МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра «Вычислительные системы и технологии»

ОТЧЕТ

по лабораторной работе

по дисциплине «Программное обеспечение

вычислительных сетей»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Кочешков А. А.

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Попов В. А.

17-В-1

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород

**2020**

1. **Ознакомится с составом встроенных учетных записей и групп компьютера.**

Зайдем под учетной записью локального администратора и рассмотрим список пользователей и групп в “Управление компьютером” -> “Локальные пользователи и группы”

1. **Изучить свойства локальных учетных записей Администратор и Гость**

Рассмотрим свойства учетных записей:

Администратор – учетная запись, имеющая SID S – 1 – 5 – поддомен – 500. Она имеет полный доступ к файлам, службам и прочим ресурсом компьютера, может создавать пользователей и формировать их разрешения, а также редактировать их в любое время. Саму учетную запись администратора невозможно удалить, а также невозможно удалить из группы “Администраторы” (куда учетная запись попадает автоматически), но имеется возможность отключить её.

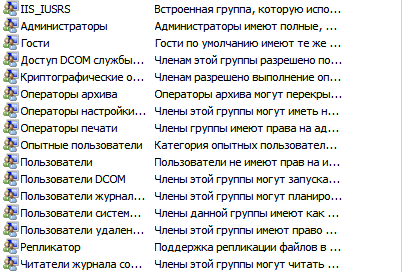
Гость – учетная запись, имеющая SID S – 1 – 5 – 32 – 546. Она позволяет временно и анонимно входить в компьютер с ограниченными правами (что предоставляет угрозу безопасности). Для неё по умолчанию отсутствует пароль. Находиться в группе гостей и учетная запись, находящаяся в группе “Администратор”, может вносить изменения в группу гостей.



1. **Изучить назначения и возможности локальных групп компьютера – члена домена.**

Рассмотрим группы компьютера:

1. IIS\_IUSRS – группа учетных записей рабочих процессов IIS. Имеет доступ ко всем файлам и системным ресурсам
2. Администраторы – группа учетных записей, имеющая полный доступ к компьютеру
3. Гости – группа учетных записей, имеющая ограниченные права доступа
4. Доступ DCOM службы сертификации – группа учетных записей, имеющая доступ к центрам сертификации организации
5. Криптографические операторы – группа безопасности, позволяющая выполнять криптографический операции
6. Операторы архива – группа учетных записей, имеющая права на архивацию и восстановление всех файлов, вне зависимости от того, разрешен ли им доступ к этим файлам или нет
7. Операторы настройки сети – группа учетных записей, имеющая права на настройку сетевых компонентов
8. Операторы печати – группа учетных записей, имеющая права создавать, удалять и совместно использовать принтеры, подключенные к контроллеру домену
9. Опытные пользователя – группа учетных записей, позволяющая выполнять несертифицированные приложения
10. Пользователи – группа учетных записей, предоставляющая безопасную среду для выполнения программ
11. Пользователи DCOM – группа учетных записей, предоставляющая работу с DCOM объектами
12. Пользователя журналов производительности – группа учетных записей, позволяющая работать с счетчиками производительности, журналами и оповещениями
13. Пользователи системного мониторинга - группа учетных записей, позволяющая отслеживать счетчики производительности.
14. Пользователи удаленного рабочего стола - группа учетных записей, предоставляющая удаленную работу с сервером
15. Репликатор - группа учетных записей, поддерживающая репликацию файлов в домене
16. Читатели журнала событий - группа учетных записей, позволяющая рассматривать журналы событий



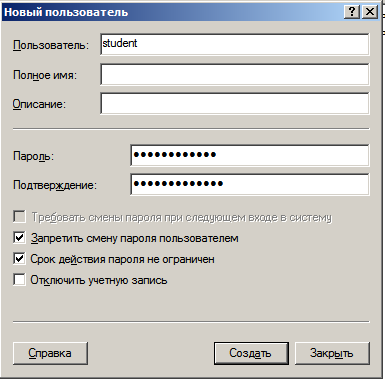
1. **Вывод**

В данном пункте был изучен состав встроенных локальных учетных записей и групп компьютера, рассмотрены их назначение и возможности.

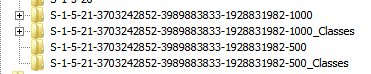
1. **Создать локальную учетную запись student и определить её свойства**
2. **Зарегистрироваться с помощью учетной записи “student”, изучить свойство и расположение профиля пользователя.**

В “Управление компьютером” –> “Локальные пользователи группы” –> “Пользователи” создадим нового пользователя student и установим пароль Password1234. Не ограничим срок действия пароля и запретим смену пароля пользователем.

После входа в учетную запись был создан профиль со стандартными папками. Все эти папки были описаны в предыдущих лабораторных.

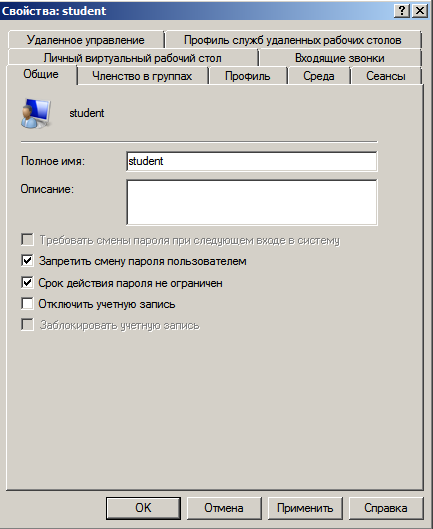


В реестре были созданы разделы нового пользователя. Нашей учетной записи был присвоен SID S – 1 – 5 – 21 - 3703242852 – 3989883833 – 1928831982 - 1000



Рассмотрим свойства учетной записи:

1. Общие – параметры, отвечающие за изменение имени пользователя, за добавления к нему описания, за отключения учетной записи, за запрет смены пароля и за срок действия пароля
2. Членство в группах – параметр, отвечающие за нахождения профиля в определенных группах
3. Профиль – параметры, предоставляющие выбор пути профиля и домашней папки, а также сценарий входа
4. Среда – параметры, позволяющие назначить запуск программы и подключение дисков и принтера при входе.
5. Сеансы – параметры, использующиеся для установки тайм-аутов и повторного подключения служб удаленных рабочих столов, а также позволяющая решать, что будет при превышении лимита и будет ли разрешено переподключение клиента
6. Личный виртуальный стол – параметр, позволяющий пользователю назначать отдельную виртуальную машину в качестве личного виртуального рабочего стола.
7. Входящие звонки – параметр, отвечающий за доступ к сети, связь с сервером и также назначения статического IP и маршрутизации
8. Удаленное управление – параметры, отвечающие за удаленное управление служб удаленных рабочих столов.
9. Профиль служб удаленных рабочих столов – параметры, отвечающие за пользовательский профиль служб удаленных рабочих столов

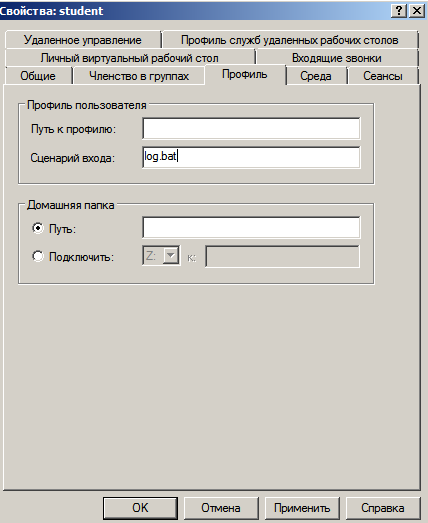


1. **Создать и применить скрипт регистрации пользователя**

Был создан bat-файл со скриптом, который записывал информацию о последнем входе (Дату можно узнать по информации об дате изменения файла).

****

После этот bat был отправлен в папку пользователя student и в настройках пользователя для student указали этот файл, как сценарий входа.

****

После зашли в student и проверили работу bat - файла

****

1. **Вывод**

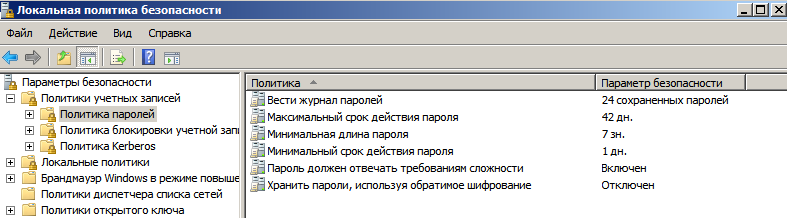
Была создана учетная запись student, изучены её свойства, домашний каталог, применен сценарий входа.

1. **С помощью консоли управления локальными параметрами безопасности определить следующие компоненты локальной политики по отношению к пользователям и их стандартные настройки: политики учетных записей, назначение прав пользователей, параметры безопасности.**
2. **Рассмотреть политики учетных записей и параметры безопасности, установленные по умолчанию.**

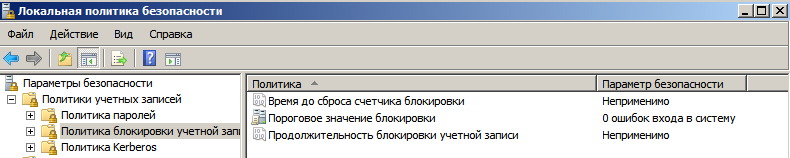
В политике учетных записей имеется 3 подраздела (Политика паролей, политика блокировки учетной записи и политика Kerberos).

Рассмотрим политику учетных записей и её значения по умолчанию:

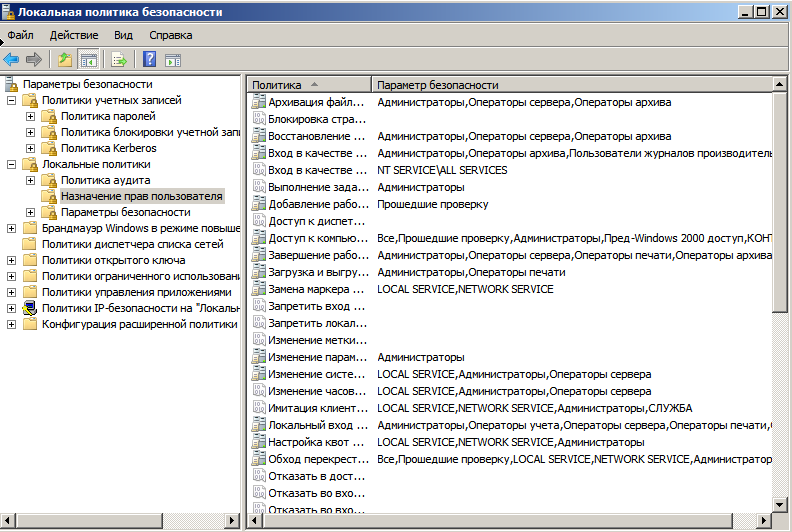
Политика паролей

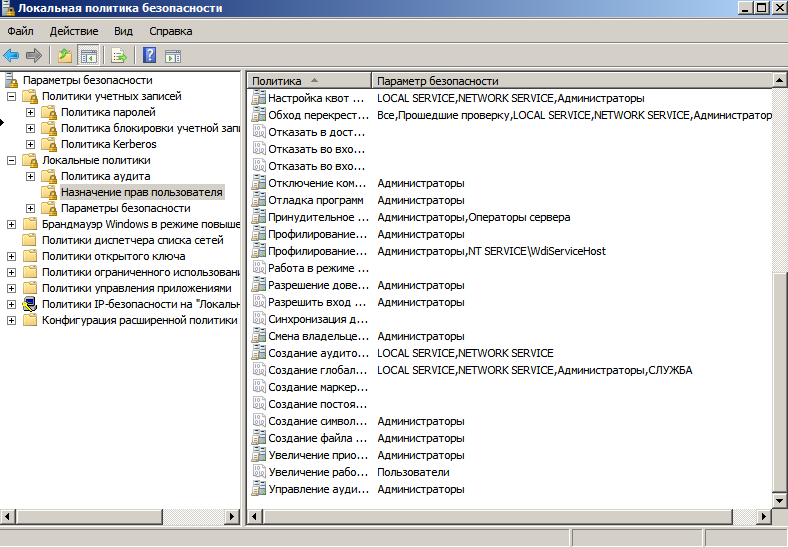
****

Политика блокировки учетной записи

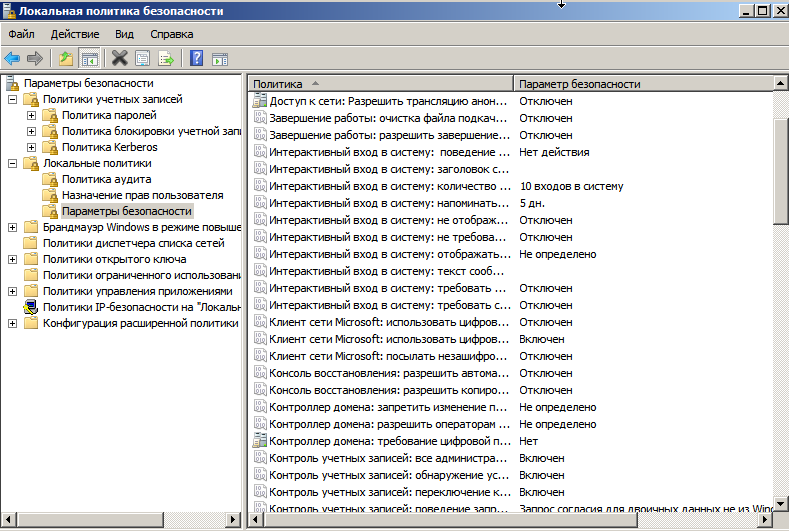
****

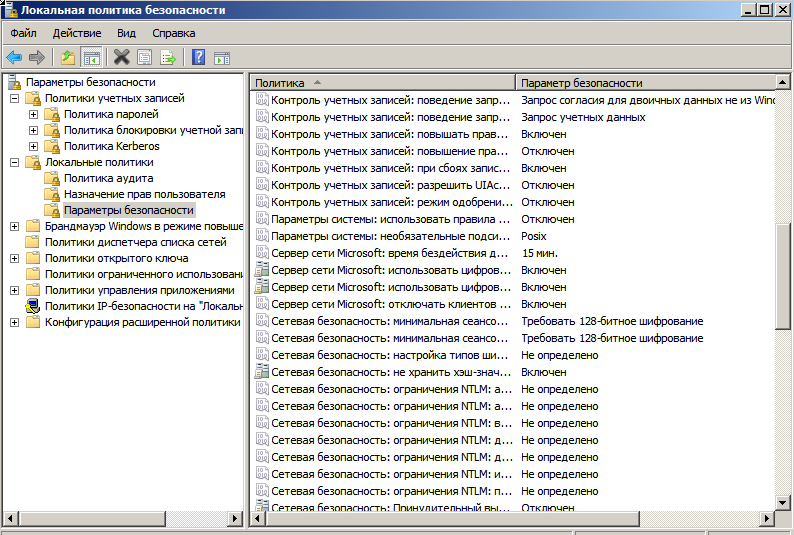
Рассмотрим локальную политику назначения прав пользователя и её значения по умолчанию:





Рассмотрим параметры безопасности и их значения по умолчанию (так как этих параметров слишком много, то рассмотрим лишь несколько):





1. **Изучить смысл и применение прав пользователей. Сформировать таблицу параметров прав пользователей в соответствии с группами**

Рассмотрим права пользователей в соответствии с группами

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Привилегии | Администраторы | Оператор архива | Оператор печати | Оператор сервера | Пользователи | Прошедшие проверку |
| Архивация файлов | + | + |  | + |  |  |
| Восстановление файлов | + | + |  | + |  |  |
| Вход в качестве пакетного задания |  | + |  |  |  |  |
| Выполнение задач по обслуживанию томов | + |  |  |  |  |  |
| Добавление рабочих станций к домену |  |  |  |  |  | + |
| Доступ компьютера к сети | + |  |  |  |  | + |
| Завершение работы системы | + | + | + | + |  |  |
| Загрузка и выгрузка драйверов устройств | + |  | + |  |  |  |
| Изменение параметров среды изготовителя | + |  |  |  |  |  |
| Изменение системного времени | + |  |  | + |  |  |
| Изменение часового пояса | + |  |  | + |  |  |
| Имитация клиента после проверки подлинности | + |  |  |  |  |  |
| Локальный вход в систему | + | + | + | + |  |  |
| Настройка квот памяти для процесса | + |  |  |  |  |  |
| Обход перекрестной проверки | + |  |  |  |  | + |
| Отключение компьютера от стыковочного узла | + |  |  |  |  |  |
| Отладка программ | + |  |  |  |  |  |
| Принудительное удаленное завершение работы | + |  |  | + |  |  |
| Профилирование одного процесса | + |  |  |  |  |  |
| Профилирование производительности системы | + |  |  |  |  |  |
| Разрешение доверия к учетным записям компьютеров и пользователей при делегировании | + |  |  |  |  |  |
| Разрешить вход в систему через службу удаленных рабочих столов | + |  |  |  |  |  |
| Смена владельцев файлов и других объектов | + |  |  |  |  |  |
| Создание аудитов безопасности |  |  |  |  |  |  |
| Создание глобальных объектов | + |  |  |  |  |  |
| Создание символических ссылок | + |  |  |  |  |  |
| Создание файла подкачки | + |  |  |  |  |  |
| Увеличение приоритета выполнения | + |  |  |  |  |  |
| Увеличение рабочего набора процесса |  |  |  |  | + |  |
| Управление аудитом и журналом безопасности | + |  |  |  |  |  |

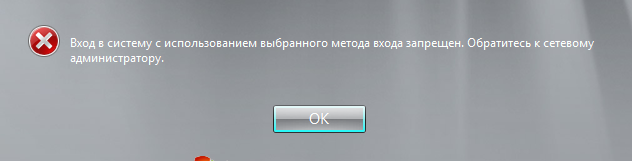
Как видим, Администраторы имеет почти все привилегии, а пользователь могут лишь увеличивать рабочий набор процесса. Также, например, операторы архива могут заниматься архивацией файлов, их восстановлением, завершением работы системы, локальным входом в систему и т.д. Операторы печати могут завершать работу системы, загружать и выгружать драйверы устройств, локально входить в систему. Операторы сервера могут заниматься архивацией файлов, их восстановлением, завершением работы системы, локальным входом в систему, изменением системного времени и часового пояса и т. д.

1. **Опробовать изменение прав по отношению к созданному пользователю**

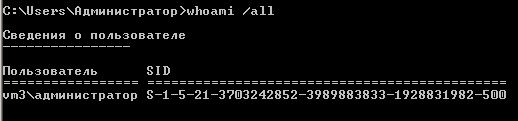
Попробуем в локальных политиках запретить пользователю student локальный вход.



После запрета, попытаемся войти в учетную запись. Заметим, что мы не смогли зайти в нее.

****

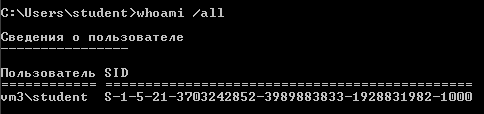
1. **С помощью команды «whoami /all» определить SID текущей учетной записи, вхождение в группы и права пользователя. Получить и сравнить эти свойства для локальных учетных записей администратора и пользователя.**



С помощью команды whoami /all мы смогли узнать SID, а также в каких группах находится пользователь и его привилегия.

Администратор находит в таких группах, как Все, Администраторы, Пользователи, Прошедшие проверку, Интерактивные, Консольные, Локальные, Проверка подлинности NTLM, Высокий обязательный уровень.

Также он имеет такие привилегии, как Настройка квот памяти для процесса, Управление аудитом и журналом безопасности, Смена владельцев файлов и других объектов, Загрузка и выгрузка драйверов устройств, Профилирование производительности системы, Изменение системного времени, Профилирование одного процесса, Увеличение приоритета выполнения, Создание файла подкачки, Архивация файлов и каталогов, Восстановление файлов и каталогов, Завершение работы системы, Отладка программ, Изменение параметров среды изготовителя, Обход перекрестной проверки, Принудительное удаленное завершение работы, Отключение компьютера от стыковочного узла, Выполнение задач по обслуживание томов, Имитация клиента после проверки подлинности, Создание глобальных объектов, Увеличение рабочего набора процесса, Изменение часового пояса, Создание символических ссылок.



Наш созданный пользователь student находится в таких группах, как Все, Пользователи, Интерактивные, Прошедшие проверку, Консольный вход, Локальные, Проверка подлинности HTLM, Средний обязательный уровень.

Также он имеет такие привилегии, как Обход перекрестной проверки и Увеличение рабочего набора процесса.

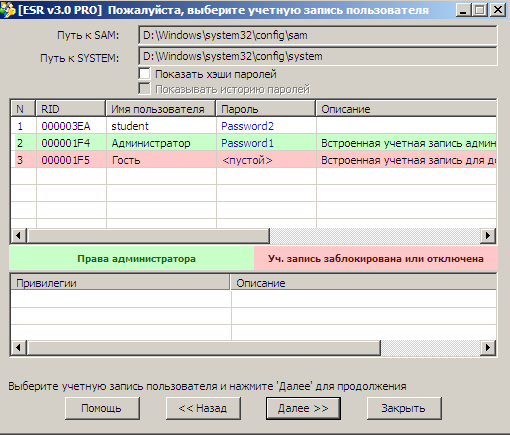
Как видим, Администратор имеет почти все права и привилегии, в отличии от того, какими правами обладает наш пользователь, ведь он имеет только стандартные права группы Пользователь.

1. **Вывод**

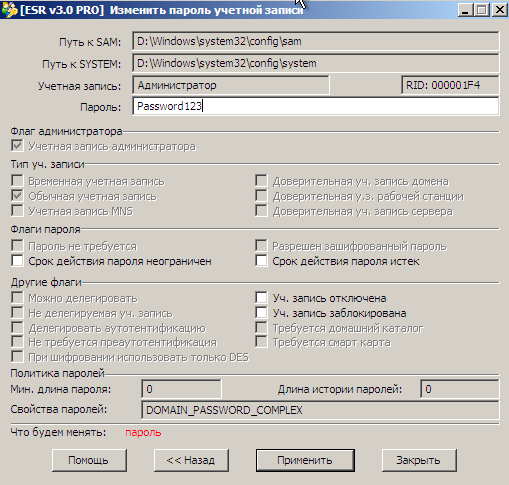
Были определены многие компоненты локальной политики и их стандартные настройки, изучены компоненты безопасности. Была сформирована таблица соответствия привилегий по основным группам, опробовано изменение прав по отношению к пользователю. С помощью команды whoami /all были изучены свойства пользователей администратора и student, проведено их сравнение.

1. **Применить загрузочную систему «Elcomsoft System Recover» для изучения базы данных учетных записей SAM, возможности редактирования свойств записей и паролей.** **Просмотреть свойства существующих учетных записей SAM в Windows Server, найти SID и RID субъектов безопасности системы. Опробовать сброс пароля.**
2. Был скачан образ ESR и запущен. Был выбран режим изменения паролей и свойств.

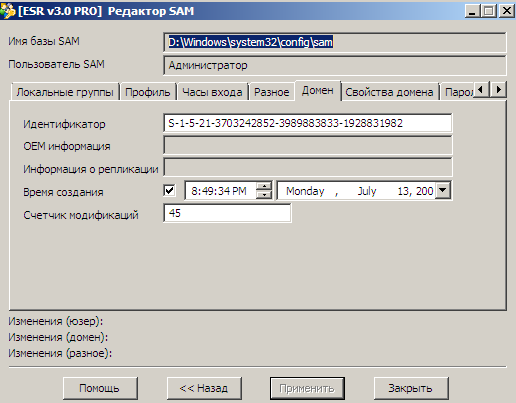
ESR успешно разгадала пароли пользователей, а так же можем увидеть их RID: 000001F4 для Администратора и 000001F5 для гостя.

****

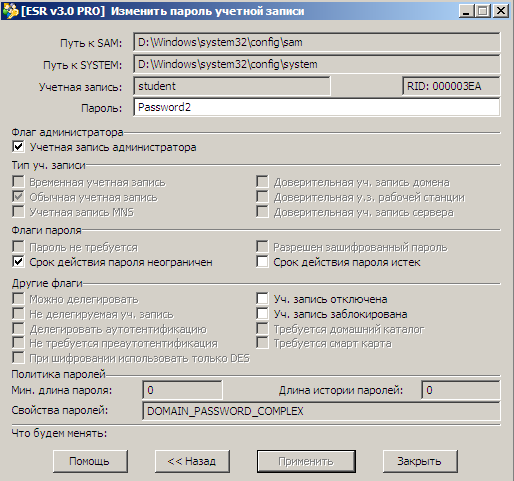
Давайте сменим пароль для Администратора. После перезагрузки можем заметить, что пароль успешно изменен.

****

В редакторе базы SAM мы можем настроить много всякого, а именно имя пользователя, его RID, его комментарий, хэши. Также можно поставить флаги по типу того, как отключение или блокировка учетной записи, требования паролей, возможность делегирования и многое другое. Также можно посмотреть информацию о последнем входе, выходе и смене пароля, о группах, можно изменить часы входа и “покопаться” в свойствах домена (Там же можно узнать SID пользователя). Но все это может испортить вашу систему и, если вы не знаете, как со всем этим работать, не лезьте в эту программу

****

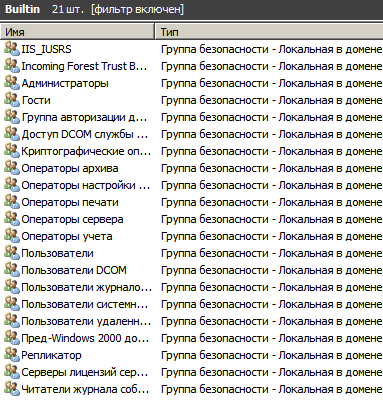
Еще мы можем давать учетной записи права администратора. Давайте студента дадим права администратора. После перезагрузки student был в группе Администраторы. Лишим student прав администратора.

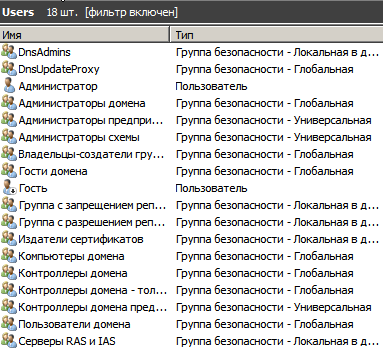
****

1. **Вывод**

Была изучена загрузочная система восстановления Elcomsoft System Recovery, найдены различные свойства учетных записей, изменены их свойства, но если хотите изменять их, то лучше делать это аккуратно и на свой страх и риск, зная, что вы хотите менять и это менять,

1. **Ознакомиться с составом встроенных доменных учетных записей и групп. С помощью консоли «Active Directory — пользователи и компьютеры» изучить состав учетных записей домена, локальных и глобальных групп домена.**
2. Группа безопасности делится на 3 области применения: Универсальная, Глобальная и Локальная в домене. Они отличаются друг от друга возможными участниками, преобразованием области, а также предоставление разрешения

****

****

Практически все группы из Builtin мы рассмотрели ранее. Рассмотрит группы из Users:

1. DnsAdmins – группа пользователей, имеющая доступ к информации DNS о сети
2. DnsUpdateProxy – группа пользователей, являющиеся DNS – клиентами
3. Администраторы домена – группа пользователей, которым позволено управлять доменом
4. Администраторы предприятий – группа пользователей, которым позволено вносить изменения в леса Active Directory
5. Администраторы схемы – группа пользователей, которым позволено вносить изменения в схемы Active Directory
6. Владельцы создателей групповой политики – группа пользователей, которым позволено вносить изменения в групповую политику в домене
7. Гости домена – группа пользователей, являющиеся гостями домена
8. Запрещающая группа репликации паролей RODC - группа без участников, управляющая политикой репликации RODC. Пароли не могут быть реплицированы на любой контроллер домена.
9. Разрешающая группа репликации паролей RODC - группа без участников, управляющая политикой репликации RODC. Приводит к тому, что новые контроллеры домена, не кэшируют учетные данные пользователя
10. Издатели сертификатов – группа пользователей, которым разрешено публиковать сертификаты в службе каталогов Active Directory
11. Компьютеры домена – группа пользователей, включающая все компьютеры, подключенные к домену (не включая контроллеры домена)
12. Контроллеры домена – группа пользователей, включающая в себя все контроллеры в домене
13. Контроллеры домена предприятия – группа пользователей, имеющая доступ к чтению всех объектов и атрибутов Active Directory
14. Пользователи домена – группа пользователей, включающая в себя учетные записи пользователей домена
15. Серверы RAS и IAS – группа компьютеров, которым разрешено использовать службы удаленного доступа

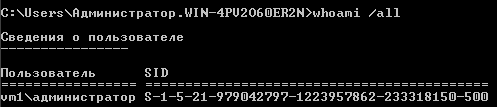
Также мы имеем такой же список пользователей: Администратор и Гость

1. **Выделить особенности встроенных локальных групп домена во вкладке Builtin, объяснить, почему у них «короткие» SID-ы**

Ранее мы рассмотрели из чего состоит SID. В середине SID присутствует ID, выданное котроллером домена, а, следовательно, в самом домене не имеет смысл указывать ID домена, поэтому SID короче.

1. **С помощью команды «whoami /all» определить свойства учётной записи администратора домена и сравнить с информацией о локальной учётной записи.**

С помощью команды whoami /all сравним свойства учетной записи администратора домена и локальной учетной записи администратора

****

Администратор домена, в-отличии от локального администратора состоит в таких группах, как Администраторы домена, группа с репликацией RDOC, Пред-Windows 2000 доступ, и имеют такие права, как добавление рабочих станций к домену.

1. **Составить полную схему связей учетных записей, глобальных, универсальных и локальных групп домена.**

|  |  |  |  |
| --- | --- | --- | --- |
| Учетные записи | Локальные группы | Универсальные группы | Глобальные группы |

Администраторы

Администраторы предприятия

Контроллеры домена

Администраторы домена

Пользователи домена

Группа с разрешением репликации RDOC

Гости домена

Администраторы схемы

Пользователи

Гости

Администратор

student

Гости

1. **Вывод**

Был изучен состав учетных записей домена, локальных и глобальных групп домена. Были выявлены различия между встроенной учетной записью администратора и администратора домена, составлена таблица связей учетных записей, глобальных, универсальных и локальных групп домена.

1. **Спланировать модель доменной сети небольшой организации.** **Определить несколько (3-5) категорий пользователей, отличающихся свойствами по отношению к системе, прикладным данным и прикладным программам.**
2. **Сформулировать требования и специфические условия работы заданных пользователей с целью последующей настройки.**

Спланируем сеть организации, принимающая технику на гарантийный ремонт. Введем условные обозначения:

Список принятой техники и список договоров клиентов – папка Set tech.

Ссылка на список принятой техники, список документации и отремонтированной техники – папка Rep tech

Ссылка на список отремонтированной ссылки и список вызванных клиентов – папка Operators

В данной организации будут следующие виды пользователей:

Администратор – следит за порядком сервера

Менеджер – следит за порядком работы

Оператор – обеспечивает связь с клиентами

Приемный отдел – принимает заявки и заключает договоры с клиентами

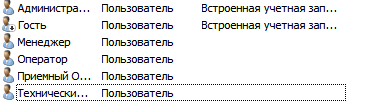
Технический отдел – работает с техникой

1. **Сформировать таблицу требований для категорий пользователей.**

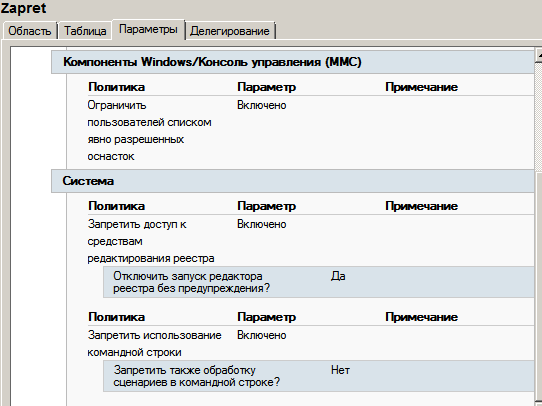
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Категория пользователей | Административные возможности | Запретные приложения | Доступ к Set tech | Доступ к Rep tech | Доступ к Operators |
| Администратор | Все | Не имеются | Есть | Есть | Есть |
| Менеджер | Пользовательские | Cmd, реестр, панель управления | Только чтение | Только чтение | Только чтение |
| Приемный отдел | Пользовательские | Cmd, реестр, панель управления | Есть | Нет | Нет |
| Технический отдел | Пользовательские | Cmd, реестр, панель управления | Только чтение | Есть | Нет |
| Операторы | Пользовательские | Cmd, реестр, панель управления | Нет | Только чтение | Есть |

1. **Создать учётные записи пользователей. Включить учётные записи в необходимые встроенные группы Windows. Спланировать собственные группы, с помощью которых можно настроить привилегии новых пользователей и специфические условия доступа пользователей к программам и данным.**

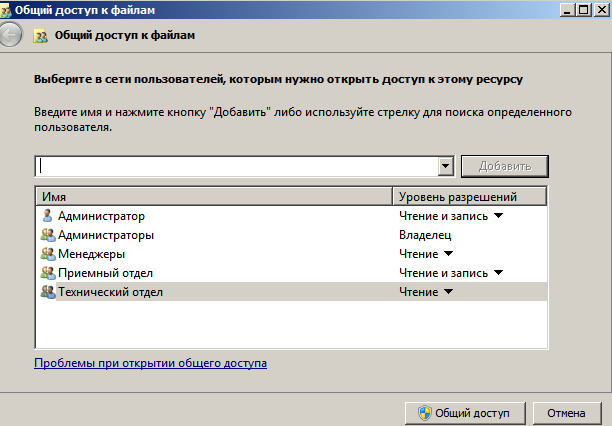
Будут созданы соответствующие группы, и пользователи.

****

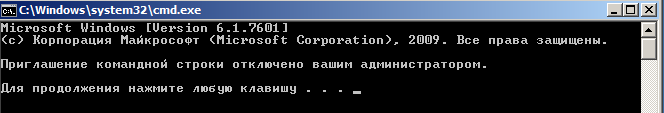
После создадим групповую политику на запрет консоли, реестра и панели управления.



Создадим сетевые ресурсы и дадим им соответствующие права для групп.



Теперь все, кроме Администратора не имею доступ к реестру, командной консоли и панели управления



1. **Вывод**

Была спланирована сеть небольшой организации, сформулированы требования и условия работы пользователей. Данная сеть была смоделирована с предоставлением доступом к определенным привилегиям, сетевым ресурсам и программам.

1. **Протокол Kerberos**
2. **Изучить процесс регистрации пользователя с помощью доменной учетной записи и роль протокола Kerberos**

Регистрация пользователя в Windows проходит следующем путем:

1. Идентификация – ввод данных пользователем
2. Аутентификация – проверка введенных данных
3. Авторизация – предоставление доступа в соответствии с проверенными данными
4. Отчетность – данные об аутентификации

При доменной аутентификации компьютеры, зарегистрированные в домене, отыскивают контроллеры DC, чтобы предъявить учетные данные доменной учетной записи пользователя при запросах аутентификации. Таким образом, если удаленный пользователь пытается получить доступ к локальному ресурсу какой-нибудь машины, то этот компьютер просит DC проверить идентификатор запрашивающего пользователя. Учетные записи пользователя домена располагаются только на DC и создаются лишь один раз. Любой компьютер-участник, которому нужно удостоверить учетную запись в домене, может обратиться к контроллерам DC в любое время. Проблемы синхронизации имен регистрации, паролей и сроков их действия не возникает, так как учетные данные и управление учетной записью осуществляются только в одном месте — на DC. Независимо от типа регистрации (локальной или доменной), Windows должна аутентифицировать запрос пользователя.

Протокол Kerberos разработан для надежной аутентификации пользователя. Он основан на принципе билетов (зашифрованных пакетов, которые выдает KDC). При успешной аутентификации, пользователю выдается удостоверение для доступа к ресурсам (TGT). После с помощью KDC пользователь, предъявляя свой TGT, получает доступ к определенному сетевому ресурсу (TGC).

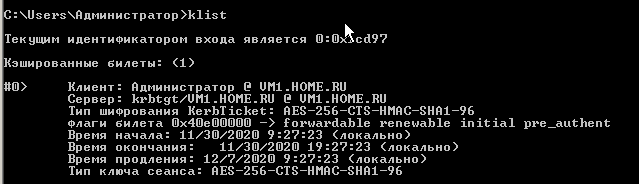
Процесс аутентификации пользователя осуществляется по следующему признаку:

1. Пользователь вводит свой логин и пароль
2. Данные, введенные пользователем, отправляются в службу KDC (Также службе передается имя домена и системное время пользователя (которое является аутентификатором). Пароль пользователя хешируется.
3. KDC сопоставляет введенные данные с данными из Active Directory. (разница между временем запроса и временем на контроллере домена не должна быть больше определенного значения, заданного в политике протокола Kerberos
4. KDC создает ключ сессии и шифрованный билет TGT
5. KDC отправляет зашифрованный аутентификатор и ключ сессии (шифруется на основе ключа клиента) клиенту
6. Компьютер получает данные от KDC, проверяет их и расшифровывает
7. Пользователь получает себе свой TGT и аутентифицируется в домене.

Процесс получения пользователем доступа к ресурсам на серверах домена:

1. Клиент предоставляет KDC свой TGT и маркер времени, которые зашифрованы
2. KDC расшифровывает полученные данные и проверяет их на подлинность
3. KDC создает билеты для сервера и клиента. Они имеют свой ключ, предоставляющий безопасное взаимодействие
4. KDC шифрует билеты и отправляет клиенту
5. Компьютер расшифровывает билеты (для билета сервера используется другой ключ, поэтому пользователь его не будет видеть)
6. Компьютер зашифровывает маркер времени и отправляет его серверу вместе с билетом сервера на ресурс, к которому хочет получить доступ (TGS)
7. Сервер расшифровывает свой ключ, тем сам идентифицирует пользователя
8. **С помощью команды klist и kerbtray из состава Resource Kit найти билеты Kerberos, определить их назначение и свойства**.

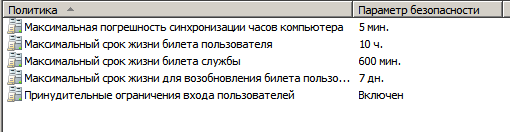
Выполним в командной строке klist, что является эквивалентом выполнения команды klist tickets. Нам вывели билет, зарегистрированный на сервере krbtgt, а также ID клиента. Билет действительны с момента входа (9:27:23) и следующие 10 часов (до 19:27:23). Срок жизни билета время следующего продления указываются в локальной политике

****

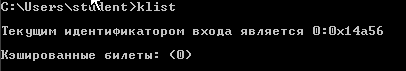
Утилита kerbtray была заменена утилитой klist, и доступ к ней не возможнен.

1. **Показать важность свойств меток времени Kerberos и необходимость синхронизации системного времени на компьютерах домена.**

Как видим из работы протокола Kerberos, описанного в 7.1, билеты требуют маркеры времени и KDC проверяет разнице между временем синхронизации сервера и клиента. В нашем случае в групповой политике Kerberos нашего домена максимальная разница времени синхронизации составляет 5 минут

****

Системное время student было изменено так, чтобы разница была больше 5 мин. Как видим билетов нам не выдали, так как погрешность синхронизации слишком велика.

**р**

1. **Вывод.**

Был изучен процесс регистрации пользователя и роль Kerberos. Опробована команда klist, показана важность временных меток Kerberos и важность синхронизации времени между компьютерами.

**Вывод:**

Были изучены групповая политика, политика Kerberos. Были рассмотрены локальные и доменные учетные записи, ESR и доменная сеть с объектами групповой политики и привилегиями