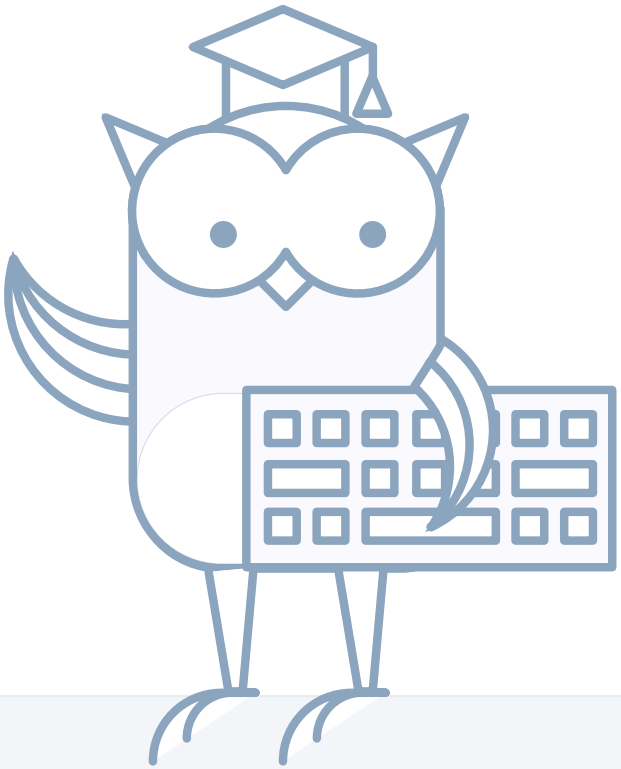
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

Структура операционной системы Windows

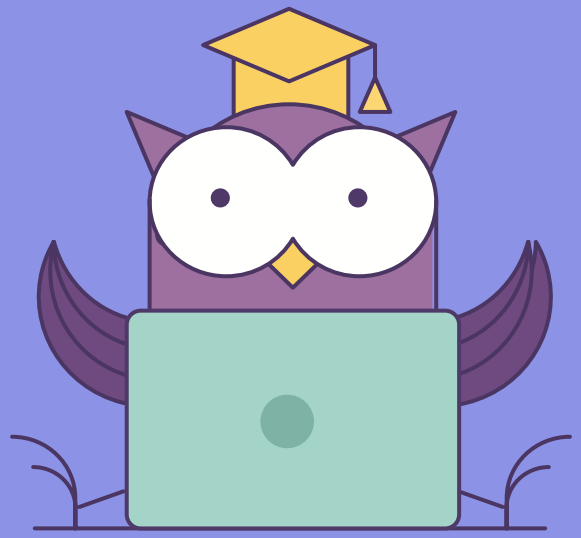
Основные механизмы разграничения доступа.

Часть 2



Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

- Операционная система Windows
  - Идентификаторы безопасности
  - Разграничение доступа к ресурсам
  - Локальное выполнение команд
- Практика:
  - PsExec
  - WMI
  - Powershell

01

Идентификаторы безопасности

Идентификатор безопасности

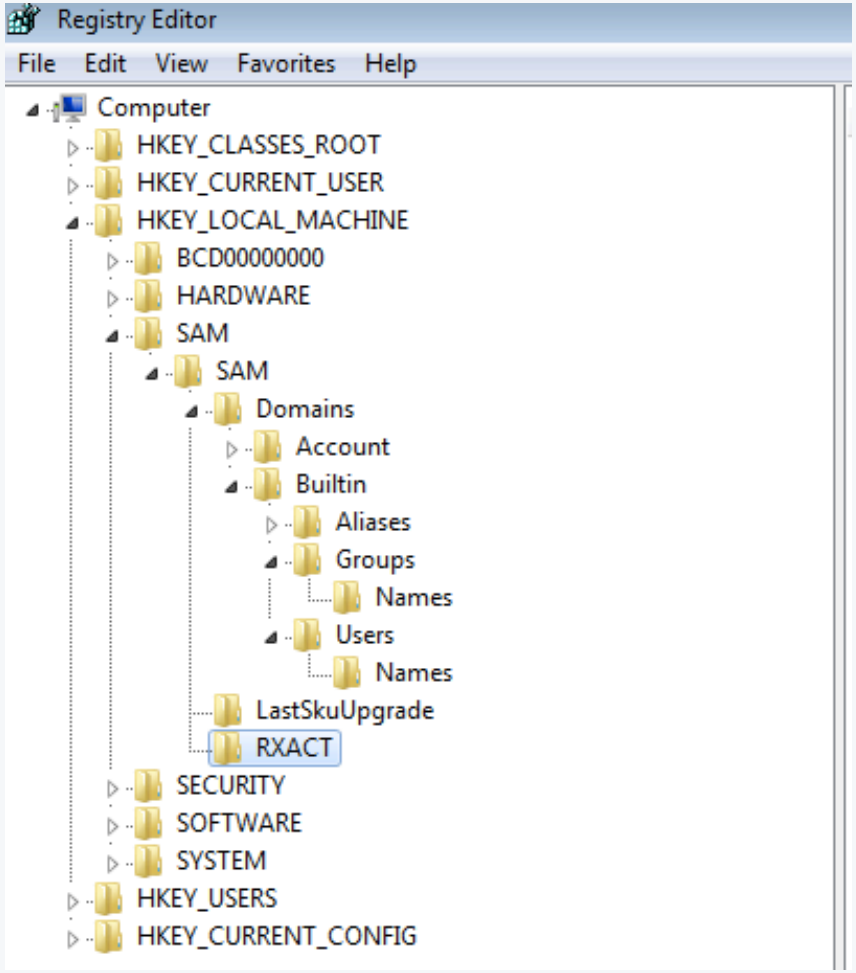
- Информация, которая идентифицирует учетную запись внутри операционной системы
- Может использоваться для идентификации:
  - Домена
  - Компьютера
  - Группы
  - Пользователя
- Создание SID производится при создании учетной записи
- Используется при предоставлении доступа к ресурсам системы

- Формат идентификатора:
  - S-R-IA-SA-SA-RID

S	**Идентификатор, который обозначает, что последовательность является идентификатором безопасности**
R	Номер редакции (Операционная система создает версию 1)
IA	Источник выдачи или создания. Операционная система использует значение 5 (могут быть и другие)
SA	Уполномоченный центр. Определяет группы и функции. Генерируется выдающей системой.
SA	
RID	Относительный идентификатор. Уникальное число, которое присваивает создающая система. (Центр)

Какая подсистема отвечает за идентификаторы?

- Одна из задач подсистемы SAM заключается в том, чтобы производить трансляцию имеет учетных записей в SID
- Данные обрабатываемые системой можно найти в ветке реестра:
  - HKEY_LOCAL_MACHINE\SAM\SAM
- Доступ к ветке разрешен только пользователю SYSTEM(По-умолчанию)
- Реализация находится в samsrv.dll
- Доступ к функция можно получить через samlib.dll



01

Практика

Psexec

Полезные команды

Задача: Получить доступ к базе SAM.

Задача: Получить хэши паролей без использования системных прав.

Чтобы выполнить практическое упражнение необходимо:

- Работающая операционная система Windows
- Пакет программ SysInternals

Полезные команды:

- psexec.exe -s -i program.exe

02

Практика

MIMI и KIWI

Токен и имперсонализация

- Любой процесс и поток в операционной системе имеет свой токен - идентификатор, который может позволить выполнять отдельные команды или получать доступ к защищаемому операционной системой объекту.
- **Токен состоит из:**
  - Идентификатор безопасности SID аккаунта пользователя
  - SID группы, к которой относится пользователь
  - Logon SID, который идентифицирует текущую сессию
  - Список привилегий, которыми обладает пользователь или его группа
  - SID владельца
  - И некоторые другие данные.

Практика

Задача:

- Изучить возможности утилиты mimikatz
- Провести вывод всех возможных в системе токенов
- Провести имперсонализацию
- Провести поиск информации в vault

Полезные команды:

- cmd.exe
- mimikatz.exe

02

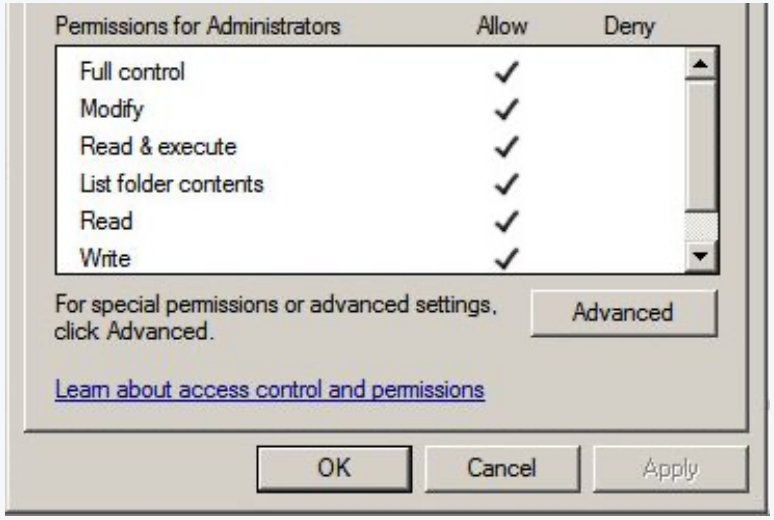
Разграничение доступа к ресурсам

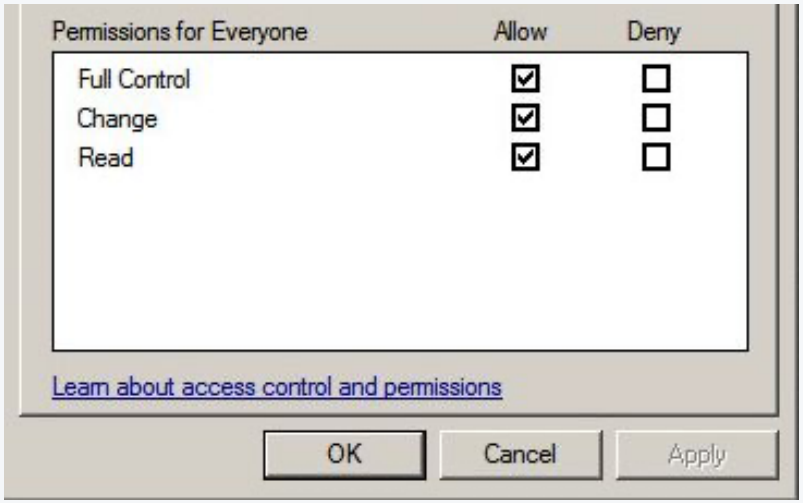
Доступ к ресурсам

- Один из способов ограничения - файловая система

- Стандартной файловой системой является NTFS
- Разрешения на доступ в NTFS применяются ко всем файлам и папкам
- По-умолчанию права одинаковы для дочерних элементов

- Отдельный механизм разграничения доступа применяется для директорий с общим доступом
- Наследование так же применяется от родительского объекта к дочернему





03

Локальное выполнение команд

Выполнение команд

- Операционная система по-умолчанию включает в себя ряд компонентов, которые могут выполнять код:
  - WMI - инструментарий управления Windows
  - PowerShell
  - WScript
  - JScript
  - VBScript

03

WMI, POWERSHELL, etc.

Практика

Задание:

- Собрать информацию о операционной системе
- Собрать информацию о пользователях
  - Общая информация
  - Привелегии
- Получить список переменных окружения
- Собрать общую информацию о запущенных процессах

Полезные команды:

systeminfo	tasklist /v
wmic qfe	net start
wmic os get osarchitecture	sc query
Set Get-ChildItem Env:| ft Key,Value	Get-ChildItem -path Registry::HKEY_LOCAL_MACHINE\SOFTWARE | ft Name
wmic logicaldisk get caption	Schticks /query /fo LIST 2>null
net accounts (user)	

Колесников Александр

Спасибо
за внимание!