Windows Objects Exploitation

Bruno Gonçalves de Oliveira - Trustwave's SpiderLabs
mphx2

$ whoami

M.S.c. in Software Engineering

Computer Engineer

Principal Security Consultant at Trustwave’s SpiderLabs

TheGoonies CTF Player

BETA Vulnerability Research & Memory Corruption Exploitation

Talks here and there

Why?

Market Share
(79%)

Very Interesting

Windows

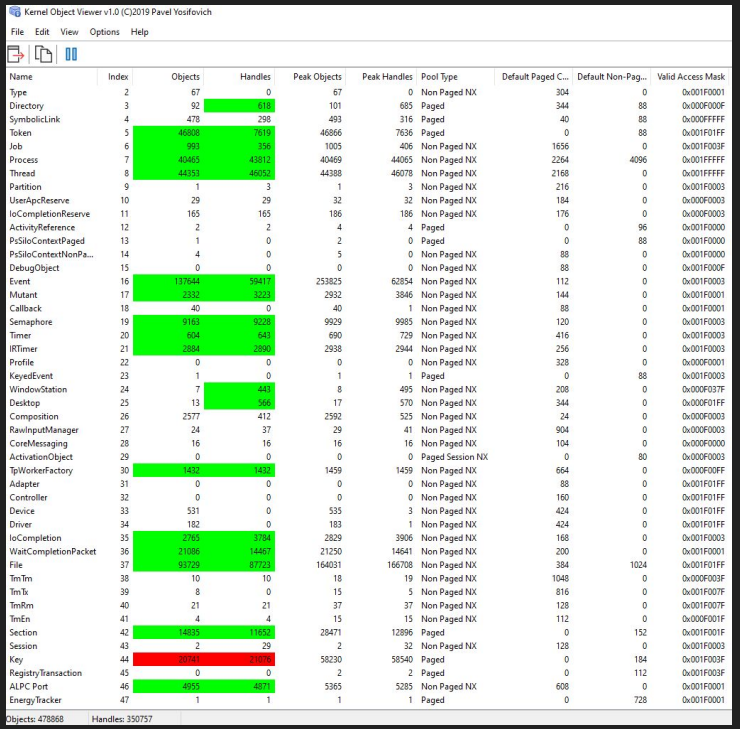
Closed Source

Objects

- *Everything* on a Windows system is an object in kernel space

- Object X Handle :
- “An object is a data structure that represents a system resource, such as a file, thread, or graphic image. An application cannot directly access object data or the system resource that an object represents. Instead, an application must obtain an object handle, which it can use to examine or modify the system resource. Each handle has an entry in an internally maintained table. These entries contain the addresses of the resources and the means to identify the resource type.”

Windows Objects



Name	Index	Objects	Handles	Peak Objects	Peak Handles	Pool Type	Default Paged C...	Default Non-Pag...	Valid Access Mask
Type	2	67	0	67	0	Non Paged NX	304	0	0x001F0001
Directory	3	92	618	101	685	Paged	344	88	0x000F000F
SymbolicLink	4	478	298	493	316	Paged	40	88	0x000FFFFF
Token	5	46808	7619	46866	7636	Paged	0	88	0x001F01FF
Job	6	993	356	1005	406	Non Paged NX	1656	0	0x001F003F
Process	7	40465	43812	40469	44065	Non Paged NX	2264	4096	0x001FFFFF
Thread	8	44353	46052	44388	46078	Non Paged NX	2168	0	0x001FFFFF
Partition	9	1	3	1	3	Non Paged NX	216	0	0x001F0003
UserApcReserve	10	29	29	32	32	Non Paged NX	184	0	0x000F0003
IoCompletionReserve	11	165	165	186	186	Non Paged NX	176	0	0x000F0003
ActivityReference	12	2	2	4	4	Paged	0	96	0x001F0000
PsSiloContextPaged	13	1	0	2	0	Paged	0	88	0x001F0000
PsSiloContextNonPa...	14	4	0	5	0	Non Paged NX	88	0	0x001F0000
DebugObject	15	0	0	0	0	Non Paged NX	88	0	0x001F000F
Event	16	137644	59417	253825	62854	Non Paged NX	112	0	0x001F0003
Mutant	17	2332	3223	2932	3846	Non Paged NX	144	0	0x001F0001
Callback	18	40	0	40	1	Non Paged NX	88	0	0x001F0001
Semaphore	19	9163	9228	9929	9985	Non Paged NX	120	0	0x001F0003
Timer	20	604	643	690	729	Non Paged NX	416	0	0x001F0003
IRTimer	21	2884	2890	2938	2944	Non Paged NX	256	0	0x001F0003
Profile	22	0	0	0	0	Non Paged NX	328	0	0x000F0001
KeyedEvent	23	1	0	1	1	Paged	0	88	0x001F0003
WindowStation	24	7	443	8	495	Non Paged NX	208	0	0x000F037F
Desktop	25	13	566	17	570	Non Paged NX	344	0	0x000F01FF
Composition	26	2577	412	2592	525	Non Paged NX	24	0	0x000F0003
RawInputManager	27	24	37	29	41	Non Paged NX	904	0	0x000F0003
CoreMessaging	28	16	16	16	16	Non Paged NX	104	0	0x000F0000
ActivationObject	29	0	0	0	0	Paged Session NX	0	80	0x000F0003
TpWorkerFactory	30	1432	1432	1459	1459	Non Paged NX	664	0	0x000F00FF
Adapter	31	0	0	0	0	Non Paged NX	88	0	0x001F01FF
Controller	32	0	0	0	0	Non Paged NX	160	0	0x001F01FF
Device	33	531	0	535	3	Non Paged NX	424	0	0x001F01FF
Driver	34	182	0	183	1	Non Paged NX	424	0	0x001F01FF
IoCompletion	35	2765	3784	2829	3906	Non Paged NX	168	0	0x001F0003
WaitCompletionPacket	36	21086	14467	21250	14641	Non Paged NX	200	0	0x001F0001
File	37	93729	87723	164031	166708	Non Paged NX	384	1024	0x001F01FF
TmTm	38	10	10	18	19	Non Paged NX	1048	0	0x000F003F
TmTx	39	8	0	15	5	Non Paged NX	816	0	0x001F007F
TmRm	40	21	21	37	37	Non Paged NX	128	0	0x001F007F
TmEn	41	4	4	15	15	Non Paged NX	112	0	0x000F001F
Section	42	14835	11652	28471	12896	Paged	0	152	0x001F001F
Session	43	2	29	2	32	Non Paged NX	128	0	0x001F0003
Key	44	26721	21078	58230	58540	Paged	0	184	0x001F003F
RegistryTransaction	45	0	0	2	2	Paged	0	112	0x001F003F
ALPC Port	46	4955	4871	5365	5285	Non Paged NX	608	0	0x001F0001
EnergyTracker	47	1	1	1	1	Paged	0	728	0x001F0001

https://github.com/zodiacon/AllTools

Takeaways

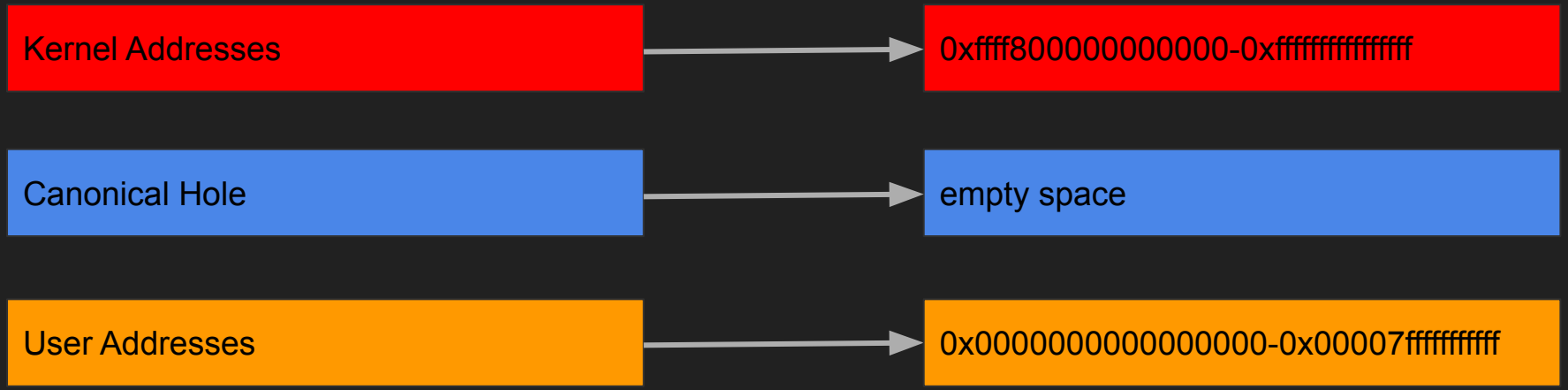
Windows Internal Knowledge

Single Write Exploitation

Famous getsystem

Memory Space

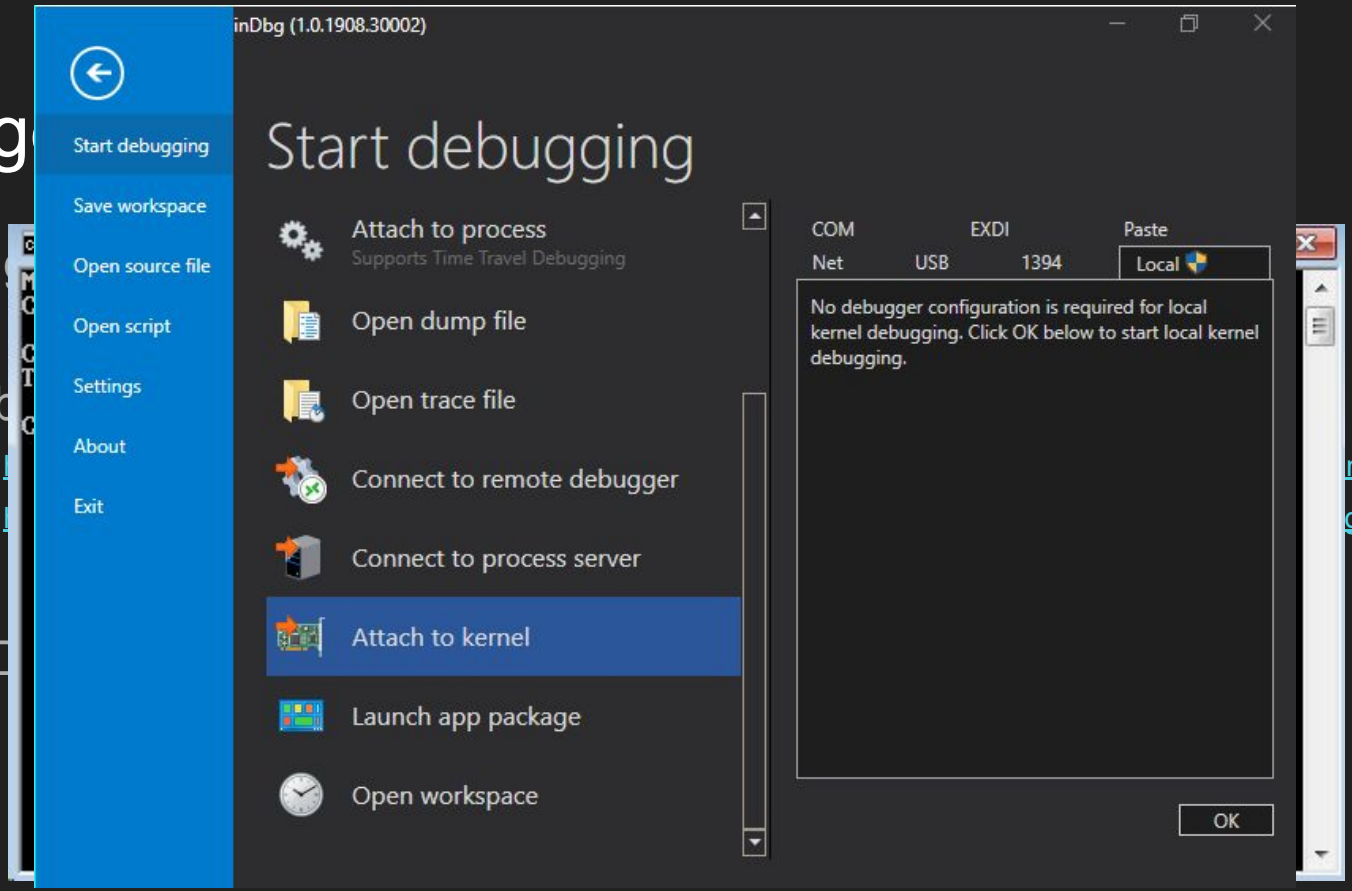
In x64:



Let's g

For debu

- Enab
  - I
  - I
- WinD



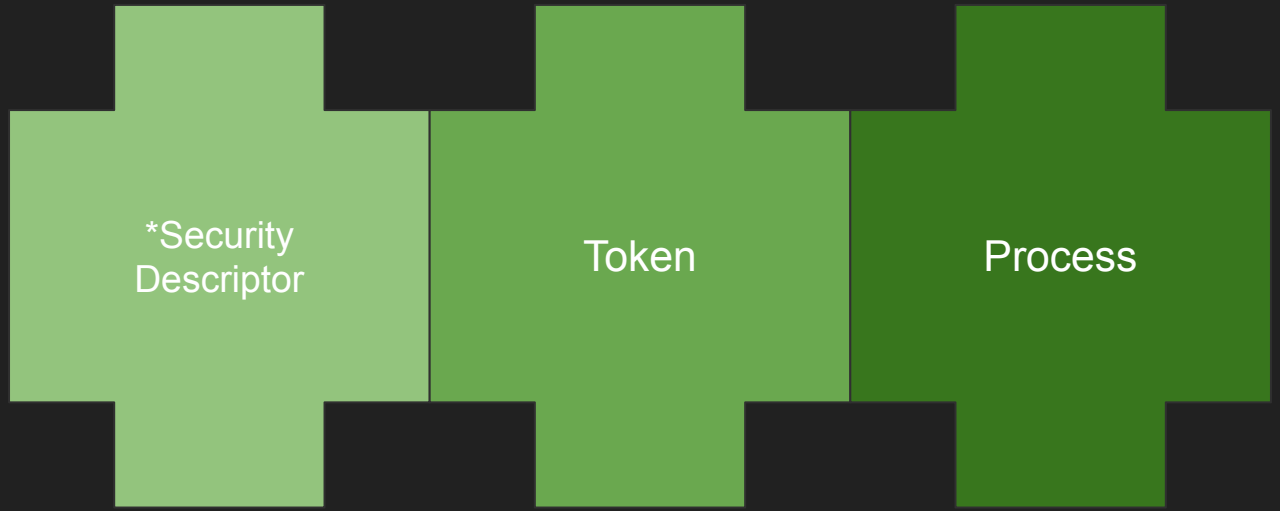
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/windows-debugging-exploiting-part-1-environment-setup/

Debugging an Object

```
lkd> !object ffffa9897b34dd20

Object: ffffa9897b34dd20  Type: (ffffa98979a8c5d0) Device

    ObjectHeader: ffffa9897b34dcf0 (new version)

    HandleCount: 0  PointerCount: 5

    Directory Object: ffffbd04676287b0  Name: 0000001b
```

!object (identify the object based on its type)
https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/-object

Target Objects



SecurityDescriptor

Not really an object

Part of *any* object header

Describe the ACL for the specific object

Debugging SecurityDescriptor

The object header (object - 0x30):

```
lkd> !process 0 0 lsass.exe
PROCESS ffff8403857c2580
    SessionId: 0  Cid: 0294    Peb: 9ea8598000  ParentCid: 021c
    DirBase: 2c310002  ObjectTable:ffffc28de2242940  HandleCount: 1302.
    Image: lsass.exe

lkd> !object ffff8403857c2580
Object: ffff8403857c2580  Type: (ffff8403828cdcb0) Process
    ObjectHeader: ffff8403857c2550 (new version)
    HandleCount: 14  PointerCount: 458369
```

```
lkd> dt _OBJECT_HEADER ffff8403857c2550
nt!_OBJECT_HEADER
   +0x000 PointerCount     : 0n458370
   +0x008 HandleCount      : 0n14
   +0x008 NextToFree       : 0x00000000`0000000e Void
   +0x010 Lock             : _EX_PUSH_LOCK
   +0x018 TypeIndex        : 0x5e '^'
   +0x019 TraceFlags       : 0 ''
   +0x019 DbgRefTrace      : 0y0
   +0x019 DbgTracePermanent : 0y0
   +0x01a InfoMask         : 0x8 ''
   +0x01b Flags            : 0 ''
   +0x01b NewObject        : 0y0
   +0x01b KernelObject     : 0y0
   +0x01b KernelOnlyAccess : 0y0
   +0x01b ExclusiveObject  : 0y0
   +0x01b PermanentObject  : 0y0
   +0x01b DefaultSecurityQuota : 0y0
   +0x01b SingleHandleEntry : 0y0
   +0x01b DeletedInline    : 0y0
   +0x01c Reserved         : 0x8908438b
   +0x020 ObjectCreateInfo : 0xfffff803`6b467c00 _OBJECT_CREATE_INFORMATION
   +0x020 QuotaBlockCharged : 0xfffff803`6b467c00 Void
   +0x028 SecurityDescriptor : 0xffffc28d`e22163ec Void
   +0x030 Body             : _QUAD
```

Debugging SecurityDescriptor

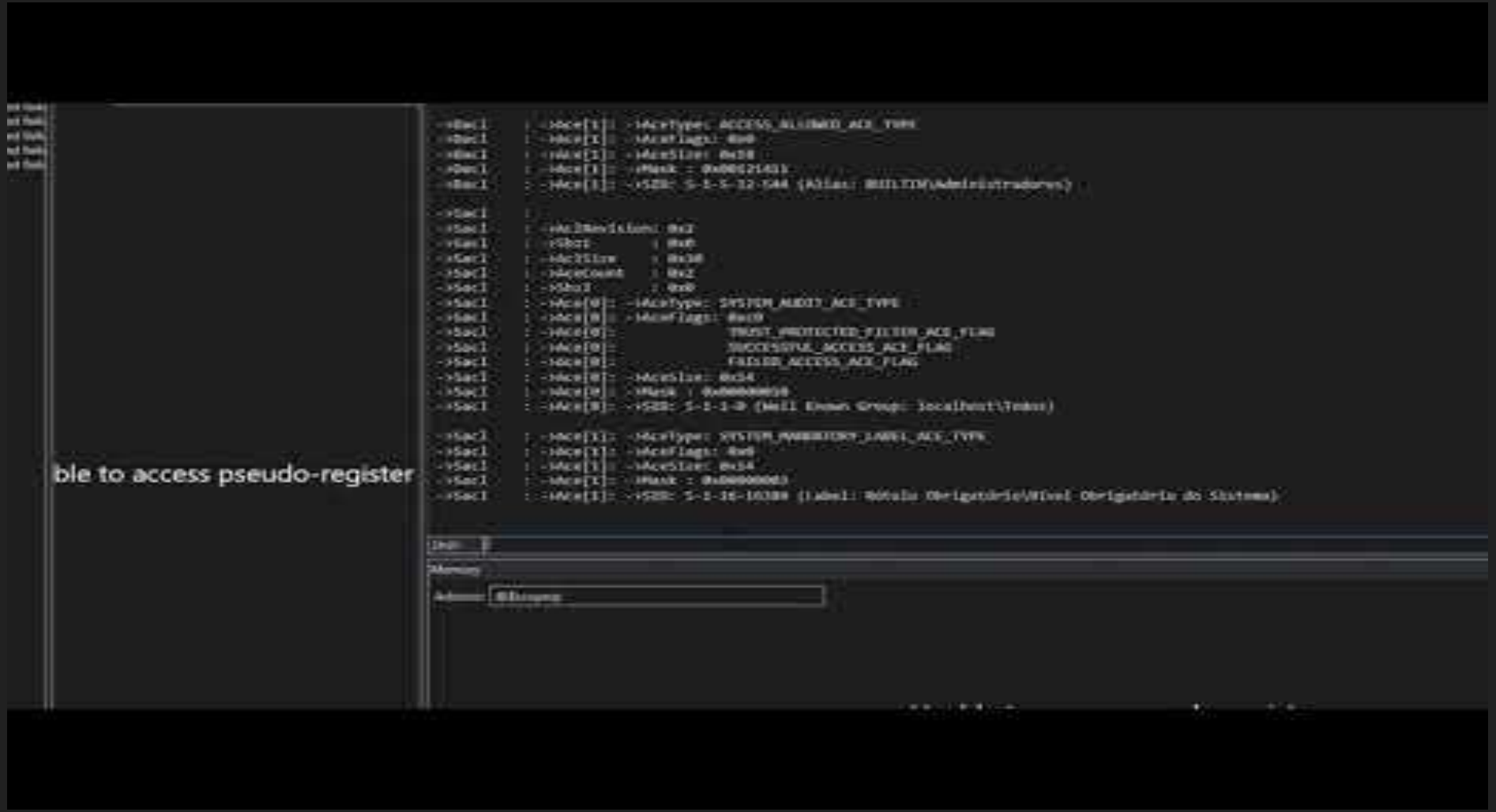
!sd https://blogs.msdn.microsoft.com/doronh/2006/03/23/debugger-commands-sd-tha

```
lkd> !sd (0xffffc28d`e22163ec & 0xFFFFFFFFFFFFFFF0) 1
->Revision: 0x1
->Sbz1    : 0x0
->Control : 0x8014
            SE_DACL_PRESENT
            SE_SACL_PRESENT
            SE_SELF_RELATIVE
->Owner   : S-1-5-32-544 (Alias: BUILTIN\Administradores)
->Group   : S-1-5-18 (Well Known Group: AUTORIDADE NT\SISTEMA)
->Dacl    :
->Dacl    : ->AclRevision: 0x2
->Dacl    : ->Sbz1       : 0x0
->Dacl    : ->AclSize    : 0x3c
->Dacl    : ->AceCount   : 0x2
->Dacl    : ->Sbz2       : 0x0
->Dacl    : ->Ace[0]: ->AceType: ACCESS_ALLOWED_ACE_TYPE
->Dacl    : ->Ace[0]: ->AceFlags: 0x0
->Dacl    : ->Ace[0]: ->AceSize: 0x14
->Dacl    : ->Ace[0]: ->Mask :0x001fffff
->Dacl    : ->Ace[0]: ->SID: S-1-5-18 (Well Known Group: AUTORIDADE NT\SISTEMA)

->Dacl    : ->Ace[1]: ->AceType: ACCESS_ALLOWED_ACE_TYPE
->Dacl    : ->Ace[1]: ->AceFlags: 0x0
->Dacl    : ->Ace[1]: ->AceSize: 0x18
->Dacl    : ->Ace[1]: ->Mask : 0x00121411
->Dacl    : ->Ace[1]: ->SID: S-1-5-32-544 (Alias: BUILTIN\Administradores)

[...]
```

The SD is always aligned.

This mask indicates that AUTORIDATE NT\SISTEMA has all the permissions on this SD.

We can update this byte!


ble to access pseudo-register

Token Object

- This object describe the ACLs on a spec

```
lkd> !process 0 0 cmd.exe
PROCESS ffffb504cf18d080
    SessionId: 1  Cid: 27c8    Peb: 4c23638000  ParentCid: 130c
    DirBase: 68800002  ObjectTable: ffffdc0c68389ac0  HandleCount:  46.
    Image: cmd.exe

lkd> !process ffffb504cf18d080 1
PROCESS ffffb504cf18d080
    SessionId: 1  Cid: 27c8    Peb: 4c23638000  ParentCid: 130c
    DirBase: 68800002  ObjectTable: ffffdc0c68389ac0  HandleCount:  46.
    Image: cmd.exe
    VadRoot ffffb504cf29ad10 Vads 31 Clone 0 Private 161. Modified 0.
Locked 8.
    DeviceMap ffffdc0c65eb21e0
    Token                             ffffdc0c64dec970
    ElapsedTime                       00:00:56.547
    UserTime                          00:00:00.000
    KernelTime                        00:00:00.000
    QuotaPoolUsage[PagedPool]         29784
    QuotaPoolUsage[NonPagedPool]      4672
    Working Set Sizes (now,min,max)  (773, 50, 345) (3092KB, 200KB, 1380KB)
    PeakWorkingSetSize                1020
    VirtualSize                       2101299 Mb
    PeakVirtualSize                   2101307 Mb
    PageFaultCount                    1191
    MemoryPriority                    BACKGROUND
    BasePriority                      8
    CommitCharge                      996
```

```
lkd> !exts.token -n ffffdc0c64dec970
_TOKEN 0xffffdc0c64dec970
TS Session ID: 0x1
User: S-1-5-21-3125529031-1994031880-777778863-1000 (User: DESKTOP-L1TSJSG\mphx2)
User Groups:
 00 S-1-5-21-3125529031-1994031880-777778863-513 (Group: DESKTOP-L1TSJSG\None)
    Attributes - Mandatory Default Enabled
 01 S-1-1-0 (Well Known Group: localhost\Todos)
    Attributes - Mandatory Default Enabled
 02 S-1-5-114 (Well Known Group: AUTORIDADE NT\Conta local e membro do grupo de
Administradores)
    Attributes - DenyOnly
 03 S-1-5-32-544 (Alias: BUILTIN\Administradores)
    Attributes - DenyOnly
 04 S-1-5-32-545 (Alias: BUILTIN\Usuários)
    Attributes - Mandatory Default Enabled
 05 S-1-5-32-559 (Alias: BUILTIN\Usuários de log de desempenho)
    Attributes - Mandatory Default Enabled
 06 S-1-5-4 (Well Known Group: AUTORIDADE NT\INTERATIVO)
    Attributes - Mandatory Default Enabled
 07 S-1-2-1 (Well Known Group: localhost\L
    Attributes - Mandatory Default Enabled
 08 S-1-5-11 (Well Known Group: AUTORIDADE
    Attributes - Mandatory Default Enabled
 09 S-1-5-15 (Well Known Group: AUTORIDADE
    Attributes - Mandatory Default Enabled
 10 S-1-5-113 (Well Known Group: AUTORIDAD
    Attributes - Mandatory Default Enabled
 11 S-1-5-5-0-189010 Unrecognized SID
    Attributes - Mandatory Default Enabled
 12 S-1-2-0 (Well Known Group: localhost\L
    Attributes - Mandatory Default Enabled
 13 S-1-5-64-10 (Well Known Group: AUTORIDAD
    Attributes - Mandatory Default Enabled
 14 S-1-16-8192 (Label: Rótulo Obrigatório\Nível Obrigatório Médio)
    Attributes - GroupIntegrity GroupIntegrityEnabled
Primary Group: S-1-5-21-3125529031-1994031880-777778863-513 (Group: DESKTOP-L1TSJSG\None)
Privs:
 19 0x000000013 SeShutdownPrivilege              Attributes -
 23 0x000000017 SeChangeNotifyPrivilege          Attributes - Enabled Default
 25 0x000000019 SeUndockPrivilege                Attributes -
 33 0x000000021 SeIncreaseWorkingSetPrivilege    Attributes -
 34 0x000000022 SeTimeZonePrivilege              Attributes -
Authentication ID:         (0,2e60b)
Impersonation Level:       Anonymous
TokenType:                 Primary
Source: User32             TokenFlags: 0x2a00 ( Token in use )
Token ID: 1748a6           ParentToken ID: 2e60e
Modified ID:               (0, 2e617)
RestrictedSidCount: 0      RestrictedSids: 0x0000000000000000
OriginatingLogonSession: 3e7
PackageSid: (null)
CapabilityCount: 0      Capabilities: 0x0000000000000000
```

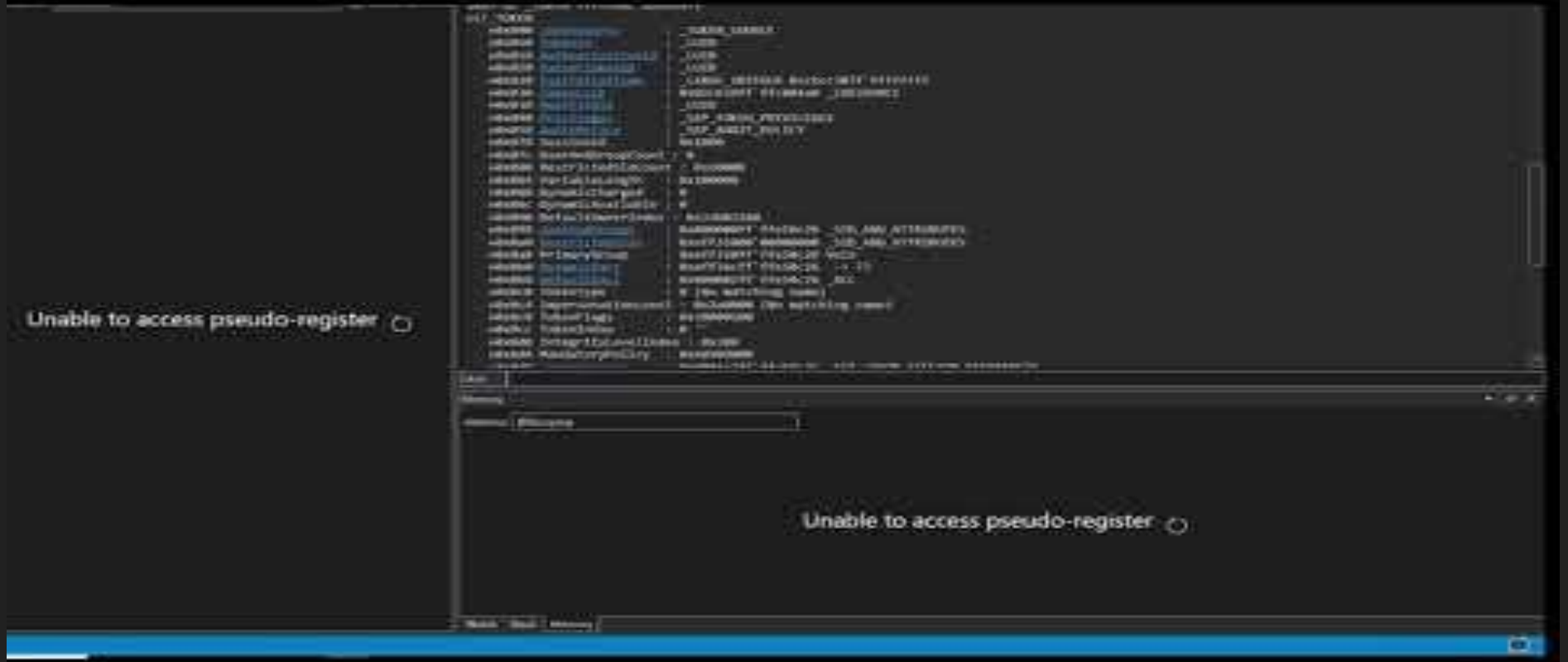
Token Object Address

_SEP_Token_Privileges Compromise

```
lkd> dt _token ffff9f00`754e797f
nt!_TOKEN
   +0x000 TokenSource      : _TOKEN_SOURCE
   +0x010 TokenId          : _LUID
   +0x018 AuthenticationId : _LUID
   +0x020 ParentTokenId    : _LUID
   +0x028 ExpirationTime   : _LARGE_INTEGER 0x40650ff
   +0x030 TokenLock        : 0x00000602`88000000 _ERESOURCE
   +0x038 ModifiedId       : _LUID
   +0x040 Privileges       : _SEP_TOKEN_PRIVILEGES
   +0x058 AuditPolicy      : _SEP_AUDIT_POLICY
   +0x078 SessionId        : 0x100000
   +0x07c UserAndGroupCount : 0
   +0x080 RestrictedSidCount : 0
   +0x084 VariableLength   : 0
   +0x088 DynamicCharged   : 0x4e7e0000
   +0x08c DynamicAvailable : 0xff9f0075
   +0x090 DefaultOwnerIndex : 0xff
   +0x098 UserAndGroups    : 0xff9f0076`8023e000
_SID_AND_ATTRIBUTES
   +0x0a0 RestrictedSids   : 0xff9f0076`8023e0ff
_SID_AND_ATTRIBUTES
   +0x0a8 PrimaryGroup     : 0xff9f0076`8023fcff Void
   +0x0b0 DynamicPart      : 0x00000000`000001ff  -> ??
   +0x0b8 DefaultDacl      : 0xffbd0100`002a0000 _ACL
[...]
```

```
lkd> dt _SEP_TOKEN_PRIVILEGES ffff9f00`754e797f+0x40
nt!_SEP_TOKEN_PRIVILEGES
   +0x000 Present          : 0x00000080`00000000
   +0x008 Enabled          : 0x00004080`00000000
   +0x010 EnabledByDefault : 0
```

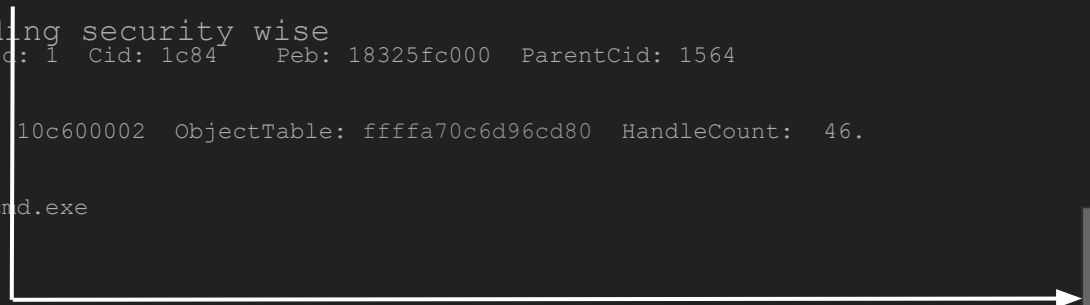
- Locate the Token in a EPROCESS Object (Win10 offset 0x358)
- The attack is based on modifying the bitmap at Token+0x40 (_SEP_Token_Privileges)


Unable to access pseudo-register
Unable to access pseudo-register

EPROCESS Object

```
lkd> !process 0 0 cmd.exe
PROCESS ffff8e8e7c537580
    SessionId: 1  Cid: 1c84    Peb: 18325fc000  ParentCid: 1564
    DirBase: 10c600002  ObjectTable: ffffa70c6d96cd80  HandleCount:  46.
    Image: cmd.exe
```

- Responsible for the processes' properties
- Including security wise



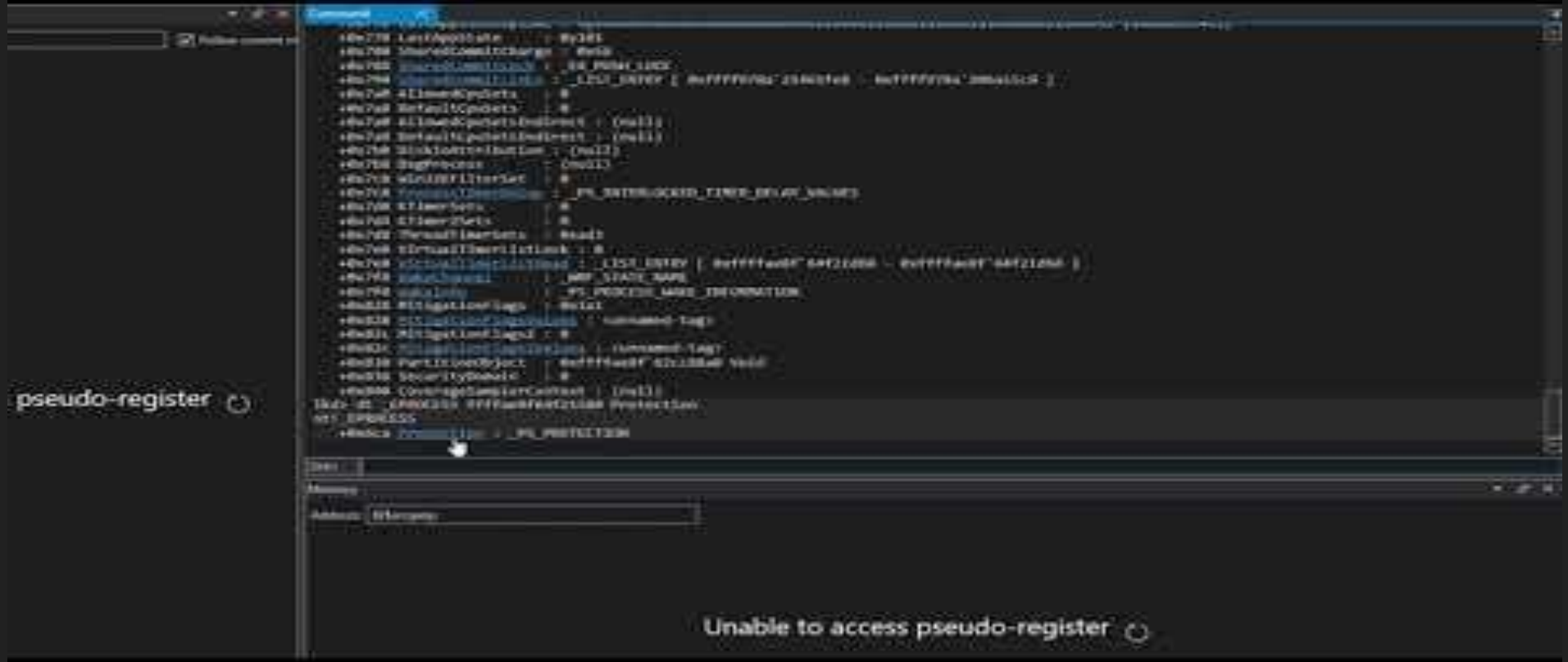
This is the EPROCESS object address

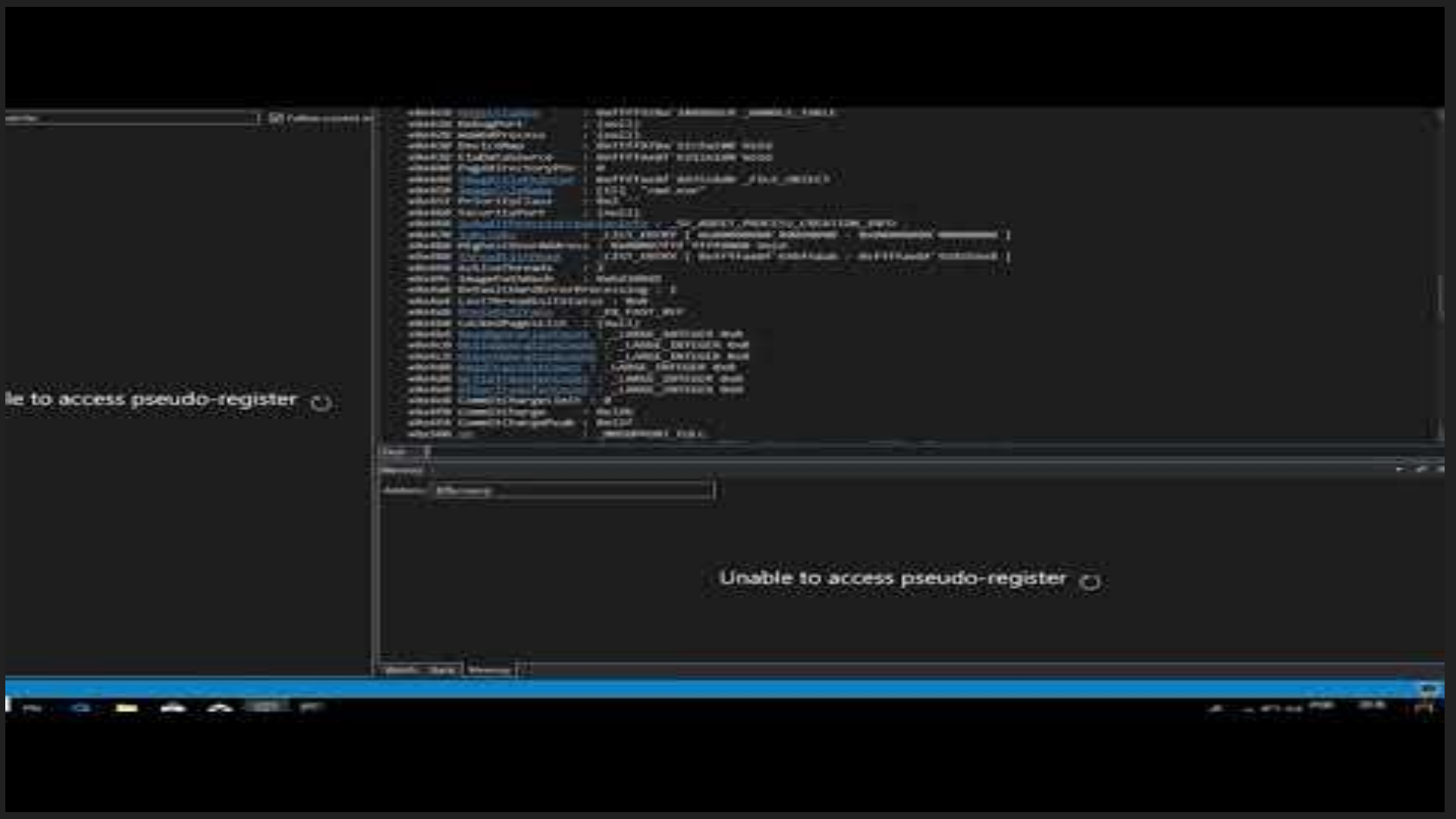
EPROCESS Security Properties

```
lkd> dt _EPROCESS ffffc30b618c9580 Token
nt!_EPROCESS
   +0x358 Token : _EX_FAST_REF
lkd> dq ffffc30b618c9580+0x358
ffffc30b`618c98d8  ffff9a88`9d01804f 00000000`00000000
ffffc30b`618c98e8  00000000`00000000 00000000`00000000
ffffc30b`618c98f8  00000000`00000000 00000000`00000000
ffffc30b`618c9908  00000000`00000000 00000000`00000000
ffffc30b`618c9918  00000000`000000a6 00000000`00000008
ffffc30b`618c9928  fffff98c`c31421c0 00000000`00000000
ffffc30b`618c9938  ffff9a88`9ee90d60 00007ff6`42e40000
ffffc30b`618c9948  00000000`b80217a8 00000000`00000000
lkd> dq ffff9a88`9d01804f
ffff9a88`9d01804f  00000000`0003eb00 00000000`0003e700
ffff9a88`9d01805f  00000000`00000000 207526b6`4ceb9000
ffff9a88`9d01806f  ffc30b5b`84a0b006 00000000`0003ecff
ffff9a88`9d01807f  00001ff2`ffffbc00 00001e60`b1e89000
ffff9a88`9d01808f  00001e60`b1e89000 00000000`00000000
ffff9a88`9d01809f  00000000`00000000 00000000`00000000
ffff9a88`9d0180af  00000000`00000000 00000500`00000000
ffff9a88`9d0180bf  0000a400`00000000 00000000`00100000
```

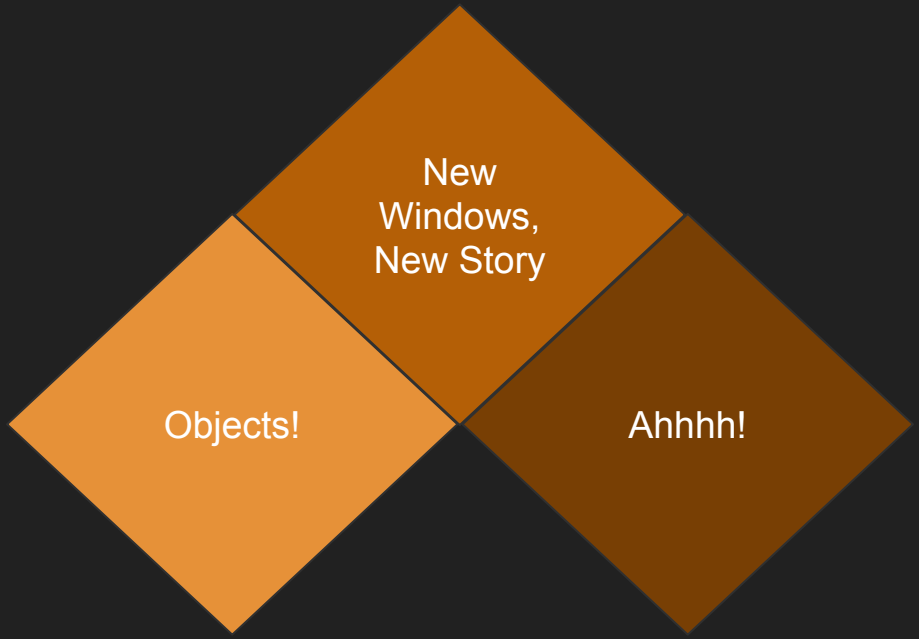
```
ffc30b635ac580 -r1 (*((ntkrnlmp!_EPROCESS
00)).MitigationFlagsValues
CESS *)0xffff9a88a41caf00)).MitigationFlagsValues [Type: <unnamed-tag>]
)] ControlFlowGuardEnabled : 0x0 [Type: unsigned long]
)] ControlFlowGuardExportSuppressionEnabled : 0x1 [Type: unsigned long]
)] ControlFlowGuardStrict : 0x1 [Type: unsigned long]
)] DisallowStrippedImages : 0x1 [Type: unsigned long]
)] ForceRelocateImages : 0x0 [Type: unsigned long]
)] HighEntropyASLREnabled : 0x1 [Type: unsigned long]
)] StackRandomizationDisabled : 0x0 [Type: unsigned long]
)] ExtensionPointDisable : 0x0 [Type: unsigned long]
)] DisableDynamicCode : 0x0 [Type: unsigned long]
)] DisableDynamicCodeAllowOptOut : 0x1 [Type: unsigned long]
)] DisableDynamicCodeAllowRemoteDowngrade : 0x1 [Type: unsigned long]
)] AuditDisableDynamicCode : 0x1 [Type: unsigned long]
)] DisallowWin32kSystemCalls : 0x0 [Type: unsigned long]
)] AuditDisallowWin32kSystemCalls : 0x1 [Type: unsigned long]
)] EnableFilteredWin32kAPIs : 0x1 [Type: unsigned long]
)] AuditFilteredWin32kAPIs : 0x1 [Type: unsigned long]
)] DisableNonSystemFonts : 0x
)] AuditNonSystemFontLoading
)] PreferSystem32Images : 0x0
)] ProhibitRemoteImageMap : 0
)] AuditProhibitRemoteImageMa
)] ProhibitLowILImageMap : 0x
[+0x000 (22:22)] AuditProhibitLowILImageMap
[+0x000 (23:23)] SignatureMitigationOptIn :
[+0x000 (24:24)] AuditBlockNonMicrosoftBina
[+0x000 (25:25)] AuditBlockNonMicrosoftBina
[+0x000 (26:26)] LoaderIntegrityContinuityEnabled : 0x0 [Type: unsigned long]
[+0x000 (27:27)] AuditLoaderIntegrityContinuity : 0x0 [Type: unsigned long]
[+0x000 (28:28)] EnableModuleTamperingProtection : 0x1 [Type: unsigned long]
[+0x000 (29:29)] EnableModuleTamperingProtectionNoInherit : 0x1 [Type: unsigned long]
[+0x000 (30:30)] RestrictIndirectBranchPrediction : 0x1 [Type: unsigned long]
```

```
lkd> dx -id 0,0,ffffc30b635ac580 -r1 (*((ntkrnlmp!_PS_PROTECTION *)0xffff9a88a41cb5ca))
(*((ntkrnlmp!_PS_PROTECTION *)0xffff9a88a41cb5ca))                 [Type: _PS_PROTECTION]
    [+0x000] Level            : 0x0 [Type: unsigned char]
    [+0x000 ( 2: 0)] Type             : 0x0 [Type: unsigned char]
    [+0x000 ( 3: 3)] Audit            : 0x0 [Type: unsigned char]
    [+0x000 ( 7: 4)] Signer           : 0x0 [Type: unsigned char]
```


pseudo-register
Unable to access pseudo-register


le to access pseudo-register
Unable to access pseudo-register

Conclusions



References

Paged Out #1 https://pagedout.institute/download/PagedOut_001_beta1.pdf

Windows Debugging & Exploitation - Environment Setup
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/windows-debugging-exploiting-part-1-environment-setup/

WinDBG Workshop @ DEFCON 27 https://github.com/hugsy/defcon_27_windbg_workshop/

Windows Internals Training https://www.pluralsight.com/authors/pavel-yosifovich

AllTools Repository (Pavel Yosifovich) - https://github.com/zodiacon/AllTools

Thank you!

Questions?