КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.807
УДК 004. 005(49)

Рабчун Дмитро Ігорович
к.т.н., доцент кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0002-5555-0910
d.rabchun@duikt.edu.ua

Легомінова Світлана Володимирівна
д.е.н., професор, завідувач кафедри управління кібербезпекою та захистом інформації
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Скрипка Олександр Володимирович
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0002-7809-2884
skrypkaoleksandr04@gmail.com

МЕТОДИ АУТЕНТИФІКАЦІЇ В ACTIVE DIRECTORY ТА ЇХ ВПЛИВ НА БЕЗПЕКУ КОРПОРАТИВНОГО СЕРЕДОВИЩА

Анотація. У статті проведено порівняльний аналіз механізмів аутентифікації NTLM та Kerberos у середовищі Active Directory, з акцентом на їхню архітектуру, типові вразливості та вплив на безпеку корпоративної IT-інфраструктури. Наведено критичний огляд основних загроз й атак на методи аутентифікації Active Directory з наданням основних характеристик та механизмів досягнення мети зловмисника, що більшою мірою пов'язано із використанням застарілих протоколів, таких як NTLM, зокрема Pass-the-Hash та Relay-атаки. Розглянуто потенційні ризики, пов'язані з некоректною конфігурацією Kerberos, включаючи атаки типу Kerberoasting, Golden Ticket та делегування доступу. На основі проведеного аналізу методів аутентифікації в Active Directory, з урахуванням їхніх особливостей, вразливостей і актуальних загроз, сформульовано рекомендації для зміцнення безпеки корпоративного середовища щодо вдосконалення політик аутентифікації, відмови від NTLM, впровадження сучасних підходів до захисту (посилення захисту Kerberos), впровадження моделі Zero Trust, застосування мультифакторної аутентифікації, проведення аудиту та постійного моніторингу безпеки, здійснення регулярного тестування на проникнення та аудитів конфігурації Active Directory, акцентування на навчанні адміністраторів щодо безпечного налаштування Active Directory та оновлень у сфері кіберзагроз. Запропоновані заходи можуть бути використані як основа для підвищення рівня захищеності доменних середовищ у великих організаціях. Доведено, що Kerberos є більш безпечним протоколом, який забезпечує взаємну аутентифікацію та використовує сучасні криптографічні алгоритми, але в разі неправильного налаштування, можливі атаки типу Kerberoasting, атаки на делегування та маніпулювання квитками. Отже,. ефективна конфігурація Active Directory потребує комплексного підходу до безпеки аутентифікаційних механізмів.

Ключові слова: методи аутентифікації; захист корпоративного середовища; загроза, вразливість; кібербезпека; кібератака; Kerberos; NTLM; криптографічні алгоритми.

ВСТУП

У сучасних корпоративних середовищах Active Directory (AD) є основною технологією управління аутентифікацією та авторизацією користувачів. Вона широко

використовується у підприємствах різного масштабу, забезпечуючи централізоване управління доступом до інформаційних ресурсів. Основними методами аутентифікації у AD є NTLM та Kerberos.

Попри їхню популярність, безпека цих механізмів має критичне значення для захисту корпоративного середовища. NTLM, який є застарілим, залишається сумісним із багатьма системами, але має відомі вразливості, включаючи Pass-the-Hash, пониження версії аутентифікації до NTLMv1 та Relay-атаки. З іншого боку, Kerberos є більш безпечним методом, проте його неправильне налаштування може призводити до атак типу «Roasting», атак на делегування та зловживання квитками. Неналежна політика аутентифікації в Active Directory може стати вектором атак для зловмисників, які прагнуть отримати несанкціонований доступ до корпоративних ресурсів. Тому детальний аналіз NTLM і Kerberos є необхідним для розробки ефективної стратегії захисту та мінімізації ризиків.

Постановка проблеми. У сфері кібербезпеки безпека Active Directory та його методи аутентифікації є предметом численних досліджень. У наукових працях та практичних дослідженнях [1], [2] широко розглядаються вразливості NTLM, зокрема атаки Pass-the-Hash та NTLM Relay, що підтверджує ненадійність цього методу в сучасних загрозах.

Інші дослідження [3], [4] акцентують увагу на Kerberos-аутентифікації, її перевагах та потенційних ризиках. Аналізуються атаки на Kerberos, вразливості в механізмах делегування, а також методи підвищення безпеки за допомогою MFA та принципу Zero Trust.

Незважаючи на ці дослідження, практичні аспекти безпечної конфігурації AD з урахуванням сучасних загроз залишаються відкритими. Багато організацій досі використовують NTLM через сумісність зі старими системами, нехтуючи потенційними загрозами. Тому необхідно провести комплексний аналіз обох механізмів аутентифікації, оцінити їхню ефективність та розробити рекомендації для підвищення безпеки Active Directory.

Мета статті. Метою даного дослідження є компаративний аналіз методів аутентифікації NTLM та Kerberos у середовищі Active Directory, їхніх вразливостей, а також впливу на загальну безпеку корпоративних інформаційних систем. У роботі розглядаються основні принципи функціонування цих механізмів, їхні переваги та недоліки, а також потенційні загрози, пов’язані з їхнім використанням. Аналіз дозволив розробити та запропонувати рекомендації щодо безпечної конфігурації Active Directory, мінімізації ризиків, пов’язаних із використанням NTLM, а також впровадження додаткових заходів безпеки для Kerberos-аутентифікації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Методи аутентифікації в Active Directory. NTLM

NTLM (NT LAN Manager) — це застарілий протокол аутентифікації, який використовується у Windows для перевірки особи користувачів та забезпечення доступу до мережевих ресурсів. Незважаючи на його довгу історію використання, NTLM має відомі вразливості, що роблять його ненадійним у сучасних корпоративних середовищах [2].

NTLM базується на механізмі Challenge-Response, у якому сервер надсилає клієнту випадковий Challenge, на який клієнт повинен сформувати відповідь, використовуючи хеш свого пароля. Процес аутентифікації в NTLM проходить такі етапи (рис. 1):

– Користувач надсилає запит на аутентифікацію до сервера, надаючи свій логін.
– Сервер надсилає користувачу випадковий Challenge, який слугує як перевірочний маркер.
– Клієнт хешує пароль та використовує його для шифрування отриманого Challenge. Отримане значення надсилається серверу, який передає її контролеру домену (KDC) для перевірки. Контролер домену, використовуючи збережений у себе NTLM-хеш пароля користувача, розшифровує повідомлення та порівнює отриману відповідь із Challenge, який надав сервер. Якщо значення співпадають, сервер надає доступ користувачу.

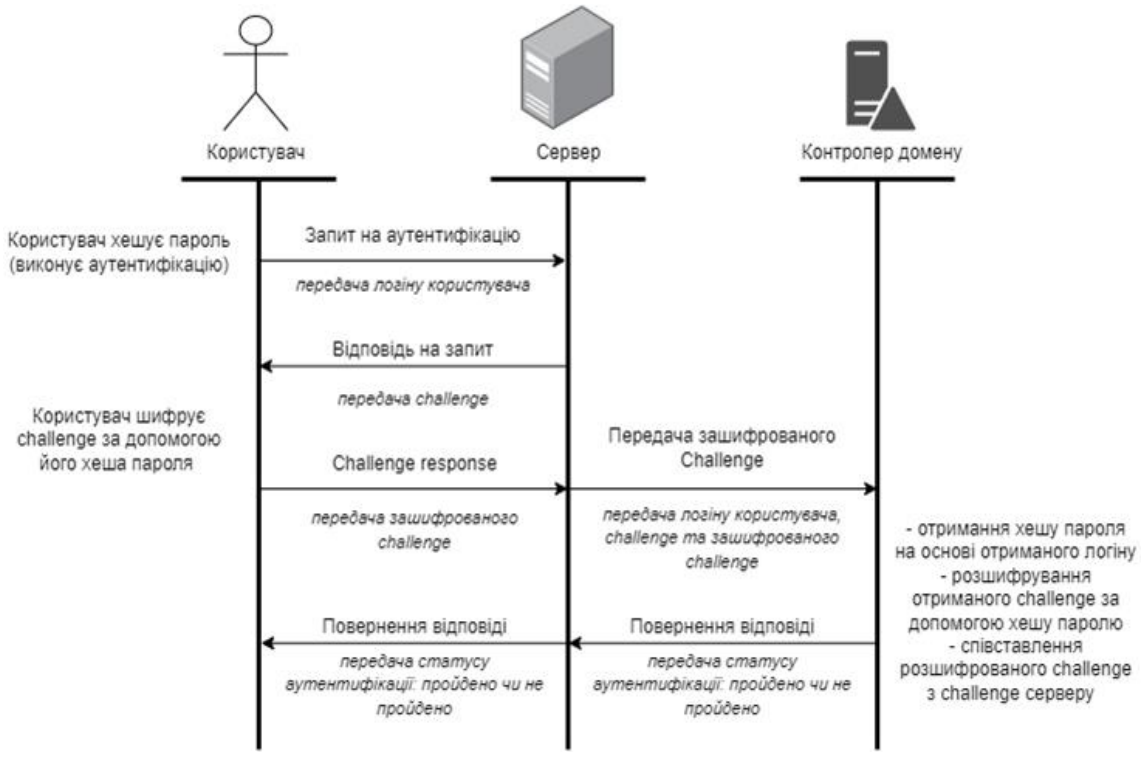

Рис. 1. Схема проходження аутентифікації NTLM в Active Directory

Основними недоліками методу аутентифікації NTLM є:

1. Відсутність взаємної аутентифікації — клієнт не перевіряє сервер, що дозволяє атаки посередника (MITM).
2. Залежність від хешів паролів — атаки на основі повторного використання хешів (Pass-the-Hash).
3. Вразливість до Relay-атак — NTLM не має механізму захисту від повторного використання аутентифікаційних даних.
4. Слабке шифрування — NTLM використовує застарілі криптографічні алгоритми, такі як MD4, що легко піддаються атакам перебору [2].

У зв’язку з цими вразливостями, Microsoft рекомендує відмовитися від NTLM на користь Kerberos або сучасніших методів аутентифікації [5]

Методи аутентифікації в Active Directory. Kerberos

Kerberos — це протокол аутентифікації, який базується на централізованій системі розподілу довіри. Його основною метою є забезпечення безпечної та взаємної аутентифікації між користувачами та сервісами без передачі паролів у мережі. Протокол працює на основі криптографічних квитків, що дозволяє зменшити ризики атак типу перехоплення або повторного використання облікових даних. Kerberos став стандартом для аутентифікації в доменних середовищах Windows, починаючи з Windows 2000. Він використовує трьохсторонню модель довіри, де центральним компонентом виступає KDC (Key Distribution Center) — сервер, що видає квитки аутентифікації та доступу до сервісів.

Аутентифікація Kerberos вимагає участі трьох учасників:

1. Користувач (Client) — це той, хто хоче отримати доступ до сервісу (наприклад, до файлів на сервері).
2. Контролер домену (KDC) — це спеціальний сервер, який відповідає за перевірку особи користувача та видачу йому «квитків».
3. Цільовий сервіс (Service Server) — це кінцева точка, до якої користувач намагається отримати доступ (наприклад, файловий сервер або база даних).

Процес аутентифікації в Kerberos відбувається наступним чином (рис. 2):

1. Користувач вводить логін і пароль на своїй системі. Хеш паролю використовується для шифрування часової мітки (timestamp). Отримане значення та логін користувача використовується для формування запиту на аутентифікацію (AS-REQ) до контролера домену (KDC).
2. KDC перевіряє дані та видає користувачу спеціальний квиток TGT (Ticket Granting Ticket) у відповідь (AS-REP). Цей квиток діє як тимчасовий «паспорт», що підтверджує особу користувача. Також даний квиток шифрується хешем користувача «krbtgt», що означає, що лише цей користувач може його переглянути та підтвердити його справжність.
3. Коли користувач хоче отримати доступ до сервісу, він надсилає свій TGT до KDC із запитом на доступ (TGS-REQ).
4. KDC перевіряє TGT та видає сервісний квиток (TGS — Service Ticket) у відповідь (TGS-REP), який у свою чергу шифрується хешем облікового запису сервісу, до якого користувач хоче отримати доступ. Користувач використовує цей сервісний квиток для отримання доступу до цільового сервісу. Сервіс може перевірити справжність квитка, оскільки він може розшифрувати його своїм хешем.

Основними перевагами Kerberos є:

1. Взаємна аутентифікація — і клієнт, і сервер підтверджують свою особу.
2. Надійне шифрування — Kerberos використовує алгоритми, такі як AES, що значно підвищує стійкість до атак перебору.
3. Механізм використання квитків TGT та TGS — кожен квиток має термін дії та унікальний ідентифікатор, що частково ускладнює повторне використання квитків.

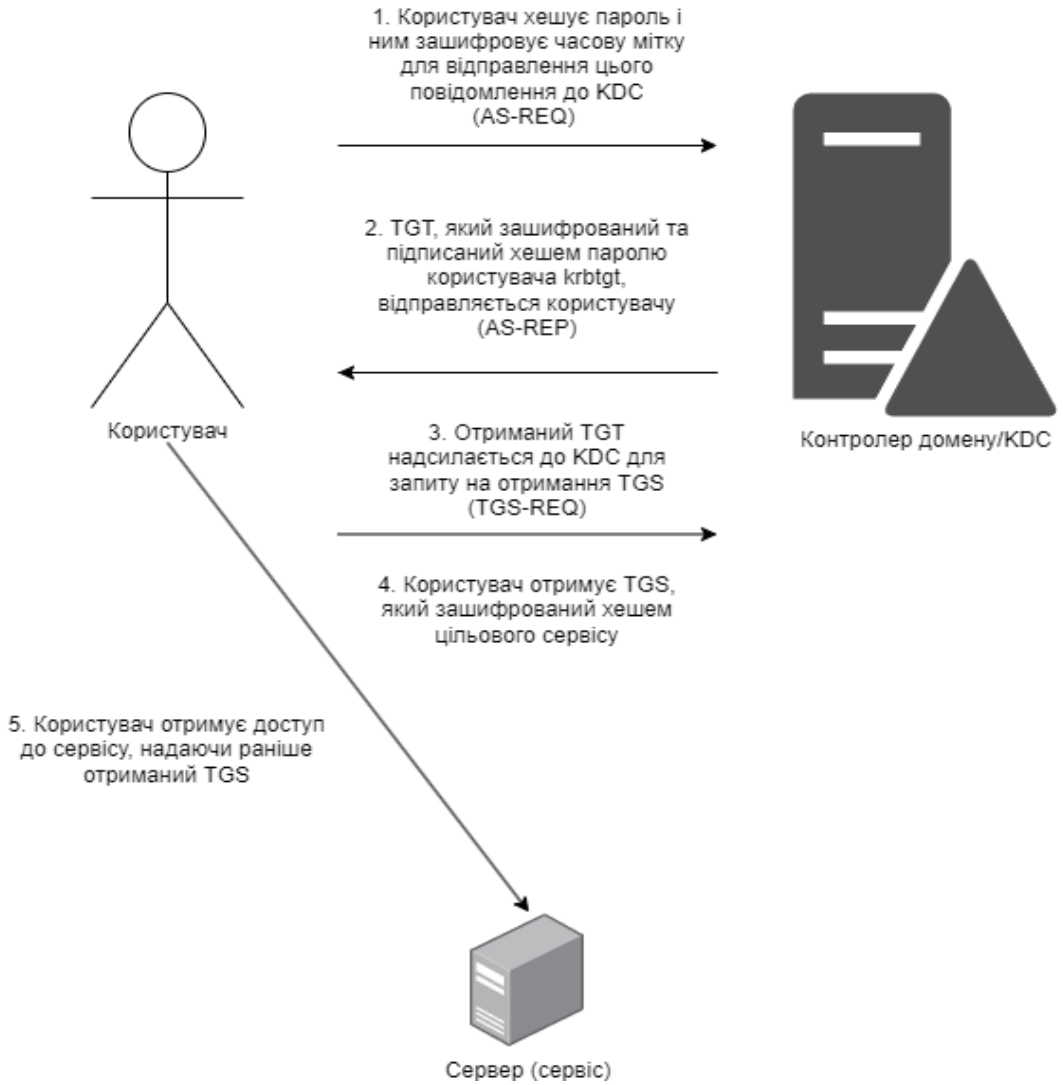

Рис. 2. Схема проходження аутентифікації Kerberos в Active Directory

ОСНОВНІ ЗАГРОЗИ І АТАКИ НА МЕТОДИ АУТЕНТИФІКАЦІЇ AD

Pass-the-Hash (PtH). Цей тип атаки дозволяє зловмиснику автентифікуватися в системі, не знаючи реального пароля користувача. Замість цього використовується хеш пароля, який можна викрасти із пам'яті процесів або файлів SAM. Оскільки NTLM не перевіряє походження хешу, така атака може бути ефективною у будь-якому середовищі, де використовується NTLM, особливо у випадку наявності привілейованих облікових записів у спільно використовуваних ресурсах [1].

NTLM Relay. Цей механізм атаки базується на перехопленні запиту автентифікації, який потім ретранслюється до іншої системи. У результаті зловмисник може отримати доступ до ресурсів, не маючи ані пароля, ані хешу. NTLM Relay ефективно працює у середовищах, де не впроваджено підписування SMB або LDAP, що робить ці протоколи вразливими до MITM-атак [6].

Kerberoasting. Ця атака передбачає отримання сервісних квитків (TGS) на облікові записи служб, які використовують слабкі паролі. Отримані квитки можна дешифрувати офлайн із використанням брутфорс- або словникових атак для виявлення пароля

сервісного облікового запису. Такий доступ часто відкриває шлях до подальших привілейованих дій у домені [7].

Golden Ticket. Golden Ticket — це техніка, яка дозволяє створити фальшиві TGT (квитки на автентифікацію), використовуючи зкомпрометований ключ krbtgt. Ці квитки можуть надавати безстроковий доступ до будь-яких ресурсів у домені, дозволяючи зловмиснику залишатися непоміченим тривалий час навіть після зміни паролів користувачів [8].

Silver Ticket. На відміну від Golden Ticket, Silver Ticket використовується для отримання доступу до окремих сервісів. Він створюється за допомогою хешу пароля конкретного сервісного облікового запису. Оскільки він не потребує взаємодії з KDC, виявлення такої атаки складніше, а захист менш очевидний [9].

Інші атаки на Kerberos. До цієї категорії входять повторне використання TGT/TGS (ticket replay), експлуатація неправильної конфігурації політик шифрування та аналіз метаданих квитків (наприклад, з використанням інструментів типу Rubeus чи Mimikatz) для побудови повного графу доступу в домені.

Розуміння вказаних загроз є передумовою для розробки ефективних рекомендацій щодо захисту інфраструктури.

РЕКОМЕНДАЦІЇ

На основі вищенаведеного аналізу методів аутентифікації в Active Directory, з урахуванням їхніх особливостей, вразливостей і актуальних загроз, сформульовано наступні рекомендації для зміцнення безпеки корпоративного середовища:

1. Відмова від NTLM:
   a. Максимально обмежити або повністю вимкнути використання NTLM у домені.
   b. Виявити системи, які ще потребують NTLM, та розробити план їх модернізації або ізоляції [2].
2. Посилення захисту Kerberos:
   a. Застосовувати складні паролі та змінювати ключ krbtgt у разі підозри на компрометацію.
   b. Обмежити unconstrained delegation та уникати конфігурацій, які дозволяють Resource-Based Constrained Delegation без контролю [3].
   c. Регулярно моніторити видачу сервісних квитків та активність, пов'язану з Kerberos.
3. Мультифакторна аутентифікація (MFA):
   a. Впровадити MFA для доступу до критичних ресурсів і адміністративних облікових записів [4].
4. Моделі Zero Trust:
   a. Впровадити Zero Trust-підхід: верифікація кожного запиту доступу незалежно від того, звідки він походить.
5. Аудит та моніторинг:
   a. Впровадити системи журналювання та моніторингу аутентифікаційної активності (наприклад, використання TGT, AS-REQ/REP, TGS-REQ/REP).
   b. Налаштувати оповіщення на підозрілу активність у контексті аутентифікації.
6. Регулярне проведення тестування на проникнення та аудитів конфігурації Active Directory:
   a. Регулярно проводити внутрішні та зовнішні тестування на проникнення з акцентом на аутентифікацію та привілейовані дії в AD.

b. Використовувати автоматизовані інструменти для перевірки конфігурацій безпеки та відповідності політик найкращим практикам.
c. Аналізувати конфігурацію Active Directory на предмет небезпечних налаштувань, таких як надмірні права делегування, неправильні ACL та інші потенційні вразливості, що можуть бути використані зловмисниками. Проводити регулярне навчання адміністраторів щодо безпечного налаштування AD та оновлень у сфері кіберзагроз.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У ході аналізу механізмів аутентифікації NTLM і Kerberos в Active Directory було виявлено ключові особливості та вразливості кожного з них, що мають значний вплив на загальну безпеку корпоративного середовища.

NTLM, хоча і сумісний зі старими системами, вважається застарілим і ненадійним методом через численні вразливості, такі як Pass-the-Hash, Relay-атаки та слабка криптографія. Його використання в сучасних середовищах створює суттєві ризики несанкціонованого доступу.

Kerberos, навпаки, є більш безпечним протоколом, що забезпечує взаємну аутентифікацію та використовує сучасні криптографічні алгоритми. Проте, за умов неправильного налаштування, можливі атаки типу Kerberoasting, атак на делегування та маніпулювання квитками (наприклад, Golden/ Silver Ticket).

Таким чином, ефективна конфігурація Active Directory потребує комплексного підходу до безпеки аутентифікаційних механізмів, з урахуванням їхніх властивостей та можливостей зловмисника**.**

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dvir Y. (2024). The End of an Era: Understanding the Security Risks of NTLM. *Silverfort Blog*. https://www.silverfort.com/blog/understanding-the-security-risks-of-ntlm/
2. Patton B. NTLM authentication: what it is and why you should avoid using it. Quest Software Blog, 2021. https://blog.quest.com/ntlm-authentication-what-it-is-and-why-you-should-avoid-using-it/ .
3. QOMPLX. (2020). QOMPLX Knowledge: Kerberos Delegation Attacks Explained *QOMPLX*. https://www.qomplx.com/blog/qomplx-knowledge-kerberos-delegation-attacks-explained/
4. Amigorena F. (2024). IS Decisions. Prevent lateral movement with multi-factor authentication (MFA). *ISDecisions*. https://www.isdecisions.com/en/blog/mfa/how-to-prevent-lateral-movement-with-mfa/ .
5. Palko M. (2023). The evolution of Windows authentication. *Windows IT Pro Blog*. https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-evolution-of-windows-authentication/ba-p/3926848
6. Mitchell D. (2024). Critical Risks and Performance Impact of Using NTLM v1 and SMB v1 Protocols: Urgent Security Concerns for Legacy Systems. *Orillia Computer Blog*. https://www.orillia-computer.ca/critical-risks-and-performance-impact-of-using-ntlm-v1-and-smb-v1-protocols
7. Özeren S. (2024). What Is a Kerberoasting Attack? *Picus Security Blog*. https://www.picussecurity.com/resource/blog/kerberoasting-attack-explained-mitre-attack-t1558.003
8. Mizrahi I. (2025). Steal or Forge Kerberos Tickets: Golden Ticket. *MITRE ATT&CK*. https://attack.mitre.org/techniques/T1558/001/
9. MITRE ATT&CK. (2025). Steal or Forge Kerberos Tickets: Silver Ticket. *MITRE ATT&CK*. https://attack.mitre.org/techniques/T1558/002/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Svitlana Lehominova
Doctor of Economics, Professor
Head of Information Security and Cyber Security Management Department
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Dmytro Rabchun
Cand. of Technical Sciences (Ph.D),
Associate Professor of Information Security and Cyber Security Department, State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-5555-0910
rabchundima92@gmail.com

Oleksandr Skrypka
Student
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0002-7809-2884
skrypkaoleksandr04@gmail.com

AUTHENTICATION METHODS IN ACTIVE DIRECTORY AND THEIR IMPACT ON CORPORATE ENVIRONMENT SECURITY

Abstract. The article provides a comparative analysis of NTLM and Kerberos authentication mechanisms in the Active Directory environment, focusing on their architecture, typical vulnerabilities, and impact on the security of corporate IT infrastructure. A critical review of the main threats and attacks on Active Directory authentication methods is provided, providing the main characteristics and mechanisms for achieving the attacker's goal, which is largely associated with the use of outdated protocols such as NTLM, in particular Pass-the-Hash and Relay attacks. Potential risks associated with incorrect Kerberos configuration are considered, including attacks such as Kerberoasting, Golden Ticket, and access delegation. Based on the analysis of authentication methods in Active Directory, taking into account their features, vulnerabilities and current threats, recommendations have been formulated to strengthen the security of the corporate environment in terms of improving authentication policies, abandoning NTLM, implementing modern approaches to protection (strengthening Kerberos protection), implementing the Zero Trust model, using multi-factor authentication, conducting audits and continuous security monitoring, conducting regular penetration testing and Active Directory configuration audits, focusing on training administrators on secure Active Directory configuration and updates in the field of cyber threats. The proposed measures can be used as a basis for increasing the level of security of domain environments in large organizations. It has been proven that Kerberos is a more secure protocol that provides mutual authentication and uses modern cryptographic algorithms, but in case of incorrect configuration, attacks such as Kerberosting, delegation attacks and ticket manipulation are possible. So,. Effective Active Directory configuration requires a comprehensive approach to the security of authentication mechanisms.

Keywords: authentication methods; corporate environment protection; threat, vulnerability; cybersecurity; cyberattack; Kerberos; NTLM; cryptographic algorithms.

REFERENCES

1. Dvir, Y. (2024, August 15). *The end of an era: Understanding the security risks of NTLM*. Silverfort. https://www.silverfort.com/blog/understanding-the-security-risks-of-ntlm/
2. Patton, B. (2021). *NTLM authentication: What it is and why you should avoid using it.* Quest Software. https://blog.quest.com/ntlm-authentication-what-it-is-and-why-you-should-avoid-using-it/
3. QOMPLX. (2020, May 29). *QOMPLX Knowledge: Kerberos delegation attacks explained.* QOMPLX. https://www.qomplx.com/blog/qomplx-knowledge-kerberos-delegation-attacks-explained/

4. Amigorena, F. (2024). *Prevent lateral movement with multi-factor authentication (MFA)*. ISDecisions. https://www.isdecisions.com/en/blog/mfa/how-to-prevent-lateral-movement-with-mfa/
5. Palko, M. (2023). *The evolution of Windows authentication. Windows IT Pro Blog*. https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-evolution-of-windows-authentication/ba-p/3926848
6. Mitchell, D. (2024). *Critical risks and performance impact of using NTLM v1 and SMB v1 protocols: Urgent security concerns for legacy systems*. Orillia Computer. https://www.orillia-computer.ca/critical-risks-and-performance-impact-of-using-ntlm-v1-and-smb-v1-protocols
7. Özeren, S. (2024). *What Is a Kerberoasting Attack?* Automated Security Validation Platform | Picus. https://www.picussecurity.com/resource/blog/kerberoasting-attack-explained-mitre-attack-t1558.003
8. *Steal or Forge Kerberos Tickets: Golden Ticket, Sub-technique T1558.001*. Enterprise | MITRE ATT&CK®. (n.d.). MITRE ATT&CK®. https://attack.mitre.org/techniques/T1558/001/
9. *Steal or Forge Kerberos Tickets: Silver Ticket, Sub-technique T1558.002*. Enterprise MITRE ATT&CK®. (n.d.). MITRE ATT&CK®. https://attack.mitre.org/techniques/T1558/002/