Windows 系统安全综述

1、账户分类及概述

1.1 用户账户

a. 不同的用户身份拥有不同的权限
b. 每个用户包含一个名称和一个密码
c. 用户账户拥有唯一的安全标识符

在服务器管理器中管理用户

a. 创建用户
b. 为用户重置密码
c. 重命名用户名
d. 启用，禁用，删除用户账户
e. 为用户设置权限

通过进程与服务区分各内置用户账户的作用

与使用者关联的用户账户

a. Administrator（管理员用户）
b. Guest（来宾用户）

与 Windows 组件关联的用户账户

a. SYSTEM（本地系统）
b. SYSTEM SERVICE（本地服务）
c. NETWORK SERVICE（网络服务）

1.2 组账户

a. 组是一些用户的集合
b. 组内的用户自动具备组所设置的权限

在服务器管理其中管理组

a. 新建组
b. 向组内添加成员
c. 重命名组
d. 删除组

需要人为添加成员的内置组

a. Administrator
b. Guests
c. Power User
d. Users（标准用户）

动态包含成员的内置组

a. Interactive（动态包含在本地登陆的用户）
b. Authenticated Users（动态包含通过验证的用户，不包含来宾用户）
c. Everyone（包含任何用户，设置开放的权限是经常使用）

1.3 克隆账户以及账户超级隐藏

在添加用户时在要添加的用户名后边多加一个 $ 符号(表示隐藏)

net user test$ /add

通过这种方式创建的用户直接使用命令行的 net user 命令是无法查看到的，但是可以通过计算机管理界面查看到存在该账户

通过修改注册表中的信息来达到完全隐藏账户的

a. 新建一个常规的隐藏账户（test$）
b. 打开注册表，找到 HKEY_LOCAL_MACHINE 下的 SAM，右键为其赋予权限之后展开
c. 将 Administrator 的权限导出，同时将 test$账户的权限和用户信息注册表导出
d. 打开导出的 Administrator 和 test 的权限注册表，用 Administrator 中的 F 的值代替 test 的权限注册表，用 Administrator 中的 F 的值代替 test 的权限注册表，用 Administrator 中的 F 的值代替 test 中的 F 的值
e. 删除之前创建的 test$用户
f. 运行之前导出的 test 的注册表和 test 的注册表和 test 的注册表和 test 权限的注册表
g. 完成完全隐藏用户的创建（只能通过注册表来查找到）

2、NTFS 文件系统及权限应用

NTFS (New Technology File System)，是 WindowsNT 环境的文件系统。新技术文件系统是 Windows NT 家族（如，Windows 2000、Windows XP、Windows Vista、Windows 7 和 windows 8.1）等的限制级专用的文件系统（操作系统所在的盘符的

文件系统必须格式化为 NTFS 的文件系统，4096 簇环境下）。NTFS 取代了老式的 FAT 文件系统。

NTFS 对 FAT 和 HPFS 作了若干改进，例如，支持元数据，并且使用了高级数据结构，以便于改善性能、可靠性和磁盘空间利用率，并提供了若干附加扩展功能。

提高磁盘读写性能

可靠性

a. 加密文件系统

b. 访问控制列表

磁盘利用率

a. 压缩

3、EFS 加密

为了提高文件的安全性，微软在 Windows 中针对 NTFS 引入了 EFS 加密技术。EFS 加密操作简单，对加密文件的用户也是透明的，文件加密后不必再试用期手动解密，只有加密则才能打开加密文件。

EFS 加密是基于公钥策略的。然后将利用 FEK 和数据扩展标准 X 算法创建加密后的文件，。如果你登录到了域环境中，密钥的生成依赖于域控制器，否则它就依赖于本地机器。

EFS 加密最简单的办法就是在目标对象上点击鼠标右键，选择“属性”，打开属性对话框,然后在常规选项卡上点击“高级”按钮，打开高级属性对话框，选中“加密内容以便保护数据”这个选项，反之解密。

4、服务

service 可以分为两个大类，服务应用程序和驱动服务。

服务应用程序指遵照 Service Control Manager 2 接口要求的，能在系统启动时自动启动的用户能够通过服务控制面板控制的那些没有用户登录也能够运行的程序。

驱动服务一般指设备驱动程序协议等应用于底层设备驱动的服务

5、病毒及防范

5.1 计算机病毒

定义

编制或者在计算机程序中插入的，破坏技术啊你功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码

特点

a. 非授权执行

b. 隐蔽性

c. 传染性

d. 潜伏性

e. 破坏性

f. 可触发性

分类

a. 文件型

b. 引导扇区型

c. 宏病毒

d. VBS 脚本病毒

e. 蠕虫

5.2 脚本病毒

a. 通常与网页相结合，将恶意的破坏性代码内嵌在网页中

b. 利用 asp，htm，html，vbs，js 类型的文件进行传播

c. 基于 VB Script 和 Java Script 脚本语言

d. 由 Windows 脚本宿主解释执行（也具有跨平台的特性）

特点

a. 隐蔽性强

浏览网页，电子邮件中的病毒可以具有双拓展名

b. 传播性广

可以自我复制，不依赖于其他文件就可以直接解释执行

c. 病毒变种多

只需要对源码稍加修改，就可以制造出新的变种病毒

5.3 计算机木马

定义

一个包含在合法程序中的非法程序

特征

a. 未经许可即获得计算机的使用权
b. 程序容量小，执行时不会占用太多资源
c. 执行后很难停止
d. 执行时不会在系统中显示出来
e. 执行一次后会驻留在系统中，可以自动加载运行
f. 自动变更文件名
g. 作为驻留程序隐藏在系统内部
h. 分为客户端和服务端

危害

文件操作，修改注册表，窃取密码，系统操控。