Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Засоби захисту та моніторингу локальної мережі організації на базі операційних систем з відкритим кодом»

Виконавець: студент IV курсу, групи КБ-42

_____ **Владислав РЕМПІНСЬКИЙ**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Іван ПАРХОМЕНКО	

Нормоконтроль	Сергій ДАКОВ	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентові **КБ-42** **Ремпінському Владиславу Юрійовичу**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи «Засоби захисту та моніторингу локальної мережі організації на базі операційних систем з відкритим кодом»

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Архітектури, топології, структури , методи захисту , методи моніторнгу , компоненти, топології , методи налаштування локальних мереж

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Поняття локальної мережі, типи , архітектура, топології та компоненти.
Вразливості локальних мереж, методи захисту та необхідність моніторингу.
Налаштування захисту локальних мереж, моніторингу та рекомендації щодо використання

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Налаштування моніторингу та захисту локальних

мереж та формування рекомендацій , щодо використання.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ (підпис) Іван ПАРХОМЕНКО. (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Владислав РЕМПІНСЬКИЙ. (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021 – 27.01.2022	*виконано*
2	Аналіз літератури	28.01.2022 – 11.02.2022	*виконано*
3	Розгляд структури локальних мереж	12.02.2022 – 24.02.2022	*виконано*
4	Дослідження основних вразливостей	25.02.2022 – 24.03.2022	*виконано*
5	Вибір методів захисту	25.03.2022 – 07.04.2022	*виконано*
6	Вибір методів моніторингу	08.04.2022 – 20.04.2022	*виконано*
7	Впровадження засобів моніторингу	21.04.2022 – 05.05.2022	*виконано*
8	Впровадження засобів захисту	06.05.2022 – 20.05.2022	*виконано*
9	Формування рекомендацій щодо використання	21.05.2022 – 04.06.2022	*виконано*
10	Оформлення пояснювальної записки	05.06.2022 – 08.06.2022	*виконано*
11	Підготовка до захисту	08.06.2022 – 13.06.2022	*виконано*

Завдання видав _____ (підпис) Іван ПАРХОМЕНКО (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Владислав РЕМПІНСЬКИЙ (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел. Основний текст займає 49 сторінки, включає в себе зміст, вступ, три розділи дипломної роботи, висновки та список джерел. У пояснювальній записці дипломної роботи міститься 26 рисунків.

Метою роботи є реалізація засобів захисту та моніторингу локальних мереж.

Для досягнення зазначеної мети поставлено наступні *завдання*:

- дослідити архітектуру та компоненти локальних мереж;
- проаналізувати вразливості локальних мереж;
- дослідити засоби , що використовуються для моніторингу та захисту локальних мереж;
- сформувати рекомендації щодо використання засобів.

Об'єктом дослідження є процес підбору, конфігурування та налаштування засобів моніторингу та захисту локальних мереж.

Предметом дослідження є сукупність елементів, що реалізують засоби моніторингу локальних мереж.

Методи дослідження – це аналіз літератури, порівняння, налаштування засобів.

Практичною цінністю отриманих результатів є забезпечення стабільної роботи локальної мережі за рахунок поєднання засобів захисту та моніторингу локальної мережі з використання операційних систем з відкритим кодом.

Ключові слова: локальна мережа, вразливості локальних мереж, моніторинг подій, захист інформації, шкідливий код, користувачі мережі, розподіл ролей, кібербезпека.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

LAN	–	Local Area Network
P2P	–	Peer to peer
UFW	–	Uncomplicated Firewall
2FA	–	Two-Factor Authentication
ПЗ	–	Програмне забезпечення
SNMP	–	Simple Network Management Protocol
CPU	–	Central processing unit
VPN	–	Virtual private network
ОС	–	Операційна система
NIC	–	Network interface card
ICMP	–	Internet Control Message Protocol
SSH	–	Secure SHell

ЗМІСТ

РЕФЕРАТ 4
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 5
ВСТУП 7
РОЗДІЛ 1 АРХІТЕКТУРА ТА СКЛАДОВІ ЛОКАЛЬНОЇ МЕРЕЖІ 9
1.1 Поняття локальної мережі 9
1.2 Типи локальних мереж 10
1.3 Архітектура локальної мережі 11
1.4 Топології локальних мереж 12
1.5 Компоненти локальних мереж 15
Висновки за розділом 1 17
РОЗДІЛ 2 МОНІТОРИНГ ТА ЗАХИСТ ЛОКАЛЬНИХ МЕРЕЖ 18
2.1 Вразливості локальних мереж 18
2.2 Методи захисту 21
2.3 Необхідність моніторингу та захисту 23
Висновки за розділом 2 24
РОЗДІЛ 3 ЗАСОБИ ЗАХИСТУ ТА МОНІТОРИНГУ ЛОКАЛЬНИХ МЕРЕЖ 25
3.1 Налаштування захисту локальних мереж 25
3.2 Налаштування моніторингу локальних мереж 27
3.3 Рекомендації , щодо використання засобів моніторингу 41
Висновки за розідлом 3 43
ВИСНОВКИ 44
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 46

ВСТУП

На сьогодні, існує безліч підприємств, які в більшості випадків складаються щонайменше з локальних мереж. Тому, необхідно мати значну кількість рішень задля забезпечення ефективності роботи та захищенності даних. У свою чергу, підприємство має включати низку потреб, таких як якісна безпека, використання сучасних технологій та взаємодія із сучасним обладнанням.

Впровадження та використання засобів захисту та моніторингу є невід'ємною складовою нашого часу. Це дає змогу завжди бути проінформованим про будь-які негаразди мережі та її стану в цілому.

Проте, перед тим, як застосовувати дані засоби, слід уважно проаналізувати всі ризики та вразливості використання даних систем.

Великими перевагами даних рішень є покращення відмовостійкості за рахунок передбачених реагувань на проблеми в системі та в цілому їх скорочені. Зменшення кількості збоїв систем за рахунок моніторингу стабільності мережі.

Мережа зазвичай має як внутрішніх, і зовнішніх користувачів, включаючи в себе як співробітників так і клієнтів, партнерів. Важливо пам'ятати про оптимальність та продуктивність мережі, адже це впливає на компанію в цлому. Наприклад, якщо у працівників не має можливості отримати доступ до необхідної для них інформації, щоб виконати ті чи інші поставлені задачі, це спричинить різке зменшення продуктивності роботи мережі.

Іноді, складність деяких мереж спричиняє різні наслідки. Наприклад кожен компонент у мережі - це потенційна точка відмови. Тому важливо запровадити в системі як мінімум резервування. Отже, у разі збою одного із серверів чи маршрутизаторів, інший сервер, який чекає відповіді, може автоматично підключитися до мережі, щоб зменшити час очікування.

Звичайно, не кожну проблему можна швидко локалізувати, поки не буде критичних ознак цього. Але, якщо відстежувати продуктивність мережі в режимі реального часу, буде змога знаходити проблеми до того, як вони перетворяться на ті

самі критичні ознаки. Наприклад, вичерпаний/перевантажений сервер слід замінити на інший ще до того, коли настане момент відмови. Але це слід робити тільки у тому випадку, якщо відмови уникнути неможливо. Завдяки моніторингу мережі можна знати повний стан усієї мережі, не слідкуючи за цим власноруч, при цьому мати можливість зробити завчасні дії, задля мінімізації та швидкому усунення будь-якої проблеми.

Мета дипломної роботи – реалізація засобів захисту та моніторингу локальних мереж.

Для досягнення зазначеної мети поставлено наступні *завдання*:

- дослідити архітектуру та компоненти локальних мереж;
- проаналізувати вразливості локальних мереж;
- дослідити засоби , що використовуються для моніторингу та захисту локальних мереж;
- сформувати рекомендації щодо використання засобів.

Об'єкт дослідження – процес налаштування засобів моніторингу та захисту локальних мереж.

Предметом дослідження є сукупність елементів, що реалізують засоби моніторингу локальних мереж.

Методи дослідження – це аналіз літератури, порівняння, налаштування засобів.

Практична цінність – налаштування моніторингу та захисту локальних мереж та формування рекомендацій , щодо використання.

РОЗДІЛ 1
АРХІТЕКТУРА ТА СКЛАДОВІ ЛОКАЛЬНОЇ МЕРЕЖІ

1.1 Поняття локальної мережі

Зазвичай локальна мережа (Local area network) визначається як під’єднане середовище в одному або кількох будівлях, у радіусі дії близько 1 кілометра, що включає в себе обчислювальні пристрої [1].

З іншого боку – це так звана група комп'ютерів і обєднаних пристроїв, які використовують спільну лінію зв'язку або бездротовий зв'язок. Зазвичай, приєднані пристрої одночасно використовують ресурси певного сервера в межах малої територіальної межі..У свою чергу LAN, часто підключається до інших мереж, а також до мережі інтернету чи якоїсь іншої глобальної мережі [2].

Також поняття LAN можна трактувати як комп’ютерну мережу, що займає відносно малу площу. Це група комп’ютерів і пов’язаних із ними пристроїв, які мають спільну лінію зв’язку або бездротовий зв’язок із сервером. Як відомом, LAN включає в себе комп’ютери та периферійні пристрої, що під’єднані до сервера на відносно малій відстані. Комп’ютери та інші мобільні пристрої можуть спільно використовувати такі ресурси, як принтер або мережеве сховище. Найчастіше локальна мережа обмежується однією кімнатою, будівлею або групою будівель.

Локальні мережі можна відрізнити від інших мереж через їх малу відстань. Загальне покриття може становити від 1 км до 10 км. Швидкість передачі даних локальних мереж набагато вища, ніж в інших типах мереж. Крім того, швидкість передачі даних низька через меншу відстань між обладнанням. Оскільки локальні мережі знаходяться в межах однієї будівлі або меншої території, вони належать певній організації. Цей локалізований контроль забезпечує більшу гнучкість у локальних мережах, ніж інші типи мереж [3].

На рисунку 1.1 можемо побачити приклад локальної мережі.

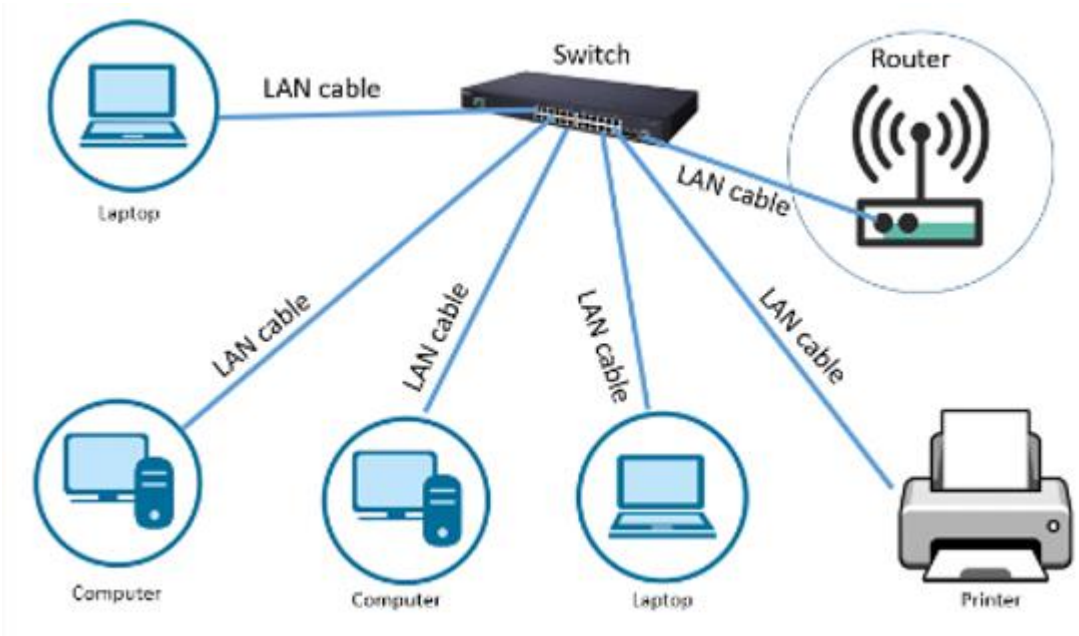

Рис.1.1 – Приклад локальної мережі

1.2 Типи локальних мереж

По перше – це клієнт-серверна локальна мережа, а саме у середовищі клієнт-серверної локальної мережі один сервер підключається до некількох пристроїв, відомих як клієнти. Клієнтські пристрої не можуть взаємодіяти з іншим, а централізована машина виконує такі дії, як керування сетевим трафиком, контроль доступу до мережі тощо. Цей тип локальної мережі може бути швидше в невеликих периметрах, але на більшому периметрі він надає велику кількість навантажень на центральний сервер.

По-друге - це однорангова (P2P) локальна мережа, тобто у локальній мережі P2P немає централізованого сервера, а всі підключені пристрої мають доступ до іншого, незалежно від того, є вони серверами чи клієнтами. Основне існування P2P LAN полягає в тому, що пристрій може вільно обмінюватися даними з іншого, щоб здійснювати потокову передачу мультимедіа, відправляти файли та виконувати аналогічні дії з обміном даними. З іншого боку, вони, як правило, менш потужні, ніж локальні мережі клієнт-сервер.

Третє – це налаштування з токен-рингом, що в залежності від архітектури ви можете класифікувати локальні мережі за категоріями Token Ring або Token Bus. У

першому випадку всі підключені пристрої використовують топологію кільце. Маркер назначається кожному підключеному пристрою в залежності від його вимог.

Четверте – це секретна шина LAN , де локальній мережі з шиною маркерів підключені вузли використовують топологію дерево, а токени передаються або ліворуч, або праворуч. Як правило, він забезпечує найкращу пропускну здатність, чим середу локальної мережі Token Ring.

Пяте – це провідна локальна мережа. Провідна локальна мережа, імовірно, є найбільш поширеним типом локальної мережі, яку використовуємо сьогодні. Вона використовує електронні хвилі для передачі даних по оптичному волокну (або варіант кабелю) замість токенів. Провідна локальна мережа надзвичайно надійна і може працювати дуже швидко, залежно від режиму центрального сервера. Однак це може погіршити гнучкість, особливо в середньому без фіксованої кількості пристроїв.

Шосте – це беспровідна локальна мережа. Вона зазвичай використовується в домашніх умовах для підключення обчислювальних пристроїв, переносимих пристроїв, інтелектуальних пристроїв та інші.

Останнє , це локальна мережа з хмарним управлінням. Це особливий тип безпроводової локальної мережі, на якій централізована хмарна платформа використовується для керування наданням мережі, політикою застосування, контролем доступу та іншими аспектами режиму та безпеки мережі. Така локальна сеть спрощує управління, що робить її належною для корпоративного використання [4].

1.3 Архітектура локальної мережі

Хоча й існує багато способів проектування архітектури мережі, проте більшість з них відноситься до одного з двох типів. Це однорангові або клієнт-серверні архітектури.

В одноранговій моделі всі пристрої мережі мають рівні обов'язки і привілеї одне з одним. Це значить, що поставлені завдання розподіляються по всій мережі.

Файли, зо знаходяться на одному комп'ютері, можуть бути використані разом із будь-яким іншим комп'ютером, що і робить кожен вузол мережним накопичувачем. Інші ресурси, наприклад принтер, що підключений до одного з пристроїв, буде помітним і для всіх інших пристроїв, що знаходяться у даній мережі.

Однорангова архітектура зазвичай використовується для невеликих мереж, таких як невелика оргнізація. Ваша домашня мережа також використовує однорангову модель.

В клієнт-серверній архітектурі всі пристрої у мережі підключені до центрального концентратора, що має назву «сервер», самі пристрої називаються «клієнтами». Сервер виконує основну частину мережевих операцій, таких як зберігання та обробку даних, клієнтських запитів, та контроль доступу та кібербезпеку.

У глобальних мережах, часто використовується клієнт-серверна модель. Наприклад, веб-сервер, на якому можна знайти чудову інформації слугує сервером, а комп'ютер є клієнтом. Клієнт-сервер також є кращою архітектурою корпоративної мережі [5].

1.4 Топології локальних мереж

Зазвичай поняття топології мережі визначають як певне фізичне розташування комп'ютерів один відносно іншого та їх спосіб з'єднання. Також, існує безліч методів з’єднання пристроїв у мережі. Розглянемо базові:

1.Топологія шина використовує магістраль, тобто один кабель, до якого підключені всі комп’ютери мережі.

Системи підключаються до цієї магістралі за допомогою Т-роз'ємів.

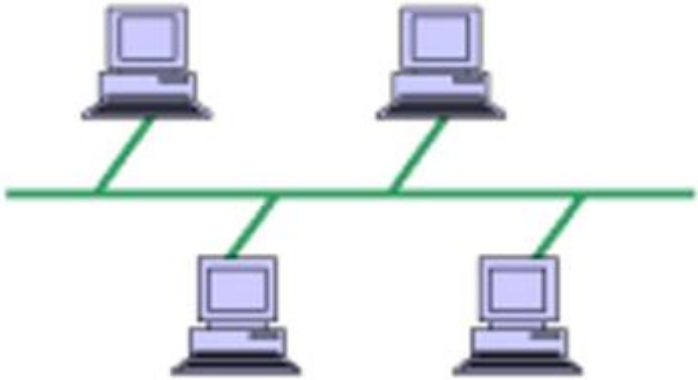

Рисунок 1.2 – Зображення топології шини

Перевагами даної топології є дешевизна і простота в реалізації, для неї потрібно менше кабелю та вона не використовує спеціалізовану мережу.

Недоліками є порушення мережі під час роботи комп’ютерів при додаванні або видаленню одного з пристроїв , а також обрив кабелю обмежити всю систему від доступу до мережі, складно усунути неполіки обладнання.

2. Топологія кільце

Дана топологія зображена на рисунку 1.3. Дані у такій мережі переміщуються по колу з одного комп’ютера на інший за допомогою кабелю, що замкнутий в «кільце».

Рисунок 1.3 – Зображення топології кільце

Перевагами даної топології є помірна проста у встановленні, а також несправності кабелю легко локалізуються. Ще до переваг відноситься просте усунення неполадок .

Недоліками даної топології - це порушення роботи мережі, що може бути спричиним розширення мережі , а також один обрив кабелю може порушити роботу всієї мережі.

3. Топологія «Зірка»

У даній топології всі комп'ютери або будь-які пристрої підключаються до центральної мережі , а саме пристрою під назвою концентратор або комутатор.

На відміну від інший топологій, у даній для кожного пристрою потрібен лише один кабель, також з'єднання "точка-точка" між пристроєм та концентратором, вона найбільш широко впроваджується і ще хаб є єдиною точкою відмови [6].

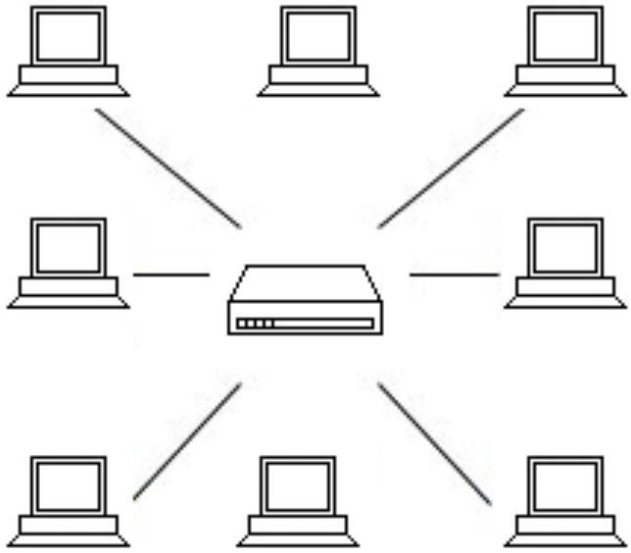

Рисунок 1.4 – Зображення топології зірка

Перевагами «Зірки» є легке розширення без перебоїв, несправність кабелю стосується лише одного користувача, а також головною перевагоє є легке усунення та ізоляція проблеми.

До не доліків - потрібно більше кабелю та складніша в реалізації

4. Топологія сітка

Кожен з комп'ютерів або пристроїв підключається до іншого, тобто безумовно пов’язаний з рештою.

У даній топології високий рівень резервування, тобто забезпечення надійності. Використовується «сітка» рідко, тому що мережа дуже складна, висока вартість кабелю та усунути несправність несправного кабелю дуже складно.

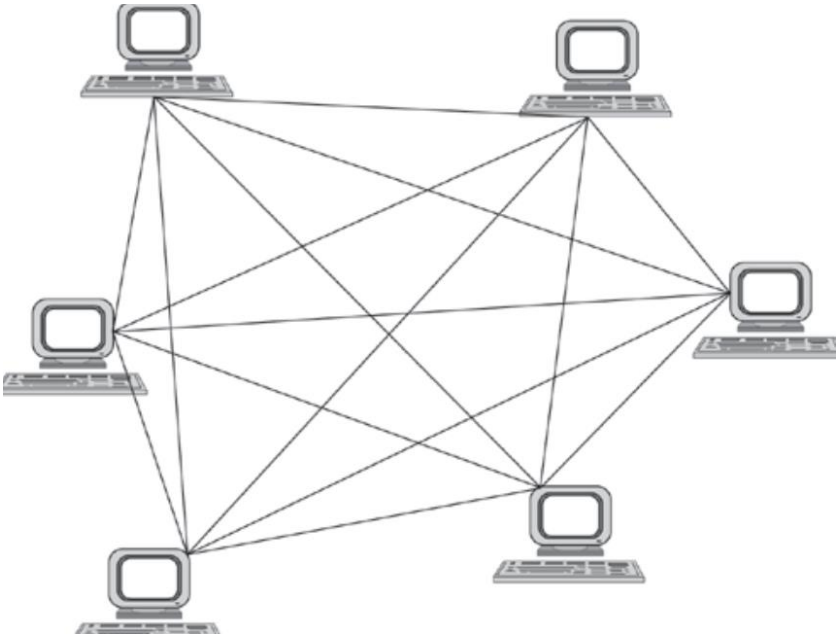

Рисунок 1.5 – Зображення топології сітка

Переваги – це те, що мережу можна розширити без порушення поточного використання, а недоліки – це потреба кабелю більше, ніж в іншій топології , а також складна реалізація [7].

1.5 Компоненти локальних мереж

LAN зазвичай складається з трьох основних елементів:

- апаратне забезпечення , що підключене до мережі;
- програмне забезпечення;
- користувачі.

Тому розділимо кожен з цих елементів на ряд компонентів.

До апаратних компонентів відностяться:

- networking interface card (NICs) – це плата для доступу до мережі;

- сервер – тобто комп’ютер, що призначений для обробки запитів і доставки даних іншим комп’ютерам(клієнтам) за допомогою локальної мережі;
- концентратори (hub) – це так звана загальна точка підключення пристроїв у мережі. HUB зазвичай використовують для з'єднання елементів локальної мережі. Він містить декілька портів. Коли пакет передається на один з портів, він копіюється на інші порти, щоб усі елементи LAN могли бачити пакети;
- комутатор (switch) – за особливостями схожий на концентратор у тому, що є центральною точкою для підключення мережевих кабелів; однак коммутатор може отримати пакет і передати його тільки на той комп'ютер, на який адресовано пакет;
- маршрутизатори(router) – це пристрій, що забезпечує підключення до Інтернету для локальних мереж. У свою чергу використовують таблицю конфігурації, щоб вирішити, куди далі повинні йти пакети;
- блок живлення(power supply) – це пристій , що використовується як для дротових, так і для бездротових мереж, яким потрібне джерело живлення;
- точка доступу(access point) – це такий апаратний пристрій чи програмне забезпечення комп'ютера, що працює як комунікаційний центр для користувачів бездротового пристрою для підключення до проводної локальної мережі;
- конектор(connector) – це мережевий роз'єм, який відноситься до будь-якого пристрою. Він використовується для з'єднання локальних мереж з апаратним забезпеченням комп’ютера [8].

Після того, як апаратне програмне забезпечення встановлене, наступним кроком буде приведення їх у робочий стан. Тобто, програмне забезпечення необхідне задля спільної та ефективної роботи пристроїв у локальній мережі. У локальній мережі можна знайти три категорії програмного забезпечення:

- операційна система кожного підключеного сервера, що вважається мозковою мережею;
- операційна система кожної підключеної станції, бо задля роботи всіх ПК необхідно мати операційну систему;
- прикладне програмне забезпечення, для якого звертаються користувачі локальної мережі. Тобто, прикладне програмне забезпечення — це так зване

програмне забезпечення, що слугує для виконання певної задачі. Найбільш поширеними прикладом є обробка текстів, аналіз електронних таблиць і управління базами даних;

- програмне забезпечення для групової роботи, що відноситься до програм, які допомагають людям, що знаходяться віддалено одне від одного;
- клієнт-серверне програмне забезпечення - це прикладне програмне забезпечення, що створюється для використання зазвичай у локальній мережі. Дане ПЗ складається з двох окремих частин - це клієнтської, що працює на користувацькій станції та серверної, що встановлюється на файловому сервері.

Також, одним з найважливіших елементів локальної мережі є люди. Однією з цілей локальної мережі є дозвіл спільного використання ресурсів. Саме цей обмін робиться людьми, що і доказує невідємною частиною структури.

У будь-якій локальній мережі бере участь дві групи людей - це ті, хто користується ресурсами,і , хто ними керує.

Користувач визначає як особа, користуючись мережевими ресурсами.

Мережевий адміністратор - це людина, що займається обслуговуванням локальної мережі. Дуже важливо, щоб адміністратор добре розумів, як влаштована мережа і як вона функціонує.

Висновки за розділом 1

У першому розділі проаналізовано архітектуру та сладові локальких мереж. Також оглянуто основні елементи LAN – це паратне забезпечення, програмне забезпечення та користувачі.

Завдяки приватній власності, високій швидкості та низькому відсотку помилок, локальні мережі привернули більше уваги, а також популярність у сфері мереж. Будь які додатки, послуги у різних сферах життя суспільства, використання ресурсів та адміністрування є основною причиною того, чому застосовуються локальні мережі. Але, у свою чергу вони мають свої вразливості.

РОЗДІЛ 2
МОНІТОРИНГ ТА ЗАХИСТ ЛОКАЛЬНИХ МЕРЕЖ

2.1 Вразливості локальних мереж

Вразливість мережі - це так звана слабкість чи вада у програмному забезпеченні, апаратному забезпеченні, організаційних процесах, компрометація яких може призвести до порушення безпеки. Наприклад шкідливе ПЗ, таке як трояни, віруси або черв'яки, зазвичай встановлюється на комп’ютері користувача або хост-сервері. Атаки соціальної інженерії, які обманом змушують користувачів надавати особисту інформацію, наприклад ім'я користувача чи пароль. Застаріле або неналаштоване програмне забезпечення, яке і створює ризик системі, на якій запущено наприклад всю мережу. Віднесемо сюди неправильно налаштовані брандмауери [9].

Шкідливе ПЗ – це таке програмне забезпечення, яке купується, завантажується або встановлюється зазвичай за неуважності. До найпоширеніших типів шкідливих програм належать:

- віруси - це найпоширеніші типи шкідливих ПЗ. Для того, щоб вірус вразив систему, користувачу необхідно натиснути або скопіювати його у систему. Більшість вірусів самореплікується без відома користувача. Ці віруси можуть поширюватися з однієї системи в іншу через електронну пошту, обмін миттєвими повідомленнями, завантаження наприклад з сайтів, USB-носії та підключення до мережі;
- кейлоггери, тобто іншими словами захоплення клавіатури – це реєстрування натискання клавіш і відправлення даних зловмиснику. Користувачі, зазвичай, не знають, що їх дії відстежуються. Проте роботодавці можуть використовувати кейлоггери для відстеження активності співробітників, вони використовуються в основному для крадіжки паролів або ж конфіденційних даних. Кейлоггери можуть

бути фізичним проводом, непомітно підключеним до периферійного пристрою, наприклад, клавіатури, або встановленим трояном;

- хробаки подібні до вірусу. Хробаки також можуть самореплікуватися та поширювати свої копії та сегменти через мережеві підключення, вкладення електронної пошти та миттєві повідомлення. Проте, на відміну від вірусів, хробаку не потрібна програма хост для запуску, самореплікації та поширення. Хробаки зазвичай використовуються проти поштових серверів, веб-серверів та серверів баз даних. Після зараження черв'яки швидко поширюються через Інтернет та комп'ютерні мережі;
- трояни - Троянські програми – це шкідливі програми, що маскуються під законне програмне забезпечення. Троянська програма буде ховатися на вашому комп'ютері, доки її не викличуть. При активації трояни можуть дозволити зловмисникам шпигувати за вами, красти ваші конфіденційні дані та отримати доступ до вашої системи через чорний хід;
- програми-вимагачі - це тип шкідливого ПЗ, що призначений для блокування доступу користувачів до їх системи або ж у відмові для доступу до даних, доки не буде виплачено наприклад «викуп»;
- логічні бомби - це тип шкідливих програм, що активуються лише при спрацьовуванні, у певний час або за кількістю входів у обліковий запис. Наприклад віруси та хробаки зазвичай містять у собі логічні бомби, для запуску шкідливого коду у заздалегідь зазначений час або при виконанні якоїсь іншої умови;
- боти або ботнети - це група ботів, що являють собою комп'ютерні системи будь-якого типу, підключені до мережі, безпека якої була скомпрометована. Зазвичай, вони управляються дистанційно;
- рекламне та шпигунське ПЗ - це небажане програмне забезпечення. Дане ПЗ призначене для зображення реклами на екранах у браузері. Зазвичай шпигунське ПЗ непомітно встановлюється у фоновому режимі під час завантаження програми без вашого відома чи дозволу. Незважаючи на незначну шкідливість, дане забезпечення може дратувати користувача;

- шпигунське програмне забезпечення, з іншого боку, є одним із видів шкідливого ПЗ, призначеного для отримання доступу до комп'ютера та спричинення його пошкодження. Воно збирає повну інформацію про користувача, таку як звички, історію переглядів та особисту інформацію. Далі зловмисники розповсюджують або ж навіть продають ваші дані рекламодавцям або компаніям, що займаються збором даних, отримують інформацію про ваш банківський рахунок або крадуть вашу персональну інформацію. Шпигунське програмне забезпечення часто завантажується в комплекті з застосунками з файлообмінників;

- руткіти - це програма-лазівка, яка дозволяє зловмиснику зберігати командування та контроль над комп'ютером без відома користувача. Такий доступ може надати повний доступ до цільової системою. Потім контролер може стежити за роботою власника, виконувати файли та віддалено змінювати конфігурації системи. Незважаючи на те, що він традиційно розгортається з використанням атак троянських коней, він стає все більш поширеним у довірених додатках. Деякі антивірусні програми можуть виявляти руткіти, проте видалити їх із системи складно. Найчастіше найкраще видалити руткіт і відновити скомпрометовану систему [10].

Шкідливе ПЗ зазвичай передається через фішингові електронні листи. Наприклад, зловмисники надсилають співробітникам компанії електронні листи, в яких містяться посилання на сайти, чи вбудовують якісь додатки в електронний лист. Якщо використовується дія, наприклад перехід за посиланням або завантаження вкладення, виконується шкідливий код, і можно легко «спіймати» вірус.

Атаки з використанням соціальної інженерії стали методом, що використовують зловмисники задля звичайного уникнення протоколів безпеки автентифікації, авторизації та отримання доступу до мережі.

Найпоширені атаки соціальної інженерії включають в себе:

- фішингові листи, тобто шахрайство з фішинговою електронною поштою - це загроза, яка спрацьовує від лиця користувача або компанії в цілому. Шахраї намагаються обманом змусити користувачів надати конфіденційну інформацію, таку

як ім'я користувача та пароль, завантажити або відкрити програму або переказати гроші. Фішинг заснований на створенні помилкової довіри, тому зловмисники часто надсилають електронні листи зі знайомих веб-сайтів;

- цільовий фішинг нагадує фішинг тим, що він намагається обманути користувача. Проте, цільовий фішинг призначений для використання особистої інформації, щоб змусити вас клацнути посилання. Зазвичай використовуються терміновість;
- спам - це масове розсилання листів для великої кількості користувачів. Електронні листи іноді є дратівливими домаганнями і зазвичай надходять від шахраїв;
- фармінг - це такий тип атаки соціальної інженерії, що перенаправляє трафік сайту користувача на неспражній сайт. Подібно до фішингу, фармінг відбувається, коли на комп'ютер встановлюється код, який змінює звичайну адресу URL на URL зловмисника;
- бекдор - це простіший тип атаки соціальної інженерії, коли зловмисник отримує несанкціонований доступ до об'єкта, слідуючи за користувачем через віддалений доступ [11].

2.2 Методи захисту

По-перше, інсталяція програми захисту від зловмисних програм і підтримання її в актуальному стані може допомогти захистити комп'ютер від вірусів та інших зловмисних програм (програм, створених зловмисниками) [12].

Наприклад від кейлоггерів доречно використовувати двофакторну автентифікацію (2FA), що додає додатковий крок між введенням паролів та доступом до облікових записів. За допомогою додаткового рівня безпеки, хакерам складніше отримати доступ до пристроїв. Як другий варіант, може бути звичайний PIN-код, що надіслається на мобільні телефони [13].

Від хробаків відмінним варіантом для захисту є проактивна технологія. Проактивний захист - це набір технологій, що застосовується в антивірусному ПЗ та

головною ціллю яких є пошук потенційно небезпечного ПЗ. На відміну від звичайних антивірусних програм, така технологія буде доречно захищати систему, а не здійснювати пошук вже відомих вірусів на жорстких дисках. При цьому вірус буде заблокований, тільки якщо він являє собою реальну загрозу ОС [14].

Для запобіганню загроз троянським коням, слід періодично оновлювати антивірус, не вимикати брандмауер та регулярно обновлювати операційна систему. Використання інформації тільки з перевірених джерел також також слугує методом захисту від троянських конів. Також слід не забувати про не бажаний перехід на сумнівні сайти та використовувати різні паролів для сервісів.

Щоб уникнути загрози програм-вимагачів слід використовувати знову ж таки антивірус, проте якщо ОС Windows 10-11, то ввімкнути захист від програм-вимагачів в налаштуваннях [15].

Аналогічно до вірусів та хробаків, можна і захиститись від логічних бомб.

Задля захисту від ненавмисного доступу до ботнету, слід уважно ставитися до ПЗ, що встановлюється на пристрої. Особливо, коли справа доходить до програмного забезпечення безпеки, наприклад VPN, ви завжди повинні переконатися, що ви встановлюєте ПЗ від надійних і незалежних компаній.

Також вже давно розроблені спеціалізовані сканери для відстеження шпигунської активності. Ці сканери не конфліктують з іншим встановленим ПЗ для захисту і можуть знайти те, що випустив з уваги антивірус.

Постійний фільтр інформації, якій надається доступ до своєї ОС дає змогу захиститися від руткітів.. Слід уникати підозрілих сайти, сумнівних листів та документів. Перевірка будь-яких USB-носіїв на наявність шкідливих програм [16].

Атакам соціальної інженерії також слід приділяти певну увагу. Завжди слід пильно обирати джерела у Інтернеті, а особливо ті, які запитують конфіденційні дані.

Ніколи не слід відкривати вміст додатків або переходити за посиланням, не вивчивши всіх деталей. Часто адреса відправника містить помилки в назвах, а посилання мають неправдоподібний вигляд. Варто також критично ставитися до отриманих повідомлень.

Задля підвищення захисту даних, слід обирати наприклад багатофакторну автентифікацію, що вимагатиме наприклад перевірку біометричних даних людини. Цей тип аутентифікації складний у реалізації та зазвичай потребує великих витрат, проте, гарантія захищеності у рази краща.

2.3 Необхідність моніторингу та захисту

Активний контроль за працездатністю локальної мережі станивить основу будь-якої організації. Контроль - це певний необхідний перший етап, що повинен виконуватися при управлінні мережею. Зважаючи на необхідність цієї функції вона часто згадується відносно інших функцій систем управління і реалізуються певними засобами. Такий розподіл функцій управління є необхідним для локальних мереж. Використання автономних засобів контролю допомагає адміністратору мережі виявити проблемні ділянки й пристрої мережі, а їх відключення або реконфігурацію він може виконувати в цьому випадку вручну. Процес контролю роботи мережі зазвичай ділять на два етапи - моніторинг і аналіз.

На першому етапі виконується звичайна процедура - це збір даних про роботу мережі:

- статистика про кількість циркулюючих в мережі кадрів та пакетів різних протоколів;
- стан портів маршрутизаторів чи концентраторів, комутаторів та інші.

На другому етапі аналізу, його пояснюють як складний та інтелектуальний процес обробки зібраної на етапі збору інформації, порівняння її з даними, що були отримані раніше та думки про можливі причини повільної та небажаної роботи мережі.

Завдання моніторингу виконуються програмнипи та апаратними засобами, мережевими аналізаторами, іноді вбудованими засобами моніторингу комунікаційних пристроїв, а також деякими агентами систем управління. Завдання ж аналізу потребує більшої участі людини та не обходиться без використання

експертних систем, нагромадженого практичного досвіду багатьох мережевих фахівців [17].

Висновки за розділом 2

У другому розділі проаналізовано основні вразливості локальних мереж та методи захисту від них.

Основними вразливостями є шкідливе ПЗ, атаки соціальної інженерії та людський чинник.

Також розглянуто основні завдання моніторингу та його необхілність, адже завдяки ньому можна зажди бути проінформованим наприклад не тільки про несанкціоновані спроби входу в систему, але й за навантаженням системи.

РОЗДІЛ 3
ЗАСОБИ ЗАХИСТУ ТА МОНІТОРИНГУ ЛОКАЛЬНИХ МЕРЕЖ

3.1 Налаштування захисту локальних мереж

Для захисту локальної мережі використано класичний брандмауер для ОС з відкритим кодом

Простими словами, брандмауер – це така спеціальна програма, яка постійно сканує, отримує та відправляє дані в інтернет. Інакше кажучи, це так звані «віртуальні стіни», що захищають пристрій в мережі від певних загроз, зокрема це:

- віруси;
- руткіти;
- шпигунські ПЗ;
- троянський кінь.

Слід зазначити, що фаєрвол – це неєдиний найращий шлях захисту комп'ютера. Для забезпечення якісної безпеки, брандмауер краще працює разом з антивірусом та якимось протишпигунським ПЗ.

Існує безліч відомих брандмауерів для операційних систем з відкритим кодом:

- ufw;
- iptables;
- monowall;
- pfsense;
- clearoOS.

У даному випадку обрано ufw.

UFW (Uncomplicated Firewall) – це простий інструментарій для налаштування і управління брандмауера для операційних систем з відкритим кодом.

По-перше , для його встановлення потрібно прописати команду apt install ufw

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.35-5).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
```

Рисунок 3.1 – Зображення процесу встановлення брандмауера

Далі дозволимо брандмауеру підключення SSH , та запустимо сам брандмауер.

Для цього використаємо команди ufw allow ssh та ufw enable

```
root@Ubuntu1804x64:~# ufw allow ssh
Rules updated
Rules updated (v6)
root@Ubuntu1804x64:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

Рисунок 3.2 – Зображення процесу запуску брандмауера

Потім потрібно дозволити роботу службі http , https, ftp(стандартний мережевий протокол прикладного рівня призначений для пересилання файлів між клієнтом та сервером в комп'ютерній мережі)

Для цього використаємо команди

ufw allow http, ufw allow https , ufw allow ftp

При необхідності , можна задати дозвіл певному IP адресу на доступ до всіх портів сервера за допомогою команди ufw allow from 109.*.72

Рисунок 3.3 – Зображення визначення ip адреси

За допомогою команди ufw status numbered перевіримо статус нашого брандмауера

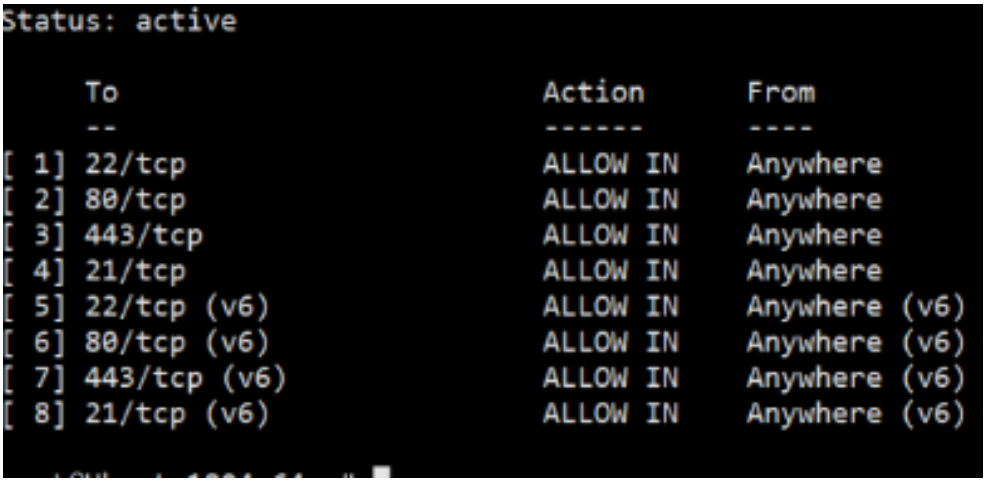

Рисунок 3.4 – Зображення статусу брандмауера

Для , наприклад , подальших конфігурацій брандмауера слід заздалегіть його вимкнути , щоб уникнути подальших збоїв , проте довгострокове його вимкнення може призвести до небажаних наслідків [18].

3.2 Налаштування моніторингу локальних мереж

Для налаштування використаємо систему моніторингу Zabbix.

Zabbix — це вільна система моніторингу деяких служб та стану наприклад локальної мережі.

Zabbix складається з кількох основних компонентів програмного забезпечення, призначення яких викладено нижче.

Перше - це ядро ПЗ Zabbix. У сервера є можливість віддалено перевіряти мережеві сервіси, використовуючи прості перевірки сервісів, проте він також є центральним компонентом, якому агенти передають будь-яку статистику а також інформацію про цілісність і доступність. Сервер - це сховище, в якому зберігаються всі дані, такі як статистичні, дані про конфігурацію та оперативні. Також сервер

виступає у ролі ПЗ, яке сповіщає адміністраторів у разі виникнення будь-яких проблем в мережі.

Zabbix може виконувати моніторинг без агентів, а також моніторинг мережевих пристроїв за допомогою SNMP агентів.

Проксі - це необов'язковий компонент розгортання Zabbix. Проксі збирає дані про продуктивність та доступність для Zabbix сервера. Всі зібрані дані заносяться в буфер на локальному рівні і передаються серверу Zabbix, до якого належить проксі.

Zabbix проксі є ідеальним рішенням для централізованого моніторингу віддалених місць, філій, мереж, які не мають місцевих адміністраторів.

Zabbix проксі може бути також використаний для розподілу та зняття навантаження з одного сервера Zabbix. У цьому випадку проксі тільки збирає дані, що забезпечує менше навантаження на ЦПУ і на введення/виведення диска на сервері.

Для активного моніторингу локальних ресурсів та додатків (таких як жорсткі диски, пам'ять, статистика процесора тощо) на системах мережі, повинні бути запущені Zabbix агенти. Агент збиратиме інформацію про роботу системи, на якій він працює, і надаватиме ці дані Zabbix серверу для подальшої обробки. У разі виникнення проблем (наприклад, жорсткий диск заповнився або аварійно завершився процес), Zabbix сервер може попереджати адміністраторів конкретного обладнання, від якого і виникла проблема.

Zabbix агенти є надзвичайно ефективними, тому що вони використовують рідні системні виклики для збору статистичної інформації.

Веб-інтерфейс наданий для забезпечення легкого доступу до даних моніторингу та конфігурації системи Zabbix звідки завгодно та з будь-якої платформи. Інтерфейс є частиною Zabbix сервера, і зазвичай (але не обов'язково), запущений на тому ж фізичному сервері як і Zabbix сервер.

Команди для встановлення:

wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb

dpkg -i zabbix-release_5.0-1+focal_all.deb

apt update

apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent

apt install mysql-server

mysql -uroot -p

mysql> create database zabbix character set utf8 collate utf8_bin;

mysql> create user zabbix@localhost identified by 'admin';

mysql> grant all privileges on zabbix.* to zabbix@localhost;

mysql> quit;

zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -uzabbix -p zabbix

nano /etc/zabbix/zabbix_server.conf

systemctl restart zabbix-server zabbix-agent apache2

systemctl enable zabbix-server zabbix-agent apache2

Далі, необхідно перейти на веб-інтерфейс для встановлення [19].

Меню входу у встановлену систему моніторингу зображена на рис. 3.5

Рисунок 3.5 – Вікно входу в систему

Логи — це такі файли, що містять у собі інформацію про роботу системи, сервера, пристроя мережі і дії користувача чи програми.

Головне призначення — це журналювання операцій, що виконуються на пристрої, для подальшого його аналізу. Постійний перегляд логів забезпечить завчасне визначення помилок у роботі системи або сервісу, діагностувати небажану активність та зібрати наприклад статистику переглядів.

У нашому випадку створено шлях збору логів для перевірки кількості під’єднань від VPN сервісу [20].

На рисунку 3.6 зображено процес додавання шляху збору логів.

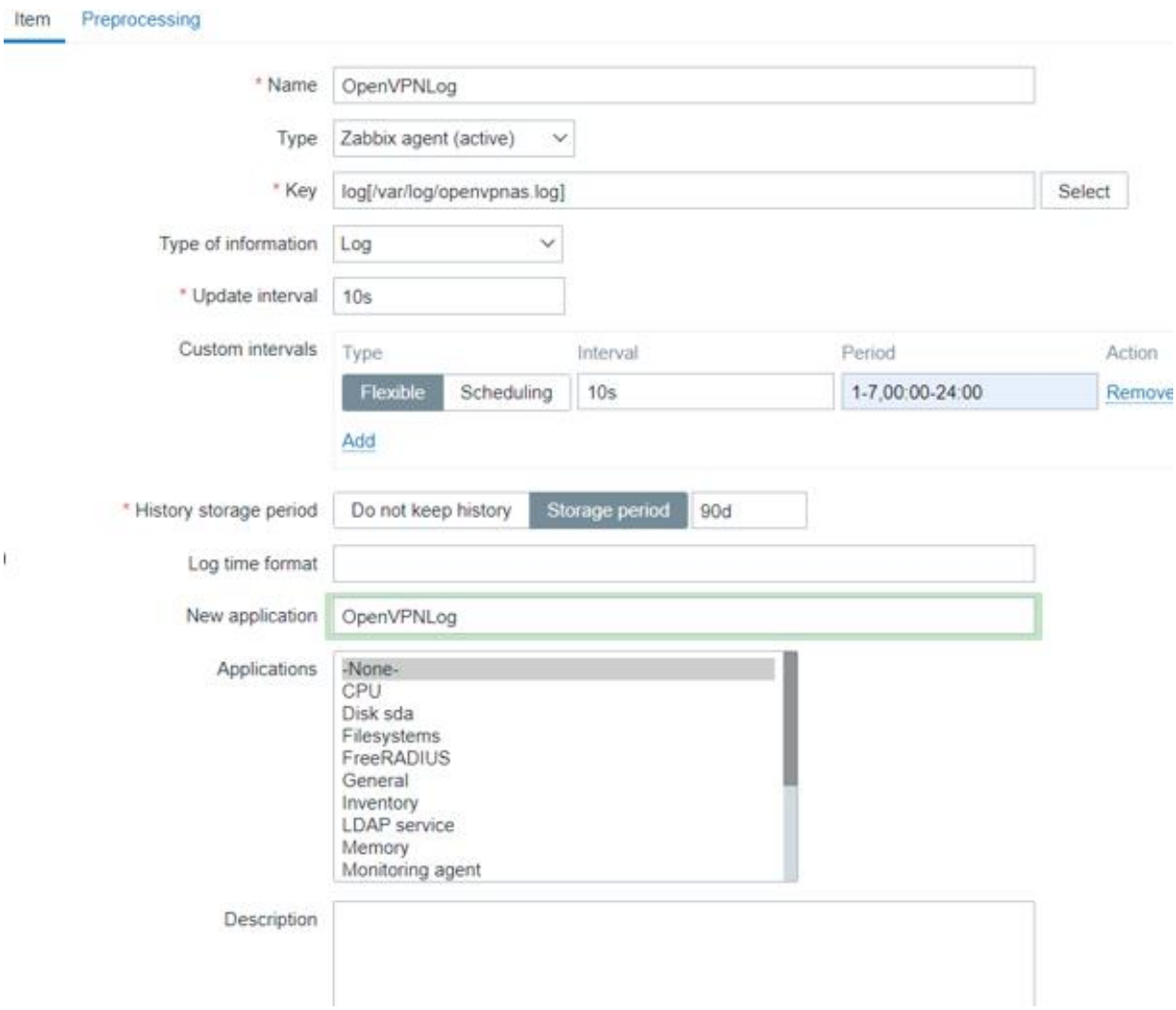

Рисунок 3.6 – Зображення процесу додавання шляху збору логів

Тригер – це певний засіб, який дозволяє оцінити дані, що були зібрані. Також за допомогою заданих умов, є можливість визначити чи має певний елемент, що містить інформацію містить якісь проблеми чи помилки.

Тригер має два стани:

- problem;
- ok.

У цілому тригер допомогає адміністратору мережі бути проінформованим про можливі спроби несанкціонованого доступу до ресурсу OpenVPN.

У цьому випадку створено тригер, задля оцінки роботи серверу FreeRadius [21].

На рисунку 3.7 зображено процес створення тригеру.

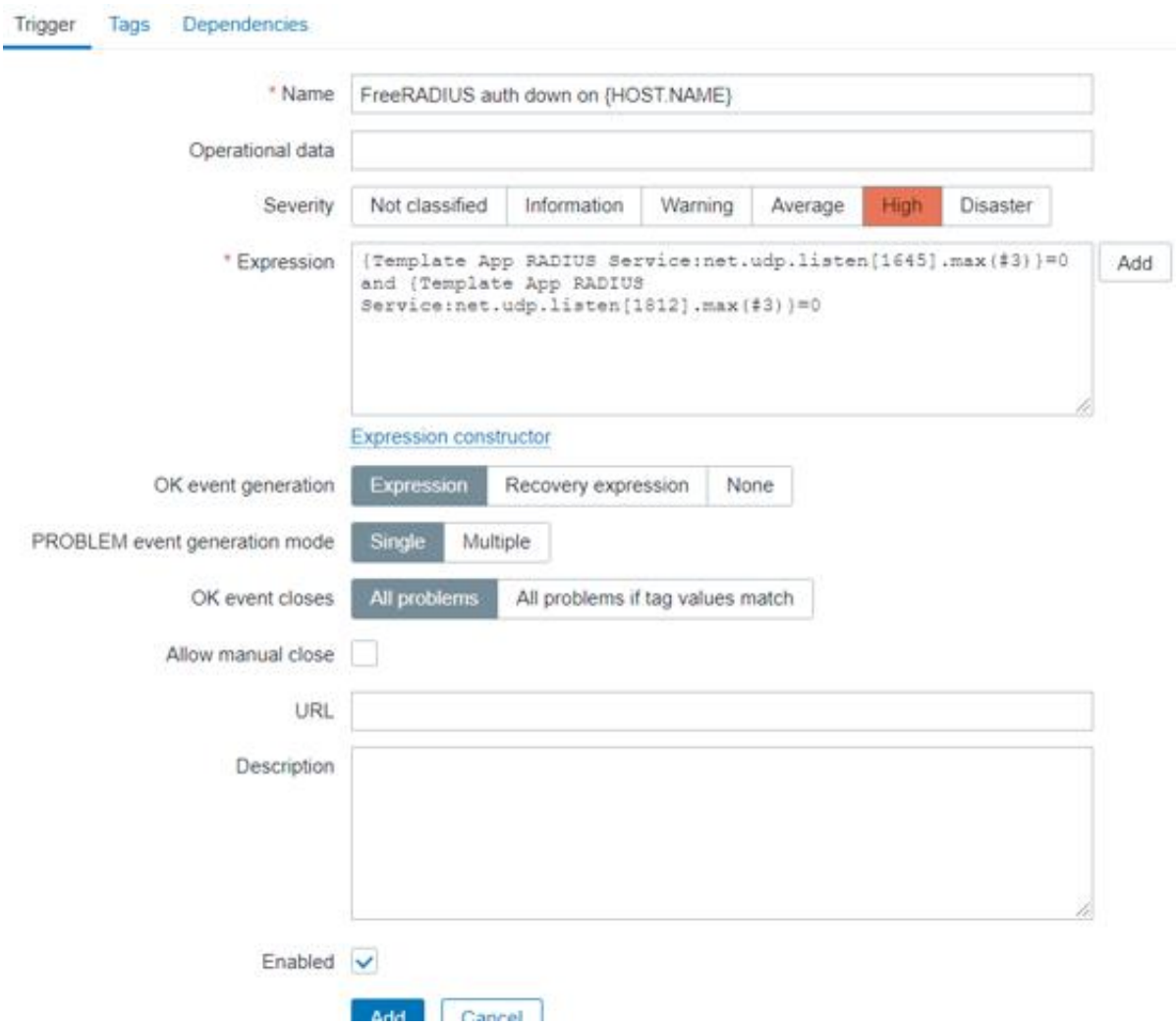

Рисунок 3.7 – Зображення процесу створення тригеру

На рисунку 3.8 зображенно процес створення наступного тригеру, що базується на перевірці проблемності логіну до сервісу OpenVPN.

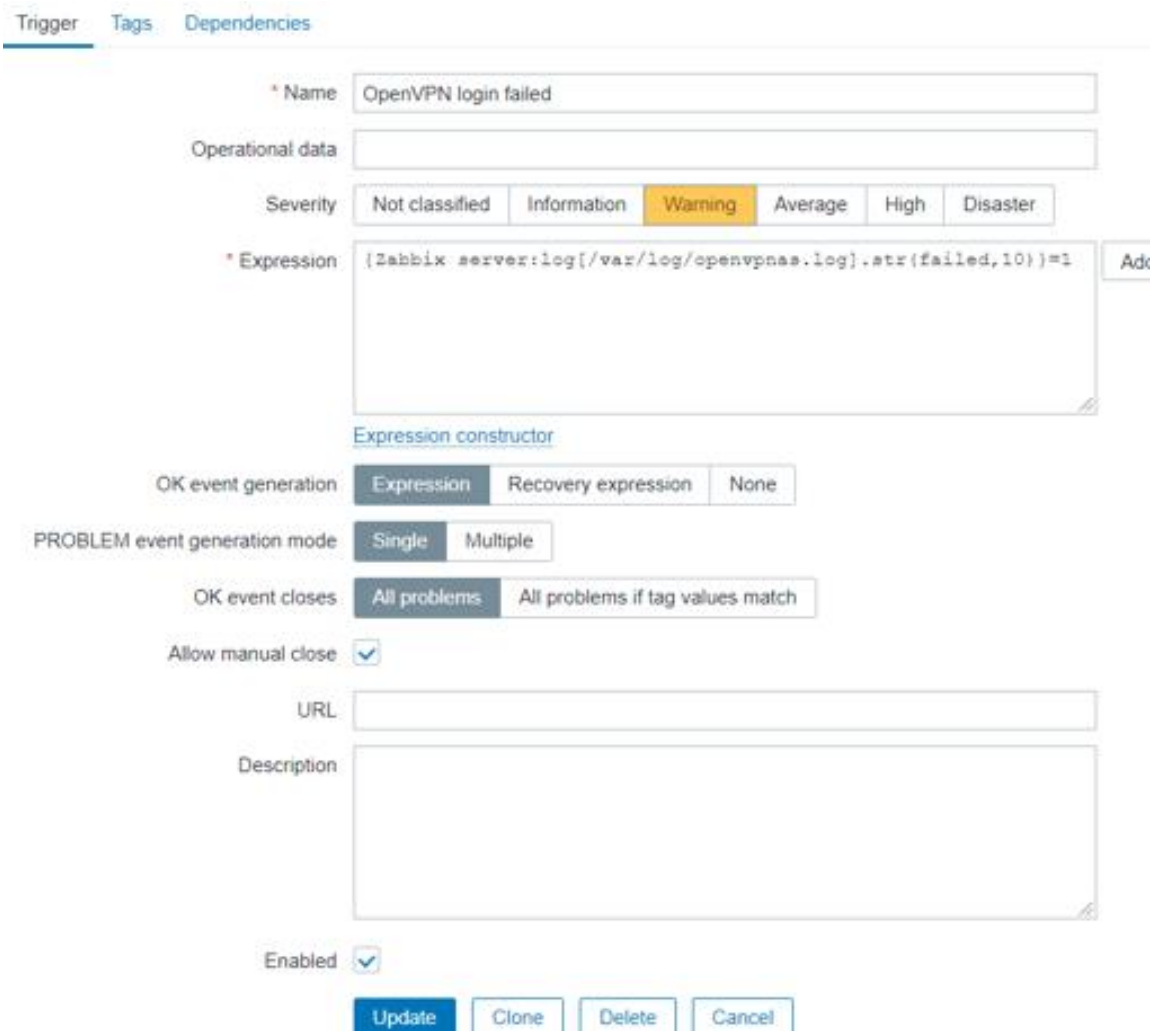

Рисунок 3.8 – Зображення процесу створення тригеру

Аналогічно бувають випадки, коли слід бути проінформованим про можливі несанкціоновані спроби доступу до самого серверу. Невдалі декілька спроб авторизації до серверу інформують адміністратора мережі, що хтось намагається зробити велику низку неприємностей мережі в цілому.

На рисунку 3.9 зображенно ще один процес створення тригеру. Він включає в себе оцінку авторизації до серверу FreeRadius.

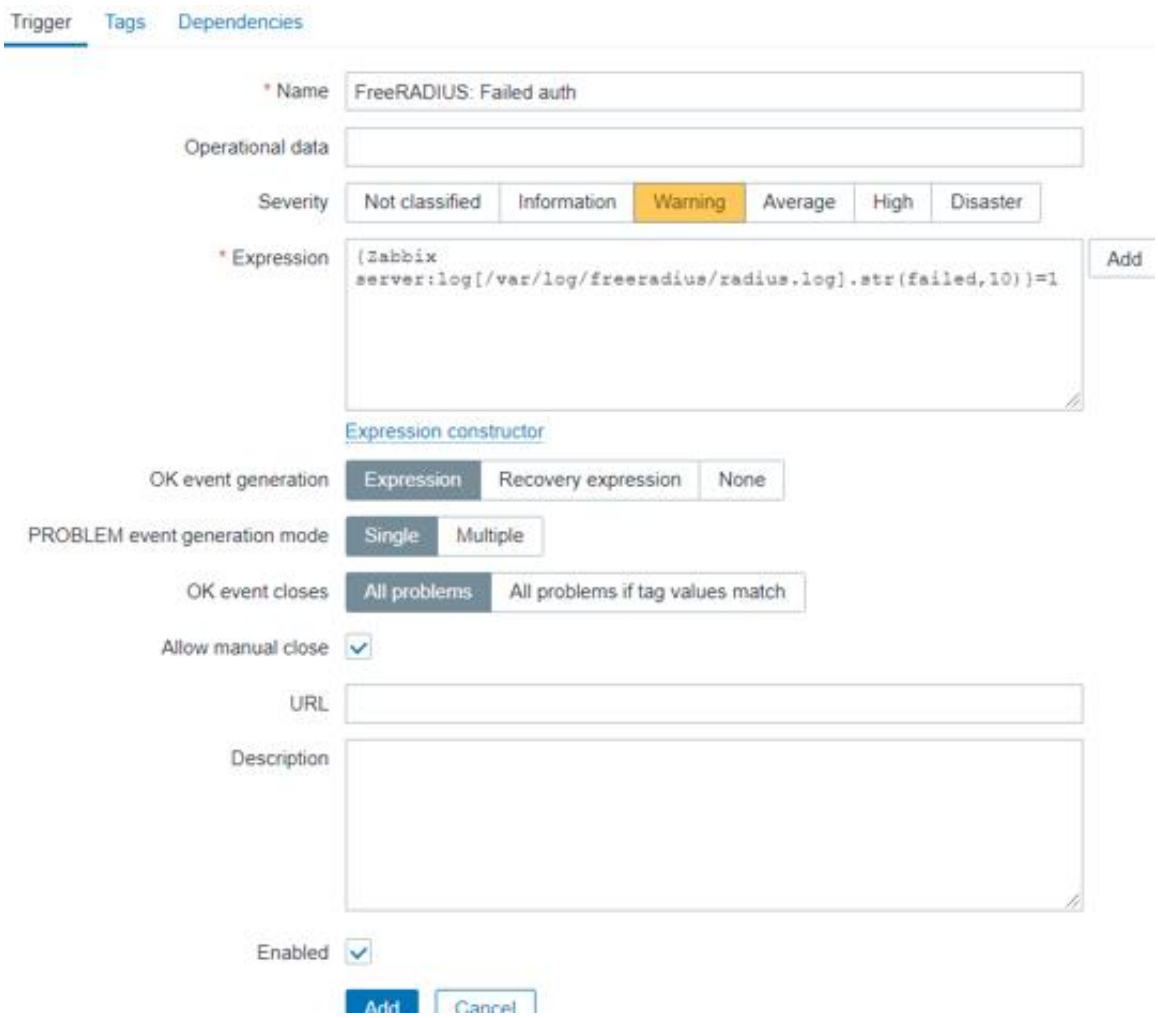

Рисунок 3.9 – Зображення процесу створення тригеру

На рисунку 3.10 чітко зображено результат спрацювань налаштованих тригерів.

Рисунок 3.10 – Зображення результату спрацьовувань

Віджет – допоміжний інструмент, який візуалізує спеціалізовану, під окремо визначену сферу діяльності, інформацію.

На рисунку 3.11 зображений віджет CPU та Memory, що моніторить стан навантажень на апаратні засоби мережі.

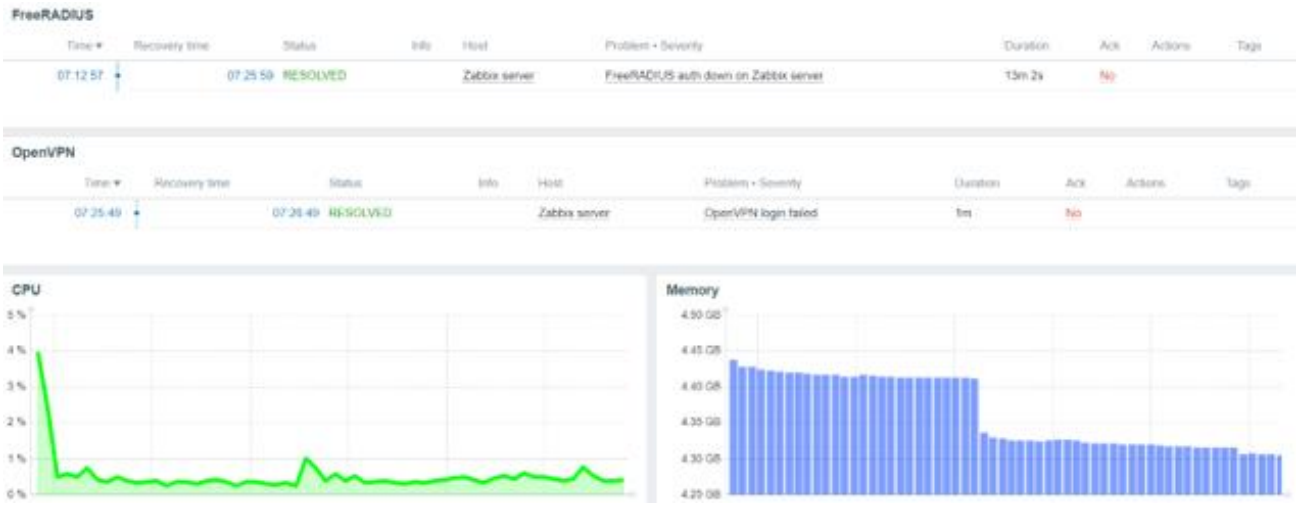

Рисунок 3.11 – Результат налаштувань віджетів

Шаблон – це набір об’єктів, що включає в себе:

- елементи даних;
- тригери;
- графіки;
- группи елементів даних;
- комплексні екрани.

Шаблони зазвичай використовуються для групування об'єктів конкретних сервісів або програм.

Таким чином, використання шаблонів є відмінним способом зниження свого навантаження та раціоналізації налаштування Zabbix.

На рисунку 3.12 зображено процес додавання шаблону.

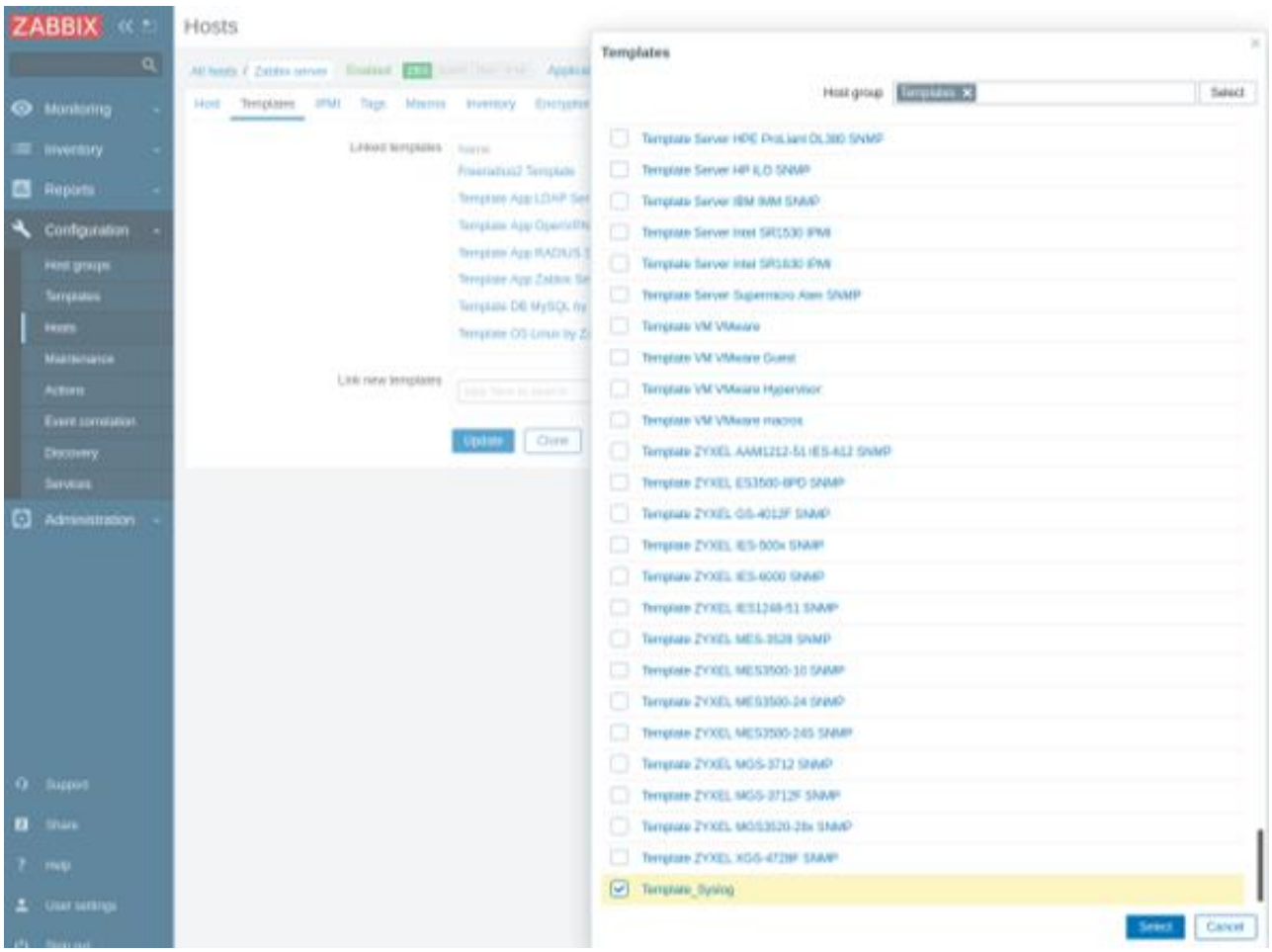

Рисунок 3.12 – Зображення процесу додавання шаблону

ICMP – це такий мережевий протокол, який входить у стек протоколів TCP/IP. Зазвичай ICMP використовують для передачі повідомлень щодо помилок та в інших виняткових ситуаціях, при передачі даних.

Також ICMP викопнує певні сервісні функції, наприклад на базі цього протоколу створені такі відомі утиліти як traceroute та ping.

Якщо з певних причин він ну увімкнений, то слід додати правила до iptables, виконавши команди з-під root/sudo:

- iptables -I INPUT -p icmp --icmp-type echo-request -j ACCEPT;
- iptables -I OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT.

Таким чином це дозволить ICMP запити на початок ланцюжка правил iptables.

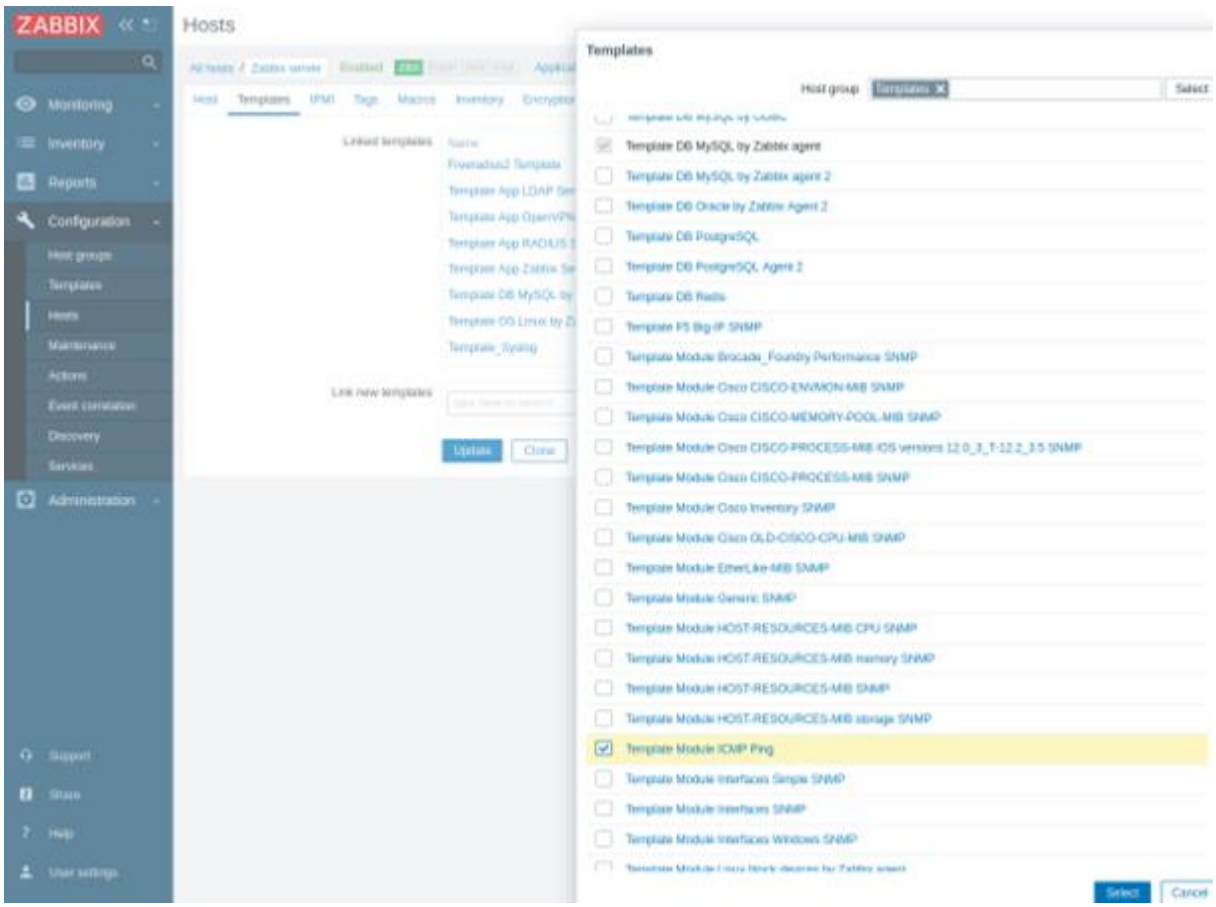

Рисунок 3.13 – Додавання шаблону ICMP

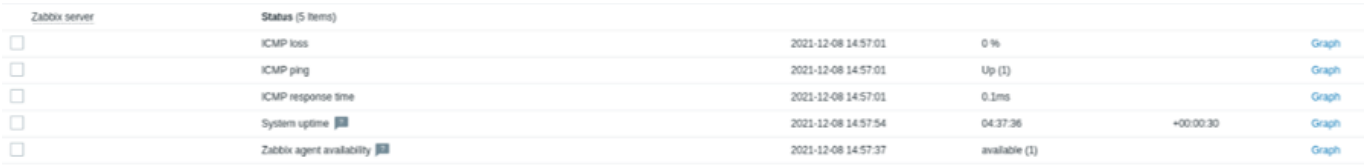

Рисунок 3.14 – Показники моніторингу ICMP

Задля отримування сповіщення від системи в Telegram, необхідно створити бота у мережі Telegram, з яким буде взаємодіяти система Zabbix.

Це спрощує навантаження адміністратора, надавши йому змогу віддалено слідкувати за системою за допомогою сповіщень.

Отримавши токен від бота, що зображений на рисунку 3.15, необхідно його використати в налаштуваннях самої системи Zabbix у розділі «Media type».

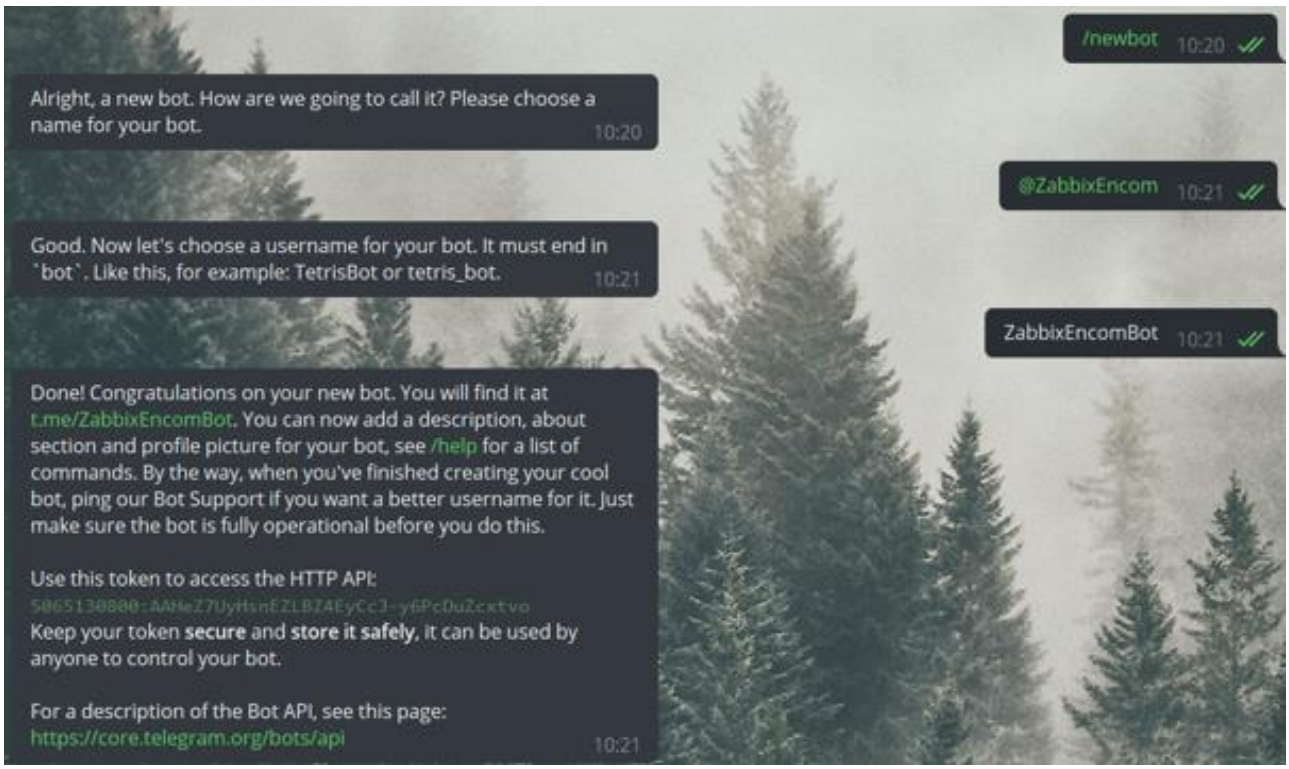

Рисунок 3.15 – Зображення процесу створення бота

Копіюємо в директорію /usr/lib/zabbix/alertscripts файли zbxtg.py та zbxtg_settings.example.py. Останній перейменовуємо на zbxtg_settings.py. Призначаємо користувача zabbix власником цих файлів: chown -R zabbix. /usr/lib/zabbix/alertscripts. Редагуємо файл zbxtg_settings.py.

```
zbx_tg_daemon_enabled_chats = ["Zabbix in Telegram Script", ]

zbx_db_host = "localhost"
zbx_db_database = "zabbix"
zbx_db_user = "zabbix"
zbx_db_password = "admin"
```

Рисунок 3.16 – Зображення місця редагування файлу

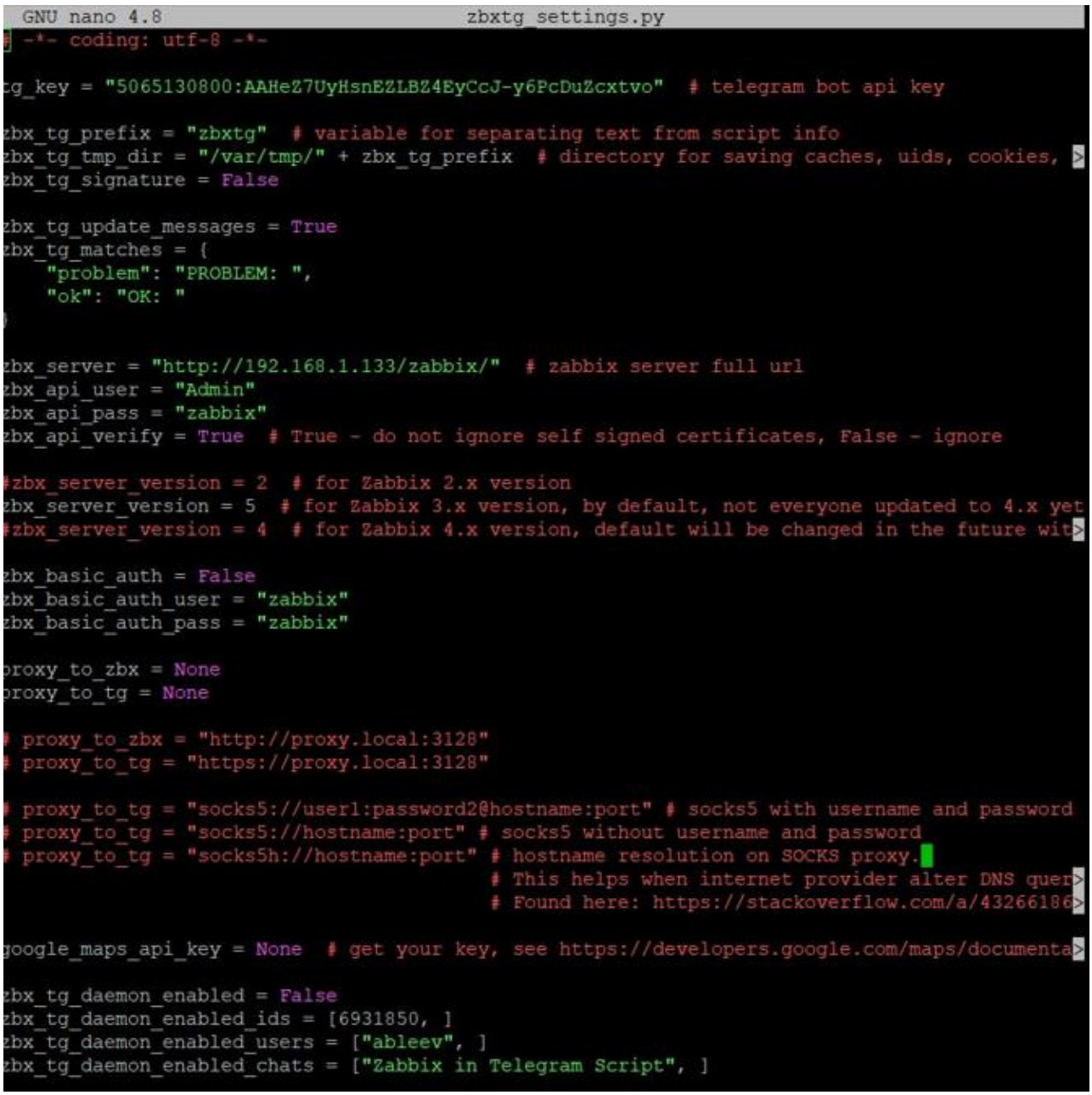

Рисунок 3.17 – Зображення редагування файлу

Далі у розділі «Media type» додаємо два нових способи сповіщень як зображено на рисунку 3.18.

Зокрема на рисунку 3.19 зображено шаблон сповіщень з типом повідломлень «Problem». Де наприклад zbxtg;graphs включає відправку графіків, zbxtg;graphs_period=10800 показує період протягом якого будується графік, ширину, висоту, заголовок тощо.

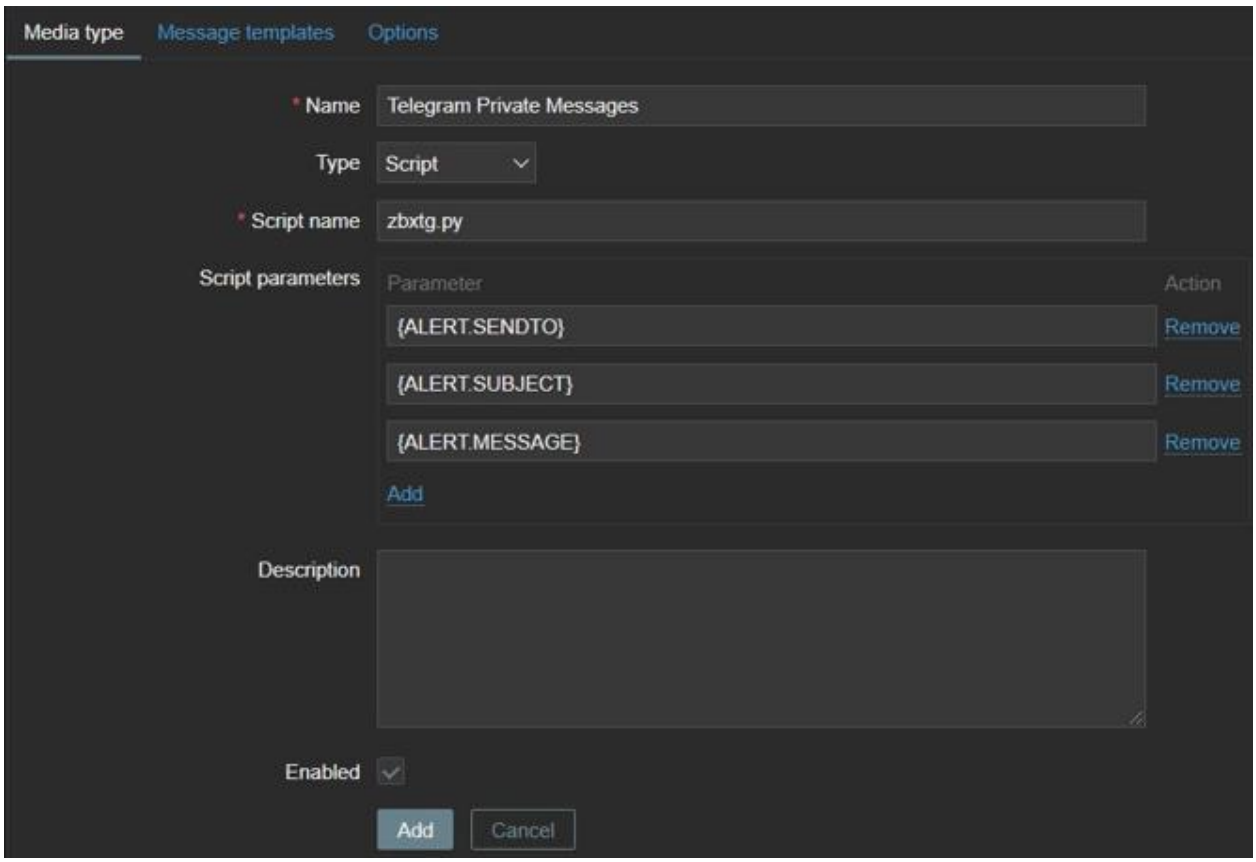

Рисунок 3.18 – Зображення процесу налаштувань сповіщень

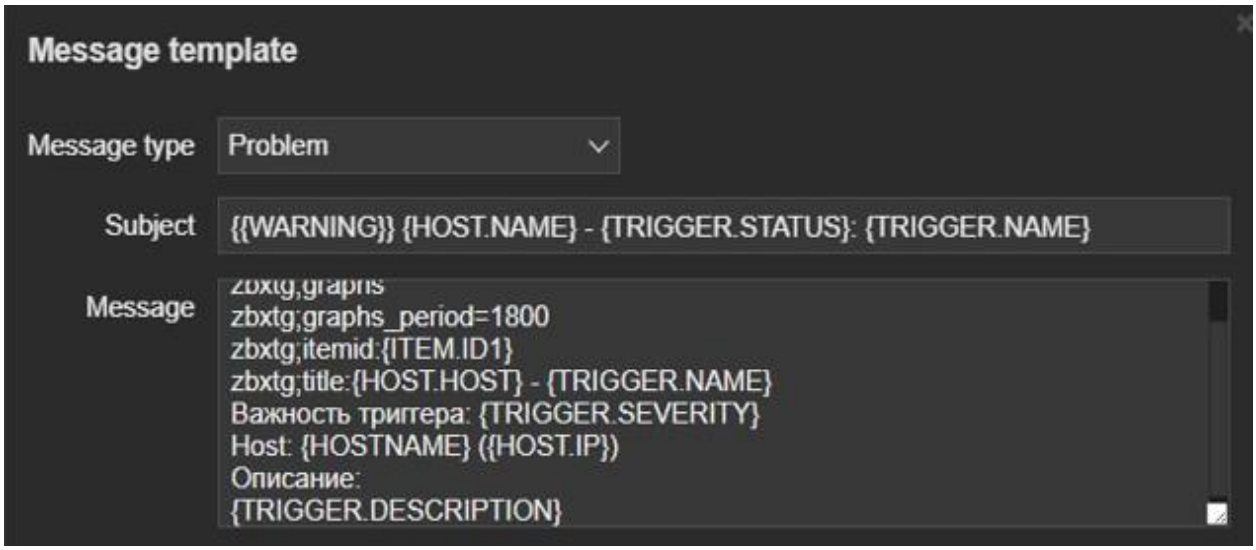

Рисунок 3.19 – Другий етап налаштувань сповіщень

На рисунку 3.20 зображено надання прав доступу на читання для групи користувачів. Це дасть змогу відправляти повідомлення тільки по тригерам цього хосту.

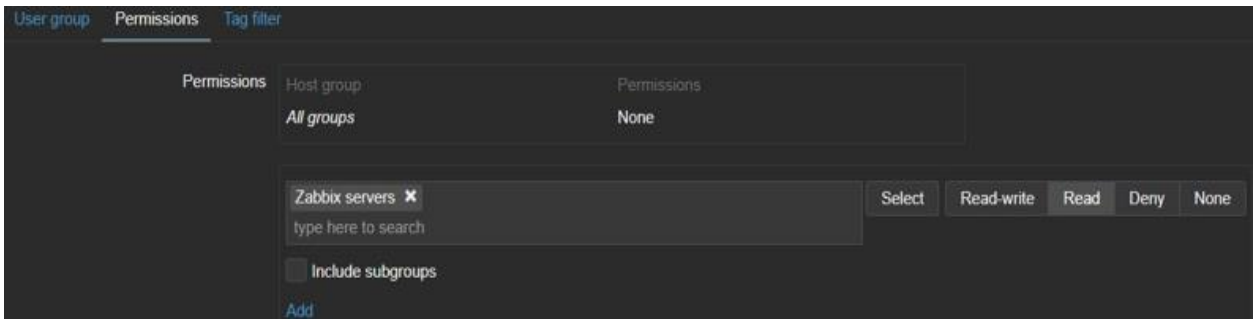

Рисунок 3.20 – Налаштування групи користувачів

На рисунку 3.21 зображено процес створення користувача і додавання його в групу Телеграму

.

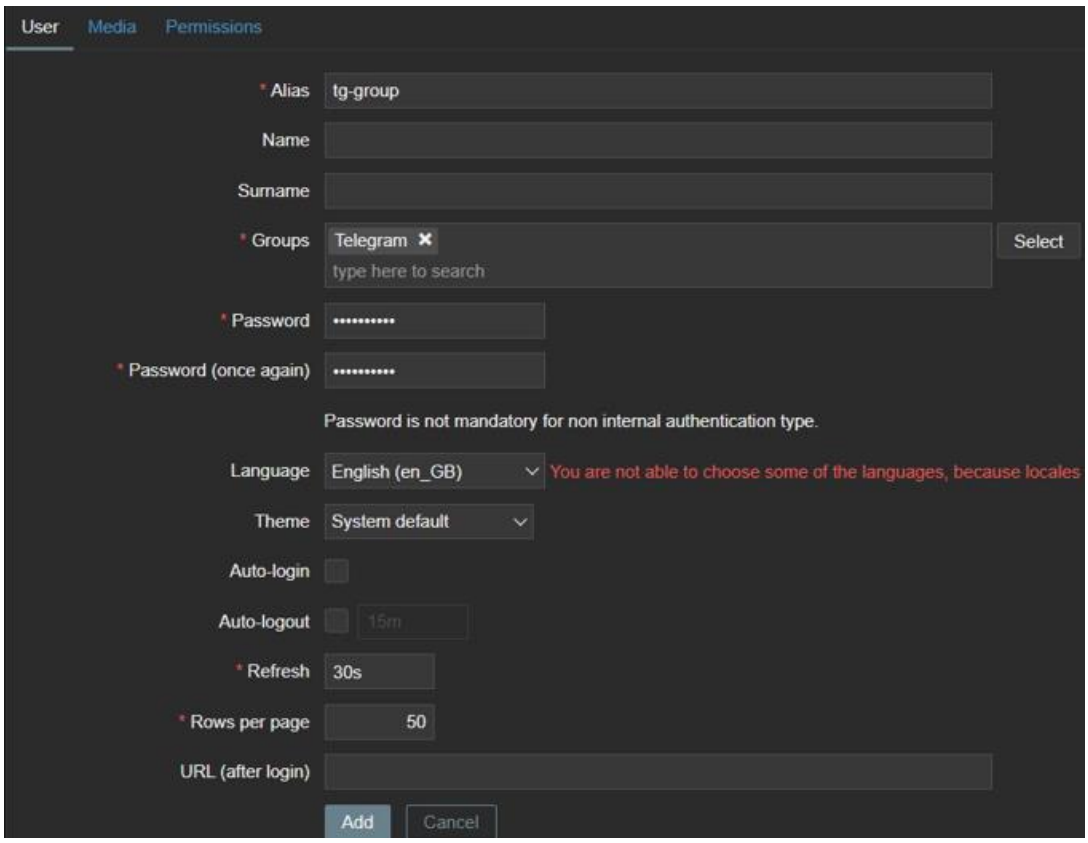

Рисунок 3.21 – Налаштування користувача

І кінцевим результатом є результат отримання повідомлень у вигляді сповіщень, про, наприклад, вимкнення серверу, як зображено на рисунку 3.22.

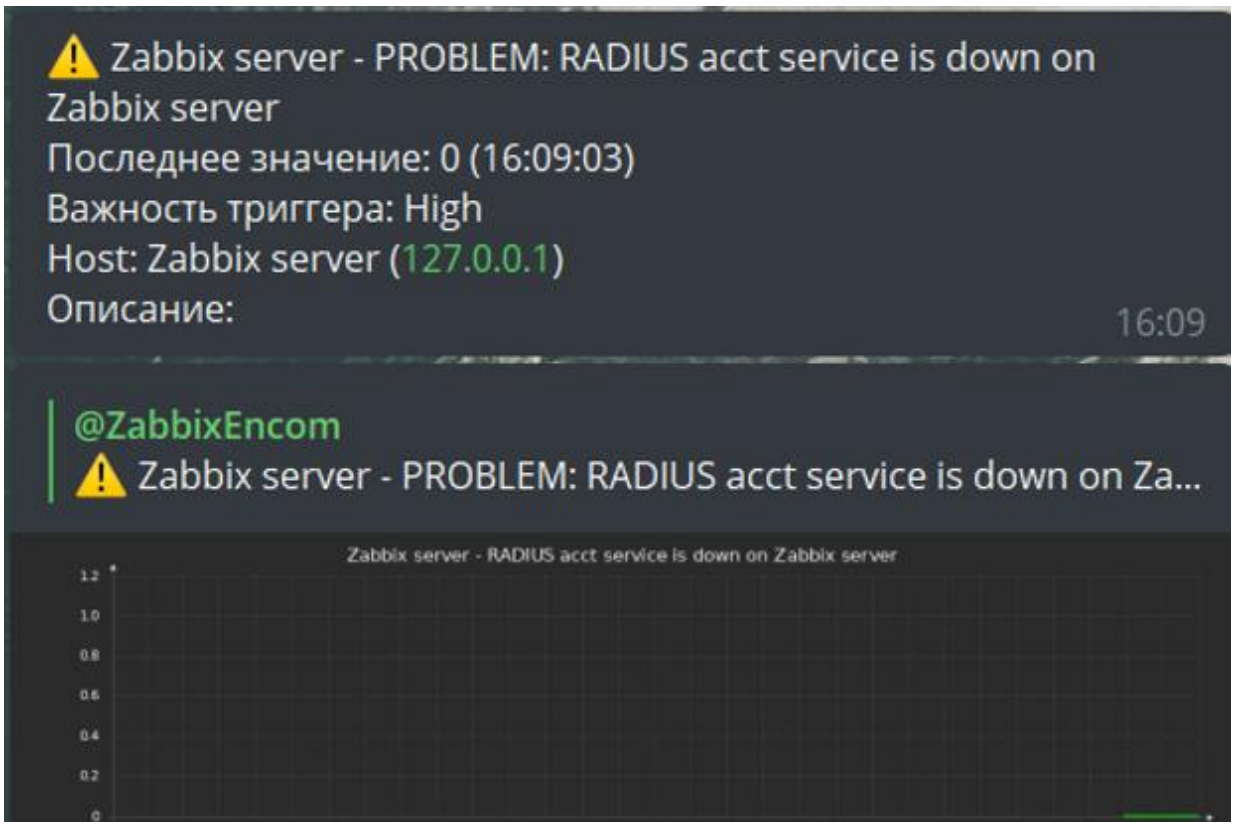

Рисунок 3.22 – Результат виводу повідомлень в боті

3.3 Рекомендації , щодо використання засобів моніторингу

Задля уникнення проблем існує декілька рекомендацій щодо використання засобів моніторингу.

По-перше, слід вирішити, яка інформація буде моніторитись. Для багатьох організацій втрата пристроїв, таких як наприклад стек комутаторів, не призведе до відсутності доступу до Інтернету. Проте слід знати, що деякі пристрої можуть спричинити серйозні наслідки, у момент їх відмови.

Також слід розуміти, за якими показниками потрібно слідкувати, адже, потрібно знати коли пристрій виходить з ладу. Велика кількість програм для моніторингу мережі використовує SNMP. Це така технологія, що дає змогу контролювати пристрої в мережі гляхом обміном важливою інформацією між агентами. Або ж інші технології чи протоколи для збору певних показників пристрою, що у свою чергу також дає можливість отримувати лише критично важливу інформацію.

Повідомлення ж корисні не постійно, а лише тоді, коли вони надходять тільки за нагальної потреби, та для певної групи людей. Слід взяти до уваги, що пошта не має бути переповнена помилковими тривогами чи сповіщеннями.

Спростити моніторинг, можна шляхом налаштування сповіщеннь лише на отримання заданою та бажаної інформації. Це і є одним з важливих критеріїв ефективного моніторингу мережі.

Перед тим, як намагатися покращити працездатність мережі, слід проаналізувати та проконтролювати продуктивність мережі з самого початку. Поточна ефективність допоможе це зробити. Таким чином, коли перевищені можливості самої мережі, це каже про те, що насправді справа стосується низької продуктивності.

Впровадження постійного моніторингу наприклад під час перебування в офісі - це чудовий шлях для стабільної роботи мережі. Проте ввімкнення постійного моніторингу, навіть не під час перебування в офісі, допоможе підтримувати правльне функціонування мережі в будь-який момент часу. Це відіграє велику роль для доступності до ресурсів. Безупинний моніторинг мережі не зіграє великої ролі на економії часу, адже існують рішення для моніторингу, які будут стежити за станом та надсилати повідомлення в режимі реального часу на потрібний ресурс навіть не знаходячись біля нього, наприклад, коли виникають певні проблеми з мережею.

Налаштування засобу, дало змогу впевнитись, що необхідність впровадження системи моніторингу існує, і це дає змогу в будь-який час бути проінформованим навіть з телефону:

- надходження необхідної інформацію про мережу;
- слідкувати за трафіком користувачів мережі;
- сповіщення про показники та стан в цілому ;
- можливість отримувати оповіщення адміністратором в будь-який час та незалежно від місця знаходження.

Таким чином система забезпечить не тільки велику функціональність моніторингу та управління, але й мобільність моніторингу та управління цією системою.

Висновки за розідлом 3

У даному розділі досліджено та налаштовано засоби захисту та моніторингу.

Зокрема налаштовано брандмауер та встановлено засіб моніторингу. Використання боту спрощує навантаження адміністратора, надавши змогу віддалено слідкувати за системою за допомогою сповіщень.

Надано рекомендації, щодо використання вищезазначених засобів таких як, наприклад, стеження за станом системи та надсилання сповіщеннь у режимі реального часу на мессенджер чи пошту. Тим самим мати постійний доступ та бути завжди проінформованим про стан мережі, адже це є одним з аспектів мобільності.

ВИСНОВКИ

Відповідно до теми дипломної роботи у першому розділі було проаналізовано архітектуру та складові локальних мереж. Зокрема досліджено компоненти та архітектуру мережі.

У другому розділі розглянуті основні вразливості локальних мереж та методи захисту.

У третьому розділі було обрано та налаштовано певні засоби захисту та моніторингу.

Щоб мати повноцінну інформції про мережу, необхіде рішення моніторингу, що в режимі реального часу дає змогу повідомити про події з будь-якого місця та в будь-який момент часу.

Для організайцій також необхідне рішення, яке просте у використанні, швидке, та недороге в обслуговуванні, і, що украй важливо надає необхідні функції. Також рішення має бути комплексним, тобто з великою кількістю можливостей та надійним. Тобто, задля високої доступності мережі необхіде відоме рішення.

Проте, при зборі великої кількості інформації про мережу, слід звертати увагу, що дані мають оброблятись швидко. При цьому відображені дані повинні включаючи у себе звітні дані, сповіщення, проблемні області та будь-яку іншу корисну інформацію. Це спростить швидко локалізувати та виправити проблему.

Оскільки мережа працює весь час, то ж різним користувачам знадобиться доступ до системи з різних причин, але не кожен має доступ до того чи іншого рівня інформації. Для цього потрібне рішення, на основі розподілу ролей, що надає дозвіл в залежності від призначення користувача в організації. Це надає належний рівень безпеки інформації в організації.

Тому, варто обирати рішення, що підтримує декілька методів моніторингу пристроїв.

Отже, метою даної дипломної роботи була реалізація засобів захисту та моніторингу локальних мереж.

Для досягнення поставленої мети були реалізовані й виконані наступні завдання:

- досліджено архітектуру та компоненти локальних мереж;
- проаналізовано вразливості локальних мереж;
- досліджено засоби , що використовуються для моніторингу та захисту локальних мереж;
- сформовано рекомендації щодо використання засобів.

Всі задачі були виконані в повному обсязі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Fiber Optic Solutions [Електронний ресурс]. – Режим доступу: https://www.fiber-optic-solutions.com/local-area-network-lan-analysis.html

2. What Is Local Area Network (LAN)? [Електронний ресурс]. – Режим доступу: https://www.toolbox.com/tech/networking/articles/what-is-local-area-network/#_001

3. What is a LAN – definition [Електронний ресурс]. – Режим доступу: https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN

4. LAN NETWORK TOPOLOGIES [Електронний ресурс]. – Режим доступу: https://www.firewall.cx/networking-topics/general-networking/103-network-topologies.html

5. Network Topologies [Електронний ресурс]. – Режим доступу: https://www.csl.mtu.edu/cs4451/www/notes/Network%20Topologies.pdf

6. What is Network Architecture? And, How Does It Work? [Електронний ресурс]. – Режим доступу: https://www.fusionconnect.com/blog/what-is-network-architecture

7. Common Types of Network Security Vulnerabilities [Електронний ресурс]. – Режим доступу: https://purplesec.us/common-network-vulnerabilities/

8. Вірус-хробак [Електронний ресурс]. – Режим доступу: https://presa.com.ua/aktualne/virus-khrobak-komp-yuternij-virus-khrobak-yak-viluchiti-virus.html#yak-zakhystytysia

9. Що таке ботнет [Електронний ресурс]. – Режим доступу: https://techukraine.net/

10. Соціальна інженерія: як шахраї використовують людську психологію в інтернеті [Електронний ресурс]. – Режим доступу: https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html

11. Топологія локальних мереж [Електронний ресурс]. – Режим доступу: https://studfile.net/preview/5153743/page:6/

12. [Електронний ресурс]. – Режим доступу: http://www.anodonta.com.ua/study/38.html

13. Моніторинг та аналіз локальних мереж [Електронний ресурс]. – Режим доступу: https://uareferat.com/

14. Як захиститися від вірусу [Електронний ресурс]. – Режим доступу: https://ukr.media/science/304566/

15. Налаштування брандмауера з UFW [Електронний ресурс]. – Режим доступу: https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-18-04-ru

16. Що таке роутер і як він працює [Електронний ресурс]. – Режим доступу: https://apelsin.net/uk/news/kak-rabotaet-router.html

17. Підключаємо Телеграм до Zabbix [Електронний ресурс]. – Режим доступу: https://osbsd.com/connecting-telegram-to-zabbix.html

18. Компоненти Zabbix[Електронний ресурс]. – Режим доступу: https://www.zabbix.com/documentation/1.8/ru/manual/installation/components

19. Zabbix [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/485538/

20. Вхід та налаштування користувача[Електронний ресурс]. – Режим доступу: https://www.zabbix.com/documentation/4.2/ru/manual/quickstart/login

21. Соціальна інженерія [Електронний ресурс]. – Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/sotsialnaya-inzheneriya/

22. Клієнт-серверна архітектура та ролі серверів [Електронний ресурс]. – Режим доступу: https://medium.com/@IvanZmerzlyi/

23. What is 2fam [Електронний ресурс]. – Режим доступу: https://experience.dropbox.com/ru-ru/resources/what-is-2fam

24. What is a Firewall? [Електронний ресурс]. – Режим доступу: https://www.forcepoint.com/cyber-edu/firewall

25. Налаштування Zabbix для ICMP-перевірок http://simon.rv.ua/nalashtuvannya-zabbix-dlya-icmp-perevirok-utilita-fping-na-linux-centos-redhat-fedora.html

26. Логічні бомби [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/zagrozu/project-updates/logicnibombi-1

27. P2P on the local network [Електронний ресурс]. – Режим доступу: https://www.slideshare.net/peterelst/p2p-on-the-local-network

28. Поняття комп’ютерної мережі, основні функції [Електронний ресурс]. – Режим доступу: https://kppk.com.ua/ELLIB/ebook/Segrienko/KSM/user-files/km_opk_2017_kl.pdf

29. Best network monitoring tools [Електронний ресурс]. – Режим доступу: https://www.softinventive.com.ua/best-network-monitoring-tools/

30. Network Monitoring Best Practices [Електронний ресурс]. – Режим доступу: https://www.whatsupgold.com/resources/best-practices/network-monitoring