УДК 004.056

ИССЛЕДОВАНИЕ ЭЛЕМЕНТОВ БЕЗОПАСНОСТИ ACTIVE DIRECTORY: ВОЗМОЖНЫЕ АТАКИ

Фролов Андрей Евгеньевич, Нагаев Дамир Маратович

Алтайский государственный университет, г. Барнаул
email: frolov@mc.asu.ru

ACTIVE DIRECTORY SECURITY ELEMENT RESEARCH: POSSIBLE ATTACKS

Frolov Andrey E., Nagaev Damir M.

Altai State University, Barnaul

Аннотация: В статье рассмотрены вопросы исследования элементов безопасности Active Directory, таких как пароли, хэш-функции, билеты и сертификаты. Каждый из элементов представлен с точки зрения его функционирования внутри доменной инфраструктуры. Наглядно показаны варианты атак на перечисленные компоненты, для более глубокого понимания того, как действуют злоумышленники внутри корпоративной сети и какие способы компрометации используют.

Ключевые слова: информационная безопасность, Active Directory, угрозы безопасности, NTLM, Kerberos, TGT.

Abstract: The paper discusses the research of Active Directory security elements such as passwords, hash functions, tickets and certificates. Each of the elements is presented from the point of view of its functioning within the domain infrastructure. Attack variants on the listed components are clearly shown, for a deeper understanding of how attackers operate within the corporate network and what methods of compromise they use.

Keywords: information security, Active Directory, security threat, NTLM, Kerberos, TGT.

Для цитирования: Фролов А.Е., Нагаев Д.М. Исследование элементов безопасности Active Directory: возможные атаки // // Проблемы правовой и технической защиты информации. 2024. №12. С.88-93.

For citation: Frolov A.E., Nagaev D.M. Active Directory security element research: possible attacks // Legal and Technical Problems of Information Security. 2024. No. 12. P.88-93.

В центре стремления к оптимизации бизнес-процессов стоит технология, которая выступает в роли надежного и универсального решения для управления и аутентификации в корпоративных сетях - Active Directory. Active Directory не просто является средством централизованного управления пользователями, группами и ресурсами, но и становится неотъемлемой частью современных инфраструктур, обеспечивая эффективное управление политиками безопасности [1] и автоматизированный доступ к ресурсам.

В условиях постоянно усиливающейся угрозы в области информационной безопасности роль Active Directory становится еще более критичной. В данной статье рассматриваются атаки на ключевые элементы безопасности службы каталогов, такие как пароли, хэш-функции, билеты и сертификаты, чтобы лучше понять их важность для обеспечения устойчивости корпоративных сетей. Перед рассмотрением атак на ключевые элементы безопасности, компоненты исследуются с точки зрения

функционирования внутри доменной инфраструктуры [2].

Пароль, как и во всех системах и сервисах представляет собой произвольные набор символов, в виде букв, цифр и специальных символов, которые задаются пользователем для доступа к сервису. Данный пароль задается исходя из парольной политики, настроенной администратором в службе каталогов. Политики паролей, позволяет определить требования к их сложности и периодичность смены, содействуя защите учетных записей.

Пароли в Active Directory хранятся в виде хеш-функции, именуемые как односторонняя функция OWF (one-way function) [3]. В Active Directory механизмы хеширования, поддерживаются в таких сетевых протоколах аутентификации как NTLM и Kerberos. Важно отметить, что в обоих случаях хэши паролей хранятся в базе данных Active Directory, размещенной на контроллерах домена, и именуемая NTDS.dit. Сравнение технологий приведено на рисунке 1.

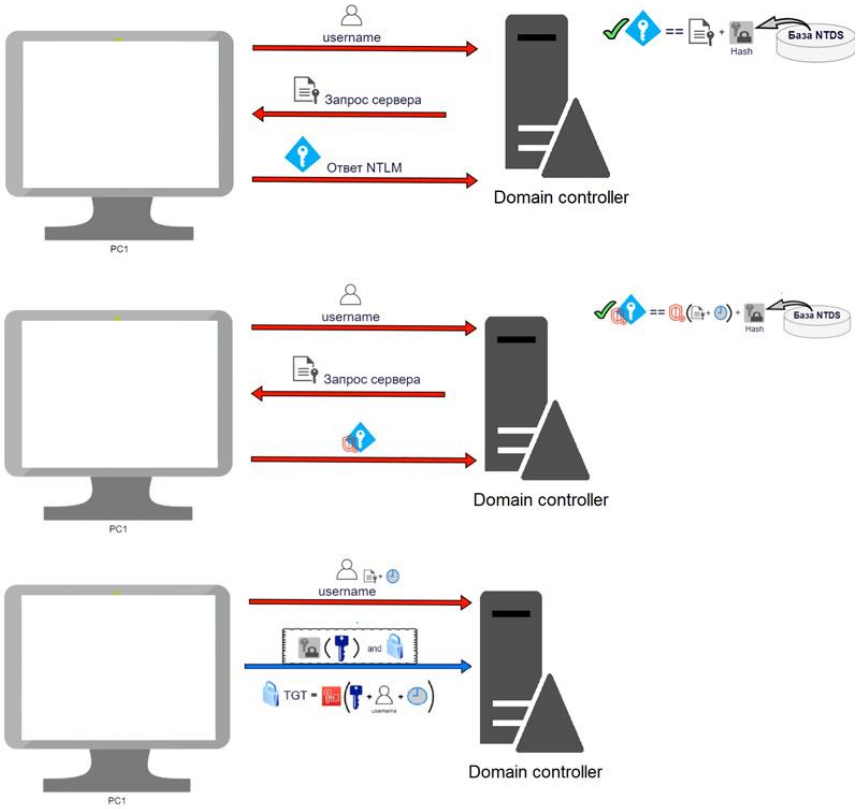

Рисунок 1. Схемы работы технологий

Протокол NTLM может применяться как в сетях рабочих групп, так и в структуре Active Directory. В сценарии с Active Directory, NTLM обеспечивает проверку подлинности учетных записей домена на компьютерах в сети. В протоколе NTLMv1 ответ (NTLM-хэш) на запрос сервера вычисляется путем использования хэша NT для шифрования серверного запроса с применением алгоритма DES. Также сеансовый ключ непосредственно шифруется с использованием хэша NT. В протоколе NTLMv2 используется более обширный объем данных для обеспечения дополнительной защиты и целостности сеанса. При вычислении ответа (NT-хэша) NTLMv2 учитывает такие элементы, как запрос сервера и метку времени.

В протоколе Kerberos предполагается, что обмен информацией между клиентом и

сервером происходит в незащищенной среде, где передаваемые пакеты могут быть перехвачены. Поэтому одной из ключевых задач протокола является подтверждение легитимности обеих сторон через взаимодействие с доменным контроллером. Основное внимание Kerberos уделяется использованию токенов, известных как «билеты», что обеспечивает пользователям возможность пройти аутентификацию.

Билеты представляют собой частично зашифрованные структуры, содержащие следующую информацию:

– целевой объект (обычно служба), для которого предназначен билет;

– связанная с клиентом информация, такая как имя и домен;

– ключ для обеспечения безопасного взаимодействия между клиентом и сервисом;

– временные метки, определяющие период, в течение которого билет действителен.

Для понимания протокола Kerberos важно учесть наличие двух типов билетов.

Первый тип – это сервисные билеты (Service ticket – ST), которые клиент предъявляет аутентификационному серверу, чтобы получить доступ к конкретной службе. Key Distribution Center (далее KDC) выдает сервисные билеты для клиентов по запросу. В структуре Active Directory клиент может получить сервисные билеты для любой службы, зарегистрированной в базе данных домена, даже если у пользователя нет прямого доступа к службе. Сервисные билеты предназначены только для чтения целевой службой и включают информацию о клиенте и ключ сеанса для установления связи с клиентом.

Чтобы получить сервисные билеты от KDC, пользователь должен предоставить билет другого типа, известный как «билет на получение билетов» (Ticket Granting Ticket, далее TGT). Согласно принципу, доступ к TGT разрешается только KDC, и все TGT шифруются с использованием ключа krbtgt, который известен как ключ KDC.

Следующим элементом, обеспечивающим безопасность службы каталогов Active Directory, являются сертификаты. Для получения сертификата, пользователь или устройство инициирует процесс, создавая запрос на сертификат (CSR), который включает в себя открытый ключ и информацию о владельце. Центр сертификации (AD CS) проверяет этот запрос, аутентифицирует пользователя и подписывает сертификат своим закрытым ключом. Выданный сертификат, содержащий открытый ключ пользователя, предоставляется обратно клиенту.

В процессе аутентификации пользователь предъявляет свой сертификат ресурсу или серверу. Получатель проверяет подлинность сертификата, используя открытый ключ центра сертификации и проверяет его статус. При успешной проверке подлинности и статуса сертификата пользователю предоставляется доступ к ресурсам, основываясь на доверии к аутентификационной информации, содержащейся в сертификате [4].

Рассмотрев основные элементы обеспечения безопасности службы каталогов Active Directory, важно понимать, каким образом за счёт данных элементов, инфраструктура организации может быть скомпрометирована злоумышленником.

Как было сказано ранее, хэши всех учетных записей Active Directory хранятся на домене контроллера в базе данных (БД) NTDS.dit. При получении доступа до данной базы можно с легкостью скомпрометировать любого пользователя, независимо от его прав в организации, будь то рядовой пользователь или администратор всей системы. На рисунке 2 изображена дамп БД NTDS.dit с помощью инструмента secretsdump из набора для работы с сетевыми протоколами impacket.

Получив NT-хэш учетных записей, можно провести атаку типа pass-the-hash, когда вместо пароля для доступа к машине или сервису, используется значение хэш функции NT. На рисунке 3 приведен пример получения доступа к commad line (cmd) машины 192.168.10.200 с помощью NT-хэша учетной записи ADMPetr. Для получения доступа используется инструмент smbexec.py из набора impacket.

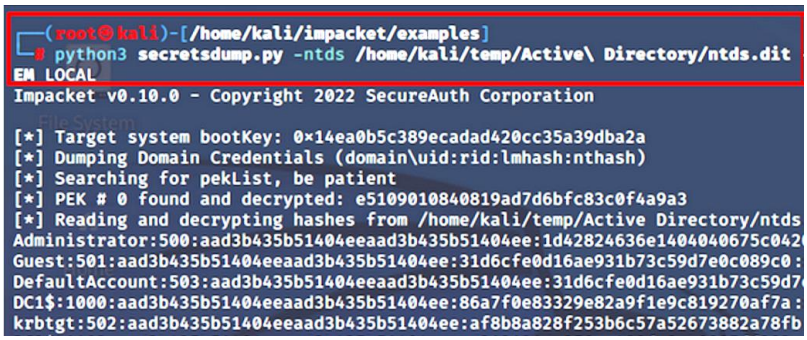

Рисунок 2. Дамп базы данных Active Directory NTDS.dit

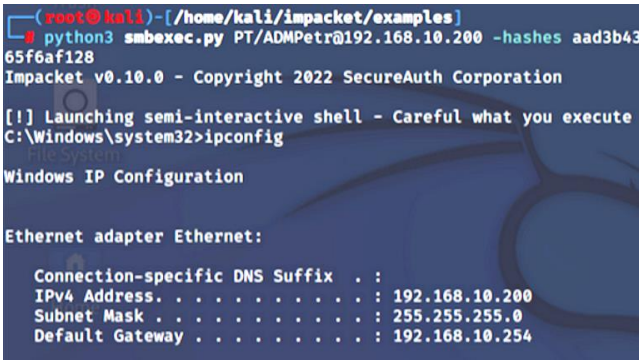

Рисунок 3. Использование NT-хэша в атаке pass-the-hash

Одна из наиболее известных атак, применяющих NTLM – атака NTLM-Relay. В данном случае злоумышленник, выступая в роли «человека посередине», использует свое положение для перенаправления процесса аутентификации NTLM на целевой сервер, что позволяет ему получить сеанс аутентификации.

Недостатком атаки NTLM-Relay является отсутствие доступа к сессионному ключу, даже если злоумышленник успешно аутентифицирован. Этот ключ зашифрован при передаче и неизвестен злоумышленнику, что мешает ему создавать действительные подписи для сообщений приложения. Если клиент и сервер используют согласование подписей, злоумышленник не сможет корректно подписывать сообщения, что, в свою очередь, исключает возможность успешного взаимодействия с сервером.

На рисунке 4 приведен пример атаки NTML Relay [5], в которой злоумышленник прослушивает запросы аутентификации NTLM машины 192.168.10.210, которая является центром сертификации AD CS.

На рисунке 5 отображен результат работы атаки NTLM-Relay, а именно перехваченный сертификат учетной записи DC$, которая является машинной учетной записью контроллера домена. Для перехвата запроса NTLM используется инструмент ntlmrelayx.py из набора impacket.

Рисунок 4. Ожидание запроса NTLM при атаке NTLM-Relay

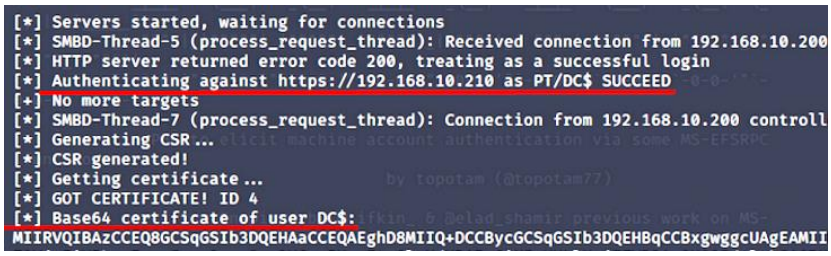

Рисунок 5. Результат работы атаки NTLM-Relay

Перехватив сертификат машинной учетной записи DC$ контроллера домена, можно запросить TGT билет с использованием протокола Kerberos. В дальнейшем, билет TGT позволит запрашивать билеты TGS, для получения доступа к сервисам, которые имеются в инфраструктуре организации. На рисунке 6 приведен пример запроса билета TGT с помощью инструмента Rubeus.

TGT в системе Kerberos шифруются с использованием ключей, связанных с учетной записью krbtgt. Зная эти ключи, возможно создание пользовательских TGT, известных как Golden Tickets [6]. Создание Golden Ticket предоставляет права, указанные в билете, что дает возможность выдавать себя за любого пользователя в домене, включая несуществующих, и получать доступ к любым службам в домене. Важно помнить, что Golden Ticket необходимо использовать в течение 20 минут, так как после этого KDC проведет проверку информации, чтобы удостовериться в корректности билета. На рисунке 7 изображено получение «золотого билета» для несуществующего пользователя. Провести атаку для получения золотого билета можно при помощи приложения mimikatz, командой «kerberos::golden».

Рисунок 6. Запрос билета TGT от имени учетной записи DC$

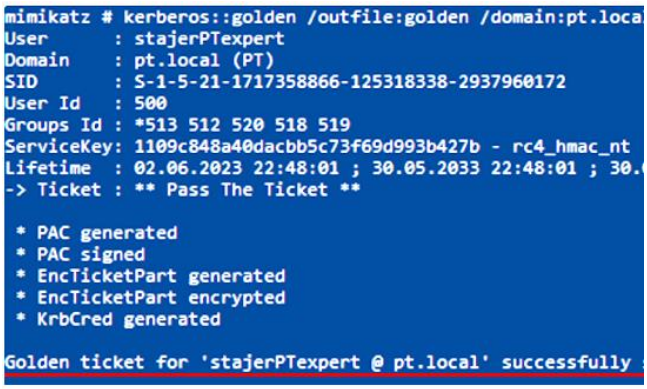

Рисунок 7. Проведение атаки для получения Golden Ticket

Получение золотого билета предоставляет злоумышленнику неограниченный доступ в сети организации. Воспользовавшись таким билетом, можно получить доступ до контроллера домена (рисунок 8), при этом не имея никаких привилегий и членства в домене.

Рисунок 8. Получение доступа до контроллера домена

В данной работе были рассмотрены только некоторые атаки на элементы, обеспечивающие безопасность службы каталогов Active Directory. Количество возможных вариантов компрометации сети за счёт данной службы увеличивается от атаки к атаке. Появляются новые и более сложные варианты обхода защиты периметра, но в основе всего этого лежат ошибки конфигурации данных элементов. По итогу, специалисту, обеспечивающему информационную безопасность в инфраструктуре организации, важно знать о том, как работают те или иные компоненты безопасности, и каким типам атак они могут быть подвержены, что позволит обеспечить наиболее глубокую защиту инфраструктуры.

Библиографический список

1. Фролов А.Е., Нагаев Д.М. Методика расследования неправомерного воздействия на компьютерную информацию при компьютерной атаке // Проблемы правовой и технической защиты информации. ПТЗИ. № 10. С. 30-36.

2. Ralf Hacker. Active Directory глазами хакера. – СПб.: БХВ-Петербург, 2021 – 176 с.

3. Active Directory passwords: All you need to know [Электронные ресурс] // URL: https://4sysops.com/archives/active-directory-passwords-all-you-need-to-know/ (дата обращения: 20.10.2023).

4. Attacking Active Directory: 0 to 0.9 [Электронные ресурс] // URL: https://zer1t0.gitlab.io/posts/attacking_ad/ (дата обращения: 11.11.2023).

5. ADCS+PetitPotam NTLM Relay: Obtaining krbtgt Hash with Domain Controller Machine Certificate [Электронные ресурс] // URL: https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/adcs-+-petitpotam-ntlm-relay-obtaining-krbtgt-hash-with-domain-controller-machine-certificate (дата обращения: 10.12.2023).

6. Погружение в AD: разбираем продвинутые атаки на Microsoft Active Directory и способы их детекта [Электронные ресурс] // URL: https://www.securitylab.ru/blog/company/pt/344797.php (дата обращения: 20.11.2023).