УДК 004.056

ОЦІНЮВАННЯ РИЗИКУ ЛАТЕРАЛЬНОГО РУХУ APT ДО SCADA-СЕГМЕНТА В СЕРЕДОВИЩІ ACTIVE DIRECTORY

Д. Даниленко[1,a], Л. Ю. Гальчинський[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

Робота присвячена оцінюванню конфігураційних ризиків Active Directory, які можуть створювати передумови для латерального руху APT-актора до критичних ресурсів. Запропоновано графову модель доменного середовища, у якій користувачі, групи, службові облікові записи та критичні ресурси розглядаються як взаємопов'язані об'єкти. Для практичної перевірки моделі розроблено прототип ADAPT Analyzer, який збирає дані з Active Directory через LDAP, визначає ризикові облікові записи, будує потенційні шляхи ескалації та розраховує інтегральний показник ризику. У лабораторному середовищі змодельовано Kerberoasting-ризик для службового облікового запису та шлях латерального руху до групи, що імітує доступ до SCADA-сегмента.

Ключові слова: Active Directory, APT, SCADA, lateral movement, Kerberoasting, LDAP, графова модель, оцінювання ризику.

Вступ

Active Directory є одним із центральних компонентів системи керування доступом у корпоративних інформаційних системах. За його допомогою централізовано адмініструються користувачі, групи, службові облікові записи, комп'ютери, політики доступу та привілейовані ролі. У разі помилок конфігурації доменне середовище Active Directory може стати однією з ключових точок компрометації під час складних багатоетапних атак, зокрема атак типу Advanced Persistent Threat (APT). Феномен APT-атак багатьма фахівцями з кібербезпеки розглядається як одне з найбільш загрозливих явищ для сфери IT [1, 2]. Одній із ключових властивостей таких загроз — персистентності — присвячено низку досліджень, зокрема [3].

Особливо небезпечними є сценарії, у межах яких зловмисник після початкової компрометації звичайного користувацького або службового облікового запису отримує можливість поступово розширювати доступ у домені. Такий процес відповідає тактиці lateral movement, що розглядається в базі знань MITRE ATT&CK як один із етапів просування зловмисника всередині цільового середовища [1]. У промислових і технологічних середовищах кінцевою ціллю такого руху можуть бути системи, пов'язані зі SCADA-сегментом.

1. Постановка задачі

Метою роботи є дослідження можливості виявлення латерального руху APT-атаки до критичного SCADA-сегмента шляхом моделювання процесу оцінювання ризику компрометації доменного середовища Active Directory.

Для досягнення цієї мети необхідно визначити типові конфігураційні вразливості Active Directory, представити об'єкти доменного середовища у вигляді графової моделі, визначити критичні цілі, розробити прототип інструмента для збору й аналізу даних, а також провести лабораторну перевірку запропонованої моделі. Окрему увагу приділено службовим обліковим записам, наявності Service Principal Name (SPN), параметру `PasswordNeverExpires` та вкладеному членству в групах.

2. Конфігураційні ризики Active Directory у контексті APT

У середовищі Active Directory значна частина ризиків пов'язана не лише з окремими вразливостями, а й з помилками конфігурації. До таких помилок належать надмірні привілеї користувачів, наявність службових облікових записів із довготривалими паролями, вкладене членство у групах, неконтрольовані зв'язки з привілейованими групами та наявність SPN у службових облікових записів.

У контексті APT-атаки такі недоліки можуть бути використані не одразу, а як частина поступового просування всередині мережі. Наприклад, після отримання доступу до звичайного користувача зловмисник може дослідити членство у групах і знайти непрямий шлях до привілейованої групи або до групи, що має доступ до критичного сегмента. У випадку службових облікових записів окремий ризик становить наявність SPN, оскільки це створює передумови для

[a]danieldanylenko@gmail.com

Kerberoasting [2, 4].

3. Модель оцінювання ризику

Запропонована модель ґрунтується на представленні Active Directory у вигляді графа. Вершинами графа є користувачі, групи, службові облікові записи та критичні ресурси. Ребрами є зв'язки членства у групах, вкладеність груп і привілейовані відношення між об'єктами. Подібний підхід до аналізу зв'язків у домені використовується в інструментах аналізу attack paths, зокрема у BloodHound [5].

У межах моделі окремо визначаються критичні цілі. До них належать привілейовані групи домену, наприклад `Domain Admins`, `Administrators`, `Backup Operators`, а також групи, що імітують доступ до SCADA-сегмента, наприклад `SCADA Operators`. Наявність шляху від звичайного користувача або службового облікового запису до такої групи інтерпретується як ознака підвищеного ризику латерального руху.

Загальний ризик для користувача можна подати як зважену суму окремих компонентів:

$$R(u) = w_1 P + w_2 S + w_3 K + w_4 W + w_5 A + w_6 C.$$

де P характеризує наявність прямого або непрямого зв'язку з привілейованими групами; S описує ознаки службового облікового запису; K враховує наявність SPN та можливість Kerberoasting; W відображає слабкі параметри пароля; A визначає наявність потенційного шляху ескалації; C характеризує наявність шляху до групи, що імітує доступ до SCADA-сегмента.

Узагальнений алгоритм роботи моделі складається з таких кроків: збір LDAP-даних про об'єкти домену; побудова графа зв'язків між користувачами та групами; визначення критичних цілей; пошук шляху від облікового запису до цільових груп; розрахунок Risk Score та формування переліку факторів ризику. На рис. 1 наведено загальну схему роботи прототипу ADAPT Analyzer, яка відображає послідовність переходу від збору даних до інтерпретації ризику та подальшого усунення небезпечних конфігурацій.

Для більш формального опису роботи модуля оцінювання ризику можна подати спрощений псевдокод алгоритму:

1. зібрати через LDAP множини користувачів, груп, комп'ютерів, SPN та атрибутів облікових записів;
2. побудувати граф $G = (V, E)$, де V — об'єкти Active Directory, а E — зв'язки членства та вкладеності груп;
3. визначити множину критичних цілей T, до якої входять привілейовані групи та групи SCADA-сегмента;
4. для кожного користувача u знайти потенційний шлях $path(u, T)$ до критичних цілей;
5. оцінити компоненти P, S, K, W, A, C та обчислити інтегральний показник $R(u)$;
6. сформувати категорію ризику, перелік факторів ризику та рекомендації щодо усунення виявлених недоліків.

4. Імплементація та експериментальна перевірка

Для практичної реалізації підходу було розроблено програмний прототип ADAPT Analyzer — Active Directory APT Risk Analyzer. Прототип написано мовою C# із використанням .NET і WPF. Збір інформації з доменного середовища відбувається через LDAP. Інструмент отримує дані про користувачів, групи, вкладене членство, службові облікові записи, SPN, параметри паролів і привілейовані відношення між об'єктами. На основі цих даних будується граф потенційних шляхів ескалації та обчислюється сумарний індекс ризику.

Експериментальне тестування проводилося в лабораторному середовищі, що складалося з контролера домену Windows Server 2022, клієнтської Windows-машини, приєднаної до домену `corp.local`, а також Kali Linux, який використовувався для перевірки окремих атакувальних сценаріїв. У домені було створено користувачів, групи, службові облікові записи та змодельовано кілька типових конфігураційних ризиків. Автентифікація Kerberos у Windows-середовищах працює на основі квитків, тому аналіз SPN і Kerberos service ticket є важливим для перевірки Kerberoasting-ризику [6].

Перший експериментальний сценарій був пов'язаний з обліковим записом `svc_web`, для якого було зареєстровано SPN `HTTP/web.corp.local` та встановлено параметр `PasswordNeverExpires`. ADAPT Analyzer класифікував цей обліковий запис як високоризиковий через наявність ознак службового облікового запису, можливість Kerberoasting та відсутність строку дії пароля. Додатково за допомогою Kali Linux було продемонстровано можливість перевірки наявності SPN та отримання Kerberos service ticket.

Другий експериментальний сценарій моделював потенційний латеральний рух до SCADA-сегмента. Для цього користувача `user1` було додано до групи `IT Support`, а групу `IT Support` — до групи `SCADA Operators`, яка в межах лабораторної моделі представляла критичний SCADA-ресурс. У результаті ADAPT Analyzer виявив шлях:

`user1` → `IT Support` → `SCADA Operators`.

Цей шлях було класифіковано як потенційний ризик латерального руху APT до критичного SCADA-сегмента. Після видалення відповідного групового зв'язку шлях до `SCADA Operators` зник, а кількість виявлених шляхів до SCADA-ресурсу в результатах аналізу зменшилася до нуля.

У табл. 1 наведено узагальнення експериментальних сценаріїв. У ній порівнюється початковий стан доменного середовища, результат аналізу ADAPT Analyzer та зміни після усунення відповідних конфігураційних ризиків. Такий формат дозволяє показати, що запропонована модель реагує не лише на

Рис. 1. Узагальнена схема роботи ADAPT Analyzer

Таблиця 1. Результати експериментальної перевірки ADAPT Analyzer

Сценарій	Виявлений стан	Після усунення
Kerberoasting-ризик	`svc_web`: SPN, `PasswordNeverExpires`, рівень `High`	SPN видалено, строк дії пароля відновлено
Латеральний рух до SCADA	`user1` → `IT Support` → `SCADA Operators`	шлях до `SCADA Operators` зник
Привілейований шлях	`user1` → `IT Support` → `Backup Operators`	потребує окремого усунення зв'язку

наявність небезпечної конфігурації, а й на її усунення.

Висновки

У роботі запропоновано модель оцінювання ризику латерального руху APT-атаки в доменному середовищі Active Directory. Модель враховує конфігураційні вразливості, службові облікові записи, SPN, слабкі параметри паролів, вкладене членство у групах та наявність шляхів до критичних SCADA-орієнтованих ресурсів. Розроблений прототип ADAPT Analyzer підтвердив можливість автоматизованого виявлення ризикових об'єктів і потенційних шляхів атаки. У лабораторному середовищі інструмент виявив службовий обліковий запис із Kerberoasting-ризиком та шлях `user1` → `IT Support` → `SCADA Operators`, що моделює латеральний рух до критичного SCADA-сегмента. Після усунення відповідних конфігураційних ризиків рівень ризику знизився, а шлях до SCADA-групи зник із результатів аналізу.

Подальший розвиток роботи передбачає інтеграцію аналізу подій Windows Event Log, зокрема Kerberos-запитів, успішних входів і змін членства у групах. Це дозволить поєднати статичний аналіз конфігурації Active Directory з поведінковими ознаками атаки. Для оцінювання таких поведінкових ознак у майбутньому можуть використовуватися підходи виявлення аномалій, які активно застосовуються в задачах кібербезпеки [7, 8].

Перелік використаних джерел

1. *MITRE ATT&CK*. Lateral Movement, Enterprise Tactic TA0008. — 2025. — URL: https://attack.mitre.org/tactics/TA0008/.
2. *MITRE ATT&CK*. Steal or Forge Kerberos Tickets: Kerberoasting, T1558.003. — 2025. — URL: https://attack.mitre.org/techniques/T1558/003/.
3. *Снігур А., Гальчинський Л.* Виявлення персистентності загроз типу APT в системах WINDOWS / Collection of Scientific Papers «SCIENTIA». — 2024. — URL: https://previous.scientia.report/index.php/archive/article/view/2231.
4. *Microsoft Learn*. Service Principal Names. — 2024. — URL: https://learn.microsoft.com/en-us/windows/win32/ad/service-principal-names.
5. *SpecterOps*. BloodHound: Six Degrees of Domain Admin. — 2016. — URL: https://posts.specterops.io/bloodhound-six-degrees-of-domain-admin-4cceb45e9470.
6. *Microsoft Learn*. Kerberos Authentication Overview. — 2024. — URL: https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview.
7. *Ahmed M., Mahmood A. N., Hu J.* A survey of network anomaly detection techniques // Journal of Network and Computer Applications. — 2016. — Vol. 60. — P. 19–31. — DOI: 10.1016/j.jnca.2015.11.016.
8. *Melnyk A., Galchynsky L.* Active Directory Golden Ticket Attack Detection // International Research Journal of Engineering and Technology. — 2023. — Vol. 10. — P. 750–759.