Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: Методи підвищення рівня захищеності інформаційних систем на базі Kerberos

Виконавець: студент IV курсу, групи КБ-41

_____ **Юрій СЕРПІНСЬКИЙ**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Лариса МИРУТЕНКО	

Нормоконтроль	Андрій ФЕСЕНКО	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Сергій ТОЛЮПА
«21» листопада 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)
освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-41** (група) **Серпінському Юрій Вікторовичу** (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Методи підвищення рівня захищеності інформаційних систем на базі Kerberos

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 17.11.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Будова та різновиди систем контролю доступу, засоби впровадження та функціонування систем контролю доступу, особливості процесів аутентифікації у середовищі Active Directory.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно проаналізувати механізм аутентифікації Kerberos, як один із засобів захисту; будовою та елементами систем на базі Active Directory; проаналізувати існуючі системи; визначити переваги та недоліки Kerberos та його аналогів; запропонувати методи покращення безпеки у інформаційних системах, побудованих на базі Active Directory.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблено рішення для удосконалення захищеності систем на базі Kerberos, наведені приклади та доповнення для використання в роботі підприємств малого та середнього бізнесу

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 18 листопада 2022 року

Завдання видала _____ (підпис) Лариса МИРУТЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Юрій СЕРПІНСЬКИЙ (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	21.11.2022 – 30.01.2023	*виконано*
2	Аналіз відкритих джерел	31.01.2023 – 14.02.2023	*виконано*
3	Загальний опис використання існуючих систем контролю доступу	15.02.2023 – 14.03.2023	*виконано*
4	Дослідження дискреційної моделі	15.03.2023 – 15.04.2023	*виконано*
5	Програмна реалізація спрощеної моделі дискреційного керування доступом	15.04.2023 – 15.05.2023	*виконано*
6	Формування рекомендацій щодо поєднання дискреційного керування доступом з іншими засобами захисту	16.05.2023 – 04.06.2023	*виконано*
7	Оформлення пояснювальної записки	05.06.2023 – 08.06.2023	*виконано*
8	Підготовка до захисту	09.06.2023 – 12.06.2023	*виконано*

Завдання видала _____ (підпис) Лариса МИРУТЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Юрій СЕРПІНСЬКИЙ (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 06 червня 2023 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 95 сторінок, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки, та список джерел. У пояснювальній записці кваліфікаційної роботи міститься 15 рисунків. Список використаних джерел містить 36 найменувань і займає 3 сторінки.

Об'єктом дослідження є процес автентифікації на основі Kerberos v5.

Предметом дослідження є контроль автентифікації на базі Kerberos v5.

Метою роботи є підвищення рівня захищеності інформаційних систем на базі Kerberos.

Методи дослідження: аналіз та комп’ютерне моделювання.

В роботі проведено аналіз існуючих недоліків, переваг та загалом особливостей систем автентифікації у середовищах з використанням Kerberos, а саме Active Directory. Запропоновано використання налаштувань та рішень для малих та середніх організацій, наведено основні кроки з підготовки та налаштування систем. Побудовано модель інформаційної системи, яка працює з використанням розглянутих рішень. Вона може використовуватися для наочної демонстрації.

Розроблено рекомендації щодо удосконалення надійності систем, іншими засобами захисту інформації, які за необхідності можна застосувати при роботі з конфіденційними даними.

Практична цінність: результати здійснених у кваліфікаційній роботі досліджень можуть бути використані в роботі малих та середніх організацій, що планують використання або вже використовують системи дискреційного керування доступом.

Подальші дослідження будуть спрямовані на поглиблення розуміння, вдосконалення та програмну реалізацію засобів захисту у середовищах Active Directory.

Ключові слова: середовище Active Directory, протокол Kerberos, автентифікація, суб’єкти доступу, об’єкти доступу, інформаційна система.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AC	–	Access Control;
ACL	–	Access Control List;
AD	–	Active Directory;
KDC	–	Key Distribution Center;
TGS	–	Ticket Granting Service;
TGT	–	Ticket Granting Ticket;
VLAN	–	Virtual Local Area Network;
VPN	–	Virtual Private Network;
НСД	–	Несанкціонований доступ;
ІС	–	Інформаційна система;
ІТ	–	Інформаційні технології;

ВСТУП

Актуальність обраного дослідження полягає в необхідності забезпечення високого рівня захищеності інформаційних систем у сучасному світі. Загрози та вразливості, що стикаються із інформаційними системами, стають все більшими і складнішими, вимагаючи використання ефективних методів захисту. Одним з потужних засобів захисту є протокол Kerberos, який забезпечує автентифікацію та авторизацію користувачів у розподілених системах.

Метою даної кваліфікаційної роботи є розробка та дослідження методів підвищення рівня захищеності інформаційних систем на базі протоколу Kerberos. Зокрема, будуть розглянуті аспекти, пов'язані з автентифікацією, авторизацією та керуванням ключами у контексті захисту інформаційних систем.

Для досягнення цієї мети необхідно *вирішити наступні завдання:*

- Проаналізувати існуючі методи захищеності інформаційних систем та їх недоліки.
- Детально вивчити протокол Kerberos, його принципи роботи та особливості.
- Розробити рекомендації щодо використання протоколу Kerberos для підвищення рівня захищеності інформаційних систем.
- Розробити та реалізувати програмний засіб або прототип системи, який демонструватиме застосування методів захищеності на базі Kerberos.
- Сформулювати рекомендації щодо поєднання системи на базі Kerberos з іншими методами захисту інформаційних систем.

Результати цього дослідження мають важливе значення для практичного використання інформаційних систем, оскільки вони сприятимуть підвищенню рівня захищеності даних та забезпеченню безпеки інформаційних ресурсів. Вивчення протоколу Kerberos та його застосування у практиці можуть допомогти організаціям впроваджувати ефективні методи захисту та забезпечити надійну захищеність їх інформаційних систем.

Для досягнення поставленої мети буде проведено аналіз літературних джерел, наукових статей та публікацій, що стосуються протоколу Kerberos та методів захищеності інформаційних систем. Також буде розроблено програмний засіб або прототип системи, який демонструватиме застосування протоколу Kerberos у контексті захисту інформаційних ресурсів.

Практична цінність. Висновки та рекомендації, отримані в результаті дослідження, можуть бути використані як практичний довідник для організацій, які прагнуть підвищити рівень захищеності своїх інформаційних систем. Застосування методів захищеності на базі протоколу Kerberos може забезпечити ефективну автентифікацію та авторизацію користувачів, а також зменшити ризик зламу системи та несанкціонованого доступу до даних.

У подальшому дослідженні можна розглянути розширення протоколу Kerberos та його застосування у нових контекстах, а також вивчити взаємодію з іншими системами захищеності для створення комплексного підходу до захисту інформаційних систем.

РОЗДІЛ 1
ОСНОВНІ КОНЦЕПЦІЇ ПРОТОКОЛУ KERBEROS

1.1 Проблематика поширеного рішення для комерційних середовищ Active Directory

Active Directory (AD) є важливим елементом корпоративних мереж у багатьох організаціях. Однак, на тлі потужних можливостей централізованого управління користувачами, групами, ресурсами та політиками безпеки, ця система має ряд проблем з безпекою. У комерційних середовищах, де високі вимоги до масштабованості, безпеки та управління, ці проблеми стають особливо актуальними.

Active Directory дуже поширена в корпоративному світі. За оцінками, від 85% до 95% компаній, що використовують Windows, використовують Active Directory для управління своїми ресурсами.

Використання AD настільки поширене, що приблизно 90% компаній з переліку Global Fortune 1000 використовують його як основний метод забезпечення безперебійної аутентифікації та авторизації.

Відповідно, він став основною мішенню для кібернетичних злочинців, щоб отримати доступ до привілейованих даних компанії. Опинившись в середині AD, кібернетичні злочинці можуть переміщатися між системами та отримати доступ до безлічі пропрієтарних та критичних для бізнесу даних у системах, якими керує AD. Додатково до цього, широке впровадження Office 365, який використовує AD для аутентифікації користувачів, розширило поле атаки з внутрішньої інфраструктури до хмарних середовищ.

1. Загрози зовнішнього втручання

AD є частою мішенню для кібератак, через своє важливе положення в корпоративних мережах. Незважаючи на вбудовані механізми безпеки, такі як Kerberos та LDAP з SSL, AD має відомі уразливості. Тактики атаки, як Pass-the-Hash або Golden Ticket, можуть бути використані зловмисниками для отримання несанкціонованого доступу до системи.

2. Недоліки управління доступом

AD має складну структуру прав і політик доступу, що може призвести до помилок у налаштуваннях безпеки. Необачне або некоректне надання привілеїв користувачам може стати великою уразливістю для системи.

3. Неспроможність багатьох вбудованих механізмів безпеки

Механізми безпеки, вбудовані в AD, можуть бути недостатніми для сучасних загроз. Наприклад, багато систем AD не підтримують двофакторну аутентифікацію, що є стандартом для багатьох сучасних систем. Крім того, AD не завжди надає достатньо гнучкості для реалізації специфічних політик безпеки, які можуть вимагати окремих організацій.

1.2 Еволюція протоколу Kerberos

Система Kerberos є однією з найпоширеніших та найефективніших систем аутентифікації та авторизації в комп'ютерних мережах. Ця система з'явилася в середині 1980-х років у Массачусетському технологічному інституті (MTI) та з тих пір пройшла значний шлях розвитку. Вона стала основою безпеки багатьох сучасних інформаційних систем, забезпечуючи надійну захисту від несанкціонованого доступу та атак.

Коріння системи Kerberos можна відстежити до проекту ATHENA, який був започаткований в MTI у 1983 році. Основною метою цього проекту було створення захищеної системи, яка дозволила б користувачам безпечно авторизуватися в комп'ютерній мережі та здійснювати конфіденційний обмін даними.

Перші версії системи Kerberos були розроблені Стівеном Міллером та Кліффордом Нідермейером. Вони випустили Kerberos V1, який використовувався у прототиповій мережі ATHENA. Однак, Kerberos V1 мав певні недоліки, особливо з точки зору безпеки, тому вирішено було розробити нову версію.

У 1988 році Стівен Міллер разом з Кліффордом Нідермейером та Джоном Коулсоном розробили Kerberos V2. Ця версія включала значні покращення безпеки та функціональності. Були введені криптографічні методи для захисту авторизаційної

інформації та ключів, а також було встановлено можливість здійснювати одноразову аутентифікацію. Однак, Kerberos V2 так і не отримав широкого поширення через певні недоліки, включаючи обмежену масштабованість та складність у використанні.

У 1993 році був випущений Kerberos V3, який став найбільш значущою версією системи. Kerberos V3 отримав широке визнання та став стандартом для безпеки мережі. В цій версії було внесено значні зміни та вдосконалення:

- Покращена криптографічна модель: Kerberos V3 використовує сильні криптографічні алгоритми для захисту авторизаційної інформації та ключів. Вона використовує шифрування на основі симетричного ключа та хешування для забезпечення конфіденційності та цілісності даних.
- Розширені можливості керування авторизацією: Kerberos V3 включав механізми для управління правами доступу до ресурсів та обмеженнями на рівні користувачів, груп та служб.
- Масштабованість: Kerberos V3 був розроблений з урахуванням потреб великих мереж і здатен обробляти велику кількість запитів на аутентифікацію та авторизацію.
- Підтримка cross-realm: Kerberos V3 дозволяв встановлювати довірчі стосунки між різними реалмами, що спрощувало аутентифікацію та авторизацію користувачів в розподілених середовищах.

У 2005 році був опублікований Kerberos V5 як RFC 4120. Ця версія стала основою для багатьох реалізацій Kerberos, які використовуються сьогодні. Kerberos V5 включав такі зміни та вдосконалення:

- Розширена підтримка криптографічних алгоритмів: Kerberos V5 підтримує широкий спектр криптографічних алгоритмів, що дозволяє використовувати сильні методи шифрування та хешування.
- Механізми для керування авторизацією: Введено нові механізми для керування доступом до ресурсів, включаючи розширені можливості управління правами користувачів та груп.
- Покращена безпека: Kerberos V5 пропонує додаткові заходи безпеки, включаючи захист від атак з перехопленням та підробкою токенів аутентифікації.

- Зручні механізми для адміністрування: Kerberos V5 надає розширені можливості для адміністрування та управління системою, забезпечуючи зручний інтерфейс та інструменти для налаштування, моніторингу та діагностики.

Kerberos в Microsoft Windows:

Починаючи з Windows 2000, Microsoft почала використовувати Kerberos як свій основний протокол автентифікації. Це був важливий крок для Kerberos, оскільки це розширило його вплив до великої кількості користувачів. Microsoft зробила деякі власні модифікації Kerberos, що породило деякі проблеми сумісності з реалізаціями Kerberos на інших платформах. Проте ці проблеми були вирішені з часом, і сьогодні Kerberos відіграє ключову роль у більшості Windows-середовищ.

Сучасний Kerberos:

Сьогодні Kerberos залишається одним з найбільш важливих стандартів для безпечної автентифікації в розподілених системах. З часом він був адаптований для використання в багатьох різних операційних системах і додатках, що робить його дуже гнучким інструментом для інформаційної безпеки. Однак, незважаючи на успіх, Kerberos все ще має деякі недоліки та вразливості. Для вирішення цих проблем він продовжує розвиватися.

Майбутнє Kerberos:

Майбутнє Kerberos може включати в себе більше інтеграцій з іншими технологіями безпеки та більше покращень в областях, де він зараз виявляється слабким. Наприклад, може бути внесено покращення у відношеннях із управлінням цифровими сертифікатами або у використанні біометричних технологій для автентифікації. З огляду на те, що зростання обсягу і складності цифрових систем продовжується, Kerberos, безсумнівно, буде продовжувати адаптуватися та розвиватися, щоб відповідати цим викликам.

У підсумку, Kerberos є прекрасним прикладом того, як важливо розвиватися та адаптуватися в сфері інформаційної безпеки. Від свого створення в 1980-х роках і до сьогоднішнього дня, Kerberos втілює неперервний процес вдосконалення та адаптації до змінюваних умов і нових викликів. І хоча майбутнє може принести нові виклики

та проблеми, Kerberos, ймовірно, продовжить бути ключовим компонентом в сфері інформаційної безпеки.

1.3 Основні компоненти та структура системи Kerberos

Kerberos - це протокол мережевої автентифікації, який використовує концепцію "довірчих третіх сторін" для забезпечення безпечного аутентифікування користувачів в розподіленій мережі. Він розроблений в Массачусетському технологічному інституті (MIT) і використовує криптографічні білети для встановлення та підтвердження ідентичності користувачів. Основні компоненти та структура Kerberos є центральними в його роботі та можуть бути описані наступним чином:

1. Клієнт (Client)

У системі Kerberos, клієнт (або Kerberos-клієнт) є сутністю, яка взаємодіє з іншими компонентами системи для отримання аутентифікації та доступу до ресурсів в мережі. Клієнт є користувачем або процесом, який виконує запити на аутентифікацію та авторизацію в системі Kerberos.

Клієнт взаємодіє з двома основними компонентами системи Kerberos: Key Distribution Center (KDC) та ресурсами мережі. KDC є центральним сервером, який відповідає за видання та керування ключами аутентифікації. Клієнт взаємодіє з KDC для отримання квитка (токен) аутентифікації, який підтверджує його ідентичність.

Після отримання квитка аутентифікації, клієнт може використовувати його для доступу до ресурсів у мережі, таких як файли, друкарки або додатки. Клієнт надсилає квиток разом з запитом на доступ до ресурсу. Ресурсний сервер перевіряє цей квиток, використовуючи спільну довіру до KDC, і надає клієнту відповідний доступ до ресурсу.

Клієнт Kerberos використовує криптографічні методи для захисту аутентифікаційної інформації та ключів. Він взаємодіє з KDC за допомогою захищених каналів зв'язку для запобігання перехоплення та підробки даних.

Клієнт може бути реалізований у вигляді програмного забезпечення, що встановлюється на комп'ютері користувача, або вбудований у операційну систему.

Він надає інтерфейс для введення облікових даних користувача та ініціює процес аутентифікації в системі Kerberos.

В цілому, клієнт в системі Kerberos є основною сутністю, яка взаємодіє з KDC та ресурсами для отримання безпечного доступу до ресурсів в мережі, забезпечуючи аутентифікацію та авторизацію користувачів.

2. Сервер аутентифікації (KDC)

Сервер аутентифікації в контексті Kerberos відомий як Key Distribution Center (KDC). Це центральний сервер, який виконує ключову роль в системі Kerberos, забезпечуючи аутентифікацію та керування ключами для користувачів і ресурсів в мережі.

Key Distribution Center складається з двох компонентів:

1) Authentication Server (AS): Цей компонент є першим контактним пунктом для клієнтів. Коли клієнт намагається аутентифікуватися в системі Kerberos, він звертається до AS, вказуючи своє ім'я користувача. AS перевіряє ім'я користувача, генерує випадковий ключ сесії та шифрує його за допомогою спільного ключа (пароля) користувача. Зашифрований ключ сесії відправляється клієнту разом з токеном аутентифікації.

2) Ticket-Granting Server (TGS): Цей компонент є відповідальним за видачу квитків (токенів) аутентифікації для доступу клієнтів до ресурсів в мережі. Клієнт, маючи токен аутентифікації від AS, звертається до TGS із запитом на отримання квитка для певного ресурсу. TGS перевіряє аутентичність клієнта та видає йому квиток (токен) аутентифікації для цього ресурсу. Клієнт може використовувати цей квиток для отримання доступу до ресурсу без потреби повторно аутентифікуватися.

Сервер аутентифікації (KDC) забезпечує безпеку процесу аутентифікації та керування ключами у системі Kerberos. Він використовує криптографічні методи для захисту передачі даних, включаючи шифрування та хешування, що забезпечує конфіденційність та цілісність інформації.

Сервер аутентифікації є центральним елементом системи Kerberos, від якого залежить успішність процесу аутентифікації та доступу до ресурсів.

3. Служба (Service)

У контексті Kerberos, служба (Service) відноситься до ресурсу або послуги, до якої користувачі можуть отримати доступ у мережі. Служби можуть включати файли, друкарки, бази даних, веб-сервери та інші ресурси, до яких необхідно аутентифікуватися та авторизуватися для отримання доступу.

У системі Kerberos, служби визначаються у вигляді принципалів (principals). Кожна служба має свій принципал, що ідентифікує її в мережі. Принципал складається з імені служби та імені хоста (hostname), який вказує на конкретний сервер, на якому розташована служба. Наприклад, для веб-сервера з ім'ям "webserver.example.com", принципал може мати вигляд "HTTP/webserver.example.com".

Користувачі, які бажають отримати доступ до певної служби, повинні пройти процес аутентифікації в системі Kerberos та отримати відповідний квиток (токен) аутентифікації. Квиток містить інформацію про аутентифікованого користувача та його права доступу до певних служб.

Після отримання квитка аутентифікації, користувач може використовувати його для запиту доступу до служби. Користувач надсилає квиток аутентифікації до служби, яка перевіряє його на валідність та довіру до сервера аутентифікації. Якщо перевірка пройдена успішно, служба надає користувачеві доступ до відповідних ресурсів або функціональності.

Система Kerberos забезпечує безпеку комунікації між користувачем та службою шляхом використання захищених каналів зв'язку та криптографічних методів шифрування. Це дозволяє запобігти перехопленню або модифікації даних під час передачі.

Отже, служба в системі Kerberos представляє ресурс або послугу, до якої користувачі можуть отримати доступ шляхом проходження процесу аутентифікації та отримання відповідного квитка аутентифікації.

4. Білети (Tickets)

В контексті системи Kerberos, білети (tickets) є криптографічними об'єктами, що використовуються для аутентифікації та авторизації користувачів. Вони містять інформацію про ідентифікацію користувача та його права доступу до ресурсів в

мережі. В системі Kerberos існує кілька видів білетів з різними особливостями та призначеннями. Основними видами білетів є:

- Ticket-Granting Ticket (TGT):

TGT є основним білетом, який видається після успішної аутентифікації користувача в системі Kerberos. Він містить інформацію про ідентифікацію користувача (принципала) та його ключ сесії. TGT використовується для отримання інших білетів без повторної аутентифікації. Користувач зберігає TGT локально та використовує його для отримання Service Ticket.

- Service Ticket:

Service Ticket видається користувачу після успішної аутентифікації та наявності TGT. Він містить інформацію про ідентифікацію користувача та права доступу до певної служби (принципала). Service Ticket використовується для отримання доступу до ресурсів, контроль яких здійснюється системою Kerberos.

- Proxy Ticket:

Proxy Ticket дозволяє користувачам делегувати свої права доступу іншим користувачам або службам. Він дає можливість третім сторонам виконувати дії від імені користувача, який делегує свої права. Proxy Ticket може бути використаний для подальшої аутентифікації та отримання Service Ticket без повторної аутентифікації.

Кожен білет містить криптографічно захищену інформацію, яка забезпечує конфіденційність і цілісність даних. Білети шифруються за допомогою ключів шифрування, які обмінюються між користувачем, KDC та службою. Це забезпечує безпеку передачі та перевірку автентичності білетів.

Особливістю білетів у системі Kerberos є їхній обмежений термін життя. Білети мають обмежений час дії (TTL), після закінчення якого вони стають недійсними. Це дозволяє зменшити ризик використання старих або скомпрометованих білетів.

Усі білети в системі Kerberos використовуються для забезпечення безпеки аутентифікації та авторизації в мережі, забезпечуючи захист від несанкціонованого доступу та зловживань. Кожен вид білета має свої особливості та використовується в різних етапах процесу аутентифікації та доступу до ресурсів.

5. Криптографічні ключі

Криптографічні ключі в контексті Kerberos є секретними значеннями, що використовуються для захисту комунікації, шифрування та розшифрування даних, а також для перевірки цілісності та автентичності інформації. У системі Kerberos криптографічні ключі грають важливу роль у процесі аутентифікації та захисту даних.

Криптографічні ключі включають наступні типи:

- Ключі користувача (User Keys): Кожен користувач у системі Kerberos має свій унікальний ключ, відомий як ключ користувача. Цей ключ використовується для захисту білетів, передачі даних та ідентифікації користувача під час процесу аутентифікації.
- Ключі служби (Service Keys): Кожна служба також має свій унікальний ключ, відомий як ключ служби. Цей ключ використовується для шифрування та розшифрування Service Ticket, а також для перевірки автентичності та цілісності даних, що передаються між клієнтом і службою.
- Ключі KDC (KDC Keys): Ключі KDC використовуються для захисту комунікації між сервером аутентифікації (KDC) і клієнтами. Ці ключі використовуються для шифрування білетів, перевірки автентичності та захисту конфіденційності даних, що передаються під час процесу аутентифікації.
- Криптографічні ключі в системі Kerberos є секретними і відомі лише власникам або відповідним серверам. Вони використовуються для розшифрування та шифрування білетів, що передаються між різними компонентами системи Kerberos. Ключі допомагають забезпечити конфіденційність, цілісність та автентичність даних, що передаються під час процесу аутентифікації і авторизації.

6. Сховище даних

В контексті Kerberos база даних (Database) використовується для зберігання та управління інформацією, необхідною для процесу аутентифікації та авторизації користувачів.

База даних Kerberos містить наступну інформацію:

- Користувачі (Users): База даних містить дані про користувачів системи Kerberos, включаючи їх ідентифікатори, паролі та інші атрибути. Ця інформація

використовується для перевірки правильності введеного пароля під час процесу аутентифікації.

- Служби (Services): База даних містить також дані про служби, до яких користувачі можуть отримати доступ. Ця інформація включає ідентифікатори служб (Service Principal Names - SPN) та відповідні ключі служб для шифрування та розшифрування білетів.
- Криптографічні ключі (Cryptographic Keys): База даних Kerberos зберігає криптографічні ключі, необхідні для захисту комунікації та шифрування білетів. Ці ключі використовуються для шифрування та розшифрування білетів, перевірки автентичності та цілісності даних.
- Журнали (Logs): База даних може містити журнали подій, які реєструють дії, пов'язані з процесом аутентифікації та авторизації. Ці журнали використовуються для моніторингу та аудиту безпеки системи Kerberos.

База даних Kerberos може бути реалізована за допомогою різних технологій, таких як реляційні бази даних або директорії, які забезпечують зберігання та ефективний доступ до інформації, необхідної для процесу аутентифікації та авторизації в системі Kerberos.

7. Realm (Реалм)

В контексті Kerberos, Realm (реалм) вказує на ідентифікаційний домен або ім'я області, в якій діє система Kerberos. Realm є частиною імені принципала (Principal), що ідентифікує об'єкти в системі Kerberos, такі як користувачі або служби.

Realm використовується для ідентифікації та відокремлення різних логічних областей або доменів у мережі. Кожен домен або організаційна одиниця може мати свій власний Realm, що відповідає його ідентифікаційній просторі.

Realm зазвичай відповідає доменному імені DNS (Domain Name System) або іншому ідентифікатору області. Наприклад, в домені "example.com" Realm може бути встановлено як "EXAMPLE.COM".

Realm використовується як частина імені принципала (Principal Name), яке включає ім'я користувача або служби разом з Realm. Наприклад, принципал може мати ім'я "user@example.com" або "service/example.com".

У контексті Kerberos, Realm використовується для визначення меж аутентифікаційного довіреного простору. Клієнти та сервери, що належать до одного Realm, можуть взаємодіяти один з одним без необхідності повторної аутентифікації.

Користувачі та служби, які належать до різних Realm, можуть спілкуватися та отримувати доступ до ресурсів за умови, що між відповідними Realm встановлена довіра і налагоджена відповідна взаємодія між Керуючими контролерами доменів.

8. Протокол

В контексті Kerberos, протокол відноситься до набору правил та процедур, які використовуються для обміну даними та взаємодії між різними компонентами системи Kerberos. Протокол визначає формати повідомлень, методи шифрування та алгоритми для забезпечення безпеки під час передачі даних.

У системі Kerberos використовуються різні протоколи для взаємодії між різними сторонами:

- Kerberos Authentication Protocol (також відомий як AS-REQ/AS-REP Protocol): Цей протокол використовується для аутентифікації користувача в системі Kerberos. Клієнт ініціює запит до сервера аутентифікації (AS) та отримує відповідь, що містить білет, який дозволяє отримати доступ до Ticket-Granting Server (TGS).
- Ticket-Granting Ticket (TGT) Exchange Protocol: Цей протокол використовується для обміну білетами між клієнтом і TGS. Клієнт запитує TGS про Service Ticket для певної служби, представляючи свій TGT. TGS генерує та надсилає Service Ticket клієнту, що дозволяє отримати доступ до служби.
- Kerberos Ticket-Granting Service (TG-S) Exchange Protocol: Цей протокол використовується для взаємодії між клієнтом і TG-S. Клієнт використовує Service Ticket для отримання доступу до TG-S, що дозволяє йому отримати Service Ticket для конкретних служб.
- Application Service Exchange Protocol: Цей протокол використовується для взаємодії між клієнтом та службою. Клієнт передає Service Ticket службі, яка його розшифровує та перевіряє права доступу клієнта до ресурсу. Після перевірки служба надає клієнту доступ до ресурсу або виконує необхідну функціональність.

Ці протоколи використовуються для забезпечення безпеки та автентифікації в системі Kerberos, зокрема для обміну білетами, перевірки цілісності даних та шифрування комунікації. Кожен протокол має свої властивості та процедури, які дозволяють ефективно та безпечно здійснювати аутентифікацію та авторизацію в системі Kerberos.

1.4 Процес автентифікації в системі Kerberos

Процес аутентифікації (рис. 1.1) за допомогою системи Kerberos складається з кількох кроків, які включають взаємодію між користувачем, сервером аутентифікації (KDC) та службою.

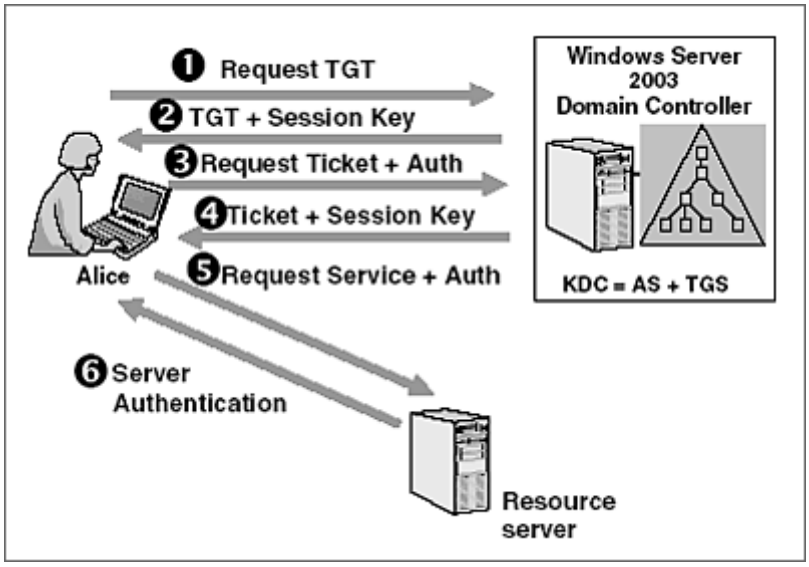

Рисунок 1.1 – Схема процесу автентифікації в системі Kerberos

Ось детальний опис кожного кроку:

Крок 1: Аутентифікація користувача

- Користувач вводить своє ім'я користувача і пароль на клієнтській стороні.
- Клієнт формує запит на аутентифікацію і передає його до сервера аутентифікації (AS) KDC.

Крок 2: Видання Ticket-Granting Ticket (TGT)

- AS перевіряє ім'я користувача і пароль, щоб переконатися, що вони правильні.

- Після успішної перевірки, AS генерує TGT, який містить інформацію про ідентифікацію користувача і ключ сесії.
- AS зашифровує TGT з використанням ключа користувача та відправляє його назад до клієнта.

Крок 3: Взаємодія з Ticket-Granting Server (TGS)

- Клієнт зберігає отриманий TGT локально і використовує його для подальшої аутентифікації.
- Клієнт формує запит до TGS, включаючи TGT і ідентифікатор служби (Service Principal Name - SPN) ресурсу, до якого користувач хоче отримати доступ.
- Клієнт передає запит до TGS KDC.

Крок 4: Видання Service Ticket

- TGS перевіряє автентичність TGT та права доступу користувача до запитуваної служби.
- Якщо перевірка пройшла успішно, TGS генерує Service Ticket для користувача, який містить інформацію про ідентифікацію користувача та права доступу до ресурсу.
- TGS зашифровує Service Ticket з використанням ключа ресурсу та відправляє його назад до клієнта.

Крок 5: Взаємодія зі службою

- Клієнт отримує зашифрований Service Ticket і використовує його для запиту доступу до ресурсу.
- Клієнт передає зашифрований Service Ticket разом з запитом до служби.

Крок 6: Підтвердження та отримання доступу

- Служба отримує зашифрований Service Ticket та розшифровує його, використовуючи свій ключ.
- Служба перевіряє інформацію про ідентифікацію користувача та права доступу, вказані в Service Ticket.
- Якщо перевірка пройшла успішно, служба підтверджує ідентичність користувача та надає доступ до ресурсу.

- Процес аутентифікації Kerberos забезпечує безпеку шляхом використання шифрування та обміну криптографічних ключів між клієнтом, KDC та службою (рис. 1.2). Всі комунікації між цими елементами здійснюються за допомогою захищених каналів зв'язку, що запобігає перехопленню та зловживанню даних під час передачі.

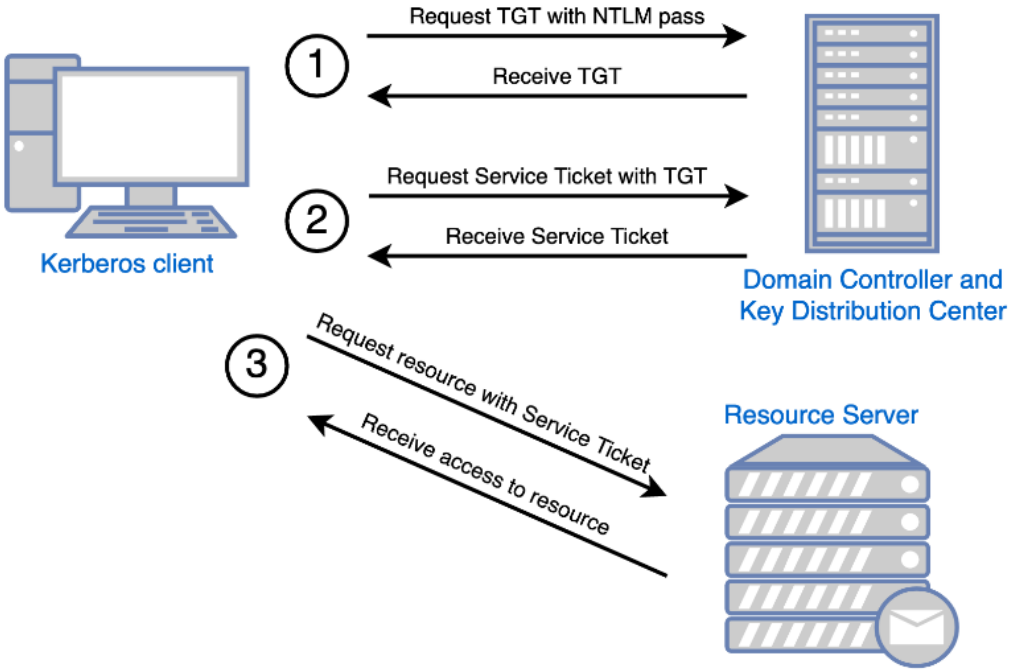

Рисунок 1.2 – Схема авторизації Kerberos

У випадку, коли авторизується не користувач, а служба, процес аутентифікації за допомогою Kerberos включає наступні кроки:

Крок 1: Реєстрація служби

- Служба реєструється в системі Kerberos шляхом створення відповідного принципала (Service Principal) для ідентифікації служби в мережі. Принципал служби складається з імені служби та імені хоста, на якому розташована служба.

Крок 2: Видання Service Key

- Після успішної реєстрації, KDC генерує спільний ключ (Service Key) для служби та зберігає його в безпечному сховищі. Цей ключ буде використовуватись для шифрування та перевірки автентичності білетів служби.

Крок 3: Отримання Service Ticket

- Коли клієнт (користувач або інша служба) бажає отримати доступ до конкретної служби, він формує запит на отримання Service Ticket.
- Клієнт передає запит на отримання Service Ticket до TGS, вказуючи ідентифікатор служби (Service Principal Name - SPN) та свій TGT.

Крок 4: Перевірка запиту та видача Service Ticket

- TGS перевіряє автентичність TGT, що міститься в запиті, та права доступу клієнта до запитуваної служби.
- Якщо перевірка пройшла успішно, TGS генерує Service Ticket для служби, який містить інформацію про ідентифікацію служби та права доступу до ресурсів.
- TGS зашифровує Service Ticket з використанням Service Key та передає його назад до клієнта.

Крок 5: Взаємодія зі службою

- Клієнт отримує зашифрований Service Ticket і використовує його для запиту доступу до служби.
- Клієнт передає запит на доступ до служби разом із зашифрованим Service Ticket до служби.

Крок 6: Підтвердження та отримання доступу

- Служба отримує зашифрований Service Ticket та розшифровує його, використовуючи свій Service Key.
- Служба перевіряє інформацію про ідентифікацію служби та права доступу, вказані в Service Ticket.
- Якщо перевірка пройшла успішно, служба підтверджує свою ідентичність та надає клієнту доступ до ресурсу або виконання необхідної функціональності.
- Процес аутентифікації служби використовує ті ж принципи та механізми, що й аутентифікація користувача, проте здійснюється між службою, KDC та клієнтом. Важливим елементом є використання спільного ключа (Service Key), що дозволяє забезпечити конфіденційність та автентичність білетів, що передаються між сторонами.

Крім користувачів та служб, система Kerberos дозволяє іншим суб'єктам, таким як комп'ютери, програми та сервіси, авторизуватись за допомогою Kerberos. Це дає можливість розширити застосування Kerberos на різні типи об'єктів і забезпечити безпеку та контроль доступу до ресурсів:

- Комп'ютери (Hosts): Комп'ютери можуть використовувати Kerberos для отримання аутентифікації та отримання доступу до мережевих ресурсів. Комп'ютери можуть бути авторизовані як принципали і отримувати Service Ticket для взаємодії з іншими службами або ресурсами у мережі. Наприклад, комп'ютер, який виконує роль файлового сервера, може використовувати Kerberos для отримання авторизації та доступу до файлів, забезпечуючи безпеку та цілісність даних.
- Програми та сервіси: Програми та сервіси можуть також використовувати Kerberos для отримання авторизації та отримання доступу до ресурсів. Наприклад, веб-сервери, сервери баз даних або інші програми можуть авторизуватись за допомогою Kerberos для отримання доступу до обмежених ресурсів у мережі. Це дозволяє забезпечити захищену комунікацію та обмін даними між клієнтами та серверами, засновані на Kerberos.
- Додаткові протоколи: Kerberos може використовуватись іншими протоколами або механізмами для авторизації та обміну даними. Наприклад, протокол LDAP (Lightweight Directory Access Protocol) може використовувати Kerberos для аутентифікації користувачів або контролю доступу до каталогів. Це дозволяє забезпечити єдину точку входу та централізований контроль доступу до даних у розподіленому середовищі.

У цих випадках, коли авторизується не користувач або служба, а інший суб'єкт, той самий процес аутентифікації та обмін білетами залишається, але використовуються різні типи принципалів та ідентифікаторів для представлення цих суб'єктів. Наприклад, комп'ютер може бути ідентифікований як принципал за допомогою імені хосту, а програма або сервіс може мати своє власне ім'я принципала. В процесі аутентифікації та авторизації використовуються відповідні ключі та білети для забезпечення безпеки та цілісності даних.

Крім того, права доступу та обмеження можуть бути налаштовані відповідно до вимог конкретного суб'єкта, який авторизується. Це дозволяє гнучко налаштовувати систему Kerberos для використання в різних сценаріях, що вимагають авторизації широкого спектру суб'єктів.

1.5 Протоколи і ключі шифрування в Kerberos

Kerberos - це система аутентифікації, яка використовує криптографічні протоколи і ключі для забезпечення безпечної ідентифікації користувачів в розподіленій мережі. Для розуміння того, як Kerberos забезпечує безпеку, важливо розглянути декілька ключових аспектів його роботи: протоколи, які він використовує, і ключі шифрування, які він генерує.

Протокол Kerberos розроблено таким чином, щоб вирішити проблему безпечного встановлення ідентичності в ненадійних мережах. Основний протокол Kerberos складається з двох основних частин: протоколу аутентифікації і протоколу видачі білетів.

- Протокол аутентифікації: Протокол аутентифікації використовується для перевірки ідентичності клієнта. Коли клієнт спочатку з'єднується з системою Kerberos, він надсилає запит до сервера аутентифікації, включаючи своє ім'я користувача. Сервер аутентифікації перевіряє цей запит і, якщо ім'я користувача вірне, створює "білет автентифікації" (Ticket-Granting Ticket, TGT) і повертає його клієнту.
- Протокол видачі білетів: Після того, як клієнт отримав TGT від сервера аутентифікації, він може використовувати цей білет, щоб звернутися до сервера видачі білетів (Ticket Granting Server, TGS) та отримати "білет служби" (Service Ticket, ST) для доступу до конкретної служби. TGS перевіряє TGT клієнта і видає ST, який клієнт може використовувати для отримання доступу до служби.

Ключі шифрування в системі Kerberos є важливою складовою для забезпечення безпеки та конфіденційності під час обміну даними. В цій статті розглянемо різні типи ключів шифрування, їх особливості, види та недоліки.

У системі Kerberos використовуються два основних типи ключів:

- Майстер-ключ (Master Key): Майстер-ключ є секретним ключем, який використовується для шифрування та розшифрування інших ключів. Він зберігається тільки на Керуючих контролерах домену (KDC) і використовується для генерації та керування іншими ключами у системі Kerberos. Майстер-ключ дуже важливий з точки зору безпеки, і його необхідно захищати від несанкціонованого доступу.
- Сеансовий ключ (Session Key): Сеансовий ключ є тимчасовим ключем, який генерується при кожному новому сеансі аутентифікації між клієнтом та сервером. Він використовується для шифрування та розшифрування даних, що передаються між сторонами. Сеансовий ключ генерується на Керуючому контролері домену після успішної аутентифікації та передається клієнту та службі для подальшого використання під час сеансу.

Види ключів шифрування

У системі Kerberos використовуються різні види ключів шифрування для різних цілей:

- Ключі шифрування користувачів: Кожен користувач має свій власний ключ шифрування, який використовується для захищеного обміну даними між клієнтом та сервером. Цей ключ генерується на основі пароля користувача та інших факторів аутентифікації.
- Ключі шифрування служб: Кожна служба також має свій власний ключ шифрування, який використовується для захищеного обміну даними між клієнтом та службою. Цей ключ генерується на основі спільного секрету між Керуючим контролером домену та службою.
- Ключі шифрування TGT: Ticket-Granting Ticket (TGT) також має свій власний ключ шифрування. Цей ключ використовується для захищеного шифрування та передачі TGT між Керуючим контролером домену та клієнтом.

Особливості ключів шифрування в Kerberos:

- Ключі шифрування використовуються тільки для захищеного обміну даними та забезпечення конфіденційності.

- Ключі шифрування генеруються випадковим чином та піддаються криптографічному захисту.
- Ключі шифрування змінюються періодично або при кожному новому сеансі, що допомагає запобігти зламу ключа та підвищує безпеку системи.

Недоліки ключів шифрування в Kerberos:

- Якщо майстер-ключ потрапляє в руки зловмисника, це може призвести до компрометації всіх інших ключів у системі Kerberos.
- Велика кількість активних сеансів та ключів шифрування може призвести до складнощів у керуванні та обслуговуванні системи.
- Зміна ключів шифрування може викликати деякий накладний розхід та вимагати оновлення усіх сторін, які використовують систему Kerberos.

Загалом, ключі шифрування є важливою складовою безпеки системи Kerberos, забезпечуючи конфіденційність та захист даних під час обміну. Важливо дотримуватись рекомендацій з керування ключами та забезпечувати їх безпеку, щоб уникнути можливих атак та компрометації системи.

1.6 Використання Kerberos в сучасних інформаційних системах

Kepberos займає центральне місце в сучасних інформаційних системах, особливо в тих, що використовують розподілені мережі. Цей протокол аутентифікації є основним стандартом для безпечної ідентифікації користувачів в розподілених системах, включаючи Інтернет та корпоративні мережі.

Роль Kerberos в операційних системах

Kerberos виконує кілька важливих функцій в операційних системах:

- Аутентифікація користувачів: Kerberos забезпечує механізми аутентифікації користувачів, що дозволяє перевіряти їхню ідентичність перед наданням доступу до ресурсів. Він забезпечує конфіденційність, цілісність та недоступність під час передачі облікових даних.

- Керування авторизацією: Kerberos дозволяє встановлювати механізми авторизації, що визначають, які ресурси та послуги можуть бути доступними для користувачів після аутентифікації.
- Шифрування та безпека даних: Kerberos використовує механізми шифрування для захисту конфіденційності даних під час їх передачі між клієнтом та сервером. Це допомагає запобігти несанкціонованому доступу до чутливої інформації.

Переваги системи Kerberos наведено на рис. 1.3:

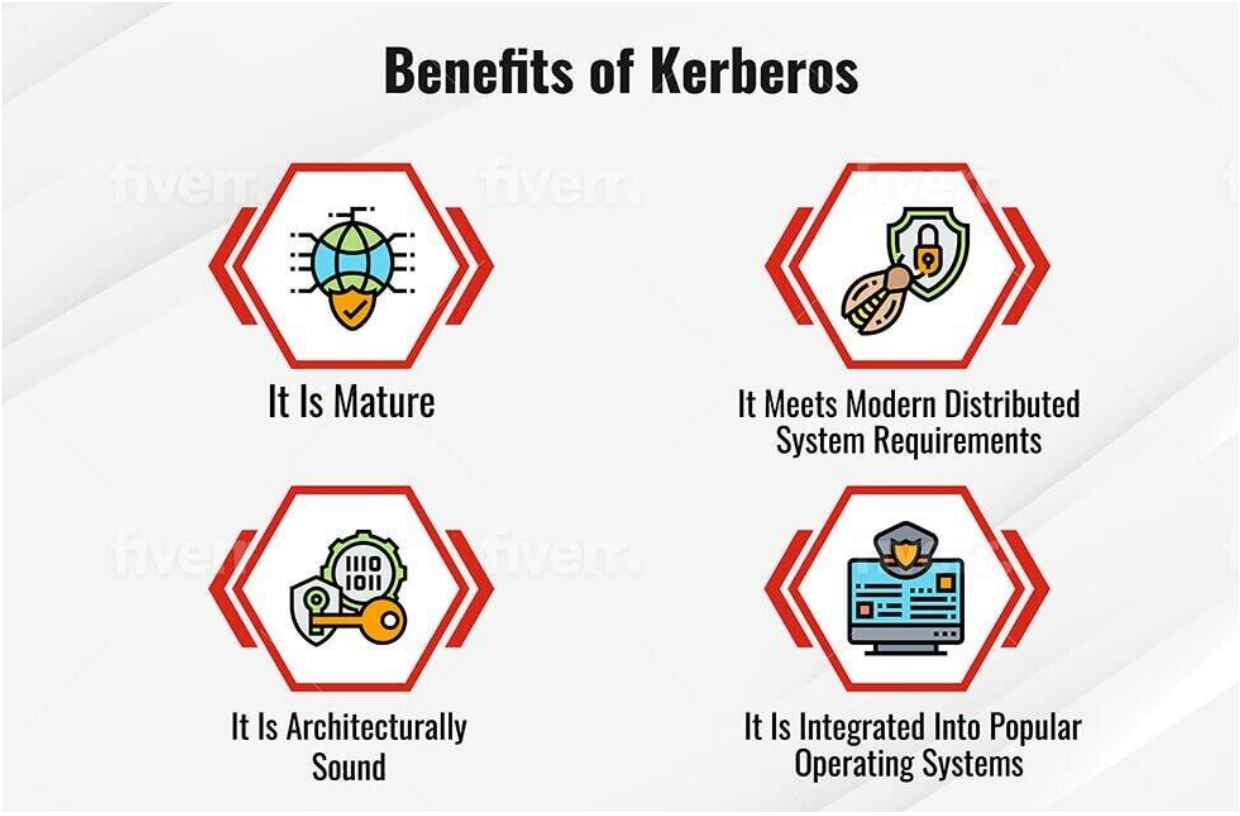

Рисунок 1.3 – Переваги системи Kerberos

Цінність та важливість Kerberos

Kerberos має переваги (рис. 1.3), цінність і важливість в операційних системах з наступних причин:

- Забезпечення безпеки: Kerberos дозволяє забезпечити безпеку системи, мінімізуючи ризик несанкціонованого доступу та зламу паролів. Він використовує сильне шифрування та ідентифікацію для захисту важливої інформації та даних.
- Централізована аутентифікація: Kerberos надає централізовану систему аутентифікації, де користувачі можуть використовувати один набір облікових даних

для доступу до різних ресурсів. Це забезпечує зручність та ефективність управління аутентифікацією.

- Переносимість та інтеграція: Kerberos є стандартом промисловості і підтримується багатьма операційними системами та додатками. Це робить його важливим інструментом для переносимості даних та інтеграції різних систем.

Поширеність Kerberos та статистичні дані

Kerberos широко використовується у різних сферах, включаючи корпоративні мережі, урядові установи та академічні середовища. Деякі статистичні дані про поширеність Kerberos:

За даними Netcraft, у 2020 році понад 33% з 99 тис. доменів Fortune 1000 використовували Kerberos для автентифікації та захисту мережі.

У розподілі операційних систем, Kerberos підтримується в операційних системах, таких як Windows Server, Linux, macOS та інші, що робить його доступним для багатьох організацій.

Крім того, Kerberos використовується у багатьох великих установах, таких як урядові агентства, банки, освітні заклади та інші організації, де безпека та конфіденційність даних мають велике значення.

Найвідоміші аналоги Kerberos

Хоча Kerberos є широко використовуваним протоколом автентифікації, існують аналоги, які також можуть бути використані для забезпечення безпеки та автентифікації, зокрема:

- Security Assertion Markup Language (SAML): SAML - це XML-протокол для обміну даними аутентифікації та авторизації між різними безпековими системами. Він широко використовується в хмарних сервісах та федерації ідентичності.

- OAuth: OAuth - це відкритий стандарт авторизації, який дозволяє користувачам надавати доступ до своїх ресурсів без розкриття свого пароля. Це широко використовується в розподілених системах та додатках соціальних мереж.

- OpenID Connect: OpenID Connect - це розширення протоколу автентифікації OAuth 2.0, яке додає можливості ідентифікації та обміну даними

користувачів між сторонами. Воно широко використовується в веб-додатках та системах одноразової аутентифікації.

Причини вибору Kerberos

Kerberos має кілька переваг, які роблять його привабливим для вибору у багатьох організацій:

- Загальноприйнятий стандарт: Kerberos є стандартом промисловості і підтримується багатьма вендорами та платформами, що робить його сумісним з різними операційними системами та додатками.
- Безпека та конфіденційність: Kerberos використовує потужні механізми шифрування для захисту даних під час обміну. Він також забезпечує міцну аутентифікацію користувачів, що дозволяє перевірити їхню ідентичність перед наданням доступу.
- Централізоване управління: Kerberos надає централізовану систему управління аутентифікацією та авторизацією, що спрощує адміністрування та підтримку.
- Широке застосування: Kerberos може бути використаний для різних сценаріїв, включаючи корпоративні мережі, хмарні сервіси, веб-додатки та багатокористувацькі середовища.

Веб-служби можуть використовувати Kerberos для аутентифікації користувачів, що надають свої власні облікові дані, або для аутентифікації веб-служби перед іншими веб-службами. Зазвичай Kerberos використовується в корпоративних або великих мережевих середовищах, де безпека є важливою пріоритетом.

Kerberos широко використовується в промисловості, особливо в сферах, де необхідний високий рівень безпеки, таких як фінансові служби, урядові організації, та в області здоров'я.

Поширеність Kerberos у веб-службах та статистичні дані

Kerberos є широко використовуваним протоколом аутентифікації у веб-службах. За даними веб-статистики Netcraft, у 2020 році понад 36% з 99 тис. доменів Fortune 1000 використовували Kerberos для аутентифікації та захисту веб-служб.

У розподілі веб-серверів, Kerberos підтримується веб-серверами, такими як Apache, Nginx, Microsoft IIS та інші, що робить його доступним для використання в багатьох середовищах.

Багато веб-додатків та фреймворків, таких як Java Spring, .NET Framework, Django тощо, підтримують Kerberos як механізм аутентифікації.

У сучасних базах даних, де безпека та захист інформації є критичними аспектами, Kerberos використовується для забезпечення безпеки, аутентифікації та контролю доступу. У цій статті розглянемо використання Kerberos у базах даних, переваги його застосування та особливості інтеграції з різними базами даних.

Забезпечення безпеки даних: Kerberos забезпечує високий рівень безпеки у базах даних шляхом застосування сильної аутентифікації та шифрування даних. Він дозволяє перевіряти ідентичність користувачів та контролювати їх доступ до конфіденційної інформації.

- Централізоване управління доступом: Kerberos дозволяє встановити єдиний централізований сервер аутентифікації для бази даних. Це спрощує управління обліковими записами користувачів та контроль їх доступу до базових об'єктів і даних.
- Інтеграція з базами даних: Kerberos може бути легко інтегрований з різними базами даних, такими як Oracle, MySQL, PostgreSQL та іншими. Багато баз даних підтримують механізми аутентифікації Kerberos та можуть використовувати його для контролю доступу до даних.
- Одноразова аутентифікація: Kerberos дозволяє встановити систему одноразової аутентифікації для баз даних. Користувачі можуть автентифікуватись один раз за допомогою своїх облікових даних Kerberos, а потім отримати доступ до різних баз даних без повторної аутентифікації.
- Аудит та моніторинг: Kerberos дозволяє проводити аудит та моніторинг дій користувачів у базах даних. Це допомагає виявляти можливі порушення безпеки та надає можливість вжити відповідних заходів для їх запобігання.
- Підтримка віртуалізації: Kerberos може бути успішно використаний у віртуальних середовищах, де бази даних можуть бути розподілені на різні сервери або

контейнери. Це дозволяє забезпечити безпеку та аутентифікацію для баз даних у розподілених середовищах.

Існують деякі статистичні дані, які підтверджують значення та поширеність використання Kerberos у базах даних:

- За даними Microsoft, використання Kerberos як механізму аутентифікації у базі даних SQL Server має кілька переваг, таких як зменшення навантаження на сервер та покращення безпеки даних. У випадку багатьох клієнтів, що підключаються до бази даних, використання Kerberos може бути більш ефективним, ніж інші методи аутентифікації.
- Згідно з дослідженням IDC, Kerberos є одним з найпоширеніших протоколів аутентифікації у великих корпоративних базах даних, де безпека та захист інформації є ключовими факторами.
- У звіті Database Trends and Applications, Kerberos названий одним з найефективніших протоколів аутентифікації у базах даних для забезпечення безпеки та захисту конфіденційної інформації.

Усі ці статистичні дані підтверджують значення та ефективність використання Kerberos у базах даних для забезпечення безпеки, аутентифікації та контролю доступу до інформації.

Kerberos є комп'ютерним мережевим протоколом, єдним з ключових стандартів автентифікації в мережах, який використовує симетричне шифрування для обміну безпечними ключами. Це робить Kerberos цінним інструментом для використання в хмарних середовищах, зокрема Azure Active Directory (Azure AD) (рис. 1.4).

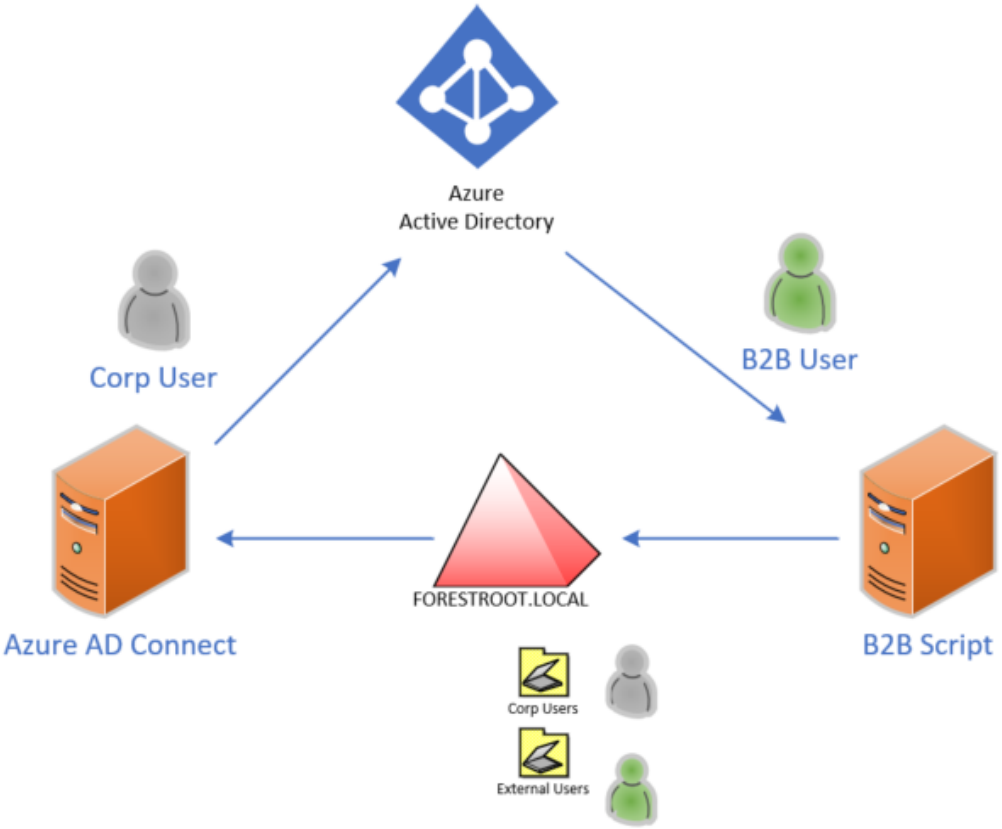

Рисунок 1.4 – Використання Kerberos в хмарних середовищах

Azure Active Directory є службою автентифікації від Microsoft для хмарних сервісів, таких як Office 365, Dynamics CRM Online та різні не-Microsoft SaaS-додатки. Завдяки своєму глибокому інтегруванню з хмарною інфраструктурою, Azure AD використовує Kerberos для безпечного і надійного підтвердження ідентифікації.

Azure AD забезпечує багатофункціональні можливості Kerberos, такі як безпечне обмін ключами, механізм обміну токенами і використання службового обліку. Це дає користувачам можливість підтвердити свою ідентичність і отримати доступ до ресурсів з усієї екосистеми Azure без необхідності вводити свій пароль після початкового входу.

Протокол Kerberos, який використовується в Azure AD, розділяється на три етапи: автентифікації, отримання білету на службу (TGS) і отримання білета до служби. При автентифікації користувач подає запит до Kerberos Key Distribution Center (KDC), щоб отримати "білет до брами" (TGT). TGT зберігається на локальному комп'ютері користувача і використовується для отримання TGS, який, в свою чергу, використовується для отримання білетів до служби.

Цей процес гарантує, що користувачі можуть автентифікуватися в Azure AD без безпосереднього надсилання своїх паролів через мережу. Замість цього, користувачі використовують безпечний обмін ключами для створення сеансових ключів, які потім використовуються для шифрування і дешифрування повідомлень.

Azure AD також підтримує SSO (Single Sign-On) за допомогою Kerberos. Сценарій SSO дозволяє користувачам вводити свої облікові дані лише один раз при вході в систему, після чого вони можуть отримати доступ до різних додатків і служб без необхідності повторного введення своїх облікових даних.

Важливо зазначити, що, хоча Azure AD і використовує Kerberos для автентифікації, це не єдина система безпеки, яку використовує Azure. Azure також використовує систему ролей і політик для управління доступом, а також різні механізми аудиту і журналювання для відстеження дій користувачів і виявлення зловмисного поведінки.

Отже, Kerberos є важливою частиною системи безпеки Azure AD, але це лише один з багатьох інструментів, які використовуються для захисту хмарних середовищ.

Висновки за розділом 1

У даному розділі було проведено огляд протоколу Kerberos та його функціональності. Протокол Kerberos відіграє важливу роль у сучасних комп'ютерних мережах, забезпечуючи безпечну автентифікацію користувачів.

Було розглянуто історію та розвиток Kerberos. Цей протокол, розроблений в Массачусетському технологічному інституті, став стандартом для забезпечення безпеки в розподілених системах.

Були досліджені основні компоненти та структура Kerberos. Це включає Керберос-сервер, відповідальний за автентифікацію користувачів, та Талони доступу, які користувачі отримують після успішної автентифікації для доступу до сервісів.

Процес автентифікації в Kerberos. Цей процес є центральним в Kerberos і включає обмін ключами між користувачем і сервером, що забезпечує високий рівень безпеки.

Були розглянуті протоколи і ключі шифрування, які використовуються в Kerberos. Ці ключі використовуються для шифрування і дешифрування інформації, що передається між користувачами та серверами, забезпечуючи безпеку обміну даними.

Нарешті, було розглянуто використання Kerberos у сучасних інформаційних системах. Як можна спостерігати, Kerberos застосовується в різних контекстах, включаючи облачні сервіси, корпоративні мережі та інтернет-сервіси.

У підсумку, Kerberos є надзвичайно важливим протоколом, який гарантує безпеку в розподілених системах. Його унікальна архітектура і високий рівень безпеки роблять його ідеальним вибором для сучасних комп'ютерних мереж.

Постановка завдання полягає у проведенні дослідження протоколу Kerberos з метою виявлення його поточних проблем, вразливостей та недоліків. Це передбачає детальне вивчення історії розвитку, основних принципів роботи, структури та компонентів системи Kerberos, а також процесів автентифікації і шифрування в ній.

Наступним кроком буде аналіз актуальних уразливостей та проблем протоколу, включаючи недоліки в процесі автентифікації, застарілі алгоритми шифрування, можливість атак на канал зв'язку та недостатній рівень аудиту і моніторингу.

На основі зібраної інформації будуть розроблені конкретні рекомендації та підходи щодо вдосконалення протоколу Kerberos. Це включає в себе покращення архітектури протоколу, застосування сучасних алгоритмів шифрування, розробку методів захисту каналу зв'язку, а також підвищення ефективності системи аудиту та моніторингу.

Крім того, планується розробка та реалізація програмного засобу або прототипу системи, який демонструватиме застосування методів захисту на базі Kerberos. Це допоможе оцінити практичну ефективність та працездатність рекомендованих підходів і технологій.

Таким чином, реалізація цих завдань дозволить підвищити ефективність застосування протоколу Kerberos в інформаційних системах, забезпечивши їх більш високий рівень захищеності та надійності.

РОЗДІЛ 2
АНАЛІЗ ВРАЗЛИВОТЕЙ СИСТЕМИ KERBEROS

2.1 Уразливості в процесі автентифікації

Перелік вразливостей в процесі автентифікації включає:

- *Pass The Hash*

Атака "Pass the Hash" (PtH) починається з того, що зловмисник викрадає хеш відповідного паролю. Це можна зробити різними способами. Наприклад, зловмисник може використовувати вразливості в операційній системі або використовувати програмне забезпечення злому, щоб вкрасти хеш-значення з комп'ютера жертви. Інший поширений сценарій включає перехоплення мережевого трафіку, де хеші передаються незахищеними.

Після того, як хеш було вкрадено, зловмисник використовує його для аутентифікації на іншій системі або службі, які приймають таку аутентифікацію. Це означає, що замість того, щоб вводити користувацькі дані (ім'я користувача та пароль), зловмисник просто вводить хеш.

Оскільки хеш є унікальним представленням пароля, система або служба, які отримують хеш, вважають його легітимною аутентифікацією. Це означає, що зловмисник отримує доступ до цільової системи або служби без необхідності знати або зламати фактичний пароль.

Одним з ключових аспектів атаки PtH є те, що вона дозволяє зловмисникам залишатися непомітними. Оскільки вони використовують легітимний хеш для аутентифікації, вони можуть уникнути багатьох традиційних систем виявлення вторгнень, які шукають підозрілі або неправильні спроби введення пароля.

- *OverPass The Hash*

Overpass-the-Hash (Pass-the-Hash) є одним з найпоширеніших типів атак на системи безпеки. Ця атака дозволяє зловмисникам здійснити несанкціонований доступ до комп'ютерної системи без необхідності знати пароль користувача. Ця атака, як правило, здійснюється за допомогою спеціального програмного забезпечення, яке

використовує витіклий хеш пароля для входу в систему як аутентифікований користувач.

Атака Overpass-the-Hash використовує техніку, що дозволяє зловмиснику використовувати витіклий хеш Kerberos для отримання TGT (Ticket Granting Ticket), який може бути використаний для доступу до ресурсів в домені. Основна відмінність між Pass-the-Hash і Overpass-the-Hash полягає в тому, що Overpass-the-Hash використовує хеші Kerberos замість NTLM.

Досить часто цей тип атаки використовується зловмисниками в рамках APT-атак (Advanced Persistent Threats), коли зловмисник проникає в систему і намагається залишатися в ній непомітним якомога довше. Використовуючи Overpass-the-Hash атаку, зловмисник може отримати доступ до важливих систем і даних, замасковуватися під легітимного користувача і продовжувати дії в системі без виявлення.

- *Pass The Ticket*

Pass The Ticket (PTT) є техніком втручання в систему, використовуваним кіберзлочинцями для доступу до захищених систем та ресурсів. Ця техніка базується на тому, що замість крадіжки власне пароля користувача, зловмисник краде "квиток" автентифікації, який використовується в системах, що базуються на Kerberos, таких як Microsoft Active Directory.

Kerberos - це мережевий протокол аутентифікації, створений MIT, який дозволяє двом сторонам в мережі довіряти одне одному безпечно. Kerberos використовує симетричне шифрування та вимагає від сторін секретного ключа. У процесі аутентифікації Kerberos використовує "квитки" для підтвердження ідентичності користувачів.

В мережах, що використовують Kerberos, коли користувач логується в систему, він надсилає запит на аутентифікацію до Kerberos Key Distribution Center (KDC). KDC видає так званий "TGT" (Ticket-Granting Ticket), який зберігається на пристрої користувача і використовується для отримання "сервісних квитків" для доступу до конкретних ресурсів.

В атакі Pass The Ticket, зловмисник перехоплює ці "сервісні квитки" і використовує їх для доступу до ресурсів. Оскільки Kerberos вважає, що запит відправлено від справжнього користувача, він надає доступ до запитуваного ресурсу.

Цей вид атаки стає особливо небезпечним, оскільки зловмисник може продовжувати використовувати перехоплені квитки, навіть якщо справжній користувач змінив свій пароль. Квиток може залишатися дійсним до його часу закінчення (часто до 10 годин у випадку Windows).

- *Pass The Cache*

Кеші підтверджень (або "ccache"), залишаються дійсниии, поки триває сеанс користувача, щоб кожна аутентифікація служби (наприклад, з'єднання з веб-сервером або поштовим сервером кілька разів) не вимагала звертання до KDC кожного разу.\

Кеші підтверджень зазвичай містить один початковий квиток, який отримується за допомогою пароля або іншого способу перевірки особи. Якщо цей квиток є квитком для надання квитків, його можна використовувати для отримання додаткових підтверджень без пароля. Оскільки кеші підтверджень не зберігають пароль, шкода для облікового запису користувача від компрометації системи може бути меншою.

Кеші підтверджень зберігають прізвище типового клієнта за замовчуванням, яке встановлюється при створенні кешу. Це ім'я показується вгорі списку klist.

Типи ccache:

У бібліотеці MIT Kerberos підтримуються кілька видів кешів підтверджень.

1) Кеші файлів: це найпростіший і найбільш універсальний тип. Для зберігання використовується простий формат файлу, в якому зберігаються одне підтвердження за одним. Це тип кешу за замовчуванням.

2) API: Цей тип реалізований лише в Windows. Він спілкується з серверним процесом, який зберігає підтвердження в оперативній пам'яті для користувача, та не записує їх на диск.

3) DIR points: Вказує на місце зберігання колекції кешів підтверджень у форматі файлу FILE. Це корисно, коли маємо справу з декількома областями Kerberos і КДЦ.

4) KEYRING: Специфічно для Linux і використовує підтримку ключових кільцевих зразків ядра для зберігання даних підтверджень в пам'яті ядра, до якої повинен мати доступ тільки поточний користувач.

5) Кеші пам'яті: для зберігання підтверджень, які не потрібно робити доступними поза поточним процесом. Кеші пам'яті швидші за кеші файлів і автоматично видаляються при завершенні процесу.

6) MSLSA: Це тип кешу, специфічний для Windows, який отримує доступ до сховища облікових даних Windows.

Атака з використанням ccache передбачає використання квитка для надання квитків для доступу до сервера програм без проведення аутентифікації через Kerberos. Зловмисник використовує знайдений або вивантажений з системи файл для авторизації.

- *Skeleton Key*

"Скелетний ключ" (Skeleton Key) - це термін, що використовується в кібербезпеки, щоб описати шкідливе ПЗ, що здатне перехоплювати процеси аутентифікації, дозволяючи атакуючому обходити процедури введення паролів або інших форм аутентифікації.

Атаки "Skeleton Key" - це метод пост-експлуатації, який вимагає від атакуючого прав доступу на рівні домену адміністратора. Між іншим, атакуючим потрібні права на налагодження на цільовому контролері домену (стандартний дозвіл для облікових записів адміністратора).

Під час атаки "Skeleton Key", атакуючий використовує свій доступ до облікового запису адміністратора домену для встановлення шкідливого програмного забезпечення на цільовому контролері домену Active Directory. Це шкідливе ПЗ має можливість "запатчити" LSASS Windows (Local Security Authority Subsystem Service), дозволяючи йому створити новий пароль (Skeleton Key) для всіх користувачів домену.

"Skeleton Key" діє, як натякає його назва: як універсальний пароль, який відкриє будь-який обліковий запис домену, до якого він прикріплений. З точки зору користувача, нічого не змінюється під час атаки "Skeleton Key": їхній звичайний

пароль продовжує надавати їм доступ до домену. Співробітники відділу IT-безпеки, які намагаються виявити зловмисну аутентифікацію, не зможуть легко визначити використання "Skeleton Key" з легітимного входу в домен.

"Skeleton Keys" - потужний інструмент для забезпечення персистентності для зловмисників. Атака була впроваджена в відкриті хакерські інструменти, такі як Mimikatz, який дає зловмисникам можливість клацати мишею для використання цих атак. Для зловмисників, атаки "Skeleton Key" можуть використовуватися як альтернатива Kerberos Golden Tickets для створення персистентності та контролю над доменом.

- *Silver Ticket*

"Silver Ticket" - це термін, що використовується в контексті атак на систему Kerberos в середовищі Active Directory (AD). Kerberos - це протокол аутентифікації, що використовується в системах AD. Його основна мета - гарантувати, що користувачі та служби є тими, ким вони стверджують бути, та забезпечити безпеку їхніх з'єднань.

Існують два основних типи квитків Kerberos: TGT (Ticket Granting Ticket) і ST (Service Ticket). TGT - це "золотий квиток", а ST - "срібний квиток". Основна відмінність між ними полягає в тому, що "золотий квиток" дає змогу отримувати "срібні квитки" для будь-якої служби в домені, тоді як "срібний квиток" діє лише для конкретної служби.

Атака "Silver Ticket" відбувається, коли зловмисник здобуває секретний ключ служби (зазвичай це пароль облікового запису служби) та створює собі власний "срібний квиток". Це дає зловмисникові змогу отримувати доступ до цільової служби без необхідності аутентифікуватися.

Цей тип атаки є особливо небезпечним, оскільки "срібні квитки", на відміну від "золотих", не перевіряються центром видачі квитків (TGS - Ticket Granting Service). Таким чином, атака "Silver Ticket" може залишатися невиявленою.

- Golden Ticket

Атака Golden Ticket в Active Directory (AD) є одним з видів привілейованих атак, який використовується для незаконного отримання доступу до AD-сервера та отримання повного контролю над ним.

Основна ідея атаки полягає в тому, щоб зловмисник зламав аутентифікаційну систему Kerberos, яка використовується в AD для забезпечення безпеки. Після успішного зламу Kerberos зловмисник може створити "золотий квиток" (Golden Ticket), який є керберосним квитком, що надає повний контроль над AD-сервером.

Основні етапи атаки Golden Ticket включають:

1) Злам Kerberos: Зловмисник повинен отримати доступ до даних, необхідних для обчислення ключа шифрування Kerberos (KRBTGT), який є основним ключем шифрування в AD. Зазвичай це вимагає отримання доступу до контролерів домену або скомпрометованих облікових записів.

2) Створення Golden Ticket: Зловмисник використовує отримані дані, щоб створити новий керберосний квиток (Golden Ticket) з необмеженими привілеями доступу. Цей квиток містить інформацію про користувача, таку як ім'я користувача, SID (ідентифікатор безпеки) та групи, до яких він належить.

3) Використання Golden Ticket: Зловмисник може використовувати створений Golden Ticket для автентифікації на будь-якому комп'ютері або сервері в AD. З огляду на те, що цей квиток містить необмежені привілеї доступу, зловмисник може виконувати будь-які дії в системі, зокрема створювати, змінювати або видаляти облікові записи користувачів, виконувати резервне копіювання або відновлення даних, і багато іншого.

- *Diamond Ticket*

Як і "золотий квиток" (golden ticket), "алмазний квиток" (diamond ticket) є TGT (Ticket-Granting Ticket), який можна використовувати для доступу до будь-якої служби від імені будь-якого користувача. "Золотий квиток" генерується повністю офлайн, шифрується за допомогою хешу krbtgt цього домену, а потім передається в сеанс входу для використання. Оскільки контролери домену не відстежують TGT, які вони видали легітимно, вони з радістю приймуть TGT, які зашифровані власним хешем krbtgt.

Існують дві поширені техніки виявлення використання "золотих квитків":

1) Пошук TGS-REQ, які не мають відповідного AS-REQ.

2) Пошук TGT, які мають смішні значення, наприклад, за замовчуванням у Mimikatz - 10-річний термін життя.

"Алмазний квиток" створюється шляхом модифікації полів легітимного TGT, який був виданий DC (Domain Controller). Це досягається шляхом запиту TGT, його розшифровки за допомогою хешу krbtgt домену, зміни потрібних полів квитка, а потім повторного його шифрування. Це долає дві згадані вище недоліки "золотого квитка", оскільки:

За TGS-REQ обов'язково передує AS-REQ.

TGT було видано DC, що означає, що він матиме всі правильні деталі з політики Kerberos домену. Хоча ці дані можна точно сфальсифікувати у "золотому квитку", це більш складно і відкриває можливість для помилок.

- *Cross-Domain Golden Ticket attack*

Головний принцип атаки Golden Ticket полягає у тому, що зловмисник викрадає ключовий хеш облікового запису KRBTGT (або ключ Ticket Granting Ticket, TGT) у домені. За допомогою цього ключа зловмисник може створювати власні TGT, які в свою чергу можуть використовуватися для отримання Ticket Granting Service (TGS) для будь-якого сервісу в домені.

Cross-Domain Golden Ticket є варіацією Golden Ticket атаки і включає створення Golden Tickets для дочірніх доменів в доменній структурі Active Directory. Це робиться з допомогою хеша облікового запису KRBTGT в головному домені. Ця атака стає можливою, тому що ключ облікового запису KRBTGT у головному домені використовується для шифрування TGT для дочірніх доменів.

Як результат, якщо зловмисник знає цей хеш у головному домені, він може створювати Golden Tickets для будь-якого домену в доменній структурі. Це дозволяє зловмиснику отримати доступ до ресурсів не лише в головному домені, але і в будь-якому дочірньому домені.

- *Unconstrained Delegation*

Unconstrained Delegation - це властивість, яка була введена в Active Directory (AD) компанії Microsoft для дозволу серверам перепроваджувати (делегувати) Kerberos аутентифікацію на користь користувача, який звертається до сервера. Коли включена, ця властивість може створювати потенційні уразливості.

"Unconstrained Delegation" дозволяє серверу приймати TGT (Ticket Granting Ticket) користувача та використовувати його для отримання сервісних квитків (Service Tickets) до інших сервісів в домені від імені користувача. З точки зору безпеки, це може стати проблемою, оскільки сервер, що має право на Unconstrained Delegation, може потенційно зловживати своїми правами та виконувати дії від імені користувача.

Атака на Unconstrained Delegation обычно використовує так звану атаку "Kerberos Golden Ticket", де атакуючий створює поддельний TGT, який дозволяє йому вільно отримувати Service Tickets для будь-якого користувача в домені.

Така атака може дати атакуючому повний контроль над ресурсами в домені. Особливо це стає небезпечним, якщо сервери, які мають право на Unconstrained Delegation, також мають високі привілеї в домені.

- *Kerberos Constrained Delegation*

Kerberos Constrained Delegation (KCD) - це механізм, що дозволяє обмежене делегування прав користувачів в середовищі Active Directory (AD). Коли він включений для певного об'єкта (наприклад, облікового запису комп'ютера або облікового запису служби), цей об'єкт може запитувати Kerberos сервісні квитки від імені користувача, але тільки для визначеного набору сервісів.

Атаки на Kerberos Constrained Delegation можуть бути потужними, оскільки вони дозволяють атакуючому використовувати делеговані права для отримання доступу до ресурсів.

Одна з таких атак називається атакою "Kerberoasting". Вона полягає в тому, що атакуючий, який має контроль над обліковим записом, що може делегувати свої права, запитує сервісний квиток для сервісу, що використовує вразливий хеш пароля

(наприклад, незашифрований MD5). Після отримання квитка атакуючий може зламати його та отримати оригінальний пароль.

Другий тип атаки використовує властивість Resource-Based Constrained Delegation (RBCD). В цьому випадку, якщо атакуючий має контроль над об'єктом, на який налаштовано RBCD, він може вказати обліковий запис, який може делегувати свої права до цього об'єкта. Це може дозволити атакуючому отримати сервісні квитки від імені будь-якого користувача в домені до цього об'єкта.

Експлуатація Kerberos Constrained Delegation (KCD) обмежується середовищами, де уже відбувся компроміс облікового запису, що має право делегувати. Ось базовий процес експлуатації KCD:

1. Отримання контролю над обліковим записом: Перш ніж можна експлуатувати KCD, атакуючому потрібно отримати контроль над обліковим записом, який має право делегувати. Це може бути досягнуто через різні методи, наприклад, за допомогою phishing, brute force атаки на паролі, або експлуатації уразливостей.

2. Запит сервісного квитка: Після отримання контролю над обліковим записом, атакуючий може використовувати його для запиту сервісних квитків від імені користувача. Він може зробити це, використовуючи інструменти, такі як Rubeus або Mimikatz.

3. Експлуатація сервісного квитка: Після отримання сервісного квитка, атакуючий може використовувати його для доступу до ресурсів, до яких він може делегувати. Наприклад, якщо обліковий запис має право делегувати до сервера файлів, атакуючий може використовувати сервісний квиток для доступу до файлів на сервері.

4. Подальше розповсюдження: Після успішної експлуатації KCD, атакуючий може використовувати доступ до ресурсів для подальшого розповсюдження в мережі, наприклад, шляхом експлуатації уразливостей на цільовому сервері або шляхом крадіжки даних для подальшої атаки.

- *Kerberos Resource-Based Constrained Delegation*

Атака Kerberos Resource-Based Constrained Delegation є одним з методів атак на Active Directory, який використовується для отримання незаконного доступу до ресурсів в мережі. Ця атака використовує уразливість в механізмі делегування обмежених ресурсів (Constrained Delegation) Kerberos, який є частиною протоколу аутентифікації Kerberos, що використовується в Active Directory.

Kerberos - це протокол аутентифікації мережі, який дозволяє користувачам отримувати доступ до різних ресурсів в мережі після проходження аутентифікації. У Active Directory, який є службою директорії в середовищі Windows, Kerberos використовується для аутентифікації користувачів і делегування прав доступу до ресурсів.

Constrained Delegation (обмежена делегація) є механізмом в Kerberos, який дозволяє серверам делегувати аутентифікаційні токени іншим серверам для забезпечення доступу до ресурсів в ім'я користувача. Це дозволяє забезпечити безшовну аутентифікацію між різними службами в Active Directory без необхідності повторної аутентифікації користувача.

Атака Kerberos Resource-Based Constrained Delegation використовує уразливість в конфігурації делегації ресурсів. Зазвичай, при налаштуванні обмеженої делегації, можна вказати, до яких служб можна делегувати доступ. Однак, якщо налаштування не здійснюється належним чином, атакуючий може використовувати цю уразливість, щоб отримати доступ до ресурсу в мережі.

Процес експлуатації Kerberos Resource-Based Constrained Delegation може включати наступні кроки:

1) Отримання доступу до хоста в мережі, на якому встановлено Active Directory.

2) Пошук ресурсу, на який можна здійснити обмежену делегацію. Це може бути сервер, до якого налаштовано делегування в Active Directory.

3) Отримання токена аутентифікації цього ресурсу, зазвичай за допомогою атаки на хеші паролю користувача або використовуючи інші методи компрометації акаунта.

4) Використання отриманого токена для отримання доступу до інших ресурсів в мережі, які доступні цьому ресурсу.

Ця атака може дозволити атакуючому отримати незаконний доступ до ресурсів в мережі, які зазвичай були б недоступними. Вона може бути особливо небезпечною, якщо атакуючий здобуває доступ до привілейованих облікових записів, оскільки він зможе виконувати дії в системі в ім'я цих облікових записів.

- Kerberoasting

Kerberoasting є методом атаки, який використовує вразливості протоколу Kerberos в середовищах Microsoft Windows. Kerberos - це протокол аутентифікації, що використовується в Windows для перевірки ідентичності користувачів та сервісів в мережі.

Kerberoast використовує цю особливість Kerberos, яка дозволяє користувачам, що мають обліковий запис в домені, запитати "Service Principal Names" (SPNs) за допомогою протоколу. SPN асоціюється з обліковим записом Windows, що використовується для запуску служби.

Ось, як Kerberoast влаштований:

a. Користувач або програма запитує SPN, який асоційований з сервісом, до якого вони хочуть отримати доступ.

b. Цей запит передається до контролера домену (Domain Controller, DC), який генерує та передає "Service Ticket" користувачеві. Цей білет зашифровано використовуючи хеш пароля облікового запису, асоційованого з SPN.

c. Користувач або програма, що використовує Kerberoast, втягує цей зашифрований білет та використовує техніку грубої сили або радуги таблиць, щоб відновити початковий хеш пароля.

Це можливо тому, що Microsoft Windows використовує алгоритм хешування RC4_HMAC для шифрування білетів Kerberos, який відомий своєю вразливістю до атак грубої сили. Оскільки віднавлення хешу пароля може бути часоємким процесом, атака Kerberoast є ефективною тільки, якщо слабкі або легко вгадувані паролі використовуються для облікових записів сервісу.

В цілому, Kerberoast використовує те, що багато служб в мережах Windows запускаються на облікових записах з особливими привілеями та з недостатньою політикою використання паролів, що робить ці облікові записи привабливими цілями для зловмисників.

- *AS-REP Roasting*

AS-REP Roasting є ще одним типом атаки на Kerberos, який використовує вразливості в протоколі аутентифікації Kerberos. Відмінність AS-REP Roasting від Kerberoasting полягає в тому, що AS-REP Roasting цільово атакує облікові записи користувачів, а не облікові записи сервісів.

AS-REP Roasting використовує властивість Kerberos, яка дозволяє користувачу отримувати "pre-authentication" білети. Pre-authentication - це процес, при якому користувач повинен довести свою ідентичність перед отриманням TGT (Ticket Granting Ticket) від контролера домену. Однак, в деяких випадках, ця функція може бути відключена.

Ось як це працює:

a. Коли pre-authentication вимкнуто для облікового запису користувача, будь-який користувач або програма може запитати TGT для цього облікового запису без необхідності перевірки.

b. Цей запит передається до контролера домену, який передає TGT, зашифрований хешем пароля користувача.

c. Зловмисник може втягнути цей зашифрований TGT і використовувати техніку грубої сили або таблиць радуги, щоб відновити початковий хеш пароля.

Така атака можлива через використання слабкого алгоритму шифрування (RC4-HMAC) для білетів Kerberos, який може бути зламаний за допомогою атак грубої сили.

- *SID-History Injection attack*

SID (Security Identifier) - це унікальний ідентифікатор, який використовується в операційних системах Microsoft Windows для ідентифікації об'єктів, таких як облікові записи користувачів та групи безпеки. Коли обліковий запис переміщується з одного домену в інший в Active Directory, інформація про SID зберігається в атрибуті SID-

History облікового запису. Це робиться для забезпечення сумісності з додатками, які використовують SID для визначення доступу.

Суть атаки SID-History Injection полягає в тому, щоб змінити атрибут SID-History в Active Directory, додавши до нього SID іншого облікового запису. Якщо атакуючий може це зробити, він може отримати ті ж права та дозволи, що і цей інший обліковий запис.

Ця атака вимагає певного рівня доступу до Active Directory, оскільки не всі користувачі можуть змінити атрибут SID-History. Таким чином, вона зазвичай використовується в рамках атаки, яка вже має високий рівень привілеїв, наприклад, після отримання доступу до облікового запису адміністратора домену.

a. Процес експлуатації вразливості може включати наступні кроки:

b. Отримання достатнього рівня доступу. Атака SID-History Injection вимагає високого рівня доступу до Active Directory.

c. Вибір цільового облікового запису. Атакуючий вибирає обліковий запис, до SID-History якого він хоче додати SID.

d. Внесення змін до SID-History. Атакуючий використовує свої привілеї для додавання SID обраного облікового запису до SID-History цільового облікового запису.

e. Експлуатація отриманих привілеїв. Атакуючий тепер може використовувати цільовий обліковий запис для доступу до ресурсів з тими ж правами, що і обліковий запис, SID якого було додано до SID-History.

- *AdminSDHolder attack*

AdminSDHolder — це об’єкт Active Directory, який, по суті, є контейнером, який, по суті, діє як шаблон дескриптора безпеки для захищених облікових записів і груп у домені Active Directory

Дескриптор безпеки включає таку інформацію, як (SID, SID первинної групи, DACL, SACL тощо), яка визначає безпеку об’єкта.

Таким чином, AdminSDHolder має великий контроль над тим, які користувачі та групи, захищені цим рівнем привілеїв, матимуть. Щоб забезпечити це, процес під

назвою SDProp буде виконуватися раз на годину, який встановлює ці дозволи дескриптора для членів групи AdminSDHolder.

Захищені облікові записи та групи в Active Directory

Зрозуміти, як працюють об’єкт AdminSDHolder і пов’язані з ним процеси, може бути дещо складніше, але зазначених вище основ загалом достатньо, щоб зрозуміти, як цей об’єкт може використовувати зловмисник.

Типова атака, яка використовує AdminSDHolder, використовує його для досягнення стійкості в середовищі. Мета полягає в тому, щоб застосувати зміни до AdminSDHolder, зокрема до списку керування доступом, застосованого до об’єкта. Атака може додати облікові записи до цього списку, щоб надати обліковому запису той самий рівень привілеїв, який зазвичай асоціюється з обліковими записами та групами, захищеними доменом, присутніми в об’єкті AdminSDHolder за замовчуванням.

Якщо організація помітить сумнівну активність облікового запису, який використовує зловмисник, можна обмежити доступ до облікового запису. Саме тут вступає в гру завдання SDProp, оскільки ці зміни буде скасовано протягом однієї години, а обліковий запис зловмисника знову матиме привілейований доступ, оскільки завдання SDProp відновить списки керування доступом, указані в групі AdminSDHolder.

У цьому випадку в обліковому записі мають бути скасовані зміни ACL з об’єкта AdminSDHolder, щоб справді видалити ці привілеї.

Враховуючи дещо складну природу об’єкта AdminSDHolder, системні адміністратори можуть легко не помітити його, що робить його цінним інструментом для зловмисників.

Щоб додатково проілюструвати наскрізні кроки, які зловмисник може фактично використати в зловмиснику AdminSDHolder, ось простий покроковий приклад атаки AdminSDHolder:

a. Зловмисник компрометує привілейовані облікові дані (наприклад, через фішинг або соціальну інженерію, вже є привілейованим інсайдером, використовуючи слабкі дозволи тощо)

b. Зловмисник змінює AdminSDHolder, додаючи нового користувача до свого списку контролю доступу (ACL)

c. Через процес SDProp дозволи AdminSDHolder надаються всім захищеним об’єктам кожні 60 хвилин (за замовчуванням), включаючи привілейовані групи, як-от адміністратори домену, адміністратори, адміністратори підприємства та адміністратори схеми.

d. Навіть якщо адміністратор побачить невідповідний дозвіл для захищеного об’єкта та видалить його, протягом години завдання SDProp поверне ці дозволи на місце.

- *Abusing Forest Trusts*

У стандартній інсталяції Active Forest є чотири основні «функції», які дозволяють здійснити цю атаку.

Контролери домену з можливістю запису в розгортаннях домену за замовчуванням налаштовані на необмежене делегування. Це означає, що будь-який користувач, який не має параметра «Обліковий запис конфіденційний і не може бути делегований» у своєму обліковому записі або не входить до групи «Захищені користувачі», надішле свій TGT у квитку служби під час доступу до сервера з необмеженим делегуванням. З того, що можна сказати та з тих, з ким спілкувалися, самі облікові записи контролерів домену майже ніколи не мають такого захисту – вони майже завжди застосовуються лише до облікових записів адміністраторів домену.

За словами Microsoft, «якщо на сервері ввімкнено повне делегування для Kerberos, сервер може використовувати квиток надання делегованого квитка (TGT) для підключення як користувач до будь-якого сервера, включно з одностороннім довірою». Це означає, що делеговані квитки TGT можуть перетинати межі довіри між лісами. Ця поведінка ввімкнена за замовчуванням, але її можна заблокувати вручну. Докладніше див. у розділі «Пом’якшення атак» далі в цьому дописі.

Зловживання RPC-викликом RpcRemoteFindFirst PrinterChange Notification(Ex), про який повідомлялося раніше (відоме як зловживання MS-RPRN, «помилка принтера»), дозволяє будь-якому члену домену «Автентифікованих користувачів»

змусити будь-яку машину, на якій запущено службу спулера, автентифікуватись на цільовому вибір зловмисника через Kerberos або NTLM. Знову ж таки, щоб дізнатися більше про «помилку принтера» Лі, перегляньте нашу розмову на DerbyCon.

Нарешті, за словами Microsoft, «коли користувачі проходять автентифікацію з довіреного лісу, вони отримують SID автентифікованих користувачів у своєму маркері. Багато прав за замовчуванням для користувачів у лісі надаються через автентифікованих користувачів». Це означає, що будь-який користувач у довіреному лісі може виконати «помилку принтера» проти машин у чужому лісі, оскільки «Автентифіковані користувачі» — це всі права доступу, необхідні для запуску примусової автентифікації.

У сукупності це означає, що якщо FORESTA має двосторонню міжлісову довіру з FORESTB, то компрометація будь-якого контролера домену (або будь-якого сервера з необмеженим делегуванням) у FORESTB може бути використана для компрометації кореня лісу FORESTA (або навпаки) і всіх доменів у ньому.

Щоб здійснити цю атаку (за допомогою публічних інструментів), зловмисник:

a. Скомпрометує будь-який сервер із необмеженим делегуванням, наприклад, контролер домену (наприклад, DCB) у FORESTB.

b. Розпочне моніторинг 4624 подій входу на скомпрометований сервер FORESTB, витягуючи нові TGT з будь-яких нових сеансів входу через встановлені LSA API. Це можна зробити за допомогою монітора Rubeus.

c. Викликаче «помилку принтера» MS-RPRN на контролері домену (наприклад, DCA) у FORESTA. Це можна зробити за допомогою коду підтвердження концепції Лі.

d. Контролер домену FORESTA автентифікуватиметься на контрольованому зловмисником сервері у FORESTB за допомогою облікового запису комп’ютера контролера домену FORESTA (у цьому випадку DCA$). TGT DC FORESTA буде міститися в службовому квитку, надісланому на сервер, контрольований зловмисником, і кешуватиметься в пам’яті протягом короткого періоду часу.

e. Зловмисник витягує TGT стороннього контролера домену за допомогою встановлених API LSA та застосовує TGT до поточного (або іншого) сеансу входу. Це знову можна зробити за допомогою Rubeus.

f. Зловмисник виконує атаку DCSYNC проти FORESTA, щоб отримати привілейований обліковий матеріал у FORESTA (наприклад, хеш облікового запису FORESTA\krbtgt).

2.2 Застарілі алгоритми шифрування та хешування

Протокол Kerberos використовує алгоритми шифрування та хешування для аутентифікації користувачів та забезпечення конфіденційності даних. Проте, деякі алгоритми, які були включені в ранні версії Kerberos, зараз вважаються застарілими та небезпечними.

Огляд використовуваних алгоритмів шифрування та хешування в Kerberos:

Kerberos використовував декілька різних алгоритмів шифрування та хешування від своєї першої реалізації.

Kerberos 4:

- DES (Data Encryption Standard)

Kerberos 5:

- DES (Data Encryption Standard)
- 3DES (Triple DES)
- AES-128 (Advanced Encryption Standard)
- AES-256
- RC4-HMAC (Rivest Cipher 4 - Hash-based Message Authentication Code)

Окрім алгоритмів шифрування, Kerberos також використовує алгоритми хешування для створення криптографічних "відбитків" даних. Хеш-функції використовуються в процесах аутентифікації і генерації ключів. Ось деякі з них:

Kerberos 4:

- Не використовує специфічних алгоритмів хешування

Kerberos 5:

- MD5 (Message Digest Algorithm 5) використовується в RC4-HMAC
- SHA-1 (Secure Hash Algorithm 1) використовується в некоторых варіантах DES та 3DES
- SHA-2 Family (включаючи SHA-256 і SHA-384) використовуються в AES

Версії алгоритмів шифрування можуть використовуватися в різних процедурах Kerberos, включаючи аутентифікацію, видачу білетів, встановлення сесійних ключів тощо.

Важливо відзначити, що DES та RC4-HMAC вважаються застарілими і можуть бути небезпечними через потенційні вразливості до атак. MD5 та SHA-1 також вважаються застарілими через потенційні вразливості до колізій. Виявлені недоліки та вразливості цих алгоритмів:

DES, або Data Encryption Standard, був створений в 1970-х роках. Це симетричний алгоритм блокового шифрування, створений IBM і прийнятий в якості стандарту від National Bureau of Standards (NBS), попередника National Institute of Standards and Technology (NIST) США. DES був вперше опублікований у 1975 році, а офіційно став стандартом США у 1977 році.

DES використовує блоки розміром 64 біти і ключ довжиною 56 бітів (плюс 8 бітів для перевірки парності), хоча деякі біти ключа не використовуються в процесі шифрування, тому ефективна довжина ключа становить лише 56 бітів.

Щодо недоліків та вразливостей DES, то є кілька основних проблем, які слід враховувати:

- Коротка довжина ключа: Основна проблема DES полягає в тому, що він має досить короткий ключ. Це робить його вразливим до атак "brute force", коли зловмисник просто пробує всі можливі комбінації ключів.
- Вразливість до атаки з використанням "повторного блоку" (repeated block attack): Оскільки DES є блоковим шифром, який шифрує кожен блок даних незалежно, він може бути вразливим до атак, коли зловмисник спостерігає за шифрованими повідомленнями і виявляє повторювані блоки.

- Вразливість до лінійного та диференціального криптоаналізу: Дослідники виявили, що DES може бути вразливим до так званих атак лінійного та диференціального криптоаналізу.

Що стосується використання DES в системах Kerberos, то небезпека полягає в тому, що якщо зловмисник здатен зламати ключ DES, він може отримати доступ до всієї інформації, захищеної Kerberos, і потенційно отримати необмежений доступ до системи.

RC4-HMAC – це варіант алгоритму шифрування RC4, що використовує хеш-функцію HMAC для забезпечення цілісності даних. RC4 сам по собі є симетричним потоковим шифром, що був створений Рональдом Ривестом у RSA Security в 1987 році. RC4 був широко використовуваний через свою простоту і швидкість, але виявлені вразливості змусили багато організацій відмовитися від його використання.

Вразливості та недоліки RC4-HMAC

Проблеми з RC4: RC4 відомий своїми вразливостями, особливо в контексті його використання у протоколах, таких як WEP та TLS. Він вразливий до ряду атак, включаючи атаки на слабкі ключі та відновлення головного ключа.

Вади HMAC: Хоча HMAC вважається відносно стійким проти колізій, він може бути вразливий до деяких типів атак, особливо якщо використовується слабка хеш-функція або якщо ключ HMAC стає відомий зловмисникові.

Відмова від RC4 в протоколах безпеки: У зв'язку з виявленнями вразливостей у RC4, декілька протоколів безпеки, зокрема SSL і TLS, відмовилися від використання RC4. Це могло негативно вплинути на довіру до RC4-HMAC.

У системах Kerberos використання RC4-HMAC може створювати ризики через вразливості, асоційовані з обома компонентами цього алгоритму. Якщо ключ шифрування або ключ HMAC стають відомими зловмисникові, це може дозволити йому шифрувати або розшифровувати повідомлення, або ж внести неавторизовані зміни в зашифровані дані. Це робить RC4-HMAC менш безпечним, ніж більш сучасні алгоритми шифрування, як-от AES.

MD5 (Message Digest Algorithm 5) - це алгоритм хешування, що був розроблений Рональдом Ривестом в 1991 році. Він був створений для заміни

попереднього алгоритму, MD4, і зазвичай використовується для перевірки цілісності даних. MD5 створює 128-бітний хеш, який представляється як 32-символьне шістнадцяткове число.

Незважаючи на свою широку популярність у минулому, MD5 має значні недоліки та вразливості, які роблять його небезпечним для використання в сучасних криптографічних системах:

- Слабка стійкість до колізій:

Було виявлено, що MD5 має серйозні слабкості в області стійкості до колізій. Колізія відбувається, коли два різні вхідні блоки даних виробляють однаковий хеш. Це означає, що зловмисники можуть замінити оригінальні дані на шкідливі, але зберегти той самий хеш MD5.

- Швидкість:

Швидкість MD5, яка раніше вважалася перевагою, зараз є його слабкістю, оскільки вона дозволяє здійснювати брутфорс атаки швидше.

- Проблеми з використанням в Kerberos та Active Directory:

Kerberos використовує MD5 для деяких криптографічних операцій, що створює потенційні слабкі місця. Active Directory також використовує MD5 в деяких процесах хешування паролів, що створює потенційні вразливості. Причина цього полягає у вище згаданій проблемі з колізіями: якщо зловмисник може створити колізію, він може обійти системи захисту Kerberos або Active Directory.

У них були виявлені серйозні слабкості, які дозволяють знайти два різних вхідних повідомлення, що дають однаковий хеш (так звана колізія). Це робить ці алгоритми непридатними для використання в безпеки.

Ризики, пов'язані з використанням застарілих алгоритмів у системі:

Використання застарілих алгоритмів шифрування та хешування може мати серйозні наслідки. Це може привести до витоку конфіденційної інформації, порушення цілісності даних, а також може дозволити зловмисникам обійти систему аутентифікації.

2.3 Можливість атак на канал зв'язку

Для початку розглянемо різні атаки на канали зв'язку в комп'ютерних мережах:

- *LDAP Relay Attack*

LDAP Relay Attack - це вид атаки, при якому зловмисник перенаправляє аутентифікаційні запити з одного LDAP-сервера на інший, що призводить до несанкціонованого доступу. Цей тип атаки вперше було виявлено в кінці 90-х років, коли почалося активне розповсюдження LDAP.

Обставини проведення LDAP Relay Attack

LDAP Relay Attack є можливою за наступних обставин:

1. Коли протокол LDAP використовується без SSL / TLS: LDAP без зашифрування може бути перехоплений зловмисником, який може перенаправити аутентифікаційний запит на інший сервер.

2. Коли протокол безпечного LDAP (LDAPS) використовується без перевірки сертифікатів: LDAPS забезпечує шифрування, але без перевірки сертифікатів зловмисник може представити себе як довірчивий сервер.

Успішна LDAP Relay Attack може мати серйозні наслідки:

1. Несанкціонований доступ: Зловмисник може отримати доступ до конфіденційної інформації, такої як облікові дані користувачів.

2. Підробка ідентифікації: Якщо зловмисник має можливість перенаправляти запити на інший сервер, він може представити себе як легітимний користувач або сервер.

Проведення LDAP Relay Attack

LDAP Relay Attack проводиться у кілька етапів:

1. Зловмисник перехоплює LDAP-запит в мережі.

2. Зловмисник перенаправляє цей запит на цільовий LDAP-сервер.

3. LDAP-сервер відповідає, думаючи, що він спілкується з легітимним користувачем.

4. Зловмисник перехоплює відповідь і використовує отриману інформацію для несанкціонованого доступу.

- *Sniffing*

Sniffing, або перехоплення мережевого трафіку, є одним із найстаріших видів атак в цифровому світі. Історія sniffing-атак на Active Directory тісно пов'язана з самою історією AD і використовуваних протоколів аутентифікації, таких як NTLM і Kerberos.

За допомогою ARP spoofing, є можливість відтворити MiTM та розсташувати себе у положенні, яке дозволить нам перехоплювати трафі, що ходить між хостами у Active Directory

За допомогою цього є можливість з легкістю зможемо отримати Імена облікових записів користувачів та доменів, так як вони відправляються по мережі у чистому вигляді, без шифрування.

- *Downgrade NTLM Attack*

Downgrade NTLM Attack – це вразливість, при якій зловмисник змушує систему використовувати старішу, менш безпечну версію NTLM, що відкриває шлях для атак. Історія цієї атаки сягає початків NTLM, коли було створено декілька версій протоколу, що з часом стали менш безпечними.

Обставини Downgrade NTLM Attack

Downgrade NTLM Attack є можливою при наступних обставинах:

- Підтримка старих версій NTLM: Якщо система дозволяє використовувати старіші версії NTLM, це може бути використано зловмисником.
- Недостатні мережеві контрольні заходи: Недостатня сегментація мережі або моніторинг можуть дозволити зловмисникам перехоплювати та модифікувати аутентифікаційні запити.

Наслідки Downgrade NTLM Attack

При успішному проведенні атаки, зловмисник може:

- Отримати Хеш, що пересилається мережею у середовищі Active Directory.
- Провести атаку "чоловік посередині" (Man-in-the-Middle), перехоплюючи та модифікуючи аутентифікаційні запити.

Порядок проведення Downgrade NTLM Attack:

1. Зловмисник перехоплює аутентифікаційний запит NTLM в мережі.

2. Зловмисник модифікує запит, змушуючи систему використовувати старішу версію NTLM.

3. Зловмисник використовує відомі вразливості старішої версії NTLM для отримання несанкціонованого доступу.

- *LLMNR & NBT-NS Poisining*

LLMNR (Link-Local Multicast Name Resolution) та NBT-NS (NetBIOS Name Service) є протоколами, які використовуються в мережах для визначення IP-адрес комп'ютерів за іменами. Вони були розроблені для забезпечення простого способу визначення адреси мережі комп'ютера. Однак, вони мають вади, які можуть бути використані зловмисниками для проведення атаки типу "Man in the Middle", відомої як отруєння LLMNR і NBT-NS.

LLMNR був впроваджений Microsoft для операційних систем, починаючи з Windows Vista, для розв'язання проблем, пов'язаних з DNS в мережах малого масштабу. Він працює в локальних мережах і використовує мультикаст для визначення адреси комп'ютера, якщо DNS-запит не дав результатів. Проблема полягає в тому, що LLMNR не використовує жодного механізму аутентифікації для перевірки того, чи відповідає відповідач запиту правильному комп'ютеру.

NBT-NS, подібно до LLMNR, є протоколом, розробленим для операційних систем Windows для розв'язання імен в локальних мережах. Він був створений до появи DNS і, подібно до LLMNR, не має жодних механізмів аутентифікації для перевірки правильності відповіді.

Зловмисники можуть використовувати ці вади для проведення атаки типу "Man in the Middle", відомої як "отруєння" LLMNR і NBT-NS. Атака виконується наступним чином: коли комп'ютер у мережі намагається встановити з'єднання з іншим комп'ютером, він спочатку спробує використовувати DNS для визначення IP-адреси цього комп'ютера. Якщо DNS-запит не успішний, комп'ютер спробує використовувати LLMNR або NBT-NS для визначення IP-адреси.

У цей момент зловмисник може втрутитись і відповісти на запит, надіславши свою IP-адресу замість правильної. Оскільки LLMNR та NBT-NS не перевіряють, чи є відповідь вірною, комп'ютер, який намагається встановити з'єднання, прийме неправильну IP-адресу і встановить з'єднання з комп'ютером зловмисника. Зловмисник тоді може перехопити інформацію, яка передається між двома комп'ютерами.

Такі атаки можуть бути особливо шкідливими, оскільки вони можуть дозволити зловмисникам отримати доступ до конфіденційної інформації, такої як імена користувачів і паролі. Щоб захиститись від таких атак, можна відключити протоколи LLMNR та NBT-NS, а також використовувати сильні паролі та шифрування для захисту даних.

2.4 Недостатній рівень аудиту та моніторингу

Kerberos — це мережева система аутентифікації, розроблена в MIT, що забезпечує сильну аутентифікацію для клієнт-серверних додатків за допомогою секретного ключа криптографії. Однак, як і будь-яка система безпеки, Kerberos потребує постійного аудиту та моніторингу, щоб гарантувати безпечність та ефективність.

Мінімальні вимоги до аудиту та моніторингу в системі Kerberos мають включати регулярний аудит журналів системи, моніторинг в реальному часі активності користувачів та системи, а також використання автоматизованих систем для ефективного аналізу даних. Крім того, важливо мати чітку стратегію реагування на інциденти, щоб швидко реагувати на будь-які виявлені проблеми.

Kerberos сам по собі не включає вбудованих інструментів аудиту та моніторингу, але забезпечує засоби для збору даних для подальшого аналізу. Він веде журнали подій, які можуть бути аналізовані за допомогою зовнішніх інструментів. Ці журнали включають важливу інформацію про всі аутентифікаційні сесії, включаючи час, дату, ім'я користувача та адресу сервісу.

Вбудовані можливості Kerberos обмежуються лише збором даних. Він не надає інструментів для їх аналізу, тривожних сигналів або автоматизації процесу аудиту. Це означає, що адміністратори системи повинні використовувати зовнішні інструменти або вручну аналізувати журнали, що може бути часозатратним.

Active Directory (AD) включає більш потужні вбудовані інструменти аудиту та моніторингу. AD підтримує ведення детальних журналів безпеки, які включають інформацію про аутентифікацію, авторизацію, оновлення каталогів та інші події. Ці журнали можна аналізувати вручну або за допомогою зовнішніх інструментів.

AD також має вбудовану підтримку аудиту групових політик, що дозволяє адміністраторам відстежувати зміни в конфігураціях безпеки. І, нарешті, AD має вбудовані інструменти для моніторингу стану служби та виконання, що можуть допомогти виявити проблеми з процесом аутентифікації або доступом до ресурсів.

Хоча AD має вбудовані інструменти аудиту та моніторингу, вони все ще можуть бути недостатніми для виявлення складних або тонко маскированих атак. Наприклад, AD не має вбудованих інструментів для аналізу поведінки або виявлення аномалій, що можуть свідчити про внутрішні загрози або витончені атаки на основі ідентифікації. Більше того, вбудовані інструменти AD можуть бути складними в налаштуванні та використанні, особливо для великих або складних середовищ.

Висновки за розділом 2

Кожен власник інформаціної системи повинен розуміти відповідальність, яка супроводжує її утримання. Kerberos здебільшого використовується у корпоративних розподілених інфраструктурах, з великою кількість користувачів та підрозділів. Особливості Kerberos полягають в чудовій маштабованості, тому вона зустрічається практично у кожному корпоративному середовищі.

Зважаючи на розміри корпорації, чим маштабніша вона, тим більше інформації у ній знаходиться, тим більше шанс, що серед цієї інформації є критична, і тому обов’язково потрібно усвідомлювати усі ризики, пов’язані з її обробкою. Важливо оцінити та обробити всі можливі ризики, наприклад:

Витік інформації: Витоки інформації відбуваються, коли недобросовісні особи отримують доступ до конфіденційних даних. Використання застарілих алгоритмів шифрування створює вразливості, які можуть бути використані для декодування зашифрованої інформації. Це може включати персональні дані, фінансову інформацію, комерційні секрети або іншу цінну інформацію. Наслідки витоку інформації можуть бути руйнівними для організації, особливо якщо втрачена інформація включає конфіденційні або чутливі дані. Організація може страждати від фінансових втрат, законодавчих санкцій або шкоди для репутації.

Несанкціонований доступ: Зловмисники можуть використовувати вразливості старих алгоритмів для отримання доступу до системи або ресурсів, які вони нормально не могли б обслуговувати. Це може означати незаконний доступ до файлів, баз даних, адміністративних прав або будь-яких інших ресурсів, які мають бути захищені. Якщо зловмисники отримують несанкціонований доступ до системи, вони можуть керувати ресурсами організації, змінювати інформацію або викрасти дані. Це може призвести до значних фінансових втрат, збоїв в роботі та порушень безпеки.

Порушення цілісності даних: Цей ризик відноситься до можливості незаконної модифікації даних. Застарілі алгоритми хешування можуть бути вразливі до колізій, де два різних вхідних повідомлення дають однаковий хеш. Це може дозволити зловмисникам змінювати дані без виявлення. Порушення цілісності даних може призвести до помилок в даних, неправильних рішень, заснованих на невірних даних, і можливої втрати важливої інформації. Організація може зіткнутися з проблемами в управлінні даними, які можуть призвести до зниження продуктивності та фінансових збитків.

Використання ресурсів: Застарілі алгоритми часто менш ефективні за сучасні аналоги, що може призвести до зайвих витрат. Організація може витратити значні ресурси на обслуговування ненадійних систем, включаючи час, гроші та обчислювальну потужність. Підвищене використання ресурсів може призвести до зниження ефективності, збільшення витрат та зниження внутрішньої продуктивності. Організація може стикнутися з вищими витратами на обслуговування та утримання своїх систем.

Юридичні ризики: Використання застарілих алгоритмів може призвести до недотримання законодавчих або нормативних вимог. Наприклад, застарілі алгоритми можуть бути в несумісності з правилами захисту даних або індустріальними стандартами, що може призвести до штрафів або санкцій. Юридичні ризики можуть включати штрафи, санкції, цивільні позови та можливе посягання на репутацію організації. Організація може стикнутися з великими фінансовими витратами та довготривалими репутаційними наслідками.

Потенційна шкода для репутації: Якщо стане відомо, що організація використовує застарілі алгоритми шифрування, це може пошкодити її репутацію. Це може призвести до втрати довіри з боку клієнтів, партнерів або акціонерів. Шкода для репутації може призвести до втрати довіри, втрати бізнесу та негативного впливу на відносини з партнерами та клієнтами. Організація може зіткнутися з втратою важливих бізнес-відносин та зниженням прибутковості.

Ризик внутрішньої безпеки: Зловмисники всередині організації можуть використовувати вразливості старих алгоритмів для неправомірного доступу до інформації. Це може включати крадіжку персональних даних, комерційних секретів або інших конфіденційних матеріалів. Ризик внутрішньої безпеки може призвести до витоку важливої інформації, порушення процедур безпеки та потенційного збитку. Організація може стикнутися з втратою контролю над своїми системами та інформацією.

Зрив сервісу: Атаки на застарілі алгоритми можуть привести до відмови в обслуговуванні, покладаючи під загрозу доступ до важливих сервісів. Це може призвести до втрати продуктивності, втрати бізнесу або інших негативних наслідків. Зрив сервісу може призвести до відмови в обслуговуванні, втрати доступу до важливих сервісів та зниження продуктивності. Організація може зіткнутися з проблемами доступності, що можуть призвести до втрати бізнесу та втрати довіри з боку користувачів.

В наступному розділі будуть запропоновані методи підвищення захищеності інформаційних систем на базі Kerberos для уникнення описаних ризиків та вразливостей.

РОЗДІЛ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ ДЛЯ ВДОСКОНАЛЕННЯ ЕФЕКТИВНОСТІ KERBEROS

3.1 Використання сучасних алгоритмів шифрування

Важливим елементом системи безпеки Kerberos є алгоритми шифрування, які використовуються для захисту інформації під час передачі через ненадійні мережі. Оскільки Kerberos був розроблений ще в 80-х роках минулого століття, деякі з алгоритмів шифрування, які були актуальними тоді, зараз можуть бути застарілими і недостатньо безпечними.

З огляду на швидкий розвиток технологій і постійне зростання обчислювальної потужності сучасних комп'ютерів, використання найсучасніших алгоритмів шифрування стає все більш важливим.

AES (Advanced Encryption Standard) є одним з найпопулярніших алгоритмів шифрування сьогодення. Він був розроблений NIST (National Institute of Standards and Technology) США і став стандартом для урядового застосування. AES є міцним і надійним вибором для захисту даних і широко використовується у всьому світі.

Kerberos підтримує використання AES, але важливо, щоб усі компоненти системи (включаючи сервери Kerberos, клієнтські машини та сервіси) були правильно налаштовані на використання AES. Додатково, важливо регулярно перевіряти, щоб всі системи були оновлені та підтримували останні версії AES.

Для покращення алгоритмів шифрування та хешування в системі Kerberos, можна використати наступні рекомендації та підходи:

Переглянути поточні алгоритми шифрування та хешування: Перше, що потрібно зробити, - це ретельно переглянути використовувані в системі алгоритми шифрування та хешування. Це включає в себе перевірку того, чи використовуються які-небудь застарілі або вразливі алгоритми.

Перевірка, які алгоритми шифрування використовуються у налаштуванні Kerberos, використовуючи утиліту kadmin для перевірки принципалів і ключів.

Це виконується наступним чином:

1. Отримати список усіх принципалів: отримати список усіх принципалів можливо за допомогою інструменту kadmin за допомогою команди, схожої на kadmin -q "listprincs".

2. Перевірити кожного принципала: для кожного принципала у списку потрібно перевірити деталі принципала за допомогою команди на зразок kadmin -q "getprinc <principal_name>". Замініть <principal_name> фактичним принципалом із вашого списку.

3. У вихідних даних команди getprinc необхідно побачити рядок, який говорить щось на зразок Key: vno 1, aes256-cts-hmac-sha1-96, no salt. Частина aes256-cts-hmac-sha1-96 — це алгоритм шифрування. Варто звернути увагу, що принципали можуть мати кілька ключів з різними типами шифрування.

Якщо кількість принципалів велика і потрібно перевірити це програмним шляхом, може знадобитися написати сценарій, який циклічно обходить кожного принципала, викликає getprinc для кожного з них і аналізує вихідні дані, щоб отримати тип шифрування.

Необхідно пам’ятати, завжди звертайись до документації або служби підтримки Kerberos щодо будь-яких конкретних деталей, які можуть стосуватися налаштування.

4. Оновити алгоритми до найновіших версій: Якщо застарілі алгоритми все ще використовуються, їх необхідно замінити на більш сучасні та безпечні варіанти. Наприклад, якщо використовується DES або 3DES, рекомендується перейти на AES.

Стандарт шифрування даних (DES) вважається небезпечним через відносно малий розмір ключа, що робить його вразливим до атак грубої сили. Рекомендується використовувати з Kerberos більш надійні типи шифрування, наприклад Advanced Encryption Standard (AES).

Ось загальні вказівки щодо того, як відмовитися від шифрування DES у налаштуваннях Kerberos. Зауважте, що конкретна реалізація може відрізнятися та потребуватиме додаткових кроків. Необхідно завжди створювати резервні копії даних і тестувати зміни в контрольованому середовищі, перш ніж застосовувати їх у робочому середовищі.

5. Перевірка принципалів, зашифрованих DES: перевірте базу даних KDC (Центр розподілу ключів) на наявність будь-яких існуючих принципалів, зашифрованих DES. Це можна зробити за допомогою інструменту kadmin у більшості реалізацій Kerberos за допомогою команди, подібної до kadmin -q "getprinc <principal_name>".

6. Необхідно повторно зашифрувати принципали за допомогою більш надійного типу шифрування: якщо знайдено принципали, які використовують шифрування DES, потрібно змінити тип шифрування на більш надійний алгоритм, як-от AES. Це можна зробити за допомогою інструменту kadmin за допомогою команди, подібної до kadmin -q "modprinc -e aes256-cts:normal <principal_name>". Ця команда змінить тип шифрування принципала на AES-256. Необхідно виконати це для кожного принципала, зашифрованого DES, знайденого на кроці 1.

7. Оновіть конфігурацію KDC: редагуючи файл kdc.conf, щоб видалити будь-які згадки про шифрування DES. У розділах [libdefaults] і [realms] необхідно переконатись, що ваші параметри default_tkt_enctypes, default_tgs_enctypes і permitted_enctypes не містять типів DES. Замініть їх сильнішими типами, наприклад AES256-CTS.

8. Оновіть конфігурацію клієнта: редагуючи файл krb5.conf на кожній клієнтській машині, щоб видалити будь-які згадки про шифрування DES. Знову необхідно дивитись на параметри default_tkt_enctypes, default_tgs_enctypes і permitted_enctypes у розділі [libdefaults].

9. Перезапуск служб Kerberos: залежно від вашої Kerberos і операційної системи потрібно перезапустити KDC і будь-які пов’язані служби Kerberos, щоб зміни набули чинності.

10. Перевірка налаштування: необхідно переконатись, що автентифікація Kerberos все ще працює належним чином. Для цього можна використовувати інструменти kinit, klist і kvno.

11. Заміна заповнювачів <principal_name> фактичними іменами принципалів у вашому середовищі Kerberos. Завжди необхідно звертатись до документації або

служби підтримки Kerberos щодо будь-яких конкретних деталей, які можуть стосуватися вашого налаштування.

12. Навчання персоналу: Усі адміністратори та персонал, який працює з Kerberos, повинні отримати достатній рівень освіти та навчання з питань безпеки, щоб вони розуміли нові алгоритми та вміли їх правильно використовувати.

На практиці це виглядає таким чином:

Коли зловмисник викрадає хеші з Kerberos, то він бачить усі види шифрування що там використовуються, побачився умовний DES, йому буде дуже просто його зламати.

1. Спроба провести атаку DCSync та викрасти ключі Kerberos (рис. 3.1).

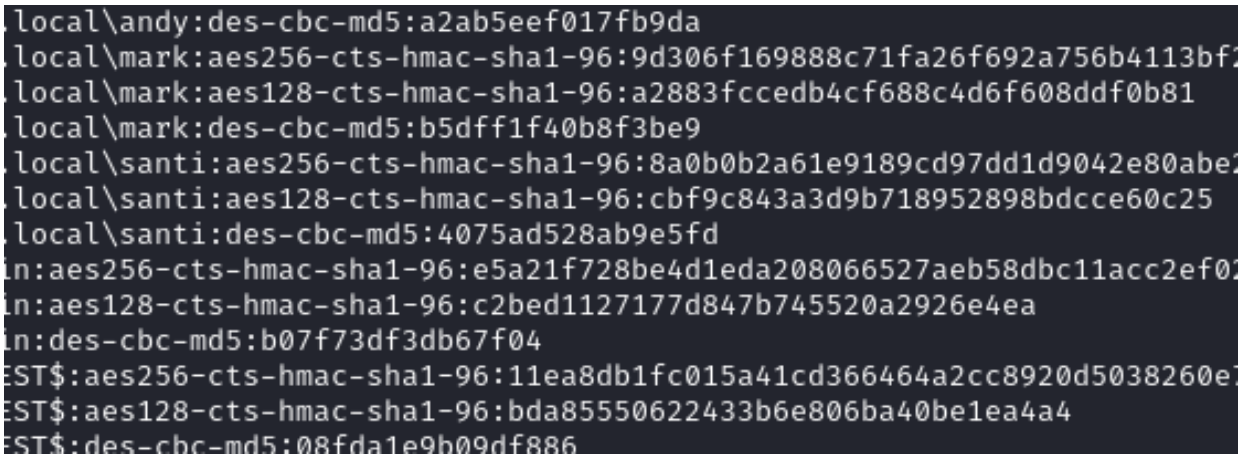

Рисунок 3.1 – Результат атаки DCSync

2. Атака пройшла успішно, скасування зберігання використовуєчи шифр DES (рис. 3.2).

3. Спроба знову відтворити дії зловмисника та викрасти ключі, відповідно до рис. 3.3.

4. Спостерігаєьбся лише шифрування AES, яке дуже стійке до зламу.

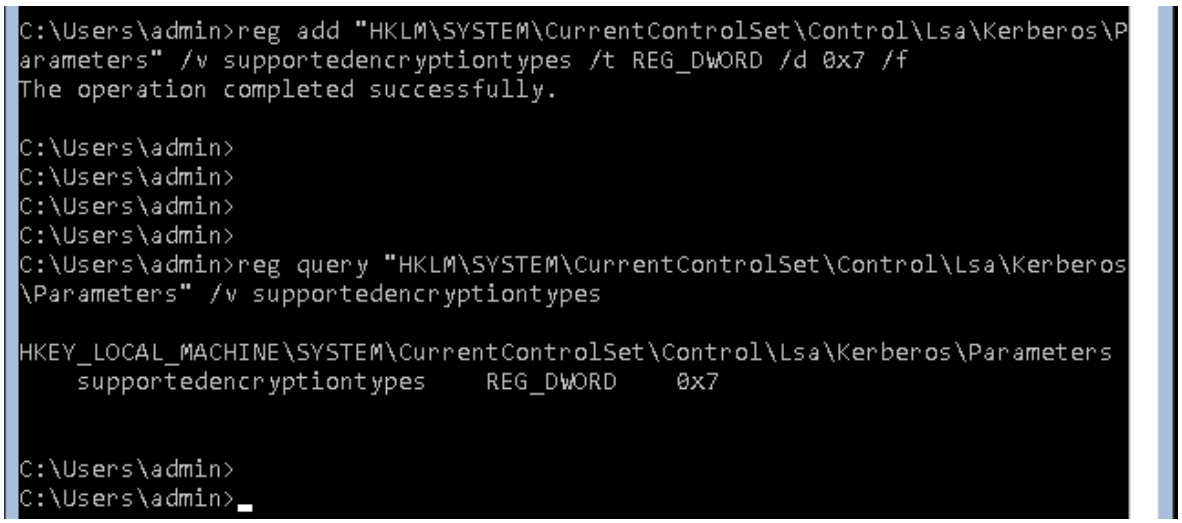

Рисунок 3.2 – Заборона використання DES

Рисунок 3.3 – Результат повторної атаки DCSync

3.2 Захист каналу зв'язку

Kerberos є протоколом мережевої аутентифікації, який використовується Active Directory для аутентифікації користувачів і служб. Протокол Kerberos використовує симетричне шифрування і взаємну аутентифікацію для забезпечення безпечного обміну інформацією в мережі. Але навіть при цьому, система завжди потребує покращення.

Деякі методи захисту каналу зв'язку в Active Directory:

- Використання шифрування: Важливо включити шифрування каналу зв'язку в Active Directory. Це можна зробити за допомогою протоколу SSL/TLS (Secure Sockets Layer/Transport Layer Security). Використання SSL/TLS дозволяє шифрувати дані, які передаються між клієнтом і сервером, запобігаючи перехопленню і читанню конфіденційної інформації.

- Використання сертифікатів: Рекомендується встановлювати SSL-сертифікати для серверів Active Directory. Це дозволяє клієнтам перевіряти автентичність сервера і гарантує, що комунікація відбувається з вірогідним джерелом.
- Використання IPSec: IPSec (Internet Protocol Security) - це набір протоколів, що забезпечують захищену комунікацію на рівні мережевого протоколу IP. Використання IPSec дозволяє шифрувати та аутентифікувати дані, які передаються між комп'ютерами, що з'єднані в мережі Active Directory.
- Обмеження доступу до каналу зв'язку: Важливо налаштувати правильні політики доступу, які обмежують доступ до каналу зв'язку лише для авторизованих користувачів. Це може включати налаштування брандмауера (firewall) для блокування недозволених підключень.
- Перевірка безпеки каналу зв'язку: Регулярно виконуйте аудит безпеки каналу зв'язку, щоб виявити можливі вразливості та проблеми. Використовуйте інструменти, які дозволяють відстежувати, аналізувати та виправляти проблеми безпеки.

Ці методи допоможуть забезпечити захист каналу зв'язку в Active Directory і зменшити ризик несанкціонованого доступу та перехоплення конфіденційної інформації.

Детальніші рекомендації щодо їх втілення:

1. Використання шифрування:

Шифрування каналу зв'язку в Active Directory дозволяє захистити дані, що передаються між клієнтами та серверами, від перехоплення та незаконного доступу. Для реалізації цього:

- Включіть протокол SSL/TLS: Налаштуйте сервери Active Directory для використання протоколу SSL/TLS. Це може вимагати отримання та встановлення SSL-сертифікатів для серверів. SSL/TLS забезпечує шифрування даних, що передаються по мережі, тим самим зменшуючи ризик перехоплення.

2. Використання сертифікатів:

Використання сертифікатів дозволяє перевіряти автентичність сервера та забезпечує безпечну комунікацію. Ось кілька рекомендацій:

- Отримайння SSL-сертифікатів: Зверніться до надійного постачальника SSL-сертифікатів та отримайте сертифікати для серверів Active Directory. Це забезпечить довіру до серверів з боку клієнтів та допоможе уникнути атак "людина посередині".
- Встановіть сертифікати: Після отримання сертифікатів встановіть їх на сервери Active Directory. Це можна зробити через керування сертифікатами у системних налаштуваннях серверів.

3. Використання IPSec:

IPSec є протоколом, який забезпечує шифрування та аутентифікацію комунікації на рівні мережевого протоколу IP. Ось як реалізувати його в Active Directory:

- Налаштуйте правила IPSec: Використовуйте налаштування групової політики для визначення правил IPSec, які будуть застосовуватись до серверів Active Directory. Ці правила повинні включати шифрування та аутентифікацію даних, що передаються.
- Включіть IPSec на комп'ютерах: Необіхно переконатись, що всі комп'ютери, які взаємодіють з Active Directory, налаштовані на використання IPSec. Це вимагає налаштування мережевих налаштувань і правил IPSec на кожному комп'ютері.

4. Використання обмеження доступу до каналу зв'язку:

Для забезпечення безпеки каналу зв'язку важливо обмежити доступ лише для авторизованих користувачів.

5. Використання брандмауеру:

Налаштуйте брандмауер на серверах Active Directory, щоб блокувати недозволений доступ до каналу зв'язку. Встановіть правила брандмауера, які дозволять тільки необхідні мережеві з'єднання.

6. Використання контролю прав доступу:

Необхідно перевірити права доступу до ресурсів Active Directory, включаючи сервери, файли та папки. Необхідно встановити строгі правила доступу та обмежте їх лише для потрібних користувачів.

7. Перевірка безпеки каналу зв'язку:

Регулярна перевірка безпеки каналу зв'язку допоможе виявити потенційні вразливості та проблеми.

8. Використання сканера безпеки:

Необхідно регулярно застосовувати спеціалізовані інструменти сканування безпеки, які перевіряють конфігурацію серверів Active Directory, шукають потенційні вразливості та рекомендують заходи щодо виправлення проблем.

9. Аудит безпеки:

Необхідно налаштувати системи журналювання та моніторингу, які відстежують активність на серверах Active Directory. Дуже важливим є аналіз журнали подій для виявлення незвичайної або підозрілої активності та реагуйте на неї.

Ці рекомендації допоможуть забезпечити захист каналу зв'язку в Active Directory і зменшити ризик несанкціонованого доступу та перехоплення конфіденційної інформації. Важливо пам'ятати про необхідність постійного оновлення та перевірки безпекових заходів для відповідності найновішим стандартам безпеки.

3.3 Покращення аудиту та моніторингу системи

Огляд існуючої системи аудиту та моніторингу Kerberos передбачає детальний аналіз поточних практик, процедур і інструментів, які використовуються в організаціях для забезпечення безпеки системи Kerberos. Тут буде розглянуто загальні практики та процедури, а також виявимо недоліки та проблеми, які повинні бути присутніми в системі аудиту та моніторингу Kerberos.

Виявлення недоліків та проблем:

- Недостатній обсяг аудит-логів: Аналіз обсягу інформації, яка фіксується в аудит-логах, та виявлення можливих прогалин у реєстрації важливих подій, які можуть бути пов'язані з безпекою системи Kerberos.
- Відсутність централізованого моніторингу: Розгляд наявних механізмів централізованого моніторингу, які дозволяють виявляти та реагувати на незвичайну або підозрілу активність в системі Kerberos.
- Недостатній рівень автоматизації: Аналіз ступеня автоматизації процесів аудиту та моніторингу, виявлення можливостей для автоматизації рутинних задач і покращення ефективності.

Виявлення потенційних загроз:

- Аналіз вразливостей: Огляд потенційних вразливостей системи Kerberos, які можуть бути використані для атак або компрометації безпеки.
- Слабкі місця в процесах аутентифікації: Виявлення можливих слабких місць у процесах аутентифікації Kerberos, які можуть використовуватися для несанкціонованого доступу.

Після проведення огляду існуючої системи аудиту та моніторингу Kerberos будуть виявлені поточні практики, процедури та ідентифіковані можливі недоліки та проблеми, які можуть бути адресовані та враховані при розробці рекомендацій для покращення аудиту та моніторингу системи Kerberos.

Оцінка ефективності Kerberos передбачає аналіз результатів проведених аудитів та моніторингу системи Kerberos, виявлення прогалин у покритті та недостатньої ефективності протоколу Kerberos. Тут буде розглянуто процес оцінки, що включає аналіз звітів, журналів подій та результатів аудиту, які дають можливість зрозуміти рівень безпеки та функціональності Kerberos.

Аналіз результатів проведених аудитів:

- Огляд звітів аудиту: Аналіз згенерованих звітів аудиту, які містять інформацію про події, зміни та активність в системі Kerberos.
- Виявлення потенційних проблем: Ідентифікація можливих проблем, вразливостей або потенційних загроз, виявлених під час аудиту системи Kerberos.

- Аналіз активності користувачів: Визначення надмірної або підозрілої активності користувачів, що може вказувати на можливі порушення безпеки.

Виявлення прогалин у покритті:

- Аналіз протоколів та процедур: Визначення прогалин у протоколах та процедурах аутентифікації, авторизації та управління ключами Kerberos.
- Виявлення потенційних слабкостей: Ідентифікація можливих слабкостей в реалізації Kerberos, які можуть бути використані для атак або компрометації безпеки.
- Перевірка відповідності стандартам: Перевірка, наскільки система Kerberos відповідає безпечним стандартам та рекомендаціям безпеки.

Виявлення недостатньої ефективності:

- Оцінка продуктивності: Визначення швидкодії та продуктивності Kerberos, виявлення можливих проблем з продуктивністю, що можуть впливати на роботу системи.
- Оцінка стійкості до атак: Аналіз стійкості Kerberos до різних типів атак, виявлення можливих слабких місць у захисті та безпеці протоколу.

Порівняння результатів оцінки з прийнятими нормами та стандартами безпеки, для визначення недостатньої ефективності Kerberos.

Після оцінки ефективності Kerberos будуть ідентифіковані можливі недоліки, прогалини у покритті та недостатньої ефективності протоколу, що можуть служити основою для розробки рекомендацій та покращень аудиту та моніторингу системи Kerberos.

Покращення аудиту та моніторингу системи Kerberos

Розширена аудит-логіка:

1.1 Розробка нових аудит-логів:

1) Визначте додаткові події та інформацію, яку бажаєте включити до аудит-логів Kerberos, наприклад, спроби неуспішної аутентифікації, доступ до критичних ресурсів, зміна прав доступу тощо.

2) Створіть нову структуру аудит-логів, яка включає необхідні поля для зберігання додаткової інформації, наприклад, час події, користувача, дію, IP-адресу тощо.

3) Розробіть механізм для збору та зберігання нових аудит-логів, наприклад, налаштуйте систему аудиту для реєстрації додаткових подій або використовуйте спеціалізований інструмент для збору логів.

1.2 Вдосконалення формату аудит-логів:

1) Визначте додаткові поля або параметри, які можуть бути корисними для аналізу та виявлення аномалій, наприклад, тип події, важливість, додаткові деталі тощо.

2) Розробіть нову структуру аудит-логів, яка включає додаткові поля та параметри, і забезпечте сумісність з існуючими інструментами для аналізу логів.

3) Налаштуйте систему аудиту, щоб використовувати оновлений формат аудит-логів і зберігати додаткову інформацію про події.

Автоматизація аудиту та моніторингу:

2.1 Впровадження інтелектуальних систем аналізу:

1) Вивчіть методи машинного навчання та штучного інтелекту, що можуть бути застосовані для аналізу аудит-логів та виявлення підозрілих активностей.

2) Зіберіть навчальний набір даних, що містить історичні дані аудиту та моніторингу, які використовувалися для розробки та навчання моделей машинного навчання.

3) Налаштуйте та навчіть моделі машинного навчання на основі навчального набору даних, щоб вони здатні були виявляти незвичайні активності, аномалії або підозрілі події.

2.2 Розробка автоматизованих правил та сценаріїв:

1) Визначте правила та сценарії, які вказують на можливі загрози або проблеми в системі Kerberos, наприклад, надмірні спроби аутентифікації, зміни прав доступу без авторизації тощо.

2) Розробіть систему або інструмент, який може автоматично перевіряти аудит-логи та моніторити систему Kerberos на виконання визначених правил та сценаріїв.

3) Налаштуйте систему, щоб автоматично виявляти підозрілу активність, генерувати сповіщення або виконувати певні дії в разі виявлення відхилень від встановлених правил.

3.1 Використання аналізу великих даних:

1) Зберіть великий обсяг даних аудиту та моніторингу, що містить історичну інформацію про активності, події та статистику системи Kerberos.

2) Застосуйте технології аналізу великих даних для виявлення залежностей, шаблонів та аномалій, які можуть вказувати на потенційні загрози або проблеми безпеки.

3) Розробіть алгоритми аналізу, що використовуються для обробки великого обсягу даних та виявлення важливих закономірностей.

3.2 Реалізація прогностичного аналізу:

1) Застосуйте методи прогностичного аналізу, такі як аналіз часових рядів або прогнозування, для передбачення майбутніх проблем або загроз безпеці на основі історичних даних.

2) Розробіть моделі прогнозування, що використовуються для передбачення можливих проблем або несправностей у системі Kerberos.

3) Використовуйте прогнозні моделі для попередження можливих проблем та прийняття заходів щодо покращення безпеки системи.

Ці кроки дозволять вам поетапно впровадити покращення аудиту та моніторингу системи Kerberos, забезпечуючи більш ефективне виявлення аномалій, підозрілих активностей та загроз безпеці. Зверніть увагу, що в реалізації цих кроків може бути необхідна експертна підтримка та використання спеціалізованих інструментів для аналізу даних та автоматизації.

Використання сучасних технологій та інструментів може суттєво покращити аудит та моніторинг системи Kerberos. Нижче розглянуті деякі з таких технологій та інструментів, які можуть бути використані для досягнення цієї мети:

- SIEM (Security Information and Event Management)

SIEM-платформи, такі як Splunk, IBM QRadar, ArcSight, Elastic SIEM тощо, дозволяють збирати, агрегувати та аналізувати дані з різних джерел, включаючи аудит-логи Kerberos. Вони надають централізований перегляд активності, виявляють аномалії та сповіщають про потенційні загрози.

- Threat Intelligence

Використання зовнішніх джерел інформації про загрози, таких як бази даних від провідних вендорів антивірусного програмного забезпечення або групи інформаційної безпеки, дозволяє виявляти відомі загрози та атаки, які можуть впливати на систему Kerberos.

- User and Entity Behavior Analytics (UEBA)

UEBA-платформи, наприклад Exabeam, Securonix, Rapid7, використовують машинне навчання для аналізу активності користувачів та виявлення незвичайних або підозрілих дій. Це допомагає виявляти атаки, зламів акаунтів або недозволений доступ до системи Kerberos.

- Security Orchestration, Automation, and Response (SOAR)

SOAR-платформи, такі як Demisto, Phantom, Swimlane, дозволяють автоматизувати процеси реагування на інциденти безпеки. Вони поєднують аналітичні дані, автоматизацію та реагування на інциденти, щоб забезпечити швидке реагування на підозрілі активності або атаки на систему Kerberos.

- Machine Learning and Artificial Intelligence

Використання методів машинного навчання та штучного інтелекту дозволяє розробити моделі, які можуть аналізувати великі обсяги даних аудиту та моніторингу Kerberos для виявлення аномалій, прогнозування загроз та виявлення невідомих атак.

- Розподілене зберігання та обробка даних

Використання технологій розподіленого зберігання та обробки даних, таких як Apache Hadoop або Apache Spark, дозволяє ефективно збирати, обробляти та аналізувати великі обсяги даних аудиту та моніторингу Kerberos.

- Контроль доступу на основі ролей (RBAC) та принципу найменших привілеїв (Least Privilege)

Використання RBAC- та Least Privilege-принципів дозволяє забезпечити обмеження доступу до ресурсів Kerberos лише на необхідний рівень, зменшуючи ризик компрометації акаунтів та привілеїв.

Кожна з цих технологій та інструментів має свої особливості та вимоги до реалізації. При впровадженні використовуйте розроблені виробниками документації та рекомендації, а також проконсультуйтеся з експертами з інформаційної безпеки для забезпечення правильної настройки та інтеграції з системою Kerberos.

3.4 Виправлення наявних вразливостей в архітектурі протоколу

I. Атаки типу Pass the Hash, Pass the Ticket, Pass the Cache, Skeleton Key

Атаки типу Pass the Hash, Pass the Ticket, Pass the Cache, Skeleton Key - це різновиди атак на системи аутентифікації, які зловмисники використовують для отримання несанкціонованого доступу до комп'ютерних систем.

Для запобігання вразливостей даного типу атак необхідно дотримуватися наступних правил:

1. Включення Defender Windows Credential Guard допомагає захистити систему від атак типу "pass the hash" та "pass the ticket". Ця функція ізолює хеші паролів користувачів, утримуючи їх в захищеному середовищі і недоступними для зловмисників.

2. Вимкнення хешів Lan Management (LM) зменшує вразливість до атак типу "pass the hash". Хеші LM більш вразливі до зламування, тому вимкнення їх допомагає запобігти зловживанню і отриманню доступу до системи через ухилення від перехоплення хеш-значень паролів.

3. Обмеження кількості облікових записів з правами адміністратора допомагає зменшити ризик атак та поширення привілеїв зловмисниками. Це рекомендується, оскільки кожен обліковий запис з правами адміністратора може стати ціллю зловмисників та потенційним джерелом зламу системи.

4. Уникання використання протоколу Remote Desktop Protocol (RDP) для керування робочими станціями користувачів є запобіжним заходом проти атак типу

"pass the hash". RDP може бути вразливим до зламування, і його використання для віддаленого адміністрування може викласти систему на ризик зламу пароля і незаконного доступу.

5. Визначення захищених адміністративних машин допомагає забезпечити безпеку при керуванні системою. Це включає використання фізично або логічно ізольованих комп'ютерів з підвищеними рівнями безпеки та обмеженим доступом, що допомагає запобігти компрометації адміністративного середовища.

6. Використання Microsoft Local Administrator Password Solutions дозволяє автоматично управляти та змінювати паролі локальних адміністраторських облікових записів на комп'ютерах. Це допомагає зменшити ризик атаки "pass the hash", оскільки паролі регулярно оновлюються і зберігаються в захищеному місці.

7. Встановлення правил брандмауера для запобігання атакам "pass the hash" допомагає контролювати комунікацію між системами і обмежувати можливості зловмисників використовувати отримані хеші паролів.

8. Надання навчання з питань безпеки користувачам системи допомагає підвищити рівень усвідомлення щодо загроз безпеці та методів захисту. Це включає навчання користувачів про потенційні ризики атак типу "pass the hash" та навички безпечного ведення роботи в мережі.

9. Обмеження прав облікових записів доменних адміністраторів допомагає зменшити потенційний вплив атаки на систему. Це включає обмеження доступу до облікових записів доменних адміністраторів лише на контролерах доменів та обмежених серверах.

10. Використання системи управління інформацією та подіями безпеки (SIEM) допомагає виявляти та реагувати на аномальну активність, включаючи атаки типу "pass the hash". SIEM забезпечує моніторинг та аналіз подій з різних джерел для виявлення потенційних загроз та вразливостей.

11. Автоматизація частої зміни паролів для системних адміністраторів допомагає зменшити ризик успішної атаки "pass the hash". Часті зміни паролів підвищують безпеку і ускладнюють заволодінням довіреними обліковими записами.

12. Скидання пароля вбудованого облікового запису KRBTGT двічі допомагає скасувати діючі golden tickets, що використовуються для аутентифікації та отримання привілеїв. Це сприяє запобіганню атакам "pass the ticket".

13. Забезпечення локальних адміністраторських облікових записів складними та унікальними паролями допомагає запобігти атакам "pass the hash". Сильні паролі зменшують ризик зламу та використання паролів для отримання доступу до системи.

14. Обмеження прав доменних адміністраторських облікових записів на контролерах доменів та обмежених серверах допомагає зменшити ризик атаки на систему. Це дозволяє обмежити можливості зловмисників у разі компрометації облікового запису доменного адміністратора.

15. Користувачеві не дозволяється бути локальним адміністратором для декількох систем. Це зменшує ризик, що компрометація одного облікового запису дозволить зловмисникам отримати доступ до багатьох систем, що може стати причиною атак типу "pass the hash".

16. Зменшення кількості облікових записів з підвищеними привілеями у вашому середовищі допомагає знизити потенційний ризик атаки "pass the hash". Обмеження кількості привілейованих облікових записів знижує поверхню атаки та забезпечує більшу контрольованість.

17. Відстежування змін налаштувань шифрування допомагає виявляти неправомірні дії та зміни, які можуть вказувати на атаки типу "pass the hash". Це дозволяє оперативно реагувати на вразливості та виявляти можливі порушення безпеки.

18. Моніторинг подій з ID 7045, 4673, 4611 та 4611 на виявлення аномалій допомагає виявляти підозрілу активність та можливі атаки, включаючи атаки "pass the hash". Аномалії в цих подіях можуть свідчити про спроби незаконного доступу до системи.

II. Атаки типу Sliver Ticket, Golden Ticket, Diamond ticket, Cross-Domain Golden Ticket attack:

Атаки типу Sliver Ticket, Golden Ticket, Diamond ticket та Cross-Domain Golden Ticket attack є методами зламу аутентифікації в мережах Windows, які базуються на зловживанні та маніпулюванні сертифікатами та квитками безпеки (security tickets).

Усі ці атаки базуються на скомпрометованому ключі шифрування Kerberos та маніпуляції квитками безпеки, що надаються для аутентифікації в мережах Windows.

Захист від таких атак включає в себе наступні кроки:

1. Приймати сильні практики гігієни паролів для облікових записів служби:

- Паролі повинні бути випадково створені, містити щонайменше 30 символів та періодично змінюватися.

2. Активувати перевірку PAC (Privilege Attribute Certificate) для виявлення та запобігання атакам з використанням Silver tickets.

- Перевірка PAC використовується для валідації привілеїв користувача в контексті безпеки. Вона дозволяє виявити підроблені PAC, які можуть бути використані для атак Silver ticket. Активація перевірки PAC допомагає запобігти використанню неправомірно отриманих привілеїв та зберегти безпеку системи.

3. Позбутися привілеїв адміністратора у кінцевих користувачів на робочих станціях та використовувати контрольовані рішення для підвищення привілеїв.

- Даний пункт вказує на необхідність обмеження адміністративних привілеїв у робочих станціях користувачів. Замість того, щоб надавати користувачам повні адміністративні права, рекомендується використовувати контрольовані рішення, які дозволяють підвищувати привілеї в разі потреби. Це зменшує ризик використання адміністративних прав користувачами та підвищує безпеку системи.

4. Зменшити адміністративний доступ до робочих станцій та серверів до мінімуму, необхідного.

- Цей пункт вказує на необхідність обмеження рівня доступу до робочих станцій і серверів лише до необхідного мінімуму. Це означає, що користувачам та адміністраторам слід мати доступ лише до тих ресурсів, які їм дійсно потрібні для виконання їх робочих обов'язків. Зменшення адміністративного доступу допомагає знизити ризик використання привілеїв для зловмисних цілей та підвищує безпеку системи.

5. Використовувати рішення, такі як Microsoft LAPS, для створення сильних, випадкових та унікальних паролів для облікових записів локальних адміністраторів і автоматично періодично їх змінювати.

- Microsoft LAPS (Local Administrator Password Solution) є рішенням, яке дозволяє автоматично створювати унікальні та сильні паролі для облікових записів локальних адміністраторів на робочих станціях. Це знижує ризик використання слабких паролів адміністраторів та сприяє безпеці системи. Паролі автоматично змінюються періодично для запобігання можливим зламам.

6. Застосовувати рекомендовані заходи для захисту від атак Kerberoasting. Kerberoasting є методом атаки, який спрямований на отримання хеш-значень паролів облікових записів сервісів в Active Directory. Для захисту від цього типу атак рекомендується виконувати такі заходи:

- Застосування сильних паролів для облікових записів служб.
- Використання захисту SSL/TLS для зв'язку з обліковими записами служб.
- Встановлення обмежень на облікові записи служб для унеможливлення локального входу до системи.
- Періодичний аудит та моніторинг активності в Active Directory для виявлення незвичайної поведінки.

7. Не дозволяти користувачам мати адміністративні привілеї в межах безпекових границь.

- Даний пункт вказує на необхідність обмеження користувачів в доступі до адміністративних привілеїв в системі. Користувачі повинні мати доступ лише до тих ресурсів, які їм дійсно потрібні для виконання їх робочих обов'язків. Це допомагає запобігти можливості зловживання адміністративними привілеями та зменшує ризик безпекових порушень.

8. Запобігати крадіжці облікових даних:

- Впроваджувати навчання щодо безпеки для співробітників.
- Використовувати мережеві та кінцеві заходи безпеки для блокування шкідливого програмного забезпечення, що краде облікові дані, та фішингових атак.

- Використовувати настроювані фільтри паролів, такі як Azure AD Password Protection, для усунення поширених паролів та зниження успішності атак методом "спробування пароля".
- Моніторити незаконну активність Mimikatz.

9. Забезпечити безпеку Active Directory (AD):

- Впровадити принцип найменшого привілею та мінімізувати кількість користувачів та облікових записів служб, які мають доступ до контролерів доменів (DC).
- Запобігати атакам DCSync, обмежуючи облікові записи з правами доменного адміністратора або "зміни даних, які реплікуються".
- Моніторити AD на незвичайну активність, таку як зміни у складі груп.

10. Шукати підроблені квитки:

- Моніторити поведінку користувачів для виявлення незвичайних відмінностей.
- Перевіряти квитки на ознаки втручання, такі як невідповідності імені користувача та ідентифікатора родственості (RID) або зміни терміну дії квитка.
- Моніторити AD на аномальну активність, включаючи зміни у складі груп.

11. Бути обережним при зміні пароля krbtgt:

- Змінювати пароль krbtgt кожні 180 днів, як рекомендація найкращих практик.
- Розглянути зміну пароля, коли співробітник, який може створити Golden Ticket, покидає організацію.
- Дотримуватися правильних процедур оновлення пароля krbtgt та забезпечувати реплікацію на всі контролери доменів.
- Періодично скидати пароль двічі, щоб знизити ризик Golden Ticket атаки.

Спробуємо використати рекоментації та захиститись від атак по типу Pass The Hash.

1. Спроба провести атаку на систему та реалізувати Pass The Hash, використовучи інструмент wmiexec (рис. 3.4), з інструментарію Impacket. Він

дозволяє авторизуватись обходячи протокол NTML та отримати інтерактивну командну оболонку за допомогою WMI.

```
┌──(root㉿kali)-[/tmp]
└─# wmiexec.py admin@10.10.10.161 -hashes ":3008c87294511142799dca1191e69a0f"
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Cor

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
PS C:\>
```

Рисунок 3.4 – Атака PassTheHash

2. Атака пройшла успішно, спроба усунути вразливість та відключити використання LM на системах. Реалізується це за допомогою групових політик (рис. 3.5).

```
PS C:\Users\admin> Import-Module GroupPolicy
PS C:\Users\admin> $gpo = Get-GPO -Name "Default Domain Policy"
PS C:\Users\admin>
PS C:\Users\admin> Set-GPRegistryValue -Guid $gpo.Id -Key "HKLM\System\Curre
ntControlSet\Control\Lsa" -ValueName "NoLMHash" -Type DWORD -Value 1


DisplayName      : Default Domain Policy
DomainName       : htb.local
Owner            : HTB\Domain Admins
Id               : 31b2f340-016d-11d2-945f-00c04fb984f9
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 9/18/2019 10:45:57 AM
ModificationTime : 6/18/2023 3:11:00 AM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 7, SysVol Version: 7
WmiFilter        :



PS C:\Users\admin>
PS C:\Users\admin> Invoke-GPUpdate -Force
PS C:\Users\admin> Invoke-GPUpdate -Force
```

Рисунок 3.5 – Заборона використання LM

3. Спроба провести атаку повторно (рис. 3.6).

```
┌──(root㉿kali)-[/tmp]
└─# wmiexec.py admin2@10.10.10.161 -hashes ":3008c87294511142799dca1191e69a0f" -shell-type powershell
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad userna
uthentication information.)

┌──(root㉿kali)-[/tmp]
└─#
```

Рисунок 3.6 – Повторна спроба атаки PtH

4. Можна спостерігати, що авторизуватись не вдалося.

III. Атаки типу Constrained Delegation, Unconstrained Delegation, Resource-Based Constrained Delegation:

Атаки типу Constrained Delegation, Unconstrained Delegation та Resource-Based Constrained Delegation використовуються для недоброякісного використання механізму делегування в Active Directory.

Всі ці типи делегації пов'язані з ризиком використання облікових записів з правами делегації для несанкціонованого доступу до ресурсів в мережі.

Щоб запобігти таким атакам, важливо дотримуватися наступних правил:

1. Уникати використання незалежної делегації. Замість цього, необхідно налаштувати обмежену делегацію, оскільки сервери, які вважаються довіреними для обмеженої делегації, зберігають тільки службові квитки (ST), а не квитки на передачу квитків (TGT). Можливість підробки дозволена лише для певного набору служб.

2. Налаштувати облікові записи з підвищеними привілеями (наприклад, адміністратори домену) з увімкненою опцією "Обліковий запис є чутливим і не підлягає делегації". Активуючи цю опцію, облікові записи з підвищеними привілеями не можуть бути делегованими, що зменшує потенційну площу атаки.

3. Використовувати групу безпеки "Захищені користувачі" ("Protected Users"). Якщо рівень домену - Windows Server 2012 R2 або вище, додавання користувачів до цієї групи обмежує делегацію з використанням обмеженої або незалежної делегації.

4. Необхідно забезпечити безпеку серверів делегації. Встановлюйте правила брандмауера на основі призначення сервера та конфігурації делегації. Переконайтеся, що сервери регулярно оновлюються та обмежують привілеї доступу для зменшення вразливостей.

5. Вимкніть делегацію Kerberos, якщо це можливо, щоб зменшити потенційні загрози безпеці.

6. Будьте обережні при наданні привілеїв і ретельно контролюйте, кому ви надаєте права на делегацію. Увімкніть можливість довіряти комп'ютерним та

користувацьким обліковим записам для делегації лише авторизованим користувачам, які потребують необмеженої делегації Kerberos.

7. Необхідно обмежити дозволи Active Directory. Регулярно переглядайте та керуйте правами доступу в Active Directory, оскільки зміна атрибутів об'єктів комп'ютера або наявність надмірних членств в групах або можливість скидання паролів можуть бути використані зловмисниками. Використовуйте інструменти, наприклад, BloodHound, для виявлення та усунення уразливостей безпеки.

8. Переконайтеся, що чутливі облікові записи, які не повинні бути делегованими, позначені як такі. Увімкніть опцію "Обліковий запис є чутливим і не підлягає делегації" або включіть облікові записи до групи "Захищені користувачі" ("Protected Users"), щоб запобігти атакам з обмеженою делегацією ресурсів.

IV. Атаки типу Kerberoasting, AS-REProasting, Abuse Forest Trusts, SID-History Injection attack:

Атаки типу Kerberoasting, AS-REProasting, Abuse Forest Trusts та SID-History Injection атаки є методами, які зловмисники використовують для отримання незаконного доступу до ресурсів у середовищі Active Directory.

У всіх цих атак спільне те, що вони використовують вразливості в аутентифікаційних та авторизаційних механізмах Active Directory для незаконного отримання доступу до ресурсів та підвищення привілеїв. Захист від цих атак включає налагодження обмежень на делегування, використання захищених груп та правильне налаштування довірчих відносин між лісами.

Для запобігання уникненню шкоди від даного типу атак рекомендовано дотримуватися наступних кроків:

1. Встановлюйте довгі та складні паролі для облікових записів служб і користувачів: важливо використовувати паролі, які складаються з комбінації великих і малих літер, цифр та спеціальних символів. Чим складніший пароль, тим складніше його підібрати зловмиснику.

2. Змінюйте паролі регулярно або згідно з встановленою політикою безпеки: рекомендується регулярно змінювати паролі для унеможливлення зламу або

використання старих паролів зловмисниками. Це може бути щорічне оновлення або встановлення конкретних строків для зміни паролів.

3. Обмежуйте дозволи облікових записів до мінімуму, необхідного для їх функціонування: уникайте надання зайвих привілеїв користувачам або службам. Кожен обліковий запис повинен мати лише необхідні дозволи для виконання своїх функцій, що допоможе зменшити потенційні ризики.

4. Уникайте розміщення облікових записів у групі Domain Admins або інших груп з високими привілегіями: необхідно обмежувати доступ до облікових записів з надлишковими привілегіями. Розміщення облікових записів у групах з високими привілеями збільшує ризик несанкціонованого доступу та можливих атак.

5. Активуйте попередню аутентифікацію Kerberos для всіх облікових записів: попередня аутентифікація Kerberos зменшує ризик атак типу Kerberoasting, вимагаючи від клієнтів надсилати початковий запит на аутентифікацію до служби.

6. Використовуйте сильні алгоритми шифрування, такі як Kerberos AES, замість менш безпечних, наприклад, RC4: використання сильних алгоритмів шифрування ускладнює розшифрування атакуючими шифрованої інформації. RC4 є застарілим і менш безпечним алгоритмом шифрування, тому рекомендується використовувати більш сучасні та безпечні алгоритми, такі як AES.

7. Періодично змінюйте паролі облікових записів користувачів і служб: через певний період часу слід змінювати паролі для усіх облікових записів. Це допоможе запобігти зламу паролів, оскільки зловмисники не матимуть довгий час доступ до старих паролів.

8. Аудитуйте зміни налаштувань попередньої аутентифікації Kerberos та переконайтеся, що вона включена за замовчуванням: важливо контролювати налаштування попередньої аутентифікації Kerberos і періодично перевіряти, що вона включена за замовчуванням. Це допоможе запобігти можливим атакам, які використовують вразливості в налаштуваннях.

9. Перевіряйте атрибути об'єктів SID History і облікові записи з привілеями SID: ретельно перевіряйте атрибути об'єктів SID History для виявлення потенційних

атак інжекції SID. Також слід перевіряти облікові записи з привілеями SID, оскільки це може бути використано зловмисниками для незаконного отримання доступу.

10. Періодично переглядайте та керуйте правами доступу в Active Directory, уникайте надлишкових привілеїв та зміни атрибутів об'єктів комп'ютера: виконуйте регулярні перевірки прав доступу в Active Directory для уникнення можливих вразливостей. Контроль за доступом до комп'ютерних об'єктів та обмеження привілеїв є важливими аспектами безпеки.

11. Використовуйте "Protected Users" security group: додавання користувачів до групи "Protected Users" обмежує можливість делегування за допомогою обмеженого або необмеженого делегування.

12. Аудитуйте та контролюйте використання лісів та міжлісових довірчих відносин: регулярно аудитуйте та контролюйте використання лісів та міжлісових довірчих відносин для виявлення можливих атак або зловживань. Забезпечення правильної конфігурації лісів та довірчих відносин є важливим для забезпечення безпеки Active Directory.

Ці рекомендації допоможуть підвищити безпеку вашої системи та запобігти атакам, пов'язаним з Kerberoasting, AS-REProasting, зловживанням довірчих відносин та інжекцією SID History.

Однією з важливих рекомендацій є регулярний аудит інформаційних систем на базі Kerberos, на прикладі показано простий аудит за допомогою інструменту з відкритим кодом PingCastle.

1. Встановлення та запуск PingCastle (рис. 3.7)

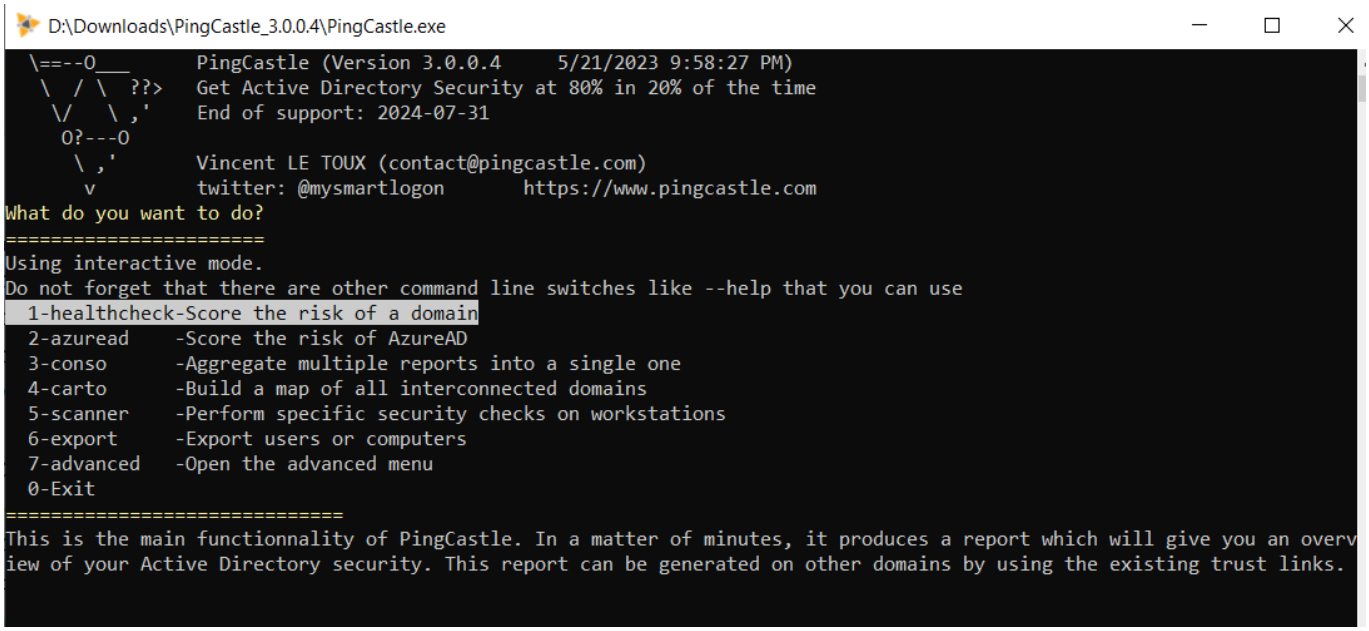

Рисунок 3.7 – Вікно інструменту Ping Castle

2. Вибирано пункт 1 (healthcheck) (рис. 3.8):

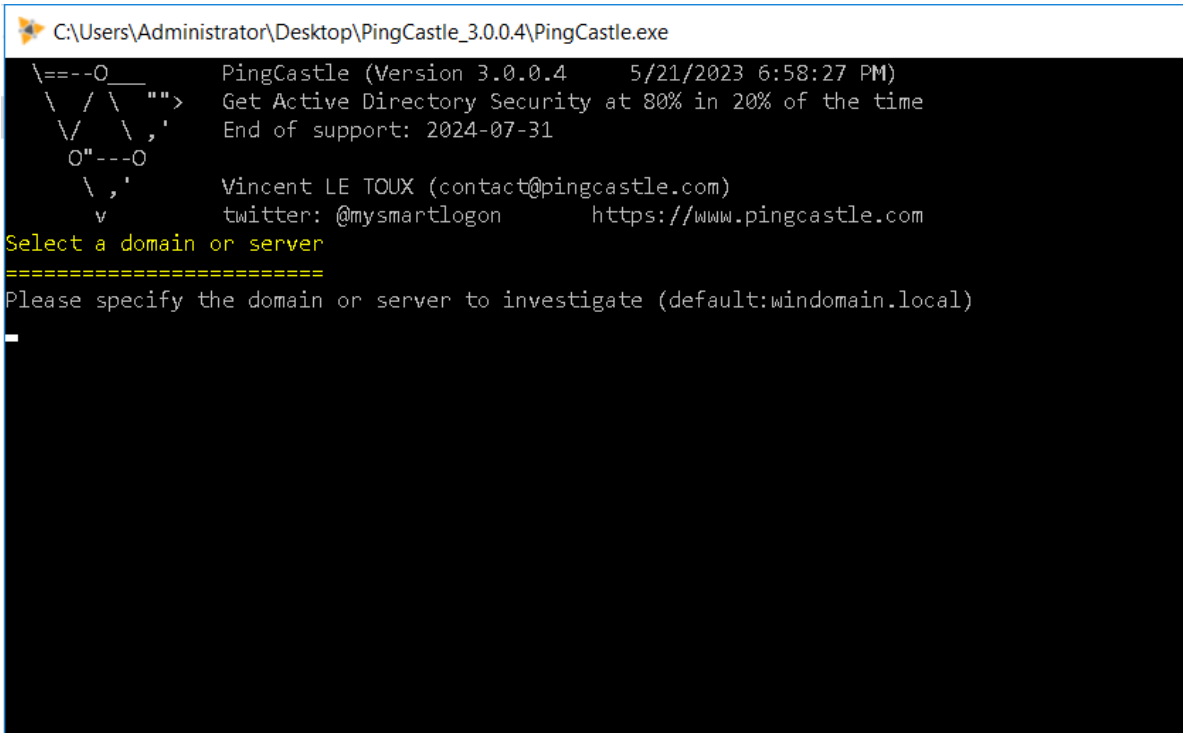

Рисунок 3.8 – Налаштування аудиту Ping Castle

3. Аудит почався, по закінченню, отримано звіт в форматі HTML (рис. 3.9), у ньому позначений стан Active Directory за деякими критеріями:

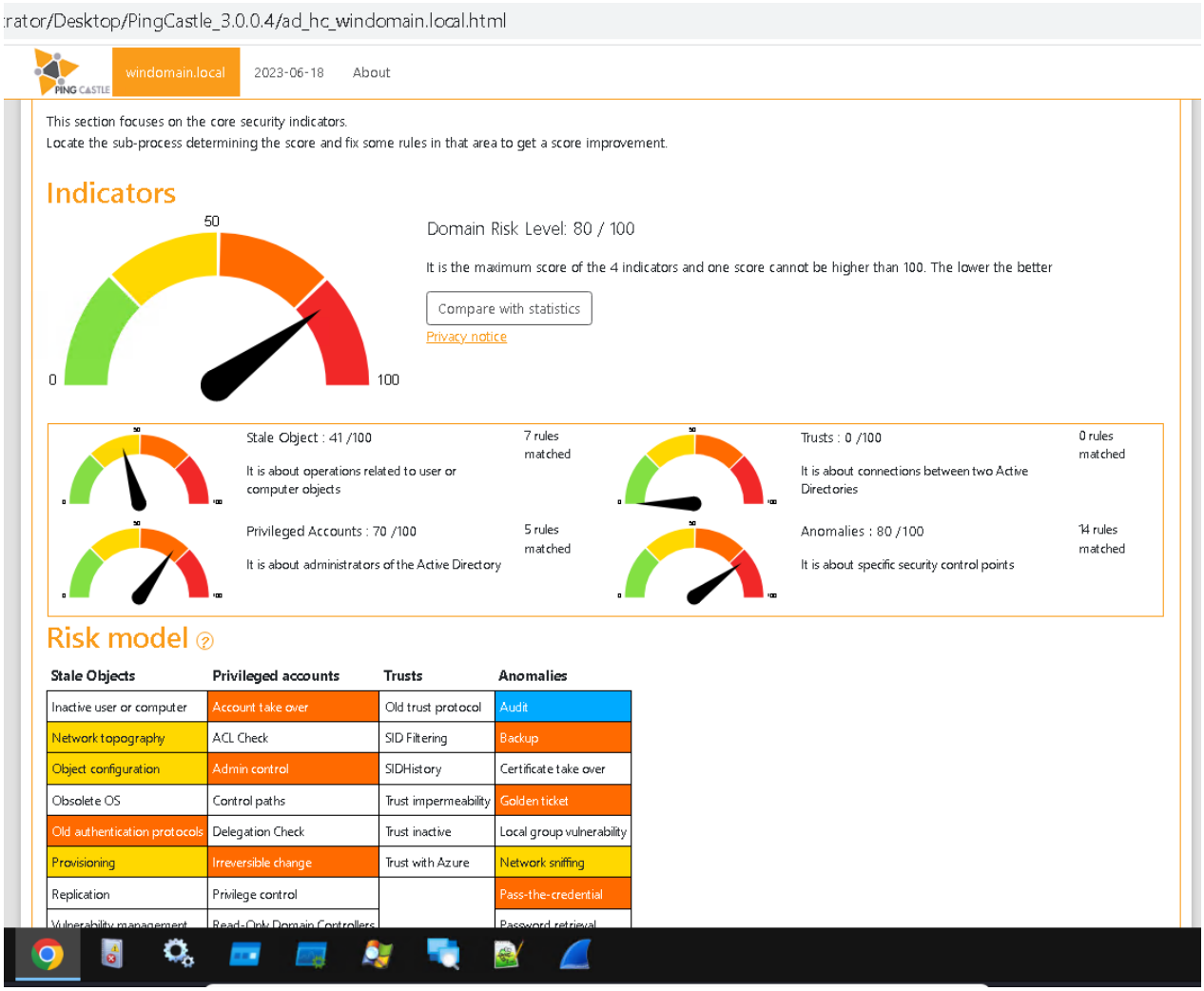

Рисунок 3.9 – Результат аудиту Ping Castle

4. Нижче у звіті можна побачити знайдені проблеми, їх критичність та опис (рис. 3.10 – 3.11):

Рисунок 3.10 – Вразливості, знайдені під час аудиту

Рисунок 3.11 – Вразливості, знайдені під час аудиту

5. Користуючись звітом, команда з ІБ повинна проаналізувати та усунути знайдені вразливості, доналаштувати систему.

Висновки за розділом 3

В ході даного розділу було викладено практичні напрацювання, що покроково супроводжують інтеграцію та підтримку системи дискреційного керування доступом в інформаційних системах. В першому пункті було описано рекомендації стосовно того, як краще підходити до вибору та підготовки до впровадження системи дискретного управління доступом, наведено опис вимог, які необхідно підготувати, перш ніж переходити до безпосереднього встановлення такої системи.

В другому пункті вже було змодельовано потенційну інформаційну систему, в якій для керування правами доступу за основу вибрана дискреційна модель. Програмний застосунок виконано у спрощеному вигляді для демонстрації саме процесу отримання доступу суб’єктів до конкретних об’єктів за алгоритмом дискреційної моделі.

В третьому ж пункті було наведено перелік рекомендацій щодо використання додаткових засобів захисту інформації спільно з дискреційним керуванням доступу для підвищення надійності та захищеності усієї інформаційної системи.

Отримані результати можуть бути корисними для невеликих або середніх організацій, що планують використовувати дискреційну систему керування доступом для підготовки наявної інформаційної системи до її впровадження.

У результаті аналізу поточних проблем та недоліків системи Kerberos, було виявлено ризики, пов'язані з уразливостями в процесі автентифікації, застарілими алгоритмами шифрування та хешування, можливістю атак на канал зв'язку, а також недостатнім рівнем аудиту та моніторингу. Кожен власник інформаційної системи повинен усвідомлювати ці ризики, оскільки їх наслідки можуть бути руйнівними для організації.

Витік інформації є серйозним ризиком, оскільки недобросовісні особи можуть отримати доступ до конфіденційних даних. Застосування застарілих алгоритмів шифрування створює вразливості, що сприяють декодуванню зашифрованої інформації. Це може призвести до втрати цінної інформації та негативного впливу на організацію.

Несанкціонований доступ до системи або ресурсів також є серйозним ризиком. Зловмисники можуть використовувати вразливості старих алгоритмів для отримання несанкціонованого доступу до файлів, баз даних або адміністративних прав. Це може призвести до неправомірного використання ресурсів організації та викрадення чутливої інформації. Порушення цілісності даних є ще одним важливим аспектом, який потребує уваги. Застарілі алгоритми хешування можуть бути вразливі до колізій, що дозволяє зловмисникам змінювати дані без виявлення. Це може призвести до неправильних рішень та втрати важливої інформації.

Використання ресурсів також є проблемою, яка потребує уваги. Недостатній рівень аудиту та моніторингу може призвести до неефективного виявлення атак, відсутності записів про події та втрати контролю над використанням ресурсів. Це може вести до зловживання правами доступу, незаконного використання ресурсів та інших небажаних наслідків.

ВИСНОВКИ

В ході проведеного дослідження було детально розглянуто основні концепції протоколу Kerberos, включаючи його структуру, автентифікацію, методи шифрування та його використання в сучасних інформаційних системах. Це надало багато уявлень про роботу протоколу, а також визначило декілька слабких місць і вразливостей, які можуть мати вплив на безпеку системи.

Зокрема, було виявлено, що у процесі автентифікації існують певні уразливості, що можуть бути зловживані. Деякі алгоритми шифрування та хешування, використовувані в Kerberos, є застарілими та потребують оновлення для відповідності сучасним стандартам. Є також потенційні ризики з атаками на канал зв'язку, а також виявлено недостатній рівень аудиту та моніторингу в системі Kerberos.

В рамках цієї роботи було також розроблено низку рекомендацій щодо вдосконалення ефективності та безпеки протоколу Kerberos. Ці рекомендації включають використання сучасних алгоритмів шифрування, покращення захисту каналу зв'язку, покращення систем аудиту та моніторингу, а також виправлення наявних вразливостей в архітектурі протоколу.

З урахуванням вищенаведеного, необхідно визнати важливість продовження досліджень в області захисту інформації та розробки нових методів та технологій для посилення безпеки протоколу Kerberos та інших систем автентифікації. Дійсно, в умовах сучасного світу, коли інформація є одним з найцінніших ресурсів, питання його захисту від несанкціонованого доступу стає все більш актуальним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Українські компанії готуються нові кібератаки - СБУ | УНІАН: https://www.unian.ua/society/2088861-na-ukrajinski-kompaniji-gotuyutsya-novi-kiberataki-sbu.html

2. Керберос / Кодекс / Orna RPG Series | New Old RPGs: https://playorna.com/codex/raids/kerberos/?lang=uk

3. Kerberos (протокол) — Вікіпедія: https://uk.wikipedia.org/wiki/Kerberos_(%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB)

4. KB5011233: Захисти в CVE-2022-21920 можуть блокувати автентифікацію NTLM, якщо автентифікацію Kerberos не вдалось - Підтримка від Microsoft: https://shorturl.at/aeBQZ

5. СБУ попереджає про можливість нової кібератаки — Наука та ІТ — tsn.ua: https://tsn.ua/nauka_it/sbu-poperedzhaye-pro-mozhlivist-novoyi-kiberataki-978260.html

6. СБУ попереджає про можливу нову кібератаку на українські підприємства і установи: https://news.dtkt.ua/state/other/44867-sbu-poperedzaje-pro-mozlivu-novu-kiberataku-na-ukrayinski-pidprijemstva-i-ustanovi

7. MIT Kerberos: List of security vulnerabilities: https://www.cvedetails.com/vulnerability-list/vendor_id-42/product_id-61/MIT-Kerberos.html

8. CVE - Search Results: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=kerberos

9. Kerberos Vulnerabilities : https://www.silverfort.com/blog/technical-analysis-of-cve-2022-33679-and-cve-2022-33647-kerberos-vulnerabilities/

10. Kerberos authentication defined: Maximizing security: https://blog.quest.com/kerberos-authentication-how-it-works-and-how-to-maximize-its-security/

11. Kerberos Tickets: Vulnerabilities and Solutions | Optiv: https://www.optiv.com/insights/source-zero/blog/kerberos-domains-achilles-heel

12. How can Kerberos protocol vulnerabilities be mitigated? | TechTarget: https://www.techtarget.com/searchsecurity/answer/How-can-Kerberos-protocol-vulnerabilities-be-mitigated

13. Kerberos Vulnerability Assessments - Attivo Networks: https://www.sentinelone.com/blog/kerberos_vulnerability_assessments/

14. Kerberos (protocol) - Wikipedia: https://en.wikipedia.org/wiki/Kerberos_(protocol)

15. Kerberos: The Network Authentication Protocol: https://web.mit.edu/kerberos/

16. What is Kerberos and How Does it Work? - Definition from SearchSecurity: https://www.techtarget.com/searchsecurity/definition/Kerberos

17. Understanding Kerberos: How It Works and Authentication Explained!: https://www.simplilearn.com/what-is-kerberos-article

18. Kerberos - GeeksforGeeks : https://www.geeksforgeeks.org/kerberos/

19. Kerberos Authentication Overview | Microsoft Learn: https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

20. Kerberos Authentication Explained: http://www.varonis.com/blog/kerberos-authentication-explained

21. What is a Golden Ticket Attack? - CrowdStrike: https://www.crowdstrike.com/cybersecurity-101/golden-ticket-attack/

22. Golden Ticket Attacks Explained and How to Defend Them - Microsoft Platform Management - Blogs - Quest Community : https://blog.quest.com/golden-ticket-attacks-how-they-work-and-how-to-defend-against-them/

23. Golden Ticket Attack: https://www.netwrix.com/how_golden_ticket_attack_works.html

24. What is Golden Ticket Attack: https://www.lepide.com/blog/what-is-a-golden-ticket-attack/

25. What is a Golden Ticket? | Security Encyclopedia: https://www.hypr.com/security-encyclopedia/golden-ticket

26. Golden Ticket Attacks Explained - QOMPLX: https://www.qomplx.com/blog/qomplx-knowledge-golden-ticket-attacks-explained/

27. Threats And Tools: https://doubleoctopus.com/security-wiki/threats-and-tools/golden-ticket/

28. Kerberos Authentication Explained: http://www.varonis.com/blog/kerberos-authentication-explained

29. Understanding Kerberos: How It Works and Authentication Explained!: https://www.simplilearn.com/what-is-kerberos-article

30. Kerberos authentication defined: Maximizing security: https://blog.quest.com/kerberos-authentication-how-it-works-and-how-to-maximize-its-security/

31. Kerberos Policy - Windows Security | Microsoft Learn: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/kerberos-policy

32. Active Directory Troubleshooting : https://www.eginnovations.com/blog/top-8-active-directory-performance-problems/

33. Guidance for troubleshooting Active Directory replication - Windows Server | Microsoft Learn: https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/troubleshoot-adreplication-guidance

34. Techniques to troubleshoot Active Directory issues | TechTarget: https://www.techtarget.com/searchwindowsserver/tip/Techniques-to-troubleshoot-Active-Directory-issues

35. Top Seven Active Directory Issues : https://blog.netwrix.com/2018/03/13/top-7-challenges-with-active-directory/

36. Strategies to Find and Fix Errors in Active Directory: https://www.scriptrunner.com/en/blog/active-directory-administration