М. П. Роденко, А. А. Оленников
Тюменский государственный университет, г. Тюмень
УДК 004.056.53

МЕТОДЫ ПРОВЕДЕНИЯ АТАК НА ПРОТОКОЛ АУТЕНТИФИКАЦИИ KERBEROS В ACTIVE DIRECTORY И СПОСОБЫ ЗАЩИТЫ ОТ НИХ

Аннотация. В статье рассматриваются методы проведения актуальных атак на протокол аутентификации Kerberos в Active Directory. Сформулированы меры защиты для предотвращения атак и минимизации ущерба от них. Полученные рекомендации для защиты от атак могут быть применены не только при создании новой информационной системы, но и для обеспечения безопасности уже используемой системы.

Ключевые слова: тестирование на проникновение, методы атак, уязвимости, active directory, kerberos, учетные данные, аутентификация, протокол, минимизация ущерба.

Введение. Службы Active Directory играют ключевую роль в обеспечении информационной безопасности корпоративных сетей. Однако, как и любая другая технология, Active Directory не защищена от возможных угроз и атак. Реальность такова, что 82% компаний не готовы противостоять внутреннему нарушителю [1]. Важно учитывать, что атаки могут привести к утечке конфиденциальной информации, к краже финансовых средств, нарушению работоспособности системы, а также к полной компрометации домена [2]. Про векторы атак на получение конфиденциальной информации описывает Рудаков А. в своей статье [3]. Злоумышленник может скомпрометировать домен многими способами, один из таких — это получение учетной записи доменного администратора, такой способ подробно описан в статье Скоропупова И. О., Бубнова А. А. и Карманова И. Н. [4]. Поэтому важно не забывать о необходимости профилактических мер, соблюдения простых правил безопасности и обеспечении защиты привилегированных пользователей. В статье Осадчая Т. С. и Щеглова А. Ю описываются меры по затруднению хищения паролей привилегированных учетных записей [5].

Demers. D. и Lee. H в своей статье рассмотрели случаи, в которых атаки на протокол Kerberos были использованы в качестве инструмента в арсенале противника, а также они описали известные способы обнаружения атаки Kerberoasting [6].

В данной статье будут рассмотрена лишь часть всех атак на протокол Kerberos. В статье Козлова А. В. Описаны атаки, такие как:

- распыления пароля;
- золотой билет;
- серебряный билет [7].

Проблема исследования. Аутентификация является одной из наиболее критических функций в Active Directory, и поэтому она находится под особым контролем злоумышленников. Одним из основных протоколов аутентификации, используемых в Active Directory, является протокол Kerberos. Но, как и любой другой протокол, Kerberos может быть подвержен атакам. По итогам внутреннего тестирования на проникновения от компании Positive Technologies, в 61% компаний успешно применялась атака Kerberoasting, которая основана на архитектурных особенностях Kerberos и направлена на получение учетных записей [8]. В статье рассмотрены методы проведения актуальных атак на протокол аутентификации Kerberos в Active Directory и рекомендации по минимизации ущерба от них [9].

Основная цель заключается в исследовании методов атак на протокол аутентификации Kerberos в Active Directory и выработка возможных мер защиты по их предотвращению. Чтобы достичь поставленной цели были поставлены следующие задачи:

- ознакомиться с протоколом аутентификации Kerberos в Active Directory;
- изучить работу службы каталогов Active Directory;
- рассмотреть методы проведения атак на Kerberos;
- выработать рекомендательные методы защиты.

Материалы и методы. Для изучения были выбраны следующие атаки на протокол аутентификации Kerberos в Active Directory:

1) AsReqRoasting;
2) AsRepRoasting;
3) Kerberoasting.

Для более полного понимания атак на протокол аутентификации Kerberos в Active Directory необходимо иметь представление о том, как происходит процесс проверки подлинности пользователей. В проверке подлинности по протоколу Kerberos участвуют:

1) Key Distribution Center (KDC) — хранилище информации о паролях пользователей. Присутствует на контроллере домена (DC);
2) Клиент, желающий пройти проверку подлинности;
3) Сервер, на котором работает необходимый сервис для клиента.

Можно описать взаимодействие между Клиентом и DC как последовательность передаваемых сообщений (рис. 1).

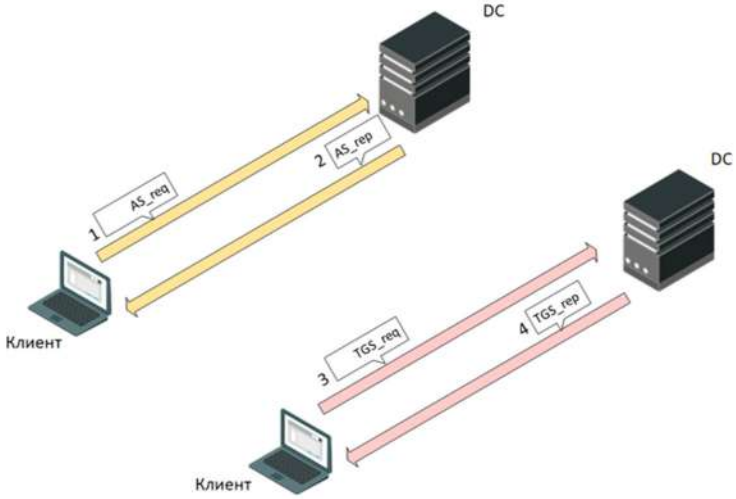

Рис.1. Описание взаимодействия между Клиентом и DC

Атака AsReqRoasting основывается на особенности включения в AS_req-сообщение штампа времени, который зашифрован с использованием хеша пароля пользователя. Для реализации данной атаки злоумышленник должен провести MITM-атаку, чтобы перехватить AS_req-сообщения и извлечь из него зашифрованный штамп времени, который затем может быть пассивно перебран (рис. 2).

Рис. 2. Злоумышленник перехватывает AS_req-сообщение

Следующая атака называется AsRepRoasting. AsRepRoasting — это метод получения учетной записи, для нее достаточно иметь только сетевой доступ к DC (рис. 3). Эта атака до сих пор эффективна, из-за того, что компании отключают на некоторых учетных записях пользователей предварительную проверку подлинности Kerberos.

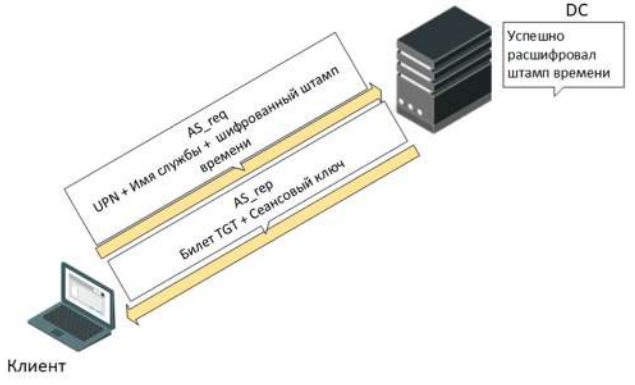

Рис. 3. Передача AS_rep-сообщение от DC

Предварительная проверка подлинности — процедура, в которой домен контроллер получает сообщение AS_req и расшифровывает штамп времени с помощью хеша пароля учетной записи пользователя. Если DC смог расшифровать штамп времени, проверка пройдена и домен контроллер вернет AS_rep-сообщение. Такое сообщение хранит в себе:

- сеансовый ключ, зашифрованный при помощи хеша пароля пользователя, он необходим для шифрования последующих сообщений Клиента к DC.;
- TGT билет, который зашифрован при помощи хеша пароля учетной записи krbtgt, и содержит сеансовый ключ;

Для успешного проведения атаки, злоумышленник выполняет запрос на получение всех учетных записи пользователей с отключенной предварительной проверки подлинности Kerberos. Далее, от их имени отправляет AS_req-сообщение к DC и получает сообщение AS_rep в ответ. Полученной сообщение содержит сеансовый ключ, который зашифрован с использованием хеша пароля учетной записи пользователя. Последний шаг данной атаки это пассивно перебрать хеш.

После прохождения предварительной проверки подлинности, Клиент отправляет TGS_req-сообщение, для получени TGS-билета (рис. 4). С этим билет пользователь может взаимодействовать с запрашиваемым сервисом

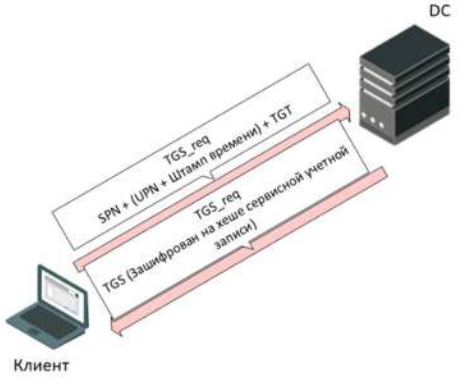

Рис. 4. Получение билета TGS

Метод Kerberoasting, позволяет злоумышленнику , при условии что пароль сервисной учетной записи недостаточно сложный , восстановить его.

Атака Kerberoasting возможна по двум причинам:

- DC не проверяет есть ли право у Клиента на посещение запрашиваемого сервиса;
- Билеты TGS зашифрованы с использованием хеша сервисной учетной записи.

Важный момент, что при атаки Kerberoasting злоумышленника интересуют SPN (имя служб в Active Directory), связанных с учетными записями пользователей, ввиду того, что их пароли возможно восстановить.

Для реализации данной атаки злоумышленнику необходимо пройти аутентификацию любым из рассмотренных ранее методов, это AsReqRoasting или AsRepRoasting. Запросить у DC существующие SPN, связанные с учетными записями пользователей. И последний шаг, пассивно перебрать полученный хеш.

Результаты. Для недопущения атак на протокол Kerberos, нужно действовать следующим рекомендациям:

1. Задать для всех сервисных учетных записей сложные и длинные пароли;
2. Проверить привилегии сервисных учетных записей и убедиться, что у заданы только необходимые права;
3. Использовать эффективный способ обнаружения атаки Kerberoasting — это SPN приманка. Специально создается учетная запись и SPN, к которым Клиент никогда не обратится;
4. Включить предварительную проверку подлинности учетных записей пользователей;
5. Использовать двухфакторную аутентификацию, например смарт-карту или мобильное устройство;
6. Использовать системы мониторинга, для отслеживания действий пользователей и изменений в системе.

Заключение. В настоящее время протокол аутентификации Kerberos является одним из основных протоколов в Active Directory.

Но, как и любой другой сетевой протокол, Kerberos может быть подвержен атакам. Благодаря рассмотренным методам проведения атак в данной статье, были выработаны рекомендации по защите от них.

СПИСОК ЛИТЕРАТУРЫ

1. Positive Technologies: Промышленные компании: векторы атак : [сайт]. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/?sphrase_id=62183 (дата обращения: 22.05.2023). — Текст: электронный.
2. Актуальные киберугрозы для промышленных организаций: итоги 2022 года. — Текст: электронный // Positive Technologies : — [сайт]. — 2023 — URL: https://www.ptsecurity.com/ru-ru/research/analytics/industrial-cybersecurity-threatscape-2022/ (дата обращения: 22.05.2023).
3. Рудаков А. В. Атаки на домен. Полечение учетных записей пользователей в домене / А. В. Рудаков // Инновации. Наука. Образование. — 2021. — № 33. — С. 1152-1165.
4. Скоропупов И. О. Методы проведения атак для получения прав администратора домена в Active Directory / И. О. Скоропупов, А. А. Бубнова, И. Н. Карманов // Интерэкспо Гео-Сибирь. — 2019. — Т. 6, № 1. — С. 187-192.
5. Осадчая Т. С. Защита от атак на учетную запись привилегированного пользователя / Т. С. Осадчая, А. Ю. Щеглов // Известия высших учебных заведений. Приборостроение. — 2018. — Т. 61, № 10. — С. 881-886.
6. Demers D. Kerberoasting: Case Studies of an Attack on a Cryptographic Authentication Technology / D. Demers, H. Lee // International Journal of Cybersecurity Intelligence & Cybercrime. — 2022. — Т. 5, № 2. — С. 3.
7. Козлов А. В. Тестирование и анализ атак на криптопротокол Kerberos с помощью программного стенда системы аутентификации / А. В. Козлов // Информатика и вычислительная техника и управление. — 2021. — № 5.
8. Weidman G. Penetration testing. A hands-on introduction to Hacking / G. Weidman. — San Francisco: No Starch Press, — 2014. — 113 p. — Direct text.
9. Итоги внутренних пентестов. — Текст : электронный // Positive Technologies: [сайт]. — 2020 — URL: https://www.ptsecurity.com/ru-ru/research/analytics/internal-pentests-2020/ (дата обращения: 23.05.2023).