

Работа 2. Исследование структур данных обеспечения безопасности в Windows

Цель работы: исследовать структуры данных Windows, используемые для обеспечения безопасности.

Задание 2.1. Определить идентификатор защиты SID текущего пользователя.

В рамках этого задания Вы должны будете научиться определять идентификатор защиты SID текущего пользователя с помощью утилит *Process Explorer* и *PsgetSid*.

Утилита *PsgetSid* специально предназначена для получения SID разных учетных записей. Данная утилита входит в набор *PsTools* и её можно скачать с сайта *Sysinternals*.

Указания к выполнению.

1. Выполните запуск утилиты *Process Explorer* от имени администратора.

2. В интерфейсе *Process Explorer* выберите процесс для исследования и нажмите кнопку **Properties**. В появившемся диалоговом окне выберите закладку **Security**, на которой отображается информация о маркера процесса (базовое имя пользователя, под записью которого работает процесс; группы, в которые входит эта запись, и ее привилегии в системе). При выборе группы в списке **Group** под списком отображается идентификатор защиты (SID) выбранной группы.

Process Explorer - Sysinternals: www.sysinternals.com [LSPACE\avtimofeev]

Process	Properties	CPU	Private Bytes	Working Set	Description	Company Name
chrome.exe		2620	55 396 K	17 584 K	Google Chrome	Google Inc.
chrome.exe		11208	62 244 K	31 868 K	Google Chrome	Google Inc.
chrome.exe		4204	0.01	56 124 K	77 264 K Google Chrome	Google Inc.
chrome.exe		7368	0.04	56 612 K	60 992 K Google Chrome	Google Inc.
cmd.exe		2100		2 896 K	3 336 K Обработчик команд Windo...	Microsoft Corporation
COCIManager.exe		4548	0.01	2 260 K	1 080 K Camera Control Interface	Logitech Inc.
Communications_Helper.exe		1376	0.32	7 196 K	1 580 K Communications Manager	Logitech Inc.
conhost.exe		4440	< 0.01	2 336 K	5 808 K Окно консоли узла	Microsoft Corporation
consent.exe		4720		3 588 K	9 036 K Согласованный пользоват...	Microsoft Corporation
consent.exe		10172		3 744 K	9 344 K Согласованный пользоват...	Microsoft Corporation
consent.exe		7032		1 552 K	4 320 K Согласованный пользоват...	Microsoft Corporation
CrossLoopService.exe		1904	< 0.01	2 352 K	708 K CrossLoop Service	CrossLoop
csrss.exe		528	< 0.01	3 236 K	2 108 K Процесс исполнения клие...	Microsoft Corporation
csrss.exe		592	0.78	9 520 K	137 928 K Процесс исполнения клие...	Microsoft Corporation
cvpnd.exe		1932	0.01	2 136 K	1 832 K Cisco Systems VPN Client	Cisco Systems, Inc.
dllhost.exe		9008		1 360 K	3 768 K COM Surrogate	Microsoft Corporation
DMMon.exe		6020	< 0.01	2 988 K	1 532 K PDM File Monitor	IBM
dwm.exe		3844	0.74	134 636 K	70 356 K Диспетчер окон рабочего ...	Microsoft Corporation
EXCEL.EXE		10760	0.05	46 332 K	34 256 K Microsoft Office Excel	Microsoft Corporation
explorer.exe		3700	< 0.01	20 740 K	952 K Проводник	Microsoft Corporation
explorer.exe		5676	0.31	152 324 K	106 824 K Проводник	Microsoft Corporation
explorer.exe		10576	0.01	27 620 K	16 156 K Проводник	Microsoft Corporation
explorer.exe		9220	0.01	28 652 K	44 116 K Проводник	Microsoft Corporation
explorer.exe		8640	0.01	44 772 K	53 584 K Проводник	Microsoft Corporation

Type	Name
ALPC Port	\RPC Control\OLE1841330722E14607ACABFDC6CF45
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\BaseNamedObjects\firefoxhomepage\Gm8QMz72ep3ssSZDBb1blWqI510VhwhPefVSB3p...
Event	\BaseNamedObjects\firefoxhomepage\Gm8QMz72ep3ssSZDBb1blWqI510VhwhPefVSB3p...
Event	\BaseNamedObjects\firefoxhomepage\Gm8QMz72ep3ssSZDBb1blWqI510VhwhPefVSB3p...
Event	\BaseNamedObjects\firefoxsearch_engine\Gm8QMz72ep3ssSZDBb1blWqI510VhwhPefVS...
Event	\BaseNamedObjects\firefoxsearch_engine\Gm8QMz72ep3ssSZDBb1blWqI510VhwhPefVS...
Event	\BaseNamedObjects\firefoxsearch_engine\Gm8QMz72ep3ssSZDBb1blWqI510VhwhPefVS...
Event	\BaseNamedObjects\firefoxsearch_engine\Gm8QMz72ep3ssSZDBb1blWqI510VhwhPefVS...
Event	\BaseNamedObjects\firefoxtoolbar\Gm8QMz72ep3ssSZDBb1blWqI510VhwhPefVSB3pAV8...
Event	\BaseNamedObjects\firefoxtoolbar\Gm8QMz72ep3ssSZDBb1blWqI510VhwhPefVSB3pAV8...

CPU Usage: 32.81% | Commit Charge: 47.87% | Processes: 116 | Physical Usage: 88.31%

explorer.exe:10576 Properties

Image	Performance	Performance Graph	Disk and Network	GPU Graph
Threads	TCP/IP	Security	Environment	Strings

User: LSPACE\avtimofeev
 SID: S-1-5-21-2609833062-1600835590-1466217079-2004
 Session: 1 Logon Session: 4bede
 Virtualized: No

Group	Flags
BUILTIN\Администраторы	Deny
BUILTIN\Пользователи	Mandatory
Logon SID (S-1-5-0-310370)	Mandatory
NT AUTHORITY\Данная организация	Mandatory
NT AUTHORITY\ИНТЕРАКТИВНЫЕ	Mandatory
NT AUTHORITY\Прошедшие проверку	Mandatory
S-1-5-21-2609833062-1600835590-1466217079-1119	Mandatory
S-1-5-21-2609833062-1600835590-1466217079-1736	Mandatory
S-1-5-21-2609833062-1600835590-1466217079-512	Deny
S-1-5-21-2609833062-1600835590-1466217079-513	Mandatory
Bce	Mandatory
КОНСОЛЬНЫЙ РУКОВОДИТЕЛЬ	..
Group SID: S-1-5-32-544	

Privilege	Flags
SeChangeNotifyPrivilege	Default Enabled
SeIncreaseWorkingSetPrivilege	Disabled
SeShutdownPrivilege	Disabled
SeTimeZonePrivilege	Disabled
SeUndockPrivilege	Disabled

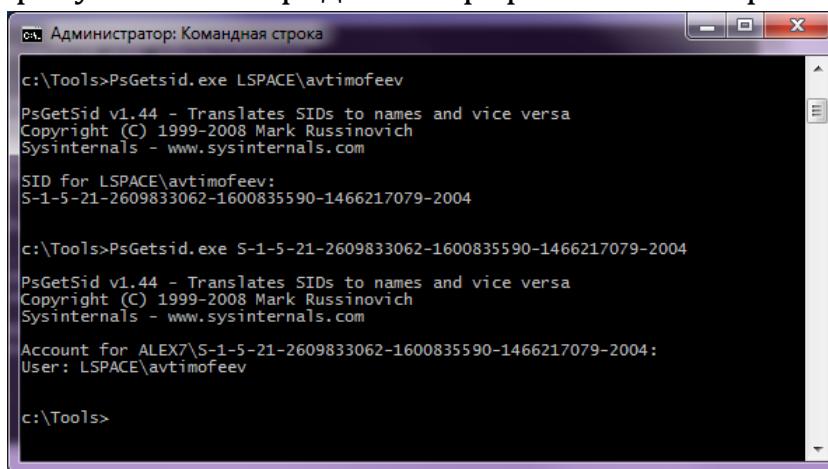
Permissions

OK Cancel

На рисунке вверху красным цветом выделен идентификатор безопасности (SID) пользователя – владельца процесса. SID представляет собой уникальное значение переменной длины, используемое в операционных системах Windows для идентификации участника безопасности или группы безопасности.

3. Скачайте и распакуйте в каталог **c:\Tools** комплект утилит *PsTools* (<http://technet.microsoft.com/ru-ru/sysinternals/bb897417>).

4. Запустите командную строку от имени администратора, перейдите в каталог **c:\Tools** и запустите утилиту *PsGetSid.exe*. В качестве параметра утилиты можно указать либо имя учетной записи, либо SID. На рисунке ниже продемонстрированы оба варианта.



```
Администратор: Командная строка

c:\Tools>PsGetsid.exe LSPACE\avtimofeev

PsGetSid v1.44 - Translates SIDs to names and vice versa
Copyright (C) 1999-2008 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for LSPACE\avtimofeev:
S-1-5-21-2609833062-1600835590-1466217079-2004

c:\Tools>PsGetsid.exe S-1-5-21-2609833062-1600835590-1466217079-2004

PsGetSid v1.44 - Translates SIDs to names and vice versa
Copyright (C) 1999-2008 Mark Russinovich
Sysinternals - www.sysinternals.com

Account for ALEX7\S-1-5-21-2609833062-1600835590-1466217079-2004:
User: LSPACE\avtimofeev

c:\Tools>
```

Удостоверьтесь, что SID полностью совпадают в первом и втором способах.

5. Подготовьте итоговый отчет с развернутыми выводами по заданию.

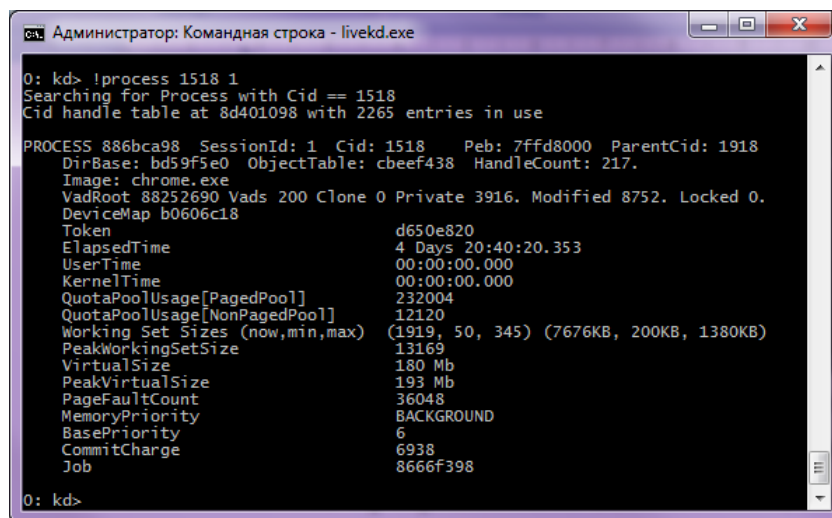
Задание 2.2. Исследовать маркер доступа (access token).

Указания к выполнению.

1. Запустите командную строку от имени администратора, перейдите в каталог **c:\Tools\LiveKD** и запустите утилиту *LiveKd.exe*.

2. Вызовите команду *!process 0 0* для вывода краткого списка процессов системы, выберите процесс для дальнейшего изучения и запишите его идентификатор (тоже самое Вы можете выполнить с помощью утилиты *Process Explorer*). В нашем случае для дальнейшего анализа выбран процесс *chrome.exe* с идентификатором *1518*. Ознакомьтесь с результатами выполнения данного шага, запишите их в отчет, выберите процесс для дальнейшего изучения.

3. Выполните команду *!process <идентификатор процесса> 1*, в этом случае Вам отобразится подробная информация о выбранном процессе. Для дальнейших исследований нас будет интересовать поле **Token**, значение которого равно *dd650e820*. Повторите действия для выбранного процесса, ознакомьтесь с результатами и запишите их в отчет.



```
0: kd> !process 1518 1
Searching for Process with Cid == 1518
Cid handle table at 8d401098 with 2265 entries in use

PROCESS 886bca98 SessionId: 1 Cid: 1518 Peb: 7ffdf8000 ParentCid: 1918
DirBase: bd59f5e0 ObjectTable: cbeef438 HandleCount: 217.
Image: chrome.exe
VadRoot: 88252690 Vads: 200 Clone: 0 Private: 3916. Modified: 8752. Locked: 0.
DeviceMap: b0606c18
Token: dd650e820
ElapsedTime: 4 Days 20:40:20.353
UserTime: 00:00:00.000
KernelTime: 00:00:00.000
QuotaPoolUsage[PagedPool]: 232004
QuotaPoolUsage[NonPagedPool]: 12120
Working Set Sizes (now,min,max): (1919, 50, 345) (7676KB, 200KB, 1380KB)
PeakWorkingSetSize: 13169
VirtualSize: 180 Mb
PeakVirtualSize: 193 Mb
PageFaultCount: 36048
MemoryPriority: BACKGROUND
BasePriority: 6
CommitCharge: 6938
Job: 8666f398

0: kd>
```

4. Ознакомьтесь с помощью команды *dt* с содержимым структуры *_TOKEN*, по адресу, определенному в предыдущем пункте, запишите результаты в отчет.

```
Администратор: Командная строка - livekd.exe
0: kd> dt _token 0xd650e820
nt!_TOKEN
+0x000 TokenSource      : _TOKEN_SOURCE
+0x010 TokenId          : _LUID
+0x018 AuthenticationId : _LUID
+0x020 ParentTokenId    : _LUID
+0x028 ExpirationTime   : _LARGE_INTEGER 0x7fffffff'ffffffff
+0x030 TokenLock        : 0x86713730 _ERESOURCE
+0x034 ModifiedId       : _LUID
+0x040 Privileges        : _SEP_TOKEN_PRIVILEGES
+0x058 AuditPolicy       : _SEP_AUDIT_POLICY
+0x074 SessionId        : 1
+0x078 UserAndGroupCount : 0xf
+0x07c RestrictedSidCount : 1
+0x080 VariableLength   : 0x210
+0x084 DynamicCharged   : 0x400
+0x088 DynamicAvailable : 0
+0x08c DefaultOwnerIndex : 0
+0x090 UserAndGroups     : 0xd650e9fc _SID_AND_ATTRIBUTES
+0x094 RestrictedSids    : 0xd650ea74 _SID_AND_ATTRIBUTES
+0x098 PrimaryGroup      : 0xe7970078 Void
+0x09c DynamicPart       : 0xe7970078 -> 0x501
+0x0a0 DefaultDacl       : 0xe7970094 _ACL
+0x0a4 TokenType         : 1 ( TokenPrimary )
+0x0a8 ImpersonationLevel : 0 ( SecurityAnonymous )
+0x0ac TokenFlags        : 0xa50
+0x0b0 TokenInUse        : 0x1 ''
+0x0b4 IntegrityLevelIndex : 0xe
+0x0b8 MandatoryPolicy   : 3
+0x0bc LogonSession      : 0xbd0ebbc0 _SEP_LOGON_SESSION_REFERENCES
+0x0c0 OriginatingLogonSession : _LUID
+0x0c8 SidHash           : _SID_AND_ATTRIBUTES_HASH
+0x150 RestrictedSidHash : _SID_AND_ATTRIBUTES_HASH
+0x1d8 pSecurityAttributes : 0x919c35c8 _AUTHZBASEP_SECURITY_ATTRIBUTES_INFORMATION
+0x1dc VariablePart      : 0xd650ea7c
0: kd>
```

5. SID учетной записи пользователя-владельца маркера и групп, в которые он входит, хранятся по адресу в поле **UserAndGroups**. SID представляет собой уникальное значение переменной длины, используемое в операционных системах Windows для идентификации участника безопасности или группы безопасности. Чтобы его прочесть снова воспользуемся командой *dt*. Запишите результаты своих действий в отчет.

```
Администратор: Командная строка - livekd.exe
0: kd> dt _SID_AND_ATTRIBUTES 0xd650e9fc
nt!_SID_AND_ATTRIBUTES
+0x000 Sid              : 0xd650ea7c Void
+0x004 Attributes       : 0x10
0: kd>
```

6. В первом поле структуры **_SID_AND_ATTRIBUTES** хранится адрес SID. Чтобы узнать какой SID расположен по данному адресу, можно воспользоваться следующей командой *!sid*. Запишите результаты своих действий в отчет.

```
Администратор: Командная строка - livekd.exe
0: kd> !sid 0xd650ea7c
SID is: S-1-5-21-2609833062-1600835590-1466217079-2004
0: kd>
```

7. Сравните информацию, выводимую командой *!token*, с данными, полученными с помощью утилиты *Process Explorer*.

8. Подготовьте итоговый отчет с развернутыми выводами по заданию.

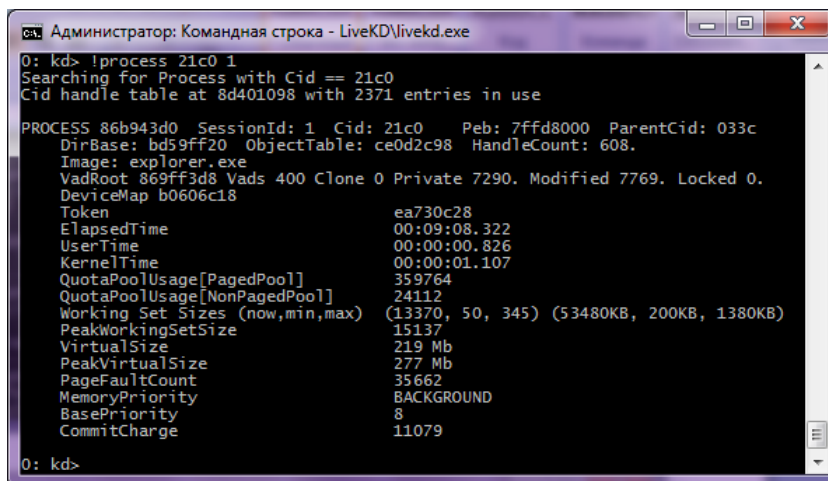
Задание 2.3. Исследовать дескриптор защиты (security descriptor).

Указания к выполнению.

1. Запустите командную строку от имени администратора, перейдите в каталог **c:\Tools\LiveKD** и запустите утилиту *LiveKd.exe*. В процессе запуска программы Вам могут быть заданы некоторые вопросы, касающиеся настроек запуска, отвечайте на них утвердительно.

2. Вызовите команду *!process 0 0*, для вывода краткого списка процессов системы, выберите процесс *explorer.exe* для дальнейшего изучения и запишите его идентификатор (тоже самое Вы можете выполнить с помощью утилиты *Process Explorer*). В нашем случае идентификатор процесса *explorer.exe* **21c0**. Запишите результаты выполнения данного пункта в отчет.

3. Выполните команду *!process <идентификатор процесса> 0*, в этом случае Вам отобразится подробная информация о процессе *explorer.exe*. Для дальнейшего изучения нам потребуется значение дескриптора объекта, для рассматриваемого примера это **86b943d0**. Повторите действия для выбранного процесса, ознакомьтесь с результатами и запишите их в отчет.



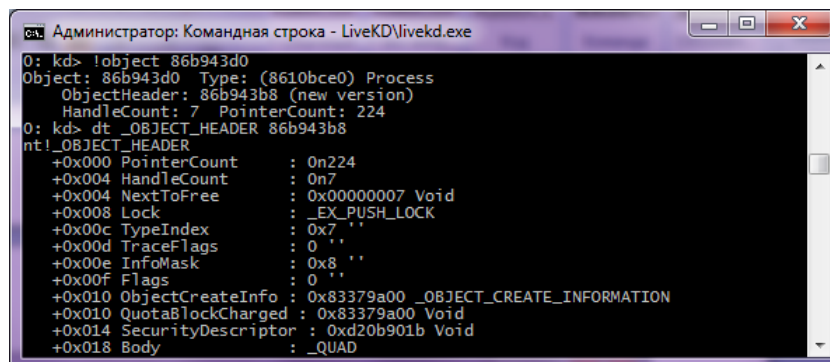
```
0: kd> !process 21c0 1
Searching for Process with Cid == 21c0
Cid handle table at 8d401098 with 2371 entries in use

PROCESS 86b943d0 SessionId: 1 Cid: 21c0 Peb: 7ffd8000 ParentCid: 033c
DirBase: bd59ff20 ObjectTable: ce0d2c98 HandleCount: 608.
Image: explorer.exe
VadRoot 869ff3d8 Vads 400 Clone 0 Private 7290. Modified 7769. Locked 0.
DeviceMap b0606c18
Token
ea730c28
ElapsedTime 00:09:08.322
UserTime 00:00:00.826
KernelTime 00:00:01.107
QuotaPoolUsage[PagedPool] 359764
QuotaPoolUsage[NonPagedPool] 24112
Working Set Sizes (now,min,max) (13370, 50, 345) (53480KB, 200KB, 1380KB)
PeakWorkingSetSize 15137
VirtualSize 219 Mb
PeakVirtualSize 277 Mb
PageFaultCount 35662
MemoryPriority BACKGROUND
BasePriority 8
CommitCharge 11079

0: kd>
```

4. Выполните команду *!process <идентификатор процесса> 0*, в этом случае Вам отобразится краткая информация о процессе *explorer.exe*. Для дальнейшего изучения нам потребуется значение дескриптора объекта, для рассматриваемого примера это **86b943d0**. Повторите действия для выбранного процесса, ознакомьтесь с результатами и запишите их в отчет.

5. С помощью команды *!object* определите адрес заголовка. Введите команду **dt _OBJECT_HEADER** и адрес поля заголовка объекта из вывода предыдущей команды для просмотра структуры данных заголовка объекта, включая значение указателя дескриптора защиты. Запишите результаты в отчет.



```
0: kd> !object 86b943d0
Object: 86b943d0 Type: (8610bce0) Process
ObjectHeader: 86b943b8 (new version)
HandleCount: 7 PointerCount: 224
0: kd> dt _OBJECT_HEADER 86b943b8
nt!_OBJECT_HEADER
+0x000 PointerCount : 0n224
+0x004 HandleCount : 0n7
+0x004 NextToFree : 0x00000007 Void
+0x008 Lock : _EX_PUSH_LOCK
+0x00c TypeIndex : 0x7 ''
+0x00d TraceFlags : 0 ''
+0x00e InfoMask : 0x8 ''
+0x00f Flags : 0 ''
+0x010 ObjectCreateInfo : 0x83379a00 _OBJECT_CREATE_INFORMATION
+0x010 QuotaBlockCharged : 0x83379a00 Void
+0x014 SecurityDescriptor : 0xd20b901b Void
+0x018 Body : _QUAD
```

6. Выполните просмотр дескриптора безопасности объекта с помощью команды *!sd*. Используйте значение поля **SecurityDescriptor**, полученное на прошлом шаге с очищенными тремя последними битами (маска -8).

Уровень доступа к объекту определяется в списке DACL маской доступа (поля Mask выделены на рисунке красным). В маске отдельные биты отвечают за определенные виды доступа. Выделяют *стандартные права доступа* (Standard Access Rights), применимые к большинству объектов, и *специфичные для объектов права доступа* (Object-Specific Access Rights). Описание стандартных прав доступа и соответствующих значений масок приведено в статье MSDN «Access Mask Format»¹. Описание прав доступа для файлов и каталогов имеется в статье MSDN «Access Mask»².

¹ [http://msdn.microsoft.com/en-us/library/windows/desktop/aa374896\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa374896(v=vs.85).aspx)

² [http://msdn.microsoft.com/en-us/library/windows/hardware/ff538834\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/hardware/ff538834(v=vs.85).aspx)


```
ca: Администратор: Командная строка - LiveKD\livekd.exe
0: kd> !sd 0xd20b901b & -8
-->Revision: 0x1
-->Sbz1 : 0x0
-->Control : 0x8814
SE_DACL_PRESENT
SE_SACL_PRESENT
SE_SACL_AUTO_INHERITED
SE_SELF_RELATIVE
-->Owner : S-1-5-21-2609833062-1600835590-1466217079-2004
-->Group : S-1-5-21-2609833062-1600835590-1466217079-513
-->Dacl :
-->Dacl : -->AclRevision: 0x2
-->Dacl : -->Sbz1 : 0x0
-->Dacl : -->AclSize : 0x68
-->Dacl : -->AceCount : 0x3
-->Dacl : -->Sbz2 : 0x0
-->Dacl : -->Ace[0]: -->AceType: ACCESS_ALLOWED_ACE_TYPE
-->Dacl : -->Ace[0]: -->AceFlags: 0x0
-->Dacl : -->Ace[0]: -->AceSize: 0x28
-->Dacl : -->Ace[0]: -->Mask : 0x001fffff
-->Dacl : -->Ace[0]: -->SID: S-1-5-21-2609833062-1600835590-1466217079-2004

-->Dacl : -->Ace[1]: -->AceType: ACCESS_ALLOWED_ACE_TYPE
-->Dacl : -->Ace[1]: -->AceFlags: 0x0
-->Dacl : -->Ace[1]: -->AceSize: 0x20
-->Dacl : -->Ace[1]: -->Mask : 0x00100001
-->Dacl : -->Ace[1]: -->SID: S-1-5-0-79882

-->Dacl : -->Ace[2]: -->AceType: ACCESS_ALLOWED_ACE_TYPE
-->Dacl : -->Ace[2]: -->AceFlags: 0x0
-->Dacl : -->Ace[2]: -->AceSize: 0x18
-->Dacl : -->Ace[2]: -->Mask : 0x00100000
-->Dacl : -->Ace[2]: -->SID: S-1-5-18

-->Sacl :
-->Sacl : -->AclRevision: 0x2
-->Sacl : -->Sbz1 : 0x0
-->Sacl : -->AclSize : 0x1c
-->Sacl : -->AceCount : 0x1
-->Sacl : -->Sbz2 : 0x0
-->Sacl : -->Ace[0]: -->AceType: SYSTEM_MANDATORY_LABEL_ACE_TYPE
-->Sacl : -->Ace[0]: -->AceFlags: 0x0
-->Sacl : -->Ace[0]: -->AceSize: 0x14
-->Sacl : -->Ace[0]: -->Mask : 0x00000003
-->Sacl : -->Ace[0]: -->SID: S-1-16-8192

0: kd>
```

Для представленного примера дескриптор защиты содержит три элемента ACE типа «доступ разрешен», а также один элемент SACL, используемый для аудита доступа к объекту. Проанализируйте элементы ACE и их маски доступа к объекту для своего примера и сделайте в отчете их расшифровку.

7. Подготовьте итоговый отчет с развернутыми выводами по заданию.