ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ПРОТИДІЇ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ ЗА ДОПОМОГОЮ SURICATA»

Виконав студент 4 курсу, групи БСД-42
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та
кібернетична безпека»
(шифр і назва спеціальності)
Задирака І.Т.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Задирака Ігор Тарасович
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розробка рекомендацій щодо застосування методів протидії вторгнень в інформаційну систему за допомогою Suricata»
керівник бакалаврської роботи Марченко Віталій Вікторович, ст. викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24» лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми протидії вторгненням в інформаційну систему.
2. Зміст проблеми вторгнення в інформаційну систему
3. Методи та засоби протидії вторгненням в інформаційну систему.
4. Рекомендації щодо застосування методів протидії вторгнень в інформаційну систему за допомогою Suricata.

5. Перелік графічного матеріалу
1. Тема бакалаврської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3.

4.

5.

6. Рекомендації щодо застосування методів та засобів протидії вторгнень в інформаційну систему за допомогою Suricata.

7. Висновки за результатами роботи.

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Визначення актуальності проблеми протидії вторгненням в інформаційну систему.	24.02.2023 р.	
2.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	15.03.2023 р.	
3.	Аналіз проблеми вторгнення в інформаційну систему.	29.03.2023 р.	
4.	Аналіз методів та засобів протидії вторгнень в інформаційну систему.	17.04.2023 р.	
5.	Розроблення рекомендацій щодо застосування методів та засобів протидії вторгнень в інформаційну систему за допомогою Suricata.	15.05.2023 р.	
6.	Оформлення результатів дослідження.	22.05.2023 р.	
7.	Підготовка доповіді до захисту.	29.05.2023 р.	

Студент _____ Задирака І.Т.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на бакалаврську роботу

студента Задираки Ігоря Тарасовича
на тему: «Дослідження шляхів та розроблення рекомендацій щодо застосування методів протидії вторгнень в інформаційну систему за допомогою Suricata»

Актуальність: Сьогодні вторгнення в інформаційну систему різних організацій і установ відбувається кожен день і кількість загроз буде тільки збільшуватися. Злодії створюють нові способи проникнення в інформаційну систему через мережу, використовуючи різні і хитрі прийоми, шляхом обману працівників підприємства тощо. Так як підприємства працюють із великою кількістю даних в їхню мережу виходить і входить трафік, і є ризик, що він може бути шкідливим, але не всі програмні засоби здатні опрацьовувати велику кількістю даних в наслідок чого, злодій може потрапити в інформаційну систему чи якийсь шкідливий програмний засіб потрапити на якусь машину, яка з'єднана до мережі підприємства. Тому для підприємств, які працюють із великою кількістю даних треба програмний засіб, який здатний обробляти велику кількість даних, такою програмою може бути Suricata. Саме вона здатна обробляти 10ГБіт/с трафіку, що для підприємства є важливим, при правильному налаштуванні, може захищати мережу підприємства і відділяє її від зовнішнього інтернету і фільтрує весь трафік який проходить через неї. Тому тема бакалаврської роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу в роботі було встановлено проблеми вторгнення в інформаційну систему.
2. Було досліджено методи та засоби протидії вторгненням в інформаційну систему підприємств.
3. Розроблення рекомендацій щодо застосування методів та засобів протидії вторгненням в інформаційну систему за допомогою Suricata.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

Недоліки:

1. У бакалаврській роботі бажано було б провести аналіз можливих умов функціонування засобу багатовимірного візуального аналізу IBM i2 Analyst's Notebook з різними інформаційними системам підприємства.
2. Експеримент із застосуванням рішення IBM i2 Analyst's Notebook бажано було б провести на вихідних даних, які відображають конкретний кіберінцидент.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговує оцінку **добре**, а студент **Задирака І.Т.** – присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Задирака І.Т. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розроблення рекомендацій щодо застосування методів протидії вторгнень в інформаційну систему за допомогою Suricata».
Бакалаврська робота і рецензія додаються.
Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Задирака І.Т. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) _____ Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент ***Задирака І.Т.*** обрав тему роботи, метою якої було дослідження шляхів та розроблення рекомендацій щодо застосування методів протидії вторгнень в інформаційну систему за допомогою Suricata. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Задирака І.Т. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану бакалаврську роботу студента Задираки Ігоря Тарасовича на оцінку **«добре»** та присвоїти йому кваліфікацію: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Задирака І.Т.
(прізвище та ініціали)
допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: .. сторінок, .. рисунків, .. таблиця, .. джерел.

Об'єкт дослідження – процес протидії вторгнень в інформаційну систему.

Предмет дослідження – методи протидії вторгнень в інформаційну систему.

Мета роботи – розробити рекомендації щодо застосування методів протидії вторгнень в інформаційну систему.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів.

В роботі приведено основні відомості про методи захисту інформаційної системи підприємства, загрози інформаційної системи підприємств.

Проаналізовано різні види загроз для інформаційної системи та наведено їх класифікацію.

Досліджено методи та засоби захисту інформаційної системи підприємства та їх переваги та недоліки.

Досліджено можливості програмного комплексу Suricata.

На основі досліджень проведених в роботі розроблено рекомендації щодо застосування методів протидії вторгнень в інформаційну систему.

Галузь використання – кібербезпека корпоративних інформаційних систем.

ЗАГРОЗИ, КІБЕРБЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення

ШПЗ – шкідливе програмне забезпечення

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

ІС - інформаційна система

DoS – Denial of Service

DDoS - Distributed Denial-of-Service

ВСТУП

Актуальність дослідження. У зв’язку зі стрімким розвитком інформаційних технологій та перенесення всієї інформації як конфіденційну, таємну в електронний формат, а також популяризація онлайн транзакцій, перенаправлення коштів на інші картки тощо. Захист інформації від її викрадення, зміни чи знищення, стає надзвичайно важливим завданням для організацій, підприємств так як злодії, хакери створюють нові методи вторгнення в інформаційну систему для викрадання цінної інформації, зупинки роботи підприємства, припинення належного функціонування підприємства.

Тому в нас час, є велика кількість випадків стороннього проникнення в інформаційні системи підприємств, організацій чи навіть критичної інфраструктури, за того що підприємство, організації чи установи не приділяють належної уваги, проблеми захисту інформаційної системи. Вторгнення в інформаційні системи підприємств можуть мати різні наслідки, від не значних і катастрофічно великих. Як приклад, такими наслідками можуть бути як: втрати персональних даних працівник фірми, клієнтів, зміна, знищення інформації або отримання доступу до інформації осіб, які не мають право доступу до неї, припинення належного функціонування підприємства, або зовсім припинення його роботи. Це може спричинити різні непередбачувані наслідки, як втрату цінних даних, втрату грошей, втрати довіри клієнтів, інвесторів до підприємства в наслідок чого підприємство може стати банкрутом та припинити своє існування чи навіть відключення критичної інфраструктури цілої країни, якщо ми кажемо про хакерську атаку на критичну інфраструктуру країни, що може спричинити до катастрофічних наслідків як для людей, так і для навколишнього середовища.

Саме тому приділення достатньої уваги захисту інформаційної системи від кібератак, є необхідним кроком для забезпечення стабільної роботи бізнесу, компаній, збереження клієнтів та постійного розвитку підприємств, компаній.

Об'єкт дослідження – процес протидії вторгнень в інформаційну систему.

Предмет дослідження – методи протидії вторгнень в інформаційну систему.

Мета роботи – розробити рекомендації щодо застосування методів протидії вторгнень в інформаційну систему за допомогою Suricata.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів.

Завдання бакалаврської роботи:

дослідити існуючі загрози та її наслідки в інформаційній системі;

проаналізувати існуючі методи та засоби захисту інформаційної системи;

дослідити можливості програмного забезпечення Suricata;

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів.

Практичне значення одержаних результатів: рекомендації щодо захисту інформаційної системи можуть бути використані у сфері забезпечення безпеки інформаційної системи в підприємствах.

1 АНАЛІЗ ПРОБЛЕМИ ВТОРГНЕННЯ В ІНФОРМАЦІЙНУ СИСТЕМУ

1.1. Аналіз загроз в інформаційній системі підприємства

Спочатку варто розібратися, що саме означають наступні терміни *інформаційна система*, *вторгнення*, *загроза*, *безпека*.

Інформаційна (автоматизована) система – це технічна система, в якій реалізується технології збирання, пересилання, оброблення та пошук інформації з використанням технічних і програмних засобів.

Далі слід розібрати термін *вторгнення*. Вторгнення в інформаційну систему – це отримання незаконного доступу до комп'ютерної системи з метою отримання, зміни або видалення інформації. Саме вторгнення може бути здійсненним шляхом використання вразливостей в програмному забезпеченні, використання шпигунського програмного забезпечення або підміни паролів. Варто розуміти що вторгнення в інформаційну систему може мати серйозні наслідки, такі як втрата конфіденційних даних, знищення даних або порушення цілісності даних.

Наступне що варто розглянути це термін *загроза*. Загроза ІС – це будь-який потенційний чи реальний інцидент, що може привести до нанесення шкоди її безпеці та привести до втрати конфіденційності цінної чи секретної інформації, зміни чи знищення даних, зупинки роботи ІС, таким чином нанести збитків інформаційній (автоматизованій) системі підприємства, підірвати довіру клієнтів до нього. Самі загрози можуть виникнути в наслідок зовнішніх чи внутрішніх факторів, таких як хакерські атаки, віруси, природні катастрофи, людські фактори чи відмови обладнання.

Наступний термін це *безпека.* Під безпекою ІС розуміється захищеність системи від випадкових чи навмисних інцидентів і також захищеність конфіденційності інформації, щоб доступ до інформації і системи отримували тільки авторизовані користувачі, доступності інформації для користувачів, тобто

щоб авторизовані користувачі мали доступ до інформації і також цілісність інформації, щоб не було несанкціонованих змін чи видалення інформації сторонніми особами, які не є авторизованими в інформаційній системі.

Варто також розібратися із терміном «вразливість ІС». Це так би мовити, слабкі місця ІС, якими можуть скористуватися хакери. Ці самі, вразливості, можуть виникнути через декілька причин: недосконале ПЗ(тобто помилки, збої в ПЗ), деякі процеси роботи системи неповноцінні, слабо кваліфікований персонал, який може необачно запустити ШПЗ в інформаційну систему підприємства, що для підприємства є дуже небезпечним, бо будь який збій в роботі підприємства може сильно вплинути на дохід, репутацію самого підприємства. Тому так важливо для всіх підприємств протидіяти вторгненням в інформаційну систему та знаходити вразливості в їхніх інформаційних системах і знешкоджувати їх, але варто пам’ятати що 100% захисту не буває.

1.2. Види та наслідки вторгнення в інформаційні системи підприємств

На 2023 рік вже існує багато різних видів загроз для ІС підприємства. І кожен із цих загроз має різні функції дії і також має різні наслідки для ІС підприємства. Їх розділяють на наступні види:

1. Фішинг(Phishing)

Фішинг – це шахрайська атака, завдяки якій шахраї намагаються отримати конфіденційну інформацію працівників підприємства, таку як логіни, паролі, номери кредитних карток через використання посилання на підроблений веб-сайт, де просять увести логін, пароль чи будь-яку іншу конфіденційну інформацію або використання електронної пошти, коли на пошту працівника підприємства приходить повідомлення від нібито якоїсь фірми, підприємства чи банку, хоча насправді це і є шахраї, які просто видають себе за офіційних осіб чи підприємств, де є якийсь файл, який просять інсталювати чи посилання, за яким наполегливо наполягають перейти[5].

Наслідки фішингу можуть бути болючими для підприємства, бо із-за цієї загрози може бути порушена конфіденційність інформації працівників чи

власників компанії. Шахраї зможуть продати цю інформацію конкурентам чи завантажити конфіденційну інформацію у відкритий доступ завдяки чому ця інформація стане відомою для осіб, які не мають дозвіл на володіння інформацією, що означає порушення конфіденційності. Що в свою чергу призведе до зниження довіри клієнтів, інвесторів до підприємства і принесе збитки для постраждалої компанії. Так як зловмисники можуть розповсюджувати ШПЗ, які можуть пошкодити або відключити системи, сервери, мережі пристрої тощо. Це може призвести до припинення роботи підприємства і втрати даних[5].

2. *Троянські програми(Trojan programs)*

Комп'ютерний вірус-троян – це вид ШПЗ, яке маскується під корисну програму чи файл і під час скачування вірус приховано скачується на комп'ютер без дозволу користувача. Вірус здатен виконувати дії, які можуть бути шкідливими для користувача, його даних або системи. На відміну від вірусу, він не здатний самостійно копіювати себе або інфікувати файли. Щоб проникнути на пристрій, троян використовує інші засоби, такі як приховане завантаження, використання вразливостей ІС або завантаження іншим шкідливим кодом.

Станом на 2023 рік трояни є одною з найпоширеніших категорією шкідливих програм, яка використовується для відкриття бекдорів, контролю інфікованого пристрою, контролю за клавіатурою, відеокамерою, мікрофоном зараженого пристрою, видалення або зміна інформації, яка знаходиться на зараженому пристрої, а також передача цієї інформації зловмисникам, інсталювання інших шкідливих програм та вірусів на пристрій. Також троян може блокувати, шифрувати певну інформацію на пристрої і вимагати за це винагороду щоб розшифрувати дані, також може використовувати заражений пристрій для інфікування інших машин[7].

Одним із перших відомих троянів, була програма-вимагач, виявлена в реальному середовищі – AIDS Trojan 1989 року. Програма шифрувала більшість імен файлів у кореневому каталозі машини і вимагала від потерпілих відправити кошти на рахунок кіберзлочинців[7].

В наслідок потрапляння вірусу-трояна на машину підприємства це може призвести до серйозних наслідків таких як[16]:

- *Викрадення даних,* троянські програми можуть надати зловмиснику віддалений доступ до зараженої машини, що дозволяє їм викрадати чутливі дані. Це можуть бути корпоративні дані, інформація клієнтів як їх персональні дані, паролі, фінансові дані та інше. Втрата цих даних може мати серйозні наслідки для конфіденційності та безпеки підприємства.

- *Виток інформації,* троянська програма у випадку встановлювання шпигунських функцій, які здатні відстежувати активність користувача, працівника компнаії, здатні перехоплювати введені дані, включаючи паролі, номери банківських карт, переписку тощо може призвести до витоку конфіденційної інформації та порушення приватності підприємства.

- *Віддалене керування,* здатність зловмисника отримати віддалений доступ до інфікованої машини, це дасть змогу зловмисникові виконувати шкідливі дії на мишині, як встановлення додаткових шкідливих програм, викрадення даних, виконання на інші системи тощо. Такий віддалений контроль над машинами може мати серйозний вплив на безпеку та функціонування підприємства.

- *Втрата контролю над системою,* трояни здатні видаляти файли на інфікованій машині, змінювати налаштування системи, блокування доступу до ресурсів тощо.

3. Черв’як (Worm)

Комп’ютерний вірус черв’як – це тип ШПЗ, яке на відміно від вірусу-троян, може створювати власні копії і розповсюджувати їх через комп’ютерні мережі та Інтернет на інші комп’ютери. Швидкість розповсюдження копій віруса може бути високою та без участі користувача зараженої машини[8].

Вірус-черв’як, також як і попередній вірус, має багато власних видів. Email Worms, цей тип вірусу-черв’яка поширюється через електронну пошту, надсилаючи свої копію на всі контакти у адресній книзі жертви. Network Worms, цей тип може розсилати свої копії через Інтернет або через внутрішню мережу підприємства. Для того щоб зламати машини, цей тип вірусу використовує

вразливості у мережевих протоколах або ПЗ. Наступний вид File Sharing Worms. Цей вид розповсюджується через файлообмінні мережі, як BitTorrent. Сам вірус може перебувати в файлах, таких як музика, фільми, ігри і заражає комп'ютер коли працівник скачав даний файл, то разом із ним інсталюється сам вірус. Instant Messaging Worms, цей тип вірусу розповсюджується через програми миттєвого обміну повідомлення як Skype, Facebook. Вони можуть використовувати підроблені посилання, коли працівник переходить по них, то в цей час вірус завантажується на комп'ютер. USB Worms, даний вид вірусу-черв'як розповсюджує свої копії через встановлену в комп'ютер заражений USB накопичувач[8].

Кожен із видів має різні цілі та можливості одні види черв'яка можуть створювати бекдори(backdoors), що дасть зловмиснику можливість дистанційно керувати ком'ютером або можуть встановлювати шпигунське ПЗ для збору конфіденційної інформації. Інші черв'яки, можуть видаляти файли, форматувати диски і навіть перенаправляти трафік мережі на інші комп'ютери. Сам вірус може попасти на комп'ютер через помилку працівників підприємства, коли хтось із працівників перейшов по не відомому посиланню чи коли працівник використовує власну заражену USB флешку і приєднує її до робочої машини.

Наслідками для підприємства можуть бути, втрата конфіденційної інформації компанії, розповсюдження персональних даних працівників компанії стороннім особам, які не мають право доступу до неї. Цей вірус-черв'як є небезпечним, бо в наслідок помилки працівника, який через свою необізнаність інсталював на машину, вірус-черв'як, може нести серйозні наслідки. Бо сам вірус може розсилати свої копії через мережу, використовуючи вразливості мережевого протоколу, завдяки чому можуть бути атаковані всі машини підприємства, які підключені до мережі, що в свою чергу може призвести до часткової або повної зупинки роботи підприємства, і може нести за собою великі збитки для самої компанії. Також зловмисник, може через заражену машину отримати доступ до ІС підприємства для викрадення цінних даних, зламати систему або здійснити додаткові атаки. Ще крім цього інфікована машина може бути залученою до

ботнету, що вимагатиме часту взаємодію зі зловмисником або виконання шкідливих процесів. Це може призвести до значного зниження продуктивності комп'ютера і впливати на загальну продуктивність системи підприємства[17].

4. Dos/DDoS-атаки

Dos/DDoS-атака – це атака на комп'ютерні системи організації, підприємства з метою порушення доступності атакованих веб ресурсів чи серверів. Тобто, здійснюється величезна кількість запитів на веб ресурс чи сервер підприємства(кількість запитів може досягати мільйони) щоб атакована система не змогла обробити таку кількість запитів в наслідок чого в її роботи виникають збої або вона взагалі перестає повноцінно працювати. Різниця між Dos/DDos полягає в тому що DDos-атаки, на відміну від DoS-атаки, здійснюється з декількох джерел, а не з одного.

Під час DDoS-атаки низка ботів або ціла бот-мережа перевантажує запитами HTTP й трафіком веб-сайт чи службу. Тобто кілька комп'ютерів намагаються захопити один пристрій, щоб користувачі втратили доступ до нього. В наслідок чого можуть виникнути затримки в обслуговуванні. Також варто зазначити, що під час атаки хакери можуть проникнути в базу даних підприємства і отримати доступ до конфіденційної інформації. Сама атака може тривати кілька годин або навіть днів[9].

Як в попередніх вірусах в DDos-атаках мають різні види: об'ємні атаки, атаки на рівні протоколу й атаки на прикладному рівні[9].

- Коли здійснюється DDos-атака, то через відкритий DNS-сервер цільовий об'єкт переповнюється трафіком із відповідей на запити DNS.
- Атака на рівні протоколу призводить до переривання роботи служби.
- Атака прикладного рівня спрямовує на веб-програми й зриває передавання даних між хостами.

У разі успішної або частково успішної DDoS/DoS-атаки на інформаційну систему підприємства можуть бути наступні наслідки[18]:

- *Недоступність сервісів*, тобто дані атаки, можуть спричинити перевантаження мережі або сервісів, що призводить до недоступності сервісів для

користувачів. Це може включати як веб-сайти, електронні поштові сервери, онлайн-платформи тощо. Недоступність сервісів може вплинути на продуктивність підприємства, призвести до втрати клієнтів і витрати на відновлення роботи системи.

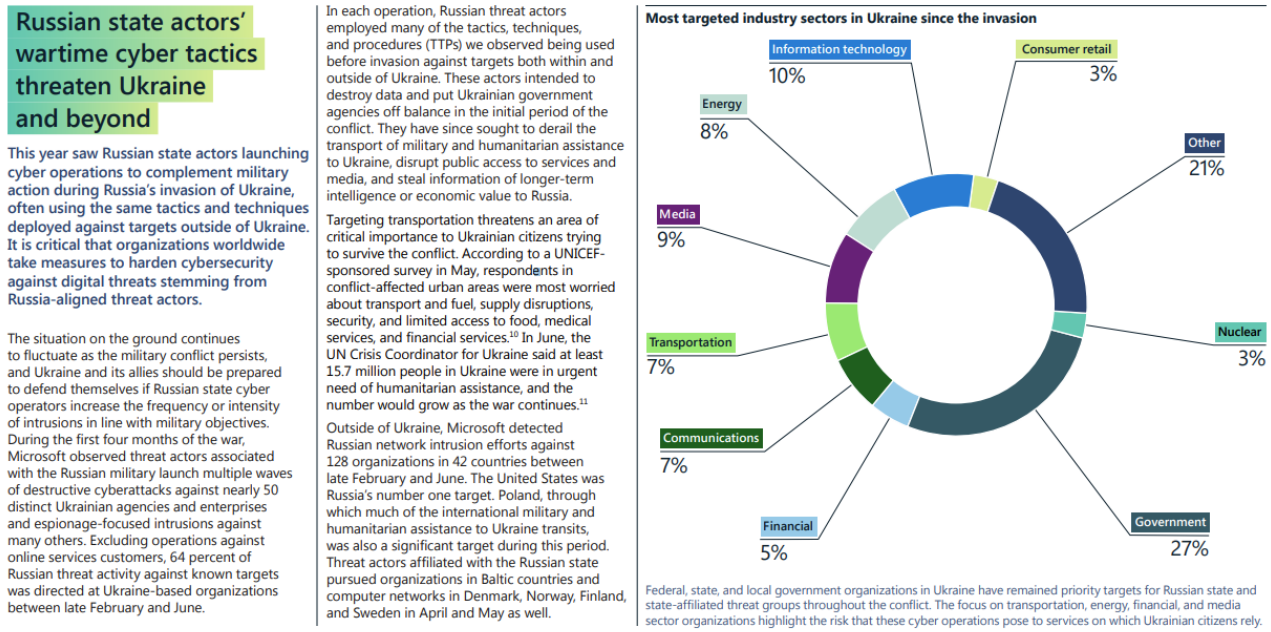
- *Втрата доходу*, якщо дана атака пройшла успішно, і в наслідок атаки, система підприємства стала не доступною для клієнтів, підприємство може зазнати значних фінансових втрат, через втрату продажів, шкоду репутації та можливі санкції з боку партнерів чи клієнтів або інвесторів.

- *Зниження продуктивності*, навіть якщо система залишиться доступною під час DDoS/DoS-атак, велика кількість шкідливого трафіку може спричинити зниження продуктивності системи, це може виявлятися в повільній роботі, відмовах у виконанні запитів або падіннях системи. Це все може призвести до зниження продуктивності, затримки у роботі, незадоволеність користувачів, погіршення якості обслуговування.

1.3. Статистика та сучасний стан кіберзагроз

Згідно минулорічним статистикам різних компаній таких як Microsoft за 2020, 2021 роки, можна побачити що кількість кіберінцидентів таких як DDoS-атак збільшується із кожним роком. У першому півріччі 2021 року за даними Azure Networking було зафіксовано збільшення DDoS-атак на 25%. В другій половині 2021 року було усунено понад 359 713 атак на глобальну інфраструктура Azure – це на 43% більше ніж у першій половині 2021 року[9].

Далі проведено статистику від компанії Microsoft, що після повномасштабного вторгнення росії в Україну. Держава агресорка здійснила низку кібератак на більшість галузей промисловості України. Статистику проведено нижче на рис.1.1.



Russian state actors' wartime cyber tactics threaten Ukraine and beyond

This year saw Russian state actors launching cyber operations to complement military action during Russia's invasion of Ukraine, often using the same tactics and techniques deployed against targets outside of Ukraine. It is critical that organizations worldwide take measures to harden cybersecurity against digital threats stemming from Russia-aligned threat actors.

The situation on the ground continues to fluctuate as the military conflict persists, and Ukraine and its allies should be prepared to defend themselves if Russian state cyber operators increase the frequency or intensity of intrusions in line with military objectives. During the first four months of the war, Microsoft observed threat actors associated with the Russian military launch multiple waves of destructive cyberattacks against nearly 50 distinct Ukrainian agencies and enterprises and espionage-focused intrusions against many others. Excluding operations against online services customers, 64 percent of Russian threat activity against known targets was directed at Ukraine-based organizations between late February and June.

In each operation, Russian threat actors employed many of the tactics, techniques, and procedures (TTPs) we observed being used before invasion against targets both within and outside of Ukraine. These actors intended to destroy data and put Ukrainian government agencies off balance in the initial period of the conflict. They have since sought to derail the transport of military and humanitarian assistance to Ukraine, disrupt public access to services and media, and steal information of longer-term intelligence or economic value to Russia.

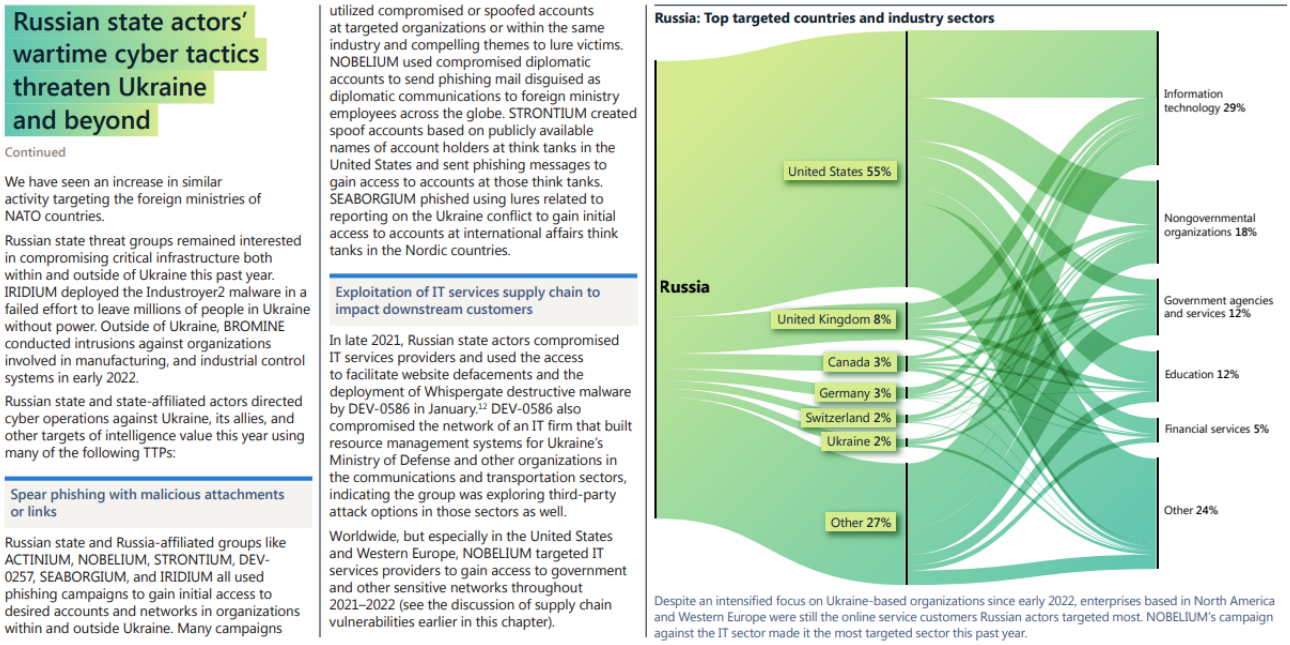
Targeting transportation threatens an area of critical importance to Ukrainian citizens trying to survive the conflict. According to a UNICEF-sponsored survey in May, respondents in conflict-affected urban areas were most worried about transport and fuel, supply disruptions, security, and limited access to food, medical services, and financial services.[10] In June, the UN Crisis Coordinator for Ukraine said at least 15.7 million people in Ukraine were in urgent need of humanitarian assistance, and the number would grow as the war continues.[11]

Outside of Ukraine, Microsoft detected Russian network intrusion efforts against 128 organizations in 42 countries between late February and June. The United States was Russia's number one target. Poland, through which much of the international military and humanitarian assistance to Ukraine transits, was also a significant target during this period. Threat actors affiliated with the Russian state pursued organizations in Baltic countries and computer networks in Denmark, Norway, Finland, and Sweden in April and May as well.

Federal, state, and local government organizations in Ukraine have remained priority targets for Russian state and state-affiliated threat groups throughout the conflict. The focus on transportation, energy, financial, and media sector organizations highlight the risk that these cyber operations pose to services on which Ukrainian citizens rely.

Рис.1.1. Статистика кібератак на промислові галузі України

Згідно статистики від Microsoft, можна побачити, що найбільш пріоритетні цілі для росії були такі сектора як: транспортний, енергетичний, фінансовий та ЗМІ. Також під кібератаки піддалися 128 організацій в 42 країн світу.



Russian state actors' wartime cyber tactics threaten Ukraine and beyond

Continued

We have seen an increase in similar activity targeting the foreign ministries of NATO countries.

Russian state threat groups remained interested in compromising critical infrastructure both within and outside of Ukraine this past year. IRIDIUM deployed the Industroyer2 malware in a failed effort to leave millions of people in Ukraine without power. Outside of Ukraine, BROMINE conducted intrusions against organizations involved in manufacturing, and industrial control systems in early 2022.

Russian state and state-affiliated actors directed cyber operations against Ukraine, its allies, and other targets of intelligence value this year using many of the following TTPs:

Spear phishing with malicious attachments or links

Russian state and Russia-affiliated groups like ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM, and IRIDIUM all used phishing campaigns to gain initial access to desired accounts and networks in organizations within and outside Ukraine. Many campaigns utilized compromised or spoofed accounts at targeted organizations or within the same industry and compelling themes to lure victims. NOBELIUM used compromised diplomatic accounts to send phishing mail disguised as diplomatic communications to foreign ministry employees across the globe. STRONTIUM created spoof accounts based on publicly available names of account holders at think tanks in the United States and sent phishing messages to gain access to accounts at those think tanks. SEABORGIUM phished using lures related to reporting on the Ukraine conflict to gain initial access to accounts at international affairs think tanks in the Nordic countries.

Exploitation of IT services supply chain to impact downstream customers

In late 2021, Russian state actors compromised IT services providers and used the access to facilitate website defacements and the deployment of Whispergate destructive malware by DEV-0586 in January.[12] DEV-0586 also compromised the network of an IT firm that built resource management systems for Ukraine's Ministry of Defense and other organizations in the communications and transportation sectors, indicating the group was exploring third-party attack options in those sectors as well.

Worldwide, but especially in the United States and Western Europe, NOBELIUM targeted IT services providers to gain access to government and other sensitive networks throughout 2021–2022 (see the discussion of supply chain vulnerabilities earlier in this chapter).

Despite an intensified focus on Ukraine-based organizations since early 2022, enterprises based in North America and Western Europe were still the online service customers Russian actors targeted most. NOBELIUM's campaign against the IT sector made it the most targeted sector this past year.

Рис.1.2. Статистика здійснення росією кібератак на різні держави світу та їх сектора

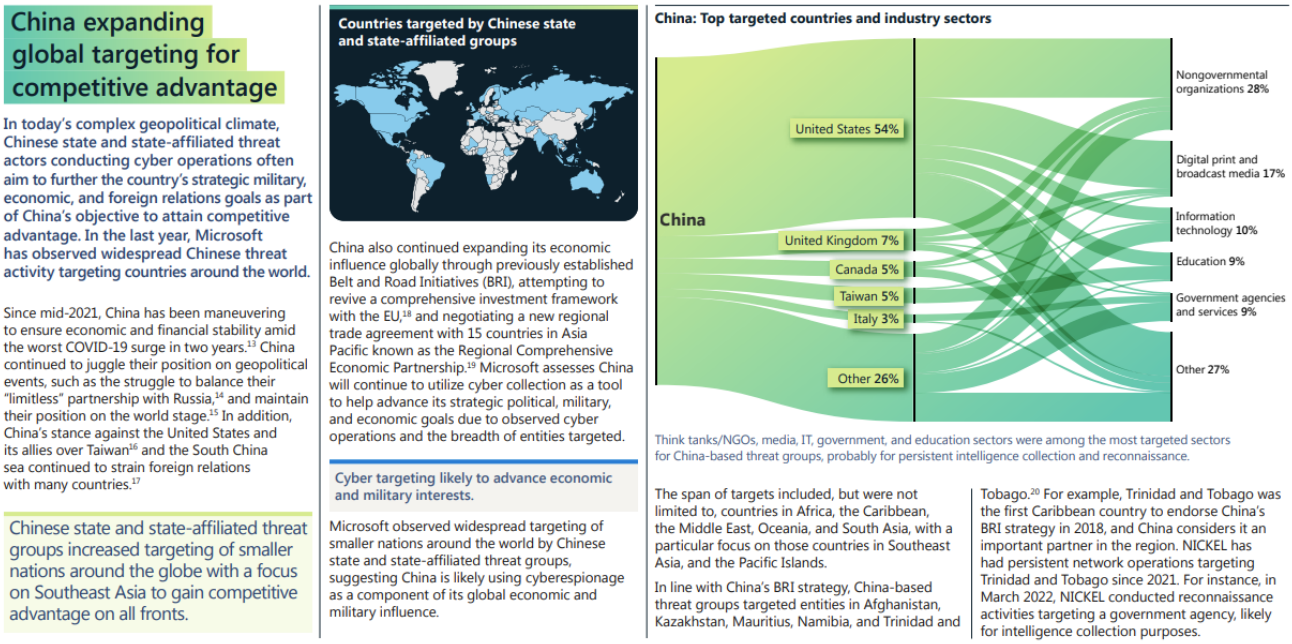


Рис.1.3. Статистика здійснення КНР кібератак на різні держави світу та їх сектора

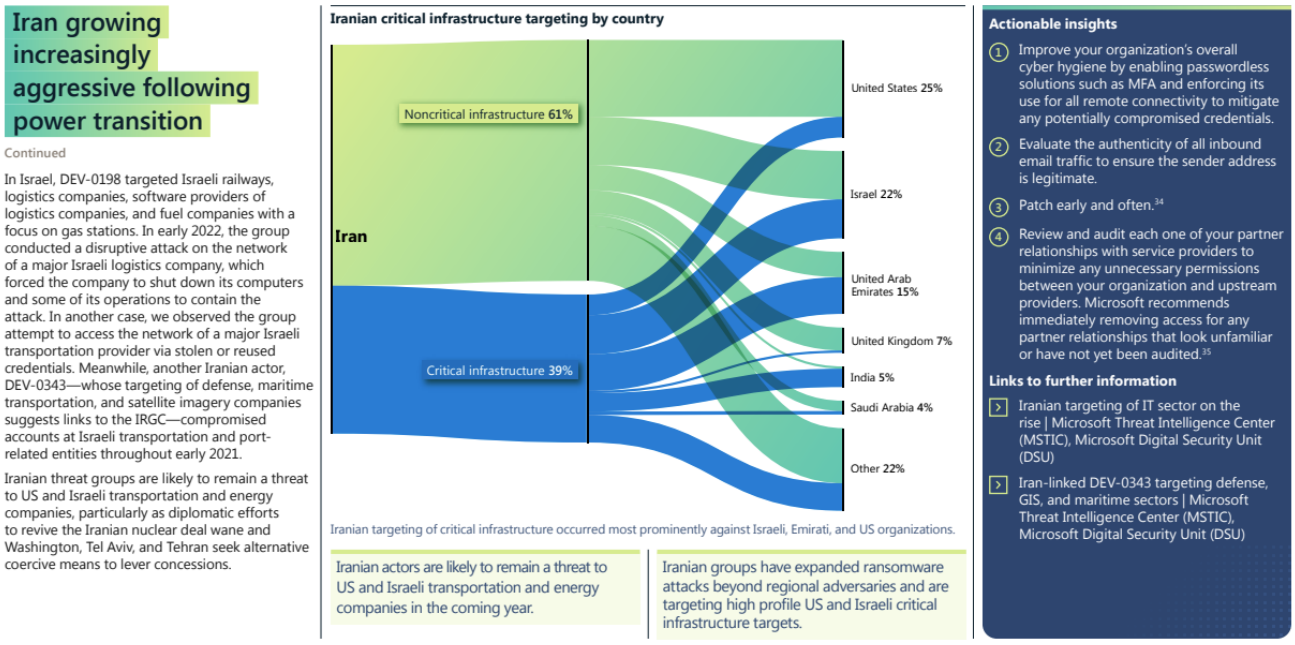
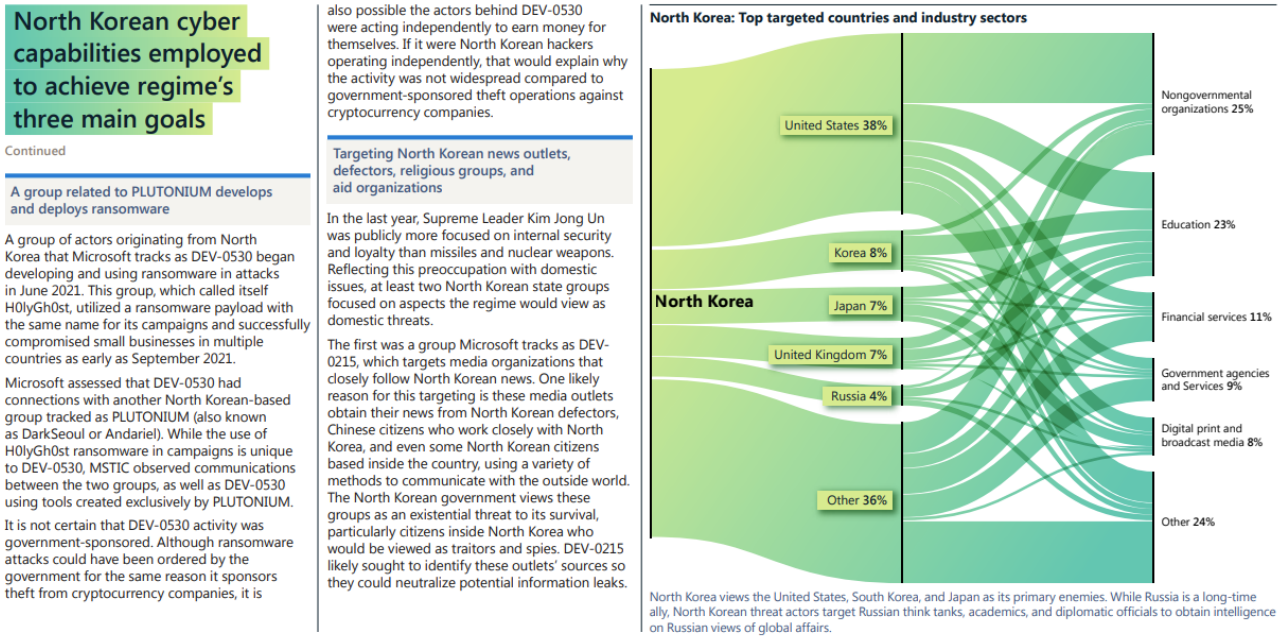


Рис.1.4. Статистика здійснення Іраном кібератак на різні держави світу та їх критичні і некритичні інфраструктури



North Korean cyber capabilities employed to achieve regime's three main goals

Continued

A group related to PLUTONIUM develops and deploys ransomware

A group of actors originating from North Korea that Microsoft tracks as DEV-0530 began developing and using ransomware in attacks in June 2021. This group, which called itself H0lyGh0st, utilized a ransomware payload with the same name for its campaigns and successfully compromised small businesses in multiple countries as early as September 2021.

Microsoft assessed that DEV-0530 had connections with another North Korean-based group tracked as PLUTONIUM (also known as DarkSeoul or Andariel). While the use of H0lyGh0st ransomware in campaigns is unique to DEV-0530, MSTIC observed communications between the two groups, as well as DEV-0530 using tools created exclusively by PLUTONIUM.

It is not certain that DEV-0530 activity was government-sponsored. Although ransomware attacks could have been ordered by the government for the same reason it sponsors theft from cryptocurrency companies, it is also possible the actors behind DEV-0530 were acting independently to earn money for themselves. If it were North Korean hackers operating independently, that would explain why the activity was not widespread compared to government-sponsored theft operations against cryptocurrency companies.

Targeting North Korean news outlets, defectors, religious groups, and aid organizations

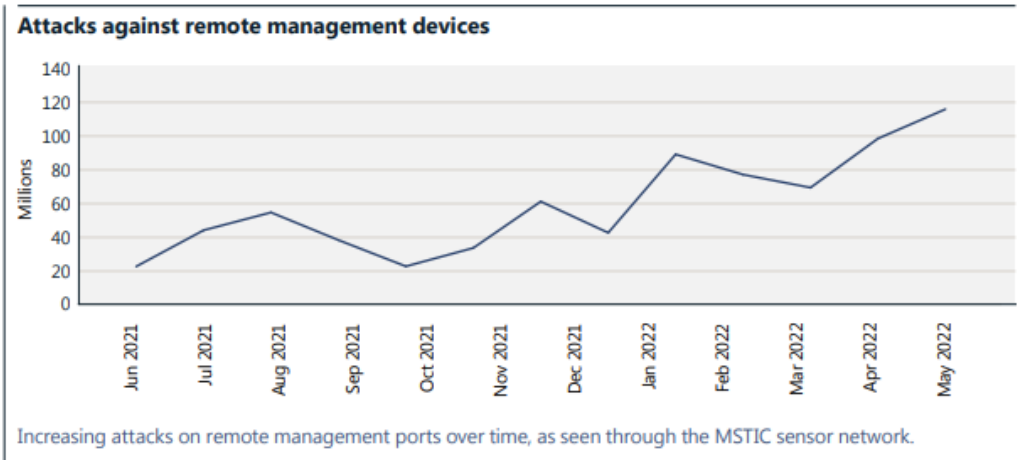
In the last year, Supreme Leader Kim Jong Un was publicly more focused on internal security and loyalty than missiles and nuclear weapons. Reflecting this preoccupation with domestic issues, at least two North Korean state groups focused on aspects the regime would view as domestic threats.

The first was a group Microsoft tracks as DEV-0215, which targets media organizations that closely follow North Korean news. One likely reason for this targeting is these media outlets obtain their news from North Korean defectors, Chinese citizens who work closely with North Korea, and even some North Korean citizens based inside the country, using a variety of methods to communicate with the outside world. The North Korean government views these groups as an existential threat to its survival, particularly citizens inside North Korea who would be viewed as traitors and spies. DEV-0215 likely sought to identify these outlets' sources so they could neutralize potential information leaks.

North Korea views the United States, South Korea, and Japan as its primary enemies. While Russia is a long-time ally, North Korean threat actors target Russian think tanks, academics, and diplomatic officials to obtain intelligence on Russian views of global affairs.

Рис.1.5. Статистика здійснення Північною Кореєю кібератак на різні держави світу та їх сектора

Наступне варто розглянути статистику з 2021 по 2022 роки щодо збільшення атак на порти віддаленого керування, як видно через мережу датчиків MSTIC.



Increasing attacks on remote management ports over time, as seen through the MSTIC sensor network.

Рис.1.6. Статистика атак на пристрої віддаленого керування

Згідно із дослідженням глобального фішингу APWG, у 2016 році спостерігалося понад 250 тисяч унікальних фішингових атак. В останні роки

кіберзлочинці намагалися зосередитися на банківских та фінансових послугах, соціальних мереж, користувачах електронного банкінгу, а також облікових даних електронної пошти[6].

Згідно оцінці від американської дослідницької компанія, яка спеціалізується на ринках інформаційних технологій – Gartner. До 2025 року кількість атак програм-вимагачів зросте до 700%, до 2025 року щонайменше 75% організацій будуть піддані атакам більше одного разу[11].

Посилаючись на прогнози Microsoft, в 2023 році кіберзлочинність продовжить зростати, оскільки з’являться нові загрози та методи атак. DDoS-атаки залишаться основним інструментом для кібератак хакерами. Також сама компанія прогнозує про появу нових ботнетів IoT DDoS в яких атаки будуть поширеними та спричинятимуть значні збої. Також йде зростання DDoS-атак через захоплення облікових записів, коли хакери отримують несанкціонований доступ до ресурсів машини для запуску DDoS-атак[12].

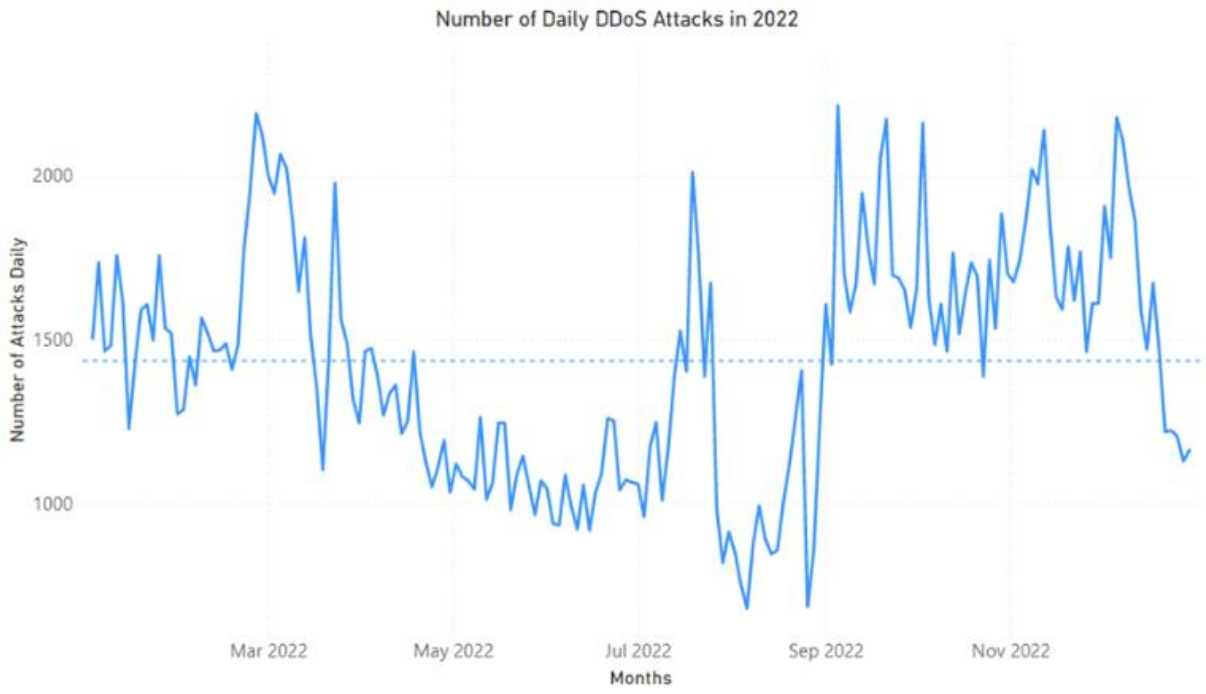


Рис.1.7. Статистика кількості атак за один день в 2022 році на глобальну інфраструктуру Microsoft

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ПРОТИДІЇ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ

2.1. Дослідження методів захисту інформаційної системи (також описати підходи можна)

Згідно статистики кібератак на великі організації як Microsoft, стало зрозуміло, що кількість кібератак буде тільки буде збільшуватися, і будуть з’являтися нові і нові види кіберзагроз, і нові методи атак. Тому, для запобігання вторгненням в інформаційну систему підприємства, є низка методів, мета яких протидіяти кіберзагрозам:

1. *Брандмауер(firewall)* – це система на основі програмного чи апаратного забезпечення, яка є, так би мовити, посередником між безпечними і неперевіреними мережами. Головна його функція – фільтрація шкідливого та потенційно небезпечного контенту та з’єднань, тобто система, яка фільтрує трафік, який входить чи виходить з мережі підприємства. Вона визначає, які з’єднані або пакети дозволені або заборонені на основі написаних, встановлених правил[13].

Брандмауер мережевого рівня виконує функцію захисту для внутрішніх систем, які складаються з декількох пристроїв. Завдяки тому, що він працює на апаратному забезпечені, даний firewall відповідає потребам підприємств будь-якого розміру[13].

Існує кілька типів брандмауерів, кожен з яких має власний вид фільтрування трафіку. Існує всього 4 покоління брандмауерів. Брандмауер *першого покоління* працює як пакетний фільтр. Він порівнює основну інформацію, як оригінальне джерело, призначення пакета, протокол з визначним переліком правил. *Друге покоління* брандмауера може відслідковувати дані про початок з'єднання та з'єднання, які є на даний момент. Третє покоління розроблене для фільтрування інформації за допомогою усіх рівнів моделі OSI, як на рис.2.1.1. Даний вид

брандмауера може розпізнавати програми та деякі поширені протоколи, як FTP, HTTP.

Завдякий цій інформації він може виявляти атаки, які намагаються обійти його через дозволений порт або несанкціоноване використання протоколу. Наступне покоління поєднує в собі всі раніше використанні методи з поглибленим оглядом відфільрованого контенту та порівняння з базою даних для виявлення потенційно небезпечного трафіку. Сучасні брандмауери мають вбудовані системи безпеки, як VPN(віртуальна приватна мережа), IPS/IDS(системи запобігання та виявлення вторгнень), управління додатками, ідентифікацією та веб-фільтрація[13].

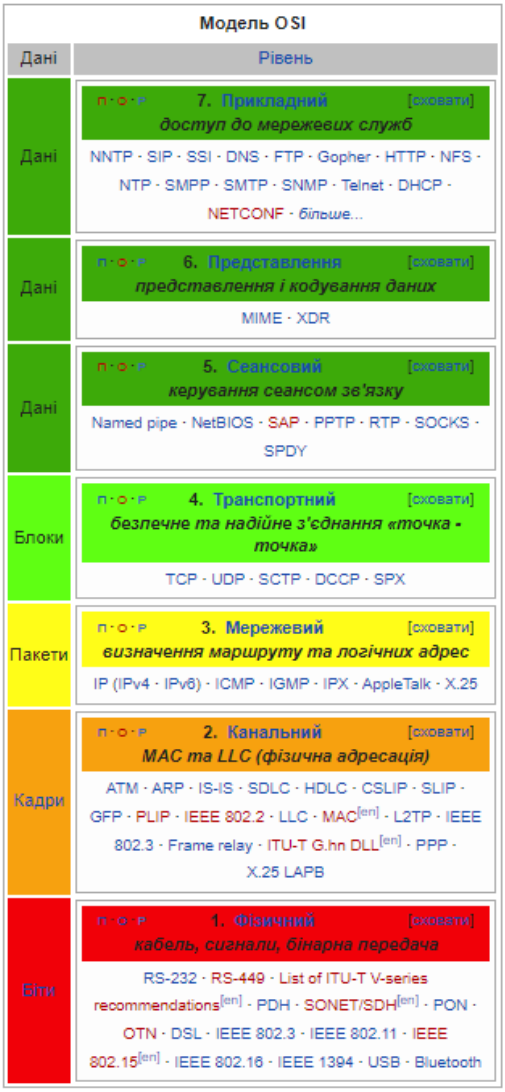


Рис.2.1 – Модель OSI[14]

Переваги використання брандмауера для підприємств, наступні контроль входу і виходу даних з мережі підприємства це допомагає зменшити ймовірність викрадення даних зловмисниками. Зменшення ризиків пристроїв підприємства стати частиною ботнету(великої групи пристроїв, що управляється кіберзлочинцями). Firewall потрібний для компаній з мережами, які складаються з декількох робочих станцій, з'єднаних з мережею Інтернет. Він створює єдину точку входу, де зовнішні загрози ідентифікуються та знешкоджуються. Також firewall відокремлює внутрішні системи компанії від публічного Інтернету, і таким чином створює захищене середовище з вільними та безпечним переміщенням даних.

2. *Шифрування даних(Data Encryption)*. Використання даного методу допомагає захистити конфіденційну інформацію в разі її втрати або крадіжки. Шифрування даних забезпечує їх конфіденційність під час передачі та зберігання.

3. *Ідентифікація* та *аутентифікація* користувачів. Дані методи є одним з основних методів захисту. Вони дозволяють переконатися, що користувач, який намагається отримати доступ до системи, є тим, за кого він себе видає. *Ідентифікація* користувача передбачає присвоєння ідентифікатора, який забезпечує можливість відрізняти одного користувача від іншого. Це може бути як ім'я користувача, номер працівника, номер клієнта тощо. *Аутентифікація* користувача в свою чергу передбачає перевірку того чи дійсно цей користувач є тим, за кого він себе видає. Найчастіше, для цього використовується логін та пароль. Користувач вводить свій логін та пароль, потім система перевіряє введені дані. Якщо логін та пароль коректні, система дозволяє доступ до ІС підприємства.

Проте варто зазначити, що ці методи не є повністю безпечним, є загрози, які можуть обійти дану систему безпеки. Зазначається що 100% захисту не буває, але використовуючи декілька методів, можна зменшити ризик вторгнення в інформаційну систему. Тому для забезпечення більшої безпеки, в додаток варто використовувати *двофакторну аутентифікацію* або *біометричну ідентифікацію*. Як приклад, це може бути згенерований пристроєм код, який можна отримати через інсталювання певного додатку чи отримати код через електронну пошту. Щодо

іншого методу ідентифікації як біометричний. Цей методи використовує відбиток пальця, розпізнавання ока, обличчя тощо.

Переваги використання методів захисту, таких як ідентифікація, аутентифікація, двофакторна аутентифікація та біометрична ідентифікація, для підприємства, наступні:

- *Вищий рівень безпеки*, використання біометричних методів ідентифікації як сканування відбитку пальця, розпізнавання обличчя або сканування сітківки ока, забезпечує високий рівень безпеки, так як біометричні дані важко підробити або скопіювати, що суттєво знижує ризик несанкціонованого доступу до системи.

- *Забезпечення безпеки*, завдяки методам захисту ідентифікації та аутентифікації дозволяють підприємствам перевірити, що користувач або пристрій, який намагається отримати доступу до системи, дійсно є тим за кого себе видає і має право доступу. Це дасть змогу уникнути несанкціонованого доступу, зламу акаунтів або викрадення інформації.

- *Зниження ризику компрометації,* тобто метод двофакторної аутентифікації додає додатковий шар безпеки, вимагаючи від користувачів надати два незалежних фактори для підтвердження своєї ідентичності, як пароль та одноразовий код, що зменшує ризики компрометації акаунтів, оскільки зловмиснику потрібно мати доступ до обох факторів.

4. Наступний метод захисту – використання антивірусного ПЗ, приклад таких антивірусних ПЗ, можуть бути наступні програми: ESET, McAffe, Avast.

- *Виявлення та блокування ШПЗ*, це допомагає виявляти та блокувати віруси, черв’яки, трояни, шпигунські ПЗ та інші види ШПЗ, які можуть спричинити пошкодження ІС, також антивірусне ПЗ може блокувати розповсюдження вірусів та запобігає їх впливу на систему. Як

- *Оновлення бази даних вірусів*, тобто антивірусне ПЗ регулярно оновлює свою базу даних вірусів, що дозволяє виявляти нові ШПЗ, які постійно з’являються. Це дає змогу захищати інформаційну систему підприємства від нових загроз.

- *Виявлення поведінкових аномалій,* деякі антивірусні програми використовують даний метод, це означає, що, виявлення аномалій, може вказувати

на наявність шкідливого ПЗ. Це дає змогу виявити нові атаки та невідомі віруси, які можуть уникнути виявлення за допомогою традиційних сигнатурних методів.

- *Захист електронної пошти та веб-переглядачів,* деякі антивіруси мають дану функцію, це означає, що програма захищає від шкідливих вкладень в електронній пошті та веб-сторінках. Програма перевіряє вхідну пошту та веб-сторінки на наявність вірусів та інших загроз, що допомагає уникнути зараження системи через ці канали.

5. *Система виявлення вторгнень(Intrusion Detection System)* – це система яка використовується для виявлення потенційних вторгнень або несанкціонованої активності в мережі або на комп'ютерах[19].

Основна мета IDS – виявлення аномальної поведінки, загроз та вторгнень у реальному часі, також даний метод може виявляти наступні види загроз, як спроби переповнення буфера, сканування портів, спроби атаки з використанням вразливостей ПЗ, зловживання привілеями, атаки з використанням ШПЗ тощо.

Переваги використання даного методу для захисту ІС наступні[19]:

- *Виявлення загроз в реальному часі*, тобто IDS дозволяє виявляти потенційні атаки та вторгнення майже миттєво, що дозволяє оперативно реагувати та зменшувати можливі шкоди.

- *Моніторинг мережевої активності*, дана система здатна аналізувати мережевий трафік та специфічні події, що відбуваються в системі, для виявлення незвичайної або підозрілої активності.

- *Захист від нових загроз*, IDS може виявляти нові типи атак та вірусів, які можуть бути невідомими для традиційних методів захисту. Він базується на аналізі аномалій та підозрілих активностей, що дозволяє виявляти невідомі загрози.

- *Зменшення ризику втрати даних*, IDS допомагає запобігати несанкціонованому доступу до важливої інформації, зменшуючи ризик втрати даних або конфіденційної інформації.

- *Покращення реакції на інциденти,* IDS система надає детальну інформацію про потенційні атаки та вторгнення, що дозволяє адміністраторам швидко

реагувати на вживати відповідних заходів для подальшого розслідування та відновлення систем.

- *Виявлення вразливостей і аналіз потенційних ризиків,* IDS допомагає виявляти вразливості в інформаційній системі підприємства та оцінювати потенційні ризики безпеки. Це дає змогу підприємству приймати заходи для підвищення рівня безпеки та запобігти можливим атакам.

- *Покращення внутрішньої політики,* IDS дозволяє контролювати активність внутрішніх користувачів та виявляти незвичайні або підозрілу діяльність. Це може виявити інсайдерські загрози, недбалість співробітників або несанкціонований доступ до ресурсів.

Отже, використання IDS як метод захисту ІС підприємства дозволяє виявляти потенційні загрози, зменшувати ризик втрати даних, забезпечувати виконання внутрішніх та зовнішніх нормативних вимог, а також підвищувати реагування на інциденти та внутрішню безпеку підприємства.

6. *Система запобіганню вторгнень(Intrusion Prevention System).* Це система захисту, яка виявляє, блокує/відхиляє запити, вторгнення та атаки на мережу або інформаційну систему підприємства. Вона працює на основі завантажених від зовнішніх постачальників чи власно написаних правил, якщо підпис збігається, система виконує написану дію, як «Alert», «Allow», «Reject», «Drop». При виявлені активних загроз IPS система приймає активні заходи для запобігання атакам, такі як блокування шкідливого трафіку, відмова в обслуговувані тих хто здійснює атаку або відключення вразливих систем[20].

Переваги для підприємства при використанні даної системи захисту[20]:

- *Захисту в реальному часі*, IPS працює в режимі реального часу, виявляючи й блокуючи атаки негайно. Це дає змогу підприємству запобігти атакам що до того, як вони завдають шкоди інформаційній системі.

- *Захист від невідомих та відомих загроз*, IPS використовує базу даних сигнатур, евристичний аналіз та інші методи для виявлення відомих і не відомих загроз. Він здатний розпізнавати нові види атак і захищати систему від них.

- *Багатофункціональність,* IPS система поєднує в собі функції виявлення, блокування та реагування на вторгнення. Він може аналізувати пакети даних, контролювати мережевий трафік, фільтрувати шкідливий вміст та реагувати на загрози.

- *Захист від широкого спектру атак,* IPS система забезпечить підприємству захист від різних видів атак, як DDoS, SQL-ін’єкції, крос-сайтові скрипти, брутфорс, сканування протів та інші загрози.

- *Підвищення продуктивності мережі,* IPS може оптимізувати мережевий трафік, виявляючи й блокуючи небажаний або шкідливий трафік. Це дає змогу знизити навантаження на мережу підприємства та підвищити її продуктивність.

Отже, застосування IPS для захисту ІС підприємства дозволяє забезпечити активний та ефективний захист від вторгнень, знизити ризики втрати даних, а також забезпечити стабільну роботу підприємства.

2.2. Різновиди IPS та (красиво назвати антивіруси які ти знайшов що захищають від вторгнень)

Існує багато IPS програм на ринку, які показують різноманітні можливості та їх призначення для захисту від різних видів загроз. Також в більшості сучасних антивірусних програм, крім функцій firewall, захист від спаму, фішингу, троянських програм також є і функції виявлення/захист вторгнень IPS/IDS. Ось декілька з них:

ESET INTERNET SECURITY – це сучасне антивірусне ПЗ, яке має різні функції захисту від різних видів загроз, ось декілька з них: firewall, захисту від спаму, захист від шпигунських ПЗ, захист від троянських програм, захист від фішингу, захист від крадіжки ідентифікатора і також має функції система запобігання/виявлення вторгнення(IPS/IDS). Ці функція є частиною технології ESET NAP(Network Attack Protection), яка сканує мережевий трафік на наявність підозрілих дій і блокує їх[15].

SNORT – Це ПЗ із відкритим кодом, призначене для виявлення і захисту від різноманітних кіберзагроз. Працює як система виявлення вторгнень(IDS), система

запобігання вторгненням(IPS), система моніторингу та система логування пакетів[22].

SURICATA – це ПЗ, яке було розроблено на основі ПЗ Snort, взагалі Suricata це більш сучасна версія Snort. Основна відмінність між ними полягає в тому що в Suricata має можливість використовувати GPU для обчислень в режимі IDS і також має більш просунуту IPS. Система розрахована на багатопотоковість, тоді як Snort є продуктом однопотоковим. Завдяки цьому Suricata здатен обробляти трафік до 10 Гбіт/сек. Тому як висновок двигун Suricata працює більше швидше а ніж його попередник – Snort. Це ПЗ із відкритим кодом як і Snort, призначений для виявлення і захисту від різноманітних кіберзагроз. Працює як система виявлення вторгнень, система попередження про вторгнення, система моніторингу та система логування пакетів[21].

MCAFEE TOTAL PROTECTION – це комплексний антивірусний продукт, що надає широкий спектр функцій захисту для комп'ютера, телефонів та інших пристроїв. Має функцію McAfee Network Security Platform(NSP), яка забезпечує захист від вторгнень на рівні мережі.

2.3. Переваги та недоліки сучасних IPS

Варто розуміти що ці продукту є одними із популярними, бо вони виконують захисні функції добре. Але варто зазначити, що дійсно, в кожного продукту є свої переваги над іншими, але також є в них і свої недоліки порівнюючи з іншими, тому є дуже важливим, розглядання сильних та слабких сторін продуктів, для того щоб розуміти, коли використовувати той чи інший продукт під ту чи іншу ситуацію. Спершу варто розглянути антивірусний продукт **ESET Internet Security**.

Переваги ESET Internet Security в тому що він має велику кількість інструментів для захисту ІС, а саме**:**

-Система виявлення вторгнень(Intrusion Detection System), система запобіганню вторгнень(Intrusion Prevention System);

-Захист від фішингу, захист онлайн платежів, забезпечує захист під час відвідування веб-сайтів;

-Захист від веб-атак;

-Забезпечує захист мережі, захист вхідного, вихідного трафіку. Дана функція називається – брандмауер;

-захист від спаму;

-захист від шпигунського програмного забезпечення;

-Захист від мережевих черв'яків;

Тепер розглянемо **недоліки ESET Internet Security:**

-Відсутній VPN, програмна не має вбудованої функції віртуальної приватної мережі(VPN);

-Обмежена можливість виявляти нові види загроз, що може становити певний ризик для користувача. Нове ШПЗ може бути не поміченим антивірусом протягом певного періоду часу, поки розробники не внесуть оновлення в базу даних загроз;

-Ціна за придбання антивірусу може бути більшою ніж деякі інші антивірусні програми;

-Відсутня функція шифрування конфіденційних даних. Дана функція, дає можливість програми шифрувати дані, щоб у випадку їх втрати, дані були зашифровані і не могли використовуватися зловмисником.

Наступний ПЗ, яке ми будемо аналізувати це **SNORT**. **Переваги** даного ПЗ наступні:

-Має велику базу даних відомих загроз, тому може виявляти різні типи атак, як атаки на мережевий протокол, атаки на ПЗ, атаки на веб-додатки тощо.

-Може діяти в режимі реального часу та заблоковувати потенційно небезпечний трафік, використовуючи для цього вбудовані механізму захисту. Завдяки функції – захист в реальному часу, може забезпечувати надійний рівень захисту мережі та зменшує ризик інцидентів з безпекою.

-Snort має відкритий вихідний код, що дає змогу користувачам адаптувати та налаштовувати систему відповідно до їх вимог та потреб.

-Snort забезпечує підтримку стандартів протоколів мережі, такі як TCP/IP, HTTP, що дає змогу програмі ефективного працювати в різних мережевих середовищах.

-Дане ПЗ, містить велику кількість правил, які дозволяють розпізнавати відомі загрози для безпеки мережі, такі як атаки типу DDoS/DoS, SQL-ін’єкції, атаки типу buffer, overflow;

-Здатен генерувати повідомлення про виявлені загрози, що дозволяє адміністраторам системи або операторам мережі знати про потенційні проблеми з безпекою;

-Є сувмісним з іншими антивірусними продуктами.

З **недоліків** даного ПЗ варто зазначити наступне:

-Встановлення та налаштування Snort може викликати труднощі. Тому до недоліку варто віднести складність встановлення та налаштування.

-Висока кількість помилкових спрацювань. При налаштування правил IPS, які визначають, який трафік повинен бути блокований, можуть спрацювати помилково, блокуючи законний трафік.

-Вимогливий до ресурсів системи, особливо під час обробки великої кількості трафіку.

-Не має офіційної технічної підтримки, бо є відкритим ПЗ із відкритим кодом.

-Snort на відмінно від свого наступника Suricata, є однопотоковим, завдяки чому двигун Snort працює повільніше і здатен обробляти менший трафік в порівнянні з Suricata.

Наступний продукт, який буде розглядатися – **SURICATA**. **Переваги** його наступні:

Як згадувалося вище, Suricata схожа на минулий продукт Snort, але є більш швидшим. Suricata має можливість використовувати GPU для обчислень в режимі IDS і має більш просунуту IPS в порівняні зі своїм попередником. Система розрахована на багатопотоковість. Завдяки цьому Suricata здатен обробляти трафік до 10 Гбіт/сек. Тому двигун Suricata працює більше швидше ніж його попередник – Snort. Тому першою перевагою буде:

-Висока швидкість. Suricata є одним з найшвидших IPS антивірусів. Може обробляти трафік зі швидкість 10 Гбіт/с;

-Наявність функцій, як виявлення вторгнень на основі зразків, має здатність обробляти кілька типів трафіку одночасно і також може аналізувати SSL-трафік;

-Suricata також є відкритим ПЗ із відкритим кодом, що дає змогу користувачам налаштувати дане ПЗ під свої потреби;

-Є сувмісним з іншими антивірусними продуктами.

До **недоліків** варто віднести наступні пункти:

-Складність встановлення та налаштування;

-Може мати проблеми з сумісністю з деякими мережевими адаптерами та операційними системами;

-Suricata, має обмежені можливості порівняно з іншими IPS антивірусами, такими як McAfee, бо в нього відсутні наступні функції: захист від шкідливих програм на рівні кінцевих точок та веб-захист.

Останній продукт, який розглянемо – **MCAFEE TOTAL PROTECTION.** З **переваг** варто згадати наступні пункти:

-Програма забезпечує комплексний захист від вірусів, троянів, шпигунських ПЗ, рекламного ПЗ тощо;

-Має можливість виявляти та блокувати атаки в реальному часі;

-Функція IPS(система запобіганню вторгнення) дозволяє захистити комп’ютер від шкідливих атак з мережі Інтернет, від DoS/DDoS-атак тощо;

-Простий та зручний інтерфейс, що дозволяє користувачам швидко налаштувати систему під свої потреби.

Недоліки:

-Висока вартість, в порівняні із деякими антивірусами, даний продукт є досить дорогим рішенням;

-Неприємна реклама, користувачі даним ПЗ, повідомляють про показ неприємної реклами та рекомендацій;

-Під час роботи з ПЗ, можуть виникнути проблеми із продуктивністю.

Згідно огляду декількох антивірусних продуктів, можна зробити висновок, що в кожному продукті є свої переваги, недоліки. Але недоліки можна компенсувати використанням додаткового ПЗ, як приклад, Suricata чи Snort можуть бути сумісними з продуктами як ESET Internet Security або McAfee Total Security. При правильному налаштуванні, можна забезпечити своєму підприємству надійний захист, захистивши мережу підприємства, вхідний, вихідний трафік, захистившись від фішингу, троянських ПЗ, шпигунських ПЗ, мережевих черв'яків, мережевих атак, як DoS/DDoS-атак, а також захист під час перебуванні в Інтернеті та здійснень онлайн платежів і шифрування даних, що дає змогу захистити дані і створити труднощі зловмисникам у випадку їх викрадення. Таким чином завдяки такому комплексному рішенню можна значно зменшити ризики безпеки підприємства та захистити конфіденційну інформацію підприємства, працівників, клієнтів тощо. Що дає змогу бізнесу більш впевнено себе почувати станом на сьогодні, коли кількість кіберзлочинів, мережевих атак, кількість ШПЗ продовжує збільшуватися.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ПРОТИДІЇ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ ЗА ДОПОМОГОЮ SURICATA

3.1. Розгортання та налаштування програмного забезпечення Suricata

Під час проведення дослідження, використовувалося операційна система Ubuntu на віртуальній машині. Suricata є одним із популярних рішень для захисту мережевого трафіку підприємства, так як підприємство може мати справу з великими кількостями даних, а Suricata здатна обробляти дані до 10 ГБіт/с, тому варто розібратися як встановити, налаштувати Suricata для виявлення вторгнень та захисту від вторгнень, перевірити на практиці як працює Suricata і переконатися в правильності налаштування його. Перш за все треба інсталювати дане ПЗ, для цього потрібно буде додати інформацію про сховище ПЗ Open Information Security Foundation(OISF) до системи Ubuntu. Тому для того щоб це зробити, варто ввести в терміналі Ubuntu наступну команду на рис.3.1.:

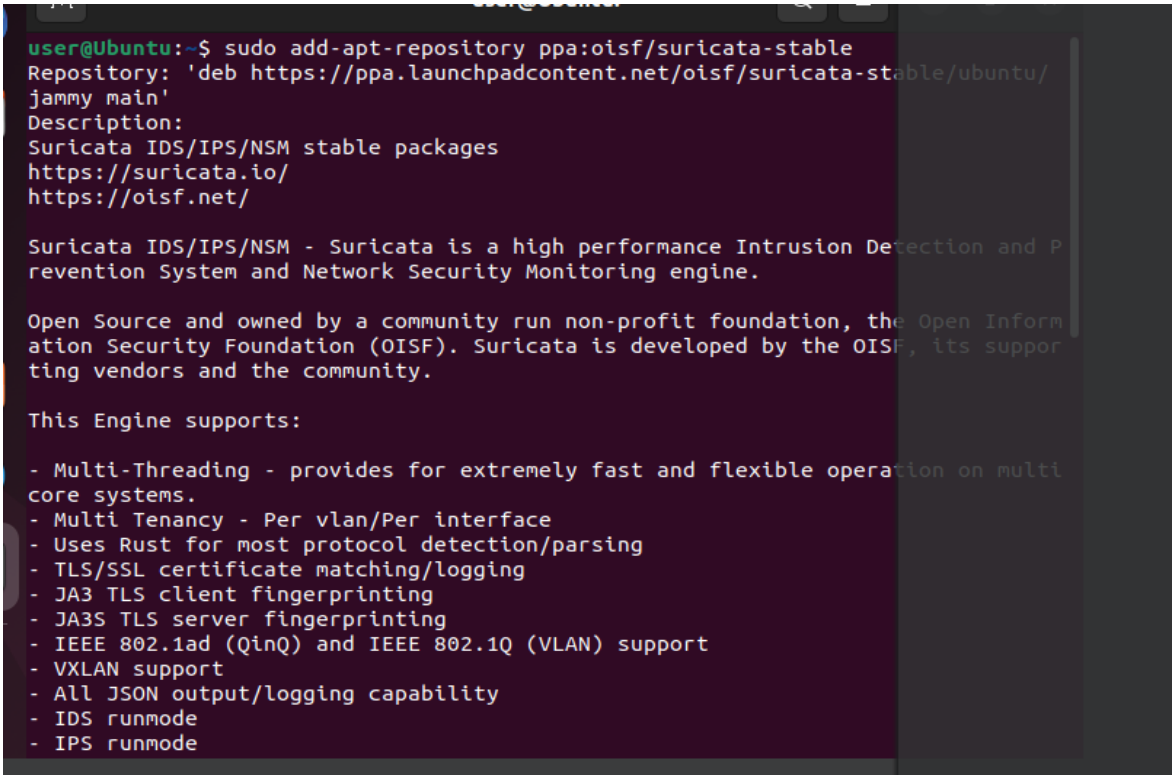


Рис.3.1. Перша команда

Наведена вище команда додає репозиторій до системи та оновлює список доступних пакетів. Далі вводимо наступну команду щоб інсталювати Suricata на рис.3.2.

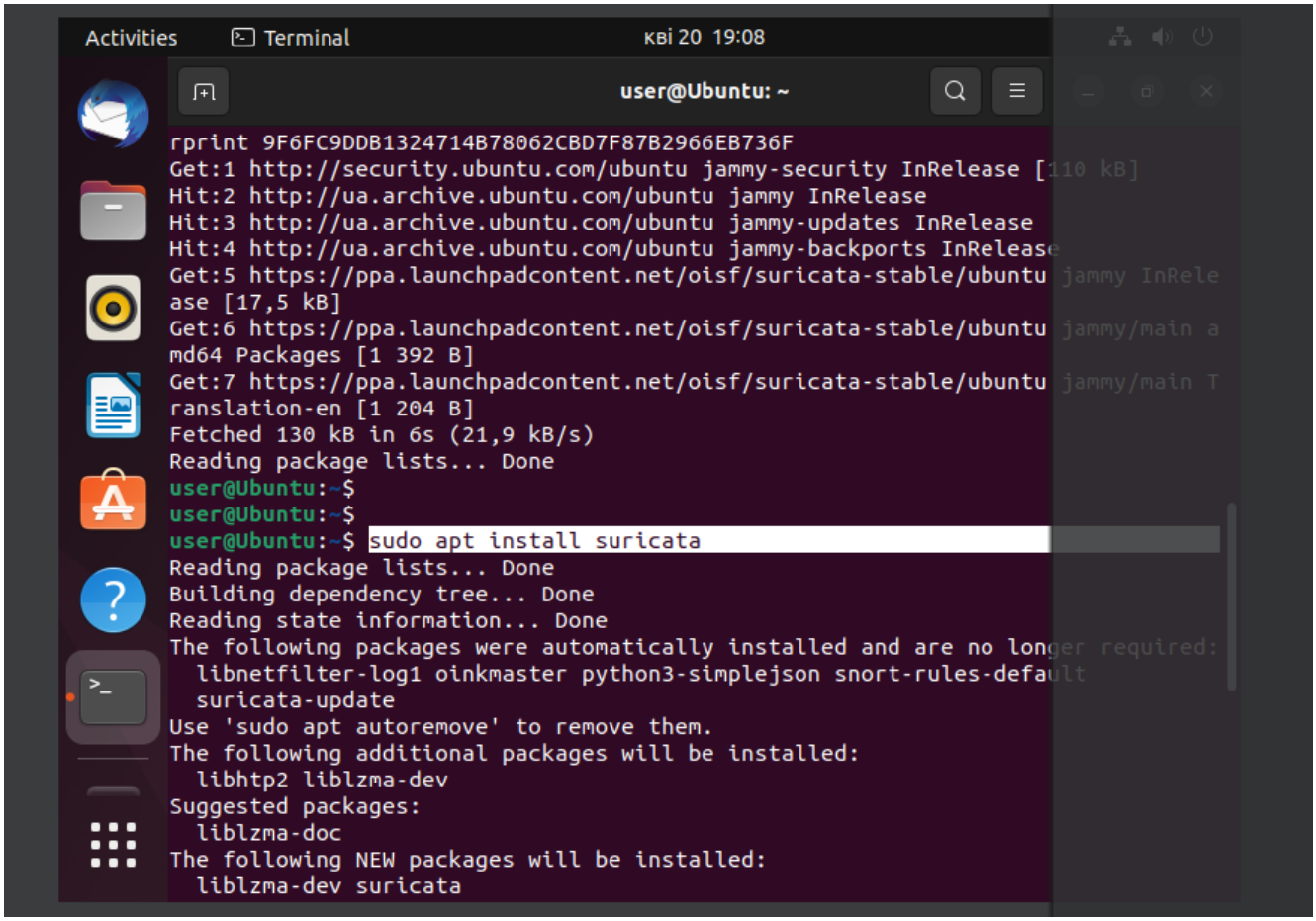


Рис.3.2. Інсталювання Suricata на Ubuntu

Після успішного інсталювання, треба зробити так, щоб після перезавантаження системи, запускалося ПЗ Suricata для цього треба ввести наступну команду на рис.3.3.:

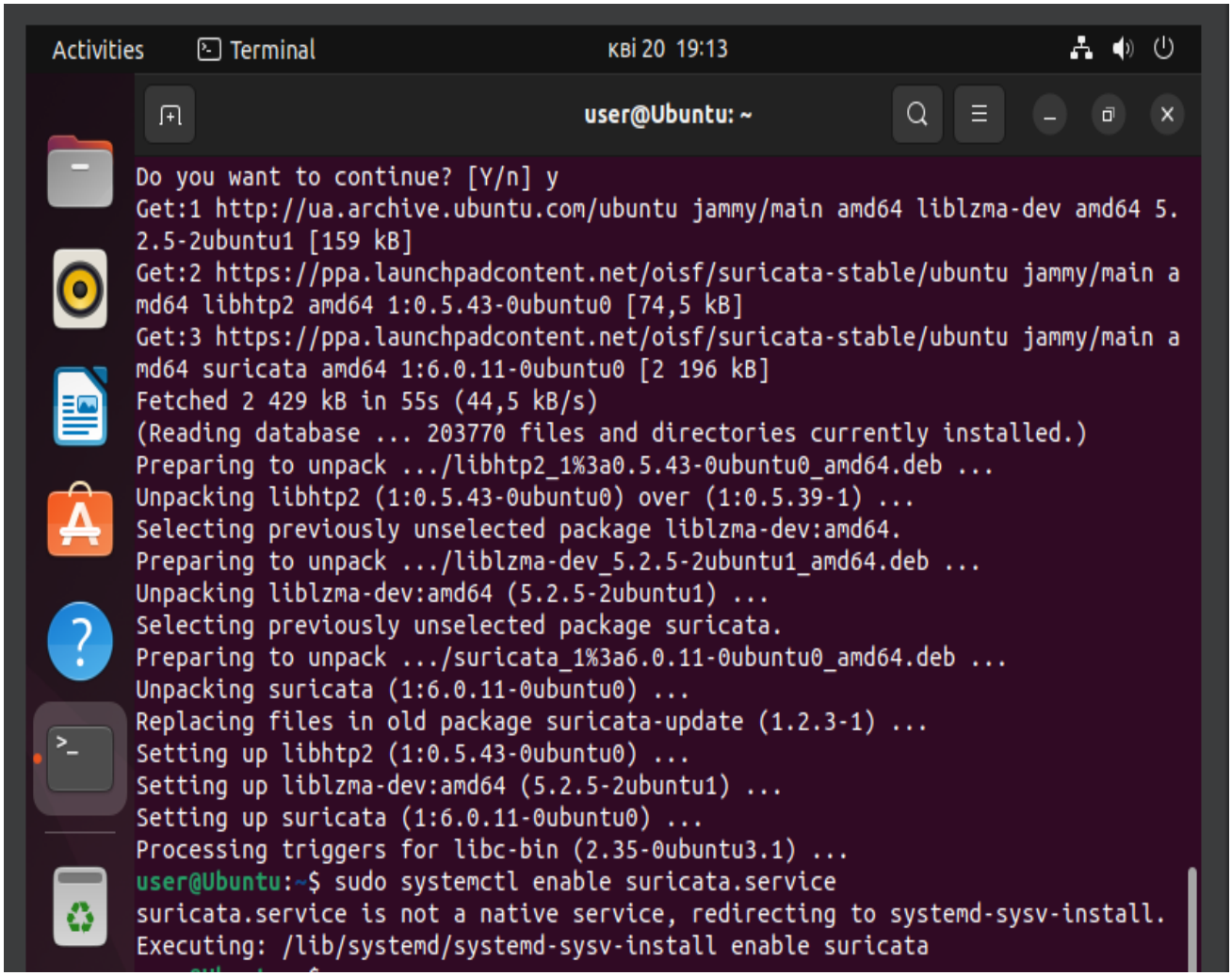


Рис.3.3. Дане повідомлення вказує на те, що службу ввімкнено

Наступне, що варто зробити це зупинити дану службу. Це варто зробити, тому що зупинка Suricata гарантує, що під час тестування та редагування файлу конфігурації(suricata.yaml) будь-які внесені зміни будуть перевірені та завантажені під час повторного запуску Suricata. Зупинити службу можна наступною командною на рис.3.4.

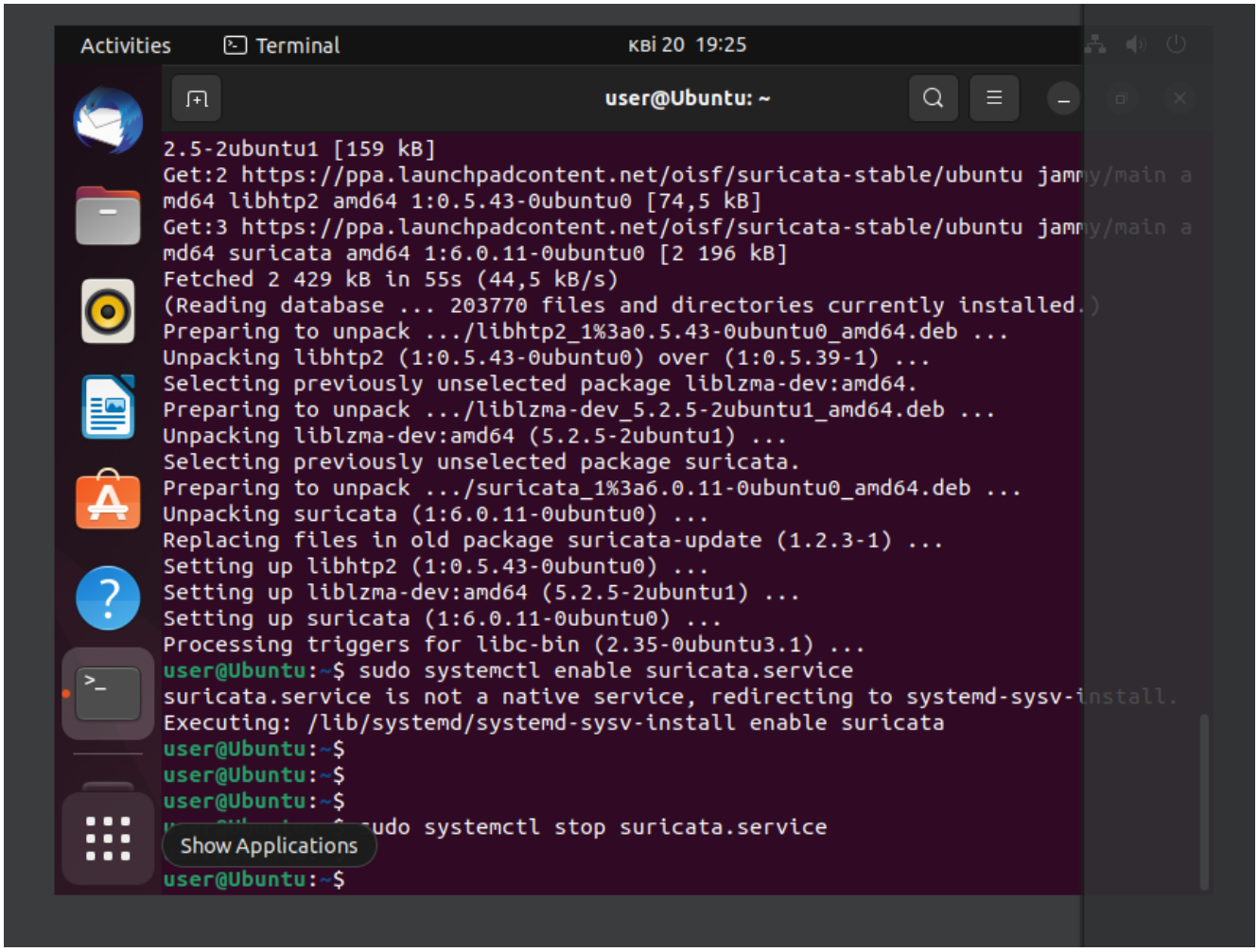


Рис.3.4. Вимкнення служби

Наступним кроком в налаштуванні ПЗ Suricata буде, визначення мережевого інтерфейсу. Але перед тим як перейти вже до практики варто розібратися що взагалі означає термін мережевий інтерфейс. Мережевий інтерфейс - це, мережевий адаптер, наприклад як Wi-Fi чи Ethernet через який Suricata отримує доступ до мережі для моніторингу трафіку та виявлення загроз.

Тепер коли відомо, що означає мережевий інтерфейс, варто спочатку дізнатися назву пристрою для мережевого інтерфейсу, який стоїть за замовчування. . Для цього треба написати наступну команду на рис.3.5.

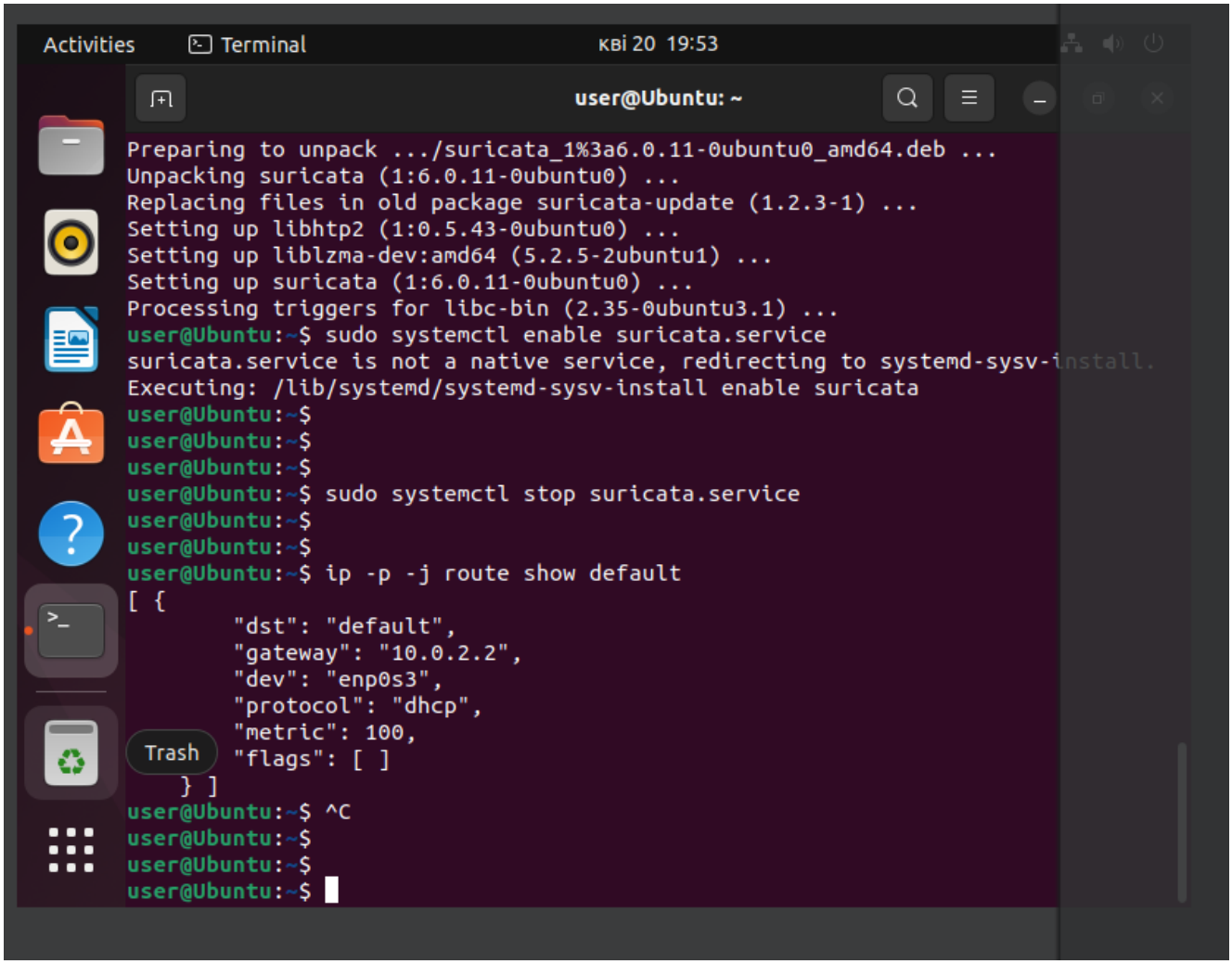


Рис.3.5. Назва мережевого інтерфейсу за замовчуванням

Рядок де написано «”dev” : “enp0s3”», вказано назву пристрою, який стоїть за замовчуванням. Бувають випадки коли, у вашого пристрою стоїть інша назва чим це записано в файлі конфігурації Suricata, там вона може бути стояти за замовчуванням як «eth0», як на рис.3.1.6.1. Тому щоб змінити ім’я на те, яке потрібно, треба зайти в файл конфігурації Suricata і там змінити ім’я і/або додати новий мережевий інтерфейс у випадку коли треба щоб Suricata перевіряв трафік відразу на кількох інтерфейсах. Тому щоб це виконати варто ввести наступні команди на рис.3.6.

```
user@Ubuntu:~$ sudo nano /etc/suricata/suricata.yaml
[sudo] password for user:
user@Ubuntu:~$
```

Рис.3.6. Команда для того щоб увійти в файл конфігурації Suricata

```
af-packet:
  - interface: eth0
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
    # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or p
    # This is only supported for Linux kernel > 3.1
    # possible value are:
    #  * cluster_flow: all packets of a given flow are sent to the same socket
    #  * cluster_cpu: all packets treated in kernel by a CPU are sent to the s
    #  * cluster_qm: all packets linked by network card to a RSS queue are sen
```

Рис.3.7. Назва «eth0» за замовчуванням мережевого інтерфейсу

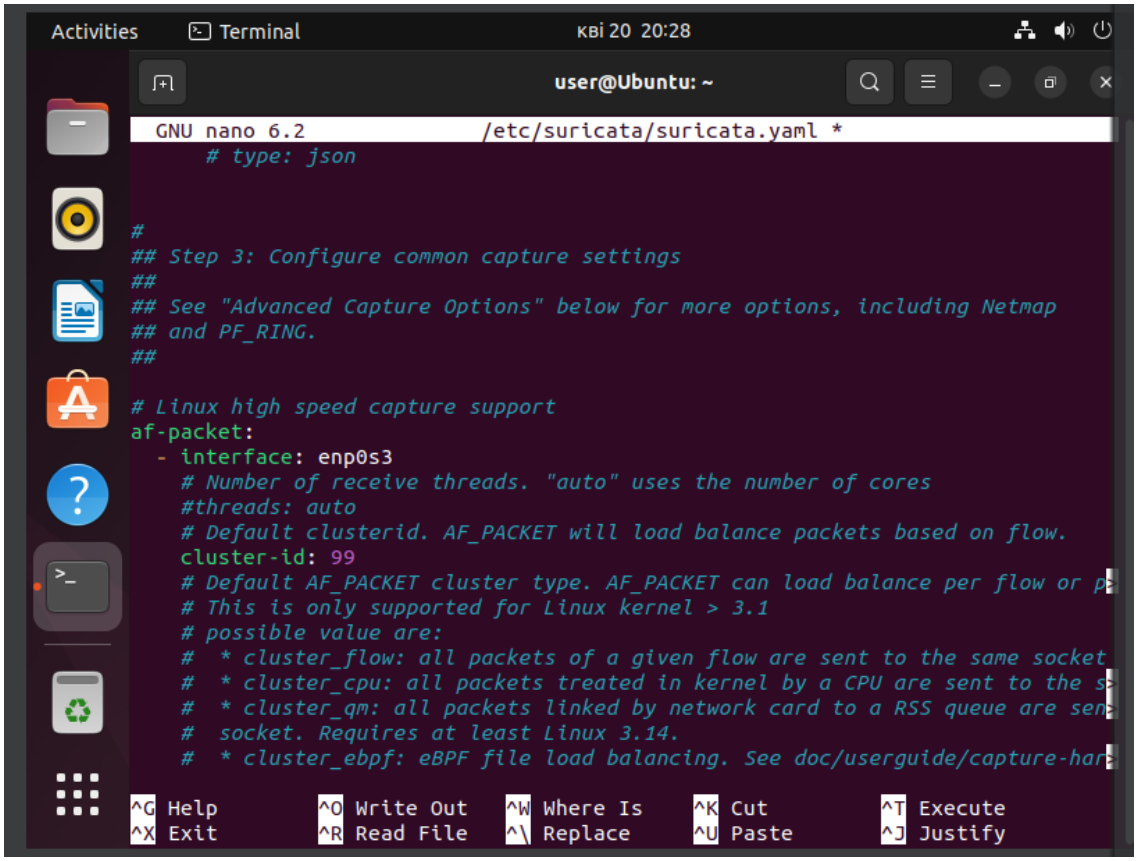


Рис.3.8. Змінюємо на назву пристрою «enp0s3», який Suricata буде перевіряти трафік

Щоб додати додатковий мережевий інтерфейс, треба спочатку знайти рядок де на писано «interface: default» і над ним писати додаткові мережеві інтерфейси рис.3.9.

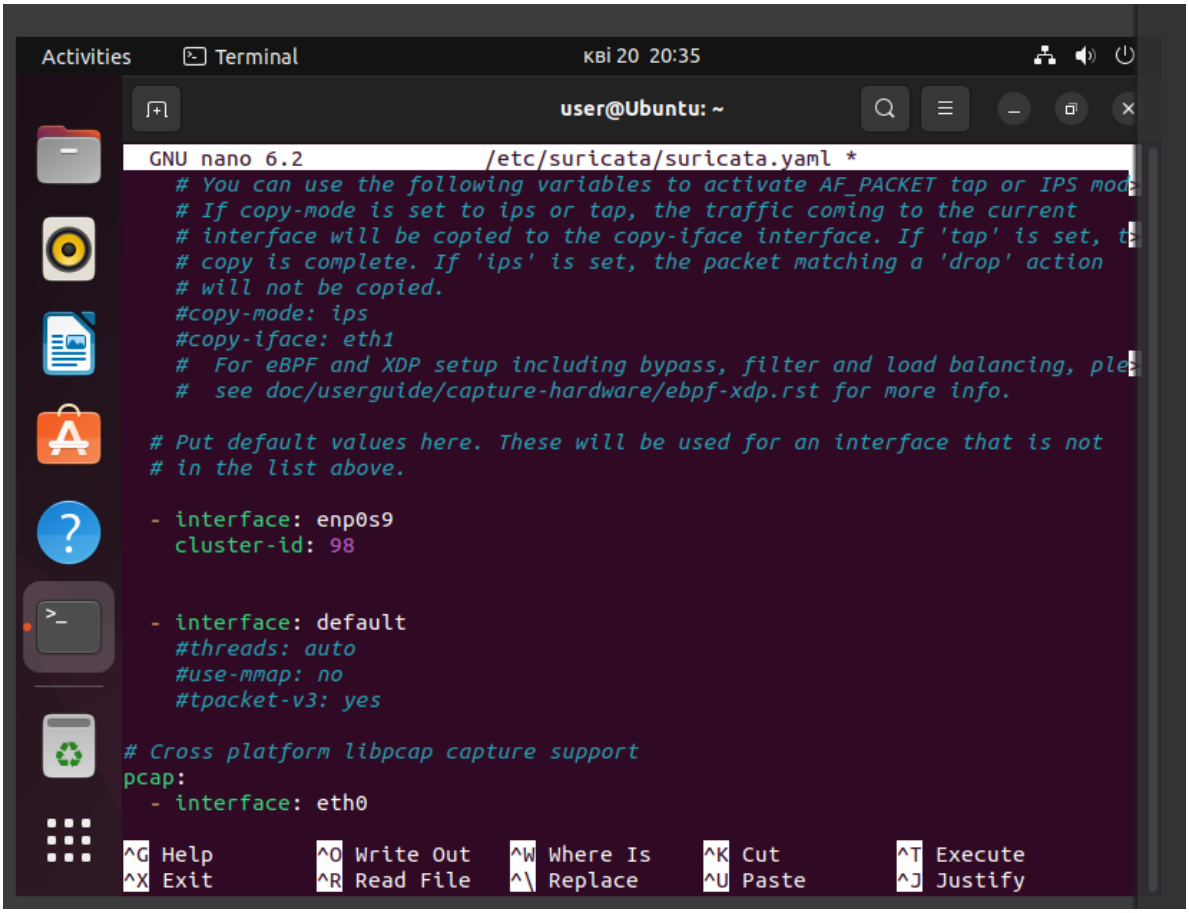


Рис.3.9. Додавання нового мережевого інтерфейсу

Наступне треба налаштувати перезавантаження живих правил. Suricata підтримує живе перезавантаження правил, це означає, що можна додавати, редагувати чи видаляти правила без необхідності перезапуску Suricata рис.3.10.

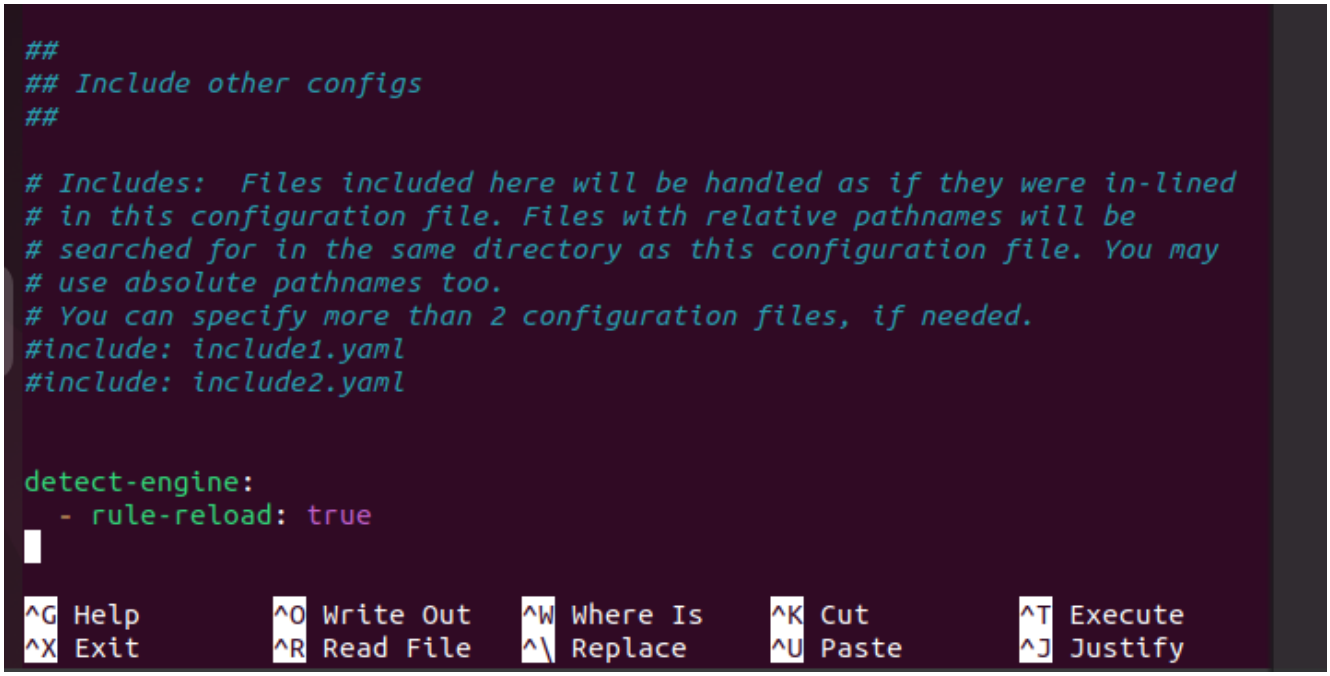


Рис.3.10. Ввімкнення функції перезавантаження живих правил

За замовчуванням пакет Suricata на даному може виявити лише обмежену кількість поганого трафіку. Використовуючи наступну команду можна завантажити набори правил від зовнішніх постачальників рис.3.11.

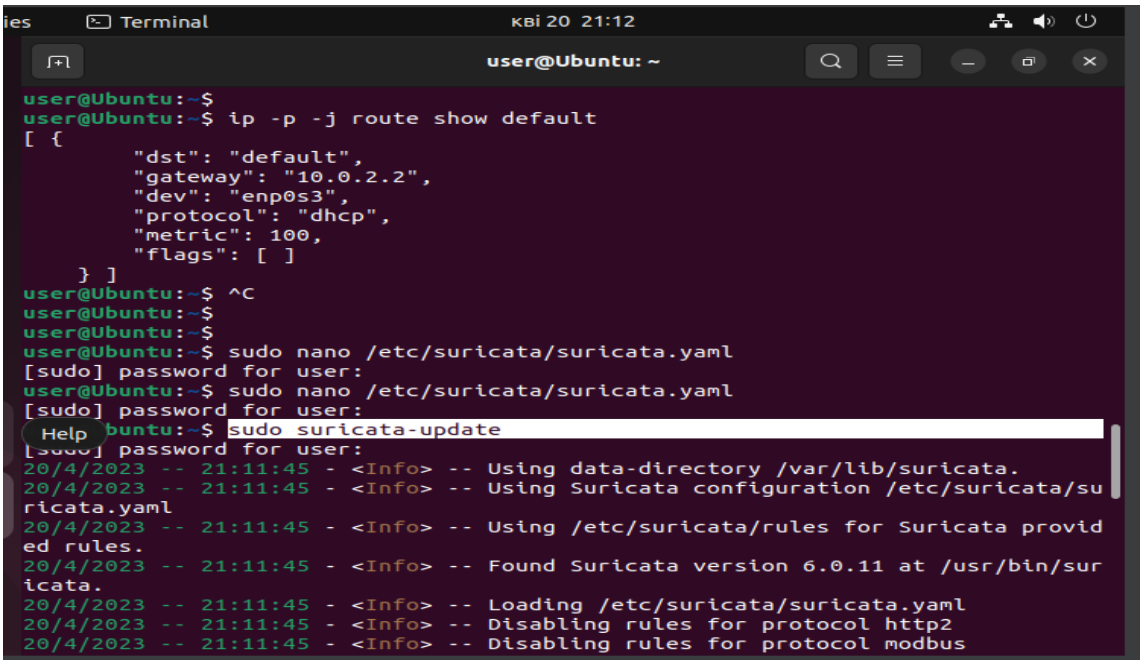


Рис.3.11. Команда для інсталювання безкоштовних правил від зовнішніх постачальників

Як бачимо, загальна кількість правил встановлено 41849, а увімкнено 33432 на рис.3.12.

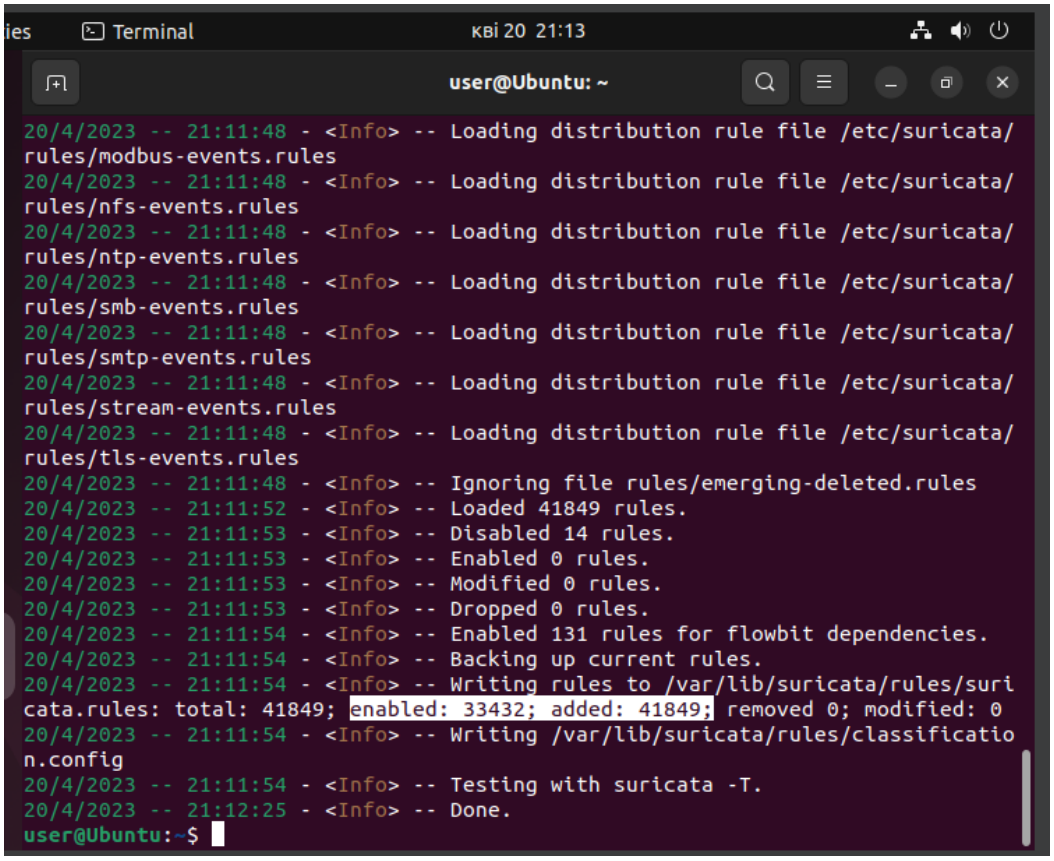


Рис.3.12. Загальна кількість установлених і увімкнених правил

Наступною командою можна переглянути кількість різних джерел, з яких було інстальовано набори правил на рис.3.13.

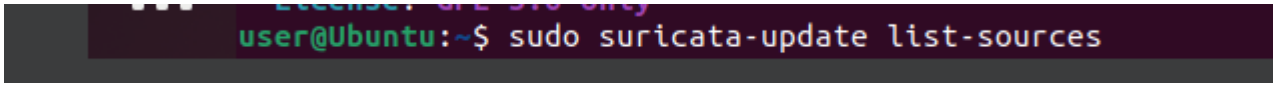


Рис.3.13. Перевірка джерел звідки було інстальовано набори правил

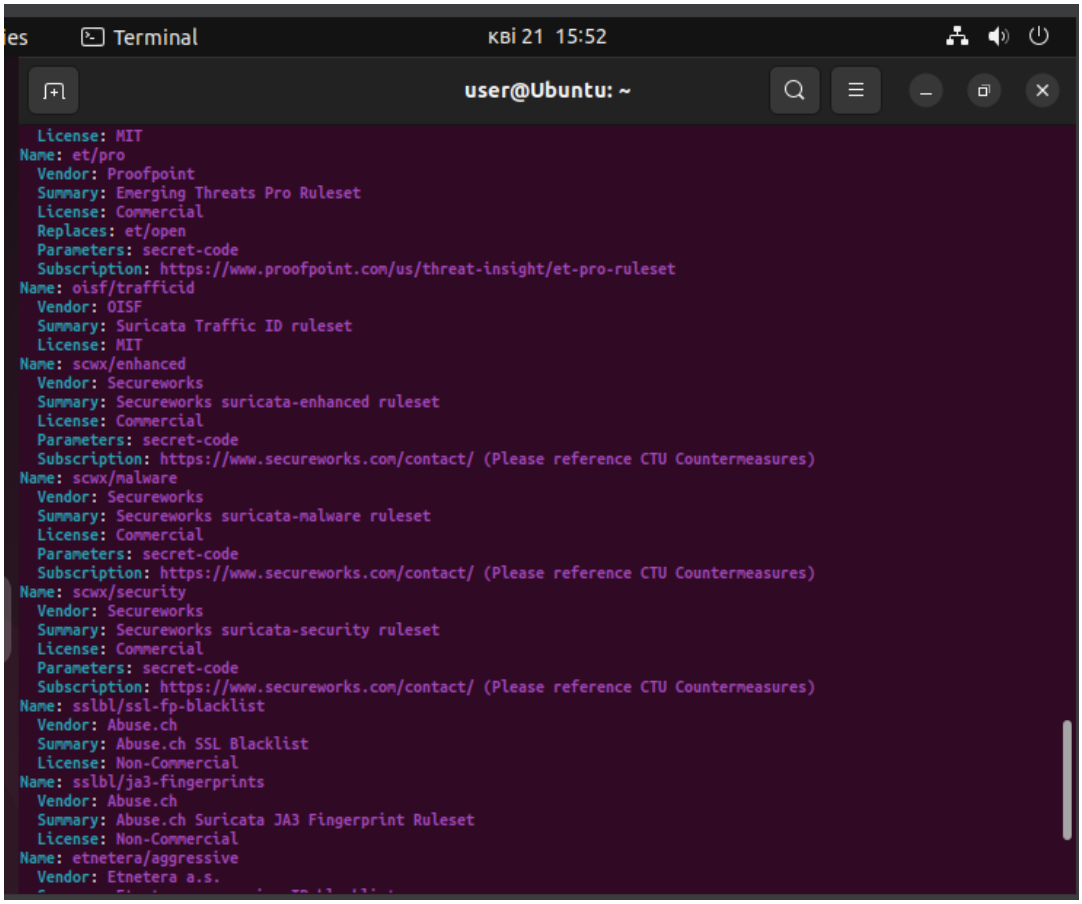


Рис.3.14. Список джерел звідки було встановлено правила

Тепер коли вказано мережевий інтерфейс за замовчуванням, ввімкнуто перезавантаження правил в реальному часі, інстальовано безкоштовні набори правил, варто було б ще перевірити конфігурації Suricata. Suricata має вбудований тестовий режим, який може перевірити всі включені правила на дійсність, щоб переконатися, що помилково не було додано правила, яких не існує. Тому для цього варто ввести наступну команду, як на рис.3.15.

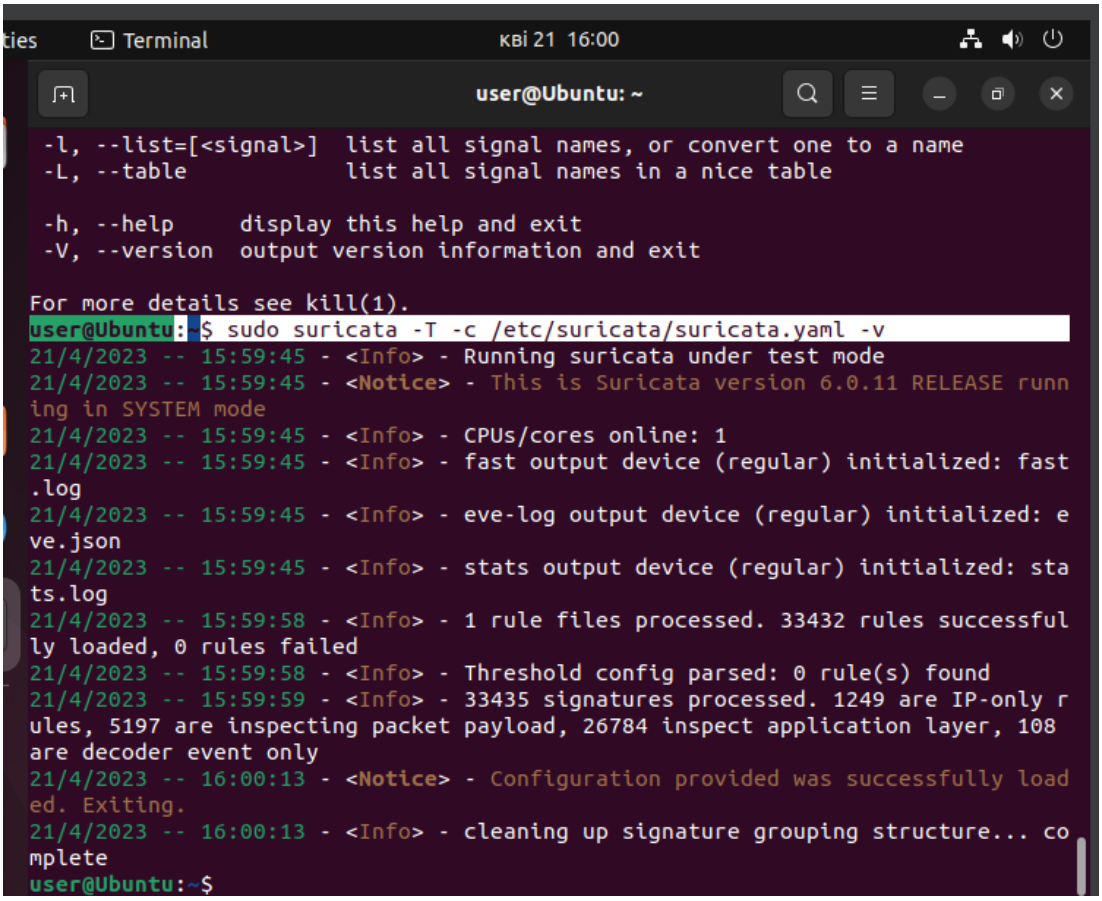


Рис.3.15. Запуск Suricata в тестовому режимі для перевірки його конфігурації на наявність несправностей

Тепер коли ми все налаштували, можна запустити Suricata, для цього потрібно вести наступну команду, як на рис.3.16

```
user@Ubuntu:~$ sudo systemctl start suricata.service
[sudo] password for user:
user@Ubuntu:~$
```

Рис.3.16. Запуск Suricata

Тепер коли в нас Suricata вже запущений, варто перевірити, його в дії. Тому спеціально для цього, створимо запит HTTP, який поверне відповідь, що відповідає правилу сповіщень Suricata на рис.3.17.

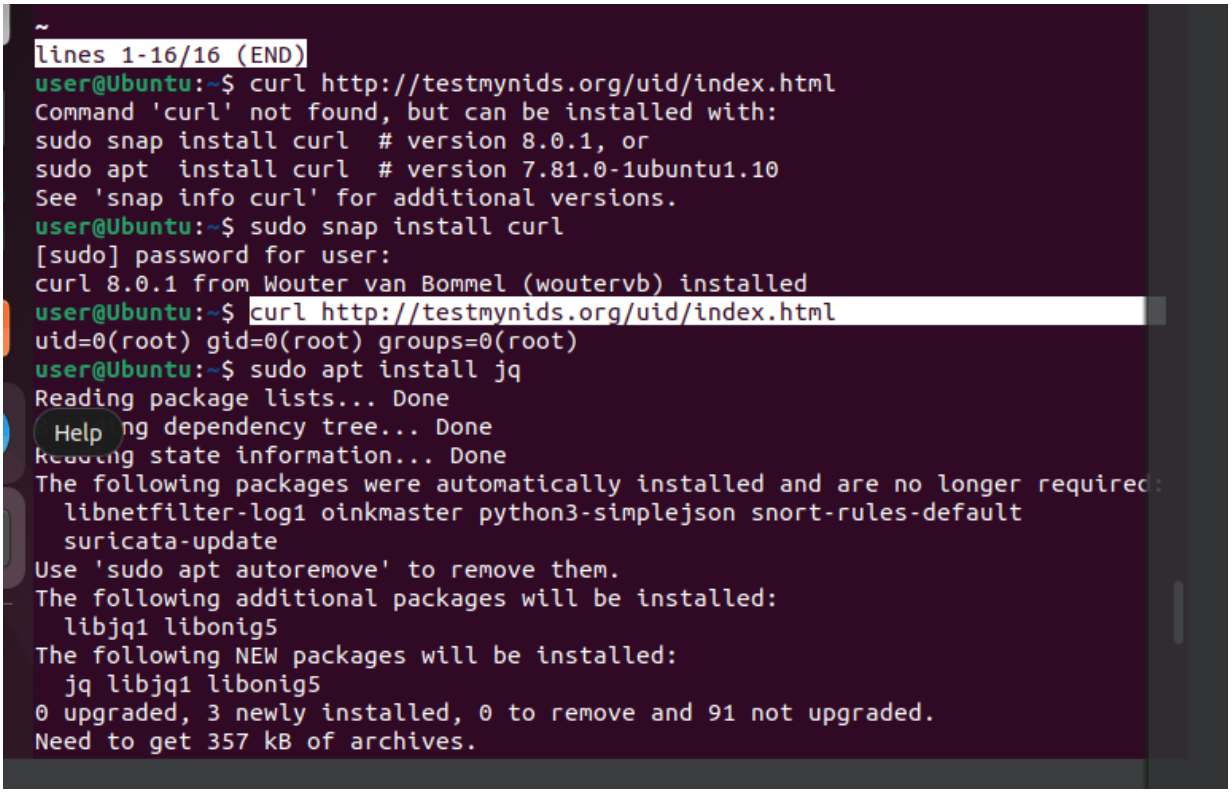


Рис.3.17. Створення запиту

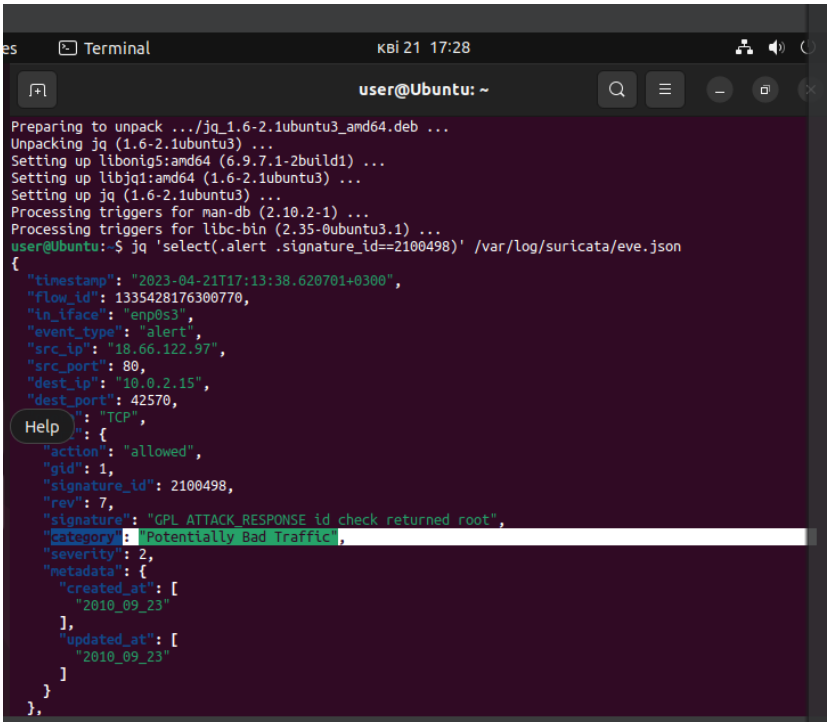


Рис.3.18. Suricata присвоїв категорію даному HTTP запиту як потенційно поганий трафік

Як бачимо на попередньому рисунку, Suricata працює, і виявив, що це небезпечний трафік, але не зважаючи, що він знає, що це поганий трафік, все рівно, він його пропустив. Це сталося, тому що Suricata за замовчуванням працює в режимі IDS, тобто, він виявляє потенційно небезпечний трафік, але на цьому більше нічого, крім попередження про небезпеку, не робить. Всього Suricata має 4 варіанти роботи.

Перший варіант роботи називається «Alert», в такому режимі зараз працює наша система. Тобто, при виявлені шкідливого трафіку, Suricata попереджає про небезпеку в лог, але крім цього нічого більше не робить.

Наступний, другий варіант роботи, називається «Drop», коли Suricata працює в такому режимі, то весь шкідливий трафік буде заблоковано і буде створено сповіщення щодо цієї події в лог.

Третій варіант, «Allow/Pass», коли Suricata виконує дану дію, це означає, що вона припинить сканування пакету та дозволить його, при цьому не згенерувавши сповіщення в лог.

І останній, варіант дій це «Reject», коли Suricata виконує цю дію, вона знищує шкідливий пакет і повідомить про це відправника про дану подію.

Тому, наступним кроком буде зробити так щоб Suricata не тільки виявляла шкідливий трафік, а і блокував його, тому щоб це зробити, потрібно змінити режим роботи Suricata із IDS в IPS. Щоб це зробити, слід виконати наступні кроки:

По-перше, треба знайти загальнодоступні IP-адреси вашого сервера. Для цього треба використати наступну команду, як на рис.3.19.

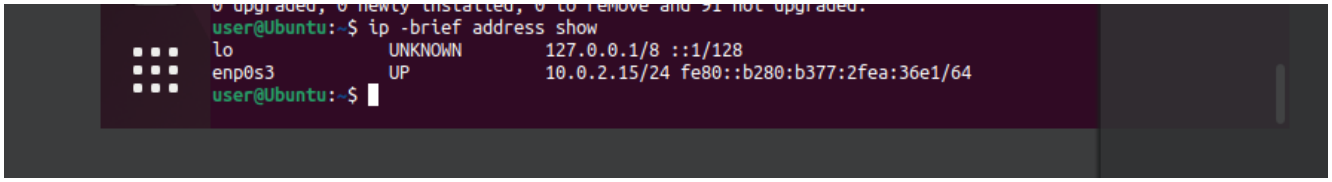


Рис.3.19. Перегляд загальнодоступних IP-адрес сервера

Назва потрібного пристрою «enp0s3», тому використовуватимемо саме його IP-адресу. Тепер для перевірки роботи варто створити спеціальний підпис для сканування трафіку SSH до портів, які не є SSH і напишемо підпис до файлу local.rules.

Рис.3.20. Відкривання файлу local.rules для додавання власних підписів

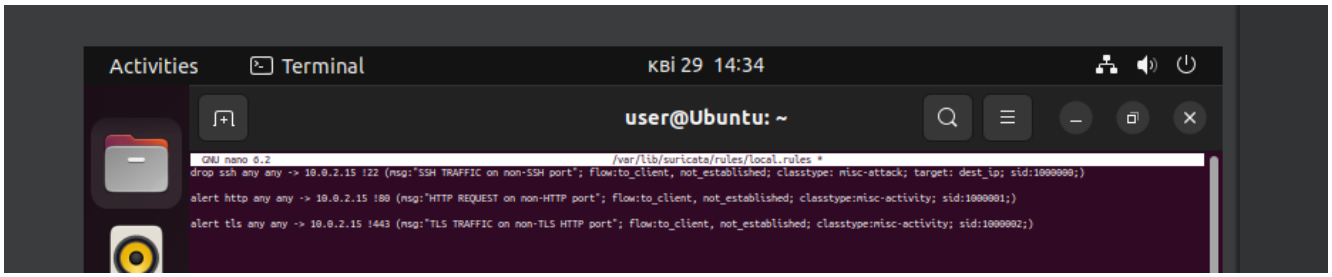


Рис.3.21. Написання власних підписів

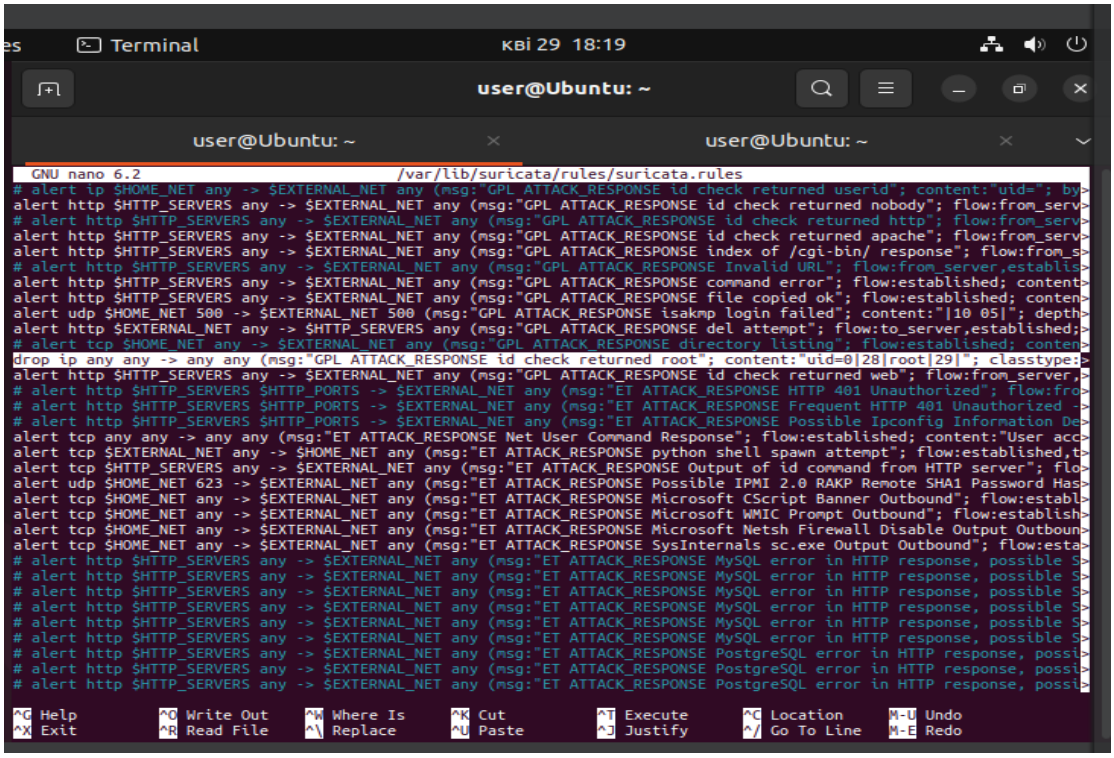


Рис.3.22. Зміна існуючого підпису із режиму «alert» в «drop»

Варто звернути увагу на те, що тепер згідно першому підпису, Suricata буде діяти в режимі «Drop», тобто в режимі IPS, але вона ще не працює в даному режимі, для того щоб Suricata перейшла в цей режим варто зробити наступне.

Переходимо в файл «/etc/default/suricata» для зміни режиму роботи Suricata.

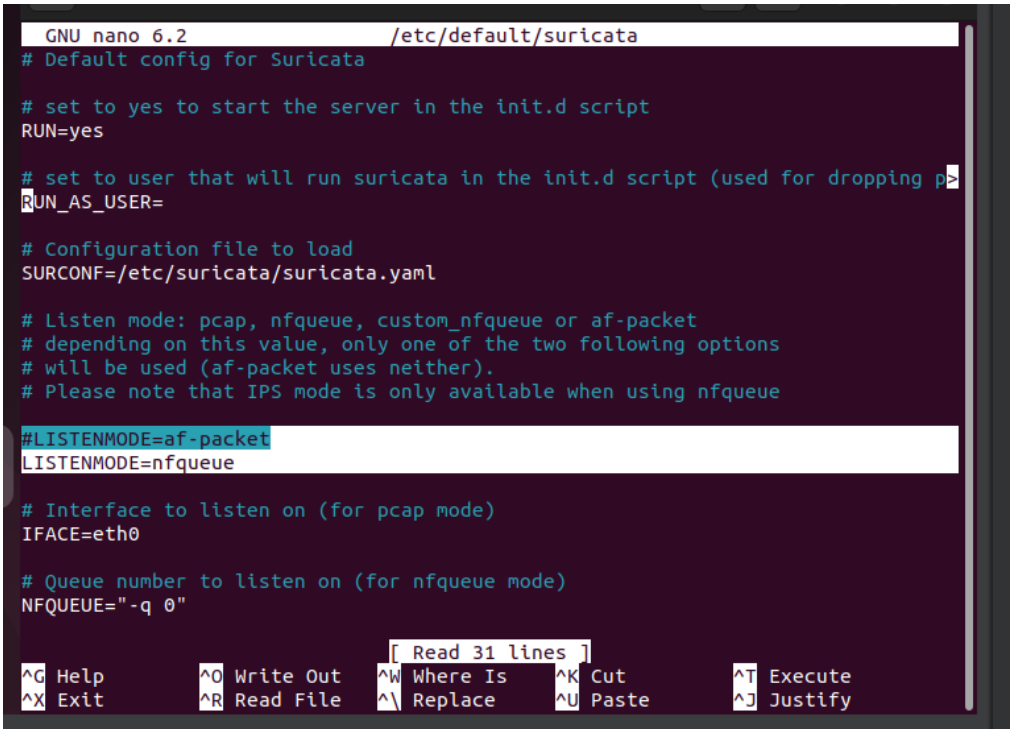


Рис.3.23. Зміна режиму Suricata із IDS в IPS

Рядок, «#LISTENMODE=af-packet» означає, що Suricata раніше працювала в режимі IDS, а наступний рядок «LISTENMODE=nfqueue» означає, що ми вказуємо Suricata працювати в режимі IPS. Після цього варто перезавантажити Suricata і після перезавантаження – перевірити його статус.

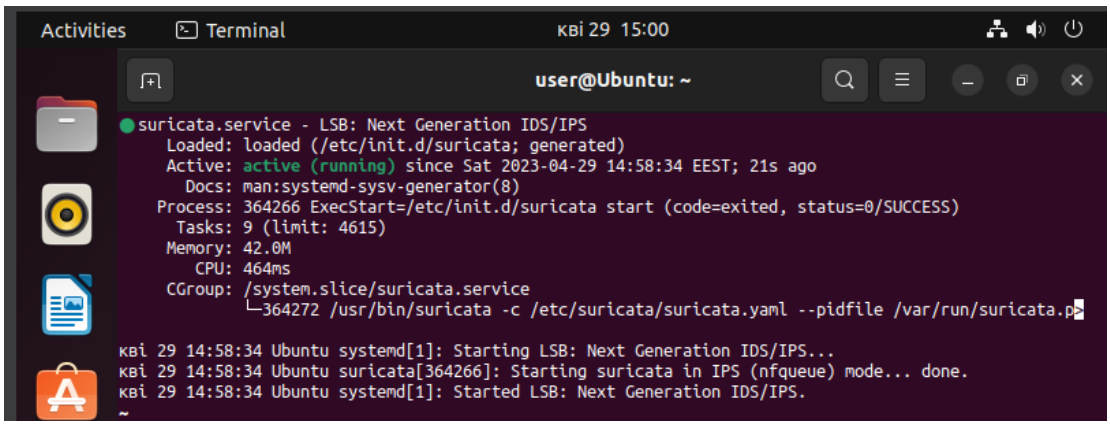


Рис.3.24. Suricata запускається в IPS режимі

Після успішного налаштування Suricata для обробки трафіку в режимі IPS, наступним кроком буде спрямування вхідних пакетів до Suricata. Для цього переходимо в файл «/etc/ufw/before.rules» і пишемо наступне, як на рис.3.25.

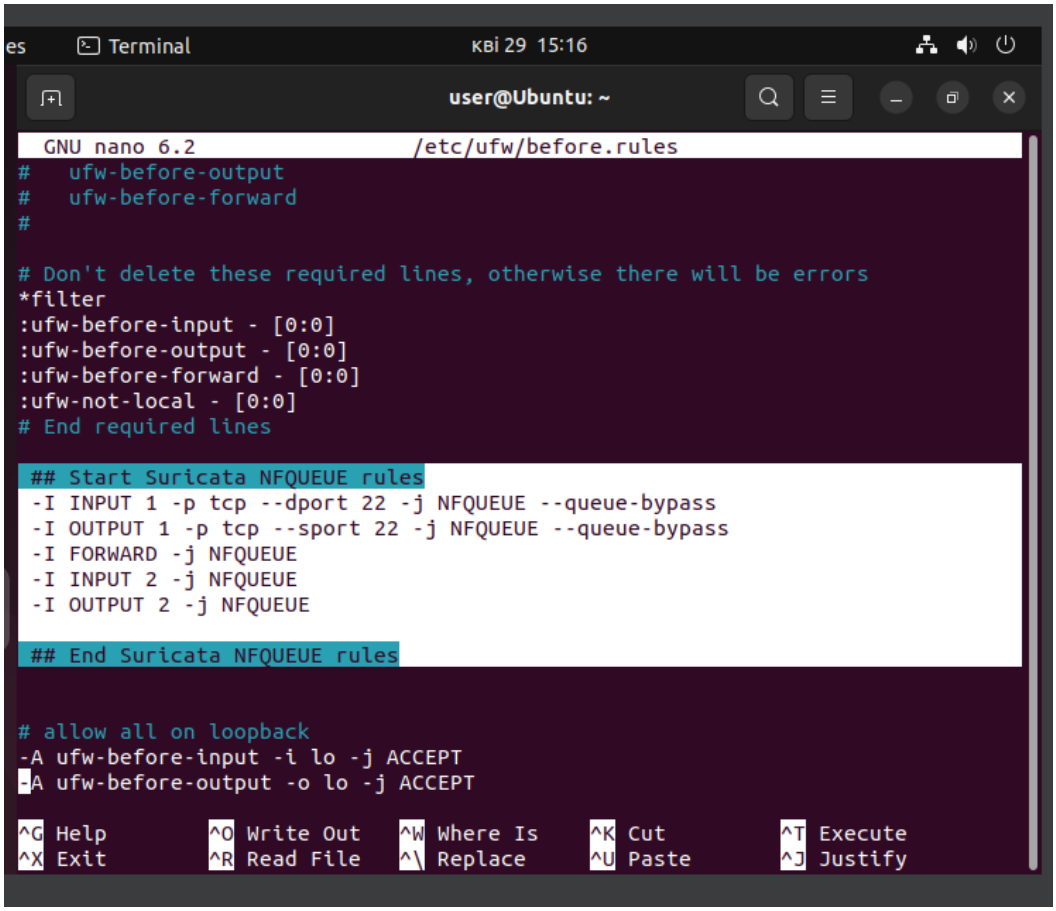


Рис.3.25. Спрямування вхідних пакетів до Suricata

Перші два правила INPUT, OUTPUT використовуються для обходу Suricata, вони треба для того щоб працівники підприємства могли підключитися до свого сервера за допомогою SSH. Якщо не використовувати ці два правила, то неправильний або надто широкий підпис може заблокувати працівникові доступ SSH. Наступне правило FORWARD, гарантує, що якщо ваш сервер діє як шлюз для інших систем, то увесь трафік також надходитиме до Suricata для обробки. Щодо останніх двох правил INPUT,OUTPUT, то коли ми їх прописуємо це, то весь залишок трафіку, який не є трафіком SSH, надсилається до Suricata для обробки.

3.2. Дослідження ефективності протидії вторгненням в інформаційну систему підприємства програмного забезпечення Suricata

Suricata показав, що здатен ефективно виявляти шкідливий трафік в режимі IDS, раніше вже було проведено успішне тестування роботи програми, і робили HTTP запит як на рис.3.26.

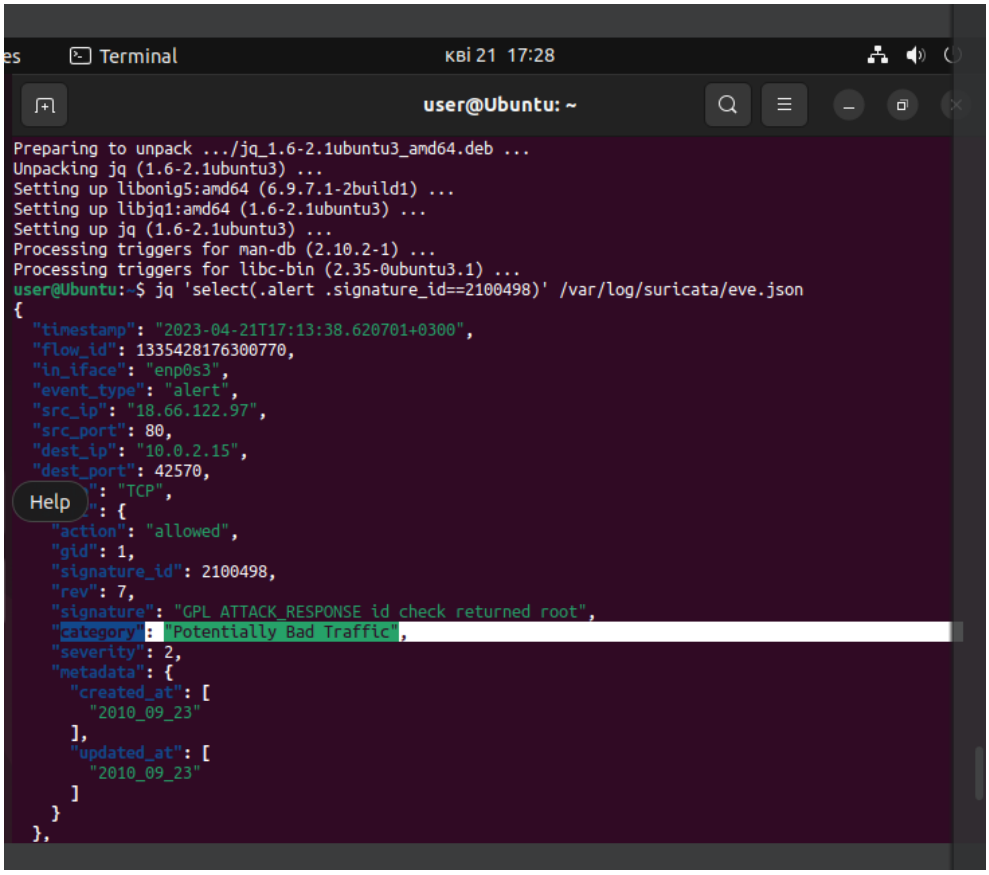


Рис.3.26. Успішне виявлення Suricata шкідливого трафіку в режимі IDS

Так як Suricata почала працювати в режимі IPS, варто перевірити її також в дії чи все працює коректно. Тому наступне, що варто зробити це зробити HTTP запит, використовуючи для цього приклад для теста роботи Suricata, яка є в документації, він потрібен для перевірки коректності роботи програми. Вводимо наступну команду «curl --max-time 5 http://testmynids.org/uid/index.html».

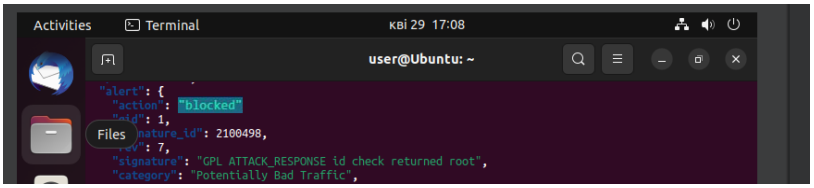


Рис.3.27. Suricata успішно працює в режимі IPS

Як бачимо в рядку action видно, що Suricata успішно відхилив тестовий запит HTTP, це означає, що тепер якщо підпис буде збігатися, програма блокуватиме потенційно небезпечний трафік.

3.3. Рекомендації щодо застосування Suricata для ефективної протидії вторгненням в інформаційну систему підприємства

Як видно, Suricata працює успішно і ефективно, виявляючи шкідливий трафік в режимі IDS та відхиляючи запит в режимі IPS. Але варто розуміти, що при не коректному налаштуванні, Suricata може пропустити шкідливий трафік, що для підприємства, будь якого розміру, може бути небезпечно, так як це може мати серйозні наслідки, як втрата, зміна цінних даних або втрата доступу клієнтів до веб ресурсу підприємства. Тому щоб Suricata працював ефективно і надійно, виявляв та блокував шкідливий трафік, слід дотримуватися наступних рекомендацій:

1. Після інсталювання Suricata, слід використати команду «suricata-update» та завантажити набори правил від зовнішніх постачальників. Це завантажить всі правила, які є безкоштовними, на даний час, їх кількість 41849, вони знаходитимуться в папці «suricata.rules».

2. Не варто перетворювати кожний підпис на drop, reject, бо є ризик заблокувати законний доступ до мережі чи серверів. Замість цього, якщо є необхідність, то в файлі local.rules можна додати власні правила, як вже було показано вище на рис.3.1.17.1. І в файлу конфігурації Suricata suricata.yaml перейти на рядок 1879 і знайти рядок «rule-files:» і додати під текстом «suricate.rules» наступний текст «local.rules». Таким чином Suricata буде використовувати правила, які були завантажені від зовнішніх джерел так і власні правила. Під час роботи в

режимі IPS Suricata продовжуватиме сповіщувати в лог-файл про підозрілий трафік. Хай пройде кілька днів або тижнів сповіщень, після чого можна проаналізувати їх і обрати відповідні правила для перетворення на reject чи drop.

3. Після редагування файлу конфігурації Suricata потрібно перезапустити Suricata за допомогою sudo systemctl restart suricata.service і потім перевірити статус Suricata за допомогою sudo systemctl status suricata.service.

4. Після додавання чи зміни ідентифікатора спільноти, вказання мережевого інтерфейсу за замовчуванням чи зміна його або увімкнення перезавантаження правил в реальному часі, варто перевірити конфігурацію за допомогою sudo suricata -T -c /etc/suricata/suricata.yaml -v. Це вбудований тестовий режим, який має Suricata, це варто роботи, тому що у випадку помилкового, наприклад, додавання файлу правил, який не існує, Suricata відразу повідомить про це. Завдяки цьому режиму, можна виправити помилки, і зменшити ризики того, що Suricata не буде працювати коректно.

5. Після налаштування Suricata, варто перевірити чи виявляє або блокує/видхіляє програма підозрілий трафік із власною згенерованою конфігурацією. Для цього перевіряємо правило ET Open із числом 2100498 за допомогою curl команди «curl http://testmynids.org/uid/index.html.».

6. Після налаштування Suricata для обробку трафіку в режимі IPS, необхідно додати правила брандмауера (ufw) для спрямування трафіку через Suricata для обробки. спрямувати вхідні пакети до Suricata, означає, що мережевий трафік буде надсилатися до Suricata за умовчуванням. Тобто Suricata встановлюється на границі мережі, щоб він міг моніторити весь вхідний і вихідний трафік. Це дозволить виявляти та блокувати потенційні загрози, що намагаються проникнути в мережу або вийти з неї.

7. Suricata не є основним безпековим рішення, тому варто використовувати Suricata як один з компонентів загальної архітектури безпеки ІС разом із іншими рішенням, такими як брандмауер, антивірусне програмне забезпечення як ESET Internet Security/McAfee Total Protection, а Suricata буде як додатковим шаром захисту.

8. Необхідно регулярно оновлювати правила. Це допоможе розпізнати нові типи загроз і збільшить ефективність системи.

9. Необхідно проводити аудит безпеки ІС та проводити тестування на проникнення, щоб перевірити ефективність Suricata та виявити можливі слабкі місця.

ВИСНОВОКИ

У ході дослідження було проаналізовано, які існують види загроз та їх наслідки для ІС. Стало зрозуміло, що існує низка різновидів загроз для інформаційних систем, як віруси, різні види троянських програм, шпигунське ПЗ, різні види хробаків(warm), DoS/DDoS-атаки, фішинг-атаки, які наслідки будуть для підприємства у випадку проникнення вище згаданих кіберзагроз в інформаційну систему підприємства, а саме загроза втрати особистих даних клієнтів, співробітників, таємних документів, зміна чи втрати інформації, порушення належного функціонування підприємства чи зовсім припинення його роботи. Що в свою чергу означає, втрату довіри клієнтів, інвесторів, різного розміру збитків і можливе банкрутство підприємства. Також було розглянуто сучасний стан кіберзагроз, згідно дослідженню від компанії Microsoft, росія, після повномасштабного вторгнення в Україну, атакувала низку галузей промисловості, секторів України, як транспортну, енергетичну, фінансову та ЗМІ, ці галузі зазнали найбільших кібератак, також були піддані інші галузі кібератакам, але не таких маштабів, як на ці галузі.

Проаналізовано, які існують сучасні методи захисту від вторгнень в інформаційну систему, такі як ідентифікація, аутентифікація, двофакторна аутентифікація, біометрична ідентифікація, firewall, антивірусне ПЗ, шифрування даних, IPS/IDS-системи, а також що кожен із цих методів означає, і яку перевагу надає підприємству в наслідок використання вище згаданих методів. Також було розглянуто сучасні антивірусні IPS системи, такі як ESET Internet Security, Snort, Suricata, McAfee Total Protection і було проаналізовано їх переваги та недоліки.

Проведено розгортання та налаштування ПЗ Suricata, спочатку, в режимі IDS, а потім було проведено зміну режим із IDS в IPS режим, було додано власні правила, де написали правила для сканування трафіку SSH, HTTP, TLS портів, зміна реагування Suricata на потенційно шкідливий трафік, тобто зміна режиму

робити із «Alert» в «Drop». Було розглянуто всі режими роботи даного ПЗ, як «Alert», «Drop», «Reject», «Allow/Pass» і що вони означають. Також було проведено тестування роботи налаштованої конфігурації в режимі IDS, де Suricata успішно було виявлено підозрілий HTTP запит і було проведено тестування Suricata в режимі IPS, де було успішно відхилено HTTP запит.

Було розроблено низка рекомендацій для ефективного, швидкого налаштування та розгортання Suricata, щоб зменшити ризики не спрацювання ПЗ і запобігти пропусканню небезпечного трафіку в інформаційну систему, використовуючи власну конфігурацію.

Варто зазначити, шо запропоновані рекомендації не дають стовідсоткової гарантії забезпечення необхідного рівня захисту ІС. Проте користуючись рекомендаціями по захисту ІС за допомогою Suricata, має можливість ефективно, швидко інсталювати, налаштувати та розгорнути ПЗ Suricata для захисту мережевого трафіку ІС підприємства від вразливостей, експлойтів, вторгнень, кібератак, несанкціонованого доступу, аномальної активності, зловживання протоколів та шкідливих програм.

Рекомендації у своїй роботі можуть використовувати системні адміністратори, безпекові аналітики, інженери з мережевої безпеки, аналітики загроз та мережевий адміністратор.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про захист інформації в інформаційно - комунікаційних системах : Закон України №1089-IX від 16.12.2020 р. / Верховна Рада України // Відомості Верховної ради. 1994. - №31. , ст.286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення 29.03.2023).
2. Інформаційна система. URL: http://www.kievoit.ippo.kubg.edu.ua/kievoit/2013/95/95.html (дата звернення 29.03.2023).
3. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему. URL: http://journals.nupp.edu.ua/sunz/article/view/323/290 (дата звернення 11.04.2023).
4. Quarterly threat trends & intelligence report November 2021. URL: https://info.phishlabs.com/hubfs/PhishLabs%20-%20QTTI%20Report%20-%20November%202021.pdf (дата звернення 13.04.2023).
5. Статистика фішингових інцидентів в Україні за 2021 рік. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34523/91970.pdf?sequence=2&isAllowed=y (дата звернення 16.04.2023).
6. Фішинг. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/ (дата звернення 12.04.2023).
7. Троян. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/troyan/ (дата звернення 13.04.2023).
8. Мережевий черв'як. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/setevoy-cherv/ (дата звернення 15.04.2023).
9. Що таке DDoS-атака? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-ddos-attack (дата звернення 16.04.2023).

10. Microsoft Digital Defense Report 2022. Illuminating the threat landscape and empowering a digital defense. URL: https://lopezdoriga.com/wp-content/uploads/2022/11/microsoft-digital-defense-report-2022.pdf (дата звернення 13.04.2023).

11. 93 Must-Know Ransomware Statistics [2022]. URL: https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=Cj0KCQjw27mhBhC9ARIsAIFsETEuz_8gO2Jlp933XW_ZMoW5ihWXn1P-32ORz5WnvroZeodjwHR_37EaAoxtEALw_wcB#ransomware-predictions-for-2023-and-beyond (дата звернення 15.04.2023).

12. 2022 in review: DDoS attack trends and insights. URL: https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/ (дата звернення 15.04.2023).

13. Брандмауер.URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/brandmauer/ (дата звернення 16.04.2023).

14. Мережева модель OSI. URL: https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B0_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI (дата звернення 16.04.2023).

15. Багаторівнений захист від різних типів загроз ESET Internet Security Комплексний захист. URL: https://www.eset.com/ua/home/internet-security/?gclid=CjwKCAjwx_eiBhBGEiwA15gLNzDWihpaqpswev4Hc8RsYYismbPXWDnvQHLU1SmpMj7eIUVtTP2oRRoCnWQQAvD_BwE (дата звернення 16.04.2023).

16. Understanding Trojan Viruses and How to Get Rid of Them URL: https://www.mcafee.com/learn/understanding-trojan-viruses-and-how-to-get-rid-of-them/ (дата звернення 16.04.2023).

17. What is a computer worm, and how does it work? URL: https://us.norton.com/blog/malware/what-is-a-

computerworm#:~:text=Worms%20can%20modify%20and%20delete,by%20overloading%20a%20shared%20network (дата звернення 16.04.2023).

18. What is a cyberattack? URL: https://www.chathamhouse.org/2022/02/what-cyber-attack?gclid=CjwKCAjwx_eiBhBGEiwA15gLN_NJsX_5BruIXGQ8Uag7sX_cbdyAfwp8Cx0ofP5WpNtOpTr17OxpXhoCObsQAvD_BwE (дата звернення 16.04.2023).

19. Intrusion detection system(IDS). URL: https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system (дата звернення 21.04.2023).

20. What is an intrusion prevention system? URL: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html#:~:text=What%20is%20an%20intrusion%20prevention,it%2C%20when%20it%20does%20occur (дата звернення 21.04.2023).

21. Suricata: What is it and how can we use it. URL: https://resources.infosecinstitute.com/topic/suricata-what-is-it-and-how-can-we-use-it/(дата звернення 20.04.2023).

22. What is Snort? URL: https://www.snort.org/ (дата звернення 20.04.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)