Корякин Владислав Юрьевич, *студент,*
РГУ нефти и газа (НИУ) имени И.М. Губкина,
г.Москва

Тищенко Эльдар Валерьевич*, студент,*
РГУ нефти и газа (НИУ) имени И.М. Губкина,
г.Москва

ОЦЕНКА ЗАЩИЩЕННОСТИ KERBEROS В FREEIPA НА ОС АЛЬТ МЕТОДИКОЙ OSSTMM

Аннотация. Переход российских организаций на отечественные доменные решения на базе FreeIPA повышает значимость оценки их защищенности, тогда как большинство работ по атакам на Kerberos выполнено для Microsoft Active Directory. В работе по методике OSSTMM с метриками Visibility, Access и Trust оценивается устойчивость базовой конфигурации FreeIPA в ОС Альт к типовым атакам на Kerberos; метрики характеризуют конфигурацию не только по факту успеха атаки, но и по барьеру входа атакующего и наблюдаемости его действий. На стенде из контроллера домена, веб-сервера, клиентской и атакующей машин реализованы три класса атак: разведка с перечислением учетных записей и подбором паролей, «человек посередине» с развертыванием поддельного KDC и компрометация keytab сервисной записи с эксплуатацией делегирования. Установлено, что конфигурация защищает от части классических атак за счет PKINIT и кэширования параметров KDC службой SSSD, но сохраняет уязвимые места в области видимости домена, парольной политики и настройки делегирования. Сформулированы рекомендации по усилению конфигурации, снижающие значения метрик Visibility, Access и Trust.

Ключевые слова: ОС Альт, FreeIPA, Kerberos, служба каталогов, тикет, принципал, OSSTMM, делегирование.

Abstract. The transition of Russian organizations to domestic domain solutions based on FreeIPA increases the importance of assessing their security, while most works on Kerberos attacks are performed for Microsoft Active Directory. In the OSSTMM methodology with Visibility, Access, and Trust metrics, the stability of the

basic FreeIPA configuration in OS Alt is evaluated against typical Kerberos attacks; metrics characterize the configuration not only by the fact of attack success, but also by the attacker's entry barrier and the observability of their actions. On the stand of a domain controller, a web server, a client and an attacking machine, three classes of attacks are implemented: reconnaissance with enumeration of accounts and password guessing, “man in the middle” with deployment of a fake KDC and compromise of the keytab of a service account with exploitation of delegation. It is established that the configuration protects against part of the classic attacks due to PKINIT and caching of KDC parameters by the SSSD service, but retains vulnerabilities in the domain visibility area, password policy and delegation settings. Recommendations have been formulated to strengthen the configuration, reducing the values of the Visibility, Access, and Trust metrics.

Keywords: OS Alt, FreeIPA, Kerberos, directory service, ticket, principal, OSSTMM, delegation.

ВВЕДЕНИЕ

Современная ИТ-инфраструктура управляется службой каталогов, централизованно хранящей данные о пользователях, устройствах и политиках. Службы каталогов (Microsoft AD, FreeIPA) решают задачи управления, аутентификации, авторизации, делегирования прав и масштабирования [4]. Согласно источнику [5], служба каталогов обеспечивает единый защищенный протокол доставки разнородных данных и иерархическую модель с разграничением прав, что делает ее пригодной для систем с высокими требованиями к безопасности. На этом построена FreeIPA, объединяющая службу каталогов, Kerberos и удостоверяющий центр.

Актуальность обусловлена ростом атак на Kerberos: по [6], число атак с компрометацией учетных данных и Kerberos выросло на 583 % за 2023 год. Одновременно идет переход на отечественные продукты и открытое ПО, так, исходя из источника [7], можно заметить, что замена Active Directory стала массовой практикой. При этом большинство работ, включая, рассматривают Kerberos в Windows с Active Directory, а защищенность отечественных решений изучена слабее. Как отмечается в [8], открытое ПО несет риски (медленное устранение уязвимостей, отсутствие гарантированной поддержки, сложность аудита), частично снимаемые вендорским сопровождением. На рынке есть несколько решений на базе FreeIPA (ALD Pro, «Атом.ДОМЕН», Dynamic

Directory), поэтому она выбрана объектом: атаки на ее базовую реализацию актуальны и для производных продуктов.

Объект исследования – инфраструктура FreeIPA, развернутая в ОС Альт.

Предмет исследования – устойчивость службы аутентификации Kerberos в составе FreeIPA к типовым атакам.

Цель работы: оценить устойчивость базовой конфигурации FreeIPA в ОС Альт к атакам на протокол Kerberos по методике OSSTMM с использованием метрик Visibility, Access и Trust.

Для достижения цели поставлены следующие задачи:

1. развернуть тестовый стенд, воспроизводящий типовую инфраструктуру FreeIPA в ОС Альт;

2. провести эксперимент по разведке с перечислением учетных записей и подбором паролей;

3. провести эксперимент по атаке «человек посередине» с развертыванием поддельного KDC;

4. провести эксперимент по компрометации keytab-файла с эксплуатацией механизма делегирования;

5. формализовать результаты по метрикам OSSTMM и сопоставить их с техниками матрицы MITRE ATT&CK [1];

6. сформулировать рекомендации по усилению конфигурации.

Научная новизна состоит в применении методики OSSTMM с количественными по смыслу метриками Visibility, Access и Trust к инфраструктуре FreeIPA в отечественной ОС Альт. Подобных публикаций по отечественным доменным решениям существенно меньше, чем по Active Directory, что и определяет вклад работы.

Практическая значимость заключается в том, что полученные результаты и сформулированные рекомендации применимы не только к FreeIPA, но и к производным отечественным продуктам (ALD Pro, «Атом.ДОМЕН», Dynamic Directory), построенным на ее основе.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ

FreeIPA представляет собой интегрированную платформу управления идентификацией и доступом для Linux-инфраструктур, объединяющую в едином решении ряд компонентов: службу каталогов 389 Directory Server (LDAP), систему сетевой аутентификации MIT Kerberos, удостоверяющий центр Dogtag PKI, DNS-сервер BIND и механизмы контроля доступа на основе хостов (HBAC) и sudo-правил [2]. Перечень основных служб и используемых ими сетевых портов приведен в таблице 1.

Таблица 1 – Компоненты FreeIPA и сетевые порты

Компонент	**Порт**
Kerberos	88, 464
Named (BIND)	53
Directory Service (LDAP)	389, 636
httpd	80, 443
NTP	123

Записи пользователей и сервисов хранятся в каталоге LDAP и одновременно служат базой Kerberos-принципалов через атрибуты krbPrincipalName, krbPrincipalKey и сопутствующие. На клиентской стороне взаимодействие с доменом обеспечивает служба SSSD, кэширующая данные о пользователях, группах и политиках и фиксирующая параметры подключения к KDC при вводе хоста в домен.

Концентрация критичных функций в одной системе делает контроллер домена высокоценной целью: компрометация сервера дает доступ к каталогу пользователей, контроль над выдачей тикетов, управление HBAC и закрытые ключи удостоверяющего центра.

Роль протокола Kerberos в FreeIPA

FreeIPA использует Kerberos v5 в реализации MIT (служба krb5kdc) [15]. Особенности интеграции Kerberos в составе FreeIPA на ОС Альт описаны в документации дистрибутива [12]. Протокол реализует трехстороннюю модель доверия между клиентом, сервисом и доверенной третьей стороной – Центром распределения ключей (KDC). KDC разделен на службу аутентификации (AS), проверяющую личность пользователя, и службу выдачи тикетов (TGS), выдающую сервисные тикеты по уже полученному мандату.

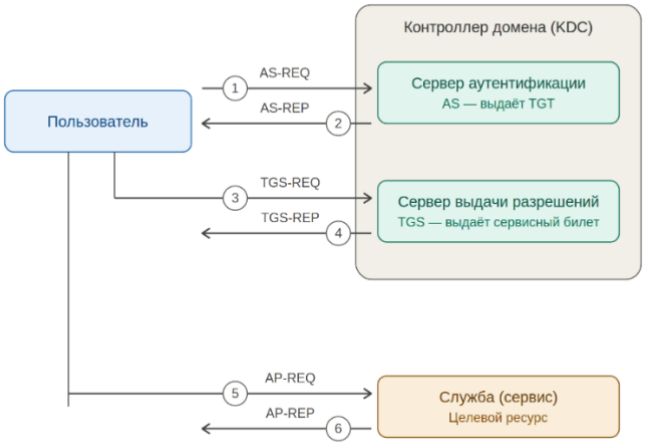

Рисунок 1 – Схема аутентификации по протоколу Kerberos

Аутентификация двухэтапна. Клиент шлет в AS запрос AS-REQ с идентификатором принципала и меткой времени, зашифрованной долгосрочным ключом; в ответ AS-REP приходит Ticket-Granting Ticket (TGT) и сессионный ключ. Затем клиент предъявляет TGT службе TGS и получает сервисный тикет, зашифрованный ключом целевого сервиса. Пароль при этом по сети не передается [15]. Время жизни тикета в базовой конфигурации – 24 часа.

База принципалов (пользовательских и сервисных) размещается в LDAP, а операции над ней выполняет служба kadmin. Для автоматической аутентификации сервисов и хостов без ввода пароля применяются keytab-файлы с долгосрочными ключами принципалов. Системный keytab хоста (/etc/krb5.keytab) использует SSSD, а для отдельных сервисов keytab выпускается администратором.

Классы атак на протокол Kerberos

Атаки на Kerberos изучены преимущественно для Microsoft Active Directory и делятся на несколько классов [3]. На этапе разведки и первичной аутентификации – AsReqRoasting, AsRepRoasting (получение pre-auth данных для оффлайн-перебора) и password spraying (подбор распространенных паролей по списку учетных записей). Отдельный класс – Kerberoasting, запрос сервисных тикетов с оффлайн-восстановлением паролей сервисных записей [9]. К атакам на канал относятся подмена KDC (Rogue KDC) с ARP/DNS-спуфингом и downgrade-атаки на метод pre-auth, опирающиеся на сохранение устаревшего encrypted-timestamp [15]. Отдельную группу образуют атаки на хранилища секретов –

кража тикетов (Pass-the-Ticket) и компрометация keytab-файлов с эксплуатацией делегирования.

Источник [9] систематизирует эти методы по статистике Positive Technologies, согласно которой Kerberoasting применялся в 61 % внутренних пентестов; в [10] он рассмотрен как элемент целевых атак с кейсами обнаружения. По отечественным решениям на базе FreeIPA таких публикаций существенно меньше. В работе реализуются три класса атак на FreeIPA: разведка с перебором учетных записей, «человек посередине» с подменой KDC и компрометация keytab с эксплуатацией делегирования.

МАТЕРИАЛЫ И МЕТОДЫ

Для проведения экспериментов был развернут тестовый стенд (рисунок 2, таблица 2). Во всех экспериментах предполагается, что у атакующего есть доступ к сети, в которой развернут домен.

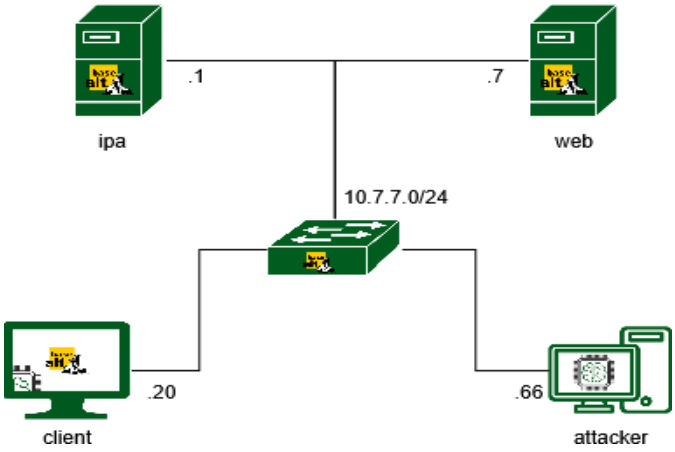

Рисунок 2 – Топология сети

Таблица 2 – Описание стенда

Хост	RAM/CPU	ОС	IP-адрес	Роль
ipa.test.ru	4 Гб / 2	Alt-server 11.1	10.7.7.1	Контроллер домена
web.test.ru	2 Гб / 2	Alt-server 11.1	10.7.7.7	Веб-сервер с ресурсами
client.test.ru	1 Гб / 2	Alt-workstation 11.1	10.7.7.20	Клиентская машина
attacker	1 Гб / 2	Kali Linux / Alt-workstation 11.1	10.7.7.66	Атакующая машина

Таблица 3 – Набор инструментов

Название	Версия	Описание

Nmap	7.98	Построение карты сети
dig	9.20.20	Опрос DNS-сервера
Kerbrute	1.0.3	Перебор пользователей домена
impacket	0.14.0.dev0	Перебор пользователей домена
bettercap	2.41.5	Перехват пакетов в сети
dsniff	2.5a2	ARP- и DNS-спуфинг
tcpdump	4.99.6	Анализ сетевого трафика
ipa-getkeytab	4.x	Получение keytab-файла сервиса

В сравнительном анализе методик [8] OSSTMM характеризуется как формализованный и структурированный документ, ориентированный на тестирование сетей и содержащий раздел метрик безопасности [11]. Это определило его выбор: метрики Visibility, Access и Trust формализуют оценку не только по факту успеха атаки, но и по барьеру входа атакующего и наблюдаемости со стороны защитника, чего нет в альтернативных методиках (ISSAF, PTES, PETA), описывающих этапы тестирования без количественной оценки [13].

Для воспроизводимости каждый эксперимент повторен трижды с одинаковым результатом; перед каждым повторением стенд откатывался до контрольной точки.

ЭКСПЕРИМЕНТАЛЬНАЯ ЧАСТЬ

Эксперимент 1. Сбор информации: разведка

Предполагается, что базовая конфигурация оставляет открытыми основные каналы разведки – анонимные LDAP-запросы, публичные DNS-записи сервисов и перечисление принципалов через KDC, – а слабая парольная политика делает реализуемой password spraying.

Цель эксперимента: определить, что видит внешний атакующий, есть ли сервисы, доступные без аутентификации, и где проходят границы доверия.

Сканирование сети показало, что LDAP по умолчанию поддерживает анонимные запросы, а опрос DNS-сервера утилитой dig дал точную информацию о KDC. Поскольку анонимные запросы в службе каталогов разрешены, через них получены структура домена, контейнеры объектов и полный список пользователей (рисунок 3); при этом запросы фиксируются в журналах.

Рисунок 3 – Запрос LDAP и получение списка пользователей

Имея список учетных записей, можно перейти к перебору паролей по словарю. Попытка получить TGT через impacket не удалась, так как pre-auth включена по умолчанию.

Перебор паролей выполнялся утилитой kerbrute. В базовой конфигурации учетная запись блокируется после шести неуспешных попыток, но окно сброса счетчика не превышает минуты, что позволяет перебирать пароли, минуя блокировку. Каждая попытка фиксируется в /var/log/krb5kdc.log.

Ограничения и реалистичность. Сценарий требует лишь сетевого доступа к сегменту домена и стандартных утилит, что делает его наиболее реалистичным из трех: разведка доступна и внешнему нарушителю, и инсайдеру. Действия фиксируются в журналах LDAP и KDC, поэтому при мониторинге обнаруживаются, хотя факт раскрытия данных это не предотвращает.

Оценка по OSSTMM. Visibility – высокая: без аутентификации атакующий получает полную карту инфраструктуры (порты, SRV-записи KDC и LDAP, структуру домена, контейнеры пользователей, версию FreeIPA и публичную часть сертификата УЦ). Access – низкий барьер: достаточно сетевой видимости сервера, нужны лишь стандартные утилиты (nmap, dig, ldapsearch, kerbrute). Trust – избыточное: конфигурация доверяет анонимным LDAP-запросам без проверки подлинности, а парольная политика не требует длины и сложности пароля, что делает реализуемой password spraying.

После харденинга, включающего запрет анонимных запросов, получить список пользователей и структуру каталога не удастся. Это также усложнит атаку перебором, так как не будет словаря возможных имен. В рамках усиления безопасности следует установить более строгую парольную политику и уменьшить число допустимых неверных попыток ввода пароля до трех – в результате перебор станет неэффективным.

Эксперимент покрывает техники T1046, T1087.002, T1590.002, T1590.005 и T1110.003 матрицы MITRE ATT&CK.

Эксперимент 2. Rogue KDC + DNS/ARP-спуфинг

Предполагается, что Rogue KDC с ARP/DNS-спуфингом в базовой конфигурации нереализуема из-за PKINIT [14] и кэширования параметров KDC службой SSSD, но допускает downgrade-атаку с последующим оффлайн-восстановлением пароля.

Цель: проверить, доверяет ли клиент FreeIPA подмененному KDC и отдает ли зашифрованные pre-auth данные для последующей оффлайн-атаки.

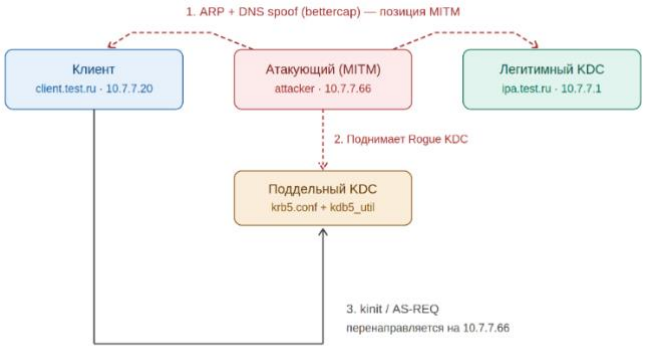

Рисунок 4 – Схема атаки Rogue KDC

Для реализации атаки необходимо развернуть поддельный KDC на атакующей машине и запустить ARP- и DNS-спуфинг.

При подмене DNS поддельный ответ запаздывал относительно легитимного на 200–300 мс, поэтому ответы легитимного сервера приходилось блокировать внутри сети.

При первых попытках клиент отказывался получать тикет, обращаясь к легитимному сервису из-за кэша SSSD.

После перезапуска SSSD клиент перезаписал данные о KDC и стал обращаться к поддельному KDC, считая его легитимным.

```
[root@client ~]# kinit admin
Password for admin@TEST.RU:
kinit: Password incorrect while getting initial credentials
[root@client ~]# kinit admin
Password for admin@TEST.RU:
[root@client ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@TEST.RU

Valid starting       Expires              Service principal
09.05.2026 02:45:15  10.05.2026 02:45:15  krbtgt/TEST.RU@TEST.RU
[root@client ~]#
```

Рисунок 5 – Запрос TGT

Атака срабатывает только при вводе устройства в домен или перезагрузке: однажды увидев адрес легитимного сервиса, клиент продолжает обращаться к нему из-за кэша SSSD.

Поддельный KDC не предлагает SPAKE и PKINIT, из-за чего клиент соглашается на понижение метода pre-auth. Сравнение поведения настоящего и поддельного KDC приведено в таблице 4.

Таблица 4 – Сравнение настоящего и поддельного KDC

Параметр	**Настоящий KDC**	**Поддельный KDC**
Предложено типов pre-auth	7	1
Выбранный клиентом метод	PA-SPAKE	PA-ETYPE-INFO2
Результат	Клиент получает легитимный тикет	Клиент получает поддельный тикет

Для защиты следует запретить понижение метода pre-auth и прописать адрес легитимного KDC в конфигурации Kerberos напрямую.

Ограничения и реалистичность. Условие успеха – сброс кэша SSSD – сужает применимость, но не делает атаку надуманной. Окно инициализации SSSD достижимо при массовом развертывании клиентов, плановых перезагрузках (в том числе после обновлений) и повторном вводе хоста в домен; атакующий в L2-сегменте может дождаться такого окна или спровоцировать перезагрузку клиента. Сценарий менее универсален, чем разведка, но практически значим для сетей с регулярной ротацией рабочих мест.

Оценка по OSSTMM. Visibility – активная фаза наблюдаема: характерный Gratuitous ARP, дублирующиеся DNS-ответы, поддельные сессии на порту 88, а также отсутствие записей в /var/log/krb5kdc.log при работающем клиенте; подготовительная фаза пассивна. Access – средний барьер: нужны позиция в L2-сегменте клиента и окно инициализации SSSD, учетные данные домена не требуются. Trust – избыточное на трех уровнях: клиент принимает DNS-ответ об адресе KDC без верификации, не требует взаимной проверки подлинности сервера и соглашается на понижение pre-auth без подтверждения.

Сценарий покрывает техники T1557.002 (ARP Cache Poisoning), T1565.002 (Transmitted Data Manipulation) в части подмены DNS-ответов, T1556 (Modify Authentication Process) при развертывании поддельного KDC, T1040 (Network Sniffing) и T1558 (Steal or Forge Kerberos Tickets) как целевую технику.

Эксперимент 3. Компрометация keytab-файла и делегирование

Владение keytab криптографически эквивалентно знанию пароля сервисного принципала и позволяет получить TGT от имени сервиса с любой машины с доступом к KDC. Дальнейшие возможности определяются правилами делегирования для скомпрометированного сервиса.

Предполагается, что без правил делегирования компрометация keytab ограничивает атакующего аутентификацией от имени самого сервиса, тогда как делегирование через S4U2Proxy открывает получение тикетов к целевым сервисам от имени произвольных пользователей.

Цель: проверить, что позволяет атакующему компрометация keytab-файла сервиса и как на это влияет настройка правил делегирования.

Сервис создан командой ipa service-add HTTP/web.test.ru, для него выпущен keytab (ipa-getkeytab) и скопирован на машину атакующего – это моделирует кражу keytab с веб-сервера.

Из keytab командой kinit -k -t получен TGT, затем командой kvno запрошен билет для admin к тому же сервису; klist подтвердил его получение (рисунок 6).

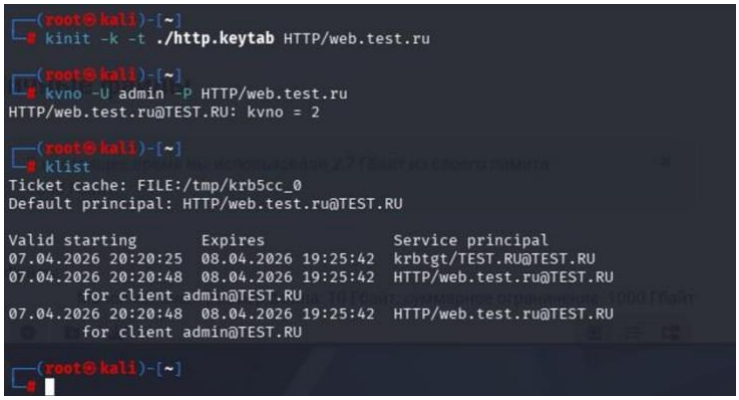

Рисунок 6 – Получение тикета

Затем от имени admin запрошен билет к стороннему сервису ldap/ipa.test.ru – без правил делегирования KDC ответил отказом.

После создания группы делегирования удалось получить тикеты к целевому сервису от имени произвольного пользователя. При избыточных правилах делегирования это открывает доступ к произвольным сервисам в области делегирования.

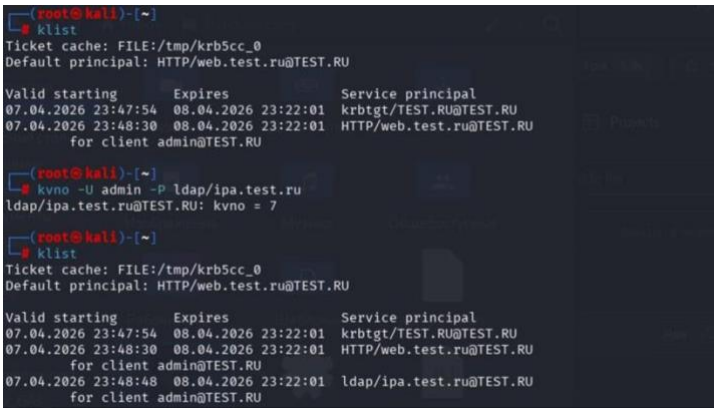

Рисунок 7 – Получение тикетов после настройки делегирования

Парное сравнение подтвердило гипотезу: без делегирования запрос через S4U2Proxy отклонен, после настройки – тикет от имени произвольного пользователя выдан. Это подтверждает роль делегирования как точки эскалации привилегий при компрометации сервисных записей.

Ограничения и реалистичность. Сценарий требует предварительной компрометации хоста с keytab – самый высокий входной барьер из трех, – но описывает фазу пост-эксплуатации: кража keytab превращает локальную компрометацию одного узла в аутентификацию от имени сервиса по всей сети. Реалистичность зависит от прав доступа к keytab и широты делегирования: при минимальных привилегиях ущерб ограничен, при ошибочно широком делегировании сценарий становится критическим.

Оценка по OSSTMM. Visibility – низкая: кража keytab локальна и не порождает сетевых событий, а kinit -k и kvno неотличимы от штатной аутентификации – в журнале фиксируется лишь факт выдачи тикетов. Access – высокий барьер на входе, низкий после получения keytab: нужна компрометация хоста с файлом, но затем keytab годен для аутентификации с любой машины до ротации ключа. Trust – избыточное: владение keytab признается доказательством подлинности сервиса, а делегирование дает право выпускать тикеты от имени произвольного пользователя через S4U2Proxy, из-за чего при широкой политике компрометация одного сервиса распространяется на все сервисы области правила.

Эксперимент показывает, что в базовой конфигурации FreeIPA устойчивость к компрометации keytab определяется не криптографическими свойствами протокола, а строгостью прав доступа к файлу и минимальностью правил делегирования. Сценарий покрывает техники T1552.004 (Unsecured Credentials: Private Keys), T1558 и T1558.003 матрицы MITRE ATT&CK.

ОБОБЩЕНИЕ РЕЗУЛЬТАТОВ

Результаты трех экспериментов сведены в три таблицы. Таблица 5 сопоставляет каждый эксперимент с техниками MITRE ATT&CK, результатом и рекомендацией по митигации. Таблица 6 содержит итоговые оценки по метрикам OSSTMM. Таблица 7 обобщает барьер входа и реалистичность каждого сценария в боевых условиях.

Таблица 5 – Сопоставление экспериментов с техниками MITRE ATT&CK и мерами защиты

Эксперимент	Техники MITRE ATT&CK	Результат	Рекомендация по митигации
Разведка	T1046, T1087.002, T1590.002, T1590.005, T1110.003	Получены структура домена, список учетных записей и метаданные сервисов; реализуем password spraying	Запретить анонимные LDAP-запросы; ужесточить парольную политику; снизить порог блокировки до трех попыток
Rogue KDC	T1557.002, T1565.002, T1556, T1040, T1558	Прямая подмена KDC невозможна из-за SSSD и PKINIT; реализуема downgrade-атака при перезапуске SSSD	Запретить понижение метода pre-auth; прописать адрес легитимного KDC в конфигурации Kerberos
Keytab + делегирование	T1552.004, T1558, T1558.003	Без делегирования – доступ только от имени сервиса; при делегировании – тикеты от имени любого пользователя	Ограничить права доступа к keytab; минимизировать правила делегирования; ротация ключей и аудит ipa-getkeytab

Таблица 6 – Итоговые оценки по метрикам OSSTMM

Эксперимент	Visibility	Access	Trust
Разведка	Высокая	Низкий барьер входа	Избыточное
Rogue KDC	Высокая в активной фазе	Средний барьер	Избыточное
Keytab + делегирование	Низкая	Высокий на входе, низкий после кражи	Избыточное

Таблица 7 – Барьер входа и реалистичность сценариев

Эксперимент	Барьер входа	Реалистичность в боевых условиях
Разведка	Минимальный (только сетевой доступ)	Высокая: выполнима внешним нарушителем и инсайдером в любой момент, без особых условий

Rogue KDC	Средний (позиция в L2 + окно инициализации SSSD)	Умеренная: требует совпадения с перезагрузкой или вводом в домен; значима при массовом развертывании и плановых перезагрузках
Keytab + делегирование	Высокий (предварительная компрометация хоста)	Зависит от окружения: критична при широком делегировании, ограничена при минимальных привилегиях; фаза пост-эксплуатации

РЕКОМЕНДАЦИИ ПО ХАРДЕНИНГУ

По результатам экспериментов сформулированы рекомендации по усилению конфигурации FreeIPA для снижения метрик Visibility, Access и Trust; для ключевых мер приведены конкретные команды.

Запрет анонимных LDAP-запросов. Анонимный доступ в 389 Directory Server управляется атрибутом nsslapd-allow-anonymous-access. Значение rootdse закрывает перечисление структуры домена и учетных записей, оставляя только корневой DSE:

```
ldapmodify -D "cn=Directory Manager" -W << EOF
dn: cn=config
changetype: modify
replace: nsslapd-allow-anonymous-access
nsslapd-allow-anonymous-access: rootdse
EOF
```

После применения ldapsearch -x к cn=users возвращает пустой результат.

Ужесточение парольной политики и порога блокировки. Политика задается через ipa pwpolicy-mod. Снижение порога блокировки до трех попыток с увеличением окна сброса счетчика делает password spraying неэффективным:

```
ipa pwpolicy-mod --minlength=12 --maxfail=3 \
    --lockouttime=1800 --failinterval=900
```

Ключевой параметр – failinterval: в базовой конфигурации окно сброса (около минуты) позволяло перебор «по кругу»; его увеличение лишает атакующего этой возможности.

Запрет понижения метода предварительной аутентификации. Downgrade на encrypted-timestamp устраняется отключением устаревшего метода в /etc/krb5.conf (секция [kdcdefaults]), где оставляются только SPAKE и PKINIT:

```
[kdcdefaults]
    pkinit_anchors = FILE:/etc/ipa/ca.crt
    disable_encrypted_timestamp = true
```

После этого поддельный KDC, не умеющий SPAKE/PKINIT, не сможет навязать клиенту слабый метод – клиент откажется от аутентификации вместо понижения. *Примечание: точное имя параметра и его поддержка зависят от версии сборки krb5 в конкретном выпуске ОС Альт, поэтому перед внедрением команду следует проверить на стенде.*

Остальные меры носят организационно-конфигурационный характер:

– прописать адрес легитимного KDC в секции [realms] файла /etc/krb5.conf напрямую, снизив зависимость от подменяемого DNS;

– ограничить права доступа к keytab-файлам на уровне файловой системы (chmod 600, владелец – соответствующая сервисная учетная запись), регулярно проводить ротацию ключей командой ipa-getkeytab и вести аудит ее вызовов;

– минимизировать число сервисов с правом делегирования и строго ограничивать перечень целевых сервисов в правилах S4U2Proxy.

ВЫВОДЫ

По методике OSSTMM оценена устойчивость базовой конфигурации FreeIPA в ОС Альт к атакам на Kerberos в трех экспериментах – разведка, перехват канала аутентификации и эксплуатация сервисных записей. Разведка показала, что без аутентификации раскрываются структура домена, перечень учетных записей и метаданные сервисов через анонимный LDAP, а слабая парольная политика делает реализуемой password spraying. Прямая подмена KDC нереализуема благодаря PKINIT и кэшированию параметров службой SSSD, но сохранение encrypted-timestamp допускает downgrade-атаку при совпадении с окном инициализации SSSD. Компрометация keytab без делегирования ограничена аутентификацией от имени сервиса, тогда как широкое делегирование через S4U2Proxy дает тикеты от имени произвольных пользователей.

В итоге базовая конфигурация защищает от части классических атак за счет обязательного PKINIT и фиксации параметров KDC службой SSSD, но сохраняет уязвимые места: анонимный LDAP, минимальную парольную политику, устаревшие методы pre-auth и риск некорректного делегирования. Сопоставление с работами по Active Directory подтверждает применимость этого класса атак к отечественным решениям, что обосновывает необходимость усиления конфигурации по сформулированным рекомендациям.

СПИСОК ЛИТЕРАТУРЫ

1. Enterprise Matrix // MITRE ATT&CK. URL: https://attack.mitre.org/matrices/enterprise/ (дата обращения: 17.05.2026).
2. FreeIPA // ALT Linux Wiki. URL: https://www.altlinux.org/FreeIPA (дата обращения: 17.05.2026).
3. Воробьев П. А., Зиятдинов Н. Р., Сенцова А. Ю. Практическое исследование протокола Kerberos: атаки, обнаружение и разработка правил детектирования // Инженерный вестник Дона. – 2025. – № 2.
4. Петров М.А. ОСНОВНЫЕ КОМПОНЕНТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ // Вестник науки. - 2024. - №8 (77). - С. 154-158.
5. CrowdStrike 2023 Threat Hunting Report // CrowdStrike. URL: https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-2023-threat-hunting-report-reveals-identity-based/ (дата обращения: 17.05.2026).
6. Боцман С. А., Карасева Е. И. Замена Active Directory на отечественные аналоги: анализ, выбор и внедрение // Universum: технические науки. – 2025. – № 8 (137). – С. 11–15.
7. Макаренко С. И., Смирнов Г. Е. Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. – 2020. – № 4. – С. 44–72.
8. Роденко М. П., Оленников А. А. Методы проведения атак на протокол аутентификации Kerberos в Active Directory и способы защиты от них // Математическое и информационное моделирование: материалы Всероссийской конференции молодых ученых. – 2023. – № 21. – С. 350–356.
9. Demers D., Lee H. Kerberoasting: Case Studies of an Attack on a Cryptographic Authentication Technology // International Journal of Cybersecurity Intelligence & Cybercrime. – 2022. – № 5(2). – С. 25–39.
10. Козлов А. В. Тестирование и анализ атак на криптопротокол Kerberos с помощью программного стенда системы аутентификации // Информатика и вычислительная техника и управление. – 2021. – № 5. – С. 80–84.

11. OSSTMM 3 – The Open Source Security Testing Methodology Manual / ISECOM, 2010. URL: https://www.isecom.org/OSSTMM.3.pdf (дата обращения: 17.05.2026).
12. Домен/Kerberos // ALT Linux Wiki. URL: https://www.altlinux.org/Домен/Kerberos (дата обращения: 17.05.2026).
13. RFC 4120. The Kerberos Network Authentication Service (V5) / C. Neuman, T. Yu, S. Hartman, K. Raeburn. – IETF, 2005. – URL: https://www.rfc-editor.org/rfc/rfc4120 (дата обращения: 17.05.2026).
14. RFC 4556. Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) / L. Zhu, B. Tung. – IETF, 2006. – URL: https://www.rfc-editor.org/rfc/rfc4556 (дата обращения: 17.05.2026).
15. Положий А.А. АНАЛИЗ ЗАЩИЩЕННОСТИ ДОМЕННОЙ ИНФРАСТРУКТУРЫ НА БАЗЕ «АЛЬТ ДОМЕН» // Теория и практика современной науки. - 2025. - №6 (120). - С. 334-345.