https://doi.org/10.31891/2307-5732-2026-365-63
УДК 004.056.5:004.738.5

ПЕТЛЯК НАТАЛІЯ
Хмельницький національний університет
https://orcid.org/0000-0001-5971-4428
e-mail: npetlyak@khmnu.edu.ua
МОСТОВИЙ СЕРГІЙ
Хмельницький національний університет
https://orcid.org/0000-0002-9505-3206
e-mail: serhii.mostovyi@khmnu.edu.ua
СОКОЛ ДАР'Я
Хмельницький національний університет
https://orcid.org/0009-0002-0374-9976
e-mail: sokoldara46@gmail.com
БЕРБЕЦ ДЕНИС
Хмельницький національний університет
https://orcid.org/0009-0000-6616-7952
e-mail: dberbets70@gmail.com

АНАЛІЗ ВРАЗЛИВОСТЕЙ ПРОТОКОЛУ KERBEROS У СЕРЕДОВИЩІ ACTIVE DIRECTORY

У статті здійснено комплексний аналіз архітектури, механізмів функціонування та типових векторів атак на протокол автентифікації Kerberos у середовищі Active Directory. Розглянуто основні вразливості, пов'язані з компрометацією облікових записів, маніпуляцією автентифікаційними квитками та використанням NTLM-хешів. Особливу увагу приділено опису атак типу Golden Ticket, Silver Ticket, Pass-the-Ticket, Kerberoasting та AS-REP Roasting, які реалізуються через конфігураційні недоліки та обмеження моделі довіри. Показано, що навіть низькопривілейовані облікові записи можуть бути використані як точка входу для складних атак. На основі проведеного дослідження сформульовано практичні рекомендації щодо підвищення стійкості до зазначених загроз шляхом посилення моніторингу, зміни політик управління обліковими записами та захисту критичних компонентів автентифікаційної інфраструктури.

Ключові слова: *Kerberos, Active Directory, безпека автентифікації, атаки на основі квитків, Golden Ticket, Kerberoasting, безпека доменної інфраструктури.*

NATALIA PETLIAK, SERHII MOSTOVYI, DARYA SOKOL, DENYS BERBETS
Khmelnytskyi National University

ANALYSIS OF KERBEROS PROTOCOL VULNERABILITIES IN ACTIVE DIRECTORY ENVIRONMENT

Kerberos is one of the most widely used authentication protocols in modern corporate environments and serves as a core security mechanism in Microsoft Active Directory infrastructures. Despite its strong cryptographic foundations and long-term adoption, Kerberos remains vulnerable to a range of attacks caused by architectural design choices, trust assumptions, and configuration weaknesses. These vulnerabilities allow attackers to compromise authentication processes, escalate privileges, and maintain long-term persistence within a domain environment. This paper presents a comprehensive analysis of the Kerberos authentication protocol in Active Directory with a focus on typical attack vectors, exploitation techniques, and systemic weaknesses. The study examines the internal architecture of Kerberos, including the role of the Key Distribution Center, Authentication Server, and Ticket Granting Service, and analyzes how trust in ticket-based authentication can be abused when critical secrets are compromised. Special attention is paid to the security implications of the krbtgt account, whose compromise enables the creation of forged Ticket Granting Tickets and undermines the entire trust model of the domain. The research analyzes widely used attack techniques such as Golden Ticket, Silver Ticket, Pass-the-Ticket, Kerberoasting, and AS-REP Roasting. These attacks demonstrate that even low-privileged user accounts can serve as an entry point for complex multi-stage intrusions. The paper highlights the role of NTLM hashes, service account misconfigurations, and credential exposure in the LSASS process as key enablers of these attacks. It is shown that many Kerberos-based attacks can bypass traditional security monitoring mechanisms, particularly when forged tickets are used without direct interaction with domain controllers. In addition, the paper reviews recent academic and practical research on Kerberos attack detection, including behavioral analysis of authentication logs, anomaly detection, and machine learning-based approaches. While such methods improve detection accuracy, they often suffer from false positives and limited adaptability to evolving attack techniques. This emphasizes the need for flexible and context-aware security monitoring solutions. Based on the conducted analysis, practical recommendations are formulated to enhance the resilience of Kerberos-based infrastructures. These include strengthening account management policies, protecting critical processes, regularly rotating sensitive credentials, and improving monitoring of ticket usage patterns. The results of this study contribute to a deeper understanding of Kerberos security risks and provide a foundation for developing more effective defensive strategies against advanced attacks targeting Active Directory authentication mechanisms.

Keywords: *Kerberos, Active Directory, authentication security, ticket-based attacks, Golden Ticket, Kerberoasting, domain infrastructure security.*

Стаття надійшла до редакції / Received 05.03.2026
Прийнята до друку / Accepted 11.04.2026
Опубліковано / Published 28.05.2026

Постановка проблеми

Попри високу криптографічну стійкість та широке впровадження протоколу Kerberos у середовищах Active Directory, його архітектурні особливості та типові конфігураційні помилки зумовлюють наявність критичних вразливостей. Однією з проблем є залежність системи від безпеки окремих облікових записів, зокрема krbtgt (Key Distribution Center Ticket Granting Ticket), компрометація якого відкриває можливість створення фальшивих квитків доступу (Golden Ticket) з довільними правами. Крім того, специфіка реалізації квиткової

моделі не передбачає механізмів перевірки актуальності вмісту квитків, що дає змогу зловмиснику тривалий час зберігати контроль над системою після одноразового втручання. Наявність методів атак, таких як Pass-the-Ticket, Silver Ticket, Kerberoasting та AS-REP Roasting, свідчить про те, що навіть низькопривілейовані облікові записи можуть слугувати точкою входу до розгалужених атак у доменних середовищах. Актуальність проблеми зумовлена також тим, що існуючі засоби журналювання й моніторингу не завжди дозволяють виявити факт компрометації на ранніх етапах, особливо коли атаки відбуваються в межах довіреного контексту. Отже, забезпечення стійкості до цих загроз вимагає ґрунтовного аналізу механізмів роботи Kerberos, виявлення вразливих місць, а також формування практичних рекомендацій щодо зниження ризиків.

Формулювання мети дослідження

Метою дослідження є комплексний аналіз типових сценаріїв компрометації протоколу Kerberos у середовищі Active Directory з акцентом на виявлення системних вразливостей, що використовуються під час атак. Дослідження передбачає визначення основних методів зловживання механізмами автентифікації та авторизації, опис відповідних векторів атак, а також формування рекомендацій щодо підвищення стійкості інфраструктури до таких загроз. Особлива увага приділяється аналізу ролі NTLM-хешів, вразливостей у конфігурації облікових записів і недостатності моніторингових рішень. Результати дослідження мають сприяти створенню практичних заходів з покращення безпеки Kerberos-інфраструктури в умовах сучасних кіберзагроз.

Аналіз останніх досліджень та публікацій

Актуальність проблеми виявлення та протидії атакам на основі протоколу Kerberos підтверджується рядом сучасних наукових досліджень, що висвітлюють зростаючу складність і поширеність загроз, пов'язаних з маніпуляціями в системах автентифікації та авторизації. У роботах [1-3] підкреслюється необхідність посиленої уваги до вразливостей, пов'язаних з підробкою квитків (TGT, TGS), атакою Pass-the-Ticket та використанням застарілих механізмів шифрування, що дозволяють зловмисникам здійснювати ескалацію привілеїв. Автори вказаних досліджень акцентують на важливості моніторингу мережевих логів, побудови профілів нормальної поведінки користувачів та впровадження гібридних підходів до виявлення аномалій.

Значна увага приділяється створенню моделей для ідентифікації ознак зловживання Kerberos-квитками, включно з використанням інструментів штучного інтелекту та машинного навчання. У публікаціях [4-6] досліджено методи аналізу поведінкових шаблонів, частот запитів до служби квитків, а також використання часових характеристик з метою ідентифікації спроб обходу авторизації. Застосування алгоритмів глибокого навчання дозволяє підвищити точність виявлення таких атак, як Kerberoasting та Overpass-the-Hash, однак водночас зростає чутливість до помилково позитивних спрацювань.

У роботах [7-9] розглянуто практичні приклади компрометації інфраструктур Active Directory за допомогою Kerberos-експлойтів, зокрема через маніпуляції з SIDHistory, DCSync і Golden Ticket. Автори пропонують застосовувати багаторівневий аналіз подій безпеки, поєднувати сигнатурні та поведінкові методи, а також впроваджувати автоматизовані системи реакції на інциденти. Наголошується на тому, що навіть складні детекційні моделі потребують постійного оновлення знань про техніки атак.

Дослідження [10-12] зосереджені на стандартизації та впровадженні кращих практик у сфері кіберзахисту аутентифікаційних механізмів, а також на адаптації систем виявлення вторгнень до контексту атак на Kerberos. Проте всі запропоновані рішення, незважаючи на їхню інноваційність, мають обмеження щодо адаптації до нових векторів атак, обхідних технік та залежність від якості вхідних даних. Таким чином, подальші дослідження повинні зосередитися на розробці гнучких, самоадаптивних систем, що здатні в реальному часі виявляти та нейтралізовувати загрози, пов'язані з порушенням цілісності автентифікаційної інфраструктури.

Викладення основного матеріалу дослідження

Протокол Kerberos реалізує модель взаємної автентифікації клієнта та сервера, забезпечуючи захищений доступ до мережевих ресурсів. Усі об'єкти, що беруть участь у процесі автентифікації або запитують доступ до ресурсів, іменуються як принципали (principals). Центральним елементом системи є Центр розподілу ключів (Key Distribution Center, KDC), який виконує функції автентифікації користувачів і видачі квитків для доступу до сервісів.

Архітектура KDC включає два логічні компоненти:

– сервер автентифікації (Authentication Server, AS), що здійснює початкову перевірку користувача;

– службу видачі квитків (Ticket Granting Service, TGS), яка відповідає за формування сервісних квитків для подальшого доступу до ресурсів.

Обидва компоненти функціонують у межах контролера домену, який має можливість запису. Аналіз поетапної роботи протоколу Kerberos є необхідним для розуміння механізмів реалізації атак у середовищі Active Directory.

Процес автентифікації відбувається у кілька послідовних етапів:

1. Клієнт формує хеш від пароля користувача, що надалі використовується як симетричний ключ для захищеного обміну з KDC.

2. Згенерований ключ використовується для шифрування мітки часу, яка надсилається до сервера автентифікації. AS здійснює перевірку, порівнюючи отриману інформацію з еталонними даними у своїй базі. Успішне дешифрування свідчить про знання користувачем правильного пароля.

3. У відповідь сервер AS надсилає клієнту тимчасовий ключ для подальшої взаємодії з KDC (зашифрований хешем користувача) та квиток на отримання сервісів (Ticket Granting Ticket, TGT), що містить

ідентифікаційні атрибути користувача та шифрується паролем облікового запису krbtgt.

4. Клієнт, використовуючи TGT, формує запит до TGS на доступ до конкретної служби.

5. У відповідь TGS надсилає два компоненти: сервісний квиток, зашифрований секретним ключем відповідного сервера, який містить відомості про користувача, сесійну інформацію та часові мітки; сесійний ключ для обміну між клієнтом і сервером, зашифрований ключем із відповіді AS.

6. Клієнт надсилає запит до сервера, супроводжуючи його сервісним квитком. Якщо сервер успішно дешифрує цей квиток, що підтверджує його справжність, запит дозволяється, і встановлюється захищене з'єднання.

Таким чином, механізм Kerberos базується на принципі довіри до об'єктів, автентифікованих KDC, із чітким розмежуванням між етапами перевірки автентичності та авторизації.

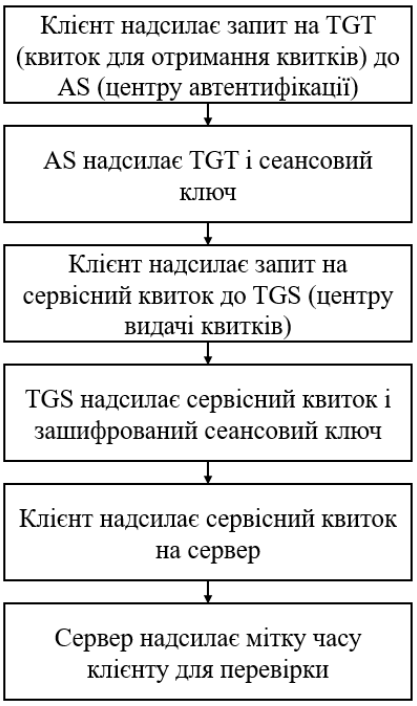

Рис. 1 - Робочий процес автентифікації Kerberos

Однією з концептуальних властивостей протоколу Kerberos є його бездискова архітектура, що передбачає відсутність збереження станів попередніх сесій у компонентах KDC. Уся контекстна інформація, необхідна для автентифікації та авторизації, передається у вигляді квитків, зокрема TGT, який шифрується паролем службового облікового запису krbtgt.

Доступ до дешифрування вмісту TGT мають лише дві сутності: сервер автентифікації (AS), який його видає, та служба видачі квитків, що формує сервісні квитки на його основі. Така модель призводить до двох ключових наслідків. По-перше, пароль облікового запису krbtgt є критично важливим елементом безпеки, оскільки компрометація цього пароля дозволяє зловмиснику створювати довільні TGT та успішно проходити автентифікацію в межах домену. По-друге, вся інформація, закладена в TGT, автоматично вважається достовірною в очах служби TGS, адже вона зашифрована елементом, якому система довіряє за замовчуванням.

Слід зауважити, що пароль облікового запису krbtgt змінюється надзвичайно рідко, часто лише у випадку повного відновлення безпеки домену після інциденту. Це створює серйозну вразливість, оскільки у випадку витоку NTLM-хешу krbtgt, зловмисник може тривалий час формувати фальшиві квитки для обходу механізмів контролю доступу, без потреби в повторній компрометації облікових записів або взаємодії з контролером домену.

Додатковою загрозою є те, що жоден механізм Kerberos не передбачає перевірку актуальності інформації, зашифрованої в TGT. Якщо зловмисник отримав TGT, що містить, наприклад, SID адміністратора домену, такий квиток дозволить здійснювати дії від імені привілейованого користувача до моменту завершення його терміну дії або зміни ключа krbtgt. Це підкреслює необхідність ретельного моніторингу використання квитків, запровадження механізмів виявлення аномальної активності, а також регулярної зміни пароля krbtgt у рамках політик відновлення безпеки Active Directory.

Протокол Kerberos, попри свою криптографічну стійкість та широке впровадження у доменних середовищах, залишається вразливим до низки атак, зумовлених як особливостями його архітектури, так і помилками конфігурації. Найбільш поширеними сценаріями компрометації є ті, що орієнтовані на підробку або повторне використання автентифікаційних квитків, зловживання NTLM-хешами та доступ до критичних компонентів, таких як обліковий запис krbtgt або процес LSASS. Одним із поширених методів є атака типу Pass-the-Ticket. У цьому випадку зловмисник отримує доступ до автентифікаційного квитка користувача (TGT або TGS) і повторно використовує його для доступу до інших сервісів, імітуючи вже автентифікованого користувача. Така атака стає можливою, якщо вдалося отримати контроль над пам'яттю системного процесу, де зберігаються

квитки. Вона є ефективною, зокрема в середовищах із реалізованим єдиним входом, оскільки зловмисник може не проходити повторну автентифікацію, використовуючи чинний TGT. Використання такого квитка не завжди супроводжується підозрілою активністю в логах, особливо якщо IP-адреса або інші параметри доступу не змінюються. Ще більш небезпечним варіантом є атака Golden Ticket. Вона передбачає повну фальсифікацію TGT на основі NTLM-хешу облікового запису krbtgt. Знаючи цей хеш, зловмисник може створити квитки, які ззовні виглядають автентичними, але містять довільну інформацію, зокрема про користувача, його SID та групи. Такий квиток приймається службою TGS як достовірний, оскільки він зашифрований ключем krbtgt. Унаслідок цього зловмисник може видавати себе за будь-якого користувача, включно з адміністраторами домену, не здійснюючи жодного запиту до контролера домену. Єдиним способом анулювання подібних квитків є дворазова зміна пароля krbtgt, що є складною і чутливою операцією в масштабних середовищах. Іншим вектором атаки є Silver Ticket. На відміну від Golden Ticket, вона не потребує компрометації krbtgt, а лише NTLM-хешу облікового запису служби, з якою планується взаємодія. Зловмисник, отримавши цей хеш, може сформувати підроблений TGS для конкретної служби (наприклад, SQL-сервера), що дозволяє доступ до неї напряму. При цьому запит до KDC не здійснюється, а отже подія не фіксується у журналах контролера домену, що значно ускладнює виявлення атаки. Зловмисник отримує рівень доступу, що відповідає повноваженням компрометованого сервісного акаунта. До атак, які можуть здійснюватися навіть з облікового запису звичайного користувача, належить Kerberoasting. Вона базується на запиті сервісного квитка до облікового запису з атрибутом SPN. Оскільки TGS для такої служби шифрується NTLM-хешем відповідного акаунта, зловмисник може зберегти цей квиток і провести офлайн-брутфорс для відновлення пароля. Ефективність атаки суттєво зростає при використанні слабких паролів або застарілих алгоритмів шифрування (наприклад, RC4). Оскільки запит на TGS не потребує підвищених прав, Kerberoasting легко реалізується з низькопривілейованих акаунтів, що значно розширює коло потенційних атакувальних точок. Атака AS-REP Roasting реалізується для акаунтів, у яких вимкнено попередню автентифікацію Kerberos. У такому випадку сервер автентифікації повертає зашифроване повідомлення (AS-REP), яке зловмисник може дешифрувати офлайн. Подібно до Kerberoasting, цей метод базується на витягуванні NTLM-хешу користувача та брутфорсі пароля. Особливо часто ця атака спостерігається у випадках, коли в організації існують тестові або застарілі облікові записи з невірно налаштованими параметрами безпеки.

Усі вищеописані сценарії так чи інакше пов’язані з компрометацією або використанням NTLM-хешів. Основним джерелом таких даних є пам’ять процесу LSASS, який зберігає облікові дані у вигляді хешів або відкритих паролів для забезпечення єдиного входу. Отримавши права адміністратора або системного користувача на одному з вузлів, зловмисник може за допомогою інструментів, таких як Mimikatz, витягнути ці облікові дані. Цей етап часто є поворотним моментом у розвитку атаки, оскільки відкриває можливості для подальших Pass-the-Hash або Golden Ticket атак. Захист LSASS є пріоритетним завданням - використання Credential Guard, обмеження прав доступу до процесу, застосування ізольованих середовищ для адміністраторів є необхідними кроками для унеможливлення таких атак. Отож, типові сценарії компрометації протоколу Kerberos демонструють, що навіть найстійкіші механізми автентифікації залишаються вразливими в умовах недостатнього контролю доступу, неправильної конфігурації або слабких паролів. Оскільки атаки не обов’язково потребують привілейованого початкового доступу, навіть звичайні облікові записи можуть слугувати точкою входу до складних ланцюгів атак. Ефективний захист полягає у регулярному аудиті налаштувань, моніторингу аномальної активності, впровадженні мінімально необхідних прав доступу та комплексній роботі над зменшенням поверхні атаки в межах Kerberos-інфраструктури.

Висновки

Проведене дослідження показало, що попри високий рівень криптографічного захисту, протокол Kerberos залишається вразливим до ряду атак, зумовлених особливостями його архітектури та недоліками конфігурації. Ключовим ризиком є можливість фальсифікації автентифікаційних квитків після компрометації облікових даних, зокрема NTLM-хешів облікових записів krbtgt або сервісних акаунтів. Запропоновані в роботі заходи зосереджуються на підвищенні безпеки за рахунок регулярного аудиту налаштувань, зміцнення контролю доступу до критичних процесів, а також удосконалення систем виявлення аномалій. Урахування векторів атак типу Kerberoasting, Pass-the-Ticket і AS-REP Roasting в політиках безпеки дозволяє суттєво знизити ризики ескалації привілеїв і забезпечити більш ефективний захист доменної інфраструктури.

Література

1. Qatinah S. H., Al-Baltah I. A. Kerberos Protocol: Security Attacks and Solution. 2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI). 2024. P. 1–7. DOI: 10.1109/ICETI63946.2024.10777133.

2. Aksüt Y. An Analysis of Kerberoasting Attack and Detection with Supervised Machine Learning Algorithms. Middle East Technical University. 2024.

3. Grippo T., Kholidy H. A. Detecting Forged Kerberos Tickets in an Active Directory Environment. Cryptography and Security. URL: https://arxiv.org/abs/2301.00044

4. Qbea’h M., Alkaabi J., Almansouri S., Alneyadi A., Alderei M. Classification of Authentication Approaches to Stop the Next Breaking: Challenges, Benefits, Drawbacks, Awareness, and Recommendations. 2023 International Conference on Computer and Applications (ICCA). 2023. P. 1–5. DOI: 10.1109/ICCA59364.2023.10401373.

5. Mokhtar B. I., Jurcut A. D., ElSayed M. S., Azer M. A. Active Directory Attacks—Steps, Types, and Signatures. Electronics. 2022. Vol. 11, No. 16. P. 2629. DOI: 10.3390/electronics11162629.

6. Dora J. R., Hluchy L. Attacks on Active Directory – Resource-based Constrained Delegation and New Patches. 2025 Cybernetics & Informatics (K&I). 2025. P. 1–6. DOI: 10.1109/KI64036.2025.10916465.

7. Matsuda W., Fujimoto M., Mitsunaga T., Watanabe K. Detection of the Silver Ticket for Seamless Single Sign-On Focusing on a Ticket Lifetime. Journal of Information Processing. 2025. Vol. 33. P. 156–167. DOI: 10.2197/ipsjjip.33.156.

8. Zhou J., Yao J., Chen X., Yu S., Xuan Q., Yang X. Lateral Movement Detection via Time-aware Subgraph Classification on Authentication Logs. Cryptography and Security. URL: https://arxiv.org/abs/2411.10279

9. Berardi D., Tippenhauer N. O., Melis A., et al. Time sensitive networking security: issues of precision time protocol and its implementation. Cybersecurity. 2023. Vol. 6. P. 8. DOI: 10.1186/s42400-023-00140-5.

10. Meghana K., Shankaramma, Thippeswamy M. N., Anu A. M., Chaithra M., Nagamani N. Enumeration and Post-Enumeration Attack on Active Directory and Their Detection Using Log Correlation Method. 2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS). 2024. P. 1–6. DOI: 10.1109/CSITSS64042.2024.10817003.

11. Kumar C., Debnath S. S., Kar A., Debbarma P., Piramanayagam S. Active Directory and Its Security Testing. Proceedings of International Conference on Advanced Communications and Machine Intelligence. 2024. Vol. 405. P. 507–519. DOI: 10.1007/978-981-97-6222-4_43.

12. Smiliotopoulos C., Barmpatsalou K., Kambourakis G. Revisiting the Detection of Lateral Movement through Sysmon. Applied Sciences. 2022. Vol. 12, No. 15. P. 7746. DOI: 10.3390/app12157746.

References

1. Qatinah S. H., Al-Baltah I. A. Kerberos Protocol: Security Attacks and Solution. 2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI). 2024. P. 1–7. DOI: 10.1109/ICETI63946.2024.10777133.

2. Aksüt Y. An Analysis of Kerberoasting Attack and Detection with Supervised Machine Learning Algorithms. Middle East Technical University. 2024.

3. Grippo T., Kholidy H. A. Detecting Forged Kerberos Tickets in an Active Directory Environment. Cryptography and Security. URL: https://arxiv.org/abs/2301.00044

4. Qbea'h M., Alkaabi J., Almansouri S., Alneyadi A., Alderei M. Classification of Authentication Approaches to Stop the Next Breaking: Challenges, Benefits, Drawbacks, Awareness, and Recommendations. 2023 International Conference on Computer and Applications (ICCA). 2023. P. 1–5. DOI: 10.1109/ICCA59364.2023.10401373.

5. Mokhtar B. I., Jurcut A. D., ElSayed M. S., Azer M. A. Active Directory Attacks—Steps, Types, and Signatures. Electronics. 2022. Vol. 11, No. 16. P. 2629. DOI: 10.3390/electronics11162629.

6. Dora J. R., Hluchy L. Attacks on Active Directory – Resource-based Constrained Delegation and New Patches. 2025 Cybernetics & Informatics (K&I). 2025. P. 1–6. DOI: 10.1109/KI64036.2025.10916465.

7. Matsuda W., Fujimoto M., Mitsunaga T., Watanabe K. Detection of the Silver Ticket for Seamless Single Sign-On Focusing on a Ticket Lifetime. Journal of Information Processing. 2025. Vol. 33. P. 156–167. DOI: 10.2197/ipsjjip.33.156.

8. Zhou J., Yao J., Chen X., Yu S., Xuan Q., Yang X. Lateral Movement Detection via Time-aware Subgraph Classification on Authentication Logs. Cryptography and Security. URL: https://arxiv.org/abs/2411.10279

9. Berardi D., Tippenhauer N. O., Melis A., et al. Time sensitive networking security: issues of precision time protocol and its implementation. Cybersecurity. 2023. Vol. 6. P. 8. DOI: 10.1186/s42400-023-00140-5.

10. Meghana K., Shankaramma, Thippeswamy M. N., Anu A. M., Chaithra M., Nagamani N. Enumeration and Post-Enumeration Attack on Active Directory and Their Detection Using Log Correlation Method. 2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS). 2024. P. 1–6. DOI: 10.1109/CSITSS64042.2024.10817003.

11. Kumar C., Debnath S. S., Kar A., Debbarma P., Piramanayagam S. Active Directory and Its Security Testing. Proceedings of International Conference on Advanced Communications and Machine Intelligence. 2024. Vol. 405. P. 507–519. DOI: 10.1007/978-981-97-6222-4_43.

12. Smiliotopoulos C., Barmpatsalou K., Kambourakis G. Revisiting the Detection of Lateral Movement through Sysmon. Applied Sciences. 2022. Vol. 12, No. 15. P. 7746. DOI: 10.3390/app12157746.