DOI 10.37882/2223–2966.2021.05.16

ТЕСТИРОВАНИЕ И АНАЛИЗ АТАК НА КРИПТОПРОТОКОЛ KERBEROS С ПОМОЩЬЮ ПРОГРАММНОГО СТЕНДА СИСТЕМЫ АУТЕНТИФИКАЦИИ

Козлов Александр Владимирович
К.т.н., доцент, Российский технологический университет МИРЭА, г. Москва
kozlov.card@gmail.com

Аннотация. В статье рассмотрен криптографический протокол Kerberos, позволяющий проводить взаимную аутентификацию сервиса и пользователя, при этом, не используя ключ шифрования пользователя в явном виде для доступа к сервисам. Данный алгоритм является результатом длительной эволюции одной из вариаций протокола Нидхема-Шрёдера.

В статье приводится структура тестового стенда для проведения моделирования основных атак на криптографический протокол Kerberos и анализа его уязвимостей. В статье описаны результаты моделирования основных атак на криптографический протокол Kerberos и проведен анализ основных уязвимостей данного протокола. Данная статья полезна для проведения криптоанализа протокола Kerberos и дальнейшего развития указанного протокола, например для реализации многофакторной аутентификации в многофункциональных информационных системах.

Ключевые слова: аутентификация, протокол, Kerberos, керберизация, уязвимости.

TESTING AND ANALYSIS OF ATTACKS ON THE KERBEROS CRYPTOPROTOCOL USING THE AUTHENTICATION SYSTEM SOFTWARE STAND

A. Kozlov

Summary. The article discusses the cryptographic protocol Kerberos, which allows for mutual authentication of the service and the user, while not using the user's encryption key explicitly to access the services. This algorithm is the result of a long evolution of one of the variations of the Needham-Schroeder protocol.

The article presents the structure of a test bench for modeling the main attacks on the Kerberos cryptographic protocol and analyzing its vulnerabilities. The article describes the results of modeling the main attacks on the Kerberos cryptographic protocol and analyzes the main vulnerabilities of this protocol. This article is useful for conducting cryptanalysis of the Kerberos protocol and further development of this protocol, for example, for implementing multi-factor authentication in multifunctional information systems.

Keywords: authentication, protocol, Kerberos, kerberization, vulnerabilities.

В настоящее время задача аутентификации становится наиболее актуальной в связи с развитием информационного общества и информационных технологий в целом.

Алгоритмы аутентификации, авторизации и идентификации на данный момент являются неотъемлемой частью систем управления доступом, систем информационной безопасности.

На данный момент существует множество методов и алгоритмов аутентификации, у всех есть свои преимущества и недостатки. В данной статье наиболее детально рассмотрен протокол Kerberos, позволяющий проводить взаимную аутентификацию сервиса и пользователя, при этом, не используя ключ пользователя в явном виде для доступа к сервисам.

Целью данной статьи является тестирование атак на протокол Kerberos на базе программного стенда системы аутентификации.

Протокол аутентификации Kerberos

Kerberos — протокол аутентификации, предназначенный для двустороннего подтверждения подлинности пользователей, сервисов и других сущностей в сети.

Основным узлом инфраструктуры Kerberos является KDC — Key Distribution Center или Центр Распределения Ключей [1, 2, 3]. Для отказоустойчивости и балансировки нагрузки на информационные системы, часто разворачивают несколько KDC. Стоит отметить, что для более высокой отказоустойчивости KDC разворачиваются на отдельных физических машинах. Системных ресур-

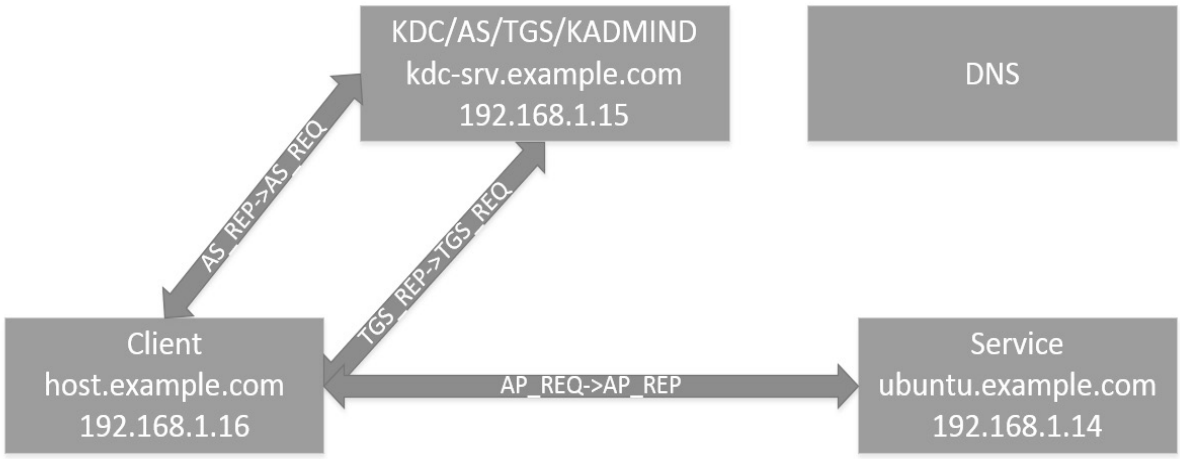

Рис. 1. Схема стенда

сов KDC потребляет немного. KDC можно представить в виде трех логических компонентов:

- База данных всех principals и ключей шифрования, ассоциированных с ними
- AS (Authentication Server) — сервер аутентификации, создающий TGT (Ticket Granting Ticket) и выдающий его в пользование клиентам, входящим в текущий realm.
- TGS (Ticket Granting Server) — сервер, управляющий и выдающий тикеты клиентам, сделавшим запрос на аутентификацию в некотором сервисе.

Протокол Kerberos 4 основан на протоколе Нидхема-Шредера с двумя основными изменениями.

Первое изменение уменьшило количество сетевых сообщений, передаваемых между клиентом и сервером аутентификации. Оригинальный протокол не имел никакой зависимости от времени, но зато имел два лишних обмена сообщениями. В Kerberos 4 у всех участников обмена должно было быть синхронизировано время и используется локальное время клиента.

Второе, более значительное изменение — создание концепции TGT (Ticket Granting Ticket), позволяющее пользователям аутентифицироваться на всех сервисах, введя свой секретный ключ только один раз.

Таким образом, сервер аутентификации был разделен на Ticket Granting Server (TGS) и сам Authentication Server (AS). Также в Kerberos 4 введен регулируемый срок жизни тикетов.

Kerberos 5 — новая версия протокола [1, 2, 5]. Если рассматривать исключительно функциональность новой версии протокола, то Kerberos 5 это Kerberos 4 с некоторым количеством расширений. Однако, с точки зрения внутреннего устройства, Kerberos 5 — совершенно новый протокол и изнутри абсолютно непохожий на Kerberos 4.

Новые возможности Kerberos 5 [1]:

- возможность использования более стойких криптографических алгоритмов (в Kerberos 4 внедрить новые алгоритмы было невозможно по ряду технических причин)
- Credential forwarding — возможность передачи тикетов для их использования на удаленный сервер после успешной аутентификации на нем
- Обратная совместимость с Kerberos 4
- Формальное описание протокола с использованием ASN.1
- Увеличение скорости работы протокола за счет отказа от двойного шифрования при обмене сообщениями. Вместо двойного шифрования теперь две части сообщения, зашифрованные разными ключами, конкатенируются.
- Согласование наиболее стойкого типа шифрования
- Больший контроль над тикетами за счёт добавления флагов — forwardable, proxiable, renewable, postdated.
- Pre-Authentication — механизм, производящий предварительную аутентификацию перед тем, как KDC сгенерирует и отправит тикет для конкретного пользователя. Наиболее часто используемый метод — PA-ENC-TIMESTAMP. Также на данный момент для усиления преаутентификации существует механизм PKINIT, использующий сертификаты X.509 для обоюдной аутентификации сервиса и клиента.

- String-to-Key Transformation теперь поддерживает большое количество криптографических алгоритмов, а не только DES. Также шифр усилен с помощью соли.

Программный стенд для тестирования

Инфраструктура тестового стенда включает в себя следующие элементы:

- KDC — основной функционал, выдача, хранение, обработка билетов.
- Сервисы и клиенты, поддерживающие функционал Kerberos.
- Kadmind — сервис администрирования базы данных принципалов
- База данных принципалов
- Вспомогательное ПО для администрирования и работы с Kerberos.
- Все хосты должны быть доступны по FQDN. Следовательно, должна работать служба DNS.
- Время должно быть синхронизировано на всех участниках процесса. Следовательно, требуется использовать сервисы времени, например NTP.

На Рисунке 1 представлена схема тестового стенда с развернутой в ходе работы инфраструктурой Kerberos.

- Key Distribution Center (Authentication Server, Ticket Granting Server), kadmind, principal database развернуты на хосте kdc-srv.example.com с IP адресом 192.168.1.15. На нем же работает DNS.
- Клиентская машина — host.example.com с IP адресом 192.168.1.16.
- Сервис — на хосте ubuntu.example.com с IP адресом 192.168.1.14.

MIT Kerberos API — интерфейс программирования приложения, который поставляется либо в виде бинарных библиотек и заголовочных файлов вместе с пакетом krb5-kdc и сопутствующими зависимостями, либо в виде исходников проекта MIT Kerberos, которые требуется собирать вручную [9, 10].

Для выполнения поставленных задач требуется развернуть на нескольких виртуальных машинах Ubuntu Server 18.04 инфраструктуру Kerberos.

Для этого необходимо произвести следующие шаги:

1. Клонировать исходный код проекта MIT Kerberos на хостовые машины.
2. Установить нужные зависимости для сборки.
3. Выполнить автоконфигурацию проекта под данную систему (autoreconf —verbose), после чего будет сгенерирован файл configure.
4. Выполнить конфигурацию проекта (./configure), тем самым создав Makefile'ы для всех исходных кодов проекта.
5. Собрать проект.
6. Создать новую базу данных принципалов, задав ей пароль.
7. Настроить Access List для Kadmind, позволяя всем принципалам с инстансом admin редактировать базу.
8. Настроить realm по умолчанию, флаги, а также адреса KDC и Kadmind:
9. На KDC настроить Key Distribution Center. Для конкретного realm можно сделать отдельные настройки.

Для того, чтобы программы могли использовать KDC для аутентификации, их нужно керберизировать, то есть, добавить в них поддержку Kerberos. Сделать это можно несколькими способами, в том числе через Kerberos API. Это самый низкоуровневый в плане абстракции от алгоритма аутентификации метод.

Тестирование атак и уязвимостей протокола Kerberos

Даже с учетом популярности протокола Kerberos для сервисов аутентификации, исследователями регулярно находятся уязвимости в его реализациях.

Самой известной атакой является атака Golden Ticket [7,8]. Данная атака является последствием утечки ключа krbtgt или его хеша. Имея ключ можно сконструировать валидный ticket granting ticket даже под несуществующего пользователя.

Пример атаки Golden Ticket на инфраструктуру Active Directory приведен ниже. Сначала с помощью модуля lsadump mimikatz производится дамп базы Security Account Manager, в которой кроме всего прочего лежат NTLM хеши паролей к данным учетным записям. Результат дампа виден на Рисунке 2 в разделе credentials.

Далее с помощью mimikatz модуля Kerberos можно сгенерировать Golden Ticket, подставляя туда хеш пароля, SID, id желаемого пользователя.

Таким образом, получен Ticket Granting Ticket от пользователя krbtgt и скомпрометирована вся инфраструктура, работающая через Kerberos.

Также в противовес Golden Ticket существует атака Silver Ticket [4, 5, 9]. При утечке ключа какого-либо сервиса или его хеша, можно сконструировать ticket granting service. Она является более незаметной, чем Golden Ticket, как минимум потому, что сконструировав тикет,

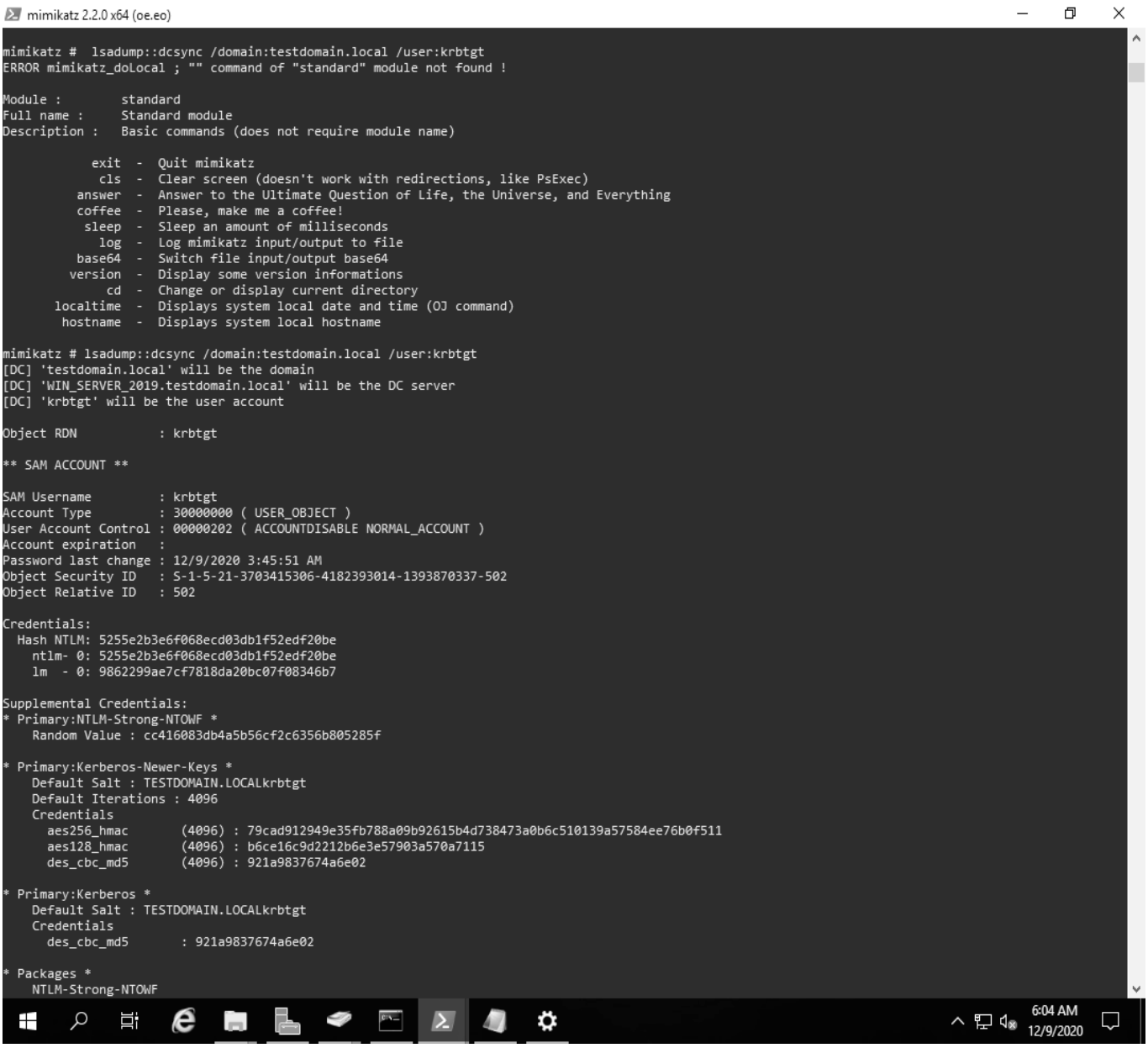

Рис. 2. Результат дампа хешей mimikatz

атакующему не понадобится общаться с KDC в принципе, и можно будет сразу обратиться к сервису. Обход Priveleged Attribute Certificate при наличии хеша пароля аналогичен. Используется для эскалации привилегий, и для закрепления в системе. Защита — мониторинг подозрительной активности, например, если произошел логин на сервис, но при этом TGS-REQ никогда для данного пользователя не запрашивался.

Стоит отметить, что если существует доступ к какому-либо аккаунту, то можно сдампить его текущий тикет для дальнейшего переиспользования, пока он не будет просрочен.

Kerberos — это stateless протокол, то есть ответ KDC не зависит от предыдущих запросов от конкретного хоста. KDC также не проверяет никаких прав доступа данного пользователя к сервису, так как архитектурно KDC занимается только аутентификацией. Таким образом, можно запрашивать у KDC любые TGS для данного сервиса, если есть доступ к его TGT или хешу пароля. Такая атака называется Kerberoasting [4, 6]. Стоит отметить, что полезны только те сервисы, у которых тикеты шифруются с помощью хеша пароля NTLM. Такие настройки обычно у меньшинства сервисов, в большинстве случаев пароль к сервису генерируется автоматически. Он длинный и брутфорсу не подлежит. Но случается, что на сер-

висы ставятся простые пароли вручную. Имея доступ к аккаунту обычного пользователя, можно получить TGS к какому-либо сервису, после чего сдампить его в файл, после чего можно начинать брутфорс хеша. Обычно это делается по словарю.

Атака Over Pass the Hash [4] производится при наличии у атакующего NTLM хеша пароля пользователя. Дело в том, что запрос AS_REQ не использует пароль в чистом виде, он использует этот хеш. То есть, имея хеш, можно стандартными утилитами получить TGT для данного пользователя

Также существует три рабочих методики входа/исследования.

Первая методика это usernames enumeration. С помощью скрипта злоумышленник запрашивает TGT для большого списка принципалов из словаря. Интерпретируя ответы KDC, можно понять, существует ли данный принципал в системе, или нет. Например, 10000 принципалов можно обработать за 5 секунд.

Вторая методика называется password spray (горизонтальная атака) — пусть имеется большое количество валидных пользователей (к примеру, две тысячи). С помощью скрипта выполняется пробный логин на каждого из них с каким-то простым паролем, и какая-то из этих попыток, вполне вероятно, может быть эффективной.

Третья методика — если есть уверенность, что нет локаутов при неверном вводе пароля, то можно пробовать брутфорсить одного конкретного пользователя по словарю.

Учитывая вышесказанное, механизм пре-аутентификации Kerberos является намного более быстрым и потенциально незаметным способом брутфорсинга аккаунтов.

Таким образом, в статье приведена методология и результаты тестирования основных атак на инфраструктуры аутентификации, использующие Kerberos, такие как: Golden ticket, Silver ticket, Kerberoasting, password spray, а также векторы сбора данных (например, usernames enumeration).

ЛИТЕРАТУРА

1. RFC4120 — The Kerberos Network Authentication Service (V5) // IETF | Internet Engineering Task Force URL: https://tools.ietf.org/html/rfc4120 (дата обращения: 16.04.2020).
2. MIT Kerberos Documentation // MIT Kerberos Consortium URL: https://web.mit.edu/kerberos/krb5-devel/doc/ (дата обращения: 10.10.2020).
3. M. Chapple, B. Ballad, E. Banks Access Control, Authentication, and Public Key Infrastructure (Jones & Bartlett Learning Information Systems Security).— 2nd Edition изд. Jones & Bartlett Learning, 2013.
4. Basic Concepts for the Kerberos Protocol // MSDN URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961976(v=technet.10)?redirectedfrom=MSDN (дата обращения: 26.11.2019).
5. Итоги внутренних пентестов — 2020 // Positive Technologies URL: https://www.ptsecurity.com/ru-ru/research/analytics/internal-pentests-2020/ (дата обращения: 07.11.2020).
6. FreeRadius Documentation // FreeRadius URL: https://freeradius.org/documentation/ (дата обращения: 10.11.2019).
7. EIGRP Message Authentication Configuration Example // Cisco URL: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/82110-eigrp-authentication.html (дата обращения: 10.10.2019).
8. Fun with LDAP and Kerberos: Attacking AD from non-Windows machines // Youtube: TroopersCON19 URL: https://youtu.be/2Xfd962QfPs (дата обращения: 09.11.2020).
9. J. Garman Kerberos: The Definitive Guide.— First Edition O'Reilly & Associates, Inc., 2003.
10. Kerberos API // OpenNet URL: https://www.opennet.ru/man.shtml?topic=gss_init_sec_context&category=3&russian=4 (дата обращения: 15.11.2020).

Журнал «Современная наука: актуальные проблемы теории и практики»