

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

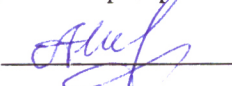
до випускної кваліфікаційної роботи бакалавра
на тему: «Проєкт підсистеми виявлення та блокування
кібератак на мережну інфраструктуру компанії»

Виконав: студент 4-го курсу групи КБ-20-2
спеціальності 125 «Кібербезпека»



Павло СКОЧКО

Керівник: Доцент кафедри КІ та КБ, к.т.н.



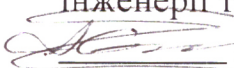
Олексій ШЕЛУХА

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



Олександр МАЄВСЬКИЙ

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
5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Скочко Павло Андрійович

Тема роботи: «Проект підсистеми виявлення та блокування кібератак на мережну інфраструктуру компанії»

затверджена Наказом університету від 5 березня 2024 р. № 98

Термін здачі студентом закінченої роботи 9 червня 2024 р.

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

- Система виявлення та запобігання вторгненням у мережу;
- Процес функціонування мережної інфраструктури;

Обладнання та програмне забезпечення:

1. Snort
2. Kali Linux
3. pfSense
4. Маршрутизатор NETGATE 2100

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Володимир Котенко	12.05.24	13.05.24 
2	Володимир Котенко	13.05.24	14.05.24 
3	Володимир Котенко	15.05.24	16.05.24 

Студент 
Керівник 

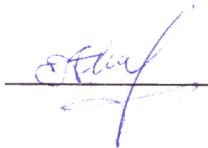
Павло СКОЧКО
Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	до 10.03.2024	Виконано
2	Розробка плану роботи	до 16.04.2024	Виконано
3	Аналіз об'єкта дослідження	до 16.04.2024	Виконано
4	Опрацювання літературних джерел	до 03.05.2024	Виконано
5	Розробка теоретичного макету	до 06.05.2024	Виконано
6	Вибір обладнання	до 19.05.2024	Виконано
7	Налаштування системи	до 29.05.2024	Виконано
8	Тестування системи	до 29.05.2024	Виконано
9	Аналіз результатів тестування	до 29.05.2024	Виконано
10	Написання пояснювальної записки	до 07.06.2024	Виконано
11	Отримання відгуку та рецензій	до 13.06.2024	Виконано
12	Захист	до 28.06.2024	Виконано

Студент 

Павло СКОЧКО

Керівник 

Олексій ШЕЛУХА

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи на тему «Проект підсистеми виявлення та блокування кібератак на мережну інфраструктуру компанії», складається з 51 сторінок, 27 рисунків, 3 таблиці, список використаних джерел містить 23 наіменувань та займає 2 сторінки.

Метою роботи є розгортання та дослідження процесу роботи системи виявлення та запобігання вторгненням для блокування кібератак на мережну інфраструктуру.

У ході роботи визначено основні завдання для розгортання та дослідження процесу роботи системи виявлення та запобігання вторгненням, проаналізовано існуючі системи та обрано оптимальне рішення для невеликої мережі компанії. Розглянуто особливості різних систем запобігання вторгненням, таких як Cisco Secure IPS, McAfee Intrusion Prevention System, Snort, Suricata, OSSEC та StoneGate Intrusion Prevention System. Показано процес розгортання та виконано дослідження процесу роботи обраної системи, Snort у поєднанні з pfSense, включаючи вибір обладнання, налаштування та тестування системи. Наведено результати тестування, які підтверджують ефективність та надійність розгонутої системи запобігання вторгненням.

Ключові слова: ЗАХИСТ МЕРЕЖІ, МОНІТОРИНГ, БЛОКУВАННЯ ВТОРГНЕНЬ, ВИЯВЛЕННЯ ВТОРГНЕНЬ, КІБЕРАТАКА, SNORT, PFSense, IPS, IDS, FIREWALL.

					ККІКБ.КР.Б – 125 – 16 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата					
Розроб.		Скочко П.А.		19.06.24	Літ.		Арк.	Аркуші	
Керівник		Шелуха О.О.		19.06.24			4	51	
Реценз.		Маєвський О.В.		19.06.24	Проект підсистеми виявлення та блокування кібератак на мережну інфраструктуру компанії				
Н. Контр.		Шелуха О.О.		19.06.24					
Затверд.		Єфіменко А.А.		19.06.24					
					ФІКТ, Гр. КБ-20-2				

ANNOTATION

The explanatory note for the qualification work on "Project of Intrusion Detection and Prevention Subsystem for Company Network Infrastructure" consists of 51 pages, including 27 figures, 3 tables, and a list of 23 references spanning 2 pages. The aim of this work is to deploy and investigate the operation process of an intrusion detection and prevention system to block cyber attacks on the company's network infrastructure.

During the study, the main tasks for deploying and researching the operation process of intrusion prevention systems were identified. Existing systems were analyzed, and an optimal solution was selected for the company's small-scale network. The features of various intrusion prevention systems such as Cisco Secure IPS, McAfee Intrusion Prevention System, Snort, Suricata, OSSEC, and StoneGate Intrusion Prevention System were considered. The deployment process and research of the selected system, Snort in conjunction with pfSense, including hardware selection, configuration, and system testing in a real environment, were demonstrated. The testing results confirmed the effectiveness and reliability of the deployed intrusion prevention system.

Keywords: NETWORK PROTECTION, MONITORING, INTRUSION PREVENTION, INTRUSION DETECTION, CYBER ATTACK, SNORT, PFSENSE, IPS, IDS, FIREWALL.

		Скочко П.А.			ККИКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ДОСЛІДЖЕННЯ СИСТЕМ ЗАПОБІГАННЯ ВТОРГНЕННЯМ ТА ПОСТАНОВКА ТЕХНІЧНОЇ ЗАДАЧІ.....	9
1.1. Аналіз досліджень та визначення основних завдань системи запобігання вторгненням.	9
1.2. Класифікація методів та технологій запобігання вторгненням.	10
1.3. Порівняльний аналіз систем виявлення та запобігання вторгнень.	19
1.4 Постановка технічного завдання.....	21
Висновки до першого розділу:	22
РОЗДІЛ 2. АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ВИБІР МОДЕЛІ СИСТЕМИ ..	23
2.1. Система виявлення несанкціонованого доступу Cisco Secure IPS.	23
2.2. Система мережевого захисту McAfee Intrusion Prevention System.	24
2.3. Система виявлення та запобігання вторгненням Snort.	25
2.4. Система виявлення та запобігання вторгненням Suricata.	26
2.5. Хост-орієнтована система запобігання вторгненням OSSEC.....	28
2.6. Апаратно-програмний комплекс StoneGate Intrusion Prevention System..	29
2.7. Вибір моделі системи виявлення та запобігання вторгненням.	30
Висновки до другого розділу:	31
РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ.....	32
3.1. Аналіз топології мережі.....	32
3.2. Вибір обладнання.....	34
3.3. Розгортання та налаштування мережевої інфраструктури.	35
3.4. Перевірка роботоспроможності системи виявлення та блокування вторгнень.	42
Висновки до третього розділу:.....	48
ВИСНОВКИ	49
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	50

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СВВ – Система Виявлення Вторгнень

СЗВ – Система Запобігання Вторгненням

DCHP – Dynamic Host Configuration Protocol

DNS – Domain Name System

DoS – Denial of Service

GPL – General Public License

HIDS – Host-Based Intrusion Detection System

IDES – Intrusion Detection Expert System

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

NIDS – Network Intrusion Detection System

SIEM – Security Information And Event Management

SQL – Structured Query Language

TCP – Transmission Control Protocol

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. У сучасному світі, де інформаційні технології відіграють ключову роль у діяльності більшості організацій, питання кібербезпеки стає надзвичайно важливим. Системи запобігання вторгненням є критично необхідними для захисту мережевої інфраструктури від різноманітних кібератак, що можуть призвести до витоку конфіденційної інформації, фінансових втрат та порушення безперебійної роботи компаній. У межах цієї роботи розглядаються методи та засоби розгортання та дослідження процесу роботи систем виявлення та запобігання вторгненням.

Метою кваліфікаційної роботи є проектування, розгортання та дослідження процесу роботи підсистеми виявлення та блокування кібератак на мережну інфраструктуру компанії з використанням системи виявлення та запобігання вторгненням.

Визначена мета обумовлює наступні завдання:

- Аналіз існуючих систем виявлення та запобігання вторгненням та їх характеристик.
- Вибір оптимальної системи виявлення та запобігання для невеликої мережі компанії.
- Розробка проєкту розгортання та дослідження процесу роботи обраної системи системи виявлення та запобігання вторгненням.
- Налаштування та тестування системи.

Об'єктом дослідження є процес моніторингу мережевого трафіку та захисту інфраструктури компанії від вторгнень.

Предметом дослідження є методи та засоби розгортання та дослідження процесу роботи системи запобігання вторгненням для захисту мережної інфраструктури.

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми виявлення та блокування кібератак на основі Snort у поєднанні з rpfSense. Проєкт включає аналіз існуючої мережевої інфраструктури, вибір відповідного обладнання, налаштування системи та її тестування.

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1. ДОСЛІДЖЕННЯ СИСТЕМ ЗАПОБІГАННЯ ВТОРГНЕННЯМ ТА ПОСТАНОВКА ТЕХНІЧНОЇ ЗАДАЧІ

1.1. Аналіз досліджень та визначення основних завдань системи запобігання вторгненням.

Системи запобігання вторгненням стали важливим елементом кібербезпеки, що розвивався у відповідь на зростання кіберзагроз та складності мережевих інфраструктур. Історія виникнення та розвитку СЗВ тісно пов'язана з еволюцією систем виявлення вторгнень, з яких вони і походять. У 1980-х роках, коли комп'ютерні мережі почали активно розширюватися, з'явилася необхідність у засобах для виявлення та реагування на несанкціоновані дії в мережах. У цей час почали з'являтися перші концепції СВВ, вони були пасивними і виконували функцію моніторингу, але не могли блокувати атаки в режимі реального часу. Першим хто запропонував такий концепт був Джеймс Андерсон, він у 1980 році у Національній агенції безпеки США запропонував інструменти для аналізу аудиторських слідів, які включали журнали доступу користувачів, журнали доступу до файлів та журнали системних подій. Ці журнали допомагали адміністраторам відслідковувати підозрілу активність. Наступними, у 1986 році, Дороті Е. Денінг та Пітер Г. Нойманн опублікували модель СВВ, яка лягла в основу для багатьох сучасних систем. Модель використовувала статистичні методи для виявлення аномалій. Розроблена система, відома як Intrusion Detection Expert System, обробляла як дані користувача, так і мережеві дані. IDES поєднувала правила для виявлення відомих типів вторгнень зі статистичним аналізом аномалій. [1] Робота Денінг і Нойманна послугувала базою для іншої системи, у 1988 році з'явилася система Multics Intrusion Detection and Alerting System. У тому ж році також з'явилася система Haystack, яка застосовувала статистику для зменшення обсягу аудиторських слідів.

У 1990 році з'явилося декілька інших важливих систем, таких як Time-based Inductive Machine, яка використовувала індуктивне навчання для виявлення аномалій, і Network Security Monitor, що використовувала

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

маскування матриць доступу для виявлення аномалій. Також був розроблений Information Security Officer's Assistant, який включав різні стратегії, зокрема статистику, перевірку профілів та експертну систему. [2]

На початку 2000-х років системи СВВ продовжували розвиватися, також почалася активна розробка і впровадження систем запобігання вторгненням. Ці системи поєднали функціональність СВВ з можливістю автоматичного реагування на загрози. СЗВ аналізують мережевий трафік, виявляють підозрілі дії та блокують їх до того, як вони зможуть завдати шкоди. Основні завдання СЗВ включають захист від різноманітних атак, таких як мережеві черв'яки, сканування портів, атаки на служби та застосунки, а також зловмисні дії користувачів. [3]

1.2. Класифікація методів та технологій запобігання вторгненням.

Системи запобігання вторгненням представляють собою комплексні програмні або апаратні рішення, спрямовані на виявлення та блокування неправомірних або шкідливих дій у комп'ютерних системах та мережах. Ці системи базуються на різноманітних алгоритмах та методах аналізу мережевого трафіку, спеціальних правилах для виявлення аномальних або підозрілих активностей. [2]

СЗВ можна поділити на мережеві системи запобігання вторгненням та хост-орієнтовані системи запобігання вторгненням. Мережеві системи встановлюються на мережевих вузлах і аналізують весь трафік, що проходить через мережу. Мережеві системи виявляють аномалії та сигнатури атак, спрямовані на мережеві пристрої. Іншою категорією є хост-орієнтовані системи, які встановлюються на окремих комп'ютерах або серверах. Вони спеціалізуються на виявленні атак, які спрямовані безпосередньо на окремі системи. Хост-орієнтовані системи аналізують системні файли, реєстри та інші параметри для виявлення незвичайної активності. [4-5]

За архітектурою, системи запобігання вторгненням можна класифікувати на централізовані, децентралізовані та розподілені. Централізовані системи зазвичай мають один центральний вузол, який відповідає за аналіз мережевого

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

трафіку та виявлення аномалій чи вторгнень. Така архітектура може бути ефективною для невеликих мереж або організацій, де збір та аналіз трафіку можуть бути зосереджені в одному місці. Децентралізовані системи мають розподілену архітектуру, де кожен вузол мережі відповідає за виявлення аномалій та вторгнень в своїй області відповідальності. Це дозволяє реалізувати більш гнучку та масштабовану систему, оскільки вона може адаптуватися до змін у мережі та обсязі трафіку без необхідності централізованого управління. Розподілені системи є комбінацією централізованих та децентралізованих підходів, де кілька вузлів спільно аналізують мережевий трафік та координують свою роботу для виявлення аномалій та вторгнень. Це дозволяє поєднати переваги обох підходів і створити більш ефективну та надійну систему запобігання вторгненням. [6-8]

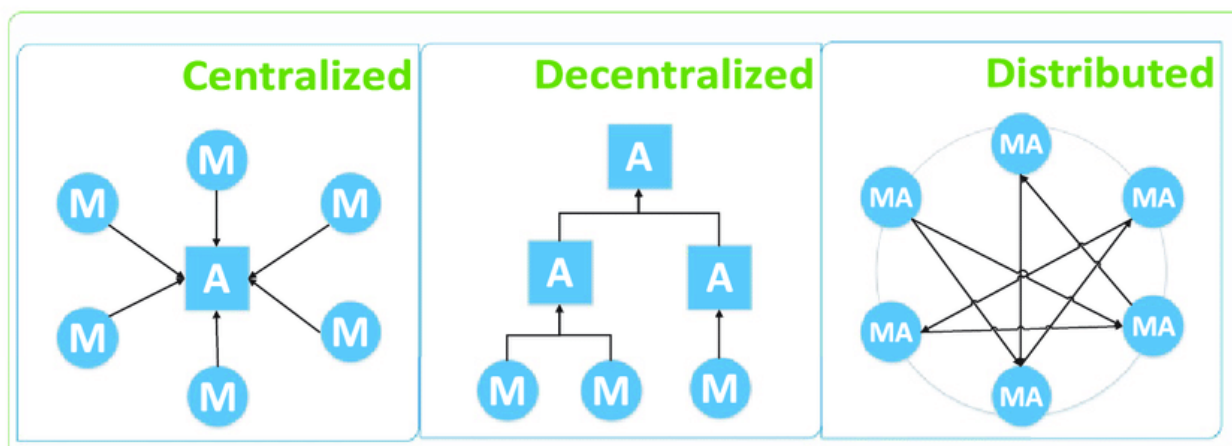


Рис. 1.1 Схематичне зображення різних архітектур

Також класифікувати СЗВ можна за методом виявлення. Існують різні підходи до методів виявлення, які можуть бути використані в системах запобігання вторгненням. Один з основних методів виявлення - сигнатурний аналіз. Цей метод полягає в пошуку вхідних даних або активності, які відповідають відомим сигнатурам атак або вразливостей. Системи, які використовують цей метод, перевіряють потік даних на відповідність відомим сигнатурам, що дозволяє їм розпізнавати вже відомі атаки та шкідливі дії. Інший метод - аналіз аномалій. Цей підхід спрямований на виявлення несподіваних, незвичних або відхилень від типової активності в мережі чи на системі. Для

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

цього методу використовуються алгоритми, що аналізують зміни в мережевому трафіку, системних ресурсах чи інших параметрах, та сповіщають адміністратора про можливі потенційні загрози. [7,9]

Функція виявлення вторгнень є однією з основних складових СЗВ. Вона відповідає за ідентифікацію потенційних загроз та шкідливих дій у мережі чи на інших об'єктах захисту. Головною метою цієї функції є раннє виявлення атак та інших небажаних подій перед їх негативним впливом на систему. Для ефективного виявлення вторгнень використовуються різноманітні методи, включаючи сигнатурний аналіз, аналіз аномалій, використання евристичних алгоритмів та машинного навчання. Системи запобігання вторгненням можуть комбінувати декілька методів для забезпечення більшої точності та ефективності виявлення. [10]

Опис методів виявлення вторгнень:

- Сигнатурний аналіз:

У СЗВ, сигнатурний аналіз є одним з основних методів виявлення та блокування атак. Сигнатура атаки - це унікальний патерн чи сигнатура, яка характеризує конкретний вид зловмисницького вторгнення. Цей метод базується на порівнянні активності в мережі з відомими сигнатурами атак, що забезпечує ефективну ідентифікацію та блокування шкідливого трафіку. Сигнатурний аналіз використовує бази даних з відомими сигнатурами атак, які регулярно оновлюються відповідно до нових загроз. При виявленні відповідності між активністю в мережі та сигнатурою атаки, система вживає відповідних заходів для блокування цієї атаки або виконання інших визначених дій, які можуть включати інформування адміністратора чи реалізацію автоматичних заходів захисту. Однією з переваг сигнатурного аналізу є його висока ефективність у виявленні відомих атак, оскільки бази даних з сигнатурами можуть бути досить великими та деталізованими. Крім того, цей метод може бути легко імплементований та швидко реагувати на нові загрози, коли вони стають відомими. Проте, сигнатурний аналіз має свої обмеження. Але

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

він має таке і недоліки, він неефективний у виявленні нових атак, які не мають відомих сигнатур, що робить систему вразливою до zero-day атак. [11]

Однією з ключових складових сигнатурного аналізу в системах запобігання вторгненням є постійне оновлення сигнатурних баз. Цей процес є необхідним для забезпечення актуальності та ефективності виявлення відомих атак. Оновлення сигнатур включає в себе пошук та ідентифікацію нових атак, аналіз їхніх особливостей та розробку відповідних сигнатур. Регулярні випуски оновлень є важливою частиною стратегії кібербезпеки. Компанії, що розробляють системи запобігання вторгненням, взаємодіють із великою кількістю джерел інформації щодо нових загроз та вразливостей. Це може включати співпрацю з іншими компаніями кібербезпеки, аналіз даних від спільноти користувачів, а також використання розвинених алгоритмів машинного навчання для виявлення нових атак на основі великої кількості даних. З моменту виявлення нової атаки до створення та включення в сигнатурну базу може пройти значний час, тому важливо мати механізми швидкого реагування на виникнення нових загроз. [12] Деякі системи використовують технології, які дозволяють вони оновлювати сигнатурні бази в режимі реального часу, щоб мінімізувати термін вразливості перед новими атаками.

Попри свою ефективність у виявленні відомих атак, сигнатурний аналіз має свої обмеження. Одним з найбільш серйозних обмежень є здатність лише виявляти атаки, для яких відомі сигнатури. Це означає, що сигнатурний аналіз не може виявити нові атаки або атаки зміненими сигнатурами, які не входять до бази даних сигнатур. Це створює ризик пропуску атак, особливо для тих, які використовуються зловмисниками з метою обходу систем виявлення вторгнень. [12] Ще одним обмеженням сигнатурного аналізу є можливість фальш-позитивних та фальш-негативних результатів. Фальш-позитивні результати виникають, коли система помилково виявляє нормальний трафік як атаку, що може призвести до великої кількості ложних сповіщень про вторгнення. З іншого боку, фальш-негативні результати виникають, коли система не виявляє

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

справжню атаку, що може призвести до пропуску загрози без відповідної реакції. Крім того, обмеженням є потреба у значних ресурсах для зберігання та обробки великих баз даних сигнатур. При зростанні кількості відомих атак збільшується обсяг бази даних, що може призвести до збільшення навантаження на систему та зниження її продуктивності.

У підсумку, хоча сигнатурний аналіз є потужним інструментом для виявлення відомих атак, важливо розуміти його обмеження та шукати додаткові методи захисту для компенсації цих обмежень.

- Аномальний аналіз:

Аномальний аналіз є ще одним методом виявлення атак, який відрізняється від сигнатурного аналізу. Замість того, щоб шукати конкретні сигнатури атак, аномальний аналіз спрямований на виявлення незвичайних або аномальних патернів в поведінці користувачів або мережевому трафіку. Цей метод базується на ідеї, що зломисники часто проявляються в мережі як нестандартні або відмінні від звичних дії. Для виявлення аномалій у поведінці користувачів або мережевому трафіку аномальний аналіз використовує різноманітні алгоритми для виявлення незвичайних патернів у поведінці користувачів та мережевому трафіку. Один з найпоширеніших методів - це статистичний аналіз, який використовує статистичні показники, такі як середнє значення та стандартне відхилення, для виявлення відхилень від звичайних патернів. Ще одним підходом є машинне навчання, яке дозволяє системі адаптуватися до нових угроз і навчатися виявляти аномальні патерни без явного визначення правил або сигнатур. Методи машинного навчання можуть використовувати різноманітні алгоритми, такі як нейронні мережі, дерева рішень, або методи кластеризації, для виявлення аномалій. Деякі алгоритми аномального аналізу використовують спеціалізовані моделі, які враховують контекст та характеристики конкретної мережі чи системи. Ці методи дозволяють виявляти відхилення від нормальних патернів та ідентифікувати потенційні загрози. [11]

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Аномальний аналіз має свої переваги та недоліки. Однією з головних переваг є здатність виявляти нові, раніше невідомі атаки або незвичайні патерни в поведінці користувачів та мережі. Це робить його ефективним інструментом для захисту від нуль-денних атак та внутрішніх загроз, які можуть не бути включені до сигнатурних баз даних. [12] Ще однією перевагою є можливість виявлення складних та незрозумілих атак, які можуть не мати явних сигнатур або відмінностей від звичайної поведінки. Алгоритми аномального аналізу можуть виявляти такі атаки на основі відхилень від звичайних патернів. Проте аномальний аналіз також має свої недоліки. Один з найбільш серйозних недоліків - це високий рівень фальш-позитивних результатів. Оскільки алгоритми виявлення аномалій шукають незвичайні патерни, вони можуть реагувати на звичайні, але несподівані ситуації як на потенційні загрози. Ще однією проблемою є складність налаштування та конфігурування алгоритмів аномального аналізу. Потрібно враховувати різні типи аномалій, специфіку мережі та вимоги до безпеки, щоб забезпечити ефективну роботу системи.

У підсумку, аномальний аналіз є важливим інструментом для виявлення нових та складних атак, але йому необхідно вдосконалення для зменшення кількості фальш-позитивних результатів та спрощення налаштування для адміністраторів.

- Нейронні мережі:

Використання нейронних мереж для виявлення атак стає все більш популярним підходом у сфері кібербезпеки. Нейронні мережі є потужними інструментами машинного навчання, які можуть навчитися виявляти складні патерни в поведінці користувачів та мережевому трафіку. Вони здатні автоматично адаптуватися до нових угроз та змін у кіберсередовищі. Один з типів нейронних мереж, які широко використовуються для виявлення атак, - це згорткові нейронні мережі. Ці мережі використовуються для обробки зображень, але їх також успішно застосовують для аналізу мережевого трафіку. Вони можуть виявляти складні патерни та аномалії у трафіку, що може бути індикатором атак. Інший тип нейронних мереж, який застосовується для

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

виявлення атак, - це рекурентні нейронні мережі. Вони призначені для аналізу послідовностей даних, що робить їх ефективними для виявлення аномальних патернів у мережевому трафіку або в діяльності користувачів. [13] Нейронні мережі можуть бути навчені на великій кількості даних про нормальну поведінку користувачів та мережевого трафіку, а також про відомі атаки. Це дозволяє їм ефективно виявляти аномалії та потенційні загрози в реальному часі.

Нейронні мережі мають кілька переваг у виявленні атак. Однією з них є їх здатність виявляти складні та незвичайні патерни, які можуть бути складні для виявлення іншими методами. Це робить їх ефективними для виявлення нуль-денних атак та інших важких загроз. Ще однією перевагою є їх здатність до навчання на основі великої кількості даних та адаптація до нових угроз та змін у кіберсередовищі. Це дозволяє їм підтримувати актуальність та ефективність виявлення атак у реальному часі. Проте нейронні мережі також мають свої недоліки. Один з найважливіших - це вимога до значних обчислювальних ресурсів для навчання та використання. Великі та складні мережі можуть потребувати значних обчислювальних потужностей, що може бути викликом для більш малих організацій чи компаній з обмеженими ресурсами. Іншою проблемою може бути складність інтерпретації результатів нейронних мереж. Через свою складність та нелінійність, нейронні мережі можуть бути складними для розуміння та пояснення результатів їх роботи, що може ускладнити аналіз та прийняття рішень для адміністраторів кібербезпеки.

У підсумку, нейронні мережі є потужним інструментом для виявлення атак, але вони також мають свої обмеження, такі як вимога до обчислювальних ресурсів та складність інтерпретації результатів.

Успішне виявлення вторгнень передбачає постійне моніторингове відстеження активності в мережі або на системі. Це може включати аналіз мережевого трафіку, перевірку системних журналів, моніторинг використання ресурсів та інші методи збору інформації. Крім того, важливим аспектом виявлення вторгнень є спроможність системи аналізувати та реагувати на нові

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

та раніше невідомі загрози. Це може бути досягнуто через постійне оновлення сигнатур атак, вдосконалення евристичних методів аналізу та застосування передових технологій штучного інтелекту. [14]

В результаті успішного виявлення вторгнення система може сповістити адміністратора про потенційну загрозу, автоматично виконати певні заходи захисту або навіть ізолювати чи блокувати зловмисну активність для запобігання подальшим негативним наслідкам.

Попередження про вторгнення є однією з основних функцій СЗВ, що дозволяє оперативно реагувати на потенційні загрози та запобігати їхньому розвитку. Ця функція передбачає сповіщення адміністраторів або відповідальних осіб про виявлення підозрілої або аномальної активності у мережі чи на системі. Попередження про вторгнення можуть бути реалізовані у вигляді повідомлень, які надсилаються на електронну пошту, системні журнали або спеціальні панелі керування. Вони можуть містити інформацію про характер атаки, час виявлення, відомості про джерело та ціль, що дозволяє адміністраторам швидко реагувати та приймати необхідні заходи захисту. Ефективність попереджень про вторгнення залежить від точності та достовірності виявлення загроз. Точність визначається здатністю системи відрізняти справжні загрози від помилкових сигналів. Достовірність включає в себе інформацію про об'єктивність та достатність даних для прийняття рішення щодо подальших дій захисту. Однак важливо також уникати надмірної кількості попереджень, оскільки це може призвести до "втоми" адміністраторів та ігнорування реальних загроз. Тому системи попереджень про вторгнення повинні бути налаштовані з урахуванням конкретних потреб та характеристик мережі чи системи, а також постійно піддаватися оновленню та вдосконаленню.

Блокування вторгнень є іншою ключовою функцією в СЗВ, спрямованою на зупинення або обмеження небажаної або шкідливої активності, виявленої системою. Ця функція має на меті негайно реагувати та вживати заходів для запобігання подальшим наслідкам атаки або вторгнення. Для забезпечення ефективного блокування вторгнень використовуються різноманітні методи та

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

стратегії. Один із найпоширеніших підходів - це автоматичне блокування, коли система автоматично вживає заходів щодо ізоляції або відмови в обслуговуванні зловмисного джерела або загрози. Це може включати в себе блокування IP-адрес, відключення користувачів або ізоляцію компрометованих систем. [10] Інший підхід - це застосування правил та політик безпеки для блокування конкретних видів трафіку або активності, що може вказувати на атаку. Наприклад, блокування певних портів, протоколів або аплікацій може допомогти зменшити ризик атак і забезпечити додатковий рівень безпеки. Крім того, важливо враховувати можливість ручного втручання та аналізу з боку адміністратора. Ручне блокування може бути необхідним для вирішення складних випадків або атак, які можуть уникнути автоматичного блокування.

Системи запобігання вторгненням мають кілька переваг, серед яких зниження ризику кібератак є однією з найважливіших. Шляхом постійного моніторингу мережевого трафіку та виявлення аномалій чи незвичайних патернів, ці системи можуть ефективно виявляти потенційні загрози та вторгнення ще до того, як вони спричинять значні збитки або витрати. Ще однією перевагою є автоматизація захисту. Багато систем запобігання вторгненням можуть автоматично реагувати на виявлені загрози, виконуючи задані дії для нейтралізації атаки або блокування потенційно шкідливого трафіку. Це дозволяє забезпечити швидку реакцію на загрози та мінімізувати час, протягом якого система перебуває у вразливому стані. Іншою перевагою є підвищення ефективності та продуктивності персоналу з безпеки. Завдяки автоматизації та інтелектуальним алгоритмам аналізу, персонал з може зосередитися на більш складних та стратегічних аспектах захисту мережі, в той час як більш стандартні завдання можуть бути автоматизовані та виконані системою запобігання вторгненням.

Одним з основних недоліків систем запобігання вторгненням є можливість помилок та хибних спрацювань. Жодна система не є ідеальною, і іноді системи запобігання вторгненням можуть реагувати на нормальну поведінку як на потенційну загрозу або навпаки, пропускаючи шкідливий

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

трафік через захист. Ще одним недоліком є складність налаштування та адміністрування. Деякі системи запобігання вторгненням можуть вимагати від користувачів глибоких знань та експертизи з мережевої безпеки для ефективного налаштування та використання. Це може стати перешкодою для менших організацій або тих, хто не має достатньої кількості кваліфікованого персоналу. Додатковим недоліком може бути обмежена здатність системи запобігання вторгненням виявляти нові та невідомі загрози. Багато систем ґрунтуються на сигнатурах атак, які вони розпізнають, а отже, вони можуть пропускати нові атаки, які ще не були включені до їх баз даних сигнатур.

У підсумку, системи запобігання вторгненням мають свої переваги та недоліки. Їхні переваги, такі як зниження ризику кібератак, автоматизація захисту та підвищення ефективності персоналу з безпеки, роблять їх важливими складовими кібербезпекової стратегії для багатьох організацій, але також необхідно і враховувати їх недоліки, такі як можливі помилки та хибні спрацювання, які можуть призвести до неправильної реакції на нормальний трафік чи навпаки, пропуску шкідливих атак.

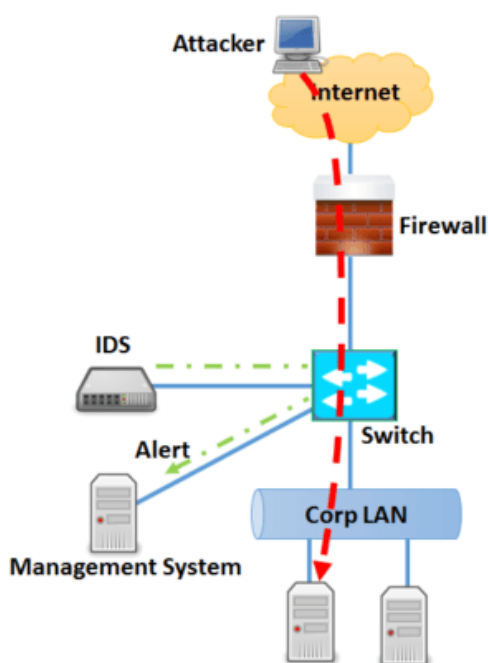
1.3. Порівняльний аналіз систем виявлення та запобігання вторгнень.

Порівняння систем запобігання вторгненням та систем виявлення вторгнень є важливим аспектом розуміння їх ролі та функцій у забезпеченні кібербезпеки. Основна відмінність між СЗВ та СВВ полягає у характері їх реакції на виявлені загрози. Системи виявлення вторгнень призначені для моніторингу мережевого трафіку та подій у системі з метою виявлення підозрілих дій або відомих шаблонів атак. Вони генерують сповіщення для адміністраторів безпеки, які потім приймають рішення про подальші дії. [4] СВВ є пасивними системами, оскільки вони лише інформують про можливі атаки, але не вживають активних заходів для їхнього запобігання. СЗВ, на відміну від СВВ, є активними компонентами захисту мережі. Вони не тільки виявляють загрози, але й автоматично реагують на них в реальному часі. СЗВ аналізують мережевий трафік і при виявленні підозрілої активності блокують її до того, як вона зможе завдати шкоди. Ця функціональність дозволяє СЗВ

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

ефективніше захищати мережі від атак, мінімізуючи час реакції на загрози та зменшуючи ризики для інформаційних систем. Ще одна важлива відмінність між СВВ та СЗВ полягає в їхньому впливі на продуктивність мережі. Оскільки СВВ працюють пасивно, вони мають мінімальний вплив на пропускну здатність мережі та її продуктивність. Водночас, СЗВ, працюючи в режимі онлайн, можуть затримувати трафік для аналізу, що може впливати на швидкість передачі даних і викликати затримки. Це вимагає від СЗВ високої продуктивності та оптимізації для мінімізації впливу на мережу. [15]

Intrusion Detection System



Intrusion Prevention System

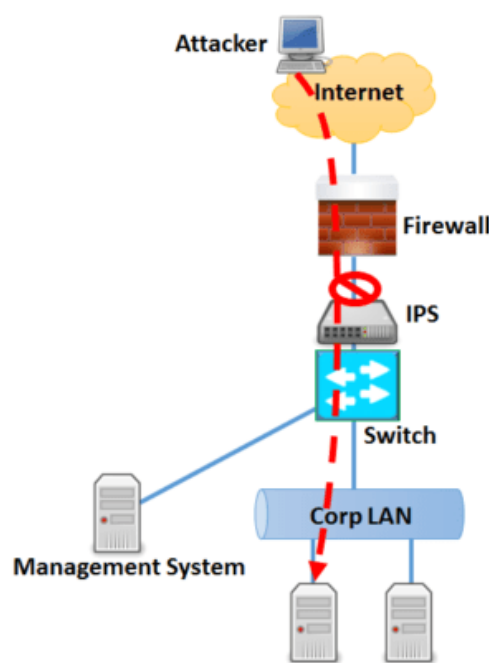


Рис. 1.2 Порівняння роботи СЗВ та СВВ

Таблиця 1.1

Порівняння СЗВ та СВВ

Критерій	Системи виявлення вторгнень	Системи запобігання вторгненням
Основна функція	Виявлення підозрілих дій та атак	Виявлення та активне блокування підозрілих дій та атак
Режим роботи	Пасивний (моніторинг та аналіз трафіку)	Активний (моніторинг, аналіз та блокування трафіку в реальному часі)

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

Таблиця 1.1 (Продовження)

Критерій	Системи виявлення вторгнень	Системи запобігання вторгненням
Розташування	Мережеве або хостове розташування	Інтеграція в мережеву інфраструктуру (між джерелом та ціллю трафіку)
Взаємодія з трафіком	Не впливає на потік трафіку, лише аналізує його	Може блокувати або перенаправляти підозрілий трафік
Сповіщення	Повідомляє адміністраторів про виявлені загрози	Блокує загрози автоматично та може повідомляти адміністраторів
Інтеграція з іншими системами	Часто інтегрується з системами управління подіями та інформацією безпеки	Може працювати автономно або з мінімальною інтеграцією з іншими системами
Основні завдання	Виявлення шаблонів атак, аналіз подій, сповіщення	Захист від атак у реальному часі, блокування мережесхем черв'яків, сканування портів
Використання ресурсів	Використовує ресурси системи для аналізу трафіку, але не впливає на продуктивність мережі	Може впливати на продуктивність мережі через активне блокування та фільтрацію

Незважаючи на ці відмінності, СВВ та СЗВ часто використовуються разом для забезпечення комплексного захисту. СВВ надають глибокий аналіз та історичні дані про атаки, тоді як СЗВ забезпечують миттєве реагування на загрози. Такий комбінований підхід дозволяє організаціям краще розуміти та контролювати свої мережі. [11]

1.4 Постановка технічного завдання.

На основі розглянутої вище інформації, виявлено нагальну потребу в розробці системи запобігання вторгненням для забезпечення безпеки мережної інфраструктури організації. Сучасні умови розвитку інформаційних технологій і зростання кількості кібератак вимагають надійного захисту інформаційних ресурсів. Це підкреслює актуальність розгортання систем виявлення та

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

запобігання вторгненням, що спрямовані на захист мережевої інфраструктури від потенційних загроз. Метою розгортання систем виявлення та запобігання вторгненням є забезпечення безпеки мережної інфраструктури організації. Для досягнення цієї мети необхідно виконати такі завдання:

- Провести аналіз існуючих систем запобігання вторгненням та їх характеристик.
- Вибрати оптимальну систему СЗВ для відповідної мережі.
- Розробити проєкт розгортання обраної системи СЗВ.
- Налаштувати та протестувати систему.

Виконання цих завдань сприятиме створенню ефективної системи захисту, яка забезпечить безперервність роботи компанії, захистить її інформаційні ресурси від несанкціонованого доступу та кібератак, а також підвищить загальний рівень безпеки мережі.

Висновки до першого розділу:

В цьому розділі було розглянуто теоретичні основи систем запобігання вторгненням. Проаналізовано історію виникнення та розвитку СЗВ, визначено їхнє значення у забезпеченні кібербезпеки сучасних мереж. Описано загальні принципи функціонування та основні компоненти систем запобігання вторгненням. Було проведено порівняння СЗВ із системами виявлення вторгнень, підкреслено їх відмінності у підходах до захисту, реакції на загрози та ефективності блокування атак.

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

РОЗДІЛ 2. АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ВИБІР МОДЕЛІ СИСТЕМИ

2.1. Система виявлення несанкціонованого доступу Cisco Secure IPS.

Cisco Secure IPS, що розроблена Cisco Systems розповсюджується на комерційній основі та доступна як в апаратному, так і в програмному вигляді. Система підтримує операційні системи Cisco IOS і Linux. [16]

Cisco Secure IPS є високоефективною системою запобігання вторгненням, розробленою компанією Cisco Systems, яка відома своїми надійними мережевими рішеннями. Cisco Secure IPS пропонує потужний захист мереж від різноманітних кіберзагроз, використовуючи передові технології аналізу та обробки трафіку. Ця система інтегрується як на апаратному, так і на програмному рівні, забезпечуючи високу гнучкість та адаптивність до різних потреб і масштабів мереж.

Основними функціями Cisco Secure IPS є моніторинг мережевого трафіку в реальному часі, виявлення та блокування відомих і невідомих атак, аналіз поведінкових аномалій, а також забезпечення відповідності політикам безпеки. Система використовує передові алгоритми машинного навчання для ідентифікації загроз та мінімізації хибних спрацьовувань. Завдяки інтеграції з іншими продуктами Cisco, такими як Cisco Firepower та Cisco Talos, IPS може використовувати оновлювані бази даних загроз і рекомендації щодо захисту від новітніх векторів атак.

Cisco Secure IPS підтримує Cisco IOS і Linux, що дозволяє ефективно впроваджувати цю систему в різноманітні мережеві середовища. Однією з головних переваг цієї системи є її здатність працювати на високих швидкостях передачі даних, що робить її ідеальною для великих корпоративних мереж і центрів обробки даних. Крім того, Cisco Secure IPS забезпечує можливість централізованого управління та моніторингу, що спрощує адміністрування та підвищує ефективність реагування на інциденти.

Завдяки своїм широким можливостям і високій надійності, Cisco Secure IPS є популярним вибором серед організацій, що прагнуть забезпечити

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

надійний захист своїх інформаційних систем від сучасних кіберзагроз. Її інтеграція з іншими засобами безпеки Cisco дозволяє створювати комплексні рішення, що забезпечують всебічний захист мережевої інфраструктури.

2.2. Система мережевого захисту McAfee Intrusion Prevention System.

Розробником системи McAfee Intrusion Prevention System є McAfee, Inc.. Вона розповсюджується на комерційній основі та доступна як в апаратному, так і в програмному вигляді. Система підтримує операційні системи Windows і Linux. [17]

McAfee Intrusion Prevention System є одним з провідних рішень у сфері захисту мереж, розробленим компанією McAfee, відомою своїми інноваційними підходами до кібербезпеки. McAfee IPS пропонує комплексний захист від різноманітних загроз, включаючи відомі й невідомі атаки, зловмисне програмне забезпечення та інші види шкідливої активності. Ця система забезпечує захист мереж на рівні корпоративних і урядових установ завдяки високій продуктивності та широкому спектру функціональних можливостей.

Основною метою McAfee IPS є виявлення та запобігання вторгненням в реальному часі. Система аналізує мережевий трафік, використовуючи передові методи глибокого аналізу пакетів та евристичні алгоритми для виявлення аномалій. McAfee IPS інтегрується з глобальною базою даних загроз McAfee Global Threat Intelligence, що дозволяє оперативно отримувати оновлення про новітні загрози та вразливості. Це забезпечує постійний захист мережі від нових і розвиваючихся атак.

McAfee IPS підтримує як апаратні, так і програмні платформи, що дозволяє адаптувати рішення під різні потреби організацій. Система може бути розгорнута на серверах під управлінням операційних систем Windows та Linux, що забезпечує гнучкість і сумісність з різноманітними інфраструктурами. Крім того, McAfee IPS має функції централізованого управління і моніторингу, що спрощує адміністрування системи та дозволяє швидко реагувати на інциденти безпеки.

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Однією з ключових особливостей McAfee IPS є її інтеграція з іншими продуктами McAfee, такими як McAfee ePolicy Orchestrator та McAfee Endpoint Security. Це дозволяє створювати комплексні рішення для забезпечення всебічного захисту інформаційних систем, що включають як мережеві, так і кінцеві точки. Завдяки використанню єдиної платформи управління, організації можуть централізовано контролювати всі аспекти безпеки, що підвищує ефективність захисту та знижує витрати на адміністрування.

McAfee Intrusion Prevention System є потужним інструментом для захисту мережевих інфраструктур від сучасних кіберзагроз. Її висока продуктивність, гнучкість у розгортанні та інтеграція з іншими засобами безпеки роблять її відмінним вибором для організацій, що прагнуть забезпечити надійний та комплексний захист своїх інформаційних активів.

2.3. Система виявлення та запобігання вторгненням Snort.

Sourcefire, Inc. (нині Cisco) є розробником системи Snort. Вона розповсюджується під відкритою ліцензією GPL, а також має комерційну версію Snort++. Snort є програмною платформою і підтримує операційні системи Linux, Windows, та Unix. [18]

Snort є однією з найбільш відомих та поширених систем виявлення та запобігання вторгненням, яка була розроблена компанією Sourcefire, Inc., що згодом стала частиною Cisco Systems. Snort є відкритим програмним забезпеченням, що дозволяє його вільно використовувати, модифікувати та розповсюджувати. Ця система забезпечує ефективний захист мереж завдяки потужним можливостям аналізу трафіку та виявлення загроз, які можуть бути адаптовані до конкретних потреб організації.

Snort працює на основі правил, які визначають шаблони мережевого трафіку, що можуть вказувати на атаки або інші підозрілі дії. Ці правила можуть бути створені вручну або завантажені з оновлюваних баз даних загроз. Snort підтримує як сигнатурний, так і аномалійний аналіз, що дозволяє виявляти як відомі, так і нові види загроз. Система може функціонувати у трьох основних режимах: sniffer (аналізатор трафіку), packet logger (записувач трафіку) та

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

network intrusion detection/prevention system (мережева система виявлення/запобігання вторгненням).

Snort підтримує різноманітні операційні системи, включаючи Linux, Windows та Unix, що робить його універсальним рішенням для різних мережових середовищ. Його гнучкість та можливість налаштування дозволяють використовувати Snort як у невеликих мережах, так і в великих корпоративних інфраструктурах. Крім того, існують комерційні версії Snort, такі як Snort++, які надають додаткові функції та підвищену продуктивність.

Snort також має можливість інтеграції з іншими засобами безпеки та управління мережею. Це дозволяє створювати комплексні рішення для забезпечення багаторівневого захисту інформаційних систем. Snort можна використовувати разом із системами управління подіями та інформацією безпеки, що надає можливість централізованого моніторингу та аналізу безпекових подій.

Завдяки своїй відкритій ліцензії, широким можливостям налаштування та високій ефективності, Snort є популярним вибором серед організацій, що прагнуть забезпечити надійний захист своїх мереж. Його здатність виявляти та запобігати вторгненням робить його важливим інструментом у боротьбі з кіберзагрозами, а постійна підтримка та розвиток спільнотою забезпечують актуальність та відповідність сучасним викликам у сфері кібербезпеки.

2.4. Система виявлення та запобігання вторгненням Suricata.

Систему виявлення та запобігання вторгненням Suricata було розроблено компанією Open Information Security Foundation (OISF), вона розповсюджується під відкритою ліцензією GPL. Suricata є програмною платформою, що підтримує різні операційні системи, включаючи Linux, Windows, Unix, та MacOS. [19]

Suricata є сучасною системою виявлення та запобігання вторгненням, розробленою Open Information Security Foundation, яка надає відкритий код для вільного використання та модифікації. Suricata відома своєю високою продуктивністю, масштабованістю та гнучкістю, що робить її ідеальним

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

рішенням для захисту мереж різного масштабу. Завдяки своїй архітектурі та передовим технологіям, Suricata забезпечує потужний захист від різноманітних кіберзагроз.

Основною перевагою Suricata є її здатність працювати у декількох режимах: як система виявлення вторгнень, система запобігання вторгненням та система моніторингу мережі. Suricata підтримує глибокий аналіз пакетів, який дозволяє детально аналізувати мережевий трафік на різних рівнях протоколів. Крім того, Suricata використовує багатопоточну архітектуру, що дозволяє ефективно використовувати ресурси сучасних багатоядерних процесорів та забезпечувати високу продуктивність навіть при великому обсязі трафіку.

Suricata підтримує різноманітні операційні системи, включаючи Linux, Windows, Unix та MacOS, що робить її доступною для широкого спектру користувачів. Її гнучкість і можливість налаштування дозволяють адаптувати систему до конкретних потреб організацій, забезпечуючи надійний захист мережі. Крім того, Suricata має вбудовану підтримку для аналізу протоколів високого рівня, таких як HTTP, TLS, FTP, SMB, і DNS, що дозволяє виявляти складні атаки на прикладному рівні.

Однією з ключових особливостей Suricata є її здатність використовувати правила Snort для виявлення загроз, що забезпечує сумісність з існуючими базами даних загроз і полегшує перехід від Snort до Suricata. Крім того, Suricata підтримує інтеграцію з іншими інструментами кібербезпеки та системами управління подіями та інформацією безпеки, що дозволяє створювати комплексні рішення для забезпечення багаторівневого захисту інформаційних систем.

Завдяки своїй відкритій ліцензії, високій продуктивності та гнучкості, Suricata є привабливим вибором для організацій, що прагнуть забезпечити надійний захист своїх мереж. Її здатність ефективно виявляти та запобігати різноманітним загрозам робить її важливим інструментом у боротьбі з кіберзагрозами. Постійна підтримка та розвиток з боку спільноти забезпечують актуальність та відповідність Suricata сучасним викликам у сфері кібербезпеки.

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

2.5. Хост-орієнтована система запобігання вторгненням OSSEC.

Система OSSEC первинно було розроблена Деніелем Сідом, а нині підтримкою займається компанія Trend Micro. OSSEC поширюється під відкритою ліцензією GPL і є програмною платформою, що підтримує різні операційні системи, такі як Linux, Windows, MacOS та Unix. [20]

OSSEC (Open Source HIDS SECurity) є відомою системою виявлення вторгнень, яка забезпечує моніторинг безпеки на хостах і є відкритим програмним забезпеченням. Спочатку розроблена Деніелем Сідом, система згодом була придбана компанією Trend Micro, що забезпечує її підтримку та розвиток. OSSEC пропонує потужні можливості для моніторингу системних подій, аналізу журналів, виявлення руткітів та реагування на загрози, що робить її важливим інструментом для забезпечення безпеки серверів і робочих станцій.

OSSEC є хостовою системою виявлення вторгнень, яка фокусується на аналізі подій, що відбуваються на окремих хостах, на відміну від мережевих систем виявлення вторгнень. Основними функціями OSSEC є аналіз лог-файлів, моніторинг цілісності файлів, виявлення руткітів, контроль політик безпеки та активне реагування на інциденти. Система здатна виявляти аномалії та підозрілі дії, що можуть вказувати на компрометацію системи або спробу атаки.

OSSEC підтримує різноманітні операційні системи, включаючи Linux, Windows, MacOS та Unix, що забезпечує гнучкість у використанні і дозволяє захищати широкий спектр хостів. Система складається з агентів, що встановлюються на хостах, та центрального сервера, який збирає та аналізує дані з агентів. Такий підхід забезпечує централізоване управління та моніторинг безпеки в реальному часі, що спрощує адміністрування і підвищує ефективність реагування на загрози.

Однією з головних переваг OSSEC є її здатність інтегруватися з іншими засобами безпеки, такими як SIEM-системи та мережеві системи виявлення вторгнень. Це дозволяє створювати комплексні рішення для забезпечення багаторівневого захисту інформаційних систем. OSSEC може бути налаштована для автоматичного виконання дій у відповідь на виявлені загрози, таких як

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

блокування IP-адрес або відправка сповіщень адміністраторам, що підвищує оперативність реагування на інциденти.

OSSEC є популярним вибором серед організацій, які прагнуть забезпечити надійний захист своїх хостів. Її відкритий код, широкі можливості налаштування та інтеграція з іншими інструментами безпеки роблять її ефективним і гнучким рішенням для виявлення та запобігання загрозам. Постійна підтримка та розвиток з боку спільноти забезпечують актуальність та відповідність OSSEC сучасним викликам у сфері кібербезпеки.

2.6. Апаратно-програмний комплекс StoneGate Intrusion Prevention System.

Система StoneGate Intrusion Prevention System первинно розроблена компанією Stonesoft, нині підтримується Forcepoint. Вона поширюється під комерційною ліцензією і може працювати як на апаратних, так і на програмних платформах. Підтримуваною операційною системою є Linux. [21]

StoneGate Intrusion Prevention System є потужною системою запобігання вторгненням, розробленою компанією Stonesoft, яка згодом стала частиною Forcepoint. StoneGate IPS пропонує високий рівень захисту мереж від різноманітних кіберзагроз, забезпечуючи ефективний моніторинг, аналіз і блокування підозрілої активності в реальному часі. Ця система підходить для великих корпоративних мереж і критично важливих інфраструктур, де необхідний надійний та масштабований захист.

Основною особливістю StoneGate IPS є її здатність забезпечувати комплексний захист мережі за допомогою глибокого аналізу пакетів та використання сучасних алгоритмів машинного навчання для виявлення аномалій та нових загроз. Система підтримує як сигнатурний, так і евристичний аналіз, що дозволяє ідентифікувати відомі та невідомі атаки. StoneGate IPS також інтегрується з глобальними базами даних загроз, що забезпечує оперативне оновлення сигнатур та захист від новітніх векторів атак.

StoneGate IPS підтримує розгортання на апаратних пристроях та програмних платформах, що працюють під управлінням операційної системи Linux. Це забезпечує гнучкість у виборі способу впровадження системи та

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

адаптацію до різних мережевих інфраструктур. Завдяки своїй модульній архітектурі, StoneGate IPS може масштабуватись відповідно до потреб організації, забезпечуючи високий рівень продуктивності навіть у великих мережах з інтенсивним трафіком.

Система забезпечує централізоване управління та моніторинг за допомогою інтегрованого інтерфейсу, що спрощує адміністрування та дозволяє швидко реагувати на інциденти безпеки. StoneGate IPS також підтримує функції автоматичного реагування на загрози, що дозволяє блокувати шкідливий трафік або виконувати інші дії у відповідь на виявлені загрози без втручання адміністратора.

Однією з ключових переваг StoneGate IPS є її здатність інтегруватися з іншими продуктами Forcepoint, такими як системи управління інформаційною безпекою та рішення для захисту кінцевих точок. Це дозволяє створювати комплексні рішення для всебічного захисту інформаційних систем, забезпечуючи багаторівневий підхід до кібербезпеки.

Завдяки своїй високій ефективності, масштабованості та гнучкості, StoneGate Intrusion Prevention System є надійним вибором для організацій, які прагнуть забезпечити надійний захист своїх мережевих інфраструктур. Її можливість виявляти та блокувати різноманітні загрози, інтеграція з іншими засобами безпеки та підтримка централізованого управління роблять її важливим інструментом у забезпеченні кібербезпеки сучасних організацій.

2.7. Вибір моделі системи виявлення та запобігання вторгненням.

Під час вибору системи запобігання вторгненням для виконання поставленої задачі було враховано кілька ключових факторів, зокрема розмір мережі, вимоги до продуктивності, вартість розгортання та можливість майбутнього розширення. Після детального аналізу існуючих рішень, було прийнято рішення використовувати Snort у поєднанні з платформою pfSense. Snort був обраний через його відкрите ліцензування та широкі можливості налаштування, що забезпечує гнучкість та економічну ефективність, особливо для невеликих мереж. Snort є потужною системою виявлення та запобігання

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

вторгненням, яка забезпечує надійний захист завдяки аналізу мережевого трафіку на основі правил. Його здатність виявляти як відомі, так і нові загрози робить його привабливим вибором для захисту інформаційних систем від різноманітних кіберзагроз. pfSense, у свою чергу, є надійною платформою для побудови мережесх рішень з відкритим кодом, яка забезпечує високу продуктивність та гнучкість у налаштуванні. [22] Інтеграція Snort з pfSense дозволяє легко налаштувати та управляти системою запобігання вторгненням без значних витрат на апаратне забезпечення та ліцензії. Це рішення є особливо ефективним для невеликих мереж, де важливо забезпечити високий рівень безпеки за мінімальних витрат.

Крім того, однією з вагомих причин вибору Snort є його сумісність з Suricata. Це означає, що у разі розширення мережі та збільшення вимог до продуктивності і функціональності системи запобігання вторгненням, можна буде легко перейти на Suricata без значних змін у існуючій інфраструктурі. Suricata підтримує ті ж правила та конфігурації, що й Snort, що забезпечує безперебійний перехід та мінімізує витрати на міграцію. [18-19]

Висновки до другого розділу:

У цьому розділі роботи було проведено огляд існуючих рішень для запобігання вторгненням, зокрема Cisco Secure IPS, McAfee Intrusion Prevention System, Snort, Suricata, OSSEC та StoneGate Intrusion Prevention System. Описано особливості кожної системи, їхні переваги та недоліки, а також специфіку використання в різних мережесх середовищах. На основі проведеного аналізу було здійснено вибір оптимальної системи для реалізації проєкту. Враховуючи потреби та розмір мережі, було обрано Snort у поєднанні з pfSense як найкраще рішення для ефективного захисту мережесх інфраструктури від кібератак.

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ

3.1. Аналіз топології мережі.

Підготовка починається з проведення детального аналізу існуючої мережевої інфраструктури. Це включає оцінку поточних мережевих налаштувань, пропускної здатності, топології мережі та ідентифікацію критично важливих вузлів і сегментів, які потребують особливого захисту. Важливо визначити, які види трафіку є найбільш вразливими до атак, а також які ресурси є найбільш цінними для організації. Цей аналіз допоможе сформулювати вимоги до системи запобігання вторгненням і визначити оптимальні точки її розміщення в мережі.

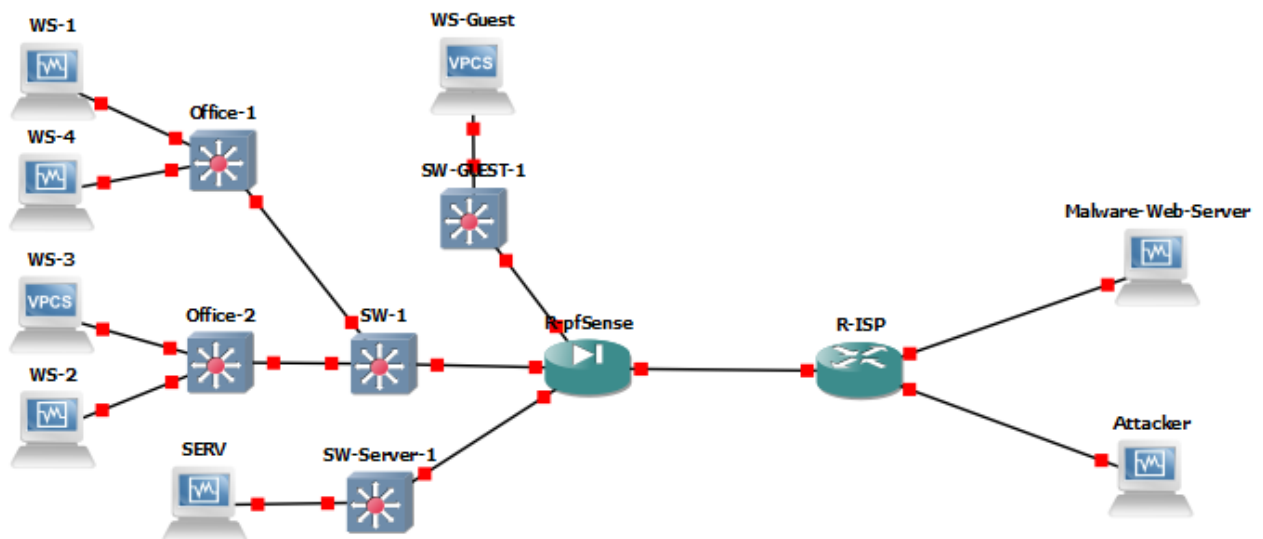


Рис. 3.1 Топологія мережі

Як видно з рис 3.1 маршрутизатор pfSense було встановлено між маршрутизатором інтернет провайдеру та мережею організації. Це розміщення дозволяє контролювати весь вхідний та вихідний трафік, забезпечуючи ефективний захист мережі від зовнішніх загроз. Наступним кроком планування було проаналізовано таблицю адресації даної мережі для кращого її розуміння. Це дозволило ідентифікувати всі активні пристрої, їх IP-адреси та відповідні підмережі, що сприяло точнішому налаштуванню фільтрів та правил безпеки.

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Це дозволить забезпечити ефективний моніторинг та управління мережевим трафіком, зокрема виявлення та блокування потенційних загроз.

Таблиця 3.1

Параметри IP-адресації мережі

Мережа / Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Пр ефі кс
Мережа VLAN A	-	215.10.1.0	255.255.255.0	/24
Робоча станція WS-1	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			
Робоча станція WS-4	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			
Маршрутизатор pfSense	em4.1011	215.10.1.1	255.255.255.0	/24
Мережа VLAN B	-	216.10.1.0	255.255.255.0	/24
Робоча станція WS-2	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			
Робоча станція WS-3	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			
Маршрутизатор pfSense	em4.1021	215.10.1.1	255.255.255.0	/24
Мережа GUEST	-	217.10.1.0	255.255.255.0	/24
Робоча станція WS-5	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			
Маршрутизатор pfSense	em5	215.10.1.1	255.255.255.0	/24
Мережа INTERNAL SERVERS	-	211.10.1.0	255.255.255.0	/24
Сервер SERV-1	Мережний адаптер	211.10.1.5	255.255.255.0	/24
	Шлюз за замовчуванням	211.10.1.1	255.255.255.0	/24
Маршрутизатор pfSense	em2	211.10.1.1	255.255.255.0	/24
Мережа R-ISP - Attacker	-	222.11.1.0	255.255.255.0	/24
Маршрутизатор R-ISP	Gig2/0	222.11.1.1	255.255.255.0	/24

Таблиця 3.1 (Продовження)

Мережа / Пристрій	Інтерфейс/Мережний адаптер/Шлюз	ІР-адреса	Маска	Пр ефі кс
Робоча станція Attacker	Мережний адаптер	222.11.1.101	255.255.255.0	/24
	Шлюз за замовчуванням	223.11.1.1	255.255.255.0	/24
Мережа R-ISP – Malware- Web-Server	-	223.11.1.0	255.255.255.0	/24
Маршрутизатор R-ISP	Gig3/0	223.11.1.1	255.255.255.0	/24
Сервер Malware-Web- Server	Мережний адаптер	223.11.1.226	255.255.255.0	/24
	Шлюз за замовчуванням	223.11.1.1	255.255.255.0	/24
Мережа R-ISP - OPNsense	-	221.11.1.0	255.255.255.0	/24
Маршрутизатор R-ISP	Gig1/0	221.11.1.101	255.255.255.0	/24
Маршрутизатор OPNsense	em3	221.11.1.111	255.255.255.0	/24

3.2. Вибір обладнання.

Виконавши підготовчі дії з аналізу мережевого середовища, наступним кроком стало визначення необхідного обладнання для розгортання системи запобігання вторгненням. Враховуючи невеликий розмір мережі та потребу в гнучкому і економічному рішенні, було вирішено використовувати маршрутизатор NETGATE 2100 із встановленою туди pfSense у поєднанні з Snort. Це поєднання забезпечує надійний захист і високу продуктивність за мінімальних витрат.

Маршрутизатор NETGATE 2100 був обраний через його відповідність вимогам невеликої мережі, високий рівень продуктивності та підтримку відкритої платформи pfSense. [22-23] NETGATE 2100 надає всі необхідні функції для ефективного управління мережею, включаючи міжмережвий екран, VPN та розширені можливості налаштування безпеки. Використання Snort як системи запобігання вторгненням дозволяє здійснювати глибокий аналіз трафіку і своєчасно виявляти та блокувати загрози.

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		34



Рис. 3.2 Маршрутизатор NETGATE 2100

Технічні характеристики NETGATE 2100 наведені у таблиці нижче:

Таблиця 3.2

Технічні характеристики NETGATE 2100 [23]

Характеристика	Значення
Процесор	1.2 GHz Dual Core ARM Cortex-A53
Оперативна пам'ять	4 GB DDR4
Внутрішнє зберігання даних	8 GB eMMC
Мережеві порти	4 x 1 Gbps Ethernet
Підтримувані VPN	IPsec, OpenVPN, WireGuard

Його технічні характеристики забезпечують достатню потужність для обробки трафіку в невеликій мережі, а також можливість масштабування у випадку зростання потреб.

3.3. Розгортання та налаштування мережевої інфраструктури.

Після вибору відповідного обладнання наступним етапом розгортання системи запобігання вторгненням є налаштування мережевого середовища для оптимальної роботи нових компонентів. Початкова конфігурація мережевих пристроїв включає налаштування основних мережевих параметрів, таких як IP-адреса, маршрути, DNS-сервери та інших параметрів, необхідних для забезпечення зв'язку між пристроями у мережі. Одним із ключових кроків є

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

налаштування мережевих інтерфейсів на маршрутизаторі, яке включає встановлення IP-адрес та маски підмережі, активацію DHCP для відповідних мереж, налаштування VLAN для сегментації мережі та встановлення правил фільтрації трафіку. Крім того, проводиться налаштування маршрутизації для забезпечення коректного пересилання пакетів між різними мережевими сегментами.

Interfaces / RISP (em3)

General Configuration

Enable ☒ Enable interface

Description: RISP
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU: 1500
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS: 1460
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address: 221.11.1.111 / 24

IPv4 Upstream gateway: None [+ Add a new gateway](#)
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Рис. 3.3 Налаштування інтерфейсу em3

Enable	☒ Enable interface
Description	LANSERV Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration	
IPv4 Address	211.10.1.1 / 24
IPv4 Upstream gateway	None + Add a new gateway

Рис. 3.4 Налаштування інтерфейсу em2

LAN	LANSERV	RISP	VLANA	VLANB
General DHCP Options				
DHCP Backend	Kea DHCP			
Enable	☒ Enable DHCP server on VLANB interface			
Deny Unknown Clients	Allow all clients When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.			
Ignore Client Identifiers	☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.			
Primary Address Pool				
Subnet	216.10.1.0/24			
Subnet Range	216.10.1.1 - 216.10.1.254			
Address Pool Range	216.10.1.10 From	216.10.1.254 To		
The specified range for this pool must not be within the range configured on any other address pool for this interface.				
Additional Pools	+ Add Address Pool If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.			
Server Options				
WINS Servers	WINS Server 1 WINS Server 2			
DNS Servers	216.10.1.1 DNS Server 2 DNS Server 3 DNS Server 4			
Other DHCP Options				
Gateway	216.10.1.1			

Рис. 3.5 Налаштування DHCP для VLAN-B

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Firewall / Rules / Edit

Edit Firewall Rule

Action Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface GUEST
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Any Source Address /

Destination

Destination ☐ Invert match VLANB subnets Destination Address /

Рис. 3.6 Налаштування правил фаєрволу для гостьової мережі

Firewall / Rules / Edit

Edit Firewall Rule

Action Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface GUEST
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Any Source Address /

Destination

Destination ☐ Invert match VLANA subnets Destination Address /

Рис. 3.7 Налаштування правил фаєрволу для гостьової мережі

Наступним кроком є налаштування системи запобігання вторгненням на базі Snort. Перш за все, необхідно встановити та активувати Snort на маршрутизаторі pfSense. Після цього проводиться конфігурація базових параметрів Snort, включаючи вибір інтерфейсів для моніторингу трафіку, встановлення правил для виявлення та блокування потенційно небезпечного

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

трафіку, а також налаштування частоти оновлення цих правил. Snort має можливість автоматичного оновлення правил із зовнішніх джерел, що дозволяє тримати систему в актуальному стані для виявлення нових загроз.

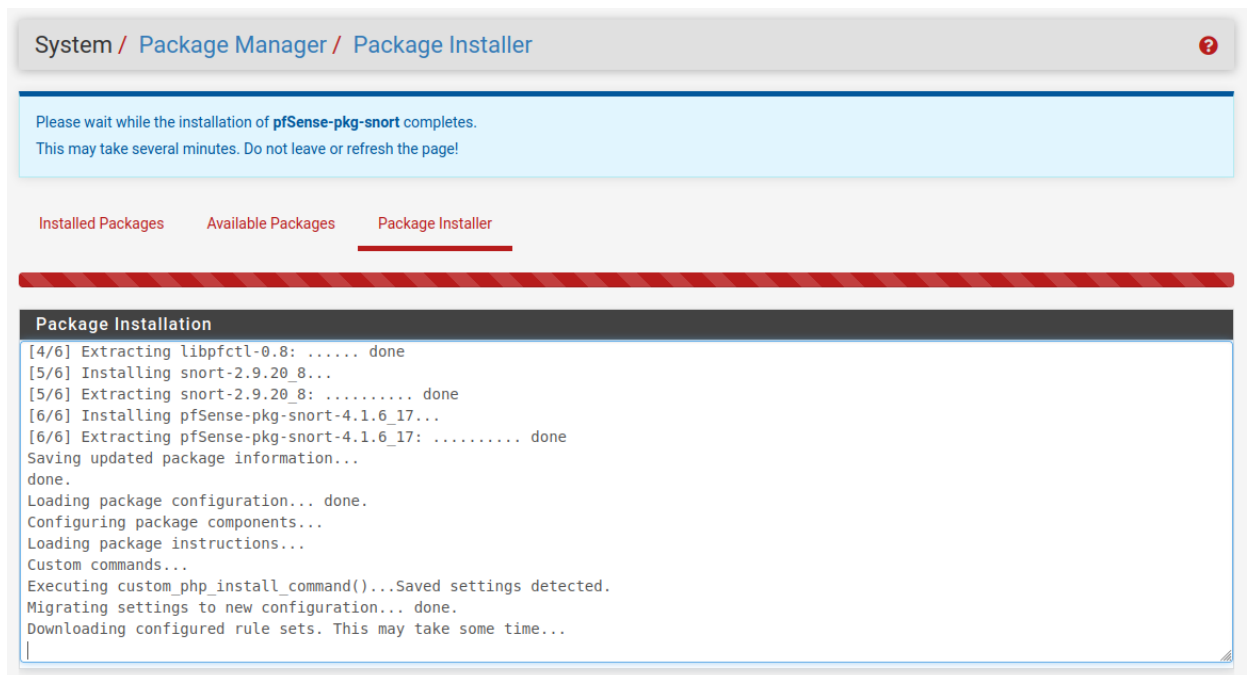


Рис. 3.8 Завантаження пакунку Snort

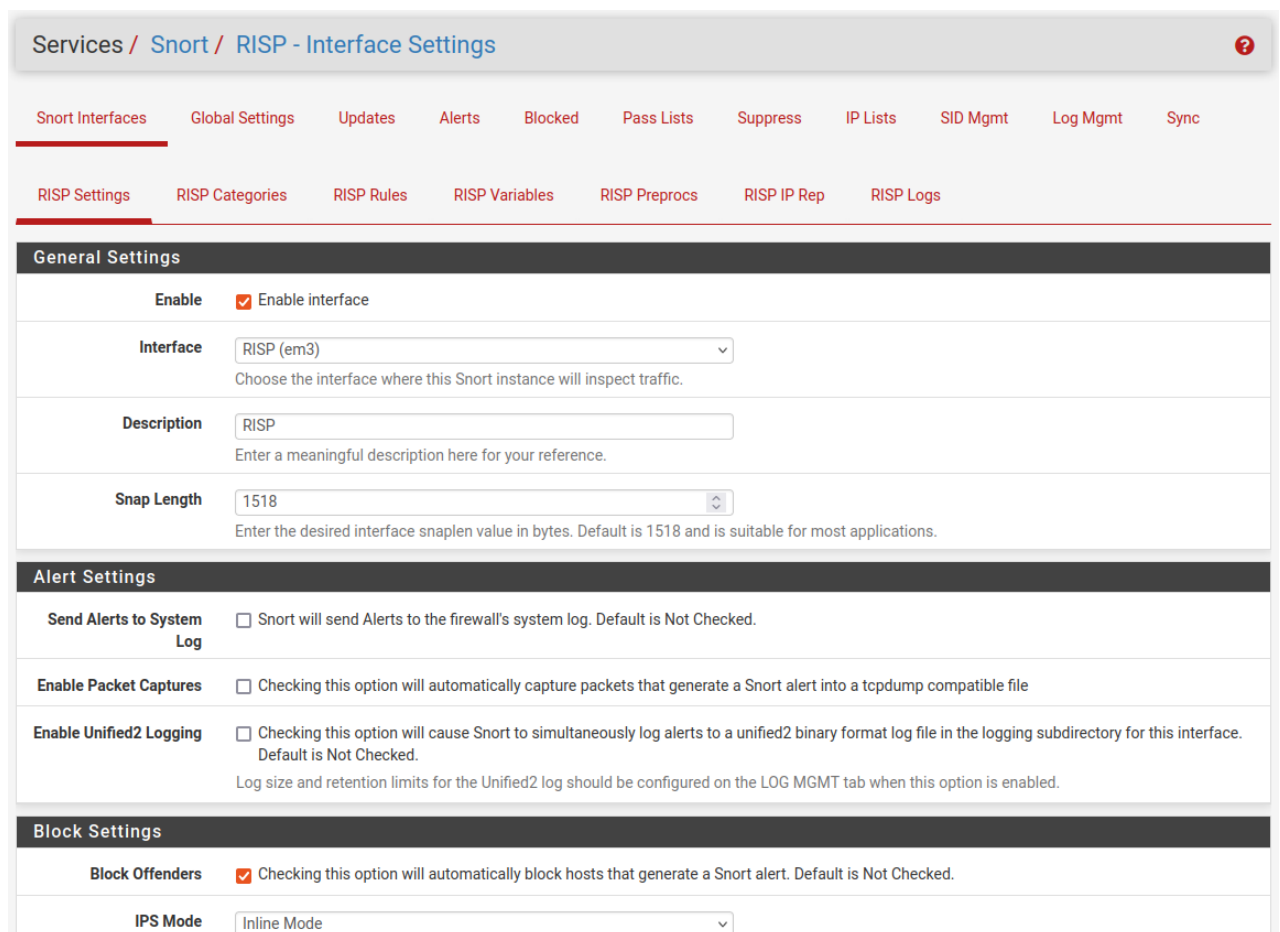


Рис. 3.9 Налаштування інтерфейсу для перевірки трафіку

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

LANSE Settings
LANSE Categories
LANSE Rules
LANSE Variables
LANSE Preprocs
LANSE IP Rep
LANSE Logs

General Settings

Enable
☒ Enable interface

Interface

LANSERV (em2)

Choose the interface where this Snort instance will inspect traffic.

Description

LANSERV

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log
☐ Snort will send Alerts to the firewall's system log. Default is Not Checked.

Enable Packet Captures
☐ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Enable Unified2 Logging
☐ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Block Settings

Block Offenders
☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Inline Mode

Рис. 3.10 Налаштування інтерфейсу для перевірки трафіку

Services / Snort / Interface Settings / RISP - Categories

Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync

RISP Settings
RISP Categories
RISP Rules
RISP Variables
RISP Preprocs
RISP IP Rep
RISP Logs

Automatic Flowbit Resolution

Resolve Flowbits
☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Auto-Flowbit Rules

View

Disabling auto-flowbit rules is strongly discouraged for security reasons. Auto-enabled flowbit rules that generate unwanted alerts should have their GID:SID added to the Suppression List for the interface instead of being disabled.

Snort Subscriber IPS Policy Selection

Use IPS Policy
☒ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection

Security

Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.
Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

Рис. 3.11 Налаштування категорій правил, що будуть використовуватись при перевірці трафіку

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Snort Subscriber Rules	
Enable Snort VRT	☒ Click to enable download of Snort free Registered User or paid Subscriber rules
Sign Up for a free Registered User Rules Account Sign Up for paid Snort Subscriber Rule Set (by Talos)	
Snort Oinkmaster Code	fac9d6f314bc076b9f51be18443f7f8f4d2f73f1 Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)
Snort GPLv2 Community Rules	
Enable Snort GPLv2	☒ Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.	
Emerging Threats (ET) Rules	
Enable ET Open	☒ Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.	
Enable ET Pro	☐ Click to enable download of Emerging Threats Pro rules
Sign Up for an ETPro Account ETPro for Snort offers daily updates and extensive coverage of current malware threats.	
Sourcefire OpenAppID Detectors	
Enable OpenAppID	☒ Click to enable download of Sourcefire OpenAppID Detectors
The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.	
OpenAppID Version	Installed Detection Package Version=366
Enable AppID Open Text Rules	☒ Click to enable download of the AppID Open Text Rules
Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is https://files.netgate.com/openappid/appid_rules.tar.gz .	
FEODO Tracker Botnet C2 IP Rules	
Enable FEODO Tracker Botnet C2 IP Rules	☒ Click to enable download of FEODO Tracker Botnet C2 IP rules
Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet.	
Rules Update Settings	
Update Interval	4 DAYS Please select the interval for rule updates. Choosing NEVER disables auto-updates.
Update Start Time	02:30 Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.
Hide Deprecated Rules Categories	☒ Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	☐ Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.
General Settings	
Remove Blocked Hosts Interval	15 MINS Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.
Remove Blocked Hosts After Deinstall	☒ Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	☒ Click to retain Snort settings after package removal.
Startup/Shutdown Logging	☐ Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

Рис. 3.12 Активація Snort та налаштування автоматичного оновлення правил

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

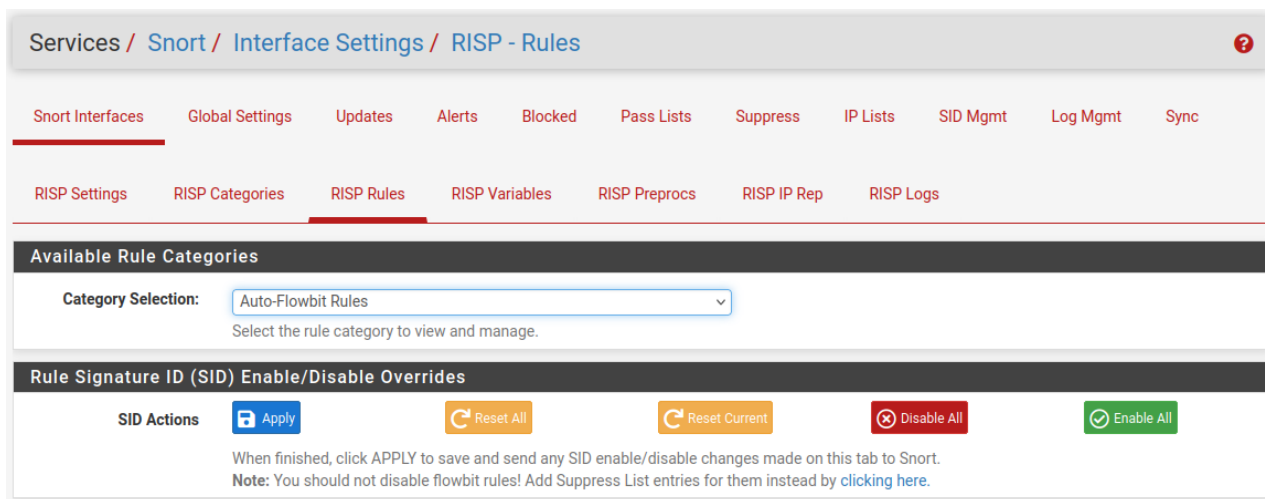


Рис. 3.13 Налаштування правил

3.4. Перевірка роботоспроможності системи виявлення та блокування вторгнень.

Виконавши налаштування системи запобігання вторгненням наступним кроком її розгортання буде тестування її роботи для перевірки ефективності та надійності впровадженого рішення. Під час тестування буде виконано перевірку роботи системи виявлення та блокування загроз. Для цього будуть використані різні атакуючі вектори, а також імітації типових загроз за допомогою спеціалізованих інструментів тестування безпеки мережі.

```
(kali@kali)-[~]
$ nmap 211.10.1.5 -sT -v -P0
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Warning: The -P0 option is deprecated. Please use -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2024-05-17 12:57 EDT
Initiating Parallel DNS resolution of 1 host. at 12:57
Completed Parallel DNS resolution of 1 host. at 12:57, 13.00s elapsed
Initiating Connect Scan at 12:57
Scanning 211.10.1.5 [1000 ports]
Discovered open port 80/tcp on 211.10.1.5
Completed Connect Scan at 12:57, 7.04s elapsed (1000 total ports)
Nmap scan report for 211.10.1.5
Host is up (0.027s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 20.08 seconds

(kali@kali)-[~]
$
```

Рис. 3.14 Спроба розвідки відкритих портів на сервері у мережі

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Alert Log View Settings

Interface to Inspect

RISP (em3)

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

6 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-05-17 16:57:28		2	TCP	Attempted Information Leak	223.11.1.226  	35528	211.10.1.5  	5815	1:2002910   	ET SCAN Potential VNC Scan 5800-5820
2024-05-17 16:57:27		2	TCP	Potentially Bad Traffic	223.11.1.226  	37630	211.10.1.5  	1433	1:2010935   	ET SCAN Suspicious inbound to MSSQL port 1433
2024-05-17 16:57:27		2	TCP	Attempted Information Leak	223.11.1.226  	44650	211.10.1.5  	5906	1:2002911   	ET SCAN Potential VNC Scan 5900-5920
2024-05-17 16:57:27		2	TCP	Potentially Bad Traffic	223.11.1.226  	44096	211.10.1.5  	5432	1:2010939   	ET SCAN Suspicious inbound to PostgreSQL port 5432
2024-05-17 16:57:27		2	TCP	Potentially Bad Traffic	223.11.1.226  	40052	211.10.1.5  	1521	1:2010936   	ET SCAN Suspicious inbound to Oracle SQL port 1521
2024-05-17 16:57:25		2	TCP	Potentially Bad Traffic	223.11.1.226  	38904	211.10.1.5  	3306	1:2010937   	ET SCAN Suspicious inbound to mySQL port 3306

Рис. 3.15 Повідомлення про підозрілу активність

 UserUser@student-VirtualBox: ~    

```
UserUser@student-VirtualBox:~$ wget 222.11.1.101/eicar.com
--2024-05-17 20:00:18-- http://222.11.1.101/eicar.com
Встановлення з'єднання з 222.11.1.101:80... з'єднано.
HTTP-запит надіслано, очікуємо на відповідь...
```

Рис. 3.17 Реакція системи на завантаження шкідливого файлу

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ		Арк
		Шелуха О.О.					43
Змн.	Арк.	№ докум.	Підпис	Дата			

```

root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# sqlmap -u http://211.10.1.5/index.php?page=login.php --data="username=asdf&password=asdf&login-php-submit-button=Login" --banner

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:21:27 /2024-06-10/

[15:21:27] [INFO] testing connection to the target URL
[15:21:28] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=3euv3bv79q6...3st3cqcj45;showhints=1'). Do you want to use those [Y/n]

[15:21:34] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:21:35] [INFO] testing if the target URL content is stable
[15:21:35] [INFO] target URL content is stable
[15:21:35] [INFO] testing if POST parameter 'username' is dynamic
[15:21:36] [WARNING] POST parameter 'username' does not appear to be dynamic
[15:21:36] [INFO] heuristic (basic) test shows that POST parameter 'username' might be injectable (possible DBMS: 'MySQL')
[15:21:37] [INFO] heuristic (XSS) test shows that POST parameter 'username' might be vulnerable to cross-site scripting (XSS) attacks
[15:21:37] [INFO] testing for SQL injection on POST parameter 'username'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]

```

Рис. 3.18 Спроба SQL-ін'єкції

33 Entries in Active Log											
Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description	
2024-06-10 19:29:35	⚠	1	TCP	Attempted User Privilege Gain	223.11.1.226	55068	211.10.1.5	80	1:2017337	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	⊕ × 🔗
2024-06-10 19:29:05	⚠	1	TCP	Attempted User Privilege Gain	223.11.1.226	35496	211.10.1.5	80	1:2017337	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	⊕ × 🔗
2024-06-10 19:22:39	⚠	2	TCP	Potentially Bad Traffic	211.10.1.5	80	223.11.1.226	57028	1:2016672	ET WEB_SERVER SQL Errors in HTTP 200 Response (error in your SQL syntax)	⊕ × 🔗
2024-06-10 19:22:39	⚠	2	TCP	Potentially Bad Traffic	211.10.1.5	80	223.11.1.226	57024	1:2016672	ET WEB_SERVER SQL Errors in HTTP 200 Response (error in your SQL syntax)	⊕ × 🔗
2024-06-10 19:22:39	⚠	2	TCP	Potentially Bad Traffic	211.10.1.5	80	223.11.1.226	57022	1:2016672	ET WEB_SERVER SQL Errors in HTTP 200 Response (error in your SQL syntax)	⊕ × 🔗
2024-06-10 19:22:39	⚠	2	TCP	Potentially Bad Traffic	211.10.1.5	80	223.11.1.226	57018	1:2016672	ET WEB_SERVER SQL Errors in HTTP 200 Response (error in your SQL syntax)	⊕ × 🔗
2024-06-10 19:22:39	⚠	2	TCP	Potentially Bad Traffic	211.10.1.5	80	223.11.1.226	57002	1:2016672	ET WEB_SERVER SQL Errors in HTTP 200 Response (error in your SQL syntax)	⊕ × 🔗
2024-06-10 19:22:38	⚠	2	TCP	Potentially Bad Traffic	211.10.1.5	80	223.11.1.226	56996	1:2016672	ET WEB_SERVER SQL Errors in HTTP 200 Response (error in your SQL syntax)	⊕ × 🔗

Рис. 3.19 Реакція СЗВ на SQL-ін'єкцію

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

```

[15:29:50] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[15:29:50] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[15:29:50] [INFO] automatically extending ranges for UNION query injection technique tests as
there is at least one other (potential) technique found
[15:30:20] [WARNING] there is a possibility that the target (or WAF/IPS) is dropping 'suspici
ous' requests
there seems to be a continuous problem with connection to the target. Are you sure that you w
ant to continue? [y/N]

```

Рис. 3.20 Повідомлення про проблеми під час SQL-ін'єкції

З приведених вище рисунків видно, що система успішно виявляє та блокує підозрілий трафік, захищаючи мережу від потенційних загроз. У процесі тестування було виявлено спробу SQL-ін'єкції та сканування портів, також система виявила спробу завантаження відомого їй шкідливого файлу та заблокувала цю спробу. Система запобігання вторгненням своєчасно реагувала на ці загрози, генеруючи відповідні сповіщення та блокуючи небезпечний трафік. Але не обійшлося і без проблем, система не змогла виявити та заблокувати/повідомити про спробу DoS атаки Synflood, тому було виконано ручне створення правила, яке б відслідковувало можливі атаки такого типу.

Рис. 3.21 Ручне створення правила

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Текст правила:

alert tcp any any -> \$HOME_NET any (threshold: type threshold, track by_dst, count 60, seconds 20; msg: "Possible TCP SYN Flood attack detected"; sid: 10000009; rev: 1;)

Alert Log View Settings

Interface to Inspect

RISP (em3)

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

184 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-06-10 21:53:31	⚠	0	TCP		4.53.7.143	42874	211.10.1.5	21	1:10000009	"Possible TCP SYN Flood attack detected"
2024-06-10 21:53:31	⚠	0	TCP		4.53.7.143	33847	211.10.1.5	21	1:10000009	"Possible TCP SYN Flood attack detected"
2024-06-10 21:53:31	⚠	0	TCP		4.53.7.143	3306	211.10.1.5	21	1:10000009	"Possible TCP SYN Flood attack detected"
2024-06-10 21:53:31	⚠	0	TCP		4.53.7.143	41267	211.10.1.5	21	1:10000009	"Possible TCP SYN Flood attack detected"
2024-06-10 21:53:31	⚠	0	TCP		4.53.7.143	27219	211.10.1.5	21	1:10000009	"Possible TCP SYN Flood attack detected"

Рис. 3.22 Реакція системи на повторну атаку

Також у системного адміністратора є можливість змінити реакцію на відповідне правило, зараз система лише створює сповіщення про підозрілу активність, якщо змінити дію яку буде виконувати система, то система буде блокувати запити. Це можна зробити за допомогою графічного інтерфейсу, або змінивши 'alert' на 'drop' на початку правила прописаного користувачем.

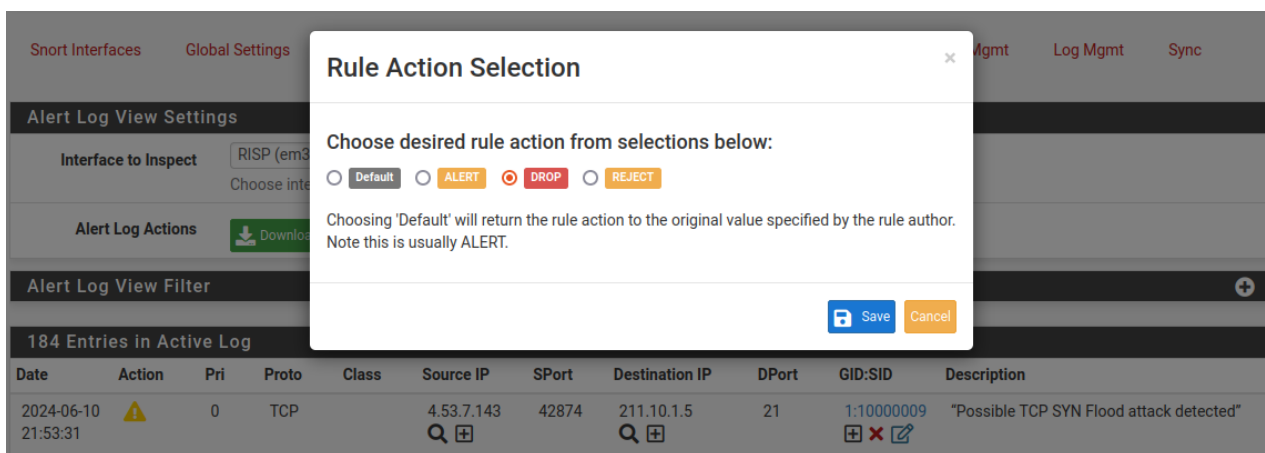


Рис. 3.23 Графічний інтерфейс для зміни дії при тригері правила

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

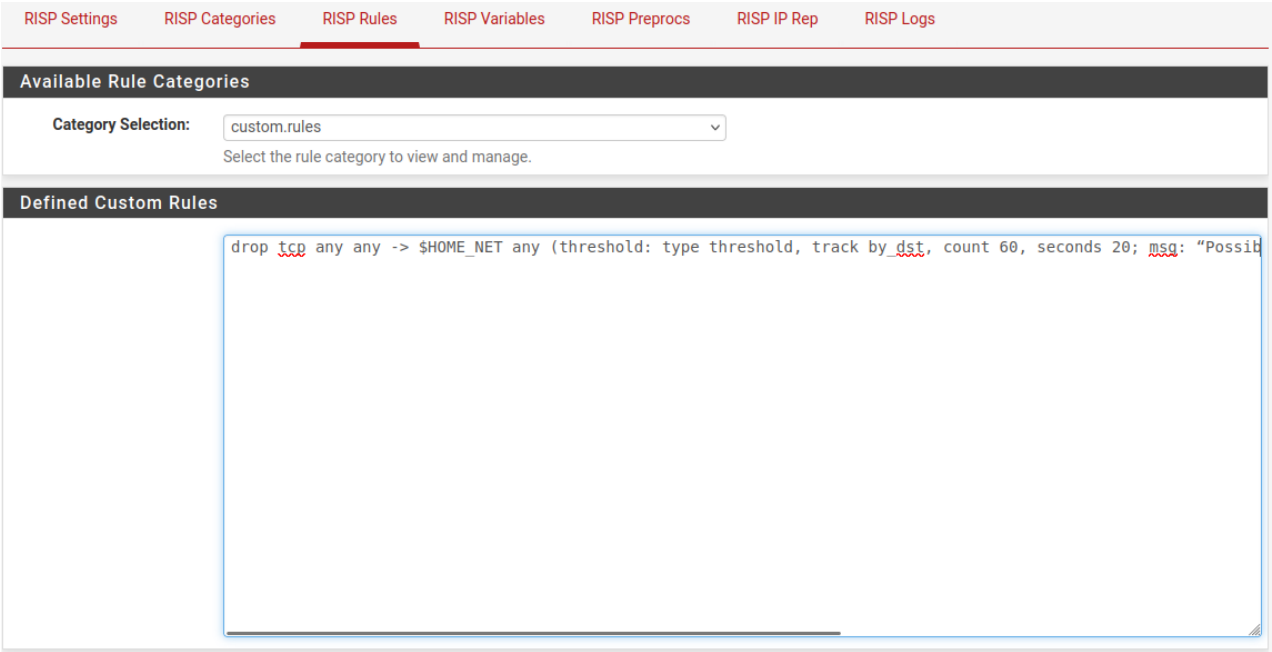


Рис. 3.24 Зміна правила прописаного користувачем

Текст правила після змін:

drop tcp any any -> \$HOME_NET any (threshold: type threshold, track by_dst, count 60, seconds 20; msg: "Possible TCP SYN Flood attack detected"; sid: 10000009; rev: 1;)

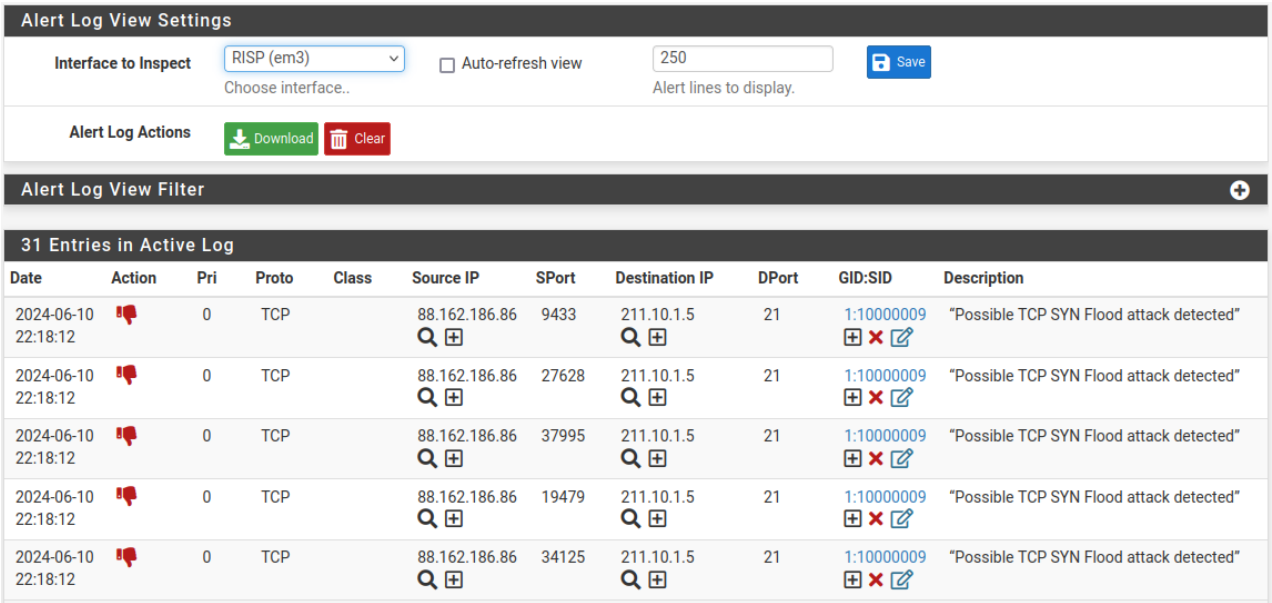


Рис. 3.25 Реакція системи на повторну атаку

Як видно з наведених рисунків, система успішно заблокувала запити, які було визначено у правилі. Таким чином, ручне створення правил та їх коригування дозволяє значно підвищити ефективність роботи системи

запобігання вторгненням, забезпечуючи надійний захист мережі від специфічних типів атак.

Виконані тести та їх результати підтверджують, що налаштування системи було виконано коректно, а обране обладнання та програмне забезпечення здатне забезпечити високий рівень безпеки мережі.

Висновки до третього розділу:

У цьому розділі роботи описується практичне розгортання системи запобігання вторгненням. Розгортання було розпочато з підготовки, яка включала детальний аналіз мережевого середовища та його структури. Далі проведено вибір обладнання, де враховано розмір мережі та обрано оптимальне рішення для розгортання Snort на платформі pfSense. Описано процес налаштування системи, зокрема конфігурацію мережевих параметрів та встановлення і налаштування Snort для ефективного моніторингу та блокування загроз. Завершальним етапом було тестування системи, яке підтвердило її здатність виявляти та блокувати різноманітні кібератаки, забезпечуючи стабільну та надійну роботу.

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

ВИСНОВКИ

У даній кваліфікаційній роботі було вирішено завдання з розгортання та дослідження процесу роботи системи виявлення та запобігання вторгненням для блокування атак на кібератак на мережну інфраструктуру компанії.

При виконанні роботи було проведено докладний аналіз різних систем запобігання вторгненням, включаючи Cisco Secure IPS, McAfee Intrusion Prevention System, Snort, Suricata, OSSEC та StoneGate Intrusion Prevention System. Для кожної системи вивчались їх переваги, недоліки та відповідність потребам невеликої мережі компанії. На основі аналізу було зроблено вибір оптимальної системи для застосування в мережі компанії з обґрунтуванням вибору на основі технічних та економічних критеріїв.

Дослідження показало, що система Snort у поєднанні з pfSense є найбільш підходящим рішенням для компанії з малою мережею. Вона забезпечує ефективний захист від різних типів кібератак, зокрема завдяки своїм відкритим характеристикам і можливостям налаштування. У результаті проведеного дослідження було розроблено та реалізовано проєкт мережі, включаючи в себе обрану систему Snort у поєднанні з pfSense. Цей проєкт враховує специфіку мережі компанії та її потреби в ефективному захисті від потенційних кібератак. Використання системи Snort дозволяє активно виявляти та блокувати загрози, що можуть поставити під загрозу інформаційну безпеку компанії. Під час налаштування системи були ураховані особливості мережевої інфраструктури компанії, що забезпечило оптимальну роботу системи в реальних умовах експлуатації.

Тестування системи дозволило підтвердити її ефективність та надійність в умовах потенційних кібератак. Отримані результати підтвердили високий рівень захисту, забезпечений обраною системою, та показали її здатність до реагування на загрози в мережевому середовищі. Розгортання цього проєкту значно підвищило загальний рівень кібербезпеки компанії, забезпечивши безперебійну роботу і захист важливих інформаційних ресурсів.

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Requirements and Model for IDES - a Real-time Intrusion-detection Expert System. / Dorothy Denning, Peter G. Neumann - SRI International, 1985. - 70 с.
2. Endorf C. Intrusion Detection and Prevention / C. Endorf, G. Schultz, J. Mellander., 2003. – 500 с.
3. Intrusion Detection: A Survey [Електронний ресурс] – Режим доступу до ресурсу: <https://ieeexplore.ieee.org/document/4693640/authors>
4. Cybersecurity: A comprehensive guide to getting started in cybersecurity / Packt Publishing, 2019. – 396 с.
5. Cybersecurity For Dummies / Joseph Steinberg - For Dummies, 2019. – 368 с.
6. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В. Л. Бурячок, Г. М. Гулак, В. Б. Толубко. – К.: ДУТ, 2015. – 449 с.
7. Кузьменко Б. В. Захист інформації / Б. В. Кузьменко, О. А. Чайковська. – Київ: Видавничий відділ КНУКіМ, 2009. – 69 с.
8. Guide to Firewalls and Network Security / Cengage Learning, 2008. – 528 с.
9. Intrusion Detection and Prevention Systems: A Review [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/345485220_Intrusion_Detection_and_Prevention_Systems_A_Review
10. Network Intrusion Detection: An Analysts Handbook Third Edition / Stephen Northcutt, Judy Novak, 2001. – 384 с.
11. Cybersecurity - Attack and Defense Strategies - Third Edition: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system / Packt Publishing, 2022 – 570
12. Mitnick K. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers / Kevin Mitnick., 2005. – 322 с

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

13. The State of the Art in Intrusion Prevention and Detection / Auerbach Publications, 2016 – 514 с.
14. Mining E. Kali Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing. Includes Valuable Basic Networking Concepts. / Ethem Mining., 2019. – 175 с.
15. Network Security Essentials: Applications and Standards, 6th edition / Pearson, 2016 – 464 с.
16. Cisco [Інтернет-ресурс] / Web-сайт: Cisco; Режим доступу <https://www.cisco.com/>, вільний.
17. McAfee [Інтернет-ресурс] / Web-сайт: McAfee; Режим доступу <https://www.mcafee.com/>, вільний.
18. Snort [Інтернет-ресурс] / Web-сайт: snort; Режим доступу <https://snort.org/>, вільний.
19. Suricata [Інтернет-ресурс] / Web-сайт: Suricata; Режим доступу <https://suricata.io/>
20. OSSEC [Інтернет-ресурс] / Web-сайт: OSSEC; Режим доступу <https://www.ossec.net/>
21. Forcepoint [Інтернет-ресурс] / Web-сайт: forcepoint; Режим доступу <https://www.forcepoint.com/>, вільний.
22. pfSense [Інтернет-ресурс] / Web-сайт: pfSense; Режим доступу <https://www.pfsense.org/>, вільний.
23. NETGATE [Інтернет-ресурс] / Web-сайт: NETGATE; Режим доступу <https://www.netgate.com/>, вільний.

		Скочко П.А.			ККІКБ.КР.Б – 125 – 16 – ПЗ	Арк
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		51