ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління привілейованими користувачами на основі побудови рольової моделі з використанням рішення Teleport»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Тетяна ПАРФЕНЮК
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
ПАРФЕНЮК Тетяна
(прізвище, ім'я)

Керівник д.т.н. професор ГАЙДУР Галина
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ABSTRACT

Text part of the qualification work: 73 pages, 32 figures, 7 tables, 22 sources.

Object of research – privileged accounts.

Subject of research – the technology of privileged account management.

The aim of research – to develop recommendations for the use of privileged account management technology in organizations based on the implementation of the role-based access model (RBAC).

Research methods – studying the literature on this topic, analyzing technical documentation, international standards and Ukrainian laws.

Privileged Access Management (PAM) technology identifies users, processes, and technologies that require privileged access, and defines the policies that apply to them. The PAM solution should include capabilities to support the policies you implement (such as automated password management and multi-factor authentication), and administrators should be able to automate the creation, modification, and deletion of accounts. The PAM solution should also continuously monitor sessions so that you can identify and investigate anomalies based on the generated reports.

Privileged Access Management is mostly used in two cases: to prevent credential theft and to ensure compliance.

The paper analyzes the main approaches to privileged user management. The market leaders in PAM solutions were identified and analyzed, which allowed us to understand the main trends in this area and the benefits of using such systems to protect privileged accounts.

In practice, it was shown how Teleport can be used to create and effectively manage privileged accounts, using a role-based model to ensure the minimum required access rights. Integration processes with other security systems to strengthen access control were also discussed.

The system was tested and evaluated using the example of use cases in large organizations. The possibilities of scaling and ensuring high availability of the system were investigated, which makes it suitable for use in corporate environments with high security requirements.

The field of application is cybersecurity of information resources of an organization.

ORGANIZATION'S INFORMATION RESOURCES, PRIVILEGED USERS, PAM, RBAC, ROLE-BASED ACCESS MODEL

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасному світі інформаційної безпеки технології управління привілейованим доступом (Privileged Access Management, PAM) набувають особливого значення. Зростаюча кількість кібератак, орієнтованих на привілейовані облікові записи, підвищує необхідність ефективних інструментів для контролю доступу до критичних ресурсів.

Привілейовані облікові записи надають зловмисникам можливість виконувати дії з підвищеними правами, що може призвести до значних збитків для компаній та організацій. Актуальність теми полягає в необхідності забезпечення надійного управління такими обліковими записами, що дозволить мінімізувати ризики витоку даних та інших небезпечних наслідків.

Об'єкт дослідження – привілейовані облікові записи.

Предмет дослідження – технологія управління привілейованими обліковими записами.

Мета роботи – розробити рекомендації щодо використання технології управління привілейованими обліковими записами в організаціях на основі реалізації рольової моделі доступу (RBAC).

Наукові завдання:

- проаналізувати концепцію облікових записів із привілейованим доступом, їх основні види;
- проаналізувати основні загрози та вразливості, що пов'язані із привілейованим доступом
- визначити основні технології управління привілейованими обліковими записами;
- дослідити основні підходи до побудови рольової моделі доступу;
- розробити технологію управління привілейованим доступом на основі побудованої рольової моделі з використанням рішення Teleport;

- розробити рекомендації щодо використання технології управління привілейованими обліковими записами з використанням рішення Teleport.

Методи дослідження – для досягнення мети дослідження було використано такі методи: аналіз, синтез, порівняння, систематизація та узагальнення. Також було застосовано методи експертної оцінки та моделювання для оцінки ефективності впровадження PAM-рішень.

Практичне значення одержаних результатів – розроблені рекомендації щодо впровадження PAM-рішень можуть бути використані для покращення контролю над доступом до систем і ресурсів, що дозволить мінімізувати ризики витоку конфіденційної інформації, внутрішніх загроз та несанкціонованих дій з боку користувачів з привілейованими обліковими записами. Також, запропоновані підходи до побудови безпечної інфраструктури управління доступом можуть бути використані для оптимізації політик безпеки та зменшення залежності від людського фактору при управлінні привілейованими обліковими записами.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ І ТЕХНОЛОГІЙ УПРАВЛІННЯ НИМИ

1.1 Привілейовані облікові записи: концепція, види і ризики

Привілейований обліковий запис — це обліковий запис, який має підвищені права доступу порівняно зі стандартними обліковими записами користувачів. Ці облікові записи зазвичай використовуються для виконання адміністративних функцій, доступу до конфіденційних даних або контролю критично важливих IT-систем. Привілейовані облікові записи мають значну владу в системі, що робить їх основними цілями для зловмисників. Ефективне управління цими обліковими записами, включаючи контроль доступу, моніторинг використання та впровадження заходів безпеки, має вирішальне значення для забезпечення загальної безпеки IT-інфраструктури організації [1].

Привілейовані облікові записи відіграють важливу роль у забезпеченні функціонування IT-інфраструктури будь-якої організації. Вони зазвичай використовуються адміністраторами або іншими відповідальними особами для виконання завдань на високому рівні, таких як інсталяція або налаштування систем, управління користувачами, конфігурація мережевих пристроїв, а також надання доступу до критичних сервісів та даних. Ці облікові записи забезпечують можливості для:

- зміни системних конфігурацій;
- встановлення або видалення програмного забезпечення;
- створення та видалення облікових записів користувачів;
- доступу до конфіденційних даних або ресурсів.

Привілейований доступ проявляється в різних формах і контекстах в організації, кожен з яких має свої нюанси. Розуміння цих нюансів має вирішальне значення для впровадження ефективних стратегій управління привілейованим доступом (PAM). Нижче наведено основні типи привілейованого доступу:

1. Привілейований доступ на основі користувачів: Ця форма привілейованого доступу найчастіше асоціюється з ролями в організації. Наприклад, системний адміністратор або мережевий менеджер мають підвищені права доступу для виконання своїх посадових обов'язків. До цієї категорії також можуть належати керівники вищого рівня, яким потрібен доступ до конфіденційних бізнес-даних.

2. Системний привілейований доступ: У сучасних інфраструктурах привілейований доступ потрібен не лише людям. Автоматизовані системи, сервіси та додатки часто вимагають підвищених дозволів для виконання певних завдань. Наприклад, автоматизовані рішення для резервного копіювання потребують доступу практично до всіх файлів у системі, щоб створити резервну копію. Аналогічно, рішення для моніторингу мережі потребують широкого доступу до мережевого трафіку та конфігурацій для виконання своїх задач.

3. Тимчасовий або контекстний привілейований доступ: Привілейований доступ не завжди є постійним станом, а може бути тимчасовим. Наприклад, розробнику може знадобитися підвищений доступ до бази даних на короткий період для налагодження. Як тільки завдання буде виконано, привілеї будуть відкликані.

4. Привілейований доступ для третіх осіб: Зовнішні постачальники або партнери також можуть потребувати привілейованого доступу для надання послуг, таких як обслуговування або підтримка.

Цей тип доступу може бути більш ризикованим, оскільки організації мають менше контролю над діями третіх сторін.

5. Екстрений привілейований доступ: У певних виняткових ситуаціях, таких як кібератака або системний збій, окремим особам може бути наданий екстрений привілейований доступ для вирішення кризи. Такий доступ часто обмежений у часі, і його слід ретельно контролювати [1].

Виходячи із цього, привілейовані облікові записи є однією з найбільш привабливих цілей для зловмисників, оскільки їх компрометація надає можливість отримати доступ до критично важливих даних та систем.

Можна виділити основні типи атак, що націлені на привілейовані облікові записи та використовуються зловмисниками найчастіше: фішинг або підбор паролів. Всі вони можуть призвести до захоплення облікового запису та доступу до всіх його прав.

Неправильне або недоречне використання привілейованих облікових записів, навіть з боку довірених осіб, може призвести до несанкціонованих змін у системі або видалення важливої інформації.

Через високий рівень доступу, наданий привілейованим обліковим записам, відсутність адекватного моніторингу та аудиту їхньої діяльності може призвести до серйозних порушень безпеки.

Управління привілейованими обліковими записами є критично важливим завданням у сучасних організаціях, оскільки саме ці облікові записи є найбільш небезпечними з точки зору потенційного компрометації. Відповідні заходи, такі як використання спеціальних систем для управління привілейованими користувачами (PAM), багатофакторна автентифікація, аудит та моніторинг у реальному часі, допомагають мінімізувати ці ризики [2].

Згідно з ENISA Threat Landscape 2024 року, проблема *Improper Privilege Management* (CWE-269) є однією з найбільш актуальних у сфері кібербезпеки. Вона посідає 22-е місце у рейтингу MITRE TOP 25 CWEs за 2023 рік, піднявшись на 7 позицій у порівнянні з 2022 роком, що свідчить про її зростаючу загрозу.

Improper Privilege Management виникає, коли системи не забезпечують належного контролю прав доступу користувачів або процесів. Це може призвести до того, що користувачі отримують доступ до функцій або даних, на які вони не мають дозволу, що підвищує ризик несанкціонованих дій або зловживань. Така проблема стає особливо гострою в контексті привілейованих користувачів, оскільки компрометація цих облікових записів може мати критичні наслідки для безпеки всієї системи.

Зростання популярності цієї вразливості свідчить про те, що управління привілеями залишається критично важливою задачею для кібербезпеки

організацій. Правильне управління доступом та чітке розмежування привілеїв допомагають знизити ризики зловживань та витоків даних [3].

Соціальна інженерія (Social Engineering Threats) у даному звіті посідає важливе місце серед актуальних кіберзагроз, становлячи 6.06% всіх загроз (рисунок 1.1), представлених у звіті. Загрози соціальної інженерії мають безпосередній зв'язок з управлінням привілейованими користувачами, адже саме привілейовані облікові записи часто є основною ціллю таких атак.

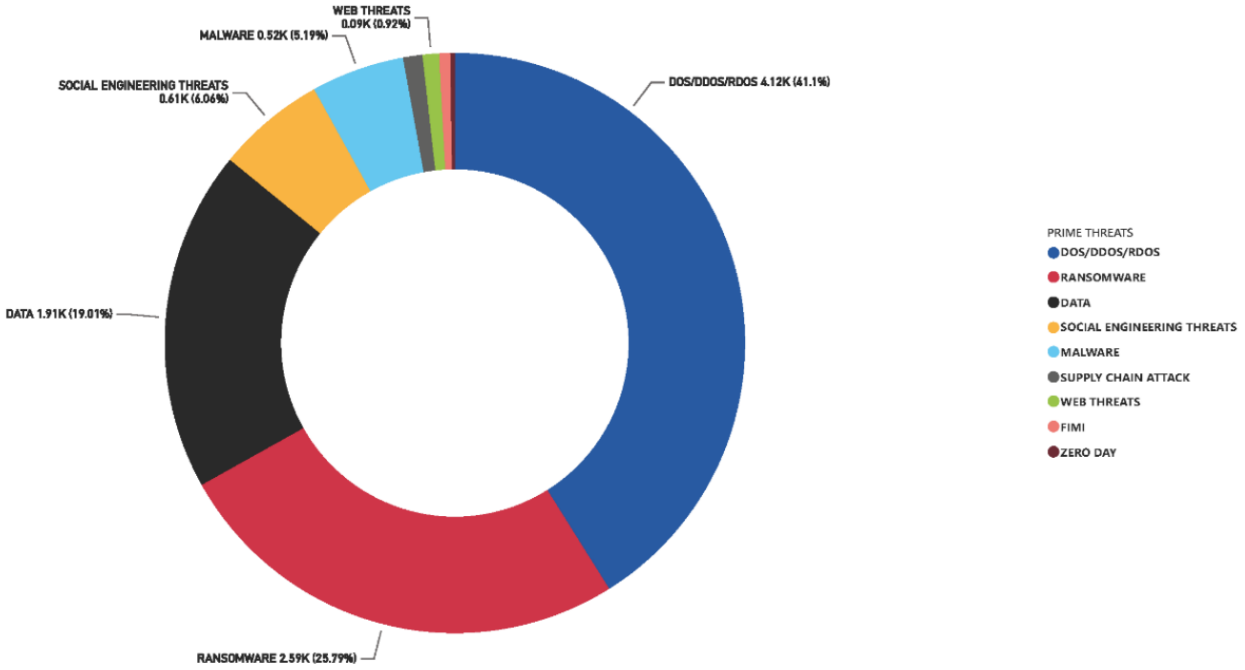


Рис. 1.1. ENISA Threat Landscape 2024

Соціальна інженерія полягає в маніпуляції людьми для отримання доступу до конфіденційної інформації або систем. Зловмисники можуть використовувати методи соціальної інженерії для обману адміністраторів або інших користувачів з високими привілеями, щоб отримати їхні облікові дані або іншу критично важливу інформацію. Це, в свою чергу, може призвести до компрометації привілейованих облікових записів і подальшого несанкціонованого доступу до корпоративних систем.

Також ця загроза становить один із основних ризиків, пов'язаних з управлінням привілейованими користувачами. Оскільки ці облікові записи мають розширені права доступу, компрометація навіть одного привілейованого облікового

запису через атаки соціальної інженерії може призвести до масштабних наслідків для організації, включаючи втрату конфіденційних даних, порушення операційних процесів і навіть повний контроль над інфраструктурою.

Згідно з 2024 Verizon Data Breach Investigations Report, внутрішні користувачі залишаються основною загрозою при зловживанні привілейованим доступом. Мотивація, як і раніше, здебільшого фінансова (88% випадків), а особисті дані є основною ціллю (83%). Крім того, зловмисники дедалі частіше викрадають внутрішню інформацію, зокрема інтелектуальну власність (46%). Зловживання доступом може включати фінансові злочини або промислове шпигунство [4].

Основні показники:

- Кількість інцидентів: 897
- Типи даних: особисті, внутрішні, банківські
- Мотиви: фінансова вигода, шпигунство

Згідно із цим же звітом, основні вектори атак, пов'язані з привілейованими акаунтами або системами: компрометація облікових даних (близько 90%), фішинг (близько 40%), експлуатація вразливостей (близько 20%).

Найбільша частка атак походить від злому облікових записів або викрадення паролів. Це підкреслює вразливість слабких або повторно використовуваних паролів, які зловмисники можуть використовувати для отримання доступу до систем із підвищеними привілеями.

Фішингові атаки є іншим поширеним методом, який використовують кіберзлочинці. Це техніка, при якій користувачів обманюють для отримання конфіденційних даних або встановлення шкідливого програмного забезпечення через шахрайські електронні листи чи повідомлення. Графік показує, що фішинг має значний вплив на порушення безпеки, проте менший порівняно з компрометацією облікових даних [4].

Метод експлуатації включає використання невиправлених вразливостей у програмному або апаратному забезпеченні для отримання несанкціонованого доступу до систем. Хоча цей метод менш поширений, ніж компрометація облікових

даних і фішинг (рисунок 1.2), він все одно відіграє важливу роль у підвищенні привілеїв зловмисниками або захопленні критичних систем [4].

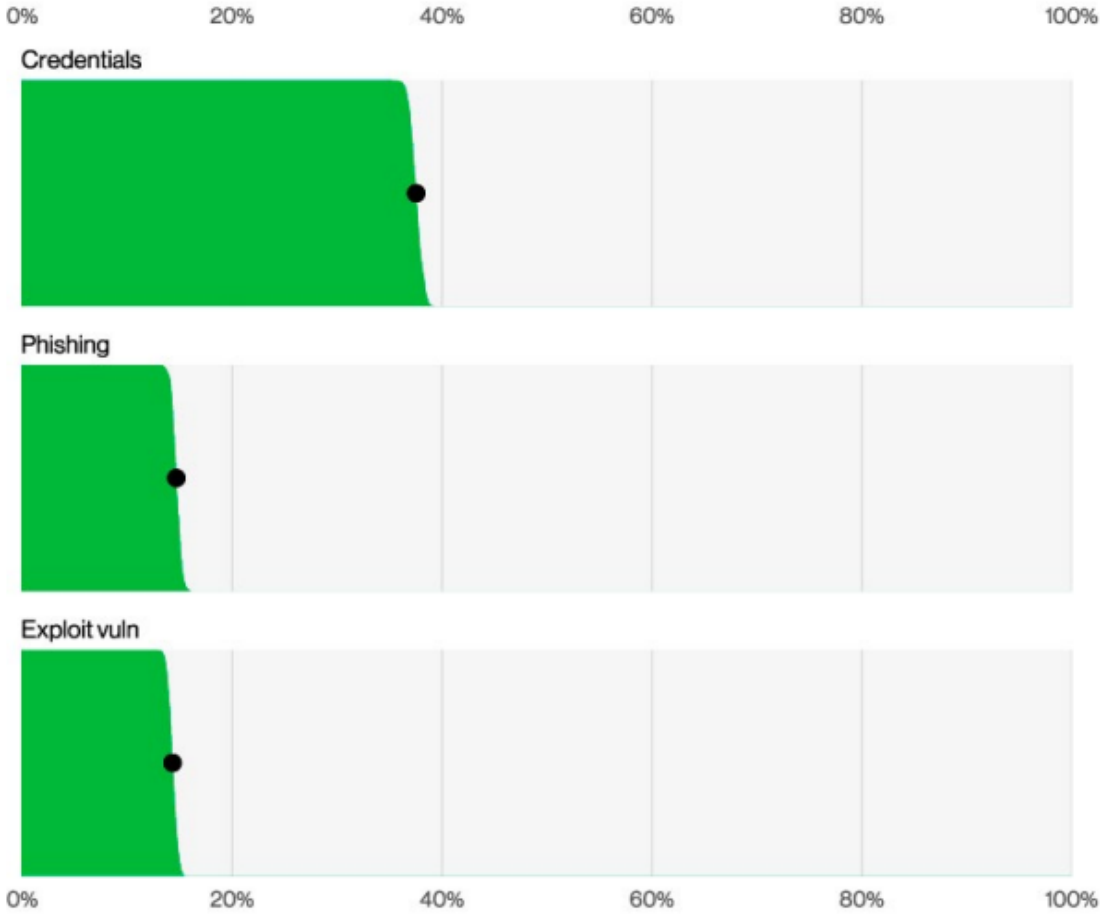


Рис. 1.2. ENISA Threat Landscape 2024

Якщо проаналізувати основні джерела загроза, то зовнішні загрози є найбільш значущою часткою за всі роки. З 2018 до 2022 року відбувається зростання їхньої активності до майже 80%, після чого показник поступово знижується в 2024 році.

Частка внутрішніх загроз знижується з приблизно 40% у 2018 році до приблизно 20% в 2022 році. Проте починаючи з 2022 року можна помітити тенденцію до зростання, і до 2024 року вона досягає більш ніж 30% (рисунок 1.3).

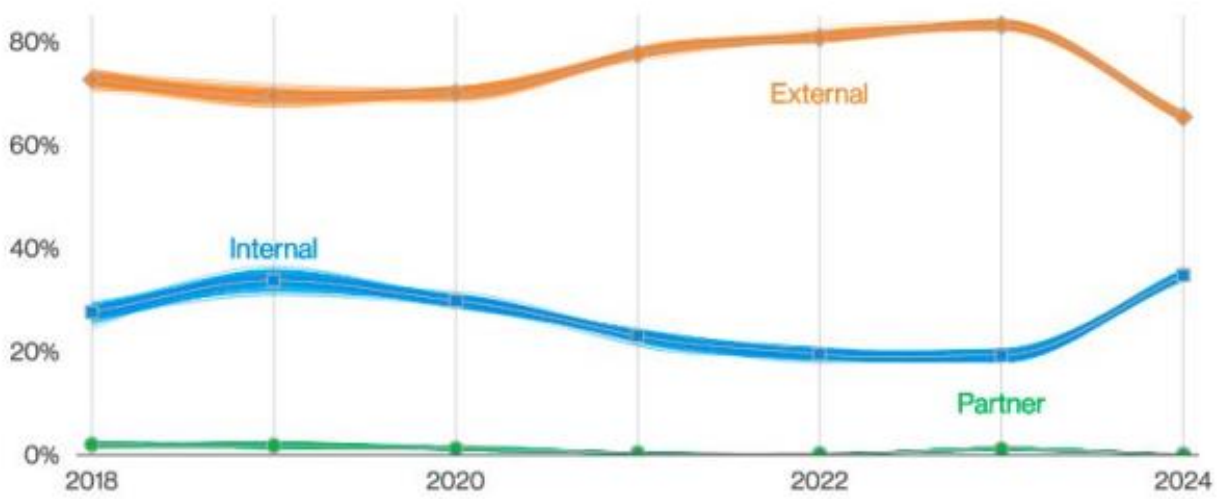


Рис. 1.3. ENISA Threat Landscape 2024

Це може свідчити про те, що організації приділяють більше уваги контролю за внутрішніми користувачами та зменшують ризики з їхнього боку.

Частка партнерських загроз залишається стабільно низькою, коливаючись в межах 1-2% протягом усього періоду. Це може свідчити про те, що загрози від партнерських організацій не є настільки суттєвими порівняно з іншими джерелами.

Загалом, основна загроза для організацій продовжує надходити від зовнішніх акторів, проте збільшується значення внутрішніх загроз, що може вимагати додаткових заходів для моніторингу та обмеження доступу співробітників.

Виходячи із цього, можна зробити висновок, що управління доступом і контроль над привілейованими обліковими записами є критично важливими для зменшення ризиків витоку даних. Внутрішні загрози, фінансово мотивовані співробітники та шпигунство продовжують бути значною загрозою для компаній. Впровадження належних політик доступу, таких як рольова модель з мінімальними привілеями та системи моніторингу, допомагає забезпечити не тільки безпеку, але й довгострокову стабільність та відповідність нормативним вимогам.

1.2 Загрози та вразливості, пов'язані з привілейованими користувачами

Привілейовані користувачі є однією із найнебезпечніших категорій у будь-якій інформаційній системі, оскільки їхні облікові записи мають розширені права

доступу до системних ресурсів та функцій. Це означає, що компрометація такого професійного запису може мати серйозні наслідки для безпеки, конфіденційності та стабільності IT-системи.

Зловживання привілеями (Privileged Abuse) — один із найбільш поширених ризиків виникає тому, що самі привілейовані користувачі можуть використовувати свої права доступу для виконання несанкціонованих дій. Це може бути як навмисне зловживання (наприклад, з міркувань фінансової вигоди), так і випадкові помилки, які можуть завдати шкоди системі або даним. Також цей ризик може бути досягнутий, якщо користувачі отримують доступ до даних або ресурсів, які не стосуються їх безпосередніх функціональних обов'язків.

До основних типів атак належать фішинг, підбір паролів, атаки за допомогою шкідливого ПЗ (Malware) та атаки з використанням вразливостей операційної системи або програмного забезпечення.

Наступним типом загроз є ескалація привілеїв (Privilege Escalation) — це техніка, яка дозволяє зловмисникам отримати привілейований доступ, починається з цифрового запису з низьким рівнем прав. Наприклад, зловмисник може використовувати вразливі системи для отримання доступу до облікових записів адміністратора або суперкористувача.

Інсайдерські загрози (Insider Threats) пов’язані із привілейованими користувачами, такими як системні адміністратори, оскільки вони мають великий доступ до критичних ресурсів. Інсайдерська загроза може виникнути у випадку, якщо ця особа вирішить використовувати свої привілеї для завдання шкоди організації, наприклад, шляхом викрадання даних, шантажу або видалення важливих ресурсів [5].

Існує низка вразливостей, що пов’язані із використанням привілейованих облікових записів. Основні загрози включають можливість несанкціонованого доступу до критично важливих ресурсів та інфраструктури, що може призвести до серйозних наслідків для інформаційної безпеки організації.

Однією з найбільш поширених вразливостей є експлуатація привілейованих облікових записів через модифікацію даних реєстру або системних налаштувань,

що дозволяє хакерам отримати доступ до критичних функцій операційної системи (OS). Зміна налаштувань реєстру є важливим методом отримання більших прав доступу, що ускладнює виявлення та реагування на атаки (наприклад, T1068: Exploitation for Privilege Escalation).

Крім того, зловмисники часто використовують встановлення додаткових програм**,** таких як шкідливе програмне забезпечення, для збирання даних або організації подальших атак. Це сприяє переміщенню по мережі для отримання доступу до більшої кількості систем та компрометації додаткових об'єктів. Важливими постексплуатаційними техніками є також захисних механізмів системи для приховування своїх дій (T1078: Valid Accounts), що ускладнює виявлення зловмисних дій (T1078.003: Domain Accounts) [5].

Серед інших методів атак — зміна конфігурацій системи/пристрою для підтримки стійкої присутності та забезпечення подальшої активації шкідливого ПЗ (T1548: Abuse Elevation Control Mechanism), а також видалення слідів активності з метою уникнення виявлення та перешкоджання розслідуванню інциденту (T1003: Credential Dumping). Це дозволяє зловмисникам приховати свою діяльність і зменшити ймовірність швидкого виявлення.

Ключовою метою багатьох зловмисників **є** отримання доступу до прав суперкористувача або адміністратора домен**у**, що надає повний контроль над всією IT-інфраструктурою компанії. Заволодіння цими привілеями може спричинити масштабні атаки на критично важливі ресурси, як показує зображення.

Таким чином, вразливості, пов'язані з привілейованими обліковими записами, можуть мати катастрофічні наслідки для організацій, якщо зловмисникам вдасться отримати доступ до критично важливих систем або зловживати адміністративними правами [5].

Згідно з MITRE ATT&CK ми можемо виділити основні техніки, пов'язані з неправильним розмежуванням привілеїв [6]:

Таблиця 1.1.

Техніки згідно з MITRE ATT&CK

Назва техніки	**Пояснення до техніки та тактики**
T1068: Ескалація привілеїв	Техніка, що передбачає використання вразливостей у програмному забезпеченні або операційних системах для підвищення привілеїв від звичайного користувача до адміністратора або суперкористувача. Зловмисники можуть отримати доступ до критичних ресурсів через використання вразливих компонентів.
T1078: Дійсні облікові записи	Техніка полягає у використанні дійсних, але скомпрометованих облікових записів для доступу до систем. Це дозволяє зловмисникам уникнути виявлення, оскільки вони використовують справжні дані доступу.
T1078.003: Облікові записи домену	Використання доменних облікових записів для отримання доступу до ресурсів в мережах організацій, що робить зловмисників важчими для виявлення.
T1548: Зловживання механізмами підвищення привілеїв	T1548.001: Setuid і Setgid — використання інструментів Setuid і Setgid для отримання прав привілейованого користувача. T1548.002: Обхід UAC — обхід механізму для підвищення привілеїв. T1548.003: Зловживання sudo — використання кешованих сесій sudo для отримання привілейованого доступу.
T1134: Маніпуляція токенами	Техніка полягає у використанні токенів доступу, щоб виконувати дії від імені привілейованих користувачів, тим самим збільшуючи свої права.

Назва техніки	**Пояснення до техніки та тактики**
T1550: Використання альтернативних методів автентифікації	Використання таких методів, як хеші паролів або токени Kerberos, дозволяє отримувати привілейований доступ до систем без необхідності знати фактичний пароль. Підтехніки: T1550.001: Pass the Hash — використання хешів замість фактичного пароля. T1550.003: Pass the Ticket — використання квитків Kerberos для автентифікації.
T1021: Віддалені сервіси	Використання віддалених сервісів для доступу до мереж. Підтехніки включають: T1021.001: RDP (Протокол віддаленого робочого столу). T1021.002: Спільні ресурси адміністратора (SMB/Windows). T1021.003: DCOM (Модель розподілених об'єктів).
T1098: Маніпуляція обліковими записами	Ця техніка передбачає маніпуляцію обліковими записами для отримання доступу до системи або зміни конфігурацій.
T1003: Вивантаження облікових даних	Отримання облікових даних з системи для подальшого використання їх у атаках. Підтехніки включають: T1003.001: Пам'ять LSASS. T1003.002: Менеджер облікових записів безпеки (SAM). T1003.003: NTDS (Active Directory)

Назва техніки	Пояснення до техніки та тактики
T1212: Експлуатація довірених відносин	Використання довірених взаємовідносин між системами для атаки на менш захищені компоненти.
T1108: Резервний доступ	Створення бекдорів або додаткових облікових записів для підтримки доступу після виявлення основних шляхів атаки.
T1075: Передача хешу	Використання хешу пароля замість фактичного пароля для отримання доступу до систем.
T1055: Ін'єкція у процеси	Впровадження шкідливого коду у привілейовані процеси, що дозволяє отримати доступ до критичних ресурсів.
T1106: Нативний API	Використання системних API для маніпуляції функціями системи або підвищення привілеїв.

1.3. Моделі управління доступом: теоретичні основи

Управління доступом — це процес, що визначає та контролює, хто має доступ до ресурсів системи, на яких умовах і до яких саме ресурсів. Правильне управління доступом є критично важливим для захисту даних, ресурсів і операцій у будь-якій організації. Основними елементами управління доступом є ідентифікація користувача, автентифікація, авторизація та аудит. Важливо також розуміти різні моделі управління доступом , які застосовуються для забезпечення безпеки в сучасних інформаційних системах [7].

Основні моделі управління доступом

1. Discretionary Access Control (DAC) — Дискреційне управління доступом. У моделі DAC власник ресурсу має право вирішувати, хто може отримати доступ до ресурсу і з якими правами. Користувачі можуть делегувати доступ іншим користувачам або групам. Основна ідея моделі базується на тому, що контроль доступу здійснюється на основі дискреційних рішень власника даних або ресурсу.

Цей підхід підтримує принцип найменших привілеїв, концепцію, яка виступає за надання користувачам найменшого обсягу доступу, необхідного для виконання їхньої роботи. Оскільки DAC покладається на прийняття рішень людиною для надання доступу, інформаційна система або власник даних повинні бути суворими у своїх перевірках запитів на доступ, щоб гарантувати, що не будуть надані надмірно дозвільні права.

На найбільш фундаментальному рівні DAC використовує списки контролю доступу (ACL) для призначення дозволів на ресурси. Списки керування доступом (ACL) містять або користувачів, або попередньо визначені групи користувачів та відповідні їм рівні доступу. Ці рівні зазвичай включають доступ до читання, запису та виконання, що дозволяє людині переглядати, змінювати або запускати процес чи програму відповідно.

Переваги цієї моделі: Гнучкість, можливість налаштування доступу до рішень користувача.

Недоліки: Високий ризик ненавмисного надання доступу, недостатня захищеність від внутрішніх загроз (інсайдерів).

Приклад впроваження моделі:

•Хтось створює ресурс, наприклад файл або папку, а автор тепер є власником, який може керувати дозволами на доступ.

•Потім власник налаштовує ACL для новоствореного ресурсу, призначаючи користувачів і групи, які повинні мати доступ з необхідними дозволами.

•Один або кілька користувачів, яким було надано дозвіл на ресурс, намагаються отримати доступ до нього, що призводить до запиту на доступ до системи DAC.

•Система DAC перевіряє, чи збігається інформація про користувача в запиті з ACL, а потім схвалює або відхиляє запит залежно від того, чи знаходить вона ACL.

Система DAC забезпечує виконання свого рішення в режимі реального часу, дозволяючи користувачеві переглядати, змінювати або запускати запитуваний ресурс до тих пір, поки відповідний ACL дозволяє цю дію [8].

2. Mandatory Access Control (MAC) — Мандатне управління доступом

Права доступу зазвичай надаються системним адміністратором і призначаються кимось в компанії, хто володіє достатніми знаннями про завдання кожного користувача. Це гарантує, що співробітники можуть виконувати свою роботу, не вдаряючись об стіни. Впровадження та оновлення зазвичай виконуються автоматично операційною системою або ядром безпеки. Коли користувач намагається отримати доступ до даних, система або надає йому доступ, або відхиляє запит. Таке автоматизоване впровадження є найкращим способом запобігання несанкціонованому втручанню.

Рішення про права доступу зазвичай приймаються на підставі наступних факторів:

- Користувачі та процеси
- Об'єкти: ресурси, до яких здійснюється звернення
- Правила та властивості: категоризації, мітки та кодові слова

Обов'язковий контроль доступу використовує **ієрархічний підхід**: кожному об'єкту у файловій системі призначається рівень безпеки на основі конфіденційності даних. Приклади рівнів безпеки: "конфіденційно" та "цілком таємно".

Користувачі та пристрої ранжуються таким же чином. Коли користувач намагається отримати доступ до ресурсу, система автоматично перевіряє, чи дозволено йому доступ.

Крім того, всім користувачам та інформації присвоюється **категорія**, яка також перевіряється при запиті доступу користувачем. Користувачі повинні відповідати обом критеріям – рівню безпеки та категорії – щоб отримати доступ до даних [9].

Переваги цієї моделі: Високий рівень безпеки, чітке дотримання політики безпеки, захист від інсайдерів.

Недоліки : Висока складність налаштування, відсутність гнучкості.

3. Role-Based Access Control (RBAC) — рольова модель управління доступом.

У системі RBAC адміністратор призначає кожному окремому користувачу одну або кілька ролей. Кожна нова роль представляє набір дозволів або привілеїв для користувача.

RBAC усуває необхідність надавати кожному окремому користувачеві індивідуальний набір дозволів користувача. Натомість, визначені ролі RBAC визначають права доступу. Цей процес полегшує організаціям адаптацію або виключення співробітників, оновлення робочих функцій і трансформацію бізнес-операцій [10].

Кожна роль вибирає набір дозволених дій у межах системи. Користувач отримує доступ до ресурсів лише через призначені йому ролі.

Переваги цієї моделі: Легкість адміністрування, чіткий розподіл прав доступу, централізоване управління.

Недоліки моделі: Складність управління великою кількістю ролей, необхідність регулярного перегляду ролей для актуалізації.

Приклад реалізації моделі: Роль фінансиста може дозволяти користувачу робити покупки, запускати програмне забезпечення для прогнозування або надавати доступ до систем ланцюга постачання. Роль відділу кадрів може дозволити користувачу переглядати кадрові файли та керувати системами виплат працівникам. Attribute-Based Access Control (ABAC) — Управління доступом на основі атрибутів

4. Attribute-Based Access Control (ABAC) — контроль доступу на основі атрибутів.

У моделі ABAC доступ додатково на основі атрибутів користувача, об'єкта та середовища. Атрибути можуть включати ідентифікатори (ім'я, посада), характеристики об'єкта (тип даних), а також контекстні дані (час доступу, сайт тощо).

Можна виділити основні групи атрибутів:

- Атрибути користувача: ідентифікатор користувача, типологія (наприклад, управління, підпорядкування), департамент, рівень допуску.

•Атрибути ресурсу: тип ресурсу (наприклад, тип документа, тип бази даних), власник ресурсу, класифікація (наприклад, класифікована, відкрита), дата створення, класифікація даних.

•Атрибути середовища: час доби, дата, географічне розташування дій, які виконуються або можуть виконуватися, наприклад IP-адреса пристрою, географічне розташування пристрою тощо, тип пристрою, поточний стан захисту мережі (наприклад – VPN, брандмауер).

Дозволи на доступ надаються залежно від значення цих атрибутів і встановлених політик.

Переваги моделі: Дуже висока гнучкість і можливість налаштування політики для конкретних ситуацій.

Недоліки моделі: Висока складність реалізації та управління великою кількістю атрибутів.

Приклад реалізації даної моделі:

• **Ініціація запиту:** суб'єкт починає запит на доступ до ресурсу у своєму середовищі.

• **Колекція атрибутів: PEP** набуває необхідних характеристик від PIP.

• **Отримання правил:** такі органи, як PDP, фактично звертатимуться до Репозиторію політик і витягуватимуть відповідні політики.

• **Оцінка політики:** запит потім перевіряється на відповідність політикам за допомогою атрибутів.

• **Прийняття рішень:** В результаті виконання рішення про контроль доступу, ПДП приймає рішення про дозвіл (дозволити або відхилити).

• **Правозастосування:** PEP виконує рішення та затверджує або відмовляє у правах доступу до ресурсу [11].

Таблиця 1.2.

Порівняння моделей управління доступом

Модель	**Гнучкість**	**Безпека**	**Легкість адміністрування**	**Застосування**

Дискреційний контроль доступу (DAC)	Висока	Середня	Складна	Персональні комп'ютери, файлові системи
Обов'язковий контроль доступу (MAC)	Низька	Висока	Складна	Військові та урядові установи
Контроль доступу на основі ролей (RBAC)	Середня	Висока	Легка	Корпоративні системи
Контроль доступу на основі атрибутів (ABAC)	Висока	Висока	Складна	Хмарні послуги, великі організації

1.4 Огляд сучасних технологій і рішень для управління привілейованими користувачами

Управління привілейованими користувачами (Privileged Access Management, PAM) є одним із ключових елементів забезпечення інформаційної безпеки. Привілейовані облікові записи мають доступ до критично важливих систем і даних, тому їхня безпека є пріоритетною для будь-якої організації. Сучасні технології PAM спрямовані на управління, моніторинг та контроль доступу привілейованих користувачів, що знижує ризик зловживань і компрометації таких облікових записів.

Згідно зі звітом Gartner за липень 2022 року (рисунок 1.4), лідерами на світовому ринку рішень для управління привілейованим доступом (Privileged Access Management, PAM) є наступні компанії:

1. **CyberArk** – Визнаний глобальним лідером у галузі PAM, відомий своїми потужними рішеннями для захисту привілейованих облікових записів та даних.
2. **One Identity** – Пропонує ефективні рішення для централізованого управління привілейованими обліковими записами, які добре підходять для великих корпоративних середовищ.
3. **Delinea (колишній Thycotic Centrify)** – Компанія забезпечує високий рівень безпеки та управління доступом, зокрема за допомогою інтегрованих інструментів для управління доступом до систем і додатків.
4. **ARCON** – Займає сильну позицію на ринку завдяки своїм рішенням для моніторингу привілейованих доступів та управління ними.
5. **BeyondTrust** – Широко відомий своєю здатністю надавати комплексні рішення для управління доступом і захисту привілейованих облікових записів.
6. **WALLIX** – Спеціалізується на забезпеченні простих у використанні інструментів для управління привілейованими доступами та контролю дій користувачів.

Ці компанії мають найвищі показники за двома основними критеріями Gartner: **"повнота бачення"** та **"здатність до виконання"**, що дозволяє їм утримувати провідні позиції на ринку рішень для управління привілейованим доступом [12].

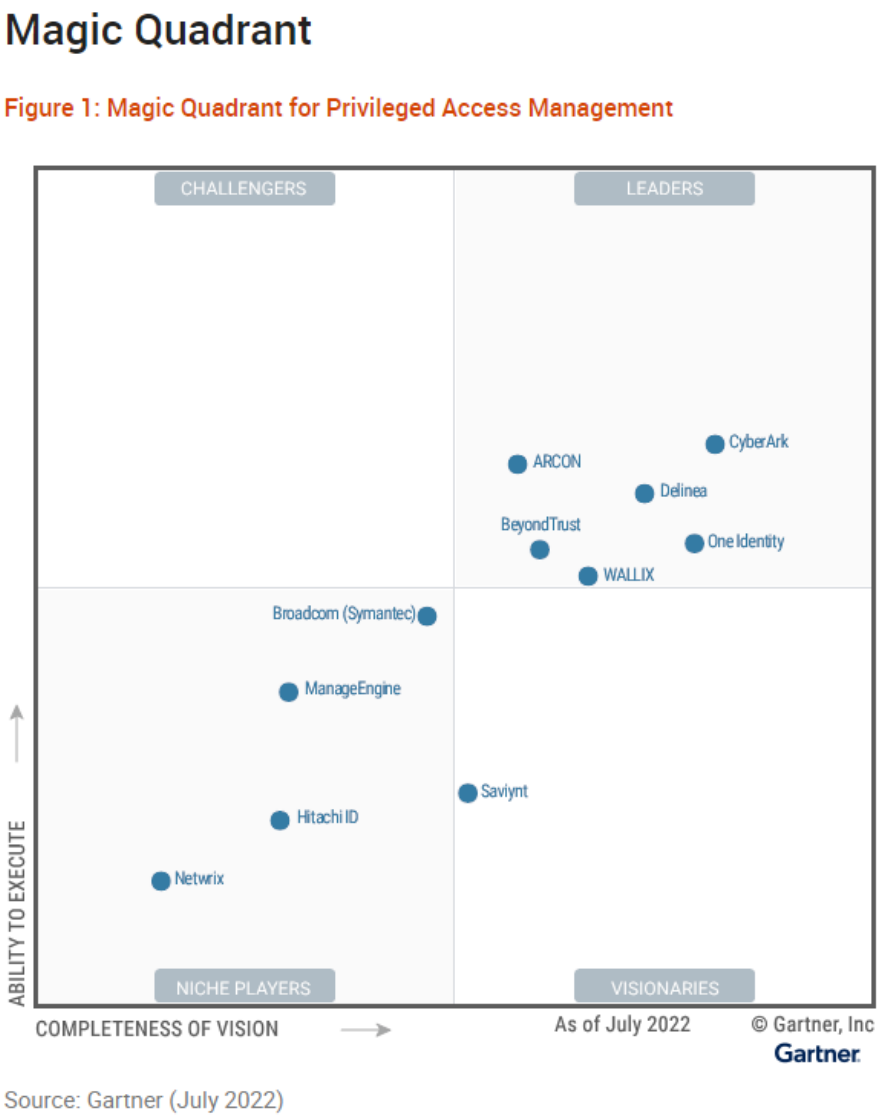


Рис 1.4. — Gartner Magic Quadrant 2022

Також відповідно до каталогу на платформі Дія Бізнес (рисунок 1.5) можна додати до цього переліку рішення Teleport, яке забезпечує високий рівень контролю та моніторингу доступу привілейованих користувачів. Teleport дозволяє керувати доступом через інтеграцію з SSO (Single Sign-On) провайдерами, багатофакторною автентифікацією (MFA) та іншими методами безпеки, що відповідають вимогам для сучасних PAM-рішень [13].

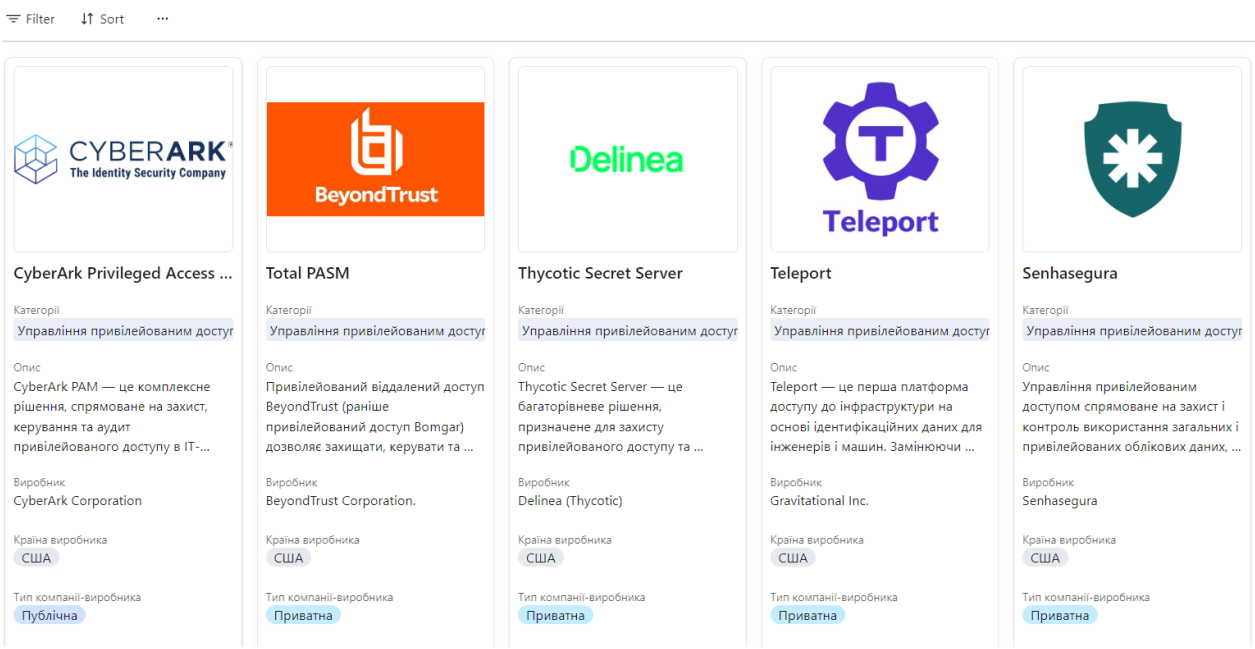


Рис. 1.5. — Платформа Дія Бізнес

Окрім Privileged Access Management (PAM), існують інші технології та рішення для забезпечення кібербезпеки та управління доступом у сучасних організаціях.

Identity and Access Management (IAM) — це ширша концепція, яка охоплює управління ідентифікацією користувачів і доступом до ресурсів організації. Основне завдання IAM — це гарантувати, що правильні люди мають доступ до відповідних ресурсів у потрібний час.

До функцій можна віднести управління користувачами та їхніми обліковими даними, автентифікація і авторизація користувачів, підтримка єдиного входу (SSO).

Технологія єдиного входу (SSO) дозволяє користувачам входити в кілька систем або додатків, використовуючи один набір облікових даних (наприклад, логін та пароль).

Серед функцій: єдиний доступ до декількох систем без повторної автентифікації, централізоване управління ідентифікацією користувачів.

Багатофакторна автентифікація (MFA) підвищує рівень безпеки доступу, вимагаючи від користувача підтвердження своєї ідентичності за допомогою двох або більше факторів: пароля, мобільного пристрою або біометричних даних.

Функціями є використання кількох методів автентифікації (паролі, смс-коди, біометрія), підвищення безпеки доступу до ресурсів.

Концепція Zero Trust означає, що кожна спроба доступу до ресурсу повинна бути перевірена незалежно від того, чи відбувається вона з внутрішньої мережі або ззовні. Це підхід, який передбачає нульову довіру до користувачів або пристроїв, доки не буде підтверджена їхня автентичність.

Цей підхід забезпечує постійну перевірку кожного запиту на доступ а також захист даних і ресурсів на основі контекстної інформації.

Висновки до першого розділу

У даному розділі роботи було розглянуто основні аспекти управління привілейованими користувачами, а також загрози та вразливості, пов'язані з ними. Було визначено, що привілейовані користувачі є ключовими фігурами в будь-якій організації, оскільки їхні облікові записи мають доступ до критично важливих систем і даних. Ефективне управління цими обліковими записами є необхідним для забезпечення безпеки IT-інфраструктури.

Основними загрозами є компрометація облікових даних через фішинг, підбір паролів, ескалацію привілеїв або використання вразливостей. Це може призвести до значних втрат для організацій, включаючи витік конфіденційної інформації та зупинку бізнес-процесів.

Також були розглянути основні моделі управління доступом, зокрема дискреційний контроль доступу (DAC), обов'язковий контроль доступу (MAC), рольове управління доступом (RBAC) та управління доступом на основі атрибутів (ABAC). Кожна з моделей має свої переваги та недоліки в контексті застосування до управління привілейованими обліковими записами.

Отже, ефективне управління привілейованими користувачами є критично важливим завданням для будь-якої організації. Використання сучасних рішень PAM та впровадження моделей контролю доступу, таких як RBAC, значно знижують ризики, пов'язані з несанкціонованим доступом та зловживанням привілеями.

2 ПЛАТФОРМА TELEPORT ЯК РІШЕННЯ ДЛЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМИ КОРИСТУВАЧАМИ

2.1 Огляд рішення Teleport: архітектура і основні можливості

Teleport — це рішення для управління доступом до інфраструктури, що включають сервери, бази даних, кластери Kubernetes, а також віддалені робочі столи з операційною системою Windows. Teleport забезпечує управління привілейованими користувачами через централізоване управління доступом та контроль активності користувачів. Ця система забезпечує високу безпеку доступу, мінімізуючи ризики, пов'язані з несанкціонованим доступом, а також спрощує процеси автентифікації та авторизації через інтеграцію з Single Sign-On (SSO) та іншими системами управління обліковими записами [14].

Архітектура рішення Teleport побудована на основі протоколів SSH та TLS, що гарантує захищеність даних та інтегровані механізми контролю доступу. Основні компоненти Teleport включають Teleport Proxy Service, Teleport Auth Service, Teleport Node, Teleport Web UI (рисунок 2.1).

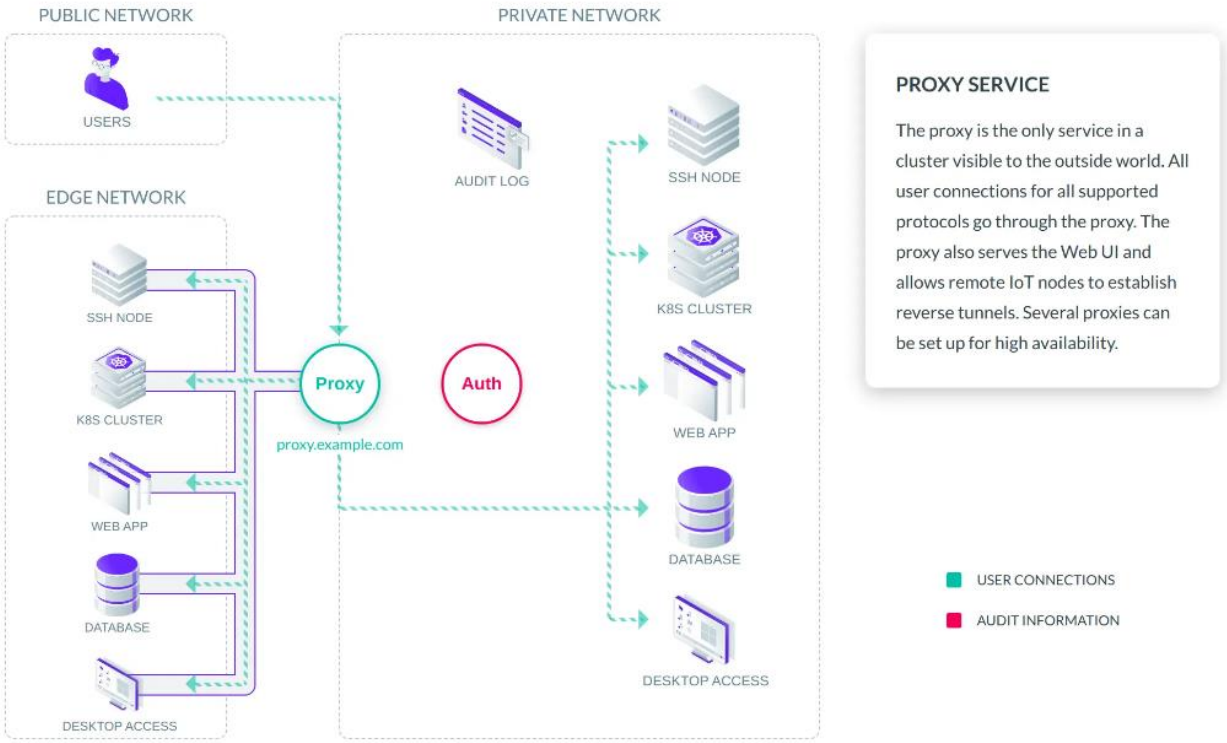


Рис. 2.1. — Архітектура Teleport

Teleport Proxy Service забезпечує інтерфейс для користувачів і виконує функцію шлюзу між клієнтами та захищеними ресурсами. Він дозволяє користувачам аутентифікуватися через єдину точку доступу за допомогою SSO або локальних облікових даних, що забезпечує централізовану автентифікацію для доступу до SSH-серверів, Windows-робочих столів та інших ресурсів.

Proxy Service підтримує роботу з різними протоколами, включаючи SSH, Kubernetes, HTTPS та бази даних, перехоплюючи трафік і забезпечуючи, що лише аутентифіковані користувачі можуть з'єднуватися з цільовими ресурсами [14].

Teleport Auth Service модуль відповідає за автентифікацію та авторизацію користувачів. Він також керує політиками доступу на основі RBAC (Role-Based Access Control) та підтримує інтеграцію з SSO-сервісами для забезпечення єдиного входу в систему.

Teleport Auth Service також зберігає журнали подій і записи активності користувачів, надаючи детальний аудит дій у системі для забезпечення відповідності вимогам безпеки.

Teleport Nodes – це вузли, що об'єднуються в кластери. Вони представляють собою ресурси, до яких надається доступ через Teleport (сервери, бази даних, Kubernetes-кластери). Кожен вузол підключається до Auth Service і реєструється для централізованого управління доступом.

Teleport Web UI – модуль забезпечує інтерфейс для адміністраторів і користувачів, дозволяючи виконувати віддалене управління інфраструктурою (рисунок 2.2). Усі операції через Web UI захищені за допомогою TLS-шифрування, що гарантує безпечне з'єднання і захист даних від перехоплення та модифікації в процесі передачі [15].

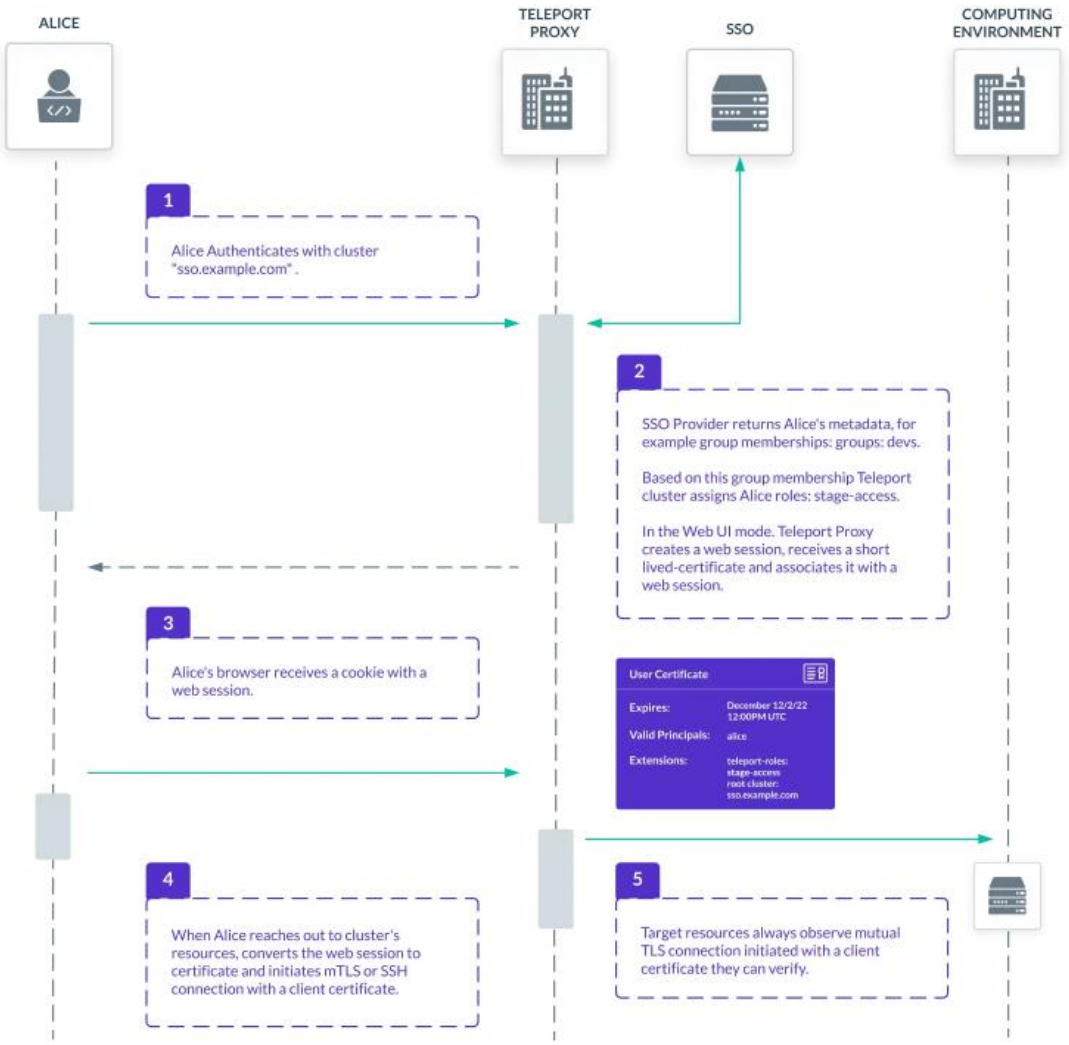


Рис. 2.2. — Архітектура WebUI

Teleport надає низку функцій, що забезпечують безпечний доступ до ресурсів організацій та спрощують управління інфраструктурою:

1. Централізоване управління доступом — Teleport дозволяє централізовано керувати доступом до різноманітних ресурсів, таких як сервери, бази даних та кластери Kubernetes. Завдяки цьому адміністратори мають можливість контролювати доступ до всіх ресурсів з одного місця, що значно підвищує ефективність управління привілеями.

2. Реалізація Role-Based Access Control (RBAC) — Teleport підтримує рольове управління доступом, що дозволяє адміністраторам створювати чіткі правила доступу на основі ролей користувачів. Це забезпечує надійний механізм контролю за привілеями і мінімізує ризики зловживань привілейованими правами.

3. Інтеграція з системами Single Sign-On (SSO) — Teleport забезпечує інтеграцію з SSO-системами, такими як Okta, Google SSO або Azure AD, що значно спрощує процес автентифікації для користувачів і дозволяє впроваджувати багатофакторну автентифікацію (MFA), підвищуючи рівень безпеки.

4. Підтримка мультипротокольних з'єднань — окрім SSH і Kubernetes, Teleport підтримує роботу з базами даних та іншими протоколами, дозволяючи адміністратору інтегрувати всі ресурси організації в одну систему доступу і контролювати доступ через єдиний портал.

5. Запис сесій та аудит — всі сесії користувачів записуються, що дозволяє адміністраторам переглядати і аналізувати дії користувачів у разі підозрілої активності або потенційних інцидентів. Журнали та записи дій зберігаються на Auth Service, що дозволяє зберігати їх у централізованій базі для аудиту.

6. Підтримка багатофакторної автентифікації (MFA) — для забезпечення додаткового рівня безпеки Teleport дозволяє налаштовувати багатофакторну автентифікацію на етапі підключення до критичних активів, що значно знижує ймовірність компрометації облікових записів привілейованих користувачів. Також багатофакторна автентифікація вимагається

7. TLS Routing — всі протоколи можуть бути зведені до одного порту для комунікацій, що спрощує налаштування мережі та забезпечує безпечну маршрутизацію трафіку.

8. Підтримка режиму Identity-Aware Proxy (IAP) — У режимі IAP приватні ключі ніколи не залишають клієнтський пристрій, що значно підвищує рівень безпеки. Всі з'єднання між клієнтом і ресурсами є взаємно автентифікованими, зменшуючи ризики, пов'язані з веб-атаками, такими як CSRF або викрадення файлів cookie.

9. Захист через тунелювання — Для ресурсів, розташованих за межами фаєрволу, Teleport використовує механізм зворотних тунелів, що дозволяє безпечно підключатися до серверів або кластерів Kubernetes через проксі-сервери без необхідності відкривати порти на зовнішній стороні мережі [15].

2.2 Порівняння Teleport з іншими рішеннями класу PAM (Privileged Access Management)

Системи управління привілейованими доступами (PAM) відіграють важливу роль у забезпеченні безпеки корпоративних мереж, надаючи можливість централізованого контролю доступу до критично важливих систем. Teleport, як сучасне рішення для управління доступом, конкурує з іншими відомими PAM-рішеннями, такими як Thycotic Secret Server. Порівняння цих рішень дозволяє краще зрозуміти, в чому полягають їх ключові відмінності та переваги.

Таблиця 2.1.

Порівняльна таблиця рішень Teleport та Thycotic

Характеристика	**Teleport**	**Thycotic Secret Server**
Тип доступу	Підтримка SSH, Kubernetes, баз даних, Windows, Applications	Підтримка RDP, SSH
Архітектура	Розподілена, підтримує роботу за фаєрволами	Локальна та хмарна інфраструктура
SSO інтеграція	Підтримка інтеграції з SSO (Okta, Azure AD)	Підтримка інтеграції з SSO
Управління доступом	Рольове управління доступом (RBAC)	Контроль доступу через політики
Аудит та моніторинг	Запис сесій та детальний аудит, що включає всі деталі події та команди, що були введені	Моніторинг сесій в реальному часі
Безпека	Підтримка TLS шифрування, IAP режим	Мультифакторна автентифікація (MFA), контроль паролів
Масштабованість	Легка масштабованість для великих інфраструктур	Масштабоване рішення для різних середовищ,

		проте складне в адмініструванні
Характеристика	**Teleport**	**Thycotic Secret Server**
Автоматизація	Автоматичне створення та відкликання доступу, можливо створювати політики, що надаватимуть тимчасовий доступ до систем	Автоматизована зміна паролів
Специфічні можливості	Підтримка зворотних тунелів для доступу до ресурсів за фаєрволами	Вбудовані шаблони для керування секретами
Інтеграція з іншими системами	Інтеграція з Kubernetes, базами даних та іншими ресурсами напряму. А також інтеграція з системами управління проектами.	Інтеграція з іншими системами через API

Teleport вигідно відрізняється своєю підтримкою різних протоколів і розширеною інтеграцією з сучасними хмарними сервісами та кластерами Kubernetes. Це робить його більш підходящим для компаній, що мають складні динамічні інфраструктури з високим рівнем автоматизації.

2.3 Переваги використання Teleport для управління доступом і безпекою

Teleport надає низку важливих переваг для управління доступом до інфраструктур та забезпечення безпеки у сучасних корпоративних середовищах. Це рішення створено для того, щоб спростити процеси автентифікації, авторизації та моніторингу, водночас знижуючи ризики компрометації доступу.

Teleport дозволяє централізовано керувати доступом до різних типів ресурсів, включаючи SSH-сервери, бази даних, кластеризовані інфраструктури Kubernetes та

віддалені робочі столи Windows. Це забезпечує єдиний портал для доступу, що значно спрощує управління інфраструктурою та зменшує кількість точок входу, що можуть бути атаковані [16].

У Teleport реалізовано механізм SSO (Single Sign-On), який забезпечує автентифікацію користувачів через сторонніх провайдерів (Azure AD, Google Workspace, Okta). Після входу користувач отримує короткостроковий сертифікат, який дозволяє доступ до ресурсів (SSH, Kubernetes, баз даних) без створення постійного облікового запису. Сертифікат діє обмежений час, що знижує ризики і підвищує безпеку. Ця схема також підтримує інтеграцію з декількома SSO-провайдерами, що робить систему більш гнучкою та стійкою до відмови одного з них. Teleport підтримує роботу із наступними SSO провайдерами: Azure Active Directory (AD), Windows Active Directory (ADFS), Google Workspace, GitHub, GitLab, OneLogin, OIDC, Okta.

Короткострокові сертифікати видаються користувачам після автентифікації через SSO-провайдер. Ці сертифікати діють протягом обмеженого – 1 годину і надають тимчасовий доступ до ресурсів, таких як SSH, Kubernetes, бази даних або десктопи. Сертифікати використовують X.509 для шифрування та автентифікації. Після закінчення часу дії сертифікат автоматично анулюється, що знижує ризик несанкціонованого доступу та підвищує безпеку системи.

У контексті використання двофакторної автентифікації (MFA), Teleport надає високий рівень безпеки під час доступу до критичних ресурсів організації. Система підтримує додаткову перевірку MFA для виконання адміністративних дій, таких як скидання облікових записів, внесення змін до конфігурації кластера, проведення оновлень, додавання нових користувачі, генерація токенів приєднання, тощо. MFA також можна налаштувати для кожної нової сесії — SSH, Kubernetes, баз даних або веб-додатків.

Окрім цього, Teleport легко масштабується для великих і розподілених інфраструктур, оскільки підтримує роботу через зворотні тунелі та забезпечує безпечне з'єднання навіть для серверів, що знаходяться за фаєрволами. Це робить

його підходящим для компаній, які мають складні хмарні або гібридні середовища [16].

Для великих організацій, побудова високо доступних кластерів вимагає ретельного підходу з використанням розподілених ресурсів і зон доступу. Основою є балансування навантаження на рівні 4 між кількома екземплярами Auth і Proxy Services, що працюють через різні центри обробки даних або хмарні зони. Інфраструктура повинна включати окреме сховище для стану кластера та запису сеансів, як-от DynamoDB або S3. Для забезпечення стійкості використовують механізми автоматичного масштабування та динамічної маршрутизації через DNS та TLS.

Балансування навантаження в кластері Teleport забезпечується через використання балансувальників навантаження рівня 4. Вони спрямовують трафік між кількома екземплярами Auth і Proxy Service, забезпечуючи безперервність роботи при високих навантаженнях. Балансувальник навантаження Proxy Service отримує трафік від користувачів та служб і передає його до доступного екземпляра Proxy. Далі трафік через балансувальник навантаження Auth Service спрямовується до Auth Service для автентифікації та управління доступом. Це дозволяє рівномірно розподіляти навантаження та забезпечує відмовостійкість системи.

Teleport має функціонал для реалізації концепції Zero Trust, згідно з якою кожен запит на доступ до ресурсів має бути перевірений і підтверджений, незалежно від того, де знаходиться користувач (внутрішня чи зовнішня мережа). Це забезпечує максимальний рівень безпеки та зменшує ризик внутрішніх і зовнішніх атак.

Плагін Teleport Jira синхронізує дошку проекту Jira із запитами на доступ, що обробляються кластером Teleport. Коли змінюється статус запиту на доступ всередині Teleport, плагін оновлює дошку. А коли оновлюється статус Запиту на доступ на дошці, плагін повідомляє про це веб-хук Jira, який запускається плагіном і змінює Запит на доступ в Teleport [16].

Teleport дозволяє записувати всі сесії користувачів, надаючи можливість перегляду команд та дій користувачів у реальному часі. Це підвищує прозорість та

дозволяє адміністраторам швидко виявляти потенційні загрози або несанкціоновану активність. Усі записи зберігаються в аудиті, що може бути використано для подальшого аналізу та відповідності вимогам безпеки.

Всі з'єднання через Teleport захищені за допомогою TLS-шифрування, що забезпечує надійний захист даних у процесі передачі. Це допомагає уникнути перехоплення або модифікації даних під час їх пересилання між клієнтами та серверами.

Teleport використовує сертифікати для автентифікації користувачів та ресурсів, автоматично створюючи та відкликаючи їх відповідно до налаштованих політик доступу. Це дозволяє уникнути проблем, пов'язаних з компрометацією паролів, та підвищує рівень безпеки доступу.

Режим Identity-Aware Proxy (IAP) у Teleport надає додатковий рівень безпеки, оскільки приватні ключі ніколи не залишають клієнтські машини, а автентифікація виконується за допомогою публічних ключів. Це забезпечує взаємну автентифікацію між клієнтами і ресурсами, знижуючи ризик атак на основі крадіжки файлів cookie або CSRF (Cross-Site Request Forgery) [16].

Teleport забезпечує просту інтеграцію з існуючими інфраструктурами, включаючи хмарні сервіси, бази даних, кластеризовані середовища Kubernetes та віддалені сервери. Він також підтримує роботу через API, що дозволяє інтегрувати його в інші системи безпеки та автоматизації.

2.4 Підтримка аудиту та моніторингу в реальному часі за допомогою Teleport

Однією з основних переваг системи Teleport є її можливості для аудиту та моніторингу сесій у реальному часі, що дозволяє забезпечити прозорість дій користувачів у привілейованому доступі та гарантувати дотримання вимог щодо безпеки. Завдяки запису сесій і зберіганню подій у вигляді аудиторських журналів, Teleport дозволяє адміністраторам виявляти та попереджати загрози, а також контролювати активність користувачів у критично важливих системах.

Teleport підтримує різні типи записів сесій, включаючи SSH, Kubernetes, віддалені робочі столи, а також бази даних. Це забезпечує комплексний огляд усіх дій, які виконуються в інфраструктурі. Основні типи записів сесій включають:

1. SSH сесії. Teleport фіксує весь вивід псевдотерміналу (PTY) для SSH-сесій, що надає адміністраторам можливість перегляду всіх команд і операцій, виконаних користувачем. Такий підхід дозволяє забезпечити повний контроль за діяльністю користувачів з привілейованим доступом [14].

Водночас, існують певні ризики щодо безпеки, оскільки користувачі можуть приховувати команди через кодування або зміну налаштувань терміналу. Для усунення цих ризиків рекомендується використовувати розширений запис сесій, заснований на технології BPF (Berkeley Packet Filter).

2. Kubernetes сесії. Для сесій Kubernetes Teleport записує всі виклики команд kubectl exec, забезпечуючи повний огляд виконаних дій у кластерах. Такий запис допомагає контролювати роботу користувачів у кластері Kubernetes і запобігати можливим загрозам.

3. Сесії віддалених робочих столів. Teleport записує вміст екрану і введення миші під час віддалених сесій робочих столів. Важливо, що запис не включає натискання клавіш, що знижує ризик перехоплення конфіденційної інформації, такої як паролі. Це робить цей тип запису безпечнішим для зберігання і моніторингу.

4. Сесії додатків. Запис сесій додатків фіксує події доступу до корпоративних додатків у вигляді audit events, що групуються за п'ятихвилинними інтервалами. Цей механізм дозволяє отримати загальний огляд активності користувачів у додатках.

5. Сесії баз даних. Teleport записує запити до баз даних, що дає змогу контролювати і аналізувати роботу користувачів з базами даних. Це підвищує прозорість операцій і дозволяє швидко виявляти підозрілу активність.

Також, Teleport підтримує два режими запису сесій: синхронний і асинхронний, які забезпечують гнучке налаштування залежно від вимог до доступності та надійності з'єднань [16].

1. Синхронний запис. У синхронному режимі всі події сесій одразу передаються до Auth Server у режимі реального часу. Якщо запис події не вдається, сесія автоматично завершується. Такий підхід забезпечує максимальну надійність для середовищ із високими вимогами до регулювання та відповідності нормативним вимогам.

Перевага цього режиму полягає в тому, що дані не зберігаються на локальних дисках вузлів або проксі-серверів, що знижує ризик їх втрати чи компрометації.

2. Асинхронний запис. У цьому режимі події тимчасово зберігаються на локальному диску сервера, а після завершення сесії передаються на Auth Server. Асинхронний запис дозволяє сесіям продовжувати роботу навіть у разі втрати з'єднання з Auth Server, що підвищує гнучкість системи.

Однак цей режим може бути вразливим до ризиків, пов'язаних із тимчасовим зберіганням даних на диску, наприклад, можливістю їхнього пошкодження або видалення до моменту передачі на сервер.

Щодо зберігання, підтримується кілька варіантів зберігання записаних сесій. Для невеликих середовищ можна використовувати локальне сховище, але для продуктивних середовищ рекомендується використовувати хмарні рішення, такі як AWS S3 або Google Cloud Storage. Це дозволяє забезпечити надійність і масштабованість зберігання даних [16].

Записані сесії можуть бути відтворені через веб-інтерфейс Teleport або за допомогою CLI. Команда tsh play дозволяє відтворювати сесії через командний рядок, а у веб-інтерфейсі сесії доступні в розділі Activity.

Teleport забезпечує запис подій, пов'язаних з активністю користувачів у системі. Це включає події автентифікації, управління сесіями, виконання команд, копіювання файлів та інші важливі дії. Нижче наведені основні типи подій, що фіксуються в журналі аудиту Teleport:

Таблиця 2.2.

Типи подій у Teleport

Назва події	**Пояснення**	**Коментарі**
auth	Фіксує спробу автентифікації користувача.	Додаткові поля: {"success": "false", "error": "access denied"} — інформує про те, чи була спроба успішною або було відмовлено в доступі.
session.start	Фіксує початок інтерактивної сесії (наприклад, SSH).	Важлива для моніторингу моменту доступу до ресурсів.
session.end	Фіксує завершення інтерактивної сесії.	Допомагає відстежувати тривалість доступу користувача до ресурсів.
session.join	Фіксує приєднання нового користувача до існуючої сесії.	
session.leave	Фіксує вихід користувача із сесії.	
session.disk	Фіксує список файлів, відкритих під час сесії.	Потребує увімкненого Enhanced Session Recording.

Назва події	**Пояснення**	**Коментарі**
session.network	Фіксує список мережевих з'єднань, зроблених під час сесії.	Потребує увімкненого Enhanced Session Recording.
session.command	Фіксує список команд, виконаних користувачем під час сесії.	Потребує увімкненого Enhanced Session Recording.
session.recording.access	Фіксує доступ до запису сесії	
exec	Фіксує виконання віддаленої команди через SSH, наприклад, tsh ssh root@node ls /.	Додаткові поля: {"command": "ls /", "exitCode": 0, "exitError": ""}.
scp	Фіксує копіювання файлів через SCP.	Додаткові поля: {"path": "/path/to/file.txt", "len": 32344, "action": "read"}.
resize	Фіксує зміну розміру терміналу під час сесії	
user.login	Фіксує вхід користувача через веб-інтерфейс або командний інтерфейс (CLI).	Додаткові поля: {"user": "alice@example.com", "method": "local"}.
app.session.start	Фіксує доступ користувача до додатка.	
app.session.chunk	Фіксує активність користувача під час сесії додатка у вигляді окремих частин ("chunks").	

Назва події	Пояснення	Коментарі
join_token.create	Фіксує створення нового токена приєднання для вузлів або баз даних.	Додаткові поля: {"roles": ["Node", "Db"], "join_method": "token"}.

Висновки до другого розділу

У другому розділі магістерської роботи було проведено детальний аналіз платформи Teleport як рішення для управління привілейованими користувачами. Оглянуті основні компоненти Teleport, включаючи архітектуру та можливості, такі як централізоване управління доступом, багатофакторна аутентифікація та інтеграція з протоколами SSH і TLS. Також було здійснено порівняння Teleport з іншими рішеннями класу PAM, що дозволило виявити ключові переваги цього інструмента для підвищення безпеки в організаціях. Окремо розглянуто можливості платформи для проведення аудиту та моніторингу в реальному часі, що значно сприяє зниженню ризиків несанкціонованого доступу.

Таким чином, у цьому розділі підкреслюється, що Teleport є потужним інструментом для організацій, що прагнуть забезпечити надійний захист своїх інформаційних ресурсів, мінімізуючи ризики, пов'язані з привілейованими обліковими записами.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ НА ОСНОВІ ПОБУДОВАНОЇ РОЛЬОВОЇ МОДЕЛІ З ВИКОРИСТАННЯМ РІШЕННЯ TELEPORT

3.1 Основи побудови рольових моделей доступу: принципи та підходи

Рольові моделі доступу є основою для управління доступом до інформаційних ресурсів в сучасних інформаційних системах. Вони дозволяють забезпечити ефективний і безпечний розподіл прав користувачів на основі чітко визначених ролей. Це забезпечує контроль доступу до критичних систем та даних, зменшуючи ризик несанкціонованого доступу та внутрішніх загроз [17].

Принцип мінімальних привілеїв (Least Privilege Principle) полягає в тому, що кожному користувачу надаються лише ті права, які необхідні для виконання його обов’язків. Це зменшує ризик використання надлишкових прав у випадку компрометації облікового запису або зловживання привілеями.

Прикладом є ситуація коли адміністратору бази даних надаються лише права на управління базою даних, але не на доступ до конфіденційної інформації або зміни системних налаштувань.

Принцип розподілу обов'язків (Separation of Duties) полягає в розподілі ролей таким чином, щоб жоден користувач не мав повного контролю над критичними процесами. Це забезпечує захист від внутрішніх загроз і помилок.

Цей принцип може бути реалізований коли один користувач може мати права на створення рахунків, але не може їх затверджувати, а інший — тільки на затвердження [18].

Принцип обмеженого часу доступу (Time-Based Access Control) надає доступ до ресурсів лише на певний період часу або у визначені години. Це зменшує можливості для атаки або компрометації систем у позаробочий час.

Прикладом є доступ до виробничих серверів дозволяється лише в робочі години або під час запланованих робіт.

Принцип відповідності ролей функціям (Role-Fit Principle) визначає, що ролі повинні чітко відображати функціональні обов'язки користувачів і надавати відповідний набір прав. Це підвищує прозорість і полегшує управління привілеями.

3.2 Налаштування ролей у Teleport: кроки та рекомендації

Реалізація рольової моделі у Teleport досягається через Role-Based Access Control (RBAC), яка дозволяє адмініструвати доступ до ресурсів на основі визначених ролей. У Teleport кожен користувач асоціюється з однією або декількома ролями, які визначають, до яких ресурсів вони мають доступ і які дії можуть виконувати. Адміністратори створюють ролі з набором правил та дозволів, що можуть включати доступ до серверів, баз даних, програм або Kubernetes-кластерів [18].

Основні елементи рольової моделі:

- Ролі — визначають дозволи для доступу до інфраструктури.
- Логіни — вказують, якими користувачами на сервері або в іншій інфраструктурі може бути виконаний вхід.
- Мітки (Labels) — використовуються для управління доступом до певних ресурсів, таких як SSH-сервери або бази даних, за допомогою призначення міток.
- Управління доступом через правила — дозволи налаштовуються на основі специфічних правил, що включають доступ до різних типів ресурсів або операцій.

RBAC дозволяє адміністраторам налаштувати як широкі, так і специфічні права доступу для користувачів або сервісів у кластері.

Розглянемо приклад, коли в організації налаштовується рольова модель доступу до інфраструктури через Teleport. Уявімо, що в організації є різні середовища, зокрема *stage*, і необхідно надати доступ до всіх вузлів із міткою "env=stage", але при цьому обмежити доступ до баз даних або резервних копій. У такому випадку можна створити роль, яка надає доступ лише до певних ресурсів і забороняє доступ до вузлів з мітками "workload=database" або "workload=backup". У такому випадку роль буде виглядати наступним чином (рисунок 3.1):

```yaml
kind: role
version: v5
metadata:
  name: example-role
spec:
  allow:
    node_labels:
      'env': 'stage'

  deny:
    node_labels:
      # Multiple labels are interpreted as an "or" operation. In this case,
      # Teleport will deny access to any node labeled as 'workload=database' or
      # 'workload=backup'
      'workload': ['database', 'backup']
```

Рис. 3.1. — Приклад ролі в Teleport

У іншому випадку в організації визначено доступ до вузлів, які мають певні ярлики (labels).

Роль example-role дозволяє доступ до вузлів з ярликом environment=test, що визначає вузли, які використовуються для тестування. Використання виразу "*" дає можливість дозволити доступ до будь-яких вузлів без конкретних обмежень. Також дозволяється використання кількох значень для ярликів, наприклад, доступ до вузлів із environment=test або staging (рисунок 3.2).

```yaml
kind: role
version: v5
metadata:
  name: example-role
spec:
  allow:
    node_labels:
      # literal strings:
      'environment': 'test'
      # the wildcard ('*') means "any node"
      '*': '*'
      # a list of alternative options:
      'environment': ['test', 'staging']
      # regular expressions are also supported, for example the equivalent
      # of the list example above can be expressed as:
      'environment': '^test|staging$'
```

Рис. 3.2. — Приклад ролі в Teleport

RBAC також дозволяє обмежувати ресурси, доступні користувачам Teleport. Це може бути корисно, якщо, наприклад, не потрібно, щоб звичайні користувачі могли редагувати SSO (auth_connector) або створювати і редагувати нові ролі (role).

Правило для зміни ресурсів RBAC складається з двох частин: ресурсів і дієслів. Ось приклад правила allow, що описує дієслово зі списком, застосоване до ресурсу SSH-сесій. Воно означає «дозволити користувачам цієї ролі бачити список активних SSH-сесій» (рисунок 3.3).

```
allow:
  - resources: [session]
    verbs: [list]
```

Рис. 3.3. — Правило для зміни доступу до ресурсів

Якщо це правило буде оголошено в розділі deny визначення ролі, воно заборонить користувачам отримувати список активних сеансів.

Нижче наведено приклад розділу дозволів, який ілюструє загальновживані правила (рисунок 3.4). Кожне правило містить список ресурсів Teleport і CRUD-операцій, які користувачеві дозволено виконувати над ними:

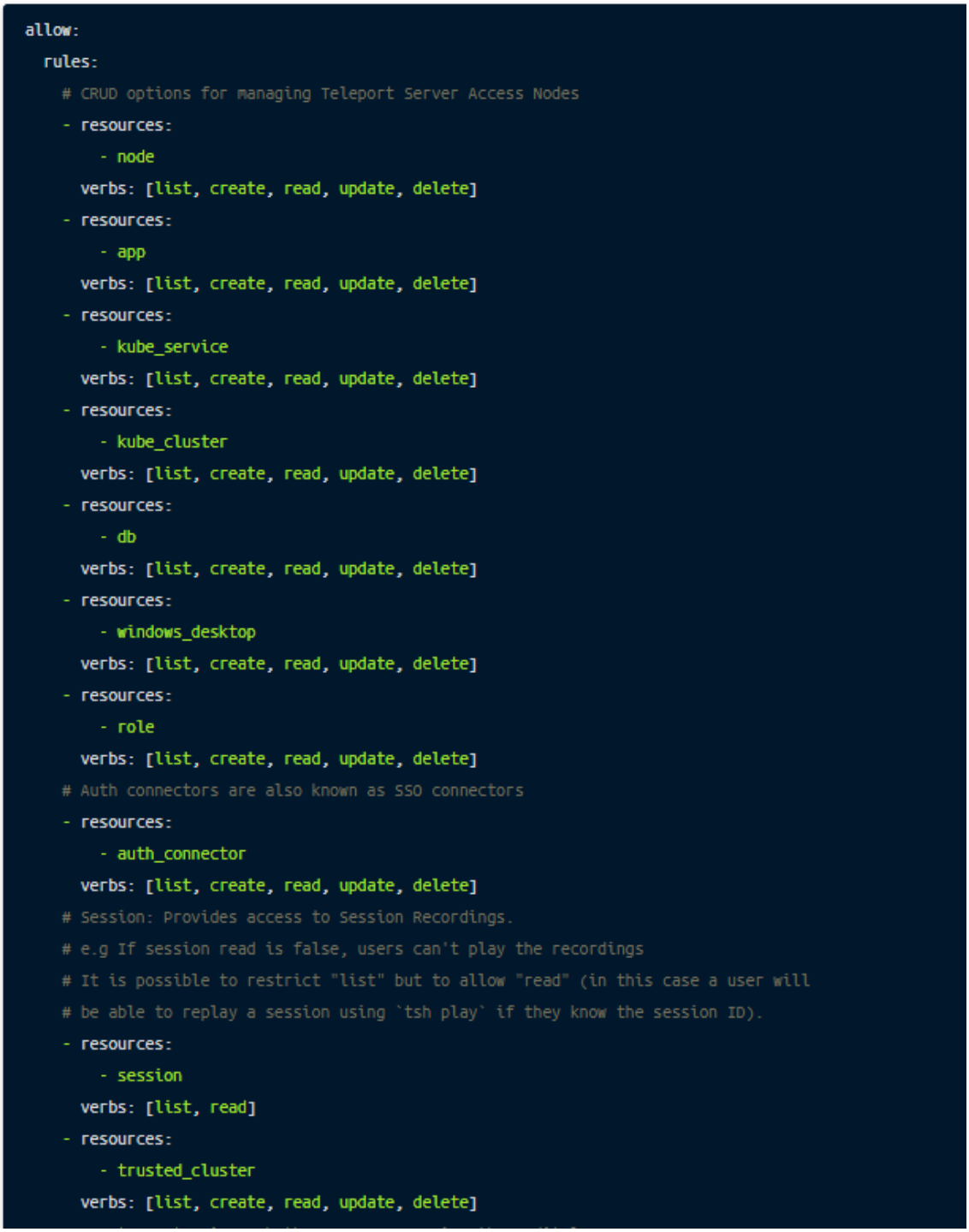


Рис. 3.4. — Шаблон доступних правил для зміни доступу до ресурсів

У Teleport є можливість обмежити доступ до записів сеансів та спільних сеансів таким чином, щоб доступ мав лише користувач, який створив сеанс (рисунок 3.5). Для цього потрібно налаштувати ролі з чітко визначеними дозволами.

```yaml
version: v5
kind: role
metadata:
  name: only-own-sessions
spec:
  allow:
    rules:
    # Users can only view session recordings for sessions in which they
    # participated.
    - resources: [session]
      verbs: [list, read]
      where: contains(session.participants, user.metadata.name)
```

Рис. 3.5. — Шаблон політики

Користувачам, що мають роль аудитора, надається доступ до всіх подій і записів сеансів. Щоб уникнути надмірних повноважень, важливо пересвідчитись, що користувач не має ролі, яка дозволяє надмірні права доступу до таких ресурсів, як сеанси або події.

Роль нижче only-own-ssh-sessions налаштована для обмеження доступу до сеансів лише для користувача, який їх створив.

У секції allow роль дозволяє доступ до всіх сеансів через ресурс session_tracker з усіма діями (вербами [*]), що включає перегляд, зміну, видалення сеансів тощо.

Однак, у секції deny введено обмеження, яке забороняє доступ до сеансів, у яких користувач не є учасником. Умова вказує, що доступ буде відхилено, якщо користувача немає серед учасників сеансу (!contains(session_tracker.participants, user.metadata.name)) (рисунок 3.6).

```yaml
version: v5
kind: role
metadata:
  name: only-own-ssh-sessions
spec:
  allow:
    rules:
    # Teleport allows session access to the user's sessions
    # and sessions they can join by default. This allows seeing any sessions.
    - resources: [session_tracker]
      verbs: ['*']
  deny:
    rules:
    # ... and then limit that access via a deny rule.
    # Deny rules take precedence over allow rules, so the resulting role
    # only allows user to see their own active sessions.
    - resources: [session_tracker]
      verbs: [list, read, update, delete]
      where: '!contains(session_tracker.participants, user.metadata.name)'
```

Рис. 3.6 — Шаблон політики

Teleport надає декілька заздалегідь налаштованих ролей, які спрощують управління доступом до ресурсів кластера та відповідними правами. Нижче наведено опис кожної ролі:

Таблиця 3.1.

Передналаштовані ролі в Teleport

Назва ролі	**Опис**	**Призначення ролі**
access	Дозволяє доступ до ресурсів кластера	Ця роль надає базові права на доступ до ресурсів кластера, таких як сервери, бази даних або кластери Kubernetes. Користувач із цією роллю може підключатися до ресурсів, але не має прав на зміну конфігурацій або доступ до аудиту.
editor	Дозволяє редагувати конфігурації кластера	Ця роль надає права на зміну конфігурацій системи. Вона корисна для адміністраторів, які відповідальні

		за налаштування кластера, але не займаються безпекою або аудитом.
Назва ролі	**Опис**	**Призначення ролі**
auditor	Дозволяє читати події кластера, журнали аудиту та переглядати записані сесії	Ця роль призначена для спеціалістів із безпеки або аудиторів, які повинні переглядати журнали подій, аудиторські логи та записані сесії для моніторингу активності та виявлення інцидентів безпеки.
requester (лише для Enterprise-версії):	Дозволяє користувачу створювати запити на доступ (Access Requests)	Ця роль використовується в корпоративних середовищах для створення запитів на тимчасовий доступ до певних ресурсів або привілеїв. Користувач може подати запит, який буде розглянутий і затверджений адміністраторами або іншими авторизованими користувачами.
reviewer (лише для Enterprise-версії)	Дозволяє переглядати та затверджувати запити на доступ (Access Requests).	Ця роль призначена для користувачів, які мають право переглядати та схвалювати або відхиляти запити на доступ, створені іншими користувачами. Це важливо для забезпечення контролю над тимчасовими правами доступу.
group-access	Дозволяє доступ до всіх груп користувачів	Ця роль надає користувачеві доступ до всіх груп у кластері, що може бути корисно для адміністраторів або

		менеджерів, які повинні взаємодіяти з різними групами користувачів у системі

Назва ролі	**Опис**	**Призначення ролі**
device-admin	Використовується для управління довіреними пристроями	Ця роль надає права адміністраторам для управління пристроями, які використовуються для доступу до кластера. Це включає додавання, видалення або налаштування довірених пристроїв у системі
device-enroll	Дозволяє користувачам реєструвати свої пристрої як довірені.	Користувачі з цією роллю можуть додавати свої пристрої до списку довірених пристроїв, що використовується для додаткової автентифікації при доступі до кластера.

Teleport також можна обмежити доступ до спільних сесій та записів сесій на основі ролей. Це дозволяє гарантувати, що лише користувачі, які створили сесію, або ті, кому надано відповідні дозволи, мають доступ до неї.

3.3. Управління користувачами та привілеями у системі Teleport

В Teleport ідентифікація користувача існує в межах кластера. Адміністратор Teleport створює облікові записи користувачів і зіставляє їх із ролями, які вони можуть використовувати для доступу до ресурсів. Це дозволяє чітко визначати, під яким обліковим записом користувач може входити в операційну систему (OS) на вузлах кластера.

Розгялнемо це на прикладі. Створимо користувачів у системі Teleport:

1. joe – має можливість входити до системних вузлів як користувач joe або root, що дозволяє йому виконувати дії на рівні адміністратора.

2. bob – може використовувати лише логін bob, що обмежує його права до рівня цього користувача.

3. kim – якщо не вказано конкретного логіну, за замовчуванням використовується логін, що збігається з ім'ям користувача Teleport, тобто у цьому випадку це буде kim.

Таблиця 3.2.

Зіставлення користувачів Teleport з обліковими записами

Користувач Teleport	**Дозволені OS Логіни**	**Опис**
joe	joe, root	Користувач joe може входити до вузлів як користувач joe або root в ОС.
bob	bob	Користувач bob може входити до вузлів лише як користувач bob в ОС.
kim	-	Якщо OS логін не вказано, за замовчуванням використовується те саме ім'я, що і користувач Teleport (у цьому випадку kim).

Для створення нового користувача, використовується команда tctl. При цьому адміністратор вказує ролі та дозволені логіни користувача для доступу до вузлів ОС.

Приклад команди для додавання нового користувача:

tctl users add joe --logins=joe,root --roles=access,editor

Teleport згенерує тимчасовий токен (термін дії — 1 година) та надасть URL для завершення налаштування користувача. Користувач повинен вставити URL у своєму браузері, щоб завершити реєстрацію, вибрати пароль і налаштувати багатофакторну автентифікацію (MFA).

URL для завершення налаштування користувача виглядатиме наступним чином:

https://<proxy_host>:443/web/invite/<token>

Після успішної автентифікації користувач отримає сертифікат, підписаний сервером Teleport Auth Server, який зберігатиметься на клієнтській машині. Цей сертифікат автоматично закінчується через 12 годин (за замовчуванням), після чого користувач повинен буде знову увійти в систему.

Після створення користувача його обліковий запис стає видимим через команду *tctl users ls*:

Вивід виглядатиме наступним чином (рисунок 3.7):

```
$ tctl users ls

User           Allowed Logins
----           --------------
admin          admin,root
kim            kim
joe            joe,root
```

Рис. 3.7. — Приклад виводу

Адміністратори можуть редагувати записи користувачів за допомогою команди tctl. Для отримання списку всіх користувачів використовується команда *tctl get users.*

Щоб редагувати конкретного користувача, наприклад, користувача joe, використовується наступна команда:

tctl edit user/joe.

Після внесення змін, збережіть і закрийте файл в редакторі, щоб застосувати нові налаштування для користувача.

Розглянемо процес управління доступом на прикладі застосування маніфестів у Teleport. Для цього, з використанням принципів Infrastructure as Code (IaC), створюються файли маніфестів для ролей та користувачів. У цьому прикладі визначено дві ролі: менеджер, який має доступ до списку користувачів і аудиторських подій, та інженер, якому надано права доступу до тестових і проміжних серверів. Після створення ролей, за допомогою інструменту tctl ці ролі застосовуються до двох користувачів, таким чином забезпечуючи кероване та захищене розмежування привілеїв.

1. Налаштуємо відповідні roles.yaml файли (рисунок 3.8).

```yaml
kind: role
version: v7
metadata:
  name: manager
spec:
  allow:
    rules:
      - resources: ['user', 'role']
        verbs: ['list','read']
      - resources: ['session', 'event']
        verbs: ['list', 'read']
---
kind: role
version: v7
metadata:
  name: engineer
spec:
  allow:
    logins: ['root', 'ubuntu', '{{internal.logins}}']
    node_labels:
      'env': ['test', 'staging']
```

Рис. 3.8. — Налаштовані ролі

2. Далі ми створюємо двох відповідних користувачів. Bob — розробник з роллю engineer. Alice — менеджер розробки з ролями manager та engineer. Налаштування користувачів прописуємо у файлі users.yaml (рисунок 3.9).

```yaml
kind: user
version: v2
metadata:
  name: alice
spec:
  roles: ['manager', 'engineer']
---
kind: user
version: v2
metadata:
  name: bob
spec:
  roles: ['engineer']
```

Рис. 3.9. — Створення ролей

3. Для застосування створених файлі необхідно використати команду tctl. Спочатку необхідно створити ролі, а потім користувачів:

tctl create -f roles.yaml

tctl create -f users.yaml

4. Після виконання попередніх кроків потрібно перевірити чи були створені необхідні користувачі із відповідними ролями.

Для цього можна скористатись веб-консоллю. Необхідно перейти в налаштування та обрати меню **Users** (рисунок 3.10).

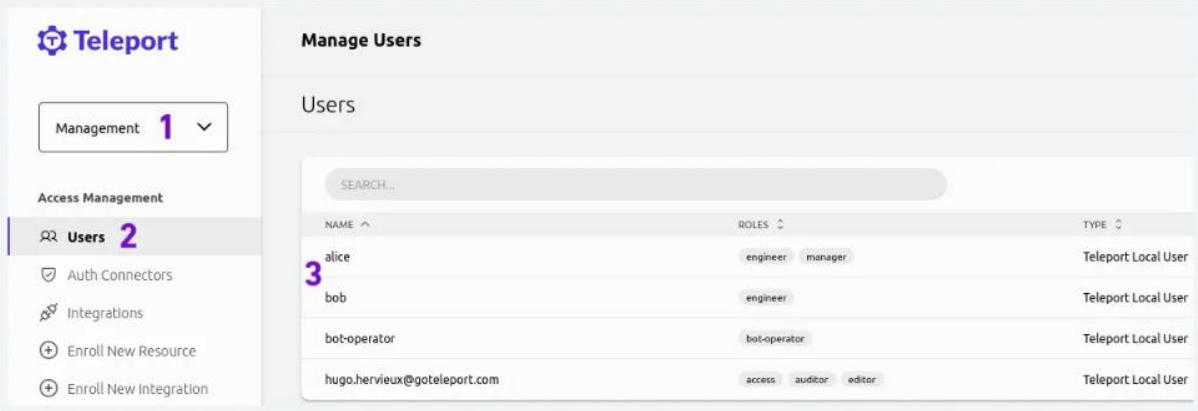


Рис. 3.10. — Перевірка створення користувачів через WebUI

Також це можна зробити через командний рядок (CLI) (рисунок 3.11, 3.12).

```
$ tctl users ls
User                          Roles
----------------------------- -----------------------
@teleport-access-approval-bot @teleport-access-approver
alice                         manager,engineer
bob                           engineer
bot-operator                  bot-operator

alternatively you can inspect the users details by doing
```

Рис. 3.11. — Перевірка створення користувачів через CLI

```
$ tctl get user/alice
kind: user
metadata:
  id: 1704849160091933780
  labels:
    teleport.dev/origin: kubernetes
  name: alice
spec:
  created_by:
    time: "2024-01-10T01:12:40.088581806Z"
    user:
      name: bot-operator
  expires: "0001-01-01T00:00:00Z"
  roles:
  - manager
  - engineer
  status:
    is_locked: false
    lock_expires: "0001-01-01T00:00:00Z"
    locked_time: "0001-01-01T00:00:00Z"
    recovery_attempt_lock_expires: "0001-01-01T00:00:00Z"
version: v2
```

Рис. 3.12. — Перевірка створення користувачів через CLI

5. Після створення локальних користувачів у Teleport, їм необхідно видати посилання для скидання пароля та налаштування багатофакторної автентифікації (MFA). Це посилання генерується за допомогою одноразового токена. Можна вручну скинути пароль користувача через команду tctl users reset alice.

В цьому випадку вивід буде виглядати наступним чином (рисунок 3.13):

```
$ tctl users reset alice
User "alice" has been reset. Share this URL with the user to complete password reset, link is valid for 8h:
https://teleport.example.com:443/web/reset/05b420fdc784597cbbb1d2ba65697cd8

NOTE: Make sure teleport.example.com:443 points at a Teleport proxy which users can access.
```

Рис. 3.13. — Скидання паролю через CLI

Можна автоматизувати процес відправки посилань для скидання пароля, використовуючи команду, яка генерує токен у форматі JSON (рисунок 3.14):

```
$ tctl users reset alice --format=json | \
    jq '"Sending an email to " + .spec.user +" that contains the link: " + .spec.url'
```

Рис. 3.14. — Автоматизація процесу скидання паролю

3.4 Впровадження політик безпеки через рольову модель

Згідно з рольовою моделлю надання доступу, Користувач – це людина, яка працює з системою і виконує певні службові обов’язки. Роль – це активно діюча в системі абстрактна сутність, з якою пов’язаний обмежений, логічно зв’язаний набір повноважень, необхідних для здійснення певної діяльності. Рольова модель застосовується досить широко, тому що вона, на відміну від інших більш строгих і формальних політик, є дуже близькою до реального життя.

Використання рольової моделі дозволяє ефективно розподіляти привілеї між користувачами на основі їхніх функціональних обов'язків, що підвищує рівень безпеки системи та знижує ризик несанкціонованого доступу.

Основим принципом побудови політик безпеки є надання користувачам лише тих прав, які їм необхідні для виконання їхніх завдань. Це мінімізує ризик використання зайвих прав у разі компрометації облікового запису або зловживання привілеями.

Таким чином рольова модель дозволяє контролювати доступ до різних ресурсів, таких як бази даних, сервери або програми, на основі ролей користувачів. Користувачі можуть мати доступ лише до певних ресурсів, що відповідають їхнім обов'язкам.

Наприклад, адміністратори можуть переглядати журнали аудиту та керувати конфігураціями, тоді як розробники можуть лише виконувати операції на серверах.

Політики безпеки можуть бути впроваджені через кілька рівнів доступу, де користувачі з різними ролями мають різні рівні доступу до інформації та ресурсів.

За допомогою ролей можна впровадити політики моніторингу та аудиту активності користувачів. Користувачі з ролями аудиторів можуть переглядати активність у системі, журнали сесій та події без можливості їх змінювати.

Також, використовуючи такі моделі, як Attribute-Based Access Control (ABAC), політики доступу можуть бути гнучкими та контекстно залежними. Наприклад,

доступ до ресурсів може надаватися залежно від місцезнаходження користувача, часу доби або інших атрибутів.

Принципи рольового управління:

- усі суб’єкти і об’єкти повинні бути однозначно ідентифікованими; — у системі має бути визначено набір ролей у системі;

- кожній ролі має бути встановлено певний обсяг повноважень;

- доступ суб’єктів до об’єктів має здійснюватися на підставі певних правил в рамках певної ролі.

Згідно з українським законодавством, є певний перелік документів, що забезпечують реалізацію політику безпеки інформації та вимагає впровадження рольової моделі управління доступом до ресурсів. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" встановлює правові засади захисту інформації в електронних системах, а також зобов'язує організації запроваджувати заходи щодо захисту даних, зокрема через обмеження доступу до інформаційних ресурсів [19].

Національний стандарт України ДСТУ ISO/IEC 27001:2015 містить вимоги до систем управління інформаційною безпекою (СУІБ) і визначає, що управління доступом має здійснюватися відповідно до встановлених ролей і обов'язків користувачів. Стандарт вимагає впровадження рольових моделей, що регламентують доступ до ресурсів відповідно до посадових обов'язків користувачів [20].

Постанова Кабінету Міністрів України №373 "Про затвердження Порядку захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних систем" описує, що для захисту інформації органи влади повинні використовувати моделі розмежування доступу, включаючи рольові моделі, які обмежують права доступу користувачів відповідно до їхніх посадових обов'язків [21].

Закон України "Про основні засади забезпечення кібербезпеки України" вимагає від організацій впровадження ефективних механізмів управління доступом для захисту інформації, в тому числі через рольові моделі, які дозволяють точніше керувати доступом до чутливих даних [22].

3.5 Проектування та впровадження RBAC в організаціях з використанням Teleport

Розглянемо приклад впровадження рольової моделі на прикладі організації, що має назву компанія "U". Компанія "U" є технологічною компанією, що розробляє програмне забезпечення та рішення на основі штучного інтелекту для підприємств. Основні активи компанії включають інтелектуальну власність, дані клієнтів та IT-інфраструктуру, яка забезпечує функціонування ключових продуктів і послуг. Захист цих активів є критично важливим для безпеки компанії, тому необхідно впровадити систему контролю доступу, що надасть користувачам доступ лише до тих ресурсів, які необхідні для виконання їхніх обов'язків.

Ключові активи компанії "U":

- ***Інтелектуальна власність***: патенти, алгоритми, вихідний код програмного забезпечення, що є основними джерелами конкурентної переваги.
- ***IT-інфраструктура***: сервери, хмарні сервіси та робочі станції, на яких зберігаються та обробляються дані.
- ***Дані клієнтів***: конфіденційна інформація, включаючи контракти та проектні документи.
- ***Персонал***: розробники, дослідники та IT-спеціалісти, які працюють над продуктами компанії.

Для захисту активів компанії необхідно впровадити Role-Based Access Control (RBAC). Основна мета RBAC полягає в тому, щоб користувачі мали доступ лише до тих ресурсів, які їм необхідні для виконання їхніх функцій. Teleport є ідеальним рішенням для впровадження RBAC завдяки своїм можливостям керувати доступом до IT-інфраструктури, серверів та хмарних ресурсів.

Визначимо ключові принципи RBAC для компанії "U":

1. ***Принцип мінімальних привілеїв***: кожному користувачу надаються лише ті права, які йому потрібні для виконання його робочих завдань. Наприклад,

розробники повинні мати доступ до тестових середовищ, але не до продакшн серверів.

2. ***Принцип розділення обов'язків***: доступ до критичних ресурсів розподіляється між кількома користувачами для зниження ризику зловживання привілеями. Наприклад, один користувач може запускати код, але не має прав змінювати конфігурацію серверів.

3. ***Прозорість і аудит***: всі дії користувачів повинні бути прозорими, а доступ до важливих ресурсів має бути відслідкований через журнали аудиту. Це допоможе виявляти потенційні загрози та несанкціоновану діяльність.

Для налаштування RBAC у компанії "U" за допомогою Teleport, необхідно створити ролі для різних груп користувачів на основі їхніх обов'язків та рівня доступу до активів компанії.

Таблиця 4.1

Створена матриця ролей

Роль	**Опис**	**Доступ до ресурсів**	**Привілеї**	**Приклад користувачів**
Developer	Розробники, що працюють над кодом і тестуванням в середовищах розробки та тестування	Тестові репозиторії вихідного коду	- Запуск і тестування коду - Немає доступу до продакшн середовища - Немає прав змінювати конфігурації серверів	Bob, команда розробників
IT Admin	Адміністратори, відповідальні	Уся IT-інфраструктура:	- Повний доступ до всіх серверів	Charlie, IT-відділ

Роль	**Опис**	**Доступ до ресурсів**	**Привілеї**	**Приклад користувачів**
	за підтримку IT-інфраструктури	сервери, хмарні ресурси, мережеві конфігурації	- Управління конфігураціями - Моніторинг та налаштування мережевих ресурсів	
Manager	Менеджери розробників або проектів, що контролюють активність	Журнали аудиту, записані сесії	- Перегляд подій аудиту - Перегляд записаних сесій - Немає прав змінювати ресурси або конфігурації	Alice, менеджери проектів
Security Auditor	Спеціалісти з безпеки, що контролюють відповідність вимогам безпеки	Журнали безпеки, аудиторські логи	- Перегляд і аналіз аудиторських логів - Немає прав змінювати конфігурації або отримувати доступ до критичних ресурсів	Dave, відділ безпеки
Product Owner	Власники продуктів, що	Інформація про	- Перегляд результатів	Erin, команда продукту

Роль	**Опис**	**Доступ до ресурсів**	**Привілеї**	**Приклад користувачів**
	приймають рішення щодо запуску і підтримки продукту	середовище, журнали подій, аналітичні звіти	тестування - Перегляд стану середовища - Немає прав втручатися в технічні процеси	
DevOps Engineer	Інженери DevOps, що відповідають за автоматизацію і підтримку CI/CD	Тестові, стадійні та продакшн сервери	- Налаштування автоматизації (CI/CD) - Розгортання і оновлення систем - Моніторинг стану продуктового середовища	Frank, DevOps команда
Compliance Officer	Відповідальні за відповідність стандартам і регулюванням	Журнали аудиту, записи доступу, інформація про дії користувачів	- Моніторинг відповідності політик і стандартів - Перегляд записаних сесій і подій - Немає доступу до змін	Grace, відділ комплаєнсу

Роль	**Опис**	**Доступ до ресурсів**	**Привілеї**	**Приклад користувачів**
			конфігурацій або ресурсів	

Опис ключових аспектів:

- Роль — визначає групу користувачів, яка виконує певні функції в організації.
- Опис — короткий опис ролі і завдань, які виконують користувачі в межах цієї ролі.
- Доступ до ресурсів — описує, до яких ресурсів або середовищ користувачі мають доступ.
- Привілеї — описує конкретні права, які користувачі мають в межах своєї ролі (зміна конфігурацій, запуск коду, моніторинг тощо).
- Приклад користувачів — приклади користувачів або команд, які можуть використовувати ці ролі.

Розглянемо конфігурації ролей у форматі YAML для кожної ролі, відповідно до таблиці рольової моделі привілейованих користувачів. Ці ролі можна використовувати в Teleport для управління доступом.

1. Роль Developer (Розробник) — користувачі, що відповідають за створення та тестування коду програмного забезпечення. Вони працюють із тестовими та стадійними середовищами, де проводиться розробка і підготовка продуктів перед їхнім впровадженням у продуктове середовище.

Доступи, що надаються: доступ до тестових і стадійних серверів (логін через обліковий запис розробника), проте немає доступу до продуктового середовища або серверів, де розміщені критично важливі сервіси.

Ролдь надається саме такою, тому що:

- Забезпечується принцип мінімальних привілеїв: розробники не повинні мати доступ до продакшн середовища, оскільки це може призвести до випадкових змін у критичних системах.

• Розмежування середовищ дозволяє розробникам фокусуватися на своєму завданні без доступу до незапланованих ресурсів, що знижує ризики потенційного зловживання або помилок.

Конфігурація виглядатиме наступним чином (рисунок 3.15):

```
kind: role
metadata:
  name: developers_role
  revision: 275b366f-ed61-481e-9d49-a062c8f51984
spec:
  allow:
    logins:
    - '{{internal.logins}}'
    node_labels:
      env: development
    rules:
    - resources:
      - session
      verbs:
      - read
      - list
      where: contains(session.participants, user.metadata.name)
  deny:
    logins:
    - guest
  options:
    cert_format: standard
    create_db_user: false
    create_desktop_user: false
    desktop_clipboard: true
    desktop_directory_sharing: true
    enhanced_recording:
    - command
    - network
    forward_agent: false
    idp:
      saml:
        enabled: true
    max_session_ttl: 8h0m0s
    pin_source_ip: false
    port_forwarding: true
    record_session:
      default: best_effort
      desktop: true
    ssh_file_copy: true
version: v7

```

Рис. 3.15. Роль Developer

2. Роль IT Admin (Адміністратор IT) — користувачі, відповідальні за підтримку всієї інфраструктури компанії. Це включає управління серверами, конфігурацію мереж, баз даних і хмарних ресурсів.

Дані користувачі мають необмежений доступ до всієї IT-інфраструктури, а саме до усіх серверів, мережевих налаштувань та хмарних сервісів.

Також, у них є можливість змінювати конфігурації, проводити оновлення та підтримувати функціональність усіх систем.

Обгрунтування ролі:

IT Admin повинен мати повний доступ до всієї інфраструктури для забезпечення стабільної роботи системи, швидкого реагування на проблеми та підтримки високого рівня безпеки. Без повного доступу адміністратори не можуть виконувати свої ключові функції з підтримки.

Відповідальність за всі ресурси вимагає надання широких привілеїв.

Конфігурація виглядатиме наступним чином (рисунок 3.16, 3.17):

```
kind: role
metadata:
  name: it_admin
  revision: f58d458a-14eb-4072-a4f7-a966a3683515
spec:
  allow:
    app_labels:
      '*': '*'
    db_labels:
      '*': '*'
    db_names:
    - '{{internal.db_names}}'
    - '*'
    db_users:
    - '{{internal.db_users}}'
    - sa
    - admin
    kubernetes_groups:
    - '{{internal.kubernetes_groups}}'
    kubernetes_labels:
      '*': '*'
    kubernetes_resources:
    - kind: '*'
      name: '*'
      namespace: '*'
      verbs:
      - '*'
    kubernetes_users:
    - admin
    logins:
    - admin
    node_labels:
      '*': '*'
    rules:
    - resources:
      - node
      verbs:
      - list
      - create
      - read
    - resources:
      - app
```

Рис. 3.16. Роль IT Admin

Рис. 3.17. Роль IT Admin

3. Роль Manager — користувачі з цією роллю керують командами розробників і контролюють роботу проєктів. Їхня функція полягає у перегляді процесів і результатів роботи команд, але вони не повинні мати можливості змінювати налаштування або вносити технічні правки.

Дані користувачі можуть переглядати журнали аудиту та записи сесій, проте у них немає прав на зміну конфігурацій або втручання у технічні процеси.

Менеджери повинні мати можливість контролювати роботу команд, однак надання їм технічних привілеїв може призвести до випадкових змін або порушень. Забезпечення прозорості процесів без права втручання допомагає уникнути помилок з боку управлінського персоналу.

Роль повинна виглядати наступним чином (рисунок 3.18):

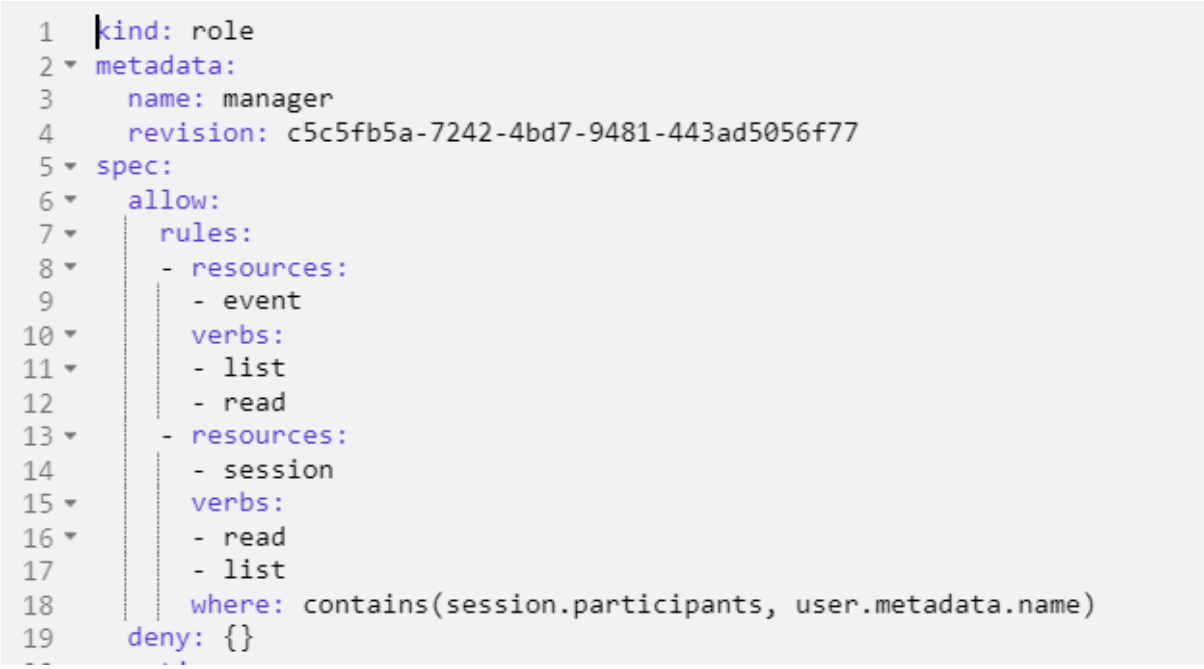


Рис. 3.18 Роль Manager

4. Роль Security Auditor (Аудитор безпеки) — ця роль належить користувачам, що відповідають за моніторинг та оцінку стану безпеки інфраструктури. Вони повинні мати доступ до журналів подій, щоб аналізувати активність і виявляти потенційні загрози.

У даних користувачів є доступ до журналів безпеки, подій і записів сесій. Також у них є можливість переглядати інформацію, але без прав на зміну конфігурацій або втручання у процеси.

Забезпечення аудиту безпеки без надання прав на зміну конфігурацій дозволяє відстежувати потенційні загрози та гарантує, що аудитори не можуть помилково або навмисно вплинути на операційну діяльність. Це сприяє об'єктивному аналізу і відповідності стандартам безпеки.

Роль виглядатиме наступним чином (рисунок 3.19, 3.20):

```yaml
kind: role
metadata:
  description: Review cluster events and replay sessions
  labels:
    teleport.internal/resource-type: preset
  name: auditor
  revision: 7374b02a-a67e-46a2-8f35-a8eee0623283
spec:
  allow:
    logins:
    - no-login-6b3e77d5-e951-4a00-90c5-e4aecba1c7f9
    rules:
    - resources:
      - session
      verbs:
      - list
      - read
    - resources:
      - event
      verbs:
      - list
      - read
    - resources:
      - session_tracker
      verbs:
      - list
      - read
    - resources:
      - cluster_alert
```

Рис. 3.19 Роль Security Auditor

```yaml
      verbs:
      - list
      - read
    - resources:
      - instance
      verbs:
      - list
      - read
    - resources:
      - security_report
      verbs:
      - list
      - read
      - use
    - resources:
      - audit_query
      verbs:
      - list
      - read
      - use
    - resources:
      - bot_instance
      verbs:
      - list
      - read
    - resources:
      - notification
      verbs:
      - list
```

Рис. 3.20 Роль Security Auditor

5. Роль Product Owner (Власник продукту) — це власники продуктів, що відповідають за управління та розвиток продуктів компанії. Вони повинні мати можливість оцінювати стан продукту, але не втручатися в технічні процеси.

Також вони повинні мати доступ до аналітичних звітів та стану середовища, але у них немає прав на зміну конфігурацій або розгортання нових систем.

Власники продуктів зосереджені на прийнятті бізнес-рішень, тому їхній доступ повинен бути обмежений до перегляду інформації про продукт. Забезпечення такої моделі мінімізує ризики помилкових змін у технічній інфраструктурі.

Роль власників продукту налаштовується так (рисунок 3.21):

```
kind: role
metadata:
  name: product_owner
  revision: 268bdf4d-bf8b-46b4-974d-a3d0f59df6b4
spec:
  allow:
    logins:
    - '{{internal.logins}}'
    node_labels:
      env: staging
    rules:
    - resources:
      - event
      verbs:
      - list
      - read
    - resources:
      - report
      verbs:
      - read
      - list
      where: contains(session.participants, user.metadata.name)
```

Рис. 3.21. Product Owner

6. Роль DevOps Engineer (Інженер DevOps) — це інженери, що відповідають за автоматизацію розгортання, підтримку CI/CD процесів та забезпечення стабільної роботи серверів у тестовому, стадійному та продакшн середовищах.

Дані співробітники мають доступ до всіх середовищ: тестового та продуктового. Також вони можуть налаштувати та автоматизовувати процеси розгортання.

DevOps інженери відповідають за безперервну інтеграцію та розгортання, тому їм необхідний доступ до всіх середовищ. Крім того, вони повинні мати можливість змінювати налаштування CI/CD, щоб забезпечувати безперервний цикл розробки та доставки продукту.

Роль повинна виглядати наступним чином (рисунок 3.22):

```
kind: role
metadata:
  name: devops_engineer
  revision: 84ea6f4b-cc2c-45a7-af99-8daaa74ed6a7
spec:
  allow:
    logins:
    - root
    - ubuntu
    node_labels:
      env:
      - test
      - staging
      - production
    rules:
    - resources:
      - ci_cd
      verbs:
      - create
      - update
      - read
    - resources:
      - deployment
      verbs:
      - create
      - update
      - read
      where: contains(session.participants, user.metadata.name)
```

Рис. 3.22 Роль DevOps Engineer

7. Роль Compliance Officer (Відповідальний за відповідність) — ці користувачі стежать за дотриманням стандартів і правил у компанії. Вони повинні мати доступ до журналів і сесій для моніторингу відповідності процесів встановленим стандартам.

Дані користувачі мають доступ до журналів аудиту, подій і записаних сесій. Також вони можуть переглядати ресурси, але без втручання в операційні процеси.

Офіцери з комплаєнсу мають бути незалежними від технічного управління, щоб забезпечити об’єктивний нагляд за дотриманням стандартів і правил. Вони не повинні мати можливість змінювати налаштування, оскільки це може створити конфлікт інтересів.

Роль офіцерів комплаєнсу повинна виглядати наступним чином (рисунок 3.23):

```yaml
kind: role
metadata:
  name: compliance_officer
  revision: cb77b5eb-0220-42bc-8ecd-505129cf7073
spec:
  allow:
    rules:
    - resources:
      - event
      verbs:
      - list
      - read
    - resources:
      - session
      verbs:
      - read
      - list
    - resources:
      - log
      verbs:
      - read
      - list
    - resources:
      - audit
      verbs:
      - read
      - list
      where: contains(session.participants, user.metadata.name)
```

Рис. 3.23 Compliance Officer

Протягом роботи продукту нам вдалось відтворити інцидент в консолі Teleport. 15 жовтня був зафіксований один сеанс, ініційований користувачем з email-адресою teleport@ideabank.ua. Сеанс відбувся з використанням слабких механізмів безпеки, що вказує на недостатню захищеність або відсутність двофакторної автентифікації, перевірки пристроїв чи вимог щодо сесійної багатофакторної автентифікації (MFA) (рисунок 3.24).

Рис. 3.24 Відтворений інцидент

Цей випадок можна інтерпретувати як потенційний ризик для організації, оскільки SSH-сеанси з недостатньою безпекою можуть створити можливості для компрометації системи.

Також Teleport забезпечує детальний облік дій користувачів, що отримують доступ до систем через SSH або віддалений доступ до робочих столів. Усі дії записуються в логах та включають такі важливі події, як з**апуск і завершення сесій,** : Teleport фіксує момент початку та закінчення віддаленої сесії для кожного користувача, що дозволяє точно відстежувати тривалість і активність під час сесії, **видача сертифікатів**, **передача даних через буфер обміну** (рисунок 3.25).

Рис. 3.25 — Моніторинг подій на консолі Teleport

Записи сесій можуть бути збережені та завантажені для подальшого перегляду або аудиту. Це особливо корисно для подальшого аналізу дій користувачів або у разі необхідності розслідування інцидентів.

Для кожного користувача видаються тимчасові сертифікати, які дозволяють здійснювати автентифікацію. Ця подія фіксується, забезпечуючи додатковий контроль за тим, хто і коли отримав доступ до системи.

Teleport також фіксує події, пов'язані з передачею даних через буфер обміну, що може допомогти запобігти несанкціонованому поширенню конфіденційної інформації.

Цей функціонал забезпечує повну прозорість активностей користувачів у системі, дозволяє зберігати журнали подій та записів сесій для подальшого аналізу,

що критично важливо для підтримки високого рівня безпеки у середовищах з привілейованим доступом.

3.6 Рекомендації щодо використання технології управління привілейованими обліковими записами з використанням рішення Teleport

Згідно з проведеним дослідженням,, ми можемо надати рекомендації щодо впровадження технології PAM на базі рішення Teleport.

Використання Teleport для управління привілейованими обліковими записами в організації пропонує комплексний і безпечний підхід до контролю доступу. Проте, щоб забезпечити ефективну роботу рішення, необхідно враховувати наступні налаштування:

1. ***Впровадження контролю доступу повинне бути налаштоване на основі ролей (RBAC)***. Виконання цієї рекомендації передбачає визначення ролей, які відповідають потребам організації, і призначення мінімально необхідних привілеїв для кожної ролі. Добре структурована політика RBAC мінімізує ризик несанкціонованого доступу та зменшує потенційний вплив скомпрометованих облікових записів. Періодично переглядайте та оновлюйте ролі, щоб відображати зміни в обов'язках та вимогах до безпеки.

2. ***Інтеграція з єдиним входом (SSO) та багатофакторною автентифікацією (MFA).*** Інтеграція Teleport з провайдерами SSO (наприклад, Okta, Azure AD або Google SSO) покращує взаємодію з користувачем і посилює процеси автентифікації. Доповнення SSO функцією MFA додає ще один шар безпеки та захищає привілейовані акаунти від атак на основі облікових даних. Отже, весь доступ до критично важливих систем, включно з тими, що управляються через Teleport, вимагає багатофакторної автентифікації.

3. ***Моніторинг та аудит сесій.*** Налаштування запису сеансів Teleport повинні бути ввімкнені для всіх дій привілейованих користувачів. Це забезпечить повний моніторинг дій, виконаних на критично важливих ресурсах, в режимі

реального часу. Також, важливо встановити сповіщення для певних дій або аномалій, щоб вчасно виявляти і розслідувати підозрілі дії.

4. ***Контроль безпеки на основі політик.*** Оскільки Teleport дозволяє адміністраторам впроваджувати політики, що регулюють доступ до ресурсів, необхідно використовувати ці можливості для створення суворих політик доступу на основі часу, місцезнаходження та атрибутів користувача. Наприклад, обмежувати доступ до критично важливих систем у неробочий час або з ненадійних мереж, щоб мінімізувати ризики.

5. ***Створення масштабованої архітектури.*** Для великих організацій впровадження масштабованої архітектури рішення безпеки має вирішальне значення, щоб впоратися зі зростаючими робочими навантаженнями і забезпечити високу доступність. Важливо розглянути стратегії балансування навантаження та відмовостійкості, а також оптимізовані конфігурації для баз даних та кластерів Kubernetes, щоб гарантувати, що інфраструктура Teleport залишатиметься надійною під час пікових навантажень.

6. ***Періодичні перегляди доступу та аудит привілеїв.*** Перевірка доступів повинна бути регулярною, щоб переконатися, що ролі та привілеї, призначені через Teleport, відповідають поточним потребам організації. Цей процес допомагає виявити і виправити застарілі або надмірні дозволи, знижуючи ризик внутрішніх загроз або випадкового зловживання привілейованими обліковими записами.

7. ***Інтеграція з іншими інструментами безпеки.*** Щоб підвищити загальний рівень безпеки, важливо інтегрувати Teleport з іншими рішеннями безпеки, такими як системи управління інформацією та подіями безпеки (SIEM), системи виявлення вторгнень і засоби захисту кінцевих точок. Це забезпечить більш комплексну систему безпеки і полегшить кореляцію подій в IT-середовищі.

8. ***Програми навчання та підвищення обізнаності.*** Всі користувачі, особливо з привілейованим доступом, повинні бути добре обізнаниними з політикою безпеки організації та найкращими практиками використання Teleport. Регулярні тренінги повинні охоплювати належне використання функцій Teleport,

розпізнавання спроб фішингу та важливість дотримання політик безпеки. Також, потрібно переконатись, що всі користувачі обізнані щодо можливих наслідків атак, що можуть бути здійснені на організацію.

Надані рекомендації щодо використання Teleport для управління привілейованими обліковими записами відповідають вимогам міжнародних стандартів, зокрема ISO/IEC 27001.

Пункт «Впровадження контролю доступу на основі ролей (RBAC)» відповідає вимогам ISO/IEC 27001, пункт A.9.1.2 (Управління доступом користувачів). Ця рекомендація передбачає встановлення чітких ролей і обмежень на основі функціональних обов'язків, що мінімізує ризик несанкціонованого доступу і відповідає принципу надання мінімальних необхідних прав.

Пункт «Інтеграція з SSO та багатофакторною автентифікацією (MFA)» узгоджується з пунктами A.9.4.2 (Безпечні процедури входу) і A.9.4.3 (Захист транзакцій). Інтеграція з єдиним входом та впровадження багатофакторної автентифікації підвищує рівень безпеки процесів автентифікації та захищає облікові записи від несанкціонованого доступу.

Пункт «Моніторинг та аудит сесій» відповідає пунктам A.12.4.1 (Журналювання подій) та A.12.4.3 (Журнали дій адміністраторів та операторів). Постійний моніторинг та аудит дій привілейованих користувачів забезпечує виявлення аномалій та запобігання інцидентам безпеки, що відповідає вимогам щодо журналювання та відстеження подій.

Пункт «Контроль безпеки на основі політик» відповідає пунктам A.9.2.1 (Реєстрація і скасування реєстрації користувачів) та A.9.2.3 (Огляд прав доступу користувачів). Забезпечення контролю доступу на основі політик дозволяє обмежити доступ до критичних ресурсів, підвищуючи безпеку та відповідність вимогам.

Пункт «Створення масштабованої архітектури» узгоджується з пунктом A.17.2.1 (Наявність відмовостійких систем) та A.14.1.2 (Захист прикладних сервісів у відкритих мережах). Забезпечення масштабованості та надійності системи Teleport гарантує високу доступність і ефективний захист критичних активів.

Пункт «Періодичні перегляди доступу та аудит привілеїв» відповідає пунктам A.9.2.5 (Перегляд привілеїв користувачів) та A.9.4.5 (Огляд доступу). Регулярні огляди та перевірки дозволяють підтримувати актуальність привілейованих прав та вчасно усувати надмірні чи застарілі права доступу.

Пункт «Інтеграція з іншими інструментами безпеки» відповідає пункту A.16.1.3 (Повідомлення про інциденти інформаційної безпеки). Інтеграція Teleport з SIEM та іншими інструментами безпеки дозволяє забезпечити комплексний підхід до моніторингу та виявлення інцидентів, що підвищує загальний рівень безпеки.

Пункт «Програми навчання та підвищення обізнаності» узгоджується з пунктом A.7.2.2 (Інформування про безпеку, освіта та навчання). Навчання користувачів забезпечує відповідальне ставлення до привілейованих облікових записів і допомагає уникнути помилок, які можуть призвести до компрометації.

Таким чином, впровадження цих рекомендацій із використанням Teleport відповідає основним вимогам міжнародного стандарту ISO/IEC 27001, забезпечуючи контроль доступу, захист даних та управління інцидентами в організації. Використання цих рекомендацій дозволить організаціям підвищити загальний рівень інформаційної безпеки та успішно впровадити у себе технології для управління привілейованим доступом.

Висновки до третього розділу

У третьому розділі магістерської роботи було детально розглянуто впровадження політик безпеки через рольову модель на основі системи Teleport та проведено аналіз ефективності цих підходів у контексті управління привілейованими обліковими записами.

Результати дослідження показали, що рольова модель є потужним інструментом для забезпечення контролю доступу в сучасних інформаційних системах. Впровадження чітко визначених ролей дозволяє знизити ризики,

пов'язані з компрометацією привілейованих облікових записів, а також забезпечує гнучке управління доступом відповідно до посадових обов'язків користувачів.

У підсумку, розглянутий підхід до впровадження політик безпеки через рольову модель не лише забезпечує високий рівень контролю доступу, але й сприяє підвищенню надійності та ефективності систем захисту інформації в умовах сучасних викликів кібербезпеки.

ВИСНОВКИ

У даній кваліфікаційній роботі було проведено дослідження процесів управління привілейованими обліковими записами (PAM) з акцентом на сучасні технології контролю доступу до критично важливих ресурсів організацій. Основною метою роботи було вивчення можливостей впровадження та ефективного використання системи Teleport для забезпечення безпеки привілейованих користувачів у корпоративних інформаційних системах.

Протягом дослідження теми та її актуальності було розглянуто загальні аспекти привілейованого доступу та загрози, які виникають через його неналежне використання. Також, було проведено аналіз основних вразливостей привілейованих облікових записів, що ґрунтується на методології MITRE ATT&CK та сучасних техніках кіберзлочинців, таких як підвищення привілеїв, компрометація облікових даних та маніпуляції маркерами доступу.

Протягом виконання роботи було досліджено реалізацію технології управління привілейованим доступом на базі рішення Teleport у системи безпеки з метою посилення контролю доступу. Було розглянуто технічні аспекти інтеграції з такими рішеннями, як системи багатофакторної автентифікації (MFA) та зовнішні SSO провайдери (GitHub, Google Workspace тощо). Було запропоновано реалізацію рольової моделі (RBAC) для управління доступом на основі ролей користувачів та їх прав, що дозволяє організаціям гнучко керувати доступом до критичних ресурсів.

При розробці технології, було впроваджено політики безпеки через рольову модель у Teleport. Дана технологія базується на проектуванні ролей користувачів, та визначенні прав доступу. В результаті виконання кваліфікаційної роботи розроблено рекомендації по впровадженню технології на базі рішення Teleport для управління привілейованим доступом та можливості масштабування Teleport та його інтеграції з іншими хмарними сервісами, що забезпечує високу надійність та продуктивність системи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cybellium Ltd: Mastering PAM [Електронний ресурс] — Режим доступу: https://cybellium.com/products/mastering-pam
2. Forrester Research: PAM Market Report: Best Practices for Managing Privileged Users [Електронний ресурс] — Режим доступу:
3. ENISA Threat Landscape 2024 [Електронний ресурс] — Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
4. Verizon Business: Privelege Misuse [Електронний ресурс] — Режим доступу: https://www.verizon.com/business/resources/reports/dbir/2024/incident-classification-patterns-intro/privilege-misuse/
5. Admin Rights in Action: How Hackers Target Privileged Accounts [Електронний ресурс] — Режим доступу: https://heimdalsecurity.com/blog/admin-rights-privileged-accounts
6. MITRE ATT&CK: Matrix — Enterprise [Електронний ресурс] — Режим доступу: https://attack.mitre.org/matrices/enterprise/
7. NIST Special Publication 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations [Електронний ресурс] — Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf
8. Builtin: Guide to Discretionary Access Control (DAC) With Examples [Електронний ресурс] — Режим доступу: https://builtin.com/articles/discretionary-access-control
9. IONOS: Mandatory Access Control (MAC): how does it work? [Електронний ресурс] — Режим доступу: https://www.ionos.com/digitalguide/server/security/what-is-mandatory-access-control-mac/
10. IBM: What is role-based access control (RBAC)? [Електронний ресурс] — Режим доступу: https://www.ibm.com/think/topics/rbac#:~:text=Role-

based%20access%20control%20%28RBAC%29%20is%20a%20model%20for,see%20customer%20accounts%20but%20can%E2%80%99t%20touch%20firewall%20settings

11. Geeksforgeeks: Attribute-Based Access Control(ABAC) [Електронний ресурс] — Режим доступу: https://www.geeksforgeeks.org/attribute-based-access-controlabac/

12. 2022 Gartner® Magic Quadrant™ for Privileged Access Management [Електронний ресурс] — Режим доступу: https://www.bankinfosecurity.com/whitepapers/2022-gartner-magic-quadrant-for-privileged-access-management-w-12024

13. Дія.Бізнес: Управління привілейованим доступом (PAM) [Електронний ресурс] — Режим доступу: https://cyber.business.gov.ua/cybercatalogue/privileged-access-management-pam

14. Teleport: Easiest, Most Secure Infrastructure Access [Електронний ресурс] — Режим доступу: https://goteleport.com/

15. Teleport Explained: Concepts & Architecture Guide [Електронний ресурс] — Режим доступу: https://goteleport.com/how-it-works/

16. Introduction to the Teleport Access Platform: Zero Trust Security for Your Infrastructure [Електронний ресурс] — Режим доступу: https://goteleport.com/docs/

17. EYER: Role-Based Access Control (RBAC): Complete Guide 2024 [Електронний ресурс] — Режим доступу: https://eyer.ai/blog/role-based-access-control-rbac-complete-guide-2024/

18. Francis M. Kugblenu Memon Asim, January 2007 Separation of Duty in Role Based Access Control System: A Case Study

19. ЗАКОН УКРАЇНИ: Про захист інформації в інформаційно-комунікаційних системах [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

20. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги. Поправка (ISO/IEC 27001:2013; Cor 1:2014, IDT)

21. КАБІНЕТ МІНІСТРІВ УКРАЇНИ: ПОСТАНОВА від 15 жовтня 2024 р. № 1175 [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/1175-2024-%D0%BF#Text

22. ЗАКОН УКРАЇНИ: Про основні засади забезпечення кібербезпеки України [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління привілейованими користувачами на основі побудови рольової моделі з використанням рішення Teleport»

КЕРІВНИК

Д.Т.Н. ПРОФЕСОР **ГАЙДУР ГАЛИНА**

ВИКОНАЛА ЗДОБУВАЧ ВИЩОЇ ОСВІТИ

ГРУПИ БСДМ-61 **ПАРФЕНЮК ТЕТЯНА**

ОБ'ЄКТ, ПРЕДМЕТ ТА МЕТА ДОСЛІДЖЕННЯ

Об'єкт дослідження – привілейовані облікові записи.

Предмет дослідження – технологія управління привілейованими обліковими записами.

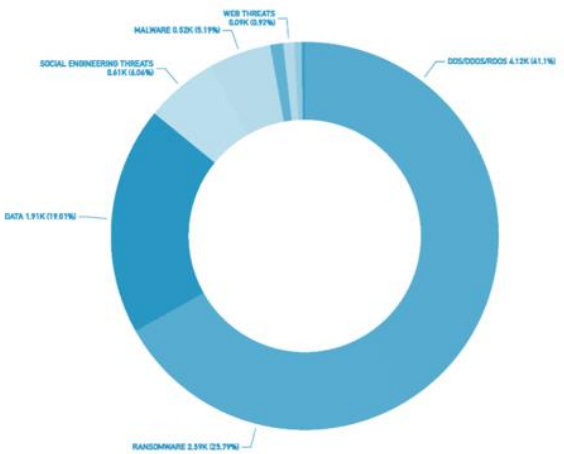
Мета роботи – розробити рекомендації щодо використання технології управління привілейованими обліковими записами в організаціях на основі реалізації рольової моделі доступу (RBAC).

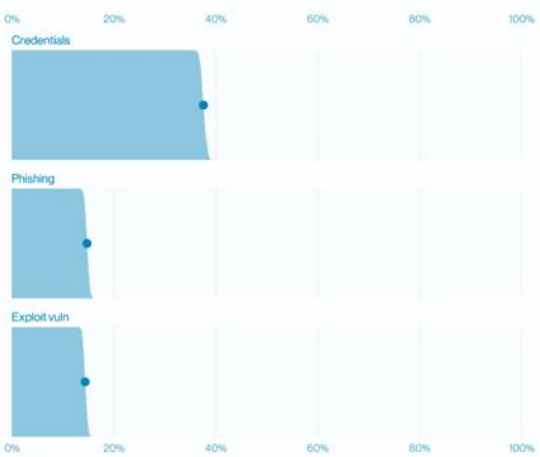
Завдання:

1. Провести аналіз привілейованих користувачів і технологій управління ними.
2. Проаналізувати платформу Teleport як рішення для управління привілейованими користувачами.
3. Розробити технологію управління привілейованим доступом на основі побудованої рольової моделі з використанням рішення Teleport.

2

Аналіз проблеми дослідження





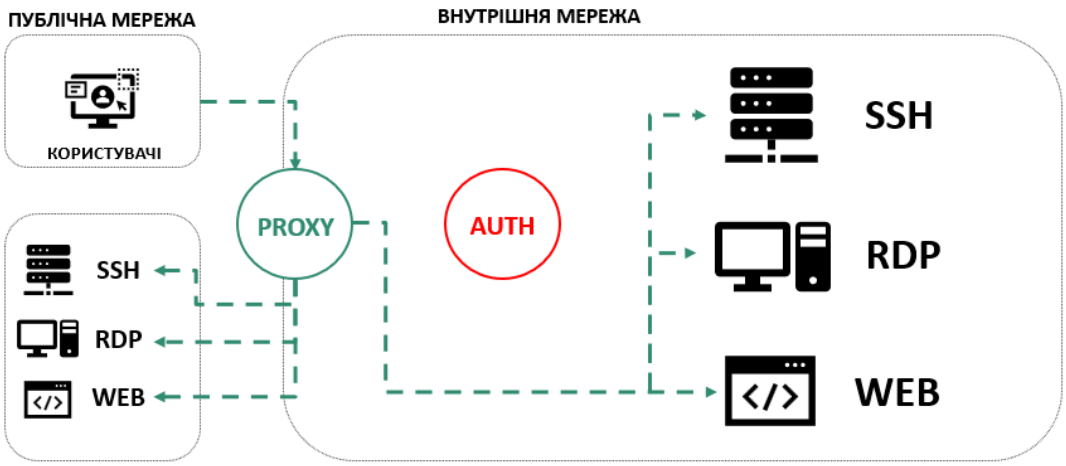
3

Порівняння моделей доступу

Модель	Гнучкість	Безпека	Легкість адміністрування	Застосування
Дискреційний контроль доступу (DAC)	Висока	Середня	Складна	Персональні комп'ютери, файлові системи
Обов'язковий контроль доступу (MAC)	Низька	Висока	Складна	Військові та урядові установи
Контроль доступу на основі ролей (RBAC)	Середня	Висока	Легка	Корпоративні системи
Контроль доступу на основі атрибутів (ABAC)	Висока	Висока	Складна	Хмарні послуги, великі організації

4

Архітектура рішення Teleport



5

Моніторинг подій на консолі

Windows Desktop Session Ended	Session b6878088-4007-4455-bdbe-c8cd786b8c29 for Windows desktop [TLeskiv@terminal-b2-bankgroup-pbank-if-ua-fb6cab90] with domain [bankgroup.pbank.if.ua] has ended for user [teleport@ideabank.ua]	2024-10-15T12:19:45.737Z	DETAILS
Session Uploaded	Recorded session [384eab95-ac99-4218-8402-a29344fb731b] has been uploaded	2024-10-15T12:19:18.421Z	DETAILS
Windows Desktop Session Started	User [teleport@ideabank.ua] started session b6878088-4007-4455-bdbe-c8cd786b8c29 on Windows desktop [TLeskiv@terminal-b2-bankgroup-pbank-if-ua-fb6cab90] with domain [bankgroup.pbank.if.ua]	2024-10-15T12:19:12.635Z	DETAILS
Certificate Issued	User certificate issued for [teleport@ideabank.ua]	2024-10-15T12:19:12.482Z	DETAILS
Windows Desktop Session Ended	Session 384eab95-ac99-4218-8402-a29344fb731b for Windows desktop [TLeskiv@terminal-b2-bankgroup-pbank-if-ua-fb6cab90] with domain [bankgroup.pbank.if.ua] has ended for user [teleport@ideabank.ua]	2024-10-15T12:19:06.283Z	DETAILS
Clipboard Data Sent	User [teleport@ideabank.ua] sent 7 bytes of clipboard data to desktop [10.10.60.3:3389]	2024-10-15T12:17:05.728824949Z	DETAILS
Windows Desktop Session Started	User [teleport@ideabank.ua] started session 384eab95-ac99-4218-8402-a29344fb731b on Windows desktop [TLeskiv@terminal-b2-bankgroup-pbank-if-ua-fb6cab90] with domain [bankgroup.pbank.if.ua]	2024-10-15T12:16:02.627Z	DETAILS

7

Рекомендації щодо використання технології PAM

1. Впровадження контролю доступу повинне бути налаштоване на основі ролей (RBAC).
2. Інтеграція з єдиним входом (SSO) та багатофакторною автентифікацією (MFA).
3. Моніторинг та аудит сесій.
4. Контроль безпеки на основі політик.
5. Створення масштабованої архітектури.
6. Періодичні перегляди доступу та аудит привілеїв.
7. Інтеграція з іншими інструментами безпеки.
8. Програми навчання та підвищення обізнаності.

8

Апробація

Результати дослідження кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Цифрова трансформація кібербезпеки» (м. Київ, 2024. Державний університет телекомунікацій)

9

Висновки

1. Досліджено основні ризики та вразливості, пов'язані з привілейованими обліковими записами.

2. Розроблено та впроваджено модель, яка дозволяє ефективно розмежувати доступ до ресурсів, дотримуючись принципу найменших привілеїв.

3. Налаштовано рольову модель доступу в Teleport, яка включає створення ролей, інтеграцію з MFA та запис сесій.

4. Розроблено рекомендації для впровадження рішення у корпоративну інфраструктуру.

ДЯКУЮ ЗА УВАГУ!