Министерство образования и науки Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

—

Институт компьютерных наук и кибербезопасности

ЛАБОРАТОРНАЯ РАБОТА № 1

«Настройки безопасности пользователей в ОС Windows»

1. по дисциплине «Безопасность современных информационных технологий»
2. Выполнил
3. студент гр. 5151004/10101 Веремейчук Я.Ю.

<подпись>

1. Преподаватель
2. асс. преподавателя Соловей Р.С.

<подпись>

1. Санкт-Петербург
2. 2024
3. Цель работы

Изучить существующие настройки безопасности пользователей в ОС Windows и возможности управления пользователями с использованием Windows API.

1. Задача

Реализовать программу для управления учетными записями и контролем доступа в ОС Windows, использующую возможности Windows API.

1. Теоретические исследования

Безопасность операционной системы Windows обеспечивает множество компонентов: SRM, LSASS, SAM, Active Directory, пакеты аутентификации, Winlogon, LogonUI и другие.

* 1. Привилегии

Привилегии являются правом выполнять под той или иной учетной записью конкретную, связанную с системой операцию, например выключение компьютера или изменение системного времени. Право учетной записи разрешает или запрещает той учетной записи, которой оно назначено, выполнять конкретный тип входа в систему, например локальный или интерактивный.

Количество привилегий, определяемых операционной системой, со временем существенно увеличилось. В отличие от прав пользователя, которые задаются LSA в одном месте, различные привилегии определяются разными компонентами, которые их же и применяют. Например, привилегия отладки, позволяющая процессу обходить проверки безопасности при открытии дескриптора другого  
процесса с помощью API-функции Windows OpenProcess, проверяется дис-  
петчером процесса. В табл. 6.9 представлен полный список привилегий и дано  
описание того, как и когда они проверяются системными компонентами.  
Когда компоненту нужно проверить маркер с целью определения наличия  
привилегии, им используются API-функции PrivilegeCheck или LsaEnumerate-  
AccountRights при работе в пользовательском режиме и SeSinglePrivilegeCheck  
или SePrivilegeCheck при работе в режиме ядра. API-функции, связанные  
с привилегиями, ничего не знают о существовании прав учетных записей, а вот  
API-функции, связанные с правами учетных записей, о наличии привилегий  
осведомлены.  
В отличие от прав учетных записей, привилегии могут быть включены или  
выключены. Чтобы проверка привилегии прошла успешно, она должна присут-  
ствовать в указанном маркере и быть включена. В основу этой схемы положена  
идея о том, что привилегии должны быть включены только при их востребо-  
ванности, чтобы процесс не мог по недосмотру выполнить привилегированную  
небезопасную операцию.

Таблица 1 – Привилегии

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Таблица 2 – Привилегии

Изображение выглядит как текст, Шрифт, снимок экрана, Параллельный

Автоматически созданное описание

Таблица 3 – Привилегии

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Таблица 4 – Привилегии

Изображение выглядит как текст, Шрифт, снимок экрана, число

Автоматически созданное описание

Таблица 5 – Привилегии

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

* 1. SID

Вместо использования имен, для идентификации всего, что производит в системе действия, Windows использует идентификаторы безопасности — security identifiers (SID). SID-идентификаторы имеются у пользователей, а также у локальных и доменных групп, у локальных компьютеров, доменов, участников доменных групп и служб. SID представляет собой числовое значение переменной длины, состоящее из номера версии SID-структуры, 48-разрядное значение идентификатора полномочий и переменное количество 32-разрядных кодов значений подчиненных полномочий или относительных идентификаторов — relative identifier (RID).

Пример: S-1-5-21-1463437245-1224812800-863842198-1128

S - префикс

1 - номер версии

5 - значение идентификатора полномочий

а затем следуют четыре значения подчиненных полномочий плюс один RID (1128).

1. Ход работы

В рамках лабораторной работы была реализована программа, управляющая учетными записями пользователей и группами.

В программе осуществляется динамическая подгрузка библиотек **Advapi32** и **Netapi32**, которые предоставляют возможность обращаться к сущностям системы безопасности и изменять их в ОС Windows.

Есть несколько способов подключения динамической библиотеки к проекту: неявное и явное подключение. При неявном необходимо передать линкеру имя библиотеки импорта, чтобы он использовал ее в процессе сборки. Но был выбран явный способ: для этого используется функция **LoadLibrary()**, которая получает имя библиотеки и возвращает ее дескриптор. Дескриптор необходимо сохранить в переменной, так как он будет использоваться всеми остальными функциями, предназначенными для работы с DLL.

netapi32 = LoadLibrary(L"C:\\Windows\\System32\\netapi32.dll");

advapi32 = LoadLibrary(L"C:\\Windows\\System32\\Advapi32.dll");

Затем при помощи GetProcAddress получим адрес исходной функции в dll и создадим переменную такого типа, привязав к ней адрес. Например:

(FARPROC&)DllLsaOpenPolicy=GetProcAddress(advapi32,"LsaOpenPolicy");

Также при завершении работы программы необходимо освободить память.

FreeLibrary(netapi32);

FreeLibrary(advapi32);

Функции **Netapi32** предоставляют информацию (SID, имена, привилегии) о глобальных/локальных группах, учётных записях пользователей, позволяют редактировать эту информацию. Функции **Advapi32** включает функции для создания, удаления, изменения учетных записей пользователей и групп, а также управления их правами доступа.

В процессе работы программа обращается к базе данных **LSA** (Local Security Authority), она предназначена для управления локальной политикой безопасности системы, аудита, авторизации, входа пользователей в систему, хранения приватных данных. Обращение к **LSA** происходит посредством открытия дескриптора объекта Policy (функция **LsaOpenPolicy()**), использования полученного дескриптора для доступа/изменения прав, предоставленных учётным записям или группам, закрытия дескриптора, не нуждающегося в дальнейшем использовании (функции для работы с **LSA** реализованы в библиотеке **Advapi32**).

Таблица 6 – Функции, которые были использованы в программе

|  |  |
| --- | --- |
| Функция | Назначение |
| advapi32 | |
| ConvertSidToStringSidW | Функция преобразует идентификатор безопасности (SID) в строковый формат, подходящий для отображения, хранения или передачи. |
| ConvertStringSidToSidW | Функция преобразует идентификатор безопасности строкового формата (SID) в действительный функциональный SID. Вы можете использовать эту функцию для получения SID, который функция ConvertSidToStringSid преобразовала в строковый формат. |
| LsaOpenPolicy | Функция открывает дескриптор объекта [политики](https://docs.microsoft.com/en-us/windows/desktop/SecMgmt/policy-object) в локальной или удаленной системе. |
| LsaEnumerateAccountRights | Функция перечисляет привилегии, назначенные учетной записи. |
| LsaNtStatusToWinError | Функция преобразует код NTSTATUS, возвращаемый функцией LSA, в код ошибки Windows. |
| LsaRemoveAccountRights | Функция удаляет одну или несколько [привилегий](https://docs.microsoft.com/en-us/windows/desktop/SecGloss/p-gly) из учетной записи. Вы можете указать привилегии, которые нужно удалить, или вы можете установить флаг для удаления всех привилегий. При удалении всех привилегий функция удаляет учетную запись. Если вы укажете привилегии, не принадлежащие учетной записи, функция их игнорирует. |
| LsaAddAccountRights | Функция назначает одну или несколько [привилегий](https://docs.microsoft.com/en-us/windows/desktop/SecGloss/p-gly) учетной записи. Если учетная запись не существует, LsaAddAccountRights создает ее. |
| LookupAccountNameW | Функция принимает в качестве входных данных имя системы и учетной записи. Он извлекает идентификатор безопасности (SID) для учетной записи и имя домена, в котором была обнаружена учетная запись. |
| netapi32 | |
| NetApiBufferFree | Функция освобождает память, которую [выделяет](https://docs.microsoft.com/en-us/windows/desktop/api/lmapibuf/nf-lmapibuf-netapibufferallocate) функция. Приложения также должны вызывать NetApiBufferFree, чтобы освободить память, которую другие функции управления сетью используют внутри для возврата информации. |
| NetUserAdd | Функция добавляет учетную запись пользователя и назначает пароль и уровень привилегий. |
| NetUserDel | Функция удаляет учетную запись пользователя с сервера. |
| NetUserGetLocalGroups | Функция извлекает список локальных групп, к которым принадлежит указанный пользователь. |
| NetLocalGroupDel | Функция удаляет учетную запись локальной группы и всех ее членов из базы данных безопасности, которая является базой данных диспетчера учетных записей безопасности (SAM) или, в случае контроллеров домена, Active Directory. |
| NetLocalGroupAdd | Функция создает локальную группу в базе данных безопасности, которая является базой данных диспетчера учетных записей безопасности (SAM) или, в случае контроллеров домена, Active Directory. |
| NetLocalGroupAddMembers | Функция добавляет членство одной или нескольких существующих учетных записей пользователей или учетных записей глобальной группы к существующей локальной группе. Функция не изменяет статус членства пользователей или глобальных групп, которые в настоящее время являются членами локальной группыю |
| NetLocalGroupEnum | Функция возвращает информацию о каждой учетной записи локальной группы на указанном сервере. |
| NetUserEnum | Функция извлекает информацию обо всех учетных записях пользователей на сервере. |
| NetUserChangePassword | Функция изменяет пароль пользователя для указанного сетевого сервера или домена. |
| NetLocalGroupDelMembers | Функция удаляет одного или нескольких членов из существующей локальной группы. Члены локальной группы могут быть пользователями или глобальными группами. |

Изображение выглядит как текст, снимок экрана, меню, Шрифт

Автоматически созданное описание

Рисунок 1 – Вывод списка пользователей

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 2 – Добавление пользователя

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 3 – Удаление пользователя

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 4 – Смена пароля

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 5 – Добавление привилегии

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

Рисунок 6 – Удаление привилегии

Изображение выглядит как текст, снимок экрана, меню, Шрифт

Автоматически созданное описание

Рисунок 7 – Список групп и привилегий

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 8 – Добавление группы

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 9 – Удаление группы

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 10 – Добавление пользователя в группу

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 11 – Удаление пользователя из группы

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 12 – Добавление привилегии

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Рисунок 13 – Удаление привилегий

1. Контрольные вопросы
2. Для чего нужны и как работают привилегии «Взятие во владение», «Архивирование файлов и каталогов», «Восстановление файлов и каталогов»?

*«Взятие во владение»* (**SE\_TAKE\_OWNERSHIP\_NAME**) позволяет владеть файлами и другими объектами. Обычно, можно получить право собственности на объект, только если его текущий владелец выдал разрешение на это. Но пользователь, обладающий данной привилегией, может владеть объектом без разрешения текущего владельца. По умолчанию, данная привилегия назначается только встроенной группе «Администраторы». Администраторы обычно используют данную привилегию для передачи и переназначения владения ресурсами, когда их нынешний владелец больше не доступен.

*«Архивирование файлов и каталогов»*. Требуется для выполнения операций резервного копирования. Эта привилегия приводит к тому, что система предоставляет всем доступом на чтение любому файлу независимо от списка управления доступом (**ACL**), указанного для файла. Любой запрос доступа, отличный от чтения, по-прежнему оценивается с помощью **ACL**. Эта привилегия требуется функциями **RegSaveKey** и **RegSaveKeyEx**. При наличии этого права доступа предоставляются следующие права доступа:

* **READ\_CONTROL**
* **ACCESS\_SYSTEM\_SECURITY**
* **FILE\_GENERIC\_READ**
* **FILE\_TRAVERSE**

Право пользователя: резервное копирование файлов и каталогов.

Если файл находится на съемных дисках и включен параметр "Аудит съемных служба хранилища", **SE\_SECURITY\_NAME** требуется **ACCESS\_SYSTEM\_SECURITY**.

Привилегия *«Восстановление файлов и каталогов»* (**SE\_RESTORE\_NAME**) требуется для выполнения операций восстановления. Эта привилегия приводит к тому, что система предоставляет все возможности управления доступом на запись в любой файл независимо от **ACL**, указанного для файла. Любой запрос доступа, отличный от записи, по-прежнему оценивается с помощью **ACL**. Кроме того, эта привилегия позволяет задать допустимый идентификатор безопасности пользователя или группы в качестве владельца файла. Эта привилегия требуется функцией **RegLoadKey** . При наличии этого права доступа предоставляются следующие права доступа:

* **WRITE\_DAC**
* **WRITE\_OWNER**
* **ACCESS\_SYSTEM\_SECURITY**
* **FILE\_GENERIC\_WRITE**
* **FILE\_ADD\_FILE**
* **FILE\_ADD\_SUBDIRECTORY**
* **DELETE**

Право пользователя: восстановление файлов и каталогов.

Если файл находится на съемных дисках и включен параметр "Аудит съемных служба хранилища", **SE\_SECURITY\_NAME** требуется **ACCESS\_SYSTEM\_SECURITY**.

1. Какой привилегией в системе должен обладать пользователь для того, чтобы он мог выполнять отладку процессов?

**SeDebugPrivilege** (SE\_DEBUG\_NAME) используется для отладки и

настройки памяти процесса, принадлежащего другой учетной записи.

1. Какие еще факторы (кроме прав доступа, привилегий, владельца) влияют на доступ субъектов к объектам в ОС Windows?

Группы безопасности (администраторы, пользователи, гости и т.д.), групповые политики (управление настройками безопасности на множестве компьютеров), политики безопасности (ОС Windows имеет механизмы управления безопасностью, которые определяют правила и ограничения для доступа к ресурсам системы. Политики безопасности могут устанавливать ограничения на уровне домена, локальной системы или отдельных объектов), разрешения **NTFS**, процесс контроля учетных записей (**UAC**): уровни целостности (измерения доверия).

1. Почему учетная запись Гостя обычно отключена по умолчанию?

Гостевая учетная запись позволяет случайным или разовым пользователям, у которых нет учетной записи на компьютере, временно войти на локальный сервер или клиентский компьютер с ограниченными правами пользователя. По умолчанию учетная запись гостя отключена и имеет пустой пароль, что делает ее уязвимой для несанкционированного доступа. Так как учетная запись гостя может предоставлять анонимный доступ, она считается угрозой безопасности. По этой причине рекомендуется оставить учетную запись гостя отключенной, если только ее использование не требуется.

1. Что такое RID?

**Relative Identifier** (RID) – конечная часть **SID**, уникальное число, которое определяет субъект безопасности и присваивается при его создании. Однозначно идентифицирует учетную запись или группу внутри домена.

1. Выводы

В ходе работы были изучены существующие настройки безопасности пользователей в ОС Windows и возможности управления пользователями с использованием Windows API, а также была реализована программа для управления учетными записями и контролем доступа в ОС Windows, использующая возможности Windows API.