Рубрика 2. Методы и системы защиты информации, информационная безопасность

УДК 004.056.5

Р. А. Богданов[1], Г. Д. Гададов[1]
[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация

ВОПРОСЫ ХРАНЕНИЯ И ЗАЩИТЫ ДОМЕННЫХ УЧЕТНЫХ ЗАПИСЕЙ В ОС СЕМЕЙСТВА WINDOWS. ИНСТРУМЕНТЫ ПОЛУЧЕНИЯ ПАРОЛЕЙ

Аннотация. В статье рассматриваются вопросы хранения и защиты доменных учетных записей в инфраструктуре Active Directory на базе Windows Server 2019. Актуальность исследования обусловлена тем, что доменная учетная запись остается одним из ключевых объектов атак на корпоративную сеть: при компрометации учетных данных злоумышленник получает возможность расширять привилегии, закрепляться в системе и получать доступ к критически важным ресурсам. Цель работы состоит в практической оценке рисков извлечения аутентификационных данных и анализе эффективности базовых защитных мер. В ходе исследования рассмотрены механизмы хранения секретов в LSASS и базе NTDS.dit, а также проведен лабораторный эксперимент с использованием Mimikatz в контролируемой среде. Сопоставлены результаты для слабого и криптостойкого пароля, а также для конфигурации с включенной защитой LSA Protection. Показано, что сложный пароль снижает вероятность быстрого восстановления пароля по хешу, однако не устраняет риск оффлайн-подбора и не предотвращает сам факт утечки хеша. Наиболее значимым результатом является подтверждение необходимости комплексной защиты: включения LSA Protection и Credential Guard, применения группы «Защищенные пользователи», разграничения привилегий и модели многоуровневого администрирования. Полученные выводы могут быть использованы при построении учебных стендов и при разработке организационно-технических мер защиты доменной инфраструктуры Windows. Дополнительно подчёркивается роль профилактических настроек в снижении вероятности повторной компрометации.

Ключевые слова: Active Directory, доменные учетные записи, информационная безопасность, уязвимости, доменная инфраструктура Windows.

Введение

В современных корпоративных сетях технология Active Directory (AD) обеспечивает централизованное управление доменной аутентификацией и доступом, фактически являясь стандартом администрирования в ОС Windows. По оценкам Microsoft, AD используется в более чем 90% предприятий (включая 95% компаний из списка самых крупных компаний США по версии американского журнала Fortune) для управления учётными записями и идентификацией пользователей [1]. Это означает, что безопасность доменных учетных данных напрямую влияет на защиту всей сети организации – компрометация контроллера домена даёт злоумышленнику привилегированный доступ и может привести к краже критически важных данных и атаке на всю инфраструктуру [2][3]. Одним из ключевых инструментов поиска угроз безопасности является утилита Mimikatz[1] — — она позволяет извлекать из памяти процесса LSASS открытые пароли, хэши, PIN-коды и Kerberos-токены [4].

Известно, что учётные данные доменных пользователей хранятся в базе AD (файл NTDS.dit) в виде зашифрованных хешей паролей (NTLM) и соответствующих Kerberos-ключей. При аутентификации и на рабочих станциях эти данные также попадают в память процесса LSASS, откуда их могут считывать компрометированные локальные процессы. Чтобы ограничить эти риски, в Windows Server 2019 и Windows 10/11 были внедрены различные механизмы защиты. Например, Credential Guard, который использует виртуализацию (Virtualization-based Security) для изоляции секретов в специальном защищённом процессе (LSAIso), так что обычный LSASS становится «пустым» для остальной системы [5]. Это защищает хранимые в памяти пароли и билеты Kerberos от прямого считывания. При включении LSA Protection (RunAsPPL) процесс LSASS становится «защищённым» (PPL), и только доверенные подписанные системные компоненты могут взаимодействовать с его памятью. В результате внедрение кода в LSASS и чтение его памяти вредоносными утилитами (в нашем случае Mimikatz) становится значительно сложнее [6]. Группа «Защищенные пользователи»

[1]Созданная французским исследователем Бенжаменом Дельпи (Benjamin Delpy). Изначально проект задумывался как исследовательский — просто чтобы доказать, что пароли в Windows реально извлечь из памяти [4].

— встроенная глобальная группа AD, которая при добавлении в неё аккаунта запрещает кеширование пароля, ограничивает протоколы аутентификации (только AES-Kerberos) и делает аккаунт менее уязвимым к атакам (например, отключает поддержку NTLM для этих пользователей) [7].

Тем не менее сохраняются значительные пробелы в защите доменных аккаунтов. Так, Credential Guard защищает локальные устройства, но не защищает саму базу AD на контроллерах домена и не влияет на протоколы внешней аутентификации (например, RDP Gateway) [5]. Многие организации до сих пор не активировали эти функции из-за совместимости или нехватки ресурсов на обновление ОС/уровня домена. Атаки типа Pass-the-Hash, Overpass-the-Hash, DCSync и особенно подделка Kerberos-билетов (Golden/Silver Ticket) остаются эффективными средствами обхода большинства текущих мер защиты. По данным Verizon, в 88% случаев успешных взломов используются украденные учётные данные, что подчёркивает недостаточную стойкость существующих решений. Кроме того, рост гибридных сред (смешанные On-Premise AD и Azure AD, синхронизация учётных записей и т.д.) создаёт новые векторы атак и усложняет обнаружение нарушений [2]. Таким образом, несмотря на внедрённые средства защиты, остаётся высокий риск компрометации доменных учётных записей, что требует дальнейших исследований уязвимостей и совершенствования архитектуры безопасности.

Объект исследования — информационная безопасность доменных инфраструктур Windows.

Предмет исследования — механизмы хранения, защиты и извлечения доменных учётных данных в среде Windows Server 2019/AD.

Цель исследования — анализ уязвимостей, архитектурных особенностей и существующих защитных мер с целью предотвращения компрометации доменных учётных записей.

Литературный обзор

В научной и практической литературе описаны многочисленные методы атак и защиты инфраструктуры, построенной на технологии AD. Многие специалисты (например, Sean Metcalf из ADSecurity, Red Canary, CIS и др.) публикуют исследования и рекомендации по защите домена. В ряде недавних работ [8][9][10][11] анализируются уязвимости AD и предлагаются алгоритмы обнаружения. Практические руководства и блоги (CIS, SecurityLab, Microsoft) детально освещают механизмы кражи паролей (DCsync, Kerberoasting, Golden Ticket и др.) и способы их предотвращения [3].

Технические материалы и белые книги Microsoft, MITRE и CIS, а также отчёты и блоги специализированных команд (Red Team/Blue Team) подчёркивают необходимость защиты ключевых компонентов AD. В руководствах Microsoft также описан подход многоуровневого управления привилегиями (AD Tiering). Согласно этому подходу, учётные записи доменных администраторов (уровень 0) не должны выполнять вход на сервера нижних уровней (уровни 1 и 2), чтобы ограничить распространение компрометированных учётных данных. Это отражено в рекомендациях по выделению «тысячелеток» безопасности (Tier0–Tier2) и ограничению доступа (например, Tier-0 админы не логинятся на рабочие станции Tier-2) [12]. Параллельно механизм AdminSDHolder служит встроенным средством непрерывного контроля прав на особо защищённых учётных записях; объект AdminSDHolder регулярно применяется (через процесс SDProp) к ACL членов привилегированных групп, обеспечивая консистентность прав [13].

Обзор инструментов атаки и защиты в литературе подчёркивает широту решения задачи. С одной стороны, Mimikatz и аналогичные утилиты позволяют осуществлять различные формы кражи учётных данных (из памяти, из Kerberos-тиков, из реестра и пр.). С другой стороны, помимо упомянутых LSA Protection и Credential Guard описаны защитные технологии по разграничению прав: минимизация числа аккаунтов в группах «Domain Admins», внедрение мультилогиновой модели, регулярная смена пароля. Изучение академических исследований и руководств позволяет сформулировать гипотезы исследования: во-первых, активация средств защиты LSA и Credential Guard резко снижает объем извлекаемых учётных данных (например, минимизируя успешные PtH-атаки); во-вторых, строжайшее соблюдение AD Tiering (запрет

логина Domain Admin на машины низших уровней) и защита AdminSDHolder ограничивают возможности злоумышленника по эскалации привилегий после утечки учётных данных; наконец, сравнение конфигураций «с защитой/без защиты» покажет качественные различия в полученных хешах и доступах, подтверждая эффективность этих мер [14].

Методы исследования

Исследование носило прикладной характер и включало практическую реализацию атаки Mimikatz для демонстрации рисков. В экспериментальной среде была развернута виртуальная лаборатория на базе Windows Server 2019 с контроллером домена Active Directory и двумя тестовыми учётными записями (одна — с правами доменного администратора, другая — локального администратора). Для сбора данных выполнялся захват NTLM-хешей. Такая форма лабораторной работы соответствует учебно-методическому подходу к изучению сетевого и системного администрирования [15].

Авторы подтверждают, что все учётные записи, пароли и хэши относятся к изолированному синтетическому учебному стенду; публикуемые строковые значения замаскированы и не являются действующими реквизитами доступа.

Процедура эксперимента включала следующие шаги: 1. Создание пользователей и настройка среды. Были созданы новые учётные записи пользователей с заданными паролями и распределены по группам (Domain Admins и Administrators). 2. Затем на контроллере домена были запущены команды Mimikatz для извлечения хешей NTLM. Результаты работы Mimikatz (извлечённые учётные данные) сохранились для анализа. 3. С помощью сторонних ресурсов был проведен анализ NTLM-хешей. 4. Использовали две практики защиты инфраструктуры (усложнение пароля и включение LSA Protection), построенной на технологии AD, провели повторную имитацию атаки и сравнили результаты.

Результаты исследования

В ходе практической части работы была успешно реализована имитация атаки на инфраструктуру Active Directory с последующим анализом защитных мер. На этапе развертывания стенда в оснастке «Active Directory — пользователи и компьютеры» была создана учетная запись пользователя с именем Stealer, которая для целей эксперимента была включена в привилегированные группы, включая Administrators и доменную группу Mim. Проверка состава групп подтвердила корректность настройки прав доступа, необходимых для проведения дальнейших манипуляций в системе.

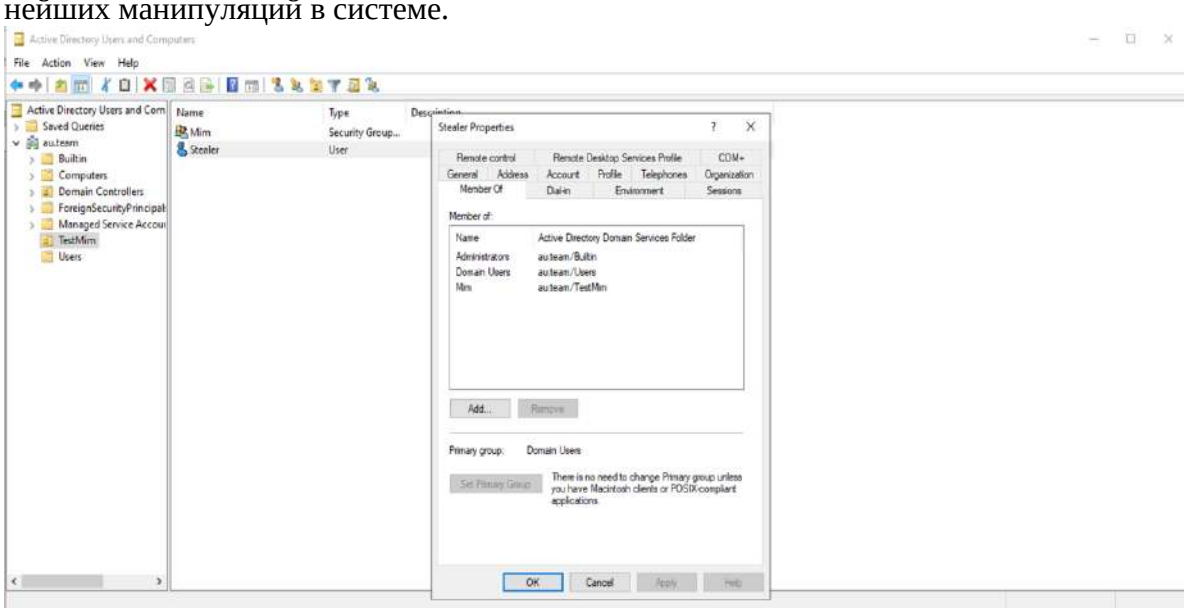

Рис. 1. Настройка прав доступа и членства пользователя Stealer в группах администраторов.

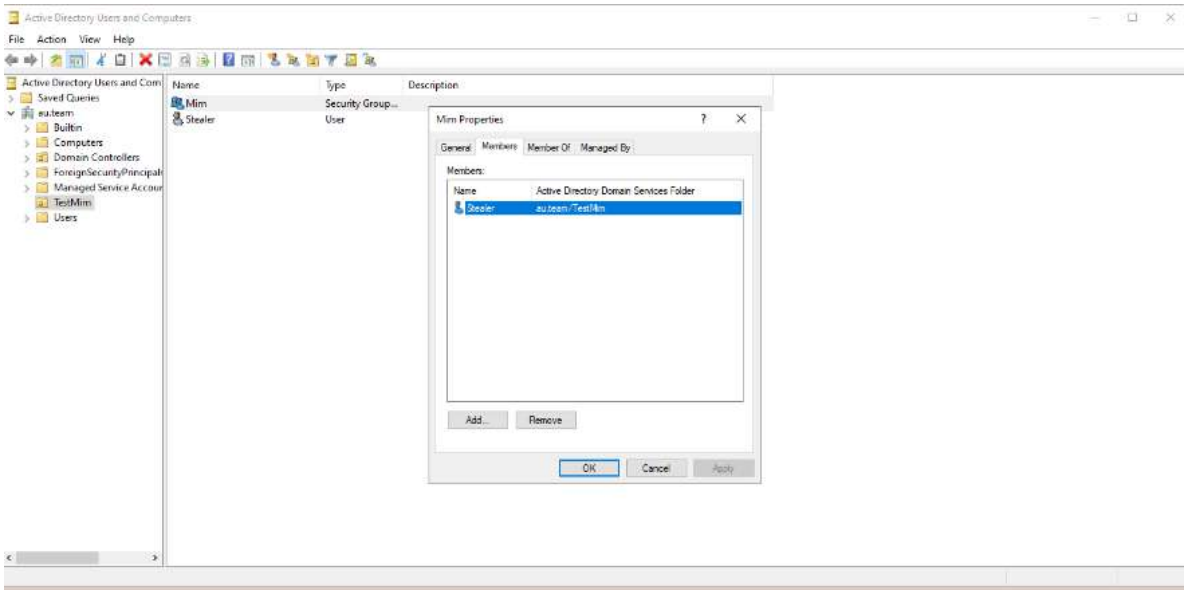

Рис. 2. Список учетных записей группы Mim

После подготовки среды был произведен запуск утилиты Mimikatz с правами локального администратора (из-под учетной записи Stealer). С помощью последовательного ввода команд privilege::debug и sekurlsa::logonpasswords был осуществлен доступ к памяти процесса LSASS [4]. В результате работы утилиты из оперативной памяти были успешно извлечены аутентификационные данные активных сессий. В частности, для учетной записи Administrator был получен NTLM-хеш: [учебное значение скрыто редакцией]. Полученные данные свидетельствуют о возможности полной компрометации учетной записи без знания исходного пароля в открытом виде.

```
cd C:\Users\Stealer\Desktop
cd .\mimikatz_trunk\
cd .\x64\
dir
.\mimikatz.exe
privilege::debug
sekurlsa::logonpasswords
```

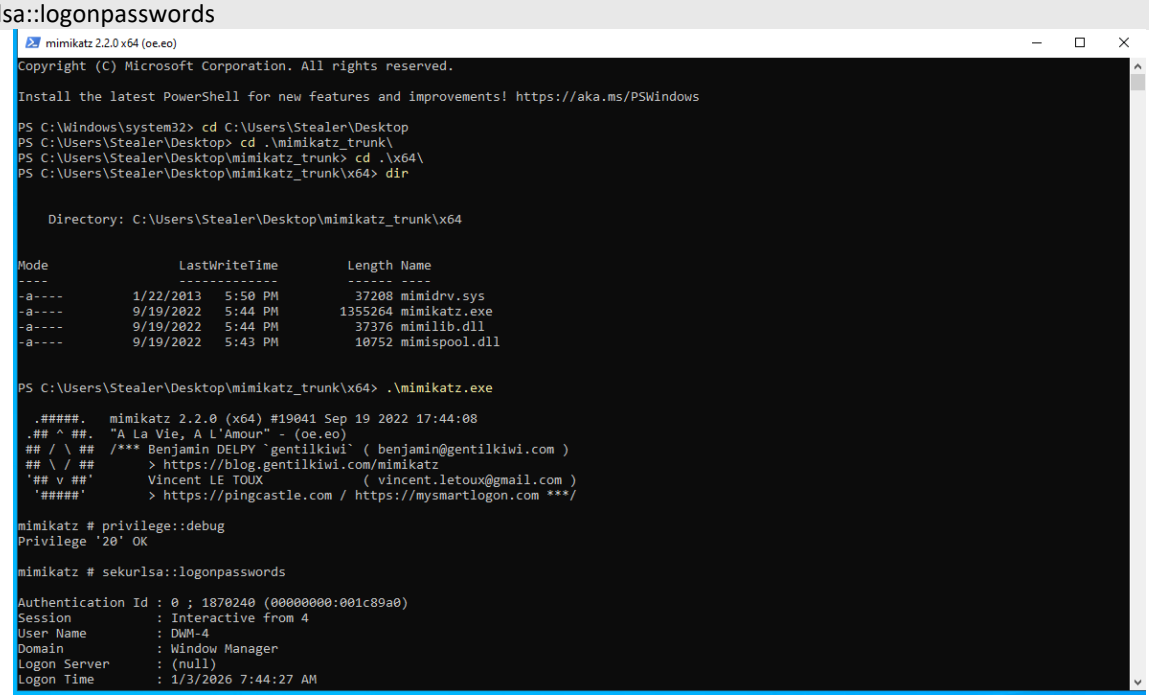

Рис. 3. Ввод команд Mimikatz

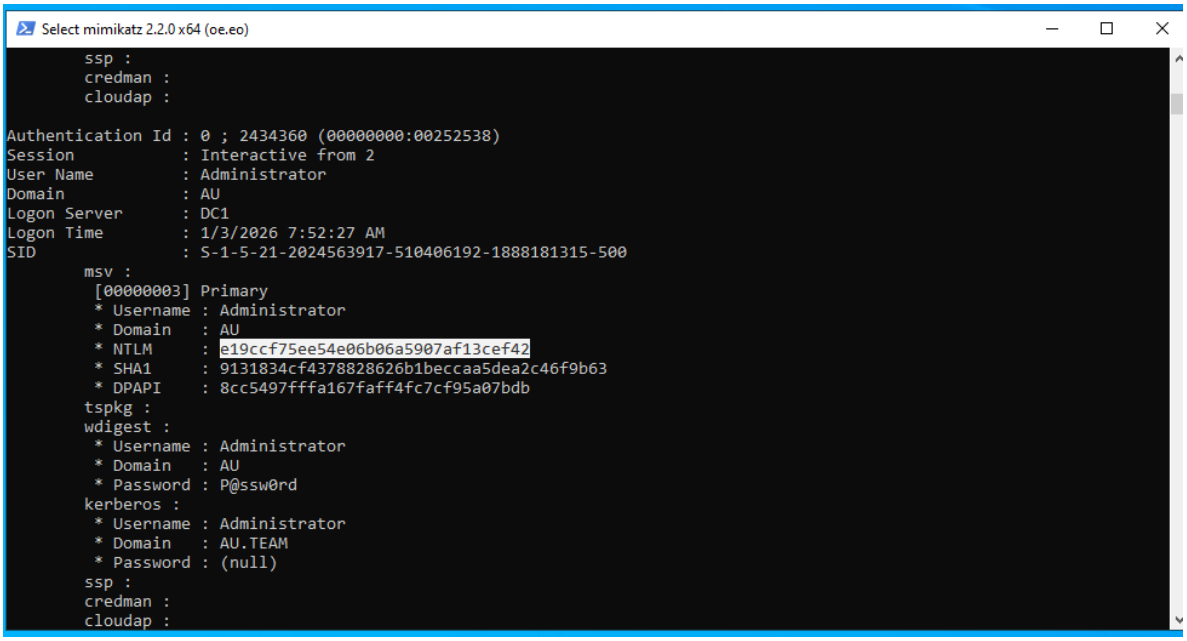

Рис. 4. Извлечение NTLM-хеша учетной записи Administrator с помощью Mimikatz

Для оценки критичности выявленной уязвимости был проведен анализ извлеченного хеша с использованием специализированных онлайн-сервисов Hashes.com и CrackStation. В обоих случаях проверка по базам данных известных паролей заняла менее секунды. Хеш был успешно дешифрован, результатом чего стал пароль «[слабый учебный пароль скрыт редакцией]». Это подтверждает, что использование простых, словарных паролей делает инфраструктуру уязвимой не только к атакам типа Pass-the-Hash, но и к быстрому восстановлению пароля злоумышленником.

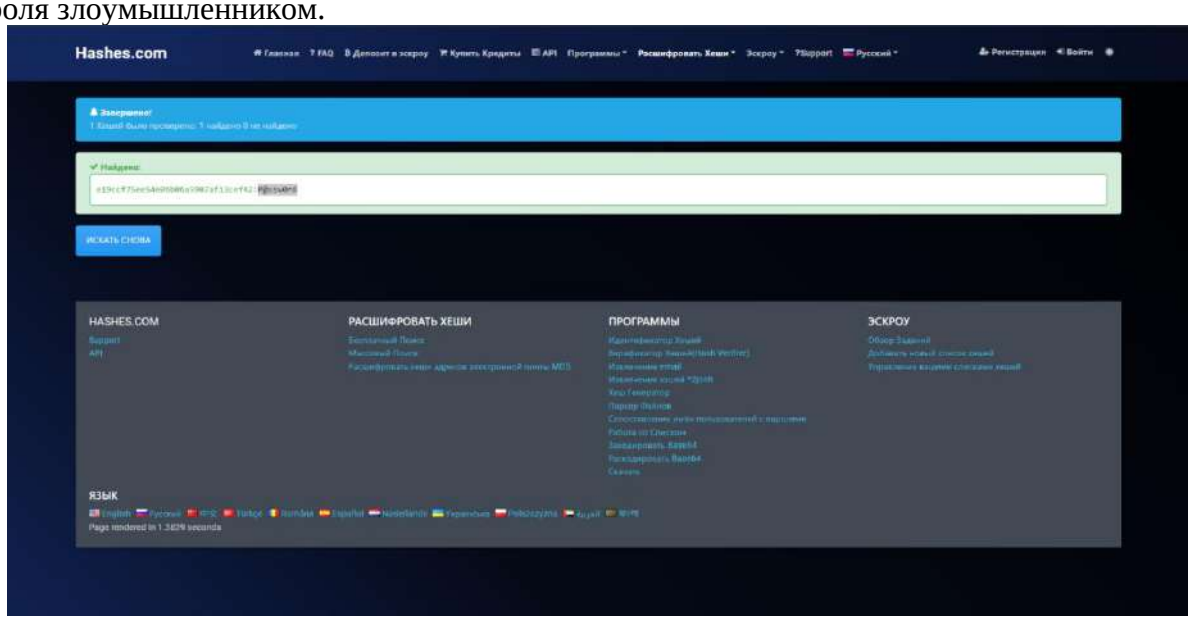

Рис. 5. Успешная дешифровка слабого пароля через онлайн-сервис (Hashes.com)

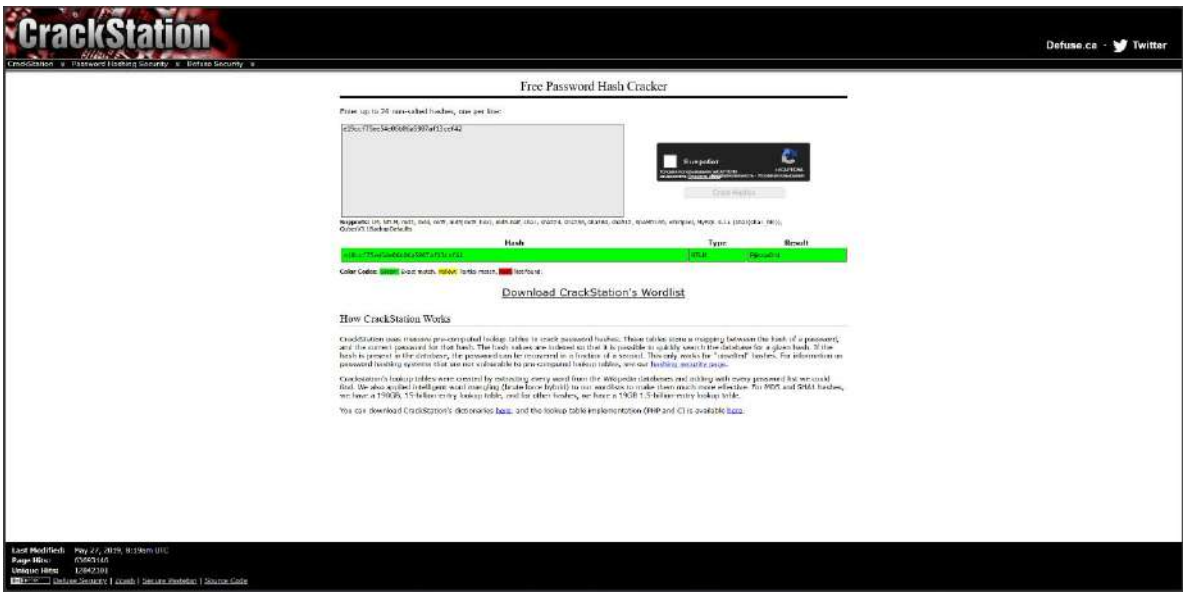

Рис. 6. Успешная дешифровка слабого пароля через онлайн-сервис (CrackStation.net)

Далее была применена практика усиления парольной политики. Для учетной записи Administrator был установлен новый, криптостойкий пароль: [стойкий учебный пароль скрыт редакцией]. После смены пароля была проведена повторная имитация атаки. Несмотря на то, что Mimikatz снова смог извлечь актуальный NTLM-хеш ([учебное значение скрыто редакцией]), попытка его анализа через сервис CrackStation завершилась неудачей — хеш не был найден в базе. Сравнительный анализ результатов показал, что использование сложных паролей и регулярная их ротация значительно повышают трудоемкость атаки, делая невозможным восстановление пароля методами простого перебора по словарям.

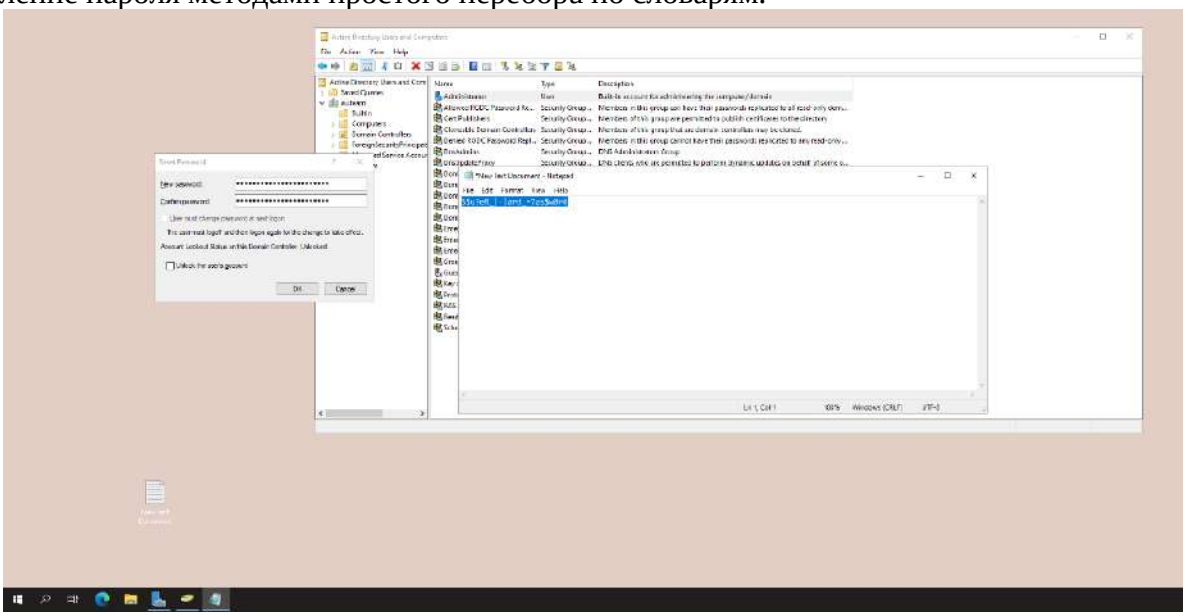

Рис. 7. Установка сложного пароля S$u?eR_|-|ard_=7as$w0r6

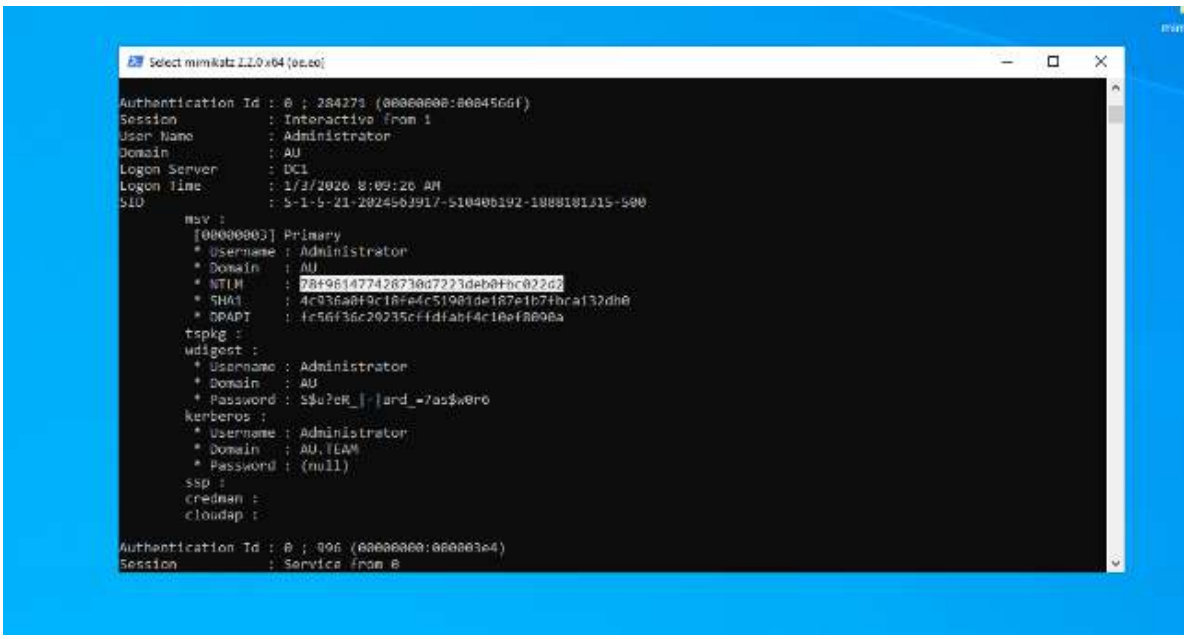

Рис. 8. Извлечение NTLM-хеша учетной записи Administrator с помощью Mimikatz после смены пароля

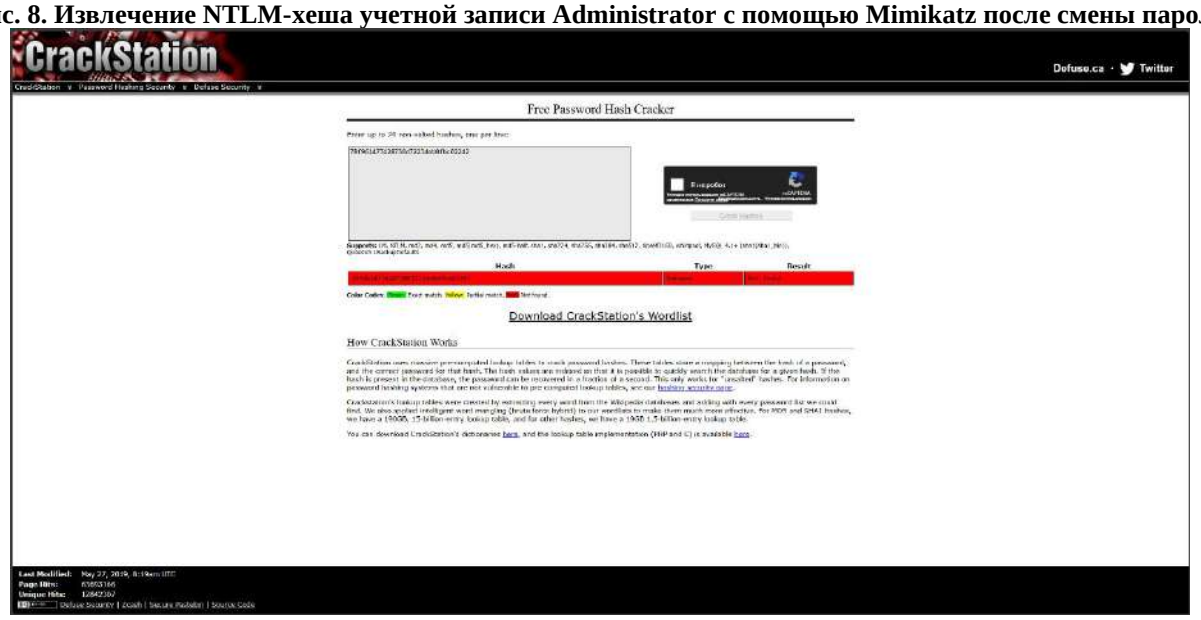

Рис. 9. Неуспешная дешифровка сильного пароля через онлайн-сервис (CrackStation.net)

На заключительном этапе эксперимента включили LSA Protection.Мы вошли в учетную запись Administrator. В редакторе реестра перешли по пути HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa, создали ключ RunAsPPL, изменили его значение данных на 00000001, чтобы настроить функцию защиты LSA с переменной UEFI. Перезапустили контроллер домена, открыли окно просмотра событий (Event Viewer) и в журнале системы нашли событие «WinInit : 12: LSASS.exe был запущен как защищенный процесс с уровнем 4». Это значит, что LSA запускается в защищенном режиме при запуске Windows.

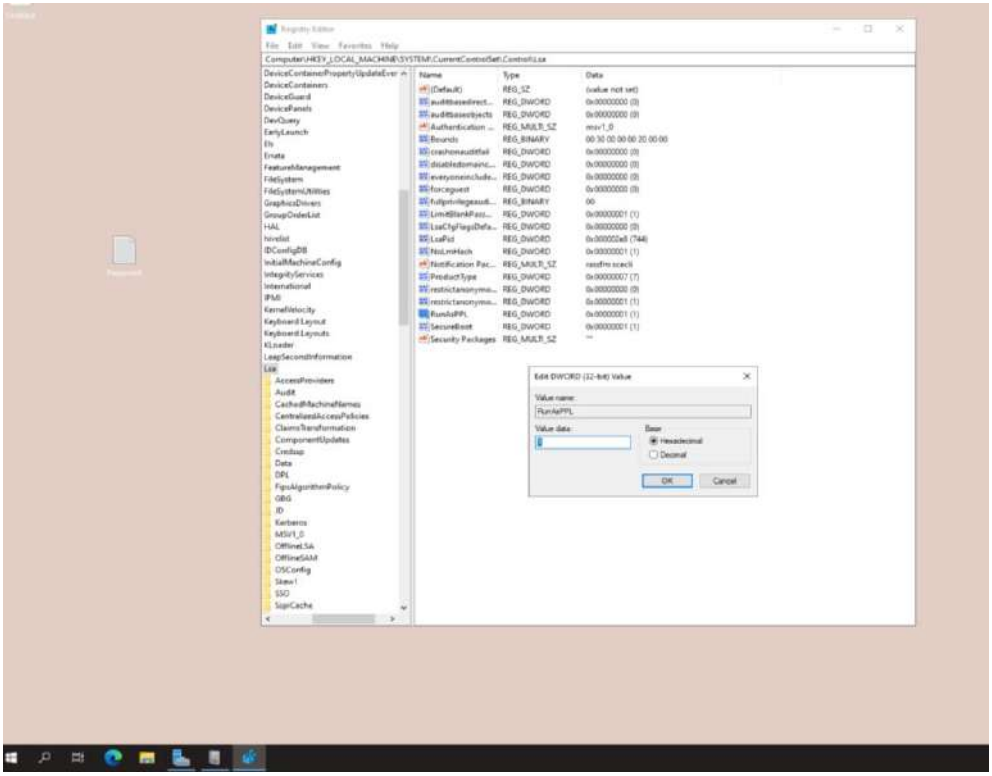

Рис. 10. Изменение значения ключа RunAsPPL в редакторе реестра

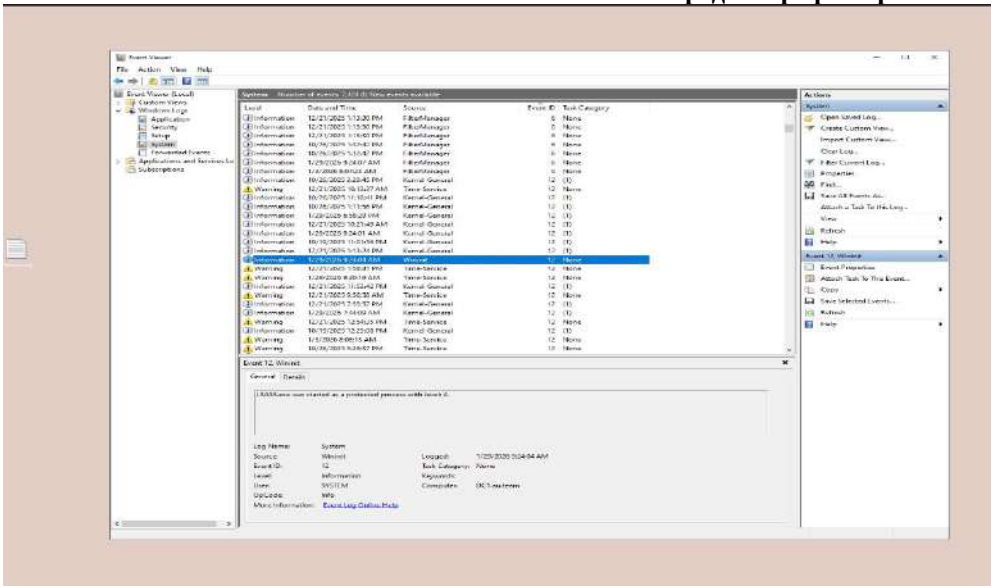

Рис. 11. Просмотр журнала событий системы

Перешли на учетную запись Stealer. Попробовали повторно извлечь NTLM-хеш, но программа выдала ошибку (см. рис. 12).

```
cd C:\Users\Stealer\Desktop
cd .\mimikatz_trunk\
cd .\x64\
.\mimikatz.exe
privilege::debug
sekurlsa::logonpasswords
```

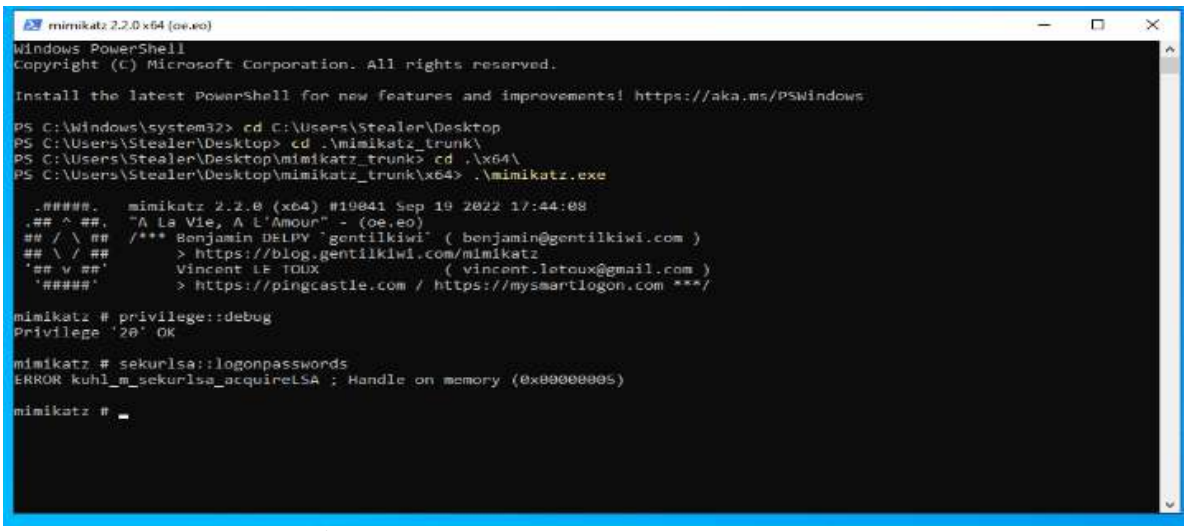

Рис. 12. Ошибка при попытке извлечь NTLM-хеш с помощью Mimikatz

Заключение

Проведенное исследование наглядно продемонстрировало уязвимость стандартных механизмов аутентификации в инфраструктуре Active Directory перед инструментами извлечения учетных данных из оперативной памяти. Экспериментальным путем было подтверждено, что использование утилиты Mimikatz позволяет злоумышленнику, обладающему правами администратора, успешно обходить локальные механизмы защиты и получать доступ к NTLM-хешам активных сессий пользователей.

Анализ результатов первой фазы эксперимента показал, что использование простых словарных паролей фактически сводит защиту к нулю, так как наличие доступных онлайн-баз позволяет восстановить пароль в открытом виде практически мгновенно. Это дает атакующему возможность не только использовать технику Pass-the-Hash, но и полноценно закрепиться в системе под легитимными данными.

Внедрение политики криптостойких паролей во второй части исследования подтвердило свою эффективность как базового эшелона защиты: несмотря на успешное извлечение хеша из памяти, его дешифровка с помощью известных словарей и радужных таблиц стала невозможной. Радужные таблицы представляют собой заранее рассчитанные сопоставления «пароль → хеш», которые позволяют быстро находить пароль по хешу без полного перебора, если пароль входит в предварительно вычисленное множество. Отсутствие записи в подобных таблицах означает только защиту от таких предопределённых словарных атак, но не исключает возможности его подбора методом полного перебора (brute-force) или подбором по маске с использованием современных GPU-акселераторов (например, Hashcat) и других специализированных инструментов. Таким образом, даже достаточно длинный и сложный пароль, оставаясь вне словарей и радужных таблиц, не гарантирует абсолютной стойкости, если злоумышленник обладает доступом к NTLM-хешу и мощным вычислительным ресурсам. Важнейшей мерой защиты является предотвращение самой утечки хеша: если хеш попадёт в руки злоумышленника, он становится объектом оффлайн-подбора вне зависимости от исходной сложности пароля. Соответственно, следует подчеркнуть важность мер защиты, предотвращающих утечки хешей: использование группы «Защищенные пользователи», многоуровневое управление привилегиями (AD Tiering) и внедрение технологий LSA Protection, Credential Guard и подобных, что в совокупности значительно повышает трудоемкость атаки и минимизирует риски компрометации сети.

В ходе эксперимента было доказано, что активация механизма LSA Protection (через параметр реестра RunAsPPL) является критически важным барьером. После настройки и подтверждения запуска процесса LSASS в защищенном режиме утилита Mimikatz не смогла получить доступ к памяти процесса даже с правами администратора. Это подтверждает, что перевод LSASS в статус защищенного процесса (PPL) эффективно блокирует попытки несанкционированного чтения секретов из памяти.

Следует отметить, что сценарий, реализованный в эксперименте, изначально стал возможен из-за фундаментального нарушения принципа разделения привилегий. В нем администратор домена (учетная запись уровня Tier 0) выполнял вход и работал на обычной рабочей станции, отнесенной к более низкому уровню доверия (Tier 1 или 2). Внедрение модели многоуровневого администрирования (Tiering) предотвратило бы саму возможность проведения такой атаки, поскольку учетные данные администраторов уровня Tier 0 (пароли, хеши, Kerberos-тикеты) никогда не кэшировались бы и не обрабатывались в памяти менее защищенных систем нижних уровней. Таким образом, даже если злоумышленник получит полный контроль над рабочей станцией, в ее памяти просто не окажется высокопривилегированных учетных данных, представляющих ценность для атак на критическую инфраструктуру. Внедрение модели Tiering является организационно-технической мерой, дополняющей технические средства вроде LSA Protection и создающей глубокоэшелонированную защиту, где компрометация одного уровня не приводит к катастрофическим последствиям для всей сети.

Библиографический список

1. Success with Enterprise Mobility + Identity [Электронный ресурс] : блог-пост // Microsoft Security Blog. Microsoft Tech Community. — 2016. — URL: https://techcommunity.microsoft.com/blog/microsoft-security-blog/success-with-enterprise-mobility-identity/248613 (дата обращения: 31.12.2025).
2. Active Directory under siege: Why traditional hardening isn’t enough [Электронный ресурс] // The Hacker News. — 2025. — URL: https://thehackernews.com/2025/11/active-directory-under-siege-why.html (дата обращения: 31.12.2025).
3. Хакер, С. Mimikatz — легенда хакерских инструментов: как работает, зачем нужен и почему его боятся все админы [Электронный ресурс] / С. Хакер // SecurityLab. — 2024. — URL: https://www.securitylab.ru/blog/personal/SimlpeHacker/355268.php (дата обращения: 31.12.2025).
4. Fazel, M. A. P. Comprehensive Mimikatz Ebook: A Practical Guide to Post-Exploitation / M. A. P. Fazel, M. Rashidi // SSRN Electronic Journal. — 2025. — DOI: 10.2139/ssrn.5190361.
5. How It Works (Credential Guard) [Электронный ресурс] // Microsoft Learn. — URL: https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/how-it-works (дата обращения: 31.12.2025).
6. Why You Should Enable LSA Protection [Электронный ресурс] // Lepide. — 2023. — URL: https://www.lepide.com/blog/why-you-should-enable-lsa-protection/ (дата обращения: 31.12.2025).
7. Protected Users Security Group [Электронный ресурс] // Microsoft Learn. — URL: https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group (дата обращения: 31.12.2025).
8. Binduf, H. O. Active Directory and Related Aspects of Security / H. O. Binduf, H. Alamoudi, S. Balahmar, H. Alshamrani, H. Al-Omar, N. Nagy // 2018 21st Saudi Computer Society National Computer Conference (NCC). — Riyadh, 2018. — P. 4474–4479. — DOI: 10.1109/NCG.2018.8593188.
9. Ebad, S. A. Lessons learned from offline assessment of security-critical systems: the case of Microsoft’s Active Directory / S. A. Ebad // International Journal of System Assurance Engineering and Management. — 2022. — Vol. 13. — P. 535–545. — DOI: 10.1007/s13198-021-01236-2.
10. Grillenmeier, G. Protecting Active Directory against modern threats / G. Grillenmeier // Network Security. — 2021. — Vol. 2021, iss. 11. — P. 15–17. — DOI: 10.1016/S1353-4858(21)00132-X.
11. Kumar, C. Active Directory and Its Security Testing / C. Kumar, S. S. Debnath, A. Kar, P. Debbarma, S. Piramanayagam // Proceedings of International Conference on Advanced

Communications and Machine Intelligence. MICA 2023. — Singapore : Springer, 2024. — DOI: 10.1007/978-981-97-6222-4_43.
12. Tier model [Электронный ресурс] // Microsoft Learn. — URL: https://learn.microsoft.com/en-us/microsoft-identity-manager/pam/tier-model-for-partitioning-administrative-privileges (дата обращения: 31.12.2025).
13. Reducing the Active Directory attack surface [Электронный ресурс] // Microsoft Learn. — URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/reducing-the-active-directory-attack-surface (дата обращения: 31.12.2025).
14. T1558.001 Golden Ticket [Электронный ресурс] // MITRE ATT&CK. — URL: https://attack.mitre.org/techniques/T1558/001/ (дата обращения: 31.12.2025).
15. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для СПО / А. Г. Уймин. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 480 с. — ISBN 978-5-8114-9255-8.

References

1. Microsoft Security Blog. (2016). Success with Enterprise Mobility + Identity. Microsoft Tech Community. Retrieved December 31, 2025, from https://techcommunity.microsoft.com/blog/microsoft-security-blog/success-with-enterprise-mobility-identity/248613
2. The Hacker News. (2025). Active Directory under siege: Why traditional hardening isn't enough. Retrieved December 31, 2025, from https://thehackernews.com/2025/11/active-directory-under-siege-why.html
3. Khaker, S. (2024). Mimikatz — the legend of hacking tools: How it works, why it is needed, and why all administrators fear it. SecurityLab. Retrieved December 31, 2025, from https://www.securitylab.ru/blog/personal/SimlpeHacker/355268.php
4. Fazel, M. A. P., & Rashidi, M. (2025). Comprehensive Mimikatz Ebook: A practical guide to post-exploitation. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5190361
5. Microsoft Learn. (n.d.). How It Works (Credential Guard). Retrieved December 31, 2025, from https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/how-it-works
6. Lepide. (2023). Why you should enable LSA Protection. Retrieved December 31, 2025, from https://www.lepide.com/blog/why-you-should-enable-lsa-protection/
7. Microsoft Learn. (n.d.). Protected Users Security Group. Retrieved December 31, 2025, from https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group
8. Binduf, H. O., Alamoudi, H., Balahmar, S., Alshamrani, H., Al-Omar, H., & Nagy, N. (2018). Active Directory and related aspects of security. In 2018 21st Saudi Computer Society National Computer Conference (NCC) (pp. 4474–4479). IEEE. https://doi.org/10.1109/NCG.2018.8593188
9. Ebad, S. A. (2022). Lessons learned from offline assessment of security-critical systems: The case of Microsoft's Active Directory. International Journal of System Assurance Engineering and Management, 13, 535–545. https://doi.org/10.1007/s13198-021-01236-2
10. Grillenmeier, G. (2021). Protecting Active Directory against modern threats. Network Security, 2021(11), 15–17. https://doi.org/10.1016/S1353-4858(21)00132-X
11. Kumar, C., Debnath, S. S., Kar, A., Debbarma, P., & Piramanayagam, S. (2024). Active Directory and its security testing. In S. L. Peng et al. (Eds.), Proceedings of International Conference on Advanced Communications and Machine Intelligence. MICA 2023. Springer. https://doi.org/10.1007/978-981-97-6222-4_43
12. Microsoft Learn. (n.d.). Tier model. Retrieved December 31, 2025, from https://learn.microsoft.com/en-us/microsoft-identity-manager/pam/tier-model-for-partitioning-administrative-privileges

13. Microsoft Learn. (n.d.). Reducing the Active Directory attack surface. Retrieved December 31, 2025, from https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/reducing-the-active-directory-attack-surface
14. MITRE ATT&CK. (n.d.). T1558.001 Golden Ticket. Retrieved December 31, 2025, from https://attack.mitre.org/techniques/T1558/001/
15. Uymin, A. G. (2022). Network and system administration. Demonstration exam CODE 1.1: Study guide for secondary vocational education (3rd ed.). Lan Publishing House.

Информация об авторах

Богданов Родион Андреевич — студент ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: bogdanov.r@gubkin.ru.

Гададов Гаджирамазан Джамалутинович — студент ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: gadadov.g@gubkin.ru

STORAGE AND PROTECTION OF DOMAIN ACCOUNTS IN WINDOWS OPERATING SYSTEMS: PASSWORD EXTRACTION TOOLS

Bogdanov R. A.[1], Gadadov G. D.[1]

[1]National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. The article examines the storage and protection of domain accounts in a Windows Server 2019 Active Directory infrastructure. The relevance of the study is determined by the fact that domain credentials remain one of the primary targets in attacks against corporate networks: once such data is compromised, an attacker may escalate privileges, maintain persistence, and gain access to critical resources. The purpose of the work is to assess, in practice, the risks associated with extracting authentication data and to analyze the effectiveness of basic protective measures. The study considers the mechanisms for storing secrets in the LSASS process and in the NTDS.dit database, and includes a controlled laboratory experiment using the Mimikatz utility. The results are compared for a weak password, a cryptographically stronger password, and a configuration with LSA Protection enabled. It is shown that a strong password reduces the probability of rapid password recovery from a hash, but it does not eliminate the possibility of offline cracking and does not prevent the leakage of the hash itself. The most significant result is the confirmation that domain infrastructure protection requires an integrated approach: enabling LSA Protection and Credential Guard, using the Protected Users group, enforcing strict privilege separation, and applying a tiered administration model. The findings may be used in educational laboratories and in the development of organizational and technical measures for protecting Windows domain infrastructures.

Keywords: Active Directory, domain accounts, information security, vulnerabilities, Windows domain infrastructure**.**

Information about the authors

Bogdanov Rodion Andreevich — student of Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: bogdanov.r@gubkin.ru

Gadadov Gadzhiramazan Djamalutinovich — student of Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: gadadov.g@gubkin.ru