ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
ИНН 1656105383 / КПП 165601001, ОГРН 1181690097071
Юридический адрес: РТ, г. Казань, ул. Гладилова, зд. 27, пом. 1020
тел. 8 (843) 207 17 17, e-mail: info@uibcom.ru
БАНКОВСКИЕ РЕКВИЗИТЫ: р/с 40702810062000043112 в Отделение "Банк Татарстан" №8610 ПАО Сбербанк, БИК 049205603, к/с 30101810600000000603

ИТОГОВЫЙ ОТЧЕТ

по результатам проведения анализа защищённости корпоративной инфраструктуры

ООО «КОМПАНИЯ»

по договору № У-000-2026 от 29 июля 2026 г.

Заказчик: ООО «КОМПАНИЯ»

Исполнитель: ООО «УИБ»
действующее на основании Устава, лицензии ФСБ России № Л051-00105-16/00559603 от 14.06.2019
лицензии ФСТЭК России № Л024-00107-00/00583453 (4035) от 10.12.2021.

Дата анализа: 30 июля 2026 г.

Россия

2026

Документ согласован

Таблица 1

Документ согласован

ФИО	ПОДРАЗДЕЛЕНИЕ	ДОЛЖНОСТЬ	ПОДПИСЬ
1	2	3	4
<ФИО>			

СОДЕРЖАНИЕ

1. ГЛОССАРИЙ

1.1. ТЕРМИНЫ ДЛЯ ЦЕЛЕЙ НАСТОЯЩЕГО ДОКУМЕНТА

АНАЛИЗ ЗАЩИЩЕННОСТИ – метод контроля уровня защищенности, основанный на выявлении и анализе известных или ранее не известных уязвимостей, которые могут использоваться для получения несанкционированного доступа к информационному ресурсу.

КОМПЬЮТЕРНАЯ АТАКА – целенаправленное несанкционированное сетевое компьютерное воздействие (или их последовательность) на информационный ресурс, осуществляемое с применением программных и (или) программно-аппаратных средств и информационных технологий в целях реализации попыток нарушения и (или) прекращения функционирования информационного ресурса или реализации угрозы безопасности информации, обрабатываемой таким ресурсом.

НАРУШИТЕЛЬ – физическое лицо случайно или преднамеренно совершившее действия в отношении активов организации, следствием которых является нарушение информационной безопасности организации, вызывающие негативные последствия (вред/ущерб) для организации.

УЯЗВИМОСТЬ – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) создает потенциальные или реально существующие условия для реализации угроз безопасности информации.

ЭКСПЛОЙТ – программное средство, используемое для автоматизированной эксплуатации уязвимостей программного обеспечения или оборудования с целью проведения компьютерной атаки.

1.2. СОКРАЩЕНИЯ

Таблица 1.2.1. Обозначения и сокращения

№	СОКРАЩЕНИЕ	ОПРЕДЕЛЕНИЕ
1	2	3
1.	БД	База данных
2.	ИБ	Информационная безопасность
3.	ИС	Информационная система
4.	Нарушитель	Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации
5.	ОС	Операционная система
6.	ПО	Программное обеспечение
7.	HTTP	Hyper Text Transfer Protocol

№	СОКРАЩЕНИЕ	ОПРЕДЕЛЕНИЕ
8.	HTTPS	Hyper Text Transfer Protocol Secure
9.	RFID	Radio Frequency Identification
10.	ЛВС	Локальная Вычислительная Сеть
11.	САЗ	Средства Антивирусной Защиты
12.	TGT	Ticket-Granting Ticket
13.	AD	Active Directory
14.	ACL	Access Control List
15.	GPO	Group Policy Object
16.	OU	Organizational Unit
17.	MitM	Man-in-the-Middle
18.	SAM	Security Account Manager
19.	NTDS	NT Directory Service

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1 ОПИСАНИЕ ДОКУМЕНТА

Настоящий документ разработан Исполнителем и согласован с Заказчиком, представляет собой отчет по результатам проведения анализа защищенности во внутреннем периметре корпоративной инфраструктуры ООО «Компания» (далее – ООО «Компания»).

2.2 ЦЕЛЬ ПРОВЕДЕНИЯ РАБОТ

Целью проведения работ является получение объективной и независимой оценки текущего уровня защищенности корпоративной инфраструктуры ООО «КОМПАНИЯ» и последующая разработка рекомендаций по повышению уровня информационной безопасности.

2.3 КРАТКОЕ ОПИСАНИЕ ПРОВЕДЕННЫХ РАБОТ

Работы проводились методом «серого ящика» – Экспертам были предоставлены 2 доменные учетные записи с привилегиями обычных пользователей (test1 и test2).
В ходе анализа защищенности проводилась оценка технических мер безопасности ООО «КОМПАНИЯ», включающая:

- Проверку организации сетевого разграничения корпоративной инфраструктуры ООО «КОМПАНИЯ», а также механизмов сетевой безопасности, применяемых на сетевом оборудовании;
- Проверку использования небезопасных сетевых и прикладных протоколов в корпоративной инфраструктуре ООО «КОМПАНИЯ»;
- Проверку использования слабой парольной политики в корпоративном домене ООО «КОМПАНИЯ»;
- Проверку небезопасного хранения парольной и иной конфиденциальной информации в корпоративной инфраструктуре ООО «КОМПАНИЯ»;
- Проверку мер защиты, применяемых в Active Directory.

2.4 ГРАНИЦЫ ПРОВЕДЕНИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ

Анализ защищенности проводился в соответствии с согласованной с представителями Заказчика методикой с использованием техник сбора данных, идентификации и эксплуатации уязвимостей, а также получения доступа к информационным системам, на основе требований и рекомендаций стандартов и лучших практик в области информационной безопасности и различных методик анализа защищенности.

Подробная информация о проверяемых объектах представлена в таблице 2.4.1.

Таблица 2.4.1. Границы проведения работ

№	НАИМЕНОВАНИЕ ПРОВЕРЯЕМОГО ОБЪЕКТА	ОПИСАНИЕ ПРОВЕРЯЕМОГО ОБЪЕКТА
1	2	3
1	Внутренний периметр корпоративной инфраструктуры ООО «КОМПАНИЯ»	Совокупность логических подсетей и информационных систем ООО «КОМПАНИЯ», доступных в офисе компании по адресу г.

2.5 ОГРАНИЧЕНИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ

Получение информации от лиц, ответственных за эксплуатацию, поддержку и сопровождение, о возникновении нарушений непрерывности работы проверяемых объектов, сбоев их функционирования и отказа в обслуживании.

2.6 ОПИСАНИЕ ИСПОЛЬЗОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В ходе работ использовано следующее программное обеспечение:

- Сканеры уязвимостей для автоматического поиска известных уязвимостей в информационной системе;
- Программное обеспечение для анализа и моделирования сетевых протоколов;
- Программное обеспечение для проверки служб на портах сервера на поддерживаемые TLS/SSL шифрования и выявления некоторых криптографических недостатков;
- Программное обеспечение для перебора паролей в offline режиме;

- Программное обеспечение для расшифровки хэша паролей в offline режиме;
- Программное обеспечение, обеспечивающее низкоуровневый программный доступ к пакетам, а также имитирующее реализацию прикладных протоколов;
- Программное обеспечение для сбора и корреляции данных о домене;
- Утилита для тестирования окружения Windows/Active Directory;
- Платформа для проведения анализа защищенности, позволяющая имитировать атаки, а также создавать и применять эксплойты.

2.7 ОПИСАНИЕ ИСПОЛЬЗОВАННОГО АППАРАТНОГО ОБЕСПЕЧЕНИЯ

В ходе работ использовано следующее аппаратное обеспечение:

- Внешние сетевые карты для работы с сетью Wi-Fi;
- Сканнер и эмулятор для работы с RFID;
- Сканнер и эмулятор для работы с беспроводными устройствами ввода на радиочастоте 2.4 ГГц;

3. ВЫВОДЫ

По результатам проведенного анализа защищенности в корпоративной инфраструктуре ООО «КОМПАНИЯ» выявлены недостатки в части обеспечения информационной безопасности, в том числе критического уровня, ведущих к захвату контроля над доменом Company.ru, к утечке чувствительной информации коммерческого характера и конфигураций различных систем, а также, в отдельных случаях, персональных данных сотрудников.

Из проведенных работ следует, что внутренний периметр ООО «КОМПАНИЯ» с технической точки зрения защищен на **крайне низком** уровне.

Критерии уровня защищенности представлены в приложении А (таблице А.1.).

В результате проведенного анализа защищенности:

- Получен административный доступ к основному корпоративному домену Company.ru;
- Скомпрометировано (получен логин и пароль в открытом виде) более 1 000 доменных учетных записей, включая высокопривилегированные;
- Выявлены недостатки в парольной политике;
- Выявлены избыточные привилегии для непривилегированных пользователей;
- Подтверждена возможность выгрузки с правами непривилегированного пользователя списка пользователей и другой информации о структуре домена;
- Подтверждены факты небезопасного хранения парольной и иной информации конфиденциального характера на сетевых хранилищах;
- Выявлены недостатки в конфигурации САЗ, ведущие к их полному обходу;
- Выявлены архитектурные недостатки построения ЛВС, создающие возможность подключения к корпоративной ИТ-инфраструктуре объектов, не являющихся её частью, а также наличию сетевой связанности между всеми сегментами сети;
- Обнаружено использование небезопасных протоколов и конфигураций, ведущих к перехвату учетных данных и доступу к различным системам;
- Выявлены технические недостатки системы контроля и управления доступом на территорию ООО «КОМПАНИЯ».

4. РЕЗУЛЬТАТЫ ПРОВЕДЕНИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ООО «КОМПАНИЯ»

4.1 Получение прав администратора домена company.ru

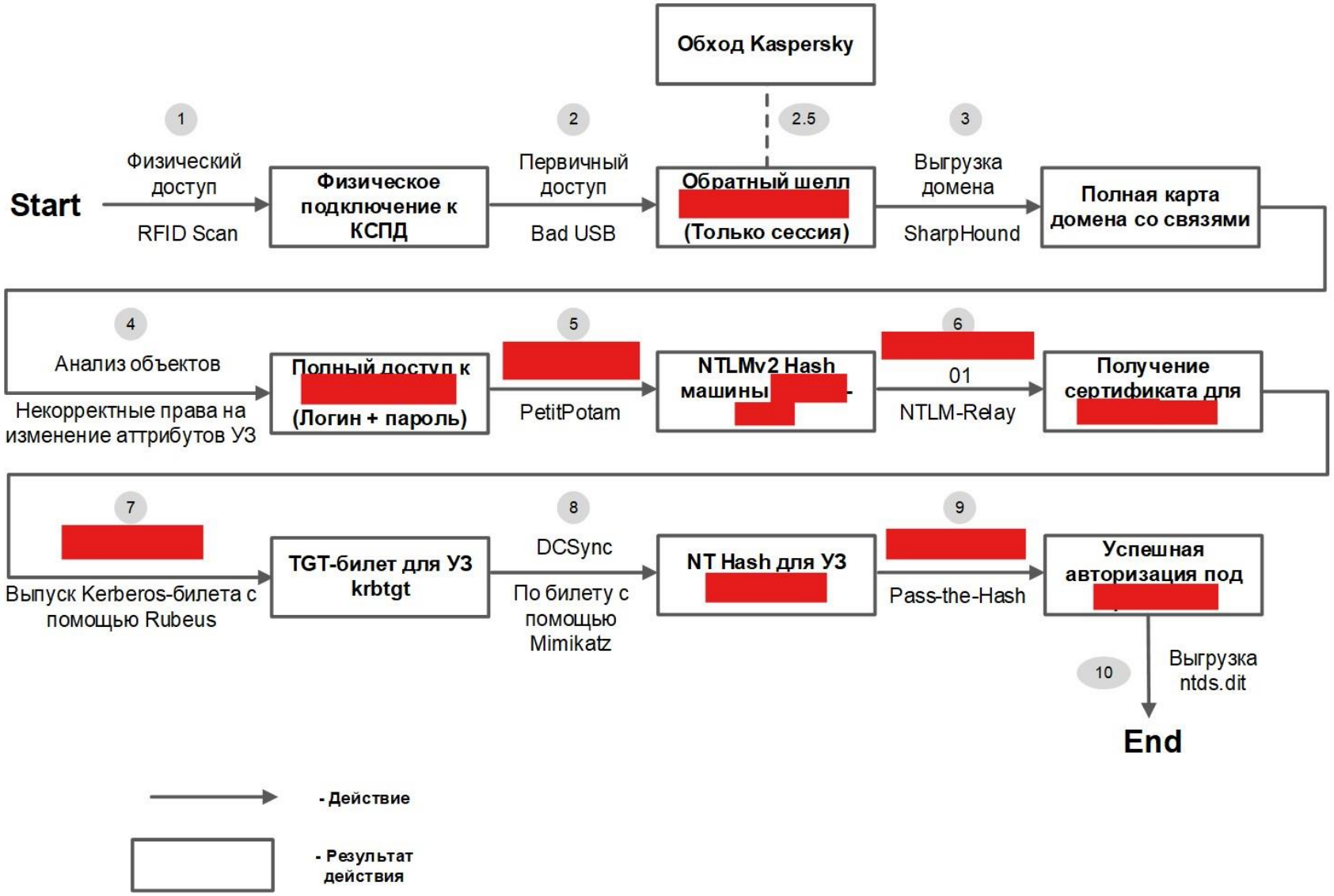
Уровень критичности: Критический

В ходе работ были обнаружены критические уязвимости и ошибки в конфигурации, позволяющие внешнему злоумышленнику, не обладающему доменной учетной записью и физическим доступом на территорию ООО «КОМПАНИЯ», получить привилегии администратора домена Company.ru и, как следствие, всех его дочерних доменов.

Цепочка действий Экспертов по захвату домена представлена на Схеме 1.

Описания действий Экспертов по захвату домена представлено в пунктах 4.1.1 – 4.1.12.

Схема 1 – Последовательность действий по получению привилегий администратора домена



4.1.1 Возможность копирования бесконтактных идентификационных карт сотрудников

Уровень критичности: Критический

Текущая конфигурация системы контроля и управления доступом, предназначенная для организации пропускного режима сотрудников на территорию ООО «КОМПАНИЯ», позволяет злоумышленнику скопировать бесконтактные идентификационные карты сотрудников для дальнейшего проникновения на территорию административных зданий ООО «КОМПАНИЯ».
Исполнителем был отсканирован временный пропуск, выданный им на время работ, и проведена успешная попытка физического проникновения в административные здания при помощи эмуляции сигнала на специализированном аппаратном устройстве.

4.1.2 Несанкционированный доступ к информационной системе через манипуляцию с беспроводным интерфейсом ввода

Уровень критичности: Критический

На пользовательских АРМ отсутствует защита от атак типа Bad USB.
В АРМ пользователя Исполнителем был незаметно подключен вредоносный «dongle» (свисток) от беспроводной мыши с последующей отправкой на него исполняемых команд.
В результате был получен обратный шелл к машине пользователя Company\user и проведено закрепление при помощи Планировщика задач.
Это позволило Экспертам исполнять команды в корпоративном домене с привилегиями данного пользователя.

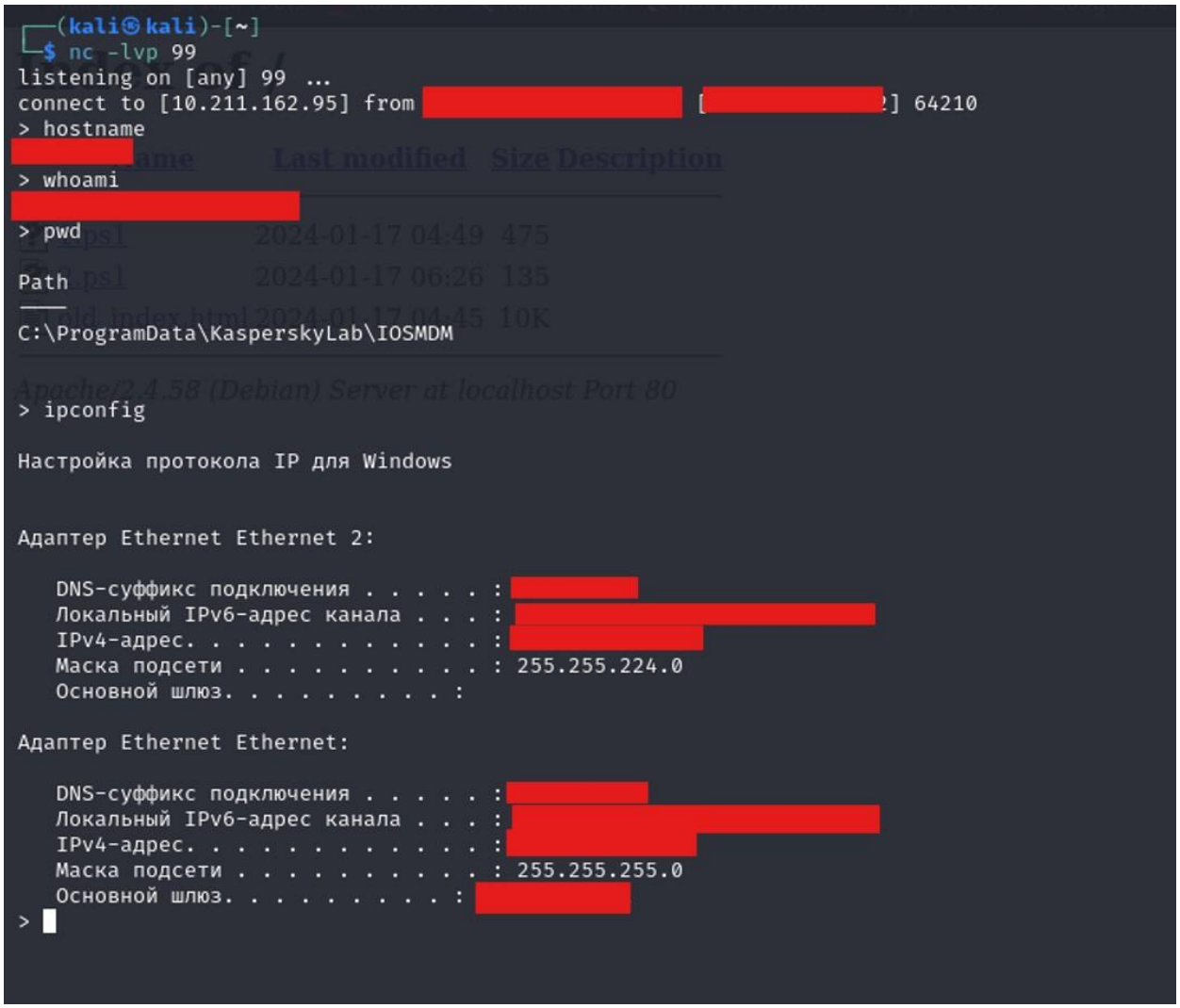


Рисунок 4.1.1 Установка соединения до АРМ пользователя

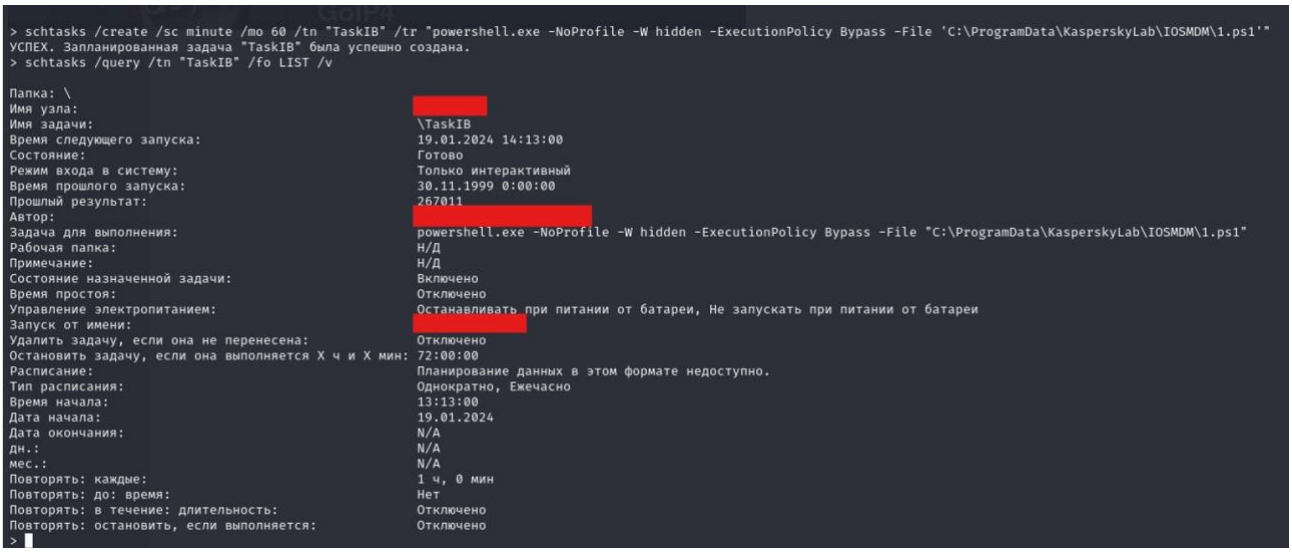


Рисунок 4.1.2 Создание задания в планировщике задач

4.1.3 Недостатки в антивирусной политике на пользовательских АРМ

Уровень критичности: Критический

В ходе работы Исполнителем обнаружены каталоги на пользовательских АРМ, входящие в исключения антивирусной проверки и права на запись в которые имеют непривилегированные пользователи. В дальнейшем, большая часть вредоносных нагрузок выполнялась из данных каталогов.

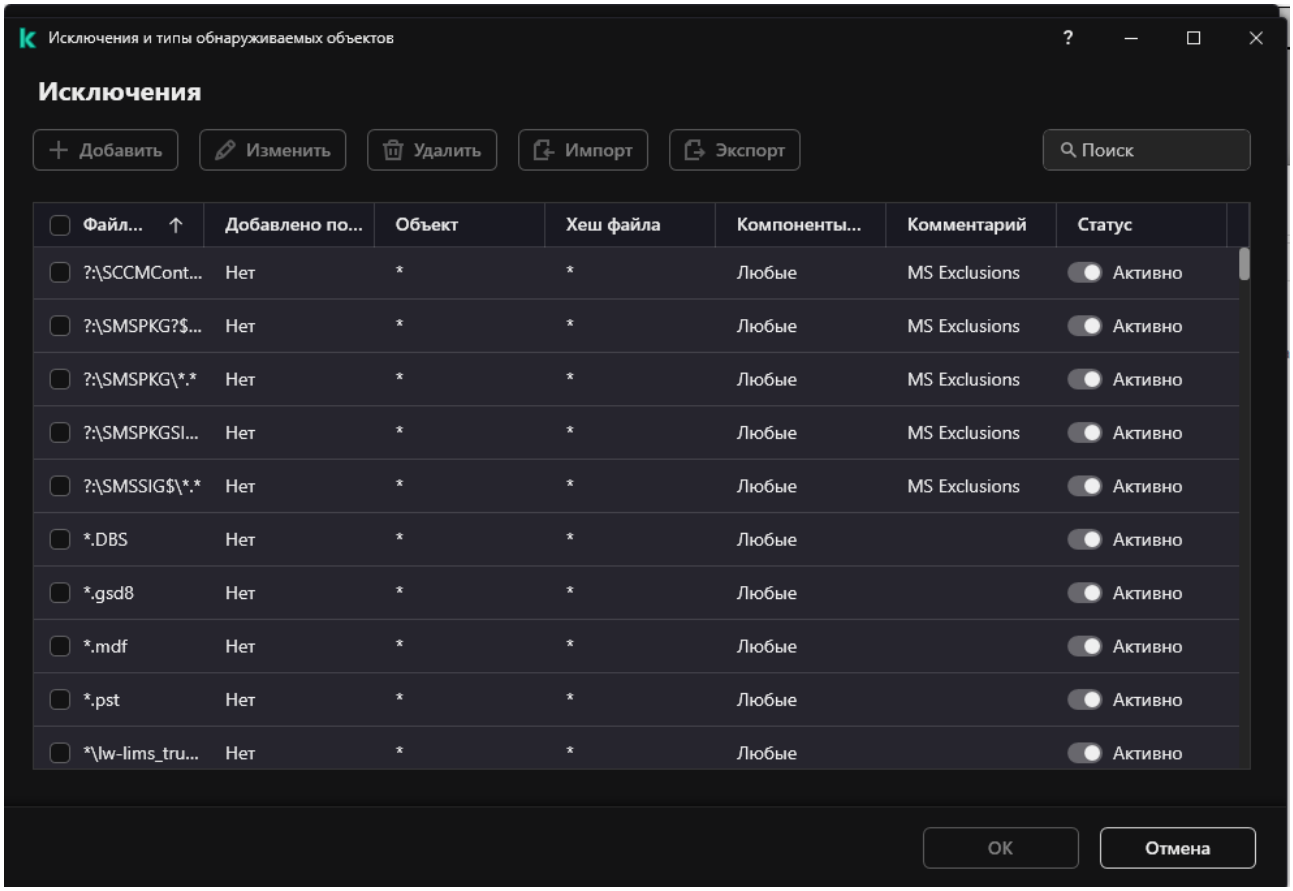


Рисунок 4.1.3 Просмотр исключений Касперского

4.1.4 Отсутствие ограничения на доступ к информации о структуре домена

Уровень критичности: Критический

В корпоративной инфраструктуре ООО «КОМПАНИЯ» не ограничен доступ к информации о структуре домена company.ru для непривилегированных в указанном домене пользователей. Для наследования групповых политик корневого контроллера домена company.ru в ООО «КОМПАНИЯ» используется локальный контейнер. Тем не менее, любые пользователи домена имеют возможность запросить его полную структуру, включающую:

– Все доменные компьютеры и сервера;
– Всех доменных пользователей (включая администраторов домена);
– Все доменные группы;
– Все групповые политики;
– Все поддомены;
– Все контейнеры.

В ходе работ Исполнителем из контроллера домена при помощи SharpHound проведена выгрузка информации о домене, используя непривилегированную УЗ. В результате была построена полная графовая карта домена.

Рисунок 4.1.4 Получение информации о структуре домена

4.1.5 Злоупотребление некорректно сконфигурированными атрибутами УЗ

Уровень критичности: Критический

При помощи карты обнаружено несколько некорректно сконфигурированных объектов, среди которых отключенная УЗ Company\user с возможностью изменения её атрибутов всеми членами, входящими в группу «Authenticated Users». В результате УЗ была включена, ей был сброшен и задан новый пароль.

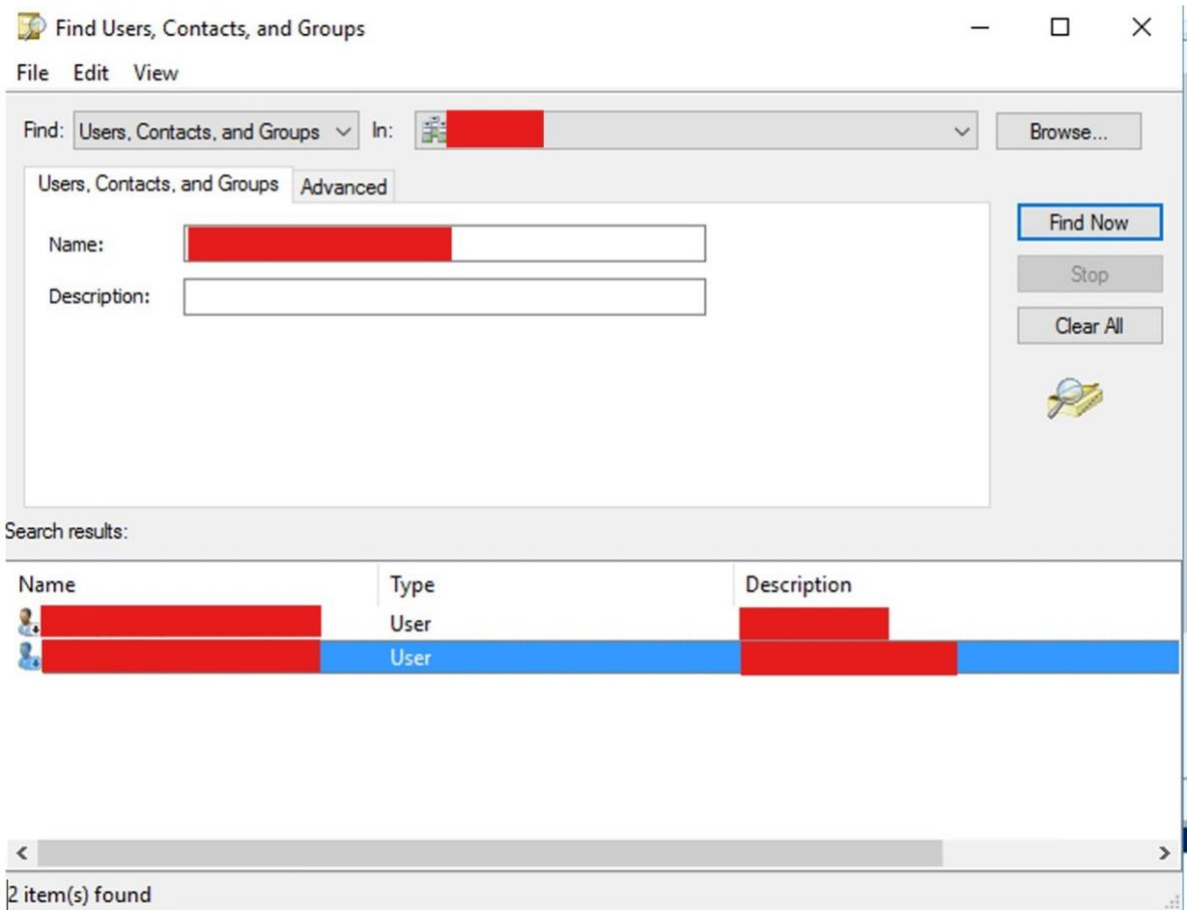


Рисунок 4.1.5 Учетная запись Company\user отключена

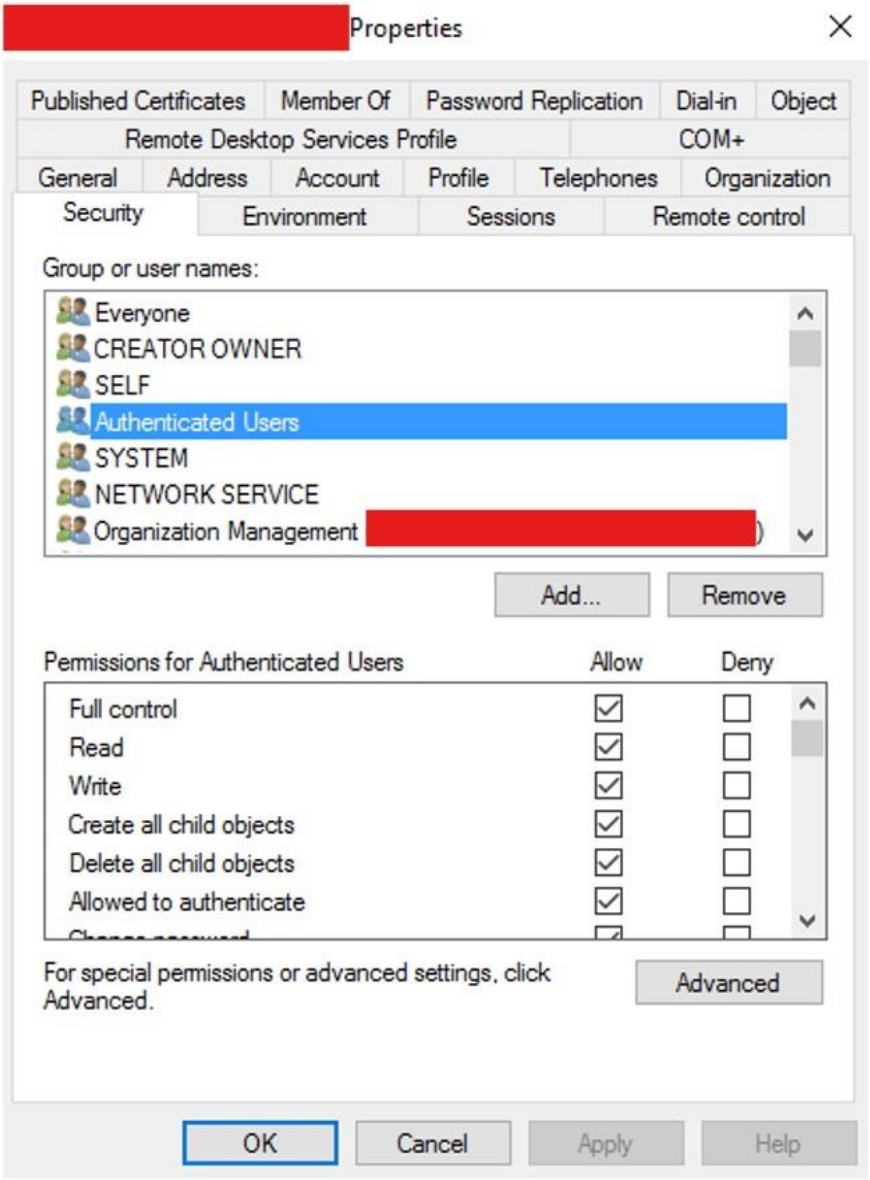


Рисунок 4.1.6 Члены группы «Authenticated Users» могут управлять данной УЗ

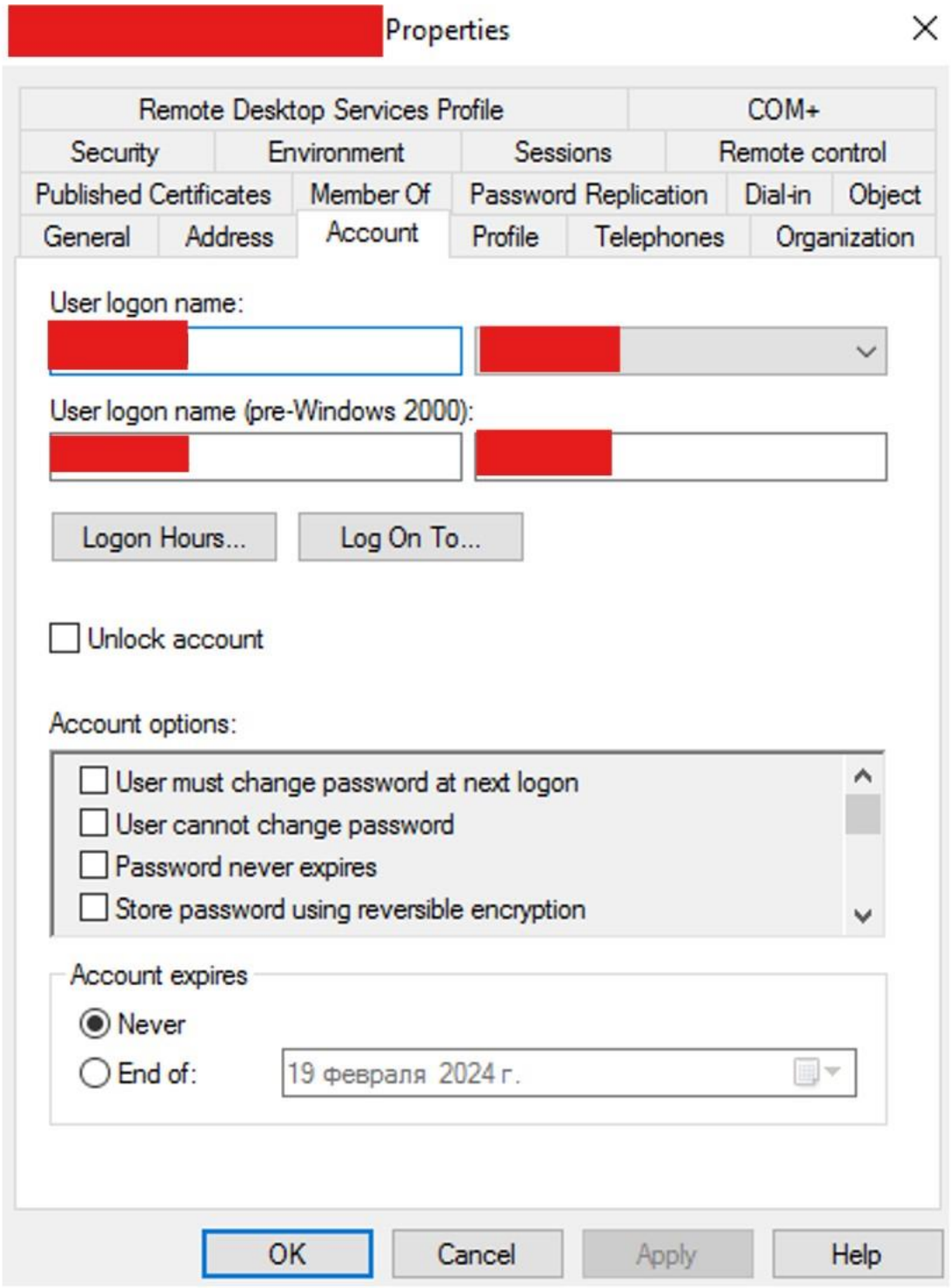


Рисунок 4.1.7 Параметры УЗ

Так же в процессе анализа AD было найдено еще 2 учетных записи, права на изменение атрибутов которых имеют все пользователи группы «Everyone».

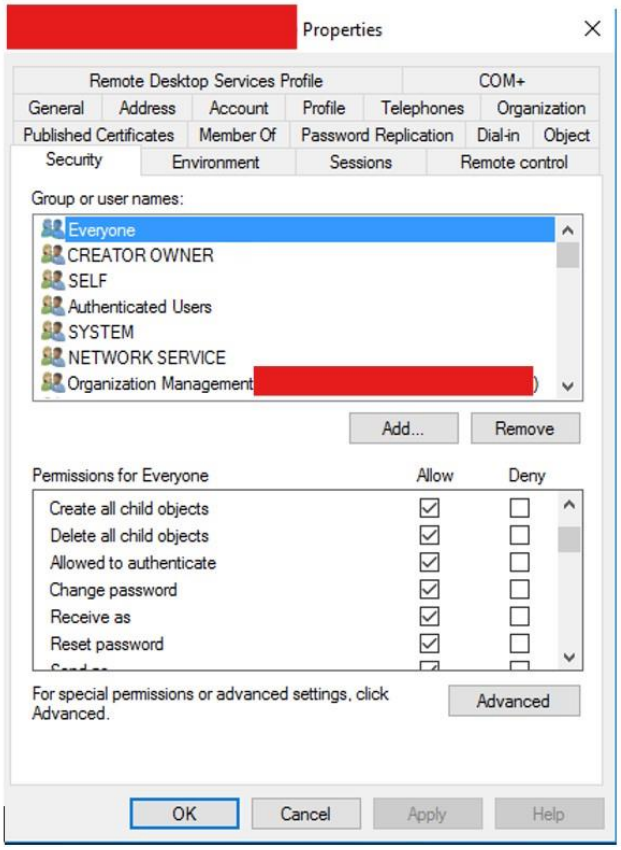


Рисунок 4.1.8 Члены группы «Everyone» могут управлять данной УЗ

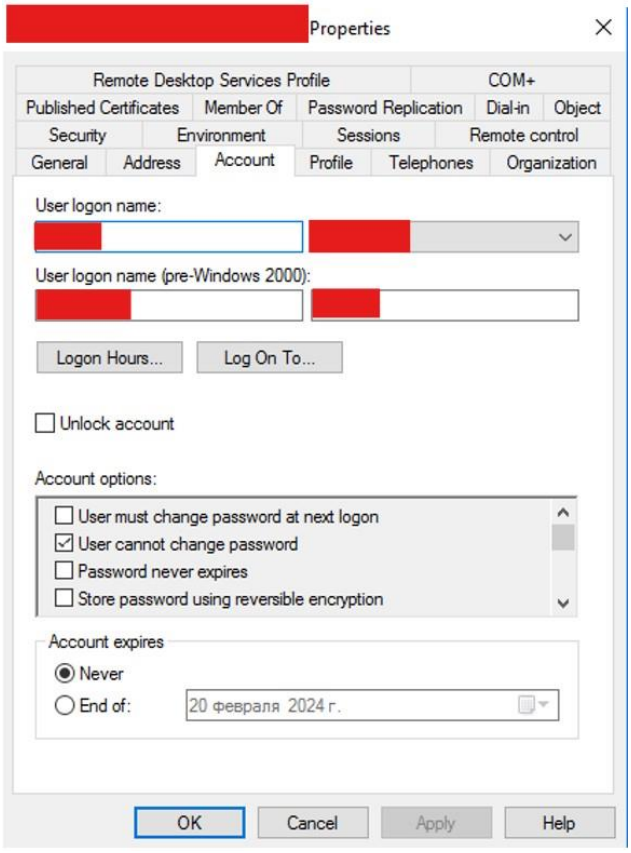


Рисунок 4.1.9 Параметры УЗ

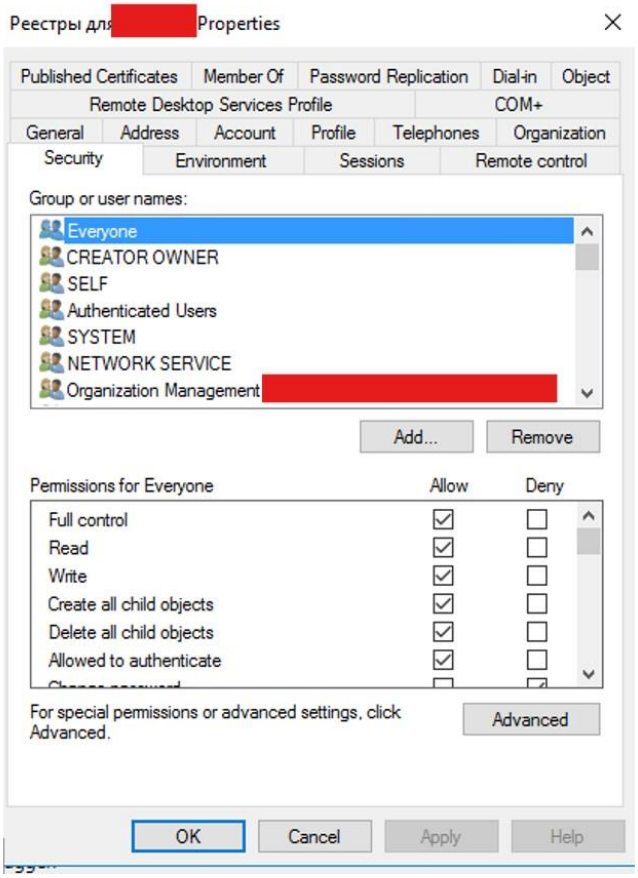


Рисунок 4.1.10 Члены группы «Everyone» могут управлять данной УЗ

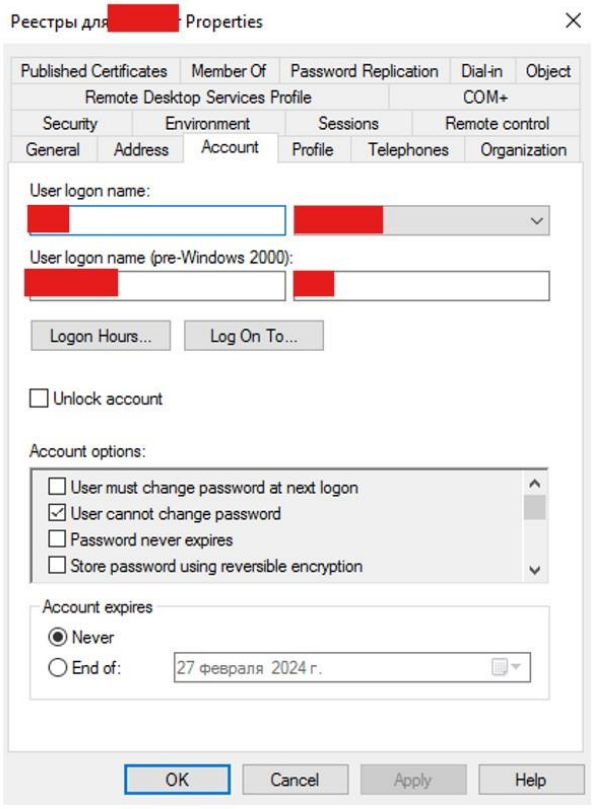


Рисунок 4.1.11 Параметры УЗ

4.1.6 Эксплуатация уязвимости PetitPotam на контроллерах домена

Уровень критичности: Критический

При помощи учетных данных user проведена атака PetitPotam на локальный контейнер контроллера домена DC1. При помощи уязвимости в протоколе MS-EFSRPC Эксперты вынудили контроллер домена авторизоваться на подконтрольном им сервере. В результате был получен NTLMv2 хэш машины DC1.

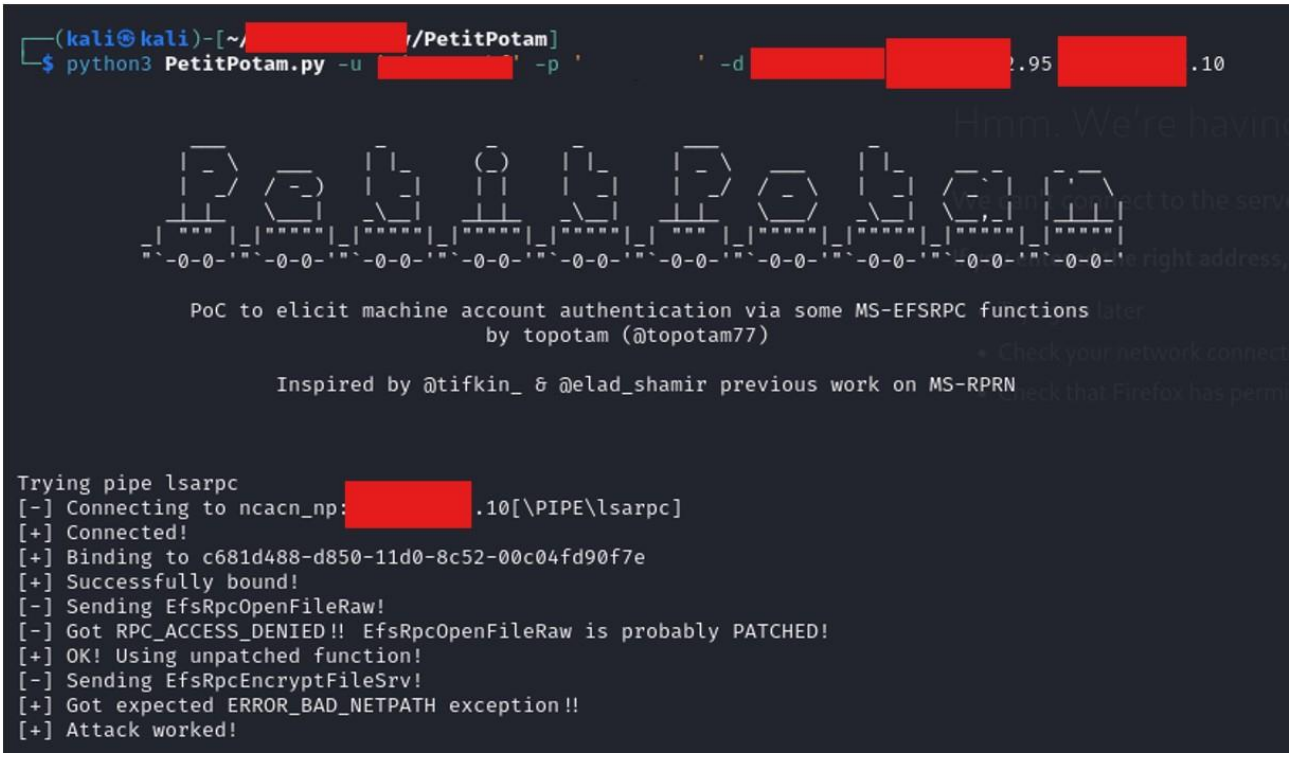


Рисунок 4.1.12 Выполнение атаки PetitPotam

Рисунок 4.1.13 Получен NTLMv2 хэш сервера DC1.COMPANY.RU

5. РЕКОМЕНДАЦИИ ПО РЕЗУЛЬТАТАМ РАБОТ

Рекомендации по результатам работ приведены в таблицах ниже (Таблица 5.1).

Таблица 5.1 – Рекомендации по устранению выявленных недостатков

№	ВЫЯВЛЕННЫЕ НЕДОСТАТКИ	УРОВЕНЬ КРИТИЧНОСТИ	РЕКОМЕНДАЦИЯ
	2	3	4
1.	4.1.1 Возможность копирования бесконтактных идентификационных карт сотрудников	Критический	Перейти на использование усовершенствованных идентификационных карт с более высоким уровнем защиты, таких как карты с технологией многофакторной аутентификации или карты на основе смарт-технологий (например, с использованием чипов с криптографической защитой).
2.	4.1.2 Несанкционированный доступ к информационной системе через манипуляцию с беспроводным интерфейсом ввода	Критический	Установить средства защиты от атак типа «Bad USB» на пользовательские АРМ. Провести обучающую сессию по кибербезопасности для сотрудников с целью повышения осведомленности о таких угрозах, как «Bad USB», и обучения их правильно реагировать на подозрительные находки и инциденты.
3.	4.1.3 Недостатки в антивирусной политике на пользовательских АРМ	Критический	Скорректировать политики Касперского, удалить из исключений каталоги, в которых непривилегированные пользователи имеют права на запись. Заблокировать возможность пользователям просматривать исключения.
4.	4.1.4 Отсутствие ограничения на доступ к информации о структуре домена	Критический	Ограничить доступ к информации о структуре домена company.ru для непривилегированных в указанном домене пользователей.
5.	4.1.5 Злоупотребление некорректно сконфигурированными атрибутами УЗ	Критический	Скорректировать привилегии указанных в отчете учетных записей. Провести аудит избыточных прав ACL в AD.

6. УСТРАНЕНИЕ СЛЕДОВ ПРОВЕДЕНИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ

Дополнительно, лицам, ответственным за эксплуатацию, поддержку и сопровождение ООО «КОМПАНИЯ», необходимо:

- Отключить учетные записи, предоставленные Экспертам на время работ;
- Удалить задачу «TaskIB» из планировщика задач с APM server.company.ru;
- Удалить каталог C:\ProgramData\KasperskyLab\IOSMDM с APM arm.company.ru;
- Удалить задачи из перечня GPO, указанных в п.4.6.1;
- Удалить задачу «TaskIB» из планировщика задач с DC1.company.ru, server-dc.company.ru;
- Исключить отключенную УЗ Company\user из всех групп.

ПРИЛОЖЕНИЕ А. КРИТЕРИИ УРОВНЯ ЗАЩИЩЕННОСТИ

Для оценки уровня защищенности целевой информационной инфраструктуры используются критерии, представленные в Таблице А.1.

Таблица А.1 – Критерии оценки уровня защищенности

№	УРОВЕНЬ	КРИТЕРИИ ОТНЕСЕНИЯ	КОММЕНТАРИЙ
1	2	3	4
1	Крайне низкий	Был получен администраторский доступ к основному корпоративному домену или домену, в котором расположены основные продуктивные ИС. *и/или* Были получены администраторские доступы на *nix Like-машины основных продуктивных ИС. *и/или* Были получены администраторские доступы в основные продуктивные ИС (на уровне приложения или СУБД). *и/или* Был получен администраторский доступ к активному сетевому оборудованию, в том числе к ядру сети. *и* Был получен доступ к значительному количеству информации ограниченного доступа в удобной форме представления	Полученные доступы явно предполагают компрометацию информации ограниченного доступа, а также полную свободу для проведения дальнейших атак. При этом Эксперт считает, что полученные доступы являются следствием масштабных системных проблем в области ИБ, а не случайного стечения обстоятельств
2	Низкий	Был получен массовый доступ (не администраторский) к элементам информационной инфраструктуры (домен, *nix like-серверы, СУБД, приложения). *или* Был получен администраторский доступ к отдельным ИС на любом уровне (ОС, СУБД, приложения). *и* Был получен доступ к значительному количеству информации ограниченного доступа в удобной форме представления	Основным критерием отнесения к данному уровню защищенности является компрометация информации ограниченного доступа, реализованная без получения полных администраторских полномочий в инфраструктуре Компания
3	Ниже среднего	Были получены единичные доступы к элементам информационной	К данному уровню относятся случаи, когда был получен

№	УРОВЕНЬ	КРИТЕРИИ ОТНЕСЕНИЯ	КОММЕНТАРИЙ
		инфраструктуры, повлекшие дальнейшие развитие атак. *и* Был получен администраторский доступ в домене или продуктивных ИС на любом уровне (ОС, СУБД, приложение). *и* Был получен доступ к значительному количеству информации ограниченного доступа в удобной форме представления. *но* Полученные результаты объективно свидетельствуют о том, что возможность развивать векторы атак у Эксперта присутствовала, но из-за временных ограничений проекта анализ защищенности был остановлен	доступ к значительному количеству информации ограниченного доступа вследствие эксплуатации уязвимостей и/или недоработок и/или получения доступа к УЗ, имеющей доступ к подобного рода информации
4	Средний	Были получены единичные доступы к элементам информационной инфраструктуры, не повлекшие дальнейшие развитие атак. *или* Был получен администраторский доступ в домене или продуктивных ИС на любом уровне (ОС, СУБД, приложение), однако данный доступ был получен вследствие единичной/случайной недоработки. *и/или* Был получен доступ к некоторому количеству информации ограниченного доступа в удобной форме представления. *но* Полученные результаты объективно свидетельствуют о том, что возможность развивать векторы атак у Эксперта присутствовала, но из-за временных ограничений проекта анализ защищенности был остановлен	К данному уровню относятся случаи, когда доступ к информации ограниченного доступа не был получен или был получен вследствие единичных/случайных недоработок
5	Выше среднего	Был получен незначительный доступ к некоторым объектам информационной инфраструктуры. *и/или* Была возможность незначительного расширения изначальных полномочий.	В ходе работ Эксперту не удалось скомпрометировать информацию ограниченного доступа, при этом объективные предпосылки к тому, что информация может быть скомпрометирована при

№	УРОВЕНЬ	КРИТЕРИИ ОТНЕСЕНИЯ	КОММЕНТАРИЙ
		и Доступ к информации ограниченного доступа получен не был. *и* Полученные результаты объективно свидетельствуют о том, что на момент прекращения анализа защищенности возможность развивать векторы атак у Эксперта отсутствовала	разумном увеличении времени проведения анализа защищенности получены не были. Был получен незначительный доступ к объектам информационной инфраструктуры
6	Высокий	Не получен доступ к объектам информационной инфраструктуры. *и* Отсутствовала возможность расширения изначальных полномочий. *и* Доступ к информации ограниченного доступа получен не был. *и* Полученные результаты объективно свидетельствуют о том, что на момент прекращения анализа защищенности возможность развивать векторы атак у Эксперта отсутствовала	В ходе работ Эксперту не удалось ни расширить свои изначальные полномочия, ни скомпрометировать информацию ограниченного доступа. При этом объективные предпосылки к тому, что информация может быть скомпрометирована при любом увеличении времени проведения анализа защищенности получены не были