

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

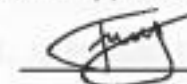
ПОЯСНЮВАЛЬНА ЗАПISKA

до випускної кваліфікаційної роботи магістра
на тему: «Методи та засоби побудови підсистем ви-
явлення вторгнень для мереж малого бізнесу»

Виконав студент 2-го курсу групи КБм-22-1
спеціальності 125 «Кібербезпека»

 Перцев О.М.

Керівник старший викладач кафедри КІ та КБ

 Покотило О.А.

Рецензент професор кафедри КІ та КБ, доктор технічних
наук, доцент

 Воротніков В.В.

« 13 » 10 2023 p.

Керівник  Покотило О.А.

Календарний план

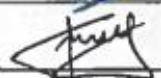
№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.11 - 03.11.23	Виконано
2	Аналіз літературних джерел	04.11.23 - 06.11.23	Виконано
3	Аналіз об'єкта дослідження	10.11.23 - 13.11.23	Виконано
4	Постановка задачі дослідження	15.11.23 - 17.11.23	Виконано
5	Структурування інформації	18.11.23 - 23.11.23	Виконано
6	Аналіз особливостей кібербезпеки в мережах малого бізнесу	24.11.23 - 01.12.23	Виконано
7	Аналіз існуючих рішень та їх обмежень	03.12.23 - 04.12.23	Виконано
8	Аналіз систем виявлення вторгнень	05.12.23 - 09.12.23	Виконано
9	Налаштування Suricata.	09.12.23 - 10.12.23	Виконано
10	Інтеграція з іншими системами безпеки	11.12.23 - 14.12.23	Виконано
11	Встановлення та налаштування тестового середовища	15.12.23 - 18.12.23	Виконано
12	Оформлення пояснювальної записки	19.12.23 - 25.12.23	Виконано
13	Оформлення презентації	27.12.23 - 28.12.23	Виконано
14	Захист	29.12.23	Виконано

Студент



Перцев О.М.

Керівник



Покотило О.А.

АНОТАЦІЯ

Кваліфікаційна робота складається з підсистеми виявлення вторгнень та пояснювальної записки до неї. Пояснювальна записка містить 54 сторінки та 27 ілюстрацій

Метою роботи є аналіз доступних рішень для підсистеми виявлення вторгнень для мереж малого бізнесу.

Проаналізовано особливості кібербезпеки в мережах малого бізнесу, існуючі рішення та їх обмеження.

Досліджено системи виявлення вторгнень такі як : Suricata. Snort та Zeek(bro)

Налаштовано CBV Suricata та інтегровано її з іншими системами безпеки, такими як : легкий агент для пересилання та інтеграції лог-файлів – Filebeat, веб-інтерфейс для візуалізації та аналізу даних - Kibana, розподільна система для зберігання та пошуку великими обсягами даних в реальному часі – Elasticsearch

Встановлено та налаштовано тестове середовище за допомогою GNS3, та віртуальних машин .

КЛЮЧОВІ СЛОВА: КІБЕРБЕЗПЕКА, CBV, IDS, SURICATA, ВТОРГНЕННЯ, ЗАХИСТ, SNORT, ZEEK, FILEBEAT, ELASTICSEARCH, KIBANA

ANNOTATION

The qualification work consists of an intrusion detection subsystem and an explanatory note to it. The explanatory note contains 54 pages and 27 illustrations.

The purpose of the work is to analyze the available solutions for the intrusion detection subsystem for small business networks.

The features of cybersecurity in small business networks, existing solutions and their limitations are analyzed.

Intrusion detection systems such as : Suricata. Snort and Zeek(bro).

Configured Suricata IPS and integrated it with other security systems, such as: a lightweight agent for sending and integrating log files - Filebeat, a web interface for data visualization and analysis - Kibana, a distribution system for storing and searching large amounts of data over time - Elasticsearch

The test environment was installed and configured using GNS3 and virtual machines.

KEYWORDS: CYBERSECURITY, SVV, IDS, SURICATA, INTRUSION, PROTECTION, SNORT, ZEEK, FILEBEAT, ELASTICSEARCH, KIBANA

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП	8
РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМ І ВИКЛИКІВ У ПОБУДОВІ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ	10
1.1. Загальний огляд систем виявлення вторгнень	10
1.2. Основні виклики та проблеми в сучасних системах виявлення вторгнень	12
1.2.1. Новітні методи обходження захисту.....	12
1.2.2. Обхід захисту.....	13
1.3. Особливості кібербезпеки в мережах малого бізнесу	14
1.4. Аналіз існуючих рішень та їх обмеження	16
РОЗДІЛ 2. МЕТОДИ ТА ІНСТРУМЕНТИ ДЛЯ ПОБУДОВИ ПІДСИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ	20
2.1 Аналіз систем виявлення вторгнень.....	20
2.1.1 Snort	20
2.1.2 Suricata.....	23
2.1.3 Zeek(Bro)	26
2.1.4 Порівняння СВВ.....	28
2.2 Налаштування Suricata.....	30
2.3 Аналіз інших систем безпеки та інтеграція з ними	37
2.3.1 Elasticsearch.....	38
2.3.2 Kibana	39
2.3.3 Filebeat.....	40
РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ.....	43
3.1. Вибір обладнання для тестового середовища	43
3.2. Тестування ефективності.....	45
3.3. Аналіз впливу Suricata на загальну кібербезпеку малого бізнесу.....	48
ВИСНОВКИ.....	51
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	51

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СВВ - Система виявлення вторгнень

IDS - Intrusion Detection System

CIDF - Common Intrusion Detection Framework

IPS - Intrusion Prevention System

DLP - Data Loss Prevention

ВСТУП

Актуальність теми. У сучасних умовах зростання кількості кібератак, малий бізнес є особливо вразливим до них. Це пов'язано з тим, що такі підприємства зазвичай мають обмежені ресурси для захисту від кібератак, а їхні інформаційні системи часто є більш незахищеними, ніж у великих компаній.

Кібератаки можуть завдати значної шкоди малим підприємствам. Вони можуть призвести до втрати даних, фінансових збитків, а також до порушення роботи підприємства.

Існує ряд методів і засобів виявлення вторгнень, які можуть бути ефективно використані для захисту малих підприємств від кібератак. Ці методи та засоби можуть бути доступними за ціною і простими у використанні, що робить їх привабливими для малого бізнесу.

Отже, методи та засоби побудови підсистем виявлення вторгнень для мереж малого бізнесу є актуальним напрямом досліджень, оскільки вони можуть допомогти захистити такі підприємства від кібератак і мінімізувати шкоду, яку вони можуть завдати.

Мета кваліфікаційної роботи. Мета роботи полягає в аналізі доступних рішень для підсистеми виявлення вторгнень для мереж малого бізнесу. Для досягнення поставленої мети було сформульовано наступні завдання:

1. Проаналізувати особливості кібербезпеки в мережах малого бізнесу та існуючі рішення та їх обмеження.
2. Дослідити системи виявлення вторгнень такі як : Suricata. Snort та Zeek(bro)
3. Налаштувати CBV Suricata та інтегрувати її з іншими системами безпеки, такими як : легкий агент для пересилання та інтеграції лог-файлів – Filebeat, веб-інтерфейс для візуалізації та аналізу даних - Kibana, розподільна система для зберігання та пошуку великими обсягами даних в реальному часі – Elasticsearch
4. Встановити та налаштувати тестове середовище за допомогою GNS3, та віртуальних машин .

Об'єктом дослідження є кібербезпека в мережах малого бізнесу та існуючі рішення та їх обмеження.

Предметом дослідження є системи виявлення вторгнень такі як : Suricata. Snort та Zeek(bro). Практичне значення роботи полягає у а налаштуванні підходящої після аналізу СВВ та тестування її

РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМ І ВИКЛИКІВ У ПОБУДОВІ СИСТЕМ ВІЯВЛЕННЯ ВТОРГНЕНЬ

1.1. Загальний огляд систем виявлення вторгнень

Система виявлення вторгнень (СВВ) - програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу до комп'ютерної системи чи мережі або несанкціонованого управління ними в основному через Інтернет. Відповідний англійський термін - Intrusion Detection System (IDS).

Системи виявлення вторгнень забезпечують додатковий рівень захисту комп'ютерних систем. Системи виявлення вторгнень використовуються для виявлення деяких типів шкідливої активності, яка може негативно вплинути на безпечність комп'ютерної системи. [1].

До такої активності відносяться мережеві атаки проти вразливих сервісів, атаки, спрямовані на підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів і черв'яків). В кінці 90-х років Агентство прогресивних захисних проєктів (Агентство просунутих дослідницьких проєктів) зробило спробу структурувати складові елементи СВВ[2]. Свою схему вони назвали Загальною системою виявлення вторгнень (Common Intrusion Detection Framework (CIDF)).

В кінці 90-х років Агентство прогресивних захисних проєктів (Агентство просунутих дослідницьких проєктів) зробило спробу структурувати складові елементи СВВ. Свою схему вони назвали Загальною системою виявлення вторгнень (CIDF).

За цією схемою архітектура СВВ включає (рисунок 1.1):

- сенсорну підсистему, призначену для збору подій, пов'язаних з безпекою системи що захищається (E-boxes);
- підсистему аналізу, призначену для виявлення атак і підозрілих дій на основі даних сенсорної системи (A-boxes);

- сховище або лог , що забезпечує накопичення подій і результатів аналізу цих подій (D-boxes);

- засоби протидії, які реєструють виявлені потенційно небезпечні події та сигналізують про це або виконують певні маніпуляції щоб зупинити атаку (C-boxes);

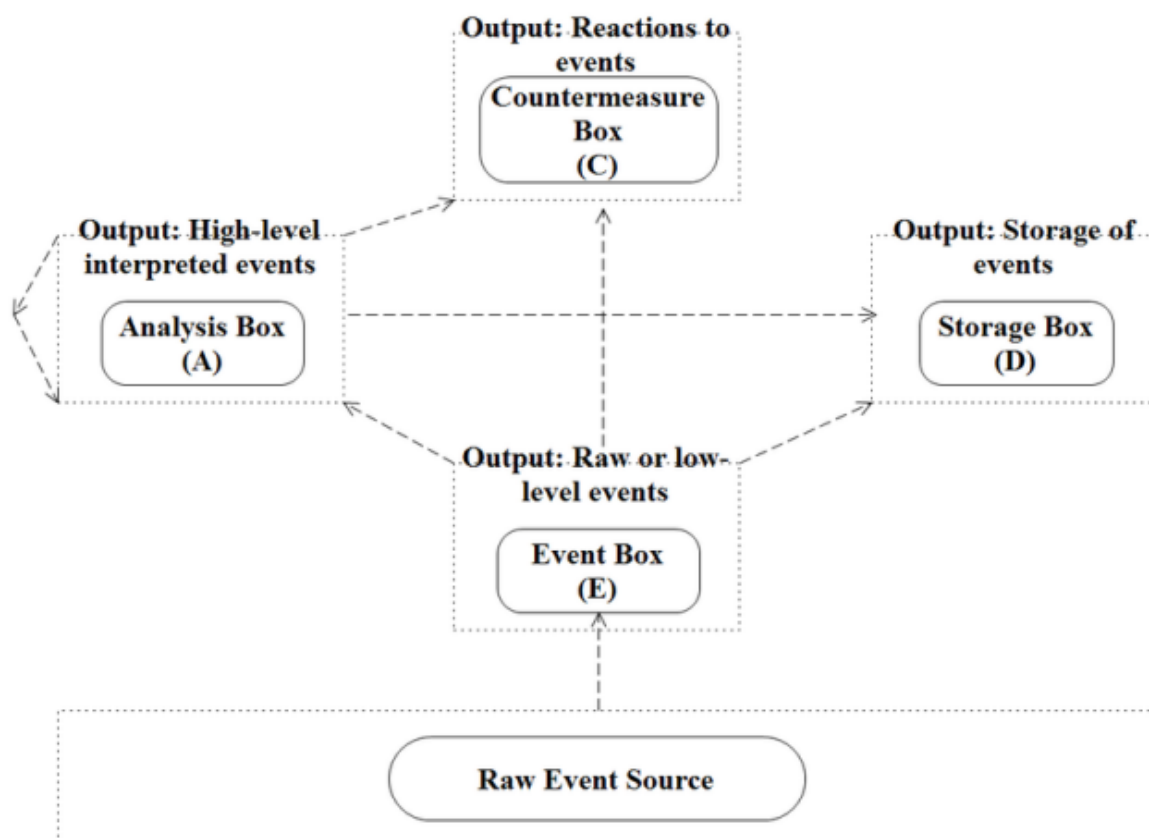


Рис. 1.1 Загальна схема роботи Системи виявлення вторгнень

Існує кілька способів класифікації СВВ в залежності від типу і розташування сенсорів, а також методів, використовуваних підсистемою аналізу для виявлення підозрілої активності. У багатьох простих СВВ всі компоненти реалізовані у вигляді одного модуля або пристрою. 15 Система запобігання вторгнень (англ. Intrusion Prevention System, IPS) - програмна або апаратна система мережевої та комп'ютерної безпеки, що виявляє вторгнення або порушення безпеки і автоматично захищає від них. Системи IPS можна розглядати як розширення Систем виявлення вторгнень (IDS), так як завдання відстеження атак залишається однаковою. Однак, вони відрізняються в тому, що IPS повинна відстежувати активність в реальному часі і швидко реалізовувати дії щодо запобігання атак.[4]

1.2. Основні виклики та проблеми в сучасних системах виявлення вторгнень

Сучасні системи виявлення вторгнень (IDS) є важливим компонентом інформаційної безпеки. Вони дозволяють виявляти та запобігати шкідливу діяльність в мережах та системах. Однак, незважаючи на значний прогрес у галузі IDS, існує ряд викликів та проблем, які необхідно вирішити.

Одним із основних викликів є зростаючий обсяг даних, що обробляються IDS. Це пов'язано з ростом кількості пристроїв, підключених до мережі, а також з використанням нових технологій, таких як хмарне обчислення та Інтернет речей.

Іншим викликом є складність сучасних атак. Зловмисники використовують все більш витончені методи для обходу виявлення IDS. Це вимагає від IDS використання більш складних алгоритмів та методів навчання.

Ще однією проблемою є необхідність балансу між чутливістю та точністю IDS. Чутлива IDS може виявити більшу кількість атак, але також може спричинити помилкові тривоги. Точна IDS, з іншого боку, може зменшити кількість помилкових тривог, але може пропустити деякі атаки.[3]

1.2.1. Новітні методи обходження захисту

Постійна еволюція атак є однією з основних проблем у сфері систем виявлення вторгнень (IDS). Зловмисники стали більш винахідливими та постійно шукають нові методи обходження захисту для незаконного доступу до систем та мереж.[7]

- Поліморфні атаки: Зловмисники використовують поліморфні методи, щоб змінювати вигляд свого шкідливого програмного забезпечення так часто, що його важко виявити стандартними сигнатурними методами, які використовують багато IDS.

- Zero-Day атаки: Атаки, які використовують вразливості в програмному забезпеченні, які виробники ще не встигли виправити або опублікувати виправлення. Такі атаки можуть залишатися непоміченими до моменту їхнього виявлення та зняття.

- Соціальна інженерія: Замаскування атаки під нормальну активність користувача або навіть використання соціальної інженерії для отримання дозволу на доступ, щоб уникнути виявлення.

- Атаки на рівні додатків: Зловмисники можуть використовувати вразливості в додатках або використовувати слабкі сторони програмного забезпечення для виконання атак.

Створення атак "під замовлення":

- Цілеспрямовані атаки: Замовники можуть спеціально створювати атаки для конкретного об'єкта, обхід захисту якого може вимагати унікальних методів виявлення.

Використання технологій штучного інтелекту (AI):

- Генерація атак за допомогою AI: Зловмисники можуть використовувати технології штучного інтелекту для створення нових типів атак, які можуть уникнути традиційних методів виявлення.

1.2.2. Обхід захисту

Другий пункт стосується обходу захисту і включає в себе різноманітні методи, які зловмисники можуть використовувати для того, щоб уникнути виявлення системами виявлення вторгнень (IDS) та проникнути в систему чи мережу[5]. Розглянемо ці методи більш детально:

- Обхід сигнатур: Зловмисники можуть використовувати поліморфні техніки для зміни вигляду свого шкідливого коду, щоб уникнути сигнатурних методів виявлення, які базуються на збігу зі заздалегідь визначеними сигнатурами.

- Використання шифрування трафіку(end-to-end): Зловмисники можуть шифрувати свій трафік, використовуючи захищені канали зв'язку, щоб ускладнити виявлення атак та забезпечити конфіденційність їхніх дій.
- Спеціалізовані методи виявлення обходу: Зловмисники можуть обходити виявлення, використовуючи особливості синтаксису мережевого трафіку, такі як фрагментація пакетів або змінення порядку фрагментів.
- Використання слабкостей в захисті: Зловмисники можуть активно шукати та використовувати непередбачувані вразливості в системах чи програмах, які не мають належного захисту.
- Спрямовані атаки: Замовники можуть проводити цілеспрямовані атаки на слабкі сторони системи чи мережі, які не відомі загальному публіці та, відповідно, не враховуються засобами виявлення загального призначення.
- Використання анонімізації: Зловмисники можуть приховувати свою реальну IP-адресу та локацію, використовуючи анонімайзери та віртуальні приватні мережі (VPN), що ускладнює відстеження їхніх дій.
- Атаки зсередини: Зловмисники, які вже мають доступ до системи, можуть використовувати свої знання про внутрішню інфраструктуру для уникнення виявлення.

1.3. Особливості кібербезпеки в мережах малого бізнесу

В сфері кібербезпеки для малого бізнесу існують ряд особливостей та викликів, які потребують уваги та ефективних стратегій захисту.

Однією з ключових особливостей є обмежені бюджетні ресурси, що може ускладнити впровадження та підтримку високого рівня кібербезпеки. Це вимагає від бізнесу знаходження ефективних, але менш вартісних заходів безпеки, таких як використання відкритих джерел та хмарних рішень.

Малі підприємства часто стають об'єктом кібератак через відсутність потужних захисних механізмів. Це підкреслює важливість ефективного захисту від

фішингу та соціально-інженерних атак. Освіченість персоналу грає ключову роль у зменшенні ризиків, тому навчання та тренінги з кібербезпеки є необхідними.

Зростання використання мобільних та віддалених робочих місць ускладнює завдання забезпечення їхньої безпеки. Малі бізнеси повинні акцентувати увагу на використанні захисних рішень для мобільних пристроїв та встановленні ефективних політик безпеки для робочих місць здалека.

Створення безпечного робочого середовища вимагає використання різноманітних засобів мережевої безпеки, таких як фаєрволи та системи виявлення вторгнень. Важливо також регулярно проводити резервне копіювання даних та тестувати процедури відновлення для гарантії ефективності заходів забезпечення неперервності бізнесу.

Узагальнюючи, кібербезпека для малого бізнесу потребує комплексного підходу, який враховує конкретні умови та обмеження цього сегменту. Забезпечення захисту від кіберзагроз вимагає поєднання технічних рішень, ефективного управління ресурсами та високого рівня освіченості персоналу.

Для свого проекту як підсистему мереж малого бізнесу я обрав малий офіс юридичної фірми.

Кібербезпека для малого офісу юридичної фірми належить до важливих аспектів діяльності, враховуючи специфічні виклики цієї галузі. Забезпечення конфіденційності та захисту чутливої інформації є ключовим завданням, вимагаючи використання шифрування, строгого контролю доступу та систем моніторингу. Управління клієнтською інформацією також виглядає складним завданням, вимагаючи високого рівня захисту через технології DLP (Data Loss Prevention).

Фірми повинні ефективно керувати електронною поштою та бути готовими до протидії фішинговим атакам, зосереджуючись на фільтрації та навчанні персоналу. Забезпечення високого рівня доступу до систем та даних, зокрема використання двофакторної аутентифікації, є важливим аспектом безпеки.

Окрім того, у віртуальних офісах та роботі здалека виникає потреба в особливих заходах безпеки, таких як використання шифрування, VPN та засобів зв'язку з

високим рівнем захисту. Важливо враховувати також правові та регуляторні вимоги, використовуючи засоби кіберзахисту, що відповідають стандартам галузі юридичних послуг.

Усі ці аспекти взаємодіють, утворюючи складне середовище, де необхідно враховувати конкретні потреби та особливості юридичної фірми для забезпечення ефективного та надійного кіберзахисту.

1.4. Аналіз існуючих рішень та їх обмеження

Існує широкий вибір рішень для підсистем виявлення вторгнень (IDS) для мереж малого бізнесу. Ці рішення можна класифікувати за такими критеріями:

- **Тип IDS:** існують два основних типи IDS: детектори аномалій та детектори екземплярів. Детектори аномалій виявляють аномалії в поведінці мережі, які можуть бути ознакою атаки. Детектори екземплярів виявляють конкретні атаки, які були відомі раніше.
- **Місце розташування:** IDS можна розміщувати на різних місцях у мережі. Існують локальні IDS, які розміщуються на окремому пристрої в мережі. Існують також розподілені IDS, які розміщуються на декількох пристроях у мережі.
- **Ціна:** IDS для малого бізнесу можуть коштувати від декількох сотень до декількох тисяч доларів.

Серед існуючих рішень для малого бізнесу можна виділити такі:

- **Вільні та відкриті джерела:** існує ряд рішень IDS з відкритим кодом, які можна використовувати безкоштовно. До таких рішень належать Snort, Suricata та Zeek(Bro). Ці рішення можуть бути хорошим варіантом для малого бізнесу, який має обмежений бюджет.
- **Продукти від постачальників безпеки:** постачальники безпеки пропонують широкий вибір рішень IDS для малого бізнесу. Ці рішення, як правило, більш зручні в використанні та пропонують більше функцій, ніж рішення з відкритим кодом. Однак вони також можуть бути більш дорогими.

Незважаючи на широкий вибір рішень IDS для малого бізнесу, існує ряд обмежень, які слід враховувати при їх виборі.

Одним із основних обмежень є складність використання. Деякі рішення IDS можуть бути складними в налаштуванні та використанні. Це може бути проблемою для малого бізнесу, який не має спеціалістів з інформаційної безпеки.

Іншим обмеженням є чутливість до помилкових тривог. IDS можуть іноді створювати помилкові тривоги, які можуть відволікати увагу від справжніх атак. Це може бути особливо проблемою для малого бізнесу, який не має ресурсів для реагування на кожну тривогу.

Ще одним обмеженням є неможливість виявлення нових атак. Зловмисники постійно розробляють нові методи атак, які можуть бути невідомими IDS. Це означає, що IDS можуть не виявляти деякі атаки.

При виборі рішення IDS для малого бізнесу слід враховувати такі фактори:

- Складність використання: оберіть рішення, яке буде простим у налаштуванні та використанні.
- Чутливість до помилкових тривог: оберіть рішення з низьким рівнем помилкових тривог.
- Здатність виявляти нові атаки: оберіть рішення, яке оновлюється новими правилами для виявлення атак.

Системи виявлення вторгнень є важливим компонентом інформаційної безпеки для мереж малого бізнесу. При виборі рішення IDS слід враховувати такі фактори, як складність використання, чутливість до помилкових тривог і здатність виявляти нові атаки.

Потрібно обрати рішення, яке підтримує різні типи мережевих пристроїв, для того щоб захистити всі пристрої у мережі, пропонує централізоване управління та має функції виявлення загроз у реальному часі.

Висновок до розділу 1

Системи виявлення вторгнень (IDS) відіграють важливу роль у забезпеченні інформаційної безпеки мереж будь-якого розміру, включаючи бізнес-мережі. Їх основна функція полягає у виявленні та запобіганні будь-яким діям, що відбуваються в мережі, таким як атаки на сервери, крадіжка даних та розповсюдження шкідливого програмного забезпечення.

Однак, незважаючи на прогрес, досягнутий в індустрії IDS, існують проблеми і занепокоєння, які потребують вирішення.

Одна з ключових проблем пов'язана зі зростаючим обсягом даних, з якими доводиться працювати IDS-службам. Цей сплеск даних в першу чергу зумовлений зростанням кількості пристроїв, підключених до мережі, і впровадженням нових технологій, таких як хмарні обчислення та Інтернет речей (IoT).

Інший виклик пов'язаний зі складністю сучасних атак. Зловмисники стають все більш витонченими у своїх методах, щоб уникнути виявлення IDS. Відповідно, IDS повинні використовувати алгоритми та методи навчання, щоб не відставати від цих еволюціонуючих загроз.

Крім того, пошук балансу між чутливістю та точністю є ще одним викликом для IDS. Хоча чутлива IDS може виявити цілий ряд атак, вона також може призвести до хибних тривог. І навпаки, точна IDS може зменшити кількість хибних тривог. Потенційно може пропустити певні типи атак.

Мережі малого бізнесу стикаються з особливостями та проблемами кібербезпеки через обмеженість ресурсів, доступних для інвестування в заходи безпеки. Крім того, таким компаніям часто не вистачає фахівців з інформаційної безпеки.

На ринку існує безліч рішень IDS, спеціально розроблених для мереж малого бізнесу. Ці рішення можна класифікувати на основі певних факторів[13];

1. Тип IDS; Існує два типи: детектори аномалій та детектори екземплярів.
2. Розташування; Ви можете вибрати між рішеннями для приміщень або розподіленими рішеннями.
3. Ціновий діапазон; Вартість може варіюватися від сотні до тисячі доларів.

Однак важливо враховувати обмеження при виборі рішення IDS.

Одним з основних обмежень є складність, пов'язана з використанням деяких рішень IDS. Це може створити труднощі для компаній, які не мають фахівців з інформаційної безпеки.

Іншим обмеженням є виникнення тривог. Хибні тривоги можуть відволікати увагу від атак, що призводить до затримок у реагуванні.

Крім того, існує проблема виявлення IDS-атак. Зловмисники постійно вдосконалюють свої методи, що дозволяє їм використовувати методи атак, які можуть бути не розпізнані IDS.

При виборі рішення IDS для бізнесу важливо враховувати наступні фактори;

1. Простота використання; Обирайте рішення, яке легко налаштовувати та експлуатувати.
2. Чутливість до хибних тривог: обирайте рішення з функцією виявлення тривог.
3. Здатність виявляти атаки; шукайте рішення, яке регулярно оновлює свої правила та механізми для виявлення нових моделей атак.

Крім того, важливо враховувати наступні аспекти;

1. Розмір мережі; Обирайте рішення, яке відповідає масштабу вашої мережі.
2. Тип бізнесу: обирайте рішення, яке відповідає вимогам вашої галузі.
3. Бюджет: визначте бюджет для впровадження системи виявлення вторгнень (IDS).

Проаналізувавши виклики та проблеми, пов'язані з розробкою систем виявлення вторгнень, ми можемо зробити наступні висновки;

IDS відіграє важливу роль у захисті мереж будь-якого розміру, включаючи ті, що належать підприємствам.

Для підвищення ефективності IDS необхідно усунути різні перешкоди і проблеми.

При виборі рішення IDS для бізнесу важливо враховувати такі фактори, як зручність для користувача, чутливість до тривог і здатність виявляти нові методи атак.

РОЗДІЛ 2. МЕТОДИ ТА ІНСТРУМЕНТИ ДЛЯ ПОБУДОВИ ПІДСИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

2.1 Аналіз систем виявлення вторгнень

Для того щоб застосувати правильну СВВ потрібно проаналізувати доступні рішення. Після аналізу відкритих джерел я виділив три СВВ які я можу використати в проєкті. Отже, у цьому порівняльному аналізі, ми детально розглянемо три визначені системи виявлення вторгнень: Snort, Suricata та Bro (Zeek). Кожна з цих систем володіє своїми унікальними особливостями та можливостями, що робить їх привабливими для використання в різних сценаріях. Давайτε розглянемо їхні переваги, недоліки та сфери застосування, щоб допомогти прийняти обґрунтоване рішення при виборі системи IDS для конкретних потреб організації чи проекту.

2.1.1 Snort

Snort - це безкоштовна відкрита система виявлення вторгнень (IDS) на основі сигнатур. Вона використовується для виявлення та реагування на зловмисну діяльність у мережі. Snort є відомою та широко використовуваною системою виявлення вторгнень (IDS) та ідентифікації вторгнень (IPS). Вироблена Marty Roesch, Snort визначається своєю високою продуктивністю, гнучкістю та можливістю виявлення широкого спектру загроз. Snort може використовуватися для виявлення широкого спектру атак, включаючи вторгнення в систему, шкідливе програмне забезпечення, фішингові атаки та атаки на веб-сервери[9].

Snort складається з декількох основних компонентів:

- Декодер пакетів. Декодер пакетів розбиває мережевий трафік на окремі пакети та визначає їх типи.
- Ядро виявлення. Ядро виявлення аналізує пакети для виявлення ознак атак.

- Модуль сповіщення. Модуль сповіщення повідомляє про виявлені атаки.

Декодер пакетів є першим компонентом, який стикається з мережевим трафіком. Він розбиває трафік на окремі пакети та визначає їх типи. Це дозволяє ядру виявлення аналізувати пакети в контексті їх протоколу.

Ядро виявлення є основним компонентом Snort. Воно аналізує пакети для виявлення ознак атак. Snort використовує кілька різних методів виявлення атак, включаючи:

Виявлення на основі сигнатур: Snort використовує базу даних відомих зловмисних сигнатур для виявлення атак. Сигнатура - це шаблон, який відповідає певному типу атаки. Snort шукає сигнатури в мережевому трафіку. Якщо Snort знаходить сигнатуру, він повідомляє про виявлену атаку.

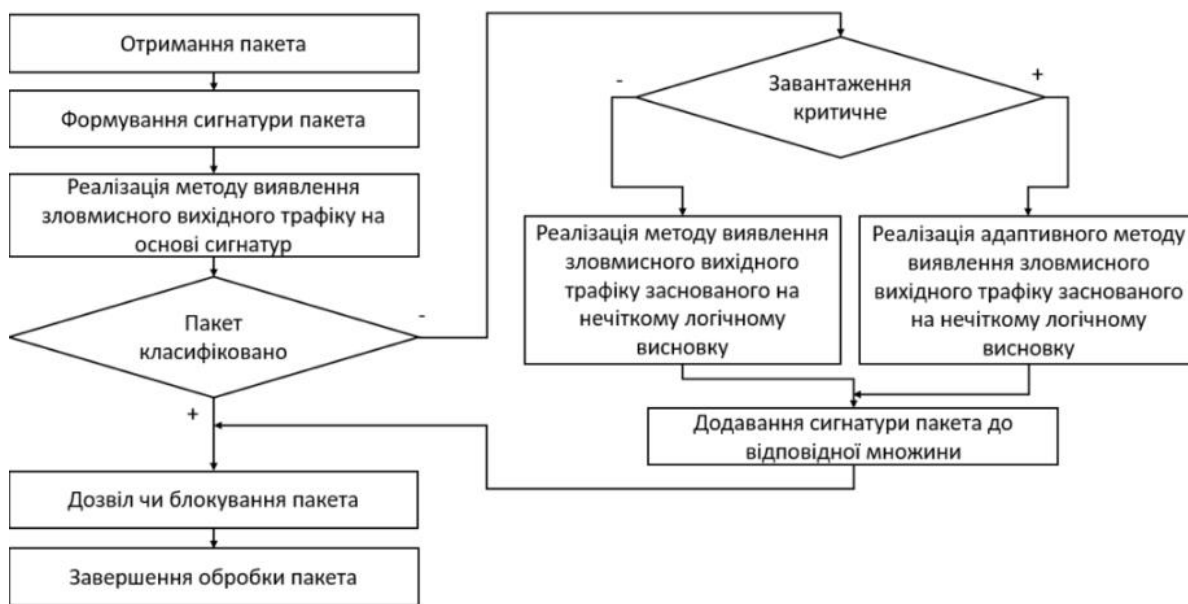


Рис 2.1 Метод виявлення на основі сигнатур

Виявлення аномалій: Snort використовує статистичний аналіз мережевого трафіку для виявлення аномалій, які можуть бути ознакою атаки. Наприклад, Snort може виявити аномалію, якщо кількість пакетів, що надходять з певного IP-адреси, раптово збільшується.

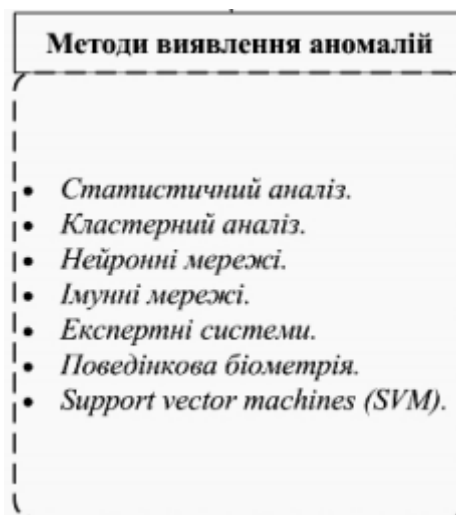


Рис 2.2 Методи виявлення аномалій

Модуль сповіщення повідомляє про виявлені атаки. Він може генерувати текстові повідомлення, відправляти електронні листи або генерувати сигнали для інших систем безпеки[12].

Snort можна налаштувати для виявлення широкого спектру атак. Налаштування Snort включає в себе:

- Оновлення баз даних сигнатур. База даних сигнатур Snort містить інформацію про відомі зловмисні сигнатури. Щоб забезпечити ефективне виявлення атак, базу даних сигнатур слід регулярно оновлювати.
- Створення правил виявлення. Правила виявлення Snort визначають, які пакети слід аналізувати та які атаки слід виявляти. Правила виявлення можна налаштувати для виявлення атак на певні протоколи, з певних джерел або з використанням певних методів.

Плюси Snort :

- Безкоштовна і відкрита. Snort є безкоштовною і відкритою системою, що дозволяє використовувати її будь-кому.
- Широкий спектр можливостей. Snort може використовуватися для виявлення широкого спектру атак.
- Гнучкість налаштування. Snort можна налаштувати відповідно до конкретних потреб організації.

- Велика спільнота користувачів. Snort має велику спільноту користувачів, яка надає підтримку та ресурси для використання системи.

Мінуси Snort:

- Залежність від сигнатур. В основному Snort базується на сигнатурах для виявлення вторгнень, що може зробити його менш ефективним у виявленні нових атак або варіантів загроз, які не входять до відомих сигнатур.
- Ложнопозитиви. Як і в інших системах виявлення вторгнень на основі сигнатур, може виникати проблема ложнопозитивів, коли Snort помічає неправильні атаки або загрози, що може призвести до неправомірних заходів забезпечення.
- Обмежена підтримка для аналізу аномалій. У порівнянні з деякими іншими системами виявлення вторгнень, Snort має обмежені можливості аналізу аномалій, що може обмежити його здатність виявляти нові та невідомі загрози.
- Застарілість деяких аспектів. Одна з критичних версій Snort, Snort 2, вже застаріла. Є новіші версії, такі як Snort 3, але їх прийняття може бути повільним у деяких організаціях.
- Відкритий код, але з комерційною підтримкою. Хоча Snort є відкритим програмним забезпеченням, комерційна підтримка може вимагати великі витрати, що може вплинути на фінансові ресурси менших організацій.

2.1.2 Suricata

Suricata - це безкоштовна відкрита система виявлення вторгнень (IDS) на основі сигнатур та поведінки. Вона використовується для виявлення та реагування на зловмисну діяльність у мережі. Suricata може використовуватися для виявлення широкого спектру атак, включаючи вторгнення в систему, шкідливе програмне забезпечення, фішингові атаки та атаки на веб-сервери. Suricata базується на мережевому движку "AF_PACKET", що робить її ефективною у виявленні та обробці трафіку в реальному часі. Вона також підтримує множину мережевих карт та може

працювати в режимі IDS або IPS. Архітектура Suricata дозволяє розділяти обробку пакетів між різними ядрами процесора, що підвищує його продуктивність.

Suricata складається з декількох основних компонентів[20]:

- Декодер пакетів розбиває мережевий трафік на окремі пакети та визначає їх типи.
- Ядро виявлення аналізує пакети для виявлення ознак атак.
- Виявлення поведінки
- Модуль сповіщення повідомляє про виявлені атаки.

Декодер пакетів є першим компонентом, який стикається з мережевим трафіком. Він розбиває трафік на окремі пакети та визначає їх типи. Це дозволяє ядру виявлення аналізувати пакети в контексті їх протоколу.

Ядро виявлення є основним компонентом Suricata. Воно аналізує пакети для виявлення ознак атак[10]. Suricata використовує кілька різних методів виявлення атак, включаючи:

Виявлення на основі сигнатур: Suricata використовує базу даних відомих зловмисних сигнатур для виявлення атак. Сигнатура - це шаблон, який відповідає певному типу атаки. Suricata шукає сигнатури в мережевому трафіку. Якщо Suricata знаходить сигнатуру, він повідомляє про виявлену атаку (Рис 2.1).

Виявлення аномалій: Suricata використовує статистичний аналіз мережевого трафіку для виявлення аномалій, які можуть бути ознакою атаки. Наприклад, Suricata може виявити аномалію, якщо кількість пакетів, що надходять з певного IP-адреси, раптово збільшується (Рис2.2).

Виявлення поведінки: Suricata використовує аналіз поведінки для виявлення атак, які неможливо виявити за допомогою методів виявлення на основі сигнатур або аномалій. Наприклад, Suricata може виявити атаку, яка використовує новий метод або техніку[8].

Модуль сповіщення повідомляє про виявлені атаки. Він може генерувати текстові повідомлення, відправляти електронні листи або генерувати сигнали для інших систем безпеки.

Suricata можна налаштувати для виявлення широкого спектру атак. Налаштування Suricata включає в себе:

- Оновлення баз даних сигнатур. База даних сигнатур Suricata містить інформацію про відомі зловмисні сигнатури. Щоб забезпечити ефективне виявлення атак, базу даних сигнатур слід регулярно оновлювати.
- Створення правил виявлення. Правила виявлення Suricata визначають, які пакети слід аналізувати та які атаки слід виявляти. Правила виявлення можна налаштувати для виявлення атак на певні протоколи, з певних джерел або з використанням певних методів.
- Конфігурація модулів виявлення. Suricata включає в себе кілька модулів виявлення, кожен з яких має свої власні налаштування. Конфігурація модулів виявлення дозволяє налаштувати Suricata для виявлення конкретних типів атак.

Плюси Suricata

- Безкоштовна і відкрита. Suricata є безкоштовною і відкритою системою, що дозволяє використовувати її будь-кому.
- Широкий спектр можливостей. Suricata може використовуватися для виявлення широкого спектру атак.
- Гнучкість налаштування. Suricata можна налаштувати відповідно до конкретних потреб організації.
- Ефективність виявлення. Suricata є ефективною системою виявлення вторгнень.

Мінуси Suricata

- Високі вимоги до ресурсів. З врахуванням своєї високої продуктивності та здатності обробки великої кількості трафіку, Suricata може вимагати значних обчислювальних ресурсів та мережевого обладнання. Це може бути недоцільним для менших організацій або об'єктів з обмеженими ресурсами.

- **Можливі ложнопозитиви.** Системи виявлення вторгнень, включаючи Suricata, можуть породжувати ложнопозитивні сигнали, що призводить до неправильних або непотрібних втручань. Це може вимагати додаткового часу для аналізу та виправлення помилкових сигналів.
- **Можливий вплив на продуктивність мережі.** Під час великих обсягів трафіку Suricata може впливати на продуктивність мережі через обробку та аналіз великої кількості пакетів. Це особливо важливо в великих організаціях з інтенсивним мережевим трафіком.
- **Оновлення сигнатур та підтримка.** Періодичні оновлення сигнатур є важливим елементом для ефективної роботи Suricata. Відсутність своєчасних оновлень може призвести до невідомості перед новими загрозами.

2.1.3 Zeek(Bro)

Zeek є платформою для аналізу трафіку, орієнтованою в першу чергу на відстеження подій, пов'язаних з безпекою, але не обмежується цим застосуванням. Надаються модулі для аналізу і розбору різних мережевих протоколів програм, що враховують стан з'єднань і дозволяють формувати детальний журнал (архів) мережевої активності. Надається предметно-орієнтована мова для написання сценаріїв моніторингу і виявлення аномалій з урахуванням специфіки конкретних інфраструктур. Система оптимізована для використання в мережах з великою пропускну здатністю. Надається API для інтеграції зі сторонніми інформаційними системами та програмами передачі даних в режимі реального часу.[11]

Zeek націлений на мережі з високошвидкісним підключенням для сканування великих обсягів даних. Розумно використовуючи техніку фільтрації пакетів, Zeek здатний досягти необхідної продуктивності на будь-якому комп'ютері. Якщо Zeek виявляє щось «цікаве», він може бути проінструкований для збору і відправлення логів, проінформувати оператора в режимі реального часу або виконати будь-яку команду, наприклад, скинути підозріле підключення.

Zeek має за мету використання в мережах, де необхідна гнучкість і високий ступінь налаштовуваності системи. Спочатку програма була розроблена як дослідницька платформа для дослідження вторгнень і аналізу даних. Вона не призначена для використання «з коробки». Системою повинні користуватися Unix фахівці з великим багажем знань по мережам.

Функціональність:

- Мережевий аналіз. Zeek проводить детальний аналіз мережевого трафіку та створює структуровані події для різних протоколів, що дозволяє глибше розуміти та виявляти аномалії.
- Специфікація протоколів. Zeek може визначати власні специфікації протоколів для виявлення вторгнень та виконання глибокого аналізу трафіку.
- Детальні події. Створені події містять розширену інформацію, таку як адреси IP, порти, типи пакетів тощо, що полегшує аналіз та виявлення аномалій.

Плюси Zeek:

- Широкий спектр протоколів. Zeek підтримує багато протоколів, включаючи HTTP, DNS, FTP, SSL, SSH та інші.
- Гнучкість та Розширюваність. Завдяки своїй мові скриптів та можливості розширювання, Zeek може бути адаптований під конкретні потреби та вимоги.
- Детальний Аналіз. Zeek надає глибокий аналіз мережевого трафіку, що дозволяє точно визначати та реагувати на загрози.
- Адаптованість до Змін. Мова скриптів Zeek дозволяє швидко адаптувати систему до нових загроз та змін в мережевому середовищі.
- Розширена Інформація Подій. Структуровані події, створені Zeek, надають розширену інформацію для аналізу та виводу.

Мінуси Zeek:

- Велике споживання ресурсів. Zeek може вимагати значних обчислювальних та мережевих ресурсів, особливо при обробці великого обсягу мережевого

трафіку. Це може призвести до необхідності потужніших серверів та інфраструктури.

- Складність конфігурації та налаштувань. Розгортання та конфігурація Zeek може бути складною для менш досвідчених користувачів. Велика кількість опцій та налаштувань може становити виклик для новачків.
- Необхідність адаптації скриптів. У деяких випадках може знадобитися написання власних скриптів для адаптації Zeek під конкретні потреби чи сценарії. Це може вимагати додаткового знання та часу.
- Вимоги до збереження даних. Зберігання та обробка великого обсягу згенерованих Zeek даних може вимагати ефективної системи управління журналами та зберіганням даних.
- Оптимізація в плані швидкодії. В деяких випадках, для досягнення оптимальної швидкодії, може знадобитися оптимізація та налаштування Zeek, що може вимагати додаткових зусиль.
- Відсутність вбудованої системи виявлення вторгнень. Хоча Zeek спроможний виділяти аномалії та створювати детальні події, він не завжди включає вбудовану систему виявлення вторгнень, як, наприклад, Snort чи Suricata. Це може вимагати інтеграції з іншими системами IDS/IPS.

2.1.4 Порівняння СВВ

Проведемо порівняльний огляд систем виявлення вторгнень Snort, Suricata та Zeek (Bro) на основі раніше наданої інформації:

Snort:

Переваги :

- Досвід. Snort є однією з найдавніших та найбільш відомих систем IDS/IPS.
- Спільнота та Документація. Має велику та активну спільноту користувачів.

- Підтримка правил. Великий вибір правил для виявлення різних видів атак.

Мінуси:

- Спрямованість на відслідковування підписів. Більш спрямований на відслідковування підписів, що може бути менш ефективним у виявленні нових атак.

Suricata:

Переваги :

- Швидкодія. Оптимізований для високопродуктивної роботи та має підтримку мультипотокості.
- Підтримка зашифрованого трафіку. Здатний до аналізу зашифрованого трафіку.
- Модульність та Розширюваність. Гнучка архітектура, що дозволяє легко розширювати та адаптувати систему.

Мінуси:

- Спільнота. Має меншу спільноту користувачів порівняно з Snort.

Zeek (Bro):

Переваги:

- Глибокий аналіз. Забезпечує глибокий аналіз різних аспектів мережевого трафіку.
- Модульність та Розширюваність. Має модульну архітектуру, що дозволяє легко розширювати та адаптувати систему.
- Структурований журнал подій. Генерує структурований журнал подій для аналізу та виявлення аномалій.

Мінуси:

- Вимогливість до ресурсів. Може вимагати значних ресурсів для ефективної роботи, особливо при аналізі великих обсягів трафіку.

Загальні відмінності:

- Мова скриптування. Snort та Suricata використовують мову скриптування Lua, тоді як Zeek використовує свою власну мову скриптування ZeekScript.
- Швидкодія. Suricata спрямований на швидкодію роботу та підтримує мультипотоківість, що може бути важливим для обробки великих обсягів трафіку.
- Аналіз зашифрованого трафіку. Усі три системи мають можливість аналізу та виявлення загроз в зашифрованому трафіку.
- Модульність. Zeek та Suricata володіють більшою гнучкістю та розширюваністю у порівнянні з Snort.

Підсумовуючи, вибір між Snort, Suricata та Zeek залежить від конкретних вимог та потреб проекту. Якщо важлива швидкодія та мультипотоківість, Suricata може бути кращим варіантом. Якщо потрібен глибокий аналіз мережі та структуровані журнали, Zeek може бути підходящим варіантом. Snort варто обрати, якщо важлива стабільність та багата база правил для виявлення вторгнень. Враховуючи обране середовище (малий офіс юридичної фірми) для виконання поставлених задач найбільш підходящою СВВ є Suricata.

2.2 Налаштування Suricata

Щоб розпочати встановлення Suricata, потрібно додати інформацію про репозиторій програмного забезпечення Open Information Security Foundation (OISF) до вашої системи Ubuntu. Для цього скористаємося командою `add-apt-repository` (Рис 2.2.1).

Запустимо цю команду, щоб додати репозиторій до системи і оновити список доступних пакунків:

```
sudo add-apt-repository ppa:oisf/suricata-stable
```

```
tds@tds-VirtualBox:~$ sudo add-apt-repository ppa:oisf/suricata-stable
[sudo] пароль до tds:
Сховище: «deb https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/ jammy mai
n»
Опис:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevent
ion System and Network Security Monitoring engine.

Open Source and owned by a community run non-profit foundation, the Open Information
Security Foundation (OISF). Suricata is developed by the OISF, its supporting vendors
and the community.
```

Рис 2.2.1 `sudo add-apt-repository ppa:oisf/suricata-stable`

Команда оновить список доступних пакунків після додавання нового сховища.

Тепер можемо встановити пакунок `suricata` за допомогою команди(Рис 2.2.2):

`sudo apt install suricata`

```
tds@tds-VirtualBox:~$ sudo apt install suricata
[sudo] пароль до tds:
Зчитування переліків пакунків... Виконано
Побудова дерева залежностей... Виконано
Зчитування інформації про стан... Виконано
Буде встановлено такі додаткові пакунки:
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhttp2
  libhyperscan5 libluajit-5.1-2 libluajit-5.1-common liblzma-dev libnet1
  libnetfilter-queue1
Пропоновані пакунки:
  liblzma-doc
НОВІ пакунки, які будуть встановлені:
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhttp2
  libhyperscan5 libluajit-5.1-2 libluajit-5.1-common liblzma-dev libnet1
  libnetfilter-queue1 suricata
оновлено 0, встановлено 11 нових, 0 відмічено для видалення і 5 не оновлено.
```

Рис 2.2.2 `sudo apt install suricata`

Тепер, коли пакунок встановлено, увімкнемо службу `suricata.service`, щоб вона запускалася при перезавантаженні системи(Рис 2.2.3). Для цього скористаюся командою `systemctl`:

`sudo systemctl enable suricata.service`

Ви маєте отримати вивід, подібний до наведеного нижче, що вказує на те, що службу увімкнено:

```
tds@tds-VirtualBox:~$ sudo systemctl enable suricata.service
[sudo] пароль до tds:
suricata.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable suricata
```

Рис 2.2.3 `sudo systemctl enable suricata.service`

Перш ніж перейти до наступного етапу налаштування, зупиніть службу за допомогою `systemctl`:

```
sudo systemctl stop suricata.service
```

Зупинка Suricata гарантує, що коли ви редагуєте і тестуєте файл конфігурації, будь-які зміни, які ви вносите, будуть перевірені і завантажені при повторному запуску Suricata.

Пакет Suricata з репозиторіїв OISF постачається з конфігураційним файлом, який охоплює широкий спектр випадків використання. Режим за замовчуванням для Suricata - це режим IDS, тому трафік не відкидається, а лише реєструється. Залишати цей режим за замовчуванням - гарна ідея, якщо ви вивчаєте Сурікату. Після того, як ви налаштували та інтегрували Suricata у середовище, і добре розумієте, про який трафік вона вас сповіщатиме, ви можете увімкнути режим IPS.

Однак, конфігурація за замовчуванням все ще має кілька налаштувань, які вам може знадобитися змінити в залежності від вашого середовища і потреб.

Suricata може включати поле Community ID у вихідні дані JSON, щоб полегшити співставлення окремих записів про події із записами в наборах даних, створених іншими інструментами.

Якщо ви плануєте використовувати Suricata з іншими інструментами, = додавання ідентифікатора спільноти зараз є гарною ідеєю.

Щоб увімкнути цю опцію, відкрийте файл `/etc/suricata/suricata.yaml` за допомогою `vim` або вашого улюбленого редактора:

```
sudo vim /etc/suricata/suricata.yaml
```

Знайдіть рядок 120, в якому написано `# Community Flow ID`. Під цим рядком знаходиться ключ `community-id`. Встановіть його значення `true`, щоб увімкнути налаштування (Рис 2.2.4):

```
# Community Flow ID
# Adds a 'community_id' field to EVE records. These are meant to give
# records a predictable flow ID that can be used to match records to
# output of other tools such as Zeek (Bro).
#
# Takes a 'seed' that needs to be same across sensors and tools
# to make the id less predictable.

# enable/disable the community id feature.
community-id: true
# Seed value for the ID output. Valid values are 0-65535.
community-id-seed: 0
```

Рис 2.2.4 /etc/suricata/suricata.yaml

Тепер, події матимуть ідентифікатор на кшталт 1:S+3BA2UmrHK0Pk+u3XH78GAFTtQ=, який використовується для кореляції записів у різних інструментах NMS.

Збережіть і закрийте файл /etc/suricata/suricata.yaml.

Також знадобиться замінити мережевий інтерфейс за замовчуванням, на якому Suricata буде перевіряти трафік. Конфігураційний файл, який постачається з пакетом OISF Suricata, за замовчуванням перевіряє трафік на пристрої з назвою eth0. В системі використовується інший мережевий інтерфейс за замовчуванням, потрібно змінити це значення.

Щоб визначити назву пристрою мережевого інтерфейсу за замовчуванням, потрібно скористатися командою `ip` наступним чином(Рис 2.2.5):

`ip -p -j route show default`

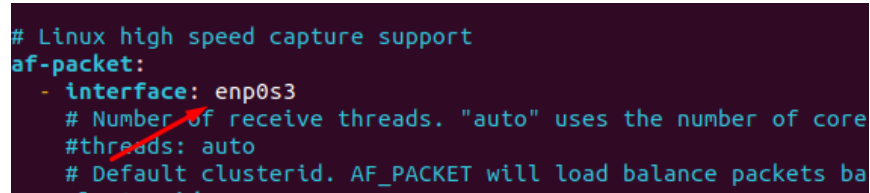
```
tds@tds-VirtualBox:~$ ip -p -j route show default
[ {
  "dst": "default",
  "gateway": "10.0.2.2",
  "dev": "enp0s3",
  "protocol": "dhcp",
  "metric": 100,
  "flags": [ ]
} ]
```

Рис 2.2.5 `ip -p -j route show default`

Рядок `dev` вказує на пристрій за замовчуванням. У наведеному прикладі виводу пристроєм є виділений інтерфейс `eth0`. У вашому виведенні може бути показано назву пристрою, наприклад, `ens...` або `eno....` Якою б не була назва, запишіть її.

Тепер редагуємо конфігурацію Suricata і перевіряємо назву інтерфейсу. Відкриваємо файл конфігурації `/etc/suricata/suricata.yaml` та змінюємо інтерфейс(Рис.2.2.6)

sudo vim /etc/suricata/suricata.yaml



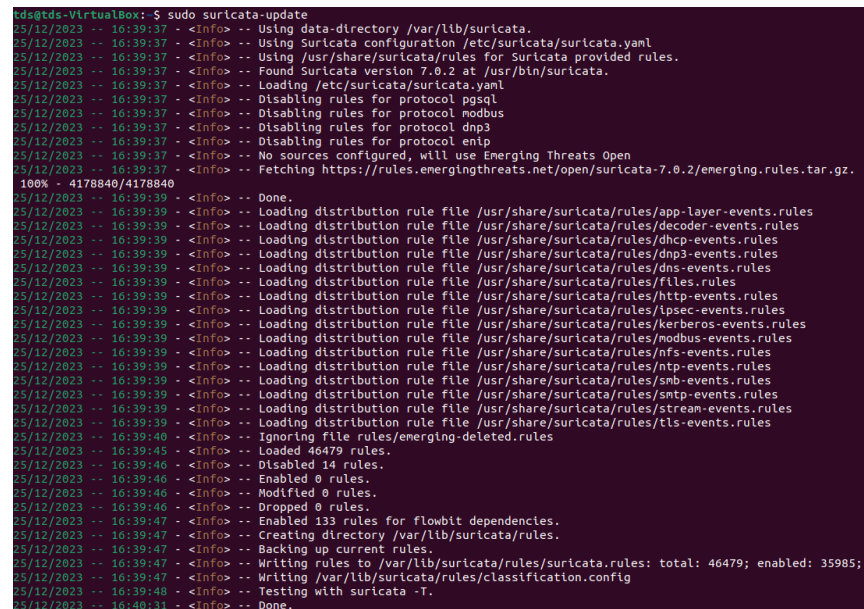
```
# Linux high speed capture support
af-packet:
- interface: enp0s3
  # Number of receive threads. "auto" uses the number of core
  #threads: auto
  # Default clusterid. AF_PACKET will load balance packets ba
```

Рис.2.2.6 *sudo vim /etc/suricata/suricata.yaml*

За замовчуванням пакет Suricata містить обмежений набір правил виявлення (в каталозі `/etc/suricata/rules`), тому ввімкнення Suricata на цьому етапі виявить лише обмежену кількість поганого трафіку.

Suricata містить інструмент під назвою `suricata-update`, який може отримувати набори правил від зовнішніх провайдерів. Запустимо його, щоб завантажити оновлений набір правил для сервера Suricata(Рис 2.2.7):

sudo suricata-update



```
ids@ids-VirtualBox:~$ sudo suricata-update
25/12/2023 -- 16:39:37 -- <info> -- Using data-directory /var/lib/suricata.
25/12/2023 -- 16:39:37 -- <info> -- Using Suricata configuration /etc/suricata/suricata.yaml
25/12/2023 -- 16:39:37 -- <info> -- Using /usr/share/suricata/rules for Suricata provided rules.
25/12/2023 -- 16:39:37 -- <info> -- Found Suricata version 7.0.2 at /usr/bin/suricata.
25/12/2023 -- 16:39:37 -- <info> -- Loading /etc/suricata/suricata.yaml
25/12/2023 -- 16:39:37 -- <info> -- Disabling rules for protocol pgsq
25/12/2023 -- 16:39:37 -- <info> -- Disabling rules for protocol modbus
25/12/2023 -- 16:39:37 -- <info> -- Disabling rules for protocol dnp3
25/12/2023 -- 16:39:37 -- <info> -- Disabling rules for protocol enip
25/12/2023 -- 16:39:37 -- <info> -- No sources configured, will use Emerging Threats Open
25/12/2023 -- 16:39:37 -- <info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.2/emerging.rules.tar.gz.
100% - 4178840/4178840
25/12/2023 -- 16:39:39 -- <info> -- Done.
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/app-layer-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/decoder-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/dhcp-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/dnp3-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/dns-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/files.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/http-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/ipsec-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/kerberos-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/modbus-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/nfs-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/ntp-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/smb-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/stream-events.rules
25/12/2023 -- 16:39:39 -- <info> -- Loading distribution rule file /usr/share/suricata/rules/tls-events.rules
25/12/2023 -- 16:39:40 -- <info> -- Ignoring file rules/emerging-deleted.rules
25/12/2023 -- 16:39:45 -- <info> -- Loaded 46479 rules.
25/12/2023 -- 16:39:46 -- <info> -- Disabled 14 rules.
25/12/2023 -- 16:39:46 -- <info> -- Enabled 0 rules.
25/12/2023 -- 16:39:46 -- <info> -- Modified 0 rules.
25/12/2023 -- 16:39:46 -- <info> -- Dropped 0 rules.
25/12/2023 -- 16:39:47 -- <info> -- Enabled 133 rules for flowbit dependencies.
25/12/2023 -- 16:39:47 -- <info> -- Creating directory /var/lib/suricata/rules.
25/12/2023 -- 16:39:47 -- <info> -- Backing up current rules.
25/12/2023 -- 16:39:47 -- <info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 46479; enabled: 35985;
25/12/2023 -- 16:39:47 -- <info> -- Writing /var/lib/suricata/rules/classification.config
25/12/2023 -- 16:39:48 -- <info> -- Testing with suricata -T.
25/12/2023 -- 16:40:31 -- <info> -- Done.
```

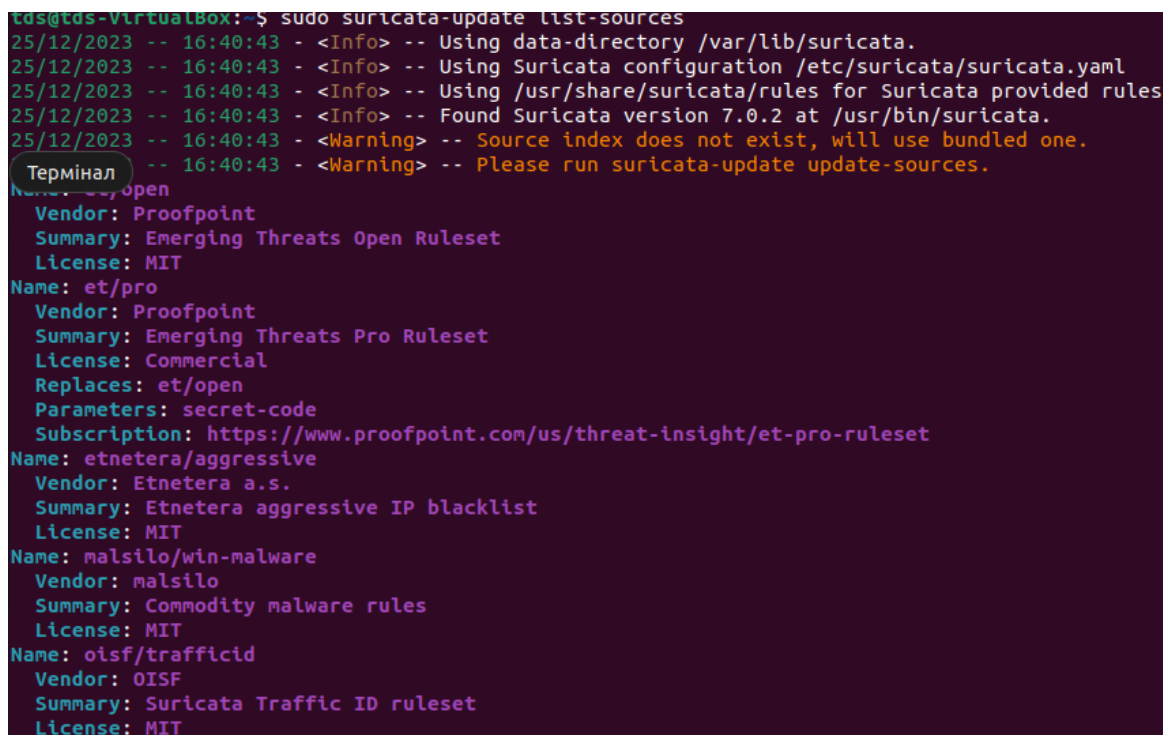
Рис 2.2.7 *sudo suricata-update*

Інструмент оновлення `suricata` може отримувати правила з різних безкоштовних і комерційних постачальників наборів правил. Деякі набори правил, такі як

набір ET Open, який був вже доданий, доступні безкоштовно, тоді як інші вимагають платної підписки.[16]

Щоб отримати набір постачальників правил за замовчуванням, використаємо flag `list-sources` у `suricata-update` таким чином(Рис 2.2.8):

`sudo suricata-update list-sources`



```

tds@tds-VirtualBox:~$ sudo suricata-update list-sources
25/12/2023 -- 16:40:43 - <Info> -- Using data-directory /var/lib/suricata.
25/12/2023 -- 16:40:43 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
25/12/2023 -- 16:40:43 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules
25/12/2023 -- 16:40:43 - <Info> -- Found Suricata version 7.0.2 at /usr/bin/suricata.
25/12/2023 -- 16:40:43 - <Warning> -- Source index does not exist, will use bundled one.
25/12/2023 -- 16:40:43 - <Warning> -- Please run suricata-update update-sources.

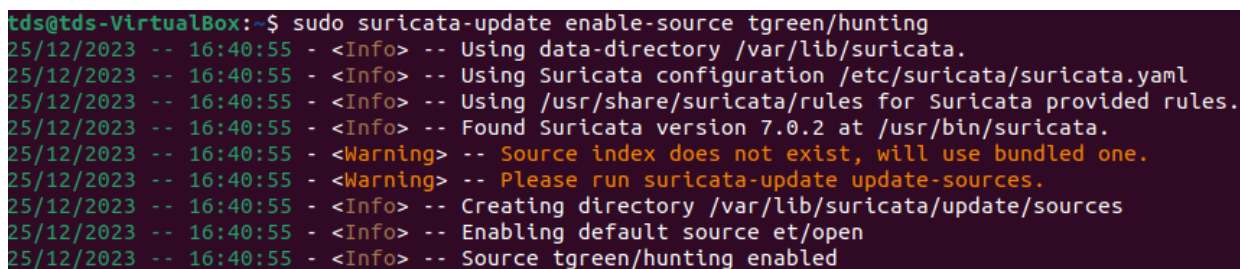
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
Name: etnetera/aggressive
  Vendor: Etnetera a.s.
  Summary: Etnetera aggressive IP blacklist
  License: MIT
Name: malsilo/win-malware
  Vendor: malsilo
  Summary: Commodity malware rules
  License: MIT
Name: oisf/trafficid
  Vendor: OISF
  Summary: Suricata Traffic ID ruleset
  License: MIT

```

Рис 2.2.8 Початок `sudo suricata-update list-sources`

Встановимо, наприклад, набір правил `tgreen/hunting`. Це можна зробити за допомогою наступної команди(Рис 2.2.9) :

`sudo suricata-update enable-source tgreen/hunting`



```

tds@tds-VirtualBox:~$ sudo suricata-update enable-source tgreen/hunting
25/12/2023 -- 16:40:55 - <Info> -- Using data-directory /var/lib/suricata.
25/12/2023 -- 16:40:55 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
25/12/2023 -- 16:40:55 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
25/12/2023 -- 16:40:55 - <Info> -- Found Suricata version 7.0.2 at /usr/bin/suricata.
25/12/2023 -- 16:40:55 - <Warning> -- Source index does not exist, will use bundled one.
25/12/2023 -- 16:40:55 - <Warning> -- Please run suricata-update update-sources.
25/12/2023 -- 16:40:55 - <Info> -- Creating directory /var/lib/suricata/update/sources
25/12/2023 -- 16:40:55 - <Info> -- Enabling default source et/open
25/12/2023 -- 16:40:55 - <Info> -- Source tgreen/hunting enabled

```

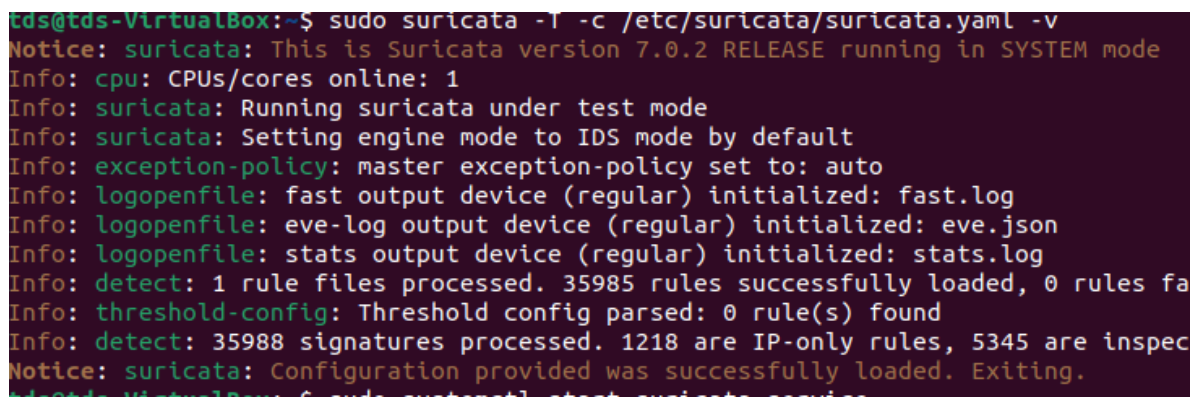
Рис 2.2.9 `sudo suricata-update enable-source tgreen/hunting`

Потім знову запусимо `suricata-update`, і новий набір правил буде додано на додаток до існуючих правил ET Open

Тепер, коли відредагували конфігураційний файл Suricata, включили необов'язковий ідентифікатор спільноти та вказали мережевий інтерфейс за замовчуванням доцільно протестувати конфігурацію.

Suricata має вбудований режим тестування, який перевірить конфігураційний файл і всі включені в нього правила на валідність. Перевірте ваші зміни з попереднього розділу, використовуючи прапорець `-T`, щоб запустити Suricata в тестовому режимі. Прапорець `-v` виведе деяку додаткову інформацію, а прапорець `-c` вкаже Suricata, де знайти її конфігураційний файл(Рис 2.2.10):

```
sudo suricata -T -c /etc/suricata/suricata.yaml -v
```



```
tds@tds-VirtualBox:~$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
Notice: suricata: This is Suricata version 7.0.2 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 1
Info: suricata: Running suricata under test mode
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 35985 rules successfully loaded, 0 rules fa
Info: threshold-config: Threshold config parsed: 0 rule(s) found
Info: detect: 35988 signatures processed. 1218 are IP-only rules, 5345 are inspec
Notice: suricata: Configuration provided was successfully loaded. Exiting.
```

Рис 2.2.10 `sudo suricata -T -c /etc/suricata/suricata.yaml -v`

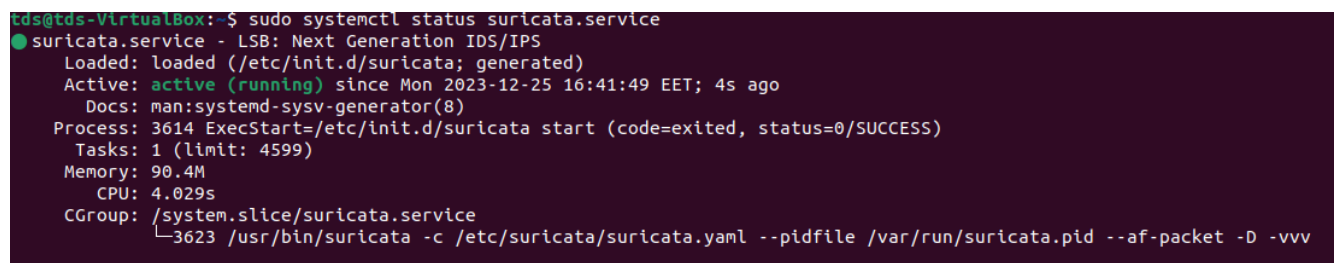
Тепер, коли є правильна конфігурація Suricata і набір правил, можемо запустити сервер Suricata використовуючи наступну команду `systemctl`::

```
sudo systemctl start suricata.service
```

Перевіряємо стан служби за допомогою команди `systemctl status`(Рис 2.2.11):

```
sudo systemctl status suricata.service
```

```
sudo systemctl status suricata.service
```



```
tds@tds-VirtualBox:~$ sudo systemctl status suricata.service
● suricata.service - LSB: Next Generation IDS/IPS
   Loaded: loaded (/etc/init.d/suricata; generated)
   Active: active (running) since Mon 2023-12-25 16:41:49 EET; 4s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 3614 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
    Tasks: 1 (limit: 4599)
   Memory: 90.4M
      CPU: 4.029s
   CGroup: /system.slice/suricata.service
           └─3623 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid --af-packet -D -vvv
```

Рис 2.2.11 `sudo systemctl status suricata.service`

Завантажений набір правил ET Open містить понад 30000 правил.

Протестуємо правило ET Open з номером 2100498 за допомогою команди curl.

Виконаємо наступне, щоб згенерувати HTTP-запит, який поверне відповідь, що відповідає правилу попередження Suricata:

curl http://testmynids.org/uid/index.html

```
tds@tds-VirtualBox:~$ curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
```

Рис 2.2.12 curl http://testmynids.org/uid/index.html

Дані відповіді в цьому прикладі призначені для того, щоб викликати сповіщення, вдаючи, що вони повертають результат команди типу id, яка може бути запущена на скомпрометованій віддаленій системі за допомогою веб-оболонки.

Тепер перевіримо журнали Suricata на наявність відповідного попередження. Існує два журнали, які увімкнено в конфігурації Suricata за замовчуванням. Перший знаходиться в /var/log/suricata/fast.log, а другий - машинозчитуваний журнал в /var/log/suricata/eve.log.[17]

Щоб перевірити наявність запису в журналі /var/log/suricata/fast.log, який відповідає запиту curl, скористаємося командою grep. Використовуючи ідентифікатор правила 2100498 з документації Quickstart, знайдемо записи, які йому відповідають, за допомогою наступної команди(Рис 2.2.13):

grep 2100498 /var/log/suricata/fast.log

```
tds@tds-VirtualBox:~$ grep 2100498 /var/log/suricata/fast.log
12/25/2023-17:04:30.612184  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned
root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 13.32.110.104
:80 -> 10.0.2.15:47330
```

Рис 2.2.13 grep 2100498 /var/log/suricata/fast.log

2.3 Аналіз інших систем безпеки та інтеграція з ними

Ця частина дипломної роботи присвячена аспектам інтеграції обраної системи виявлення вторгнень, Suricata, з іншими сучасними системами безпеки. Мета цього дослідження полягає в розкритті можливостей оптимізації та посилення ефективності Suricata через взаємодію з різними компонентами кібербезпекового стеку.

В контексті застосування Suricata для виявлення вторгнень в мережах малого бізнесу, наша робота розглядає проблеми та перспективи інтеграції з іншими системами безпеки з метою створення комплексної та злагодженої оборони від сучасних кіберзагроз.

2.3.1 Elasticsearch

Elasticsearch - це розподілена система для зберігання та пошуку великими обсягами даних в реальному часі. Вона базується на відкритому коді та використовує Apache Lucene для повнотекстового пошуку та аналізу. Ваш запит до Elasticsearch може бути структурованим запитом SQL-подібною мовою, яка дозволяє швидко та ефективно витягувати інформацію з великого обсягу даних.

Основні характеристики Elasticsearch:

Розподілена архітектура: Elasticsearch розроблено для масштабованості та ефективної роботи з великими обсягами даних. Він розподілений на вузли (nodes), які можуть бути розгорнуті на різних серверах, але діють як єдина система.

Індексація та пошук в реальному часі: Elasticsearch забезпечує швидку індексацію та можливість виконувати пошук в режимі реального часу, що робить його ідеальним для систем, де швидкість важлива[19].

Повнотекстовий пошук: Використовуючи Apache Lucene, Elasticsearch забезпечує повнотекстовий пошук, який враховує не тільки сам текст, але і його семантичний зміст, що дозволяє точні та контекстні результати.

RESTful API: Elasticsearch надає RESTful API, що дозволяє взаємодіяти з ним з використанням звичайних HTTP-запитів. Це спрощує роботу з Elasticsearch та інтеграцію з різними системами.

Можливості аналізу: Elasticsearch має вбудовані можливості аналізу даних, включаючи можливості обробки та агрегації даних, а також можливості визначення власних аналізаторів для оптимізації обробки текстових даних.

Щодо використання Elasticsearch з Suricata[17]:

Спеціалізований пошук логів: Elasticsearch може використовуватися для зберігання та пошуку логів великими обсягами даних, що робить його ідеальним для систем моніторингу мережі, таких як Suricata.

Швидкий та ефективний пошук: Elasticsearch надає швидкий та ефективний спосіб здійснення пошуку в реальному часі в журналах, що генеруються Suricata.

Можливості агрегації: Ви можете використовувати можливості агрегації Elasticsearch для отримання статистики та висновків з логів Suricata.

Гнучкість та легкість інтеграції: Elasticsearch можна легко інтегрувати з іншими інструментами для визначення та візуалізації результатів моніторингу мережі.

Встановлення Elasticsearch з Suricata допоможе вам створити потужний та ефективний інструмент моніторингу мережі з можливістю швидкого та точного пошуку великими обсягами даних.

2.3.2 Kibana

Kibana - це веб-інтерфейс для візуалізації та аналізу даних, які зберігаються в Elasticsearch. Використовуючи Kibana, ви можете легко створювати різноманітні візуальні елементи, такі як графіки, діаграми, таблиці, які надають інтуїтивний та інтерактивний інтерфейс для розуміння та аналізу великих обсягів даних.

Основні функції Kibana:

Дашборди: Kibana дозволяє створювати дашборди, які об'єднують різноманітні візуальні елементи на одному екрані. Дашборди можна налаштовувати та призначати для відображення конкретних аспектів даних.

Візуалізації: Ви можете створювати різноманітні візуальні елементи, такі як графіки, кругові діаграми, картки теплової мапи та інші, для представлення та аналізу ваших даних.

Пошук та фільтрація: Kibana забезпечує потужні засоби пошуку та фільтрації даних. Ви можете використовувати складні запити та створювати фільтри для точного визначення даних, які вас цікавлять.

Розділення на індекси: Дані в Elasticsearch зазвичай розділяються на індекси. Kibana дозволяє вам вибирати конкретні індекси для аналізу та візуалізації.

Легкість використання: Kibana має інтуїтивний та дружелюбний інтерфейс, який дозволяє швидко орієнтуватися та використовувати різні функції.

Чому встановлювати Kibana разом із Suricata:

Моніторинг мережі в реальному часі: Kibana може відобразити дані в реальному часі, що дозволяє миттєво спостерігати за активністю мережі, виявляти загрози та реагувати на них.

Легка аналітика та візуалізація: Kibana надає зручні інструменти для аналізу та візуалізації журналів Suricata. Ви можете створювати графіки, таблиці та інші елементи, що допомагають розуміти та визначати патерни в мережевому трафіку.

Зручне створення звітів та аналітичних панелей: Kibana дозволяє вам створювати красиві звіти та аналітичні панелі для презентації результатів аналізу мережі.

Спільна інтеграція з Elasticsearch: Kibana тісно інтегрована з Elasticsearch, що полегшує використання всіх переваг розподіленого зберігання та швидкого пошуку.

Встановлення Kibana забезпечить потужний інструмент для аналізу та візуалізації даних, які Suricata збирає, сприяючи ефективному моніторингу мережі та виявленню потенційних загроз.

2.3.3 Filebeat

Filebeat - це легкий агент для пересилання та агрегації лог-файлів з різних джерел до систем зберігання та аналізу, таких як Elasticsearch або Logstash. Filebeat розроблений Elastic і є частиною Elastic Stack, який також включає Elasticsearch, Kibana та Logstash. Основною функцією Filebeat є надсилання лог-даних з різних джерел до централізованого місця для подальшого аналізу та візуалізації.

Основні характеристики Filebeat:

Легкість встановлення та використання: Filebeat має простий процес встановлення і конфігурації, що дозволяє швидко розпочати збір та надсилання лог-даних.

Автоматична відстеження змін: Filebeat відстежує зміни в лог-файлах та надсилає тільки нові або змінені записи, що дозволяє ефективно використовувати мережевий ресурс.

Підтримка різних джерел: Filebeat підтримує зчитування лог-файлів з різних джерел, таких як системні логи, логи веб-серверів, логи додатків та інші.

Модульна архітектура: Filebeat використовує модульну архітектуру, що дозволяє додавати різні модулі для обробки конкретних видів лог-даних, спрощуючи конфігурацію.

Інтеграція з Elastic Stack: Filebeat легко інтегрується з іншими компонентами Elastic Stack, зокрема з Elasticsearch, для подальшої обробки та аналізу даних.

Чому встановлювати Filebeat разом із Suricata:

Централізований збір та аналіз лог-даних: Filebeat дозволяє централізовано збирати лог-дані з різних джерел, включаючи лог-файли Suricata, для подальшого аналізу та візуалізації.

Відслідковування та агрегація подій: Filebeat може агрегувати дані з різних джерел у централізований потік подій, що полегшує відстеження подій та виявлення патернів.

Мінімізація втрати даних: Filebeat надсилає лише нові або змінені записи, що дозволяє мінімізувати втрату даних та оптимізувати використання мережевих ресурсів.

Легка інтеграція з Elastic Stack: Filebeat легко інтегрується з Elasticsearch, що спрощує подальшу аналітику та візуалізацію лог-даних з використанням Kibana.

Модульність та розширюваність: Filebeat може бути розширений за допомогою модулів для обробки різноманітних лог-форматів, зокрема лог-файлів Suricata, забезпечуючи гнучкість та можливість адаптації до різних вимог.

Встановлення Filebeat для збору лог-даних від Suricata дозволить вам ефективно використовувати та аналізувати дані, що Suricata збирає, а також інтегрувати їх у централізований моніторинг та аналітику за допомогою Elastic Stack.

Висновки до розділу 2

В другому розділі було розглянуто та проаналізовано СВВ такі як Snort, Suricata та Zeek(Bro). Після порівняльного аналізу враховуючи обране середовище (малий офіс юридичної фірми) для виконання поставлених задач було обрано Suricata.

Налаштували Suricata

Встановили і налаштували Elasticsearch і Kibana на окремому сервері. налаштували обидва інструменти так, щоб вони були доступні на приватній IP-адресі. Також налаштували параметри автентифікації Elasticsearch і Kibana за допомогою модуля безпеки храск, який входить до складу кожного інструменту.

Після завершення кроків з налаштування Elasticsearch і Kibana, встановили і налаштували Filebeat на сервері Suricata. За допомогою Filebeat заповнили інформаційні панелі Kibana і почали надсилати логи Suricata до Elasticsearch.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1. Вибір обладнання для тестового середовища

Для мережі було обрано маршрутизатор Cisco ISR4331(Рис. 3.1). Модель маршрутизатора має пропускну швидкість від 100 до 300 Мбіт, 3 порти для WAN або LAN 10/100/100. Два порти RJ-45, та два порти SFP. Також роутер має слот для модуля SM-X та декілька слотів для NIM (Network Interface Modules)(Рис. 3.2). Загальна пам'ять маршрутизатора становить 4 Гб у стандарті, та може бути розширена до 16 Гб, як і Флеш-пам'ять.

Серія Cisco 4331 розроблена з урахуванням вимог додатків сьогоденних філій з гнучкістю дизайну для майбутніх застосувань. Модульна архітектура розроблена для підтримки розширених вимог клієнтів, збільшення пропускну здатності та повністю інтегрованого розподілу потужності для модулів.

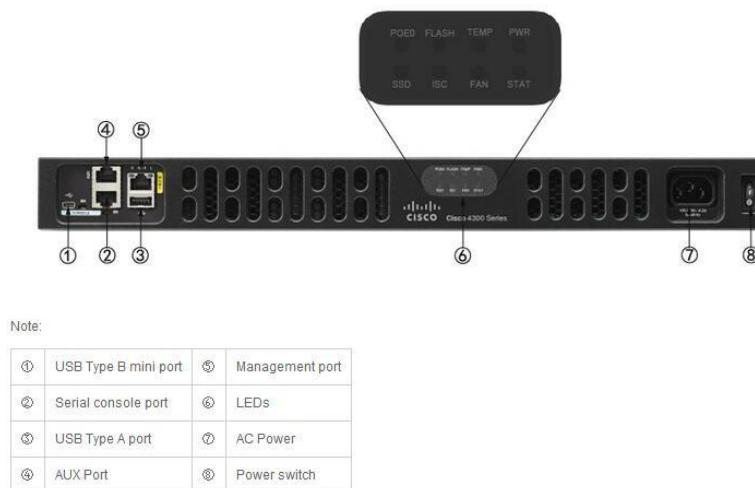


Рис. 3.1 Маршрутизатор Cisco ISR4331/K9

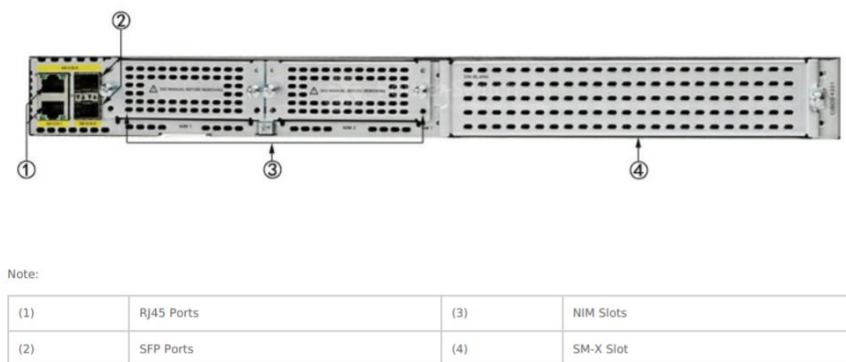


Рис. 3.2 Модулі маршрутизатора ISR4331/K9

Кількість портів комутатора є суттєвим фактором при виборі, також як і швидкість передачі портів. У даній мережі було використано виключно багаторівневі комутатори на 24 порти. Найбільш оптимальним є комутатор Cisco Catalyst 3650-24PS, (Рис 3.3).



Рисунок 3.3 – Cisco Catalyst 3650-24PS

Cisco Catalyst 3650-24PS – це комутатор наступного покоління, що може забезпечити основу для повного зближення провідних та бездротових мереж на одній платформі. Серія 3650 побудована на вдосконаленому Cisco StackWise®-160 і користується новою інтегральною схемою (ASIC), специфічною для додатків Cisco Unified Access™ (UADP). 3650 також мають 12-дюймовий фактор нижчої форми глибини, так що ви можете розмістити їх у щільних серверних шафах у віддалених відділеннях та офісах, де його позиція може викликати занепокоєння. Крім того, багатогігабітні комутатори 3650 підтримують швидкість та стандарти бездротового зв'язку поточного та нового покоління (включаючи 802.11ac Wave 2) для існуючої інфраструктури кабелів.



Рис. 3.4 Модулі комутатора Cisco Catalyst 3650

3.2. Тестування ефективності

Тепер, коли все налаштовано можемо перейти до тестування ефективності встановленої раніше системи виявлення вторгнень Suricata та доповнень до неї, а саме Elasticsearch, Kibana і Filebeat.

Спочатку перевіримо пустий лог Elastic

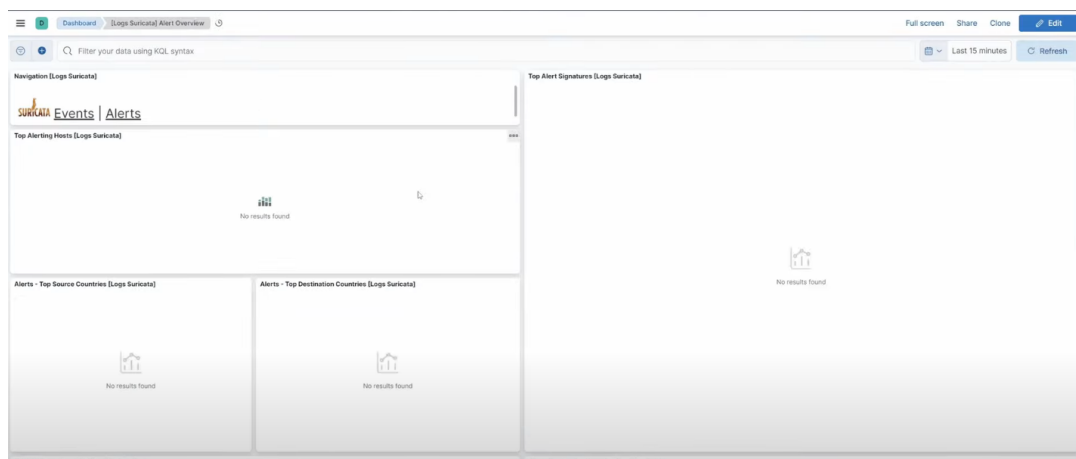


Рис 3.5 Пустий лог

Після цього виконаємо команду:

```
curl http://testmynids.org/uid/index.html
```

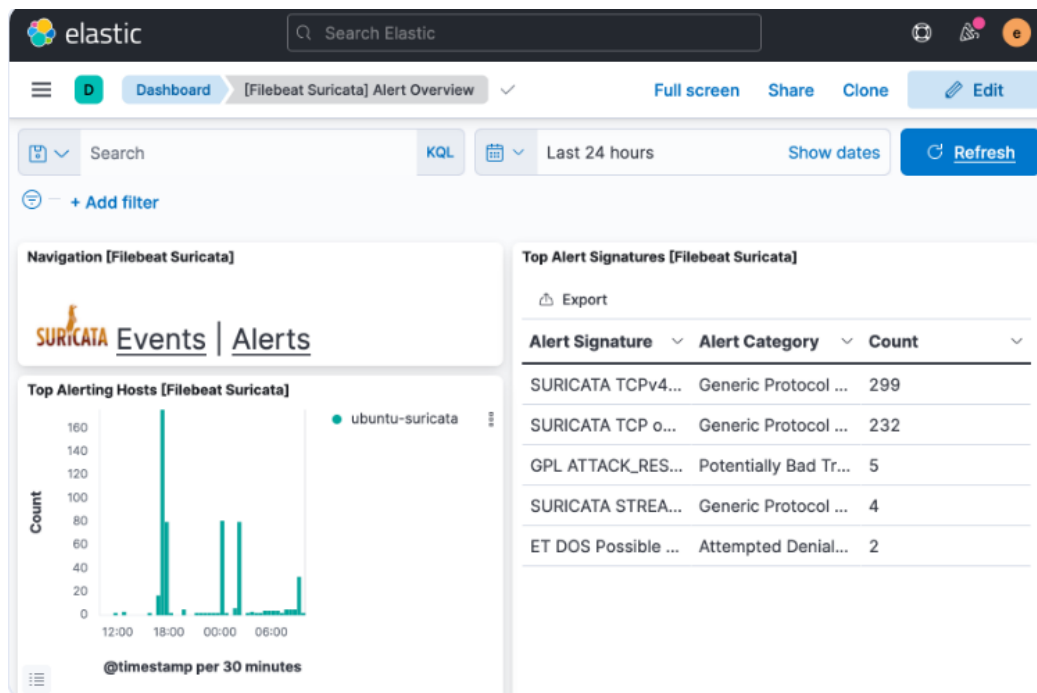
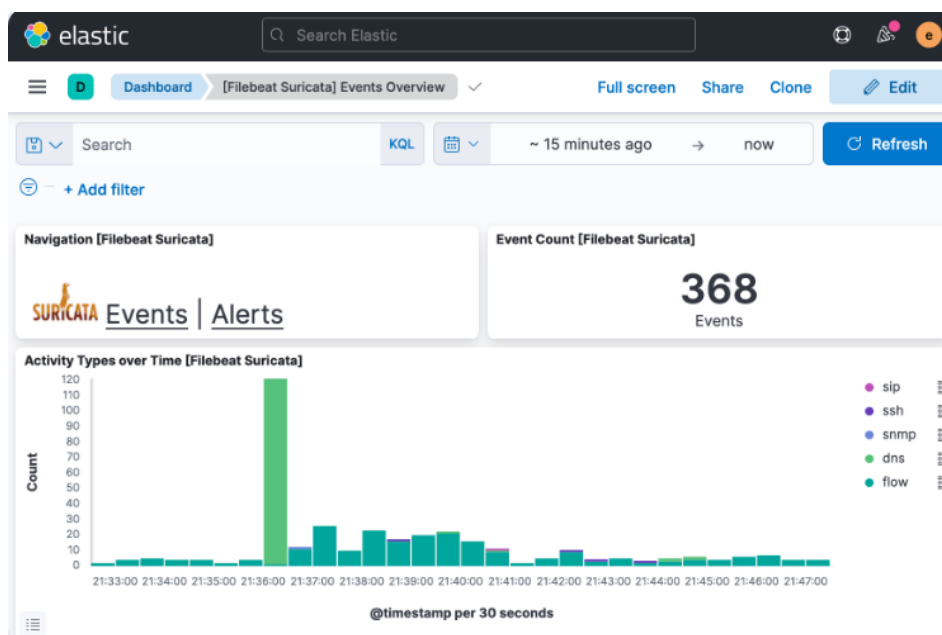


Рис 3.6 Suricata Alerts dashboard

Бачимо що дані про це були записані, перейдемо до вкладки Events



3.7 Інформаційна панель Kibana, яка показує огляд усіх зареєстрованих подій Suricata

Перейдемо за посиланням <https://github.com/3coresec/testmynids.org>.

Це, за словами автора, простий проект, який має на меті централізувати тестування на виявлення зловмисних подій системами виявлення вторгнень (IDS). Качаємо скрипт за посиланням, робимо його виконуючим файлом (.exe) та запускаємо. Нас зустрічає вікно (Рис 3.8)

```

  _____
 |  _   _  |
 | | | | | |
 | |_| | | |
 |  _  | | |
 | | | | | |
 |_|_|_|_|_|

tmNIDS - NIDS detection tester - @3CORESec
Project: https://github.com/3CORESec/testmynids.org

Choose which test you'd like to run:

1) Linux UID
2) HTTP Basic Authentication
3) HTTP Malware User-Agent
4) Bad Certificate Authorities
5) Tor .onion DNS response and known IPs connection
6) EXE or DLL download over HTTP
7) PDF download with Embedded File
8) Simulate SSH Outbound Scan
9) Miscellaneous domains (TLD's, Sinkhole, DDNS, etc)
10) Anonymous filesharing website
11) CHAOS! RUN ALL!
12) Quit!
#? █

```

Рис 3.8 Скрипт tmNIDS

Прописуємо 11, щоб запустити все та переходимо до elastic. Тиснемо кнопку refresh (Рис 3.9) І бачимо такий результат (Рис 3.10.1)

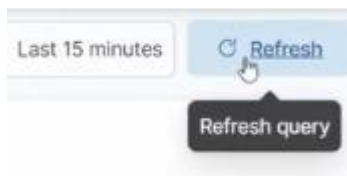


Рис 3.9 Кнопка refresh

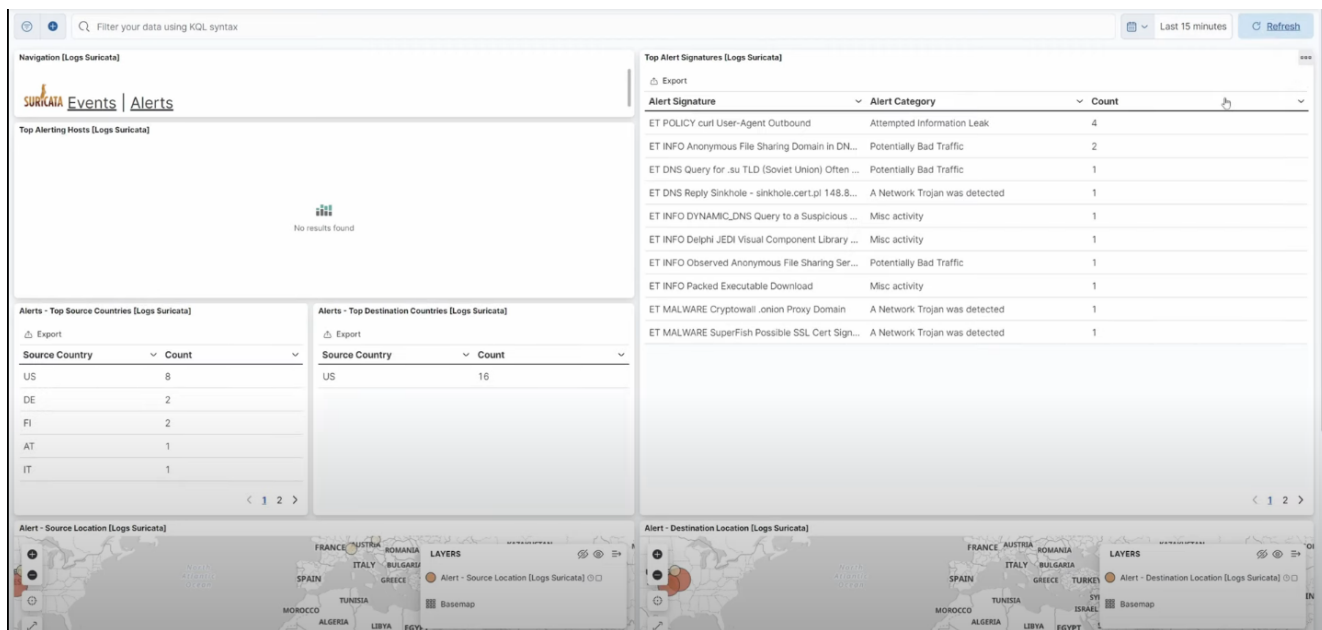


Рис 3.10. Інтерфейс elastic після скрипта

Перейдемо до вкладки Suricata Events Dashboard та подивимося що там (Рис 3.11)

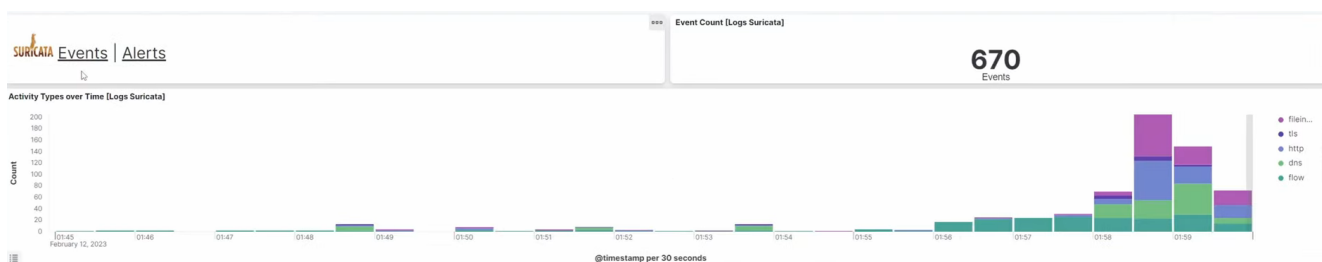


Рис 3.11 Suricata Events Dashboard

Після перевірки працездатності бачимо, що всі запити, надіслані скриптом були знайдені та записані до логів.

3.3. Аналіз впливу Suricata на загальну кібербезпеку малого бізнесу

1. Виявлення та Запобігання Атак:

- *Переваги:* Suricata забезпечує високоефективне виявлення та запобігання різноманітних кібератак, включаючи вторгнення, віруси, та шкідливі програми.
- *Вплив:* Забезпечення надійного виявлення атак важливо для малого бізнесу, оскільки це дозволяє уникати потенційних втрат і зберегти конфіденційність даних.

2. Продуктивність та Масштабованість:

- *Переваги:* Suricata володіє високою продуктивністю та масштабованістю, що робить її придатною для використання в мережах будь-якого розміру.
- *Вплив:* Малі бізнеси можуть використовувати Suricata навіть з обмеженими ресурсами, забезпечуючи ефективність та масштабованість в залежності від зростання бізнесу.

3. Конфігурація та Налаштування:

- *Переваги:* Suricata має гнучку систему налаштувань, яка дозволяє адаптувати його до конкретних потреб та характеристик мережі малого бізнесу.
- *Вплив:* Зручність налаштування дозволяє ефективно використовувати Suricata навіть для тих, хто не має великого досвіду у сфері кібербезпеки.

4. Відкритий Код та Спільнота:

- *Переваги:* Як відкритий код, Suricata має активну спільноту, яка постійно вдосконалює та оновлює систему.
- *Вплив:* Можливість залучення до спільноти та використання безкоштовних ресурсів забезпечує стабільність та тривалу підтримку.

5. Інтеграція з Іншими Системами:

- *Переваги:* Suricata може ефективно інтегруватися з іншими системами безпеки та інструментами, що підвищує його функціональність.
- *Вплив:* Інтеграція дозволяє створити комплексну систему безпеки для захисту від різних видів загроз.

6. Вартість та Віддача від Інвестицій:

- *Переваги:* Suricata є безкоштовним та відкритим програмним забезпеченням, що знижує витрати на кібербезпеку.
- *Вплив:* Доступність безкоштовного рішення позитивно впливає на бюджет малого бізнесу, забезпечуючи віддачу від інвестицій.

7. Адаптованість до Загроз:

- *Переваги:* Suricata постійно оновлюється для виявлення нових та розвиваючихся загроз.
- *Вплив:* Здатність адаптуватися до нових загроз дозволяє малому бізнесу ефективно захищати свою мережу від постійно змінюючихся атак.

Враховуючи переваги Suricata, можна визначити його значний позитивний вплив на загальну кібербезпеку малого бізнесу, забезпечуючи ефективну та доступну систему виявлення вторгнень.

Висновки до розділу 3

В 3 розділі проаналізовано компоненти, які складають мережу офісу малої юридичної фірми.

Протестовано працездатність за допомогою спеціально розробленої для цього утіліти та отримали позитивний результат.

Проаналізовано вплив Suricata на загальну кібербезпеку малого бізнесу, та виявлено що, Suricata навіть для тих, хто не має великого досвіду у сфері кібербезпеки, забезпечує високоефективне виявлення та запобігання різноманітних кібератак, включаючи вторгнення, віруси, та шкідливі програми. Також є гнучкою для інтегрування додаткових систем безпеки при тому є безкоштовною та невибагливою до ресурсів.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було розглянуто сучасні системи виявлення вторгнень, інтеграції з різними системами безпеки, їх переваги та недоліки

Досліджено, що системи виявлення вторгнень (IDS) відіграють важливу роль у забезпеченні інформаційної безпеки мереж будь-якого розміру, включаючи бізнес-мережі. Їх основна функція полягає у виявленні та запобіганні будь-яким діям, що відбуваються в мережі, таким як атаки на сервери, крадіжка даних та розповсюдження шкідливого програмного забезпечення.

Було розглянуто та проаналізовано СВВ такі як Snort, Suricata та Zeek(Bro). Після порівняльного аналізу враховуючи обране середовище (малий офіс юридичної фірми) для виконання поставлених задач було обрано Suricata.

Встановили і налаштували Elasticsearch і Kibana на окремому сервері. налаштували обидва інструменти так, щоб вони були доступні на приватній IP-адресі. Також налаштували параметри автентифікації Elasticsearch і Kibana за допомогою модуля безпеки храск, який входить до складу кожного інструменту.

Після завершення кроків з налаштування Elasticsearch і Kibana, встановили і налаштували Filebeat на сервері Suricata. За допомогою Filebeat заповнили інформаційні панелі Kibana і почали надсилати логи Suricata до Elasticsearch.

Проаналізовано вплив на загальну кібербезпеку малого бізнесу

В результаті отримана систему виявлення вторгнень, яка буде коректно функціонувати, швидко отримувати найновіші оновлення, буде безкоштовною та не вибагливою до системи.

Зважаючи на все вище сказане, можна вважати мету кваліфікаційної роботи успішно досягнутою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Scarfone Karen. Guide to Intrusion Detection and Prevention Systems (IDPS) – 2007. — 127 p.
2. Mattord Verma. Principles of Information Security — 2008. — 300 p.
3. Sen Sevil. Power-Aware Intrusion Detection in Mobile Ad Hoc Networks — 2006. — 20 p.
4. Anderson Ross. Security Engineering: A Guide to Building Dependable Distributed Systems — 2007. — 388 p.
5. Jackson Kathleen. A Phased Approach to Network Intrusion Detection — 1991. — 30 p.
6. Syngress. Snort IDS and IPS Toolkit — 2007. — 197 p.
7. ДСТСЗІ СБ України. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» — 2003. — 16 с.
8. М. В. Грайворонський, О. М. Новіков. Безпека інформаційно-комунікаційних систем — 2009. — 608 с.
9. А. Завада, О. Самчишин, В. Охрімчук, "Аналіз сучасних систем виявлення атак і запобігання вторгненням", Інформаційні системи, Житомир: Збірник наукових праць ЖВІ НАУ, Т. 6, № 12, С. 97-106, 2012.
10. В. І. Мешков, В. О. Віролайнен, Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах, УДК 004.056+65.012.12, Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ [Електронний ресурс] – Режим доступа: URL: <https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf>
11. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему / В. В. Берковський, О. С. Безсонов // Системи управління, навігації та зв'язку. - 2017. - Вип. 3. - С. 57-62. - [Електронний ресурс] – Режим доступа: URL: http://nbuv.gov.ua/UJRN/suntz_2017_3_17
12. С. Казмірчук, А. Корченко, Т. Паращук, Аналіз систем виявлення вторгнень, ЗАХИСТ ІНФОРМАЦІЇ, ТОМ 20, №4, ЖОВТЕНЬ-ГРУДЕНЬ 2018, DOI:

10.18372/2410-7840.20.13425, УДК 004.056.53(045), С. 259-276 [Електронний ресурс]. Режим доступу: URL: <http://jrn1.nau.edu.ua/index.php/ZI/article/download/13425/18726>

13. І.Терейковський, А.Корченко, Т.Паращук, Є.Педченко, Аналіз відкритих систем виявлення вторгнень, DOI: 10.18372/2225-5036.24.13431, УДК 004.056.53(045), 2018, vol. 24, issue 3, С. 201-216

14. Cisco IPS 4500 Series. Описание продукта Cisco IPS 4500. Київ : ТОВ Інфобезпека, 2018. [Електронний ресурс]. Режим доступу: URL: http://www.infobezpeka.com/products/apatnye/Cisco_IPS_4500_Series/

15. Prelude SIEM (Intrusion Detection System) – Wikipedia, [Електронний ресурс]. Режим доступу: URL: [https://en.wikipedia.org/wiki/Prelude_SIEM_\(Intrusion_Detection_System\)](https://en.wikipedia.org/wiki/Prelude_SIEM_(Intrusion_Detection_System))

16. Camisso J. How To Build A SIEM with Suricata and Elastic Stack on Ubuntu 20.04. *DigitalOcean | Cloud Hosting for Builders*. URL: <https://www.digitalocean.com/community/tutorials/how-to-build-a-siem-with-suricata-and-elastic-stack-on-ubuntu-20-04> .

17. Camisso J. How To Create Rules, Timelines, and Cases from Suricata Events Using Kibana's SIEM Apps. *DigitalOcean | Cloud Hosting for Builders*. URL: <https://www.digitalocean.com/community/tutorials/how-to-create-rules-timelines-and-cases-from-suricata-events-using-kibana-s-siem-apps>

18. Associates C. D. How to Setup a Suricata IPS: Part 1. Critical Design. URL: <https://www.criticaldesign.net/post/how-to-setup-a-suricata-ips>.

19. Associates C. D. How to Setup a Suricata IPS: Integrating Suricata with ELK Stack. Critical Design. URL: <https://www.criticaldesign.net/post/how-to-setup-a-suricata-ips-elk-stack>.

20. Installation – Suricata 8.0.0-dev documentation. Suricata User Guide – Suricata 8.0.0-dev documentation. URL: <https://docs.suricata.io/en/latest/install.html>.