УДК 004.056.53

УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ KERBEROASTING

В.В. Дубовский, Е.С. Белоусова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Статья посвящена анализу угрозы безопасности Active Directory, известной как Kerberoasting, которая использует уязвимости протокола Kerberos для получения хешей паролей учетных записей сервисов. Авторы рассматривают основные этапы аутентификации Kerberos, методы проведения кибератаки, а также инструменты, используемые нарушителями. В работе предложены рекомендации по защите инфраструктуры Active Directory: использование стойких алгоритмов шифрования, мониторинг журналов безопасности и применение сложных паролей для учетных записей. Статья актуальна для специалистов в области кибербезопасности, занимающихся защитой корпоративных сетей.

Ключевые слова: Active Directory; Kerberos; Kerberoasting; аутентификация; хеши паролей; угрозы AD; мониторинг журналов.

KERBEROASTING INFORMATION SECURITY THREAT

V.V. Dubovsky, E.S. Belousova
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. This article analyzes the Active Directory security threat known as Kerberoasting, which exploits vulnerabilities in the Kerberos protocol to obtain hashes of service account passwords. The authors review the main stages of Kerberos authentication, methods of cyberattack, and tools used by the attackers. The paper offers recommendations for protecting Active Directory infrastructure: using strong encryption algorithms, monitoring security logs and using complex passwords for accounts. The article is relevant for cybersecurity specialists involved in the protection of corporate networks.
Keywords: Active Directory; Kerberos; Kerberoasting; authentication: hash password: AD threats: log monitoring.

Введение

В условиях, когда кибербезопасность становится критически важной, защита Active Directory (AD) является приоритетной задачей для организаций. Специалисты отмечают, что AD в 90 % случаев выступает либо вектором кибератаки, либо средством закрепления или повышения привилегий в домене. При этом более 40% кибератак на AD оказываются успешными [1]. Около 90 % компаний в мире используют AD для управления учетными записями, что делает ее привлекательной целью для нарушителей. В последние годы наблюдается значительное увеличение числа кибератак на Active Directory. Это связано с тем, что данная система является важнейшим хранилищем информации, включая учетные записи и права доступа сотрудников. Распространенными угрозами для инфраструктуры AD являются Roasting-атаки (AS-REP Roasting, Kerberoasting). Техники таких атак представлены в MITRE ATT&CK: T1558 (Steal or Forge Kerberos Tickets) [2] и T1595 (Active Scanning) [3]. С уверенностью можно утверждать, что такие кибератаки являются одними из наиболее популярных в корпоративных сетях.

Roasting-атаки используют уязвимости в протоколе Kerberos для получения хешей паролей учетных записей. Kerberos – это протокол, который позволяет пользователям аутентифицироваться в сети и получать доступ к службам. По умолчанию Kerberos использует подключение TCP, порт 88 и является основным протоколом аутентификации для учетных записей домена, начиная с операционной системы Windows 2000. Благодаря Kerberos пользователю не нужно постоянно вводить свой пароль, а серверу не нужно знать пароль каждого пользователя. В 2023 году Microsoft объявила об отказе от использования аутентификации NTLM (NT LAN Manager), в пользу протокола Kerberos [4], что также подтверждает актуальность исследования уязвимостей данного протокола. Основное отличие Kerberos от NTLM заключается в процессе аутентификации. При использовании NTLM аутентификация осуществляется на сервере, к которому обращается клиент. Kerberos полагается на службу Центра распространения ключей KDC (Key Distribution Center), работающую на контроллере домена (DC). Целью работы является выявить уязвимости процесса аутентификации пользователя по протоколу Kerberos на основе его изучения, проанализировать механизмы кибератак и их влияние на безопасность Active Directory.

Основная часть

Процесс аутентификации по протоколу Kerberos осуществляется в соответствии со следующими этапами:

1. Пользователь авторизируется в системе. В результате успешной авторизации отправляется запрос AS-REQ (Authentication Service REQuest) на сервер аутентификации (AS) службы KDC. Запрос AS-REQ (Authentication Service REQuest) включает в себя: временную метку (timestamp), которая шифруется с использованием хэша пароля пользователя; идентификатор пользователя (Client Principal Name), который отправляется в незашифрованном виде (например, username@domain.name), чтобы KDC мог идентифицировать пользователя.

2. KDC проверяет имя пользователя и его хэш пароля в базе NTDS, расшифровывает временную метку. Если метка была расшифрована, то KDC отвечает клиенту сообщением AS-REP (Authentication Service REPly), содержащим сгенерированный ключ сеанса для KDC, метку времени, TGT (Ticket-Granting Ticket), срок действия билета TGT. Ключ сеанса для KDC, метка времени и срок действия TGT шифруются с использованием хэша пароля пользователя. Это позволяет гарантировать, что только легитимный клиент сможет расшифровать эти данные и получить доступ к TGT.

TGT содержит аналогичные данные (ключ сеанса, метку времени и срок действия), но также включает идентификатор клиента (Client Principal Name). Важно отметить, что TGT зашифрован с использованием хэша пароля специальной учетной записи KDC – krbtgt. Это гарантирует, что только KDC может создавать и проверять TGT, обеспечивая безопасность процесса аутентификации. По умолчанию срок действия TGT составляет 10 часов.

При попытке получения клиентом доступа к какому-либо сервису в домене отправляется запрос на получение билета для службы (TGS-REQ) на KDC, которое включает в себя аутентификатор (идентификатор клиента, временную метку), TGT и Principal сервиса. Аутентификатор зашифрован с использованием сеансового ключа, который был выдан KDC при получении TGT. Principal сервиса указывает, к какому конкретному сервису (например, файловому серверу или базе данных) клиент пытается получить доступ.

Сервер выдачи разрешений TGS (Ticket Granting Service) в KDC при обработке запроса TGS-REQ выполняет следующие шаги:

1. Проверяет, существует ли указанный в запросе сервис. Если сервис не найден, запрос отклоняется.

2. Сервер расшифровывает TGT и извлекает: сеансовый ключ для KDC, идентификатор клиента, временную метку.

3. Сервер расшифровывает аутентификатор и проверяет, совпадает ли идентификатор клиента из TGT с идентификатором, указанным в аутентификаторе, а также проверяет временную метку, которая не должна превышать 2 минут.

4. TGS выполняет подтверждения подлинности запроса, проверяя срок действия TGT, идентификатор клиента; временную метку аутентификатора.

5. Если все проверки пройдены, TGS отправляет клиенту сообщение TGS-REP, которое содержит зашифрованные на сеансовом ключе для KDC данные о принципале сервиса, к которому предоставлен доступ, временную метку, ключ сеанса для сервиса и срок действия билета для сервиса (TGS). Кроме того, в сообщении TGS-REP содержится сам билет TGS, зашифрованный с использованием секретного ключа

сервиса. Такой подход обеспечивает безопасность билета TGS, который может расшифровать только KDC и тот сервис, для которого он предназначен.

Основной уязвимостью рассмотренного процесса аутентификации по протоколу Kerberos является то, что любой аутентифицированный пользователь домена может запросить билет Kerberos для любой учетной записи сервиса (Service Account), если он знает Service Principal Name (SPN) этой учетной записи. Получив билет Kerberos для учетной записи сервиса, нарушитель может использовать его для брутфорс-атаки, так как этот билет зашифрован NTLM-хэшем пароля сервисной учетной записи. Если пароль слабый, нарушитель получает контроль над учетной записью сервиса.

Большинство сервисов выполняются машинными учетными записями (COMPUTERNAME$), которые имеют случайно сгенерированные пароли длиной 120 символов, что делает нецелесообразным применение брутфорса. Иногда сервисы выполняются учетными записями пользователей. Учетная запись пользователя имеет пароль, установленный человеком, который с гораздо большей вероятностью будет предсказуемым. Кибератака Kerberoasting ориентирована на подобные учетные записи.

Пример реализации кибератаки может быть рассмотрен на основе использования нарушителем модуля PowerView на захваченном устройстве, находящемся в домене с операционной системой Windows. Данный модуль осуществляет поиск учетных записей служб, зарегистрированных в домене. Это позволяет нарушителю получить список всех учетных записей, связанных с сервисами, такими как SQL Server, HTTP, Exchange и другими. Результат выполнения команды для перечисления всех SPN в домене можно увидеть на рис. 1.

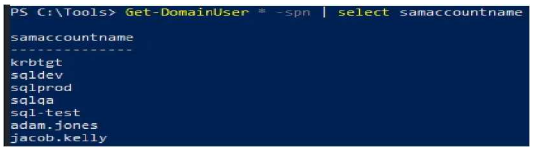

Рис. 1. Перечисление SPN с помощью модуля PowerView
Fig. 1. SPN enumeration using the PowerView module

В результате получения нарушителем списка SPN, возможно формирование запроса TGS для найденных учетных записей. Запросы отправляются с задержкой, маскируя их в общем потоке сетевого трафика. TGS зашифрован хэшем пароля учетной записи службы, что позволяет нарушителю, перехватив билет, попытаться подобрать пароль в автономном режиме. На рис. 2 представлен пример выполнение команды для запроса TGS.

Рис. 2. Запрос TGS для полученного SPN
Fig. 2. TGS request for a received SPN

После получения билета, нарушитель может в автономном режиме, без риска блокировки учетной записи, перебирать пароли, используя различные средства и методы для расшифровки, например Hashcat. Результат успешного перебора пароля можно увидеть на рис. 3.

Рис. 3. Результат получения учетных данных с помощью Hashcat
Fig 3. Result of obtaining credentials using Hashcat

Атакующий может провести аналогичные действия с устройства с ОС Linux, используя скрипт GetUserSPNs.py, который входит в набор инструментов Impacket. Нарушитель запускает скрипт, указав домен, контроллер домена и учетные данные. В результате нарушитель также может получить TGS билет, который использовать для брутфорса с использованием Hashcat.

Заключение

Несмотря на существование различных методов обнаружения и предотвращения Roasting-атак, они остаются актуальной проблемой для многих организаций. Это связано с рядом факторов, включая сложность настройки и мониторинга Active Directory, недостаточную осведомленность администраторов о существующих угрозах и использование устаревших версий программного обеспечения.

Для защиты от Roasting-атак рекомендуется убедиться, что предварительная аутентификация включена для всех учетных записей, кроме случаев, когда это необходимо для совместимости со старыми протоколами. Рекомендуется использовать стойкие алгоритмы шифрования Kerberos, такие как AES, и отказаться от устаревшего RC4. Регулярно следует проверять журналы на подозрительную активность, особенно для сервисных учетных записей. Обнаружение атак возможно путем мониторинга событий в журналах безопасности, таких как Event ID 4769 и 4768, связанных с изменениями учетных записей и запросами билетов Kerberos. Также необходимо использовать длинные и сложные пароли для учетных записей и ограничивать их права доступа.

Список использованных источников

1. Скоропупов И.О., Бубнова А.А., Карманов И.Н. Методы проведения атак для получения прав администратора домена в Active Directory // Интерэкспо Гео-Сибирь. 2019. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/metody-provedeniya-atak-dlya-polucheniya-prav-administratora-domena-v-active-directory.

2. Еремеев М.А., Смирнов С.И., Прибылов И.А. ОБНАРУЖЕНИЕ ВРЕДОНОСНЫХ ДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА НА ОСНОВЕ ЖУРНАЛОВ СОБЫТИЙ ПРИ РАССЛЕДОВАНИИ ПРОДОЛЖАЮЩЕГОСЯ КИБЕРИНЦИДЕНТА // Инновационные аспекты развития науки и техники. 2021 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/detection-of-malicious-actions-of-an-attacker-based-on-event-logs-when-investigating-an-ongoing-cyber-incident.

References

1. Skoropupov I.O., Bubnova A.A., Karmanov I.N. Attack methods for obtaining domain administrator rights in active directory // Interexpo Geo-Siberia. 2019. [Electronic resourse]. – Mode of access: https://cyberleninka.ru/article/n/metody-provedeniya-atak-dlya-polucheniya-prav-administratora-domena-v-active-directory. – Date of access: 20.02.2025

2. Eremeev M.A., Smirnov S.I., Pribylov I.A. DETECTION OF MALICIOUS ACTIONS OF AN ATTACKER BASED ON EVENT LOGS WHEN INVESTIGATING AN ONGOING CYBER INCIDENT // Innovative aspects of science and technology development. 2021 [Electronic resourse]. – Mode of access: https://cyberleninka.ru/article/n/detection-of-malicious-actions-of-an-attacker-based-on-event-logs-when-investigating-an-ongoing-cyber-incident.

Сведения об авторах

Дубовский В.В., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», v.dubovski007@gmail.com.
Белоусова Е.С., кандидат технических наук, доцент кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», belousova@bsuir.by.

Information about the authors

Dubovsky V.V., student of the Faculty of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", v.dubovski007@gmail.com.
Belousova E.S., PhD, Associate Professor of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", belousova@bsuir.by.