teacher Labels classroom corners with different opinions; students choose one and discuss their reasoning. This allows diverse viewpoints to appear. One more idea, which encourages students to speak is Speed Debating – Students pair up and argue both sides of a topic within a time limit. This forces them to think quickly and articulate their ideas effectively.

☞ Example: For a topic like «Social media is more harmful than beneficial», students can debate and provide real-life examples to support their arguments.

4. Use Thought-Provoking Prompts

Many students struggle to think of what to say. Using visual and conceptual prompts helps develop ideas and generates discussions. Teachers should show controversial statements (e.g., «Robots will replace soldiers in the future.») and ask students to react. This encourages analytical thinking. «Would you rather...?» questions help encourage comparisons. Having students respond to pictures, quotes, or real-world scenarios can involve students in alive discussion.

☞ Example: Show a picture of a war scene from science fiction film and ask, «What do you think war will be like in 2050?» This helps students develop speculative language and express opinions.

References

1. Gebhard, J. G. (2006). Teaching English as a foreign or second language: A teacher self-development and methodology guide. University of Michigan Press.
2. Hornby, G. (1995). Definition of speaking skill. New York: The Publisher.
3. Kagan, S. (n.d.). Kagan (2009). Kagan Cooperative Learning. San Clemente. CA: Kagan Publishing.

НЕБЕЗПЕЧНІ ПРОТОКОЛИ ТА МЕТОДИ ШИФРУВАННЯ У ACTIVE DIRECTORY

Антон АНТОНЮК,
здобувач другого (магістерського) рівня вищої освіти
Рівненський державний гуманітарний університет

Павло КІНДРАТ,
кандидат юридичних наук, доцент, доцент кафедри цифрових технологій та методики навчання інформатики
Рівненський державний гуманітарний університет

Анотація. Розглянуто застарілі та небезпечні протоколи автентифікації й шифрування в Active Directory – LAN Manager, NTLMv1 та RC4-HMAC у Kerberos – а також показано їхні вразливості, що відкривають шлях до атак типу brute-force, pass-the-hash і relay. Запропоновано практичні кроки з міграції на безпечніші механізми (NTLMv2, Kerberos з AES) та вимкнення небезпечних алгоритмів через групові політики.
Ключові слова: Active Directory, NTLM, Kerberos, криптографічна безпека.

Anton ANTONIUK, Pavlo KINDRAT. Insecure Protocols and Encryption Methods in Active Directory

Abstract. Examined outdated and insecure authentication and encryption protocols in Active Directory – LAN Manager, NTLM v1, and RC4-HMAC in Kerberos – and highlights their vulnerabilities that enable brute-force, pass-the-hash, and relay attacks. Practical steps are proposed for migrating to more secure mechanisms (NTLM v2, Kerberos with AES) and disabling unsafe algorithms through Group Policy.
Key words: Active Directory, NTLM, Kerberos, cryptographic security.

Active Directory (AD) – це служба каталогів, що широко використовується для автентифікації та авторизації в середовищах Windows. З часом протоколи автентифікації та алгоритми шифрування, які використовуються в AD, еволюціонували: від застарілих і небезпечних (LAN Manager, NTLMv1) до більш захищених (NTLMv2, Kerberos з AES). Однак задля сумісності багато середовищ досі підтримують старі методи, що створює вразливості («Основи Active Directory»).

LAN Manager – один із ранніх протоколів автентифікації Microsoft (кінця

1980-х), який використовує LM-хеш паролю. Цей протокол має критичні криптографічні слабкі місця. Алгоритм LM-хешування обмежує довжину паролю 14 символами та не враховує регістр літер (усі літери переводяться в верхній регістр). Більше того, пароль ділиться на дві частини по 7 символів, і хеш обчислюється окремо для кожної половини. Через це комплексність пароля значно знижується – фактично складність 14-символьного паролю стає еквівалентною лише складності двох окремих 7-символьних паролів. Відсутність *salting* (додавання випадкових даних до паролю перед хешуванням) дозволяє використовувати попередньо обчислені *rainbow*-таблиці для надшвидкого зламу LM-хешів. Наслідок – LM-хеші можна зламати за лічені секунди за допомогою rainbow-таблиць або за кілька хвилин брутфорсом. Ці слабкості роблять протокол LAN Manager неприйнятним для використання у сучасних системах. Починаючи з Windows NT, LM був замінений на NTLM, а у сучасних версіях Windows хеші LM за замовчуванням не зберігаються («Інформація про те, чому не…»).

NTLMv1 – це протокол автентифікації на основі механізму виклику-відповіді (*challenge-response*), що прийшов на заміну LM у Windows NT. NTLMv1 використовує більш сильний алгоритм обчислення хешу пароля (так званий NT-хеш на основі MD4, який враховує регістр і може містити до 127 символів), тож він усунув частину проблем LM. Однак NTLM версії 1 на сьогодні вважається дуже слабким протоколом автентифікації. Він вразливий до цілого ряду атак, таких як: bruteforce, pass-the-hash та інших. Через ці вразливості NTLMv1 підлягає повному вимкненню. Microsoft впровадила вдосконалений NTLMv2 ще у Windows NT 4.0 SP4, тож NTLMv1 слід розглядати тільки як спадщину, несумісну з безпековими вимогами сьогодення («Інформація про те, чому не…»).

NTLMv2 – покращена версія NTLM, що усуває деякі слабкі місця NTLMv1. Вона додає до механізму автентифікації клієнтський випадковий компонент і мітку часу, що робить відповіді більш стійкими до перебору та повторного

відтворення (replay). NTLMv2 використовує HMAC-MD5 для формування відповіді на виклик, з ключем на основі NT-хешу (MD4) пароля. Ці вдосконалення значно підвищують стійкість протоколу: зокрема, *challenge* має змінну довжину і включає випадковість від клієнта, тому попередньо обчислені таблиці майже непридатні. NTLMv2 став стандартним для несумісних з Kerberos сценаріїв починаючи з Windows 2000 і досі підтримується в сучасних системах. Втім, попри поліпшення, NTLMv2 все ще суттєво поступається Kerberos у безпеці. Він успадкував більшість концептуальних проблем NTLM-протоколів: pass-the-hash та NTLM Relaying. Отже, NTLMv2 слід розглядати як мінімально припустимий протокол автентифікації у Windows-середовищі, і лише за відсутності Kerberos. У доменних середовищах, де клієнт і сервер – члени одного AD-домену, завжди переважно використовується Kerberos; NTLMv2 застосовується лише як запасний варіант для сумісності («Інформація про те, чому не…»).

Kerberos – це протокол автентифікації з розподілом секретних ключів (*shared-secret key*), який став стандартним у AD з часів Windows 2000. Він значно безпечніший завдяки взаємній автентифікації (клієнт і сервер обидва підтверджують особу через квитки, видані центром Kerberos – контролером домену) та використанню квитків з симетричним шифруванням. Втім, і в Kerberos є потенційно небезпечні застарілі методи шифрування, серед яких алгоритм RC4.

RC4 – поточний шифр, який використовувався Microsoft для сумісності в реалізації Kerberos (шифрування RC4-HMAC). Історично облікові записи в AD отримували RC4-ключ для Kerberos, побудований на основі NT-хешу паролю. RC4 вважався достатньо надійним у 90-х, але нині цей алгоритм застарів: відомі вразливості та статистичні перекоси в генерації ключового потоку, що робить його менш стійким, ніж сучасні алгоритми (наприклад, AES). У контексті Active Directory наявність RC4 як дозволеного типу шифрування відкриває шлях до атак типу Kerberoasting, що дозволяє потенційно отримати квиток цільового акаунта

та виконати брутфорс атаку для підбору пароля. Проблема RC4 полягає в тому, що злам таких квитків відбувається на кілька порядків швидше, ніж злам квитків, зашифрованих AES**.** Дослідження показують, що паролі з квитків RC4 можна розкрити більш ніж в 800 разів швидше, ніж якби ті самі паролі були захищені AES-шифруванням. Наприклад, практичний експеримент продемонстрував, що квиток Kerberos з RC4 може бути зламаний за 25 хвилин, тоді як такий самий квиток з AES – за понад 13 днів на тому ж обладнанні. Це колосальна різниця, яка робить RC4 надзвичайно привабливим для атакуючих. Крім того, оскільки ключ RC4 в Kerberos фактично еквівалентний NTLM-хешу паролю, компрометація квитка дозволяє отримати цей хеш і потім застосувати «Pass-the-Hash» в інших сервісах. Через небезпечність RC4, Microsoft поступово відмовляється від нього. У нових версіях Windows Server (2016+), за наявності AES-ключів у акаунтів, Kerberos за замовчуванням віддає перевагу AES. Оновлення безпеки (наприклад, CVE-2022-37966) змінили поведінку контролерів домену, встановивши AES як тип шифрування за умовчанням для сесійних ключів замість слабкого RC4. У Windows Server 2022 RC4 взагалі позбавлений статусу безпечного: його використання в домені деактивовано або жорстко обмежено («Методи шифрування в…»).

Для поліпшення безпеки інфраструктури рекомендується («Рекомендації щодо імплементації…»):

- повністю вимкнути LM та NTLMv1 протоки, використовуючи групові політики;
- мінімізувати використання NTLMv2;
- впровадити використання AES шифрування в Kerberos.

Список використаних джерел

1. Основи Active Directory. Вилучено з: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
2. Інформація про те, чому не варто використовувати LAN та NTLMv1.

Вилучено з: https://miriamxyra.com/2017/11/08/stop-using-lan-manager-and-ntlmv1/

3. Методи шифрування в протоколі Kerberos. Вилучено з: https://syfuhs.net/lessons-in-disabling-rc4-in-active-directory
4. Рекомендації щодо імплементації безпеки у Active Directory. Вилучено з: https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/active-directory-hardening-series---part-1-%E2%80%93-disabling-ntlmv1/3934787

References

1. Basics of Active Directory. Retrievered from: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
2. Reasons for not using LAN and NTLMv1. Retrievered from: https://miriamxyra.com/2017/11/08/stop-using-lan-manager-and-ntlmv1/
3. Encryption methods in Kerberos protocols. Retrievered from: https://syfuhs.net/lessons-in-disabling-rc4-in-active-directory
4. Recommendations about implementing security in Active Directory: Retrievered from: https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/active-directory-hardening-series---part-1-%E2%80%93-disabling-ntlmv1/3934787

ПІДГОТОВКА ІНЖЕНЕРІВ-ПРОГРАМІСТІВ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ В УМОВАХ ЗМІШАНОГО НАВЧАННЯ

Микола БІЛЕЦЬКИЙ,

аспірант

Рівненський державний гуманітарний університет

Анотація. У статті проаналізовано основні причини, що зумовлюють стрімку цифровізацію освітнього процесу, імплементацію дистанційного та змішаного