SAM 子键与 SECURITY 子键

学生姓名	maybeLocalhost
学　　号	
专业班级	
指导教师	
学　　院	计算机学院
完成时间	2021.06

目录

一、注册表

1.1 注册表概念

注册表是 windows 操作系统、硬件设备以及客户应用程序得以正常运行和保存设置的核心“数据库”，也可以说是一个非常巨大的树状分层结构的数据库系统。

注册表记录了用户安装在计算机上的软件和每个程序的相互关联信息，它包括了计算机的硬件配置，包括自动配置的即插即用的设备和已有的各种设备说明、状态属性以及各种状态信息和数据。利用一个功能强大的注册表数据库来统一集中地管理系统硬件设施、软件配置等信息，从而方便了管理，增强了系统的稳定性。

1.2 注册表功能

注册表中记录了用户安装在计算机上的软件和每个程序的相关信息，通过它可以控制硬件、软件、用户环境和操作系统界面的数据信息文件。注册表文件的数据信息保存在 system.dat 和 user.dat 中、利用 regedit.exe 程序能够存取注册表文件。

1.3 注册表编辑器

在运行里输入“regedit.exe”即可进入注册表编辑器。注册表编辑器主要由以下三个部分组成：

- 根键：这个称为 HKEY……，某一项的句柄项：附加的文件夹和一个或多个值；
- 子键：在某一个项（父项）下面出现的项（子键）；
- 值项：带有一个名称和一个值的有序值，每个项都可包括任何数量的值项，值项由三个部分组成：名称、数据类型和数据。

(1) 名称：不包括反斜线的字符、数字、代表符和空格的任意组合。同一键中不可有相同的名称；

(2) 数据类型：包括字符串、二进制和双字节等；

(3) 数据：值项的具体值，它的大小可以占用 64KB。

1.4 注册表结构分析

注册表包括以下 5 个根键：

(1) HKEY_CLASSES_ROOT

说明：该根键包括启动应用程序所需的全部信息，包括扩展名，应用程序与文档之间的关系，驱动程序名，DDE 和 OLE 信息，类 ID 编号和应用程序与文档的图标等。

(2) HKEY_CURRENT_USER

说明：该根键包括当前登录用户的配置信息，包括环境变量，个人程序以及桌面设置等。

(3) HKEY_LOCAL_MACHINE

说明：该根键包括本地计算机的系统信息，包括硬件和操作系统信息，安全数据和计算机专用的各类软件设置信息。

(4) HKEY_USERS

说明：该根键包括计算机的所有用户使用的配置数据，这些数据只有在用户登录系统时才能访问。这些信息告诉系统当前用户使用的图标，激活的程序组，开始菜单的内容以及颜色，字体。

(5) HKEY_CURRENT_CONFIG

说明：该根键包括当前硬件的配置信息，其中的信息是从 HKEY_LOCAL_MACHINE 中映射出来的。

二、HKEY_LOCAL_MACHINE

HKEY_LOCAL_MACHINE 是一个显示控制系统和软件的处理键。HKLM 键保存着计算机的系统信息。它包括网络和硬件上所有的软件设置。（比如文件的位置，注册和未注册的状态，版本号等等）这些设置和用户无关，因为这些设置是针对使用这个系统的所有用户的。HKEY_LOCAL_MACHINE 根键包含 5 个子键，分别为 HARDWARE 子键、SAM 子键、SECURITY 子键、SOFTWARE 子键和 SYSTEM 子键。

2.1 HARDWARE 子键

HARDWARE 子键包括了系统使用的浮点处理器、串口等信息：ACPI:存放高级电源管理接口数据；DEVICEMAP：用于存放设备映射；DEscriptION：存放有关系统信息；RESOURCEMAP：用于存放资源列表。

2.2 SAM 子键

SAM 是 Security Account Manger 的简称，SAM 子键中包含用户与用户组帐户的有关信息,这些信息统称为 SAM 数据库。该子键受系统保护，用户不能看到里面的内容。在 WinNT/Win2000/WinXP/Win2003/Win Vista 密码文件位于 “%systemroot%\system32\config\”的 sam 文件。

2.3 SECURITY 子键

SECURITY 子键包含安全设置的有关相关信息，比如用户的访问权限设置、密码原则和本机用户组的成员等，该子键同样受系统保护，内容不可见。

2.4 SOFTWARE 子键

SOFTWARE 子键中保留的是所有已安装的 32 位应用程序的信息，各个程序的控制信息分别安装在相应的子键中，由于不同的计算机安装的应用程序互不相同，因此这个子键下面的子键信息也不完全一样。

2.5 SYSTEM 子键

SYSTEM 子键是启动时所需的信息和修复系统时所需要的信息：currentcontrol:保存了当前驱动程序控制集中的所有信息

三、使用 SAM 子键更改用户权限

操作系统所有的用户信息都保存在注册表中，但是如果直接使用“regedit.exe”命令打开注册表，该键值是隐藏的。我们可以利用工具软件 psu.exe 得到该键值的查看和编辑权。将 psu.exe 拷贝对方主机的 C 盘下，并在任务管理器查看对方主机 winlogon.exe 进程的 ID 号。

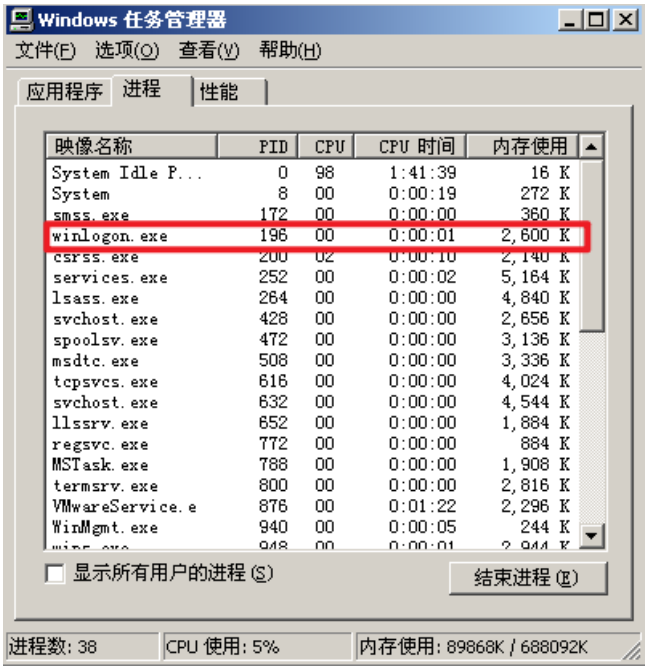

图 1 winlogon.exe 进程的 ID 号

其进程号为 196，保证注册表关闭，并执行以下命令：

```
psu -p regedit -i 196
```

```
C:\>psu -p regedit -i 196

Psu 1.01 (Process Super user) for Windows NT/2000 System Administrator
Creates a process in the context of the other user's security context
without using that user's password.
(c)2001 . support by batman.lee at 263.net
```

图 2 运行 psu.exe 得到该键值的查看和编辑权

执行完命令以后，自动打开了注册表编辑器，查看 SAM 下的键值：

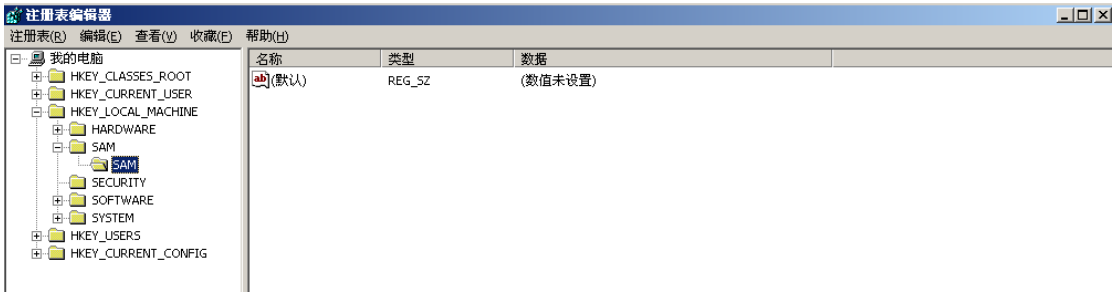

图 3 查看 SAM 下的键值

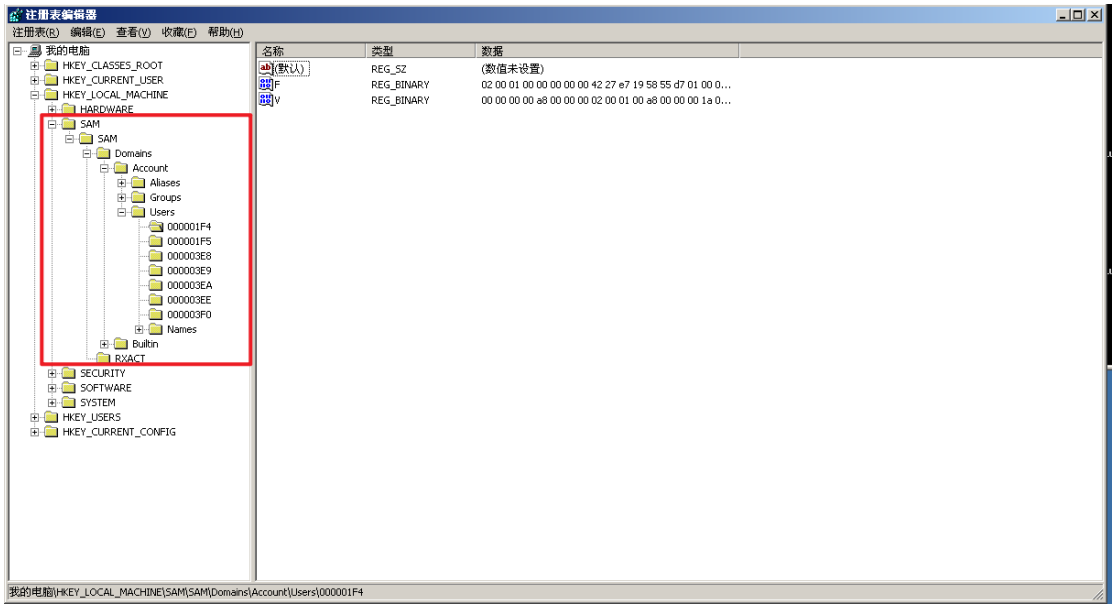

图 4 查看 SAM 下的键值

查看 Administrator 和 guest 默认的键值，在 Windows 2000 操作系统上，Administrator 一般为 0x1f4，guest 一般为 0x1f5。

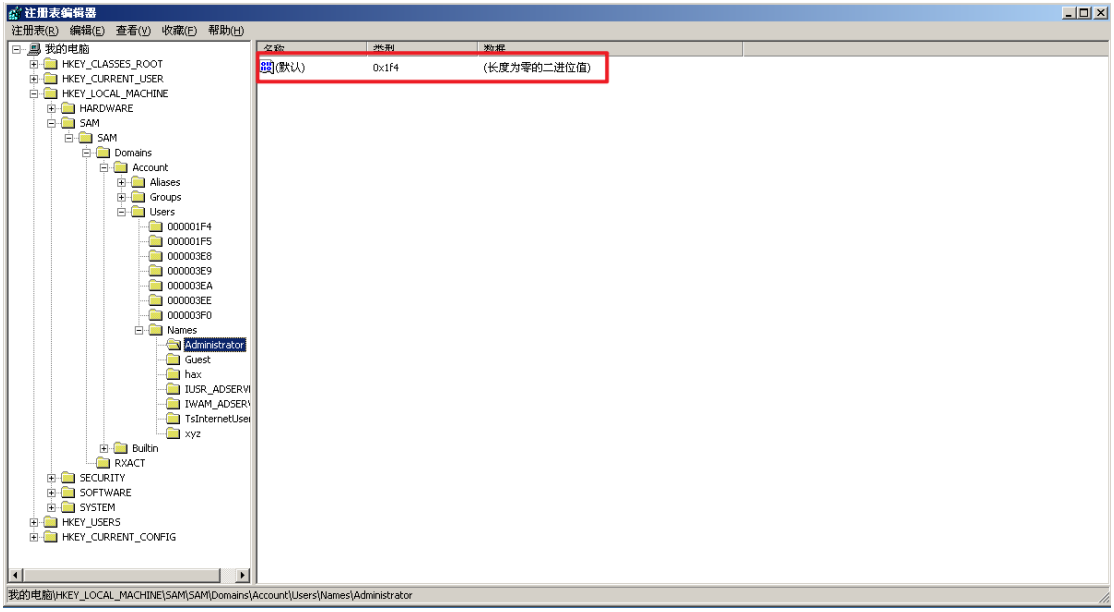

图 5 Administrator 键值

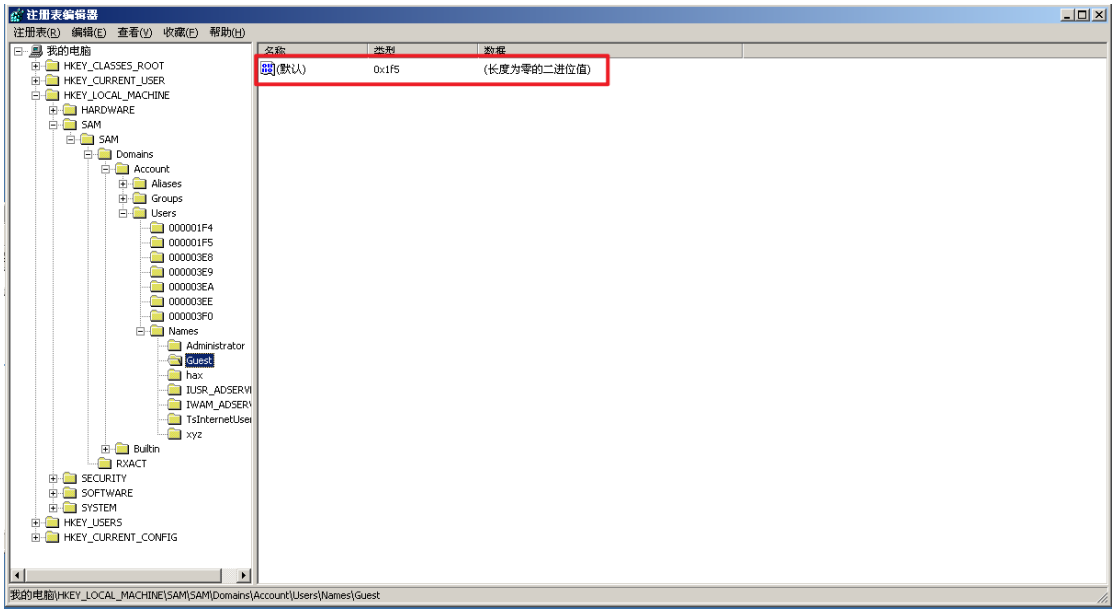

图 6 guest 键值

根据“0x1f4”和“0x1f5”找到 Administrator 和 guest 帐户的配置信息：

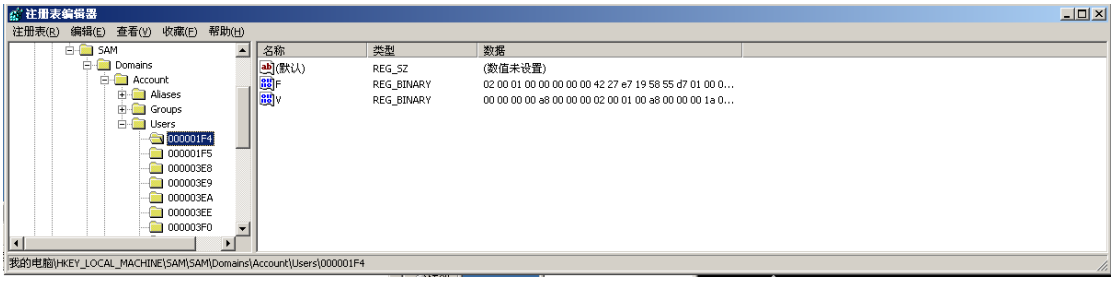

图 7 Administrator 帐户的配置信息

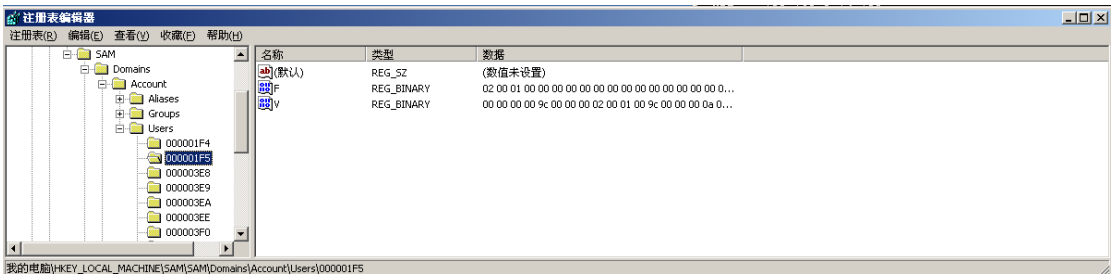

图 8 guest 帐户的配置信息

注册表编辑器右边栏目中的 F 键值中保存了帐户的密码信息，双击“000001F4”目录下键值“F”，可以看到该键值的二进制信息，将这些二进制信息全选，并拷贝到出来。

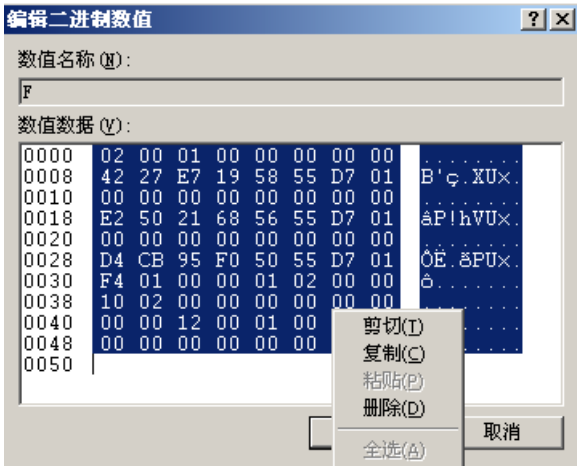

图 9 拷贝 Administrator 的二进制信息

将拷贝出来的信息全部覆盖到“000001F5”目录下的“F”键值中：

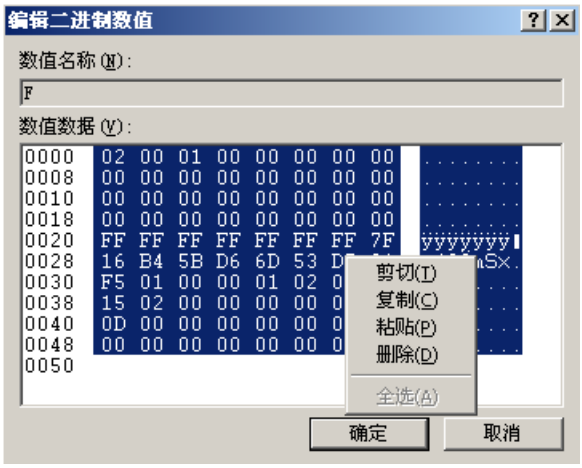

图 10 覆盖到“000001F5”目录下的“F”键值中

Guest 帐户已经具有管理员权限了。为了能够使 Guest 帐户在禁用的状态登录，下一步将 Guest 帐户信息导出注册表。选择 User 目录，然后选择菜单栏“注册表”下的菜单项“导出注册表文件”，将该键值保存为一个配置文件。

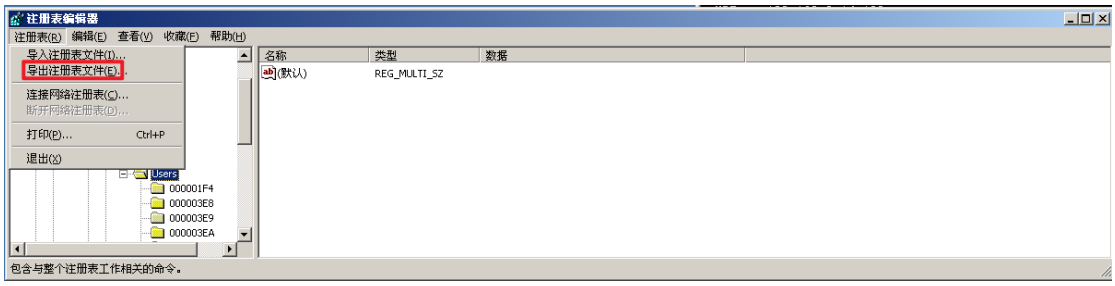

图 11 导出注册表文件

打开计算机管理对话框，并分别删除 Guest 和“00001F5”两个目录：

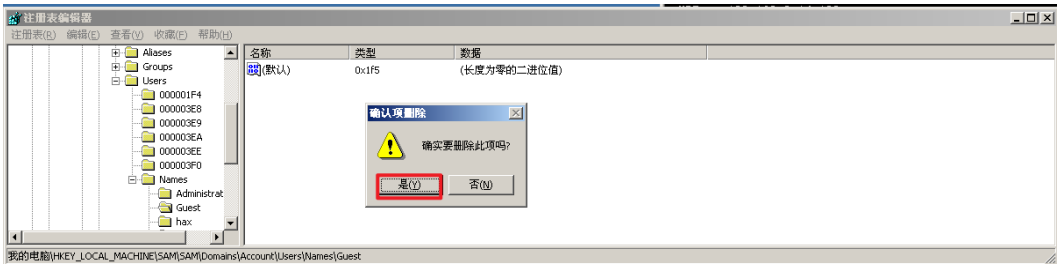

图 12 删除 Guest 和“00001F5”两个目录

然后再将刚才导出的信息文件，再导入注册表：

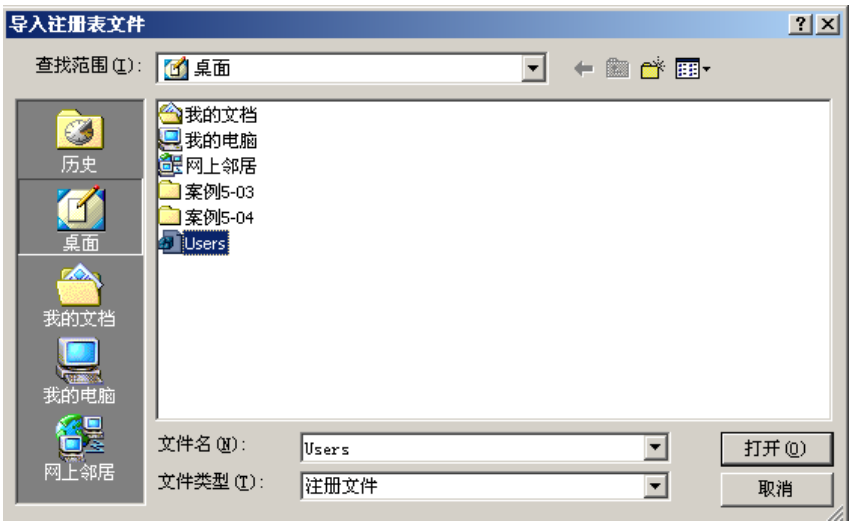

图 13 导入注册表

再查看一下计算机管理窗口中的 Guest 帐户：

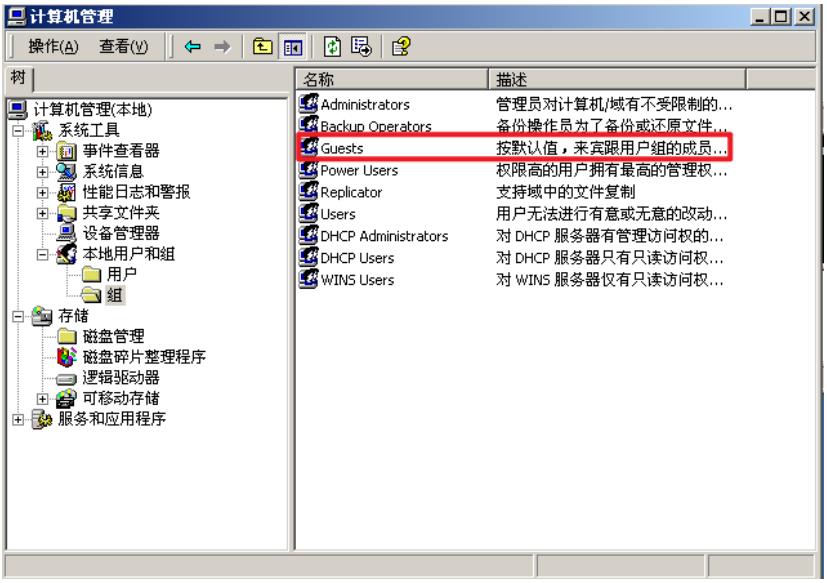

图 14 查看 Guest 帐户

注销退出系统，然后用用户名：“guest”，密码：“123”登录系统：

图 15 使用 Guest 账户登陆成功