Como fazer bug bounty em aplicativos Windows

BUG BOUNTY ALÉM DE WEB

whoami_

- Giuliano Sanfins - Campinas/SP
- Eng. de Computação - Analista de segurança SiDi
- Foco em análises de aplicações Windows
- OSED - Offsec Exploit Developer
- CVE-2025-36537, CVE-2025-9870, CVE-2025-9871, CVE-2025-9869

LinkedIn_

/giuliano-sanfins

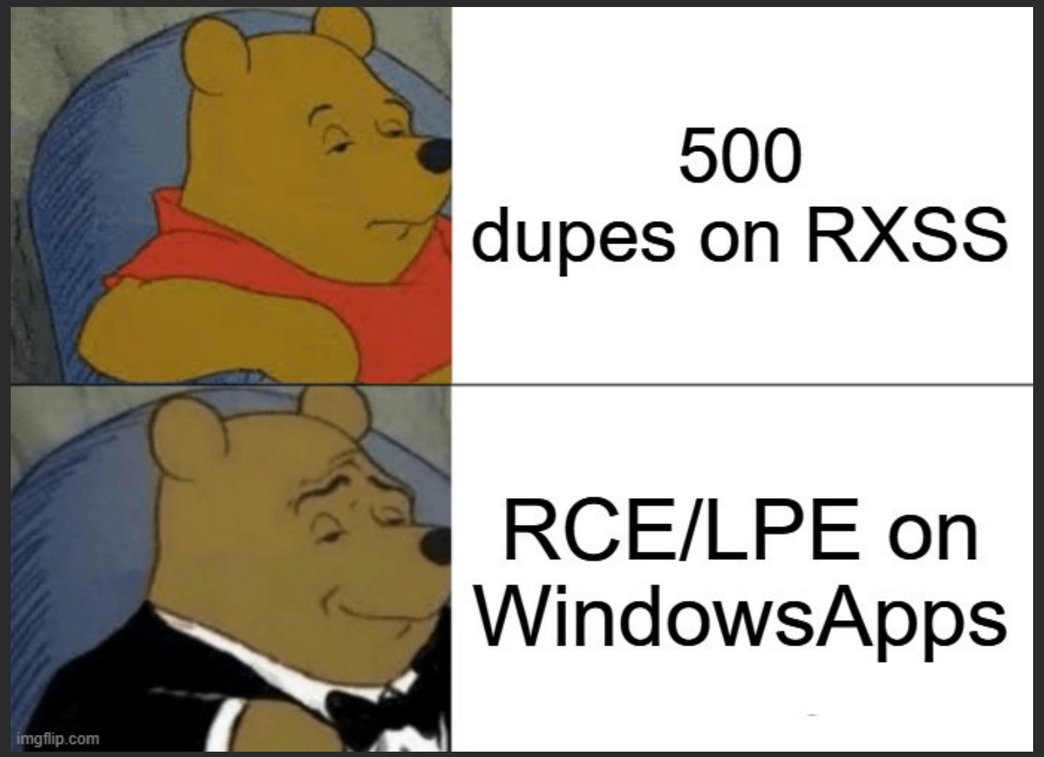
Twitter_

@0x_alibabas

Por que analisar apps Windows

Fugindo da saturação Web

- Web: Você compete contra milhares de hunters, bots e scanners que acham falhas em minutos.
- Windows: A barreira de entrada técnica e o medo do desconhecido afasta o pessoal.



Web ≠ Windows

- Escopo: Em web você ataca a infraestrutura e dados sensíveis da empresa, em Windows você ataca o software.

- Recompensa: Não parece alarmante? Só um RCE? Recompensa menor.

Alguns programas famosos

Microsoft

Programa de Bounty	Recompensa Máxima (USD)
Microsoft Windows Insider Preview	Até $100,000
Microsoft Hyper-V	Até $250,000
Microsoft Applications and On-Premises Servers	Até $30,000
Microsoft Edge (Chromium-based)	Até $30,000
Windows Defender Application Guard	Até $30,000
Microsoft 365 Insider	Até $15,000
Microsoft .NET	Até $15,000
Microsoft Defender	Até $20,000

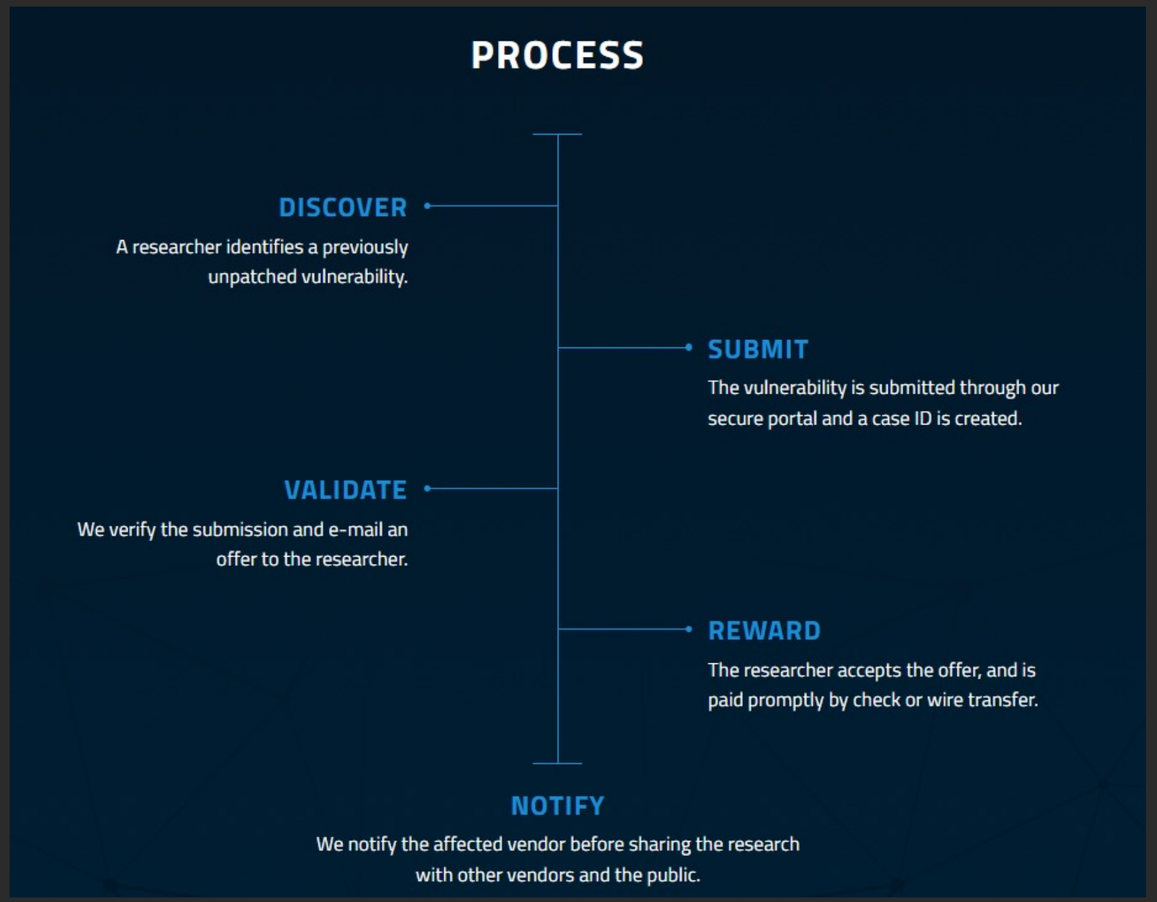
NVIDIA

Malwarebytes

zoom

Achou em um binário sem BB?

ZDI/Pwn2own



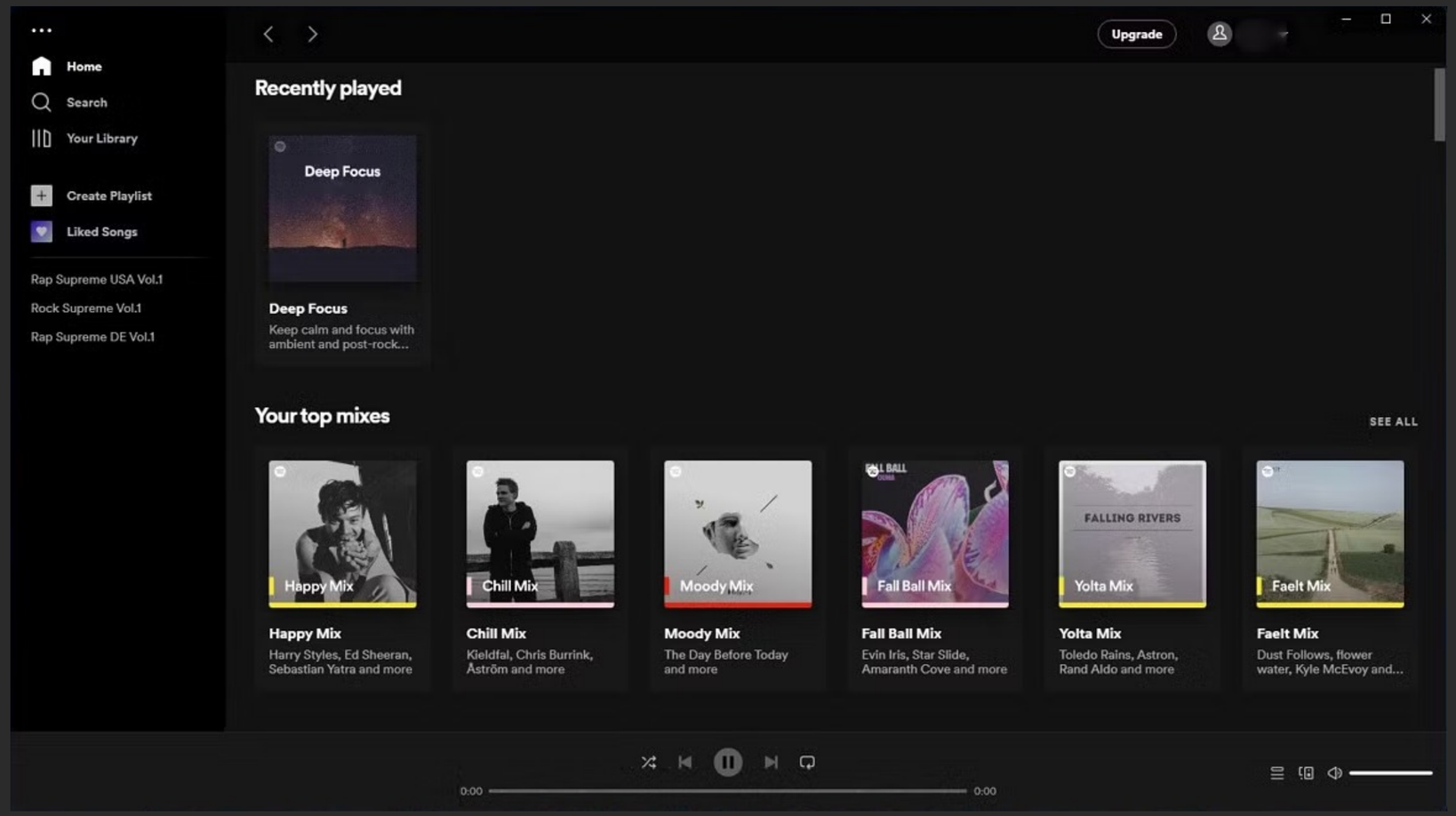
Histórico

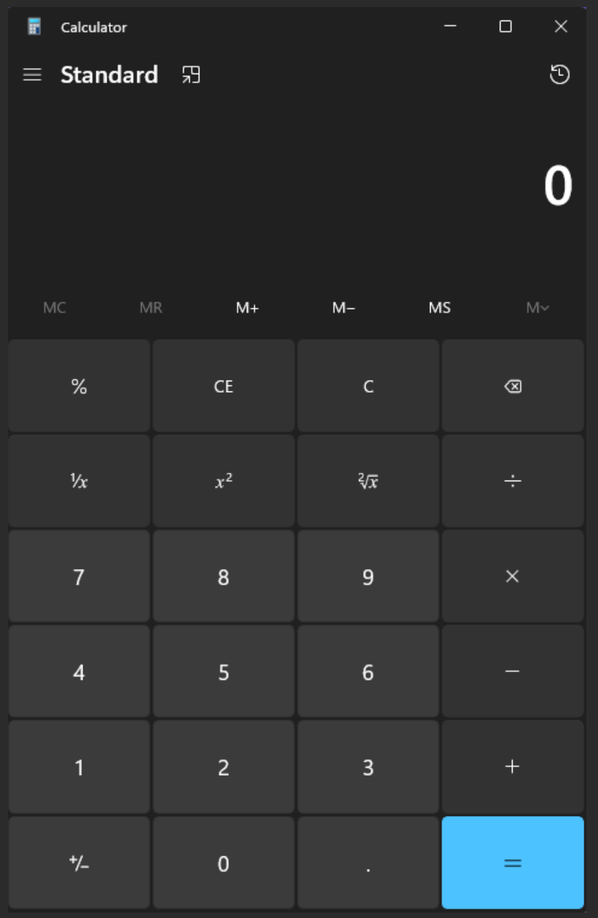
Histórico


Windows 3.11
Windows 98
Windows XP
Windows 7
Windows 8
Windows 11

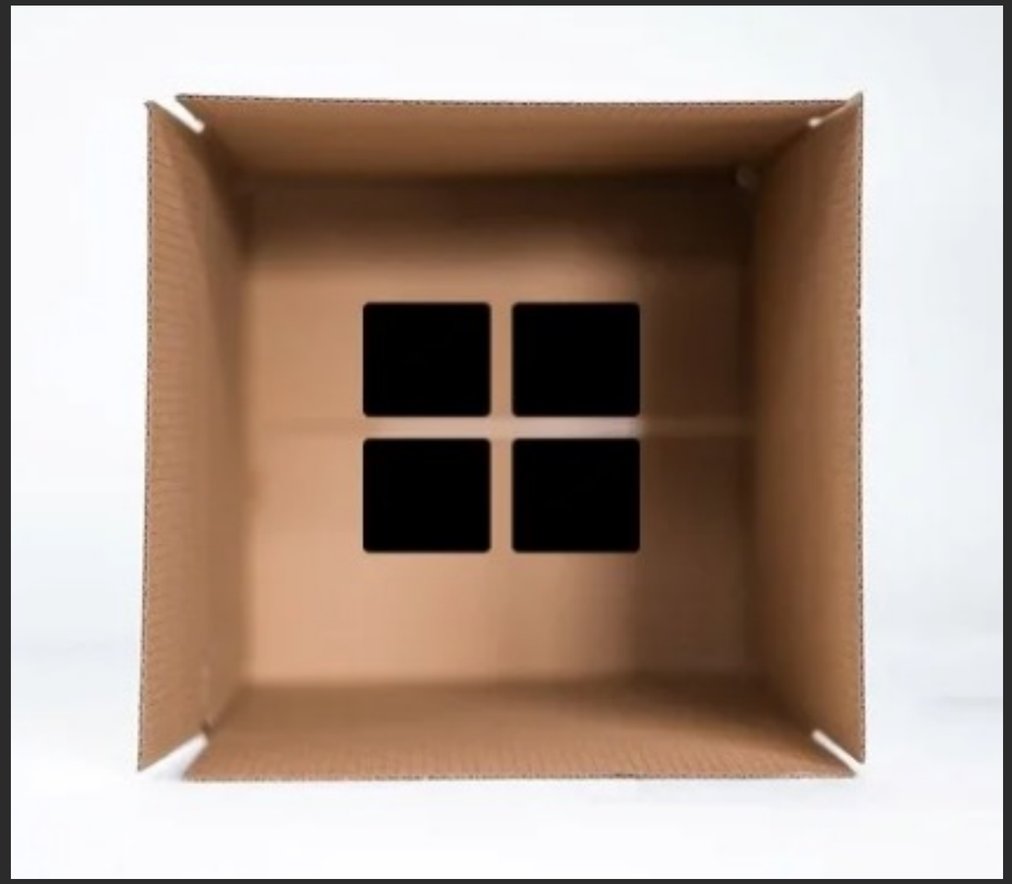
UWP – Universal Windows Platform

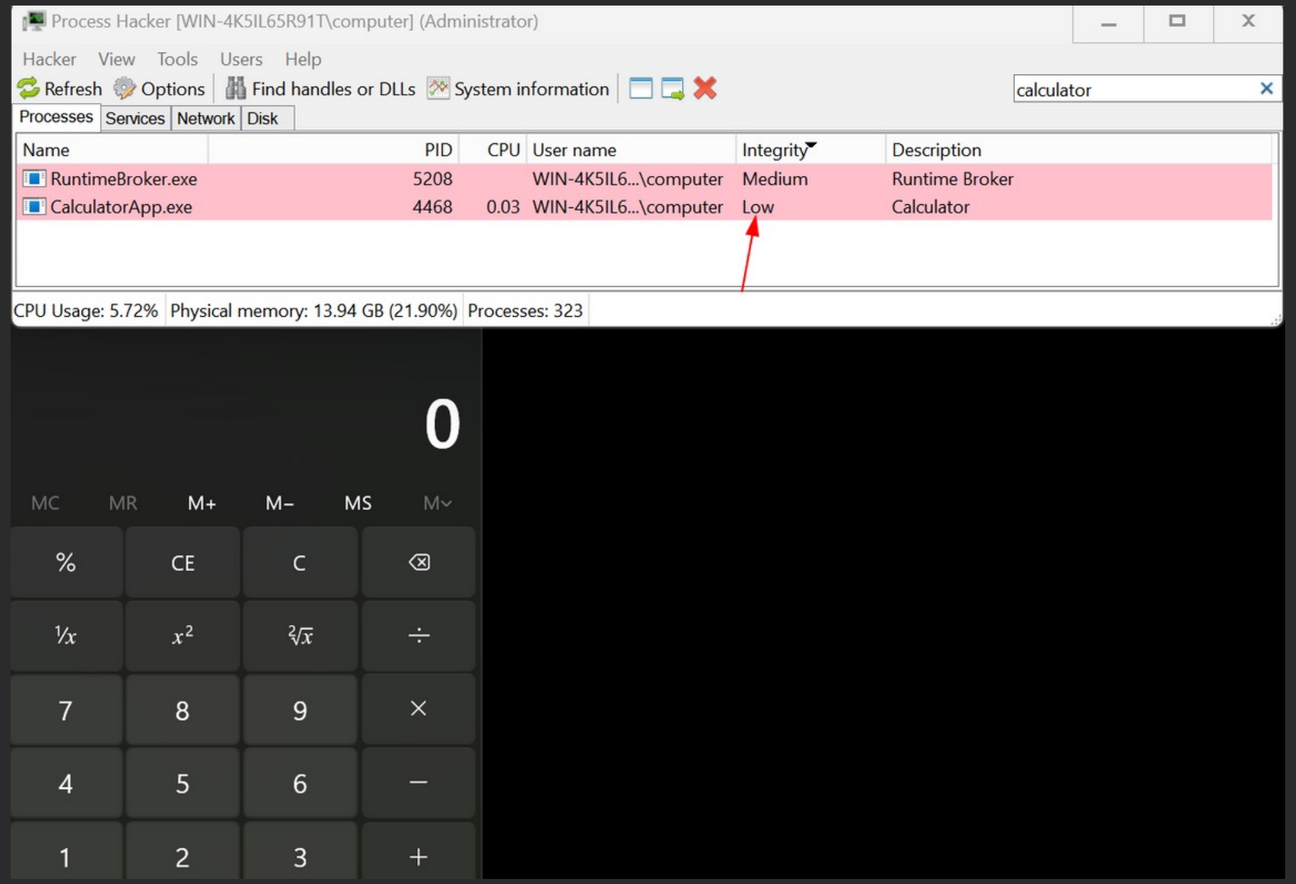
UWP apps


Upgrade
Home
Search
Your Library
Create Playlist
Liked Songs
Rap Supreme USA Vol.1
Rock Supreme Vol.1
Rap Supreme DE Vol.1
Recently played
Deep Focus
Deep Focus
Keep calm and focus with ambient and post-rock...
Your top mixes
SEE ALL
Happy Mix
Happy Mix
Harry Styles, Ed Sheeran, Sebastian Yatra and more
Chill Mix
Chill Mix
Kieldfal, Chris Burrink, Åström and more
Moody Mix
Moody Mix
The Day Before Today and more
Fall Ball Mix
Fall Ball Mix
Evin Iris, Star Slide, Amaranth Cove and more
FALLING RIVERS
Yolta Mix
Yolta Mix
Toledo Rains, Astron, Rand Aldo and more
Faelt Mix
Faelt Mix
Dust Follows, flower water, Kyle McEvoy and...
0:00
0:00

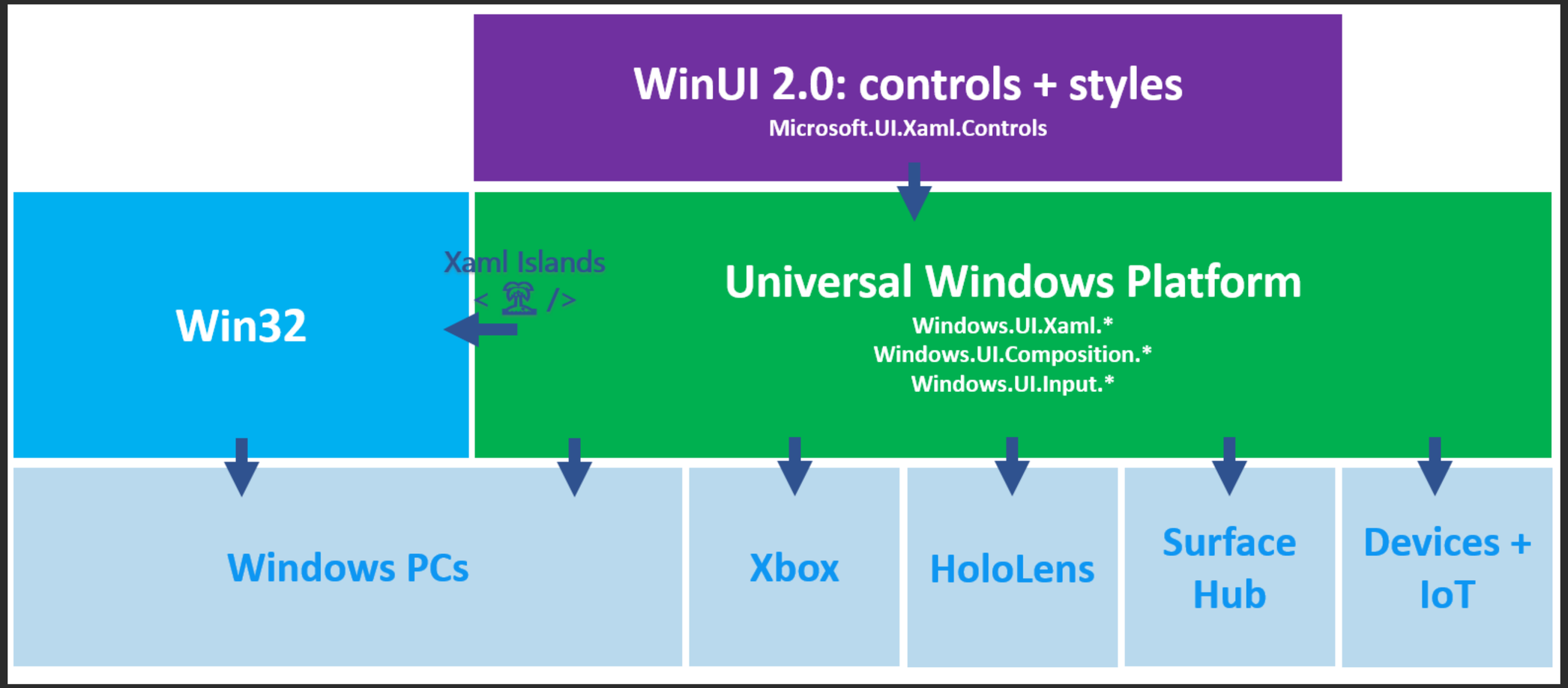

Calculator
Standard
0
MC
MR
M+
M−
MS
M
%
CE
C
1/x
x²
∛x
÷
7
8
9
×
4
5
6
−
1
2
3
+
+/-
0
.
=

UWP Sandbox

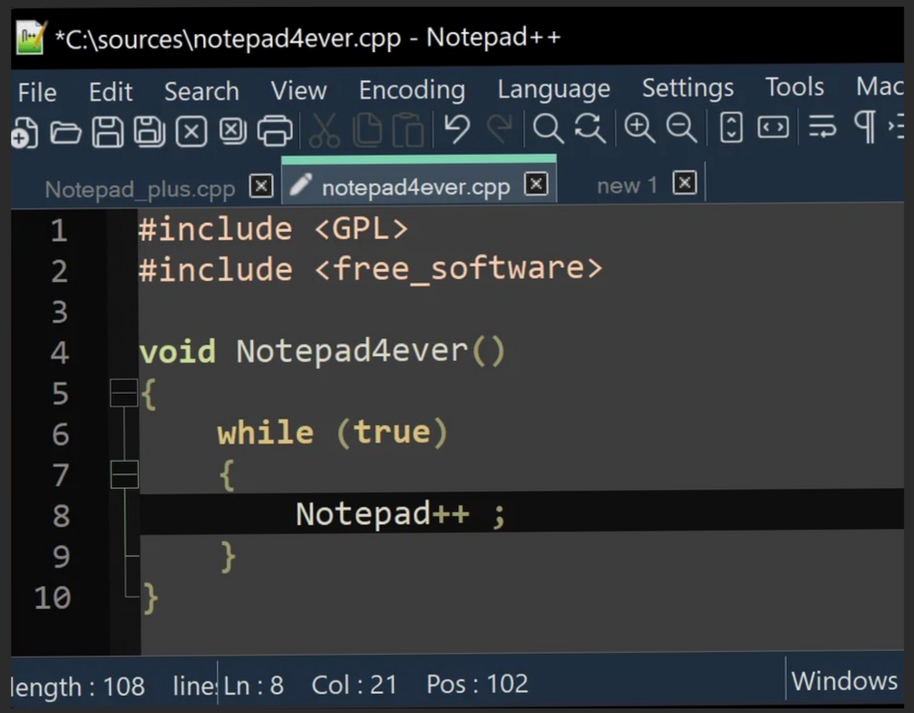



Process Hacker [WIN-4K5IL65R91T\computer] (Administrator)
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
calculator
Processes Services Network Disk
Name PID CPU User name Integrity Description
RuntimeBroker.exe 5208 WIN-4K5IL6...\computer Medium Runtime Broker
CalculatorApp.exe 4468 0.03 WIN-4K5IL6...\computer Low Calculator
CPU Usage: 5.72% Physical memory: 13.94 GB (21.90%) Processes: 323
0
MC MR M+ M− MS M
% CE C
1/x x² ∛x ÷
7 8 9 ×
4 5 6 −
1 2 3 +

Win32


WinUI 2.0: controls + styles
Microsoft.UI.Xaml.Controls
Win32
Xaml Islands
< />
Universal Windows Platform
Windows.UI.Xaml.*
Windows.UI.Composition.*
Windows.UI.Input.*
Windows PCs
Xbox
HoloLens
Surface Hub
Devices + IoT

Win32 apps

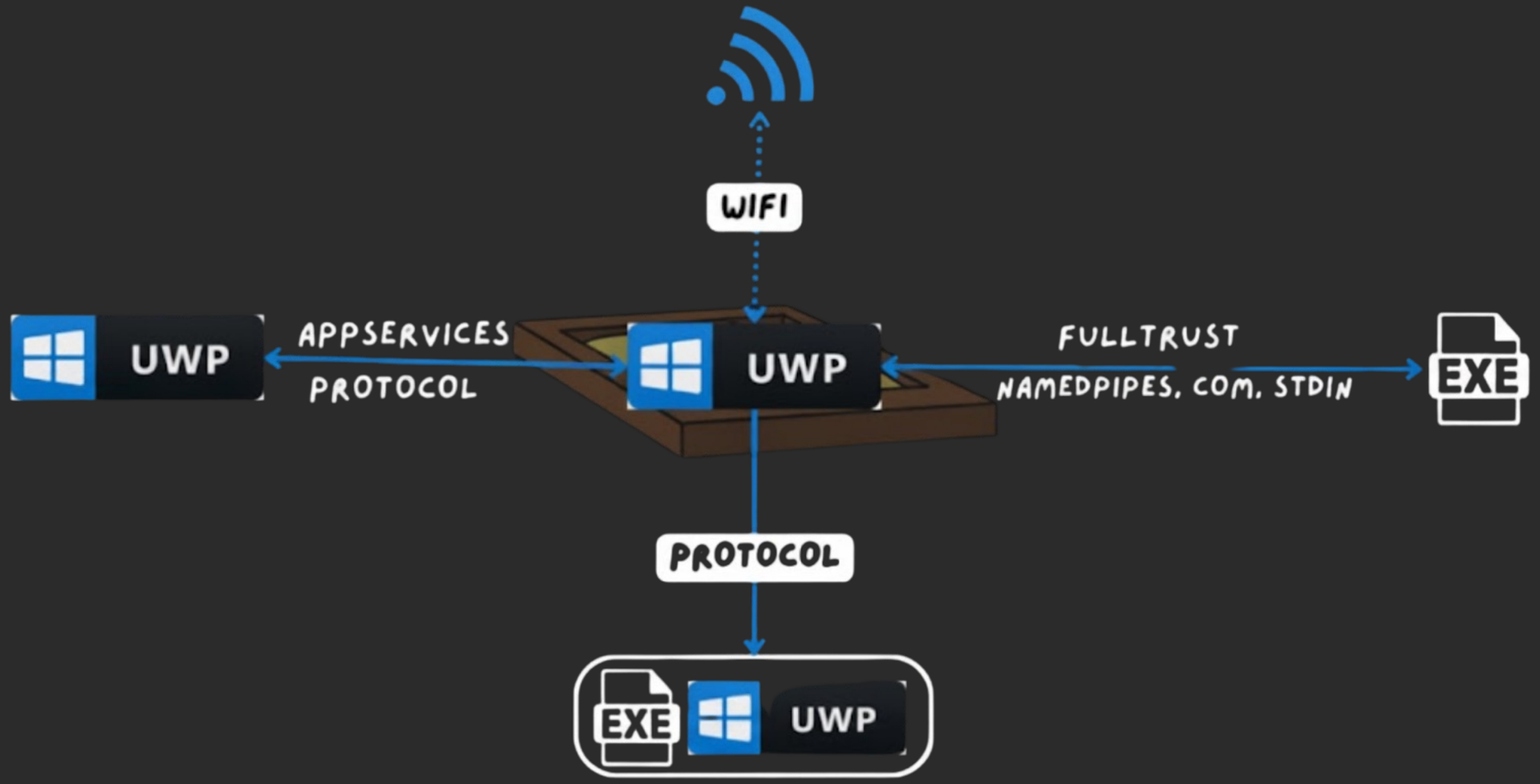

*C:\sources\notepad4ever.cpp - Notepad++
File Edit Search View Encoding Language Settings Tools Mac
Notepad_plus.cpp
notepad4ever.cpp
new 1
#include <GPL>
#include <free_software>
void Notepad4ever()
{
while (true)
{
Notepad++ ;
}
}
length : 108 line: Ln : 8 Col : 21 Pos : 102 Windows


Office

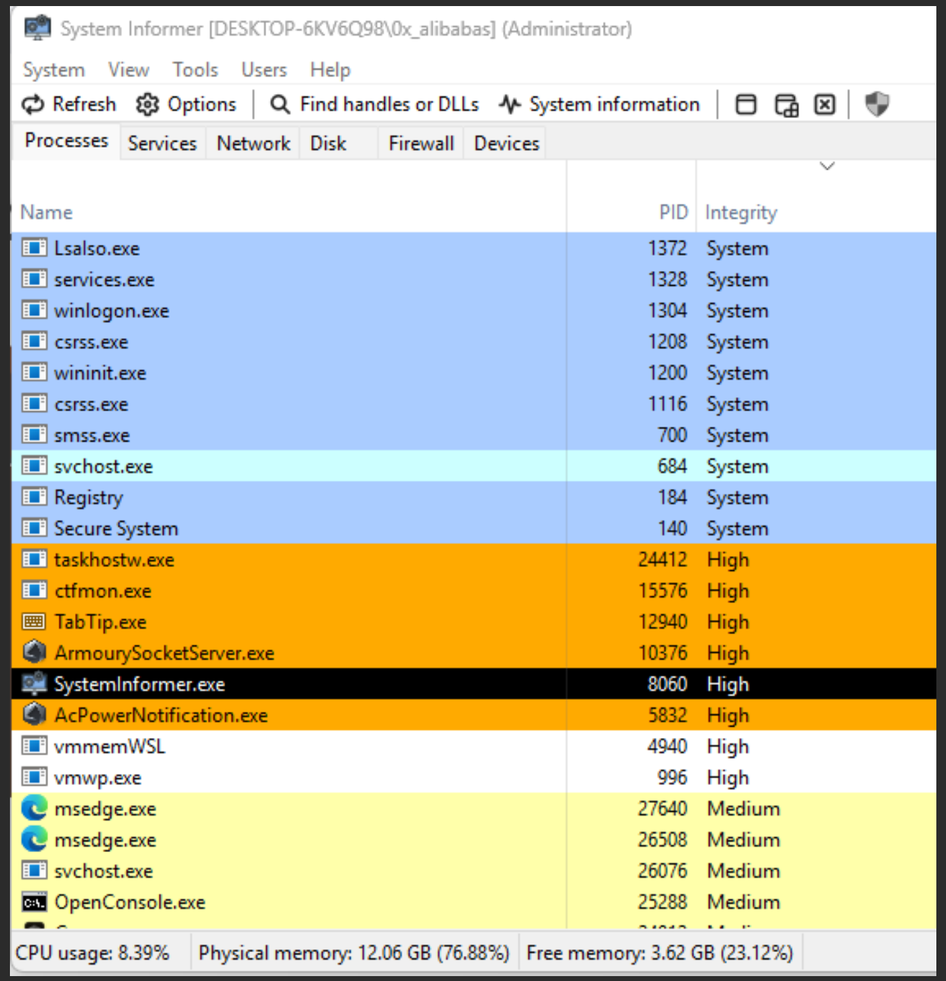
Win32

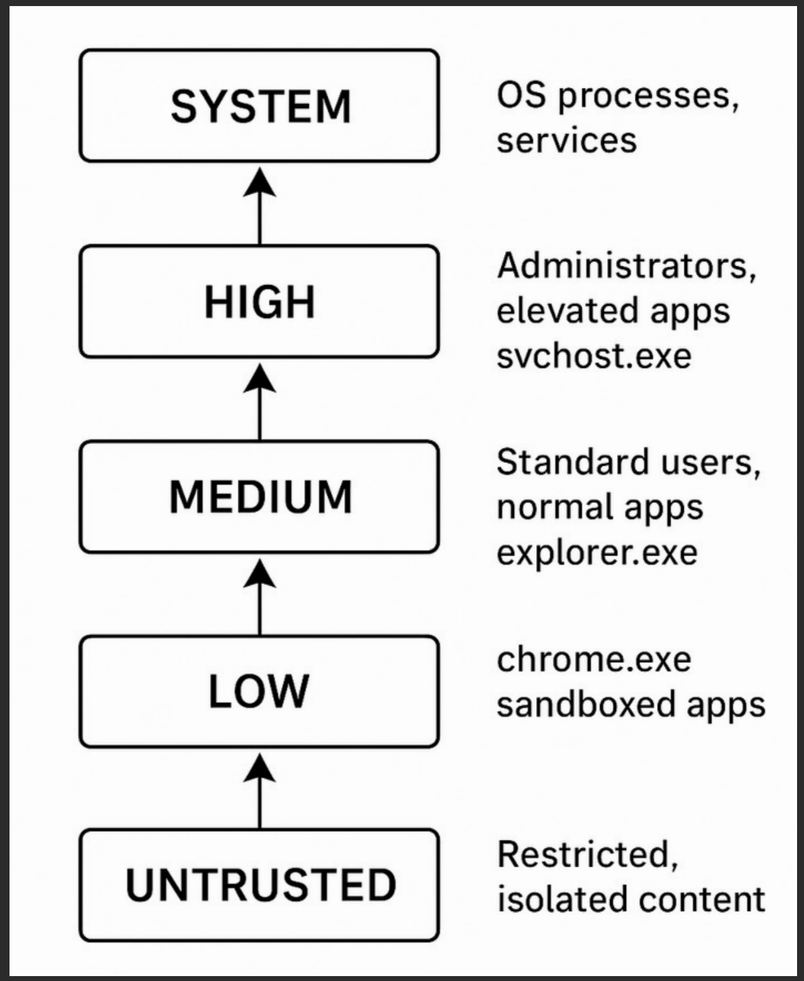
Entrypoints e Integrity Levels

Entrypoints

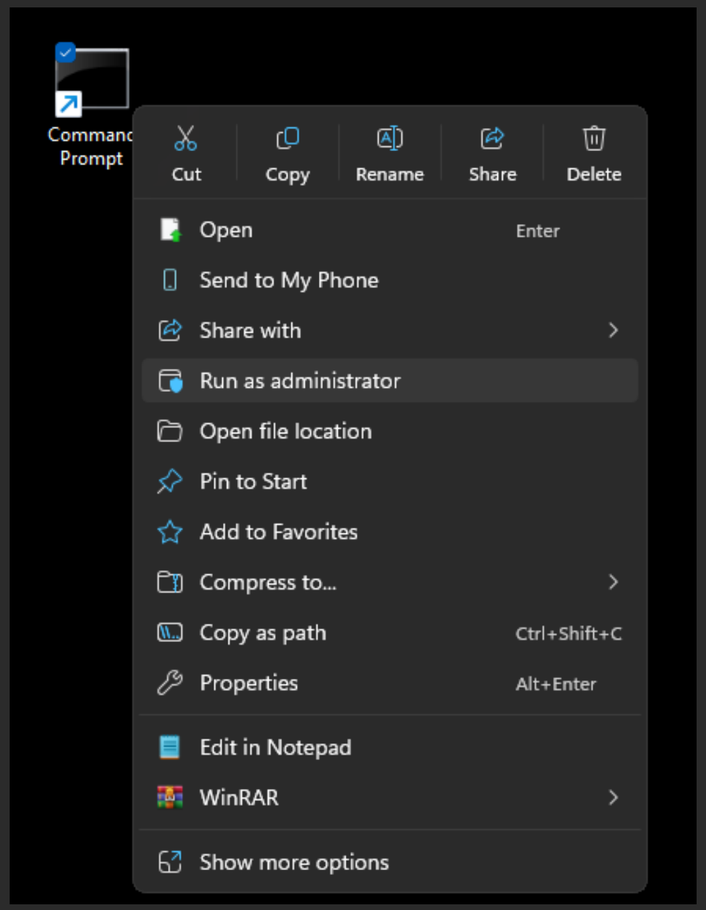


Integrity level





Name	PID	Integrity	User ...	Description	P
NordUpdateService.exe	6744	System	...\SYST	NordSec Update ...	
nordvpn-service.exe	5888	System	...\SYST	nordvpn-service	
NordVPN.exe	2404	Medium	...\0x_al	NordVPN	



High IL

Integrity level

Low Medium High SYSTEM

Inter-Process Communication

IPC Mechanism	Descrição / Caso de Uso
WinRT / UWP App Services	Comunicação de aplicativo moderno (UWP para UWP/Win32)
COM / DCOM	Component Object Model (objetos locais e remotos)
RPC (Remote Procedure Call)	Executar código em máquinas/processos remotos
Named Pipes	Fluxo de dados confiável, bidirecional e ordenado
Windows Sockets (Winsock)	Rede TCP/UDP padrão
Shared Memory (File Mapping)	Método mais rápido para compartilhamento de dados
Window Messages (HWND)	Comunicação de thread de UI (SendMessage)
Mailslots	Comunicação de transmissão unidirecional
Events / Mutexes / Semaphores	Sincronização e sinalização

Falhas Comuns

Falhas comuns

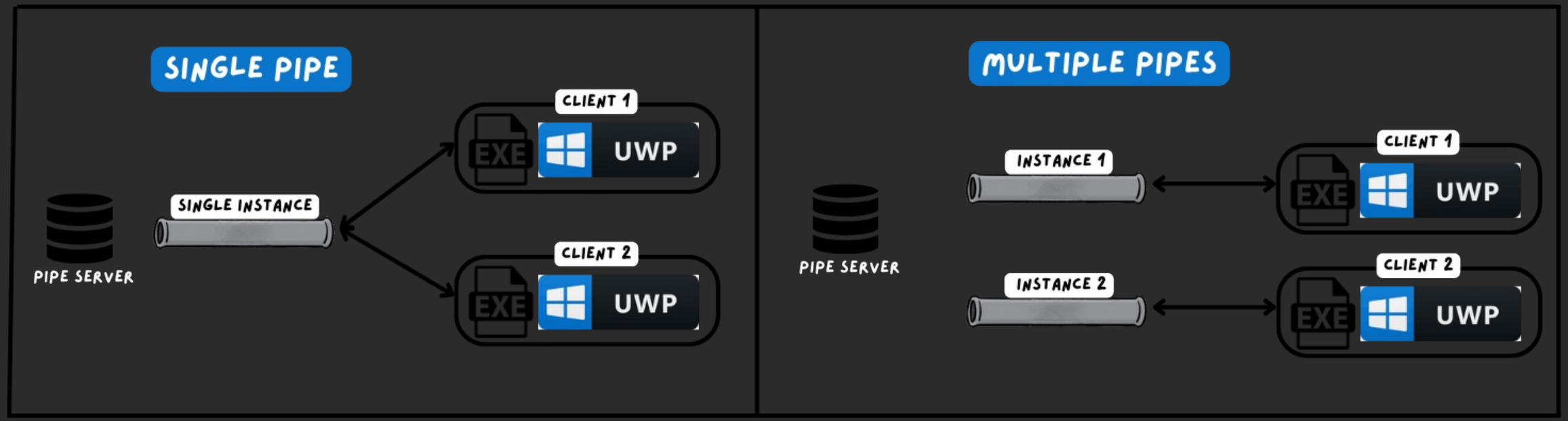
- Aplicações com alto privilégio fazendo operações de arquivo em caminhos controláveis por usuários sem privilégio - também válido para registro (HKCU vs HKLM)

- Má configuração de IPCs: NamedPipes sem permissões corretas, COM exportados, checagem de assinatura/hash mal feitos

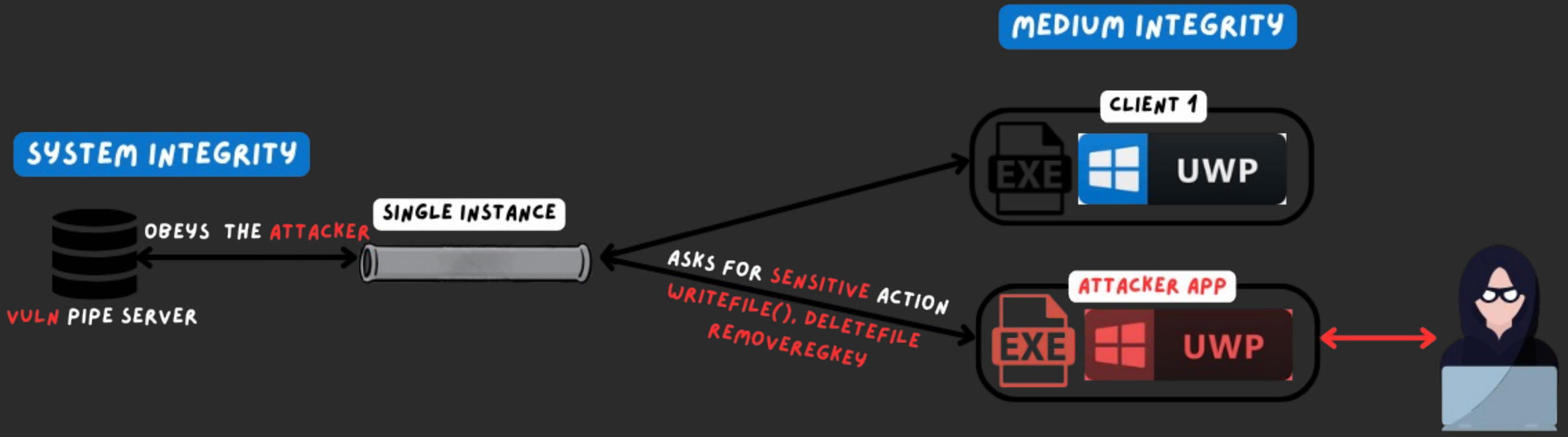
NamedPipes

NamedPipes

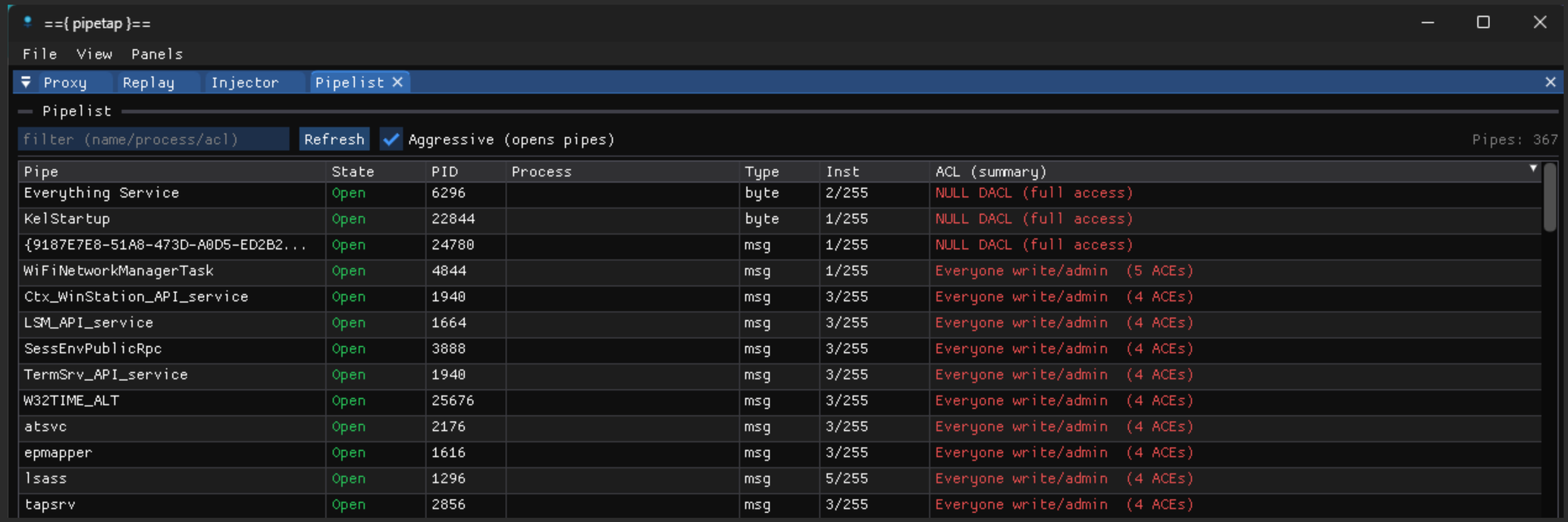
- São como arquivos no filesystem
- Seguem o padrão: \\.\pipe\PipeName (. sendo PC local)
- Desenvolvedor precisa configurar a permissão corretamente



NamedPipes

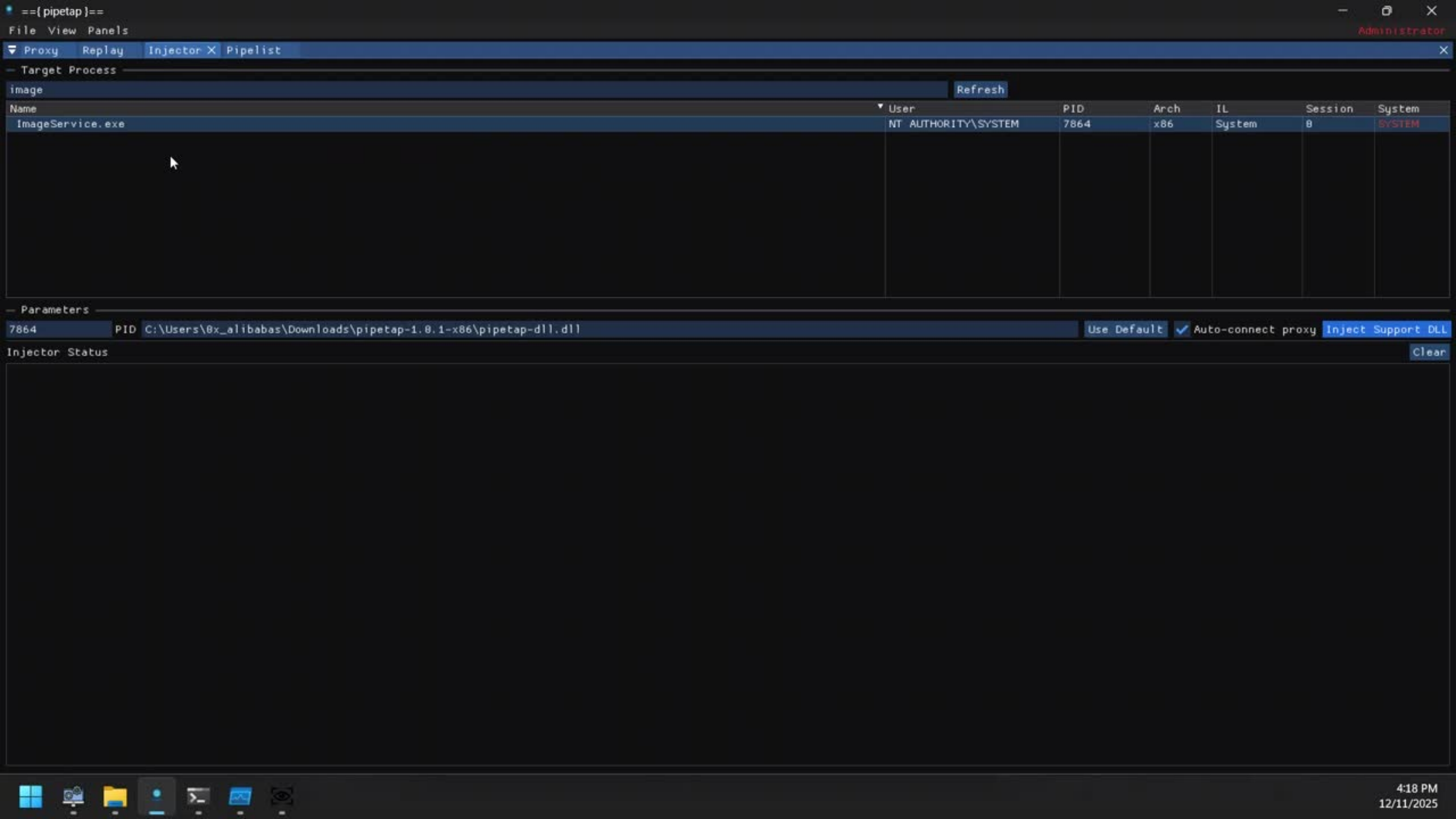

MEDIUM INTEGRITY
CLIENT 1
EXE
UWP
SYSTEM INTEGRITY
SINGLE INSTANCE
OBEYS THE ATTACKER
VULN PIPE SERVER
ASKS FOR SENSITIVE ACTION
WRITEFILE(), DELETEFILE
REMOVEREGKEY
ATTACKER APP
EXE
UWP

Permissões NamedPipes



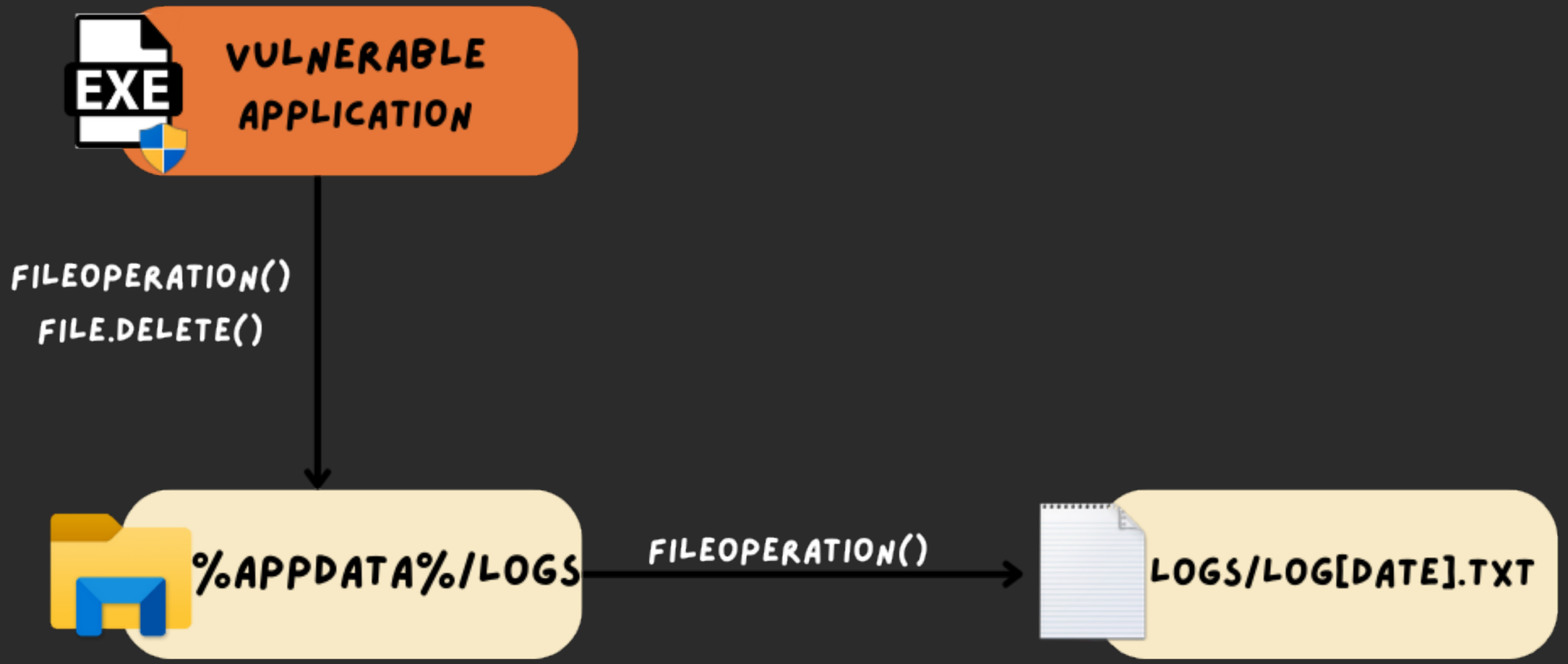

```
Accesschk v6.15 - Reports effective permissions for securable objects
Copyright (C) 2006-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

\\.\Pipe\eventlog
  RW Everyone
  RW NT SERVICE\EventLog
  R  OWNER RIGHTS
  R  NT AUTHORITY\LOCAL SERVICE
```

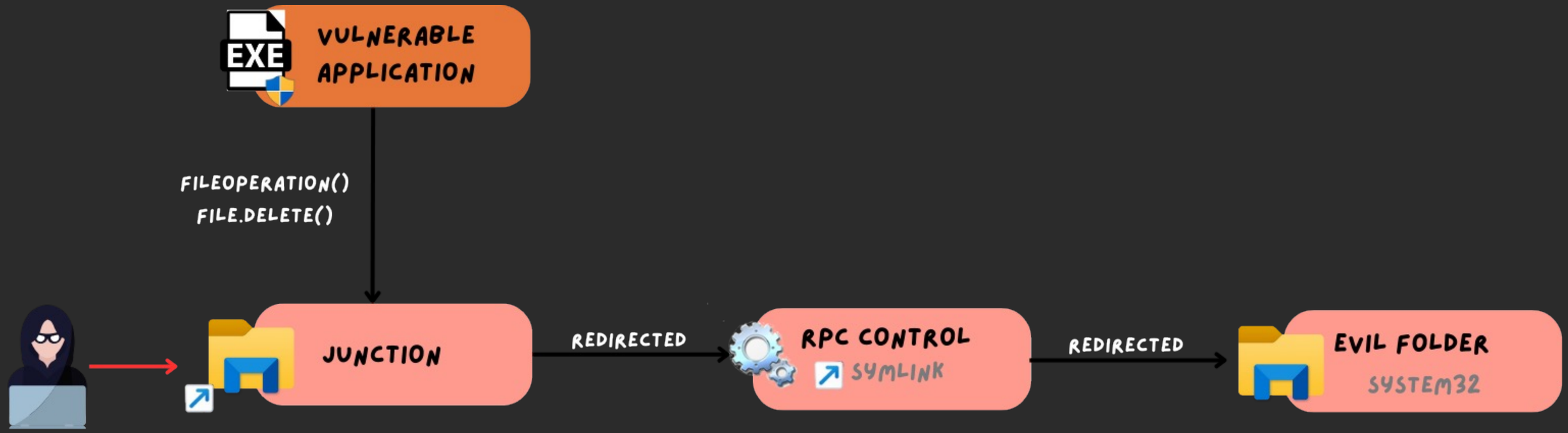

==[pipetap]==
File View Panels
Administrator
Proxy Replay Injector Pipelist
Target Process
image
Refresh
Name User PID Arch IL Session System
ImageService.exe NT AUTHORITY\SYSTEM 7864 x86 System 0 SYSTEM
Parameters
7864 PID
C:\Users\0x_alibabas\Downloads\pipetap-1.0.1-x86\pipetap-dll.dll
Use Default
Auto-connect proxy
Inject Support DLL
Injector Status
Clear
4:18 PM
12/11/2025

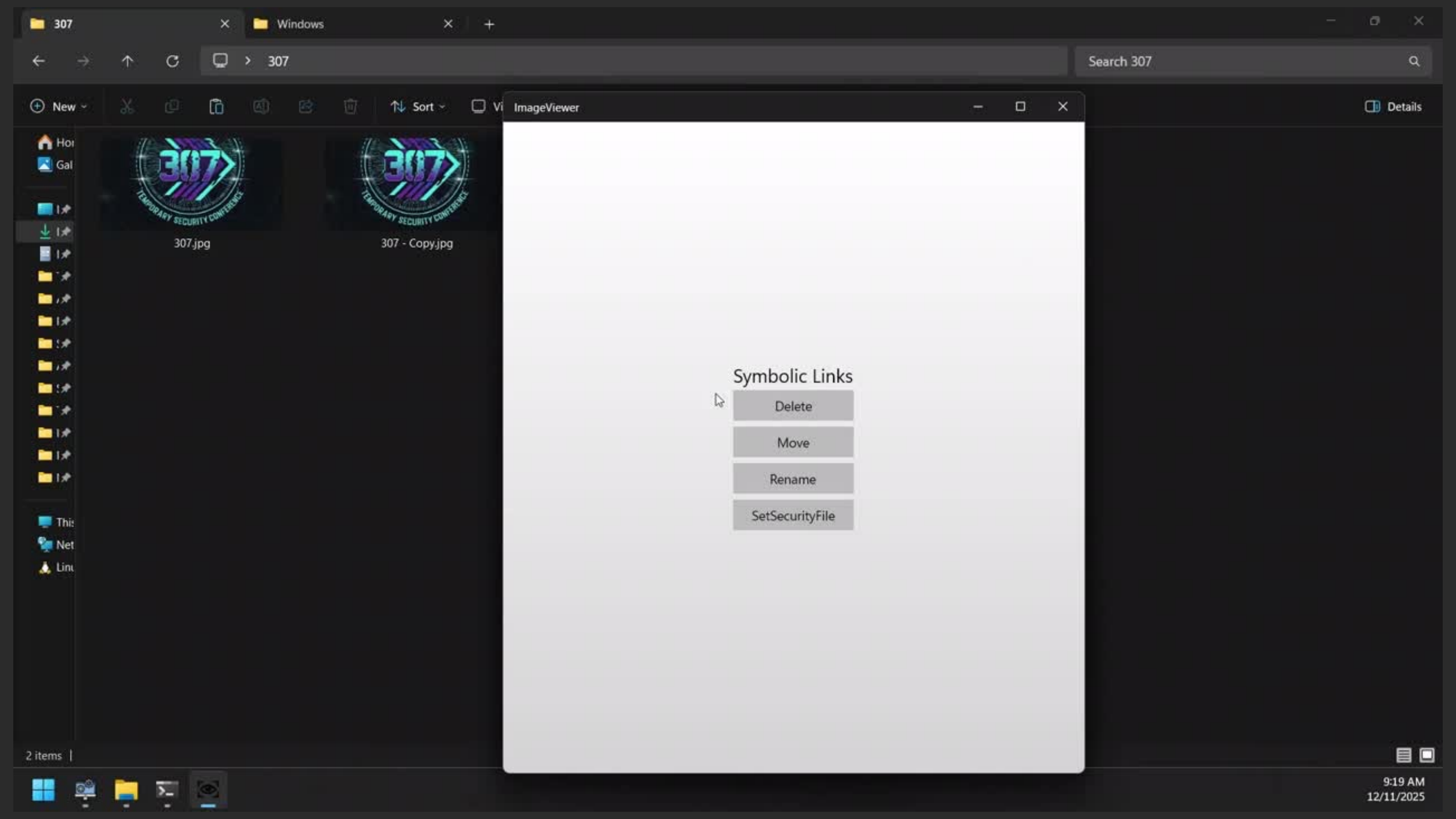
Symbolic Links

Symbolic Links



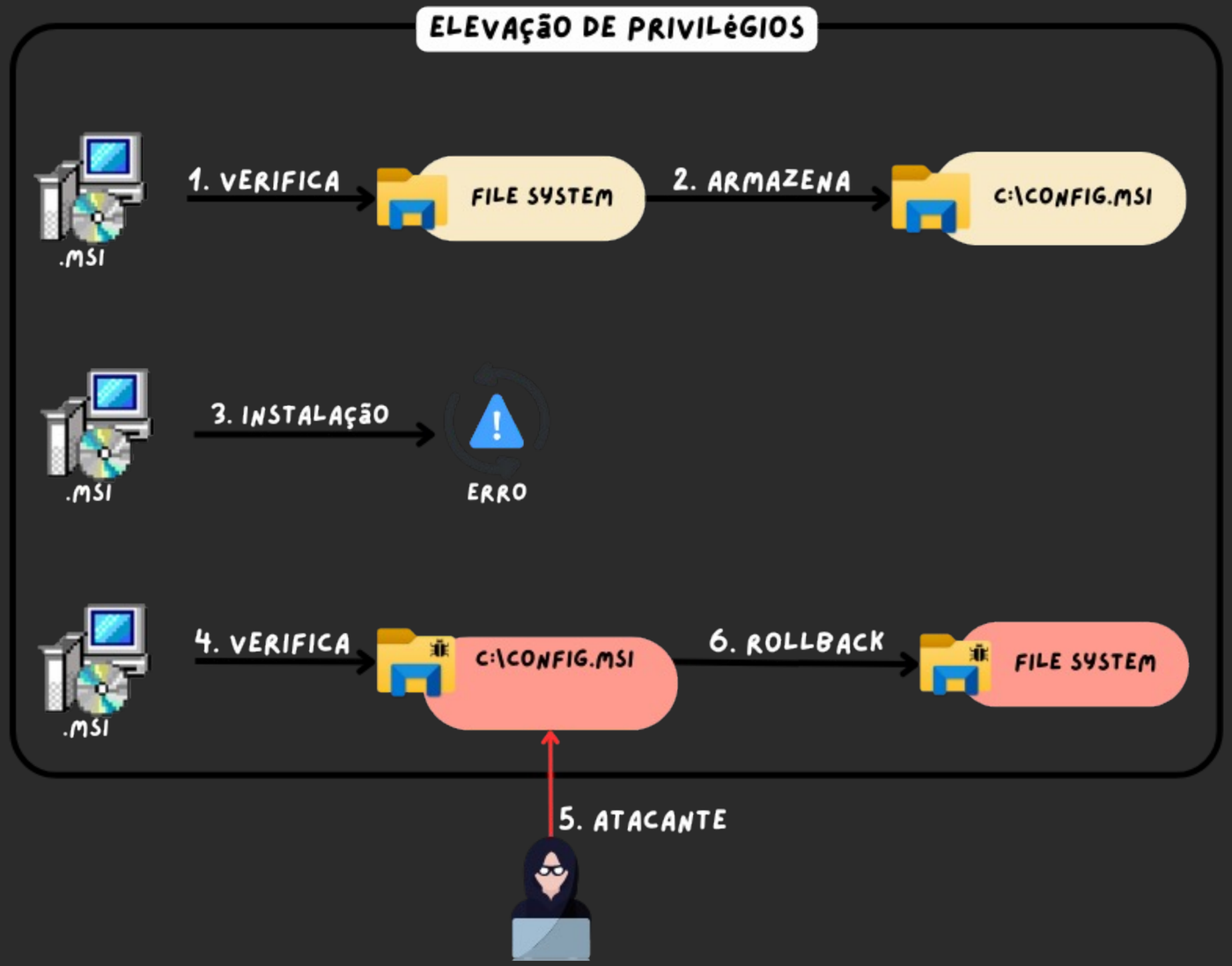
Symbolic Links




307
Windows
307
Search 307
New
Sort
Details
307.jpg
307 - Copy.jpg
ImageViewer
Symbolic Links
Delete
Move
Rename
SetSecurityFile
2 items
9:19 AM
12/11/2025

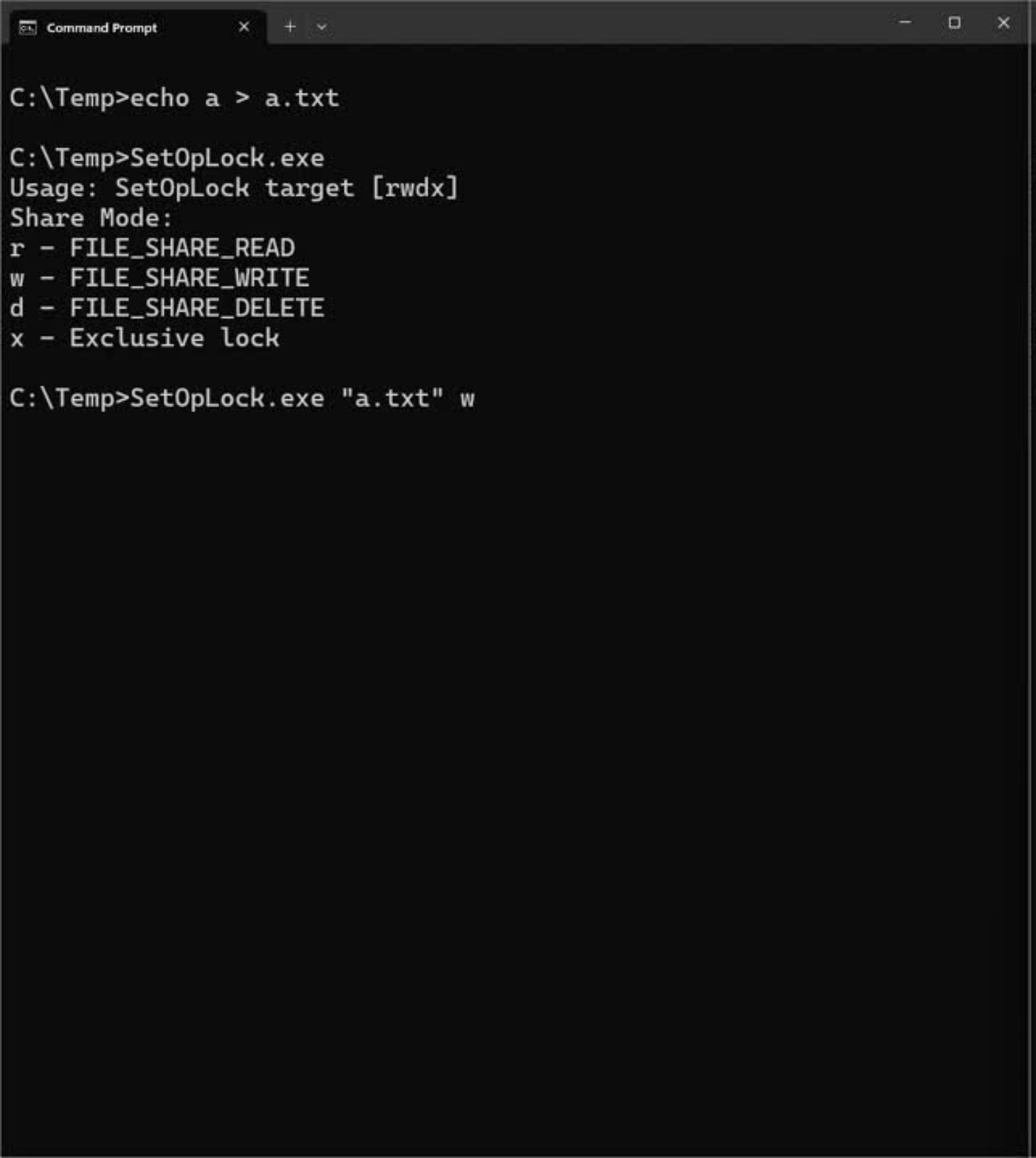
Deleção arbitrária

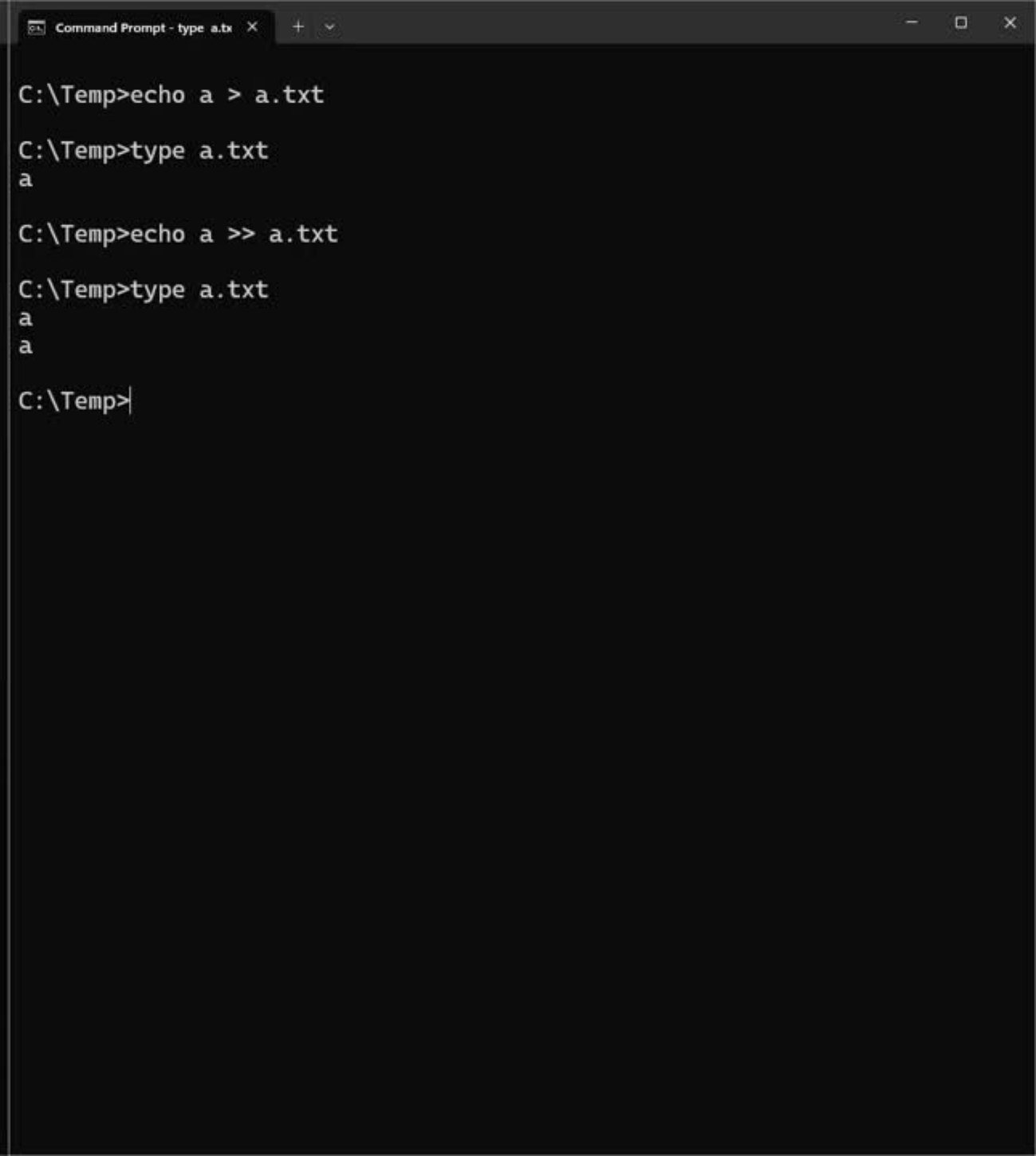
Deleção arbitrária



Impacto

Oplocks


Command Prompt
C:\Temp>echo a > a.txt
C:\Temp>SetOpLock.exe
Usage: SetOpLock target [rwdx]
Share Mode:
r - FILE_SHARE_READ
w - FILE_SHARE_WRITE
d - FILE_SHARE_DELETE
x - Exclusive lock
C:\Temp>SetOpLock.exe "a.txt" w


Command Prompt - type a.tx
C:\Temp>echo a > a.txt
C:\Temp>type a.txt
a
C:\Temp>echo a >> a.txt
C:\Temp>type a.txt
a
a
C:\Temp>

Demo


```
Microsoft Visual Studio Debu
[+] Config.msi directory created!
[+] File to export macro: C:\windows\temp\92075f2e-d674-4011-a9ea-62886b86538b\1.xml
[+] File C:\windows\temp\92075f2e-d674-4011-a9ea-62886b86538b\1.xml.tmp created!
[*] MSI file: C:\windows\temp\MSIA03E.tmp
[+] Rollback script overwritten!
Error: 4390
error :2

C:\Users\computer\Desktop\RazerEoP2\RazerEoP2\x64\Release\RazerEoP.exe (process 30640) exited with code 0.
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the conso
le when debugging stops.
Press any key to close this window . . .
```

```
Administrator: C:\windows\system32\cmd.exe
Microsoft Windows [Version 10.0.22621.3085]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>whoami
nt authority\system

C:\Windows\System32>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeAssignPrimaryTokenPrivilege Replace a process level token        Disabled
SeLockMemoryPrivilege         Lock pages in memory                 Enabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process   Disabled
SeTcbPrivilege                Act as part of the operating system  Enabled
SeSecurityPrivilege           Manage auditing and security log     Enabled
SeTakeOwnershipPrivilege      Take ownership of files or other objects Disabled
SeLoadDriverPrivilege         Load and unload device drivers       Disabled
SeProfileSingleProcessPrivilege Profile single process             Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority       Enabled
SeCreatePagefilePrivilege     Create a pagefile                    Enabled
SeCreatePermanentPrivilege    Create permanent shared objects      Enabled
SeBackupPrivilege             Back up files and directories        Disabled
SeRestorePrivilege            Restore files and directories        Disabled
SeShutdownPrivilege           Shut down the system                 Disabled
SeAuditPrivilege              Generate security audits             Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                Enabled
SeCreateSymbolicLinkPrivilege Create symbolic links                Enabled

C:\Windows\System32>
```

Casos reais

Caso 1 - Redacted

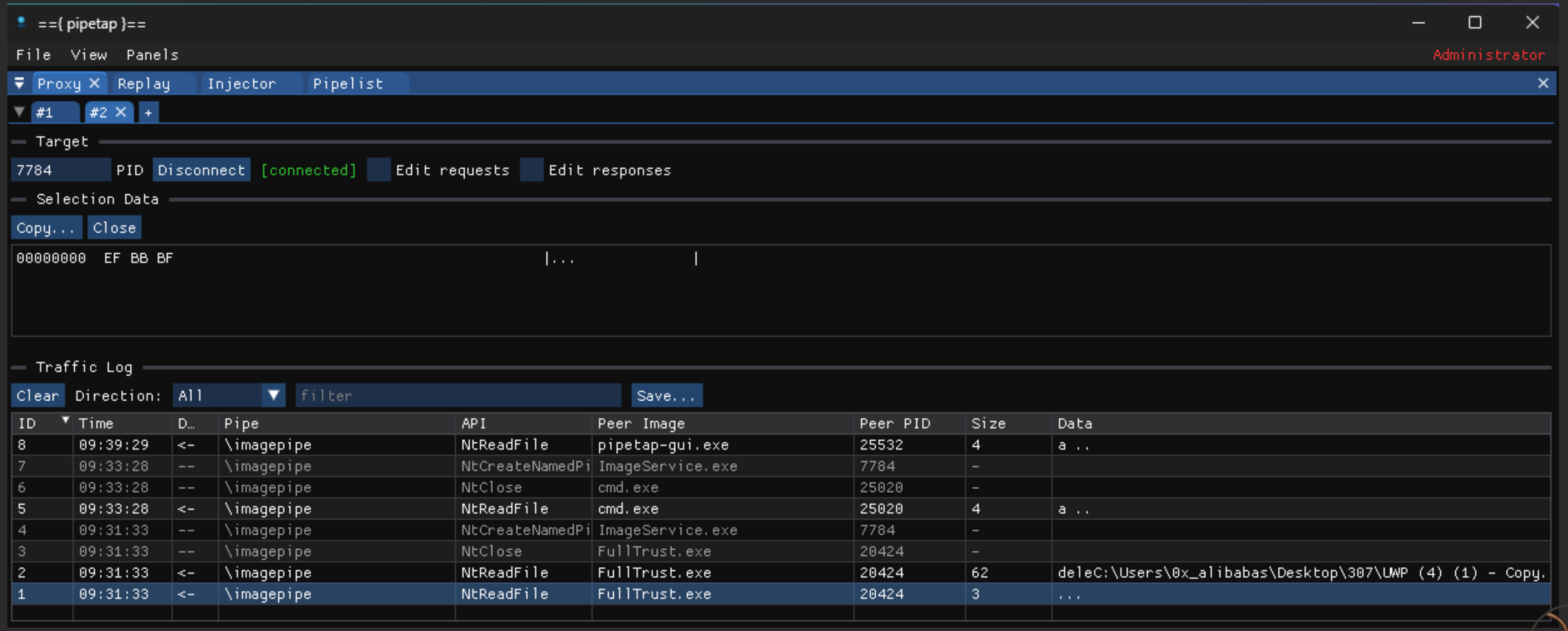
Caso 2 - Redacted

Caso 3 - Redacted

Tools

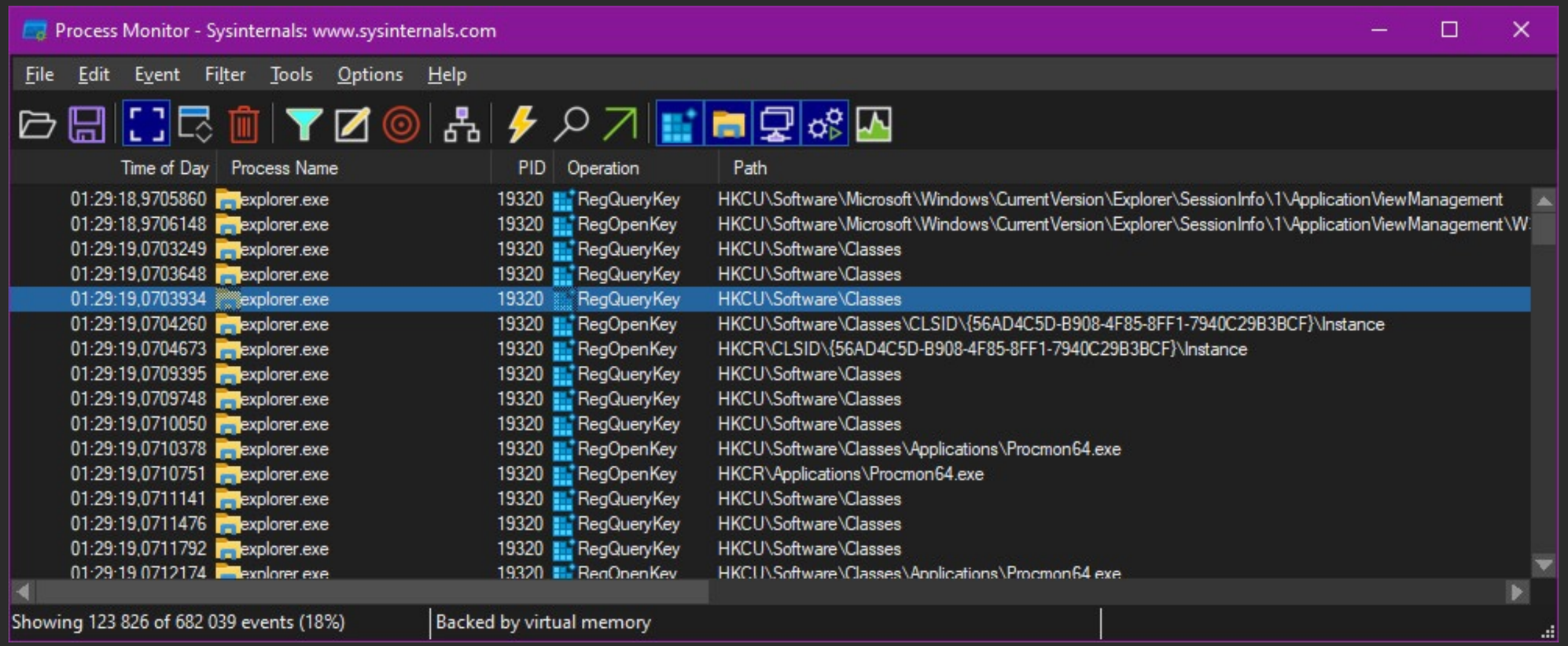
PipeTap

https://github.com/sensepost/pipetap



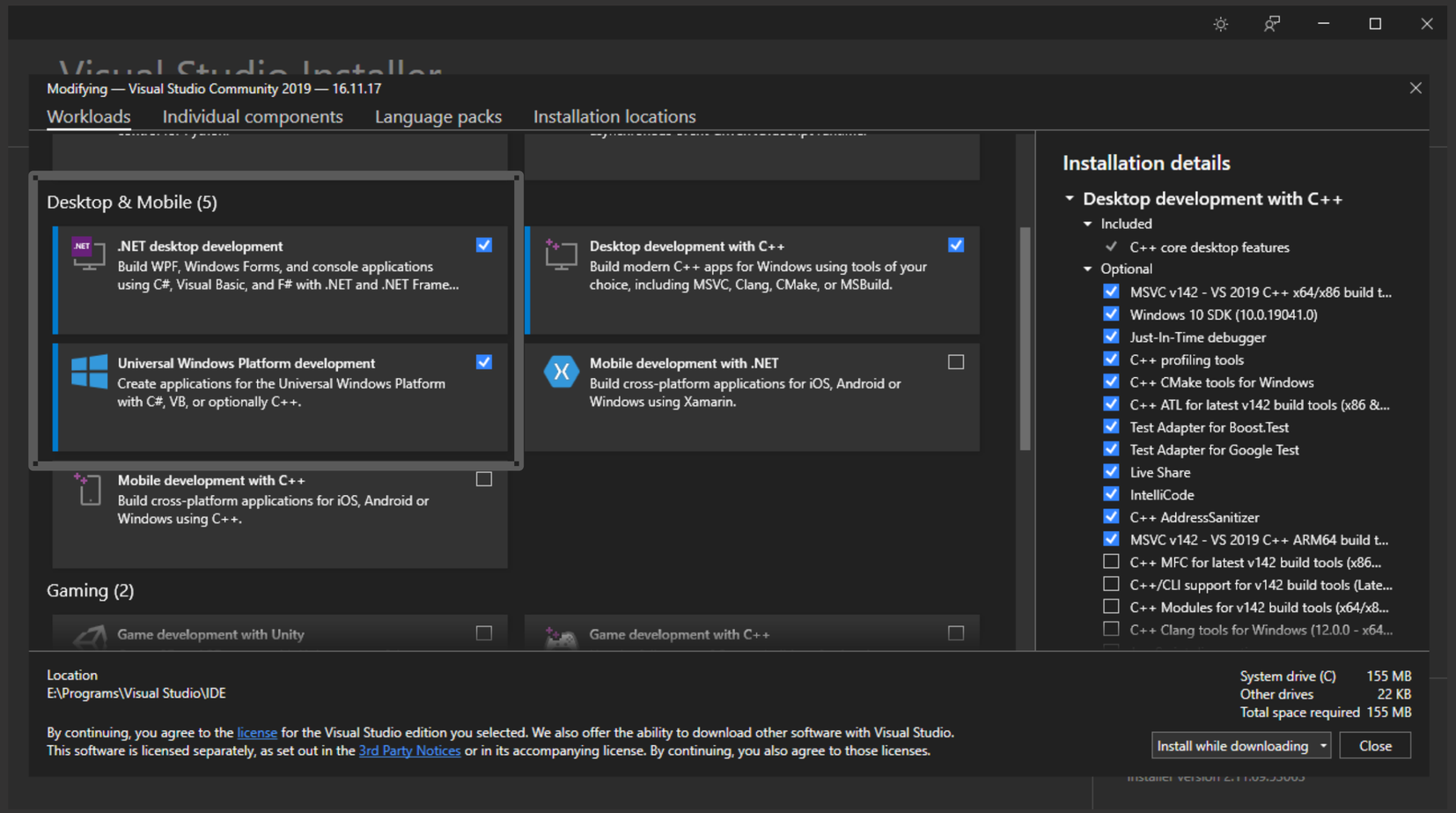
Process Monitor

https://learn.microsoft.com/en-us/sysinternals/downloads/procmon



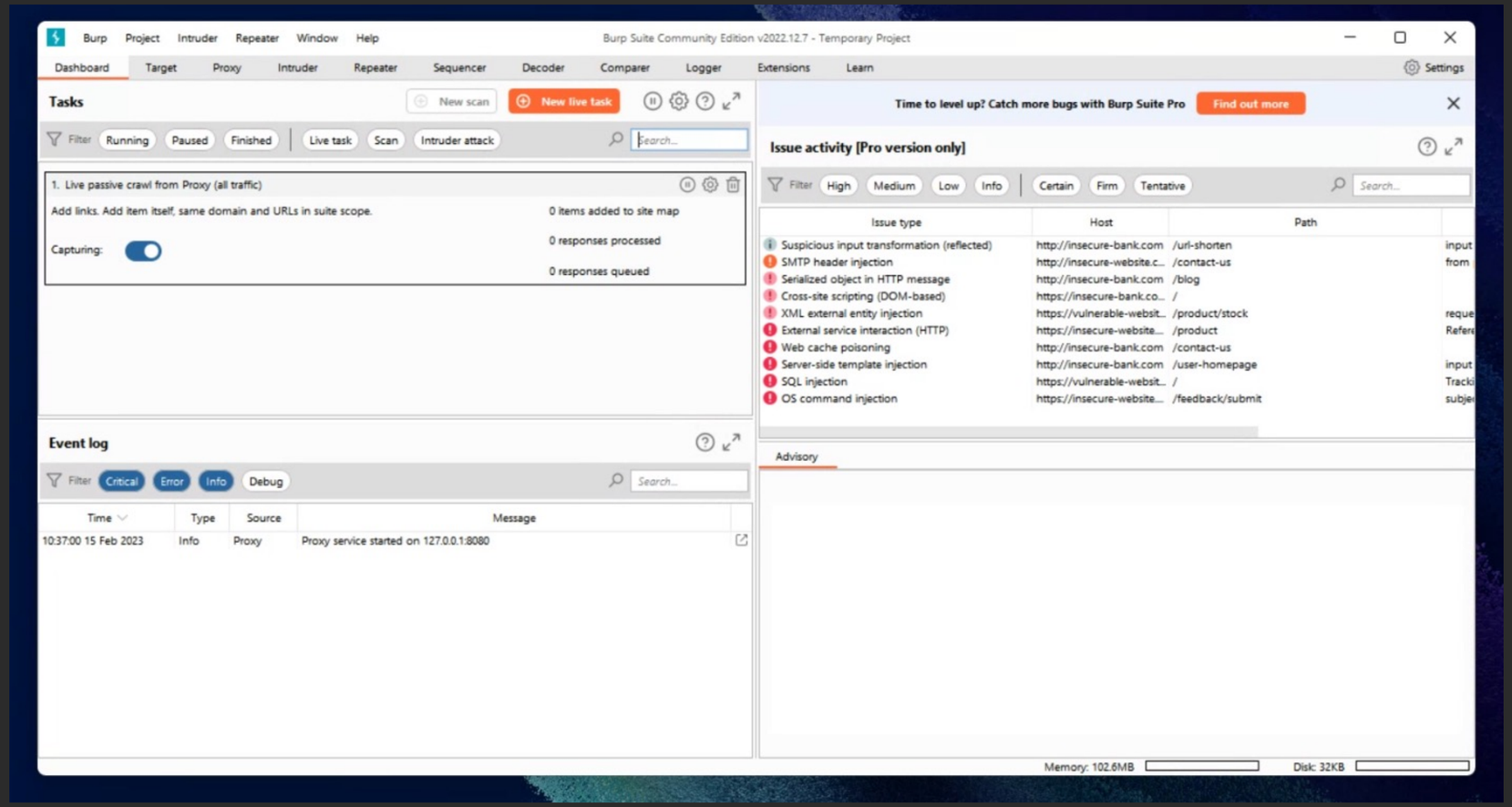
Visual Studio

https://visualstudio.microsoft.com/



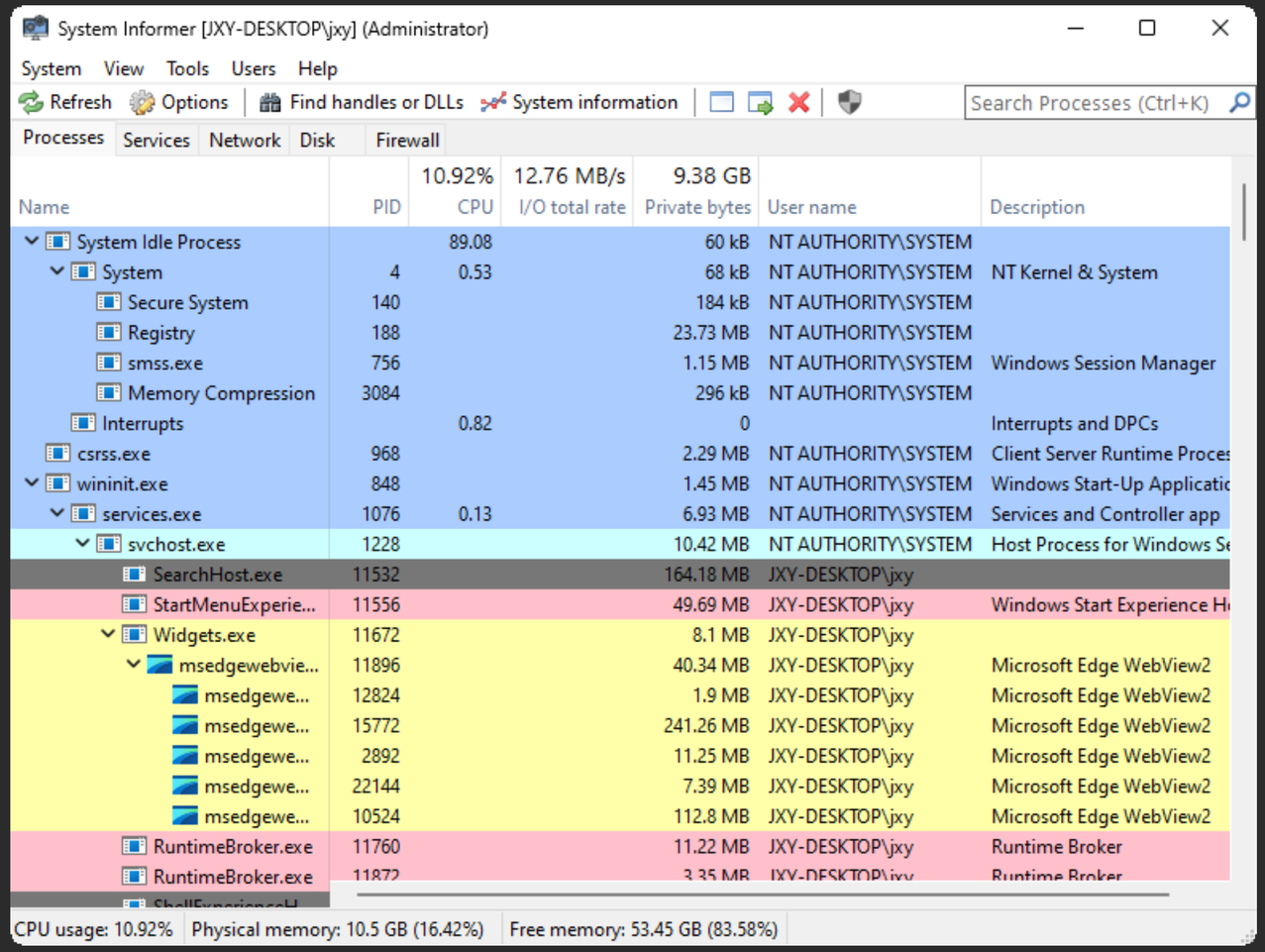
Burp Suite

https://portswigger.net/burp



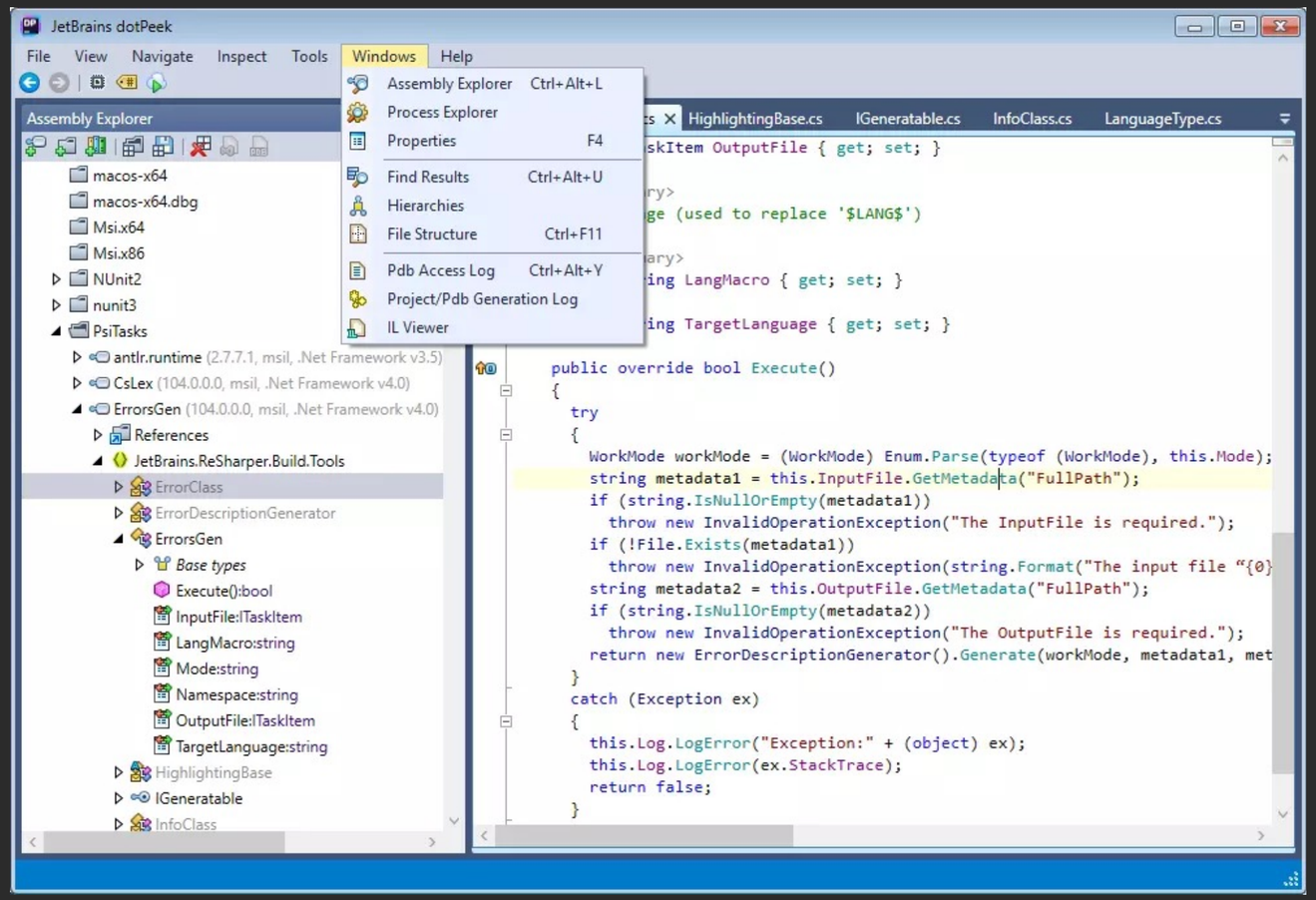
Process Explorer / System Informer

https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer
https://systeminformer.sourceforge.io/



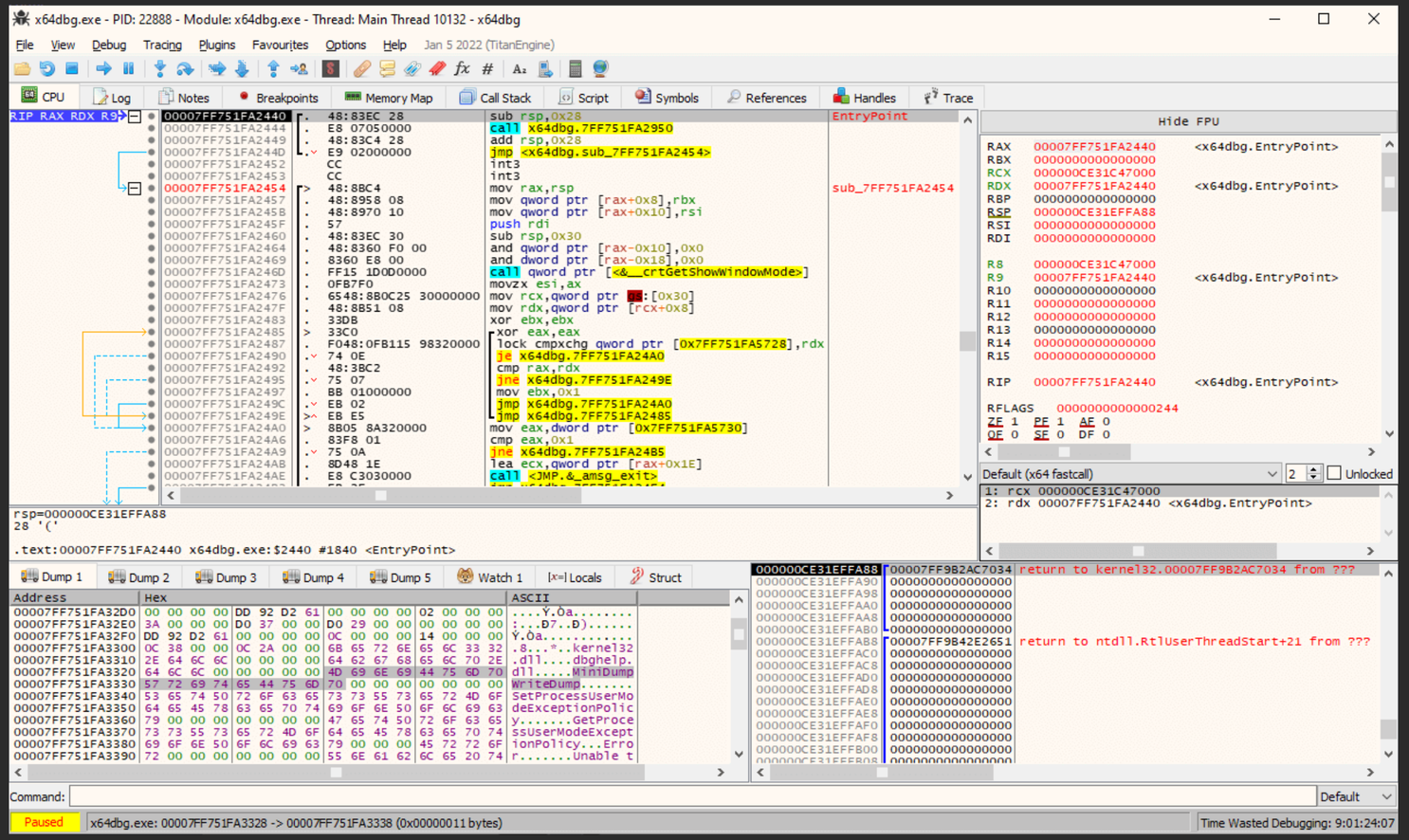
dotPeek

https://www.jetbrains.com/decompiler/



x64dbg

https://github.com/x64dbg/x64dbg



Obrigado!

LinkedIn_
/giuliano-sanfins

Twitter_
@0x_alibabas