策略安全配置

账户锁定策略配置：

账户锁定时间

账户锁定阈值

重置账户锁定计数器

7 组策略和注册表安全设置

7.2 组策略安全配置

审核配置：

审核策略更改

审核登录事件

审核对象访问

审核进程跟踪

审核目录服务访问

审核特权使用

审核系统事件

审核账户登录事件

审核账户管理

7 组策略和注册表安全设置

7.2 组策略安全配置

软件限制策略：

使用软件限制策略可以实现以下目的：

控制软件在系统中的运行能力。

允许用户在多用户计算机上仅运行特定文件。

控制软件限制策略是作用于所有用户，还是仅作用于计算机上的某些用户。

阻止任何文件在本地计算机、组织单位、站点或域中运行。

软件限制策略使用下列4个规则来标识软件：

哈希规则。使用可执行文件的加密密钥。

证书规则。使用软件发布者为可执行文件提供的数字签名证书。

路径规则。使用可执行文件位置的本地路径、通用命名约定路径或注册表路径。

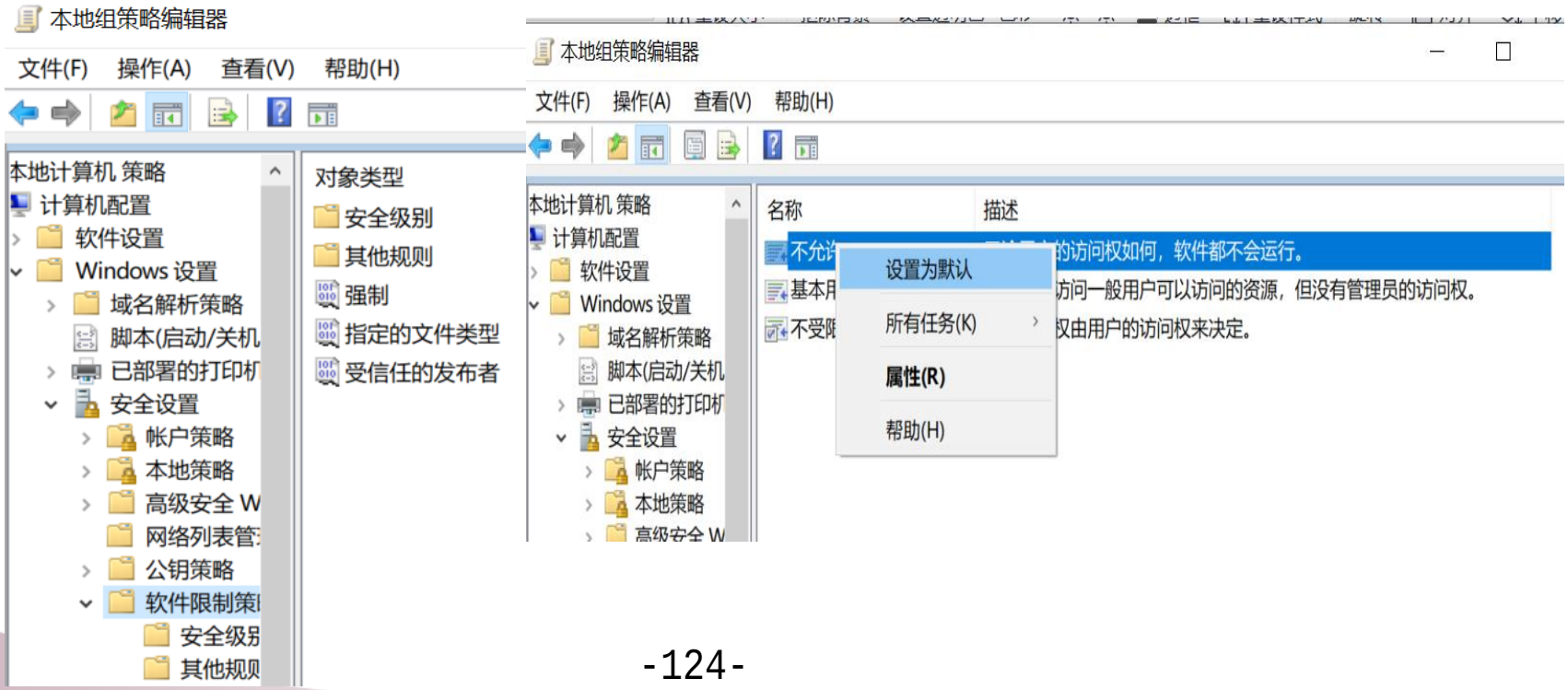
网络区域规则。使用可执行文件源自的Internet区域。

7 组策略和注册表安全设置

7.2 组策略安全配置

软件限制策略：

安全级别设置

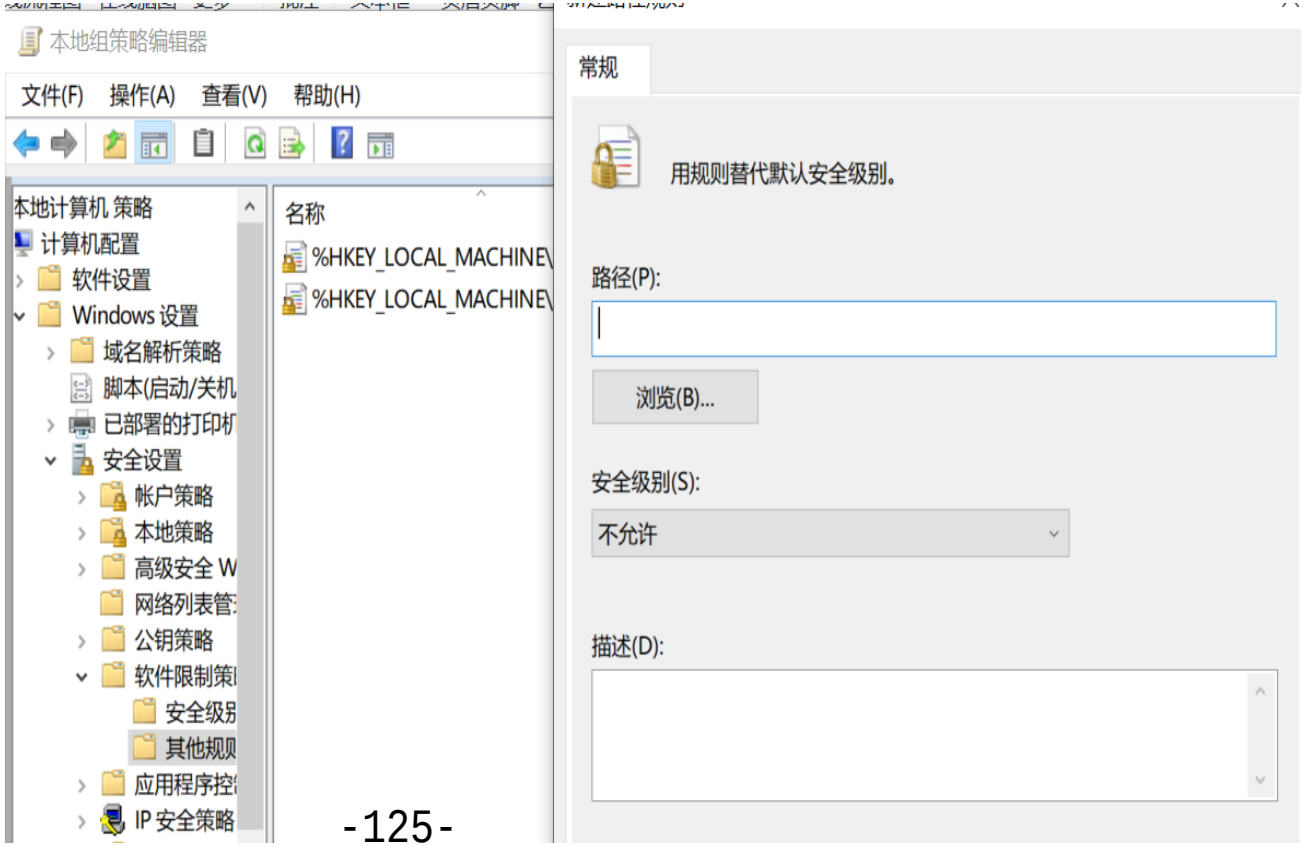


7 组策略和注册表安全设置

7.2 组策略安全配置

软件限制策略：

路径规则设置



目录

8 系统漏洞与补丁更新

8.1 系统漏洞的定义

系统漏洞（System vulnerabilities）是指应用软件或操作系统软件在逻辑设计上的缺陷或错误，被不法者利用，通过网络植入木马、病毒等方式来攻击或控制整个电脑，窃取电脑中的重要资料和信息，甚至破坏系统。

8 系统漏洞与补丁更新

8.2 系统漏洞的管理流程

现状分析

补丁跟踪

补丁分析

部署安装

疑难处理

补丁检查

8 系统漏洞与补丁更新

8.3 补丁检查

8.3.1 systeminfo命令

Systeminfo命令是Windows中用于显示关于计算机及其操作系统的详细配置信息，包括操作系统配置、安全信息、产品 ID 和硬件属性，如 RAM、磁盘空间和网卡和补丁信息等。

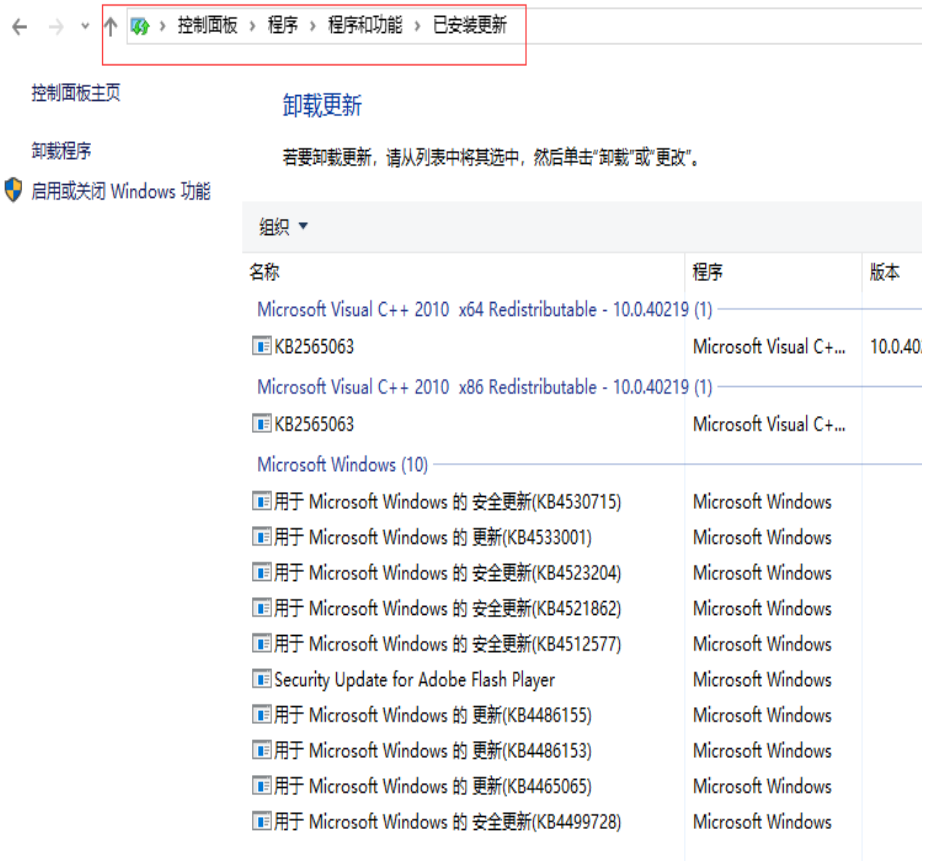
8 系统漏洞与补丁更新

8.3 补丁检查

8.3.2 控制面板检查

Win10之前，在控制面板的windows update里可以检查系统更新

最新的win10以及server16系统中，可以再卸载程序面板的已安装更新选项里检查所有补丁，并进行卸载更改等操作。



8 系统漏洞与补丁更新

8.4 补丁更新

手动更新

自动更新

离线更新

8 系统漏洞与补丁更新

8.4 补丁更新

8.4.1手动更新

进入Microsoft安全中心查看漏洞公告

http://technet.microsoft.com/zh-cn/security/default.aspx

8 系统漏洞与补丁更新

8.4 补丁更新

8.4.1手动更新

点击已发布的安全公告，查看所发布的漏洞详情

Microsoft 安全公告 MS16-148 - 严重

Microsoft Office 安全更新 (3204068)

发布日期：2016 年 12 月 13 日

版本：1.0

执行摘要

此安全更新可修复 Microsoft Office 中的多个漏洞。最严重的漏洞可能在用户打开经特殊设计的 Microsoft Office 文件时允许远程执行代码。成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响较小。

有关详细信息，请参阅**受影响的软件和漏洞严重等级**部分。

此安全更新通过更正以下行为修复这些漏洞：

- Microsoft Office 初始化变量的方式。
- Microsoft Office 验证输入的方式。
- Microsoft Office 重新检查注册表数值的方式。
- Microsoft Office 分析文件格式的方式。
- 受影响版本的 Office 和 Office 组件处理内存中对象的方式。
- Microsoft Office for Mac Autoupdate 验证程序包的方式。

如需了解漏洞的更多信息，请参阅**漏洞信息**部分。

8 系统漏洞与补丁更新

8.4 补丁更新

8.4.1手动更新

在漏洞详情页中，找到我们安装的受影响的操作系统或软件

受影响的软件	Microsoft Office 安全功能绕过漏洞 – CVE-2016-7262	Microsoft Office 信息泄漏漏洞 – CVE-2016-7264	Microsoft Office 信息泄漏漏洞 – CVE-2016-7265	Microsoft Office 安全功能绕过漏洞 – CVE-2016-7266
Microsoft Office 2007				
Microsoft Excel 2007 Service Pack 3 (3128019)	**重要** 远程执行代码	**重要** 信息泄漏	**重要** 远程执行代码	**重要** 远程执行代码
Microsoft Word 2007 Service Pack 3 (3128025)	不适用	不适用	不适用	不适用

8 系统漏洞与补丁更新

8.4 补丁更新

8.4.1手动更新

选择语言并点击下载，开始下载补丁程序。

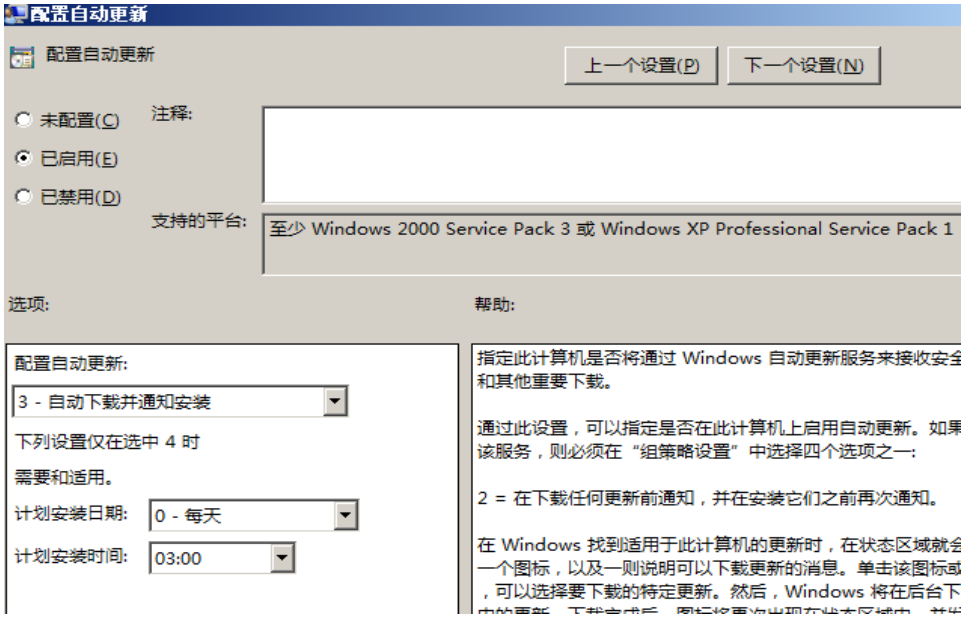
补丁下载完成之后，将补丁拷贝到需要安装该补丁的操作系统上进行安装。

8 系统漏洞与补丁更新

8.4 补丁更新

8.4.2自动更新

在cmd命令行下执行命令gpedit.msc打开组策略编辑器。依次单击展开“本地计算机”—“计算机配置”—“管理模板”—“Windows 组件”—“Windows Update”，双击“配置自动更新”策略，打开策略配置对话框。勾选“已启用”并配置自动更新计划



8 系统漏洞与补丁更新

8.4 补丁更新

8.4.3离线更新

离线补丁的更新与手动更新基本相同，只多出了拷贝补丁的操作，这种情况下，我们一般推荐先在一台离线主机上进行病毒查杀管理。

8.4.3注意事项

1、确认你的操作系统大版本、小版本

2、确认补丁和版本的对应是否一致

3、有些补丁包，需要先安装更早的补丁包。

4、有些补丁需要重启，部分服务器不得随意重启

谢 谢