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: Засоби виявлення вразливостей в інфраструктурі Active Directory клієнт-серверної мережі

Виконавець: студент IV курсу, групи КБ-42

_____ **Владислав ГРИЦІВ**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**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
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-42** (група) **Гриціву Владиславу Сергійовичу** (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Засоби виявлення вразливостей в інфраструктурі Active Directory клієнт-серверної мережі

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Відомості про принципи роботи та вразливості Active Directory, володіння C# для розробки власних інструментів виявлення вразливостей.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Нормативно-правова база у сфері захисту інформації, архітектура Active Directory, механізми взаємодії клієнтських хостів з домен контроллером, процес надання доступу до інформації та поширені загрози, види методів автентифікації, архітектура підсистеми, програмний засіб.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Застосування висновків та рекомендацій, описаних в цій роботі, може допомогти організаціям підвищити рівень безпеки своїх систем на основі Active Directory, зменшуючи ризик витоку інформації та інших інцидентів безпеки.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

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

Завдання прийняв до виконання _____ (підпис) Владислав ГРИЦІВ (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2022 – 4.11.2022	*виконано*
2	Аналіз відкритих джерел	28.01.2023 –20.02.2023	*виконано*
3	Освоєння основних концепцій і термінології, що стосуються Active Directory та клієнт-серверних мереж.	21.02.2023 – 04.03.2023	*виконано*
4	Вивчення типів вразливостей Active Directory та методів їх виявлення. Вивчення існуючих інструментів виявлення вразливостей.	05.03.2023 – 06.04.2023	*виконано*
6	Написання теоретичної частини роботи, що включає в себе основи Active Directory, типи вразливостей та існуючі методи їх виявлення.	07.04.2023 – 11.04.2023	*виконано*
7	Розробка власного інструменту виявлення вразливостей.	12.04.2023 – 16.04.2023	*виконано*
8	Тестування інструменту виявлення вразливостей та аналіз результатів.	17.04.2023 – 20.04.2023	*виконано*
9	Порівняльний аналіз існуючих засобів виявлення вразливостей та розробленого інструменту.	21.04.2023 – 09.05.2023	*виконано*
10	Оформлення пояснювальної записки	10.05.2023 – 12.06.2023	*виконано*

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

Завдання прийняв до виконання _____ (підпис) Влад ГРИЦІВ (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 48 сторінок, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки та список джерел. Крім того, робота містить 1 додаток із загальною кількістю сторінок 3. У пояснювальній записці кваліфікаційної роботи міститься 11 рисунків, 1 таблиця та 19 літературних джерел.

Метою роботи є розробка програмного засобу для виявлення вразливостей в інфраструктурі Active Directory.

Об'єктом дослідження є процес виявлення вразливостей в інфраструктурі Active Directory.

Предметом дослідження – механізми і засоби виявлення вразливостей в інфраструктурі Active Directory клієнт-серверної мережі.

Методи дослідження:

- аналіз відкритих джерел,
- аналіз вразливостей,
- практичні експерименти,
- синтез.

Практична цінність роботи полягає в тому, що було розроблено програмну реалізацію засобу, що виявляє вразливості в інфраструктурі Active Directory, що можуть бути використані адміністраторами мережі та професіоналами з безпеки інформації.

Ключові слова: Active Directory, вразливості безпеки, клієнт-серверна мережа, виявлення вразливостей, моніторинг, аудит, політики безпеки.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕННЬ 7

ВСТУП 8

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ТА СТРУКТУРА ACTIVE DIRECTORY 10

1.1 Визначення та функції Active Directory 10

1.2 Компоненти інфраструктури Active Directory 12

1.3 Принципи роботи Active Directory в контексті клієнт-серверних мереж 13

1.4 Ролі серверів в Active Directory 15

1.5 Об'єкти та атрибути в Active Directory 16

1.6 Політики безпеки в Active Directory 18

1.7 Механізми аутентифікації та авторизації в Active Directory 19

1.8 Реплікація та синхронізація даних в Active Directory 22

1.9 Масштабованість та висока доступність в Active Directory 23

Висновки за розділом I 24

РОЗДІЛ 2 ВРАЗЛИВОСТІ В ІНФРАСТРУКТУРІ ACTIVE DIRECTORY ТА ЗАСОБИ ЇХ ВИЯВЛЕННЯ 25

2.1 Основні типи вразливостей 25

2.2 Основні методи атак для експлуатації вразливостей в Active Directory 26

2.3 Наслідки вразливостей для інфраструктури Active Directory 28

2.4 Внутрішні засоби безпеки в Active Directory 29

2.5 Зовнішні інструменти для виявлення вразливостей 31

2.6 Порівняння інструментів для виявлення вразливостей 32

2.7 Атаки на паролі користувачів в Active Directory 33

2.8 Вразливості в механізмах реплікації Active Directory 35

2.9 Можливість розповсюдження зловмисних програм через Active Directory 36
Висновки за розділом II 38
РОЗДІЛ 3 РОЗРОБКА ТА ВПРОВАДЖЕННЯ ПРОГРАМНОГО ЗАСОБУ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В ACTIVE DIRECTORY 39
3.1 Специфікація вимог до програмного інструменту 39
3.2 Проектування архітектури програмного інструменту 40
3.3 Проектування архітектури програмного інструменту 41
3.4 Реалізація програмного інструменту 42
3.5 Тестування та впровадження програмного інструменту 43
Висновки за розділом III 44
ВИСНОВКИ 46
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 47
ДОДАТОК А 49

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕННЬ

AD	-	Active Directory.
DC	-	Domain Controller.
DNS	-	Domain Name System.
DHCP	-	Dynamic Host Configuration Protocol.
GC	-	Global Catalog.
ACL	-	Access Control List.
RODC	-	Read-Only Domain Controller.
FSMO	-	Flexible Single Master Operations.
SAM	-	Security Account Manager.
SID	-	Security Identifier.
OU	-	Organizational Unit.
GPO	-	Group Policy Object.
GUI	-	Graphical User Interface.
CLI	-	Command Line Interface.
LDAP	-	Lightweight Directory Access Protocol.
TCP/IP	-	Transmission Control Protocol/Internet Protocol.
SMB	-	Server Message Block.
RPC	-	Remote Procedure Call.
API	-	Application Programming Interface.
UDP	-	User Datagram Protocol.
Kerberos	-	Network authentication protocol.
NTLM	-	NT LAN Manager.

ВСТУП

Світ цифрової технології та інформації постійно еволюціонує, викликаючи зміни в тому, як бізнеси та організації керують своїми інформаційними ресурсами. В контексті інформаційної ери, безпека даних стала одним з найважливіших факторів успіху для багатьох організацій, особливо в умовах поширення кіберзлочинності та її потенційно негативного впливу на стабільність та продуктивність.

Active Directory (AD) — це розподілена служба керування ідентифікаторами, що забезпечує централізоване управління ресурсами в комп'ютерних мережах. AD є важливим компонентом більшості корпоративних мереж, оскільки він дозволяє адміністраторам керувати правами доступу та управлінням ресурсами, такими як сервери, робочі станції та принтери. AD також є критичною компонентою в системах ідентифікації та аутентифікації, що робить його привабливою мішенню для зловмисників.

У зв'язку з цим, виникає необхідність у систематичному аналізі можливих вразливостей в інфраструктурі AD та засобах їх виявлення, що є предметом цієї роботи. Основна мета цієї кваліфікаційної роботи - провести комплексне дослідження та аналіз вразливостей в інфраструктурі AD, а також оцінити існуючі засоби виявлення цих вразливостей та можливість їх вдосконалення або створення нових засобів виявлення.

Для досягнення цієї мети були поставлені наступні завдання:

1. Вивчити теоретичні аспекти Active Directory, його функціональність та структуру.
2. Вивчити та проаналізувати основні типи вразливостей, що могут виникнути в інфраструктурі Active Directory.
3. Ознайомитись із основними методами атак на інфраструктуру Active Directory.
4. Вивчити наслідки вразливостей для інфраструктури Active Directory.
5. Дослідити внутрішні засоби безпеки в Active Directory.
6. Проаналізувати зовнішні інструменти для виявлення вразливостей.
7. Провести порівняльний аналіз засобів виявлення вразливостей.

8. Розробити власний інструмент виявлення вразливостей.
9. Провести тестування та аналіз результатів застосування розробленого інструменту.

Методи дослідження, що використовуються в цій роботі, включають теоретичний аналіз, практичне тестування та експериментальне дослідження. Для аналізу використовуються відомості з наукових джерел, технічної документації, статей, блогів та форумів, присвячених кібербезпеці. Практична частина роботи включає розробку власного інструменту для виявлення вразливостей в інфраструктурі Active Directory, а також його тестування та аналіз результатів.

Практичне значення роботи полягає в можливості використання результатів дослідження та розробленого інструменту для покращення безпеки в інфраструктурі Active Directory. Виходячи з результатів дослідження, можна сформувати рекомендації щодо підвищення рівня безпеки мереж, які використовують Active Directory, що може сприяти зменшенню ризику кібератак та зловмисних дій.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ТА СТРУКТУРА ACTIVE DIRECTORY

1.1 Визначення та функції Active Directory

Active Directory (AD) — це технологія, розроблена компанією Microsoft, що використовується в операційних системах Windows для обслуговування та керування доменами. Вона включає в себе широкий спектр служб, які забезпечують роботу різних компонентів IT-інфраструктури в мережі. Active Directory є важливою частиною Windows Server і є визначальним для багатьох аспектів IT-інфраструктури, включаючи безпеку, автоматизацію та управління доступом до ресурсів [1].

Однією з основних функцій Active Directory є аутентифікація та авторизація користувачів та комп'ютерів в мережі Windows. AD зберігає інформацію про об'єкти на мережі та дозволяє адміністраторам організовувати дані з метою надання користувачам і комп'ютерам необхідних прав доступу до ресурсів, таких як файли, принтери та сервери.

Active Directory дозволяє також керувати користувацькими обліковими записами, що включає створення, видалення, зміну облікових записів користувачів та груп, а також призначення та виконання політик безпеки. За допомогою AD адміністратори можуть встановлювати політики, що контролюють доступ до ресурсів та використання систем, що сприяє підвищенню безпеки мережі.

Active Directory використовує розподілену базу даних для зберігання і керування інформацією. Це означає, що дані можуть бути реплікові між багатьма серверами, що забезпечує більшу доступність, надійність та швидкість доступу до даних. Крім того, це дозволяє Active Directory масштабуватися для підтримки великих організацій і розподілених мереж.

Active Directory використовує ієрархічну структуру, що дозволяє організувати користувачів, комп'ютери та інші ресурси в спосіб, що відображає структуру

організації. Це включає в себе концепції, такі як домени, дерева та ліси, які дозволяють групувати та управляти об'єктами на різних рівнях.

Крім того, Active Directory використовує протокол LDAP (Lightweight Directory Access Protocol) для доступу до його бази даних. LDAP є відкритим стандартом, який дозволяє клієнтам та іншим серверам взаємодіяти з AD.

Важливою функцією Active Directory є забезпечення безпеки. AD дозволяє адміністраторам встановлювати політики безпеки на рівні домену, що дозволяє контролювати доступ до ресурсів, обмежувати дії користувачів, забезпечувати аудит та відстежування активності користувачів.

Використовуючи Active Directory, адміністратори можуть легко виконувати задачі, такі як розподіл ресурсів, керування обліковими записами користувачів та встановлення політик безпеки. AD дозволяє адміністраторам виконувати ці задачі централізовано, що значно спрощує процеси управління та підтримки.

AD використовує протокол Kerberos для аутентифікації, що забезпечує безпечний спосіб передачі об'єктів інформації в мережі. Крім того, AD підтримує інтеграцію з іншими службами Microsoft, такими як Exchange Server, SharePoint та Azure AD, що дозволяє організаціям створювати єдину, зв'язану інфраструктуру.

Active Directory також має вбудовані засоби для резервного копіювання та відновлення даних, що забезпечує захист від втрати даних та збоїв системи. Ці засоби, разом з можливістю реплікації даних між серверами, забезпечують високу доступність та надійність служби.

Використовуючи Active Directory, організації можуть створити стабільну, безпечну та легко управляєму IT-інфраструктуру, яка відповідає їх потребам та вимогам.

Відповідно, Active Directory відіграє ключову роль в управлінні корпоративними мережами, надаючи потужні засоби для управління користувачами, комп'ютерами, ресурсами, політиками безпеки та іншими важливими аспектами IT-інфраструктури.

1.2 Компоненти інфраструктури Active Directory

Active Directory складається з різних компонентів, кожен з яких виконує свою роль у створенні цілісної і надійної структури керування ресурсами мережі [2].

Об'єкти AD - це окремі елементи в Active Directory, які представляють ресурси, такі як користувачі, групи, комп'ютери, принтери та файли. Кожен об'єкт має набір атрибутів, які визначають його властивості.

Домен - основна одиниця структури Active Directory. Домен складається з об'єктів, які підкоряються спільній політиці безпеки та знаходяться на одній або декількох машинах, що контролюються серверами домену.

Дерево доменів - це ієрархічна структура доменів, зв'язаних відносинами довіри. Домени в дереві поділяють спільне простір імен, базуючись на головному домені.

Ліс - це набір дерев доменів, які поділяють спільний каталог схеми, конфігурацію каталогу та глобальний каталог. Ліси використовуються для організації та управління доменами на вищому рівні.

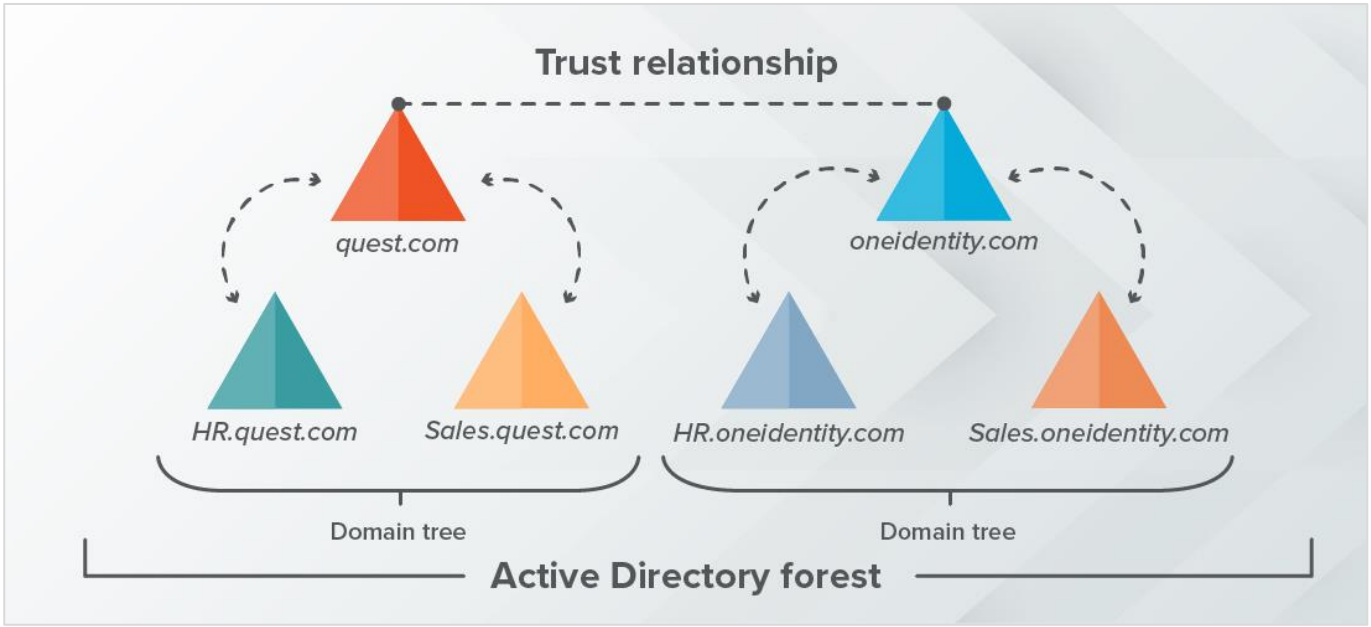

Рисунок 1.1 — Приклад взаємовідносин у лісі

Сервери домену - це машини, на яких встановлено Active Directory і які виконують роль контролерів домену. Вони зберігають повну копію всіх даних

домену, управляють взаємодією користувачів та комп'ютерів в домені, а також виконують реплікацію даних між іншими серверами домену.

Глобальний каталог - це спеціальний тип контролера домену, який зберігає інформацію про всі об'єкти в лісі. Він використовується для швидкого пошуку об'єктів та отримання інформації про них в межах всього лісу.

Схема Active Directory - це формальне визначення всіх типів об'єктів та їх атрибутів, які можуть бути збережені в Active Directory. Схема визначає, які об'єкти та їх атрибути можуть бути створені в Active Directory, і як вони повинні взаємодіяти один з одним.

Політики груп - це інструменти для управління конфігураціями користувачів і комп'ютерів в домені або в лісу. За допомогою політик груп адміністратори можуть встановлювати налаштування безпеки, управляти встановленням програмного забезпечення, налаштовувати скрипти входу та виходу, та інше.

Сервіси об'єднаних каталогів (Federation Services) - це складова Active Directory, яка дозволяє користувачам з різних доменів або мереж взаємодіяти з ресурсами інших доменів без необхідності входу за кожним разом, коли вони переходять з одного домену до іншого [8].

Сервіси сертифікатів - це служба, яка дозволяє створювати, розповсюджувати, зберігати та відкликати сертифікати безпеки. Ці сертифікати можуть використовуватися для підтвердження ідентичності користувачів, комп'ютерів або служб, шифрування даних та забезпечення інтегральності даних [13].

Таким чином, компоненти Active Directory разом створюють гнучку, масштабовану та надійну структуру для управління ресурсами мережі, надаючи адміністраторам потужні засоби для контролю доступу, безпеки та автоматизації.

1.3 Принципи роботи Active Directory в контексті клієнт-серверних мереж

Active Directory (AD) — це важлива складова клієнт-серверної мережі в середовищі Windows. Його головна роль полягає в управлінні ресурсами та об'єктами мережі, включаючи користувачів, групи, комп'ютери, домени та інші. Однак для

розуміння його ролі в контексті клієнт-серверних мереж, важливо розглянути принципи його роботи [5].

Аутентифікація та авторизація: Коли користувач намагається отримати доступ до ресурсу в мережі, AD відіграє важливу роль у процесі аутентифікації та авторизації. Спочатку, AD перевіряє ідентичність користувача (аутентифікація), а потім визначає, чи має користувач права доступу до запитаного ресурсу (авторизація).

Реплікація даних: AD автоматично реплікує дані між контролерами домену в мережі. Це означає, що всі контролери домену мають останню версію інформації AD, що підвищує надійність і доступність даних.

Керування політиками: AD дозволяє адміністраторам встановлювати та застосовувати політики на рівні домену, що дозволяє контролювати налаштування безпеки, управляти встановленням програмного забезпечення, налаштовувати скрипти входу та виходу, та інше [6].

Пошук і організація ресурсів: AD використовує ієрархічну структуру для організації об'єктів в мережі. Крім того, AD використовує глобальний каталог для швидкого пошуку ресурсів в межах лісу.

Захист інформації: Active Directory використовує різні технології, включаючи протокол Kerberos, для забезпечення безпеки даних та транзакцій в мережі.

Сервіси сертифікатів: AD включає служби сертифікатів, які дозволяють створювати, розповсюджувати та відкликати сертифікати безпеки для підтвердження ідентичності користувачів, комп'ютерів або служб.

Загалом, Active Directory відіграє важливу роль в управлінні ресурсами клієнт-серверної мережі, надаючи інструменти для аутентифікації користувачів, захисту даних, встановлення політик, організації та пошуку ресурсів, а також реплікації даних між контролерами домену.

1.4 Ролі серверів в Active Directory

В Active Directory (AD) сервери можуть виконувати різні ролі, в залежності від завдань, що ставляться перед ними. Нижче представлені основні ролі серверів в Active Directory.

Контролери домену (Domain Controllers, DC): Контролери домену є основними серверами в Active Directory. Вони зберігають повну копію всіх об'єктів та атрибутів Active Directory для свого домену, включаючи облікові дані користувачів та інформацію про політики. Контролери домену відповідають за аутентифікацію користувачів, обробку змін до об'єктів Active Directory і реплікацію цих змін до інших контролерів домену.

Глобальні каталоги (Global Catalog Servers, GC): GC – це контролери домену, які зберігають не тільки повну копію всіх об'єктів в своєму домені, але й часткові копії всіх об'єктів в лісу. GC використовуються для швидкого пошуку об'єктів в межах всього лісу і відіграють важливу роль в процесі входу в систему, особливо при вході в систему користувачів з великими групами безпеки.

Сервери імен (DNS Servers): Active Directory використовує систему доменних імен (DNS) для визначення місцезнаходження контролерів домену та інших ресурсів. DNS сервери відповідають за перетворення доменних імен на IP-адреси, що дозволяє комп'ютерам в мережі знайти і взаємодіяти з ресурсами.

Сервери з відкритим доступом (Read-Only Domain Controllers, RODC): RODC – це спеціальний тип контролера домену, який зберігає тільки для читання копію бази даних Active Directory. Вони використовуються в розташуваннях з обмеженими ресурсами або високим рівнем ризику, таких як віддалені офіси. RODC може обробляти запити на читання безпосередньо, але будь-які зміни, які він отримує, він передає на повноцінний контролер домену.

Операційні майстри (Operations Masters або FSMO Roles): Є п'ять ролей FSMO (Flexible Single Master Operations), які виконують важливі завдання, що вимагають одного контролера для запобігання конфліктів. Ці ролі включають: RID Master, PDC Emulator, Infrastructure Master, Schema Master та Domain Naming Master. Кожен з них

відповідає за виконання специфічних завдань в мережі, від контролю RID пулу до управління змінами схеми AD.

Отже, різноманітні ролі серверів в Active Directory забезпечують гнучкість та надійність системи, дозволяючи ефективно управляти ресурсами, а також забезпечувати безпеку та стійкість роботи мережі.

1.5 Об'єкти та атрибути в Active Directory

В Active Directory (AD) вся інформація представлена у вигляді об'єктів, які мають різні атрибути. Ось огляд основних об'єктів та атрибутів в AD [16].

Об'єкти Active Directory – це окрема одиниця даних в Active Directory. Він може відображати будь-що, від користувача або комп'ютера до групи або принтера. Кожен об'єкт в Active Directory має унікальне ім'я, яке використовується для його ідентифікації.

Основні типи об'єктів, які ви зустрінете в Active Directory, включають користувачів, комп'ютери, групи, організаційні одиниці (OU), контролери домену, а також ресурси, такі як принтери та спільні папки [14].

Атрибути Active Directory.Кожен об'єкт в Active Directory має ряд атрибутів, які визначають його властивості. Наприклад, об'єкт "користувач" може мати атрибути, такі як ім'я, прізвище, адреса електронної пошти, пароль та інші.

Атрибути в Active Directory мають дві важливі характеристики: вони можуть бути обов'язковими або необов'язковими, а також одномандатними або багатомандатними. Обов'язкові атрибути повинні мати значення для кожного об'єкта, тоді як необов'язкові можуть залишатися порожніми. Одномандатні атрибути можуть мати тільки одне значення, тоді як багатомандатні можуть мати кілька значень.

Наприклад, для об'єкта "користувач" атрибут "ім'я" буде обов'язковим і одномандатним, тоді як атрибут "телефон" може бути необов'язковим і багатомандатним, дозволяючи користувачу мати кі лька номерів телефону [17].

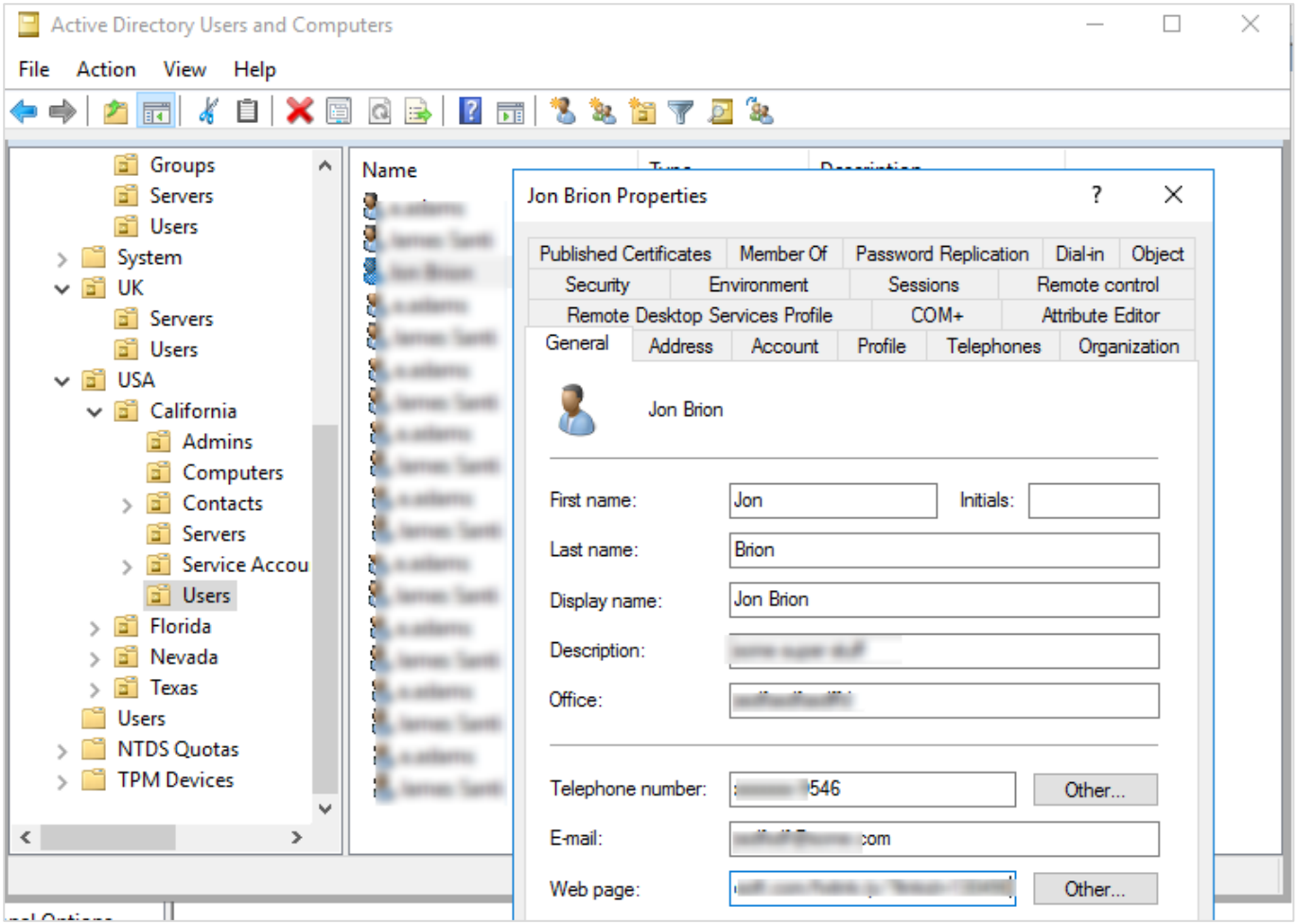

Рисунок 1.2 — Вікно з інформацією про об’єкт

Схема Active Directory визначає, які об'єкти та атрибути можуть бути в базі даних AD. Вона включає визначення всіх типів об'єктів та атрибутів, що можуть бути використані, та встановлює правила для того, як об'єкти можуть взаємодіяти один з одним. Наприклад, вона може вказувати, які атрибути є обов'язковими для кожного типу об'єкта, та як об'єкти можуть бути організовані в доменах та OU.

Отже, об'єкти та атрибути є основою, на якій побудована структура Active Directory. Вони дозволяють Active Directory зберігати та організовувати інформацію про ресурси мережі та користувачів, надаючи гнучкість та потужність, необхідні для управління сучасною IT-інфраструктурою.

1.6 Політики безпеки в Active Directory

Політики безпеки в Active Directory (AD) відіграють критичну роль в управлінні доступом до ресурсів та захисту інформації в мережі. Вони дозволяють адміністраторам визначати, хто може отримати доступ до чого, і які дії вони можуть виконувати.

1. *Групові політики*

Одним з ключових інструментів для управління безпекою в AD є групові політики (Group Policy Objects, GPO). GPO - це набір параметрів, які можуть бути застосовані до об'єктів (користувачів, комп'ютерів, організаційних одиниць), для управління різноманітними налаштуваннями, включаючи налаштування безпеки[3].

Наприклад, адміністратор може використовувати GPO для встановлення вимог до складності паролів, блокування облікового запису після певної кількості невдалих спроб входу, обмеження доступу до певних системних служб, встановлення правил файрволу, та багато іншого [9].

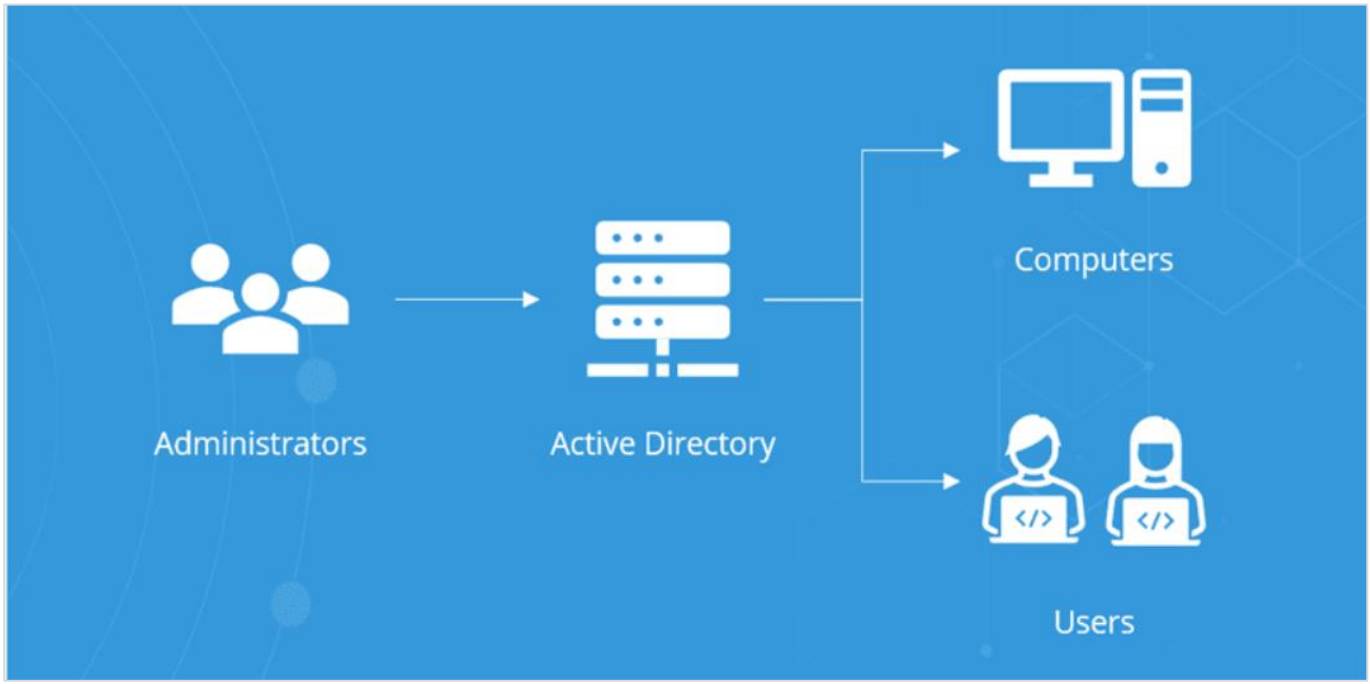

Рисунок 1.3 — Шлях розповсюдження політик

2. *Права доступу та дозволи*

AD використовує модель доступу на основі ролей (Role-Based Access Control, RBAC) для визначення того, хто може отримати доступ до ресурсів і які дії вони можуть виконувати [4].

Адміністратори можуть встановлювати дозволи на рівні об'єктів або атрибутів, визначаючи, хто може читати, модифікувати або видаляти конкретні об'єкти або їх атрибути. Дозволи можуть бути надані індивідуальним користувачам або групам.

3. *Аудит та моніторинг*

Active Directory надає можливість аудиту та моніторингу активності для забезпечення безпеки. Адміністратори можуть відстежувати спроби входу, зміни до об'єкт ів або атрибутів, та інші події, що мають відношення до безпеки. Це включає можливість генерації сповіщень або звітів про підозрілу активність.

4. *Безпека на рівні мережі*

Active Directory також інтегрується з іншими компонентами мережевої безпеки, такими як файрволи, системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS), для забезпечення багаторівневої захищеності [15].

Отже, політики безпеки в Active Directory відіграють важливу роль у захисті мережевих ресурсів і даних користувачів. Через гнучкість і потужність цих інструментів, адміністратори можуть розробити детальні та ефективні стратегії безпеки, що відповідають потребам їх організацій.

1.7 Механізми аутентифікації та авторизації в Active Directory

Active Directory, як потужна інфраструктура керування доменами в середовищі Windows, надає різноманітні механізми аутентифікації та авторизації, що гарантують безпеку і контроль доступу до ресурсів в мережі. Ці механізми грають важливу роль у забезпеченні конфіденційності, цілісності та доступності даних, а також у забезпеченні обмеження доступу до ресурсів згідно з політиками безпеки організації.

Основні методи аутентифікації, що використовуються в Active Directory, включають парольну аутентифікацію, сертифікатну аутентифікацію, одноразові

паролі та біометричну аутентифікацію. Парольна аутентифікація є найбільш поширеним методом, де користувачі повинні ввести унікальний пароль для підтвердження своєї ідентичності. Active Directory зберігає хеші паролів користувачів та порівнює їх зі значеннями, введеними під час аутентифікації.

Сертифікатна аутентифікація використовує цифрові сертифікати для перевірки ідентичності користувачів. Користувачі мають особисті сертифікати, видані довіреною стороною, які використовуються для встановлення безпечного з'єднання та аутентифікації. Цей метод дозволяє впроваджувати більш сильні механізми аутентифікації з використанням відкритих стандартів шифрування та цифрових підписів.

Одноразові паролі також широко використовуються в Active Directory. Кожен раз, коли користувач аутентифікується, йому надсилається новий одноразовий пароль, який використовується для підтвердження ідентичності. Цей механізм дозволяє знизити ризик підміни паролів та забезпечує додатковий рівень безпеки

Біометрична аутентифікація стає все більш популярною в сучасних системах безпеки. Вона використовує біометричні дані користувачів, такі як відбитки пальців, розпізнавання обличчя або розпізнавання голосу, для підтвердження їхньої ідентичності. Active Directory зберігає та перевіряє біометричні дані користувачів, що дозволяє забезпечити більш точну та надійну аутентифікацію.

Після успішної аутентифікації, Active Directory використовує різні механізми авторизації для контролю доступу користувачів до ресурсів. Це включає надання ролей, групового членства, контролю доступу на рівні об'єктів та політик безпеки. Механізми авторизації гарантують, що користувачі отримують лише необхідний рівень доступу до ресурсів, забезпечуючи таким чином контроль і безпеку даних.

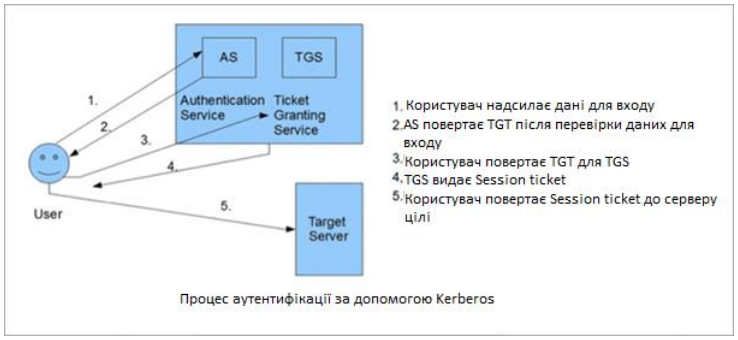

Рисунок 1.4 — Процес аутентифікації за допомогою Kerberos

Active Directory також надає можливість делегування прав доступу, дозволяючи адміністраторам делегувати обмежені права на керування окремими областями директорії до інших користувачів або груп. Це може бути особливо корисним в великих організаціях, де може бути неефективно або непрактично, щоб одна особа або невелика команда керувала всіма аспектами Active Directory.

Active Directory також підтримує використання політик групи (Group Policy), які дозволяють адміністраторам централізовано керувати робочими станціями, серверами та користувачами в мережі. За допомогою політик групи, адміністратори можуть встановлювати налаштування безпеки, встановлювати програмне забезпечення, керувати налаштуваннями системи та багато іншого.

Active Directory також використовує службу каталогів DNS (Domain Name System) для ідентифікації та маршрутизації трафіку в мережі. DNS відіграє важливу роль в Active Directory, оскільки він використовується для визначення місця розташування серверів та служб в мережі.

Active Directory також підтримує використання служби сертифікатів (Certificate Services), яка дозволяє організаціям випускати, керувати та відкликати цифрові сертифікати. Ці сертифікати можуть бути використані для забезпечення безпечного з'єднання, шифрування даних та цифрового підпису.

Всі ці функції та можливості роблять Active Directory потужним інструментом для управління мережевими ресурсами, контролю доступу та забезпечення безпеки в середовищі Windows.

Загально кажучи, механізми аутентифікації та авторизації в Active Directory відіграють критичну роль у забезпеченні безпеки мережі та контролю доступу до ресурсів. Залежно від потреб організації та рівня безпеки, вибір певних методів аутентифікації та механізмів авторизації допомагає забезпечити надійність та захищеність Active Directory.

1.8 Реплікація та синхронізація даних в Active Directory

Реплікація та синхронізація даних в Active Directory відіграють важливу роль у забезпеченні надійності, доступності та цілісності даних у розподіленій інфраструктурі. Active Directory використовує механізми реплікації для автоматичного копіювання та оновлення даних між різними контролерами доменів, що забезпечує їхню узгодженість та консистентність.

Реплікація в Active Directory базується на моделі "мастер-слейв", де є один головний (мастер) контролер домену, відомий як головний контролер домену (Primary Domain Controller, PDC), та один або більше службових (слейв) контролерів домену, відомих як вторинні контролери домену (Secondary Domain Controllers, SDC). Головний контролер домену має авторитетну копію даних, яка використовується для оновлення та розповсюдження змін на вторинні контролери домену[12].

Механізми реплікації в Active Directory забезпечують автоматичну передачу змін в даних, включаючи створення, видалення та оновлення об'єктів домену, групове членство, політики безпеки та інші атрибути. При зміні даних на головному контролері домену, ці зміни автоматично реплікуються на вторинні контролери домену шляхом передачі та оновлення реплікаційних пакетів.

Реплікація в Active Directory має кілька важливих особливостей, які забезпечують надійність та ефективність процесу. Наприклад, реплікація відбувається на рівні об'єктів, що означає, що лише змінені або нові об'єкти передаються та оновлюються, замість повного копіювання всіх даних. Крім того, реплікація відбувається з використанням протоколу Lightweight Directory Access Protocol (LDAP), що дозволяє ефективно передавати зміни та керувати процесом реплікації.

Синхронізація даних в Active Directory відбувається між контролерами доменів в реальному часі, щоб забезпечити однаковість даних у всій інфраструктурі. Коли користувачі вносять зміни до своїх облікових записів або роблять зміни у структурі

домену, ці зміни синхронізуються між контролерами доменів, щоб забезпечити їхню актуальність та узгодженість.

Реплікація та синхронізація даних в Active Directory є ключовими елементами його функціональності та надійності. Вони дозволяють забезпечити доступність та цілісність даних у розподіленій інфраструктурі, забезпечуючи їхню узгодженість та актуальність на всіх контролерах доменів. Це важливо для підтримки стабільної та безпечної роботи Active Directory в організації.

1.9 Масштабованість та висока доступність в Active Directory

Масштабованість та висока доступність є ключовими характеристиками Active Directory, які дозволяють ефективно управляти даними та забезпечити надійну роботу інфраструктури. Active Directory розроблено з урахуванням потреб організацій різного розміру та масштабів, що дозволяє масштабувати його від невеликих до дуже великих розподілених середовищ [7].

Одним з ключових елементів масштабованості є можливість додавання додаткових контролерів домену до інфраструктури. Кожен доданий контролер домену розподіляє навантаження та забезпечує резервування даних, забезпечуючи більшу швидкість та доступність. Це дозволяє організації масштабувати свою інфраструктуру відповідно до зростаючих потреб та забезпечити стабільну роботу Active Directory навіть при великому обсязі даних та великій кількості користувачів.

Active Directory також підтримує високу доступність шляхом використання механізмів резервування та реплікації даних. Наявність резервних контролерів домену дозволяє автоматично перехоплювати навантаження та забезпечувати безперебійну роботу в разі відмови головного контролера домену. Даний підхід гарантує високу доступність сервісу Active Directory і надійність роботи всієї інфраструктури.

Забезпечення масштабованості та високої доступності в Active Directory важливо для забезпечення ефективності та надійності роботи організаційної інфраструктури. Відповідне масштабування дозволяє підтримувати продуктивність при зростанні обсягу даних та кількості користувачів.

Висока доступність забезпечує безперебійну роботу інфраструктури та забезпечує швидке відновлення в разі відмови системи.

Усі ці функції та характеристики Active Directory дозволяють організаціям ефективно управляти своїми даними, забезпечувати безпеку та контроль доступу, а також масштабувати та забезпечувати високу доступність своєї інфраструктури. Це допомагає забезпечити стабільну та ефективну роботу Active Directory у всіх сценаріях використання організаційної інфраструктури.

Висновки за розділом І

У даному розділі було розглянуто теоретичні основи та структуру Active Directory - центрального компонента інфраструктури Windows, який відповідає за управління користувачами, групами, об'єктами та політиками безпеки.

Були описані ключові поняття та компоненти Active Directory, такі як домен, контролер домену, об'єкти та атрибути, а також ролі серверів.

Аналізуючи ці поняття, можна зрозуміти, що Active Directory є потужною та гнучкою інструментальною системою для управління користувачами та ресурсами в розподіленій мережі. Вона забезпечує централізоване управління, автентифікацію, авторизацію та аудит дій користувачів, що є ключовими елементами забезпечення безпеки інфраструктури.

Структура Active Directory базується на моделі каталогу, де об'єкти інформації ієрархічно організовані в об'єкти контейнерів, що дозволяє логічно групувати і керувати доступом до них. Також було розглянуто концепції схеми даних та реплікації, що забезпечують розподіленість та надійність даних в Active Directory.

Розуміння теоретичних основ та структури Active Directory є важливим для розробки та впровадження рішень безпеки, адміністрування та розширення функціональності в межах організаційної інфраструктури. Цей розділ створив необхідну основу для подальшого дослідження вразливостей та засобів їх виявлення, а також розробки програмного інструменту для підвищення безпеки та ефективності роботи Active Directory.

РОЗДІЛ 2
ВРАЗЛИВОСТІ В ІНФРАСТРУКТУРІ ACTIVE DIRECTORY ТА ЗАСОБИ ЇХ ВИЯВЛЕННЯ

2.1 Основні типи вразливостей

Active Directory (AD) як важливий компонент корпоративних мереж є мішенню для зловмисників, які намагаються експлуатувати його вразливості для досягнення своїх цілей. Вразливості в Active Directory можна класифікувати на основі різних критеріїв, таких як тип атаки, який може бути використаний для їх експлуатації, або компонент системи, який вони впливають. Далі ми розглянемо найбільш поширені типи вразливостей.

1. Некоректна конфігурація - це одна з найбільш поширених причин вразливостей в Active Directory. Помилки в конфігурації можуть виникнути через різні причини, включаючи неправильні налаштування політик безпеки, використання застарілих протоколів або слабких шифрувальних алгоритмів.
2. Привілейований доступ - якщо зловмисник здатний здобути привілейований доступ до компонентів Active Directory, вони можуть використовувати це для виконання різних шкідливих дій, включаючи створення або зміну об'єктів, зміну політик безпеки або викрадення облікових даних.
3. Вразливості в програмному забезпеченні - це вразливості, які виникають через помилки або недоліки в коді програмного забезпечення, яке використовується в Active Directory. Вони можуть включати багато різних типів проблем, включаючи вразливості, які дозволяють виконання довільного коду, підняття привілеїв або обход механізмів безпеки.
4. Слабкі паролі - це інший поширений тип вразливостей. Якщо користувачі використовують слабкі а бо легко вгадувані паролі, це може дозволити зловмисникам легко зламати облікові записи і отримати доступ до системи [18].

5. Відмова в обслуговуванні (DoS) - Цей тип вразливостей включає в себе атаки, які мають на меті завалити систему або сервіс таким чином, щоб він став недоступним для законних користувачів. Наприклад, зловмисник може спробувати використати велику кількість ресурсів сервера, щоб завантажити його та зробити недоступним для інших користувачів.
6. Пасивне перехоплення (Passive Interception) - це тип вразливості, при якому зловмисник здатний перехоплювати даних без втручання в їх передачу. Вони можуть це використовувати для викрадення облікових даних, перехоплення конфіденційної інформації або вивчення поведінки системи для планування майбутніх атак.

2.2 Основні методи атак для експлуатації вразливостей в Active Directory

Зловмисники використовують різноманітні методи атак для експлуатації вразливостей в Active Directory. Розуміння цих методів допомагає організаціям більше дізнатися про загрози, з якими вони можуть зіткнутися, та розробити ефективні стратегії захисту. Ось деякі з найпоширеніших методів атак:

1. Pass-the-Hash (PtH) атаки: Цей метод атаки полягає в крадіжці хешів паролів з системи і використанні їх для доступу до інших ресурсів у мережі. Зловмисники часто використовують PtH атаки для отримання привілейованого доступу до Active Directory.

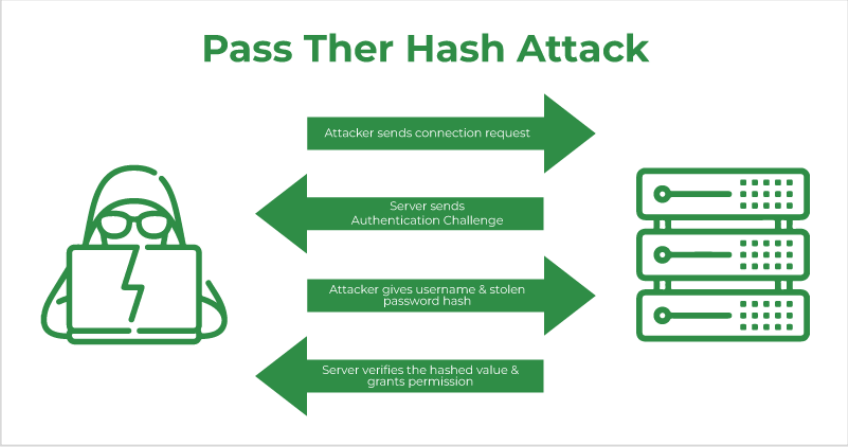

Рисунок 2.1 — Принцип атаки Pass the Hash

2. Атаки з використанням керберосінга: Kerberos - це протокол аутентифікації, який використовується в Active Directory. Зловмисники можуть використовувати різні техніки, такі як Golden Ticket або Silver Ticket атаки, для експлуатації вразливостей в Kerberos та отримання доступу до ресурсів.

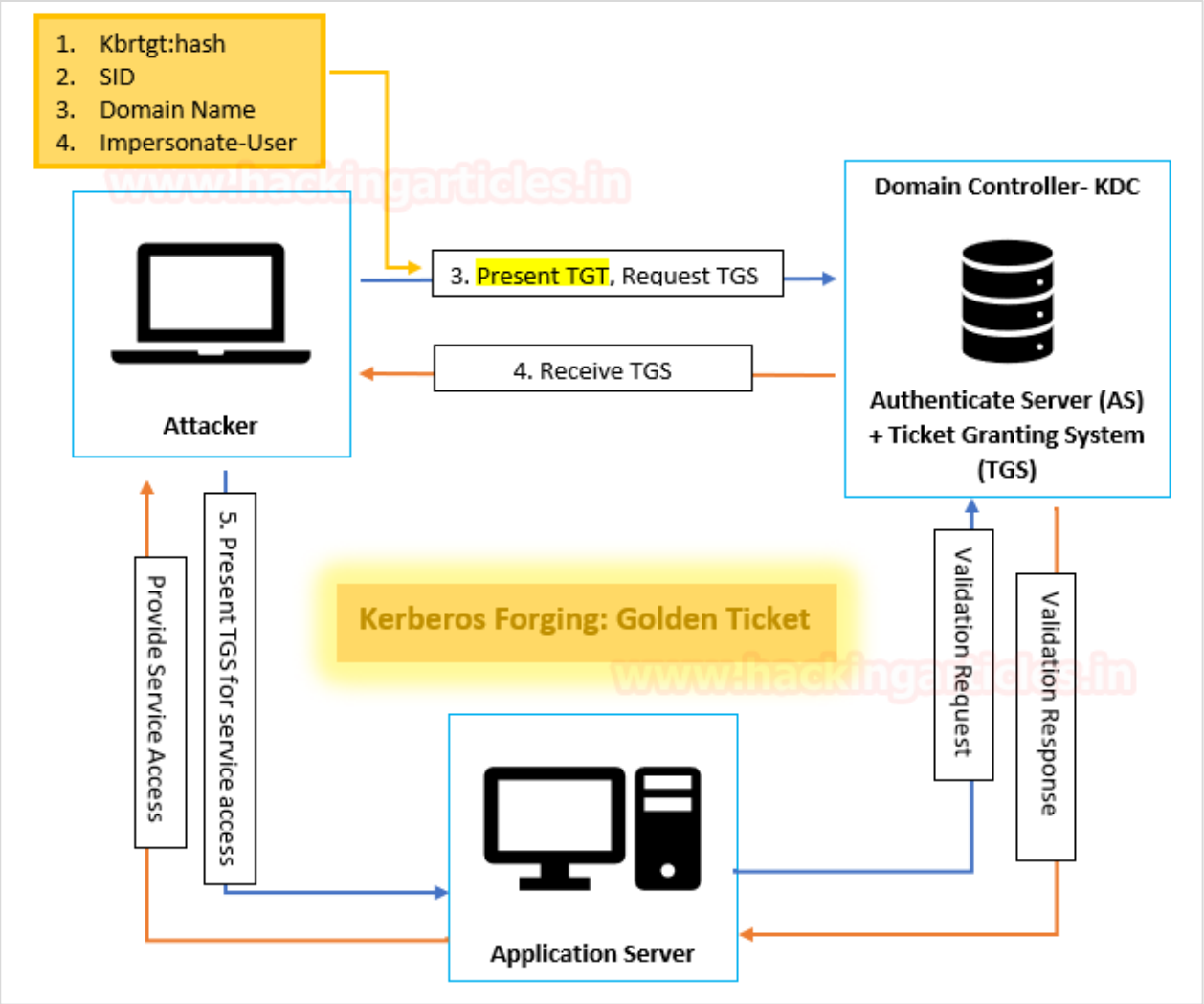

Рисунок 2.2 — Принцип створення Golden Ticket

3. LDAP Injection: LDAP Injection - це тип атаки, при якому зловмисник вставляє зловмисний код в LDAP запити, що дозволяє йому виконувати небажані дії, такі як отримання, зміна або видалення даних в Active Directory.
4. Атаки на службу DNS: Active Directory тісно пов'язаний з DNS, і зловмисники можуть використовувати різні атаки на DNS, такі як DNS poisoning або DNS spoofing, для перехоплення трафіку або перенаправлення користувачів на шкідливі веб-сайти.

5. Brute Force атаки: Цей метод полягає в неперервній спробі вгадати облікові дані користувача, використовуючи велику кількість спроб та комбінацій.
6. Атаки з використанням соціальної інженерії: Зловмисники можуть використовувати соціальну інженерію для отримання облікових даних користувача або іншої конфіденційної інформації. Це може включати підробку електронних листів, веб-сайтів або інших комунікаційних каналів, що використовуються організацією.

Всі ці методи атак створюють серйозні загрози для безпеки Active Directory. Тому важливо розробити стратегії захисту, які враховують ці загрози, а також використовувати засоби виявлення вразливостей для пошуку і виправлення потенційних слабких місць в інфраструктурі. В наступних розділах ми розглянемо деякі з цих засобів та стратегій.

2.3 Наслідки вразливостей для інфраструктури Active Directory

Вразливості в Active Directory можуть мати серйозні наслідки для організацій, включаючи порушення безпеки даних, втрату продуктивності, фінансові втрати та пошкодження репутації. Детальніше розглянемо кожен з цих наслідків:

1. Порушення безпеки даних: Найбільш безпосереднім наслідком вразливостей Active Directory є можливість незаконного доступу до конфіденційних даних. Це може включати персональні дані користувачів, корпоративну інформацію, інформацію про клієнтів та багато іншого.
2. Втрата продуктивності: Атаки, що експлуатують вразливості Active Directory, можуть призвести до відмови в обслуговуванні, що змушує IT-персонал витрачати час і ресурси на відновлення послуг. Це може спричинити значні втрати продуктивності для організації.
3. Фінансові втрати: Порушення безпеки можуть мати великі фінансові наслідки, включаючи витрати на відновлення системи, втрату бізнесу через відмову в обслуговуванні, а також можливі штрафи за недотримання нормативів з захисту даних.

4. Пошкодження репутації: Порушення безпеки можуть серйозно пошкодити репутацію організації, що може мати довгострокові наслідки, включаючи втрату довіри клієнтів та партнерів.

Оскільки наслідки вразливостей Active Directory можуть бути такими серйозними, важливо активно шукати і виправляти потенційні вразливості, використовуючи засоби виявлення вразливостей і розробляючи е фективні стратегії захисту. Це може включати регулярні аудити безпеки, впровадження політик мінімальних привілеїв для обмеження доступу до ресурсів Active Directory, використання многофакторної автентифікації для захисту облікових записів користувачів, і розробку плану відновлення від інцидентів для швидкого реагування на можливі порушення безпеки.

Важливо пам'ятати, що захист інфраструктури Active Directory - це не одноразове завдання, а постійний процес. Технології постійно розвиваються, так само як і тактики та методи, які використовують зловмисники. Організації повинні бути готові адаптуватися до цих змін, щоб забезпечити захист своєї мережі та даних.

У наступному розділі ми розглянемо деякі основні засоби та методи виявлення вразливостей в Active Directory, які можуть допомогти організаціям виявити та виправити потенційні вразливості перед тим, як вони стануть серйозною загрозою.

2.4 Внутрішні засоби безпеки в Active Directory

Active Directory обладнано різними засобами безпеки, які допомагають захищати інфраструктуру від різних видів загроз. Детальніше розглянемо деякі з них:

1. Керування обліковими записами: Active Directory дозволяє адміністраторам контролювати облікові записи користувачів, включаючи створення, видалення, блокування та розблокування облікових записів. Адміністратори можуть також налаштовувати правила паролів, включаючи вимоги до складності паролів та періоди дії паролів.
2. Мінімізація привілеїв: Active Directory підтримує принцип найменших привілеїв, який полягає в наданні користувачам та адміністраторам лише тих

прав доступу, які їм дійсно потрібні для виконання їхніх обов'язків. Це допомагає обмежити можливість зловмисного використання облікових записів.

3. Політики безпеки: Active Directory дозволяє адміністраторам створювати і застосовувати політики безпеки на різних рівнях, включаючи політики на рівні домену, політики на рівні об'єктів (наприклад, користувачів або груп) та політики на рівні ресурсів.
4. Аудит: Active Directory має вбудовані можливості аудиту, які дозволяють адміністраторам слідкувати за активністю в системі. Це включає в себе відстеження входів та виходів користувачів, змін облікових записів та спроб доступу до ресурсів.
5. Багатофакторна аутентифікація: Active Directory може інтегруватися з різними системами багатофакторної аутентифікації, що дозволяє зміцнити захист облікових записів, додаючи додатковий рівень перевірки автентичності. Це може включати в себе використання фізичних токенів, біометричних даних або одноразових паролів.
6. Керування сертифікатами: Active Directory підтримує використання сертифікатів для захисту даних та ідентифікації користувачів та серверів. Це включає в себе підтримку інфраструктури відкритого ключа (PKI), яка дозволяє випуск, управління та перевірку цифрових сертифікатів [19].
7. Відмовостійкість та відновлення: Active Directory має вбудовані механізми для забезпечення відмовостійкості, включаючи реплікацію даних між серверами. Додатково, Active Directory підтримує резервне копіювання та відновлення даних, що дозволяє відновити систему в разі втрати даних або серйозного збою.

Усі ці внутрішні засоби безпеки формують багаторівневу стратегію захисту, яка допомагає знизити ризики, пов'язані з вразливостями Active Directory. Однак, важливо зазначити, що жоден засіб безпеки не є непробивним, і важливо постійно оновлювати та аудитувати системи безпеки, щоб вони залишались ефективними в міру зміни загроз та технологій.

2.5 Зовнішні інструменти для виявлення вразливостей

Поруч з внутрішніми механізмами безпеки Active Directory, існують і зовнішні інструменти, які спеціалізуються на виявленні та усуненні вразливостей в інфраструктурі Active Directory. Деякі з них описані нижче:

1. Microsoft Baseline Security Analyzer (MBSA).

   Цей безкоштовий інструмент від Microsoft може виявити відсутні або застарілі патчі безпеки в системах на основі Windows, включаючи сервери Active Directory. MBSA також може перевірити налаштування безпеки та інші потенційні проблеми.
2. Nessus: Nessus - це один з найбільш популярних сканерів вразливостей, який може виявити широкий спектр потенційних проблем, включаючи вразливості в Active Directory. Nessus може аналізувати налаштування безпеки, відсутні патчі безпеки та інші вразливості.
3. Netwrix Auditor: Netwrix Auditor - це рішення для аудиту безпеки, яке може допомогти виявити зміни в Active Directory, які можуть вказувати на вразливості. Це включає зміни в облікових записах користувачів, групах та політиках безпеки.
4. BloodHound: BloodHound використовує графову теорію для виявлення ненадійних відносин та вразливостей в доменних управліннях Active Directory.
5. PingCastle: PingCastle - це інструмент для оцінки стану безпеки Active Directory. Він виконує перевірку наявності вразливостей, здійснює аналіз ризиків та генерує звіти.
6. ADAudit Plus.

   Це рішення від ManageEngine дозволяє моніторити і аудитувати зміни в Active Directory в режимі реального часу. Інструмент також допомагає визначати відхилення від стандартних налаштувань безпеки.
7. SolarWinds Access Rights Manager.

Цей інструмент допомагає в аудиті та керуванні правами доступу в Active Directory, що може виявити потенційні вразливості, які стосуються надмірних або невідповідних прав доступу.

8. Specops Password Auditor сканує Active Directory на наявність слабких, повторюваних або старих паролів, які можуть бути вразливими до атак.

Всі ці інструменти мають свої унікальні особливості та можуть бути використані для покращення безпеки в інфраструктурі Active Directory. Однак, важливо зауважити, що ніякий інструмент не може замінити постійний моніторинг, регулярні аудити безпеки та освіту користувачів щодо найкращих практик безпеки.

2.6 Порівняння інструментів для виявлення вразливостей

Для розуміння, які інструменти найефективніші для виявлення вразливостей в Active Directory, важливо провести порівняльний аналіз. Нижче наведено порівняльну таблицю деяких популярних засобів, засновану на таких критеріях, як здатність до виявлення вразливостей, легкість використання, можливості кастомізації та підтримка (Таблиця 2.1).

Ця таблиця служить для ілюстрації відмінностей між різними інструментами і може бути використана як початкова точка при виборі інструменту для виявлення вразливостей в Active Directory. Проте, потрібно пам'ятати, що кожна організація має унікальні вимоги, і тому вибір засобу повинен бути заснований на конкретних потребах та обставинах.

Таблиця 2.1

Порівняння інструментів для виявлення вразливостей

Засіб	**Здатність до виявлення вразливостей**	**Легкість використання**	**Можливості кастомізації**	**Підтримка**
MBSA	Висока	Висока	Середня	Висока
Nessus	Висока	Середня	Висока	Висока
Netwrix Auditor	Середня	Висока	Висока	Висока
BloodHound	Висока	Низька	Висока	Середня
PingCastle	Середня	Висока	Середня	Середня
ADAudit Plus	Висока	Висока	Висока	Висока
SolarWinds Access Rights Manager	Середня	Висока	Висока	Висока
Specops Password Auditor	Середня	Висока	Середня	Висока

2.7 Атаки на паролі користувачів в Active Directory

Активний каталог Active Directory включає механізми аутентифікації та авторизації, які гарантують безпеку доступу до ресурсів в мережі. Однак, паролі користувачів є однією з основних складових цих механізмів і становлять важливу ланку у забезпеченні безпеки Active Directory. Атаки на паролі користувачів можуть використовуватись зловмисниками для отримання несанкціонованого доступу до ресурсів, розширення привілеїв або компрометації конфіденційної інформації.

Одним з найпоширеніших типів атак на паролі є перебір (brute-force) паролів. Зловмисники можуть використовувати автоматизовані скрипти або спеціалізовані програми для спроби відгадати пароль, використовуючи різні комбінації символів,

словникові атаки або методи, що базуються на зламі раніше викрадених паролів. Успішна атака перебору паролів може дозволити зловмиснику отримати доступ до облікових записів користувачів і виконувати дії в їхньому імені.

Крім того, існують інші методи атак на паролі, такі як атаки з використанням соціальної інженерії, фішингу, використання слабких паролів, аналіз хешів паролів і так далі. Зловмисники можуть спробувати використати слабкості в процесі створення та керування паролями, такі як використання повторюваних або простих паролів, недостатня довжина паролів, відомі логіни або паспорти, які можуть бути використані для підбору.

З метою запобігання атакам на паролі користувачів в Active Directory, рекомендується впровадження сильних політик паролів, які вимагають використання складних символьних комбінацій, встановлення обмежень на максимальну довжину паролів, регулярну зміну паролів та використання механізмів двофакторної аутентифікації. Також важливо забезпечити своєчасне оновлення і патчі для системи Active Directory, що містять виправлення вразливостей аутентифікації та захисту паролів.

На практичному рівні, для виявлення можливих вразливостей в паролях користувачів Active Directory можна використовувати спеціалізовані програмні інструменти, які сканують і аналізують політики паролів, перевіряють силу паролів, виявляють використання однакових паролів для різних облікових записів, моніторять активність введення паролів та надають рекомендації щодо покращення безпеки паролів.

Ретельний аналіз та запобігання атакам на паролі користувачів у Active Directory є важливим аспектом забезпечення безпеки мережі. Здійснення заходів по підвищенню безпеки паролів та використання відповідних інструментів може значно зменшити ризик несанкціонованого доступу до ресурсів та захистити інформацію, що зберігається в Active Directory.

2.8 Вразливості в механізмах реплікації Active Directory

Механізми реплікації в Active Directory відіграють важливу роль у забезпеченні доступності, цілісності та надійності даних. Реплікація дозволяє зберігати копії даних на різних контролерах доменів, забезпечуючи швидкий доступ до інформації та автоматичну синхронізацію змін.

Проте, існують певні вразливості, пов'язані з механізмами реплікації в Active Directory, які можуть бути використані зловмисниками для злому системи або несанкціонованого доступу до даних. Деякі з найпоширеніших вразливостей включають:

1. Несправність механізмів аутентифікації: Якщо механізми аутентифікації між контролерами доменів не належним чином налаштовані, це може призвести до вразливості в реплікації, дозволяючи зловмисникам отримувати несанкціонований доступ до даних.
2. Атаки на канали реплікації: Зловмисники можуть перехоплювати трафік реплікації між контролерами доменів, використовуючи атаки на мережу або вразливості в каналах комунікації, і отримувати несанкціонований доступ до передаваних даних.
3. Проблеми з конфігурацією та автоматичною синхронізацією: Неправильна конфігурація параметрів реплікації або неправильна автоматична синхронізація можуть призвести до втрати даних або некоректної синхронізації змін між контролерами доменів.
4. Вразливості у протоколах реплікації: Вразливості, пов'язані з протоколами реплікації, можуть бути використані для здійснення атак, включаючи перехоплення, модифікацію або спотворення передаваних даних.

Для запобігання вразливостям в механізмах реплікації в Active Directory рекомендується вживати наступні заходи безпеки:

- Регулярно оновлюйте програмне забезпечення, у тому числі і патчі для системи Active Directory, що містять виправлення вразливостей у механізмах реплікації.

- Налаштуйте належність і аутентифікацію між контролерами доменів згідно з найкращими практиками безпеки.
- Застосовуйте заходи безпеки на мережевому рівні, такі як шифрування трафіку реплікації та використання захищених протоколів комунікації.
- Використовуйте механізми моніторингу та журналування для виявлення підозрілого або некоректного поведінки механізмів реплікації.

Важливо бути свідомим вразливостей, пов'язаних з механізмами реплікації в Active Directory, і приділяти достатню увагу їх запобіганню та виявленню. Дотримання рекомендацій безпеки допоможе забезпечити стабільну та надійну роботу інфраструктури Active Directory і запобігти можливим наслідкам вразливостей реплікації.

2.9 Можливість розповсюдження зловмисних програм через Active Directory

До цього розглядалися вразливості в інфраструктурі Active Directory та засоби їх виявлення. Тепер ми звернемо увагу на можливість розповсюдження зловмисних програм через саму Active Directory та способи захисту від цих загроз.

1. Механізми розповсюдження зловмисних програм:
    - Використання привілейованих облікових записів: Зловмисники можуть використовувати облікові записи з підвищеними привілеями, які мають доступ до Active Directory, для розповсюдження шкідливого програмного забезпечення через мережу.
    - Використання служб доменних контролерів: Зловмисники можуть використовувати служби доменних контролерів для розповсюдження зловмисних програм шляхом компрометації реплікації даних в Active Directory.
    - Використання служб керування груповою політикою: Зловмисники можуть змінювати групові політики в Active Directory, що дозволяє їм

розповсюджувати шкідливі скрипти або виконувати зловмисні команди на комп'ютерах користувачів.

2. Методи виявлення та запобігання:
   - Моніторинг активності облікових записів: Ретельний моніторинг активності облікових записів в Active Directory може допомогти виявити незвичні або підозрілі дії, що можуть свідчити про спроби розповсюдження зловмисних програм.
   - Обмеження привілеїв облікових записів: Встановлення обмежень на привілеї облікових записів, особливо тих, які мають доступ до важливих ресурсів в Active Directory, може унеможливити зловмисникам розповсюдження шкідливого програмного забезпечення.
   - Постійне оновлення та застосування патчів: Регулярне оновлення і застосування патчів на серверах Active Directory та клієнтських комп'ютерах може унеможливити використання вразливостей для розповсюдження зловмисних програм.
   - Ефективні політики паролів: Встановлення сильних та складних політик паролів допоможе унеможливити зловмисникам вгадати або підбрати паролі користувачів, що може захистити від розповсюдження зловмисних програм через скомпрометовані облікові записи.
3. Ідентифікація та валідація джерел даних: Забезпечення ідентифікації та валідації джерел даних, що використовуються для взаємодії з Active Directory, може запобігти неправомірним діям та розповсюдженню зловмисних програм через систему.
4. Захист від соціально-інженерних атак: Зловмисники можуть використовувати соціально-інженерні методи для отримання доступу до Active Directory та розповсюдження зловмисних програм. Навчання користувачів щодо розпізнавання та уникнення підступів зловмисників може значно зменшити ризик таких атак.

Загалом, виявлення та запобігання розповсюдженню зловмисних програм через Active Directory вимагає поєднання технічних заходів безпеки, ефективних політик та

постійного моніторингу. Своєчасна ідентифікація потенційних загроз та вжиття заходів щодо їх запобігання допоможуть зберегти інфраструктуру Active Directory від розповсюдження зловмисних програм та забезпечити безпеку організації.

Висновки за розділом ІІ

У даному розділі були розглянуті вразливості, що можуть виникати в інфраструктурі Active Directory, а також засоби їх виявлення. Було описано основні типи вразливостей, такі як недостатня конфігурація, слабкі паролі, підданість атакам та інші. Були розглянуті методи атак, які можуть бути спрямовані на інфраструктуру Active Directory, такі як атаки перебором, використанням слабких точок входу, зловживання привілеїв та інші.

Наслідки вразливостей для інфраструктури Active Directory можуть бути серйозними, включаючи втрату конфіденційної інформації, порушення прав доступу, підміну даних, зупинку системи та інші негативні наслідки. Тому важливо виявляти та виправляти вразливості вчасно.

У розділі було розглянуто внутрішні та зовнішні засоби для виявлення вразливостей в Active Directory. Внутрішні засоби включають вбудовані інструменти та механізми, що дозволяють моніторити та аналізувати безпеку інфраструктури. Зовнішні інструменти включають сторонні програми та сервіси, які надають розширені можливості для виявлення вразливостей.

Порівняльний аналіз засобів виявлення вразливостей дозволяє оцінити їх ефективність, функціональність та придатність для конкретних потреб організації. Розуміння різних засобів та їх переваг допомагає обрати найкращий варіант для виявлення та виправлення вразливостей в інфраструктурі Active Directory.

Загалом, в даному розділі були проаналізовані вразливості в інфраструктурі Active Directory, а також засоби їх виявлення. Розуміння цих аспектів є важливим для розробки та впровадження ефективних заходів безпеки та забезпечення надійності та захищеності Active Directory.

РОЗДІЛ 3
РОЗРОБКА ТА ВПРОВАДЖЕННЯ ПРОГРАМНОГО ЗАСОБУ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В ACTIVE DIRECTORY

3.1 Специфікація вимог до програмного інструменту

Специфікація вимог до програмного інструменту визначає що саме програмний засіб повинен робити та які функції повинен виконувати. На основі аналізу вимог, були визначені наступні основні характеристики та функції для розробки інструменту виявлення вразливостей в Active Directory:

1. Збір інформації про домен Active Directory. Програмний інструмент повинен здатний збирати всю необхідну інформацію про структуру Active Directory, включаючи деталі про користувачів, групи, об'єкти, політики тощо.
2. Аналізувати ACL (Access Control List). Інструмент повинен аналізувати списки контролю доступу для різних об'єктів в Active Directory, зокрема для користувачів, груп і комп'ютерів.
3. Аналіз ролей користувачів. Програма повинна виявляти ролі користувачів в Active Directory, щоб визначити їх дозволи і обмеження.
4. Виявлення Unconstrained Delegation. Інструмент повинен здатний виявляти ненадійні делегації в Active Directory, які можуть дозволити атакуванням отримати більше прав.
5. Аналіз відносин між доменами. Інструмент повинен аналізувати відносини між різними доменами в лісі Active Directory, що може виявити потенційні вектори атаки.
6. Інтерфейс користувача. Програмний інструмент повинен мати інтуїтивно зрозумілий інтерфейс користувача, який дозволить адміністраторам легко користуватися програмою і зрозуміти результати аналізу.

Усі ці вимоги стали основою для проектування архітектури програмного інструменту і визначення ключових функцій, які будуть розглянуті в наступних пунктах.

3.2 Проектування архітектури програмного інструменту

При розробці архітектури програмного засобу для виявлення вразливостей в Active Directory, основна увага була приділена виконанню трьох ключових функцій: збір інформації, аналіз даних та візуалізація результатів.

Збір інформації виконується шляхом прямого взаємодії з Active Directory через API, використовуючи вбудовані засоби .NET Framework. Це включає отримання даних про структуру домену, деталі об'єктів, ACL, ролі користувачів, відносини між об'єктами і так далі.

Аналіз даних полягає в пошуку потенційних вразливостей або небезпечних конфігурацій на основі зібраної інформації. Цей процес включає аналіз ACL, виявлення відносин між користувачами та об'єктами, перевірку на unconstrained delegation, і так далі.

Візуалізація результатів включає представлення зібраної інформації користувачеві в зручній формі. Це може включати графічне представлення структури домену, відображення деталей об'єктів, показ виявлених вразливостей та надання рекомендацій щодо їх усунення.

Ця архітектура дозволяє забезпечити гнучкість та ефективність інструменту, оскільки він може працювати безпосередньо на клієнтській машині, забезпечуючи високу швидкість обробки даних та негайну відповідь на дії користувача.

3.3 Проектування архітектури програмного інструменту

Для впровадження власного інструменту виявлення вразливостей у Active Directory, розглянемо набір ключових алгоритмів, які дозволять здійснювати аналіз ACL, вивчати ролі користувачів, перевіряти наявність вільної делегації (unconstrained delegation) та аналізувати відносини між доменами.

1. Аналіз ACL: Для перевірки ACL потрібен алгоритм, який дозволяє витягнути ACL з об'єктів Active Directory та зрозуміти, яким користувачам дозволено виконувати різні дії. Цей алгоритм повинен зосередитися на розборі різних прав доступу та їх відповідних контролерах доступу.
2. Аналіз ролей користувачів: Розробка алгоритму для аналізу ролей користувачів включає в себе витягування інформації про членство користувачів в групах, їх права та обов'язки в контексті Active Directory. Важливо аналізувати і виокремлювати особливо високопривілейованих користувачів.
3. Аналіз Unconstrained Delegation: Unconstrained delegation є потенційно небезпечною конфігурацією, яка дозволяє об'єкту Active Directory передавати довіреність (delegation) без обмежень. Алгоритм повинен ідентифікувати будь-які об'єкти, які використовують unconstrained delegation.
4. Аналіз відносин між доменами: У великих мережах може бути кілька доменів Active Directory, які взаємодіють між собою. Аналіз відносин між доменами включає в себе виявлення довірчих відносин між різними доменами і визначення, як це може впливати на безпеку.

Кожен з цих алгоритмів вимагає глибокого розуміння механізмів Active Directory і специфіки їх роботи. У разі успішної реалізації, вони дозволять програмному інструменту ефективно виявляти потенційні вразливості і місця для оптимізації безпеки в середовищі Active Directory.

3.4 Реалізація програмного інструменту

Наступний крок у процесі розробки - це власне реалізація програмного інструменту. Для цього ми використовуємо мову програмування C#, яка дозволяє нам взаємодіяти з API Active Directory для збору необхідної інформації і виконання аналізу (Рис.3.1).

Після написання і тестування коду, його можна використовувати для виявлення потенційних проблем безпеки в середовищі Active Directory.

Код даного програмного засобу можна переглянути у додатку А кваліфікаційної роботи.

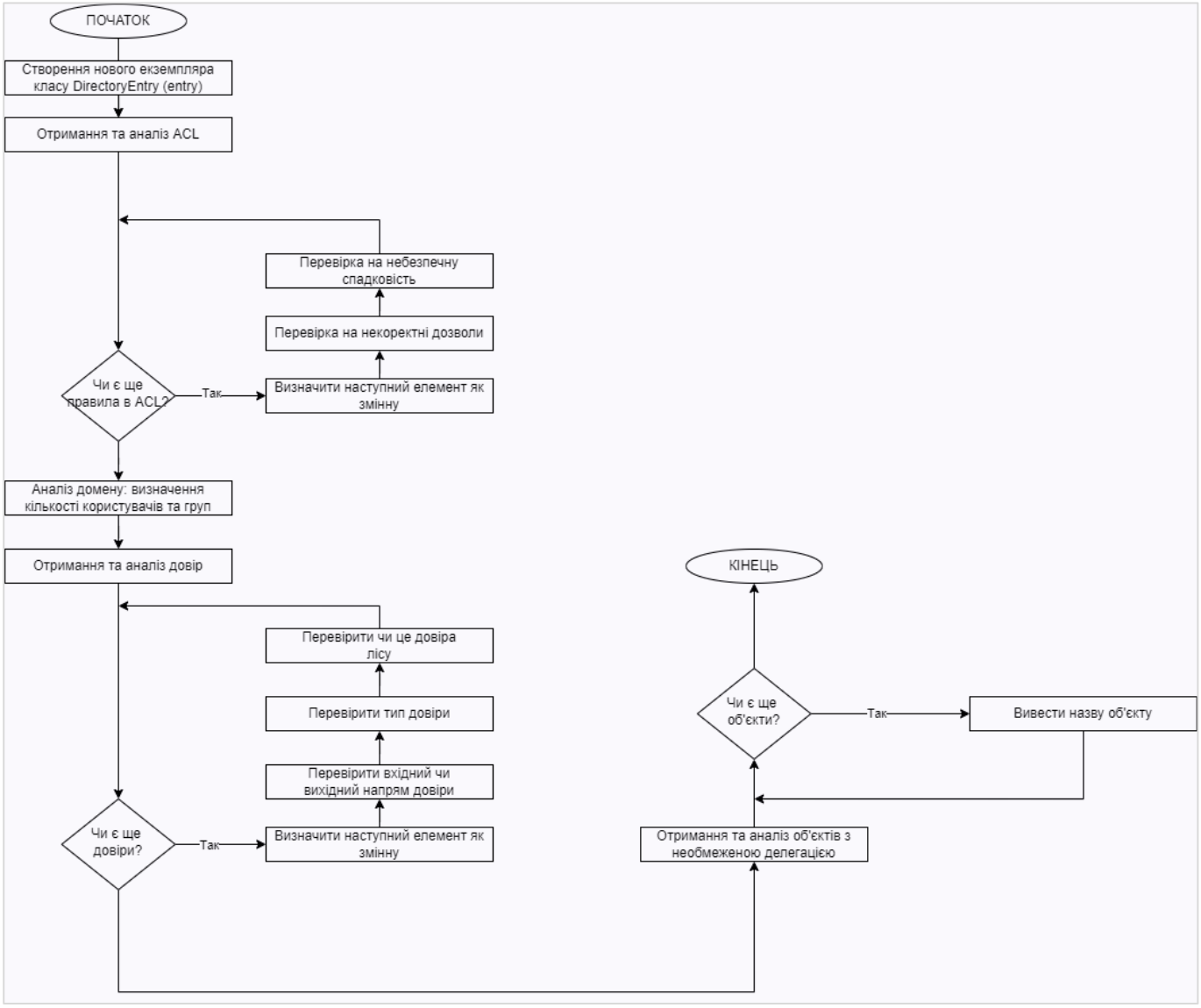

Рисунок 3.1 — Блок-схема програмної реалізації

3.5 Тестування та впровадження програмного інструменту

Тестування та впровадження програмного інструменту буде включати наступні кроки:

1. Тестування функціональності - проведення тестів для перевірки роботи основних функцій програмного інструменту. Це включає перевірку правильності збору і аналізу інформації з Active Directory, виявлення базових вразливостей та виведення результатів.
2. Тестування стійкості - виконання тестів для перевірки стабільності та надійності програмного інструменту. Впевнення в тому, що він працює без збоїв та надійно опрацьовує великий обсяг даних.
3. Впровадження розгортання програмного інструменту на відповідному середовищі, налаштування необхідних дозволів та забезпечення правильного виконання. Підготовка середовища для виконання скрипту.

Завершення цих кроків дозволить впровадити та використовувати програмний інструмент для аналізу базових вразливостей Active Directory.

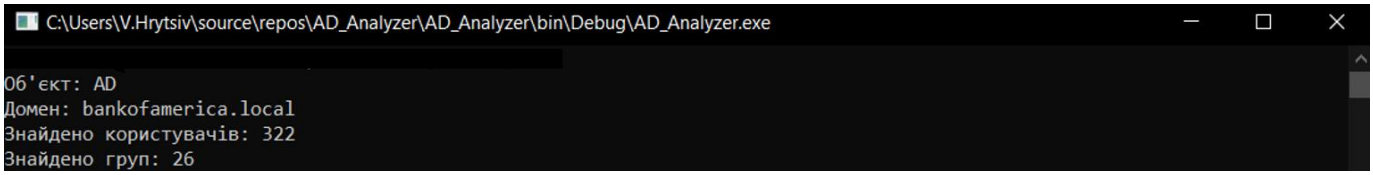

Рисунок 3.2 — Виведення інформації про групи та користувачів

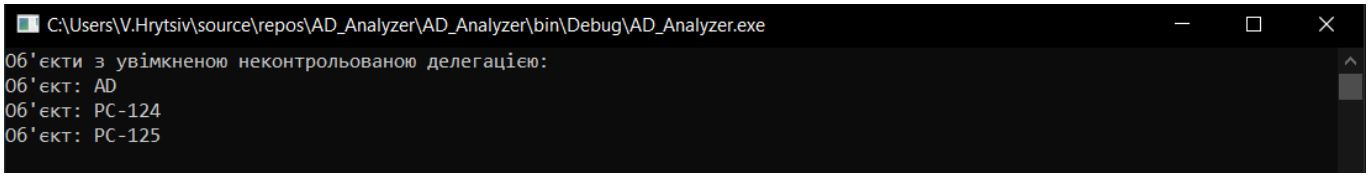

Рисунок 3.3 — Виведення інформації про об’єкти з Unconstrained Delegation

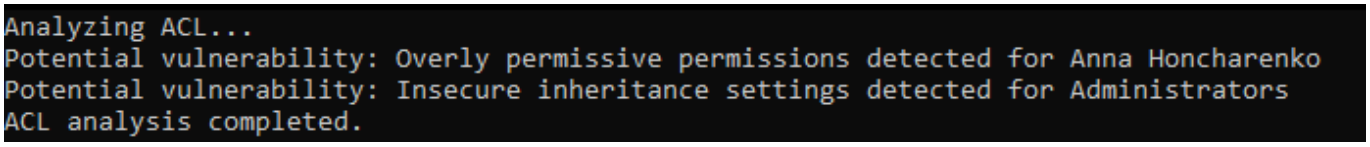

Рисунок 3.4 — Виведення інформації про вразливості після аналізу ACL

```
Analyzing unconstrained delegation...
Objects with unconstrained delegation:
Object: n.shevchenko
Object: m.bondarenko
Object: i.krasnov
Unconstrained delegation analysis completed.
```

Рисунок 3.4 — Виведення інформації про користувачів з unconstrained delegation

```
Analyzing domain relationships...
Trust relationship with domain: dev.company.local
Trust direction: Outgoing
Trust type: External
----------------------------------
Trust relationship with domain: company2.local
Trust direction: Incoming
Trust type: Forest
Trust is a forest trust
----------------------------------
Domain relationship analysis completed.
```

Рисунок 3.5 — Виведення інформації про зв’язки між доменами

Висновки за розділом III

У даному розділі була розглянута розробка та впровадження програмного інструменту для виявлення вразливостей в Active Directory. Були описані основні етапи розробки, включаючи уточнення вимог, проектування архітектури, розробку алгоритмів аналізу та реалізацію програмного інструменту.

Специфікація вимог до програмного інструменту визначила основні функціональність і вимоги, що повинні бути задоволені. Архітектура програмного інструменту була проектована з урахуванням потреб безпеки, ефективності та легкості використання.

Розробка алгоритмів аналізу дозволила визначити ключові критерії для виявлення вразливостей, такі як недостатній рівень безпеки, некоректні налаштування, аномальні права доступу та інші. Реалізація програмного інструменту була здійснена на основі встановлених алгоритмів та вимог, забезпечуючи функціональність знаходження та аналізу вразливостей.

Тестування та впровадження програмного інструменту підтвердило його працездатність та ефективність. В процесі тестування було проведено аналіз реальних даних з інфраструктури Active Directory та виявлено різноманітні вразливості. Впровадження інструменту дозволило покращити рівень безпеки інфраструктури та забезпечити зменшення ризику зловживання та несанкціонованого доступу.

Отже, розробка та впровадження програмного інструменту для виявлення вразливостей в Active Directory є актуальною та корисною задачею, що допомагає забезпечити надійність та безпеку інфраструктури. Результати роботи можуть бути використані для покращення захищеності та ефективності роботи Active Directory в організаціях.

ВИСНОВКИ

В ході виконання цієї роботи було проведено розгорнуте дослідження в області безпеки інфраструктури Active Directory.

Аналізуючи особливості роботи клієнт-серверних мереж, основний акцент було зроблено на структуру та функціонування Active Directory, що стає центром управління та контролю в більшості корпоративних мереж. Було детально розглянуто принципи роботи Active Directory, його архітектуру, ролі серверів, а також політики безпеки, що використовуються в ньому.

Особливу увагу було приділено вразливостям, що можуть виникнути в інфраструктурі Active Directory. Було розглянуто основні типи вразливостей та методи атак, які можуть використовуватися зловмисниками для неправомірного доступу до системи. Зрозуміло, що вразливості можуть мати серйозні наслідки для інфраструктури Active Directory та призвести до втрати даних або несанкціонованого доступу до них.

Акцентувавши увагу на засобах виявлення вразливостей, було проаналізовано як внутрішні механізми безпеки Active Directory, так і зовнішні інструменти. Основними критеріями при виборі засобу були його ефективність, швидкість роботи та легкість використання.

На основі проведеного аналізу було розроблено власний інструмент для виявлення вразливостей в інфраструктурі Active Directory. Він забезпечує збір інформації про домен, аналізує ACL, ролі користувачів, виявляє unconstrained delegation та аналізує відносини між доменами.

Розроблений інструмент було випробовано на практиці, що дозволило переконатися в його ефективності та відповідності висунутим вимогам.

Отже, виконана робота дозволила не тільки детально дослідити принципи роботи та безпеки Active Directory, але й розробити власний інструмент для виявлення його вразливостей. Впровадження такого інструменту може стати важливим кроком в підвищенні безпеки корпоративних мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Microsoft Docs - Active Directory: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
2. TechNet - Understanding Active Directory: https://technet.microsoft.com/en-us/library/cc780336(v=ws.10).aspx
3. TechNet - Group Policy: https://technet.microsoft.com/en-us/library/cc725828(v=ws.11).aspx
4. Microsoft Docs - Active Directory Rights Management Services Overview: https://docs.microsoft.com/en-us/windows-server/identity/ad-rms/ad-rms-overview
5. Book: "Mastering Active Directory: Understand the Core Functionalities of Active Directory Services Using Microsoft Server 2016 and PowerShell" by Dishan Francis.
6. Microsoft Docs - AD DS Administration Center: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/active-directory-administration-center
7. Microsoft Docs - Active Directory Schema: https://docs.microsoft.com/en-us/windows/win32/adschema/active-directory-schema
8. Microsoft Docs - Understanding Active Directory Domain Services (AD DS) Functional Levels: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels
9. Microsoft Docs - How to configure Group Policy for LAPS: https://docs.microsoft.com/en-us/windows/security/identity-protection/password-management/configuring-password-settings
10. Windows Server - Security Guide: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material
11. Book: "Active Directory: Designing, Deploying, and Running Active Directory" by Brian Desmond, Joe Richards, Robbie Allen, Alistair G. Lowe-Norris

12. Microsoft Docs - Active Directory Replication: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/active-directory-replication
13. Microsoft Docs - Introduction to Active Directory Services: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727030(v=technet.10)
14. Microsoft Docs - Understanding Sites, Domains, and Organizational Units: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-active-directory-domain-services--ad-ds--logical-structure
15. TechNet - Active Directory Replication Over Firewalls: https://technet.microsoft.com/en-us/library/dd772723(v=ws.10).aspx
16. Book: "Learn Active Directory Management in a Month of Lunches" by Richard Siddaway
17. Microsoft Docs - Managing Users, Groups, and Logon Hours Using AD DS: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-manage-users-groups-and-logon-hours
18. Microsoft Docs - AD DS: Best Practices for Enforcing Password Policies: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd277399(v=ws.10)
19. Microsoft Docs - Active Directory Certificate Services Overview: https://docs.microsoft.com/en-us/windows-server/identity/ad-cs/ad-cs-overview

ДОДАТОК А

```
using System;
using System.Collections.Generic;
using System.DirectoryServices;
using System.DirectoryServices.ActiveDirectory;
using System.Security.AccessControl;

public class ADVulnerabilityScanner
{
    public static void Main()
    {
        // Під'єднатися до домену
        using (DirectoryEntry entry = new DirectoryEntry("LDAP://company.local.tm"))
        {
            // Проаналізувати ACL
            AnalyzeACL(entry);
            AnalyzeActiveDirectory(entry);

            // Проаналізувати ролі користувачів
            AnalyzeDomainRelationships();

            // Проаналізувати unconstrained delegation
            AnalyzeUnconstrainedDelegation(entry);

            // Проаналізувати взаємовідносини доменів
            Console.ReadLine();
        }
    }

    public static void AnalyzeActiveDirectory(DirectoryEntry entry)
    {
        // Збір загальної інформації про домен
        string domainName = entry.Properties["name"].Value.ToString();
        Console.WriteLine("Домен: " + domainName);

        // Збір інформації про користувачів
        DirectorySearcher userSearcher = new DirectorySearcher(entry);
        userSearcher.Filter = "(objectClass=user)";
        SearchResultCollection userResults = userSearcher.FindAll();
        Console.WriteLine("Знайдено користувачів: " + userResults.Count);

        // Збір інформації про групи
        DirectorySearcher groupSearcher = new DirectorySearcher(entry);
        groupSearcher.Filter = "(objectClass=group)";
        SearchResultCollection groupResults = groupSearcher.FindAll();
        Console.WriteLine("Знайдено груп: " + groupResults.Count);

        // Додатковий аналіз та виведення результатів
        // Розширте цей метод, додавши логіку аналізу згідно ваших вимог

        // Закриття пошуку
        userResults.Dispose();
        groupResults.Dispose();
    }

    public static void AnalyzeDomainRelationships()
    {
        // Отримати поточний домен
        Domain currentDomain = Domain.GetCurrentDomain();

        // Отримати всі домені
        TrustRelationshipInformationCollection trustedDomains =
currentDomain.GetAllTrustRelationships();
```

```
        foreach (TrustRelationshipInformation trustInfo in trustedDomains)
        {
            Console.WriteLine($"Trust relationship with domain: {trustInfo.TargetName}");

            // Перевірити вхідний чи вихідний напрям довіри
            if (trustInfo.TrustDirection == TrustDirection.Outbound)
            {
                Console.WriteLine("Trust direction: Outgoing");
            }
            else if (trustInfo.TrustDirection == TrustDirection.Inbound)
            {
                Console.WriteLine("Trust direction: Incoming");
            }

            // Перевірити тип довіри
            Console.WriteLine($"Trust type: {trustInfo.TrustType}");


            // Перевірити чи це довіра лісу
            if (trustInfo.TrustType == TrustType.Forest)
            {
                Console.WriteLine("Trust is a forest trust");
            }


            Console.WriteLine("-----------------------------------");
        }
    }

    public static void AnalyzeACL(DirectoryEntry entry)
    {
        // Отримання ACL
        ActiveDirectorySecurity activeDirectorySecurity =
(ActiveDirectorySecurity)entry.ObjectSecurity;

        // Аналіз ACL
        AuthorizationRuleCollection acl = activeDirectorySecurity.GetAccessRules(true, true,
typeof(System.Security.Principal.SecurityIdentifier));

        foreach (AuthorizationRule rule in acl)
        {
            // Перевірка на некоректні дощволи
            if (rule is FileSystemAccessRule fsAccessRule)
            {
                if (fsAccessRule.AccessControlType == AccessControlType.Allow &&
fsAccessRule.FileSystemRights == FileSystemRights.FullControl)
                {
                    Console.WriteLine($"Potential vulnerability: Overly permissive permissions
detected for {fsAccessRule.IdentityReference}");
                }
            }

            // Перевірка на небезпечну спадковість
            if (rule is ActiveDirectoryAccessRule adAccessRule)
            {
                if (adAccessRule.InheritanceFlags != InheritanceFlags.None)
                {
                    Console.WriteLine($"Potential vulnerability: Insecure inheritance settings
detected for {adAccessRule.IdentityReference}");
                }
            }
        }
    }

    public static void AnalyzeUnconstrainedDelegation(DirectoryEntry entry)
```

```
    {
        DirectorySearcher searcher = new DirectorySearcher(entry);
        searcher.Filter = "(userAccountControl:1.2.840.113556.1.4.803:=524288)"; // Пошук
об'єктів з увімкненою неконтрольованою делегацією
        SearchResultCollection results = searcher.FindAll();

        Console.WriteLine("Об'єкти з увімкненою неконтрольованою делегацією:");
        foreach (SearchResult result in results)
        {
            string objectName = result.Properties["name"][0].ToString();
            Console.WriteLine("Об'єкт: " + objectName);
        }

        results.Dispose();
    }

}
```