

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

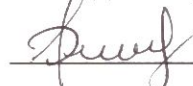
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми аутентифікації користу-
вачів комп'ютерної мережі організації на базі рішень
TekRADIUS та FreeRADIUS»

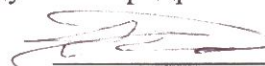
Виконав: студент 3-го курсу групи КБк-22-1
спеціальності 125 «Кібербезпека»

 Ілля КУЛЕНКО

Керівник: Старший викладач кафедри КІ та КБ,

 Єлизавета ТРОКОЗ

Рецензент: Завідувач кафедри КІ та КБ, к.т.н., доцент,

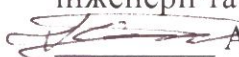
 Андрій ЄФІМЕНКО

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Куленко Ілля Вікторович

Тема роботи: «Проект підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі рішень TekRADIUS та FreeRADIUS»

затверджена Наказом університету від 3 березня 2025 р. № 80/с

Термін здачі студентом закінченої роботи 20 червня 2025 р.

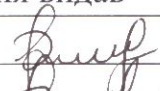
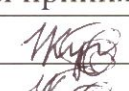
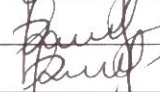
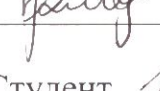
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

- підсистема аутентифікації на основі TekRADIUS і FreeRADIUS;
- безпечний процес аутентифікації користувачів у комп'ютерній мережі організації.

Обладнання та програмне забезпечення:

1. Емулятор GNS3
2. Маршрутизатор Cisco ISR4451
3. Комутатори Cisco C9200CX та Cisco C9200L-24P
4. ОС Windows Server 2019 та Linux Ubuntu 22.04 LTS
5. Сервери FreeRADIUS та TekRADIUS

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є. М.	12.03.2025 	12.03.2025 
2	Трокоз Є. М.	10.04.2025 	10.04.2025 
3	Трокоз Є. М.	05.05.2025 	05.05.2025 

Студент  Ілля КУЛЕНКО

Керівник  Єлизавета ТРОКОЗ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Узгодження теми, мети та завдань	05.03.2025 – 12.03.2025	Виконано
2	Теоретичний аналіз RADIUS та AAA	12.03.2025 – 02.04.2025	Виконано
3	Порівняльний аналіз рішень	02.04.2025 – 10.04.2025	Виконано
4	Моделювання загроз і аналіз ризиків	10.04.2025 – 17.04.2025	Виконано
5	Проектування мережевої архітектури	17.04.2025 – 26.04.2025	Виконано
6	Підготовка та налаштування тестового середовища	05.04.2025 – 13.05.2025	Виконано
7	Встановлення й конфігурація серверів	14.05.2025 – 22.05.2025	Виконано
8	Тестування системи безпеки	23.05.2025 – 30.05.2025	Виконано
9	Інтеграція 802.1X та журналювання	31.05.2025 – 06.06.2025	Виконано
10	Завершення оформлення та підготовка до захисту	07.06.2025 – 20.06.2025	Виконано
11	Оформлення презентації	21.05.2025 – 23.05.2025	Виконано
12	Захист	24.06.2025	Виконано

Студент  Ілля КУЛЕНКО

Керівник  Єлизавета ТРОКОЗ

АНОТАЦІЯ

У межах кваліфікаційної роботи розроблено підсистему аутентифікації користувачів у корпоративній комп'ютерній мережі навчального закладу на основі RADIUS-серверів TekRADIUS і FreeRADIUS із дотриманням принципів моделі AAA. Пояснювальна записка містить 129 сторінок, включає 133 рисунка, 11 таблиць, 50 джерел у списку літератури, який розміщено на 5 сторінках.

Метою випускної кваліфікаційної роботи є проектування, впровадження та аналіз безпечної, масштабованої підсистеми аутентифікації в умовах корпоративної мережі з використанням рішень TekRADIUS та FreeRADIUS.

У ході виконання роботи визначено основні вимоги до підсистем аутентифікації, проаналізовано базові характеристики серверів TekRADIUS і FreeRADIUS, розглянуто особливості їх функціонування, налаштування та інтеграції з іншими компонентами інфраструктури. Побудовано модель загроз і порушника, сформовано мережеву архітектуру з сегментацією на основі VLAN та резервуванням GLBP. Показано розробку прототипу в середовищі GNS3, наведено результати тестування безпеки, стійкості та продуктивності підсистеми, зокрема з використанням протоколів 802.1X, RadSec, IPSec та журналювання подій.

Ключові слова: АУТЕНТИФІКАЦІЯ, RADIUS, FREERADIUS, TEKRAIDUS, AAA, 802.1X, СИСТЕМА ДОСТУПУ, VLAN, ЖУРНАЛЮВАННЯ, RADSEC, EAP-TLS.

					ККІКБ.КР.Б – 125 – 5 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі рішень TekRADIUS та FreeRADIUS	Лім.	Арк.	Аркушів
Розроб.		Куленко І.В.		23.06.25				
Керівник		Трокоз Є.М.		23.06.25			4	144
Реценз.		Сфіменко А.А.		23.06.25		ФІКТ, Гр. КБк-22-1		
Н. контр.		Трокоз Є.М.		23.06.25				
Затверд.		Сфіменко А.А.		23.06.25				

ANNOTATION

As part of the bachelor's qualification project, a user authentication subsystem was developed for the corporate computer network of an educational institution based on TekRADIUS and FreeRADIUS servers, in accordance with the principles of the AAA model. The explanatory note contains 129 pages, includes 133 figures, 11 tables, and a list of 50 references spanning 5 pages.

The aim of the final qualification work is to design, implement, and analyze a secure and scalable authentication subsystem for a corporate network using TekRADIUS and FreeRADIUS solutions.

During the project, the main requirements for authentication subsystems were identified, the basic characteristics of TekRADIUS and FreeRADIUS servers were analyzed, and the features of their operation, configuration, and integration with other infrastructure components were examined. A threat and adversary model was built, and a network architecture was designed with VLAN-based segmentation and GLBP-based redundancy. The development of a working prototype in the GNS3 environment was demonstrated. The results of security, resilience, and performance testing of the subsystem were provided, including the use of 802.1X, RadSec, IPSec protocols, and event logging mechanisms.

Keywords: AUTHENTICATION, RADIUS, FREERADIUS, TEKRADIUS, AAA, 802.1X, ACCESS SYSTEM, VLAN, LOGGING, RADSEC, EAP-TLS.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП	9
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ АУТЕНТИФІКАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ	11
1.1. Концепція та роль аутентифікації, авторизації та обліку в мережевій безпеці	11
1.2. Протокол RADIUS: архітектура, принципи роботи та застосування ...	13
1.3. Вимоги до підсистем аутентифікації для корпоративних мереж	16
1.4. Безпека протоколу RADIUS	24
1.5. Аналіз існуючих рішень RADIUS-серверів	29
РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА ОБҐРУНТУВАННЯ ВИБОРУ ДЛЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ	34
2.1. Модель загроз та модель порушника	34
2.2. Топологія мережі	42
2.3. Розробка схеми адресації мережі	47
2.4 Відповідність підсистеми вимогам	49
РОЗДІЛ 3. ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ МЕРЕЖІ	55
3.1. Налаштування мережі	55
3.2. Інтеграція підсистеми аутентифікації та порівняння рішень	65
3.3 Перевірка безпеки підсистеми аутентифікації	83
3.4 Забезпечення безпеки підсистеми та її перевірка	90
3.5 Перевірка працездатності підсистеми автентифікації	108
ВИСНОВКИ	122
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	124
ДОДАТКИ	129

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AAA – Authentication, Authorization, Accounting – автентифікація, авторизація та облік

ACL – Access Control List – список контролю доступу

AD – Active Directory – служба каталогів від Microsoft

ARP – Address Resolution Protocol – протокол визначення MAC-адреси

CA – Certification Authority – центр сертифікації

CLI – Command Line Interface – інтерфейс командного рядка

DAI – Dynamic ARP Inspection – динамічна перевірка ARP-трафіку

DHCP – Dynamic Host Configuration Protocol – протокол автоматичної конфігурації хостів

DoS – Denial of Service – відмова в обслуговуванні

EAP – Extensible Authentication Protocol – розширюваний протокол автентифікації

EAP-TLS – EAP з використанням TLS (Transport Layer Security)

FreeRADIUS – Відкритий сервер автентифікації, авторизації та обліку

GLBP – Gateway Load Balancing Protocol – протокол балансування шлюзів

GNS3 – Graphical Network Simulator – програмне середовище для моделювання мереж

GUI – Graphical User Interface – графічний інтерфейс користувача

IPSec – Internet Protocol Security – набір протоколів для захисту IP-трафіку

LDAP – Lightweight Directory Access Protocol – протокол доступу до служби каталогів

MD5 – Message Digest 5 – алгоритм хешування

MITM – Man-in-the-Middle – атака типу «людина посередині»

NAS – Network Access Server – сервер доступу до мережі

OTP – One-Time Password – одноразовий пароль

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

PAP – Password Authentication Protocol – протокол автентифікації за паролем

PEAP – Protected Extensible Authentication Protocol

RADIUS – Remote Authentication Dial-In User Service – служба віддаленої автентифікації

QoS – Quality of Service – якість обслуговування

RBAC – Role-Based Access Control – контроль доступу на основі ролей

SSH – Secure Shell – захищений протокол віддаленого доступу

SSL – Secure Sockets Layer – захищений протокол прикладного рівня

Syslog – Система журналювання подій

TekRADIUS – Комерційний RADIUS-сервер для Windows

TLS – Transport Layer Security – захист транспортного рівня

TCP – Transmission Control Protocol – протокол управління передачею

UDP – User Datagram Protocol – протокол датаграм користувача

VLAN – Virtual Local Area Network – віртуальна локальна мережа

802.1X – Стандарт IEEE для контролю доступу до дротових/бездротових мереж

ПЗ – програмне забезпечення

ОС – операційна система

ОЗ – обліковий запис

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Безпека інформаційних систем і централізоване управління доступом до ресурсів є ключовими вимогами для стабільного функціонування сучасних корпоративних, навчальних і державних організацій. Зростання кількості віддалених підключень, мобільних пристроїв та інцидентів інформаційної безпеки зумовлює необхідність у впровадженні ефективних механізмів контролю доступу. Одним із перевірених рішень для забезпечення комплексної моделі безпеки є використання протоколу RADIUS у поєднанні з архітектурою AAA (Authentication, Authorization, Accounting). Такий підхід дозволяє централізовано здійснювати аутентифікацію користувачів, визначати їхні права доступу та вести облік дій, що підвищує загальний рівень захищеності інформаційної інфраструктури.

Сучасні RADIUS-сервери, як-от FreeRADIUS і TekRADIUS, забезпечують високу гнучкість конфігурації, підтримку різноманітних методів аутентифікації (включно з EAP-TLS), сумісність з базами даних та можливість інтеграції з іншими системами доступу. Їх застосування особливо актуальне у великих освітніх установах, де щогодини здійснюється значна кількість запитів і необхідна чітка сегментація прав доступу до мережевих ресурсів.

Метою кваліфікаційної роботи є проектування, впровадження та комплексний аналіз підсистеми аутентифікації користувачів у корпоративній мережі вищого навчального закладу на базі RADIUS-серверів TekRADIUS і FreeRADIUS.

Визначена мета обумовлює виконання таких завдань:

- дослідити та узагальнити вимоги до підсистем аутентифікації в контексті безпеки, продуктивності та масштабованості;
- порівняти архітектурні та функціональні можливості RADIUS-серверів TekRADIUS і FreeRADIUS;
- розробити мережеву архітектуру з інтегрованою AAA-підсистемою аутентифікації;

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

- побудувати моделі загроз і порушника для обґрунтування вибору безпекових механізмів;
- реалізувати прототип підсистеми аутентифікації та провести тестування її основних характеристик;
- оцінити ефективність розробленої підсистеми відповідно до функціональних і безпекових критеріїв.

Об'єктом дослідження є процес аутентифікації користувачів у корпоративній комп'ютерній мережі організації, зокрема механізми забезпечення безпеки та управління доступом на основі системи AAA.

Предметом дослідження є методи та технології розгортання, налаштування та тестування підсистеми аутентифікації користувачів на базі серверів TekRADIUS і FreeRADIUS з метою забезпечення захищеного, масштабованого та контрольованого доступу до мережевих ресурсів організації.

У процесі виконання кваліфікаційної роботи було розроблено прототип підсистеми аутентифікації користувачів мережі на базі TekRADIUS і FreeRADIUS із налаштованими механізмами аутентифікації, авторизації та обліку, а також виконано його функціонально-продуктивне та безпекове тестування.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ АУТЕНТИФІКАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

1.1. Концепція та роль аутентифікації, авторизації та обліку в мережівій безпеці

AAA (Authentication, Authorization, Accounting) – це стандартна система, яка використовується для управління доступом у комп'ютерних мережах.

Аутентифікація – перший крок у процесі AAA та відіграє ключову роль у запобіганні несанкціонованому доступу. Вона забезпечує, що лише легітимні користувачі, пристрої чи системи можуть отримати доступ до мережі. Процес аутентифікації може включати:

- введення імені користувача та пароля;
- використання біометричних даних, таких як відбитки пальців чи розпізнавання обличчя;
- багатофакторну аутентифікацію, яка комбінує кілька методів, наприклад, пароль і код із мобільного додатка.

На рис. 1.1 наведено приклади рекомендованих методів аутентифікації.

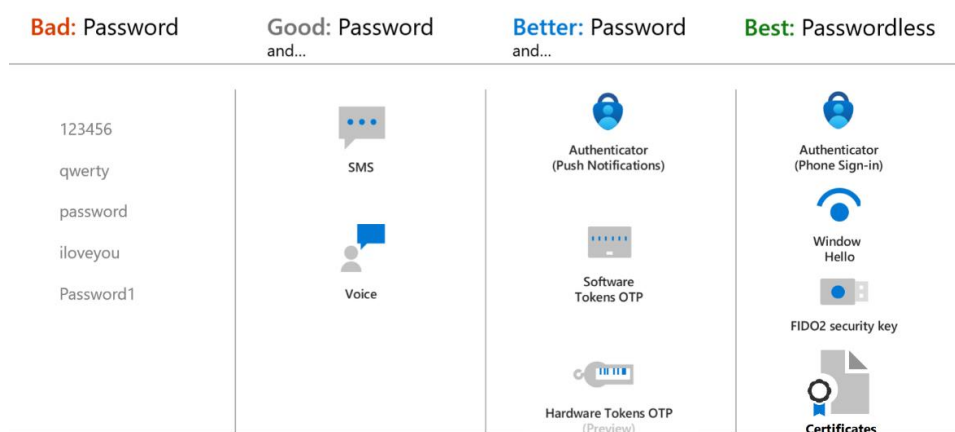


Рисунок 1.1 – Гарні практики з аутентифікації

Аутентифікація є необхідною для захисту від несанкціонованого доступу через IP-адреси, особливо в умовах віддаленого доступу. Наприклад, якщо хтось намагається підключитися до корпоративної мережі, аутентифікація перевіряє їхні облікові дані, щоб переконатися, що вони мають право на

доступ. Це зменшує ризик компрометації мережі через крадіжку ідентичності [1, розділ 4.1].

Також може включати шифрування пакетів даних, що передаються, щоб запобігти перехопленню чутливої інформації [1, розділ 6.2]. Це особливо важливо для захисту конфіденційних даних, таких як фінансові чи медичні записи.

Після того, як користувач успішно пройшов аутентифікацію, авторизація визначає, які дії чи ресурси йому дозволено використовувати. Це допомагає реалізувати принцип найменшого привілею, який передбачає, що користувачі повинні мати лише мінімальний рівень доступу, необхідний для виконання їхніх завдань.

Наприклад, за даними сайту Fortinet, авторизація може визначити, до яких VLAN або списків контролю доступу має доступ користувач [29]. У корпоративному середовищі це може означати, що працівник відділу фінансів має доступ до фінансових баз даних, але не до технічної документації.

Авторизація допомагає зменшити ризик внутрішніх загроз, таких як зловживання привілеями, та зовнішніх атак, коли зловмисники отримують доступ через компрометовані облікові записи. Вона забезпечує гранулярний контроль, що є ключовим для захисту критичних систем [7].

Облік відповідає за відстеження та фіксацію дій користувача під час його роботи в мережі. Це включає запис таких даних, як:

- тривалість сеансу;
- обсяг переданих даних;
- ресурси, до яких було отримано доступ.

Облік є важливим для аудиту, білінгу та аналізу використання мережі. У постачальників інтернет-послуг облік може використовуватися для розрахунку плати за використаний трафік [15], тоді як у корпоративних мережах – для виявлення аномалій, які можуть вказувати на безпекові інциденти.

Він також допомагає у розслідуванні інцидентів безпеки, надаючи детальні журнали, які можна аналізувати для виявлення джерела атаки чи зловживання. Наприклад, якщо виявлено несанкціонований доступ, журнали обліку

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

можуть показати, коли і як це сталося, що є критично важливим для реагування на інциденти [16].

AAA часто реалізується за допомогою централізованих серверів, таких як RADIUS (Remote Authentication Dial-In User Service), TACACS+ (Terminal Access Controller Access-Control System Plus) або Diameter. Ці протоколи забезпечують стандартизований спосіб реалізації аутентифікації, авторизації та обліку. RADIUS широко використовується для аутентифікації користувачів у мережах постачальників інтернет-послуг [26].

Цей підхід дозволяє централізовано керувати доступом, що особливо важливо для великих мереж, де локальна аутентифікація на кожному пристрої може стати неефективною.

1.2. Протокол RADIUS: архітектура, принципи роботи та застосування

RADIUS (Remote Authentication Dial-In User Service) є стандартизованим протоколом, визначеним у RFC 2865 - RADIUS, для реалізації функцій автентифікації, авторизації та обліку у мережах [44]. Він широко використовується для централізованого управління доступом, особливо в умовах, коли потрібна безпека та масштабованість.

RADIUS базується на клієнт-серверній моделі [44], де:

- мережевий доступний сервер (NAS), такий як маршрутизатор, комутатор, VPN-сервер чи точка доступу Wi-Fi, виступає клієнтом RADIUS. NAS відповідає за ініціацію запитів на автентифікацію, авторизацію та облік, передаючи інформацію про користувача (наприклад, ім'я користувача, пароль, IP-адресу) до сервера RADIUS;
- сервер RADIUS приймає запити від NAS, перевіряє облікові дані користувача, виконує авторизацію та повертає конфігураційну інформацію. Він може діяти як проксі-клієнт, передаючи запити до інших серверів RADIUS або зовнішніх систем автентифікації, таких як LDAP чи Active Directory.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Вигляд архітектури протоколу RADIUS з різними пристроями зображено на рис. 1.2.

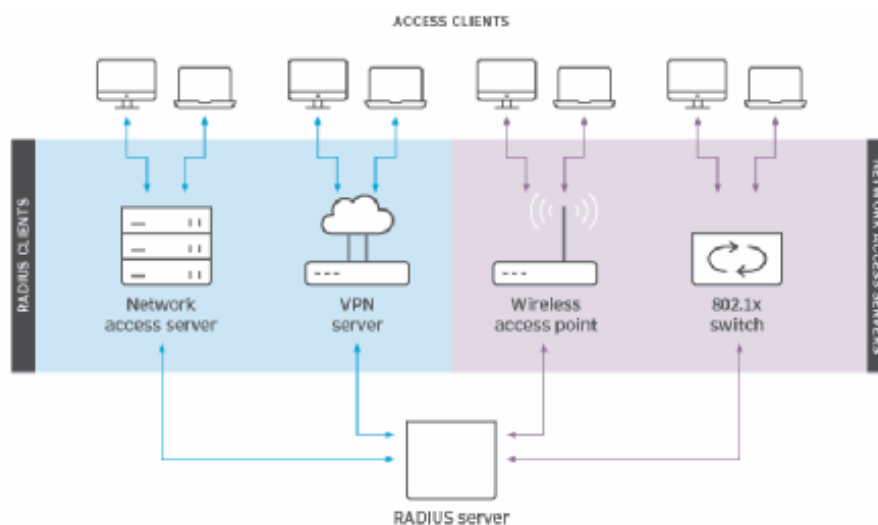


Рисунок 1.2 – Архітектура мережевого доступу

Ця архітектура забезпечує централізоване управління, що зменшує адміністративне навантаження, особливо в великих мережах. RADIUS розподіляє безпекові процеси (на сервері) від комунікаційних процесів (на NAS), що дозволяє мати єдине централізоване сховище для інформації про авторизацію та автентифікацію [48].

Принципи роботи RADIUS є наступними:

- безпека – транзакції між клієнтом і сервером автентифікуються за допомогою спільного секретного ключа, який ніколи не передається через мережу. Паролі користувачів шифруються між NAS і сервером, що запобігає перехопленню [44];
- гнучкість – протокол підтримує різні методи автентифікації, що робить його придатним для різних сценаріїв. Наприклад, він може інтегруватися з існуючими системами безпеки, такими як Kerberos чи SQL-бази даних [48];
- розширюваність – використовує структуру атрибут-довжина-значення (Attribute-Length-Value – ALV), що дозволяє додавати нові атрибути без порушення сумісності з існуючими реалізаціями. Це забезпечує гнучкість для майбутніх розширень [44];

- транспортний протокол – використовує UDP для передачі даних, з офіційно призначеними портами 1812 для автентифікації та авторизації та 1813 для обліку. Раніше використовувався порт 1645, але він конфліктував із сервісом "datametrics" [44].

Сервер, що розглядається, має широкий спектр застосувань, включаючи:

- використовується для автентифікації користувачів у dial-up, DSL, VPN та інших типах з'єднань. Як-от, постачальники інтернет-послуг (ISP) часто використовують RADIUS для перевірки доступу до мережі [26][48];

- забезпечує централізоване управління доступом як в корпоративних так і в освітніх установах, дозволяючи контролювати доступ до внутрішніх ресурсів [3];

- дозволяє відстежувати використання мережі для білінгу та статистики, наприклад, тривалість сеансу, обсяг переданих даних, що важливо для ISP та корпоративних мереж [15];

- RADIUS інтегрується з VPN-сервісами для автентифікації користувачів, забезпечуючи безпечний доступ до віддалених ресурсів [10, розділ 5.1].

Протокол RADIUS підтримує кілька методів автентифікації, що забезпечують гнучкість і безпеку. Згідно з RFC 2865 та RFC 3579 [34][44], до них належать:

- PAP (Password Authentication Protocol) – найпростіший метод, де пароль користувача передається у відкритому вигляді, але зашифрований між NAS і сервером. Це базовий метод, який підходить для простих сценаріїв, але менш безпечний через можливість перехоплення;

- CHAP (Challenge-Handshake Authentication Protocol) – використовує механізм виклику-відповіді, де сервер відправляє випадковий виклик, а клієнт відповідає зашифрованим паролем, що робить його більш безпечним, ніж PAP;

- EAP (Extensible Authentication Protocol) – найбільш гнучкий метод, який дозволяє використовувати широкий спектр механізмів автентифікації.

Як зазначено в RFC 3579 [34], EAP підтримує:

- смарт-карти;

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

- одноразові паролі;
- сертифікати (наприклад, eap-tls);
- kerberos;
- біометрію та інші методи.

EAP дозволяє NAS діяти як “проксі”, передаючи EAP-пакети між клієнтом і сервером RADIUS, що дає змогу серверу обробляти складні методи автентифікації без необхідності їх реалізації на NAS.

Крім того, RADIUS може бути розширений для інтеграції з іншими системами автентифікації, такими як LDAP, Active Directory чи SQL-дані бази, що робить його придатним для складних мережових середовищ [48].

Нижче наведено табл. 1.1, яка містить короткий опис методів автентифікації.

Таблиця 1.1

Порівняння методів автентифікації

Метод	Опис	Рівень безпеки	Приклади використання
PAP	Передача пароля у відкритому вигляді	Низький	Прості сценарії, базова автентифікація
CHAP	Виклик-відповідь, шифрування пароля	Середній	Безпечніший доступ до мережі
EAP	Гнучкий, підтримує смарт-карти, сертифікати	Високий	Корпоративні мережі, VPN, Wi-Fi

1.3. Вимоги до підсистем автентифікації для корпоративних мереж

Функціональні вимоги

Ці вимоги охоплюють автентифікацію, авторизацію, облік, інтеграцію з іншими системами, централізоване управління, сумісність із мережевою інфраструктурою. Нижче наведено детальний аналіз цих вимог.

Сучасні організації потребують гнучкості у виборі методів автентифікації для різних сценаріїв, таких як доступ до Wi-Fi, VPN або корпоративних ресурсів.

Підсистема повинна підтримувати:

- PAP [44];
- CHAP [44];
- EAP – гнучкий протокол, який підтримує розширені методи, такі як:
 - EAP-TLS – використовує сертифікати для безпечних середовищ [46];
 - EAP-TTLS/PEAP: тунельовані методи захисту даних [37][41];
 - EAP-SIM/АКА: аутентифікації в мобільних мережах [26][45];
 - LEAP – легкий протокол для бездротових мереж від Cisco [4].
- MFA – поєднання кількох факторів входу, таких як пароль і код із мобільного додатка, для підвищення безпеки, особливо для віддалених працівників [12];
- OTP [38].

Така різноманітність дозволяє адаптувати підсистему до потреб організації, забезпечуючи як прості, так і безпечні методи аутентифікації.

Після аутентифікації підсистема повинна визначати права доступу користувачів на основі їхніх ролей або політик. При цьому потрібне точне керування доступом, що є критичним для безпеки та ефективності, для цього повинно бути забезпечене наступне:

- призначення ролей користувачам;
- використання атрибутів RADIUS, таких як Service-Type, Framed-IP-Address чи Filter-Id, для визначення доступу до VLAN, IP-адрес чи груп користувачів [44];
- підтримка стандарту IEEE 802.1X [47], для контролю доступу на основі портів;

Облік дозволяє відстежувати активності користувачів для аудиту, білінгу чи аналізу безпеки.

А саме вимоги зі сторони обліку до підсистеми такі:

- журналювання даних та подій [43];

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

- підтримка типів записів Accounting-Start, Accounting-Stop, Interim-Update для відстеження проміжних оновлень сеансів [43];
- можливість інтеграції до зовнішніх систем (білінг або аналітика) задля передачі даних обліку [17];
- наявність політик обліку, наприклад, періодичність Interim-Update [43].

Для ефективної роботи підсистема має інтегруватися з:

- каталогами користувачів (AD, LDAP) [17];
- різними мережевими пристроями;
- серверами DHCP (інтегрована можливість) [27];
- системами моніторингу (Lucent/Ascend) [9].

Підсистема повинна забезпечувати єдину точку керування для аутентифікації, авторизації та обліку.

Підтримка Single Sign-On (SSO) дозволяє користувачам аутентифікуватися один раз для доступу до кількох систем, що підвищує зручність [2]. Наприклад, після входу до мережі користувач може отримати доступ до навчальних порталів чи VPN без повторної аутентифікації.

Підсистема повинна бути сумісною з:

- різними сучасними пристроями, такі як Cisco, Mikrotik, Juniper для роботи в гетерогенних мережах [9];
- операційними системами Linux та Windows для гнучкого розгортання;
- конфігураціями VLAN, DHCP, VPN для адаптації до різних топологій.

Підсистема повинна надавати інструменти для:

- створення та управління групами користувачів і профілями;
- налаштування атрибутів доступу, таких як рівні привілеїв.

Безпекові вимоги

Безпекові вимоги є основою для створення надійних підсистем аутентифікації, які захищають мережі організацій від кіберзагроз. Буде проаналізовано шифрування, MFA, стійкість від кібератак та додаткові аспекти пов'язані з безпекою.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Шифрування є критично важливим для захисту даних, що передаються між Network Access Server (NAS) і сервером RADIUS. Буде розглянуто вимоги, щодо забезпечення шифрування.

Використання протоколу RadSec, описаного в RFC 6614, забезпечує шифрування на транспортному рівні, усуваючи вразливості UDP, який не має вбудованого шифрування. Це запобігає перехопленню паролів чи інших чутливих даних [50].

Атрибут User-Password шифрується за допомогою MD5-хешування та спільного секрету, як описано в RFC 2865. Однак MD5 вважається застарілим через вразливості до атак із колізіями, тому рекомендується використовувати сучасніші алгоритми, такі як SHA-256 [26][27].

Для управління пристроями та передачі даних рекомендується використовувати IPSec або SSHv2, що забезпечують шифрування на рівні застосунків [20].

Багатофакторна аутентифікація є гарною практикою для підвищення безпеки, особливо в умовах зростання віддаленої роботи та складних атак.

MFA включає щось, що користувач знає (пароль), має (токен чи смарт-карта) і є (біометричні дані, наприклад відбитки пальців). Дослідження показують, що MFA значно знижує ризик несанкціонованого доступу [49].

До MFA можна віднести використання EAP-TLS, яке базується на сертифікатах, є безпековим методом, рекомендованим для корпоративних мереж [34].

Варто додати, що біометричні методи, такі як розпізнавання обличчя чи відбитків пальців, стають популярними, через зручність та безпеку [18].

Підсистема аутентифікації повинна бути стійкою до різноманітних кіберзагроз.

Для цього, підсистема повинна притримуватися наступних рекомендацій:

- обов'язкове використання атрибута Message-Authenticator, описаного

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

в RFC 3579 [34], забезпечує перевірку цілісності повідомлень, що запобігає атакам, таким як Blast-RADIUS [26][27];

- унікальні Request Authenticator, як зазначено в RFC 2865 [44], запобігають повторному використанню пакетів;
- TLS забезпечує взаємну аутентифікацію між клієнтом і сервером, що знижує ризик перехоплення (MITM) [5].

Сучасні загрози, такі як атаки на основі штучного інтелекту чи IoT-пристрої, вимагають додаткових заходів:

- використання AI для виявлення аномалій у поведінці користувачів [32];
- урахування обмежених ресурсів IoT-пристроїв при реалізації аутентифікації [20];
- впровадження MFA та навчання користувачів для захисту від фішингу [33].

Відповідність стандартам

Сучасні підсистеми аутентифікації, побудовані на базі протоколу RADIUS, такі як TekRADIUS і FreeRADIUS, повинні відповідати міжнародним стандартам і рекомендаціям, щоб забезпечити безпеку, взаємодію та відповідність регуляторним вимогам. Ці стандарти охоплюють технічні специфікації протоколу, рекомендації щодо безпеки та галузеві регуляції. Нижче наведено детальний аналіз ключових стандартів, які є обов'язковими для таких систем.

IETF (Internet Engineering Task Force) розробила основні стандарти для протоколу RADIUS, які є фундаментом для будь-якої підсистеми аутентифікації.

Стандарт RFC 2865: Remote Authentication Dial In User Service – визначає протокол RADIUS для аутентифікації та авторизації. Він включає вимоги до структури пакетів та атрибутів. Він також встановлює використання спільного секрету для захисту даних і MD5-хешування для приховування паролів [44].

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

RFC 2866: Radius Accounting – доповнює попередній стандарт, визначаючи механізми обліку, які дозволяють журналювати дії користувачів, такі як тривалість сеансів і обсяг переданих даних. Це критично для аудиту та аналізу безпеки [43].

RFC 6614: TLS Encryption for RADIUS – вводить RadSec, який забезпечує шифрування трафіку RADIUS за допомогою TLS, усуваючи вразливості UDP, такі як перехоплення даних [50].

RFC 3579: RADIUS Support for EAP – описує інтеграцію EAP у RADIUS, що дозволяє використовувати розширені методи аутентифікації, такі як EAP-TLS, EAP-TTLS і EAP-PEAP, для підвищення безпеки [34].

RFC 5216: EAP-TLS – визначає метод EAP-TLS, який використовує сертифікати для аутентифікації, що є безпечним рішенням для корпоративних мереж [46].

Ці стандарти забезпечують технічну основу, гарантуючи сумісність із мережевими пристроями та безпечну передачу даних.

IEEE (The Institute of Electrical and Electronics Engineers) є важливими для підсистем аутентифікації, особливо в контексті контролю доступу до мережі.

IEEE 802.1X – стандарт для контролю доступу на основі портів (PNAC), який використовує RADIUS як сервер аутентифікації. IEEE 802.1X забезпечує аутентифікацію пристроїв перед наданням доступу до локальних або бездротових мереж, що є стандартом для корпоративних середовищ. Він використовує EAP over LAN (EAPOL) для передачі даних аутентифікації між клієнтом (supplicant), аутентифікатором (наприклад, комутатором) і сервером аутентифікації [47]. Цей стандарт є критично важливим для захисту від несанкціонованого доступу, наприклад, атак типу “додавання апаратного забезпечення”.

NIST (National Institute of Standards and Technology) надає рекомендації для цифрової аутентифікації, які є актуальними для сучасних організацій.

NIST SP 800-63B. Digital Identity Guidelines – документ містить рекомендації щодо електронної аутентифікації, включаючи використання

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

багатофакторної аутентифікації (MFA), захист від атак типу "людина посередині" та вимоги до шифрування. Він підкреслює важливість використання сильних методів аутентифікації, таких як сертифікати чи біометричні дані, що може бути реалізовано через EAP у RADIUS [12].

ISO (International Organization for Standardization) та IEC (International Electrotechnical Commission) розробили стандарти для управління інформаційною безпекою.

ISO/IEC 27001: Information Security Management – стандарт визначає вимоги до систем управління інформаційною безпекою (ISMS), включаючи контроль доступу та аутентифікацію. Підсистема аутентифікації повинна відповідати ISO/IEC 27001, щоб забезпечити систематичне управління ризиками безпеки, наприклад, через журналювання та аудит [30].

Залежно від галузі діяльності організації, підсистема аутентифікації може потребувати відповідності специфічним регуляційним документам.

GDPR (General Data Protection Regulation) – регламент Європейського Союзу для захисту персональних даних, яка вимагає безпечного зберігання та обробки даних користувачів, включаючи дані аутентифікації [1].

HIPAA (Health Insurance Portability and Accountability Act) – регламент США для захисту медичних даних, яка включає вимоги до аутентифікації для доступу до чутливої інформації [13].

PCI DSS (Payment Card Industry Data Security Standard) – стандарт для захисту даних платіжних карток, який вимагає використання сильних методів аутентифікації та шифрування [42].

Продуктивні вимоги

Продуктивні вимоги є важливими для забезпечення безперебійного доступу до мережевих ресурсів, особливо в умовах великої кількості користувачів і високих навантажень. Для систем, побудованих на базі протоколу RADIUS ці вимоги охоплюють масштабованість, швидкість обробки запитів, надійність, ефективне використання ресурсів.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Масштабованість є ключовою вимогою для підсистем аутентифікації, оскільки сучасні організації можуть мати від сотень до десятків мільйонів користувачів, які одночасно потребують доступу до мережі. Основні вимоги масштабованості включають в себе наступне:

- система повинна бути здатною обробляти від кількох запитів на секунду до десятків тисяч [8];
- система має ефективно працювати в мережах із сотнями тисяч чи навіть мільйонами користувачів [23][38];
- підсистема повинна підтримувати розподілену обробку запитів через проксі, балансування навантаження та резервне копіювання [40];
- система має дозволяти налаштування для адаптації до різних рівнів навантаження, як приклад таймери “watchdog” та конфігурація Primary/Secondary Failover [31].

Швидкість обробки запитів є важливою для зручності користувачів і продуктивності мережі, особливо під час пікових навантажень, тому для забезпечення швидкодії потрібно, щоб:

- система повинна обробляти запити аутентифікації за мілісекунди, щоб уникнути затримок, які можуть вплинути на користувацький досвід [8];
- система має забезпечувати високу пропускну здатність для обробки великої кількості запитів [23][38];
- використання UDP як транспортного протоколу, як визначено в RFC 2865 [44], забезпечує швидку передачу даних, хоча може вимагати додаткових механізмів для забезпечення надійності.

Надійність потрібна для забезпечення безперервної роботи підсистеми аутентифікації, особливо в організаціях, де простої можуть призвести до значних втрат.

- система повинна мати мінімальний час простою, що досягається через використання резервних серверів і механізмів автоматичного переключення [8];

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

- підсистема має бути стійкою до збоїв апаратного забезпечення, програмного забезпечення чи мережесих з'єднань. Наприклад, RELIANOID підтримує конфігурації високої доступності для RADIUS, що включають розподіл повідомлень між декількома серверами [24];

- регулярні перевірки стану серверів, такі як “check_radius” у RELIANOID, дозволяють швидко виявляти проблеми та забезпечувати стабільну роботу системи. Ці перевірки включають параметри, як-от кількість повторних спроб і тайм-аут, для оцінки продуктивності сервера [24].

Ефективне використання ресурсів досить важливе для зниження витрат і забезпечення стабільної роботи системи на стандартному апаратному забезпеченні. Для цього потрібно притримуватись наступних правил:

- система повинна бути оптимізована для роботи на звичайному обладнанні без надмірного споживання ресурсів [35];

- використання UDP зменшує навантаження на мережу, але для безпеки може бути потрібен RadSec, який додає шифрування, що потребує до-даткових ресурсів [50].

- вибір бази даних суттєво впливає на продуктивність, особливо для функцій обліку. Наприклад, кожне повідомлення обліку може генерувати кілька запитів на запис до бази даних, що обмежує пропускну здатність до кількох сотень чи тисяч записів на секунду [35]. Рекомендується використовувати швидкі бази даних, такі як SQL із пам'ятними таблицями, для зменшення затримок [23].

1.4. Безпека протоколу RADIUS

Структура пакетів RADIUS та процес аутентифікації

Для розуміння моделі безпеки буде проаналізовано структуру пакетів. Згідно з RFC 2865, пакети RADIUS є основою для обміну даними між Network Access Server (NAS) та сервером RADIUS [44]. Структура пакету включає наступні компоненти [44]:

- код – 1 октет, який визначає тип пакету, приклад значень:

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

- 1: Access-Request (запит на доступ);
- 2: Access-Accept (доступ дозволено);
- 3: Access-Reject (доступ відхилено);
- 4: Accounting-Request (запит на облік);
- 5: Accounting-Response (відповідь на облік);
- 11: Access-Challenge (запит на додаткову автентифікацію);
- 255: Reserved (зарезервовано).

- ідентифікатор – 1 октет, який використовується для зв'язування запитів і відповідей. Кожен запит має унікальний ідентифікатор, який повторюється у відповіді, що дозволяє NAS ідентифікувати, до якого запиту належить відповідь;

- довжина – 2 октети, які вказують загальну довжину пакету, включаючи заголовок (20 октетів) та атрибути. Це поле забезпечує правильне розпізнавання кінця пакету;

- аутентифікатор – 16 октетів, які є ключовим елементом безпеки, тому що:

- у запитах (наприклад, Access-Request) це випадкове число, відоме як Request Authenticator, яке генерується NAS для забезпечення унікальності запиту та захисту від повторних атак;

- у відповідях (наприклад, Access-Accept, Access-Reject) це Response Authenticator, який є хешем, розрахованим на основі спільного секрету, Request Authenticator і вмісту пакета.

- атрибути – змінної довжини, містять інформацію про користувача та налаштування, наприклад:

- User-Name (ім'я користувача);
- User-Password (пароль користувача, зашифрований);
- NAS-IP-Address (IP-адреса NAS);
- NAS-Port (порт NAS);
- Service-Type (тип послуги);
- Framed-IP-Address (IP-адреса для користувача).

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Атрибути мають формат Type-Length-Value (TLV), де Type – ідентифікатор атрибута, Length – довжина значення, а Value – саме значення. Це дозволяє гнучко розширювати функціональність протоколу.

Вигляд структури наведено на рис. 1.3 [22], а структура атрибутів зображена на рис. 1.4 [44].

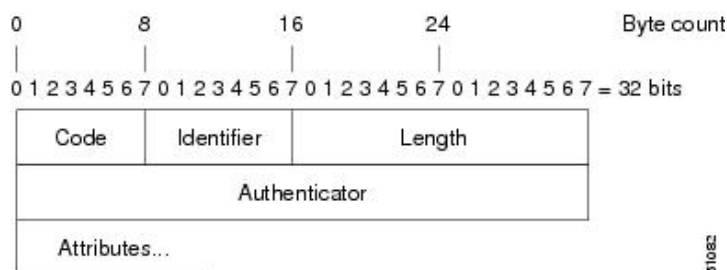


Рисунок 1.3 – Структура пакету RADIUS

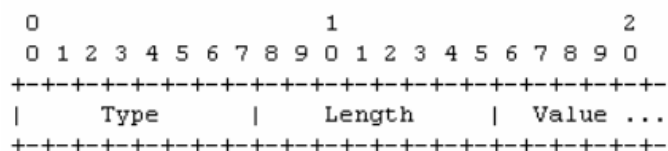


Рисунок 1.4 – Структура атрибутів

Пакети RADIUS відіграють ключову роль у процесі аутентифікації, який включає такі кроки [44]:

1. Надсилання Access-Request – NAS формує цей пакет, що надсилається до сервера по протоколу UDP, який містить:

a. Атрибути User-Name і User-Password (пароль зашифрований за допомогою спільного секрету та MD5).

b. Request Authenticator – випадкове 16-октетне число, яке забезпечує унікальність запиту та допомагає захистити від повторних атак.

2. Обробка сервером RADIUS – він отримує пакет, перевіряє Request Authenticator і використовує спільний секрет для розшифрування пароля. Після цього він шукає користувача в базі даних (наприклад, у файлі користувачів або через LDAP) і перевіряє автентичність. Якщо аутентифікація успішна, сервер формує пакет Access-Accept, якщо ні – Access-Reject. У деяких випадках може бути відправлено Access-Challenge для додаткової автентифікації (наприклад, введення PIN-коду).

3. Надсилання відповіді – сервер формує відповідь, яка містить Response Authenticator:

NAS отримує відповідь, перевіряє Response Authenticator, використовуючи свій спільний секрет і оригінальний Request Authenticator, щоб переконатися, що відповідь автентична.

Цей процес забезпечує, що лише авторизовані користувачі отримують доступ до мережесих ресурсів, а пакети не були змінені під час передачі.

Модель безпеки RADIUS.

Як описано в RFC 2865 [44], модель базується на трьох ключових механізмах, які тісно пов'язані зі структурою пакетів:

1. Спільний секрет (Shared Secret).

Між клієнтом (NAS) і сервером RADIUS встановлюється спільний секрет, який використовується для аутентифікації повідомлень. Цей секрет ніколи не передається через мережу, що забезпечує автентичність та цілісність обміну даними [7, розділ 3]. Спільний секрет є основою для усіх криптографічних операцій, таких як захист паролів і аутентифікація пакетів. Він має бути щонайменше 16 октетів і не піддаватися вгадуванню, щоб захистити від атак методом повного перебору [7, сторінка 16].

2. MD5-хешування.

Алгоритм MD5 використовується для захисту паролів та аутентифікації повідомлень. Наприклад, атрибут User-Password (який містить пароль) шифрується шляхом операції XOR з Request Authenticator і хешується з використанням спільного секрету [7, розділ 5.2]. Це забезпечує, що навіть якщо пакет перехоплено, пароль не може бути легко відновлено без знання спільного секрету.

Однак варто зазначити, що використання MD5 з часом стало вважатися менш надійним через його вразливості [26][27], що підкреслює необхідність додаткових механізмів безпеки.

3. Автентифікатори (Authenticators).

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

У пакеті Access-Request включається 16-октетне випадкове число, відоме як Request Authenticator. Воно використовується для захисту від повторних атак (replay attacks) та для приховування паролю [7, розділ 3]. Це випадкове число має бути непередбачуваним і унікальним протягом терміну дії спільного секрету, щоб запобігти повторним атакам.

У відповідях сервера (Access-Accept, Access-Reject, Access-Challenge) поле Authenticator містить MD5-хеш, що було розглянуто в попередньому пункті. Це дозволяє клієнту перевірити автентичність відповіді від сервера [7, розділ 3]. Цей механізм забезпечує, що відповідь дійсно походить від авторизованого сервера.

Хоча розглянуті механізми забезпечують базовий рівень безпеки, вони мають певні вразливості:

- використання UDP як транспортного протоколу робить RADIUS вразливим до атак на рівні транспорту, оскільки UDP не забезпечує шифрування [26][27];
- відсутність шифрування від кінця до кінця означає, що якщо задіяні проксі-сервера, дані можуть бути виявлені на кожному етапі, що створює ризики, особливо при використанні кількох проксі-серверів [14];
- нещодавнє дослідження, представлене на конференції USENIX Security 2024, має назву “RADIUS/UDP Considered Harmful”, де автори, включаючи дослідників з Cloudflare, Centrum Wiskunde & Informatica, BastionZero і Microsoft Research, зазначають, що RADIUS отримав мало формального аналізу безпеки в академічних колах, попри його широке використання [11]. Стаття описує можливість атак MITM (man-in-the-middle), коли злоумисник може підробити повідомлення про прийняття протоколу у відповідь на фальшивий запит входу, а також вразливості, пов’язані з використанням UDP, такі як атака Blast-RADIUS, вона представлена на рис. 1.5, яка може призвести до відмови в обслуговуванні або несанкціонованого доступу.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

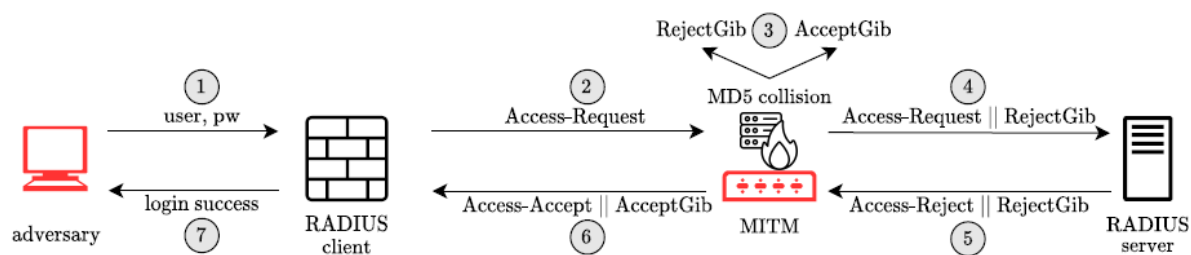


Рисунок 1.5 – Атака Blast-RADIUS

Для покращення безпеки, тобто вирішення попередньо розглянутих проблем – можна використовувати розширення, такі як:

- RADIUS over TLS (RadSec), описане у RFC 6614, яке забезпечує шифрування на рівні транспорту, усуваючи вразливості, пов’язані з UDP [50];
- атрибут Message-Authenticator, використовуючи аутентифікацію на основі EAP, який додає додаткову перевірку цілісності повідомлень [34];

1.5. Аналіз існуючих рішень RADIUS-серверів

Порівняння серверів FreeRADIUS та TekRADIUS: функціонал, ліцензійні умови, сумісність

FreeRADIUS є одним із найпопулярніших відкритих серверів RADIUS, який використовується провайдерами інтернет-послуг, телекомунікаційними компаніями та освітніми установами. Його ключові характеристики включають в себе [9]:

- високу розширюваність завдяки модульній архітектурі;
- підтримку всіх стандартних протоколів автентифікації, таких як PAP, CHAP, MS-CHAP, EAP (з підтримкою EAP-TLS, PEAP, EAP-TTLS тощо);
- інтеграцію з різними серверними частинами, включаючи LDAP, AD, SQL, а також звичайні текстові файли, що дозволяє централізоване управління користувачами;
- облік, який легко обробляти для білінгу та моніторингу пропускну здатності;
- використання в масштабах від малих бізнесів до великих мереж, здатних обробляти тисячі підключень за секунду;

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

- однак управління здійснюється через командний рядок, що вимагає технічних знань і може бути складним для початківців, особливо через об'ємну документацію.

TekRADIUS – розроблений компанією Kaplansoft, є сервером RADIUS, призначеним виключно для Windows. Його функціонал включає в себе [22][46]:

- графічний інтерфейс користувача (GUI), що значно полегшує управління для користувачів, які віддають перевагу візуальному підходу;
- підтримка методів аутентифікації, таких як в FreeRADIUS, а саме: PAP, CHAP, MS-CHAP v1-v2, EAP;
- вбудований DHCP-сервер, що є унікальною особливістю для управління IP-адресами;
- підтримку різних баз даних залежно від видання: Microsoft SQL Server, SQLite, MySQL, MariaDB, PostgreSQL, Oracle;
- додаткові функції, такі як проксі RADIUS-запитів, підтримка IPv6, OTP-аутентифікація (Google/Microsoft Authenticator), квоти на основі часу та обсягу даних, всі ці функції є платними, входять до версії Enterprise;
- платні версії (Enterprise, SP) пропонують розширені можливості, такі як: VoIP-білінг, Fair Usage Policy, деякі EAP, включаючи EAP-TLS, сповіщення через SMS/електронну пошту;
- однак, на відміну від FreeRADIUS, обмежений Windows-платформою, що може бути недоліком для користувачів Unix-подібних систем.

Нижче наведено таблицю, яка підсумовує ключовий функціонал серверів [22][23][46]:

Таблиця 1.2

Порівняння безкоштовного функціоналу серверів

Аспект	FreeRADIUS	TekRADIUS
Платформа	Загалом Unix-системи	Тільки Windows (Vista-11, Server 2008-2022)
Інтерфейс управління	Командний рядок	GUI

Порівняння безкоштовного функціоналу серверів

Аспект	FreeRADIUS	TekRADIUS
Підтримка протоколів автентифікації	PAP, CHAP, MS-CHAP, EAP, Digest	Такі ж самі, але більшість обмежено платною версією
Бази даних	LDAP, SQL, AD	SQL Server, SQLite, ODBC (MySQL, MariaDB, PostgreSQL та Oracle)
Масштабованість	Висока, широко використовується у великих мережах	Невеликі або середні мережі
Додаткові функції	Модульність, веб-інтерфейс	Вбудований DHCP

FreeRADIUS розповсюджується під ліцензією GNU GPLv2, що робить його повністю безкоштовним для використання, модифікації та розповсюдження [36]. Це відкрите програмне забезпечення, яке підтримується активною спільнотою, що забезпечує регулярні оновлення та підтримку [36]. Його можна знайти в репозиторіях більшості Linux-дистрибутивів або скомпілювати вручну. Комерційна підтримка від InkBridge Networks [36], але сам сервер залишається безкоштовним, що робить його привабливим для організацій, які прагнуть мінімізувати витрати.

TekRADIUS має комерційний підхід: базова версія доступна безкоштовно з обмеженим функціоналом, для розширених можливостей потрібні платні ліцензії.

Enterprise-версія коштує \$239 [28] і включає підтримку [39]: EAP-TLS, EAP-TTLS, EAP-SIM, LEAP, динамічне створення самопідписаних сертифікатів для сеансів PEAP, аутентифікацію NTLM для методів аутентифікації MS-CHAP, зіставлення атрибутів на основі регулярних виразів, аутентифікацію OTP.

SP-версія коштує \$579 [28] і додає функції [39]: VoIP-білінгу, підтримку IPv6, алфавітно-цифровий запис клієнта RADIUS, транспорт TLS сповіщення через SMS/електронну пошту, відправку пакету роз'єднання (PoD) або виконання визначеної користувачем команди завершення сеансу, коли користувач витрачає весь кредит.

FreeRADIUS в основному призначений для Unix-подібних систем, таких як Linux, BSD, і інших Unix-подібних ОС. Його можна знайти в репозиторіях більшості Linux-дистрибутивів, що полегшує встановлення. Хоча теоретично його можна скомпілювати для Windows, це не є стандартним сценарієм, і він більше підходить для серверів на базі Linux.

Сумісність з клієнтами включає підтримку Juniper, а також сценарії, такі як DSL, Wi-Fi, комутатори та маршрутизатори [9]. Використовується в системах із мільйонами користувачів і обробляє мільйони запитів щодня, що робить його ідеальним для великих організацій.

TekRADIUS розроблений виключно для Windows, тестується на версіях від Vista до серверів 2022 року [27]. Це робить його зручним для користувачів, які працюють у Windows-середовищі, але обмежує його використання в інших ОС.

Він підтримує інтеграцію з Active Directory, що полегшує управління в корпоративних мережах на базі Windows [27]. Сумісність з клієнтами аналогічна, оскільки обидва сервери реалізують стандарт RADIUS, але платформа Windows може бути перевагою для певних мереж. Підходить для малих і середніх організацій, але для великих систем може знадобитися комерційна версія для підвищення продуктивності.

З урахуванням вищенаведених характеристик доцільно провести узагальнене порівняння розглянутих серверів автентифікації за низкою ключових критеріїв. Це дозволяє візуалізувати функціональні відмінності між серверами. Узагальнені результати порівняння наведено в таблиці 1.3.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Переваги та недоліки серверів

Рішення	Переваги	Недоліки
FreeRADIUS	Відкритий вихідний код і безкоштовний	Крута крива навчання
	Модульність	Обмеження платформи для основної версії
	Підтримка кількох платформ	Документація може бути складною
	Масштабованість	Відсутність вбудованого GUI
	Регулярні оновлення	
	DHCP-сервер	
	Широка спільнота	
TekRADIUS	Простота використання (GUI)	Обмеження платформою Windows
	Стабільність на Windows	Не є відкритим вихідним кодом
	Вбудований DHCP-сервер	Вартість для розширених функцій
	Комерційна підтримка	Менша масштабованість

Висновки до першого розділу

У першому розділі викладено основні теоретичні засади підсистеми аутентифікації на базі протоколу RADIUS: розглянуто архітектуру AAA, структуру й механізми захисту пакетів RADIUS із застосуванням атрибутів “атрибут-довжина-значення” (Attribute–Length–Value), а також сучасні розширення для шифрування UDP-трафіку. Проведено аналіз відкритого сервера FreeRADIUS, що виявив його високу гнучкість завдяки модульній архітектурі, підтримці стандартних методів аутентифікації та інтеграції з різними сховищами облікових даних. Огляд TekRADIUS показав переваги графічного інтерфейсу й вбудованого DHCP-модуля для Windows-середовищ. Порівняння обох рішень підтвердило їх взаємне доповнення за функціональністю та умовами розгортання.

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА ОБҐРУНТУВАННЯ ВИБОРУ ДЛЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ

2.1. Модель загроз та модель порушника

Розробка моделі порушника

Модель порушника – це опис потенційних зловмисників, їхніх мотивів, можливостей і методів атак на систему. Вона є частиною ширшої практики моделювання загроз, яка допомагає зрозуміти, як захистити мережу організації.

Модель порушника є ключовим елементом аналізу безпеки, оскільки вона:

- визначає, хто може атакувати систему та які мають мотиви;
- описує можливості та методи зловмисників, що допомагає передбачити потенційні атаки;
- служить основою для моделі загроз, дозволяючи зв'язати загрози з конкретними порушниками;
- допомагає розробити ефективні заходи захисту, враховуючи специфіку зловмисників.

На відміну від моделі загроз, яка фокусується на ризиках для системи (наприклад, підробка, витік інформації), модель порушника зосереджена на характеристиках зловмисників і їхніх діях.

Модель порушника включає два основні типи зловмисників: зовнішні та внутрішні. Кожен тип має свої мотиви, можливості, методи та цілі:

1. Зовнішній порушник.

Особа або група, яка не має легітимного доступу до системи і намагається проникнути ззовні. Це можуть бути хакери, кіберзлочинці або зовнішні агенти, які прагнуть скомпрометувати мережу.

Можлива мотивація: зловживання привілеями, помста, фінансова вигода або несанкціонований доступ до обмежених ресурсів.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Цілі наступні:

- підвищення привілеїв до адміністративного рівня для повного контролю;
- маніпуляція даними в базі даних для приховування дій або отримання вигоди;
- несанкціонований доступ до чутливих ресурсів, таких як конфігураційні файли.

Рівні компетенції:

- знання мережевих протоколів, зокрема RADIUS, і методів експлуатації;
- вміння використовувати спеціалізовані інструменти, такі як wireshark або metasploit;
- навички соціальної інженерії для фішингових атак.

Ресурси:

- доступ до інтернету та обладнання для перехоплення трафіку;
- час для дослідження вразливостей;
- фінансові ресурси для придбання інструментів або інформації про систему.

Обмеженнями цього типу зловмисників є те, що в них відсутній легітимний доступ до системи, що вимагає складніших методів для проникнення.

Порушники використовують різні методи та техніки для досягнення своїх цілей.

Методи:

- MITM-атаки, що дозволяють перехоплювати трафік між клієнтом і NAS або між NAS і RADIUS-сервером для отримання облікових даних або маніпуляції даними;
- використання вразливостей, таких як Blast- RADIUS, для підробки відповідей аутентифікації;
- фішингові атаки для отримання облікових даних користувачів;

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

- атаки типу DoS для перевантаження NAS або RADIUS-серверів для порушення роботи системи.

Техніки:

- використання інструментів для аналізу мережевого трафіку;
- створення фальшивих веб-сторінок або використання фішингових поштових листів;
- використання скриптів для автоматизації атак;
- використання ботнетів для DDoS-атак.

2. Внутрішній зловмисник.

Особа або група з легітимним доступом до системи, яка зловживає привілеями для несанкціонованих дій. Це можуть бути співробітники, адміністратори або контрагенти.

Мотивацією цієї групи може бути: зловживання привілеями, помста, фінансова вигода або несанкціонований доступ до обмежених ресурсів.

Можливі цілі:

- підвищення привілеїв до адміністративного рівня для повного контролю;
- маніпуляція даними в базі даних для приховування дій або отримання вигоди;
- несанкціонований доступ до чутливих ресурсів, таких як конфігураційні файли.

Компетенції:

- знання внутрішньої конфігурації мережі, включаючи розташування серверів і баз даних;
- навички роботи з адміністративними інструментами для зміни конфігурації;
- розуміння процедур безпеки, що дозволяє обходити захист.

Ресурси:

- легітимний доступ до системи, наприклад, через робочу станцію або адміністративний інтерфейс;

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

- фізичний доступ до пристроїв у мережі;
- знання паролів, ключів або інших засобів аутентифікації.

Обмеженням може бути відсутність адміністративних привілеїв, що обмежує доступ до всіх компонентів системи.

Методи:

- видалення або зміна записів у журналах сесій для приховування дій;
- отримання доступу до облікових даних або інших чутливих даних в базах даних;
- модифікація налаштувань NAS або RADIUS-серверів для обходу захисту або підвищення привілеїв;
- використання знань про систему для обходу захисних механізмів або уникнення виявлення.

Техніки:

- використання адміністративних інструментів для зміни конфігураційних файлів;
- виконання sql-запитів для маніпуляції даними в базі даних;
- використання легітимного доступу для тестування вразливостей системи.

Потенційні цілі атаки для зовнішнього порушника:

- облікові дані користувачів, що потрібні для подальшого використання в інших атаках;
- встановлення контролю над NAS або серверами для маніпуляцій або шпигунства;
- порушення роботи мережі через DoS-атаки для створення хаосу або відволікання;
- отримання конфіденційної інформації для конкурентної вигоди.

Потенційні цілі атаки для внутрішнього порушника:

- отримання адміністративного доступу для повного контролю;
- зміна або видалення даних у базі даних для приховування дій;

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

- несанкціонований доступ: отримання доступу до чутливих ресурсів, таких як конфігураційні файли.

Розробка моделі загроз

Модель загроз – це систематизований підхід до ідентифікації, аналізу та оцінки потенційних загроз і вразливостей інформаційної системи, мережі чи програмного забезпечення.

При побудові моделі загроз використовується методологія STRIDE, рекомендована стандартами OWASP Threat Modeling і Microsoft SDL [49][50], а також враховуються специфічні вразливості протоколу RADIUS, такі як Blast-RADIUS (CVE-2024-3596) [11].

Для створення моделі загроз буде виконано наступні дії:

- описати компоненти системи, потоки даних та межі довіри;
- використати модель порушника для аналізу загроз;
- виявити та проаналізувати загрози, оцінити ризики;
- запровадити заходи захисту.

Підсистема аутентифікації включає в себе такі компоненти:

- користувацькі пристрої (клієнти), які підключаються до мережі;
- сервери доступу (NAS), що передають запити аутентифікації;
- RADIUS-сервери, які обробляють запити аутентифікації та авторизації;
- бази даних, де зберігаються облікові дані користувачів і журнали сесій.

Потоки даних наступні:

1. Клієнт надсилає облікові дані до NAS.
2. NAS формує Access-Request і надсилає його до RADIUS-сервера.
3. RADIUS-сервер звертається до бази даних для перевірки.
4. База даних повертає результат перевірки.
5. RADIUS-сервер надсилає NAS відповідь Access-Accept, Access-Reject або Access-Challenge.
6. NAS надає або забороняє доступ клієнту.

7. NAS надсилає Accounting-Request до RADIUS-сервер для журналювання сесії.

Межі довіри можна позначити так:

- між клієнтом і NAS, мережа може бути незахищеною (наприклад, відкритий wi-fi);
- між NAS і RADIUS-сервером, можливі атаки типу “людина посередині” (MITM);
- між RADIUS-сервером і базою даних – внутрішній зв’язок, але можливі загрози від внутрішніх порушників.

Для аналізу загроз використано методологію STRIDE, яка включає шість категорій: Spoofing (Підробка), Tampering (Маніпуляція), Repudiation (Відмова від дій), Information Disclosure (Витік інформації), Denial of Service (Відмова в обслуговуванні), Elevation of Privilege (Підвищення привілеїв).

На таблиці А.1 наведено загрози для ключових компонентів і потоків даних.

Оцінка ризиків базується на якісній шкалі. Якісна оцінка ризиків – це підхід, який базується на описовому аналізі потенційних загроз, вразливостей та наслідків для системи, а не на точних числових вимірах. Цей метод орієнтується на експертну оцінку шляхом класифікації ризиків за категоріями, наприклад, як “низький”, “середній” чи “високий” ризик, залежно від ймовірності виникнення загрози та потенційного впливу/наслідків на бізнес чи інфраструктуру.

Ймовірність може бути:

- висока – легко реалізується через відомі вразливості або прості методи;
- середня – вимагає певних ресурсів, знань або умов;
- низька – складно реалізувати через високі вимоги до ресурсів чи навичок.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

Наслідки наступні:

- високі – серйозні порушення, такі як несанкціонований доступ, втрата конфіденційності чи цілісності;
- середні – помірні порушення, такі як тимчасові збої або часткова втрата даних;
- низькі – незначні незручності, такі як короткочасні перебої.

Таблиця 2.1

Матриця якісного аналізу

Ймовірність\Наслідки	Низькі	Середні	Високі
Висока	Середня	Високий	Високий
Середня	Низький	Середні	Високий
Низька	Низький	Низький	Середній

Нижче наведено детальну оцінку ризиків для всіх загроз (див. табл. А.2 та табл. 2.2), ідентифікованих у моделі загроз, згрупованих за компонентами та потоками даних. Кожна загроза оцінюється за ймовірністю, наслідками, ризиком, залишковим ризиком та заходами захисту.

Таблиця 2.2

Загрози потокам даних

Компонент	Тип загрози	Ймовірність	Наслідки	Ризик	Залишковий ризик	Захід захист
Клієнт → NAS	Підrobка	Середня	Високі	Високий	Середній	802.1X з EAP-TLS
	Маніпуляція	Низька	Середні	Середній	Низький	802.1X з EAP-TLS
	Витік інформації	Низька	Середні	Середній	Низький	802.1X з EAP-TLS
	Відмова в обслуговуванні	Середня	Середні	Середній	Низький	Storm control, обмеження швидкості
NAS → Клієнт	Підrobка	Низька	Високі	Середній	Низький	802.1X з EAP-TLS
	Маніпуляція	Низька	Середні	Середній	Низький	802.1X з EAP-TLS

Загрози потокам даних

Компонент	Тип загрози	Ймовірність	Наслідки	Ризик	Залишковий ризик	Захід захист
NAS → RADIUS	Підrobка	Висока	Високі	Високий	Середній	RadSec, Message-Authenticator
	Маніпуляція	Середня	Високі	Високий	Низький	RadSec
	Витік інформації	Середня	Високі	Високий	Низький	RadSec
	Відмова в обслуговуванні	Середня	Високі	Високий	Середній	Обмеження швидкості запитів, налаштування firewall
RADIUS → NAS	Підrobка	Висока	Високі	Високий	Середній	RadSec, Message-Authenticator
	Маніпуляція	Середня	Високі	Високий	Низький	RadSec
	Відмова в обслуговуванні	Низька	Середні	Середній	Низький	Моніторинг, виявлення аномалій
RADIUS → База даних	Маніпуляція	Низька	Високі	Середній	Низький	SSL/TLS
	Витік інформації	Низька	Високі	Середній	Низький	SSL/TLS
База даних → RADIUS	Підrobка	Низька	Високі	Середній	Низький	SSL/TLS, перевірка автентичності
	Маніпуляція	Низька	Високі	Середній	Низький	SSL/TLS
	Витік інформації	Низька	Високі	Середній	Низький	SSL/TLS

Обґрунтування оцінки:

- висока ймовірність через відому вразливість Blast-RADIUS, високі наслідки через несанкціонований доступ. З RadSec і Message-Authenticator ризик знижується до середнього;

- маніпуляція даними в базі даних дорівнює середній ймовірності через внутрішні загрози, високі наслідки через втрату цілісності. З RBAC і шифруванням ризик стає низьким;
- відмова від дій – низька ймовірність через стандартне журналювання, низькі наслідки. Захищене журналювання знижує ризик до мінімуму.
- витік інформації (Клієнт → NAS) – низька ймовірність через 802.1X, середні наслідки через компрометацію даних. З шифруванням ризик стає низьким;
- відмова в обслуговуванні (RADIUS-сервер) – середня ймовірність через DoS, високі наслідки через зупинку аутентифікації. Обмеження запитів знижують ризик до середнього;
- підвищення привілеїв (NAS) – середня ймовірність через внутрішні загрози, високі наслідки через контроль. Сильна аутентифікація знижує ризик до низького.

Більшість загроз мають високий ризик без захисту, але з рекомендованими заходами захисту, такими як RadSec, 802.1X з EAP-TLS, RBAC і обмеження запитів, залишковий ризик знижується до середнього або низького рівня. Ця матриця допомагає пріоритизувати заходи захисту для забезпечення безпеки системи аутентифікації.

Всі попередньо проаналізовані загрози, компоненти та зв'язки буде представлено у вигляді моделі загроз, яку було побудовано за допомогою OWASP Threat Dragon, що проілюстровано на рис. Б.1.

2.2. Топологія мережі

Було розроблено уявний план першого поверху вищого навчального закладу (див. рис. 2.2), на якому можна побачити такі місця як: Wi-Fi Guest – гостьова зона з точкою доступу; Just RM – звичайна кімната/аудиторія; Recr RM with Wi-Fi – зона відпочинку також з точкою доступу; Admin RM – приміщення адміністраторів; LAB1 ST (в подальшому LAB) – студентська лабораторна аудиторія; LAB2/LAB3 TC (в подальшому Staff_Room_1/2) – виклада-

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

цькі аудиторії.

На основі уявного плану навчального закладу побудовано схему мережі, яка зображена на рис. 2.3.

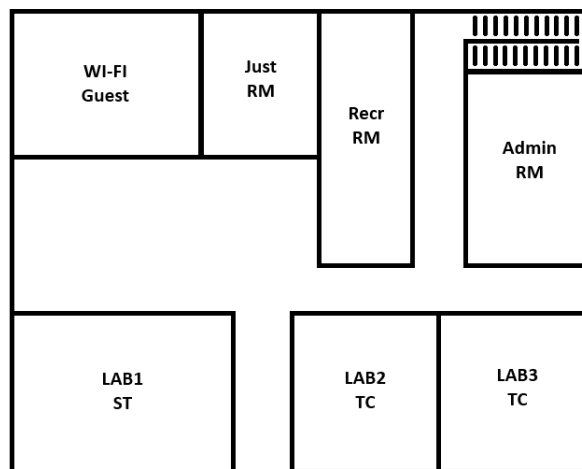


Рисунок 2.2 – План першого поверху вищого навчального закладу

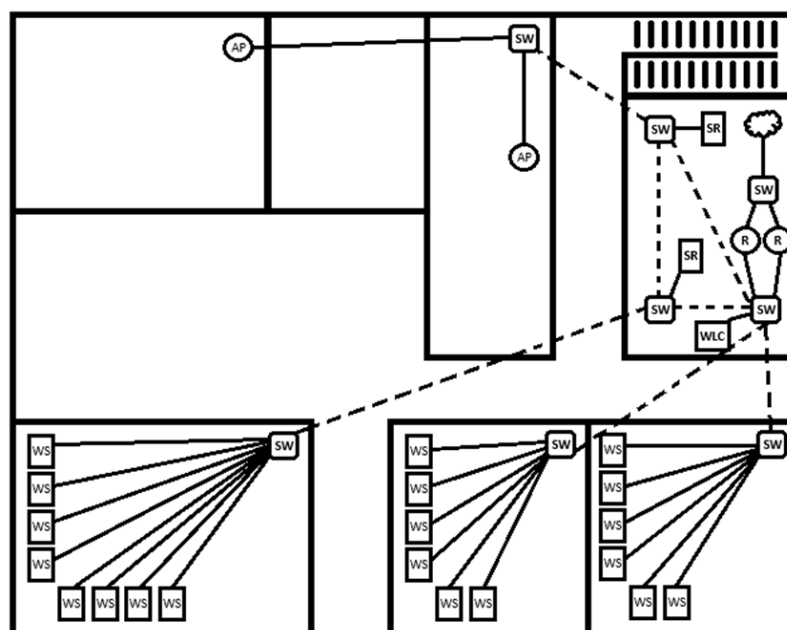


Рисунок 2.3 – Схема розміщення мережевих та кінцевих пристроїв на першому поверсі

При розробці та побудові топології мережі було додержано таких гарних практик як:

- сегментована мережа – мережу було поділено на сектори, що в подальшому будуть мати свій номер VLAN, для більш структурованої та безпечної роботи мережі;

- резервування та висока доступність – використання декількох комутаторів та маршрутизаторів забезпечує резервування та підвищує надійність мережі, зменшуючи ризик відмови одного з пристроїв;
- централізоване управління – топологія включає критичні пристрої, такі як маршрутизатори R1/R2 і підключення до хмари в зоні Admin_Room, що забезпечує централізоване управління мережевою інфраструктурою та адміністративними функціями;
- використання RADIUS-серверів – сервери для аутентифікації користувачів, підвищують безпеку та контроль доступу до мережевих ресурсів.
- масштабованість – можна легко масштабувати мережу шляхом додавання нових пристроїв або комутаторів без значних змін в архітектурі;
- висока продуктивність – розподіл мережі на окремі зони дозволяє оптимізувати продуктивність, зменшуючи ширококомовний трафік і забезпечуючи якісну роботу мережі.

Змодельована підсистема мережі, у емуляторі GNS3, представлена на рисунку 2.4.

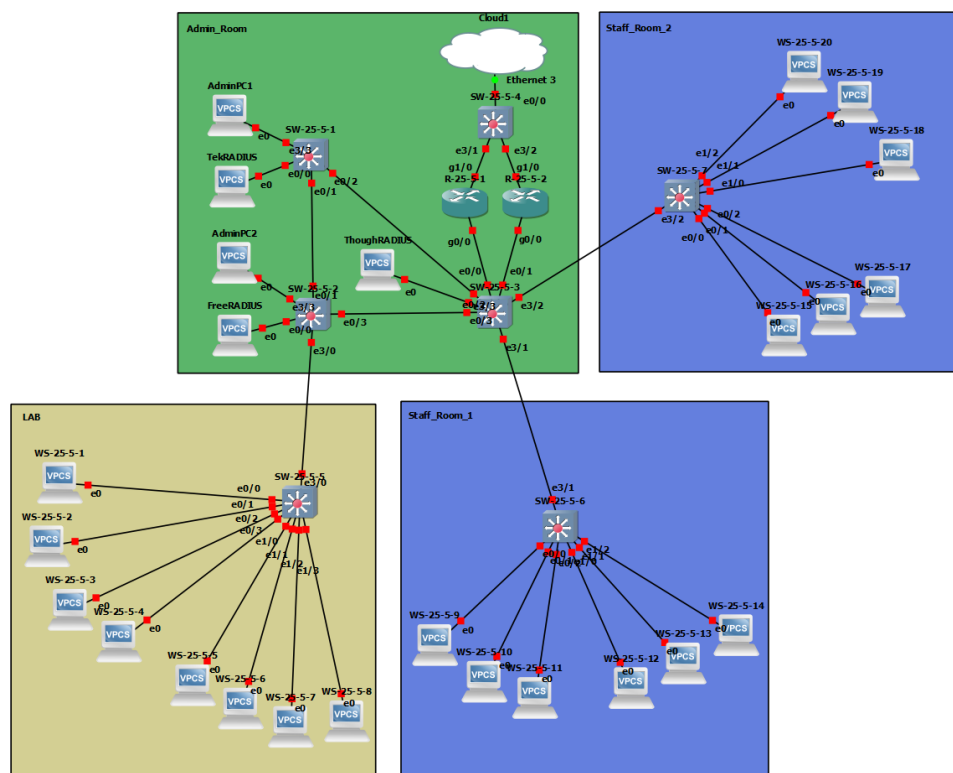


Рисунок 2.4 – Загальна топологія мережі

Мережа організації буде розроблена на базі RADIUS-серверів, таких як TekRADIUS та FreeRADIUS, включаючи також базові та безпекові налаштування. Самим головним в цьому проекті буде порівняння можливостей наведених раніше серверів.

Для того, щоб обрати оптимальні апаратні ресурси, потрібно звернути увагу на потреби нашої мережі, а саме, для комутаторів потрібна підтримка безпекових налаштувань, таких як: 802.1X з EAP-TLS, Radius, RadSec, Storm Control, Vlan, ACL, а також враховуючи топологію повинна бути підтримка RSTP для швидкого усунення петель мережевого трафіка.

З боку маршрутизаторів потрібна підтримка протоколів таких самих, як у комутаторів, і звісно, що деякі підтримуються та потрібні тільки для світлів, але повинен бути ще GLBP. А також саме головне це порти з високою пропускну здатністю (гігабітні), комутатори SW-1/2/3/4 також повинні мати високу пропускну здатність, іншим SW потрібна більша кількість портів (мегабітні) та хоча б 1 високошвидкісний порт.

Проаналізувавши вимоги мережі, було підібрано наступне мережеве обладнання:

Було обрано модель комутатора – Cisco C9200CX-8UXG-2XH-A на рівень ядра та дистрибуції, а саме як комутатори SW-1/2/3/4. Цей вибір є чудовим тому як, він має такі характеристики:

- підтримка всіх необхідних протоколів;
- 4 порти UPoE GE, 4 порти UPoE 10 GE, 2 порти з 10 GE SFP+ (uplink);
- підтримка IEEE 802.3bt (UPOE) з живленням до 240 Вт;
- без вентиляторів, що зменшує шум та знижує витрати на енергію;
- резервування живлення (HVDC/AC) для безперебійної роботи.

Переваги для рівня дистрибуції та ядра:

- висока пропускну здатність дозволяє обробляти значні обсяги трафіку, що важливо для рівня дистрибуції та ядра;
- підтримка функцій рівня 2 (L2) та рівня 3 (L3), що дозволяє виконувати різні задачі на рівні дистрибуції та ядра;

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

- підтримка MACsec-128/256 для забезпечення криптографічного забезпечення;

- підтримка SD-Access Fabric Edge Node, що полегшує управління мережею.

Для рівня доступу було обрано комутатор наступної моделі Cisco C9200L-24P-4G-A, бо він має такі характеристики:

- підтримка таких протоколів як 802.1X з EAP-TLS, Radius, RadSec, VLAN;

- 24 порти Ethernet PoE GE забезпечують достатню кількість портів для підключення кінцевих пристроїв у мережі;

- 4 порти GE Uplink для підключення до магістралі;

- оперативна пам'ять 2 ГБ, Flash 4 ГБ;

- Cisco IOS XE з підтримкою потокової телеметрії та API для автоматизації завдань (наприклад, моніторинг стану портів, налаштування QoS).

Переваги для рівня доступу:

- підтримка командного інтерфейсу (CLI) та графічного веб-інтерфейсу (GUI) дозволяє просто налаштовувати та керувати комутатором;

- підтримка Power over Ethernet (PoE) дозволяє підключати пристрої, такі як IP-телефони та бездротові точки доступу, без додаткових кабелів;

- підтримка різних функцій безпеки, що забезпечує захист мережі;

- висока надійність завдяки резервуванню живлення/вентиляторів та знижені витрати на енергію завдяки сертифікації ENERGY STAR.

Обґрунтування вибору маршрутизатора Cisco ISR4451-X-VSEC/K9:

- підтримка всіх головних протоколів третього рівня;

- наявність 2 портів PoE GE/SFP, 2 GE/SFP;

- 3 слоти для підключення додаткових модулів (NIM);

- пам'ять: 4 ГБ DRAM та 8 ГБ Flash.

Переваги для рівня ядра

- велика пропускна здатність дозволяє обробляти значні обсяги трафіку, що важливо для рівня ядра;

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

- підтримка NIM дозволяє розширювати функціональність маршрутизатора за рахунок додаткових модулів;
- підтримка криптографічних алгоритмів та функцій безпеки для захисту даних;
- легке управління через CLI та GUI, що полегшує налаштування та моніторинг.

2.3. Розробка схеми адресації мережі

Для розробки схеми адресації мережі розподіл адрес по діапазону буде проводитись таким чином, щоб використати оптимальну кількість IP-адрес, забезпечивши при цьому потреби підключених вузлів.

Розрахунок IP-адрес для підмереж наведений у таблицях 2.3. - 2.7.

Таблиця 2.3

Адресація підмережі Admin

Призначення	IP-адреса
Адреса мережі	191.25.5.0/28
Маска мережі	255.255.255.240
Інверсна маска	0.0.0.15
Мінімальна адреса	191.25.5.1
Максимальна адреса	191.25.5.14
Широкомовна адреса	191.25.5.15
Шлюз за замовчуванням	191.25.5.11
Діапазон використаних адрес	191.25.5.6 - 191.25.5.14, 191.25.5.2 - 191.25.5.3
Діапазон вільних адрес	191.25.5.1, 191.25.5.4 - 191.25.5.5

Таблиця 2.4

Адресація підмережі LAB

Призначення	IP-адреса
Адреса мережі	192.25.5.0/28
Маска мережі	255.255.255.240

Адресація підмережі LAB

Призначення	IP-адреса
Інверсна маска	0.0.0.15
Мінімальна адреса	192.25.5.1
Максимальна адреса	192.25.5.14
Широкомовна адреса	192.25.5.15
Шлюз за замовчуванням	192.25.5.12
Діапазон використаних адрес	192.25.5.10 - 192.25.5.12
Діапазон вільних адрес	192.25.5.1 - 192.25.5.9, 192.25.5.13 - 191.25.5.14

Таблиця 2.5

Адресація підмережі Staff1

Призначення	IP-адреса
Адреса мережі	193.25.5.0/28
Маска мережі	255.255.255.240
Інверсна маска	0.0.0.15
Мінімальна адреса	193.25.5.1
Максимальна адреса	193.25.5.14
Широкомовна адреса	193.25.5.15
Шлюз за замовчуванням	193.25.5.10
Діапазон використаних адрес	193.25.5.8 - 193.25.5.10
Діапазон вільних адрес	193.25.5.1 - 193.25.5.7, 193.25.5.11 - 193.25.5.14

Таблиця 2.6

Адресація підмережі Staff2

Призначення	IP-адреса
Адреса мережі	194.25.5.0/28
Маска мережі	255.255.255.240
Інверсна маска	0.0.0.15
Мінімальна адреса	194.25.5.1

Адресація підмережі Staff2

Призначення	IP-адреса
Шлюз за замовчуванням	194.25.5.10
Діапазон використаних адрес	194.25.5.8 - 194.25.5.10
Діапазон вільних адрес	194.25.5.1 - 194.25.5.7, 194.25.5.11 - 194.25.5.14

2.4 Відповідність підсистеми вимогам

Буде проаналізовано вимоги, що були визначені в першому розділі, тобто: функціональні, безпекові, нормативні та експлуатаційні. Кожне рішення аналізується за цими категоріями, щоб оцінити їх придатність для реалізації підсистеми.

Функціональні вимоги включають підтримку різних методів аутентифікації, авторизації, обліку, інтеграцію з системами, централізоване управління, SSO та сумісність із пристроями та операційними системами.

Аналіз рішення FreeRADIUS по функціональним вимогам:

- підтримує PAP, CHAP, MS-CHAP, EAP (EAP-TLS, PEAP, EAP-MS-CHAP v2, EAP-SIM, EAP-AKA), MFA та OTP, що відповідає вимогам гнучкості аутентифікації;
- забезпечує рольову авторизацію, використання атрибутів RADIUS (Service-Type, FramedIPAddress, Filter-Id) та підтримку IEEE 802.1X для контролю доступу на основі портів;
- підтримує облік Accounting-Start, Accounting-Stop, Interim-Update, інтеграцію з зовнішніми системами для білінгу та аналізу;
- сумісний з LDAP, Active Directory, MySQL, PostgreSQL, Oracle, DHCP-серверами та системами моніторингу;
- централізоване управління – надає командний рядок і веб-інтерфейс dialupadmin для управління;

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

- підтримує SSO для зручності користувачів;
- сумісність – працює з пристроями Cisco, Mikrotik, Juniper та операційними системами Linux, Windows, Unix;
- управління користувачами та групами – це надає інструменти для створення профілів і груп користувачів.

Серверу TekRADIUS відповідність вимогам наступна:

- у безкоштовній версії підтримує PAP, CHAP, MS-CHAP, EAP-MD5, MS-CHAP v2, але розширені методи, такі як EAP-TLS, OTP доступні лише в платних версіях;
- підтримує рольову авторизацію, атрибути RADIUS та IEEE 802.1X;
- облік – забезпечує журналювання сеансів, але є обмеження інтеграції з зовнішніми системами в безкоштовній версії;
- сумісний з SQL Server, SQLite, через ODBC: MySQL, MariaDB, PostgreSQL, Oracle та DHCP-серверами;
- централізоване управління – надає зручний Windows-інтерфейс для управління;
- підтримує SSO;
- працює з пристроями Cisco, Mikrotik, але обмежений платформою Windows;
- також надає інструменти для управління профілями та групами.

Безпекові вимоги включають шифрування даних, підтримку MFA та захист від кіберзагроз, таких як атаки типу MITM чи Blast-RADIUS.

Unix-орієнтоване рішення включає в себе:

- шифрування – підтримує RadSec (RFC 6614), TLS, IPSec для захисту даних між клієнтом і сервером;
- MFA – забезпечує підтримку EAP-TLS, PEAP, OTP, що відповідає вимогам до багатофакторної аутентифікації;
- захист від кіберзагроз – використовує Message-Authenticator (RFC 3579), унікальний Request Authenticator, TLS для взаємної аутентифікації, а також підтримує інтеграцію з AI для виявлення аномалій.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Рішення на базі Windows:

- підтримує RadSec (RFC 6614), але в платних версіях, в безкоштовній буде використано TLS-MD5;
- підтримує, але розширені методи MFA, такі як EAP-TLS, OTP доступні лише в платних версіях;
- використовує Message-Authenticator і TLS, але менш розвинутий у порівнянні з конкурентним сервером.

Нормативні вимоги передбачають відповідність стандартам IETF, IEEE, NIST, ISO/IEC, а також регламентам GDPR, HIPAA, PCI DSS, в залежності від специфіки підприємства.

FreeRADIUS відповідає стандартам IETF: RFC 2865, RFC 2866, RFC 2289, RFC 6614, RFC 3579, RFC 5281, IEEE 802.1X (RFC 3580).

TekRADIUS відповідає таким самим стандартам, що й попередньо розглянуте рішення, а також включає такі IETF: RFC 3162, RFC 4818, RFC 6911.

Стандарт ISO/IEC 27001 визначає вимоги до системи управління інформаційною безпекою і включає контроль доступу в додатку Annex A.9 Контроль доступу [34, сторінка 11]. Основні вимоги:

- політика контролю доступу (A.9.1.1);
- реєстрація та скасування доступу користувачів (A.9.2.1, A.9.2.6);
- управління привілейованим доступом (A.9.2.3);
- захист секретної інформації для аутентифікації (A.9.2.4);
- безпечні процедури входу (A.9.4.2).
- Відповідність вимогам наступна:
- використання RADIUS забезпечує контроль доступу та авторизацію, що відповідає політикам доступу;
- підтримка інтеграції з LDAP/AD та баз даних відповідає вимогам до реєстрації користувачів;
- підтримка MFA та шифрування відповідає вимогам до захисту секретної інформації, а також безпечного входу;

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

- централізоване управління та сегментація мережі сприяють управлінню доступом.

NIST SP 800-63B надає рекомендації щодо цифрової ідентифікації [12], зокрема аутентифікації, з трьома рівнями забезпечення безпеки (AAL1, AAL2, AAL3). Вимоги включають:

- AAL1 – однофакторна аутентифікація;
- AAL2 – двофакторна аутентифікація;
- AAL3 – багатофакторна аутентифікація з апаратними аутентифікаторами.

Реалізація цих вимог виконується в наступних прикладах:

- PAP/CHAP, відповідає базовим вимогам, тобто перший рівень;
- через MFA та OTP, відповідає другому рівню;
- використання EAP-TLS – третій рівень.

Так як регламенти HIPAA та PCI DSS потребують контролю та захисту за медичною інформацією та платіжних даних, які відсутні в проєкті, тому було вирішено розглянути лише регламент GDPR, що може бути корисним для цієї підсистеми.

GDPR регулює захист персональних даних громадян ЄС [1], з акцентом на:

- законність, прозорість та справедливість обробки;
- дані збираються для чітких цілей;
- мінімізація даних – збирати лише необхідні дані;
- точність, обмеження зберігання, цілісність та конфіденційність.

Опис системи вказує на часткову відповідність, а саме наявність шифрування забезпечує конфіденційність даних.

Проте є прогалини у мінімізації даних та процедурах згоди, як зазначено в документі.

Для дотримання хоча б мінімальної відповідності потрібно:

1. Забезпечити, щоб система збирала лише необхідні дані для аутентифі

фікації, наприклад, ідентифікатор користувача та пароль, без надмірної інформації.

2. Встановити чіткі процедури, щоб інформувати користувачів про обробку їх даних і отримувати явну згоду, наприклад, через інтерфейс для налаштувань.

3. Забезпечити механізми для реалізації прав, таких як доступ, виправлення чи видалення даних, відповідно до GDPR.

Експлуатаційні вимоги включають масштабованість, швидкість, надійність і ефективність використання ресурсів.

Щодо Unix-подібного рішення:

- використовується у Fortune 500, Tier 1 ISP, обробляє тисячі запитів на секунду, тобто від малих до великих мереж;
- обробка запитів у мілісекунди, залежить від бази даних, є інструменти моніторингу (radclient, radsniff) для мінімізації затримок;
- регулярні оновлення та підтримка, можливість використання резервних серверів, автоматичний failover;
- оптимізований для стандартного обладнання, використовує in-memory таблиці для обліку.

В свою чергу TekRADIUS:

- залежить від бази даних (є такі версії додатку LT (SQLite Edition) – невеликі мережі, OD (ODBC Edition) – середні мережі, звичайний TekRADIUS (Microsoft SQL Server Edition) – корпоративні рішення);
- оптимізовано під ОС Windows, працює як служба;
- присутнє журналювання та резервування серверу;
- продуктивність залежить від бази даних, інтеграція з AD/LDAP.

Висновки до другого розділу

У другому розділі побудовано модель порушника та загроз за методологією STRIDE, виконано якісний аналіз ризиків для кожного компонента та потоків даних, а також запропоновано захисні заходи, які знизили залишковий

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

ризик до середнього рівня. Розроблено топологію мережі з сегментацією через VLAN, механізмами резервування й централізованого управління, а також схему IP-адресації для підмереж. Обґрунтовано вибір мережевого обладнання зі стосовними характеристиками продуктивності та безпеки. Завершальний аналіз відповідності розробленої підсистеми функціональним, безпековим, нормативним і експлуатаційним вимогам засвідчив готовність до практичної реалізації.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

РОЗДІЛ 3. ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ МЕРЕЖІ

3.1. Налаштування мережі

Перед початком налагоджень та встановлення рішень варто розповісти про те, що було проведено аналіз образів пристроїв, що потрібні для розробки проєкту, в середовищі емуляції GNS3, а саме було знайдено маршрутизатор і комутатор, що підтримує налаштування сучасних методів захисту. Але при тестуванні, стало зрозуміло, що маршрутизатор на жаль використати не вдасться, бо він споживає досить великі ресурси системи, тому буде використано наявний образ маршрутизатора.

Буде налаштовано адресацію пристроїв, далі показано один приклад налаштування того чи іншого типу пристрою, всі інші налаштовані по аналогії.

Лістинг команд налаштування адресації маршрутизатора, паралельно з цим виконуються налаштування шлюзів VLAN, протоколу резервування та балансування навантаження GLBP та сервер DHCP:

```
R-25-5-2(config)#int gi 1/0
R-25-5-2(config-if)#description Connection to Cloud1
R-25-5-2(config-if)#ip address dhcp
R-25-5-2(config-if)#no shut
R-25-5-2(config-if)#ex
R-25-5-2(config)#int gi0/0.10
R-25-5-2(config-subif)#encapsulation dot1q 10
R-25-5-2(config-subif)#ip addr 191.25.5.10 255.255.255.240
R-25-5-2(config-subif)#glbp 10 ip 191.25.5.11
R-25-5-2(config-subif)#glbp 10 priority 90
R-25-5-2(config-subif)#glbp 10 preempt
R-25-5-2(config-subif)#ex
R-25-5-2(config)#int gi 0/0.20
R-25-5-2(config-subif)#encapsulation dot1q 20
```

```

R-25-5-2(config-subif)#ip addr 192.25.5.11 255.255.255.240
R-25-5-2(config-subif)#glbp 11 ip 192.25.5.12
R-25-5-2(config-subif)#glbp 11 priority 90
R-25-5-2(config-subif)#glbp 11 preempt
R-25-5-2(config-subif)#ex
R-25-5-2(config)#int gi 0/0.30
R-25-5-2(config-subif)#encapsulation dot1q 30
R-25-5-2(config-subif)#ip addr 193.25.5.9 255.255.255.240
R-25-5-2(config-subif)#glbp 12 ip 193.25.5.10
R-25-5-2(config-subif)#glbp 12 priority 90
R-25-5-2(config-subif)#glbp 12 preempt
R-25-5-2(config-subif)#ex
R-25-5-2(config)#int gi 0/0.40
R-25-5-2(config-subif)#encapsulation dot1q 40
R-25-5-2(config-subif)#ip addr 194.25.5.9 255.255.255.240
R-25-5-2(config-subif)#glbp 13 ip 194.25.5.10
R-25-5-2(config-subif)#glbp 13 priority 90
R-25-5-2(config-subif)#glbp 13 preempt
R-25-5-2(config-subif)#ex
Маршрутизація:
R-25-5-2(config)#ip route 0.0.0.0 0.0.0.0 dhcp
NAT:
R-25-5-2(config)#int gi 0/0
R-25-5-2(config-if)#ip nat inside
R-25-5-2(config-if)#ex
R-25-5-2(config)#int gi 1/0
R-25-5-2(config-if)#ip nat outside
R-25-5-2(config-if)#ex
R-25-5-2(config)#access-list 1 permit 191.25.5.0 0.0.0.15
R-25-5-2(config)#access-list 2 permit 192.25.5.0 0.0.0.15

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-25-5-2(config)#access-list 3 permit 193.25.5.0 0.0.0.15
R-25-5-2(config)#access-list 4 permit 194.25.5.0 0.0.0.15
R-25-5-2(config)#ip nat inside source list 1 int gi1/0 overload
R-25-5-2(config)#ip nat inside source list 2 int gi1/0 overload
R-25-5-2(config)#ip nat inside source list 3 int gi1/0 overload
R-25-5-2(config)#ip nat inside source list 4 int gi1/0 overload
DHCP:
R-25-5-1(config)#ip dhcp excluded-address 191.25.5.2 191.25.5.3
R-25-5-1(config)#ip dhcp excluded-address 191.25.5.6 191.25.5.14
R-25-5-1(config)#ip dhcp excluded-address 192.25.5.10 192.25.5.12
R-25-5-1(config)#ip dhcp excluded-address 193.25.5.8 193.25.5.10
R-25-5-1(config)#ip dhcp excluded-address 194.25.5.8 194.25.5.10
R-25-5-1(config)#ip dhcp pool Admin10
R-25-5-1(dhcp-config)#network 191.25.5.0 255.255.255.240
R-25-5-1(dhcp-config)#default-router 191.25.5.11
R-25-5-1(dhcp-config)#dns-server 1.1.1.1
R-25-5-1(dhcp-config)#domain-name Kulenko.net
R-25-5-1(dhcp-config)#lease 0 1 0
R-25-5-1(dhcp-config)#ex
R-25-5-1(config)#ip dhcp pool LAB20
R-25-5-1(dhcp-config)#network 192.25.5.0 255.255.255.240
R-25-5-1(dhcp-config)#default-router 192.25.5.12
R-25-5-1(dhcp-config)#dns-server 1.1.1.1
R-25-5-1(dhcp-config)#domain-name Kulenko.net
R-25-5-1(dhcp-config)#lease 0 1 0
R-25-5-1(dhcp-config)#ex
R-25-5-1(config)#ip dhcp pool Staff30
R-25-5-1(dhcp-config)#network 193.25.5.0 255.255.255.240
R-25-5-1(dhcp-config)#default-router 193.25.5.10
R-25-5-1(dhcp-config)#dns-server 1.1.1.1

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-25-5-1(dhcp-config)#domain-name Kulenko.net
R-25-5-1(dhcp-config)#lease 0 1 0
R-25-5-1(dhcp-config)#ex
R-25-5-1(config)#ip dhcp pool Staff40
R-25-5-1(dhcp-config)#network 194.25.5.0 255.255.255.240
R-25-5-1(dhcp-config)#default-router 194.25.5.10
R-25-5-1(dhcp-config)#dns-server 1.1.1.1
R-25-5-1(dhcp-config)#domain-name Kulenko.net
R-25-5-1(dhcp-config)#lease 0 1 0
R-25-5-1(dhcp-config)#ex

```

Протокол Spanning-Tree:

```

SW-25-5-3(config)#spanning-tree mode rapid-pvst
SW-25-5-3(config)#spanning-tree vlan 10 priority 4096
SW-25-5-3(config)#spanning-tree vlan 20 priority 4096
SW-25-5-3(config)#spanning-tree vlan 30 priority 4096
SW-25-5-3(config)#spanning-tree vlan 40 priority 4096
SW-25-5-3(config)#int eth3/3
SW-25-5-3(config-if)#spanning-tree portfast edge
SW-25-5-3(config-if)#exit
SW-25-5-3(config)#int range eth 3/2, eth 3/1, eth0/0, eth0/1
SW-25-5-3(config-if-range)#spanning-tree portfast edge trunk

```

Безпекові налаштування наведено далі, до них відноситься налаштування VLAN, ACL.

VLAN на рівні дистрибуції:

```

SW-25-5-3(config)#int vlan 10
SW-25-5-3(config-if)#ip addr 191.25.5.7 255.255.255.240
SW-25-5-3(config-if)#no shut
SW-25-5-3(config-if)#ex
SW-25-5-3(config)#vlan 10
SW-25-5-3(config-vlan)#ex

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-25-5-3(config)#vlan 20
SW-25-5-3(config-vlan)#ex
SW-25-5-3(config)#vlan 30
SW-25-5-3(config-vlan)#ex
SW-25-5-3(config)#vlan 40
SW-25-5-3(config-vlan)#ex
SW-25-5-3(config)#int range eth 0/3, eth 0/2, eth 0/0, eth 0/1, eth 3/1, eth 3/2
SW-25-5-3(config-if-range)#sw trunk encapsulation dot1q
SW-25-5-3(config-if-range)#sw mode trunk
SW-25-5-3(config-if-range)#ex
SW-25-5-3(config)#int range eth 3/1, eth 3/2
SW-25-5-3(config-if-range)#sw trunk allowed vlan 10,30,40
SW-25-5-3(config-if-range)#sw trunk native vlan 999
SW-25-5-3(config-if-range)#spanning-tree portfast trunk
SW-25-5-3(config-if-range)#ex
SW-25-5-3(config)#int range eth 0/0, eth 0/1
SW-25-5-3(config-if-range)#sw trunk allowed vlan 10,20,30,40
SW-25-5-3(config-if-range)#sw trunk native vlan 999
SW-25-5-3(config-if-range)#spanning-tree portfast trunk
SW-25-5-3(config-if-range)#ex
SW-25-5-3(config)#int range eth 0/2, eth 0/3
SW-25-5-3(config-if-range)#sw trunk allowed vlan 10,20
SW-25-5-3(config-if-range)#sw trunk native vlan 999
ACL:
R-25-5-2(config)#ip access-list extended ADMIN_ACCESS
R-25-5-2(config-ext-nacl)#permit udp any any eq bootpc
R-25-5-2(config-ext-nacl)#permit udp any any eq bootps
R-25-5-2(config-ext-nacl)#permit ip 191.25.5.0 0.0.0.15 any
R-25-5-2(config-ext-nacl)#permit ip any 191.25.5.0 0.0.0.15
R-25-5-2(config-ext-nacl)#exit

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-25-5-2(config)#
R-25-5-2(config)#ip access-list extended LAB_ACCESS
R-25-5-2(config-ext-nacl)#permit udp any any eq bootpc
R-25-5-2(config-ext-nacl)#permit udp any any eq bootps
R-25-5-2(config-ext-nacl)#permit  udp  192.25.5.0  0.0.0.15  191.25.5.0
0.0.0.15 eq 1812
R-25-5-2(config-ext-nacl)#permit  udp  192.25.5.0  0.0.0.15  191.25.5.0
0.0.0.15 eq 1813
R-25-5-2(config-ext-nacl)#permit tcp 192.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
established
R-25-5-2(config-ext-nacl)#permit  icmp  192.25.5.0  0.0.0.15  191.25.5.0
0.0.0.15 echo-reply
R-25-5-2(config-ext-nacl)#deny ip 192.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
R-25-5-2(config-ext-nacl)#deny ip 192.25.5.0 0.0.0.15 193.25.5.0 0.0.0.15
R-25-5-2(config-ext-nacl)#deny ip 192.25.5.0 0.0.0.15 194.25.5.0 0.0.0.15
R-25-5-2(config-ext-nacl)#permit ip 192.25.5.0 0.0.0.15 any
R-25-5-2(config-ext-nacl)#permit ip any 192.25.5.0 0.0.0.15
R-25-5-2(config-ext-nacl)#exit
R-25-5-2(config)#ip access-list extended STAFF1_ACCESS
R-25-5-2(config-ext-nacl)#permit udp any any eq bootpc
R-25-5-2(config-ext-nacl)#permit udp any any eq bootps
R-25-5-2(config-ext-nacl)#permit  udp  193.25.5.0  0.0.0.15  191.25.5.0
0.0.0.15 eq 1812
R-25-5-2(config-ext-nacl)#permit  udp  193.25.5.0  0.0.0.15  191.25.5.0
0.0.0.15 eq 1813
R-25-5-2(config-ext-nacl)#permit tcp 193.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
established
R-25-5-2(config-ext-nacl)#permit  icmp  193.25.5.0  0.0.0.15  191.25.5.0
0.0.0.15 echo-reply
R-25-5-2(config-ext-nacl)#deny ip 193.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-25-5-2(config-ext-nacl)#deny ip 193.25.5.0 0.0.0.15 192.25.5.0 0.0.0.15
R-25-5-2(config-ext-nacl)#permit ip 193.25.5.0 0.0.0.15 any
R-25-5-2(config-ext-nacl)#permit ip any 193.25.5.0 0.0.0.15
R-25-5-2(config-ext-nacl)#exit
R-25-5-2(config)#
R-25-5-2(config)#ip access-list extended STAFF2_ACCESS
R-25-5-2(config-ext-nacl)#permit udp any any eq bootpc
R-25-5-2(config-ext-nacl)#permit udp any any eq bootps
R-25-5-2(config-ext-nacl)#permit  udp  194.25.5.0  0.0.0.15  191.25.5.0
0.0.0.15 eq 1812
R-25-5-2(config-ext-nacl)#permit  udp  194.25.5.0  0.0.0.15  191.25.5.0
0.0.0.15 eq 1813
R-25-5-2(config-ext-nacl)#permit tcp 194.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
established
R-25-5-2(config-ext-nacl)#permit  icmp  194.25.5.0  0.0.0.15  191.25.5.0
0.0.0.15 echo-reply
R-25-5-2(config-ext-nacl)#deny ip 194.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
R-25-5-2(config-ext-nacl)#deny ip 194.25.5.0 0.0.0.15 192.25.5.0 0.0.0.15
R-25-5-2(config-ext-nacl)#permit ip 194.25.5.0 0.0.0.15 any
R-25-5-2(config-ext-nacl)#permit ip any 194.25.5.0 0.0.0.15
R-25-5-2(config-ext-nacl)#exit
R-25-5-2(config)#int gi 0/0.10
R-25-5-2(config-ext-nacl)#ip access-group ADMIN_ACCESS in
R-25-5-2(config-subif)#ip access-group ADMIN_ACCESS out
R-25-5-2(config)#int gi 0/0.20
R-25-5-2(config-subif)#ip access-group LAB_ACCESS in
R-25-5-2(config-subif)#ip access-group LAB_ACCESS out
R-25-5-2(config-subif)#exit
R-25-5-2(config)#int gi 0/0.30
R-25-5-2(config-subif)#ip access-group STAFF1_ACCESS in

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

R-25-5-2(config-subif)#ip access-group STAFF1_ACCESS out

R-25-5-2(config-subif)#exit

R-25-5-2(config)#int gi 0/0.40

R-25-5-2(config-subif)#ip access-group STAFF2_ACCESS in

R-25-5-2(config-subif)#ip access-group STAFF2_ACCESS out

Також потрібно створити резервні локальні адміністративні облікові записи у разі повної втрати зв'язку з серверами, разом з цим налаштовано протокол SSHv2.

Далі буде наведено лістинг команд, що будуть застосовані як маршрутизаторам так і комутаторам.

R-25-5-1(config)#security passwords min-length 10

R-25-5-1(config)#security authentication failure rate 3 log

R-25-5-1(config)#username adminkul privilege 15 secret adminkulpass!@#

R-25-5-1(config)#enable secret cisco12345

R-25-5-1(config)#ip domain-name Kulenko.net

R-25-5-1(config)#crypto key generate rsa modulus 2048

R-25-5-1(config)#ip ssh version 2

R-25-5-1(config)#ip ssh time-out 120

R-25-5-1(config)#ip ssh authentication-retries 5

R-25-5-1(config)#line vty 0 4

R-25-5-1(config-line)#transport input ssh

R-25-5-1(config-line)#transport output ssh

R-25-5-1(config-line)#logging synchronous

R-25-5-1(config-line)#exit

R-25-5-1(config)#line con 0

R-25-5-1(config-line)#privilege level 15

R-25-5-1(config-line)#exit

R-25-5-1(config)#line aux 0

R-25-5-1(config-line)#privilege level 15

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування NTP-серверу відбуватиметься на маршрутизаторах:

R-25-5-1(config)#clock timezone EET 2

R-25-5-1(config)#clock summer-time EEST recurring last Sun Mar 02:00 last
Sun Oct 03:00

R-25-5-1(config)#service timestamps log datetime msec

R-25-5-1(config)#ip name-server 1.1.1.1 1.0.0.1

R-25-5-1(config)#ip domain lookup

R-25-5-1(config)#ntp server 0.ua.pool.ntp.org

R-25-5-1(config)#ntp server 1.ua.pool.ntp.org

R-25-5-1(config)#ntp server 2.ua.pool.ntp.org

R-25-5-1(config)#ntp server 3.ua.pool.ntp.org

R-25-5-1(config)#ntp authenticate

R-25-5-1(config)#ntp authentication-key 5 md5 adminkul!@#

R-25-5-1(config)#ntp trusted-key 5

R-25-5-1(config)#ntp master 10

R-25-5-1(config)#ntp update-calendar

Приклад налаштування NTP-клієнтів:

SW-25-5-5(config)#clock timezone EET 2

SW-25-5-5(config)#clock summer-time EEST recurring last Sun Mar 02:00
last Sun Oct 03:00

SW-25-5-5(config)#service timestamps log datetime msec

SW-25-5-5(config)#ntp authenticate

SW-25-5-5(config)#ntp authentication-key 5 md5 adminkul!@#

SW-25-5-5(config)#ntp trusted-key 5

SW-25-5-5(config)#ntp server 191.25.5.11 key 5

SW-25-5-5(config)#ntp source Vlan10

SW-25-5-5(config)#ntp update-calendar

Приклад налаштування Syslog-клієнтів

SW-25-5-5(config)#logging on

SW-25-5-5(config)#logging host 191.25.5.2 transport tcp port 514

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

SW-25-5-5(config)#logging host 191.25.5.3 transport tcp port 514

SW-25-5-5(config)#logging userinfo

SW-25-5-5(config)#logging buffered 20480

SW-25-5-5(config)#logging trap notifications

Приклад налаштування RADIUS-клієнтів:

SW-25-5-5(config)#aaa new-model

SW-25-5-5(config)#radius server LUfreeRAD

SW-25-5-5(config-radius-server)#address ipv4 191.25.5.2 auth-port 1812
acct-port 1813

SW-25-5-5(config-radius-server)#key freeRAD!@#pass!@!

SW-25-5-5(config-radius-server)#exit

SW-25-5-5(config)#radius server TekRAD

SW-25-5-5(config-radius-server)#address ipv4 191.25.5.3 auth-port 1812
acct-port 1813

SW-25-5-5(config-radius-server)#key supersecretTEK

SW-25-5-5(config-radius-server)#exit

SW-25-5-5(config)#aaa group server radius radserversGR

SW-25-5-5(config-sg-radius)#server name LUfreeRAD

SW-25-5-5(config-sg-radius)#server name TekRAD

SW-25-5-5(config-sg-radius)#exit

SW-25-5-5(config)#aaa authentication login default group radserversGR
local

SW-25-5-5(config)#aaa authorization exec default group radserversGR local

SW-25-5-5(config)#aaa accounting exec default start-stop group
radserversGR

SW-25-5-5(config)#aaa accounting commands 0 default start-stop group
radserversGR

SW-25-5-5(config)#aaa authorization console

SW-25-5-5(config)#exit

SW-25-5-5(config)#line vty 0 4

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-25-5-5(config-line)#login authentication default
SW-25-5-5(config-line)#authorization exec default
SW-25-5-5(config-line)#accounting exec default
SW-25-5-5(config-line)#exit
SW-25-5-5(config)#line con 0
SW-25-5-5(config-line)#no privilege level 15
SW-25-5-5(config-line)#login authentication default
SW-25-5-5(config-line)#login authentication default
SW-25-5-5(config-line)#authorization exec default
SW-25-5-5(config-line)#accounting exec default

```

3.2. Інтеграція підсистеми аутентифікації та порівняння рішень

Налаштування адресації на операційних системах Linux Ubuntu та Windows Server 2019 зображено на рис. 3.1 та рис. 3.2.

```

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN-LC3L4510EH9
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-A1-60-40
Dhcp Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e5c4:f971:7491:ce3f%2(Preferred)
IPv4 Address. . . . . : 191.25.5.3(Preferred)
Subnet Mask . . . . . : 255.255.255.240
Default Gateway . . . . . : 191.25.5.11
Dhcpv6 IAID . . . . . : 34078759
Dhcpv6 Client DUID. . . . . : 00-01-00-01-2F-D1-FA-47-08-00-27-A1-60-40
DNS Servers . . . . . : 191.25.5.11
                        8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>

```

Рисунок 3.1 – Налаштування адресації в ОС Windows Server

```

student@student-VirtualBox:~$ ifconfig
ethp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 191.25.5.2 netmask 255.255.255.240 broadcast 191.25.5.15
    ether 08:00:27:50:75:25 txqueuelen 1000 (Ethernet)
    RX packets 20041 bytes 25326729 (25.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9985 bytes 1132371 (1.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Рисунок 3.2 – Налаштування адресації в ОС Linux Ubuntu

Після проведених налаштувань можна перейти до встановлення та порівняння рішень. Будуть використані виключно ліцензійні відкриті версії.

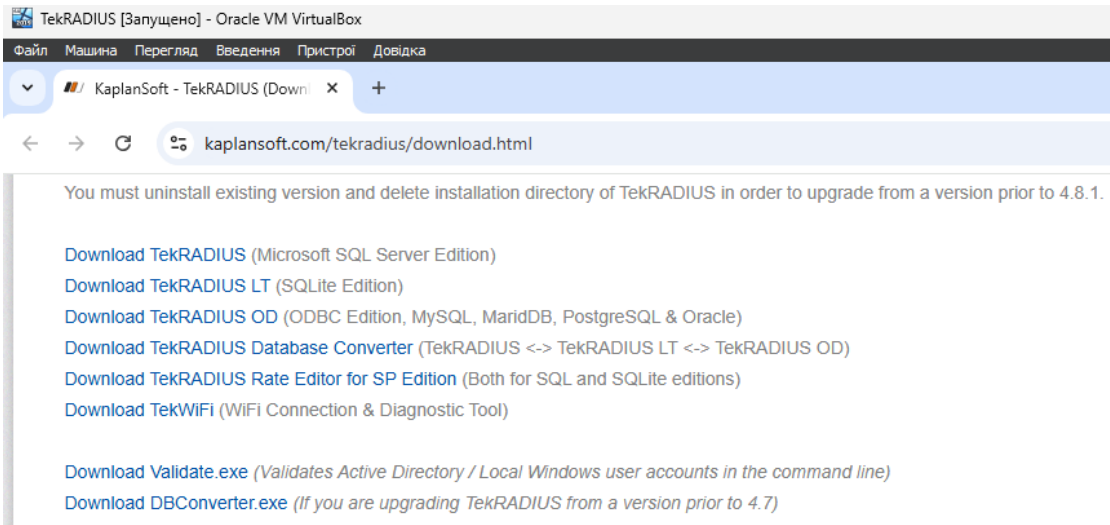


Рисунок 3.3 – Безкоштовні варіації встановлення TekRADIUS

Було обрано версію TekRADIUS LT на базі SQLite – легка, вбудована БД. Вибір обумовлений простотою розгортання, низькими вимогами до ресурсів та достатністю для цілей демонстрації в рамках дипломного проєкту, при цьому визнаючи його обмеження для великих виробничих середовищ.

При встановленні потрібно було обов’язково встановити додаткове ПЗ: .NET Framework 4.8 та Visual C++ Redistributable.

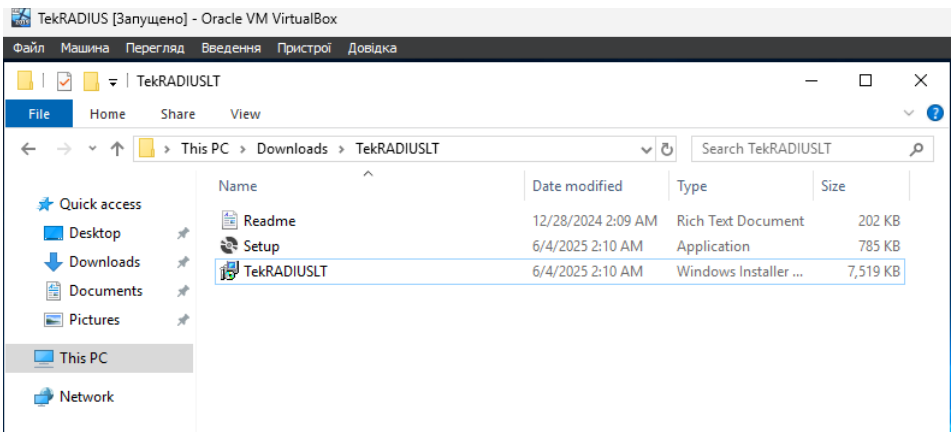


Рисунок 3.4 – Директорія інсталятора рішення

Одразу при запуску інсталятора відбувається перевірка на наявність .NET Framework 4.8, у разі відсутності неможливо взагалі встановити серверне рішення.

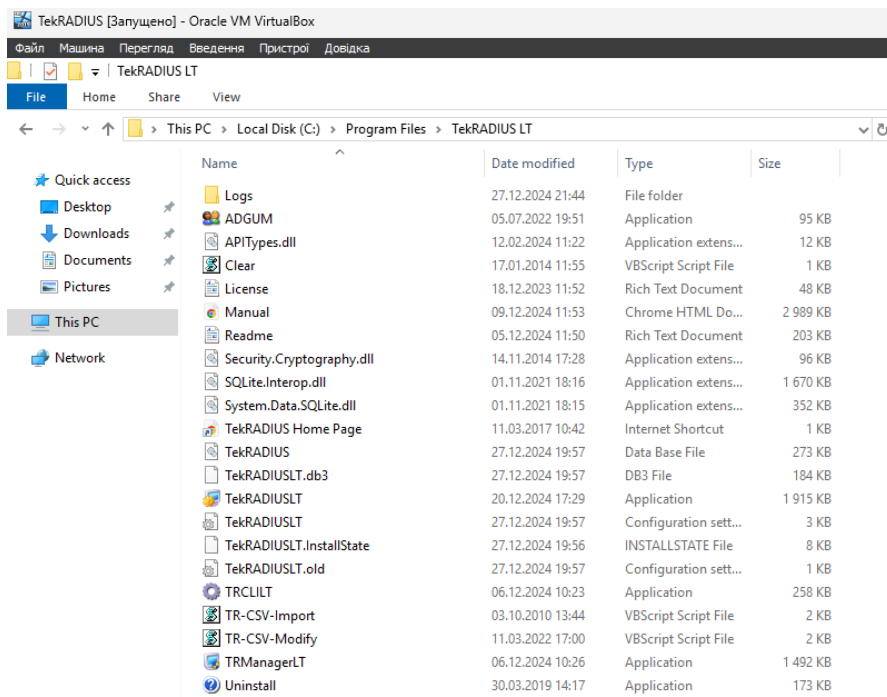


Рисунок 3.5 – Директорія інстальованого рішення

Далі буде встановлено FreeRADIUS з GUI, для зручного ознайомлення та налаштування, а саме з daloRADIUS. А базу даних було обрано MariaDB, як стандартний і найпоширеніший вибір для цього рішення, через її масштабованість, швидкість, надійність та широку підтримку, а також через підтримку цієї БД веб-інтерфейсу daloRADIUS.

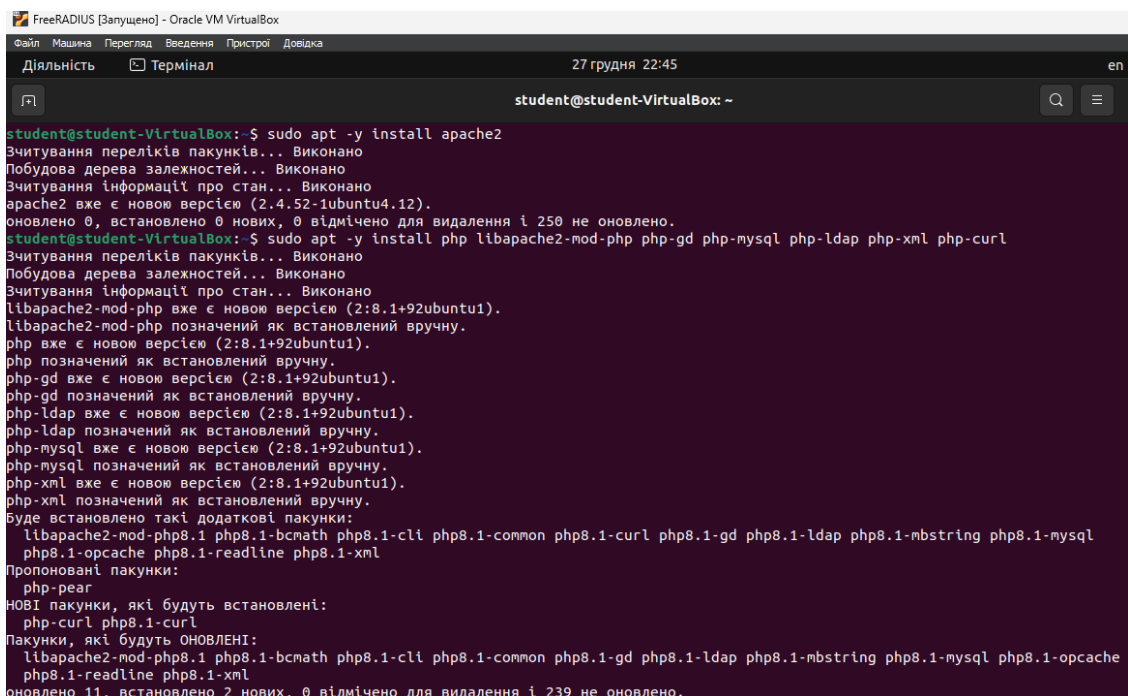


Рисунок 3.6 – Встановлення Apache та PHP

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

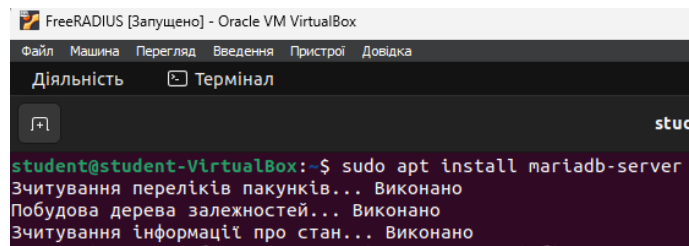


Рисунок 3.7 – Встановлення MariaDB

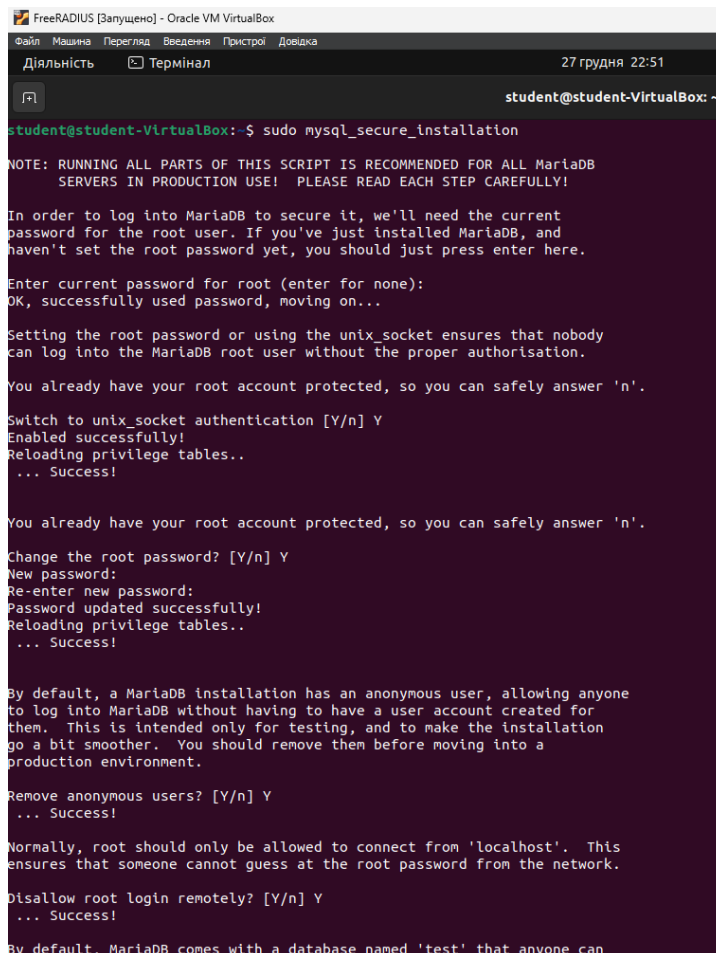


Рисунок 3.8 – Виконання скрипту для більшої безпеки MariaDB

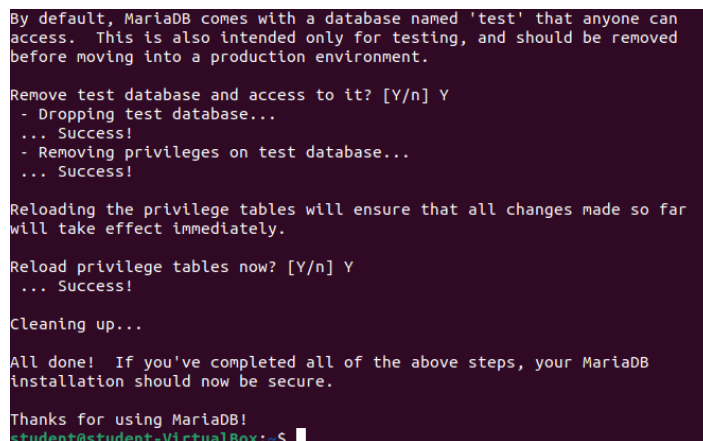


Рисунок 3.9 – Продовження виконання скрипту для забезпечення безпеки

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

```

FreeRADIUS [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
Діяльність  Термінал  27 грудня 22:59
student@student-VirtualBox: ~

student@student-VirtualBox:~$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 85
Server version: 10.6.18-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE radius;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> CREATE USER 'radius'@'localhost' IDENTIFIED BY 'Adminkulpass123';
Query OK, 0 rows affected (0,016 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON radius.* TO 'radius'@'localhost';
Query OK, 0 rows affected (0,003 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> EXIT;

```

Рисунок 3.10 – Створення бази даних для FreeRADIUS

```

FreeRADIUS [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
Діяльність  Термінал  27 грудня 23:01
student@student-VirtualBox: ~

student@student-VirtualBox:~$ sudo apt install freeradius freeradius-mysql freeradius-utils
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей... Виконано
Зчитування інформації про стан... Виконано
Наступні пакунки були встановлені автоматично і більше не потрібні:
  libaio1 libmecab2 libprotobuf-lite23 mecab-ipadic mecab-ipadic-utf8 mecab-utils
Використовуйте 'sudo apt autoremove' щоб видалити їх.
Буде встановлено такі додаткові пакунки:
  freeradius-common freeradius-config freetds-common libct4 libfreeradius3 make
Пропоновані пакунки:
  freeradius-krb5 freeradius-ldap freeradius-postgresql freeradius-python3 snmp make-doc
НОВІ пакунки, які будуть встановлені:
  freeradius freeradius-common freeradius-config freeradius-mysql freeradius-utils freetds-
оновлено 0, встановлено 9 нових, 0 відмічено для видалення і 234 не оновлено.
Необхідно завантажити 1 761 kB архівів.
Після цієї операції об'єм зайнятого дискового простору зросте на 6 750 kB.

```

Рисунок 3.11 – Встановлення FreeRADIUS та необхідних модулів

```

FreeRADIUS [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
Діяльність  Термінал  22:51
root@student-VirtualBox: /etc/freeradius/3.0

GNU nano 6.2  mods-available/sql
server = "localhost"
port = 3306
login = "radius"
password = "adminkulpass!@#"

# Connection info for Mongo
# Authentication Without SSL
#   server = "mongodb://USER:PASSWORD@192.16.0.2:PORT/DATABASE?authSource=admin"

# Authentication With SSL
#   server = "mongodb://USER:PASSWORD@192.16.0.2:PORT/DATABASE?authSource=admin"

# Authentication with Certificate
# Use this command for retrieve Derived username:
# openssl x509 -in mycert.pem -inform PEM -subject -nameopt RFC2253
# server = mongodb://<DERIVED USERNAME>@192.168.0.2:PORT/DATABASE?authSource=admin

# Database table configuration for everything except Oracle
radius_db = "radius"

```

Рисунок 3.12 – Налаштування FreeRADIUS для використання MariaDB

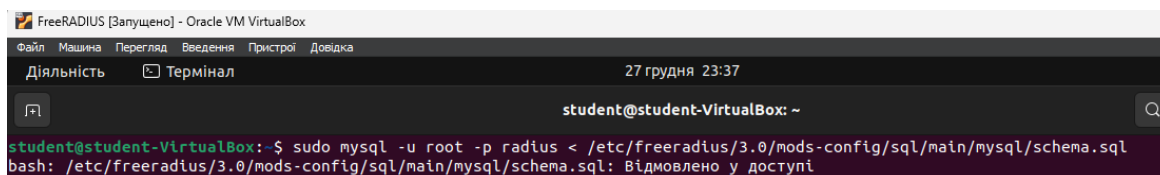


Рисунок 3.13 – Імпортовано початкову схему бази даних

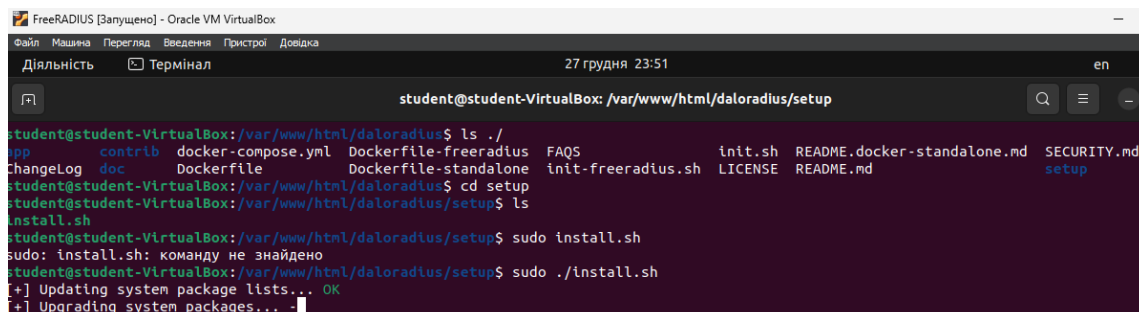


Рисунок 3.14 – Встановлення daloRADIUS

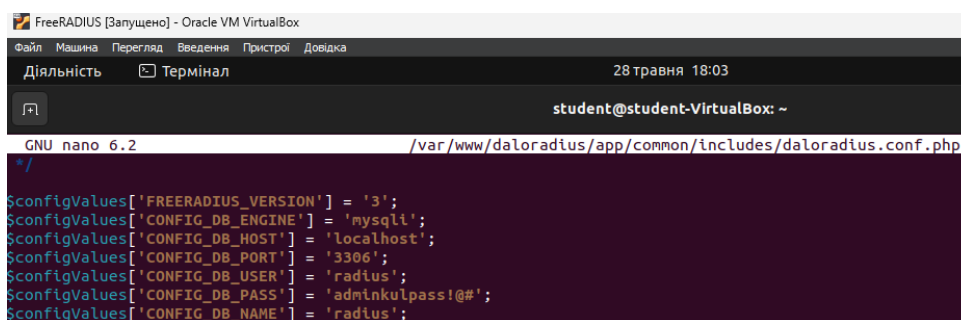


Рисунок 3.15 – Налаштування конфігураційного файлу daloRADIUS

Після всіх виконаних операцій встановлення та налаштування потрібно перезапустити служби пов'язані з сервером.

Перехід до веб-інтерфейсу відбувається за допомогою введення локальної адреси поточної робочої станції, як видно на рис. 3.16.

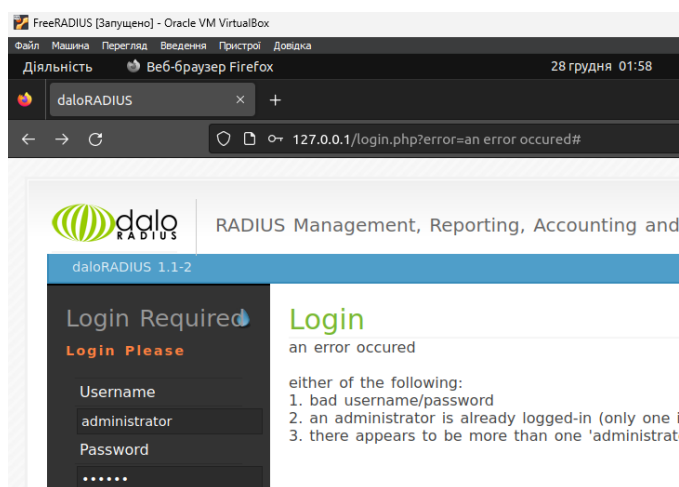


Рисунок 3.16 – Успішно відкрито графічний інтерфейс daloRADIUS

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		70

Як можна побачити на попередніх рисунках, що TekRADIUS встановити було набагато легше ніж Unix-орієнтований сервер разом з daloRADIUS. Спочатку переглянемо можливості та вигляд інтерфейсу серверів.

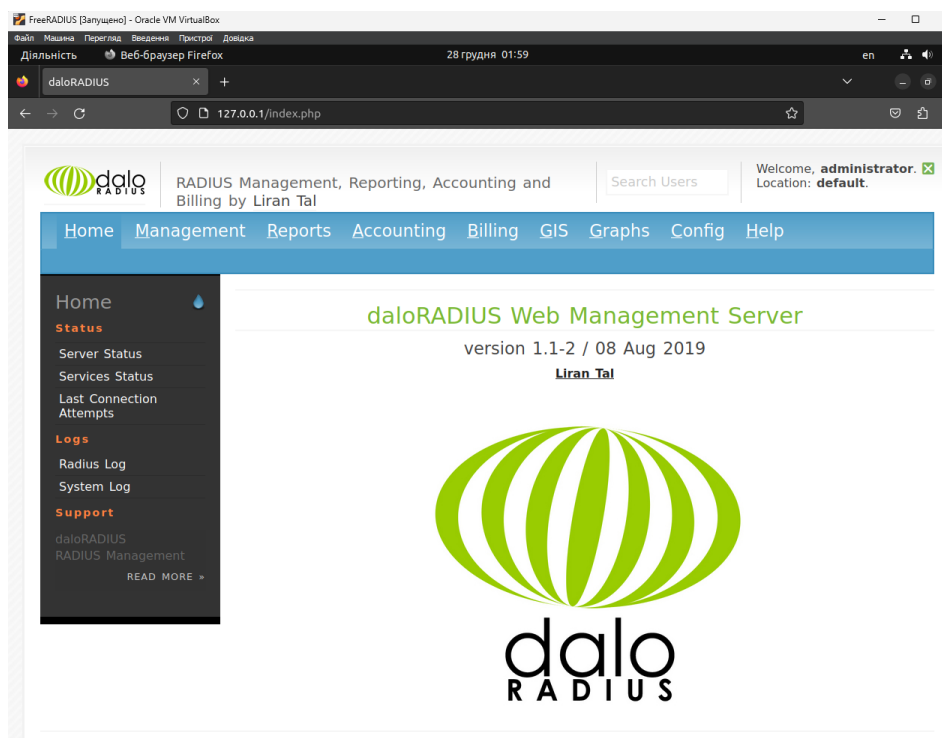


Рисунок 3.17 – Перегляд веб-інтерфейсу

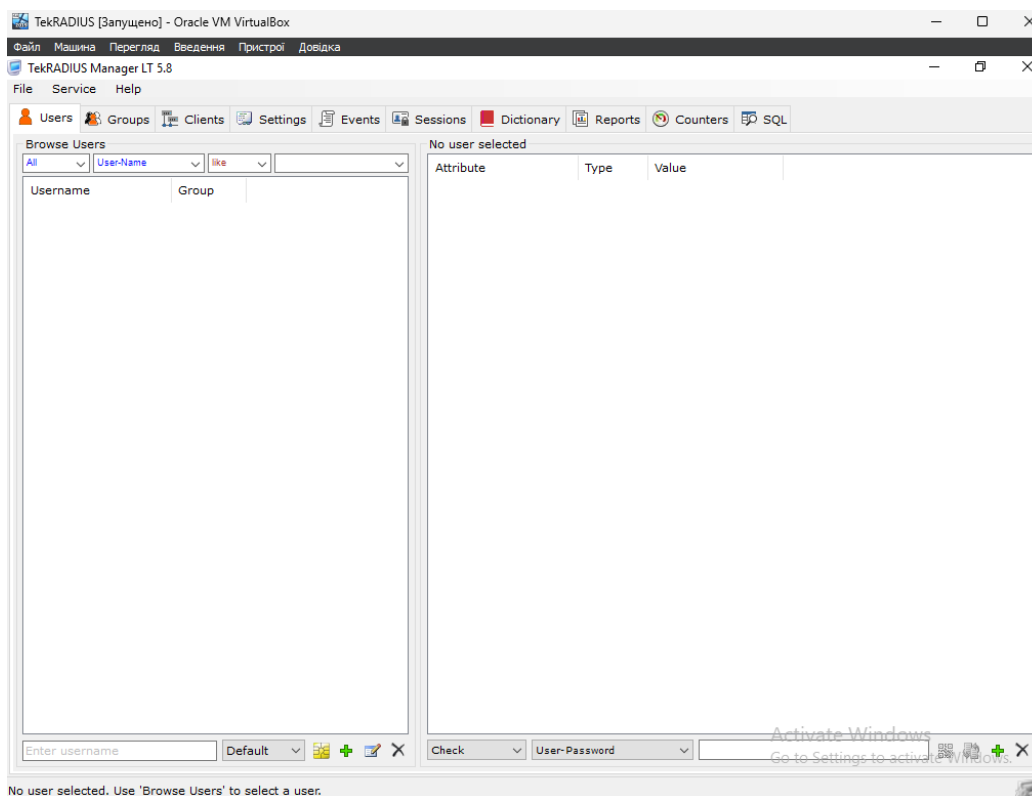


Рисунок 3.18 – Перегляд інтерфейсу TekRADIUS

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

.Переглядаючи інтерфейс цих серверів, можна сказати, що наявність інтерфейсу в Unix-орієнтованому рішенні, у вигляді daloRADIUS, є дуже корисним для користувачів та спрощує більшість налаштувань, але це не повністю звільняє користувача від налаштувань конфігураційних файлів.

В свою чергу TekRADIUS виглядає більш мінімалістично, при цьому інформація на інтерфейсі сприймається менш навантажено.

Наступним етапом є порівняння конфігураційних файлів та можливостей керування користувачами між цими двома серверами.

FreeRADIUS – повністю конфігурується за допомогою текстових файлів. Це забезпечує надзвичайну гнучкість, але вимагає знання структури директорій та синтаксису файлів.

Ключові директорії та файли є наступними:

- /etc/freeradius/3.0/ (або схожий шлях, залежить від дистрибутива) – основна директорія конфігурації;
- radiusd.conf – головний конфігураційний файл, що визначає загальні параметри сервера (порти, debug рівень, завантаження модулів);
- mods-available/ – містить конфігурації для всіх доступних модулів (наприклад, sql, ldap, eap, pap, mschap);
- mods-enabled/ – символічні посилання на модулі, які активні на сервері;
- clients.conf – визначає RADIUS-клієнтів (NAS), яким дозволено підключатися до сервера (їхні IP-адреси та shared secrets);
- users – локальна текстова база даних користувачів;
- sites-available/ – містить конфігурації віртуальних серверів або потоків обробки запитів (наприклад, default, inner-tunnel);
- sites-enabled/ – символічні посилання на активні віртуальні сервери.

Unix-орієнтований сервер можна використовувати без БД, вписуючи користувачів у файл clients.conf, як зображено на рис. 3.19, де можна окремо для кожного клієнта увімкнути або вимкнути обов’язкове використання атрибута “message authenticator”.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

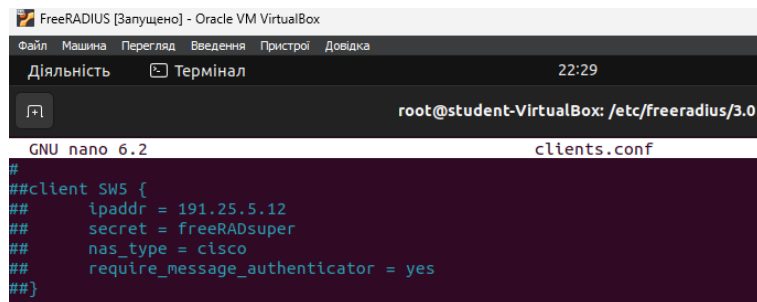


Рисунок 3.19 – Конфігураційний файл clients

При використанні бази даних MariaDB, як у випадку цього проєкту, FreeRADIUS читає клієнтів з таблиці nas, як показано на рисунку 3.20.

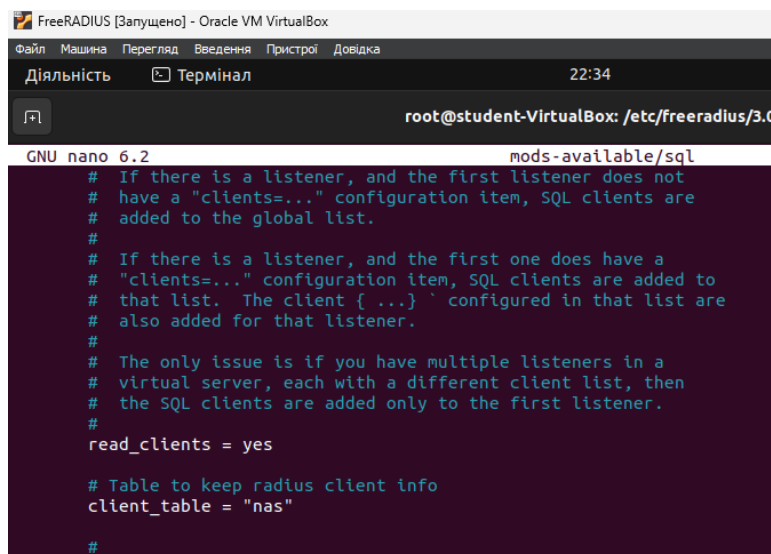


Рисунок 3.20 – Фрагмент конфігураційного файлу модулю sql

Веб-інтерфейс daloRADIUS створює записи в таблиці nas (див. рис. 3.21), а сервер потім читає ці записи через свій SQL-модуль, тому і немає потреби редагувати текстові файли клієнтів вручну.

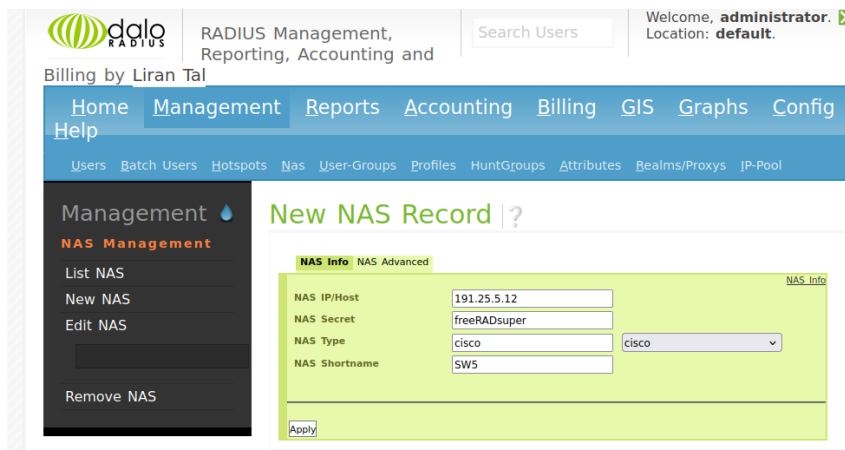


Рисунок 3.21 – Форма створення нового клієнта

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

Форма створення включає в себе такі поля як: IP-адреса клієнта, секретний ключ, тип та коротку назву пристрою.

The screenshot shows the 'Edit NAS Record' form in the FreeRADIUS web interface. The form is titled 'Edit NAS Record :: 191.25.5.12'. It contains two sections: 'NAS Info' and 'NAS Advanced'. The 'NAS Info' section has fields for 'NAS IP/Host' (191.25.5.12), 'NAS Secret' (freeRADsuper), 'NAS Type' (cisco), and 'NAS Shortname' (SW5). The 'NAS Advanced' section has fields for 'NAS Ports' (0), 'NAS Community', 'NAS Virtual Server', and 'NAS Description'. There are 'Apply' buttons at the bottom of each section.

Рисунок 3.22 – Форма створення NAS

При редагуванні клієнтів можна додатково налаштувати (див. рис. 3.22) такі параметри як: порти, спільнота (для групування клієнтів), відповідність віртуальним серверам, опис.

The screenshot shows the 'NAS Listing in Database' table in the FreeRADIUS web interface. The table has the following columns: NAS ID, NAS IP/Host, NAS Shortname, NAS Type, NAS Ports, NAS Secret, NAS Virtual Server, NAS Community, and NAS Description. The table contains one record with the following values: NAS ID: 5, NAS IP/Host: 191.25.5.12, NAS Shortname: SW5, NAS Type: cisco, NAS Ports: 0, NAS Secret: freeRADsuper, NAS Virtual Server: (empty), NAS Community: (empty), and NAS Description: (empty). There is a 'Delete' button next to the record.

NAS ID	NAS IP/Host	NAS Shortname	NAS Type	NAS Ports	NAS Secret	NAS Virtual Server	NAS Community	NAS Description
5	191.25.5.12	SW5	cisco	0	freeRADsuper			

Рисунок 3.23 – Список створених клієнтів

Для порівняння в іншому сервері всі дії робляться виключно в інтерфейсі, а збережені клієнти зберігаються безпосередньо в локальній базі даних SQLite. Попередній сервер навпроти, використовує веб-інтерфейс як надбудова над сервером, який використовує зовнішню БД.

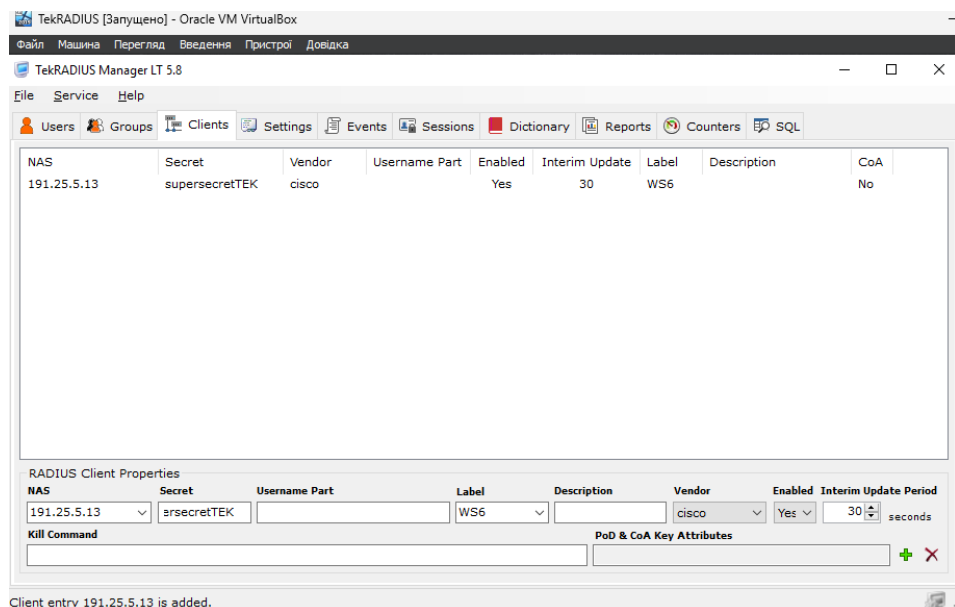


Рисунок 3.24 – Вкладка і форма створення клієнта

Форма створення має схожі поля, але є і такі, що відрізняються або були зовсім відсутні у попередньо розглянутого сервера, ось як ці:

- Username Part – це поле дозволяє модифікувати ім'я користувача, яке він отримує від NAS, перед тим, як шукати його в своїй базі даних або передавати далі (наприклад, до Active Directory). Приклад використання: якщо користувачі входять як “user@domain.com”, але хочете, щоб сервер шукав їх просто як “user” у своїй локальній базі даних, можна вказати в цьому полі @domain.com, щоб сервер видалив цю частину;
- Label – схоже поле на shortname, що в попередньому сервері;
- Vendor – аналог поля NAS Type;
- Enabled – дозволяє увімкнути або вимкнути NAS;
- Interim Update Period – визначає, як часто NAS повинен надсилати проміжні облікові повідомлення (Accounting Interim-Update) до сервера. Ці повідомлення містять оновлену інформацію про поточну сесію користувача (наприклад, скільки трафіку було використано);

- Kill Command – функція, яка дозволяє примусово відключити активну сесію користувача на NAS. Клієнт повинен підтримувати CoA/PoD для того, щоб ця функція працювала;
- PoD & CoA Key Attributes – дозволяє вказати, які атрибути сервер повинен використовувати для ідентифікації сесії, яку потрібно відключити, коли він надсилає команду PoD (Packet of Disconnect) або CoA (Change of Authorization) до NAS.

Далі буде переглянуто механізм створення користувачів та концепцію груп у серверах.

У формі створення присутні три можливих способи автентифікації користувачів, за допомогою: ОЗ користувача, MAC-адреси пристрою, PIN-код. Для створення користувача потрібне: ім'я, пароль, тип збереженого паролю і належність до певної групи. А для двох інших потрібні дані, що відповідають назвам самих способів, і до них також можна додати прив'язку до групи.

Рисунок 3.25 – Форма створення користувача

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

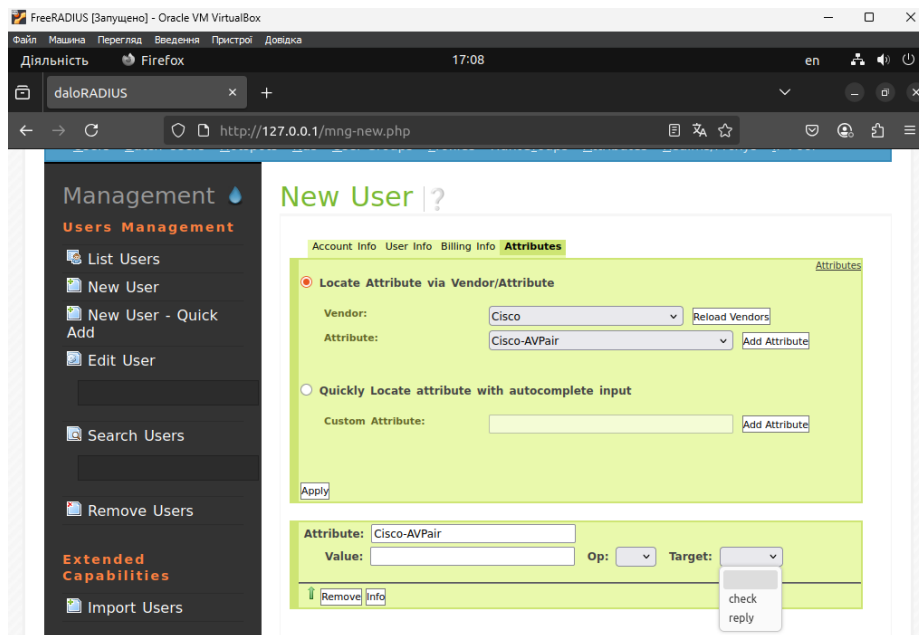


Рисунок 3.26 – Форма додавання атрибутів користувачеві

Важливим є здатність присвоєння атрибутів безпосередньо користувачам для тонкого налаштування. У вкладці атрибутів є вибір між атрибутами, що стосуються певних вендорів, або швидкого пошуку атрибутів (для досвідчених користувачів). При створенні атрибута ціллю можуть бути наступні параметри: Check – перевірка на відповідність певним критеріям, або Reply – надавання інструкцій керування сесією, після успішної аутентифікації.

Концепція груп в серверах RADIUS дозволяє централізовано керувати дозволами для великої кількості користувачів, призначаючи їм спільні атрибути.

Вкладка атрибутів виглядає так само як і при створенні користувачів, що видно з рисунку 3.27, тому і налаштування відбуватимуться зрозуміліше.

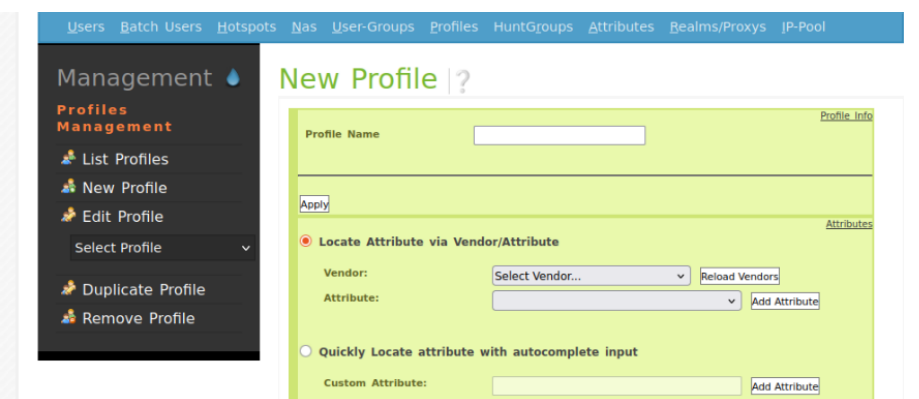


Рисунок 3.27 – Форма створення груп користувачів

Порівняємо створення користувачів та груп з сервером на базі ОС Windows Server 2019.

Спочатку проаналізовано форму створення користувача (див. рис. 3.28).

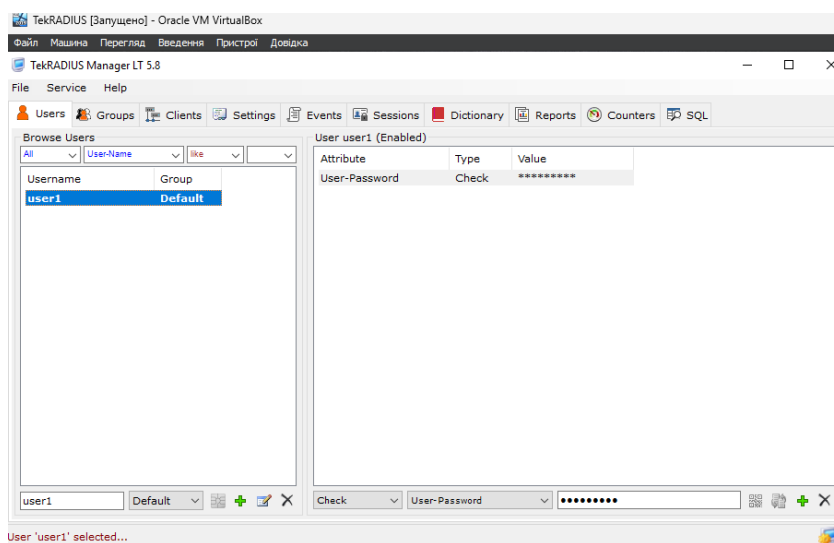


Рисунок 3.28 – Вкладка створення користувача

Схожий процес як у попереднього сервера, відрізняється лише інтерфейс, пароль задається у вигляді атрибуту. Так само можна індивідуально до кожного користувача застосовувати атрибути.

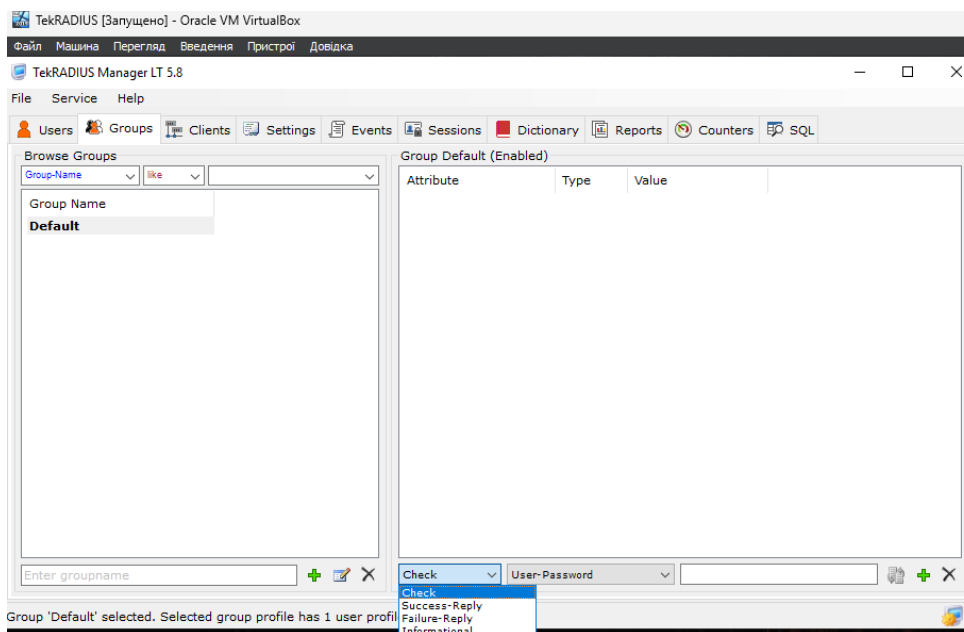


Рисунок 3.29 – Вкладка створення групи

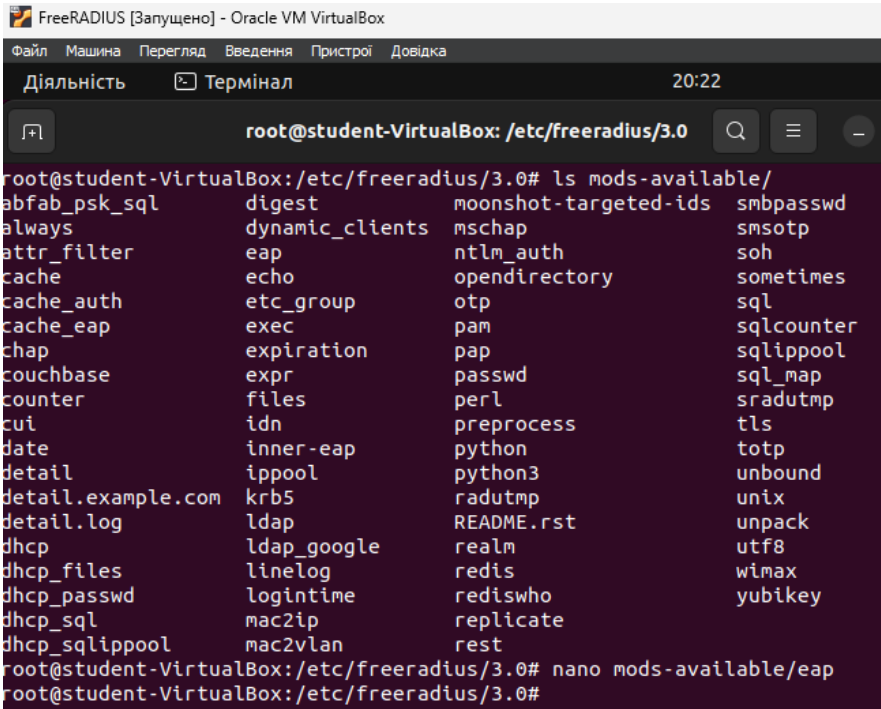
Щодо процесу керування групами – так само, майже різниці немає, лише було помічено дещо нові цілі атрибутив.

В цьому сервері є різні Reply: Success – те ж саме, що й звичайний Reply, але застосовується при відповіді від серверу Access-Асепт, Failure – навпаки при відповіді Access-Reject, а от Informational – не впливають безпосередньо на процес автентифікації або авто-ризації, а слугують для зберігання додаткової інформації, яка може бути використана сервером внутрішньо або для обліку (наприклад, для стеження за використаною квотою).

Стосовно методів автентифікації між суплікантами наче всі заявлені та стандартні методи присутні в обох серверах. А от Radius over TLS, у вигляді безкоштовного протоколу безпеки, присутній лише в рішенні freeRADIUS, як і було з’ясовано ще в теоретичній частині проєкту.

Для перегляду можливих для підключення модулів у Unix-орієнтованому сервері (див. рис. 3.30), включаючи наявні методи автентифікації, потрібно перейти за наступним шляхом “dir_freeradius/mods-availbale/”.

Віртуальні сервери в контексті роботи сервера freeRADIUS потрібні для обробки різних типів RADIUS-запитів від різних джерел або для різних цілей, використовуючи при цьому унікальні набори правил, політик та модулів. Знаходяться вони за шляхом “dir_freeradius/sites-availbale/”.



```
FreeRADIUS [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
Діяльність  Термінал  20:22
root@student-VirtualBox: /etc/freeradius/3.0
root@student-VirtualBox:/etc/freeradius/3.0# ls mods-available/
abfab_psk_sql      digest             moonshot-targeted-ids  smbpasswd
always            dynamic_clients   mschap                 smsotp
attr_filter        eap               ntlm_auth              soh
cache             echo              opendirectory          sometimes
cache_auth        etc_group         otp                    sql
cache_eap         exec              pam                    sqlcounter
chap              expiration        pap                    sqlippool
couchbase         expr              passwd                 sql_map
counter           files             perl                   sradius
cui              idn               preprocess             tls
date              inner-eap         python                 totp
detail            ippool            python3                unbound
detail.example.com krb5              radutmp                unix
detail.log        ldap              README.rst             unpack
dhcp              ldap_google       realm                  utf8
dhcp_files        linelog           redis                  winax
dhcp_passwd       logintime         rediswho               yubikey
dhcp_sql          mac2ip            replicate
dhcp_sqlippool    mac2vlan          rest
```

Рисунок 3.30 – Перегляд доступних модулів

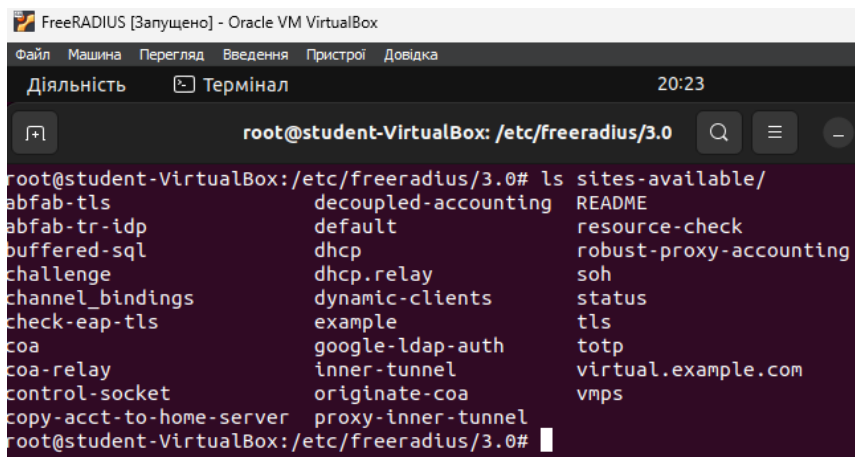


Рисунок 3.31 – Перегляд наявних віртуальних серверів

У конкурентного сервера на ОС Windows відсутні модулі та віртуальні сервери. Є загальна вкладка налаштувань, де можна обрати метод автентифікації по замовчуванню (див. рис. 3.32), який буде використовуватися при умові, якщо явно не вказано метод в атрибутах користувача/групи.

На тому ж самому рисунку, можна побачити деякі “сірі” поля налаштування, що вказує на неможливість внесення змін, через відсутність включення якихось додаткових функцій або недостатню підтримку безкоштовної версії.

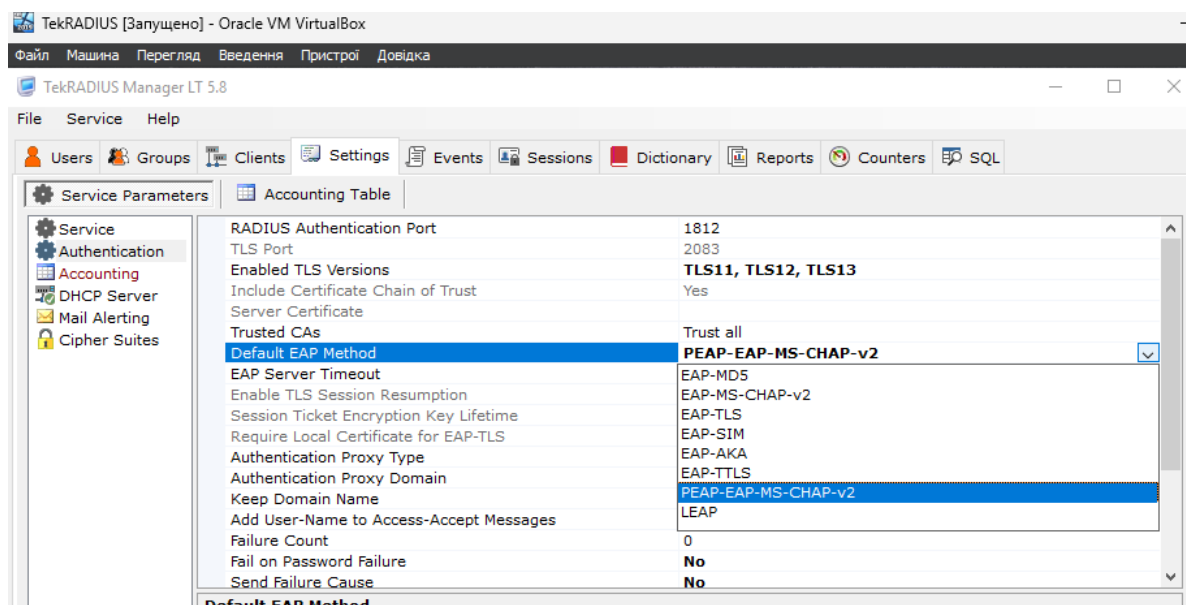


Рисунок 3.32 – Перелік методів автентифікації

На жаль відсутній спосіб використання протоколів TLS/TCP, що забезпечують надійний, цілісний та конфіденційний обмін пакетами, як видно на рис. 3.33.

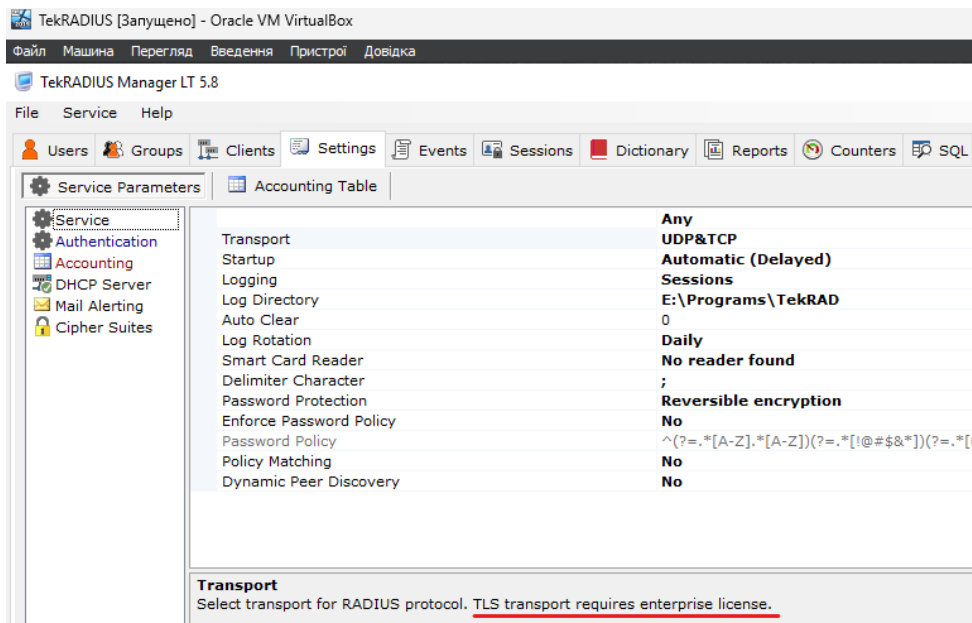


Рисунок 3.33 – Повідомлення про платний безпековий протокол

Облік в цих двох рішеннях представлений на наступних двох рис. 3.34 та рис. 3.35.

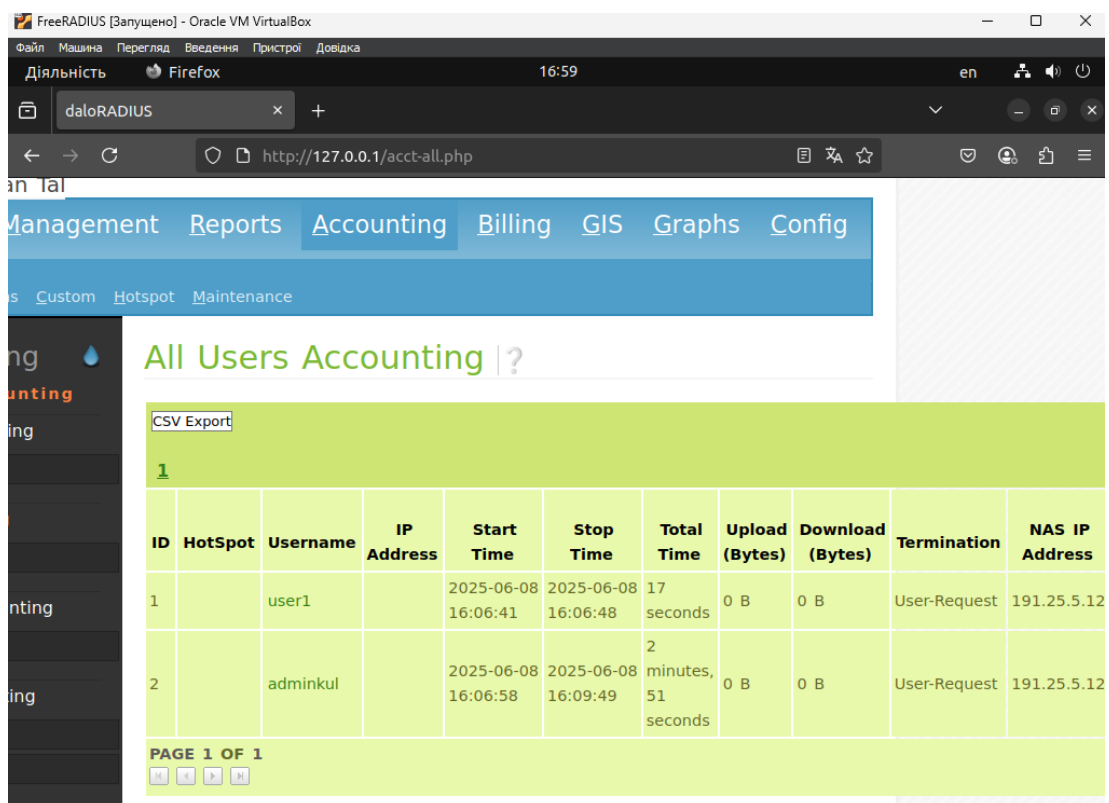


Рисунок 3.34 – Вкладка обліку в FreeRADIUS

Як можна побачити, на цій вкладці досить багато різної корисної інформації, яка може бути корисною в різних ситуаціях та бізнес-процесах.

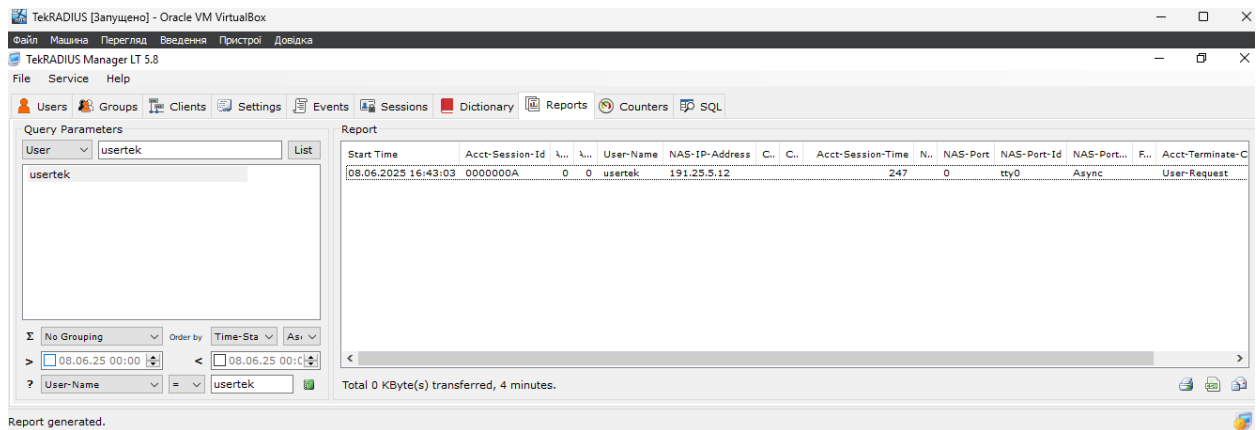


Рисунок 3.35 – Вкладка обліку в TekRADIUS

В порівнянні з конкурентним сервером, виглядає складніше для сприйняття, але також містить немало інформації, щодо сесій користувачів.

Окрім обліку акаунтів, в обох серверів присутній аудит всіх подій, збереження відбувається в реальному часі, у файлах розширення log. Будуть зображені файли обох серверів на рис. 3.36 та 3.37.

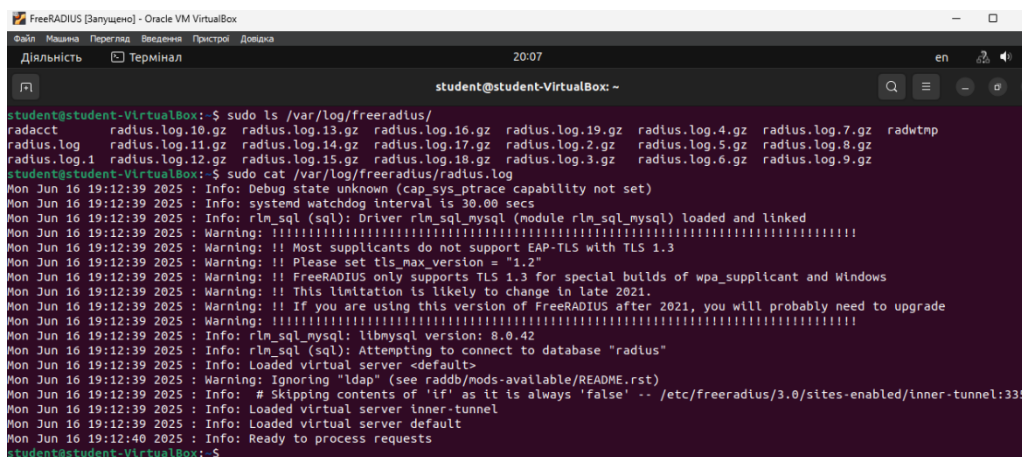


Рисунок 3.36 – Аудит сервера Unix-орієнтованого сервера

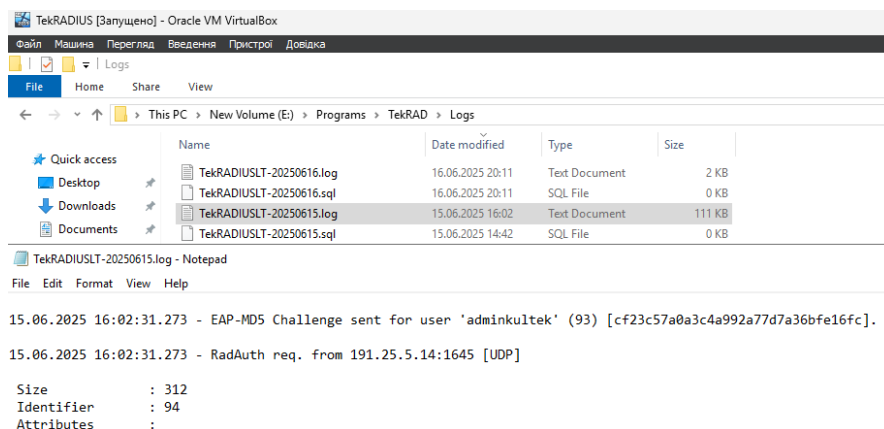


Рисунок 3.37 – Аудит сервера Windows-орієнтованого сервера

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3 Перевірка безпеки підсистеми аутентифікації

Спочатку буде перевірено безпеку протоколу RADIUS без налаштованих функцій безпеки, окрім вже налаштованих VLAN та списків доступу, для цього буде проведено атаку Blast-RADIUS.

При пошуку інформації про проведення цієї атаки було виявлено, що вона вимагає обчислення зіткнення MD5 у реальному часі. Це включає в себе два основні етапи: “день народження” (birthday stage) для пошуку початкових бітів та “близьке зіткнення” (near-collision stage) для доведення різниці у внутрішньому стані хешу до нуля. Автори дослідження цієї атаки використовували кластер із 47 CPU (Intel Xeon E5-2699 v4, E5-2680 v3, E7-4860 v2) та одну машину з чотирма GPU Tesla T4. Вони оптимізували код ПЗ під назвою “hashclash”, що дозволило обчислювати зіткнення приблизно за 5 хвилин [27, розділ 4].

А для проведення атаки мінімальними системними вимогами, в цьому ж дослідженні, є: CPU AMD 5950X та GPU NVIDIA RTX 3080. При цьому дослідження виконання цієї атаки з двома 22-байтовими префіксами призвело до 512-байтової колізії з ймовірністю 25% протягом 85 хвилин [27, розділ 4].

Виходячи з попередньо проаналізованих даних, буде розглянуто принцип цієї атаки, а також виконано скрипт, що демонструє реальну атаку. Хоча б для дослідження дієздатності запроваджених, в подальшому, засобів захисту від цієї атаки, буде виконано MITM-атаку, для підтвердження або заперечення наявності вразливості.

Буде виконано MITM атаку, для перехоплення повідомлення Access-Request, для цього під'єднано віртуальну машину уявного злочинця (див. рис. 3.38), замість легітимного комп'ютера, на базі ОС Kali Linux.

Проведення атаки буде проводитись між сервером FreeRADIUS та клієнтом SW-5.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

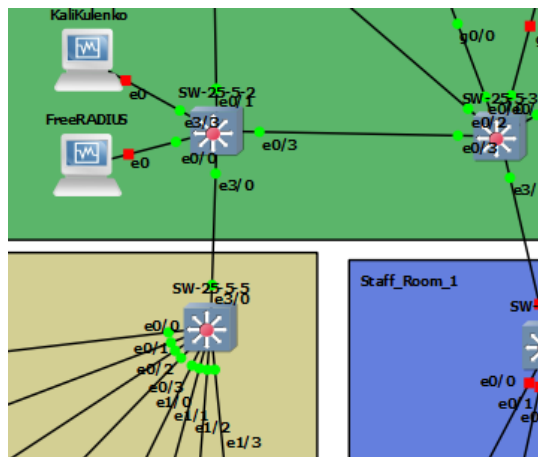


Рисунок 3.38 – Під'єднано комп'ютер порушника

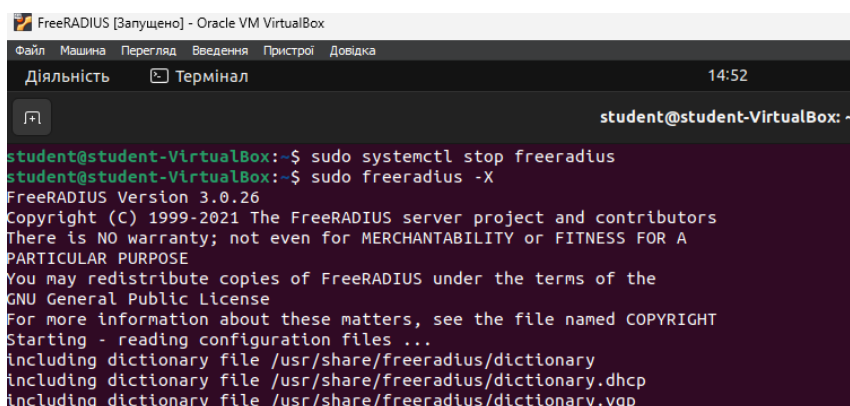


Рисунок 3.39 – Запущено сервер в режимі debug

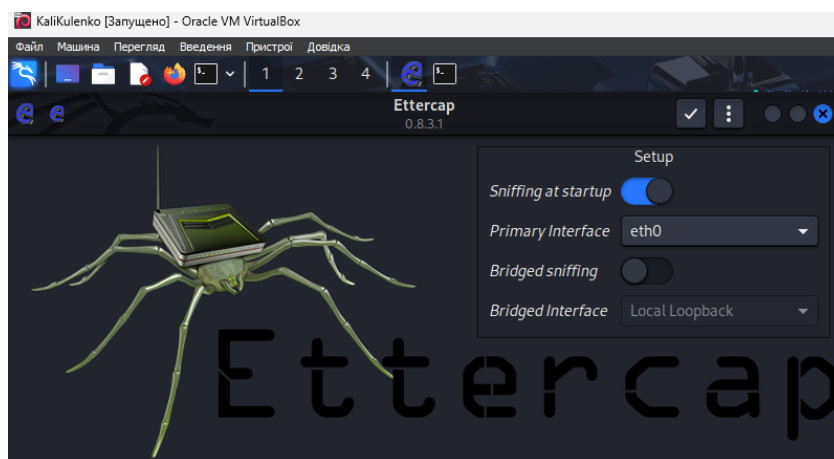


Рисунок 3.40 – Використання Ettercap для виконання MITM

Було використано саме ПЗ Ettercap, через наявний досвід з цією програмою, а також через її універсальні можливості виконання різних атак MITM.

Для виконання атаки ARP Poisoning потрібно обрати дві цілі (див. рис. 3.41), між якими повинен знаходитись комп'ютер злочинця.

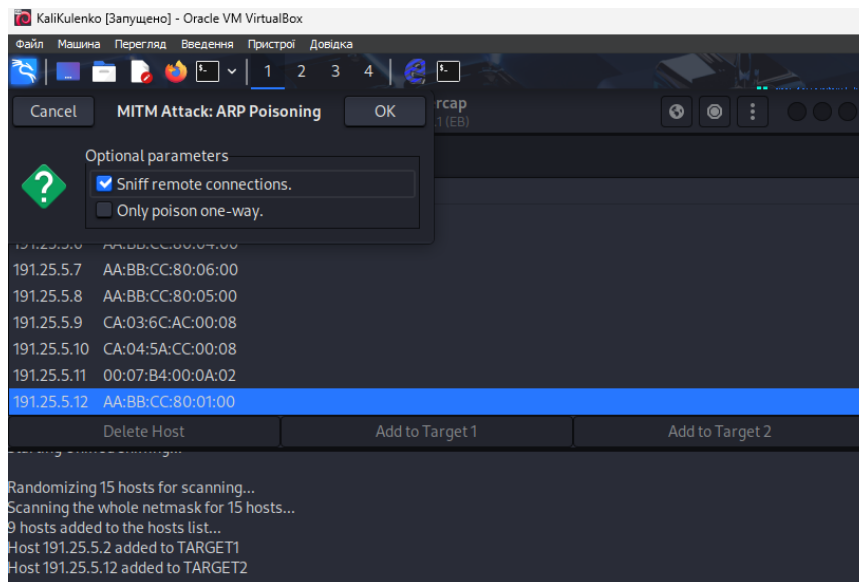


Рисунок 3.41 – Виконання MITM атаки за допомогою ARP Poisoning

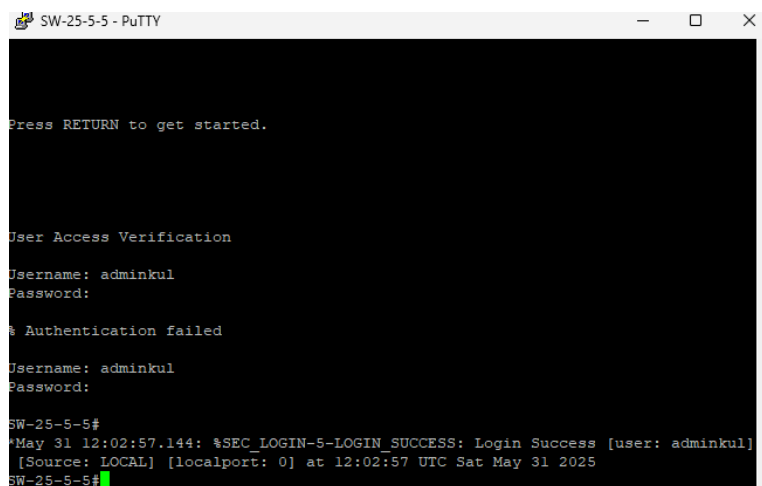


Рисунок 3.42 – Ініційовано аутентифікацію на клієнті

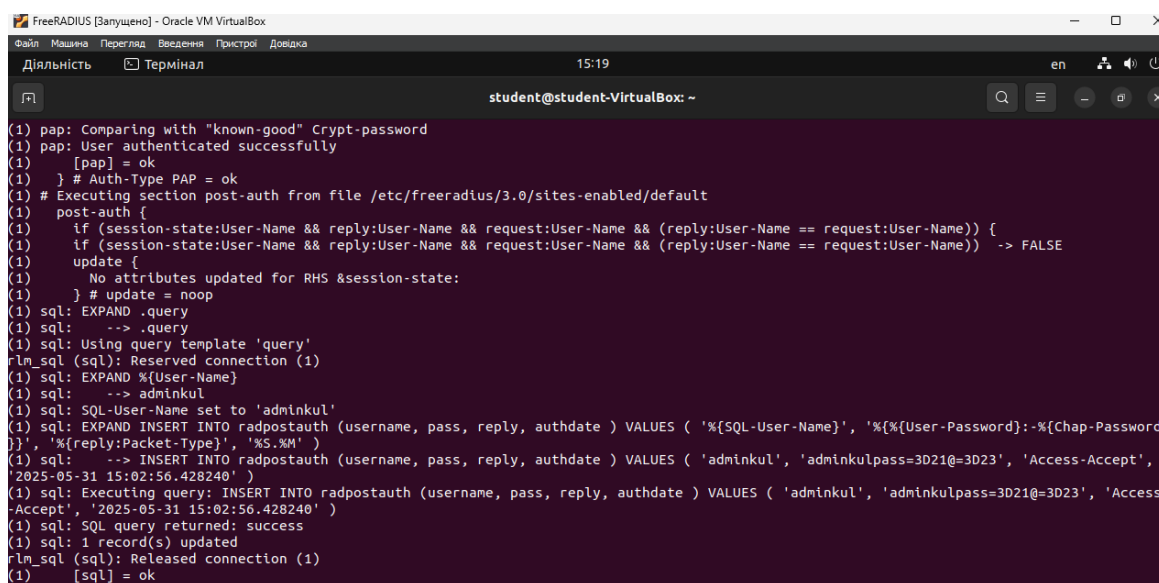


Рисунок 3.43 – Сервер під час спроб аутентифікації

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

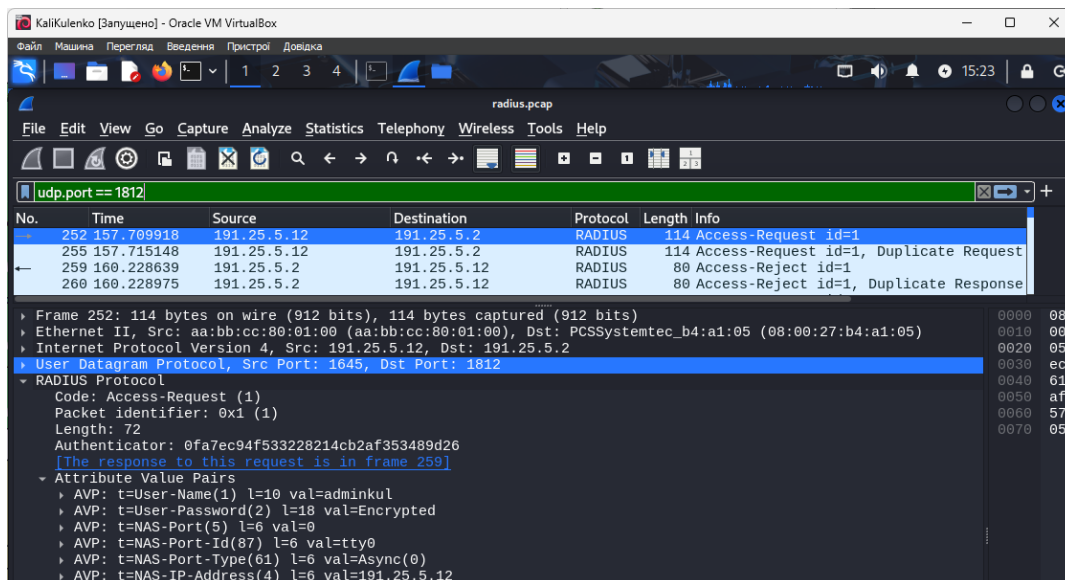


Рисунок 3.44 – Перегляд перехопленого пакету з Access-Request

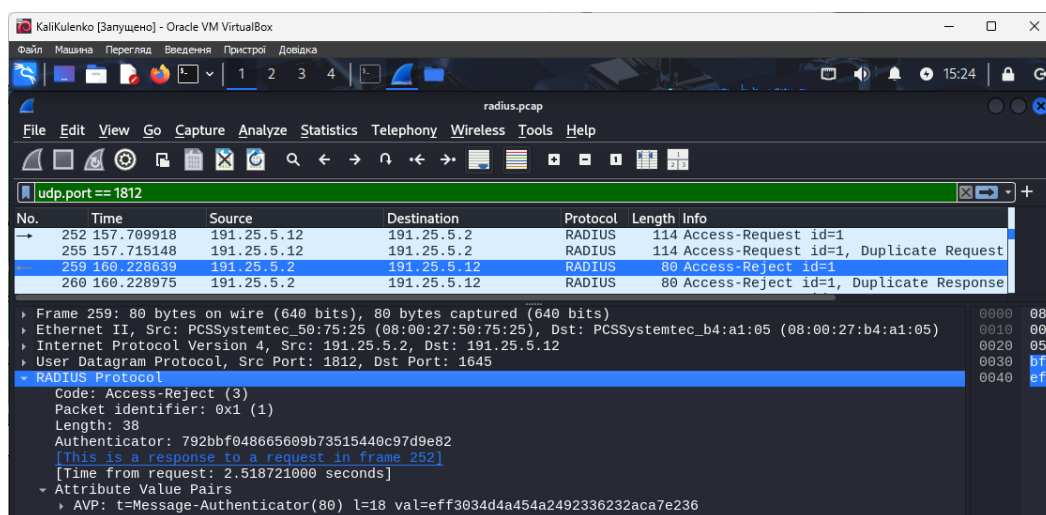


Рисунок 3.45 – Перегляд перехопленого пакету з Access-Reject

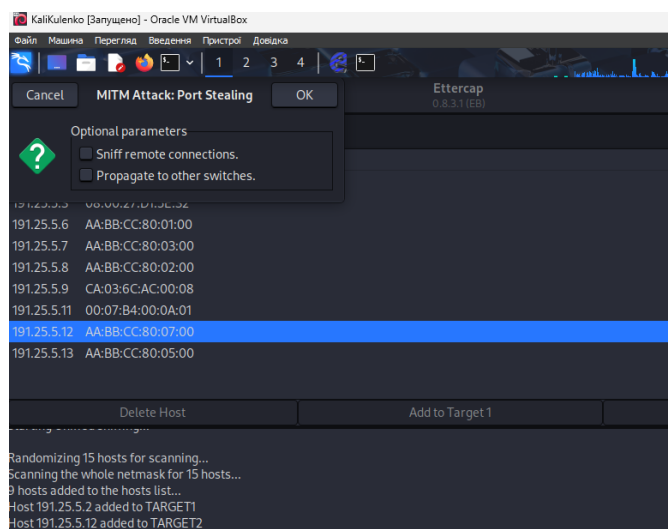


Рисунок 3.46 – Можлива атака за допомогою Port Stealing

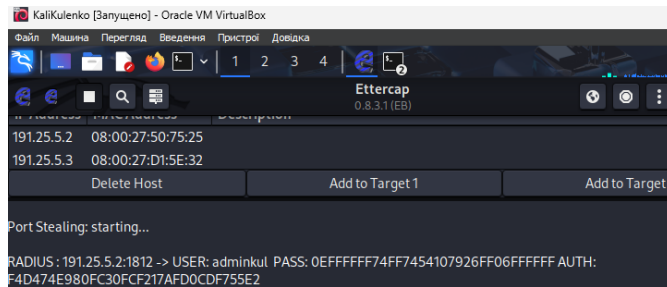


Рисунок 3.47 – Успішно реалізовано атаку за допомогою Port Stealing

В результаті перехоплення було успішно отримано необхідні дані з пакетів для подальшої реалізації атаки. На рисунку 3.48 представлено приклад реальної атаки з утворення MD5-колізії.

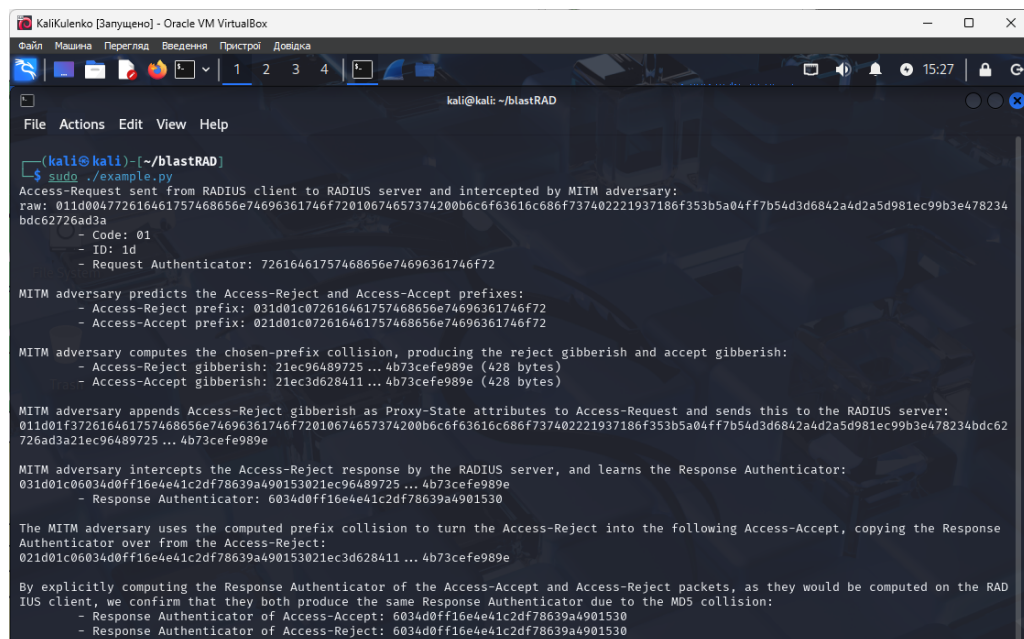


Рисунок 3.48 – Виконання демонстраційного скрипту атаки з MD5 колізією

Як говорилось в статті [11], що детально розглядає дану атаку – для її пом'якшення або повного захисту потрібно використовувати наступні заходи:

- обов'язкове використання атрибута Message-Authenticator, так як він містить HMAC-MD5 хеш усього пакету, що забезпечує його цілісність;
- перехід на Radius over TLS/DTLS;
- використання довгих та випадкових спільних секретів;
- обмеження доступу мережі, наприклад за допомогою VLAN;
- заміна MD5 хешування на більш сучасні алгоритми, такі як SHA-2 або SHA-3.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

Крім рекомендацій, щодо захисту протоколу RADIUS, є немалозначуща вразливість, що дозволяє злочинцям виконувати MITM атаки в розроблюваній підсистемі аутентифікації, а саме вразливість, що була використана ARP Poisoning, а також було визначено, що Port Stealing також є вразливістю цієї мережі. Тому для вирішення цих проблем буде виконано налаштування DAI (обов'язково разом з DHCP Snooping для коректної роботи протоколу) та Port Security.

Демонстрація атаки DHCP Spoofing відображена на рис. 3.49 та рис. 3.50.

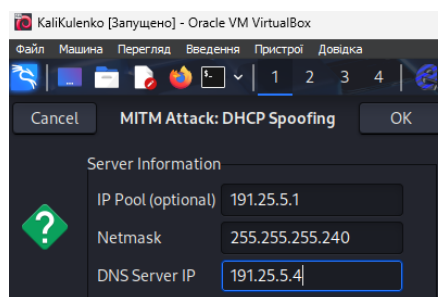


Рисунок 3.49 – Запуск налаштованої атаки

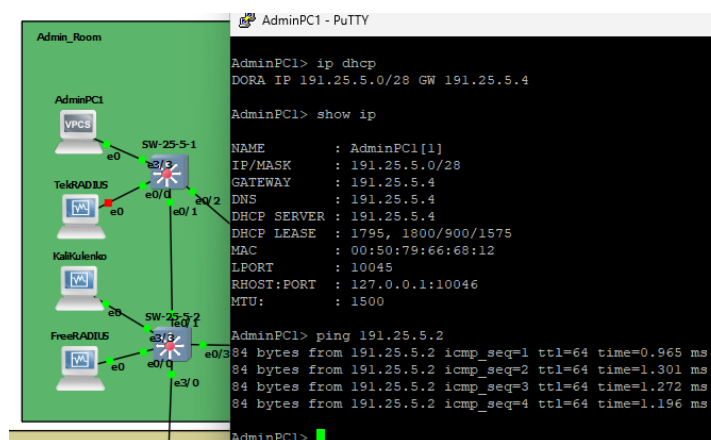


Рисунок 3.50 – Демонстрація присутньої вразливості

Так само буде перевірено вразливість автентифікації на рівні суплікантів, тобто користувачів, що під'єднані до NAS. Ця вразливість могла бути набагато серйозніше, якби не налаштовані раніше протоколи VLAN та ACL, завдяки яким користувачі, що будуть під'єднані до певного сегменту мережі, будуть мати доступ лише до тих частин мережі, до яких дозволений доступ у списках доступу.

Але все ж, не зважаючи на більш безпечну роботу на рівні доступу, є прогалина, у вигляді неавторизованого фізичного доступу (підключення нелегітимного користувача до порту комутатора, наприклад з рівнем доступу VLAN20) або є можливість використати цей безпековий протокол – 802.1x, для зручності (у вигляді динамічного призначення VLAN), як приклад буде наведено ситуацію (див. рис. 3.51 та рис 3.52): Іван з відділу LAB (VLAN 20) підключається до будь якого порту у відділі Staff_Room_1, в свою чергу RADIUS автентифікує його і призначає до VLAN 30.

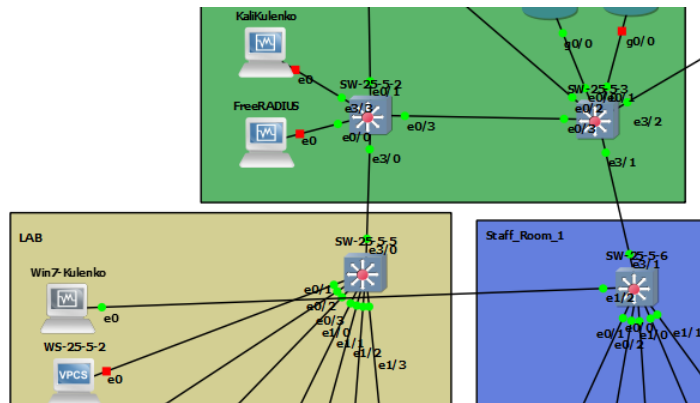


Рисунок 3.51 – Приклад можливого порушення безпеки

```

Win7-Kulenko [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
Windows PowerShell
PS C:\Users\Admin> ipconfig

Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . : Kulenko.net
    Локальный IPv6-адрес канала . . . . : fe80::4d43:b0d4:6db1:d209%11
    IPv4-адрес . . . . . : 193.255.5.1
    Маска подсети . . . . . : 255.255.255.240
    Основной шлюз . . . . . : 193.255.5.10

Туннельный адаптер isatap.Kulenko.net:

    Состояние среды . . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : Kulenko.net
  
```

Рисунок 3.52 – Отриманий доступ до сегменту Staff_Room_1

Сам протокол автентифікації користувачів (суплікантів) буде використовувати метод EAP-TLS в сервері, де це доступно, а якщо ні, то буде обрано метод максимально безпечний із можливого вибору.

Із аудиту та моніторингу присутнє налаштування RADIUS облік та log-файли серверів, цього не достатньо для моніторингу безпеки, діагностики проблем та ведення аудиту, тому буде також налаштовано Syslog на всіх

мережевих пристроях, а сервери, що тримають RADIUS, будуть виступати в ролі Syslog-серверів.

3.4 Забезпечення безпеки підсистеми та її перевірка

Для початку розглянемо забезпечення безпеки транспортного протоколу UDP для двох серверів.

Спочатку увімкнемо обов’язкову перевірку атрибуту Message-Authenticator, для цього потрібно в конфігураційному файлі сервера вказати значення “yes”, як видно на рисунку .

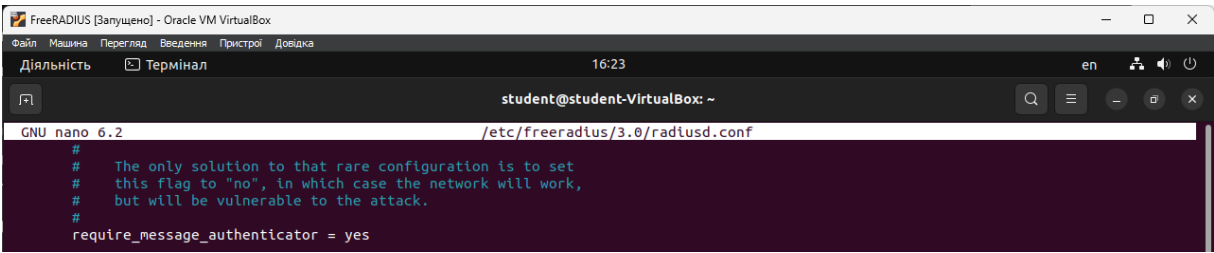


Рисунок 3.53 – Увімкнення перевірки атрибуту Message-Authenticator

Також на сервері є корисне правило, в конфігураційному файлі, що дозволяє вимкнути дозвіл на використання атрибута, який використовують при здійсненні атаки.

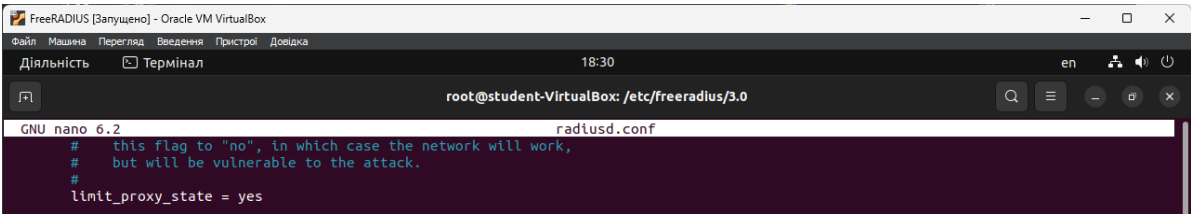


Рисунок 3.54 – Увімкнення обмеження для атрибуту Proxy-State

В порівнянні з конкурентним сервером подібні безпекові функції відсутні.

Були спроби налаштувати безпечну передачу пакетів RADIUS, що виявилися невдалими, тому буде налаштовано IPSec, як альтернативу RadSec та radsecproxy.

Тунелі будуть з’єднані безпосередньо з серверами, починаючи з пристроїв NAS, а саме з комутаторами рівня доступу.

Спочатку буде наведено приклад налаштування на пристрої NAS:

```
SW-25-5-5(config)#crypto ikev2 keyring freeRAD_keyring
```

```
SW-25-5-5(config-ikev2-keyring)#peer freeRAD_peer
```

```
SW-25-5-5(config-ikev2-keyring-peer)#address 191.25.5.2
```

```
SW-25-5-5(config-ikev2-keyring-peer)#pre-shared-key 6 m[W4Nc%D1s]4b  
=2tV&
```

```
SW-25-5-5(config-ikev2-keyring-peer)#exit
```

```
SW-25-5-5(config-ikev2-keyring)#exit
```

```
SW-25-5-5(config)#crypto ikev2 proposal ikev2_proposal
```

```
SW-25-5-5(config-ikev2-proposal)#encryption aes-cbc-256
```

```
SW-25-5-5(config-ikev2-proposal)#integrity sha384
```

```
SW-25-5-5(config-ikev2-proposal)#group 16
```

```
SW-25-5-5(config-ikev2-proposal)#exit
```

```
SW-25-5-5(config)#crypto ikev2 policy ikev2_policy
```

```
SW-25-5-5(config-ikev2-policy)#proposal ikev2_proposal
```

```
SW-25-5-5(config-ikev2-policy)#exit
```

```
SW-25-5-5(config)#crypto ikev2 profile freeRAD_profile
```

```
SW-25-5-5(config-ikev2-profile)#match identity remote address 191.25.5.2  
255.255.255.240
```

```
SW-25-5-5(config-ikev2-profile)#authentication local pre-share
```

```
SW-25-5-5(config-ikev2-profile)#authentication remote pre-share
```

```
SW-25-5-5(config-ikev2-profile)#keyring local freeRAD_keyring
```

```
SW-25-5-5(config-ikev2-profile)#dpd 10 2 periodic
```

```
SW-25-5-5(config)#crypto ipsec transform-set ipsec_transform esp-aes 256  
esp-sha384-hmac
```

```
SW-25-5-5(cfg-crypto-trans)#mode tunnel
```

```
SW-25-5-5(cfg-crypto-trans)#exit
```

```
SW-25-5-5(config)#crypto ipsec profile ipsec_freeRAD_profile
```

```
SW-25-5-5(ipsec-profile)#set ikev2-profile freeRAD_profile
```

```
SW-25-5-5(ipsec-profile)#set transform-set ipsec_transform
```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-25-5-5(ipsec-profile)#set pfs group16
SW-25-5-5(ipsec-profile)#exit
SW-25-5-5(config)#ip access-list extended freeRAD_TRAFFIC
SW-25-5-5(config-ext-nacl)#permit udp host 191.25.5.12 host 191.25.5.2 eq
1812
SW-25-5-5(config-ext-nacl)#permit udp host 191.25.5.12 host 191.25.5.2 eq
1813
SW-25-5-5(config-ext-nacl)#permit udp host 191.25.5.2 host 191.25.5.12 eq
1812
SW-25-5-5(config-ext-nacl)#permit udp host 191.25.5.2 host 191.25.5.12 eq
1813
SW-25-5-5(config)#crypto map ipsec_map 11 ipsec-isakmp
SW-25-5-5(config-crypto-map)#set peer 191.25.5.2
SW-25-5-5(config-crypto-map)#set transform-set ipsec_transform
SW-25-5-5(config-crypto-map)#set ikev
SW-25-5-5(config-crypto-map)#set ikev2-profile freeRAD_profile
SW-25-5-5(config-crypto-map)#match address freeRAD_TRAFFIC
SW-25-5-5(config)#int vlan 10
SW-25-5-5(config-if)#crypto map ipsec_map

```

Для встановлення тунелю напряму з ОС Linux Ubuntu буде використано ПЗ під назвою StrongSwan, що дозволяє виступати в ролі кінцевої точки VPN-тунелю IPSec.

Для повноцінної та коректної роботи ПЗ, потрібно налаштувати конфігураційний файл (див. рис. 3.55), в якому всі параметри зазначені на комутаторі повинні повністю збігатися. PSK-ключ повинен також співпадати (див. рис. 3.56).

Підтвердження того, що успішно встановлено тунельне з'єднання демонструє рис. 3.57.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

```
FreeRADIUS [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
Діяльність  Термінал  15:32

root@student-VirtualBox: /etc/freeradius/3.0

root@student-VirtualBox:/etc/freeradius/3.0# cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
    strictcrpolicies=no
    # uniqueids = no

# Add connections here.

conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    mobike=no

conn SWS-IPSEC-TUNNEL
    leftid=191.25.5.2
    left=191.25.5.2
    leftsubnet=191.25.5.2/28

    rightid=191.25.5.12
    right=191.25.5.12
    rightsubnet=191.25.5.12/28

    ike=aes256-sha384-modp4096!

    esp=aes256-sha384!

    pfs=modp4096

    type=tunnel
    authby=psk
    dpdtimeout=20
    dpddelay=5
    auto=start

# Sample VPN connections
```

Рисунок 3.55 – Конфігураційний файл обговорюваного ПЗ

```
FreeRADIUS [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
Діяльність  Термінал  15:33

root@student-VirtualBox: /etc/freeradius/3.0

root@student-VirtualBox:/etc/freeradius/3.0# cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.
191.25.5.2 191.25.5.12 : PSK "m[W4Nc%D1s]4b=2tV&"
root@student-VirtualBox:/etc/freeradius/3.0#
```

Рисунок 3.56 – Файл з pre-shared key (PSK)

```
SW-25-5-5(config)#do sh crypto ikev2 sa
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 191.25.5.12/500 191.25.5.2/500 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA384, Hash: SHA384, DH Grp:16, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/2845 sec

IPv6 Crypto IKEv2 SA

SW-25-5-5(config)#
```

Рисунок 3.57 – Підтверджуюча команда правильної роботи протоколу

Успішно вдалося встановити тунель між Linux Ubuntu та комутатором рівня доступу SW-5.

Задля налаштування тунелю з ОС Windows Server 2019 буде застосовано вбудований засіб під назвою “Routing and Remote Access” або скорочено RRAS. Процес налаштування та перевірки наведено на рис. від 3.58 до 3.60.

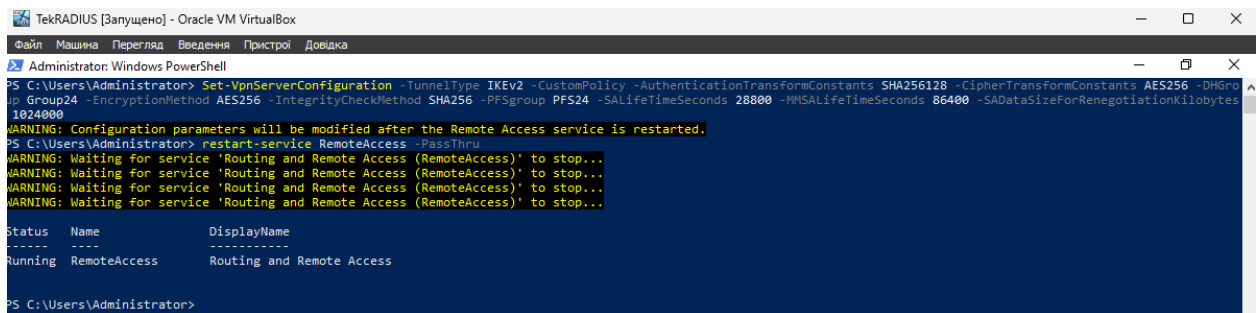


Рисунок 3.58 – Налаштування RRAS для тунелю IPSec

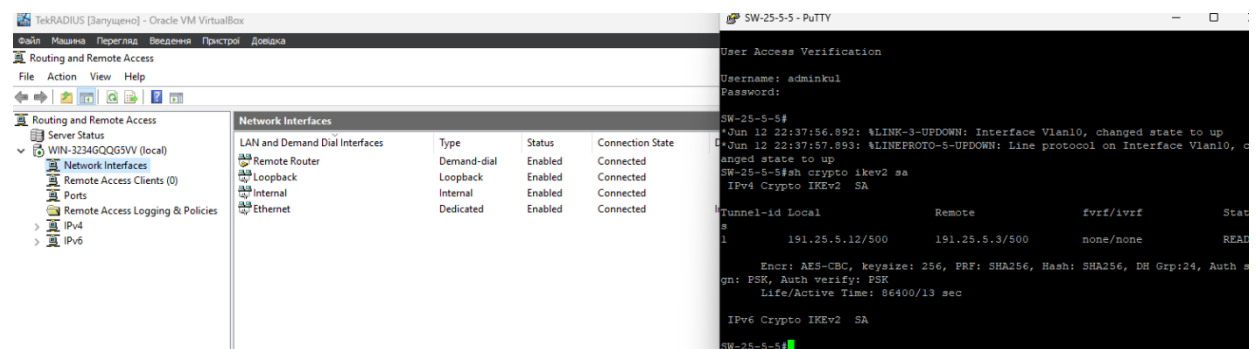


Рисунок 3.59 – Успішно встановлено з'єднання тунелю

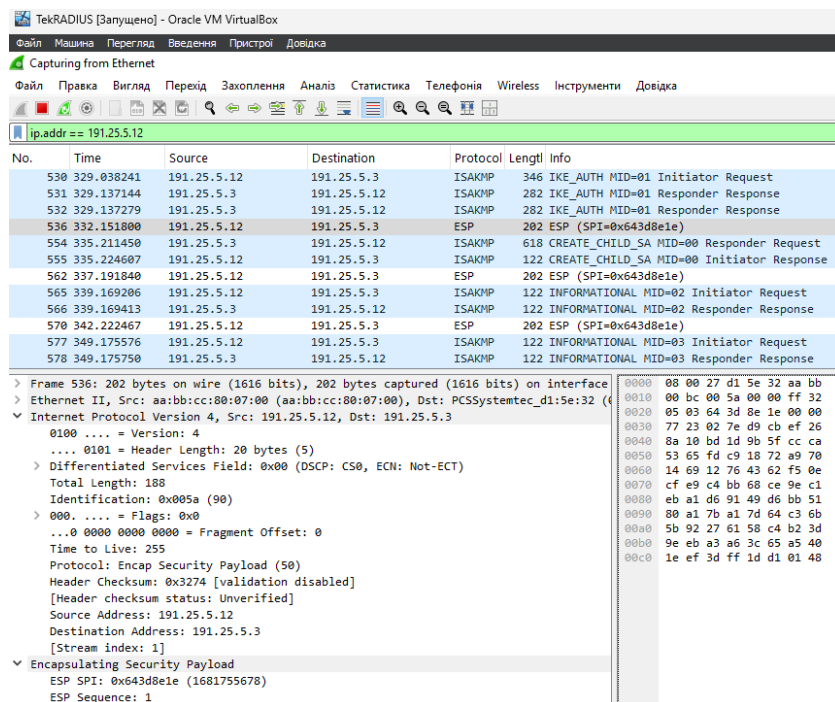


Рисунок 3.60 – Безуспішна відповідь протоколу ESP

На жаль не вдалося налаштувати протокол IPSec напряму між ОС Windows Server 2019 та комутатором рівня доступу.

Після цих безпекових налаштувань було проведено повторну атаку MITM, використовуючи ARP Poisoning, за допомогою ОС Kali Linux.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

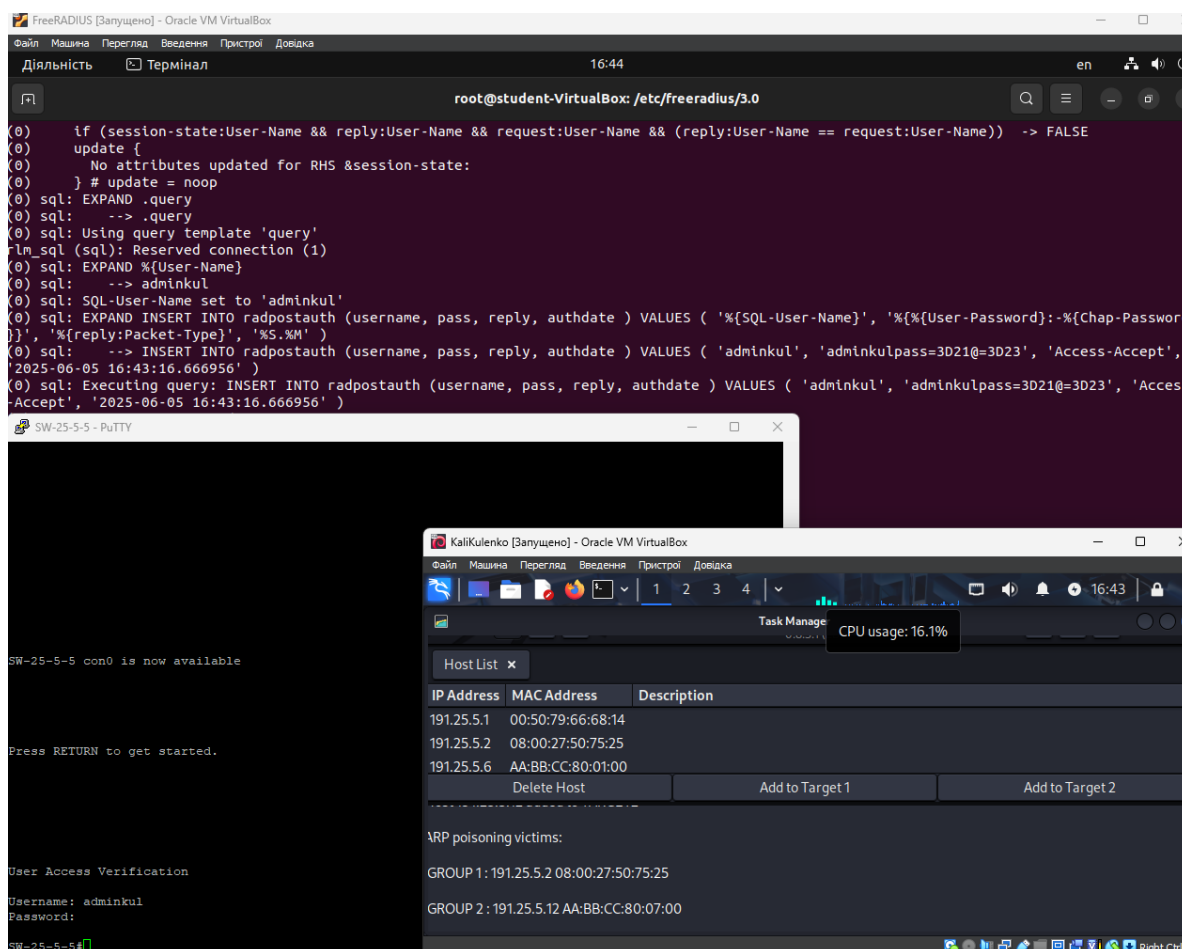


Рисунок 3.61 – Проведено повторну атаку MITM

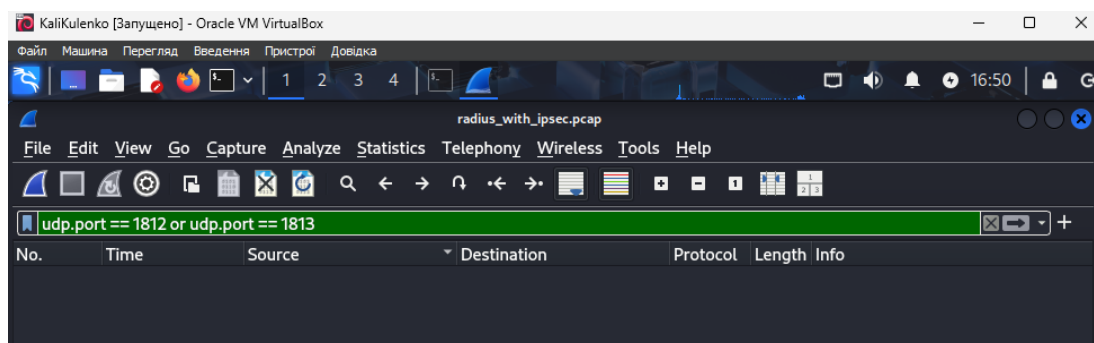


Рисунок 3.62 – Не знайдено пакети RADIUS

Відсутність пакетів RADIUS є чудовою новиною, так як це означає, що протокол тунелювання працює як потрібно і пакети, згідно правил, які було задано при налаштуванні протоколу, інкапсулюється і шифрується, для безпечного транспорту пакетів.

На рисунках 3.63 та 3.64 продемонстровано запити та відповіді в зашифрованому вигляді.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

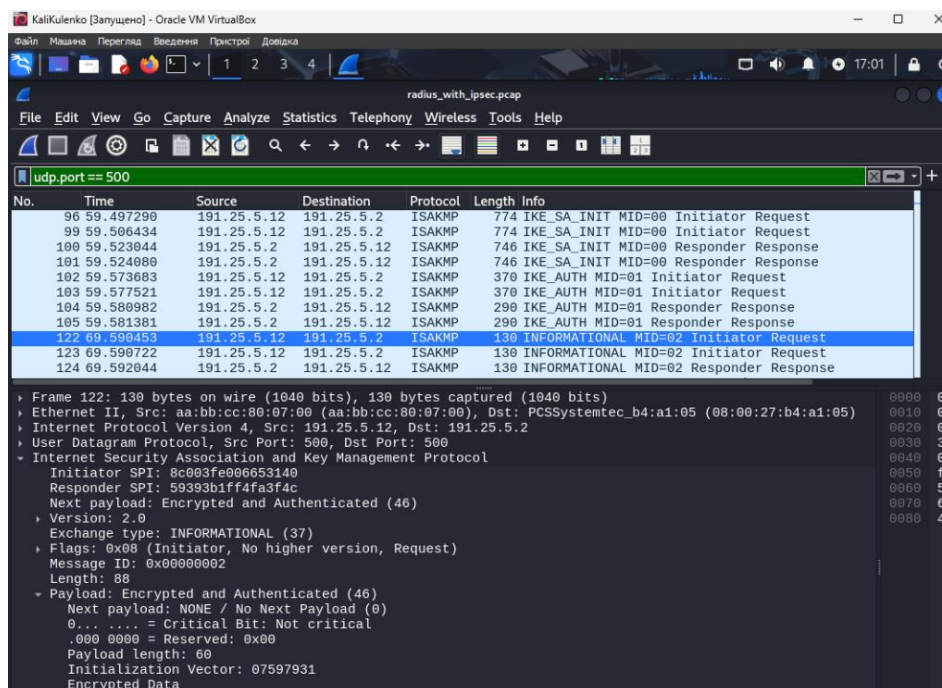


Рисунок 3.63 – Зашифрований запит від SW-5

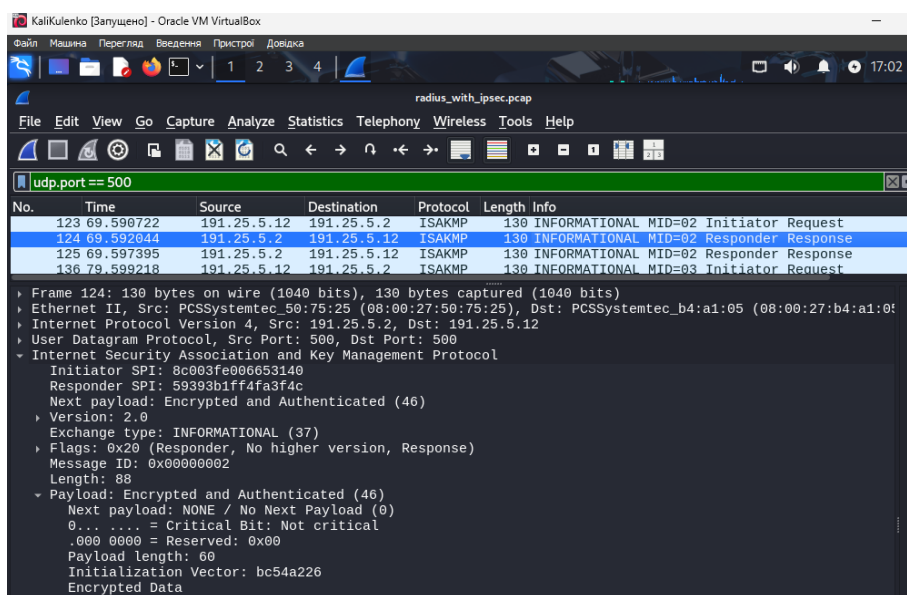


Рисунок 3.64 – Зашифрована відповідь від ОС Linux Ubuntu

Також було перевірено встановлення тунельного з'єднання між SW-1 та SW-5, як альтернатива прямого з'єднання IPSec між SW-5 та ОС Windows Server 2019.

Налаштування тунелю IPSec з іншої сторони, тобто з комутатора SW-1 виглядає схоже з SW-5, але при цьому правила корисного трафіку повинні бути віддзеркалені.

Налаштування та перевірка відображені на рисунках 3.65 - 3.67.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

Рисунок 3.65 – Успішно встановлено з’єднання між двома комутаторами

Рисунок 3.66 – Налаштований корисний трафік

Рисунок 3.67 – Помилка replay check failed

Після встановлення IPsec тунелю між комутаторами SW-1 (191.25.5.6) та SW-5 (191.25.5.12) за допомогою протоколу IKEv2, було виявлено, що трафік даних, зокрема RADIUS-автентифікація, не проходить через тунель. Системні повідомлення комутатора SW-5 постійно фіксували помилку, яка зображена на рис. 3.67. Ця помилка вказує на відхилення зашифрованих пакетів

через спрацювання механізму захисту від повторного відтворення, яка називається replay protection, що свідчить про порушення послідовності пакетів, їх дублювання або надмірну затримку під час передачі через тунель.

Після отримання помилки були спроби її вирішити, що підтверджують наступні рисунки 3.68 - 3.70.

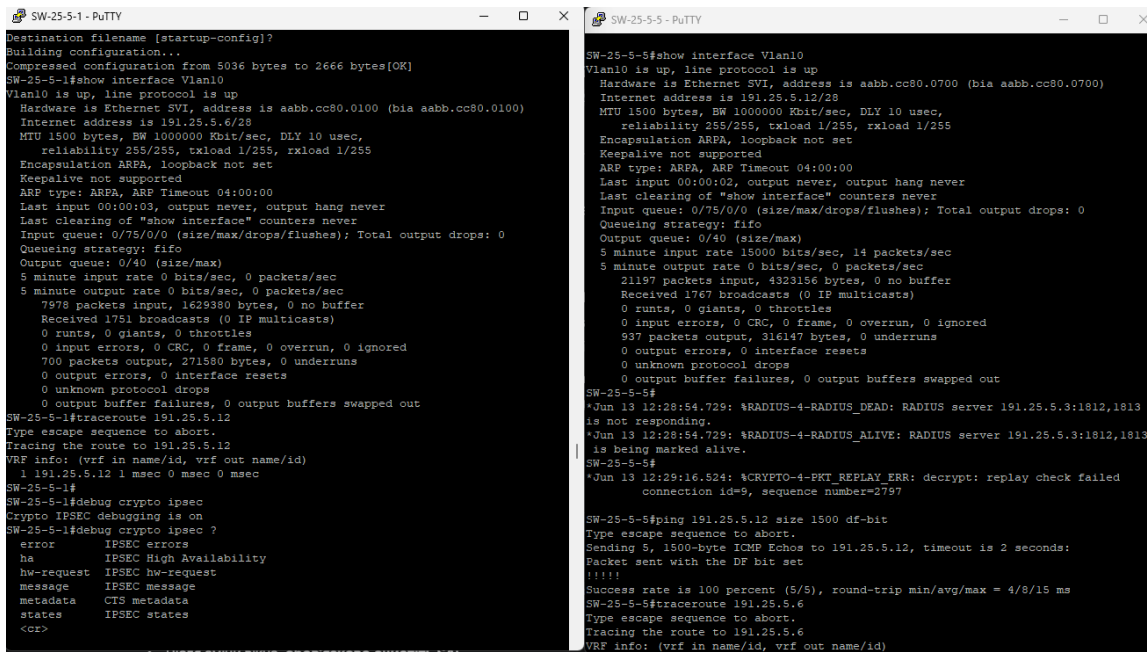


Рисунок 3.68 – Спроба перевірити причину помилки

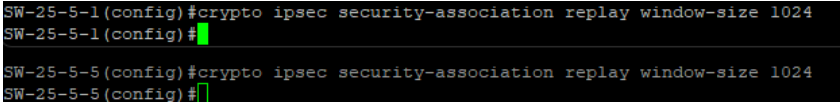


Рисунок 3.69 – Спроба вирішення проблеми

Спроби діагностики та вирішення включають в себе:

- перевірка інтерфейсів за допомогою команди “show interface Vlan10”, що в ролі каналів, на наявність помилок в лічильниках помилок;
- тестування командою “ping size 1500 df-bit” для перевірки підтримки MTU 1500 на всьому шляху без необхідності фрагментації;
- команда “tracert” з обох комутаторів дозволяє переконатися, що трафік проходить по симетричному шляху, без асиметричних маршрутів, які могли б спричинити зміну порядку пакетів або їхню затримку.;
- збільшення “вікна” останніх отриманих номерів пакетів (див. рис. 3.69), для дозволу системі сприймати розсинхронізацію або затримку пакетів.

```
User Access Verification
Username: user
*Jun 13 13:18:07.904: %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
connection id=13, sequence number=2796
Username: user1
Password:
% Authentication failed
Username: █
```

Рисунок 3.70 – Не вдалося вирішити помилку

```
*Jun 13 13:22:44.867: %SYS-5-CONFIG_I: Configured from console by adminkul on co
nsole
User Access Verification
Username: user1
Password:
SW-25-5-5>en
SW-25-5-5#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-25-5-5(config)#
*Jun 13 13:22:55.160: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by user1
on console
SW-25-5-5(config)# █
SW-25-5-1(config)#int vlan 10
SW-25-5-1(config-if)#no crypto map ipsec_map
SW-25-5-1(config-if)#ex
SW-25-5-1(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 5014 bytes to 2665 bytes[OK]
SW-25-5-1(config)# █
```

Рисунок 3.71 – Перевірка працездатності без тунелювання

Попередньо проведені діагностичні кроки дозволили виключити найбільш поширені мережеві причини проблеми, такі як фізичні помилки, перевантаження каналу, проблеми з MTU або асиметричною маршрутизацією. Це дозволяє зробити висновок, що проблема непрацездатності IPsec тунелю, що проявляється у вигляді PKT_REPLAY_ERR, лежить на більш високому рівні – імовірно, пов'язана з внутрішньою обробкою IPsec на комутаторах, такою як продуктивність центрального процесора, використання пам'яті, або є наслідком програмної помилки (багу) у поточному образі комутатора.

Враховуючи, що протокол IPSec допоміг уникнути вразливості пакетів RADIUS, можна рахувати, що проблема пакетів вирішена, але лише для сервера FreeRADIUS.

Далі буде налаштовано DAI з DHCP Snooping, а також Port Security.

Приклад налаштування попередніх двох протоколів на рівні доступу:

```
SW-25-5-5(config)#ip dhcp snooping
SW-25-5-5(config)#no ip dhcp snooping information option
SW-25-5-5(config)#ip dhcp snooping vlan 10,20,30,40
```

```

SW-25-5-5(config)#ip arp inspection vlan 10,20,30,40
SW-25-5-5(config)#ip arp inspection validate src-mac dst-mac
SW-25-5-5(config)#int eth 3/0
SW-25-5-5(config-if)#ip dhcp snooping trust
SW-25-5-5(config-if)#ip arp inspection trust
SW-25-5-5(config-if)#exit
SW-25-5-5(config)#int range eth0/1-3, eth1/0-3
SW-25-5-5(config-if-range)#switchport port-security
SW-25-5-5(config-if-range)#switchport port-security maximum 1
SW-25-5-5(config-if-range)#switchport port-security violation restrict
SW-25-5-5(config-if-range)#switchport port-security aging time 2
SW-25-5-5(config-if-range)#switchport port-security aging type inactivity
SW-25-5-5(config-if-range)#ip dhcp snooping limit rate 30
SW-25-5-5(config-if-range)#ip arp inspection limit rate 10 burst interval 1
SW-25-5-5(config-if-range)#exit
SW-25-5-5(config)#errdisable recovery cause all
SW-25-5-5(config)#errdisable recovery interval 120

```

Приклад налаштування, що й попередній, але на рівні розподілу:

```

SW-25-5-2(config)#int range eth 0/1, eth 0/3, eth 3/0
SW-25-5-2(config-if-range)#ip dhcp snooping trust
SW-25-5-2(config-if-range)#ip arp inspection trust
SW-25-5-2(config-if-range)#exit
SW-25-5-2(config)#ip dhcp snooping
SW-25-5-2(config)#no ip dhcp snooping information option
SW-25-5-2(config)#ip dhcp snooping vlan 10,20,30,40
SW-25-5-2(config)#ip arp inspection vlan 10,20,30,40
SW-25-5-2(config)#ip arp inspection validate src-mac dst-mac ip
SW-25-5-2(config)#int range eth3/3, eth 0/0
SW-25-5-2(config-if-range)#switchport port-security
SW-25-5-2(config-if-range)#switchport port-security maximum 1

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				100
Змн.	Арк.	№ докум.	Підпис	Дата		

```
SW-25-5-2(config-if-range)#switchport port-security violation restrict
SW-25-5-2(config-if-range)#switchport port-security aging time 2
SW-25-5-2(config-if-range)#switchport port-security aging type inactivity
SW-25-5-2(config)#ip source binding 0800.2750.7525 vlan 10 191.25.5.2 int
eth0/0
```

```
SW-25-5-2(config)#errdisable recovery cause all
```

```
SW-25-5-2(config)#errdisable recovery interval 120
```

Перевірка попередньо налаштованих безпекових протоколів буде виконано під час ініціації автентифікації на серверах RADIUS.

Машина злочинця, що здійснює спроби атак між сервером та користувачем, а також паралельно відбувається перегляд реакції комутатора, до якого під'єднаний злочинець, можна побачити на рис. 3.72 – 3.74, де явно видно активні дії захисних протоколів зі сторони комутатора.

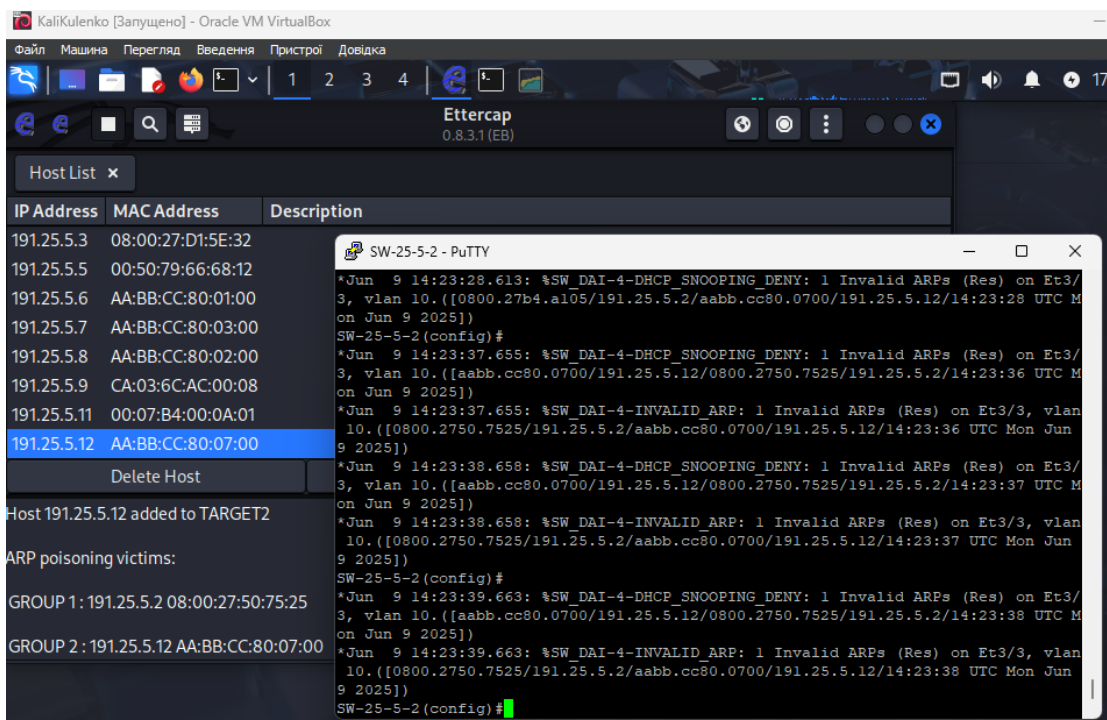


Рисунок 3.72 – Інтерфейс ПЗ Ettercap та повідомлення від комутатора

На цьому рисунку видно як блокується трафік за допомогою захисних механізмів DAI на пару з DHCP Snooping, а в інтерфейсі ПЗ Ettercap, на машині злочинця відсутні успішні дії.

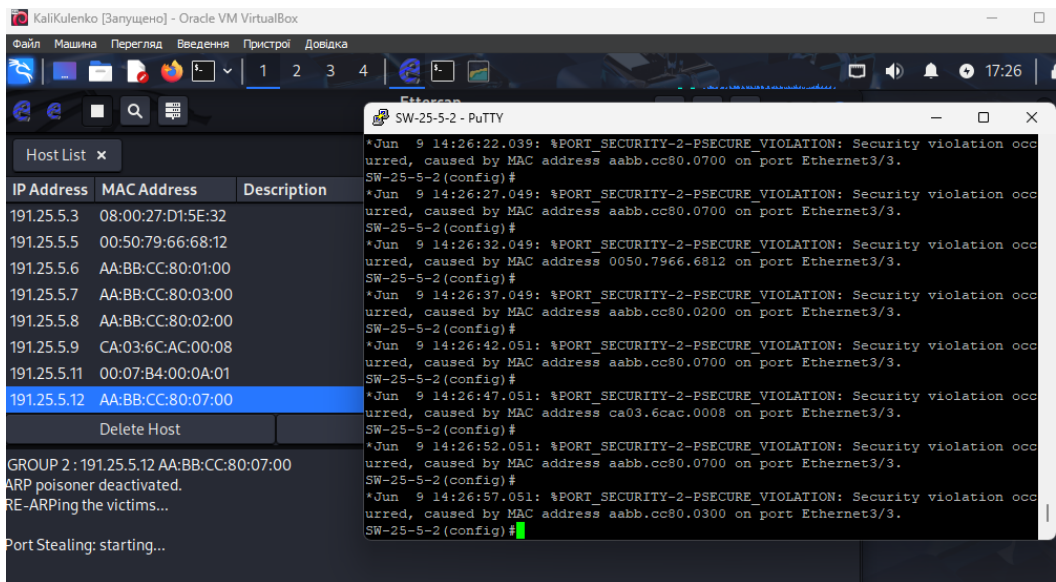


Рисунок 3.73 – Інтерфейс ПЗ Ettercap та повідомлення від комутатора

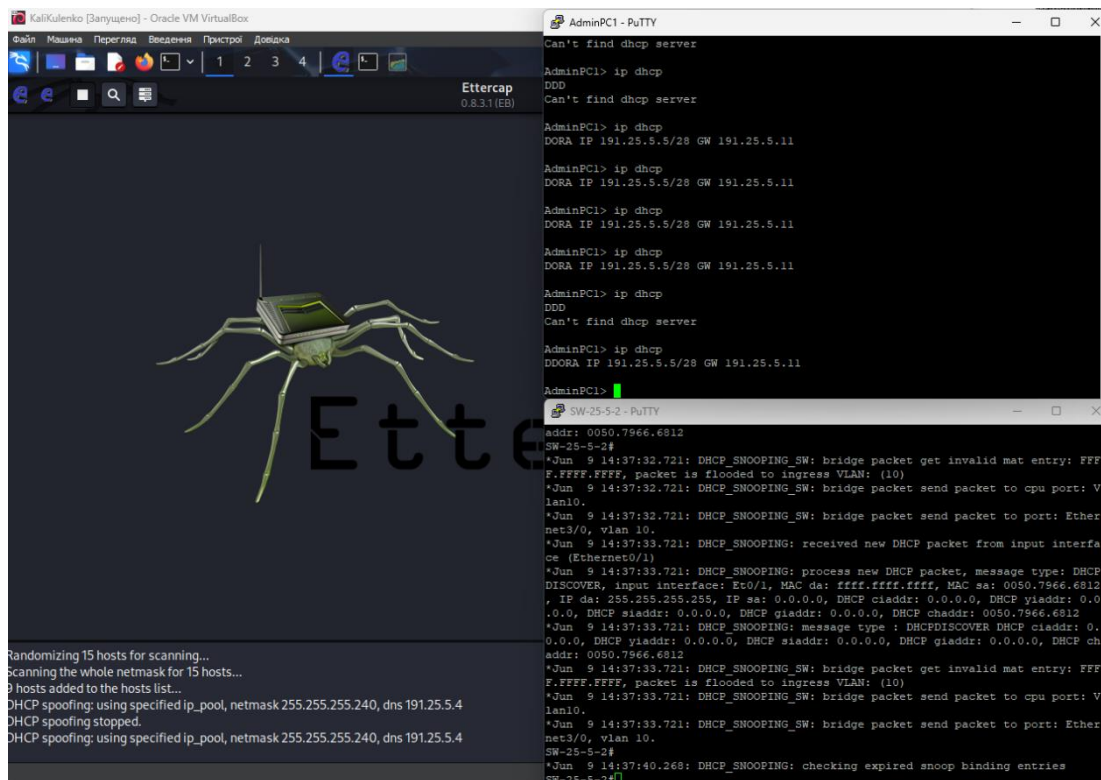


Рисунок 3.74 – Інтерфейс ПЗ Ettercap та повідомлення від комутатора

Залишилось налаштувати протокол 802.1X, а також впровадити аудит за допомогою встановлення серверу Syslog, налаштування його та клієнтів – мережевих пристроїв.

Приклад налаштування протоколу 802.1X зі сторони NAS, тобто комутаторів, що на рівні доступу, представлено далі:

SW-25-5-5(config)#dot1x system-auth-control

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		102

```
SW-25-5-5(config)#aaa authentication dot1x default group radserversGR
SW-25-5-5(config)#aaa authorization network default group radserversGR
SW-25-5-5(config)#int range eth0/0-3, eth1/0-3
SW-25-5-5(config-if-range)#authentication port-control auto
SW-25-5-5(config-if-range)#dot1x pae authenticator
```

На стороні серверу freeRADIUS буде налаштовано метод аутентифікації EAP-TLS між клієнтом Windows 7.

Для початку було створено ключі та запити на підписання сертифікатів, а також одразу і підписано за допомогою файлу сертифікаційного центру. Для безпеки було обмежено доступ всім, крім відповідного користувача та групи під назвою “freerad”. Попередні дії зображено на рис. 3.75.

```
root@student-VirtualBox:/etc/freeradius/3.0/certs# ls clients/
userW7.crt userW7.csr userW7.key userW7.pfx
root@student-VirtualBox:/etc/freeradius/3.0/certs# sudo chown -R freerad:freerad /etc/freeradius/3.0/certs
root@student-VirtualBox:/etc/freeradius/3.0/certs# sudo chmod -R 640 /etc/freeradius/3.0/certs
root@student-VirtualBox:/etc/freeradius/3.0/certs# sudo chmod 600 /etc/freeradius/3.0/certs/ca/ca.key
root@student-VirtualBox:/etc/freeradius/3.0/certs# sudo chmod 600 /etc/freeradius/3.0/certs/server/server.key
root@student-VirtualBox:/etc/freeradius/3.0/certs# sudo chmod 600 /etc/freeradius/3.0/certs/clients/*.key
root@student-VirtualBox:/etc/freeradius/3.0/certs# ls server/
server.crt server.csr server.key
root@student-VirtualBox:/etc/freeradius/3.0/certs# ls ca/
ca.crt ca.key
root@student-VirtualBox:/etc/freeradius/3.0/certs#
```

Рисунок 3.75 – Шляхи до створених файлів та зміна прав доступу

Також необхідно налаштувати та відредагувати конфігураційний файл методу автентифікації, що зображено на рис. 3.76 - 3.78.

```
GNU nano 6.2 mods-enabled/eap
#
# Invoke the default supported EAP type when
# EAP-Identity response is received.
#
# The incoming EAP messages DO NOT specify which EAP
# type they will be using, so it MUST be set here.
#
# For now, only one default EAP type may be used at a time.
#
# If the EAP-Type attribute is set by another module,
# then that EAP type takes precedence over the
# default type configured here.
#
default_eap_type = tls

# A list is maintained to correlate EAP-Response
# packets with EAP-Request packets. After a
# configurable length of time, entries in the list
# expire, and are deleted.
#
timer_expire = 60
```

Рисунок 3.76 – Конфігураційний файл EAP

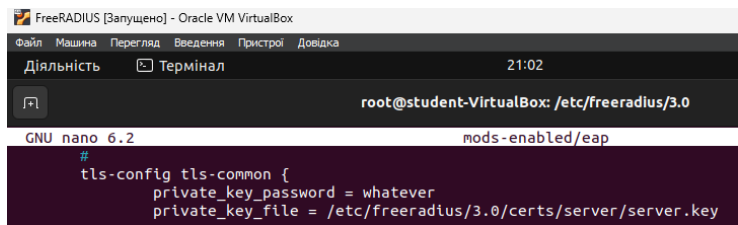


Рисунок 3.77 – Зміна шляхів до ключа

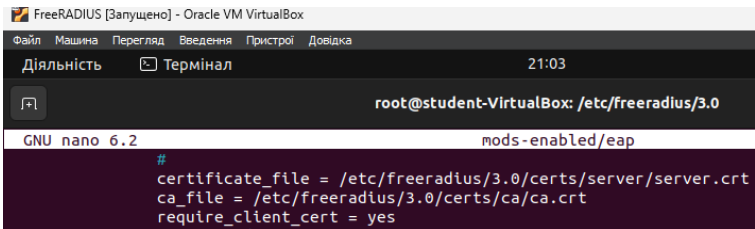


Рисунок 3.78 – Зміна шляхів до сертифікатів

Для встановлення тунелю TLS обов’язково потрібно мати на клієнтській машині: сертифікат довіреного органу та підписаний цим органом клієнтський сертифікат. Попередні дії було виконано на сервері Linux Ubuntu та передано необхідні файли на клієнтську ОС, за цим були спроби імпортування потрібних сертифікатів, як видно з рис. 3.79.

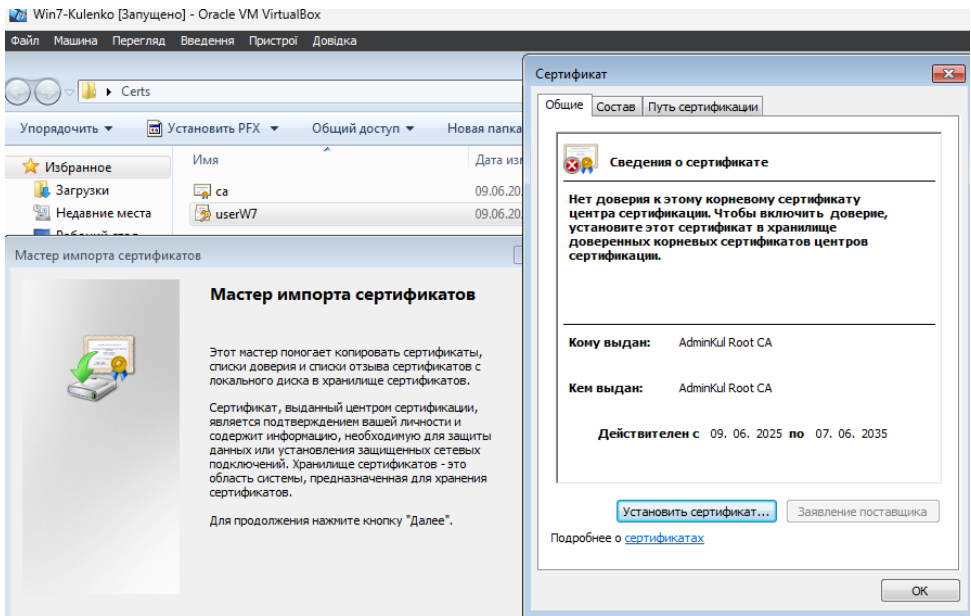


Рисунок 3.79 – Спроби імпортування сертифікатів на ОС Windows 7

Не вдалося імпортувати сертифікати на клієнт з ОС Windows 7. Тому було успішно протестовано на ОС Windows 10. Процес імпортування той же самий, що й було продемонстровано на попередньому рисунку.

Після імпортування виконується налаштування з'єднання за допомогою вибору методу автентифікації і обирання сертифікатів серверу, з яким планується встановлення безпечного тунелю. Успішне налаштування та встановлення зв'язку видно на рис. 3.80.

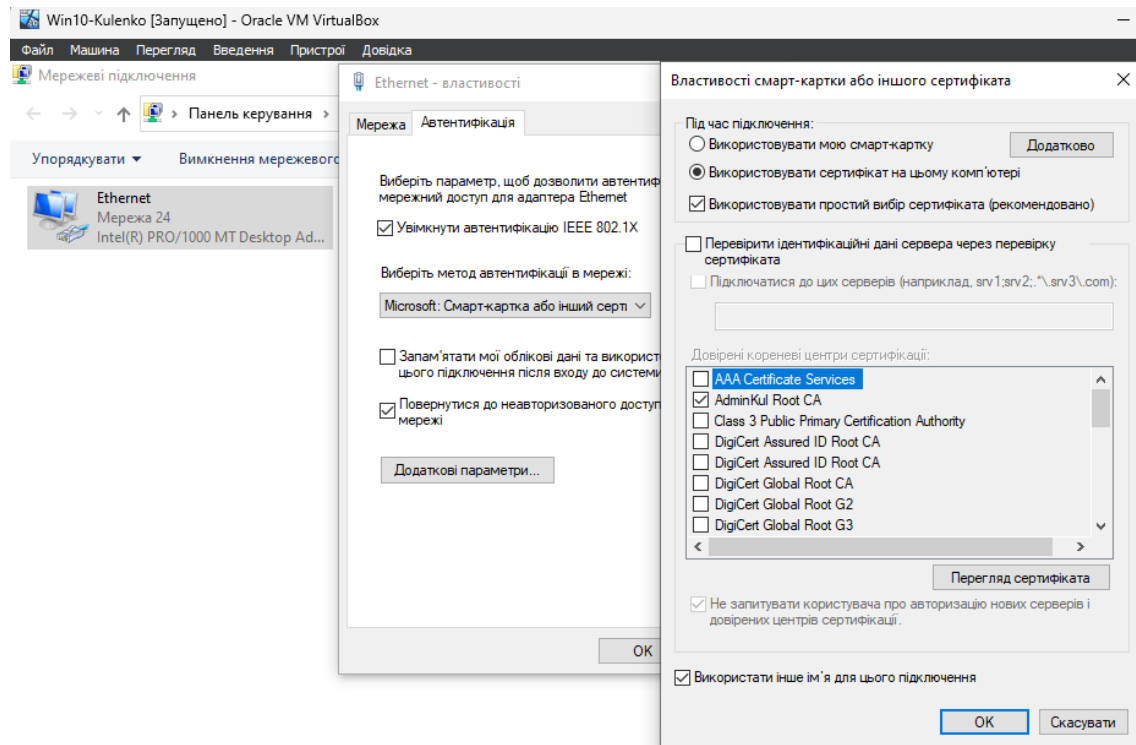


Рисунок 3.80 – Вибір методу та сертифікату з'єднання

Підтвердження успішного встановлення тунельного з'єднання TLS є отримання доступу до мережі (див. рис. 3.81).

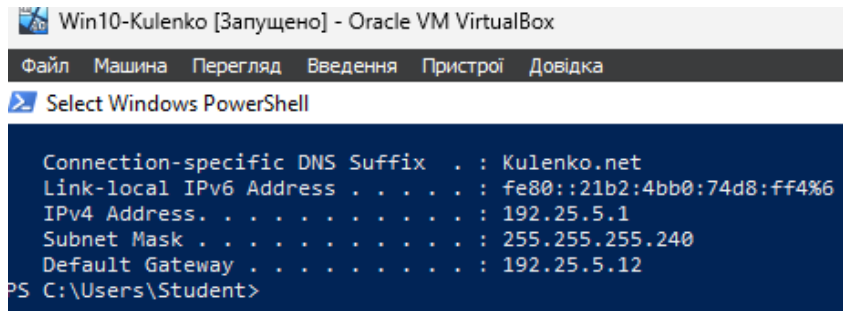


Рисунок 3.81 – Успішне отримання доступу до мережі

Для остаточного розуміння того, що автентифікація успішно працює і встановлено TLS-з'єднання, це було перевірено запуском сервера у debug-режимі (див. рис. 3.82).


```

Win7-Kulenko [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
C:\Windows\system32\cmd.exe

C:\Users\Admin>ipconfig

Windows IP Configuration

Ethernet adapter ?????????? ?? ????????? ?????:

    Connection-specific DNS Suffix  . : Kulenko.net
    Link-local IPv6 Address . . . . . : fe80::4d43:b0d4:6db1:d209%11
    IPv4 Address. . . . . : 193.25.5.1
    Subnet Mask . . . . . : 255.255.255.240
    Default Gateway . . . . . : 193.25.5.10

Tunnel adapter isatap.Kulenko.net:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : Kulenko.net

Tunnel adapter 6TO4 Adapter:

    Connection-specific DNS Suffix  . : Kulenko.net
    IPv6 Address. . . . . : 2002:c119:501::c119:501
    Default Gateway . . . . . : 2002:c058:6301::c058:6301

C:\Users\Admin>_

```

Рисунок 3.84 – Консоль управління клієнта з виданим адресом підмережі

Задля забезпечення всебічного аудиту та моніторингу мережі буде встановлено Syslog-сервер на ті ж самі сервера, що містять RADIUS-сервера, для ОС Windows обрано таке рішення як “Visual Syslog Server”, а для ОС Linux Ubuntu – “rsyslog”.

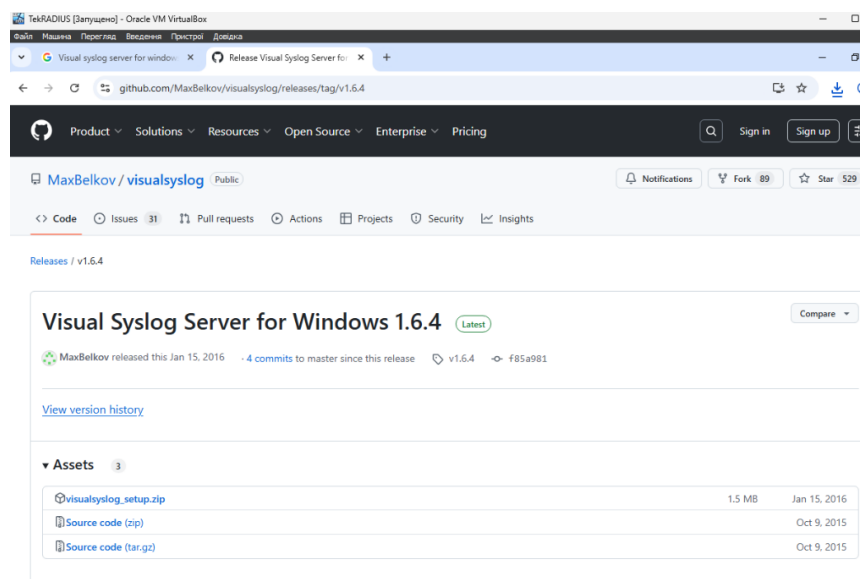


Рисунок 3.85 – Сторінка встановлення Syslog-сервера для Windows

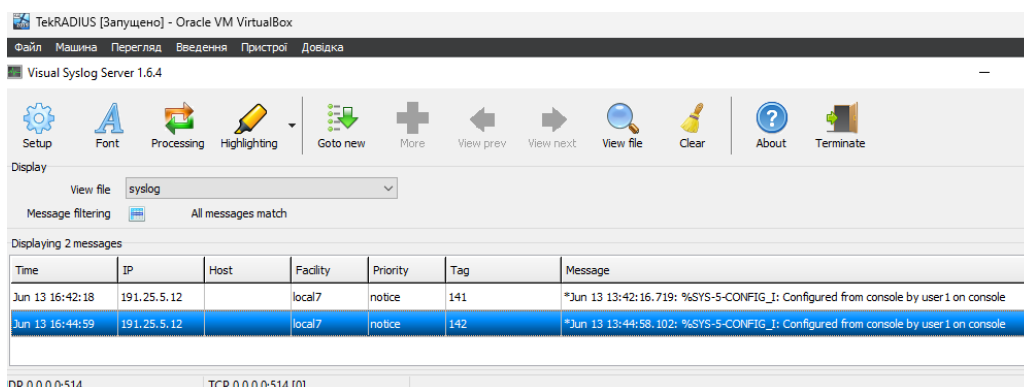


Рисунок 3.86 – Інтерфейс ПЗ Visual Syslog Server

```

student@student-VirtualBox: ~$ sudo apt install rsyslog
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей... Виконано
Зчитування інформації про стан... Виконано
rsyslog вже є новішою версією (8.2112.0-2ubuntu2.2),
оновлено 0, встановлено 0 нових, 0 відмічено для видалення і 3 не оновлено.
student@student-VirtualBox: ~$ cat /etc/rsyslog.d/40-cisco.conf
# Модуль для прийому по UDP
module(load="imudp")
input(type="imudp" port="514")

# Модуль для прийому по TCP
module(load="imtcp")
input(type="imtcp" port="514")

# Створимо динамічний шлях до файлу
$Stemplate RemoteCiscologs, "/var/log/cisco/%HOSTNAME%.log"

# Якщо повідомлення прийшло з нашої мережі...
if $fromhost-ip starts with '191.25.5.' then {
    # ...тоді записати його у файл, використовувати наш шаблон.
    action(type="omfile" dynaFile="RemoteCiscologs")

    # & - означає "зупинити подальшу обробку цього повідомлення".
    # Це потрібно, щоб логи Cisco не дублювалися у загальний /var/log/syslog.
    & ~
}

student@student-VirtualBox: ~$ tree /var/log/cisco/
/var/log/cisco/
└── 191.25.5.12.log

0 directories, 1 file
student@student-VirtualBox: ~$ cat /var/log/cisco/191.25.5.12.log
Jun 13 19:12:38 191.25.5.12 147: *Jun 13 16:12:16.099: %SYS-3-LOGGINGHOST_FAIL: Logging to host 191.25.5.3 port 514 failed
Jun 13 19:12:38 191.25.5.12 148: *Jun 13 16:12:28.102: %SYS-3-LOGGINGHOST_FAIL: Logging to host 191.25.5.2 port 514 failed
Jun 13 19:15:34 191.25.5.12 149: *Jun 13 16:15:27.478: %SYS-5-CONFIG_I: Configured from console by user1 on console
student@student-VirtualBox: ~$

```

Рисунок 3.87 – Встановлено та налаштовано ПЗ rsyslog

Схожа ситуація як з рішенням RADIUS-серверів, в ОС Windows встановлення ПЗ відбувається набагато простіше, але і при цьому більшість конфігураційних файлів та налаштувань присутні на ОС Linux Ubuntu.

3.5 Перевірка працездатності підсистеми автентифікації

Перевірка буде відбуватися тестуванням головних мережевих функцій і працездатності, які були втілені та налаштовані раніше. Це потрібно щоб зрозуміти чи можна назвати налагоджену підсистему такою, що виконує поставлені раніше цілі та водночас порівняти можливості двох серверів на практиці.

Спочатку буде проведено тестування правильного налаштування VLAN та списків доступу (на певний час вимкнено dot1x).

Після цього буде протестовано і продемонстровано роботу протоколу 802.1x з Static та Dynamic VLAN, разом з цим як себе ведуть сервера та NAS-пристрої під час автентифікації.

Процес перевірки відбуватиметься у вигляді перевірки зв'язку між різним групами VLAN (сегментами мережі), а також накладених правил списку доступу на ці сегменти.

Виконані тести перших двох сегментів представлені на рис. 3.88 та рис 3.89.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		108

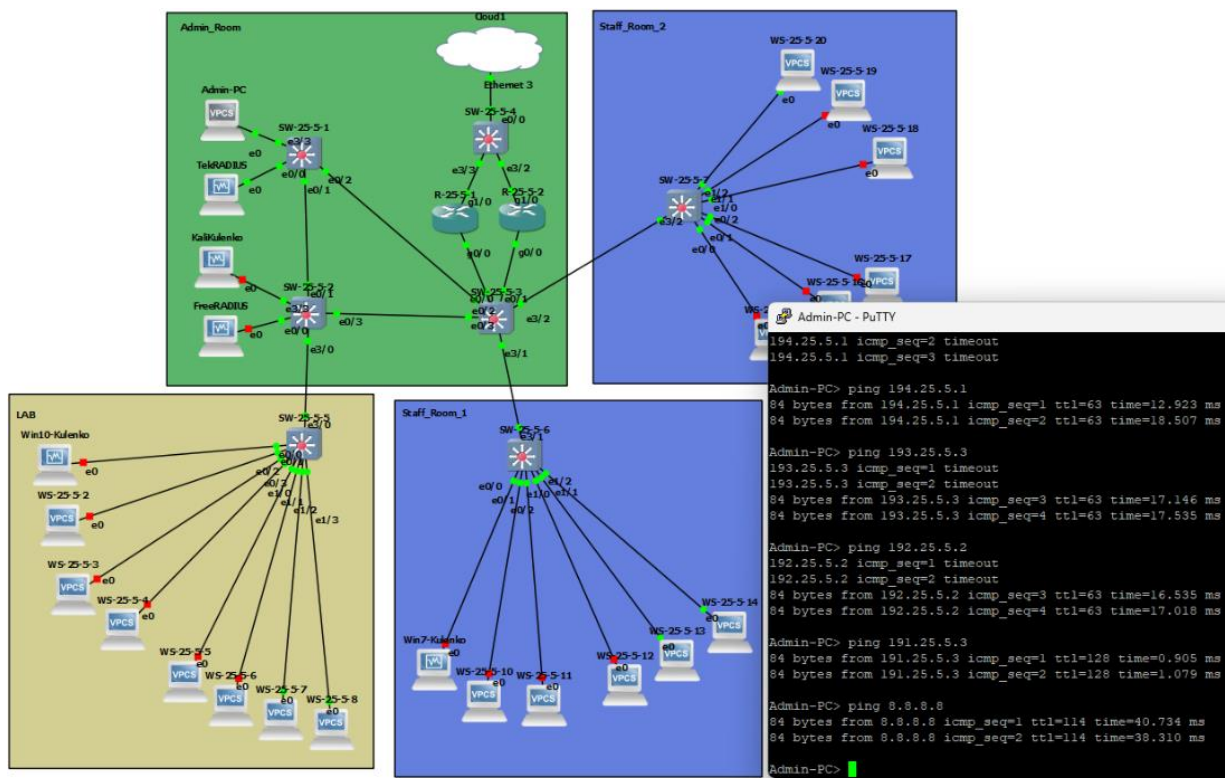


Рисунок 3.88 – Перевірка зв'язку з VLAN 10

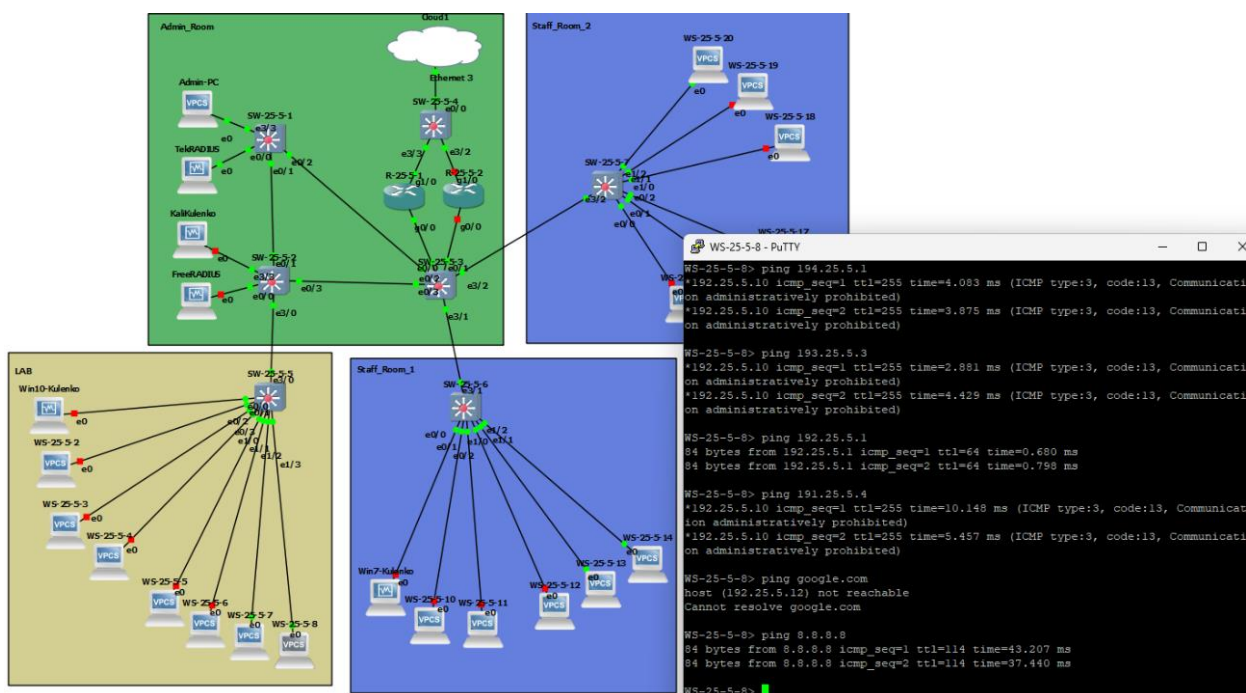


Рисунок 3.89 – Перевірка зв'язку з VLAN 20

Успішно перевірено два сегмента мережі на працездатність запланованої та побудованої мережі.

Перевіримо ще два сегменти, що представлено на рис. 3.90 та рис. 3.91.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				109
Змн.	Арк.	№ докум.	Підпис	Дата		

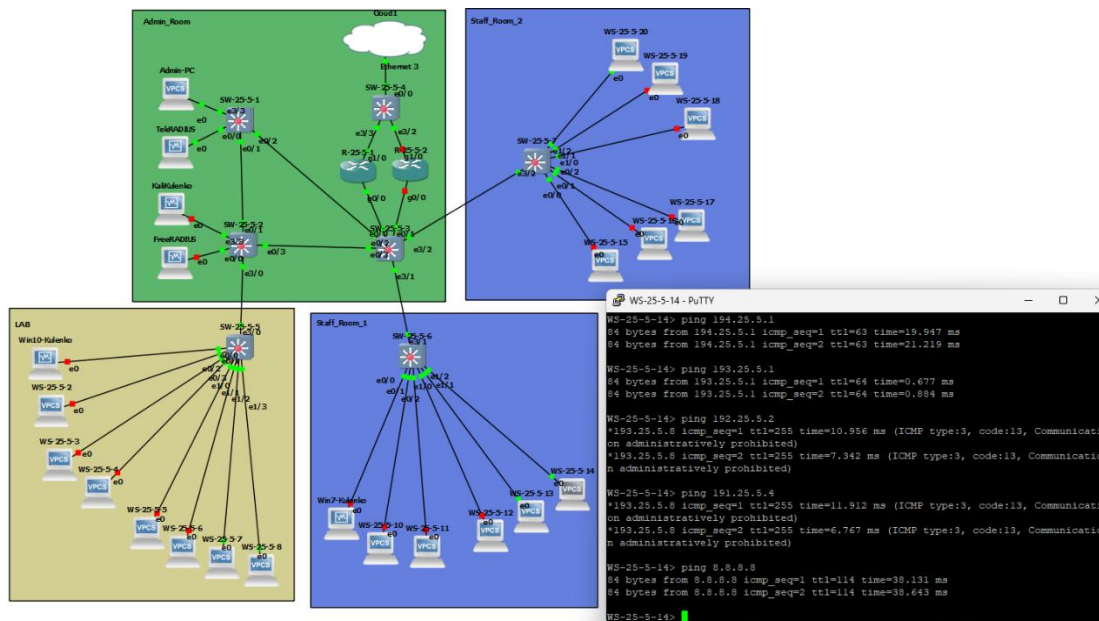


Рисунок 3.90 – Перевірка зв'язку з VLAN 30

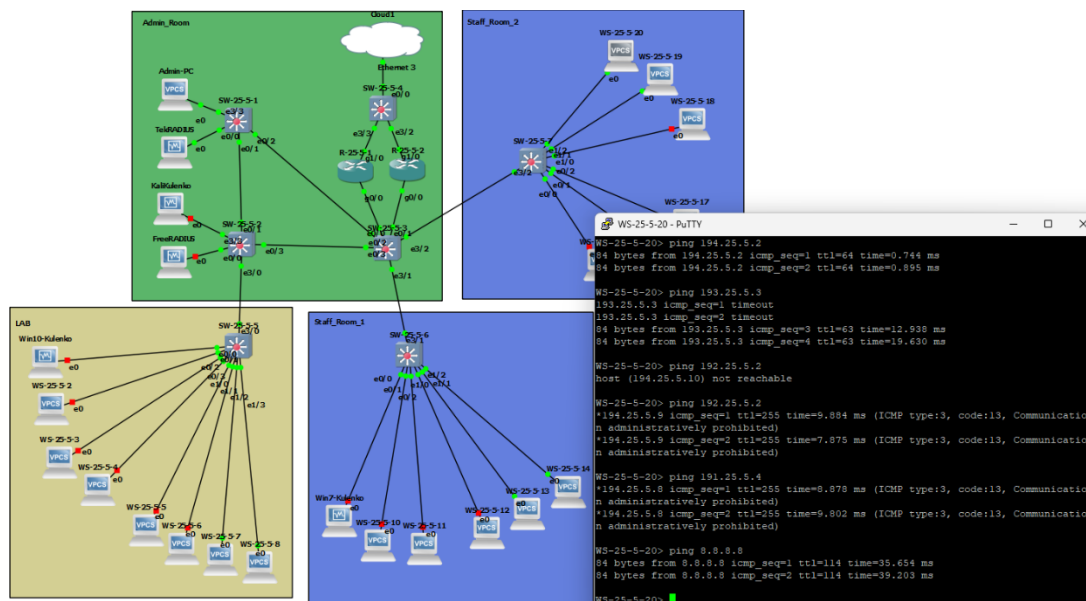


Рисунок 3.91 – Перевірка зв'язку з VLAN 40

Списки доступу та VLAN налаштовані коректно і повністю виконують свої функції так як потрібно.

Наступним пунктом буде перевірка функціонування серверів RADIUS з протоколом 802.1x без Dynamic VLAN.

Спочатку перевіримо автентифікацію FreeRADIUS сервера з клієнтом за допомогою метода EAP-TLS.

Було підготовлено невеличкий список користувачів для тесту (див. рис. 3.92).

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				110
Змн.	Арк.	№ докум.	Підпис	Дата		

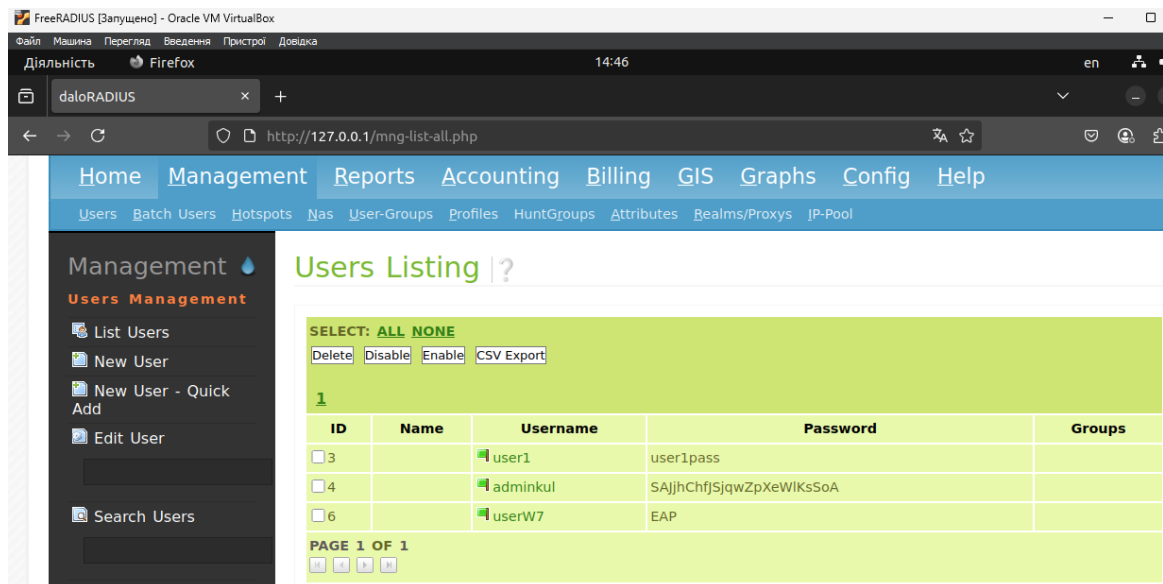


Рисунок 3.92 – База даних сервера

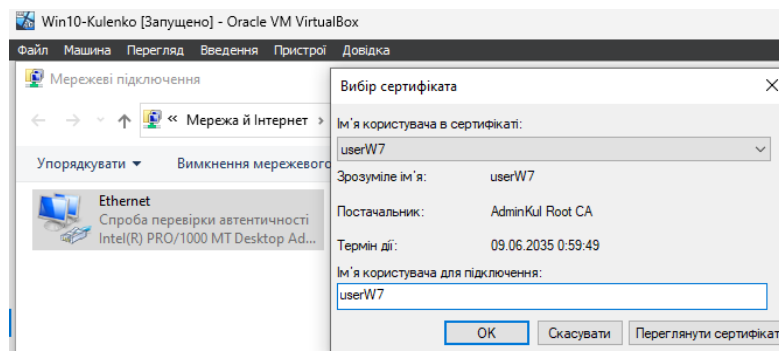


Рисунок 3.93 – Вибір користувача з сертифікату

Для перевірки TLS-з'єднання паралельно показано отриману адресу та виконано довідникові команди на комутаторі (аутентифікатор) доступу.

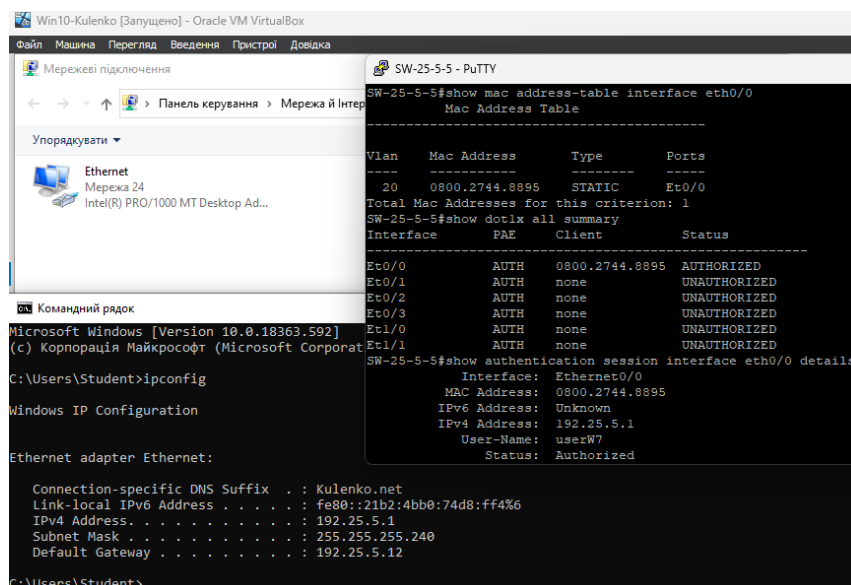


Рисунок 3.94 – Успішний доступ до мережі

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				111
Змн.	Арк.	№ докум.	Підпис	Дата		


```
FreeRADIUS [Запущено] - Oracle VM VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
Діяльність Термінал
root@student-VirtualBox: /home/student

(60) } # authenticate = reject
(60) Failed to authenticate the user
(60) Using Post-Auth-Type Reject
(60) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(60) Post-Auth-Type REJECT {
(60) sql: EXPAND .query
(60) sql: --> .query
(60) sql: Using query template 'query'
rlm_sql (sql): Reserved connection (16)
(60) sql: EXPAND %{User-Name}
(60) sql: --> user1
(60) sql: SQL-User-Name set to 'user1'
(60) sql: EXPAND INSERT INTO radpostauth (username, pass, reply, authdate) VALUES ( '%{SQL-User-Name}', '%{User-Password}:%{Chap-Password}', '%{reply:Packet-Type}', '%S.%M' )
(60) sql: --> INSERT INTO radpostauth (username, pass, reply, authdate) VALUES ( 'user1', '', 'Access-Reject', '2025-06-14 14:48:42.486975' )
(60) sql: Executing query: INSERT INTO radpostauth (username, pass, reply, authdate) VALUES ( 'user1', '', 'Access-Reject', '2025-06-14 14:48:42.486975' )
(60) sql: SQL query returned: success
(60) sql: 1 record(s) updated
rlm_sql (sql): Released connection (16)
(60) [sql] = ok
(60) attr_filter.access_reject: EXPAND %{User-Name}
(60) attr_filter.access_reject: --> user1
(60) attr_filter.access_reject: Matched entry DEFAULT at line 11
(60) [attr_filter.access_reject] = updated
(60) [eap] = noop
(60) policy remove_reply_message_if_eap {
(60) if (&reply:EAP-Message && &reply:Reply-Message) {
(60) if (&reply:EAP-Message && &reply:Reply-Message) -> FALSE
(60) else {
(60) [noop] = noop
(60) } else = noop
(60) } # policy remove_reply_message_if_eap = noop
(60) } # Post-Auth-Type REJECT = updated
(60) Delaying response for 1.000000 seconds
making up in 0.3 seconds.
making up in 0.6 seconds.
(60) Sending delayed response
(60) Sent Access-Reject Id 63 from 191.25.5.2:1812 to 191.25.5.12:1645 length 44
```

Рисунок 3.98 – Сервер у debug-режимі під час безуспішного з’єднання

Username	Password	Start Time	RADIUS Reply
user1		2025-06-14 14:48:42.486975	Access-Reject
user1		2025-06-14 14:45:55.203202	Access-Accept
user1		2025-06-14 14:44:09.967298	Access-Accept
userW7		2025-06-14 14:43:19.967245	Access-Accept
userW7		2025-06-14 14:43:13.257390	Access-Accept
userW7		2025-06-14 14:42:56.438437	Access-Accept
userW7		2025-06-14 14:36:21.594368	Access-Accept
userW7		2025-06-14 14:32:39.617595	Access-Accept
host/userW7		2025-06-14 14:30:46.714178	Access-Accept

Рисунок 3.99 – Перегляд останніх спроб аутентифікації

Схожі порівняльні тести будуть виконані за допомогою сервера TekRADIUS.

Так само, підготовлений список користувачів на рис. 3.100.

Username	Group
adminkultek	AdminPC
admintek	Default
user1	Default
user1stKIV	UserST1PC
user2	Default
user2stSAV	UserST2PC
userlabVBV	UserLABPC

Рисунок 3.100 – Список створених користувачів

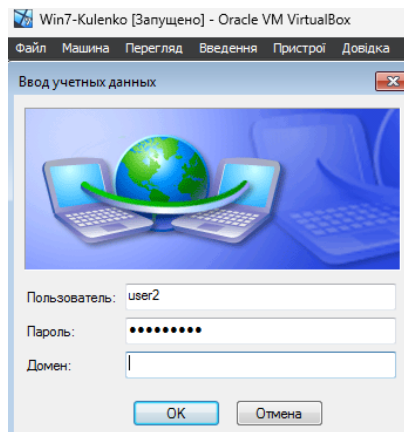


Рисунок 3.101 – Форма входу на клієнті Windows 7

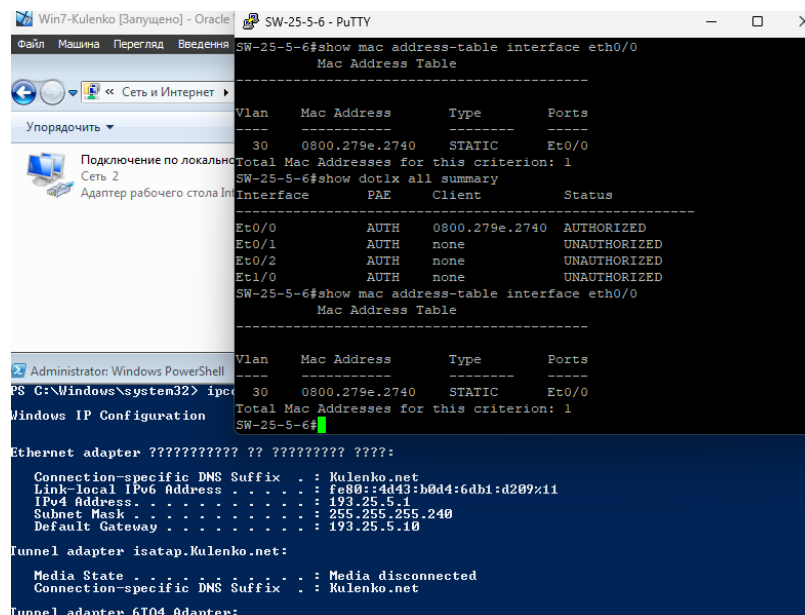


Рисунок 3.102 – Успішна автентифікація

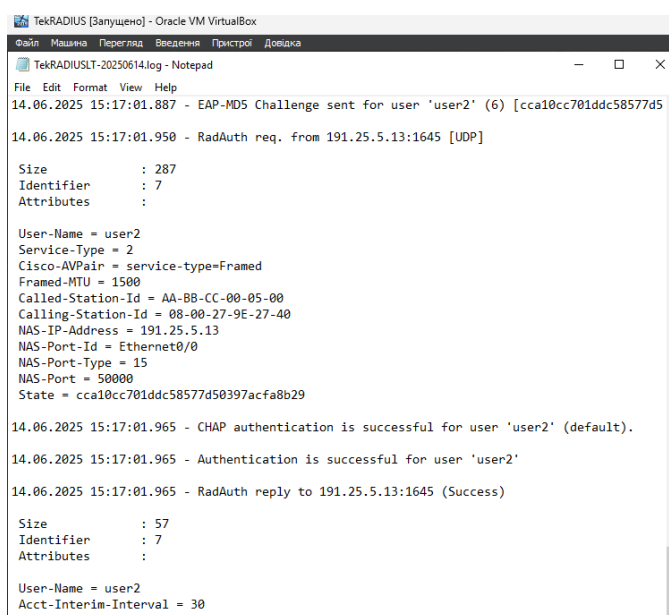


Рисунок 3.103 – Перегляд файлу журналювання

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				114
Змн.	Арк.	№ докум.	Підпис	Дата		

Також перевірено невдалий результат автентифікації на наступних рисунках.



Рисунок 3.104 – Форма з некоректними даними

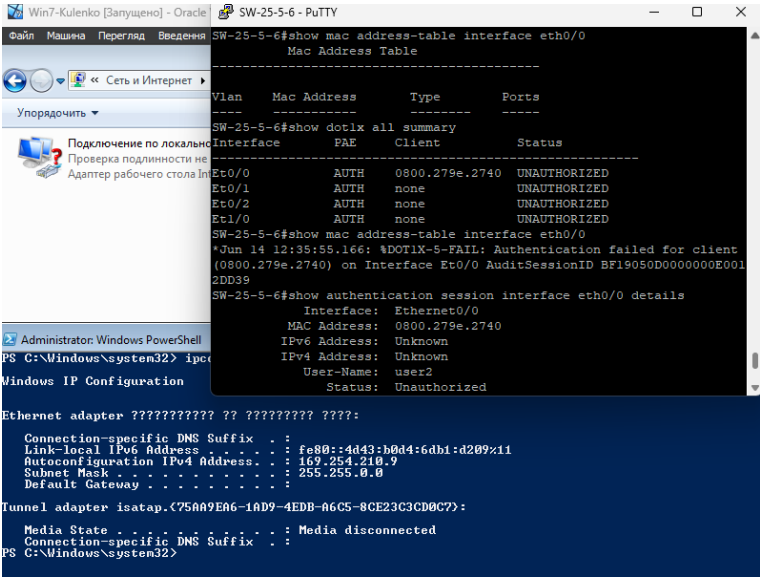


Рисунок 3.105 – Підтверджуючі командний рядок та комутатор

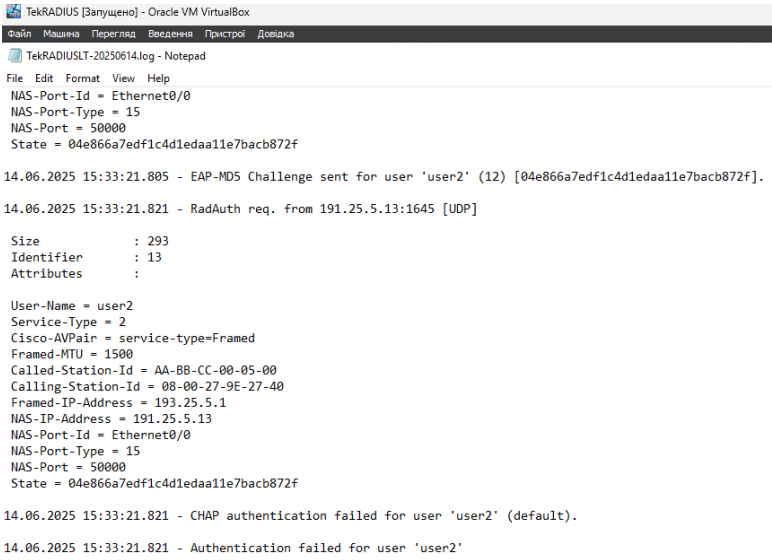


Рисунок 3.106 – Файл журналювання з невдалою автентифікацією

Наступним кроком тестування буде використання RADIUS-серверів з Dynamic VLAN, це потрібно виконати для порівняння зручності налаштування груп користувачів та функціональної перевірки працездатності Dynamic VLAN.

Задля тестування було створено групи, що мають по декілька атрибутів, які вказують на відповідність певній групі VLAN. Щоб реалізувати даний механізм потрібно вимкнути на комутаторах рівня доступу відповідність портів певним групам VLAN, щоб коректно працював цей механізм.

Приклад вимикання відповідності групам VLAN:

SW-25-5-5(config)#int range eth0/0-3, eth1/0-2

SW-25-5-5(config-if-range)#no switchport access vlan 20

Попередні дії було також виконано в підмережах LAB, Staff_Room_1/2.

Спочатку проведемо перевірку з сервером FreeRADIUS.

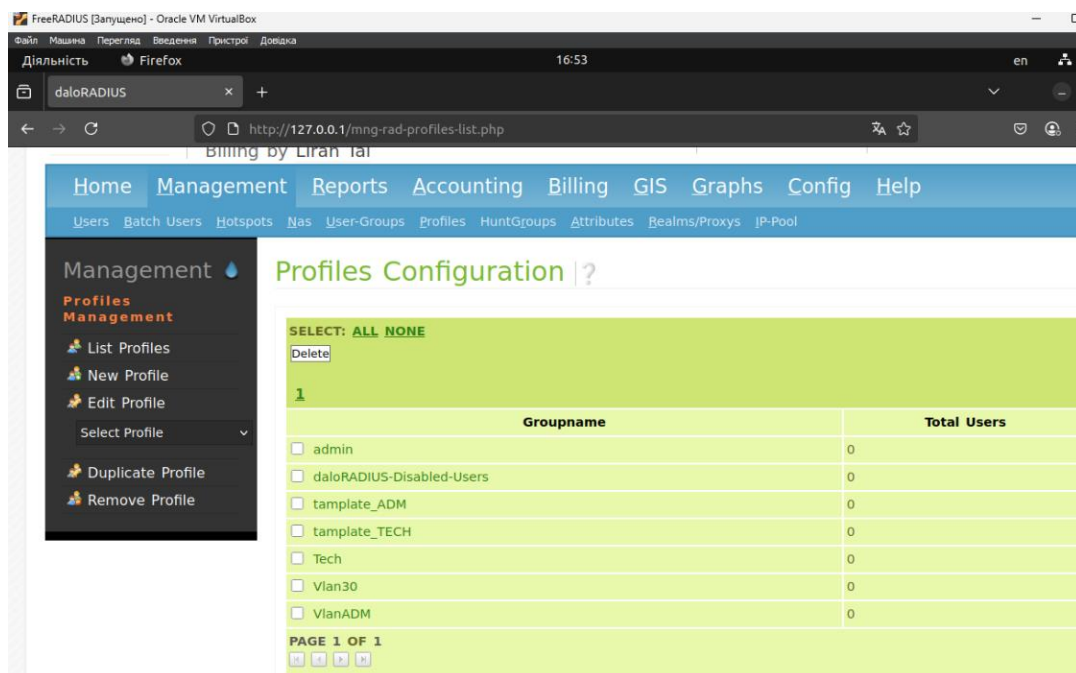


Рисунок 3.107 – Список створених груп користувачів

Із наведених на рис. 3.107, буде застосовано групи Vlan30 та VlanADM. В цих двох групах присутні такі атрибути як: Tunnel-Type (тип тунельного протоколу), Tunnel-Medium-Type (тип протоколу, що буде інкапсульований) та Tunnel-Private-Group-Id (група належності до VLAN).

Буде розписано застосовані атрибути, наприклад для групи Vlan30. Tunnel-Type = 13 (VLAN), Tunnel-Medium-Type = 6 (802), Tunnel-Private-Group-Id = 30 (номер групи VLAN). Дані атрибути видно з рис. 3.108.

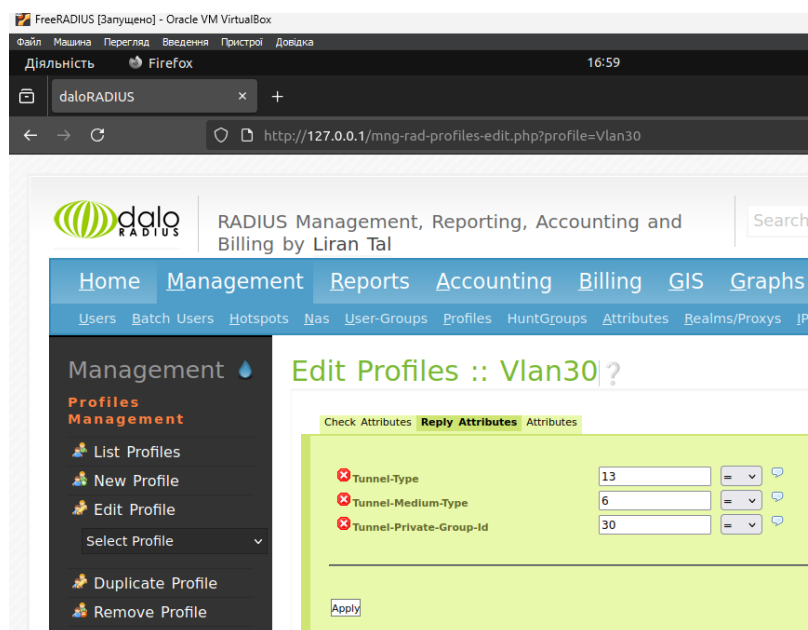


Рисунок 3.108 – Форма налаштованих атрибутів Dynamic VLAN

Для експерименту створено користувачів, для існуючих груп. Приклад їх створення наведено на наступному рис. 3.109.

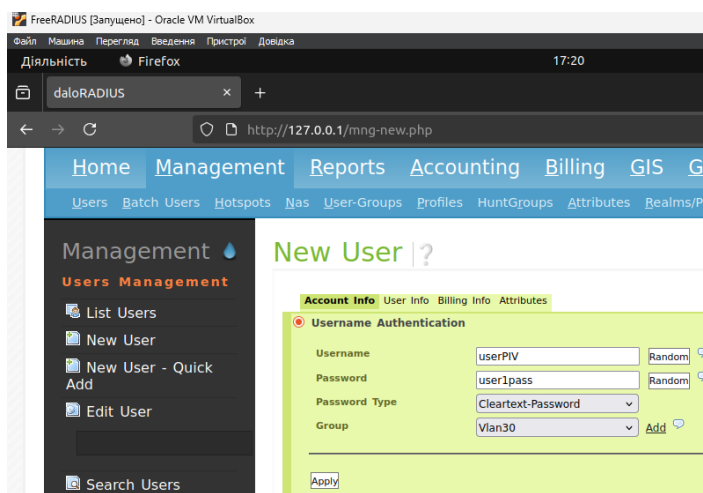


Рисунок 3.109 – Форма створення користувача

Було під'єднано віртуальні комп'ютери з інших підмереж, для перевірки працездатності Dynamic VLAN.

По аналогії з експериментами з Static VLAN, порядок тестування залишився незмінним.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				117
Змн.	Арк.	№ докум.	Підпис	Дата		

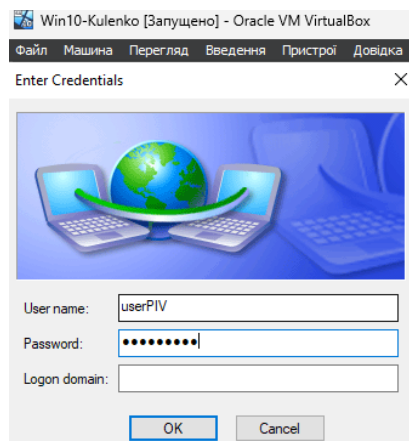


Рисунок 3.110 – Виконання аутентифікації до Ubuntu-сервера

Деяка відмінність все ж присутня – це перевірка зв’язку з іншими підмережами, включаючи перевірку з WAN (див. рис. 3.111).

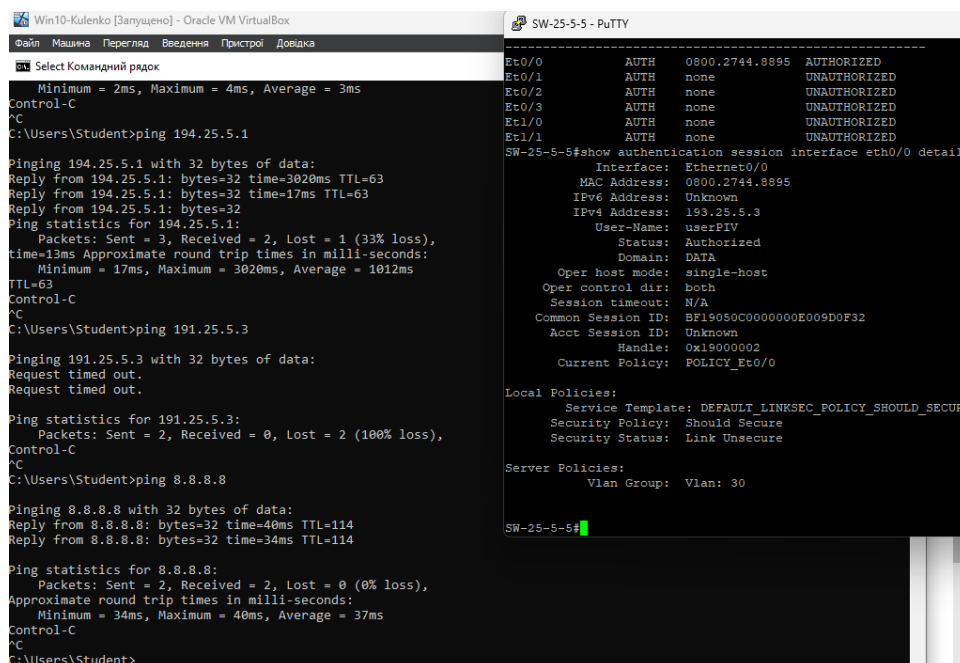


Рисунок 3.111 – Перевірка зв’язку та довідникові команди комутатора

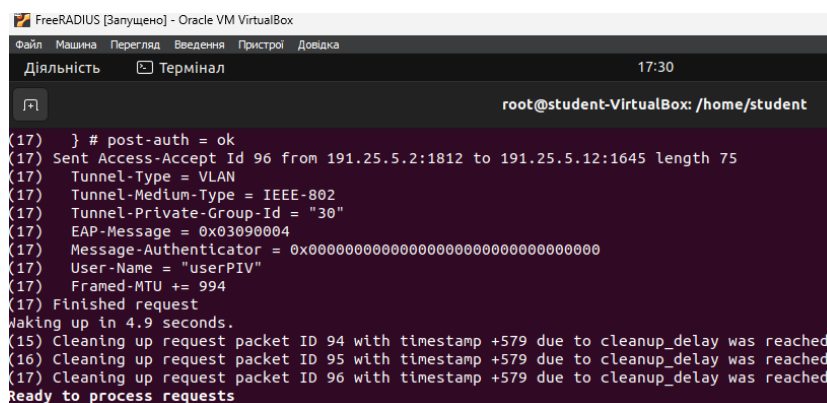


Рисунок 3.112 – Сервер під час перевірки коректних даних

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				118
Змн.	Арк.	№ докум.	Підпис	Дата		

На наступному рис. 3.113 відображено підключення користувача до того ж сервера, з належністю до групи VLAN10, та паралельними перевірками зв'язку та довідникових команд комутатора, для наочності експерименту.

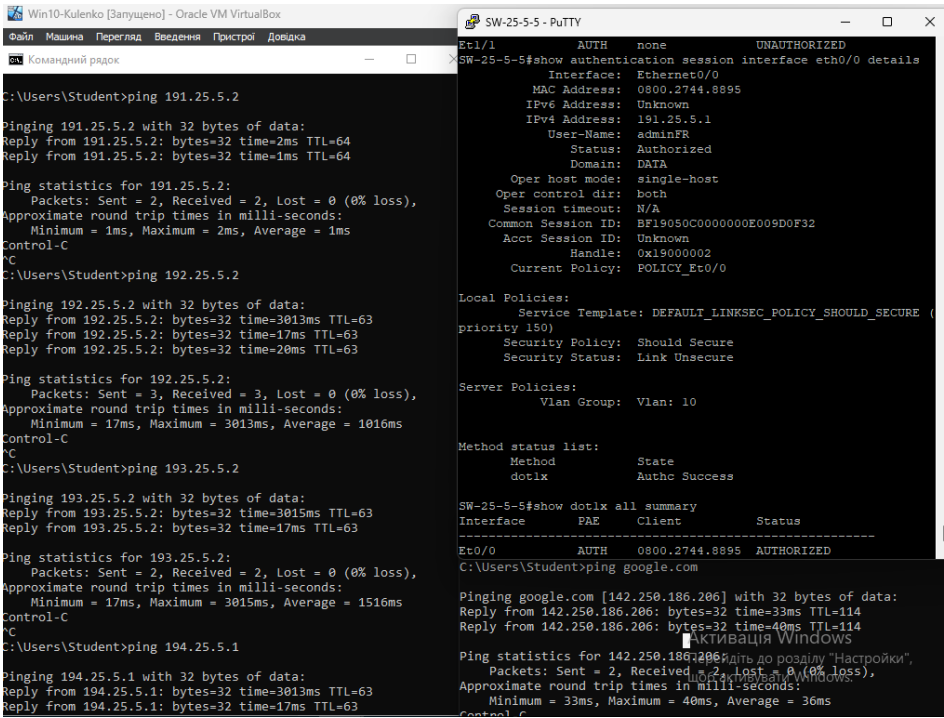


Рисунок 3.113 – Перевірка зв’язку та довідникові команди комутатора

Тепер буде протестовано працездатність, попередньо перевіреного механізму, на Windows-сервері. Це відбуватиметься у підмережі Staff_Room_2.

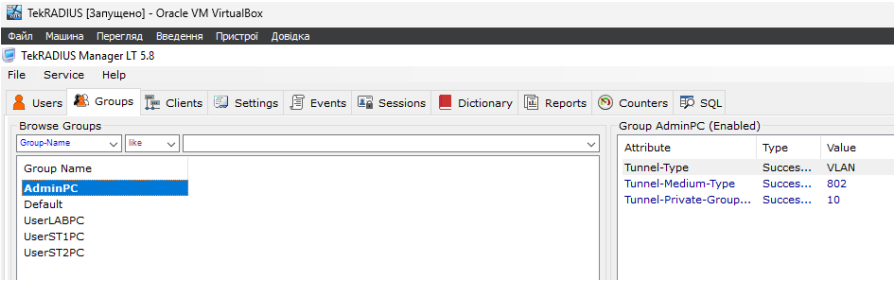


Рисунок 3.114 – Список створених груп користувачів

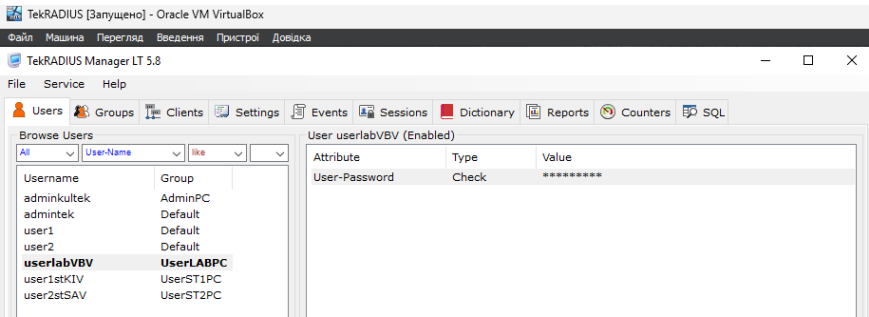


Рисунок 3.115 – Список створених користувачів

На рис. 3.116 використано користувача user1stKIV, що відповідає групі VLAN20.

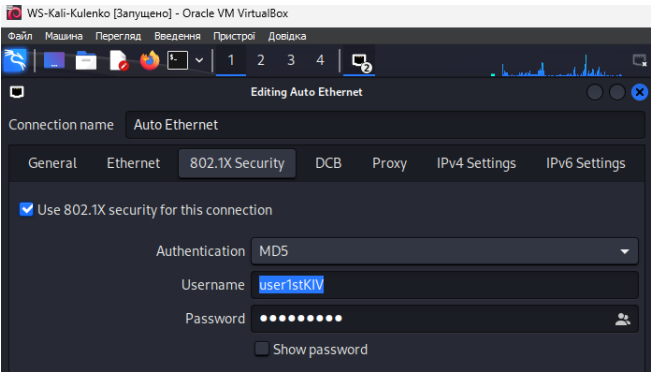


Рисунок 3.116 – Виконання аутентифікації на клієнті Kali Linux

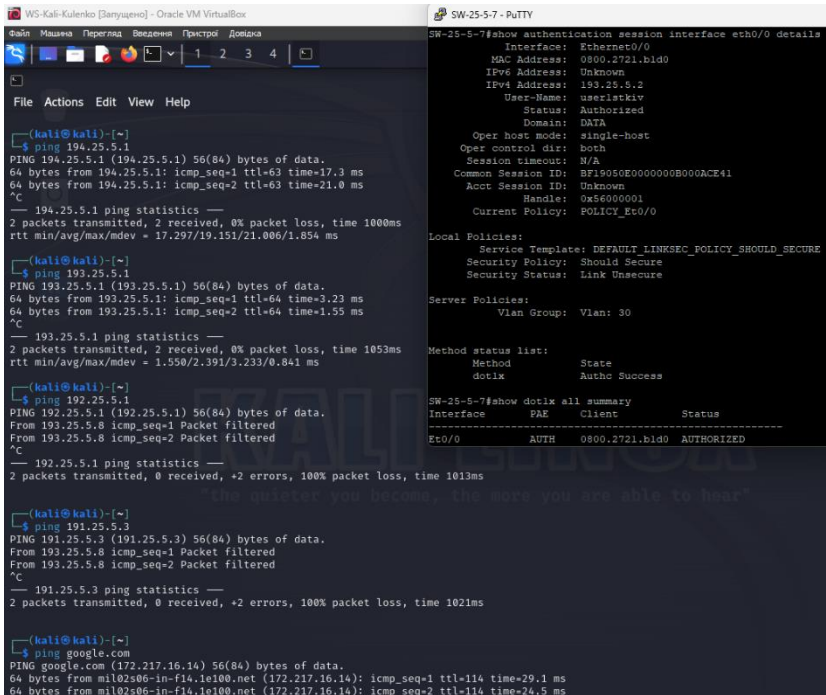


Рисунок 3.117 – Перевірка зв’язку та довідникові команди комутатора

На рис. 3.118 для порівняння виконано вхід за користувачем adminkultek (VLAN 10).

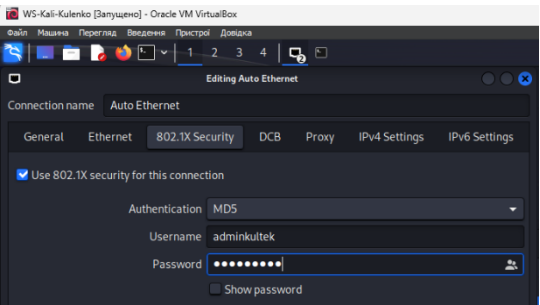


Рисунок 3.118 – Здійснення аутентифікації на клієнті Kali Linux

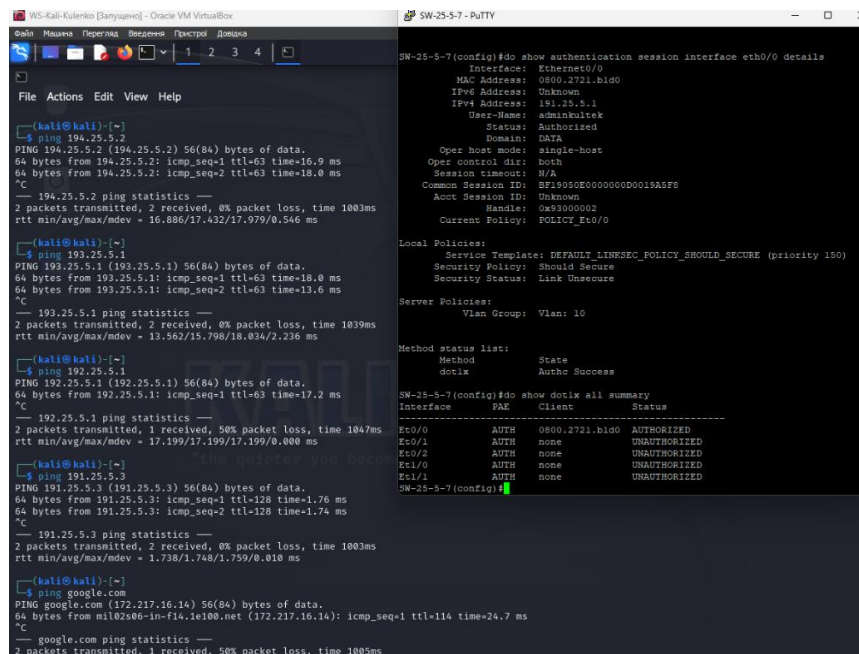


Рисунок 3.119 – Перевірка зв’язку та довідникові команди комутатора

Висновки до третього розділу

У третьому розділі реалізовано прототип підсистеми аутентифікації в середовищі GNS3: налаштовано сегментацію VLAN, резервування через GLBP та захищене адміністрування по SSH; встановлено TekRADIUS на Windows Server та FreeRADIUS із веб-інтерфейсом daloRADIUS на Ubuntu. Порівняно GUI TekRADIUS і конфігурацію через файли в FreeRADIUS, підтвердивши простоту початкового налаштування та гнучкість тонкого налаштування. Перевірено безпеку шляхом моделі Man-in-the-Middle (ARP Poisoning) і додано перевірку Message-Authenticator, а також налаштовано IPSec-тунель для захисту RADIUS-трафіку за обмежень віртуалізації та ОС. Для запобігання підроблення DHCP-повідомлень реалізовано Dynamic ARP Inspection та DHCP Snooping із Port Security. Інтеграція 802.1X із динамічним призначенням VLAN і централізованим журналюванням через Syslog продемонструвала виконання ключових функцій аутентифікації, авторизації й обліку.

Таким чином, третій розділ підтвердив працездатність обраних рішень у лабораторних умовах і визначив обмеження емуляції та використаних безкоштовних редакцій ПЗ, що вимагають доопрацювання та перевірки в реальному середовищі.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		121

ВИСНОВКИ

У ході виконання випускної кваліфікаційної роботи було досягнуто поставленої мети – розроблено та практично реалізовано підсистему контролю доступу до мережевих ресурсів на базі серверів TekRADIUS і FreeRADIUS. На теоретичному етапі виконано глибокий аналіз AAA-моделі з акцентом на протокол RADIUS, оцінено міжнародні стандарти та проведено порівняння комерційного рішення TekRADIUS із відкритим FreeRADIUS, що створило надійну основу для побудови функціональної моделі.

Практична частина включала побудову тестового середовища в GNS3 із сегментацією мережі через VLAN, реалізацію резервування (GLBP, Rapid-PVST) та налаштування безпечного адміністративного доступу SSH із політиками паролів і обмеженням спроб входу. Налаштовано служби DHCP і списки доступу для кожного сегмента, що забезпечило відокремлення адміністративного та користувацького трафіку. Встановлено TekRADIUS на Windows Server із вбудованою SQLite та FreeRADIUS на Ubuntu з MariaDB і веб-інтерфейсом daloRADIUS, що підтвердило швидкість розгортання першого рішення й гнучкість другого.

Безпекова перевірка охопила моделі MITM-атак (ARP Poisoning, Port Stealing, DHCP Spoofing), після чого реалізовано захист через Message-Authenticator, IPSec-тунелі між клієнтами й серверами, а також механізми Dynamic ARP Inspection, DHCP Snooping і Port Security для запобігання підробленому трафіку. Інтеграція 802.1X із динамічним призначенням VLAN і централізованим журналюванням через Syslog засвідчила виконання ключових функцій аутентифікації, авторизації та обліку.

Оцінка відповідності реалізованої системи вихідним вимогам показала, що всі критичні показники (конфіденційність, цілісність, доступність, масштабованість) виконані в повному обсязі. Запропонована архітектура може бути впроваджена в організаціях різного масштабу, а модульність FreeRADIUS і GUI TekRADIUS забезпечує простоту експлуатації та можливість розширення.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				122
Змн.	Арк.	№ докум.	Підпис	Дата		

Перспективи подальших досліджень включають інтеграцію багатофакторної автентифікації (FIDO2/WebAuthn), автоматизований AI-аналіз журналів для ефективного виявлення аномалій та розгортання RADIUS-проксі в контейнеризованому середовищі з інтеграцією з хмарними каталогами (Azure AD, LDAP-SSO).

Проведена робота закладає міцну основу для побудови сучасних AAA-підсистем відповідно до міжнародних стандартів інформаційної безпеки та готова до подальшого вдосконалення в умовах мінливих загроз і вимог ринку.

Отже, проведена робота не лише підтвердила працездатність обраної концепції, а й надала практично готовий до впровадження інструментарій для побудови сучасної підсистеми аутентифікації відповідно до міжнародних стандартів інформаційної безпеки. Дослідження закладає основу для подальшого вдосконалення та розширення функціональних можливостей в умовах мінливих загроз і вимог ринку.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				123
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Блохін М. Ю. GDPR ЯК ПОТЕНЦІЙНЕ ДЖЕРЕЛО ВДОСКОНАЛЕННЯ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ. *Часопис цивілістики*. № 42. С. 44–48. DOI:10.32837/chc.v0i42.434.
2. Andjarwirawan J. Single Sign-On (SSO) Implementation Using Keycloak, RADIUS, LDAP, and PacketFence for Network Access. *Teknika*. Вип. 14, № 1. Р. 41–46. DOI:10.34148/teknika.v14i1.1089.
3. Astriani M. S., Pradono S. E-School Implementation Using Radius Server and Authentication Mechanism. *ComTech: Computer, Mathematics and Engineering Applications*. Вип. 3, № 2. Р. 908–916. DOI:10.21512/comtech.v3i2.2321.
4. Cisco LEAP. [Електронний ресурс]: Режим доступу : <https://community.cisco.com/t5/wireless-mobility-knowledge-base/cisco-leap/tap/3133135> (дата звернення: 18.06.2025)
5. Das M. L., Samdaria N. On the security of SSL/TLS-enabled applications. *Applied Computing and Informatics*. Вип. 10, № 1. Р. 68–81. DOI:10.1016/j.aci.2014.02.001.
6. Dobbertin H. The Status of MD5 After a Recent Attack. *CryptoBytes*. Вип. 2, № 2. 16 р.
7. Ferraiolo D. F. Role-Based Access Control (RBAC): Features and Motivations. Р. 8. 1995.
8. FreeRADIUS – Scalability. [Електронний ресурс]: Режим доступу : <https://wiki.freeradius.org/features/Scalability> (дата звернення: 18.06.2025)
9. FreeRADIUS Technical Guide. [Електронний ресурс]: Режим доступу : <https://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf> (дата звернення: 18.06.2025)
10. Fu C., Wang B., Wang W. та ін. A Generic High-Performance Architecture for VPN Gateways. *Electronics*. Вип. 13, № 11. С. 2031.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				124
Змн.	Арк.	№ докум.	Підпис	Дата		

DOI:10.3390/electronics13112031.

11. Goldberg S., Haller M., Heninger N. та ін. RADIUS/UDP Considered Harmful. 19 p. 2024.

12. Grassi P. A., Fenton J. L., Newton E. M. та ін. Digital identity guidelines: authentication and lifecycle management. Gaithersburg, MD : National Institute of Standards and Technology, 2017. 79 p. NIST SP 800-63b. DOI:10.6028/NIST.SP.800-63b. 2017.

13. HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules. *MLN*. 2023. 5 p.

14. Hosia A. Comparison between RADIUS and Diameter. 2003.

15. Javed A., Hanif A., Azam M. A. та ін. Development of Postpaid and Prepaid Billing System for ISPs. 2015.

16. Kent K., Souppaya M. P. Guide to computer security log management. (Gaithersburg, MD, 2006). Gaithersburg, MD : National Institute of Standards and Technology, 2006. 72 p. NIST SP 800-92. DOI:10.6028/NIST.SP.800-92. 2006.

17. Lee B. What is the RADIUS Protocol? JumpCloud. [Електронний ресурс]: Режим доступу : <https://jumpcloud.com/blog/what-is-the-radius-protocol> (дата звернення: 18.06.2025)

18. Maayan G. D. 5 User Authentication Methods that Can Prevent the Next Breach. ID R&D. [Електронний ресурс]: Режим доступу : <https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/> (дата звернення: 18.06.2025)

19. Microsoft Security Development Lifecycle Threat Modelling. [Електронний ресурс]: Режим доступу : <https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling> (дата звернення: 18.06.2025)

20. Ndibanje B., Lee H.-J., Lee S.-G. Security Analysis and Improvements of Authentication and Access Control in the Internet of Things. *Sensors*. Вип. 14, № 8. P. 14786–14805. DOI:10.3390/s140814786.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				125
Змн.	Арк.	№ докум.	Підпис	Дата		

21. OWASP Threat Modeling Project | OWASP Foundation. [Електронний ресурс] : Режим доступу : <https://owasp.org/www-project-threat-model/> (дата звернення: 18.06.2025)

22. RADIUS Attributes Overview and RADIUS IETF Attributes. Cisco. [Електронний ресурс] : Режим доступу : http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_radatt/configuration/15-1mt/RADIUS_Attributes_Overview_and_RADIUS_IETF_Attributes.html (дата звернення: 18.06.2025)

23. Radius server performance tips. [Електронний ресурс] : Режим доступу : <https://kkalev.wordpress.com/2007/03/25/radius-server-performance-tips/> (дата звернення: 18.06.2025)

24. Remote Authentication Dial-In User Service (RADIUS) reliability and scalability. RELIANOID. [Електронний ресурс] : Режим доступу : <https://www.relianoid.com/resources/knowledge-base/howtos/remote-authentication-dial-in-user-service-radius-reliability-and-scalability/> (дата звернення: 18.06.2025)

25. Stallings W. Network security essentials: applications and standards. Sixth edition, global edition. Harlow, United Kingdom London New York : Pearson, 2017. 47 p. ISBN 978-1-292-15485-5.

26. Szilagyi D., Sood A., Singh T. RADIUS: A REMOTE AUTHENTICATION DIAL-IN USER SERVICE. 12 p. 2009.

27. KaplanSoft. TekRADIUS – RADIUS Server for Windows (Datasheet). [Електронний ресурс] : Режим доступу : <https://www.kaplansoft.com/tekradius/Docs/TekRADIUS-Datasheet.pdf> (дата звернення: 18.06.2025)

28. TekRADIUS Pricing, Features, and Reviews (Jun 2025). [Електронний ресурс] : Режим доступу : <https://www.softwaresuggest.com/tekradius> (дата звернення: 18.06.2025)

29. Fortinet. What Is AAA Security? [Електронний ресурс] : Режим доступу : <https://www.fortinet.com/resources/cyberglossary/aaa-security> (дата звернення: 18.06.2025)

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				126
Змн.	Арк.	№ докум.	Підпис	Дата		

30. ДСТУ ISO/IEC 27001:2015. Київ: ДП «УкрНДНЦ», 2016. [Електронний ресурс]: Режим доступу: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf (дата звернення: 18.06.2025)
31. Aboba B. D., Wood J. Authentication, Authorization and Accounting (AAA) Transport Profile. Internet Engineering Task Force, 2003. 41 p. DOI:10.17487/RFC3539. 2003.
32. Admass W. S., Munaye Y. Y., Diro A. A. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*. Vol. 2, 01.01.2024. P. 100031. DOI:10.1016/j.csa.2023.100031.
33. Barkadehi M. H., Nilashi M., Ibrahim O. et al. Authentication systems: A literature review and classification. *Telematics and Informatics*. Vol. 35, Issue 5. P. 1491–1511. DOI:10.1016/j.tele.2018.03.018.
34. Calhoun P. R., Aboba B. D. RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP). Internet Engineering Task Force, 2003. 46 p. DOI:10.17487/RFC3579. 2003.
35. FreeRADIUS – Performance. [Електронний ресурс]: Режим доступу: <https://wiki.freeradius.org/features/Fast> (дата звернення: 18.06.2025)
36. FreeRADIUS Development :: The FreeRADIUS project – Documentation. [Електронний ресурс]: Режим доступу: <https://www.freeradius.org/documentation/freeradius-server/4.0.0/developers/index.html> (дата звернення: 18.06.2025)
37. Funk P., Blake-Wilson S. Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0). Internet Engineering Task Force, 2008. 51 p. DOI:10.17487/RFC5281. 2008.
38. II P. J. N., Straw M., Metz C. et al. A One-Time Password System. Internet Engineering Task Force, 1998. 25 p. DOI:10.17487/RFC2289. 1998.
39. KaplanSoft. TekRADIUS – FAQ. [Електронний ресурс]: Режим доступу: <https://www.kaplansoft.com/tekradius/faq.html> (дата звернення: 18.06.2025)

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				127
Змн.	Арк.	№ докум.	Підпис	Дата		

40. Massameno D. RADIUS Extensions for Server Load Balancing. Internet Engineering Task Force, 2020. 17 p. 2020.
41. Palekar A., Josefsson S., Simon D. et al. Protected EAP Protocol (PEAP) Version 2. Internet Engineering Task Force, 2004. 87 p. 2004.
42. PCI DSS Certification. GetPCI. [Електронний ресурс] : Режим доступу : <https://getpci.com/> (дата звернення: 18.06.2025)
43. Rigney C. RADIUS Accounting. Internet Engineering Task Force, 2000. 28 p. DOI:10.17487/RFC2866. 2000.
44. Rubens A., Rigney C., Willens S. et al. Remote Authentication Dial In User Service (RADIUS). Internet Engineering Task Force, 2000. 76 p. DOI:10.17487/RFC2865. 2000.
45. Salowey J. A., Haverinen H. Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM). Internet Engineering Task Force, 2006. 92 p. DOI:10.17487/RFC4186. 2006.
46. Simon D., Hurst R., Aboba B. D. The EAP-TLS Authentication Protocol. Internet Engineering Task Force, 2008. 34 p. DOI:10.17487/RFC5216. 2008.
47. Smith A. H., Zorn G., Roesse J. et al. IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines. Internet Engineering Task Force, 2003. 30 p. DOI:10.17487/RFC3580. 2003.
48. The RADIUS Protocol | FreeRADIUS Documentation. [Електронний ресурс] : Режим доступу : <https://networkradius.com/doc/current/introduction/RADIUS.html> (дата звернення: 18.06.2025)
49. Theofanos M., Garfinkel S., Choong Y.-Y. Secure and Usable Enterprise Authentication: Lessons from the Field. *IEEE Security & Privacy*. Vol. 14, Issue 5. P. 14–21. DOI:10.1109/MSP.2016.96.
50. Wierenga K., McCauley M., Winter S. et al. Transport Layer Security (TLS) Encryption for RADIUS. Internet Engineering Task Force, 2012. 22 p. DOI:10.17487/RFC6614. 2012.

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				128
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				129
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиці опису та аналізу загроз компонентів підсистеми

Таблиця А.1

Опис загроз ключових компонентів та потоків даних

Компонент/ Потік	Тип загрози	Опис	Потенційний зловмисник
Клієнти	Підробка	Зловмисник імітує легітимного клієнта для отримання доступу.	Зовнішній
	Маніпуляція	Запит клієнта змінюється під час передачі.	Зовнішній
	Витік інформації	Облікові дані перехоплюються в незахищеній мережі.	Зовнішній
	Відмова в обслуговуванні	Клієнт не може підключитися до мережі через перевантаження.	Зовнішній
NAS	Підробка	Зловмисник імітує NAS для перехоплення або перенаправлення трафіку.	Зовнішній
	Витік інформації	Чутлива інформація, що проходить через NAS, може бути викрадена.	Внутрішній/ Зовнішній
	Маніпуляція	Запит клієнта змінюється під час передачі.	Внутрішній/ Зовнішній
	Відмова від дій	Дії на NAS не журналюються або можуть бути заперечені.	Внутрішній
	Відмова в обслуговуванні	NAS перевантажується, що блокує доступ для легітимних користувачів.	Зовнішній
	Підвищення привілеїв	Зловмисник отримує адміністративний доступ до NAS.	Внутрішній/ Зовнішній
RADIUS	Підробка	Зловмисник імітує RADIUS-сервер, наприклад, через Blast-RADIUS	Зовнішній
	Маніпуляція	Конфігурація, база даних користувачів або трафік змінюється.	Внутрішній/ Зовнішній

Опис загроз ключових компонентів та потоків даних

Компонент/ Потік	Тип загрози	Опис	Потенційний зловмисник
RADIUS	Відмова від дій	Облікові дані користувачів або дані сесій можуть бути викрадені.	Внутрішній
	Витік інформації	Чутлива інформація, що проходить через NAS, може бути викрадена.	Внутрішній/ Зовнішній
	Відмова в обслуговуванні	Сервер перевантажується запитами.	Зовнішній
	Підвищення привілеїв	Зловмисник отримує адміністративний доступ до сервера.	Внутрішній/ Зовнішній
База даних	Маніпуляція	Данні змінюються або видаляються.	Внутрішній
	Відмова від дій	Зміни в базі даних не можуть бути відстежені.	Внутрішній
	Витік інформації	Чутлива інформація користувачів може бути доступна.	Внутрішній/ Зовнішній
	Відмова в обслуговуванні	База даних заблокована або сповільнена.	Внутрішній/ Зовнішній
	Підвищення привілеїв	Зловмисник отримує вищий рівень доступу в базі даних.	Внутрішній
Клієнт -> NAS	Підробка	Зловмисник надсилає фальшиві запити аутентифікації.	Зовнішній
	Маніпуляція	Запит змінюється під час передачі.	Зовнішній
	Витік інформації	Облікові дані надсилаються в відкритому вигляді.	Зовнішній
	Відмова в обслуговуванні	Велике число запитів до NAS.	Зовнішній
NAS -> Клієнт	Підробка	Фальшиві повідомлення про надання/відмову доступу.	Зовнішній

Компонент/ Потік	Тип загрози	Опис	Потенційний зловмисник
NAS -> Клієнт	Маніпуляція	Повідомлення змінюється під час передачі.	Зовнішній
NAS -> RADIUS	Підробка	Фальшиві пакети Access-Request.	Зовнішній
	Маніпуляція	Пакет Access-Request змінюється.	Зовнішній
	Витік інформації	Облікові дані перехоплюються.	Зовнішній
	Відмова в обслуговуванні	Велике число запитів Access-Request до RADIUS-сервера.	Зовнішній
RADIUS -> NAS	Підробка	Фальшива відповідь Access-Accept/Reject	Зовнішній
	Маніпуляція	Відповідь змінюється під час передачі.	Зовнішній
	Відмова в обслуговуванні	Відповіді блокуються або затримуються.	Зовнішній
RADIUS -> База даних	Маніпуляція	Запит до бази даних змінюється.	Внутрішній
	Витік інформації	Запит може розкривати чутливу інформацію.	Внутрішній
База даних -> RADIUS	Підробка	Фальшива відповідь від бази даних.	Зовнішній
	Маніпуляція	Відповідь змінюється під час передачі.	Зовнішній
	Витік інформації	Облікові дані передаються і можуть бути перехоплені.	Зовнішній

Аналіз загроз ключових компонентів та потоків даних

Компонент	Тип загрози	Ймовірність	Наслідки	Ризик	Залишковий ризик	Захід захист
Клієнти	Підrobка	Середня	Високі	Високий	Середній	802.1x з EAP-TLS
	Маніпуляція	Низька	Середні	Середній	Низький	Попередній захід
	Витік інформації	Низька	Середні	Середній	Низький	Попередній захід
	Відмова в обслуговуванні	Середня	Середні	Середній	Низький	Обмеження швидкості запитів, налаштування firewall
NAS	Підrobка	Низька	Високі	Середній	Низький	TLS, RadSec.
	Витік інформації	Середня	Високі	Високий	Низький	Шифрування, обмеження доступу
	Маніпуляція	Низька	Низькі	Низький	Низький	Обмеження доступу, аудит
	Відмова від дій	Низька	Середні	Середній	Низький	Захищене журналювання
	Відмова в обслуговуванні	Середня	Високі	Високий	Середній	Storm control, ACL, VLAN
	Підвищення привілеїв	Середня	Високі	Високий	Низький	Сильна аутентифікація, RBAC
RADIUS	Підrobка	Низька	Високі	Середній	Низький	RadSec
	Маніпуляція	Середня	Високі	Високий	Низький	Обмеження доступу, аудити
	Відмова від дій	Низька	Низькі	Низький	Низький	Захищене журналювання
	Витік інформації	Низька	Середні	Середній	Низький	Шифрування, обмеження доступу
	Відмова в обслуговуванні	Середня	Високі	Високий	Середній	Обмеження швидкості запитів, налаштування firewall

Аналіз загроз ключових компонентів та потоків даних

Компо- нент	Тип загрози	Ймовір- ність	Нас- лідки	Ризик	Залишко- вий ризик	Захід захист
RADIUS	Підвищення привілеїв	Середня	Високі	Висо- кий	Низький	Сильна аутен- тифікація, ау- дити
База да- них	Маніпуляція	Середня	Високі	Висо- кий	Низький	RBAC, шифру- вання, резервні копії
	Відмова від дій	Низька	Низькі	Низь- кий	Низький	Захищене жур- налювання
	Витік інфор- мації	Середня	Високі	Висо- кий	Низький	Шифрування, RBAC
	Відмова в об- слуговуванні	Низька	Сере- дні	Серед- ній	Низький	Моніторинг, обмеження за- питів
	Підвищення привілеїв	Середня	Високі	Висо- кий	Низький	RBAC, моніто- ринг аномалій

Модель загроз

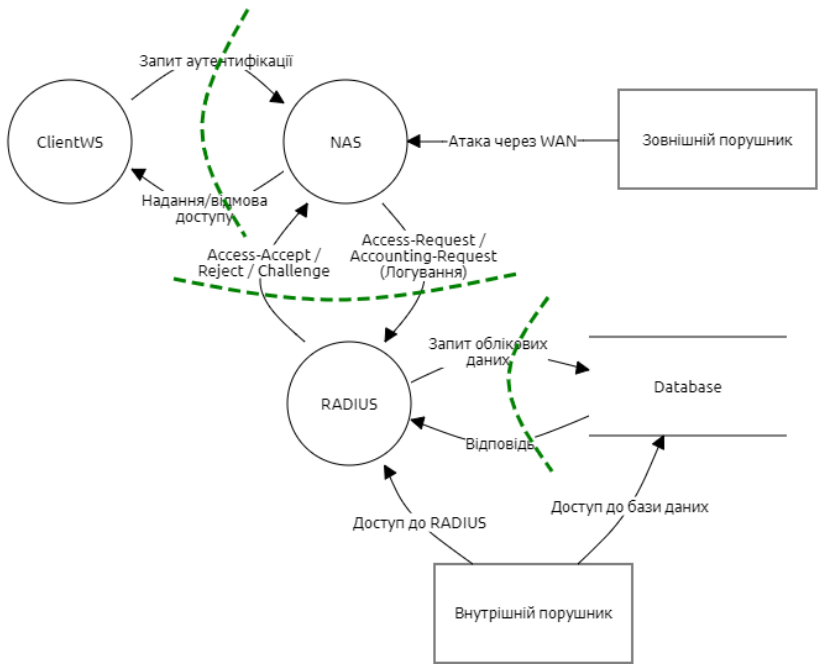
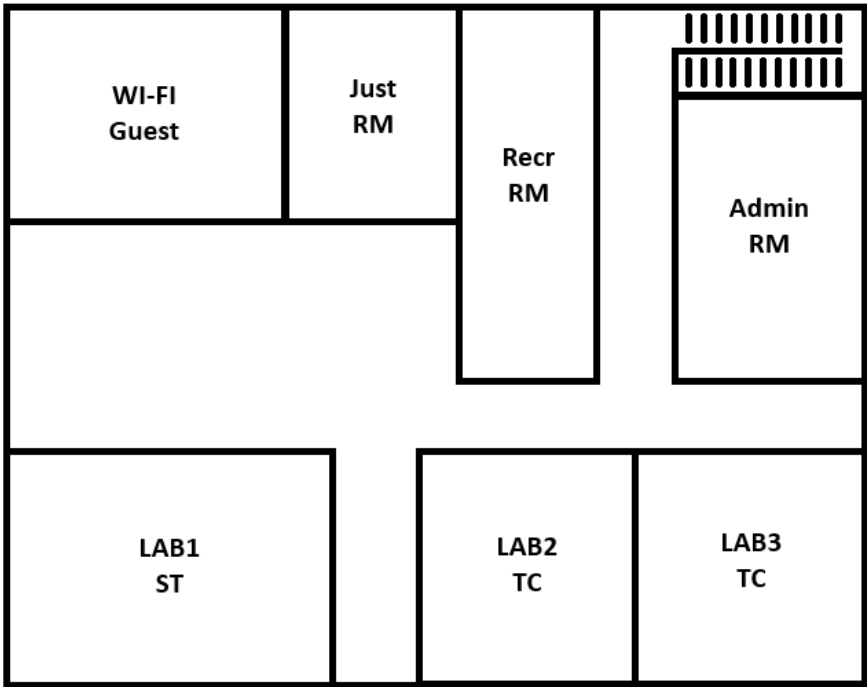


Рисунок Б.1 – Узагальнена модель загроз підсистеми аутентифікації

План будівлі підприємства та його топологія



План першого поверху вищого навчального закладу

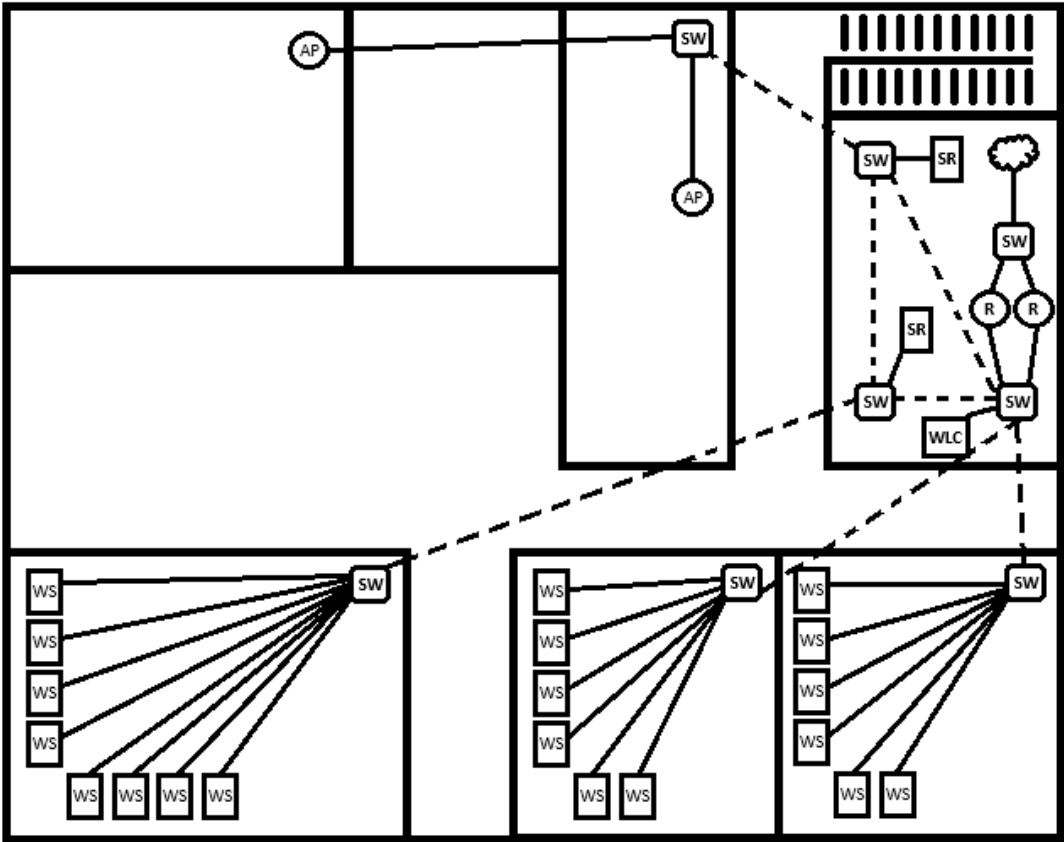
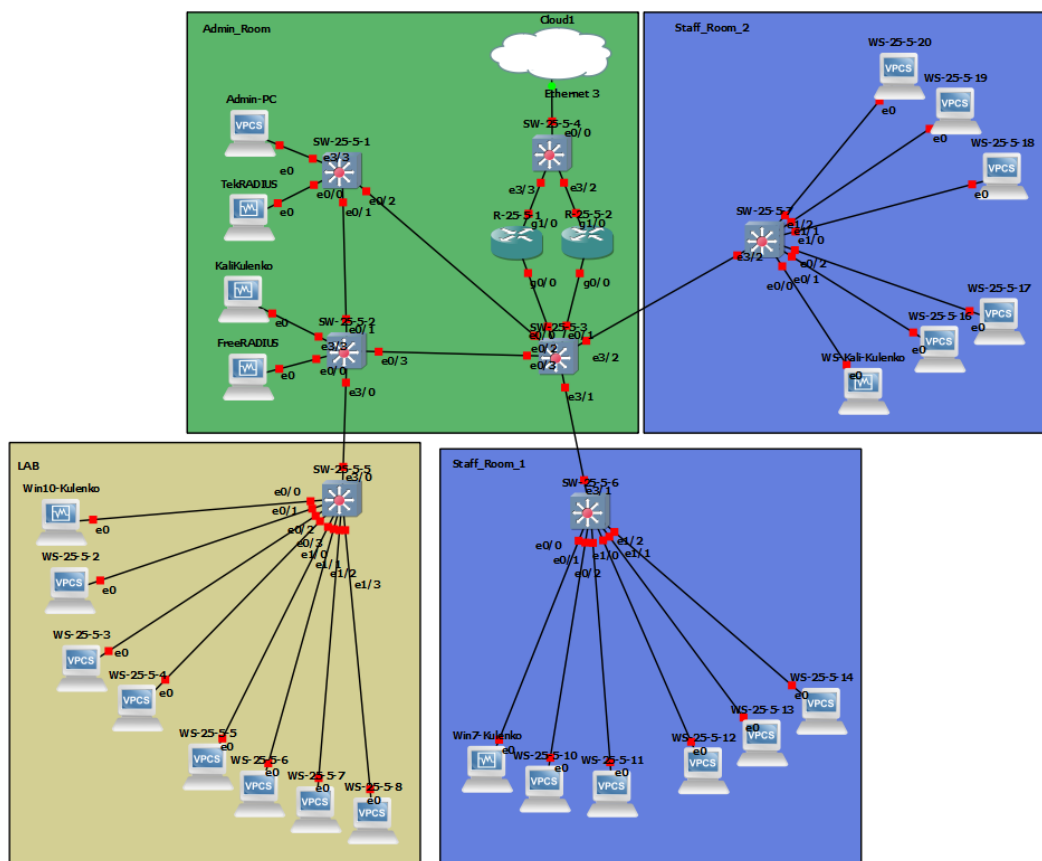


Схема розміщення мережевих та кінцевих пристроїв на першому поверсі



Кінцевий вигляд побудованої мережі

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				137
Змн.	Арк.	№ докум.	Підпис	Дата		

Конфігурації мережевих пристроїв

R-25-5-1#show running-config

Building configuration...

Current configuration : 5734 bytes

!

upgrade fpd auto

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R-25-5-1

!

boot-start-marker

boot-end-marker

!

security authentication failure rate 3 log

security passwords min-length 10

logging message-counter syslog

enable secret 5 \$1\$5ZP\$/Qq8UHph3OH7ak4mbjY7.

!

no aaa new-model

clock timezone EET 2

clock summer-time EEST recurring last Sun Mar

2:00 last Sun Oct 3:00

ip source-route

no ip icmp rate-limit unreachable

ip cef

!

ip dhcp excluded-address 191.25.5.6 191.25.5.14

ip dhcp excluded-address 192.25.5.10 192.25.5.12

ip dhcp excluded-address 193.25.5.8 193.25.5.10

ip dhcp excluded-address 194.25.5.8 194.25.5.10

ip dhcp excluded-address 191.25.5.2 191.25.5.3

!

ip dhcp pool Admin10

network 191.25.5.0 255.255.255.240

default-router 191.25.5.11

dns-server 1.1.1.1

domain-name Kulenko.net

!

ip dhcp pool LAB20

network 192.25.5.0 255.255.255.240

default-router 192.25.5.12

dns-server 1.1.1.1

domain-name Kulenko.net

!

ip dhcp pool Staff30

network 193.25.5.0 255.255.255.240

default-router 193.25.5.10

dns-server 1.1.1.1

domain-name Kulenko.net

!

ip dhcp pool Staff40

network 194.25.5.0 255.255.255.240

default-router 194.25.5.10

dns-server 1.1.1.1

domain-name Kulenko.net

!

ip domain name Kulenko.net

ip name-server 1.0.0.1

no ipv6 cef

!

multilink bundle-name authenticated

!

username adminkul privilege 15 secret 5

\$1\$PX1I\$eaUIQfxUUmoUc1IPB/w/X.

archive

log config

hidekeys

!

ip tcp synwait-time 5

ip ssh authentication-retries 5

ip ssh version 2

!

interface Ethernet0/0

no ip address

shutdown

duplex auto

!

interface GigabitEthernet0/0

no ip address

duplex full

speed 1000

media-type gbic

negotiation auto

!

interface GigabitEthernet0/0.10

encapsulation dot1Q 10

ip address 191.25.5.9 255.255.255.240

ip access-group ADMIN_ACCESS in

ip nat inside

ip virtual-reassembly

glbp 10 ip 191.25.5.11

glbp 10 priority 110

glbp 10 preempt

!

interface GigabitEthernet0/0.20

encapsulation dot1Q 20

ip address 192.25.5.10 255.255.255.240

ip access-group LAB_ACCESS in

ip nat inside

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				138
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip virtual-reassembly
glbp 11 ip 192.25.5.12
glbp 11 priority 110
glbp 11 preempt
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 193.25.5.8 255.255.255.240
ip access-group STAFF1_ACCESS in
ip nat inside
ip virtual-reassembly
glbp 12 ip 193.25.5.10
glbp 12 priority 110
glbp 12 preempt
!
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 194.25.5.8 255.255.255.240
ip access-group STAFF2_ACCESS in
ip nat inside
ip virtual-reassembly
glbp 13 ip 194.25.5.10
glbp 13 priority 110
glbp 13 preempt
!
interface GigabitEthernet1/0
description Connection to Cloud1
ip address dhcp
ip nat outside
ip virtual-reassembly
negotiation auto
!
interface GigabitEthernet2/0
no ip address
shutdown
negotiation auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 dhcp
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface GigabitEthernet1/0 overload
ip nat inside source list 2 interface GigabitEthernet1/0 overload
ip nat inside source list 3 interface GigabitEthernet1/0 overload
ip nat inside source list 4 interface GigabitEthernet1/0 overload
!
ip access-list extended ADMIN_ACCESS
permit udp any any eq bootpc
permit udp any any eq bootps
permit ip 191.25.5.0 0.0.0.15 any
permit ip any 191.25.5.0 0.0.0.15
ip access-list extended LAB_ACCESS

```

```

permit udp any any eq bootpc
permit udp any any eq bootps
permit udp 192.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
eq 1812
permit udp 192.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
eq 1813
permit tcp 192.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
established
permit icmp 192.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
echo-reply
deny ip 192.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
deny ip 192.25.5.0 0.0.0.15 193.25.5.0 0.0.0.15
deny ip 192.25.5.0 0.0.0.15 194.25.5.0 0.0.0.15
permit ip 192.25.5.0 0.0.0.15 any
permit ip any 192.25.5.0 0.0.0.15
ip access-list extended STAFF1_ACCESS
permit udp any any eq bootpc
permit udp any any eq bootps
permit udp 193.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
eq 1812
permit udp 193.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
eq 1813
permit tcp 193.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
established
permit icmp 193.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
echo-reply
deny ip 193.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
deny ip 193.25.5.0 0.0.0.15 192.25.5.0 0.0.0.15
permit ip 193.25.5.0 0.0.0.15 any
permit ip any 193.25.5.0 0.0.0.15
ip access-list extended STAFF2_ACCESS
permit udp any any eq bootpc
permit udp any any eq bootps
permit udp 194.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
eq 1812
permit udp 194.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
eq 1813
permit tcp 194.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
established
permit icmp 194.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
echo-reply
deny ip 194.25.5.0 0.0.0.15 191.25.5.0 0.0.0.15
deny ip 194.25.5.0 0.0.0.15 192.25.5.0 0.0.0.15
permit ip 194.25.5.0 0.0.0.15 any
permit ip any 194.25.5.0 0.0.0.15
!
access-list 1 permit 191.25.5.0 0.0.0.15
access-list 2 permit 192.25.5.0 0.0.0.15
access-list 3 permit 193.25.5.0 0.0.0.15
access-list 4 permit 194.25.5.0 0.0.0.15
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		139

```

line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
logging synchronous
login
transport input ssh
transport output ssh
!
ntp authentication-key 5 md5
104F0D140C19191E00450A68 7
ntp authenticate
ntp trusted-key 5
ntp master 10
ntp update-calendar
end

```

SW-25-5-1#show running-config
Building configuration...

```

Current configuration : 4308 bytes
!
! Last configuration change at 10:17:40 EEST Mon
Jun 23 2025
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-25-5-1
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging userinfo
logging buffered 20480
logging console discriminator EXCESS
enable secret 5
$1$gHdg$6l3py88bW.3qonQuSGO3K0
!
username adminkul privilege 15 secret 5
$1$ltiI$9pSfo274zF.zGD0gWSBOZ0
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring last Sun Mar
2:00 last Sun Oct 3:00
!
ip arp inspection vlan 10,20,30,40

```

```

ip arp inspection validate src-mac dst-mac
no ip icmp rate-limit unreachable
!
ip dhcp snooping vlan 10,20,30,40
no ip dhcp snooping information option
ip dhcp snooping
no ip domain-lookup
ip domain-name Kulenko.net
ip cef
no ipv6 cef
!
errdisable recovery cause uddld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause l2ptguard
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause pppoe-ia-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause unicast-flood
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause inline-power
errdisable recovery cause arp-inspection
errdisable recovery cause link-monitor-failure
errdisable recovery cause oam-remote-failure
errdisable recovery cause loopback
errdisable recovery cause psp
errdisable recovery interval 120
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 10,20,30,40 priority 4096
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
crypto ipsec security-association replay window-size
1024
!
interface Ethernet0/0
switchport access vlan 10
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.27d1.5e32
switchport port-security aging time 2
switchport port-security aging type inactivity

```

		Куленко І.В.			ККИКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				140
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport port-security
spanning-tree portfast edge
!
interface Ethernet0/1
switchport trunk allowed vlan 10,20,30,40
switchport trunk encapsulation dot1q
switchport trunk native vlan 911
switchport mode trunk
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet0/2
switchport trunk allowed vlan 10,20,30,40
switchport trunk encapsulation dot1q
switchport trunk native vlan 911
switchport mode trunk
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
switchport access vlan 10
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0050.7966.6813
switchport port-security aging time 1
switchport port-security
spanning-tree portfast edge
!
interface Vlan1
no ip address
shutdown

```

```

!
interface Vlan10
ip address 191.25.5.6 255.255.255.240
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip source binding 0800.27D1.5E32 vlan 10
191.25.5.3 interface Et0/0
logging trap notifications
logging host 191.25.5.2 transport tcp port 514
logging host 191.25.5.3 transport tcp port 514
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
logging synchronous
login
!
ntp authentication-key 5 md5
094D4A04100B1C07074D2469 7
ntp authenticate
ntp trusted-key 5
ntp source Vlan10
ntp update-calendar
ntp server 191.25.5.11 key 5
!
end
SW-25-5-5#show running-config
Building configuration...

Current configuration : 8819 bytes
!
! Last configuration change at 10:08:20 EEST Mon
Jun 23 2025
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-25-5-5
!
boot-start-marker
boot-end-marker
!

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				141
Змн.	Арк.	№ докум.	Підпис	Дата		

```

logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
logging userinfo
logging buffered 20480
logging console discriminator EXCESS
!
username adminkul privilege 15 secret 5
$1$O.ps$y26W2x6YCvBYMLCKSYK.
aaa new-model
!
aaa group server radius radserversGR
server name LUfreeRAD
!
aaa authentication login default group radserversGR
local
aaa authentication dot1x default group radserversGR
aaa authorization console
aaa authorization exec default group radserversGR
local
aaa authorization network default group rad-
serversGR
aaa accounting exec default start-stop group rad-
serversGR
!
aaa session-id common
clock timezone EET 2 0
clock summer-time EEST recurring last Sun Mar
2:00 last Sun Oct 3:00
!
ip arp inspection vlan 10,20,30,40
ip arp inspection validate src-mac dst-mac
no ip icmp rate-limit unreachable
!
ip dhcp snooping vlan 10,20,30,40
no ip dhcp snooping information option
ip dhcp snooping
no ip domain-lookup
ip domain-name Kulenko.net
ip cef
no ipv6 cef
!
dot1x system-auth-control
errdisable recovery cause udd
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause l2ptguard
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause pppoe-ia-rate-limit
errdisable recovery cause mac-limit

```

```

errdisable recovery cause unicast-flood
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause inline-power
errdisable recovery cause arp-inspection
errdisable recovery cause link-monitor-failure
errdisable recovery cause oam-remote-failure
errdisable recovery cause loopback
errdisable recovery cause psp
errdisable recovery interval 120
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
crypto ikev2 proposal ikev2_proposal
encryption aes-cbc-256
integrity sha256
group 24
!
crypto ikev2 policy ikev2_policy
proposal ikev2_proposal
!
crypto ikev2 keyring freeRAD_keyring
peer freeRAD_peer
address 191.25.5.2
pre-shared-key 6 m[W4Nc%D1s]4b=2tV&
!
crypto ikev2 keyring tekRAD_keyring
peer tekRAD_peer
address 191.25.5.6
pre-shared-key 6 hwJ14vdgJvF8NF9J7iSw
!
crypto ikev2 profile freeRAD_profile
match identity remote address 191.25.5.2
255.255.255.240
authentication remote pre-share
authentication local pre-share
keyring local freeRAD_keyring
dpd 10 2 periodic
!
crypto ikev2 profile tekRAD_profile
match identity remote address 191.25.5.6
255.255.255.240
authentication remote pre-share
authentication local pre-share
keyring local tekRAD_keyring
dpd 10 2 periodic
!
crypto ipsec security-association replay window-size
1024

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		142

```

!
crypto ipsec transform-set ipsec_transform esp-aes
256 esp-sha256-hmac
mode tunnel
!
!
crypto ipsec profile ipsec_freeRAD_profile
set transform-set ipsec_transform
set pfs group24
set ikev2-profile freeRAD_profile
!
crypto ipsec profile ipsec_tekRAD_profile
set transform-set ipsec_transform
set pfs group24
set ikev2-profile tekRAD_profile
!
!
crypto map ipsec_map 11 ipsec-isakmp
set peer 191.25.5.2
set transform-set ipsec_transform
set ikev2-profile freeRAD_profile
match address freeRAD_TRAFFIC
!
interface Ethernet0/0
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.2744.8895
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
ip arp inspection limit rate 10
authentication port-control auto
dot1x pae authenticator
ip dhcp snooping limit rate 30
!
interface Ethernet0/1
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0050.7966.680e
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
ip arp inspection limit rate 10
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
ip dhcp snooping limit rate 30
!
interface Ethernet0/2
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 2

```

```

switchport port-security aging type inactivity
switchport port-security
ip arp inspection limit rate 10
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
ip dhcp snooping limit rate 30
!
interface Ethernet0/3
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
ip arp inspection limit rate 10
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
ip dhcp snooping limit rate 30
!
interface Ethernet1/0
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
ip arp inspection limit rate 10
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
ip dhcp snooping limit rate 30
!
interface Ethernet1/1
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
ip arp inspection limit rate 10
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
ip dhcp snooping limit rate 30
!
interface Ethernet1/2
switchport mode access
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
ip arp inspection limit rate 10
spanning-tree portfast edge
ip dhcp snooping limit rate 30

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				143
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet1/3
 switchport access vlan 20
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
 0050.7966.6810
 switchport port-security aging time 2
 switchport port-security aging type inactivity
 switchport port-security
 ip arp inspection limit rate 10
 spanning-tree portfast edge
 ip dhcp snooping limit rate 30
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
 switchport trunk allowed vlan 10,20,30,40
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 911
 switchport mode trunk
 ip arp inspection trust
 ip dhcp snooping trust
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 191.25.5.12 255.255.255.240
 crypto map ipsec_map
!
 ip default-gateway 191.25.5.11
 ip forward-protocol nd
!
 no ip http server
 no ip http secure-server
!
 ip access-list extended freeRAD_TRAFFIC
  permit udp host 191.25.5.12 host 191.25.5.2 eq 1812
  permit udp host 191.25.5.12 host 191.25.5.2 eq 1813
  permit udp host 191.25.5.2 host 191.25.5.12 eq 1812
  permit udp host 191.25.5.2 host 191.25.5.12 eq 1813
 ip access-list extended tekRAD_TRAFFIC
  permit udp host 191.25.5.3 host 191.25.5.12
  permit udp host 191.25.5.12 host 191.25.5.3
!
 logging trap notifications
 logging source-interface Vlan10
 logging host 191.25.5.2 transport tcp port 514
 logging host 191.25.5.3 transport tcp port 514
!
 radius server LUFreeRAD
  address ipv4 191.25.5.2 auth-port 1812 acct-port
 1813
  key freeRAD!@#pass!@!
!
 radius server TekRAD
  address ipv4 191.25.5.3 auth-port 1812 acct-port
 1813
  key supersecretTEK
!
 control-plane
!
 line con 0
  exec-timeout 0 0
  logging synchronous
 line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line vty 0 4
  logging synchronous
!
 ntp authentication-key 5 md5
 050A02022842451C15443751 7
 ntp authenticate
 ntp trusted-key 5
 ntp source Vlan10
 ntp update-calendar
 ntp server 191.25.5.11 key 5
!
end

```

		Куленко І.В.			ККІКБ.КР.Б – 125 – 5 – ПЗ	Арк.
		Трокоз Є.М.				144
Змн.	Арк.	№ докум.	Підпис	Дата		