

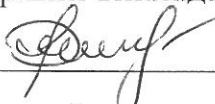
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА
до випускної кваліфікаційної роботи бакалавра
на тему:
«Проект підсистеми аутентифікації користувачів
комп'ютерної мережі організації»

Виконав студент 4-го курсу, групи КБ-1
спеціальності 125 «Кібербезпека»

 Дятел Я. Д.

Старший викладач кафедри КІ та КБ, Байлюк Є.М.

 Байлюк Є.М.

Старший викладач кафедри КІ та КБ Покотило О.А.

 Покотило О.А.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Єфіменко А. А.
«12» квітня 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Дятла Ярослава Дмитровича**

Тема роботи: **Проект підсистеми аутентифікації користувачів комп'ютерної мережі організації**

затверджена Наказом по університету від «12» квітня 2021 р. № 134/с

Термін здачі студентом закінченої роботи – **17 червня 2021 р.**

Вихідні дані для роботи:

1. Протоколи аутентифікації
2. Гетерогенна комп'ютерна мережа
3. Служба каталогів корпорації Microsoft
4. Визначення та аналіз можливих атак та вразливостей

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Байлюк Є.М.	12.04.2021	12.04.2021
2	Байлюк Є.М.	28.04.2021	28.04.2021
3	Байлюк Є.М.	20.05.2021	20.05.2021

Керівник  Байлюк Є.М.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання на кваліфікаційну роботу	12 квітня 2021 – 13 квітня 2021	Виконано
2	Огляд літератури за тематикою роботи	13 квітня 2021 – 24 квітня 2021	Виконано
3	Знаходження існуючих алгоритмів та способів аутентифікації	24 квітня 2021 – 28 квітня 2021	Виконано
4	Вибір необхідного протоколу для роботи	28 квітня 2021 – 4 травня 2021	Виконано
5	Детальне вивчення обраного протоколу	4 травня 2021 – 8 травня 2021	Виконано
6	Проектування підсистеми для дослідження роботи протоколів аутентифікації	8 травня 2021 – 15 травня 2021	Виконано
7	Проведення дослідження стосовно можливих типів атак	15 травня 2021 – 18 травня 2021	Виконано
8	Огляд та аналіз проходження трафіку в мережі	18 травня 2021 – 21 травня 2021	Виконано
9	Визначення оптимальних рішень стосовно захисту систем	21 травня 2021 – 27 травня 2021	Виконано
10	Формування та оформлення звітної документації	27 травня 2021 – 13 червня 2021	Виконано
11	Підготовка до захисту кваліфікаційної роботи	13 червня 2021 – 15 червня 2021	Виконано
12	Створення презентації та підготовка доповіді	15 червня 2021 – 17 червня 2021	Виконано
13	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	17 червня 2021 – 20 червня 2021	Виконано
14	Захист	24 червня	Виконано

Студент  Дятел Я.Д.

Керівник  Байлюк Є. М.

РЕФЕРАТ

Випускна кваліфікаційна робота складається з теоретичної частини стосовно методів та способів аутентифікації користувачів, також проектування підсистеми захисту комп'ютерної мережі, дослідження трафіку, можливих типів атак та пояснювальної записки. Пояснювальна записка до кваліфікаційної роботи складається з 72 сторінок, 40 рисунків та 4 таблиць.

Метою роботи є аналіз можливих вразливостей та розробка захисту клієнт-серверної частини мережі від несанкціонованого доступу до ресурсів.

В роботі визначено основні поняття ідентифікації, аутентифікації, авторизації та аудиту користувачів. Розглянуто сучасний протоколи аутентифікації Kerberos та проаналізовано його аналоги. Розроблена підсистема аутентифікації користувачів у гетерогенній мережі та досліджено процес проходження в ній трафіку. Наведено сценарії можливих атак на протокол Kerberos та наявність вразливостей служби каталогів Active Directory.

КЛЮЧОВІ СЛОВА: ЗАХИСТ, БЕЗПЕКА, ПРОТОКОЛ, АУТЕНТИФІКАЦІЯ, KERBEROS, ACTIVE DIRECTORY, МЕРЕЖА, LINUX.

КІК.КБ.Б-125-06-ПЗ

					КІК.КБ.Б-125-06-ПЗ				
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми аутентифікації користувачів комп'ютерної системи організації Пояснювальна записка	Літ.	Арк.	Аркушів	
Розроб		Дятел Я.Д.		25.06.21					
Керівник		Байлюк С.М.		25.06.21			4		
Рецензент		Покотило О.А.		25.06.21		ДУЖП, група КБ-1			
Зав. каф.		Сфіменко А.А.		25.06.21					

ABSTRACT

The final qualification work consists of a theoretical part on methods and ways of user authentication, as well as the design of a computer network security subsystem, traffic research, possible types of attacks and an explanatory note. The explanatory note to the qualification work consists of 72 pages, 40 figures and 4 tables.

The purpose of this work is to analyze possible vulnerabilities and develop protection of the client-server part of the network from unauthorized access to resources.

The basic concepts of identification, authentication, authorization and audit of users are defined in the work. The modern Kerberos authentication protocols are considered and its analogues are analyzed. The subsystem of user authentication in the heterogeneous network is developed and the process of traffic passing in it is investigated. Scenarios for possible Kerberos attacks and Active Directory vulnerabilities are listed.

KEY WORDS: PROTECTION, SECURITY, PROTOCOL, AUTHENTICATION, KERBEROS, ACTIVE DIRECTORY, NETWORK, LINUX.

					КІК.КБ.Б-125-06-ПЗ	
Эм						
Арк.	№ документа	Підпис	Дата			5

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система
ПК – персональний комп'ютер
MAC – Media Access Control address
IP – Internet Protocol address
NAC – Network Access Control
NIC – Network Interface Controller
DHCP – Dynamic Host Configuration Protocol
IdM – Identity Managment
SSO – Single sign-on
AAA – Authentication, Authorization, Accounting
CRM – Customer relationship management
ACL – Access-Control List
RAS – Remote Access Service
DSL – Digital Subscriber Line
NAS – Network Access Server
RADIUS – Remote Authentication Dial-In User Service
PAP – Password Authentication Protocol
CHAP – Challenge-Handshake Authentication Protocol
EAP – Extensible Authentication Protocol
PPP – Point-to-Point Protocol
LDAP – Lightweight Directory Access Protocol
TACACS+ – Terminal Access Controller Access-Control System Plus
AD – Active Directory
TCP – Transmission Control Protocol
AVP – Attribute-Value Pairs
IMS – IP Multimedia Systems
KDC – Key Distribution Center
AS – Authentication Server
TGT – Ticket Granting Ticket

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		6

TGS – Ticket Granting Service

DNS – Domain Name System

GNS3 – Graphical Network Simulator

VB – Virtual Box

NTLM – NT LAN Manager

SSSD – System Security Services Daemon

DC – Domain Controller

FQDN – Fully Qualified Domain Names

NTP – Network Time Protocol

ID – Identifier

SID – Security Identifier

GUI – Graphical User Interface

SPN – Service Principal Name

OU – Organizational unit

MFA – Multi-Factor Authentication

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			7

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1. ІДЕНТИФІКАЦІЯ, АУТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ ТА АУДИТ	11
1.1 ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ	13
1.2 УПРАВЛІННЯ СУТНОСТЯМИ	16
1.3 УПРАВЛІННЯ ПАРОЛЯМИ	17
1.3.1 Синхронізація паролів	18
1.3.2 Самостійне скидання паролів	19
1.3.3 Допоміжне скидання паролів	19
1.4 АНАЛІЗ ТА ПОРІВНЯННЯ ПРОТОКОЛІВ АУТЕНТИФІКАЦІЇ	24
1.4.1 Протокол RADIUS	24
1.4.2 Протокол TACACS+	26
1.4.3 Протокол DIAMETER	29
1.4.4 Протокол KERBEROS	30
1.5 ДОСЛІДЖЕННЯ ПРОЦЕСІВ АУТЕНТИФІКАЦІЇ ПРОТОКОЛУ KERBEROS	33
РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	37
2.1 РОЗРОБКА СХЕМИ МАКЕТУ МЕРЕЖІ, ТАБЛИЦЬ КОМУТАЦІЇ ТА ІР-АДРЕСАЦІЇ	37
2.2 РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ АУТЕНТИФІКАЦІЇ У ГЕТЕРОГЕННІЙ МЕРЕЖІ З ВИКОРИСТАННЯМ WINDOWS SERVER 2019 НА БАЗІ ПРОТОКОЛУ KERBEROS	39
2.3 ПРОВЕДЕННЯ ДОСЛІДЖЕННЯ СТОСОВНО МОЖЛИВИХ ТИПІВ АТАК НА ПРОТОКОЛ KERBEROS	51
РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАХИСТУ ВІДНОСНО ДОМЕННОЇ СЛУЖБИ ACTIVE DIRECTORY	57
3.1 ОБСТЕЖЕННЯ ТА АНАЛІЗ ПРОХОДЖЕННЯ ТРАФІКУ В МЕРЕЖІ KERBEROS ЗА ДОПОМОГОЮ ПРОГРАМНОГО ДОДАТКУ WIRESHARK	57
3.2 ВИЗНАЧЕННЯ НАЙКРАЩИХ ПРАКТИК ACTIVE DIRECTORY СТОСОВНО ЗАХИСТУ СИСТЕМ	67
ВИСНОВКИ	70
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	72

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		8

ВСТУП

Актуальність теми. Будь яка пошукова система в Інтернеті по запиту «аутентифікація» надає більше одного мільйона посилань на різні інформаційні ресурси. Цей очевидний факт підтверджує, що підтримка безпеки входу користувачів є давньою проблемою системних адміністраторів та спеціалістів з інформаційної безпеки та кібербезпеки.

Завдання ідентифікації і аутентифікації користувачів є ключовим завданням захисту інформації від несанкціонованого доступу. В останнє десятиліття інтенсивно розвивається напрямок електронної цифровий аутентифікації, в якій збір інформації відбувається з мінімальною участю людини. Технології автоматичної аутентифікації найбільш повно відповідають вимогам комп'ютерних систем і систем управління, де потрібно чітко розпізнавати об'єкти в режимі реального часу.

Перед отриманням доступу до ресурсів комп'ютерної системи користувач повинен зареєструватися. Даний процес, в незалежності від системи, складається з трьох взаємопов'язаних послідовно виконуваних процедур: ідентифікації, аутентифікації і авторизації.

При цьому, під ідентифікацією розуміється процедура розпізнавання суб'єкта за його унікальним ідентифікатором. Для контролю процедури ідентифікації використовується аутентифікація, процедура перевірки автентичності суб'єкта, яка дозволяє достовірно переконатися в тому, що суб'єкт, який пред'явив свій ідентифікатор, насправді є саме тим суб'єктом, ідентифікатор якого він використовує.

Мета ідентифікації і аутентифікації полягає в тому, щоб гарантувати, що в корпоративній інформаційній системі працюють тільки легальні користувачі. Ці дві процедури можна вважати основою програмно-технічних засобів безпеки, оскільки вся розмежувальна політика доступу до ресурсів реалізується щодо ідентифікаторів користувачів. Після проходження суб'єктом процедури аутентифікації йому надаються певні права доступу до ресурсів системи, тобто

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		9

виконується авторизація. Для кожного суб'єкта в системі визначається набір з таких прав, які він може використовувати при зверненні до її ресурсів.

Задля підтвердження свій автентичності суб'єкт повинен надати деяку секретну інформацію, яка повинна бути доступна тільки йому одному. Він може пред'являти системі різні види інформації, звані чинниками аутентифікації.

Виділяють три фактори аутентифікації, які можуть використовуватися в різних комбінаціях: «на основі знання чого-небудь» (наприклад, пароль, PIN-код), «володіння чимось» (наприклад, смарт-карта, токен) та «на основі біометричних характеристик» (наприклад, відбиток пальця, голос). Аутентифікація, в процесі якої використовується два і більше фактори, називається багатофакторною. Вона є безпечнішою, на відміну від однофакторної.

Метою випускної роботи є розробка проекту підсистеми аутентифікації користувачів комп'ютерної мережі організації.

Встановлена мета обумовлює наступні завдання:

- розгляд та порівняння протоколів аутентифікації;
- розгляд протоколу RADIUS;
- розгляд протоколу TACACS+;
- дослідження процесів аутентифікації протоколу Kerberos;
- розробка підсистеми для дослідження роботи протоколів аутентифікації та дослідження проведення атак;
- проектування структурних складових системи;

Об'єктом дослідження є протокол Kerberos та пов'язані з ними процедури аутентифікації.

Предметом дослідження гетерогенна комп'ютерна мережа з операційними системами сімейства Windows та Linux.

В роботі було використано метод системного підходу дослідження інформації.

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			10

РОЗДІЛ 1. ІДЕНТИФІКАЦІЯ, АУТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ ТА АУДИТ

Аби користувач зміг отримати доступ до ресурсів, спочатку йому необхідно довести, що він являється тим, ким він себе називає, має необхідні облікові дані та отримав належні йому права або привілеї для виконання операцій, які він запросив. Після успішного виконання даних дій, користувач може отримати доступ до мережевих ресурсів та використовувати їх. Однак, необхідно відслідковувати діяльність користувача та забезпечити відповідальність за його дії.

Ідентифікація описує метод, за допомогою якого суб'єкт (користувач, програма чи процес) стверджує, що має певну особистість (ім'я, обліковий запис, номер або електронна адреса). Ідентифікація може бути представлена з використанням імені користувача або номеру облікового запису. Для правильної аутентифікації, суб'єкт зазвичай повинен надати другу частину набору облікових даних. Цим елементом може бути пароль, пароліна фраза, криптографічний ключ, персональний ідентифікаційний номер (PIN), анатомічний атрибут (відбиток пальця, візерунок оболонки ока, риси обличчя тощо) або токен. Ці два елементи облікових даних порівнюються з інформацією, котра буда попередньо збережена для даного об'єкту. У випадку коли дані профілю відповідають збереженій інформації, суб'єкт аутентифіковано.

Після того, як індивід надасть необхідні дані та буде аутентифікований належним чином, структура, до якої він намагається отримати доступ, повинна визначити, чи надані йому необхідні права та привілеї для реалізації запрошених дій. Якщо система задовольняє звернення – абонента авторизовано.

Хоча ідентифікація, аутентифікація, авторизація та облік мають близькі та доповнюючи один одного твердження, кожне з них має різні функції, які виконують певні вимоги в процесі управління доступом. Користувач може бути правильно ідентифікований та аутентифікований в мережі, але у нього може не бути авторизації для доступу до ресурсів на файловому сервері. З іншого боку,

					КІК.КБ.Б-125-06-ПЗ	11
Зм	Арк.	№ документа	Підпис	Дата		

користувачу може бути наданий дозвіл на використання файлів на сервері, проте поки він не буде належним чином ідентифікований та аутентифікований, ці дані будуть недоступні. [2]

На наступному рисунку зображено чотири етапи, які повинен пройти суб'єкт, аби отримати доступ до ресурсів.

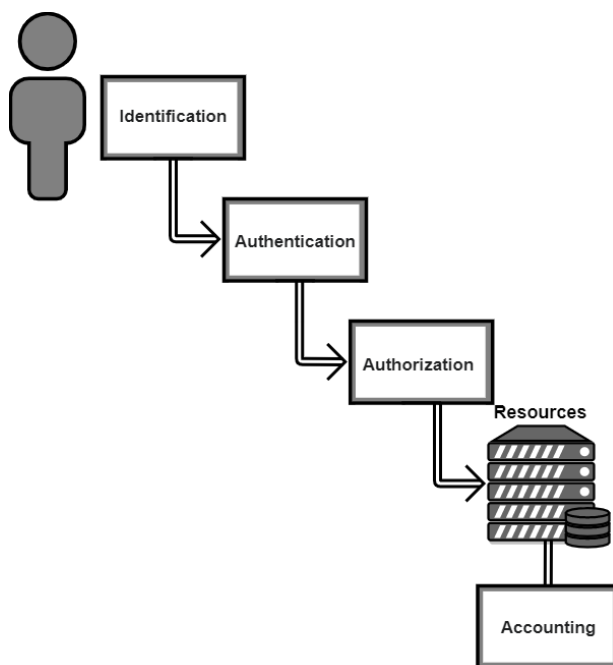


Рисунок 1.1 – Шлях від користувача до необхідних йому даних

Особа повинна нести відповідальність за діяльність, здійснену в мережі. Єдиний спосіб забезпечити облік – це однозначно ідентифікувати суб'єкт і реєструвати його дії.

Далі наведено огляд основних концепцій контролю доступу:

1. Ідентифікація:

- суб'єкти, що надають ідентифікаційну інформацію;
- ім'я користувача, ідентифікатор користувача, номер рахунку.

2. Аутентифікація:

- перевірка ідентифікаційної інформації;
- парольна фраза, значення PIN-коду, відбиток пальця, смарт-картка, одноразовий пароль.

3. Авторизація:

– використання ідентичності суб'єкта разом з іншими критеріями для визначення операцій, які суб'єкт може здійснити над об'єктами;

– «Я знаю, хто ти, що я тобі дозволяю робити?».

4. Аудит:

– журнали аудиту та моніторинг для відстеження предметної діяльності з об'єктами.

Логічний контроль доступу – це технічні інструменти, використовувані для ідентифікації, аутентифікації, авторизації та обліку. Ці програмні компоненти, забезпечують контроль права на доступ до систем, програм, процесів та інформаційних ресурсів. Елементи управління технічним доступом можуть бути інтегровані в операційні системи, додатки, додаткові пакети безпеки або системи управління базами даних та телекомунікаціями. Синхронізація усіх засобів управління та забезпечення покриття всіх вразливих місць, не створюючи перекриття функціональних можливостей, може виявитися доволі складним завданням. Однак, якби це було просто, фахівці з кібербезпеки не були б так затребувані.

Особа повинна бути підтверджена в процесі аутентифікації. Данна процедура зазвичай передбачає двоетапний процес: введення публічної інформації про себе (ім'я користувача, номер працівника, номер рахунку або ідентифікатор відділу), а потім надання приватної інформації (статичний пароль, когнітивний пароль, смарт-токен, одноразовий пароль або PIN-код). Використання загальнодоступної інформації – є етапом ідентифікації при вході, закрита – частина аутентифікації двоступеневого процесу. Кожна техніка, яка використовується для ідентифікації та аутентифікації, має свої плюси і мінуси.

1.1 Ідентифікація та аутентифікація

Після того, як особа була визначена за наявністю відповідного ідентифікатора користувача або подібного способу, необхідне підтвердження нею своєї автентичності. Для аутентифікації можна використовувати три загальні фактори: те, що людина знає, те, що у неї є, і те, ким вона являється. Ці

					КІК.КБ.Б-125-06-ПЗ	13
Зм	Арк.	№ документа	Підпис	Дата		

фактори також називають аутентифікацією за знаннями, за правом власності та за характеристикою відповідно.

Те, що людина знає (за допомогою знань), може бути, наприклад, паролем, PIN-кодом, дівочим прізвищем матері або комбінацією із замком. Аутентифікація людини за допомогою чогось, що вона знає, зазвичай є найменш витратним методом для реалізації. Недоліком цього методу є те, що інша людина може отримати ці знання та отримати несанкціонований доступ до ресурсу.

Те, чим володіє людина (за правом власності), може бути ключем, картою, що проводить пальцем, картою доступу чи значком. Цей метод є загальним для доступу до об'єктів, але його також можна використовувати для доступу до чутливих систем або для аутентифікації систем. Недоліком цього методу є те, що предмет можна загубити або викрасти, що може призвести до несанкціонованого доступу.

Щось специфічне для людини (за характеристикою) стає дещо цікавішим, воно ґрунтується на фізичній ознаці. Аутентифікація особи на основі унікального фізичного атрибута називається біометрією. [20]

Мультифакторна аутентифікація містить два або всі три з цих методів. Використання біометричної системи саме по собі не забезпечує надійної аутентифікації, оскільки містить лише один із трьох варіантів. Біометрія забезпечує те, ким особа є, але не те, що вона знає чи має. Щоб існував надійний процес аутентифікації, дана система повинна поєднуватися з механізмом, який перевіряє один з двох інших методів. Наприклад, багато разів людині доводиться вводити PIN-код на клавіатурі перед тим, як проводити біометричне сканування. Це відповідає категорії «те, що людина знає». І навпаки, від людини може вимагатись провести магнітну карту через зчитувач до біометричного сканування. Це задовольняло б категорію «що є у людини». Незалежно від того, яка система ідентифікації використовується, для того, щоб бути надійною, вона повинна включати більше двох факторів.

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			14

Ідентичність – це складне поняття з безліччю різноманітних нюансів, починаючи від філософського і закінчуючи практичним. Людина може мати кілька цифрових посвідчень. Наприклад, користувачем може бути «Ivanov» в середовищі домену Windows, «IlyaI» на сервері Unix, «IvanovIlyya» на мейнфреймі, «ІО» в режимі обміну миттєвими повідомленнями, «IvanovOIlyya» в центрі підтвердження та «IlyyaO» на Facebook. Якщо компанія хоче централізувати весь існуючий контроль доступу, ці різні ідентифікаційні дані однієї і тієї ж особи можуть спричинити надмірний стрес у адміністратора безпеки. Створення або випуск захищених ідентифікаційних даних повинен включати три ключові аспекти: унікальність, не образність та посвідчення особи.

Перший, унікальність, стосується ідентифікаторів, які є специфічними для конкретної особи, тобто кожен користувач повинен мати унікальний ідентифікатор для підзвітності. Такі речі, як відбитки пальців та сканована сітківка, можна вважати унікальними елементами визначення особистості.

Не образність означає, що жодна частина набору облікових даних не повинна вказувати на мету цього рахунку. Наприклад, ідентифікатор користувача не повинен бути «administrator», «security-admin» або «db_owner».

Третім ключовим аспектом є визначення особистості. Ці елементи надані іншим органом влади як засіб підтвердження особи. Ідентифікаційні картки є свого роду захисним елементом, який вважається формою видачі посвідчення особи.

Хоча більша частина цього розділу стосується аутентифікації користувачів, важливо усвідомити, що вона також можлива і на основі систем. Комп'ютери та пристрої можна ідентифікувати, аутентифікувати, сканувати та контролювати на основі їх апаратних адрес (MAC) та / або адрес Інтернет-протоколу (IP). Мережі можуть мати технологію контролю доступу до мережі (NAC), яка здійснює аутентифікацію систем, перш ніж їм буде дозволено доступ до мережі. Кожен мережевий пристрій має апаратну адресу, яка

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата	15	

вбудована в мережеву карту інтерфейсу (NIC), і програмну адресу (IP), яка або призначається сервером DHCP, або налаштована локально. [19]

1.2 Управління сутностями

Управління особистими даними (Identity Managment) – є широким та завантаженим терміном, який охоплює використання різних продуктів для AAA-систем за допомогою автоматизованих засобів. Саме тому, в даному розділі лише зазначиться невеликий перелік компонентів: управління обліковими записами користувачів, контроль доступу, управління паролями, Single sign-on (SSO) функцією, управління правами та дозволами для облікових записів користувачів, а також аудит і контроль усіх цих елементів.

Нагадаємо, що AAA розшифровується як аутентифікація, авторизація та аудит. Аутентифікація – це процес перевірки особистості користувача, щоб визначити, чи повинен користувач мати дозвіл на доступ до пристрою. Авторизація – це дія обмеження або дозволу доступу до певних функцій у пристрої після аутентифікації користувача. Відповідно аудит – це запис дій, здійснених користувачем після її аутентифікації та авторизації.

IdM вимагає управління однозначно ідентифікованими сутностями, їх атрибутами, обліковими даними та правами. Дозволяє організаціям створювати та управляти життєвими циклами цифрових посвідчень (створювати, підтримувати, припиняти) своєчасно та автоматизовано. Постійне збільшення складності та різноманітності мережевих середовищ лише збільшує складність відстеження того, хто до чого і коли може отримати доступ. Організації мають різні типи додатків, мережеві операційні системи, бази даних, системи управління корпоративними ресурсами (ERM), системи управління взаємовідносинами з клієнтами (CRM), каталоги та мейнфрейми - усі вони використовуються для різних бізнес-цілей. Користувачі зазвичай отримують доступ до декількох різних типів систем протягом своїх щоденних завдань, що ускладнює контроль доступу та забезпечує необхідний рівень захисту для різних типів даних. Ця складність, як правило, призводить до непередбачених

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			16

дір в захисті активів, дублювання та суперечливому контролі. Метою технологій управління ідентифікацією є спрощення адміністрування цих завдань.

Нижче наведено перелік основних типових питань, з якими сьогодні працюють підприємства при контролі доступу до активів:

- розмежування доступу для кожного співробітника, клієнта та партнера;
- визначення того, хто схвалює та надає дозволи;
- прийняття рішень про оновлення політик безпеки;
- з'ясування процесу скасування та/або позбавлення доступу;
- налаштування централізованого моніторинг та контролювання доступу на різних операційних платформах;
- виконання всіх необхідних норм.

Традиційний процес управління ідентифікацією проводився вручну, використовуючи служби каталогів з дозволами, списки контролю доступу (ACL) та профілі. Цей підхід виявився нездатним відповідати складним вимогам, отже його замінили автоматизованими програмами, багатими функціональними можливостями, які працюють разом для створення інфраструктури IdM. Основними цілями технологій IdM є впорядкування управління ідентифікацією, аутентифікація, авторизація та аудит суб'єктів у багатьох системах на всьому підприємстві.

Далі буде розглянуто декілька основних методів, які зазвичай використовуються для підтвердження того, що користувач є тим, за кого він себе видає. В наші дні це зазвичай робиться за допомогою використання паролів, персональних ідентифікаційних номерів (ПІН-кодів), біометрії (наприклад, сканування відбитків пальців) та жетонів доступу. Почнемо з найпоширенішого з усіх методів аутентифікації: пароля.

1.3 Управління паролями

Надалі в цьому розділі буде розглянуто вимоги до пароля, проблеми безпеки та найкращі практики.

					КІК.КБ.Б-125-06-ПЗ	17
Зм						
Арк.	№ документа	Підпис	Дата			

Працівники довідкової служби та адміністратори зазвичай скаржаться на кількість часу, який їм потрібно витратити на скидання паролів, коли користувачі їх забули. Інше питання - кількість різних паролів, які користувачі повинні пам'ятати для різних платформи всередині мережі. Коли пароль змінюється, адміністратор повинен підключитися безпосередньо до цього програмного забезпечення для управління конкретною платформою та змінити значення пароля. Це може здатися не надто клопітним, але якщо в організації є понад 100 користувачів, 6 різних платформ і 25 додатків, задання постійного внесення змін до пароля може призвести до плутанини.

Були розроблені різні типи технологій управління паролями, щоб позбутися цих недоліків за допомогою ІТ та довідкової служби, забезпечивши більш безпечну та автоматизовану систему управління паролями.

Найбільш поширене управління паролями наступні переліки:

- Синхронізація паролів. Зменшує складність відстеження різних паролів для різних систем.
- Самостійне скидання пароля. Зменшує обсяги дзвінків до служби підтримки, дозволяючи користувачам скидати власні паролі.
- Допоміжне скидання пароля. Спрощує процес вирішення проблем із паролями для користувачів. Даний метод можна здійснювати за допомогою інших механізмів аутентифікації (таких як біометричні дані або токени).

1.3.1 Синхронізація паролів

Технології синхронізації паролів можуть дозволити користувачеві підтримувати лише один пароль у кількох системах. Якщо у користувачів занадто багато паролів, які їм потрібно відстежувати, вони, зазвичай, запишуть свої паролі на папері. Такий спосіб є простішим для користувача, але більш небезпечний.

Мета полягає в тому, щоб вимагати від суб'єкта запам'ятовувати лише один пароль, що дозволяє організації застосовувати більш надійні та безпечні

					КІК.КБ.Б-125-06-ПЗ	18
Зм						
Арк.	№ документа	Підпис	Дата			

вимоги до пароля, в такому випадку, користувач швидше за все не матиме проблем із довшими, складнішими рядками значень.

Вразливістю даного методу є те, що для різних ресурсів використовується лише один пароль, хакер повинен з'ясувати лише один набір облікових даних, щоб отримати несанкціонований доступ до всіх ресурсів. Але якщо умови задання паролю є більш вимогливими (16 символів, відсутність словникових співставлень, щонайменше три символи, великі та малі літери тощо), та пароль регулярно змінюється, баланс між безпекою та зручністю використання може бути прийнятним.

1.3.2 Самостійне скидання паролів

Деякі продукти реалізовані так, аби легко дозволити користувачам скинути власні паролі. Це не означає, що користувачі мають будь-які привілейовані дозволи на системи, що дозволяють їм змінювати власні облікові дані. Натомість під час реєстрації облікового запису користувача можна попросити користувача надати кілька особистих питань (домашній улюбленець, прізвище в школі, улюблений гравець тощо) у формі запитань-відповідей. В тих випадках, коли користувач не згадає свій пароль, йому може знадобитися інший механізм аутентифікації (смарт-картка, токен тощо) та відповісти на попередні запитання, щоб легко підтвердити свої особисті дані. Якщо все виконується правильно, особі буде надіслано електронне повідомлення із відновленням паролю.

1.3.3 Допоміжне скидання паролів

Деякі продукти створені для працівників довідкової служби, яким потрібно працювати з окремими людьми, коли вони забули свій пароль. Співробітник служби довідки не повинен знати або запитувати у особи її пароль, це загрожує безпеці системи. Технічна підтримка також не повинна просто змінювати пароль для того, хто зателефонує, без попередньої аутентифікації цієї особи.

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			19

Це може спровокувати атаки типу соціальної інженерії, коли зловмисник телефонує до довідкової служби і вказує, що він є кимось, ким він, насправді не являється. Якби це сталося, зловмисник мав би дійсний пароль співробітника і міг би отримати несанкціонований доступ до коштовностей компанії. Продукти, що надають функцію допоміжного скидання пароля, дозволяють особі технічної підтримки аутентифікувати абонента перед скиданням пароля. Цей процес, зазвичай виконується за допомогою процесу запитів та відповідей на них.

Персонал довідкової служби та абонент повинні бути ідентифіковані та аутентифіковані за допомогою інструмента управління паролями, перш ніж можна буде змінити пароль. Після оновлення пароля система, до якої користувач проходить аутентифікацію, повинна вимагати від користувача змінити пароль знову. Це забезпечить те, що лише вона буде знати свій пароль.

Управління акаунтами в компаніях часто не виконується ефективно та результативно. Управління обліковими записами займається створенням акаунтів користувачів у всіх системах, зміною привілеїв облікових записів, коли це необхідно, та виведенням їх з експлуатації, коли вони більше не потрібні. У більшості середовищ ІТ-відділ створює облікові записи вручну. В різних системах, користувачі отримують надмірні права та дозволи, а коли працівник залишає компанію, багато, або всі облікові записи залишаються активними. Це пов'язано з тим, що централізована технологія управління акаунтами не була застосована.

Продукти управління обліковими записами намагаються атакувати ці проблеми, дозволяючи адміністратору керувати записами користувачів у декількох системах. Коли є декілька каталогів, що містять профілі користувачів або інформацію про доступ, програмне забезпечення для керування обліковим записом дозволяє виконувати реплікацію між каталогами, щоб кожен містив однакову актуальну інформацію.

А тепер давайте подумаємо, як налаштовуються облікові записи. У багатьох середовищах, коли новому користувачеві потрібен обліковий запис,

					КІК.КБ.Б-125-06-ПЗ	20
Зм						
Арк.	№ документа	Підпис	Дата			

адміністратор мережі налаштовує облікові записи та надає певний тип привілеїв та дозволів. Але звідки адміністратор мережі знає, до яких ресурсів повинен мати доступ цей новий користувач і які дозволи слід призначити новому обліковому запису? У більшості ситуацій він цього не робить, ігноруючи дану проблему.

Це те, як користувачі отримують занадто великий доступ до багатьох зайвих для нього речей. Натомість, що має відбутися замість реалізації робочого процесу таким чином. Цей запит, як правило, схвалюється менеджером працівника, і рахунки автоматично налаштовуються в системах, або створюється квиток для технічного персоналу для створення необхідного рахунку.

Якщо є запит на зміну дозволів для акаунту або якщо потрібно вивести його з експлуатації, він проходить той самий процес. Запит надходить до менеджера (або до того, кого доручено виконувати це завдання затвердження), той, в свою чергу, схвалює його, і відбуваються зміни в різних облікових записах.

Компонент автоматизованого робочого циклу є загальним у продуктах для керування відповідними даними про суб'єкта. Це не тільки зменшує потенційні помилки, які можуть мати місце в управлінні обліковим записом, але кожен крок (включаючи затвердження облікового запису) реєструється та відстежується. Це забезпечує підзвітність та надає документацію для використання у зворотному відстеженні, якщо щось піде не так. Це також допомагає гарантувати, що до облікового запису надається лише необхідний обсяг доступу, а також відсутність «осиротілих» акаунтів користувачів, що залишаються активними, коли працівники залишають компанію.

Як і у випадку з продуктами SSO, продукти управління корпоративними рахунками, як правило, дорогі і можуть зайняти роки, щоб правильно розповсюдити їх по всьому підприємству. Однак нормативні вимоги змушують все більше компаній витрачати гроші на такі типи рішень.

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			21

Можливості єдиного входу (Single sign-on). Співробітникам, як правило, протягом дня потрібен доступ до багатьох різних комп'ютерів, серверів, баз даних та інших ресурсів, щоб виконати необхідні завдання. Це часто вимагає від працівників запам'ятовування кількох ідентифікаторів користувачів та паролів для цих різних комп'ютерів.

В утопії користувачеві потрібно буде ввести лише один ідентифікатор користувача та один пароль, щоб мати доступ до всіх ресурсів усіх мереж, в яких працює цей користувач. У реальному світі це важко здійснити для всіх типів систем. Через поширення клієнт-серверних технологій мережі перейшли від централізовано керованих мереж до різноманітних розподілених середовищ.

Поширення відкритих систем та збільшення різноманітності програм, платформ та операційних систем змусили кінцевого користувача запам'ятати кілька ідентифікаторів та паролів користувачів, лише щоб мати доступ до різних ресурсів у власній мережі та використовувати їх. Хоча різні ідентифікатори та паролі повинні забезпечувати більший рівень безпеки, в кінцевому випадку, вони ставлять під загрозу безпеку (оскільки користувачі їх записують) і спричиняють більше зусиль та накладних витрат на персонал, який керує та підтримує мережу.

Як може підтвердити будь-який робітник мережі або адміністратор, занадто багато часу приділяється скиданню паролів для користувачів, які їх забули. Більше ніж на одного працівника впливає продуктивність, коли потрібно перепризначити забуті паролі. Співробітник мережі, який повинен скинути пароль, може працювати над іншими завданнями, а користувач, який забув пароль, не може виконати своє завдання, поки співробітник мережі не закінчить скидання.

Системні адміністратори повинні керувати кількома обліковими записами користувачів на різних платформах, і всі вони повинні координуватися таким чином, щоб підтримувати цілісність політики безпеки. Часом складність може бути величезною, що призводить до поганого управління контролем доступу та генерування багатьох вразливих місць безпеки.

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			22

Збільшені витрати на управління різноманітним середовищем, проблеми безпеки та звички користувачів у поєднанні з надзвичайним бажанням користувачів запам'ятати лише один набір облікових даних породили ідею єдиного входу (SSO). Ці можливості дозволяють користувачеві одноразово вводити облікові дані та мати доступ до всіх ресурсів у первинному та вторинному мережевих доменах. Це зменшує кількість часу, який користувачі витрачають на аутентифікацію ресурсів, і дозволяє адміністратору впорядковувати облікові записи користувачів та краще контролювати права доступу. Також покращує безпеку, зменшуючи ймовірність того, що користувачі записуватимуть паролі, а також зменшує час адміністратора, витрачений на додавання та видалення облікових записів та зміну дозволів доступу. Якщо адміністратору потрібно вимкнути або призупинити певний обліковий запис, він може зробити це повсюдно, замість того, щоб змінювати конфігурації на кожній платформі.

Які ж все таки перешкоди зустрічаються в подібних системах? В основному – проблеми сумісності. Щоб SSO насправді працював, кожна платформа, програма та ресурс повинні приймати однотипні облікові дані в одному форматі та тлумачити їх значення однаково.

Існує також проблема безпеки, яку слід розглянути в даному середовищі. Як тільки б зломисник зміг розкрити один набір облікових даних, він мав би доступ до кожного ресурсу в середовищі, до якого має доступ скомпрометований обліковий запис. Це, безумовно, правда, але одна з ідей даної технології полягає в тому, що якщо користувач повинен запам'ятати лише один пароль, а не десять, тоді варто застосовувати більш надійну політику щодо паролів. Якщо користувач має запам'ятати лише один пароль, він може бути більш складним і безпечним, оскільки у суб'єкта немає дев'яти інших, з якими б йому довелося мати справу.

Технології єдиного входу бувають різних типів. Кожен має свої переваги та недоліки, вади та якісні характеристики. Доволі рідко можна зустріти справжнє SSO-середовище; швидше, ви побачите скупчення комп'ютерів та

					КІК.КБ.Б-125-06-ПЗ	
Зм						23
	Арк.	№ документа	Підпис	Дата		

ресурсів, які приймають однакові облікові дані. Однак для інших ресурсів адміністратору або користувачеві потрібно більше роботи для доступу до систем. [8]

1.4 Аналіз та порівняння протоколів аутентифікації

Підтримка безпеки та цілісності системи в мережі є надзвичайно важливою, і вона охоплює кожного користувача, програму, службу та сервер в мережевій інфраструктурі. Це вимагає розуміння всього, що працює в мережі, та способу використання цих служб. Основою метою цієї безпеки є підтримка доступу до цих програм та служб та забезпечення цього доступу.

Аутентифікація користувача є першим пріоритетом при відповіді на запит, зроблений користувачем до програмному додатку. Існує декілька механізмів, необхідних для аутентифікації при наданні доступу до даних. У цьому підрозділі буде розглянуто найбільш поширені протоколи і розглянуто їх переваги й недоліки.

1.4.1 Протокол RADIUS

Remote Authentication Dial-In User Service – це мережевий, клієнт-серверний протокол, який частіше використовується для централізації аутентифікації та авторизації клієнтів Remote Access Service (RAS). RAS - це послуга, яка використовується для дозволу на комутовані з'єднання з віддаленими клієнтами, а також Digital Subscriber Line (DSL) та оптоволоконної оптики. Мережа може мати Network Access Server (NAS), котрий запитує реєстраційні дані віддаленого користувача та передає їх назад на RADIUS-сервер, де зберігаються імена користувачів та значення паролів.

Уявімо, що користувач входить до сервісів Google, Amazon або Yandex (мається на увазі, що це може відбуватися з будь-якої точки світу). Наївно гадати, що ці організації беруть ім'я користувача та пароль і копіюють їх на всі свої сервери. Це був би адміністративний кошмар! Коли абонент отримує

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			24

доступ до одного із серверів для регіону, в якому проживає, їх сервер взаємодіє із сервером аутентифікації.

Цей сервер аутентифікації, в даному випадку – RADIUS, надає вам доступ та права на ці ресурси. Згодом, перевіряє облікові дані, які використовує особа. З відповідною інформацією забезпечує належний доступ до мережі залежно від того, ким можете бути суб'єкт, та відстежує, коли він здійснював вхід та вихід із системи. [14]

Сервер доступу та програмне забезпечення замовника обговорюють процедуру «рукостискання» та узгоджують протокол аутентифікації (Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP) або Extensible Authentication Protocol (EAP)). Клієнт надає серверу доступу ім'я користувача та пароль. Це спілкування відбувається через з'єднання Point-to-Point Protocol (PPP). Сервер доступу та RADIUS-сервер спілкується через протокол RADIUS.

Після того, як аутентифікація завершена належним чином, системі клієнта надається IP-адреса та параметри підключення, а також доступ до Інтернету. NAS повідомляє серверу аутентифікації, коли сеанс починається і зупиняється відповідно до оплати. RADIUS також використовується в корпоративному середовищі, щоб забезпечити віддаленим співробітникам та домашнім користувачам доступ до мережевих ресурсів.

Дане середовище дозволяє компаніям підтримувати профілі користувачів у центральній базі даних. Коли суб'єкт набирає номер і має належну аутентифікацію, йому призначається попередньо налаштований профіль, який контролює, до яких ресурсів він може отримати доступ. Ця технологія дозволяє компаніям мати єдину адміністративну точку входу, яка забезпечує стандартизацію безпеки та спрощений спосіб відстеження використання та статистики мережі.

RADIUS був розроблений компанією Livingston Enterprises для своєї серії серверів мережевого доступу, але потім був опублікований як набір стандартів (RFC 2865 та RFC 2866). Це означає, що це відкритий протокол, який будь-який

					КІК.КБ.Б-125-06-ПЗ	25
Зм	Арк.	№ документа	Підпис	Дата		

постачальник може використовувати та маніпулювати ним, щоб він працював у межах своїх окремих продуктів. Виходячи з цього, його можна використовувати в різних типах реалізацій.

Формат конфігурацій та облікові дані користувача можуть зберігатися на серверах LDAP, різних базах даних або текстових файлах. На рис.1.2. зображено кілька варіантів використання RADIUS у мережі.

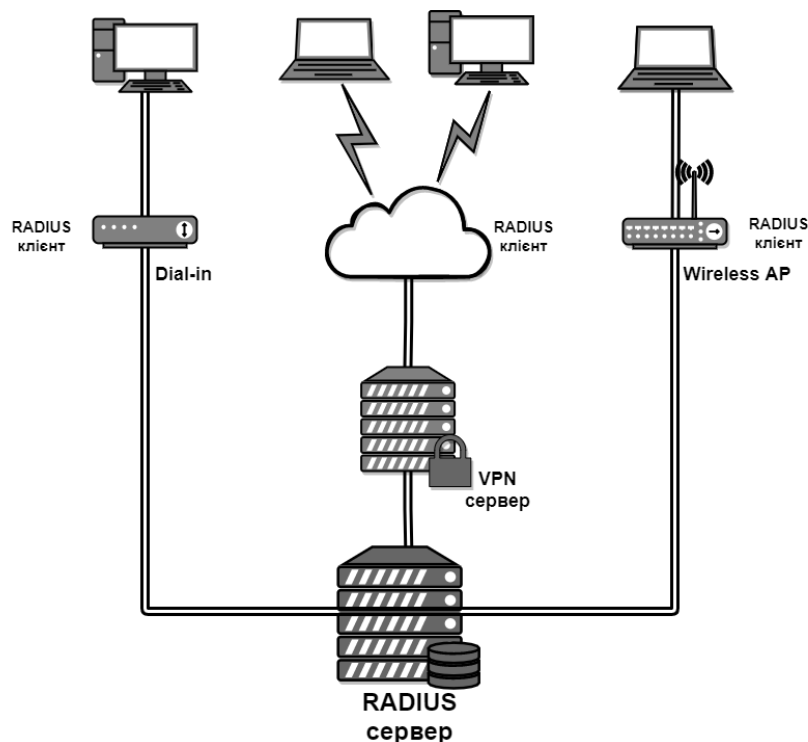


Рисунок 1.2 – Приклад можливих реалізацій інфраструктури RADIUS

1.4.2 Протокол TACACS+

Terminal Access Controller Access-Control System Plus – це клієнт-серверний протокол, розроблений Міністерством оборони США, а пізніше вдосконалений Cisco Systems. TACACS+ широко застосовується сьогодні, щоб забезпечити адміністрування пристроїв для маршрутизаторів, серверів мережевого доступу та інших обчислювальних пристроїв в мережі через один або кілька централізованих серверів. Даний протокол відокремлює функцію авторизації, тому він забезпечує додаткову гнучкість та детальний контроль доступу до того, хто може запускати команди на певних мережевих пристроях. Кожна така команда, введена користувачем, надсилається назад на центральний

сервер TACACS+ для авторизації, який потім перевіряє команду з авторизованим списком команд для кожного користувача або групи. Для зв'язку між клієнтом та сервером використовує різні типи повідомлень залежно від функції. Іншими словами, для аутентифікації можуть використовуватися інші повідомлення, ніж для авторизації та аудиту. [8]

Також цей протокол може визначати політики на основі користувача, типу пристрою, місцезнаходження або часу доби. Служба може використовувати локально налаштованих користувачів або користувачів та групи, визначені в Active Directory або LDAP, для управління доступом до пристроїв у відповідній мережі. Це дає можливість єдиного входу (SSO), що підвищує рівень безпеки, спрощує управління та полегшує роботу користувачів.

Основні відмінності між RADIUS і TACACS+. RADIUS був розроблений для аутентифікації та реєстрації комутованого пульта дистанційного керування користувачів до мережі, а TACACS+ використовується найчастіше для доступу адміністратора до мережевих пристроїв, таких як маршрутизатори та комутатори. Це зазначено в назвах протоколів.

Основна функціональна різниця між RADIUS і TACACS+ полягає в тому, що TACACS+ відокремлює функцію авторизації, де RADIUS поєднує в собі і аутентифікацію, і авторизацію. Незважаючи на те, що це може здатися невеликою деталлю, це значно впливає на впровадження AAA в мережевому середовищі.

Загалом, система контролю доступу контролера доступу терміналів, в основному здійснює ту саму функціональність, що й RADIUS, з деякими відмінностями в його характеристиках. По-перше, TACACS+ використовує TCP як транспортний протокол, тоді як RADIUS використовує UDP. Оскільки UDP - це безпроводний протокол, він не буде виявляти або виправляти помилки передачі. Отже, RADIUS повинен мати необхідний додатковий код для виявлення пошкодження пакетів, тривалих тайм-аутів або скинутих пакетів. Оскільки розробники TACACS+ вирішили використовувати TCP, програмному

					KIK.KB.B-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		27

забезпеченню даного протоколу не потрібно мати додаткових налаштувань для пошуку та вирішення цих проблем передачі. TCP - це протокол, орієнтований на підключення, і в цьому полягає його робота та відповідальність. [24]

Таблиця 1.1

Порівняння протоколів RADIUS та TACACS+

RADIUS	TACACS+
Поєднує аутентифікацію та авторизацію	Відокремлює всі три елементи AAA, роблячи налаштування більш гнучкими
Менш безпечний – хешує лише паролі	Більш безпечний – шифрує весь пакет включаючи ім'я користувача, пароль та атрибути
Потребує вміст конфігурації авторизації на кожному з мережевих пристроїв	Центральне управління для конфігурування авторизацією
Не здійснює журналювання команд	Повна реєстрація команд

RADIUS шифрує пароль користувача лише під час його передачі від клієнта на сервер. Інша інформація, як-от ім'я користувача, бухгалтерія та авторизовані послуги, передається у відкритому тексті. Можна трактувати це, як відкрите запрошення для зломисників збирати інформацію про сеанс для повторних атак. Постачальники, які інтегрують RADIUS у свої продукти, повинні розуміти ці слабкі місця та впроваджувати інші механізми безпеки для захисту від таких типів атак. TACACS + шифрує всі ці дані між клієнтом і сервером і, отже, не має вразливостей, властивих протоколу RADIUS.

Який протокол для AAA-сервера використовувати, необхідно вибирати в залежності від завдання. Якщо це адміністрування пристроїв, то TACACS+ стане кращим варіантом, а якщо доступ до мережі, то більш універсальний і швидкий – RADIUS. Інколи, вони обидва використовують разом, розподіляючи навантаження, виходячи з можливості протоколів.

Пам'ятаємо, що по суті, це є протоколи, котрі являються лише узгодженими способами спілкування. RADIUS-клієнт, при взаємодії з відповідним сервером робить це за допомогою того ж протоколу, який насправді є лише набором визначених полів (AVP), які прийматимуть певні значення. Як аналогію, припустимо, особа надсилає іншій людині документ, який містить декілька аркушів паперу, на кожному з яких надруковано

заголовок: ім'я, прізвище, посада, кабінет. Ви, відповідно, заповнюєте ці поля своїми даними і надсилаєте їх їй назад. В основному так працюють протоколи; система, що відправляє, просто заповнює поля вказаною інформацією, яку отримує служба для отримання та обробки. Оскільки TACACS+ дозволяє більш детально контролювати, що користувачі можуть, а що не можуть робити, TACACS+ має більше AVP, що дозволяє адміністратору мережі визначати ACL, фільтри, права користувача та багато іншого.

Також RADIUS не реєструє команди, які використовуються адміністратором. Він лише реєструє початок та проміжні записи цього сеансу. Це означає, що якщо одночасно входять два або більше адміністраторів, із журналів RADIUS неможливо визначити, який адміністратор ввів які команди.

1.4.3 Протокол DIAMETER

DIAMETER – це стандартний протокол наступного покоління, що використовується для обміну інформацією щодо аутентифікації, авторизації та обліку (AAA) в мережах Long-Term Evolution (LTE) та IP Multimedia Systems (IMS).

Він був отриманий та вдосконалений завдяки широко поширеному AAA-протоколу RADIUS, забезпечуючи більш надійні, безпечні та гнучкі транспортні механізми для мобільних мереж передачі даних. Різноманітні мережеві функції LTE та IMS використовуються в DIAMETER, включаючи функції Charging Rules Function (PCRF), Home Subscriber Server (HSS) and Online Charging System (OCS). Протокол забезпечує загальну структуру для обміну повідомленнями AAA, а також визначає стандартний набір команд і атрибутів запиту та відповіді AAA.

В даному розділі не будуть детально розглядатися можливості даного протоколу, в зв'язку з його незначним поширенням та підтримкою виробниками AAA-рішень. Порівняння DIAMETER стосовно інших AAA-протоколів можна побачити в наступній таблиці.

					КІК.КБ.Б-125-06-ПЗ	29
Зм	Арк.	№ документа	Підпис	Дата		

Порівняльна таблиця AAA-протоколів

	RADIUS	DIAMETER	TACACS+
Комунікація	Клієнт-серверний протокол	Одноранговий протокол	Клієнт-серверний протокол
Транспортний протокол	UDP	TCP або SCTP	TCP
Типи аутентифікації	PAP, CHAP, EAP	PAP, CHAP, EAP	PAP, CHAP, EAP/802.1x
Багатопротокольна підтримка	Працює через PPP-з'єднання	Mobile IP, EoPPP, VoIP, roaming protocols	AppleTalk, NetBIOS, та IPX
Особливості	Відкритий протокол	Вільно розповсюджуваний	Пропріетарний протокол Cisco
Основне призначення	Доступ до мережі	Стільниковий зв'язок	Адміністрування пристроїв

1.4.4 Протокол KERBEROS

Kerberos – це протокол безпеки комп'ютерної мережі, який аутентифікує запити на обслуговування між двома або більше надійними хостами в ненадійній мережі, як-от Інтернет. Він використовує криптографічний секретний ключ (secret key) та надійну третю сторону для аутентифікації клієнт-серверних програм та перевірки ідентифікації користувачів.

Протокол забезпечує механізм, який дозволяє як користувачам, так і машинам ідентифікувати себе в мережі та отримувати визначений, обмежений доступ до областей та служб, які налаштовані адміністратором. Протокол аутентифікує сутності, перевіряючи їх ідентичність, а також захищає ці дані, аби сторонні не могли отримати до них доступ і використовувати їх або підробляти.[9]

Більшість звичайних мережевих служб використовують схеми аутентифікації на основі паролів, коли користувач надає пароль для доступу до певного мережевого сервера. Однак передача інформації про аутентифікацію для багатьох служб є незашифрованою. Щоб така схема була безпечною, мережа повинна бути недоступною для сторонніх, і всі комп'ютери та користувачі мережі повинні мати довіреність.

Kerberos – це назва технології безпеки, яка забезпечує функціональність аутентифікації з метою захисту активів компанії. Даний протокол аутентифікації був розроблений в середині 1980-х років в рамках проекту Athena від MIT. Він працює за клієнт-серверною моделлю і базується на симетричній криптографії ключів. Протокол використовується роками в системах Unix і в даний час є методом аутентифікації за замовчуванням для операційних систем Windows 2000 та пізніших версій. Крім того, Apple OS X, Oracle Solaris та Red Hat Enterprise Linux використовують аутентифікацію Kerberos.

Комерційні продукти, що підтримують Kerberos стають все частішими, адже він є прикладом SSO системи для середовищ і є фактичним стандартом для розподілених мереж. Kerberos включає широкий спектр можливостей захисту, що надає компаніям набагато більшу гнучкість та масштабованість, коли їм потрібно забезпечити охоплюючу архітектуру безпеки. Він має чотири елементи, необхідні для контролю доступу до підприємств: масштабованість, прозорість, надійність та безпека.

Однак ця відкрита архітектура також викликає проблеми сумісності. Коли постачальники мають велику свободу налаштовувати протокол, зазвичай це означає, що жоден постачальник не налаштує його однаково. Kerberos використовує симетричну криптографію ключів та забезпечує наскрізну безпеку. Хоча він дозволяє використовувати паролі для аутентифікації, він був розроблений спеціально для усунення необхідності передавати паролі через мережу. Більшість таких реалізацій працюють із загальними секретними ключами.[17]

Аутентифікація Kerberos використовує мітки часу як частину свого протоколу. Коли годинник сервера Kerberos і клієнтського комп'ютера не синхронізовані, стає неможливим належним чином пройти аутентифікацію. Зазвичай запас співпадання часу становить 5 хвилин.

Key Distribution Center (KDC) є найважливішим компонентом у середовищі Kerberos. Дозволяє зберегти секретні ключі (secret key) всіх

					KIK.KB.B-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		31

користувачів та служб на Authentication Server (AS). Крім того, надає послугу аутентифікації, а також функціональність розподілу ключів. Клієнти та служби довіряють цілісності KDC, і ця довіра є основою безпеки Kerberos.

Центр надає послуги безпеки принципалам, які можуть бути користувачами, програмами або мережевими службами. AS повинен мати їх облікові записи та надати, за потреби, разом з відповідним ключем. Для користувачів пароль хешується у секретний ключ, котрий може використовуватися для передачі конфіденційних даних між довіреними сутностями та KDC і використовується для цілей аутентифікації користувачів. Квиток генерується Ticket Granting Service (TGS) на KDC і передається довіреному суб'єкту, скажімо користувачу, який повинен пройти аутентифікацію в іншого довіреного суб'єкта, скажімо, файлового сервера.

Більш детально про процес аутентифікації у Kerberos середовищі буде описано у другому розділі.

Система Kerberos може бути скомпрометована, якщо користувач у мережі використовує служби, які невідомі Kerberos, передаючи пароль у звичайному тексті. Вкрай не рекомендується користуватися такими послугами (включаючи telnet та FTP). Іншим зашифрованим протоколам, таким як SSH або SSL, надається перевага перед незашифрованими службами, але це все ще не ідеальні рішення.

Слабкі сторони Kerberos. Нижче наведено деякі потенційно вразливі місця протоколу:

- До KDC необхідний постійний доступ. Якщо центр розподілу не працює, ніхто не зможе звернутись до ресурсів чи послуг. Резервування в такому випадку є важливою складовою.

- Секретні ключі тимчасово зберігаються на робочих станціях користувачів, а це означає, що зловмисник може отримати ці криптографічні ключі.

					КІК.КБ.Б-125-06-ПЗ	32
Зм	Арк.	№ документа	Підпис	Дата		

– Сеансові ключі розшифровуються і розміщуються на робочих станціях користувачів або в кеш-пам'яті, або в таблиці ключів. Знову ж таки, зловмисник може захопити ці ключі.

– Kerberos вразливий до вгадування пароля (Brute-force attack). KDC не знає, чи відбувається атака за словником.

– Мережевий трафік не захищений Kerberos, якщо шифрування не ввімкнено.

– Якщо ключі занадто короткі, вони можуть бути вразливими до атак грубої сили.

– Протокол потребує синхронізації годинників клієнта та сервера.

Kerberos повинен бути прозорим (працювати у фоновому режимі, без необхідності розуміння користувачем), масштабованим (працювати у великих гетерогенних середовищах), надійним (використовувати розподілену архітектуру сервера) та захищеним (забезпечувати аутентифікацію та конфіденційність).

1.5 Дослідження процесів аутентифікації протоколу Kerberos

За допомогою простої аутентифікації на основі пароля не можна вважати мережу, підключену до Інтернету, безпечною. Будь-який зловмисник, який отримує доступ до мережі, може використовувати простий аналізатор пакетів або пакетний сніфер для перехоплення імен користувачів та паролів, компрометації облікових записів користувачів, що безпосередньо загрожує цілісності всієї інфраструктури безпеки.

Kerberos виключає передачу незашифрованих паролів через мережу та усуває потенційну загрозу від зловмисника, який сканує мережу.

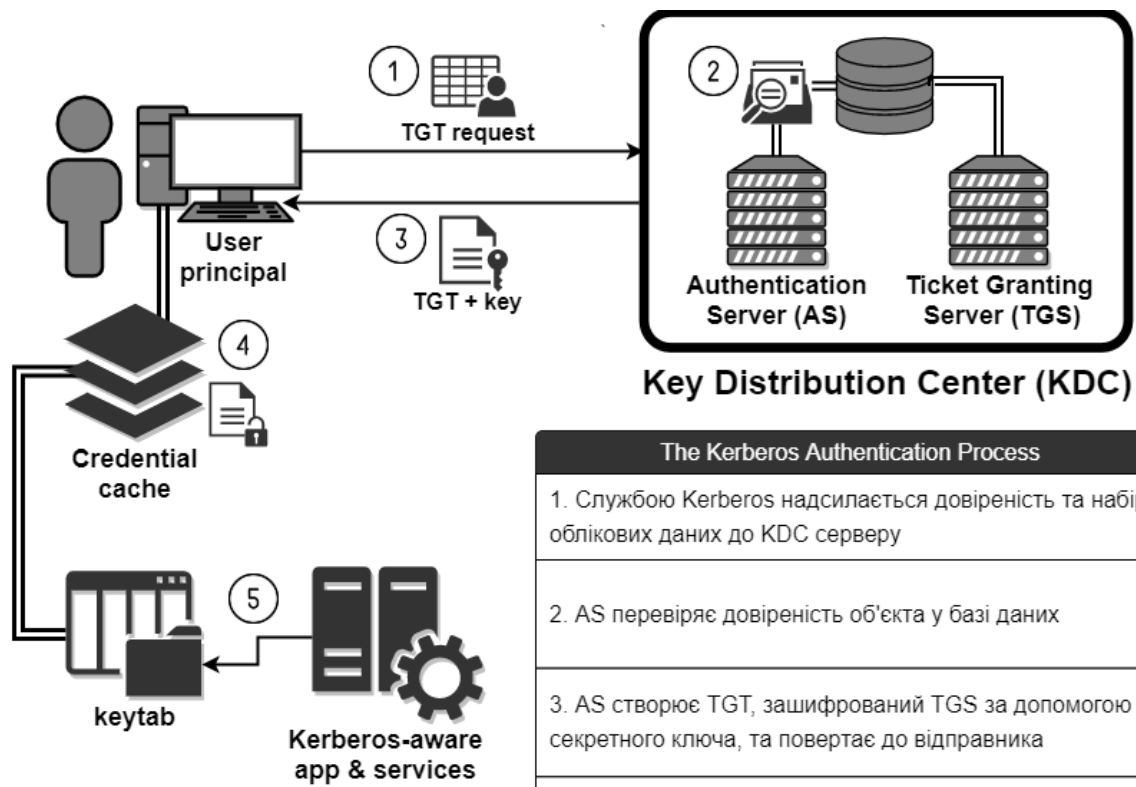
Замість того, щоб аутентифікувати кожного користувача для кожної мережевої служби окремо, як із простою аутентифікацією пароля, Kerberos використовує симетричне шифрування та надійну третю сторону (центр розподілу ключів) для аутентифікації користувачів у наборі мережеских послуг. KDC та комп'ютери, якими він керує, становлять єдине середовище.

					KIK.KB.B-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		33

Коли користувач надсилає запит, KDC відправляє набір облікових даних (квиток), специфічних для цього сеансу, назад на машину користувача, і служби Kerberos шукають квиток безпосередньо на робочій станції користувача, а не вимагають від нього аутентифікації за допомогою пароля.

Як показано на малюнку 1.3, кожен користувач ідентифікується в KDC довіреним об'єктом. Коли користувач мережі Kerberos входить на свою робочу станцію, його довіреність надсилається до KDC як частина запиту Ticket Granting Ticket (TGT) із сервера аутентифікації (AS). Цей запит може бути відправлений програмою для входу, щоб він був прозорим для користувача, або може бути надісланий вручну після входу.

Потім KDC перевіряє довіреність суб'єкта у своїй базі даних. Якщо така буде знайдена, KDC створить TGT, зашифрує його за допомогою секретного ключа та надішле назад.



Термін дії Ticket Granting Ticket закінчується через певний проміжок часу (зазвичай 10-24 години) і зберігається в кеші облікових даних клієнтської машини

The Kerberos Authentication Process	
1.	Службою Kerberos надсилається довіреність та набір облікових даних до KDC серверу
2.	AS перевіряє довіреність об'єкта у базі даних
3.	AS створює TGT, зашифрований TGS за допомогою секретного ключа, та повертає до відправника
4.	Клієнтська програма входу розшифровує TGT за допомогою ключа та зберігає у кеші облікових даних
5.	Після автентифікації Kerberos-aware services можуть перевіряти незашифрований список розпізнаних довіреностей та їх ключів, що зберігаються у key table.

Рисунок 1.3 – Покроковий процес аутентифікації Kerberos

Kerberos покладається на можливість розпізнавання пристроїв та на точні позначки часу для видачі квитка та визначення закінчення його терміну дії. Таким чином, даний протокол вимагає як точної синхронізації годинника, так і діючої служби доменних імен (DNS) для коректної роботи.

Наступним кроком клієнтська програма входу розшифровує TGT за допомогою ключа, яку вона обчислює, використовуючи пароль користувача. Цей ключ використовується лише на клієнтській машині і не передається по мережі. Квиток (облікові дані), надіслані KDC, зберігаються в локальному файлі, так називаємоу: кеші облікових даних. Після аутентифікації сервіси підтримки Kerberos можуть перевіряти незашифрований список розпізнаних довіреностей та їх ключів, що зберігаються у відповідну таблицю (keytab).

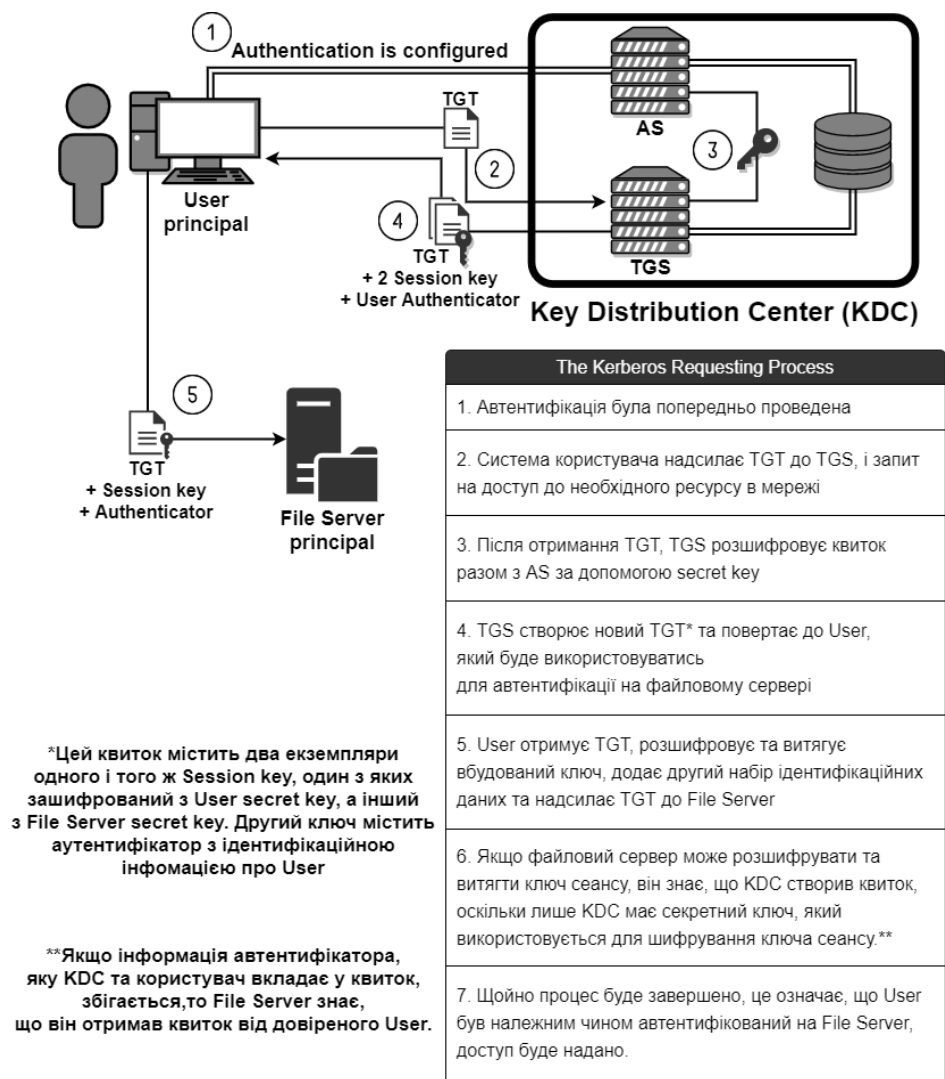


Рис. 1.4 – Процес підключення до файлового серверу

Термін дії TGT закінчується через певний проміжок часу (зазвичай від десяти до двадцяти чотирьох годин) і зберігається в кеші облікових даних клієнтської машини. Після випуску TGT користувачеві не потрібно повторно вводити свій пароль, поки термін дії TGT не закінчиться, або поки він не вийде і не увійде знову. [21]

Щоразу, коли користувачеві потрібен доступ до мережевої послуги, клієнтське програмне забезпечення використовує TGT для запиту нового квитка для цієї конкретної послуги у сервера видачі квитків (TGS).

Отже, Kerberos представляє собою відкритий стандарт, який підтримується багатьма спільнотами розробників з відкритим кодом. Тому технічно спроможні організації можуть повністю підтримувати власне використання Kerberos, оскільки вони мають повний доступ до технології, а також до спільнот розробників. Крім того, багато інших продуктів та інструментів вже інтегровано з Kerberos, що може ще більше зменшити зусилля з розвитку.

РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1 Розробка схеми макету мережі, таблиць комутації та IP-адресації

Для проектування, необхідної для виконання прикладу аутентифікації, мережі, буде використано середовище розробки Graphical Network Simulator (GNS3). Емулятор дозволяє створювати різні мережеві топології безпосередньо на комп'ютері. Найчастіше GNS використовується в якості лабораторного стенду, де можна перевірити ту чи іншу технологію або схему.

Крім того, надає можливість підключити віртуальну робочу станцію і запускати всередині оригінальне програмне забезпечення. Всі основні компоненти пристрою, в тому числі процесор, пам'ять і пристрої введення / виводу легко емулюються у середовищі, завдяки чому отримується повнофункціональна модель пристрою.

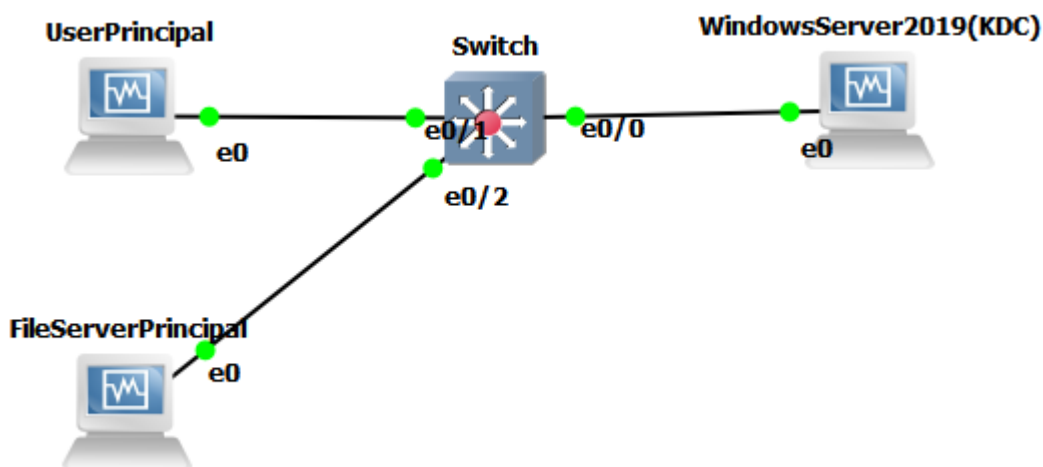


Рисунок 2.1 – Проект побудованої мережі для демонстрації процесу аутентифікації протоколу Kerberos

Для створеного проекту використовуватись наступні мережеві складові:

- Windows Server 2019 (KDC);
- DNS для внутрішнього домену;
- User Principal;
- File Server Principal;

Таблиця 2.1

Параметри адресації мережі

Мережа/пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс
Підмережа А	–	192.168.0.0	255.255.255.248	/29
Control Domain Center (Windows Server 2019)	Eth 0	192.168.0.1	255.255.255.248	/29
Switch	Інтерфейс Vlan1	192.168.0.5	255.255.255.248	/29
User Principal	Eth 0	192.168.0.2	255.255.255.248	/29
File Server Principal	Eth 0	192.168.0.3	255.255.255.248	/29

Таблиця 2.2

Параметри інтерфейсів пристроїв

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Control Domain Center (Windows Server 2019)	Eth 0	Switch	Eth 0/0
Switch	Eth 0/0	Control Domain Center	Eth 0
	Eth 0/1	User Principal	Eth 0
	Eth 0/2	File Server Principal	Eth 0
User Principal	Eth 0	Switch	Eth 0/1
File Server Principal	Eth 0	Switch	Eth 0/2

Згідно до розробленої таблиці 2.1, було виконано налаштування параметрів IP-адресації локальних пристроїв. Приклад налаштування для Windows Server приведено на рисунку 2.2.

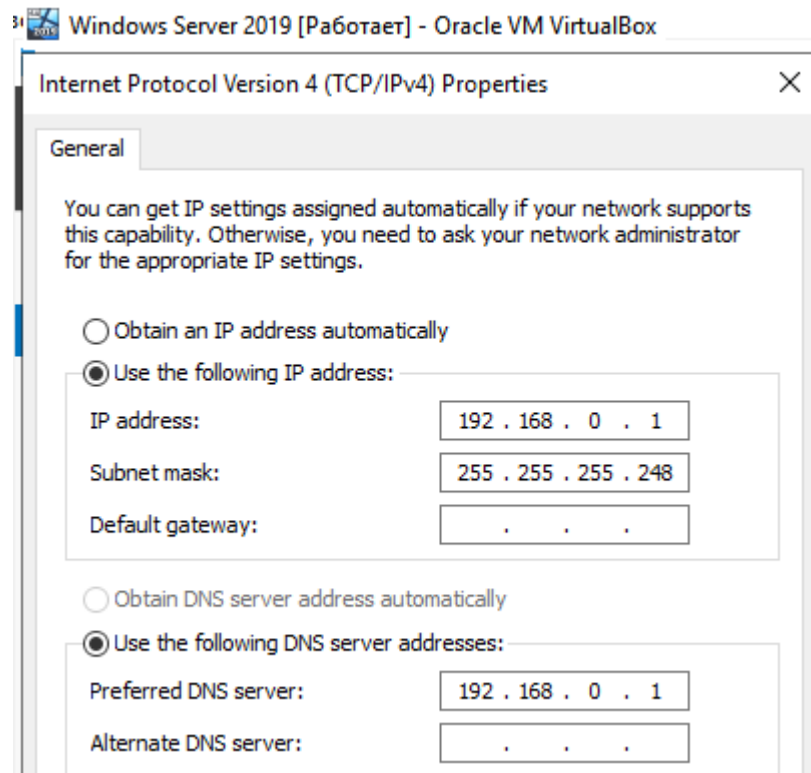


Рисунок 2.2 – Налаштування IP-адресації на Windows Server 2019

Приклад налаштування адресації на Linux машині зображений на наступному рисунку(рис.2.3):

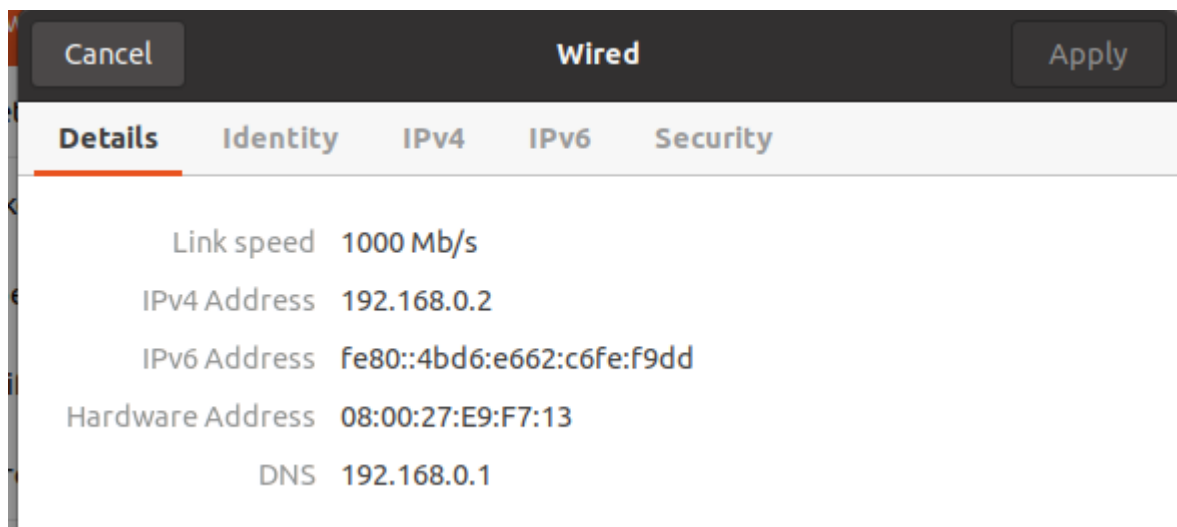


Рисунок 2.3 – Приклад налаштування IP-адресації на Linux-пристрої

2.2 Розгортання та налаштування аутентифікації у гетерогенній мережі з використанням Windows Server 2019 на базі протоколу Kerberos

Першим необхідним кроком буде здійснення встановлення Windows Server. Для цього нам знадобиться VirtualBox – програмне забезпечення, яке

КІК.КБ.Б-125-06-ПЗ					39
Зм.	Арк.	№ документа	Підпис	Дата	

імітує справжній комп'ютер, що дає можливість користувачеві встановлювати, запускати і використовувати інші операційні системи, як звичайні додатки.

Віртуальна машина створює ізольоване оточення на комп'ютері, яке складається з віртуальних компонентів реального ПК: жорсткого диска, відеокарти, оперативної пам'яті, різних контролерів пристроїв і т.п.. Таким чином, встановлена в VirtualBox операційна система буде повністю впевнена в тому, що вона працює на реальному обладнанні.

У деяких випадках при роботі з VirtualBox можуть знадобитися особливі настройки машини, але сам процес установки ОС ідентичний для обох варіантів. В даному випадку використовується інтеграція VB-хостів у середовище розробки GNS3.

Менеджер встановлення пропонує вибір з двох методів: просунутий (зі збереженням інформації, налаштувань та додатків) та вибірковий (з форматуванням диску для «чистої» конфігурації системи). Обрано другий метод, оскільки створено новий віртуальний жорсткий диск без наявних на ньому образів.

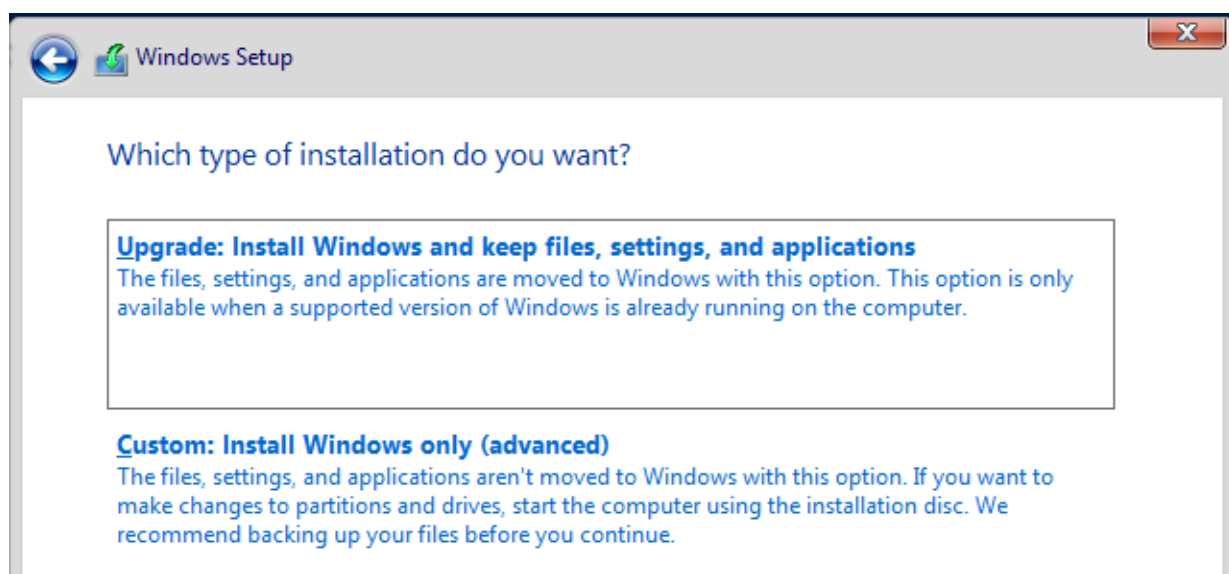


Рисунок 2.4 – Вибір методу інсталювання серверу

В ході процесу система перезавантажиться, після чого необхідно буде створити новий пароль для входу до облікового запису.

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		40

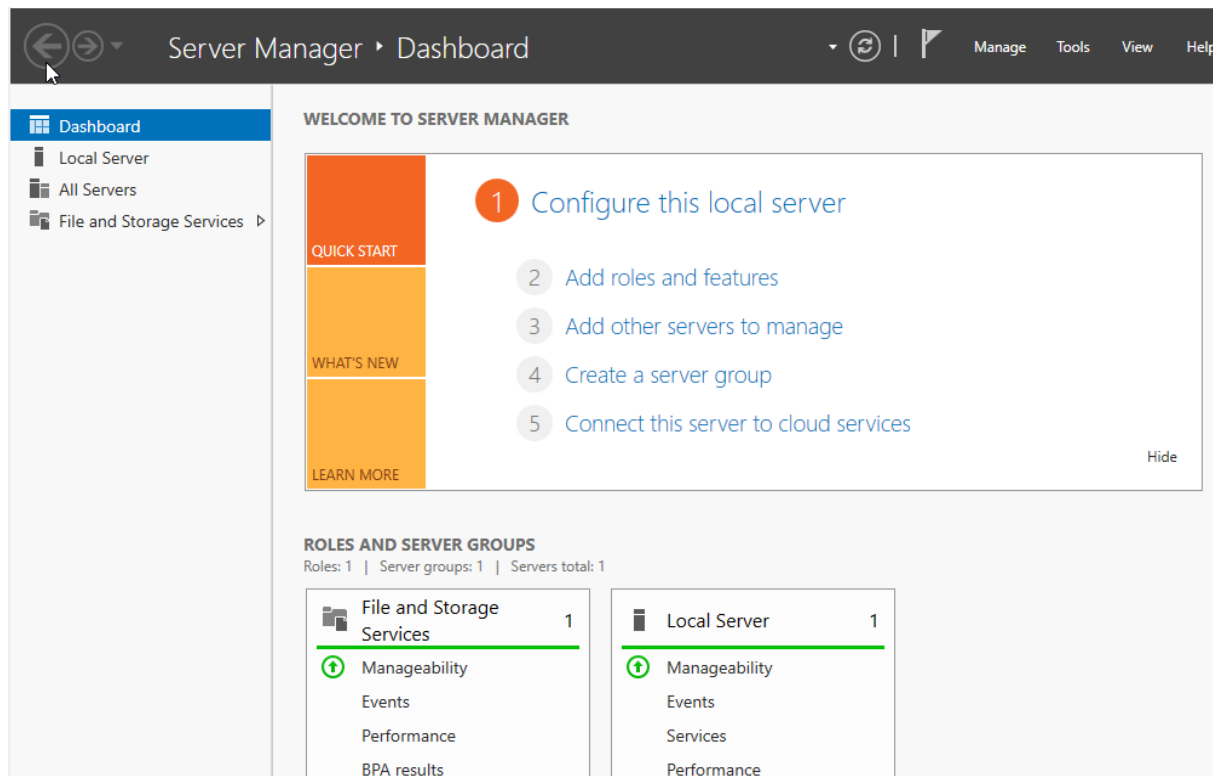


Рисунок 2.5 – Головний екран консолі управління (Server Manager)

Наступним кроком, задля використання Domain Name System (DNS) – системи, що дозволяє перетворити доменне ім'я в IP-адресу сервера і навпаки, необхідно налаштувати DNS-сервер на домені. Це мережева служба, яка забезпечує і підтримує роботу DNS. Служба DNS-сервера не вимоглива до ресурсів машини. Для коректного функціонування знадобиться установка додаткових ролей на сервер, використовуючи «Майстер Додавання Ролей і Компонентів», який можна знайти в «диспетчері Сервера».[11]

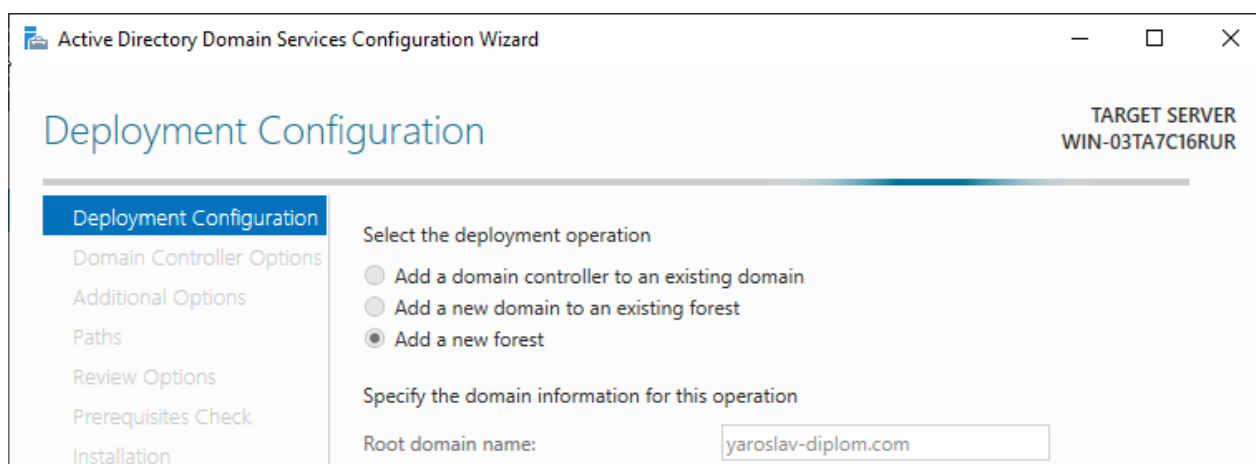


Рисунок 2.6 – Вікно створення доменного імені

Переконалися у правильності встановлених додаткових компонентів та ролей можна виконавши дії на наступному рисунку.

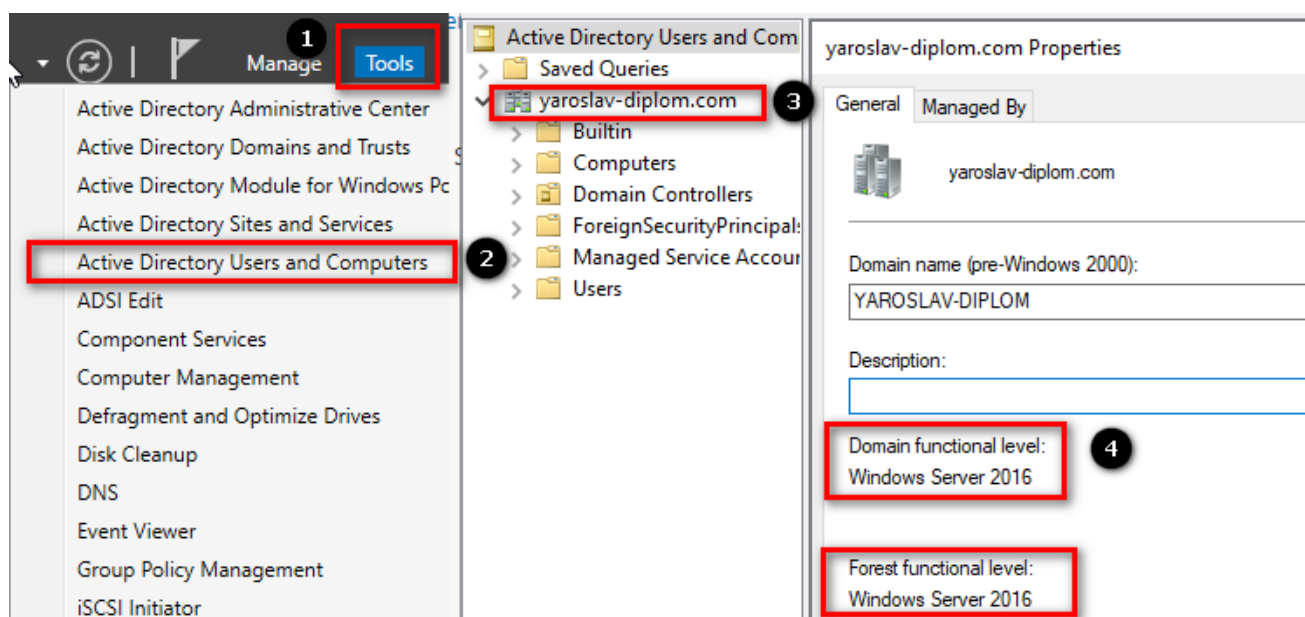


Рисунок 2.7 – Процес перевірки після інсталювання

Після успішного налаштування DNS на Windows Server, можемо приступити до інсталювання та налаштування Linux системи як клієнта Kerberos. Це дозволить отримати доступ до будь-яких служб, як тільки користувач успішно увійде в систему.

Підготовка учасника до приєднання до домену Active Directory. Нажаль, одного лише протоколу недостатньо для того, щоб Linux користувач існував у системі Windows. Kerberos забезпечує лише аутентифікацію: він не знає про групи користувачів, домашні каталоги і т. ін.

Зазвичай для цих налаштувань використовується Samba – стандартний набір програм сумісності Windows для Linux та Unix систем. Проте, в деяких випадках застосовують System Security Services Daemon (SSSD), каталог-клієнтський компонент Linux. Samba - це безкоштовне програмне забезпечення, ліцензоване за загальною публічною ліцензією GNU, проект Samba є членом організації Software Freedom Conservancy.

Samba є важливим компонентом для плавної інтеграції серверів Linux / Unix та робочих столів у середовища Active Directory, що може функціонувати як і контролер домену, так і як звичайний член домену. [22]

Active Directory (AD) використовує DNS у фоновому режимі для пошуку інших Domain Controller (DC) і служб, таких як Kerberos. Таким чином, члени домену AD та сервери повинні мати можливість досягати зони AD DNS.

Далі налаштовуємо IP-адресацію на відповідному інтерфейсі, оскільки встановлена Ubuntu-Desktop, це робиться через налаштування. В графі «DNS» вказуємо IP-адресу нашого DC.

Перш за все, внесемо зміни в файл /etc/hosts/ на Linux клієнті для задання пріоритету пошуку домену, як показано на наступному рисунку.

```
GNU nano 4.8 /etc/hosts Modified
127.0.0.1 localhost
127.0.1.1 userprincipalVB
192.168.0.1 win-03ta7c16rur win-03ta7c16rur.yaroslav-diplom.com
# The following lines are desirable for IPv6 capable hosts
```

Рисунок 2.8 – Внесення змін в файл /etc/hosts/

Тепер необхідно перевірити зв'язок с сервером, використовуючи команду ping та вказавши Fully Qualified Domain Names (FQDN), аби достовірно переконатися в правильності введених даних та наявності зв'язку.

```
userprincipal@userprincipalVB:~$ ping win-03ta7c16rur.yaroslav-diplom.com
PING win-03ta7c16rur (192.168.0.1) 56(84) bytes of data:
64 bytes from win-03ta7c16rur (192.168.0.1): icmp_seq=1 ttl=128 time=1.60 ms
64 bytes from win-03ta7c16rur (192.168.0.1): icmp_seq=2 ttl=128 time=0.927 ms
^C
--- win-03ta7c16rur ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.927/1.262/1.598/0.335 ms
```

Рисунок 2.9 – Результат виконання команди ping до FQDN

Нашалтування Kerberos. Створюємо та налаштовуємо новий конфігураційний файл за замовчуванням; деталі на наступному рисунку.

```
userprincipal@userprincipalVB:~$ sudo mv /etc/krb5.conf /etc/krb5.conf.default
userprincipal@userprincipalVB:~$ sudo nano /etc/krb5.conf
GNU nano 4.8 /etc/krb5.conf

[libdefaults]
default_realm = YAROSLAV-DIPLOM.COM
dns_lookup_kdc = true
dns_lookup_realm = false
```

Рисунок 2.10 – Вікно конфігурування KERBEROS аутентифікації

Наступним кроком необхідно налаштувати синхронізацію часу, адже Kerberos вимагає синхронізованого часу для всіх членів домену. Тому рекомендується налаштувати клієнт NTP.

Використовуючи ntpd демон, котрий зчитує конфігурацію з файлу /etc/ntp.conf, нашілюємо базові параметри синхронізації годинників з відповідними серверами(див. рис. 2.11). Знайти необхідні пули серверів України для зв'язки часу можна за посиланням: <https://www.pool.ntp.org/zone/ua>.

При використанні Unix у віртуальній машині, слід зазначити tinker panic 0 у кінці файлу ntp.conf. Це рекомендується, оскільки віртуальні машини не мають фізичного годинника, тому вони можуть будь-коли призупинити роботу та запуснитися через кілька годин.

```
userprincipal@userprincipalVB:~$ sudo nano /etc/ntp.conf
GNU nano 4.8 /etc/ntp.conf Modified
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
server 0.ua.pool.ntp.org
server 1.ua.pool.ntp.org
server 2.ua.pool.ntp.org
server 3.ua.pool.ntp.org

tinker panic 0

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
^X Exit          ^R Read File    ^\ Replace      ^U Paste Text   ^T To Spell
```

Рисунок 2.11 – Встановлення пулів серверів для синхронізації часу

Тепер, для розгортання Kerberos на клієнті, необхідно інсталиювати пакет, що називається krb5-user.

```
userprincipal@userprincipalVB:~$ sudo apt install krb5-user
userprincipal@userprincipalVB:~$ sudo apt install krb5-user
Reading package lists... Done
Building dependency tree
Reading state information... Done
krb5-user is already the newest version (1.17-6ubuntu4.1).
```

Рисунок 2.12 – Встановлення необхідного пакету

Якщо звернутися до AD компоненту «Користувачі та пристрої», то стане зрозуміло що наразі не відбувається відображення Linux клієнта у домені.

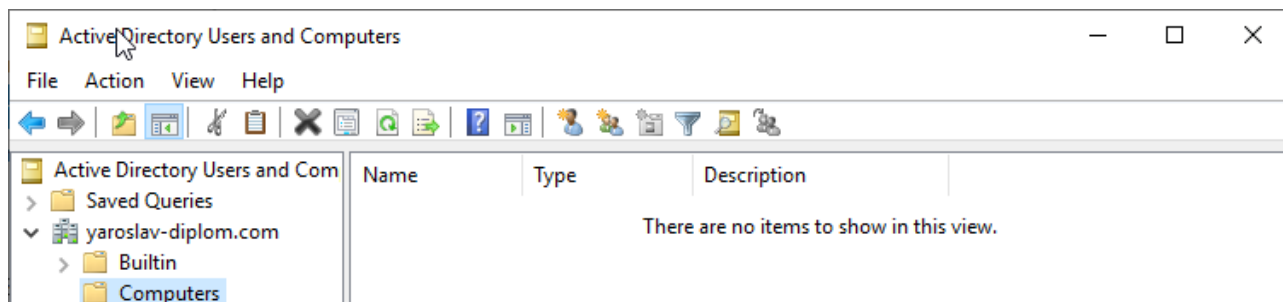


Рисунок 2.13 – Огляд компонентів служби директорії

Саме тому варто скористатися будь-яким обліковим записом з Unix хоста, застосувавши команду `kinit`, для отримання належного TGT, наявність якого можна перевірити командою `klist`. Утиліті `kinit` не потрібно, аби принципал існував як локальний користувач у системі. Якщо суб'єкта не зазначено, тоді інструмент використовуватиме ім'я користувача який ініціалізував `kinit`.

```
userprincipal@userprincipalVB:~$ kinit user1
Password for user1@YAROSLAV-DIPLOM.COM:
userprincipal@userprincipalVB:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: user1@YAROSLAV-DIPLOM.COM

Valid starting    Expires          Service principal
20.06.21 14:02:45  21.06.21 00:02:45  krbtgt/YAROSLAV-DIPLOM.COM@YAROSLAV-DIPLOM.COM
renew until 21.06.21 14:02:40
```

Рисунок 2.14 – Процес входу до облікового запису домену та отримання відповідного квитка

Наразі необхідно скористатися службою `winbind`, що працює на клієнтах Samba і діє як проксі для зв'язку між відповідними модулями, що працюють на комп'ютері Linux, з одного боку, і Active Directory, що працює на контролері домену, з іншого. Зокрема, Winbind використовує Kerberos для перевірки автентичності за допомогою AD і LDAP для отримання інформації про користувачів і групи. Для цього заповнимо конфігураційний файл пакету Samba необхідними полями, як зображено на наступному рисунку.[30]

```

userprincipal@userprincipalVB:~$ sudo apt install winbind
Reading package lists... Done
Building dependency tree
Reading state information... Done
winbind is already the newest version (2:4.11.6+dfsg-0ubuntu1.9).
userprincipal@userprincipalVB:~$ sudo nano /etc/samba/smb.conf

#===== Global Settings =====

[global]
workgroup = YAROSLAV-DIPLOM
security = ADS
realm = YAROSLAV-DIPLOM.COM
kerberos method = system keytab
winbind use default domain = Yes

```

Рисунок 2.15 – Встановлення демону winbind та задання необхідних параметрів

Нарешті можна провести реєстрацію користувача у контролері домену, одним із способів буде використання мережевої утиліти Samba, а саме вводу команди, яка зазначена на рисунку 2.16.

```

userprincipal@userprincipalVB:~$ sudo net ads join -U Administrator
Enter Administrator's password:
Using short domain name -- YAROSLAV-DIPLOM
Joined 'USERPRINCIPALVB' to dns domain 'yaroslav-diplom.com'
userprincipal@userprincipalVB:~$

```

Рисунок 2.16 – Виконання команди net ads join

Тепер Linux система відображається у відповідних списках AD та DNS на домені Windows Server. Хоча, навідміну від http, imap, xmpp сервісів, реєстрація принципалів при використанні winbind у мережі – є необов'язковим пунктом.

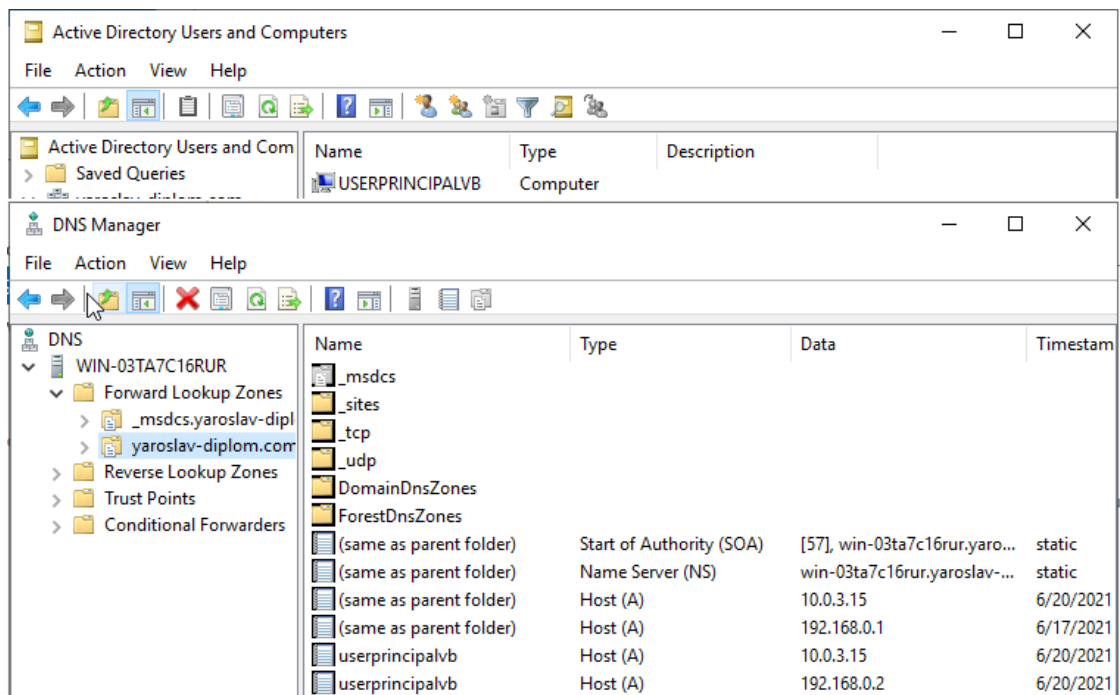


Рисунок 2.17 – Відображення наявності клієнтів у домені

Зробимо декілька аналогічних перевірок виконаних налаштувань на самій Unix машині. Спершу, наявність зв'язку з контролером домену, далі переконатися, що машина знаходиться у DNS та перезавантажити сервіс winbind. Тепер маємо можливість відобразити список усіх існуючих користувачів домену. Усі вищезазначені дії показано на наступному рисунку.

```
userprincipal@userprincipalVB:~$ sudo net ads testjoin
Join is OK
userprincipal@userprincipalVB:~$ sudo host userprincipalVB
userprincipalVB has address 192.168.0.2
userprincipal@userprincipalVB:~$ service winbind restart
userprincipal@userprincipalVB:~$ wbinform -u
administrator
guest
krbtgt
user1
```

Рисунок 2.18 – Виконання діагностичних команд

Як можна помітити, у списку присутній незвичний користувач krbtgt. AD використовує обліковий запис KRBtgt у домені для квитків Kerberos. Обліковий запис KRBtgt – це локальний обліковий запис за замовчуванням, який діє як аккаунт надання послуги для служби розподілу ключів (KDC). Його не можна видалити, а також назву запису не можна змінити. Він наявний у середовищі Active Directory з моменту його першого введення. Кожен домен AD має пов'язаний обліковий запис KRBtgt, який використовується для шифрування та підписання всіх квитків Kerberos для цього домену, завдяки якому всі контрольовані доменні контролери знають пароль облікового запису, щоб розшифрувати квитки Kerberos для перевірки.

Вихід Unix системи із домену в режимі Active Directory Security Mode (ADS) можна здійснити за допомогою команди net ads leave – U [username] та видалення таблиці ключів rm /etc/krb5.keytab.

Тепер поговоримо про аутентифікацію в режимі ADS/DOMAIN. Виконавши команду id user1, стане ясно, що даний суб'єкт існує лише на домені.

```
userprincipal@userprincipalVB:~$ id user1
id: 'user1': no such user
```

Рисунок 2.19 – Виконання команди id, задля перевірки Linux-атрибутів

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		
					47	

Справа в тому, що у користувачів фізичних Unix машин мають бути Linux-атрибути, типу userID, groupID, shell і т.п., які відсутні також і на DC (у Windows версії). Для усунення цієї проблеми можна прописати атрибути вручну, але можливий і інший варіант вирішення задачі, наприклад, використовуючи сервіс winbind. А саме, доповнивши конфігураційний файл директивами, як зображено на рисунку 2.20. Вкажемо, що необхідно завантажувати інформацію про користувачів, групи, встановимо значення часу (в секундах) кешування демоном цієї інформації. Задамо інтервал призначуваних ідентифікаторів на стороні фізичної машини, шаблон імені домашніх каталогів користувачів та визначимо параметри, які будуть використовуватись у командному інтерпретаторі. Однак на файловому сервері, на відміну від користувацької станції, краще буде вказати /usr/sbin/nologin для template shell, щоб унеможливити підключення до машини по ssh, або через консоль. Після збереження налаштувань, необхідно перезавантажити winbind.

```
GNU nano 4.8 /etc/samba/smb.conf
[global]
    workgroup = YAROSLAV-DIPLOM
    security = ADS
    realm = YAROSLAV-DIPLOM.com
    kerberos method = system keytab
    winbind use default domain = Yes

    winbind expand groups = 1
    winbind enum users = yes
    winbind enum groups = yes
    winbind cache time = 36
    #idmap config * : range = 3000-7999
    #idmap config YAROSLAV-DIPLOM : backend = ad
    idmap config YAROSLAV-DIPLOM : range = 10000-20000
    template homedir = /home/%U
    template shell = /bin/bash
```

Рисунок 2.20 – Внесення змін до конфігураційного файлу smb.conf

Як було зазначено вище, на AD DC відсутні атрибути для Linux користувачів, проте для кожного з них наявний унікальний Security ID (SID). Завдяки попереднім діям, зі зміною конфігурацій, у нас з'явилась можливість визначити ID користувача за цим ідентифікатором, командою, виконання якої зображено на наступному рисунку.

```

userprincipal@userprincipalVB:~$ wbinfo --ping-dc
checking the NETLOGON for domain[YAROSLAV-DIPLOM] dc connection to "WIN-03TA7C1
6RUR.yaroslav-diplom.com" succeeded
userprincipal@userprincipalVB:~$ wbinfo -n user1
S-1-5-21-192730637-3344049542-2382873173-1105 SID_USER (1)
userprincipal@userprincipalVB:~$ wbinfo -n user2
S-1-5-21-192730637-3344049542-2382873173-1109 SID_USER (1)
userprincipal@userprincipalVB:~$ wbinfo -S `wbinfo -n user1|cut -d' ' -f1`
10000
userprincipal@userprincipalVB:~$ wbinfo -S `wbinfo -n user2|cut -d' ' -f1`
10001
userprincipal@userprincipalVB:~$ wbinfo -i user1
user1:*:10000:10000:~/home/user1:/bin/bash
userprincipal@userprincipalVB:~$ wbinfo -i user2
user2:*:10001:10000:~/home/user2:/bin/bash

```

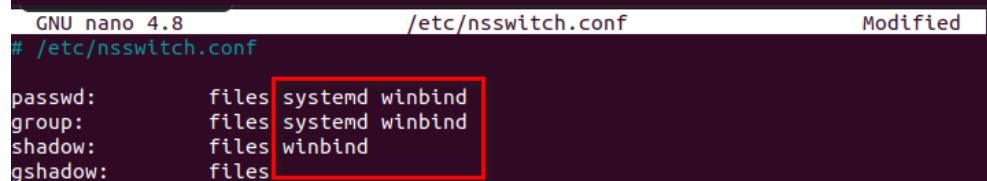
Рисунок 2.21 – Визначення атрибутів Linux за SID користувача

Проте, ми лише зробили доступними користувачів через сервіс winbind, Linux клієнту ж нічого не відомо про даних суб'єктів, тому варто виправити це, модифікувавши систему управління користувачами, як показано на наступному рисунку.

```

userprincipal@userprincipalVB:~$ id user1
id: 'user1': no such user
userprincipal@userprincipalVB:~$ id user2
id: 'user2': no such user
userprincipal@userprincipalVB:~$ sudo apt install libnss-winbind

```



```

GNU nano 4.8 /etc/nsswitch.conf Modified
# /etc/nsswitch.conf

passwd:    files systemd winbind
group:     files systemd winbind
shadow:    files winbind
gshadow:   files

userprincipal@userprincipalVB:~$ id user1
uid=10000(user1) gid=10000(domain users) groups=10000(domain users)
userprincipal@userprincipalVB:~$ id user2
uid=10001(user2) gid=10000(domain users) groups=10000(domain users)

```

Рисунок 2.22 – Редагування файлу зчитування інформації про користувачів

Тепер отримавши атрибути для користувачів, можемо спробувати зайти до облікового запису, використовуючи пароль з AD для існуючого користувача user3. Вхід здійснений через консольний інтерфейс, для зручної демонстрації.

```

Ubuntu 20.04.2 LTS userprincipalVB tty3
userprincipalVB login: user3
Password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be applied immediately.

```

Рисунок 2.23 – Процес входу до облікового запису, який знаходиться на домені

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		
					49	

Створення файлового серверу Samba. Для коректного функціонування відповідного серверу, перш за все необхідно виконати аналогічні налаштування, як і для звичайного Linux клієнта. Якщо все зроблено правильно, FileServerPrincipal відобразиться як в AD, так і в DNS (рис. 2.24).

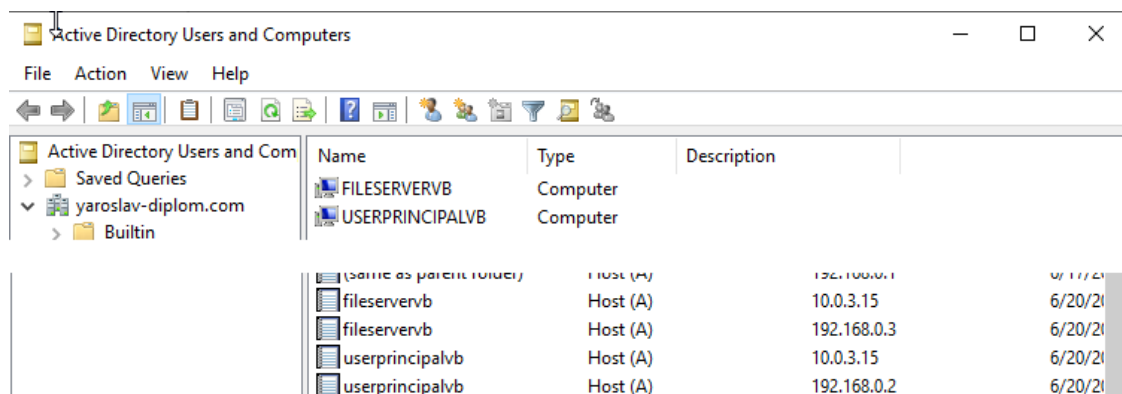


Рисунок 2.24 – Відображення відповідних користувачам записів у AD

Наступним кроком буде встановлення файлового сервісу Samba. Також створимо пустий каталог для розміщення сумісного файлового ресурсу та надамо доступ Linux користувачу, що знаходиться в системі за замовчуванням.

```
fileserver@fileserverVB:~$ sudo apt install samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
samba is already the newest version (2:4.11.6+dfsg-0ubuntu1.9).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
fileserver@fileserverVB:~$ sudo mkdir -p /disk1/samba && sudo chown games /disk1/samba
```

Рисунок 2.25 – Процес встановлення файлового серверу Samba

Тепер перейдемо безпосередньо до налаштування конфігурацій сервера. Задамо загальний файловий ресурс та зазначимо для нього наступні поля: шлях, групу користувачів які будуть мати належний доступ, обмеження на читання та запис, доступ через користувача.

```
GNU nano 4.8 /etc/samba/smb.conf Modified
[corp_share]
    path = /disk1/samba
    valid users = @YAROSLAV-DIPLOM\\group1
    read only = no
    force user = games
```

Рисунок 2.26 – Надання доступу до сервісів серверу

Наразі все, тепер можемо спробувати підключитися до створеного каталогу з робочої станції. Отримавши TGT користувача, є можливість звернутись до сервісу. Використаємо GUI для демонстрації (див. рис. 2.27).

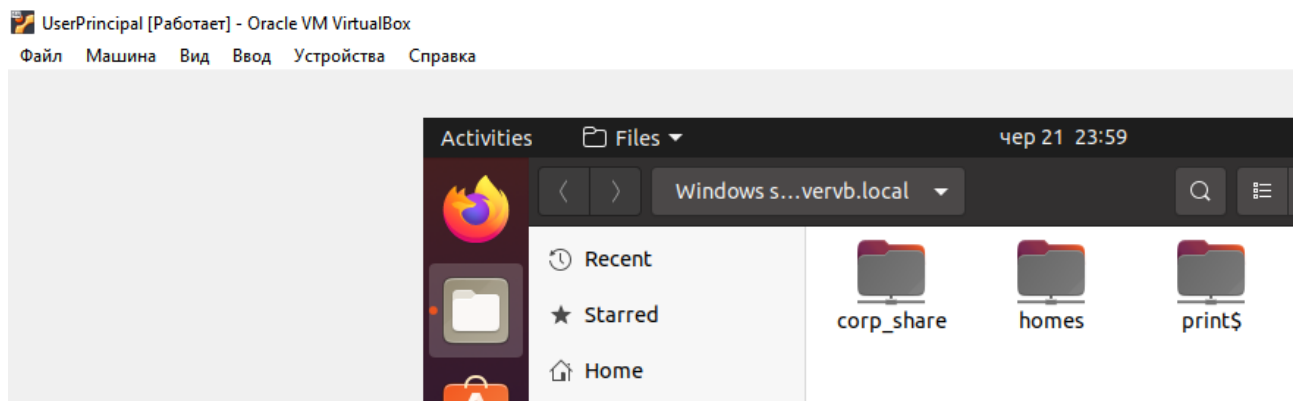


Рисунок 2.27 – Успішне підключення до ресурсів файлового сервера

Хоча Kerberos застерігає від загальних та поширених загроз, його доволі важко реалізувати з наступних причин:

- Kerberos передбачає, що кожен користувач є довіреним суб'єктом, проте використовує ненадійний хост у ненадійній мережі. Його основна мета полягає в тому, щоб запобігти передачі незахищених паролів у цій мережі. Однак, якщо хтось, окрім користувача, має доступ до KDC який видає TGT – суцільна система аутентифікації Kerberos знаходяться під загрозою.

- Аби забезпечити захист мережі з Kerberos, необхідно або використовувати лише довірені клієнт-серверні додатки, яким відомий даний протокол, або взагалі не використовувати його.

2.3 Проведення дослідження стосовно можливих типів атак на протокол Kerberos

Не існує такого заходу безпеки який був би на 100% неприступний, і Kerberos не є винятком. Оскільки даний протокол існує більше 25 років, за цей проміжок часу хакери мали можливість знаходити безліч шляхів обходу заходів безпеки, як правило, за допомогою підробки квитків, використання грубої сили (підбору паролей), а також використання шкідливих програм для зниження шифрування.[9]

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		51

Незважаючи на це, Kerberos все ще є одним із найкращих способів аутентифікації SSO технології. Протокол є достатньо гнучким, щоб використовувати більш надійні алгоритми шифрування, бути спроможним боротися з новими загрозами, при умові що користувачі практикують хороші політики вибору пароля. [2]

Клієнтам можна заборонити аутентифікацію за допомогою механізмів, які використовує Kerberos для запобігання атакам "повторного відтворення". Під час атаки зловмисний користувач захоплює мережевий трафік і повторює його, щоб обдурити сервер аутентифікації, аби той прийняв зловмисника як довіреного суб'єкта, який надає облікові дані.

Аутентифікація Kerberos запобігає повторній атаці за допомогою двох механізмів:

- Клієнт Kerberos на локальному комп'ютері шифрує позначку часу всередині аутентифікатора, а потім відправляє її до центру розподілу ключів (KDC). Коли KDC перевірить час, який він розшифровує з посилання, на знаходження його в межах визначеного проміжку (за замовчуванням - п'ять хвилин), система може припустити, що представлені облікові дані справжні.

- Усі квитки, видані KDC, мають термін дії. Таким чином, якщо квиток порушено, його не можна використовувати поза визначеним часовим діапазоном, як правило – досить коротким, щоб мінімізувати ризик повторної атаки.

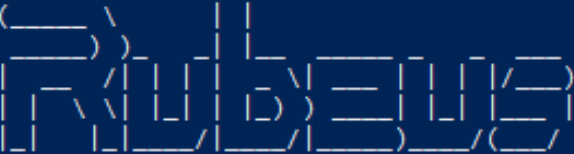
Через ці механізми аутентифікація Kerberos покладається на дату та час, встановлені на KDC та клієнті. Якщо між ними є занадто велика різниця, KDC не може визначити, чи є запит законним. Тому життєво важливо синхронізувати час на всіх комп'ютерах мережі, щоб аутентифікація могла нормально функціонувати. Перекіс годинника можна легко діагностувати, переглянувши інформацію в системному журналі.

Розбір атак на Kerberos за допомогою Rubeus. Даний інструмент сумісний з C # версії 3.0 (.NET 3.5), призначений для проведення атак на компоненти

					KIK.KB.B-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		52

Kerberos на рівні трафіку і хоста. Може успішно працювати як і з зовнішньої машини, так і всередині доменної мережі (клієнтського доменного хоста).

```
PS C:\Users\vtsonpanakis\Desktop> .\Rubeus.exe monitor /interval:5
```



v1.5.0

```
[*] Action: TGT Monitoring  
[*] Monitoring every 5 seconds for new TGTS  
  
[*] 3/11/2020 3:27:47 PM UTC - Found new TGT:
```

Рисунок 2.28 – Вигляд робочої області додатку Rubeus

За допомогою даного інструменту можна реалізувати наступні атаки:

- Kerberos User Enumeration and Brute Force;
- Kerberoast;
- AS-REP Roasting;
- Silver Ticket;
- Golden Ticket;
- Overpass The Hash/Pass The Key (PTK);
- Pass-The-Ticket / Ticket Dump;
- Unconstrained Delegation;
- Constrained Delegation;

Kerberos brute-force. Завдяки тому, що Kerberos є протоколом аутентифікації, на нього можна проводити атаки методом перебору імен користувачів і відповідних паролів, але тут потрібно бути обережним, так як «брут» може заблокувати облікові записи користувачів. Нижче наведено список застосунків, окрім Rubeus, якими можна здійснити атаку на порт 88, який використовується Kerberos, для переліку дійсних імен користувачів та паролів:

- Metasploit;
- Nmap;
- Kerbrute.

В результаті даного методу отримуються існуючі користувачі та паролі, так само, як і TGT, що зберігаються на локальній файловій системі. Надалі розглянуто більш просунуті техніки атак на протокол Kerberos.

Kerberoasting – це техніка, яка дозволяє зловмиснику викрасти квиток Ticket Grant Service (TGS), який зашифрований за допомогою RC4, для грубого перебору хешу служб додатків для вилучення свого пароля.

При надсиланні запиту на отримання квитка TGS контролеру домену KDC для будь-якої служби, яка зареєструвала SPN, KDC генерує TGS, не ідентифікуючи авторизацію користувача щодо запитуваної послуги.

Зловмисник може використовувати цей квиток в автономному режимі, щоб грубо примусити ввести пароль для службового облікового запису.

ASREPRoasting – агресивна техніка проти Kerberos, яка дозволяє отримувати хеші паролів для користувачів, які не потребують попередньої перевірки автентичності. У такому випадку зловмисник може відновити Kerberos AS-REP, зашифрований паролем користувача RC4-HMAC, і він може спробувати зламати цей квиток в автономному режимі, отримавши AS-REP хеш, розшифрувавши який, отримується пароль користувача.

Golden ticket в Active Directory надає носіям необмежений доступ. Безпека протоколу Kerberos базується на використанні спільних секретів для шифрування та підписання повідомлень. Деякі з цих ключів відомі стороні, якій довіряють (KDC) та клієнтам, але одна, зокрема, відома лише KDC: secret key для користувача krbtgt, чий хеш пароля використовується для підписати або шифрування квитків Kerberos, видані KDC. Іншими словами, компрометація хешу krbtgt дозволяє хакеру поводитися так, ніби він і є AD доменом.

Як тільки супротивник скомпрометує хеш krbtgt, він має «золотий квиток». Використовуючи його, можливо підробляти квитки Kerberos, наприклад: видавати квитки для користувачів, які не існують, додавати користувачів до груп, до яких вони не належать, або видавати квитки, термін служби яких значно перевищує налаштований максимум. Фактично,

					КІК.КБ.Б-125-06-ПЗ	54
Зм	Арк.	№ документа	Підпис	Дата		

супротивником є AD і він може отримати доступ до будь-якого вибраного ним ресурсу. Ця можливість є надзвичайно потужною і важкою для виявлення.

Silver ticket attack. Подібно за концепцією до «золотого квитка», атака передбачає компрометацію облікових даних та зловживання архітектурою протоколу Kerberos. Однак, на відміну від Golden ticket attack, який надає супротивнику необмежений доступ до домену, Silver ticket attack дозволяє зловмисникові лише підробляти TGS. Дані квитки зашифровані хешем пароля, отже, якщо суперник викраде хеш для облікового запису служби, він може створювати подібні TGS для сервісу послуг.

Незважаючи на те, що сфера застосування даного квитка може бути меншою за подібну атаку, вона все ще є потужним інструментом у наборі супротивника, що забезпечує постійний та прихований доступ до ресурсів. Оскільки потрібен лише хеш пароля службового облікового запису, його також набагато простіше виконати, ніж «золотий квиток».

Overpass The Hash/Pass The Key (PTK). Ця атака спрямована на використання NTLM хешу користувача для запиту квитків Kerberos, як альтернативу загальному протоколу Pass The Hash over NTLM. Тому це може бути особливо корисним у мережах, де протокол NTLM відключений, і лише Kerberos дозволений як протокол аутентифікації. Для здійснення цієї атаки необхідний хеш (або пароль) NTLM цільового облікового запису користувача. Таким чином, як тільки хеш користувача отриманий, може бути надісланий запит на TGT для цього облікового запису. Нарешті, можна отримати доступ до будь-якої служби або машини, на яку обліковий запис користувача має дозволи.

Pass The Ticket (PTT). Дана атака схожа на Overpass-the-hash / Pass-the-key, атакуючий намагається отримати квиток доменного користувача (бажано того, хто має максимальні привілеї в домені) і завантажити його в поточну сесію. Один із способів отримання TGT квитків - дамп квитків локально, на поточній доменній машині. Rubeus може вивантажити квитки, що зберігаються в lsass директиві, за допомогою дії «dump», а «triage» покаже, які квитки зберігаються в системі на даний момент.

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			55

Unconstrained Delegation (необмежену делегування) – це привілея в домені, яка може бути надана обліковим записам користувачів або комп'ютерів. Вона дозволяє проходити перевірку автентичності на сервісі в мережі від імені іншого облікового запису. Один з етапів проведення тестування безпеки домену Active Directory - пошук облікових записів з включеним делегуванням, зазвичай для цих цілей використовують Powerview утиліту, але можна і вручну, використовуючи стандартний модуль AD.

Constrained Delegation. Якщо зломисникові вдалося скомпрометувати обліковий запис користувача або комп'ютера, для якого включено обмежене делегування, то він може видати себе за будь-якого користувача домену та виконати аутентифікацію в службі, до якої дозволено делегування.[9]

Отже, в другому розділі було проведено розробку підсистеми аутентифікації користувачів з використанням Windows Server2019 у якості контролера домену, та Linux хостів для налаштування клієнтів у середовищі розробки GNS3. Крім того, здійснений перелік та опис атак на протокол, за допомогою іструменту Rubeus. Проте, незважаючи на переваги використання Kerberos для автентифікації, варто зазначити, що як і у решти подібних протоколів, за немалий час існування вдалося виявити значну частину вразливостей. Враховуючи ці дані, необхідно розумітись на захисті слабких місць безпеки протоколу Kerberos та в системах яких він найчастіше використовується. Про це і буде зазначено в наступному розділі роботи.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАХИСТУ ВІДНОСНО ДОМЕННОЇ СЛУЖБИ ACTIVE DIRECTORY

3.1 Обстеження та аналіз проходження трафіку в мережі Kerberos за допомогою програмного додатку Wireshark

В даному розділі буде здійснено опис мережевого трафіку Kerberos, перехопленого під час входу користувача в домен, на прикладі Windows Server.

Оскільки даний протокол, в основному, є незашифрованим, за винятком квитків, аутентифікаторів та деяких інших деталей, які покладаються на шифрування повідомлень та полів. Це полегшує дослідження пакетів Kerberos за допомогою інструменту Wireshark. [25]

Нижче наведено зведення послідовності повідомлень при здійсненні аутентифікації(рис.3.1):

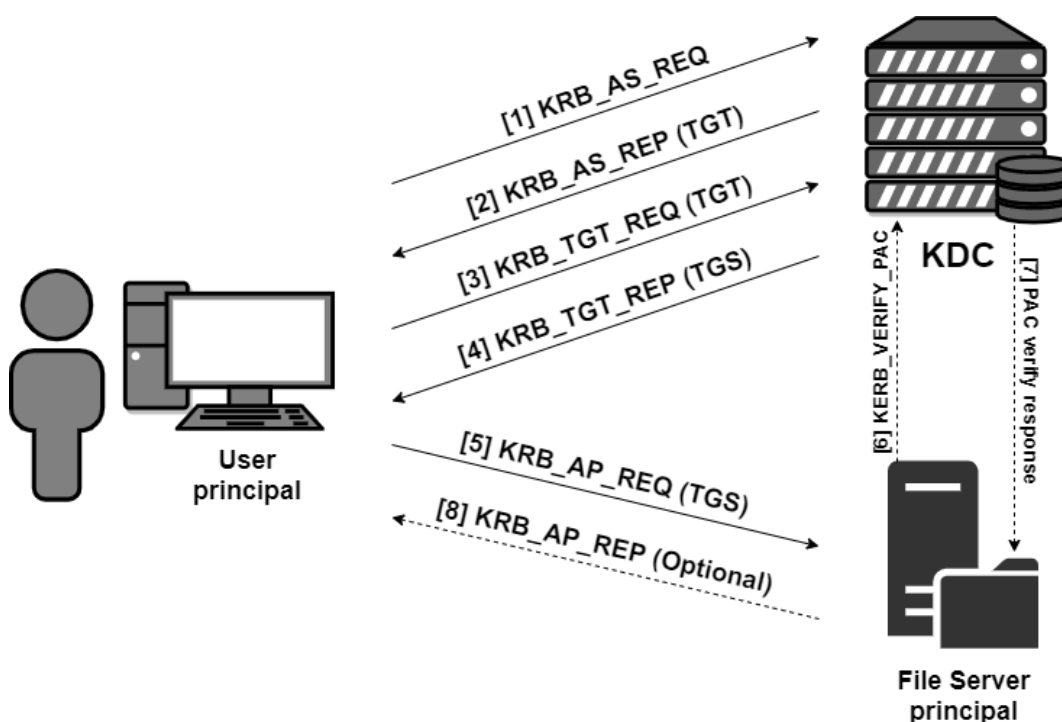


Рисунок 3.1 – Послідовність встановлення з'єднання по протоколу Kerberos

Вхід користувача домену. На рисунку 3.2 показано початкове з'єднання TCP між приєднаним до домену RCBJ (його DNS ім'я - rcbj.net) сервером Windows та DC коли користувач "RCBJ \ rcbj" намагався увійти через Remote Desktop Protocol (RDP).

Обмін службами аутентифікації. Перші три пакети є типовим SYN-SYNACK-ACK рукостисканням (handshake), яке відбувається при будь-якому TCP-з'єднанні.

	Time	Source	Destination	Protocol	Length	Info
147	3.358737	172.31.40.187	172.31.41.127	TCP	66	49953 → 88 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=8961 WS=256
148	3.358807	172.31.41.127	172.31.40.187	TCP	66	88 → 49953 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=8961
149	3.359115	172.31.40.187	172.31.41.127	TCP	54	49953 → 88 [ACK] Seq=1 Ack=1 Win=573440 Len=0
150	3.359159	172.31.40.187	172.31.41.127	KRB5	266	AS-REQ
151	3.360964	172.31.41.127	172.31.40.187	KRB5	222	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
152	3.361374	172.31.40.187	172.31.41.127	TCP	54	49953 → 88 [FIN, ACK] Seq=213 Ack=169 Win=573184 Len=0
153	3.361391	172.31.41.127	172.31.40.187	TCP	54	88 → 49953 [ACK] Seq=169 Ack=214 Win=573440 Len=0
154	3.361428	172.31.41.127	172.31.40.187	TCP	54	88 → 49953 [RST, ACK] Seq=169 Ack=214 Win=0 Len=0

Рисунок 3.2 – Вигляд початкового з'єднання між сервером та контролером

Четвертим пакетом, який надсилається із сервера Windows (клієнта) на KDC, є повідомлення AS-REQ (це тип повідомлення KRB_KDC_REQ). Повідомлення AS-REQ виглядає наступним чином(рис.3.3):

```

Kerberos
  > Record Mark: 208 bytes
  as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padata: 1 item
      PA-DATA PA-PAC-REQUEST
        padata-type: KRB5-PADATA-PA-PAC-REQUEST (128)
        padata-value: 3005a0030101ff
    req-body
      Padding: 0
      kdc-options: 40810010 (forwardable, renewable, canonicalize, renewable-ok)
      cname
        name-type: KRB5-NT-PRINCIPAL (1)
        cname-string: 1 item
          CNameString: rcbj
      realm: RCBJ
      sname
        name-type: KRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: krbtgt
          SNameString: RCBJ
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 2137798680
  
```

Рисунок 3.3 – Зміст повідомлення запиту до KDC

Служба аутентифікації потребує наявності даних попередньої аутентифікації (pre-authentication data). Отже, вона повертає таку помилку Kerberos:

```

  ▾ Kerberos
    > Record Mark: 164 bytes
    ▾ krb-error
      pyno: 5
      msg-type: krb-error (30)
      stime: 2018-05-01 16:57:31 (UTC)
      susec: 100523
      error-code: eRR-PREAUTH-REQUIRED (25)
      realm: RCBJ
    ▾ sname
      name-type: KRB5-NT-SRV-INST (2)
      ▾ sname-string: 2 items
        SNameString: krbtgt
        SNameString: RCBJ
    > e-data: 304c3029a103020113a2220420301e3015a003020112a10e...

```

Рисунок 3.4 – Зміст повідомлення протоколу Kerberos про помилку

Повідомлення про помилки Kerberos визначено у RFC 4120. На цьому етапі з'єднання TCP закрито. На рисунку 3.5 можна спостерігати пакети FIN, ACK та RST (скидання), які є частиною стандартного припинення з'єднання.

Використовуючи секретний ключ користувача, отриманий із пароля Windows, клієнт шифрує поточну мітку часу та використовує її для заповнення даних попередньої аутентифікації повідомленням KRB5-PADATA-ENC-TIMESTAMP у запиті.

152	3.361374	172.31.40.187	172.31.41.127	TCP	54 49953 → 88 [FIN, ACK] Seq=213 Ack=169 Win=573184 Len=0
153	3.361391	172.31.41.127	172.31.40.187	TCP	54 88 → 49953 [ACK] Seq=169 Ack=214 Win=573440 Len=0
154	3.361428	172.31.41.127	172.31.40.187	TCP	54 88 → 49953 [RST, ACK] Seq=169 Ack=214 Win=0 Len=0

Рисунок 3.5 – Відображення закриття TCP сесії

Встановлено новий зв'язок. Нове повідомлення AS-REQ надсилається Службі аутентифікації KDC. По суті, відбувається те саме звернення, яке було надіслано вперше, проте тепер заповнені дані попередньої аутентифікації.

Після обробки запиту служба аутентифікації повертає KRB_AS_REP клієнту (робочій станції). Це виглядає наступним чином(рис.3.6):

```

  ▾ Kerberos
    > Record Mark: 1503 bytes
    ▾ as-rep
      pvno: 5
      msg-type: krb-as-rep (11)
      ▾ padata: 1 item
        ▾ PA-DATA PA-ENCTYPE-INFO2
          ▾ padata-type: kRB5-PADATA-ETYPE-INFO2 (19)
            > padata-value: 30173015a003020112a10e1b0c5243424a2e4e4554726362...
          crealm: RCBJ.NET
        ▾ cname
          name-type: kRB5-NT-PRINCIPAL (1)
          ▾ cname-string: 1 item
            CNameString: rcbj
      ▾ ticket
        tkt-vno: 5
        realm: RCBJ.NET
        ▾ sname
          name-type: kRB5-NT-SRV-INST (2)
          ▾ sname-string: 2 items
            SNameString: krbtgt
            SNameString: RCBJ.NET
        ▾ enc-part
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          kvno: 2
          cipher: 5dbdeb506c29e737cad64273964c1ae597bde3a886ca1565...
      ▾ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 3
        cipher: 336a56f643b3768488f8e7a5044fb57281b97bef6bdc060b...

```

Рисунок 3.6 – Відповідь DC на запит клієнта

Ці поля даних представляють собою «message 1», яке зашифроване секретним ключем користувача, отриманим із пароля та «message 2», що містить TGT. Крім того, присутні деякі метадані у даному запиті.

Отже, на даний момент у клієнта є сеансовий ключ, який він розшифрував за допомогою секретного ключа користувача та TGT (який містить той самий session key, серед іншого зашифрований за допомогою TGS secret key). На наступному кроці в квитку буде присутній доступ до сеансового ключа між клієнтом та TGS.

Далі клієнт (робоча станція) встановлює нове підключення до програмного інтерфейсу і надсилає повідомлення TGS-REQ, яке виглядає наступним чином(рис.3.7):

```

  tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    padata: 2 items
      PA-DATA PA-TGS-REQ
        padata-type: kRB5-PADATA-TGS-REQ (1)
        padata-value: 6e8204d9308204d5a003020105a10302010ea20703050000...
          ap-req
            pvno: 5
            msg-type: krb-ap-req (14)
            Padding: 0
            > ap-options: 00000000
            ticket
              tkt-vno: 5
              realm: RCBJ.NET
              sname
                name-type: kRB5-NT-SRV-INST (2)
                sname-string: 2 items
                  SNameString: krbtgt
                  SNameString: RCBJ.NET
              enc-part
                -----
                authenticator
                  PA-DATA Unknown:167
                  padata-type: Unknown (167)
                  padata-value: 3009a00703050040000000
            req-body
              Padding: 0
              > kdc-options: 40810000 (forwardable, renewable, canonicalize)
              realm: RCBJ.NET
              sname
                name-type: kRB5-NT-SRV-HST (3)
                sname-string: 2 items
                  SNameString: host
                  SNameString: ec2amaz-danl2uj.rcbj.net
              till: 2037-09-13 02:48:05 (UTC)
              nonce: 1525504810
              etype: 5 items
                ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)

```

Рисунок 3.7 – Вигляд TGS-REQ повідомлення

Структура даного запиту TGT-REQ подібна до AS-REQ, яке ми розглядали раніше, і це має сенс, враховуючи, що обидва ці повідомлення мають загальне визначення KRB_KDC_REQ (RFC 4120, розділ 5.4.1). Однак багато з цих полів є необов'язковими і відсутні тут. RFC4120 зазначає наступне:

Клієнт готує повідомлення KRB_TGS_REQ, надаючи заголовок аутентифікації як елемент поля, що відповідає за попередню аутентифікацію, і включаючи ті самі поля, що використовуються в повідомленні KRB_AS_REQ, разом із декількома необов'язковими: поле даних авторизації для використання сервера додатків та додаткові квитки, необхідні для деяких опцій.

Під час підготовки заголовка аутентифікації клієнт може вибрати sub-session key, яким буде зашифрована відповідь сервера Kerberos. Якщо клієнт вибирає даний ключ, слід подбати про випадковість його вмісту.

У наведеному вище зразку повідомлення можна побачити, що поле даних попередньої аутентифікації заповнено заголовком типу RA-TGS-REQ (див. RFC 4120, розділ 5.2.7.1) структури даних – воно містить TGT та аутентифікатор для цього кроку і має тип AP-REQ.

Це представляє собою «message 3» (TGT із «message 2» та ідентифікатор запитуваної послуги, `krbtgt@rcbj.net` для нашого входу в домен Windows) та «message 4» (Authenticator, зашифрований за допомогою session key, встановленого між клієнтом та TGS) з попереднього опису.

На даний момент TGS використовує свій секретний ключ для дешифрування TGT. Потім він може отримати ключ сеансу клієнта та TGS із розшифрованого квитка. Надалі, використовуючи session key для розшифровки аутентифікатора (поле `enc-part`), може порівняти ім'я користувача в аутентифікаторі з іменем у TGT. Якщо ці два імена збігаються, TGS продовжує, як зображено нижче (рис.3.8). В іншому випадку повернеться сповіщення про помилку.

```

▼ Kerberos
  > Record Mark: 1499 bytes
  ▼ tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    crealm: RCBJ.NET
    ▼ cname
      name-type: kRB5-NT-PRINCIPAL (1)
      ▼ cname-string: 1 item
        CNameString: rcbj
    ▼ ticket
      tkt-vno: 5
      realm: RCBJ.NET
      ▼ sname
        name-type: kRB5-NT-SRV-HST (3)
        ▼ sname-string: 2 items
          SNameString: host
          SNameString: ec2amaz-danl2uj.rcbj.net
      ▼ enc-part
        etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
        kvno: 1
        cipher: f0ecac66daa2f616a2a15bbe1f756df290fbd10fc65cc3c7...
    ▼ enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
      cipher: 7bf6683484269c6d0b0535e704aebc043edda6df39db7c2b...
  
```

Рисунок 3.8 – Служба надання квитків відповідає повідомленням TGS-REP

Сюди входять «message 5» між клієнтом та сервером або Service Ticket, зашифрований за допомогою секретного ключа служби якої звертаються, в даному випадку облікового запису комп'ютера робочої станції та «message 6» (ключ клієнт-серверного сеансу, зашифрований клієнт-TGS ключем). Для подальшого роз'яснення, який secret key використовується для розшифровки ST у «message 5», нагадується, що кожна робоча станція та сервер, зареєстровані в Домені Windows, мають обліковий запис машини, який має пов'язану з ним secret key (сформований пароль).

Отримавши повідомлення, клієнт може розшифрувати ключ клієнт-серверного сеансу, який йому потрібен для наступного кроку, і зашифрований квиток, доступний для подання бажаних служб. За умови достатнього часу типовий користувач Windows зробить щось, що передбачає доступ до віддаленої служби (мережева файлова система, принтер, електронна пошта тощо).

Клієнт-серверний обмін (або його відсутність). Під час входу в систему Windows користувачем домену остаточний обмін повідомленнями KRB-AP-REQ та KRB-AP-REP насправді не відбувається, оскільки скористованою послугою, насправді, є вхід до локальної робочої станції (або сервера Windows), який був ініціалізований послідовністю аутентифікації Kerberos на початку. Отже, з позиції наявності прикладу, який демонструє даний протокол, він є не ідеальним, проте доволі поширений.

Сучасне шкідливе програмне забезпечення, особливо віруси-вимагачі, пристосувалися використовувати традиційні тактики та методи тестів на проникнення (pentesting) задля зараження мереж.

Захистити організацію від Kerberoasting атак не завжди просто. Хоча немає можливості змінити правила, за якими функціонують квитки, оскільки вони є частиною архітектури Kerberos, наступні елементи керування можуть мінімізувати ймовірність успішних атак:

– Встановлення суворої політики паролів, яка вимагає принаймні 25 символів для облікових записів сервісів та додатків. Це суттєво обмежує,

					КІК.КБ.Б-125-06-ПЗ	63
Зм						
Арк.	№ документа	Підпис	Дата			

наскільки швидко зловмисник може зламати пароль, якщо буде захоплено квиток.

– Увімкнення ведення журналу аудиту на контролері домену для реєстрації успішних запитів на квитки служби надання квитків Kerberos, зокрема тих, які надсилаються із слабким шифруванням RC4 або DES, та налаштування інформації про безпеку та моніторингу подій або інструменту управління журналами для попередження про ці події.

Запобігання Kerberoasting може бути здійснено ще за допомогою декількох методів, кожен із яких рекомендується до застосування, задля покращення безпеки Active Directory.

Необхідне надійне налаштування політик та контролера домену, пов'язаних з Kerberos, одними із яких являються наступні:

- Увімкнення шифрування AES Kerberos (або інший більш сильний алгоритм шифрування), а не RC4, де це можливо;
- Розглянення можливості використання групових керованих облікових записів сервісів послуг, а не службових, зі статичними паролями;
- Переконавання, що всі облікові записи служб мають випадково сформовані паролі із понад 25 символів.

Надалі, буде розглянуто більш загальні методи та способи передбачення та протидії вже існуючих вразливостей в доменній службі.

Величезна більшість великих підприємств використовують Microsoft Active Directory для управління привілеями облікових записів.

Неможливість встановити пріоритет для активної, динамічної стратегії безпеки AD може мати значні наслідки. Служба каталогів централізує доступ та авторизацію користувачів на всіх рівнях організації, що робить її основною ціллю для реалізації кібератак хакерів. Потрапляючи в систему, експлойти часто можуть посилювати привілеї суб'єктів, отримуючи доступ до безлічі мережевих ресурсів. Одне порушення безпеки AD може поставити під загрозу всю цифрову інфраструктуру компанії, що дозволить хакерам красти приватну

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			64

системну інформацію з усіх облікових записів користувачів, баз даних та програм у системі.

Розробка стандартів моніторингу та аудиту у режимі реального часу, може стати безцінним ресурсом для підприємств, які прагнуть захистити свої мережі. Розробка процесу, який дозволяє уповноваженому персоналу контролювати та перевіряти всю систему на наявність будь-якої несанкціонованої або небезпечної діяльності, яка може поставити мережу під загрозу. Впровадження рішення, яке оцінює зміни поведінки користувачів та трафіку у мережі, може допомогти виявити незвичні дії у системі якомога швидше, аби уникнути потенційної кібератаки.

Active Directory Auditing – це процес збору даних про об'єкти та атрибути AD, а також аналіз та звітування щодо цих даних для визначення загального стану каталогу. Організації проводять аудит, по-перше, задля захисту AD від зловмисників, які переслідують облікові дані, та, по-друге, для забезпечення безперебійної роботи мережі.

Перевіряючи домен, є можливість зменшити ризики безпеки, виявляючи та виправляючи умови, при яких групи та безпосередньо призначені дозволи можуть використовуватись для отримання доступу до мережесих ресурсів. Також необхідно розкривати та виправляти такі шкідливі додатки, які сповільнюють або призводять до зависання використовуваного ПО, задля підвищення ефективності роботи.

Аудит Active Directory складається з п'яти кроків, які допомагають визначити пріоритети основних дій у існуючій мережі.

Крок 1: Опитування та аналіз. Необхідно сканувати та скласти карту середовища AD, задля визначення таких параметрів:

- кількість облікових записів і груп;
- види та кількість наявних вразливостей системи;
- існуючі дозволи на контролери домену (DC) та організаційні підрозділи (OU).

Дізнавшись, що знаходиться у середовищі AD, можна почати сортувати.

					КІК.КБ.Б-125-06-ПЗ	65
Зм	Арк.	№ документа	Підпис	Дата		

Крок 2: Зосередження на тому, що має найбільше значення. Визначення пріоритетності зусиль на основі висновків. Три важливих місця, з яких варто почати:

- Привілейований доступ до AD; Вивчення таких важливих об'єктів, як групова політика та адміністратори домену / підприємства;
- Виправлення груп; Оцінка груп, які фактично мають однаковий рівень членства з добре відомими принципами безпеки, як усі «Domain Users» або «Groups»;
- Привілейований доступ користувачів; Визначення, які користувачі мають підвищений або прямий доступ.

Крок 3: Залучення «зацікавлених сторін». Отримання підтримки для вирішення пріоритетних питань. Наприклад, можливе використання сканування дозволів для ідентифікації «зацікавлених сторін» на основі того, хто має доступ до Active Directory, а також тих, хто має доступ до об'єктів AD. Наприклад, визначення менеджера груп або користувачів, які знатимуть, чому дозволи були встановлені певним чином, наприклад, делеговані дозволи адміністратора для виконання певних завдань, таких як скидання паролів.

Крок 4: Огляд та виправлення. Маючи в системі «зацікавлені сторони», необхідно перевірити членство в групах та усунути проблемні та вразливі місця AD. По-перше, обмежити привілейований доступ до AD, перевіривши, чи є правильні користувачі в адміністраторах домену та підприємства. Цей підхід з найменшими привілеями зменшує шанс зловмисного адміністратора зловживати привілеями, отримуючи доступ до конфіденційних даних або додаючи неавторизованого користувача до членства групи. По-друге, залучення власників до управління групами, аби визначити, чи правильно встановлені відповідності стосовно всіх членів груп, і що група в цілому має доступ до необхідних ресурсів.

Крок 5: Виконання процесу повторно. Зробити процес безперервним циклом. Після визначення головних пріоритетів, стає необхідним повернення до першого кроку і повторення процесу для наступного пріоритету. Наприклад,

					КІК.КБ.Б-125-06-ПЗ	66
Зм						
Арк.	№ документа	Підпис	Дата			

іншою дією може бути забезпечення того, щоб паролі AD відповідали політиці змін і не зберігалися в пам'яті. [18]

3.2 Визначення найкращих практик Active Directory стосовно захисту систем

Впровадження та підтримка політик безпеки AD може допомогти протистояти фішингу, зловмисному програмному забезпеченню та іншим кібератакам, а також захистити користувачів та ресурси мережі. Нижче наведений список дій, які слід застосувати для посилення кібербезпеки у системах.

- Проведення інвентаризації. Найефективніший спосіб підтримувати найвищі стандарти кібербезпеки AD - це ретельна інвентаризація всієї вашої системи. Основні списки повинні включати ідентифікацію всіх комп'ютерів, пристроїв, користувачів та доменів для OU.

- Оцінка поточних налаштувань безпеки. Active Directory пропонує конфігурацію безпеки за замовчуванням. Як правило, цих дій недостатньо для забезпечення захисту мережі. Після встановлення завжди необхідно переглядати існуючу конфігурацію безпеки, аби належним чином налаштувати параметри відповідно до конкретних вимог.

- Встановлення моделі "найменших привілеїв". Дана стратегія полягає в обмеженні доступу користувачів до ресурсів у системі на основі того, що є важливим для виконання запланованої ролі або функції. Такий підхід допомагає мінімізувати загальний вплив та ризик викрадення даних у випадку компрометації системи. Систематичний перегляд всіх поточних дозволів надає можливість визначити будь-які необхідні, навіть найменші з них, зміни привілеїв.

- Обмеження прав адміністратора AD. Недостатньо буде відділяти окремі привілеї користувачів. Крім того, важливо надавати адміністративні та «суперкористувацькі» привілеї лише тим, хто потребує такого рівня доступу для належної роботи у організації.

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		67

– Розробка комплексного підходу до захисту контролера домену. Компрометований DC, зокрема центр розповсюдження ключів Kerberos (KDC), може підірвати цілісність усієї мережі в цілому. Якщо хакер отримає доступ до системи такого рангу, він може миттєво підключитися до всього, що входить до інфраструктури. Першим кроком є фізичне відокремлення контролерів домену від інших серверів. Багато підприємств використовують зачинену кімнату, до якої не мають доступу сторонні суб'єкти. Цей додатковий рівень безпеки може допомогти запобігти зовнішньому проникненню.

– Використання Multi-Factor Authentication (MFA). Зловмисник може легко зламати віддалених користувачів, часто навіть не викриваючи себе. Багатофакторна аутентифікація пропонує один із найкращих способів захисту віддалених пристроїв від онлайн-атак. Рішення MFA вимагає від користувача надання ним двох чи більше доказів своєї автентичності, перед тим як отримати доступ до системи.

– Навчання персоналу. Співробітники можуть становити значний ризик для безпеки компаній, що використовують AD. Навіть найбільш доброзичливий з них, може ненавмисно натиснути фішингове посилання або отримати спам електронною поштою, призначені для розкриття інформації приватної компанії. Розуміння справжніх загроз та володіння інструментами розпізнавання небезпеки забезпечить їх вміннями, необхідними для уникнення компрометації системи.

Зловмисники використовують викрадені дані організацій, розміщуючи їх в Інтернеті, щоб змусити жертв платити. У більшості випадків протиправні дії націлені на Active Directory, задля легкого розповсюдження програм-вимагачів після отримання привілеїв домену.[6]

Як тільки злочинець закріплюється в організації, він не може рухатися далі без доступу до привілейованого облікового запису користувача, тому негайно шукатиме привілеї високого рівня, задля отримання доступу до потрібної інформації в організації. Досягнувши необхідних привілеїв, хакер може створювати бездіяльні облікові записи, надаючи їм бекдор-доступ так, що

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		68

навіть якщо їх виявлять, вони можуть непомітно повернутися до середовища. Зловмисник може навіть стерти свої криміналістичні сліди, рухаючись поступово через мережу організації.

Незважаючи на критичну затребуваність, управління та захист Active Directory є надзвичайно складним процесом, який потребує величезного досвіду та постійної уваги.

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			69

ВИСНОВКИ

В ході дослідження протоколів аутентифікації користувачів було, розкрито тему проекту підсистеми аутентифікації користувачів комп'ютерної мережі. Було розглянуто значну кількість профільної літератури та створено схему для дослідження протоколів ідентифікації, автентифікації та обліку. В контексті дослідження системи доменних підґрунтям була документація Cisco, навчальні посібники авторів «R. Allen», «B. Desmond» та «S. Harris», документація, яка опублікована IETF в документах RFC 2866, 6733, 1510 та ін.

В першому розділі кваліфікаційної роботи було розглянуто теоретичні відомості про принципи ідентифікації, автентифікації, авторизації та аудиту, а саме: етимологію походження механізмів ідентифікації та автентифікації, принципи управління сутностями та управління паролями. В контексті розгляду управління паролями було досліджено та проаналізовано такі поняття, як: синхронізація паролів, самостійне скидання паролів та допоміжне скидання. Було розглянуто та проведено аналітичне порівняння таких протоколів автентифікації, як Radius, Tacs+, Diameter та Kerberos. Було сформовано та обґрунтовано використання протоколу Kerberos в сучасних системах, як основний безпечний протокол автентифікації.

В другому розділі було здійснено проектування підсистеми для дослідження роботи протоколів автентифікації та дослідження проведення атак. Було розкрито питання дослідження процесів аутентифікації протоколу Kerberos. Було розроблено схему макету мережі, розроблено таблиці комутації та запроектовано таблиці IP адресації. Було виконано розгортання та налаштування автентифікації у гетерогенній мережі з використанням Windows Server 2019 на базі протоколу Kerberos. Було проведено дослідження стосовно можливих типів атак на протокол Kerberos.

В третьому розділі було досліджено засоби захисту відносно доменної служби Active Directory. Було виконано обстеження та аналіз проходження трафіку в мережі Kerberos за допомогою програмного додатку WireShark. Було

					КІК.КБ.Б-125-06-ПЗ	70
Зм	Арк.	№ документа	Підпис	Дата		

досліджено та визначено найкращі практики Active Directory стосовно захисту засобів автентифікації в сучасних мережах.

В результаті виконання кваліфікаційної роботи було отримано працюючу схему, таблиці адресації та комутації для виконання демонстрації роботи автентифікації на базі протоколу Kerberos. Було отримано звіти з програмного застосунку WireShark та проаналізовано отриманий трафік. Було обрано найкращі методи захисту користувацької авторизації. Було сформовано порівняльні таблиці протоколів авторизації та сформовано пояснювальну записку у вигляді звіту з результатами виконаної роботи.

Дослідження було проведено за допомогою системного підходу. Було розкрито тему проекту підсистеми аутентифікації користувачів комп'ютерної мережі. Тому можна вважати завдання кваліфікаційної роботи виконаним.

					КІК.КБ.Б-125-06-ПЗ	
Зм						
Арк.	№ документа	Підпис	Дата			71

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bani M. Detecting Kerberoasting activity using Azure Security Center [Електронний ресурс] / Bani Malui // Microsoft. – 2018. – Режим доступу до ресурсу: <https://docs.microsoft.com/en-us/archive/blogs/motiba/detecting-kerberoasting-activity-using-azure-security-center>. Microsoft. (n.d.). Service Principal Names. Retrieved March 22, 2018.
2. Gibson D. CompTIA Security+ All-in-One Exam Guide / D. Gibson. – Virginia Beach: StudyGuide Copyright, 2017. – 1197 с.
3. Protection from Kerberos Golden Ticket [Електронний ресурс] // CERT-EU. – 2014. – Режим доступу до ресурсу: https://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf.
4. Gibson, D. (2017). CompTIA SECURITY+ Get Certified Get Ahead SY0401 Study Guide. Virginia Beach, VA: YCDA, LLC
5. Jennifer G. Steiner; Clifford Neuman; Jeffrey I. Schiller. "Kerberos: An Authentication Service for Open Network Systems" (PDF). S2CID 222257682. Retrieved 2019-05-07.
6. Reyor B. Defending Against Active Directory Kerberos Attacks [Електронний ресурс] / Bill Reyor // Blumira. – 2021. – Режим доступу до ресурсу: <https://www.blumira.com/active-directory-kerberos-attacks/>.
7. Meyers, M. (2015). All in One CompTIA Network+ Certification Exam N10-006. McGraw-Hill Education: New York, NY.
8. Harris S. CISSP All-in-One Exam Guide / S. Harris, F. Maymi. – New York: McGraw-Hill Education, 2016. – 1289 с. – (Library of Congress Cataloging-in-Publication Data). – (Seventh Edition).
9. Medin T. Attacking Kerberos - Kicking the Guard Dog of Hades [Електронний ресурс] / Tim Medin // Red Siege. – 2014. – Режим доступу до ресурсу: <https://www.redsiege.com/wp-content/uploads/2020/08/Kerberoastv4.pdf>.

					КІК.КБ.Б-125-06-ПЗ		
Зм	Арк.	№ документа	Підпис	Дата			72

10. PÉREZ E. Kerberos (I): How does Kerberos work? [Електронний ресурс] / ELOY PÉREZ // Tarlogic. – 2019. – Режим доступу до ресурсу: <https://www.tarlogic.com/en/blog/how-kerberos-works/>.
11. Белов А. Настройка DNS-сервера на Windows Server 2012 и старше [Електронний ресурс] / Антон Белов. – 2019. – Режим доступу до ресурсу: <https://serverspace.ru/support/help/configuring-a-dns-server-on-windows-server-2012-or-later/>.
12. Solie K. Ccie Practical Studies (Cisco Press Practical Studies Series) / K. Solie, L. Lynch. – California: Cisco Systems, 2001. – 1366 с.
13. Schroeder W. Invoke-Kerberoast [Електронний ресурс] / W. Schroeder, M. Hart. – 2016. – Режим доступу до ресурсу: <https://powersploit.readthedocs.io/en/latest/Recon/Invoke-Kerberoast/>.
14. Remote Authentication Dial In User Service (RADIUS) [Електронний ресурс] / [C. Rigney, S. Willens, A. Rubens та ін.] // Network Working Group. – 2000. – Режим доступу до ресурсу: <https://www.ietf.org/rfc/rfc2865.txt?number=2865>.
15. Diameter Base Protocol [Електронний ресурс] / [V. Fajardo, J. Arkko, J. Loughney та ін.] // Internet Engineering Task Force. – 2012. – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc6733>.
16. Metcalf S. Mimikatz and Active Directory Kerberos Attacks [Електронний ресурс] / Sean Metcalf // ADSecurity. – 2014. – Режим доступу до ресурсу: <https://adsecurity.org/?p=556>.
17. Kohl J. The Kerberos Network Authentication Service (V5) [Електронний ресурс] / J. Kohl, C. Neuman // Network Working Group. – 1993. – Режим доступу до ресурсу: <https://www.zora.uzh.ch/id/eprint/174650/1/Shibboleth-final.pdf>.
18. Svidergol B. Active Directory Cookbook: Solutions for Administrators & Developers / B. Svidergol, R. Allen., 2013. – 860 с. – (Submit Errata). – (4th Edition).

					КІК.КБ.Б-125-06-ПЗ	
Зм	Арк.	№ документа	Підпис	Дата		
					73	

19. Schiller E. Shibboleth based Authentication, Authorization, Accounting and Auditing in Wireless Mesh Networks [Электронный ресурс] / E. Schiller, A. Monakhov, P. Kropf // University of Zurich. – 2011. – Режим доступа до ресурсу: <https://www.zora.uzh.ch/id/eprint/174650/1/Shibboleth-final.pdf>.

20. Настройка основных средств аутентификации, авторизации и учета на сервере доступа [Электронный ресурс] // Cisco Systems. – 2005. – Режим доступа до ресурсу: https://www.cisco.com/c/ru_ru/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html?referring_site=RE&pos=1&page=https://www.cisco.com/c/ru_ru/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html.

21. Metcalf S. Cracking Kerberos TGS Tickets Using Kerberoast – Exploiting Kerberos to Compromise the Active Directory Domain [Электронный ресурс] / S. Metcalf // ADSecurity. – 2015. – Режим доступа до ресурсу: <https://adsecurity.org/?p=2293>.

22. Setting up Samba as a Domain Member [Электронный ресурс] // Samba. – 2019. – Режим доступа до ресурсу: https://wiki.samba.org/index.php/Setting_up_Samba_as_a_Domain_Member.

23. T-Cross. Разбираем атаки на Kerberos с помощью Rubeus. Часть 1 [Электронный ресурс] / T-Cross. – 2020. – Режим доступа до ресурсу: <https://habr.com/ru/company/tomhunter/blog/507140/>.

24. T-Cross. Разбираем атаки на Kerberos с помощью Rubeus. Часть 2 [Электронный ресурс] / T-Cross // T.Hunter. – 2020. – Режим доступа до ресурсу: <https://habr.com/ru/company/tomhunter/blog/509290/>.

25. Methods of Authentication: PPP, AAA, and EAP [Электронный ресурс] // TheCybersecurityMan. – 2017. – Режим доступа до ресурсу: <https://thecybersecurityman.com/2017/12/22/methods-of-authentication-ppp-aaa-and-eap/>.

26. Security+: Authentication Services (RADIUS, TACACS+, LDAP, etc.) (SY0-401) [Электронный ресурс] // INFOSEC. – 2017. – Режим доступа до

					КИК.КБ.Б-125-06-ПЗ	
Эм	Арк.	№ документа	Підпис	Дата		74

ресурсы: <https://resources.infosecinstitute.com/certification/security-plus-authentication-services-radius-tacacs-ldap-etc-sy0-401/>.

27. Broeckelmann R. Kerberos Wireshark Captures: A Windows Login Example [Электронный ресурс] / Robert Broeckelmann // Medium. – 2018. – Режим доступа до ресурсу: <https://medium.com/@robert.broeckelmann/kerberos-wireshark-captures-a-windows-login-example-151fabf3375a>.

28. Configuring AAA Services [Электронный ресурс] // Cisco Systems. – 2015. – Режим доступа до ресурсу: https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-0/security/configuration/guide/sc40crsbook_chapter1.html.

29. Rosencrance L. Authentication in cybersecurity [Электронный ресурс] / Linda Rosencrance // TechTarget. – 2018. – Режим доступа до ресурсу: <https://searchsecurity.techtarget.com/definition/authentication>.

30. Mehl B. Authentication Protocols: LDAP vs Kerberos vs OAuth2 vs SAML vs RADIUS [Электронный ресурс] / Bernhard Mehl // Kisi. – 2018. – Режим доступа до ресурсу: <https://www.getkisi.com/blog/authentication-protocols-overview>.

31. Callaway C. Kerberos [Электронный ресурс] / Caleb Callaway // Ubuntu documentation. – 2021. – Режим доступа до ресурсу: <https://help.ubuntu.com/community/Kerberos>.

32. Fun with LDAP, Kerberos (and MSRPC) in AD Environments [Электронный ресурс] // ropnop. – 2018. – Режим доступа до ресурсу: <https://speakerdeck.com/ropnop/fun-with-ldap-kerberos-and-msrpc-in-ad-environments?slide=58>.