УДК 004.056

Положий Артём Алексеевич

Студент

РГУ нефти и газа (НИУ) имени И. М. Губкина

АНАЛИЗ ЗАЩИЩЁННОСТИ ДОМЕННОЙ ИНФРАСТРУКТУРЫ НА БАЗЕ «АЛЬТ ДОМЕН»

Аннотация: *В работе проведён анализ безопасности доменной инфраструктуры, построенной на базе отечественного программного обеспечения «Альт Домен». Рассматриваются актуальные угрозы, включая атаки Pass-the-Hash, SMB Relay и Kerberoasting. Выполнено практическое моделирование атак в изолированной среде с целью оценки устойчивости и выявления уязвимостей. Предложены рекомендации по усилению защиты, основанные на конфигурации контроллера домена, использовании современных алгоритмов шифрования и политик безопасности. Сделан вывод о применимости «Альт Домен» в условиях импортозамещения.*

Ключевые слова: информационная безопасность, доменная инфраструктура, Альт Домен, Pass-the-Hash, SMB Relay, Kerberoasting, импортозамещение, Samba, NTLM, Kerberos.

УДК 004.056

Polozhii A.A.

Student

Gubkin Russian State University of Oil and Gas

SECURITY ANALYSIS OF DOMAIN INFRASTRUCTURE BASED ON "ALT DOMAIN"

Annotation: This article presents a security analysis of domain infrastructure based on the Russian software platform "Alt Domain". The research focuses on relevant threats, including Pass-the-Hash, SMB Relay, and Kerberoasting attacks. Practical simulations of attacks were conducted in an isolated environment to assess resistance and identify vulnerabilities. Recommendations for strengthening security are proposed, including domain controller configuration, the use of modern encryption algorithms, and security policies. The study concludes that "Alt Domain" is a viable solution under import substitution policies.

Keywords: information security, domain infrastructure, Alt Domain, Pass-the-Hash, SMB Relay, Kerberoasting, import substitution, Samba, NTLM, Kerberos.

ВВЕДЕНИЕ

Проблема обеспечения информационной безопасности в условиях стремительного роста киберугроз и цифровой трансформации организаций приобретает первостепенное значение. В последние годы на фоне политики импортозамещения особую актуальность приобретают отечественные решения, способные заменить зарубежные продукты корпоративного класса. Одним из таких решений является "Альт Домен" – комплексное программное обеспечение для построения доменной инфраструктуры, основанной на ОС семейства Альт и сервере каталогов Samba. Его внедрение позволяет обеспечить централизованное управление учетными записями, политиками доступа, средствами аутентификации и авторизации.

В то же время, несмотря на наличие встроенных механизмов безопасности, доменная инфраструктура остаётся потенциальной целью для различных атак. Среди наиболее распространённых методов атак на такие системы можно выделить: повторное использование хэшей паролей (Pass-the-hash), ретрансляцию аутентификационных данных (SMB Relay) и получение сервисных билетов Kerberos с целью их взлома (Kerberoasting). Эти атаки позволяют злоумышленнику получить доступ к ресурсам без знания действительных паролей, что делает их особенно опасными в условиях неправильно сконфигурированной инфраструктуры.

В данной работе рассматриваются как теоретические аспекты построения защищённой доменной инфраструктуры на базе Альт Домен, так и практическое моделирование атак, а также разработка защитных мероприятий. Целью данной работы является комплексный анализ защищенности Альт Домен и разработка практических рекомендаций по обеспечению безопасности доменной инфраструктуры.

Объектом исследования является программный комплекс «Альт Домен», разработанный компанией «Базальт СПО» на основе Samba, предназначенный для централизованного управления гетерогенными корпоративными сетями, включающими системы на базе Windows и Linux. Предмет исследования – защищенность «Альт Домен» от известных атак, включая SMB Relay, Pass-the-hash и Kerberoasting

ЛИТЕРАТУРНЫЙ ОБЗОР

Современная научная и прикладная литература уделяет значительное внимание вопросам защиты информационных систем, включая безопасность доменной инфраструктуры. Основной упор в исследованиях традиционно делается на платформу Microsoft Active Directory. Так, например, в публикации Скоропупова И. О., Бубновой А. А. и Карманова И. Н. [9] рассматриваются методы реализации атак на доменные инфраструктуры на базе семейства Windows. Авторы на конкретных примерах демонстрируют сценарии получения прав администратора домена через эксплуатацию уязвимостей в аутентификационных протоколах и ошибках конфигурации. Эти материалы служат ценным источником при анализе рисков, связанных с эксплуатацией даже современных решений

Однако в последние годы, в свете государственной политики импортозамещения, наблюдается рост интереса к отечественным решениям. Одним из таких решений является "Альт Домен", основанный на ОС Альт и службе каталогов Samba.

В работе Романенко О. В. и Осяевой А. А. [7] подчёркивается, что переход на ОС Альт в рамках миграции доменной инфраструктуры представляет собой логичный и обоснованный шаг в условиях отказа от проприетарного ПО. Авторы анализируют возможности интеграции сервисов

аутентификации и управления доступом, а также описывают практические аспекты развёртывания домена на базе Альт. Особое внимание в исследовании уделено вопросу обеспечения совместимости и безопасности, включая настройку Kerberos и LDAP-сервисов, а также реализацию механизмов централизованной авторизации.

Таким образом, проведённый литературный анализ подтверждает актуальность темы исследования и демонстрирует необходимость разработки и апробации практических мер по обеспечению защищённости доменной среды на базе Альт Домен.

МЕТОДЫ ИССЛЕДОВАНИЯ

Методология данного исследования основана на практическом моделировании атак в тестовой среде, построенной с использованием компонентов Альт Домен, Samba 4 и Kali Linux. В ходе работы был развёрнут отдельный домен с контроллером, созданным на базе ОС Альт Сервер 10, в котором были задействованы основные службы: Kerberos, LDAP, DNS, а также политики безопасности.

«Альт Домен» – служба каталогов (доменная служба), позволяющая централизованно управлять компьютерами и пользователями в корпоративной сети с операционными системами (ОС) на ядре Linux и Windows по единым правилам из единого центра. В системе реализовано хранение данных о пользователях, компьютерах (рабочих станциях) и других объектах корпоративной сети, а также управление профилями пользователей и компьютеров с помощью групповых политик в доменах MS Active Directory и Samba DC [3]. Альт Домен представляет широкие функциональные возможности:

- управление смешанной (гетерогенной) ИТ-инфраструктурой

- администрирование компьютеров с ОС «Альт», в домене Windows с помощью инструментов, аналогичных инструментам Microsoft, поддержка схем домена 2012, 2012R2, 2016, 2019,
- постепенный переход с MS Active Directory на «Альт Домен» без потери работоспособности ИТ-инфраструктуры,
- обеспечение отказоустойчивости ИТ-инфраструктуры (репликации между контроллерами доменов),
- объединение компьютеров в группы для централизованного администрирования по единым правилам,
- управление правами пользователей в группах,
- создание шаблонов групповых политик,
- настройка интервала времени повторного применения групповой политики,
- единая точка аутентификации (технология единого входа, SSO),
- дистанционная установка и регулярное обновление программного обеспечения на всех компьютерах группы,
- интеграция сервисов и оборудования,
- управление файлами и папками,
- отображение на рабочем столе ссылок на доступные сетевые диски,
- настройка внешнего вида рабочего стола пользователя,
- управление браузерами (Firefox, Яндекс Браузер и др.) через все возможные для этих браузеров политики.

На клиентских и атакующих машинах были установлены необходимые инструменты тестирования: Impacket (GetUserSPNs.py, ntlmrelayx.py, secretsdump.py), Responder, а также вспомогательные утилиты nmap, smbclient

и krb5-user. Тестирование проводилось в изолированной виртуальной сети с контролируемыми условиями, что позволило безопасно воспроизвести сценарии реальных атак.

В рамках практической части работы была смоделирована атака Pass-the-hash в среде, полностью построенной на базе свободного программного обеспечения. Целью моделирования являлась проверка возможности использования хэшей паролей для получения доступа к доменным ресурсам без знания реального пароля пользователя. В процессе атаки предполагалась следующая последовательность: получение NTLM-хэша учетной записи домена, использование данного хэша для аутентификации на сервере и выполнение удалённых команд с привилегиями пользователя, чей хэш был скомпрометирован.

На первом этапе была подготовлена целевая учетная запись в домене — это может быть, как стандартная пользовательская запись, так и запись с расширенными привилегиями (например, член группы "Администраторы домена"). В контексте смоделированной атаки предполагалось, что хэш учетной записи уже доступен злоумышленнику, как это могло бы произойти в результате других атак — например, извлечения данных из локальной системы.

На втором этапе осуществлялась непосредственная попытка аутентификации с использованием ранее полученного NTLM-хэша. В ходе выполнения атаки атакующая система установила соединение с сервером в домене, указав в качестве пароля хэш NTLM, что является сутью атаки Pass-the-hash. Протокол NTLM, по своей природе, не требует знания оригинального пароля: он полагается на криптографическое сравнение

хэшей, и, следовательно, при корректной реализации запроса принимает предоставленный хэш как действительные учетные данные.

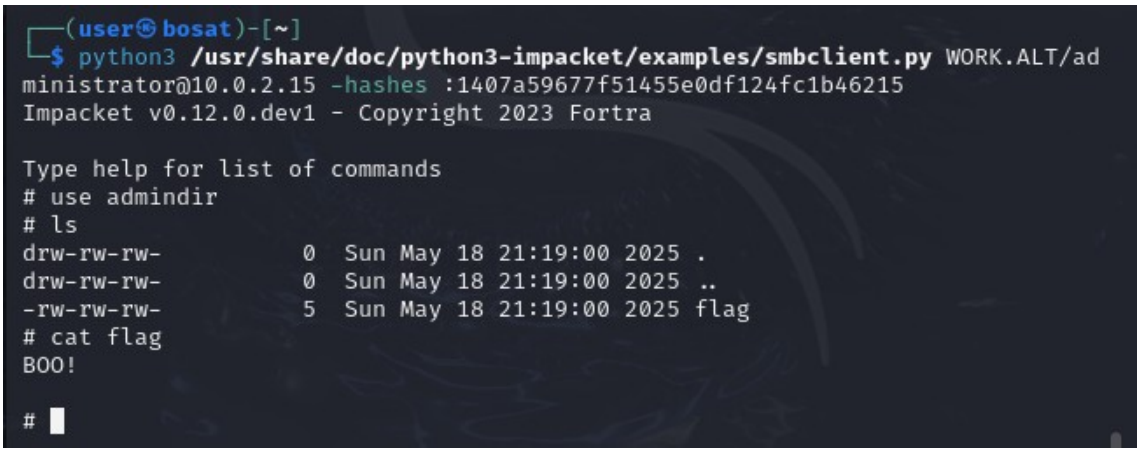

Рисунок 1 – Атака Pass-the-hash

После успешного прохождения аутентификации атакующая сторона получила возможность выполнять команды на удаленной машине в контексте скомпрометированной учетной записи. В тестовой инфраструктуре это сопровождалось подключением к общей сетевой папке, доступной только участникам группы "Администраторы домена". Фактически, с точки зрения целевого сервера, сессия выглядела как нормальное подключение пользователя из домена, прошедшего проверку подлинности.

В качестве основной меры по защите от атаки Pass-the-hash необходимо исключить использование аутентификации по NTLM вообще – установить *ntlm auth = no* в smb.conf. При попытке использовать хэш вместо пароля получим ошибку:

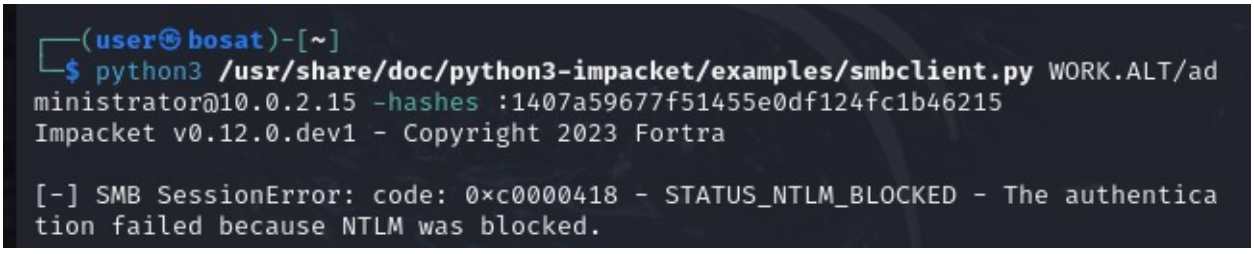

Рисунок 2 – Попытка атаки Pass-the-hash после применения защитных мер

Если использовать NTLM необходимо, то следует исключить хранение или передачу необработанных хэшей. В домене нужно настроить политику, запрещающую хранение LM-хэша и минимизирующую использование NTLM, а также не использовать NTLM v1. Также следует использовать многофакторную аутентификацию для доступа к особым ресурсам, а все сервисные и администраторские учётные записи должны иметь уникальные, сложные пароли, которые меняются регулярно.

SMB Relay представляет собой классическую атаку типа «Человек посередине» (Man-in-the-Middle), в рамках которой злоумышленник, расположенный в одной сети с жертвой, перехватывает попытку аутентификации клиента на определённый сетевой ресурс и ретранслирует её на целевой сервер от своего имени. В случае, если сервер не применяет защитные механизмы, такие как обязательная цифровая подпись SMB, происходит успешная аутентификация злоумышленника с использованием легитимных учетных данных жертвы.

Первоначально была проверена конфигурация целевого сервера. Одним из ключевых условий успешной атаки SMB Relay является отключённая обязательная подпись SMB (SMB signing). На Альт Домен этот параметр включен по умолчанию, соответствующий параметр в конфигурации был изменён, что позволило проводить ретрансляцию NTLM-сообщений без прерывания соединения.

Server signing = disabled

Просканировав сеть утилитой nmap, получим следующее сообщение, которое говорит о том, что можно провести атаку.

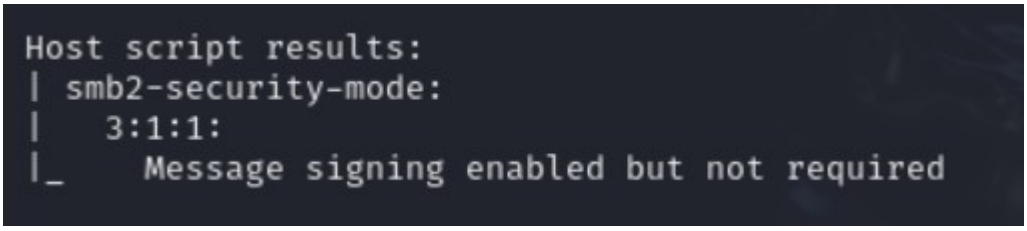

Рисунок 3 – Сканирование сети

Кроме того, чтобы инициировать подключение жертвы к атакующему хосту, использовался простой механизм — доступ к сетевому ресурсу вида `\\attacker_ip\share`, инициированный с клиентской машины, также находящейся в домене и работающей под управлением ОС Альт. Подобный доступ может быть спровоцирован, например, через запуск скрипта, переход по ссылке в почтовом сообщении или автоматическую загрузку внешнего ресурса в документах (например, LibreOffice или PDF).

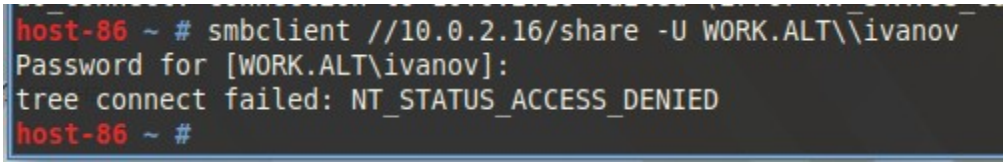

Рисунок 4 – Моделирование подключения жертвы

В атаке используются утилиты Responder и ntlmrelayx.py, входящий в состав Impacket. Во-первых, необходимо правильно настроить Responder для отключения SMB и HTTP-ответов, поскольку они будут пересылаться в ntlmrelayx, и в конечном итоге ретранслироваться. Для этого необходимо изменить строки в файле /etc/responder/Responder.conf:

SMB = Off

HTTP = Off

После этого запустим Responder:

Рисунок 5 – Прослушивание входящих подключений

После запуска утилиты ntlmrelayx.py атакующая машина начала слушать входящие подключения на портах SMB (445 TCP) и HTTP (80 TCP). Как только жертва инициировала запрос к атакующему узлу, ее система отправила NTLM-запрос на аутентификацию, который был перехвачен и немедленно ретранслирован к серверу домена.

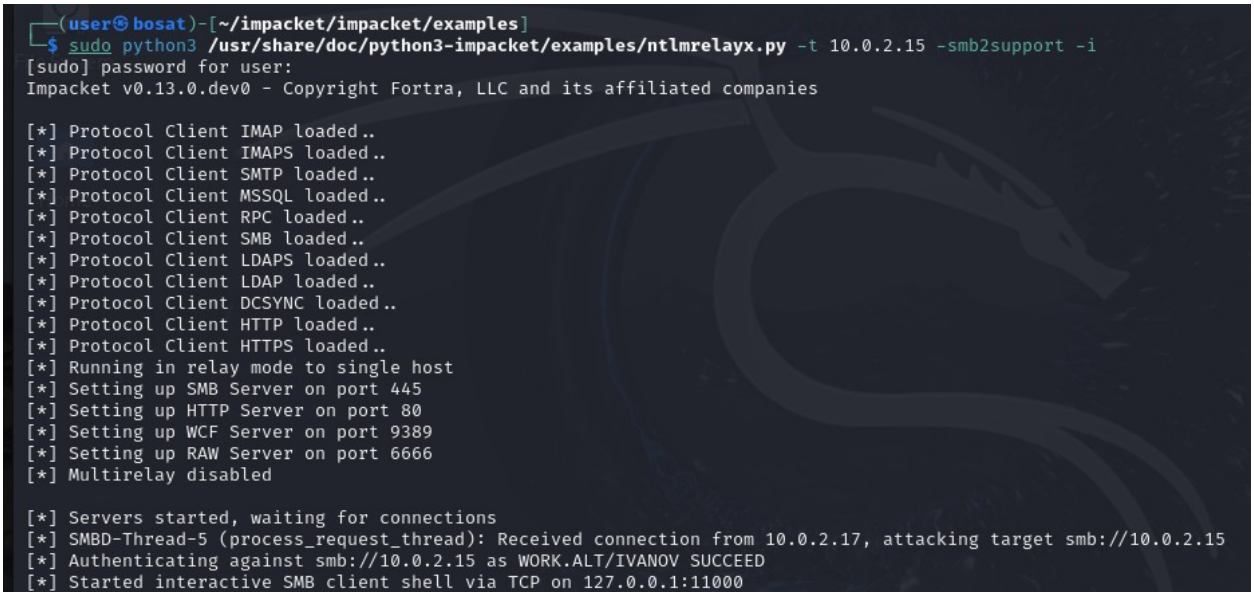

Рисунок 6 – Ретрансляция запроса

После установления сессии атакующий получил возможность выполнять действия от имени жертвы:

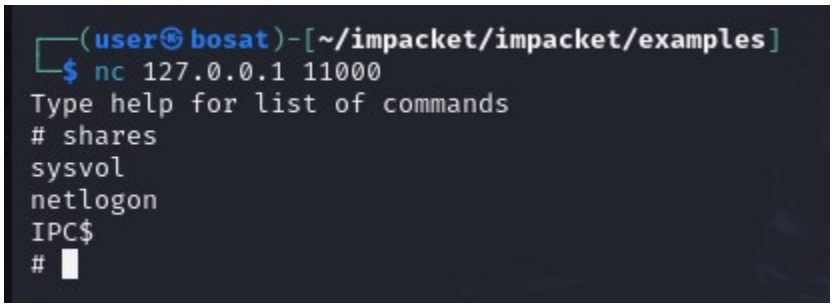

Рисунок 7 – Подключение к целевому ресурсу

«Альт Домен» изначально спроектирован с учетом требований безопасности: ОС «Альт СП» сертифицирована ФСТЭК и реализует российские криптографические стандарты. Сервер с развернутым «Альт Домен» поддерживает протоколы SMB2/SMB3 с шифрованием трафика, и по умолчанию использует проверку подлинности – SMB-подпись, для защиты от перехвата.

Для защиты от атаки SMB Relay в конфигурации Samba (/etc/samba/smb.conf) рекомендуется принудительно включить подпись SMB-сессий для клиентов и сервера. Пример настроек в секции global:

server signing = mandatory

client signing = mandatory

restrict anonymous = 2

disable netbios = yes

smb ports = 445

ntlm auth = mschapv2-and-ntlmv2-only

Параметр `restrict anonymous = 2` ограничивает анонимный доступ к контроллеру. Отключение NetBIOS и использование исключительно порта 445 обеспечивает работу только по современным протоколам. Отключение NTLMv1 исключает уязвимые подключения. При использовании этих мер, провести атаку станет невозможно:

Рисунок 8 – Демонстрация мер защиты

Для облегчения проведения атаки Kerberoasting были вручную настроены SPN-записи на одной из сервисных учётных записей, имитирующей типичную инфраструктуру с SQL-сервером, и были ослаблены криптографические настройки в файле конфигурации `smb.conf`, разрешив использование слабого алгоритма RC4. На атакующей машине под управлением Kali Linux был установлен и настроен инструмент GetUserSPNs.py из набора Impacket, реализующий механизм запроса SPN и извлечения сервисных билетов.

Атака запускалась из командной строки Kali Linux, после успешной аутентификации пользователя в домене. Запрос был направлен на получение

билетов сервисных учётных записей с SPN. Инструмент корректно обнаружил наличие сервиса и сформировал TGS-запрос к контроллеру домена.

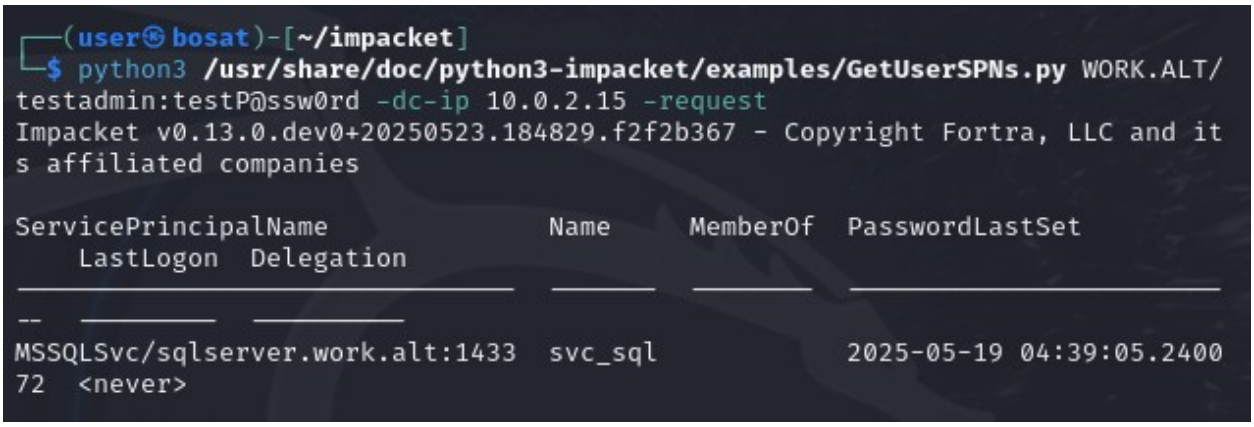

Рисунок 9 – Поиск активных SPN

Однако при попытке обработки ответа с билетом возникла ошибка Kerberos уровня: KRB_AP_ERR_INAPP_CKSUM, связанная с несовпадением типа подсчета контрольных сумм.

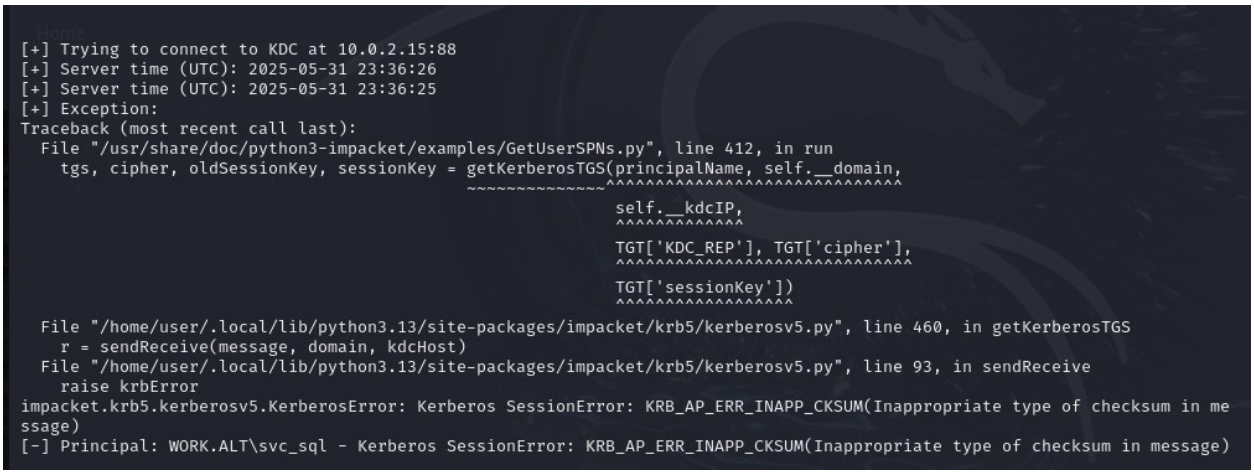

Рисунок 10 – Ошибка при проведении атаки

Ошибка указывает на то, что сгенерированный билет не может быть расшифрован или проверен из-за нарушения алгоритмической совместимости между клиентом и сервером. Несмотря на то, что были разрешены алгоритмы

RC4 и отключены современные типы шифрования (AES), Альт Домен в роли KDC продолжал применять криптографические механизмы, несовместимые с теми, которые ожидает утилита Impacket.

Следует отметить, что в отличие от классического Active Directory, Samba в качестве KDC имеет ограниченную поддержку алгоритмов и зачастую не реплицирует поведение Windows по умолчанию. Даже при наличии SPN и ослабленных политик, реализация протокола Kerberos на базе Samba может по-прежнему использовать алгоритмы и структуры пакетов, несовместимые с утилитами, рассчитанными на работу с Microsoft KDC. При всем этом протокол Kerberos работал без ошибок во взаимодействии с легитимными пользователями – выдача билетов, введение машин в домен осуществлялись успешно.

Защита от Kerberoasting включает в себя следующие настройки – в /var/lib/samba/private/krb5.conf или /etc/krb5.conf следует явно указать сильные алгоритмы шифрования – например, только AES-256/128 (и/или ГОСТ 28147) для ключей билетов Kerberos. Также необходимо запретить поддержку устаревших RC4/DES. Для критических сервисных аккаунтов необходимо снять флаги TrustedForDelegation и TrustedToAuthForDelegation. Учетные записи администраторов домена следует добавлять в группу Protected Users – это снимет использование NTLM/RC4 и запретит делегирование. Кроме того, не следует назначать лишние SPN (Service Principal Name) ненадежным учетным записям.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

В рамках данной работы была проведена теоретическая и практическая оценка безопасности доменной инфраструктуры, построенной на базе решения «Альт Домен». Основной задачей исследования являлась имитация

наиболее распространённых атак на службы аутентификации и сетевые протоколы (в частности, Pass-the-hash, SMB Relay и Kerberoasting), а также анализ эффективности встроенных и настраиваемых механизмов защиты в «Альт Домен» для противодействия подобным угрозам.

В ходе моделирования атак было установлено, что реализация домена на базе программно-аппаратного комплекса «Альт Домен» обеспечивает базовую защищённость за счёт ряда предустановленных параметров. В частности, по умолчанию в «Альт Домен» включена цифровая подпись SMB-соединений, реализована поддержка современных и отечественных криптографических алгоритмов, включая ГОСТ, а также предлагается использование механизма централизованных политик безопасности. Благодаря этим особенностям инфраструктура с «Альт Домен» уже на этапе развертывания имеет повышенный уровень устойчивости к распространённым атакам, нацеленных на перехват учетных данных, их повторное использование или подмену соединений.

Во время практической части работы удалось успешно провести атаку SMB Relay при отключении подписи SMB на целевой машине, что подтвердило уязвимость при нарушении рекомендуемой конфигурации. Моделирование атаки Pass-the-hash также увенчалось успехом при наличии захваченного хэша NTLM, что в очередной раз подчеркивает важность управления учетными записями и минимизации привилегий. Атака Kerberoasting не дала ожидаемых результатов из-за сбоев, связанных с криптографической несовместимостью, что, в свою очередь, демонстрирует защитную роль современных шифровальных алгоритмов и ограничений в реализации Kerberos на стороне контроллера домена.

ЗАКЛЮЧЕНИЕ

В работе были рассмотрены практические рекомендации по защите доменной инфраструктуры на базе «Альт Домен»: включение обязательной подписи и шифрования SMB-соединений, применение современных алгоритмов Kerberos, ограничение делегирования, отказ от устаревших схем аутентификации, настройка групповых политик и использование встроенных групп безопасности. Все предложенные меры могут быть реализованы средствами самой платформы без необходимости привлечения сторонних решений.

Таким образом, «Альт Домен» является конкурентной альтернативой для построения защищённой доменной инфраструктуры в организациях, предъявляющих высокие требования к информационной безопасности. Использование отечественных стандартов шифрования, сертифицированных ОС, гибких политик доступа и совместимости с AD-протоколами делает эту платформу особенно актуальной в условиях импортозамещения и повышенного внимания к вопросам защиты информационных систем.

Проведённый анализ и практическое моделирование подтверждают, что при корректной настройке и соблюдении рекомендаций «Альт Домен» способен эффективно противостоять целому ряду распространённых атак, сохраняя стабильность и совместимость с привычными для администраторов методами управления корпоративной сетью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. АЛЬТ ДОМЕН. Инструкция по установке. Ред. 2.0 [Электронный ресурс]. — URL: https://www.basealt.ru/fileadmin/user_upload/manual/ALT_Domain_install.pdf (дата обращения: 10.03.2025).

2. Альт Домен. Руководство администратора. Редакция апрель, 2025 [Электронный ресурс]. — URL: https://docs.altlinux.org/ru-RU/domain/10.4/html-single/alt-domain/index.html#domain-controller-login (дата обращения: 09.03.2025).

3. АЛЬТ ДОМЕН [Электронный ресурс]. — URL: https://www.basealt.ru/alt-domain (дата обращения: 10.03.2025).

4. Аутентификация в системах Windows. Часть 1: NTLM [Электронный ресурс]. — URL: https://interface31.ru/tech_it/2015/03/autentifikaciya-v-sistemah-windows-chast-1-ntlm.html (дата обращения: 25.02.2025).

5. Бекматов А.К., Эргашов Ф.Т. Обеспечение аутентификации в сети передачи данных // Экономика и социум. — 2025. — №1-2 (128). — URL: https://cyberleninka.ru/article/n/obespechenie-autentifikatsii-v-seti-peredachi-dannyh (дата обращения: 02.03.2025).

6. Основы Active Directory [Электронный ресурс]. — URL: https://xakep.ru/2024/10/15/active-directory-basics/ (дата обращения: 11.04.2025).

7. Романенко О.В., Осяева А.А. Миграция доменной инфраструктуры: ALT Linux как вариант импортозамещения // Вестник науки и образования. — 2024. — №9 (152)-2. — URL: https://cyberleninka.ru/article/n/migratsiya-domennoy-infrastruktury-alt-linux-kak-variant-importozamescheniya (дата обращения: 13.05.2025).

8. Руководство администратора. Доменная инфраструктура на базе Samba [Электронный ресурс]. — URL: https://docs.altlinux.org/ru-RU/domain/10.4/html-single/samba/index.html#id843 (дата обращения: 27.04.2025).

9. Скоропупов И.О., Бубнова А.А., Карманов И.Н. Методы проведения атак для получения прав администратора домена в Active Directory // Интерэкспо Гео-Сибирь. — 2019. — №1. — URL: https://cyberleninka.ru/article/n/metody-provedeniya-atak-dlya-polucheniya-prav-administratora-domena-v-active-directory (дата обращения: 02.05.2025).

10. Уймин А.Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование: практикум. — СПб.: Лань, 2024. — 116 с. — ISBN 978-5-507-48647-2.

11. Уймин А.Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1. — 3-е изд., стер. — СПб.: Лань, 2022. — 480 с. — ISBN 978-5-8114-9255-8.

12. Kerbrute: разведка Active Directory через Kerberos [Электронный ресурс]. — URL: https://www.securitylab.ru/blog/personal/SimlpeHacker/355272.php (дата обращения: 12.05.2025).

13. SMB Relay Attacks and How to Prevent Them in Active Directory [Электронный ресурс]. — URL: https://tcm-sec.com/smb-relay-attacks-and-how-to-prevent-them/ (дата обращения: 17.05.2025).