Отчет по аудиту информационной безопасности Windows Server 2019 DC Active Directory

Ответственный специалист:

Резепин Николай Артемович, специалист по информационной безопасности.

План аудита:

1. Аудит установленного DC
   - Паролей
   - Учетных записей
   - Служб

2. Анализ утилитой AD ACL Scanner
3. Выявление уязвимостей утилитой BloodHound

Цель аудита:

Целью проведенного аудита информационной безопасности является выявление уязвимостей, слабых мест и конфигурационных недочетов в сервере Windows Server 2019 развернутой на нем системе DC Active Directory и составление рекомендаций по устранению обнаруженных проблем.

Используемые инструменты:

- PowerShell
- AD ACL Scanner
- BloodHound

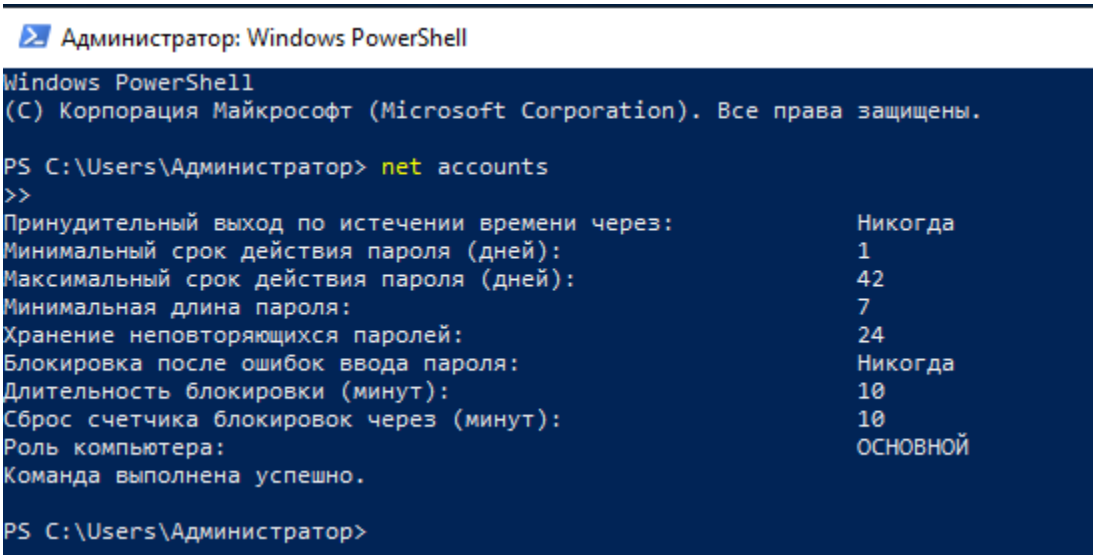
Проведение аудита

1. Аудит установленного DC

1.1. Аудит паролей:

Результаты отчета:

- Проверка политики паролей



Уязвимости:

- Минимальная длина пароля: **7 символов**;
- Блокировка учетной записи после неудачных попыток: **Отключена**;
- Длительность блокировки: **10 минут**.

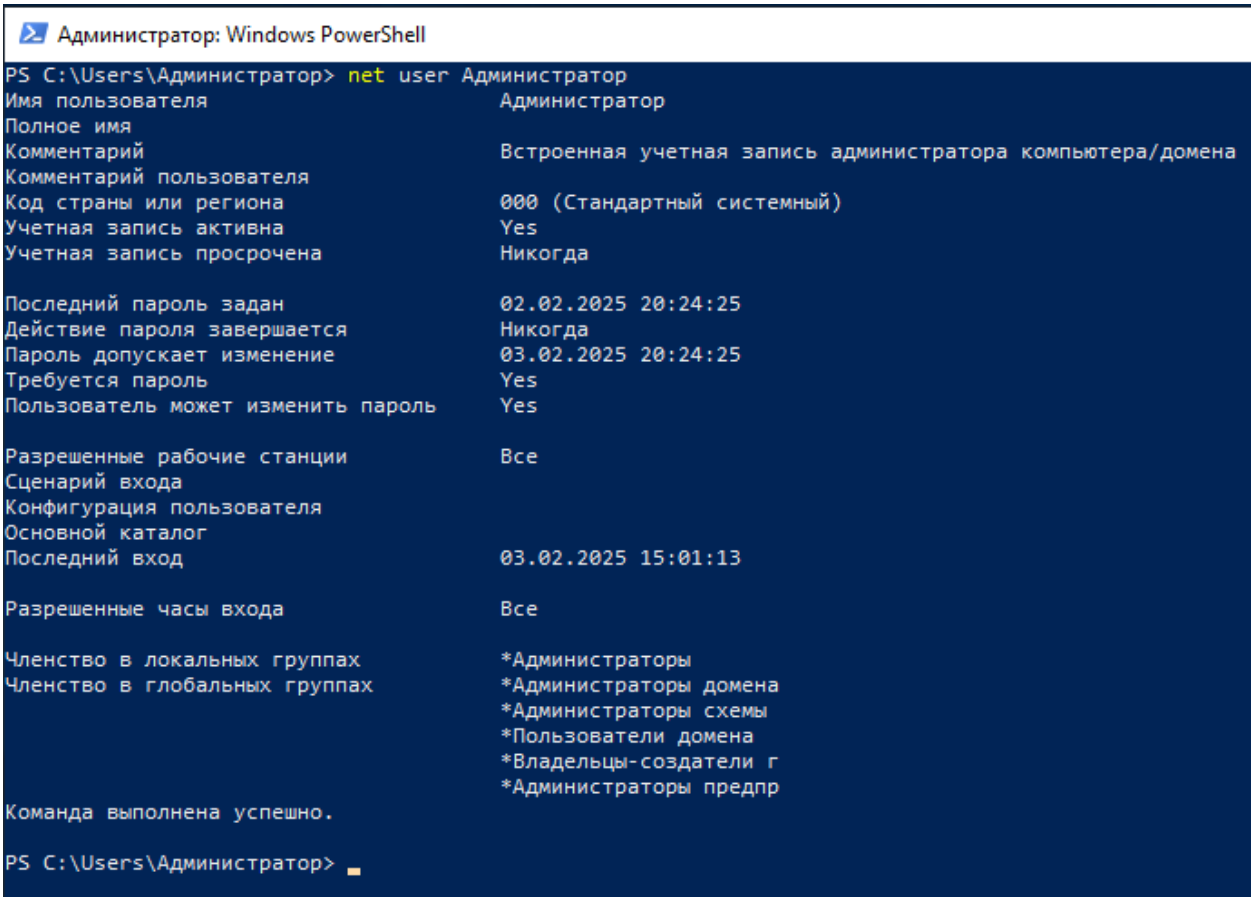
Рекомендации:

- Увеличить минимальную длину пароля до **10-15 символов**;
- Включить блокировку после нескольких неудачных попыток входа;
- Увеличить длительность блокировки **(от 30 до 60 минут)**.

1.2. Аудит учетных записей:

Результаты отчета:

- Проверка учетной записи «Администратор»



Уязвимости:

Членство пользователя **«Администратор»** в группах:

- Администраторы домена (высокая опасность);
- Администраторы схемы (редко используется, потенциально опасно);
- Администраторы предприятия (риск захвата домена).

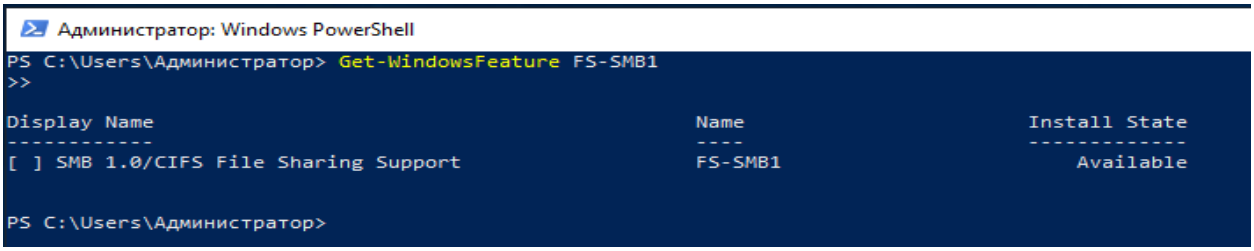
Рекомендации:

- Для работы использовать отдельный администраторский аккаунт без членства в потенциально опасных группах.

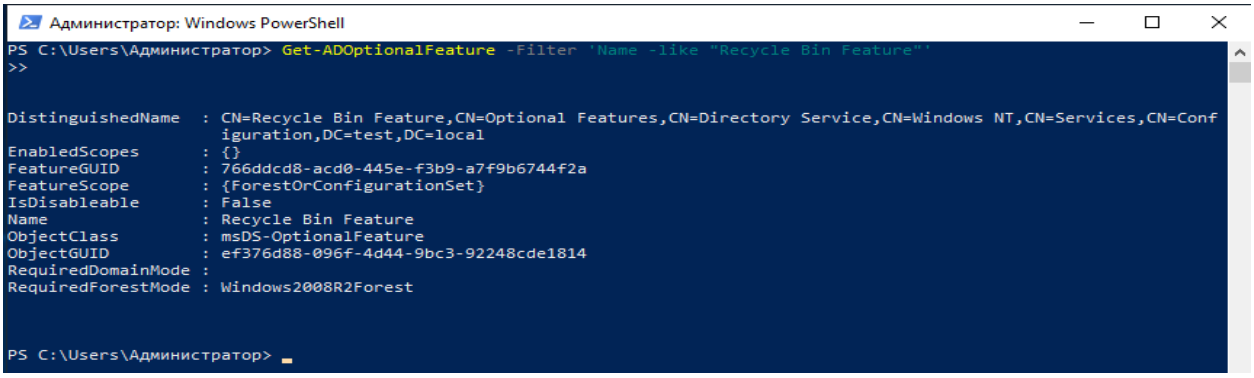
1.3. Аудит служб:

Результаты отчета:

- Проверка статуса SMBv1



- Проверка статуса корзины Active Directory (AD Recycle Bin)



Уязвимости:

- SMBv1 включен (опасно, устаревший и уязвимый протокол);
- Корзина Active Directory отключена (риск безвозвратного удаления объектов AD).

Рекомендации:

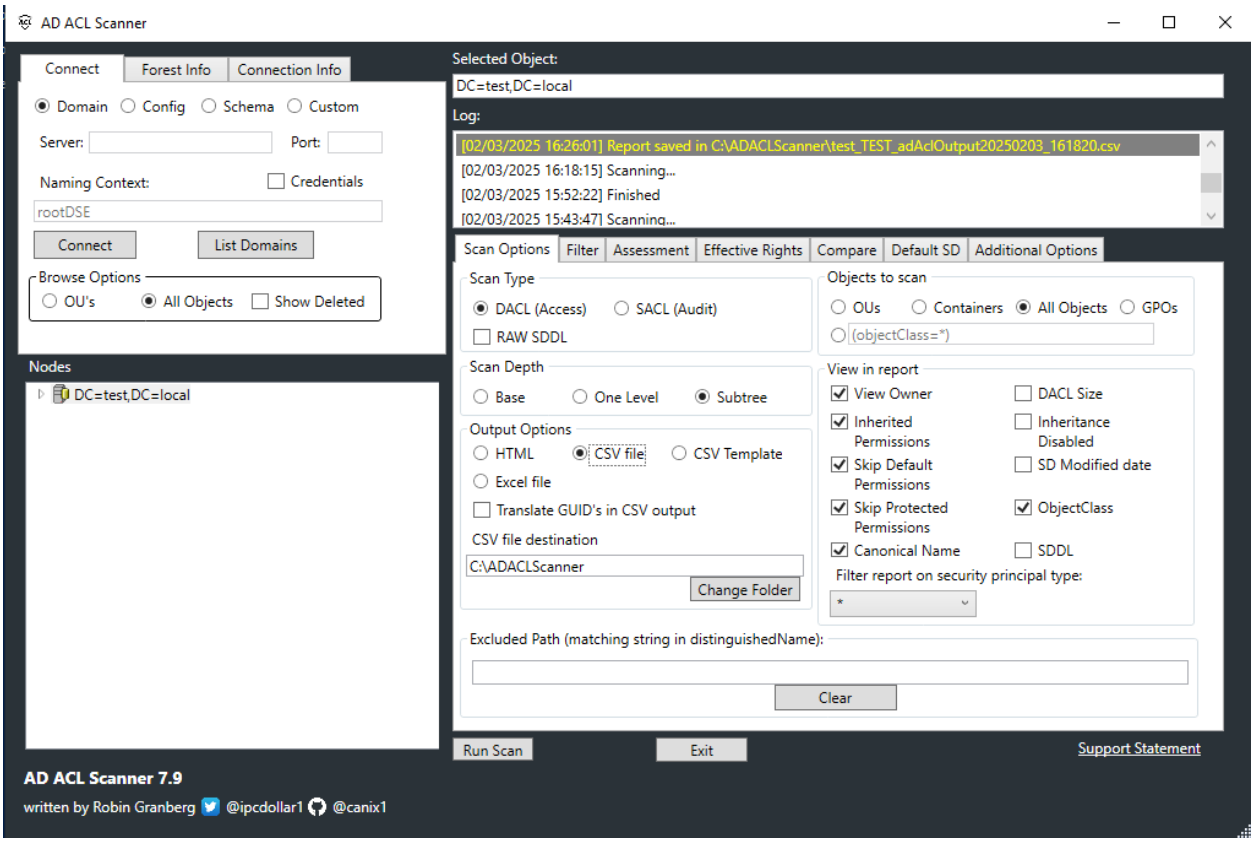
- Отключить SMBv1;
- Включить Корзину AD.

Ресурсы:

- Исходный отчет: см. **reports/GPOReport.html**
- Скриншоты: см. **screenshots/DC**

2. Анализ утилитой AD ACL Scanner

Предварительные настройки **AD ACL Scanner:**



Ресурсы:

- Исходный отчет: см. **reports/TEST-test.htm**
- Скриншоты: см. **screenshots/AD-ACL-Scanner**

Результаты отчета:

2.1. Некорректный разрешения

Уязвимость:

- Обнаружены записи с запретом на изменение пароля для следующих пользователей.

Объекты:

- student1, student2 и другие записи в OU All students.

Риски:

- Запрет смены пароля нарушает политику безопасности и затрудняет управление учетными записями.

Рекомендации:

- Провести анализ разрешений и удалить лишние;
- Разрешить пользователям безопасно менять пароли.

2.2. Избыточные привилегии для критических объектов

Уязвимость:

- Обнаружены разрешения на полный доступ и модификацию критических объектов.

Объекты:

- domainDNS, builtinDomain, test, local.

Риски:

- Злоупотребление привилегиями и нарушения целостности AD;
- Потенциальное компрометирование критических данных.

Рекомендации:

- Проверить, кому предоставлены права на полный доступ и модификацию;
- Ограничить разрешения только для групп с высоким уровнем доверия.

2.3. Отключенное наследование прав

Уязвимость:

- Некоторые записи имеют отключенное наследование.

Объекты:

- test, local, Builtin.

Риски:

- Невозможность централизованного управления правами;
- Возможные ошибки в конфигурации безопасности из-за ручных изменений.

Рекомендации:

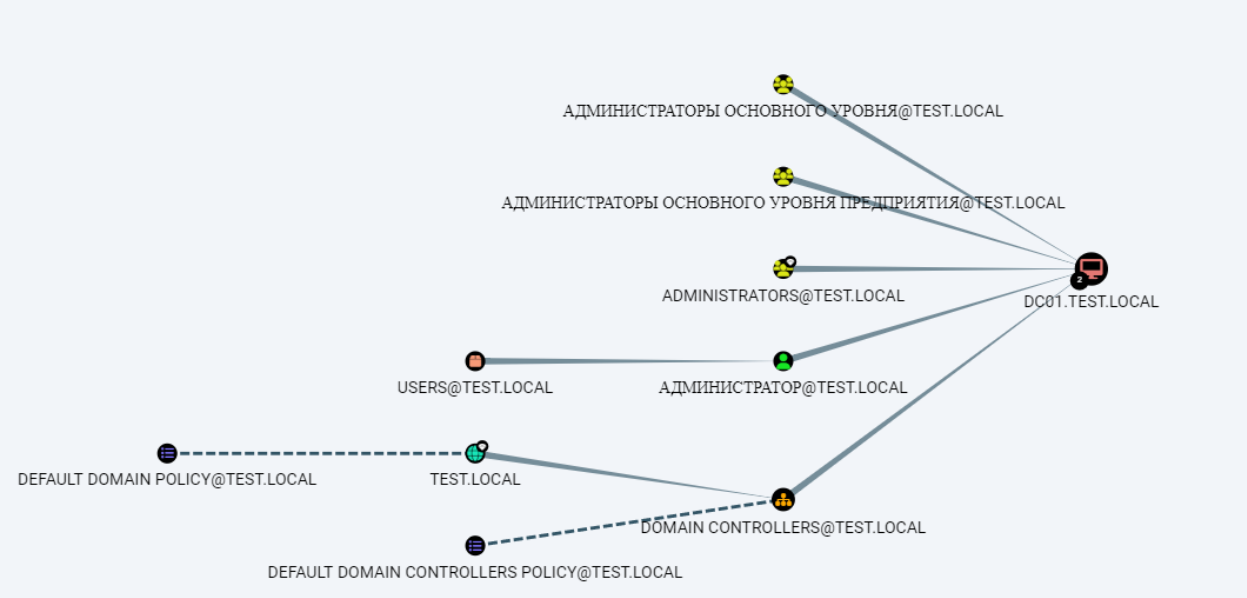
- Провести аудит отключенного наследования и восстановить его;
- Исключить случаи отключенного наследования, которые могут нарушать политику безопасности.

3. Выявление уязвимостей утилитой BloodHound

3.1. Неограниченное делегирование

Результаты отчета:

- Unconstrained Delegation



Уязвимость:

- Обнаружены системы с включенным Unconstrained Delegation.

Риски:

- Компрометация привилегированных учетных записей;
- Возможность эскалации прав и доступа к другим серверам.

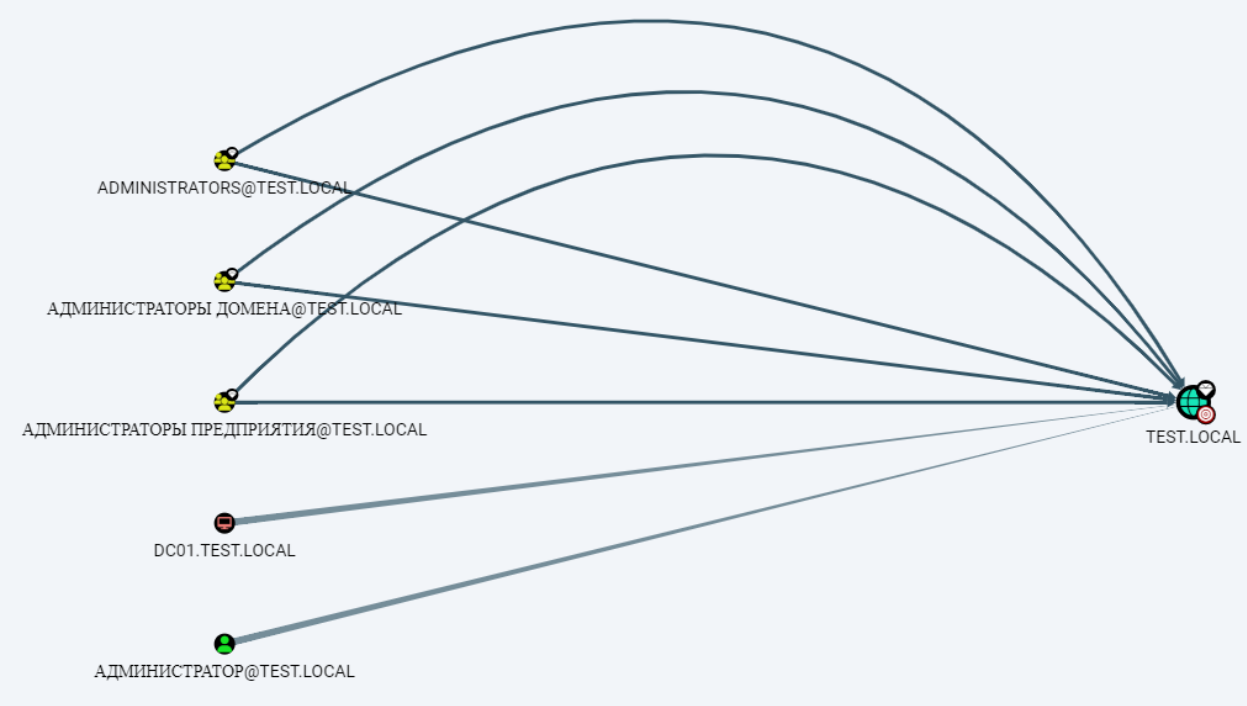
Рекомендации:

- Отключить Unconstrained Delegation на всех серверах;
- Регулярно проверять делегирование прав через GPO.

3.2. Учётные записи с правами DCSync

Результаты отчета:

- DCSync



Уязвимость:

- Выявлены учетные записи и группы, обладающие правами DCSync.

Риски:

- Возможность извлечения хэшей паролей всех пользователей;
- Полная компрометация домена.

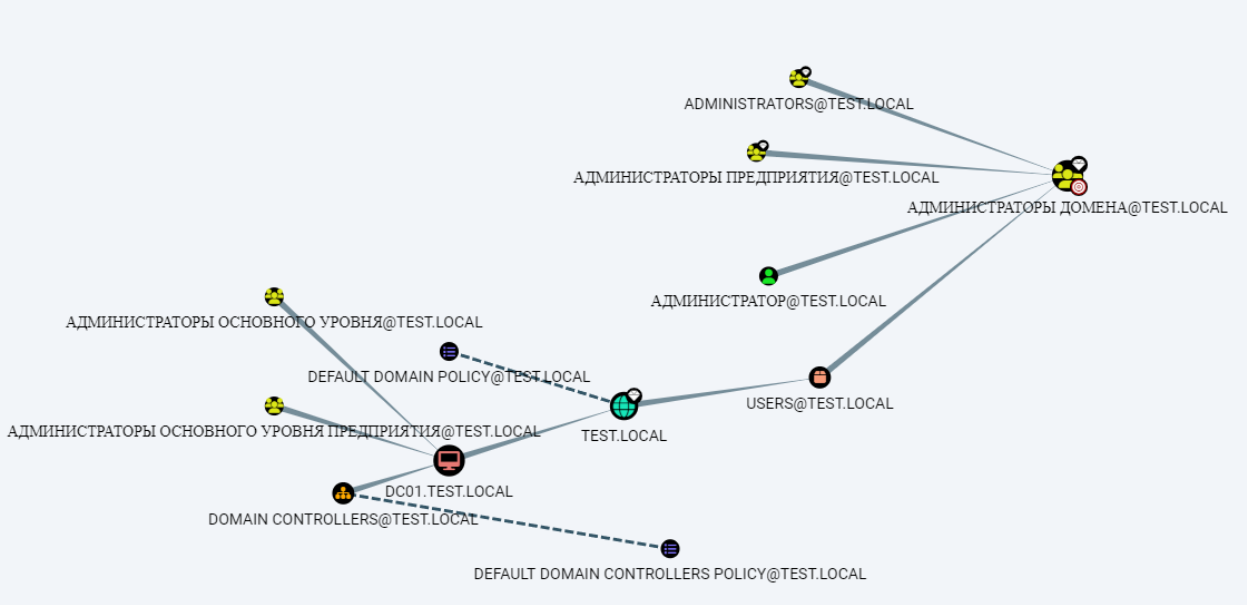
Рекомендации:

- Оставить данные права только у контроллеров домена;
- Внедрить мониторинг запросов на репликацию данных.

3.3. Кратчайшие пути к администраторам домена

Результаты отчета:

- Shortest paths to Domain Admins



Уязвимость:

- Выявлены маршруты, позволяющие получить права администратора домена через короткие цепочки действий.

Риски:

- Повышенная вероятность компрометации привилегированных учетных записей.

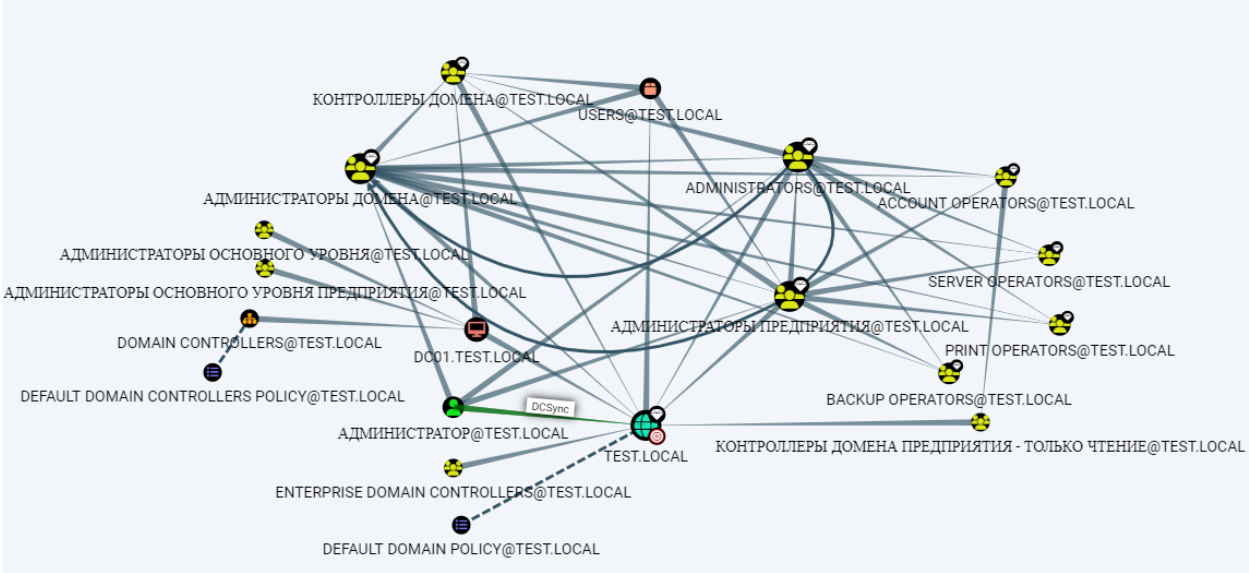
Рекомендации:

- Удалить избыточные привилегии у пользователей и групп;
- Внедрить принцип минимальных прав;
- Сегментировать сетевой доступ для взаимодействия с критическими системами.

3.4. Кратчайшие пути к высокоценным целям

Результаты отчета:

- Shortest paths to High Value Targets



Уязвимость:

- Обнаружены маршруты, позволяющие получить доступ к критическим учетным записям и ресурсам.

Риски:

- Возможность нарушения конфиденциальности и целостности данных.

Рекомендации:

- Ограничить доступ к высокоценным целям;
- Настроить мониторинг всех попыток доступа к данным объектам;
- Проводить регулярные проверки прав доступа.

Ресурсы:

- Скриншоты: см. **screenshots/blood-hound**

Вывод по проведенному аудиту:

В результате проведенного мною аудита были выявлены серьезные уязвимости и слабые места, которые могут привести к компрометации доменной инфраструктуры.

Реализация предложенных рекомендаций позволит значительно повысить уровень безопасности Active Directory и снизить риски несанкционированного доступа.