# 实验4 操作系统安全技术-访问控制与系统审计

1. 实验目的

通过实验掌握Windows账户与密码的安全设置、文件系统的保护和加密、审核和日志的启用，建立一个Windows操作系统的基本安全框架。

2. 实验原理

我们从账户口令、文件系统、日志和审核、安全漏洞扫描等方面对Windows操作系统安全进行介绍。

（1）账户和口令。首先需要保障账户和密码的安全。

（2）文件系统。NTFS文件系统是Windows操作系统中的一种安全的文件系统，管理员或用户可以设置每个文件夹的访问权限，从而限制一些用户和用户组的访问，以保障数据的安全。

（3）加密文件系统EFS。EF的加密功能对敏感数据文件进行加密，可以加强数据的安生性，并且减小计算机、磁盘被窃或者被拆换后数据失窃的隐患。EFS采用了对称和非对称两种加密算法对文件进行加密，首先系统利用生成的对称密钥将文件加密成为密文，然后采用EFS证书中包含的公钥将对称密钥加密后与密文附加在一起。文件采用EFS加密后，可以控制特定的用户有权解密数据，这样即使攻击者能够访问计算机的数据存储器，也无法读取用户数据。只有拥有EFS证书的用户，采用证书中公钥对应的私钥，先解密公钥加密的对称密钥，然后再用对称密钥解密密文，才能对文件进行读写操作。EFS属于NTFS文件系统的一项默认功能，同时要求使用EFS的用户必须拥有在NTFS卷中修改文件的权限。

4）审核与日志。通过本地安全策略开启审核，对关键数据进行监控，结果在日志文件中体现。

3. 实验环境

NTFS支持下的Windows系统。

4. 实验内容

（1）分区格式检查

进入资源管理器，右击“E盘”，检查是否为NTFS分区？若不是，则将该分区重新格式化成NTFS格式。若没有E盘，则先进入“Windows管理工具”🡪“计算机管理”🡪“管理工具”🡪“磁盘管理”，创建一个E盘!

图形用户界面

描述已自动生成

在E盘中新建一个RAV文件夹，并从Windows\system32中将notepad.exe复制进去。

（2）创建工作用户和工作目录

在“命令提示符”下键入以下命令，完成后进入资源管理器和管理工具检查操作结果,记录能否访问三个文件夹？为什么？

E:

Md user1 建立子目录

Md user2

Md user3

Net user st1 /add 建立用户

Net user st2 /add

Net user st3 /add

Cacls user1 /g st1:f 赋予指定用户权限

Cacls user2 /g st2:f

Cacls user3 /g st3:f

文本

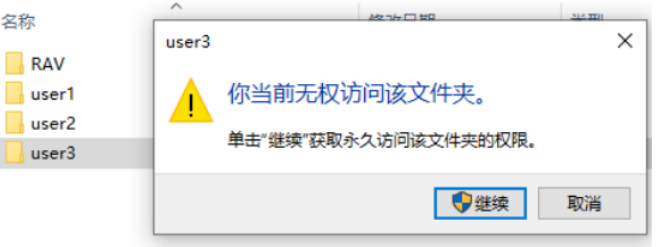
描述已自动生成

图形用户界面, 文本, 应用程序, Word

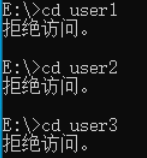
描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成



当前用户没有这三个文件夹的访问权限，所以无法进入这三个文件夹。



（3）加密文件系统EFS的使用

1）注销系统，并以ST3登录，进入“资源管理器”，打开user3文件夹（此时为什么能访问了？）。新建一个文本文件aaa.txt，内容为1234。完成后存盘关闭文件。

图形用户界面, 应用程序

描述已自动生成

文本

描述已自动生成

可以进入user3文件夹，新建文件aaa.txt

图形用户界面, 文本, 应用程序

描述已自动生成

2）右击aaa.txt，选择“属性”🡪 “高级”，选中“加密内容保护数据”，并“确定”返回。

3）注销系统，再用“administrator”登录（默认口令为123456）。访问user3目录，若不能访问，则更改“安全”权限，添加administrator的访问权。

4）打开aaa.txt，记录结果!

图形用户界面, 文本, 信件

描述已自动生成

（4）熟悉“共享”和“安全”权限内容

进入“资源管理器”，打开E盘内容，右击目标文件夹RAV，选择“属性”，依次了解“共享”和“安全”的组成内容。

（5）系统审计的实现

1）进入“控制面板”-“管理工具”-“本地安全策略”-“本地策略”，将“对象访问”审核打开（选中“成功”）。

图形用户界面, 文本, 应用程序

描述已自动生成

2）进入目标文件夹RAV的“属性”🡪“安全”🡪“高级”🡪“审核”。按以下要求设置审核规则：添加需审核用户(组)为“everyone”

1、运行文件 成功 失败

2、创建文件夹 成功

3、删除文件夹 成功 失败

图形用户界面, 文本, 应用程序

描述已自动生成

图形用户界面

中度可信度描述已自动生成

（6）通过事件查看器查看审计结果

进入“管理工具”🡪“事件查看器”，查看“应用程序”、“系统日志”、“安全日志”的结果，了解前述审计规则的记录状况。

如，下图是事件查看器中的一条用WPS打开RAV中的一个Word文件的记录。

图形用户界面, 应用程序

描述已自动生成

5. 实验小结

理解访问权限、审计的作用。