МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

МАБРОУК Аладдін Джаафарович

Система виявлення інцидентів кібербезпеки з використанням Security Onion / Cyber Security Incident Detection System Using Security Onion

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -21
А.Д. Маброук

Науковий керівник
В.В.Яцків

Кваліфікаційну роботу
допущено до захисту:

«____» _____ ___2024 р.

Завідувач кафедри
_____ **В.В.Яцків**

ТЕРНОПІЛЬ - 2024

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
«____» _____ 20___ року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

МАБРОУК АЛАДДІН ДЖААФАРОВИЧ
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Система виявлення інцидентів кібербезпеки з використанням Security Onion / Cyber Security Incident Detection System Using Security Onion
керівник роботи д.т.н., професор В.В. Яцків

затверджені наказом по університету від 12 грудня 2023 року № 753

2. Строк подання студентом закінченої кваліфікаційної роботи 12 грудня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
− проаналізувати основні компоненти та функціональні можливості Security Onion;
− розгорнути і налаштувати Security Onion у віртуалізованому середовищі за допомогою Proxmox;
− використати контейнер Ubuntu з налаштованим WireGuard для збору та аналізу трафіку з віртуальних машин (ВМ);
− налаштувати SPAN порт для перенаправлення мережевого трафіку на Security Onion, щоб забезпечити моніторинг і виявлення інцидентів.
5. Перелік графічного матеріалу у роботі:
– основні типи програмного забезпечення для моніторингу трафіку;
– класифікація програм для моніторингу трафіку;

– схема роботи віртуального маршрутизатора для передачі віддзеркаленого трафіку;

– архітектура моніторингу трафіку у віртуальному середовищі;

– алгоритм налаштування моніторингу трафіку для віртуальних машин.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 12 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз систем виявлення інцидентів кібербезпеки	12.2023 р. – 03.2024 р.	
2	Архітектура систем виявлення інцидентів кібербезпеки	03.2024 р. – 06.2024 р.	
3	Розробка та дослідження системи виявлення інцидентів кібербезпеки	06.2024 р. – 11.2024 р.	

Студент _____ А.Д. Маброук

(підпис)

Керівник роботи _____ В.В. Яцків

АНОТАЦІЯ

Кваліфікаційна робота на тему «Система виявлення інцидентів кібербезпеки з використанням Security Onion» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека та захист інформації» освітньо-професійної програми «Кібербезпека» написана обсягом 57 сторінки і містить 18 ілюстрації та 42джерела за переліком посилань.

Метою роботи є підвищення ефективності виявлення інцидентів кібербезпеки з використанням Security Onion.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи виявлення кіберзагроз, методи виявлення кібератак на основі фреймворка Security Onion..

Результати дослідження: Удосконалено алгоритми використання Security Onion у центрі операцій безпеки.

Показано можливість та переваги використання навігатора Security Onion для візуалізації та покращення можливостей виявлення загроз.

Результати роботи можуть бути застосовані при розгортанні власної системи розвідки кіберзагроз та центру безпеки операцій.

Ключові слова: SECURITY ONION, WIREGUARD, PROXMOX, КІБЕРЗАГРОЗА, МОНІТОРІНГ, SPAN-PORT, МАРШРУТИЗАТОР, ГІПЕРВІЗОР.

ABSTRACT

Qualification work on the topic "Cybersecurity Incident Detection System Using Security Onion" for obtaining the degree of "Master" in the specialty 125 "Cybersecurity and Information Protection" under the educational and professional program "Cybersecurity" consists of 57 pages and includes 18 illustrations and 42 sources listed in the references.

The purpose of the work is to enhance the effectiveness of cybersecurity incident detection using Security Onion.

Research methods. To address the tasks outlined in this qualification work, the following methods were used: methods for detecting cyber threats and methods for identifying cyberattacks based on the Security Onion framework.

Research results: Enhanced algorithms for utilizing Security Onion in a Security Operations Center.

The study demonstrates the potential and advantages of using the Security Onion navigator for visualization and improving threat detection capabilities.

The results of the work can be applied when deploying a custom cyber threat intelligence system and a Security Operations Center.

Keywords: SECURITY ONION, WIREGUARD, PROXMOX, CYBER THREAT, MONITORING, SPAN PORT, ROUTER, HYPERVISOR

ЗМІСТ

ВСТУП

У наш час кібербезпека стає дуже важливою для захисту інформаційних систем на всіх рівнях. З появою нових технологій і зростанням обсягу даних, які передаються, збільшується і кількість кіберзагроз. Це може призвести до серйозних наслідків, таких як витік конфіденційних даних, фінансові втрати або навіть проблеми з критично важливою інфраструктурою.

Щоб захиститися від таких загроз, важливо мати ефективний моніторинг і вміти вчасно виявляти потенційні атаки. Одним із популярних рішень для виявлення інцидентів у кібербезпеці є система Security Onion. Це потужний набір інструментів для моніторингу мережевого трафіку та аналізу загроз, який допомагає будувати ефективні системи для виявлення і реагування на інциденти [1, 2].

Метою цієї роботи є вивчення та аналіз можливостей системи Security Onion для моніторингу трафіку в серверному середовищі, що працює на гіпервізорі Proxmox. Досягнення визначеної мети передбачає вирішення таких завдань:

1) проаналізувати основні компоненти та функціональні можливості Security Onion;

2) розгорнути і налаштувати Security Onion у віртуалізованому середовищі за допомогою Proxmox;

3) використати контейнер Ubuntu з налаштованим WireGuard для збору та аналізу трафіку з віртуальних машин (ВМ);

4) налаштувати SPAN [20] порт для перенаправлення мережевого трафіку на Security Onion, щоб забезпечити моніторинг і виявлення інцидентів.

Об’єкт дослідження – процеси виявлення інцидентів кібербезпеки з використанням Security Onion.

Предметом дослідження – методи та алгоритми виявлення інцидентів кібербезпеки з використанням Security Onion.

Наукова новизна одержаних результатів. Удосконалено алгоритми використання Security Onion у центрі операцій безпеки.

Практичне значення отриманих результатів. Проведено налаштування віртуалізованих середовищ, а також конфігурацію мережевого трафіку за допомогою SPAN порту та WireGuard.

Публікації та апробація КР.

1. Маброук А.Д. Система виявлення інцидентів кібербезпеки з використанням SECURITY ONION. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ – 2022), Тернопіль, 2024. – С. 33–35.

2**.** Маброук А.Д. Розгортання security onion на базі гіпервізора proxmox. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. – С. 105-106.

1 АНАЛІЗ СИСТЕМ ВИЯВЛЕННЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ

1.1. Основні типи систем виявлення інцидентів кібербезпеки

Системи виявлення інцидентів кібербезпеки, або IDS (Intrusion Detection Systems), призначені для того, щоб стежити за тим, що відбувається в мережі, і виявляти можливі загрози чи підозрілу активність. Це такі собі «сигналізації» для вашої мережі, які попереджають, якщо щось пішло не так. Вони є ключовим компонентом забезпечення кібербезпеки в сучасних мережах. Вони призначені для моніторингу трафіку, виявлення аномалій та ідентифікації потенційних загроз. Основна мета IDS – виявляти вторгнення до того, як вони зможуть завдати шкоди, або фіксувати події для подальшого аналізу.

Системи виявлення вторгнень поділяються [3, 4]:

1) за місцем розташування:

– мережева IDS (NIDS). Розташовується в ключових точках мережі (наприклад, шлюзах чи хабах) і аналізує весь мережевий трафік.

– хостова IDS (HIDS). Інстальована безпосередньо на пристроях, таких як сервери чи кінцеві точки, і аналізує журнали подій та системну активність;

2) за принципом виявлення:

– сигнатурний (Signature-based). Порівнює мережеву активність із базою відомих шаблонів атак;

– аномалійний (Anomaly-based). Виявляє відхилення від нормальної поведінки системи;

– гібридний. Поєднує сигнатурний і аномалійний підходи для забезпечення більшого охоплення загроз.

Принцип роботи IDS [5, 6].

1. Збір даних:

- мережева IDS аналізує пакети в реальному часі;
- хостова IDS читає журнали подій, системні файли та стежить за поведінкою процесів.

2. Попередня обробка:

- видаляються дублікатні дані;
- пакети проходять нормалізацію, наприклад, розбирання протоколів на рівні TCP/IP.

3. Повідомлення та реакція:

- IDS може лише попереджати про можливу атаку;
- для автоматичної реакції потрібна інтеграція з IPS (Intrusion Prevention System).

Є різні види таких систем, і кожен з них має свої переваги та недоліки.

За принципом роботи системи виявлення загроз поділяються:

1) системи на основі сигнатур (Signature-based IDS). Цей тип систем працює за принципом порівняння даних, які проходять через мережу, з відомими шаблонами атак. Якщо система бачить щось, що схоже на відому атаку, вона одразу сигналізує про це. Перевага таких систем у тому, що вони дуже точно виявляють відомі загрози і майже не допускають помилок. Але їхня слабкість у тому, що вони не можуть виявити нові, невідомі атаки, для яких ще немає шаблонів;

2) системи на основі аномалій (Anomaly-based IDS). Ці системи працюють по-іншому. Вони «вивчають», як мережа зазвичай працює, і якщо помічають якісь незвичні зміни, то повідомляють про це. Вони можуть використовувати алгоритми машинного навчання або статистичні моделі для порівняння нормальної активності з поточною. Це дає їм можливість виявляти нові загрози, але часто вони можуть видавати більше помилкових спрацьовувань, оскільки нормальна діяльність мережі інколи може змінюватися;

3) гібридні системи (Hybrid IDS). Ці системи об’єднують підходи обох попередніх типів. Вони використовують як шаблони для виявлення відомих загроз, так і аналіз аномалій для знаходження нових. Це допомагає досягти балансу між точністю і здатністю знаходити нові атаки.

Кожна організація обирає ту чи іншу систему залежно від своїх потреб і типів загроз, з якими вона може зіткнутися. Іноді найкраще використовувати кілька видів систем разом, щоб максимально захистити мережу від різних видів атак.

Принцип роботи IDS.

4. Збір даних:
   - мережева IDS аналізує пакети в реальному часі;
   - хостова IDS читає журнали подій, системні файли та стежить за поведінкою процесів.
5. Попередня обробка:
   - видаляються дублікатні дані;
   - пакети проходять нормалізацію, наприклад, розбирання протоколів на рівні TCP/IP.
6. Виявлення загроз:
   - сигнатурні системи шукають збіг із відомими зразками атак (наприклад, DoS, SQL-ін’єкції).
   - аномалійні системи визначають аномалії за допомогою моделей машинного навчання, статистичних методів чи евристик.
7. Повідомлення та реакція:
   - IDS може лише попереджати про можливу атаку;
   – для автоматичної реакції потрібна інтеграція з IPS (Intrusion Prevention System).

1.2 Порівняння існуючих рішень для моніторингу трафіку

Системи виявлення вторгнень (Intrusion Detection Systems, IDS) є ключовим компонентом забезпечення кібербезпеки в сучасних мережах. Вони призначені для моніторингу трафіку, виявлення аномалій та ідентифікації потенційних загроз [7, 8].

Моніторинг трафіку – це важлива частина захисту будь-якої інформаційної системи. Для цього є багато різних інструментів, як платних, так і безкоштовних. Ось кілька найпоширеніших варіантів (рисунок 1.1).

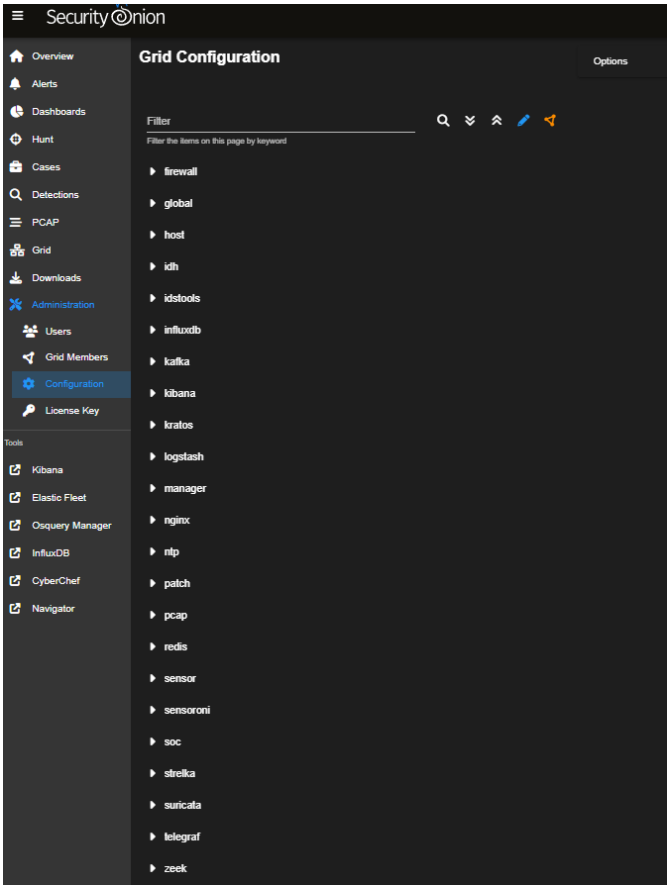

Рисунок 1.1 – список наявних компонентів в SecurityOnion

1. Snort. Snort – це дуже популярна програма з відкритим кодом, яка допомагає захищати комп'ютерні мережі. Вона працює як система для виявлення загроз та аналізу мережевого трафіку. Snort може виявляти та навіть зупиняти атаки на мережу, наприклад, якщо хтось намагається зламати сервер або отримати доступ до даних без дозволу.

Як показано на рисунку 1.2, Snort складається з п'яти основних частин. Декодер пакетів відповідає за прийом пакетів від різних мережевих інтерфейсів і проведення первинного аналізу пакетів. Препроцесор – це плагін для подальшої обробки декодованих пакетів. Його функції включають нормалізацію URI HTTP, дефрагментацію пакетів, повторне збирання потоку

TCP тощо. Ядром Snort є механізм виявлення, який може зіставляти пакети відповідно до налаштованих правил. Зіставлення правил має вирішальне значення для загальної продуктивності Snort. Після успішного зіставлення система сповіщає систему журналювання та оповіщення на основі поведінки, визначеної в правилах. Тоді система виведе попередження або відповідно зареєструє. Користувачі також можуть визначити модуль виводу для збереження сповіщень або журналів у певній формі, такій як база даних або файл XML [9, 10].

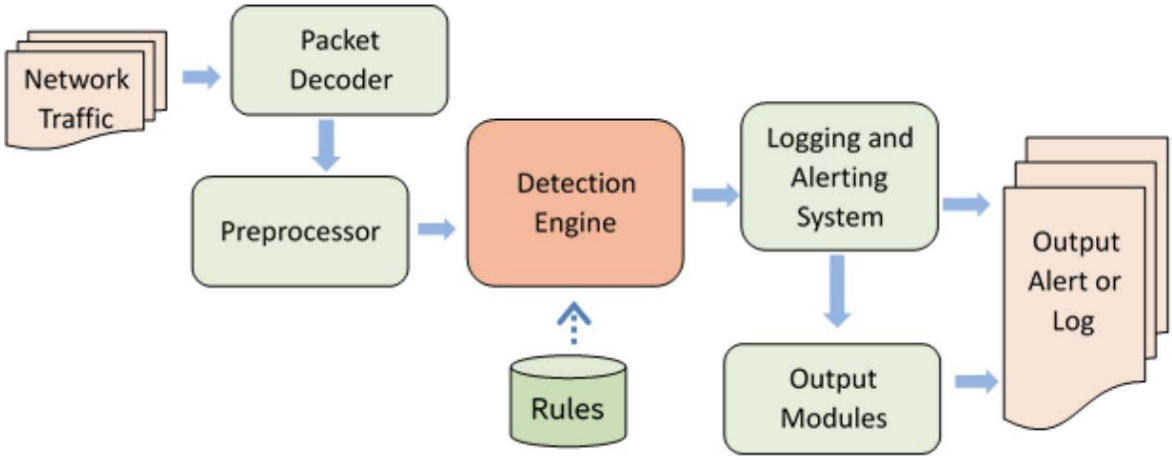

Рисунок 1.2 – Архітектура Snort

Програма використовує спеціальні «сигнатури» – це своєрідні шаблони, які допомагають розпізнати відомі загрози. Крім цього, Snort здатна помічати аномалії, тобто незвичну активність у мережі, яка може бути небезпечною.

Snort відома завдяки [11]:

– відкрите джерело. Програму можна завантажити безкоштовно, і її код доступний для змін, що дуже зручно;

– велика спільнота. Багато людей використовують Snort, тому постійно оновлюються її функції та сигнатури загроз;

– гнучкість. Її можна налаштувати так, щоб вона працювала саме під потреби вашої мережі.

Snort використовують для:

– слідкувати за тим, що відбувається в мережі, у реальному часі;

– виявляти атаки і попереджати про загрози;

– захищати від небажаних дій, наприклад, зупиняти шкідливий трафік.

Завдяки своїй популярності й можливості працювати разом з іншими системами, такими як Security Onion, Snort залишається одним із найкращих рішень для захисту мереж.

2. Suricata. Suricata – це ще одна програма з відкритим кодом, яка допомагає захищати мережі від атак (рисунок 1.3).

Рисунок 1.3 – IDS Suricata

Вона, як і Snort, використовує сигнатури та аналіз аномалій для виявлення загроз у мережевому трафіку.

Однак головна особливість Suricata – це її здатність працювати з великими обсягами даних, тому вона добре підходить для великих компаній або провайдерів інтернету.

Suricata особлива тим, що [12, 13]:

− висока швидкість. Suricata може обробляти великий трафік завдяки підтримці багатоядерних процесорів. Це означає, що вона працює швидко навіть у великих мережах;

− гнучкість. Програма легко налаштовується під потреби користувача.

− аналіз трафіку. Suricata може аналізувати не тільки сигнатури загроз, а й виявляти дивну активність у мережі, що допомагає знайти нові види атак.

Suricata популярна завдяки:

− можливість обробки великих обсягів даних. Це важливо для великих мереж із високим навантаженням;

− сучасний дизайн. Suricata працює швидко завдяки тому, що вона розроблена з використанням новітніх технологій;

− підтримку. Як і у Snort, у Suricata велика спільнота, яка допомагає вирішувати проблеми та оновлювати програму.

Suricata використовується для [12]:

− моніторингу великих корпоративних мереж;

− аналізу мережевого трафіку для пошуку загроз;

− інтеграції з іншими системами кібербезпеки, наприклад, Security Onion.

Suricata – це потужний інструмент, який не тільки забезпечує високий рівень безпеки, а й дозволяє ефективно працювати навіть у великих мережах. ЇЇ високопродуктивний механізм, побудований на основі сучасної багатопоточної архітектури, може обробляти багатогігабітний трафік, пропонуючи підтримку апаратного прискорення для підвищення ефективності. Це гарний вибір для тих, хто шукає сучасне та швидке рішення для захисту [24].

3. Zeek (раніше відома як Bro). Zeek – це ще одна потужна система для аналізу мережевого трафіку з відкритим кодом. Вона не тільки виявляє загрози та аномалії, але й дозволяє детально досліджувати, що відбувається в

мережі. Завдяки своїм можливостям, Zeek часто використовують для більш глибокого аналізу мережевих процесів і розуміння взаємодій між різними пристроями.

Його можна розглядати як такий, що містить три окремі частини (рисунок 1.4). Перша частина передбачає завантаження розвідувальних даних. По-друге, це механізм для вказівки системі розвідки, що частина даних, яку потрібно перевірити, була переглянута. Третій обробляє, коли виявлено позитивний збіг [24].

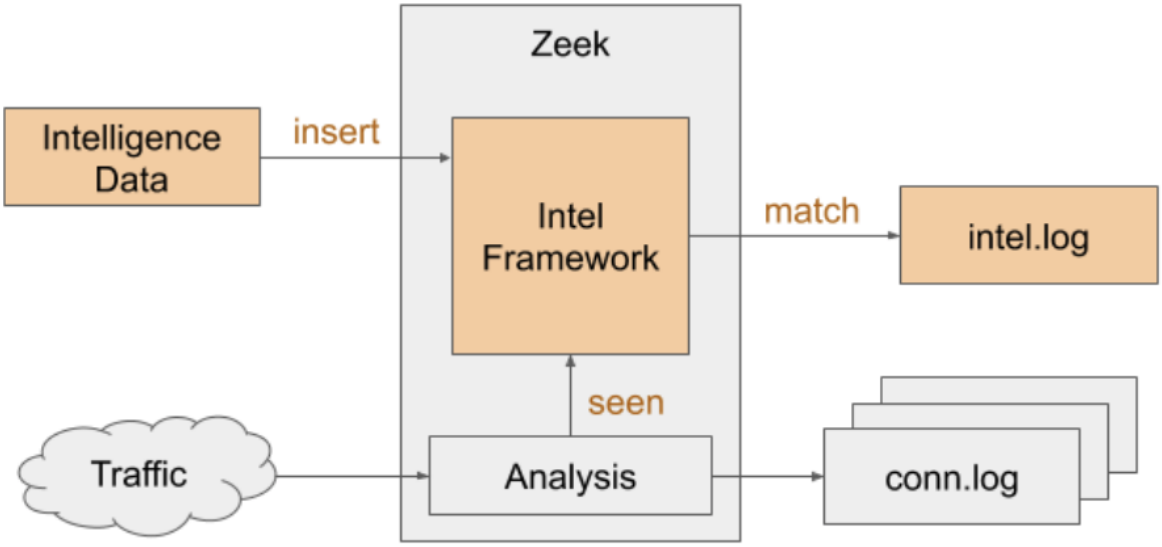

Рисунок 1.4 – IDS Zeek

Zeek унікальний тим, що має [15,16]:

– глибокий аналіз. Zeek збирає багато деталей про кожну сесію в мережі, наприклад, хто з ким спілкується, який обсяг даних передається і що саме передається. Це дозволяє отримати повну картину того, що відбувається у мережі.

– розширені можливості. Zeek надає більше інформації, ніж інші інструменти, що допомагає краще розуміти мережеві процеси та потенційні загрози;

– гнучкість і налаштування. Zeek можна налаштовувати під конкретні потреби, створюючи спеціальні скрипти для збору і аналізу даних.

До переваги необхідно віднести:

− детальний аналіз. Можливість отримати вичерпну інформацію про мережеві взаємодії;

− глибока інтеграція. Підходить для створення складних систем аналізу кіберзагроз.

Серед недоліки треба відмітити:

– складність налаштування. Zeek потребує більше часу та зусиль для налаштування, особливо якщо ви новачок;

– вимоги до ресурсів. Для стабільної роботи система потребує більше обчислювальних ресурсів, ніж інші інструменти.

Zeek використовують для:

− часто застосовують у великих компаніях і організаціях, де важливо мати повну картину мережевого трафіку. Це може бути корисним для:

− виявлення складних атак і аномалій;

− детального аналізу мережевих сесій і взаємодій;

− інтеграції з іншими системами безпеки, як-от Security Onion, для комплексного захисту.

Завдяки своїм можливостям Zeek стає чудовим доповненням до інших інструментів кібербезпеки, дозволяючи глибше занурюватися в аналіз і виявлення загроз [24].

1.3 Аналіз системи Security Onion

Security Onion – платформа для виявлення інцидентів кібербезпеки (рисунок 1.5), яка об’єднує кілька відкритих інструментів, щоб забезпечити комплексний підхід до моніторингу, аналізу та візуалізації мережевого

трафіку. Її розробили для того, щоб спростити процес захисту інформаційних систем у різних мережевих середовищах. Security Onion має кілька основних компонентів і можливостей, які допомагають у цьому [17, 18]:

1) Suricata. Suricata – це система, що займається моніторингом і аналізом трафіку, використовуючи як сигнатурний аналіз (знаходження відомих загроз за шаблонами), так і аналіз аномалій (виявлення підозрілої поведінки в мережі). Вона може працювати в режимі реального часу, що дозволяє обробляти великі обсяги даних і виявляти атаки швидко та ефективно.

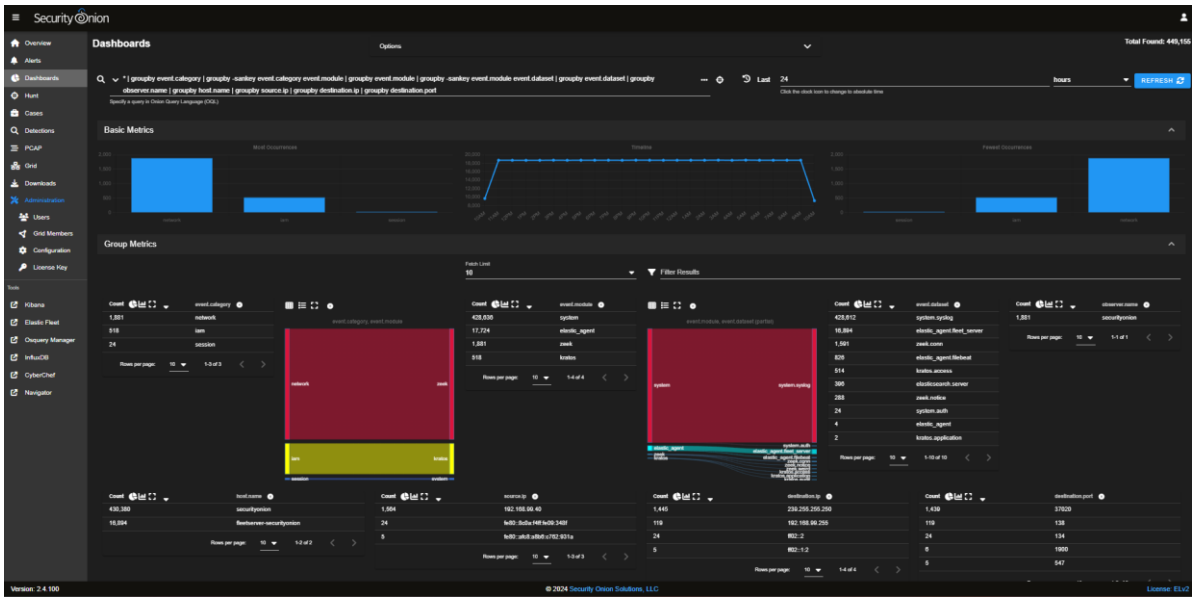

Рисунок 1.5 – Інтерфейс Security Onion.

2) Zeek (раніше відома як Bro). Zeek є інструментом для глибшого аналізу мережевого трафіку. Вона допомагає зрозуміти складні взаємодії між пристроями в мережі та надає можливість використовувати кастомні скрипти для розширення функцій, що робить її дуже гнучкою. Це дозволяє проводити детальний моніторинг і виявляти аномалії на більш високому рівні.

3) ELK Stack (ElasticSearch, Logstash, Kibana)

– ELK Stack – це набір інструментів, який відповідає за зберігання, обробку та візуалізацію даних;

− ElasticSearch забезпечує швидкий пошук і доступ до великих обсягів інформації;

− Logstash відповідає за збирання даних, їх обробку та форматування;

− Kibana використовується для створення графіків і дашбордів, які дають зрозумілу візуалізацію результатів моніторингу.

4) Wazuh. Wazuh – це інструмент для збору даних із різних пристроїв (хостів) у мережі. Він допомагає виявляти загрози та управляти політиками безпеки, забезпечуючи повний контроль над захистом хостів [19, 20].

Завдяки цим компонентам Security Onion є універсальною платформою для моніторингу кіберзагроз і виявлення інцидентів, що дозволяє швидко реагувати на загрози та глибоко аналізувати мережеву активність.

Security Onion підтримує як пасивний, так і активний моніторинг трафіку, що дозволяє використовувати її для різних завдань у різних мережевих середовищах. Пасивний моніторинг означає, що система просто спостерігає за трафіком, не втручаючись у його потік, а активний моніторинг дозволяє системі реагувати на загрози в реальному часі, наприклад, блокувати підозрілу активність.

Однією з важливих особливостей Security Onion є її здатність інтегруватися з іншими системами безпеки. Це робить її універсальним рішенням для виявлення та аналізу загроз, оскільки ви можете додавати інші інструменти або рішення, щоб ще більше покращити захист мережі.

Основні переваги Security Onion:

− Інтеграція з іншими інструментами безпеки. Це дозволяє легко поєднувати її з існуючими рішеннями, що використовуються в організації.

− Масштабованість. Система може бути адаптована під різні об’єми мережевого трафіку — від невеликих мереж до великих корпоративних середовищ.

− Відкритий вихідний код. Це дає можливість налаштувати Security Onion відповідно до конкретних потреб вашої організації, що особливо корисно для тих, хто має унікальні вимоги до безпеки.

Ці особливості роблять Security Onion гнучким і потужним інструментом для захисту інформаційних систем.

5) Шифрування. Шифрування в Security Onion забезпечує безпечну передачу та зберігання даних у системі виявлення кіберзагроз. Простими словами, це механізм, який робить інформацію недоступною для сторонніх осіб, якщо вони не мають спеціального «ключа» для розшифрування.

Захист переданої інформації: Коли дані передаються між компонентами Security Onion (наприклад, від сенсора до сервера), вони шифруються. Це запобігає їх перехопленню або зміні під час передачі.

Захист логів і даних: Журнали подій, трафік і збережені файли також можуть бути зашифровані, щоб захистити інформацію навіть у разі фізичного доступу до серверів.

Сертифікати та ключі: Для шифрування використовується SSL/TLS, який базується на сертифікатах. Вони перевіряють, чи з’єднання є справжнім, чи не підмінене.

Це потрібно щоб злочинці не могли викрасти дані про мережевий трафік, які Security Onion аналізує. Щоб інформація, яка зберігається, залишалась конфіденційною навіть у разі компрометації системи.

У загальному, шифрування в Security Onion працює «за лаштунками» і потребує мінімальної взаємодії користувача, якщо все налаштовано правильно. Для недосвідченого користувача це просто ще один рівень захисту даних у системі.

Переваги Security Onion.

1. Інтеграція багатьох інструментів. Платформа об’єднує кілька рішень для збору, зберігання та аналізу даних в одній системі.

2. Відкритий код**:** Security Onion є безплатний і дозволяє налаштовувати систему під специфічні потреби.

3. Потужний аналіз мережевого трафіку. Включає можливості IDS/IPS (Suricata), розширений аналіз протоколів (Zeek) та управління журналами (Kibana).

4. Широка спільнота**:** Велика кількість документації та підтримка від спільноти користувачів.

Недоліки Security Onion:

1) складність налаштування. Для роботи потрібні базові знання мережевої безпеки та вміння працювати з Linux;

2) високі вимоги до ресурсів. Для ефективного моніторингу великої мережі потрібне потужне апаратне забезпечення;

3) не завжди зручний інтерфейс. Аналіз великих обсягів даних може бути складним для недосвідчених користувачів.

Альтернативні засоби моніторингу трафіку.

1. SolarWinds Network Performance Monitor (NPM) (рисунок 1.6) [39]

Рисунок 1.6 – Інтерфейс панель керування SolarWinds.

Переваги:

- Інтуїтивний інтерфейс, зручний для новачків.
- Потужний інструмент для моніторингу мережевої продуктивності в реальному часі.
- Підтримка багатьох типів пристроїв та протоколів.

Недоліки. Висока вартість ліцензії.

PRTG Network Monitor (рисунок 1.7) [40]

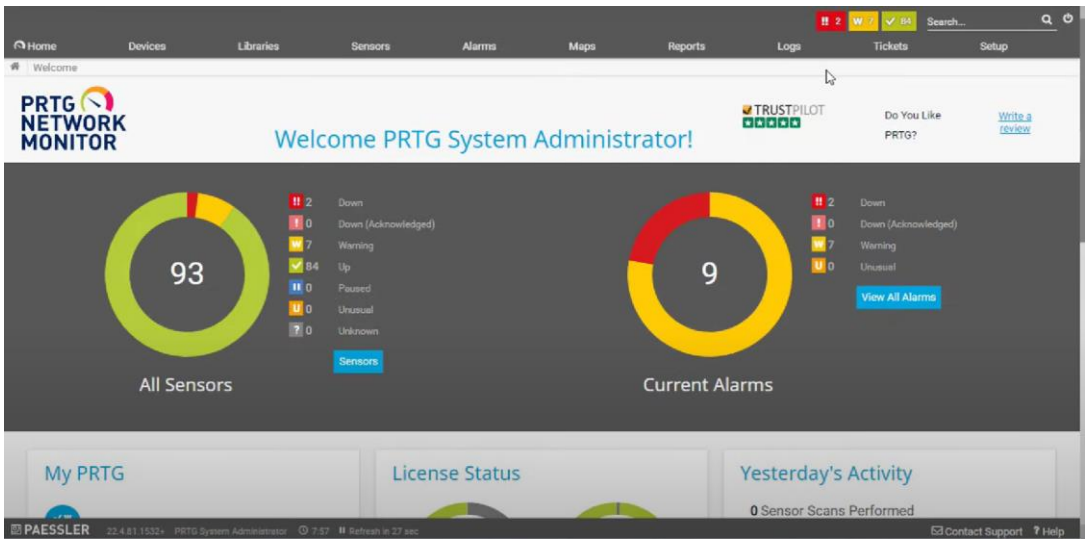

Рисунок 1.7 – Інтерфейс панель керування PRTG Network Monitor.

Переваги:

– простий у налаштуванні;

– все в одному рішення для моніторингу трафіку, серверів, пристроїв IoT;

– безплатний версія для невеликих мереж.

Недоліки. Може бути перевантаженим функціями для невеликих проєктів.

1. Nagios (рисунок 1.8) [41].

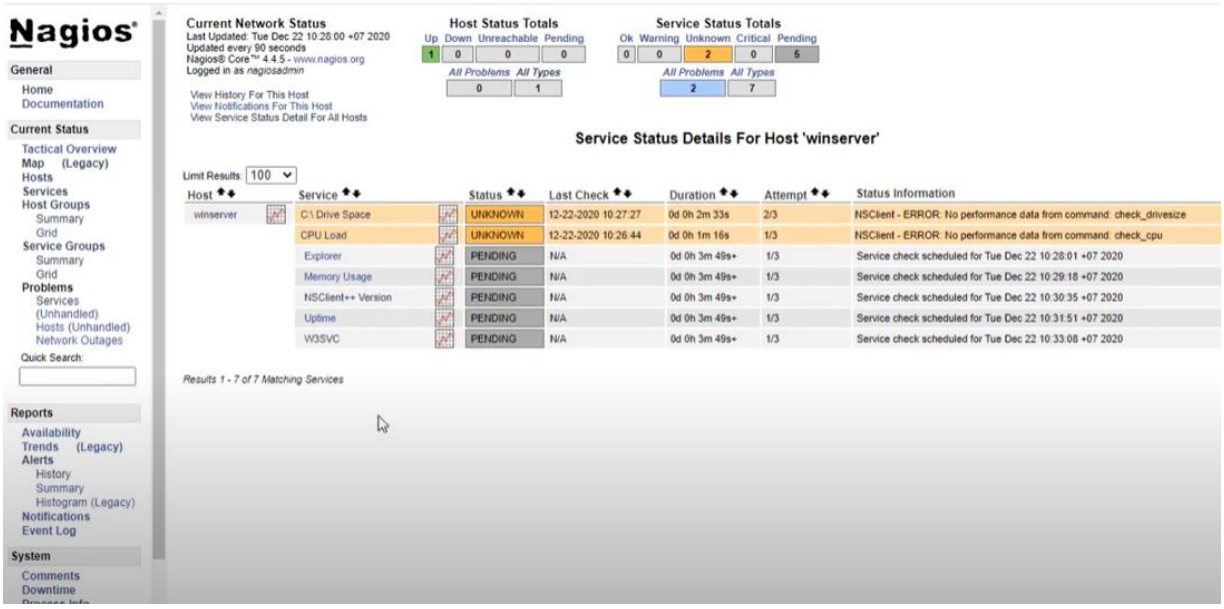

Рисунок 1.8 – Інтерфейс панель керування Nagios.

Переваги:

– гнучке налаштування та можливість розширення за допомогою плагінів;

– підходить як для моніторингу мережі, так і серверів;

– доступність відкритої версії (Nagios Core).

Недоліки: Складний у вивченні для початківців.

2. Wireshark (рисунок 1.9) [42]

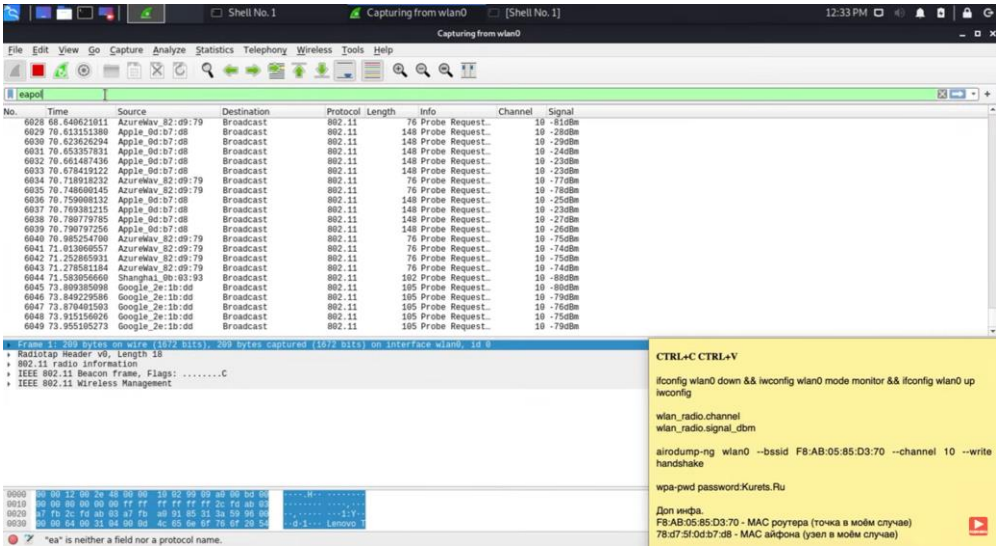

Рисунок 1.9 – Інтерфейс панель керування Wireshark.

Переваги:

- потужний аналізатор трафіку з детальною фільтрацією;
- підходить для діагностики проблем мережі та аналізу загроз;
- повністю безплатний.

Недоліки. Зосереджений на аналізі трафіку в реальному часі, а не на довготривалому моніторингу.

2 АРХІТЕКТУРА СИСТЕМ ВИЯВЛЕННЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ

2.1. Структура системи Security Onion і Proxmox

Security Onion – це потужна платформа для виявлення загроз і моніторингу безпеки, яка має відкритий вихідний код. Вона включає в себе безліч інструментів, що дозволяють збирати, аналізувати та візуалізувати дані про мережеву активність. Основні компоненти, які входять до складу Security Onion, включають такі інструменти, як Suricata, Zeek (раніше відомий як Bro), ElasticSearch, Kibana та інші. Це створює єдину платформу для управління інцидентами в сфері кібербезпеки.

Використання Security Onion допомагає організаціям виявляти і аналізувати загрози в реальному часі. Це спрощує процеси виявлення атак, фішингових спроб, зловмисних програм та інших кіберзагроз. Платформа надає можливість візуалізувати дані, що сприяє швидкому реагуванню на інциденти і забезпечує зручний доступ до важливої інформації для фахівців з безпеки.

Proxmox VE – це платформа для віртуалізації (рисунок 2.1), яка дозволяє запускати кілька віртуальних машин і контейнерів на одному фізичному сервері. Proxmox підтримує різні типи віртуалізації, включаючи KVM (для віртуальних машин) і LXC (для контейнерів). Це відкритий і багатофункціональний інструмент, що дозволяє ефективно управляти віртуалізацією на високому рівні.

Proxmox є ідеальним рішенням для розгортання інфраструктури, необхідної для тестування і моніторингу безпеки. Завдяки своїй гнучкості, Proxmox дозволяє швидко створювати нові середовища, що дуже корисно для фахівців з кібербезпеки, які прагнуть впроваджувати нові рішення або перевіряти їхню ефективність у реальних умовах.

Ця комбінація Security Onion і Proxmox VE може стати основою для потужної інфраструктури кібербезпеки, яка дозволяє ефективно виявляти загрози та забезпечувати безпеку інформації в організації (рис.2.1).

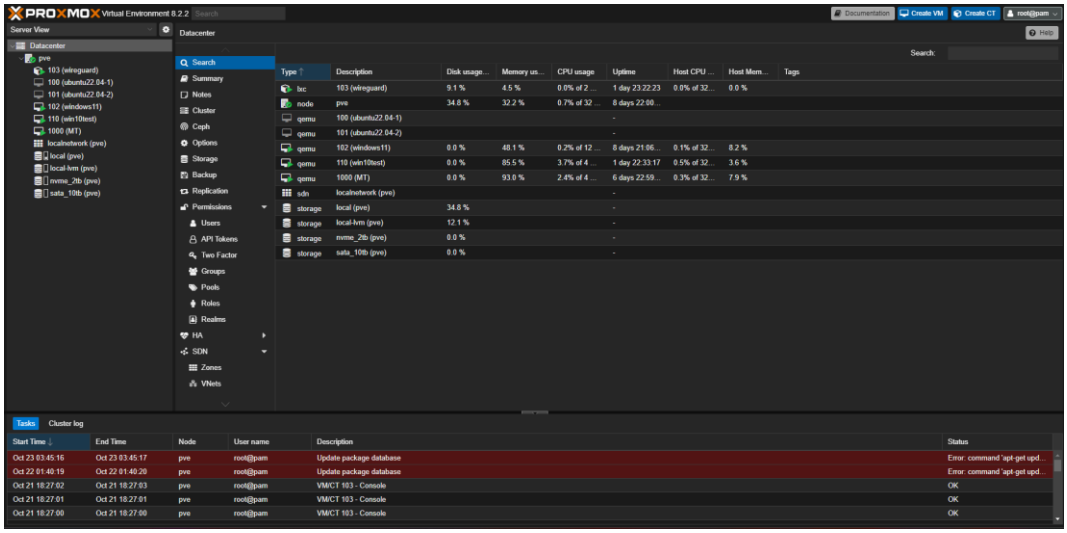

Рисунок 2.1 – Інтерфейс Proxmox.

У комбінації Security Onion і Proxmox VE ці дві платформи надають гнучке та масштабоване рішення для виявлення інцидентів кібербезпеки. Використовуючи Proxmox, можна легко налаштувати віртуалізовану інфраструктуру для розгортання Security Onion. Це дозволяє створювати ізольовані середовища, в яких можна проводити моніторинг мережевого трафіку в реальному часі.

Наприклад, за допомогою Proxmox можна створити кілька віртуальних машин або контейнерів, кожен з яких може бути призначений для певних задач, таких як аналіз трафіку, управління журналами або виявлення загроз. Це дозволяє не лише тестувати різні конфігурації безпеки, а й проводити експерименти з новими інструментами або методами моніторингу, не порушуючи основну інфраструктуру.

Також важливо відзначити, що ця архітектура дозволяє масштабувати ресурси в залежності від потреб організації. Коли навантаження зростає, можна додавати нові віртуальні машини або контейнери для розподілу навантаження, що забезпечує безперервність роботи системи. Таким чином,

спільне використання Security Onion і Proxmox VE є потужним рішенням для забезпечення кібербезпеки, яке дозволяє ефективно реагувати на загрози і адаптуватися до змін у середовищі.

2.2. Архітектура та компоненти Security Onion

Архітектура Security Onion складається з кількох основних компонентів, які працюють у тандемі для забезпечення глибокого моніторингу та аналізу мережевого трафіку. Приведемо короткий опис основних компонентів.

1. Suricata – це основний інструмент для виявлення вторгнень (IDS/IPS). Він аналізує мережевий трафік, шукаючи відомі сигнатури атак і виявляючи аномалії. Suricata забезпечує захист у режимі реального часу і може блокувати атаки, якщо система налаштована як IPS.

2. Zeek (Bro) – ще один важливий компонент для глибокого аналізу мережевого трафіку. Zeek спеціалізується на зборі та обробці інформації про мережеві взаємодії, які можуть вказувати на потенційні загрози. Цей інструмент забезпечує детальний аналіз трафіку та збирає лог-файли для подальшого аналізу.

3. ElasticSearch, Logstash, Kibana (ELK Stack) – це три ключові компоненти, які відповідають за обробку та візуалізацію даних:

− ElasticSearch – індексує та зберігає великі обсяги даних, що забезпечує швидкий пошук і доступ до інформації.

− Logstash – відповідає за обробку даних, їх перетворення та підготовку до зберігання та аналізу.

− Kibana – дозволяє створювати дашборди та візуалізувати результати аналізу даних у вигляді графіків, таблиць і діаграм.

4. Wazuh – компонент для моніторингу та управління хостами. Він допомагає виявляти загрози та реагувати на них, забезпечуючи

централізоване управління журналами подій і підключення хостів до загальної системи виявлення.

5. TheHive – система для управління інцидентами кібербезпеки. Вона дозволяє команді реагувати на загрози, вести облік інцидентів, призначати завдання та координувати дії для оперативного реагування.

Всі ці компоненти (працюють разом, створюючи потужну платформу для забезпечення високого рівня безпеки та моніторингу в реальному часі рисунок 2.2). Це дозволяє організаціям швидко та ефективно реагувати на загрози, зменшуючи ризики та потенційні втрати.

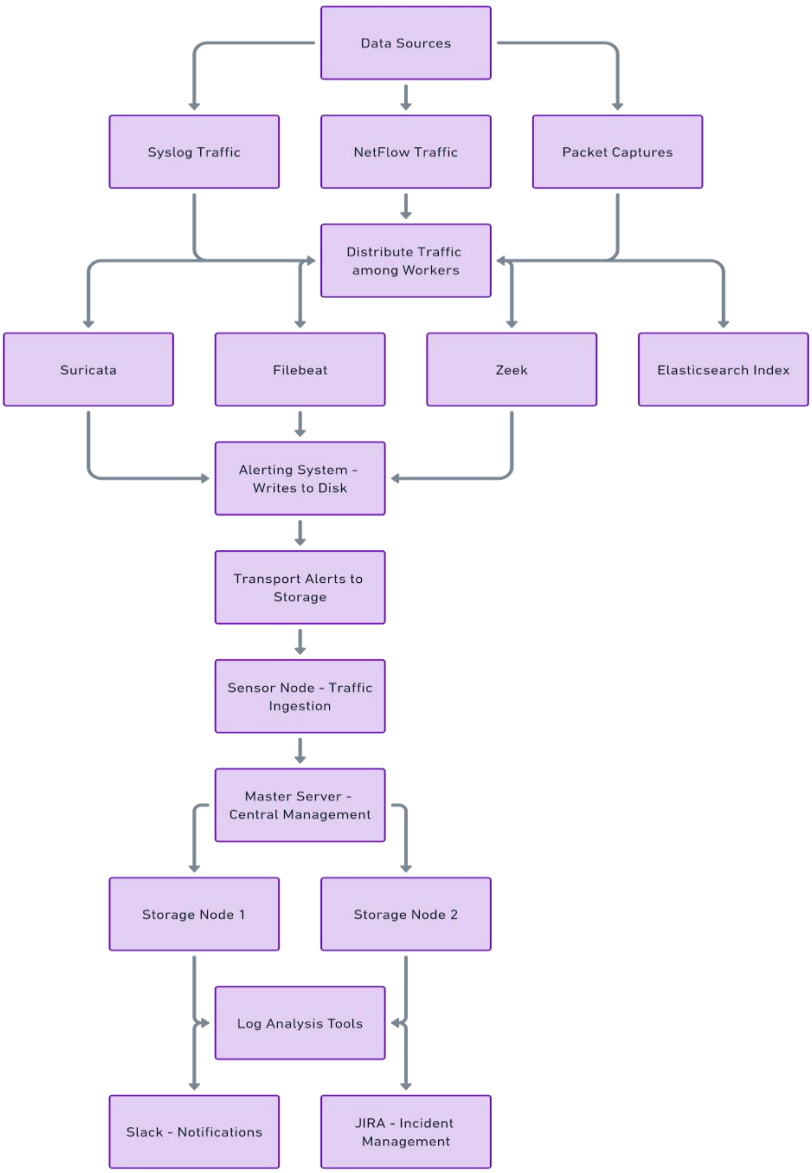

Рисунок 2.2 – Архітектура компонента в SecurityOnion.

Інтеграція системи виявлення інцидентів, такої як Security Onion, у корпоративну інфраструктуру — це складний процес, який потребує врахування як технічних, так і організаційних аспектів. Першим кроком є проведення ретельного аудиту існуючої мережі для виявлення критичних точок моніторингу. Це можуть бути ключові маршрутизатори, шлюзи або сервери, через які проходить великий обсяг чутливих даних. Саме на цих вузлах доцільно розгорнути Security Onion для отримання максимальної ефективності.

Другий етап – це налаштування збору та кореляції даних. Security Onion дозволяє збирати логи з різних джерел: мережевих пристроїв, серверів і кінцевих точок. Завдяки цьому забезпечується глибоке бачення мережевої активності, а також можливість виявлення складних загроз шляхом порівняння подій із різних джерел.

Важливим аспектом є інтеграція Security Onion з іншими засобами кібербезпеки, наприклад, фаєрволами, антивірусними системами або SIEM-системами. Це дозволяє автоматизувати реагування на виявлені загрози, що зменшує час між виявленням атаки і вжиттям заходів. Наприклад, Security Onion може передавати зібрані дані до SIEM-системи, де вони будуть проаналізовані, а результати надіслані у вигляді звіту.

Навчання персоналу також є ключовим фактором успішної інтеграції. Співробітники повинні бути добре ознайомлені з роботою Security Onion, як з технічної сторони, так і в контексті реагування на інциденти. Регулярні тренінги допоможуть команді безпеки ефективніше використовувати можливості системи та залишатися в курсі нових функцій і загроз.

Нарешті, постійна підтримка системи і її адаптація до нових викликів є необхідною умовою для забезпечення належного рівня захисту. З появою нових загроз і технологій важливо регулярно оновлювати сигнатури, змінювати правила виявлення, а також оптимізувати налаштування

мережевого трафіку, щоб Security Onion завжди була надійною та актуальною.

Системи виявлення інцидентів (IDS) дійсно відіграють ключову роль у забезпеченні кібербезпеки, але, як і будь-яка технологія, вони мають свої обмеження та виклики. Одним із основних викликів є точність виявлення загроз, оскільки помилкові позитиви та негативи можуть значно вплинути на ефективність системи.

Помилки позитивні та негативи. Помилки позитивні виникають, коли система помилково ідентифікує звичайний трафік як загрозу. Наприклад, коли система фіксує легітимні дії користувачів чи сервісів як підозрілі. Це призводить до того, що команди безпеки отримують зайві тривоги і витрачають час на їх аналіз. Постійні помилкові спрацювання можуть знизити увагу до дійсно небезпечних ситуацій.

Помилки негативні є ще серйознішою проблемою, адже це випадки, коли справжня загроза не розпізнається системою. Наприклад, якщо нова форма атаки не описана в підписах IDS, то вона може залишитися непоміченою, і атакуючі зможуть безперешкодно діяти. Це може статися через те, що сигнатури не були вчасно оновлені або система не налаштована для виявлення нових видів атак.

Наслідки для організацій. Такі неточності можуть мати суттєвий вплив на ефективність роботи фахівців з кібербезпеки. Постійні помилкові позитиви відволікають увагу команди від серйозних загроз, створюючи додаткове навантаження та знижуючи продуктивність. З іншого боку, помилкові негативи можуть призвести до того, що справжні атаки залишаться непоміченими, що, в свою чергу, загрожує серйозними втратами для компанії.

Щоб зменшити ризики, необхідно постійно оновлювати сигнатури системи, а також використовувати комбіновані підходи до виявлення загроз, такі як сигнатурний і аномалійний аналіз, що дозволяє збільшити ефективність виявлення загроз.

Складність налаштування та підтримки. Системи виявлення інцидентів часто потребують індивідуального налаштування для кожної мережі, щоб врахувати її особливості та правильно виявляти загрози. Це вимагає:

− аналізу трафіку. Потрібно розуміти характер мережевого трафіку, щоб коректно налаштувати правила виявлення. Недостатня увага до цього етапу може призвести до виникнення помилкових спрацьовувань;

− налаштування правил і політик. Кожна мережа має свої унікальні особливості, тому потрібно вручну налаштовувати правила виявлення загроз, що займає багато часу та потребує спеціалізованих знань;

− інтеграція з іншими компонентами. IDS повинна бути сумісною з іншими системами безпеки, такими як фаєрволи або SIEM-системи, для забезпечення максимальної ефективності. Помилки в інтеграції можуть призвести до вразливостей в системі безпеки.

Підтримка таких систем також вимагає регулярних оновлень правил і сигнатур, що потребує постійної уваги з боку команди безпеки. Це може створювати додаткове навантаження на персонал, особливо у великих організаціях, де обсяг роботи значно збільшується.

Масштабованість. Масштабованість є ще одним викликом для систем IDS, особливо в контексті зростання організацій:

– збільшення обсягу трафіку. Більші організації зазвичай мають більші обсяги мережевого трафіку. Традиційні IDS можуть не справлятися з обробкою великого трафіку або затримками у виявленні загроз. Це може призвести до недостатньо швидкого реагування на інциденти;

– складність централізації моніторингу: У великих організаціях часто існують кілька підрозділів і відокремлених мереж. Централізований моніторинг безпеки в таких умовах може бути ускладнений, а деякі ділянки мережі можуть залишитися без належного контролю, що створює «сліпі зони» для атак;

– оптимізація систем. Масштабування системи потребує регулярного огляду та оптимізації правил виявлення, щоб уникати перевантаження та забезпечити високий рівень ефективності.

Потреба в кваліфікованих фахівцях. Ефективна робота систем виявлення інцидентів залежить від рівня кваліфікації персоналу:

− нестача кваліфікованих кадрів: Сучасні IDS-системи вимагають від фахівців глибоких знань у галузі кібербезпеки, а також здатності розуміти та налаштовувати специфічні правила. Однак багато організацій стикаються з дефіцитом кваліфікованих кадрів;

− труднощі з навчанням. Навіть якщо організація наймає нових співробітників, їх підготовка може зайняти тривалий час, під час якого система може залишатися вразливою до нових загроз;

− висока вартість утримання персоналу. Фахівці з кібербезпеки часто коштують дорого, і організаціям складно утримувати таких співробітників на постійній основі, особливо якщо бюджет на кібербезпеку обмежений.

Ці виклики підкреслюють необхідність ретельного планування, підтримки та постійного навчання персоналу для забезпечення високого рівня захисту інформаційних систем.

Системи виявлення інцидентів (IDS) постійно вдосконалюються, і їх розвиток визначають кілька сучасних тенденцій. У цьому розділі розглянемо кілька ключових напрямків, які впливають на те, як системи IDS функціонуватимуть у майбутньому.

Штучний інтелект і машинне навчання. Сучасні IDS все частіше використовують штучний інтелект (ШІ) та машинне навчання (МН) для аналізу великих обсягів даних. Це дозволяє системам краще розуміти, що відбувається в мережі, та виявляти загрози раніше невідомими методами.

Наприклад, ШІ може вивчати звичайну поведінку користувачів і системи, а потім виявляти аномалії, які можуть бути ознакою кіберзагрози. Машинне навчання допомагає прогнозувати можливі атаки, використовуючи історичні дані, що значно підвищує захист.

6. Інтеграція з DevSecOps. Це новий підхід, який об’єднує розробку програм, безпеку і операційну підтримку. Ідея полягає в тому, щоб безпека була врахована ще на етапі розробки програмного забезпечення. IDS інтегрується в цей процес, допомагаючи виявляти уразливості ще до запуску програми.

7. Автоматизація реагування на інциденти. Час реагування на інциденти відіграє ключову роль. Автоматизовані системи можуть самостійно виконувати певні дії у відповідь на загрози. Наприклад, блокувати шкідливі IP-адреси або обмежувати доступ до певних сегментів мережі, що допомагає зменшити час на вирішення проблеми.

8. Хмарні технології. З розвитком хмарних обчислень з’являються гібридні рішення, де частина ресурсів знаходиться в хмарі, а частина – на локальних серверах. Це робить системи IDS більш гнучкими та дозволяє швидко адаптуватися до змін у потребах компанії.

9. Приватність і відповідність законам. У сучасному світі захист особистих даних є важливим аспектом. IDS повинні не лише виявляти загрози, а й гарантувати, що приватні дані користувачів залишаються конфіденційними. Системи мають дотримуватися законодавства, такого як GDPR, і надавати чітке пояснення своїх дій.

Вибір системи виявлення інцидентів (IDS) – це важливий етап у забезпеченні кібербезпеки для будь-якої організації. Правильна система може суттєво підвищити захист, тоді як неправильний вибір може залишити організацію вразливою. Ось кілька ключових рекомендацій, які можуть допомогти у прийнятті обґрунтованого рішення.

1. Оцінка потреб організації. Перед тим як обрати систему виявлення інцидентів, важливо чітко зрозуміти, що саме потрібно вашій організації.

2. Аналіз загроз. Визначте, які саме загрози можуть загрожувати вашій інфраструктурі. Це можуть бути атаки ззовні, внутрішні загрози або проблеми з конкретними програмами чи серверами.

3. Масштаб і складність мережі. Розгляньте, наскільки велика ваша мережа. Вимоги до системи виявлення інцидентів будуть різними для невеликої компанії та великої організації з багатьма підрозділами.

4. Проведення тестування рішень. Тестування кількох систем дозволить оцінити їхню ефективність.

– Демонстраційні версії. Багато постачальників пропонують безкоштовні демо-версії або пробні періоди. Використовуйте ці можливості, щоб оцінити функції системи в реальних умовах.

– Порівняння функціональності. Оцініть різні можливості, такі як виявлення загроз, налаштування правил, інтеграція з іншими системами безпеки та швидкість реагування на інциденти.

Залучення команди безпеки до процесу вибору. Важливо включити фахівців з безпеки у вибір системи.

– Фахівці з кібербезпеки. Ваша команда знає специфіку загроз, з якими стикається організація, і може допомогти знайти систему, яка найкраще відповідатиме цим потребам.

– Взаємодія з іншими відділами. Обговоріть вимоги до системи з іншими відділами, такими як IT, управління ризиками чи юридичний. Це може допомогти уникнути потенційних конфліктів.

Урахування можливості масштабування. Обираючи IDS, врахуйте, як система може адаптуватися до змін у вашій організації.

– Зростання організації. Коли ваша компанія розвивається, система повинна легко впоратися з новими підключеннями та підвищити обсяг моніторингу без зниження продуктивності.

– Гнучкість у налаштуваннях. Переконайтеся, що система дозволяє легко додавати нові правила та модулі.

Оцінка вартості. Ціна системи – важливий фактор, який потрібно враховувати.

– Загальні витрати на володіння. Витрати на налаштування, навчання персоналу та технічну підтримку, окрім початкової ціни.

– Порівняння з іншими рішеннями. Зробіть аналіз витрат на різні системи та визначте, які з них пропонують найкраще співвідношення ціни та якості.

7. Підтримка та обслуговування. Не менш важливим є рівень підтримки, який пропонує постачальник системи.

– Технічна підтримка. Чи надає постачальник цілодобову підтримку? Які канали зв'язку доступні (телефон, електронна пошта, чат)?

– Оновлення системи. Як часто постачальник оновлює систему? Чи забезпечує він своєчасні оновлення та вдосконалення?

Security Onion – це популярне рішення для моніторингу трафіку, аналізу загроз та виявлення кіберінцидентів. Воно поєднує кілька потужних інструментів, таких як Suricata, Zeek, Kibana, Wazuh тощо, для глибокого аналізу мережевої активності.

2.3. Платформа Proxmox для віртуалізації

Proxmox VE – це сучасна платформа для віртуалізації, яка підтримує як повну віртуалізацію (KVM), так і контейнерну віртуалізацію (LXC). Це означає, що ви можете запускати кілька віртуальних машин (ВМ) і контейнерів на одному фізичному сервері. Це робить Proxmox ідеальним інструментом для створення гнучких і масштабованих середовищ, особливо коли мова йде про системи для виявлення загроз.

Основні характеристики Proxmox VE:

− управління кількома віртуальними машинами. Ви можете створювати та керувати кількома ВМ одночасно, що дозволяє максимально ефективно використовувати ресурси вашого сервера;

− підтримка контейнерів LXC. Для менш ресурсоємних завдань ви можете використовувати контейнерну віртуалізацію, що може бути корисно в багатьох випадках;

– підтримка зберігання даних. Proxmox надає доступ до різних типів зберігання, таких як локальні диски, мережеві сховища (NAS, SAN) та навіть розподілені файлові системи (Ceph);

– масштабованість і управління кластерами. Ви можете створювати кластери з кількох серверів, що забезпечує високу доступність та баланс навантаження.

Завдяки цим можливостям Proxmox є чудовою платформою для розгортання Security Onion. Вона забезпечує зручне управління віртуальними середовищами, що є важливим для тестування і моніторингу загроз.

Альтернативні програмне забезпечення для віртуалізації з їх перевагами та недоліками порівняно з Proxmox:

2. Vmware vSphere (рисунок 2.3) [37].

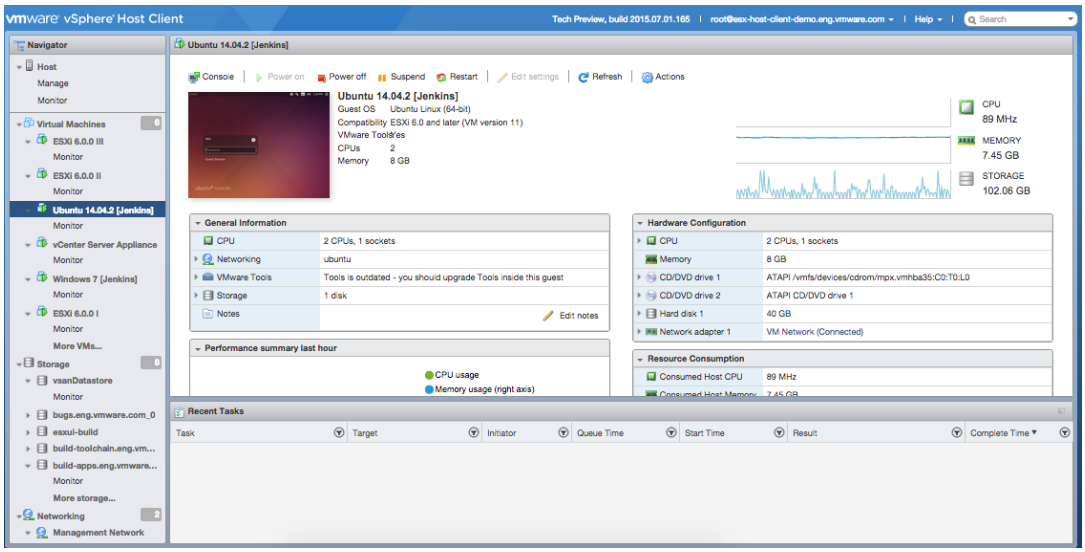

Рисунок 2.3 – Інтерфейс панель керування Vmware vSphere.

Переваги:

– висока стабільність та надійність. Ідеально підходить для великих корпоративних середовищ;

– широкі можливості керування. Інтеграція з іншими продуктами Vmware та багатий функціонал для адміністрування;

– віртуалізація мереж та зберігання. Висококласна підтримка таких технологій, як vSAN та NSX;

– підтримка великих кластерів. Можливість роботи з тисячами віртуальних машин.

Недоліки:

– вартість. Дуже дороге програмне забезпечення, особливо для малого бізнесу чи ентузіастів;

– складність для новачків. Потрібен досвід роботи або навчання для повноцінного використання.

2) XenServer (рисунок 2.4) [38].

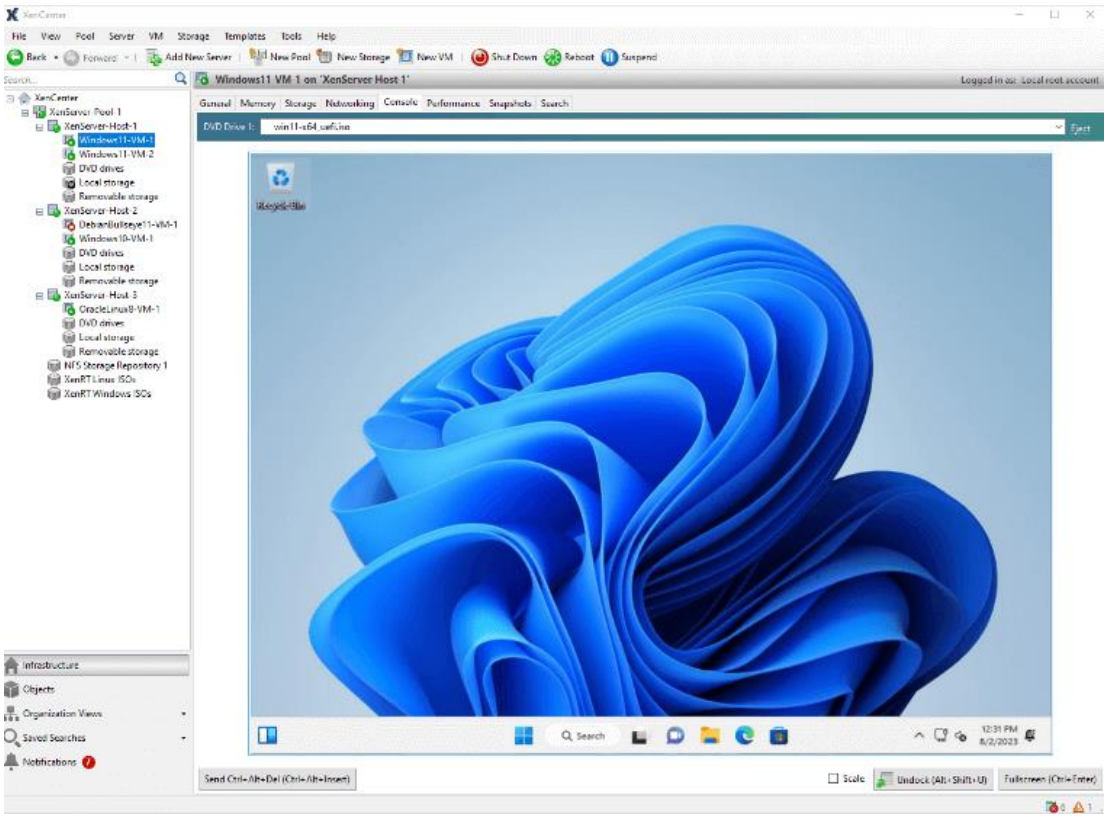

Рисунок 2.4 – Інтерфейс панель керування XenServer

Переваги:

– безкоштовна базова версія. Підходить для невеликих проєктів;

− підтримка віртуалізації графіки (vGPU). Корисно для графічно інтенсивних завдань;

− хороша продуктивність. Ефективне використання ресурсів.

Недоліки:

− менше спільноти. Порівняно з Proxmox чи Vmware, підтримка від користувачів обмежена;

− деякі функції лише у платній версії.

2.4. Розгортання Security Onion на Proxmox

Security Onion — забезпечцє моніторинг мережевої безпеки та виявлення інцидентів. Вона допомагає збирати, аналізувати та корелювати мережевий трафік. З іншого боку, Proxmox — це система віртуалізації, яка дозволяє створювати та управляти віртуальними машинами (ВМ) і контейнерами. Коли ці дві технології поєднуються, ми отримуємо чудовий інструмент для моніторингу та аналізу мережевих загроз.

Підготовка Proxmox.

1.1. Інсталяція Proxmox. Перш ніж почати, потрібно встановити Proxmox на сервер. Для цього спершу завантажте ISO-образ Proxmox з офіційного сайту. Потім запишіть його на USB-носій або DVD. Далі завантажте сервер з цього носія і слідуйте інструкціям інсталяції. Після успішного встановлення ви зможете отримати доступ до веб-інтерфейсу Proxmox через браузер.

1.2. Налаштування мережі. Після установки Proxmox важливо перевірити, чи сервер підключений до мережі і має статичну IP-адресу. Це забезпечить стабільну роботу системи віртуалізації та управління віртуальними машинами.

2. Створення віртуальної машини для Security Onion.

2.1. Створення нової віртуальної машини (VM). У веб-інтерфейсі Proxmox натисніть на опцію «Create VM» (Створити VM). Вам потрібно буде вказати назву для віртуальної машини (наприклад, «SecurityOnion») і вибрати ISO-образ Security Onion. Його можна завантажити з офіційного сайту Security Onion і додати до сховища Proxmox. Потім налаштуйте основні параметри ВМ, такі як кількість ядер CPU, обсяг оперативної пам’яті та місце на диску.

2.2. Налаштування ресурсів: Security Onion вимагає достатньо ресурсів для нормальної роботи, тому варто виділити їй адекватні параметри (рисунок 2.5):

- CPU. Мінімум 4 ядра.
- RAM. Не менше 16 ГБ оперативної пам’яті.
- Диск. Для початкової конфігурації достатньо 200 ГБ, але більше дискового простору дозволить зберігати більше даних мережевого трафіку.

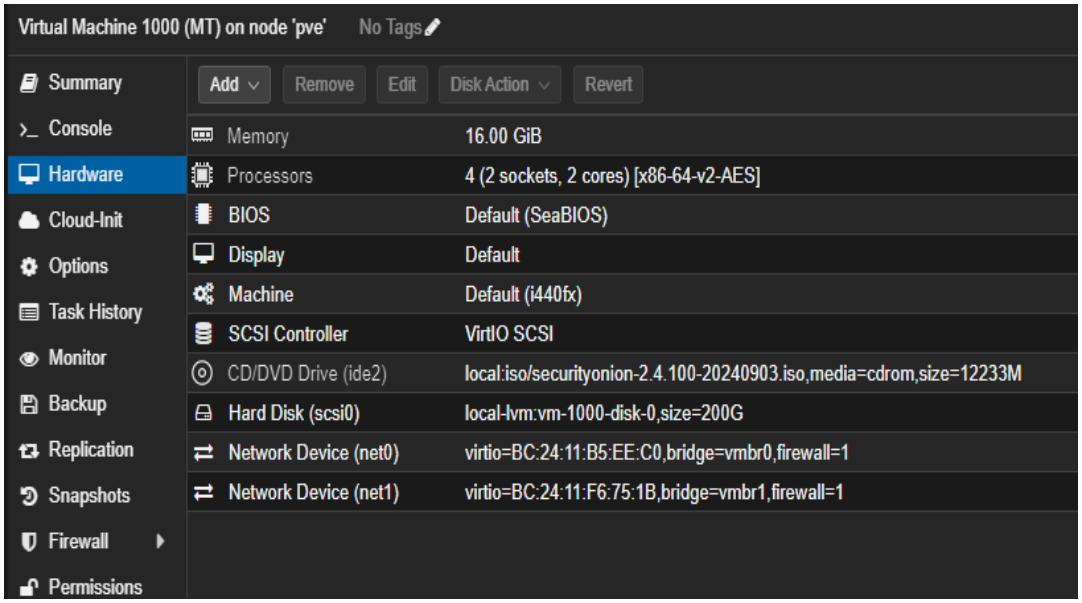

Рисунок 2.5 – Конфігурація ВМ для Security Onion в гіпервізорі Proxmox

Ці кроки допоможуть вам налаштувати Proxmox для роботи з Security Onion і забезпечити ефективний моніторинг мережевих загроз.

3. Встановлення Security Onion.

3.1. Завантаження віртуальної машини. Коли буде створена віртуальна машина, наступний крок – необхідно завантажити її з ISO-образа Security Onion, так само, як ви б це робили з звичайного диска для установки.

3.2. Процес інсталяції. Установка Security Onion не є складною. Після того, як система завантажиться, з’явиться майстер встановлення. Він проведе вас через всі етапи, крок за кроком. Вам потрібно буде обрати конфігурацію – наприклад, «Standalone», якщо плануєте використовувати все на одному сервері. Також вам буде потрібно налаштувати мережеві інтерфейси та встановити оновлення.

Налаштування мережі. Security Onion вимагає доступу до мережі, щоб ефективно моніторити трафік. Зазвичай використовують декілька мережевих інтерфейсів: один для управління, а інший для захоплення трафіку. Останній можна підключити до SPAN-порту [20] або TAP-пристрою на маршрутизаторі чи комутаторі.

4. Конфігурація та запуск Security Onion.

4.1. Первинне налаштування: Після установки вам буде потрібно ввести кілька базових налаштувань, таких як IP-адреса для доступу до веб-інтерфейсу, облікові дані адміністратора та інші важливі параметри.

4.2. Запуск інструментів моніторингу: Security Onion постачається з кількома корисними інструментами, такими як Zeek (раніше відомий як Bro), Suricata та Kibana, які допомагають аналізувати та візуалізувати дані. Після налаштування вони почнуть автоматично збирати та обробляти мережевий трафік.

5. Доступ до веб-інтерфейсу.

5.1. Вхід у веб-інтерфейс. Коли всі налаштування завершені, ви зможете зайти у веб-інтерфейс Security Onion. Для цього потрібно просто ввести IP-адресу вашої віртуальної машини в браузері. Через цей інтерфейс можна переглядати зібрані дані про мережевий трафік, створювати звіти та аналізувати потенційні загрози.

6. Налаштування мережевого моніторингу.

Підключення до мережі. Щоб Security Onion міг правильно аналізувати мережевий трафік, потрібно налаштувати SPAN-порт [20] або TAP-пристрій на вашому мережевому комутаторі. Це дозволить відправляти копії мережевого трафіку на один із інтерфейсів Security Onion.

6.2. Збір та аналіз трафіку: Після того як ви налаштуєте SPAN-порт [20], система почне збирати та аналізувати мережеві пакети. Ви зможете бачити деталі трафіку, виявляти підозрілу активність та переглядати загрози через веб-інтерфейс.

3 РОЗРОБКА ТА ДОСЛІДЖЕННЯ СИСТЕМИ ВИЯВЛЕННЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ

3.1. Налаштування контейнера Ubuntu та використання WireGuard для маршрутизації

Використання WireGuard [19] для маршрутизації трафіку через контейнер Ubuntu – це дійсно ефективний спосіб створення безпечної VPN-мережі, яка допоможе вам захистити свій трафік. Це особливо корисно для моніторингу даних або забезпечення віддаленого доступу до ресурсів через захищений тунель. Розглянемо покрокову інструкцію для налаштування такої системи.

Створення контейнера Ubuntu на Proxmox [23].

1.1 . Створення контейнера:

- увійдіть до веб-інтерфейсу Proxmox;
- створіть новий контейнер (LXC) з образом Ubuntu, наприклад, Ubuntu 22.04;
- виділіть достатньо ресурсів — мінімум 1 CPU та 1 ГБ RAM, залежно від ваших потреб;
- призначте контейнеру статичну IP-адресу у вашій локальній мережі для зручного доступу.

1.2. Налаштування мережі. Під час створення контейнера необхідно додати мережевий інтерфейс. Він дозволить контейнеру отримати доступ до локальної мережі та Інтернету.

2. Встановлення та налаштування WireGuard [19].

2.2. Встановлення WireGuard:

- після запуску контейнера підключіться до нього через SSH або за допомогою консолі Proxmox;
- оновіть пакети та встановіть WireGuard командою (рисунок 3.1).

```
curl -O https://raw.githubusercontent.com/angristan/wireguard-install/master/wireguard-install.sh
chmod +x wireguard-install.sh
./wireguard-install.sh
```

Рисунок 3.1 – Командна стрічка для встановлення wireguard.

Після встановлення та запуску ./wireguard, треба підтвердити конфігурацію мережи, після цього створюється клієнт (наприклад назвемо openwrt).

Налаштування NAT (маскараду). Використайте правила IPTables для реалізації NAT, щоб клієнти могли виходити в Інтернет через сервер (рисунок 3.2).

```
Last login: Mon Oct 21 07:53:43 UTC 2024 on tty1
root@wireguard:~# sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Рисунок 3.2 – Командна стрічка для реалізації NAT

Альтернативні програмне забезпечення в якості віртуального маршрутизатора з їх перевагами та недоліками порівняно з wireguard.

3. OpenVPN (рисунок 3.3).

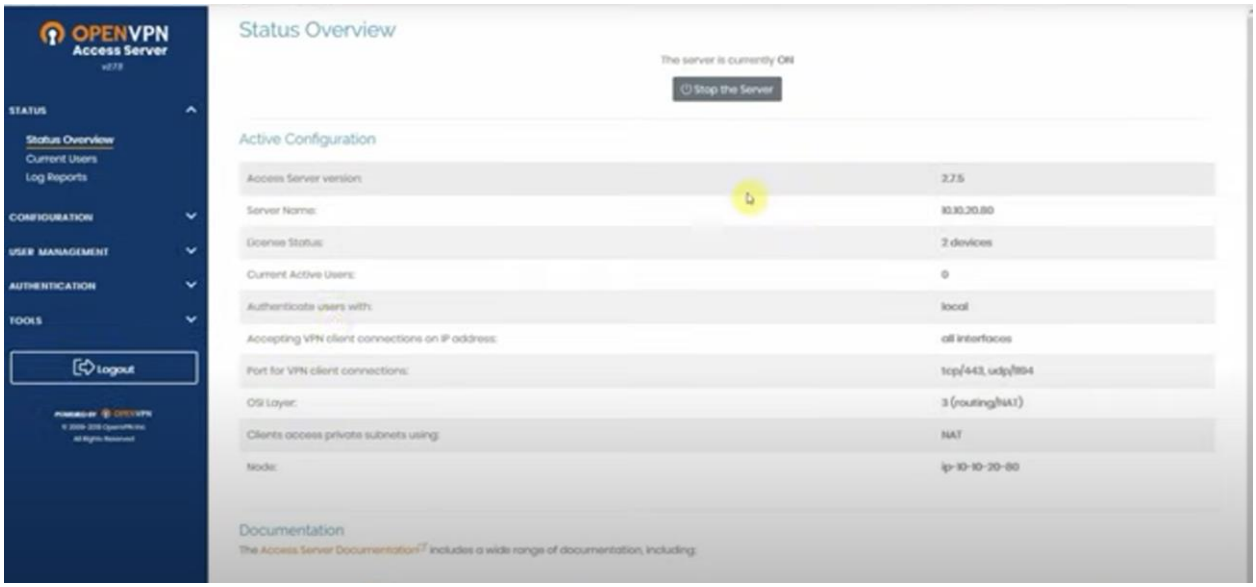

Рисунок 3.3 – Інтерфейс панель керування OpenVPN

Переваги:

− гнучкість налаштувань. OpenVPN підтримує широкий набір протоколів (TCP/UDP) та може працювати через проксі-сервери [32];

− широка підтримка платформ. Доступний на багатьох операційних системах і пристроях;

− масштабованість. Добре працює для великих мереж завдяки підтримці PKI (публічних ключів).

Недоліки:

− складніша конфігурація. Потребує більше часу для налаштування порівняно з WireGuard;

− продуктивність. Хоча OpenVPN залишається надійним, швидкість передачі даних нижча через складніший процес шифрування [32];

− вимоги до ресурсів. Споживає більше обчислювальної потужності.

Ipsec [34].

Переваги:

− високий рівень безпеки. Стандарт у багатьох корпоративних середовищах для VPN;

− сумісність із мережевими пристроями. Добре працює з маршрутизаторами та міжмережевими екранами;

− широке використання. Підтримується більшістю платформ і вбудовується в ядро Linux.

Недоліки:

− складність налаштування. Ipsec потребує більш детального налаштування ключів, сертифікатів та політик;

− менша продуктивність. Швидкість може бути нижчою через складні алгоритми шифрування;

− складність виявлення проблем. Труднощі у налагодженні, якщо щось не працює.

ZeroTier [36]

Переваги:

− простота у використанні. Мінімальне налаштування, доступне навіть для недосвідчених користувачів;

− глобальна маршрутизація. Дозволяє створювати віртуальні мережі, що працюють через Інтернет без потреби у статичних IP;

− підтримка NAT Traversal. Працює без проблем із пристроями за NAT.

Недоліки:

− залежність від хмарної платформи. Для роботи потрібні сервери ZeroTier, що може бути обмеженням у корпоративних мережах;

− безпека. Менш прозорий у порівнянні з WireGuard, оскільки його протокол не є повністю відкритим;

− продуктивність. Трохи поступається WireGuard за швидкістю.

OpenSwitch [35].

Переваги:

− можливість роботи з великими мережами. Ідеально підходить для комутаторів і мережевої маршрутизації;

− гнучкість налаштувань SPAN [20]. Підтримує складні сценарії моніторингу мережевого трафіку;

− відкритий код. Добре інтегрується з іншими інструментами для моніторингу.

Недоліки:

− не підходить для VPN. Це програмне забезпечення більше орієнтоване на мережеву маршрутизацію, а не на шифрування;

− складність у налаштуванні. Потрібні знання мережевих технологій для правильного налаштування.

OpenWrt (рисунок 3.4) [33].

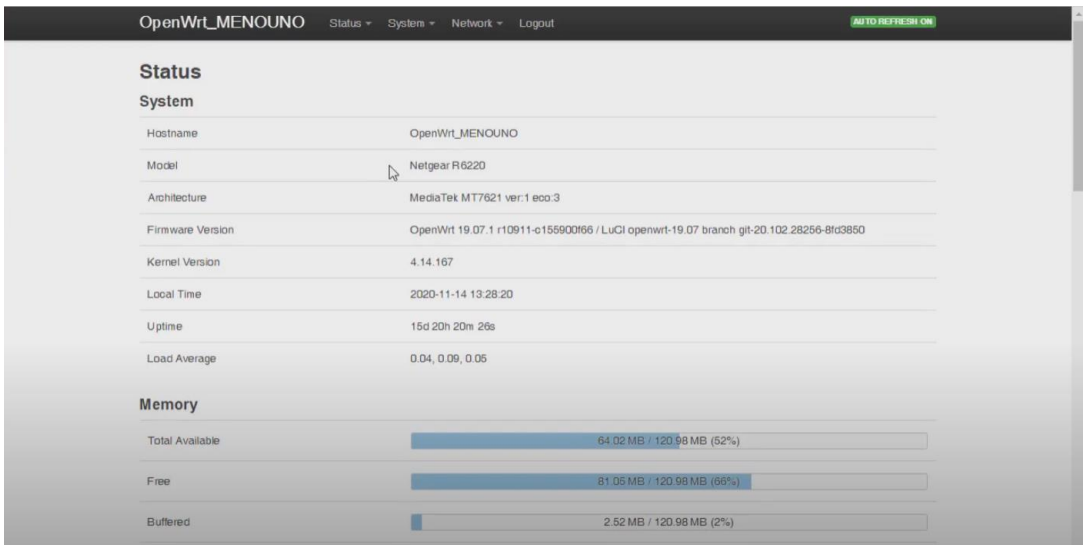

Рисунок 3.4 – Інтерфейс панель керування OpenWRT

Переваги:

- гнучкість та модульність;
- підтримка SPAN-порту;
- підтримка VPN;
- відкрите програмне забезпечення;
- масштабованість;
- моніторинг трафіку.

Недоліки:

- складність налаштування;
- залежність від обладнання;
- менша швидкість у порівнянні з WireGuard;
- відсутність підтримки корпоративного рівня.

3.2 Налаштування SPAN порту для моніторингу трафіку

SPAN (Switched Port Analyzer) – це функція на комутаторах, яка дозволяє віддзеркалювати (копіювати) трафік з одного або кількох портів на інший порт для аналізу. Ця технологія використовується для моніторингу

мережевого трафіку без втручання в роботу мережі. Вона особливо корисна для систем виявлення загроз, таких як **Security Onion**, які можуть аналізувати копії мережевого трафіку [20].

SPAN дозволяє налаштувати комутатор таким чином, щоб копіювати весь трафік, який проходить через певний порт або групу портів, на окремий порт, до якого можна підключити пристрій для моніторингу, наприклад сервер із Security Onion [20].

Типи SPAN.

1. Local SPAN. Копіює трафік з одного або декількох портів комутатора на інший порт на тому ж самому комутаторі.

2. Remote SPAN (RSPAN). Дозволяє віддзеркалювати трафік на порт, який знаходиться на іншому комутаторі у віддаленому сегменті мережі.

Крок 1. Підготовка до налаштування SPAN.

1. Визначте порти для моніторингу. Вам потрібно визначити порти, трафік яких ви хочете моніторити. Наприклад, якщо ви хочете спостерігати за трафіком серверів або робочих станцій, потрібно вибрати відповідні порти.

2. Визначте SPAN порт. Це порт, на який буде копіюватися трафік. До цього порту підключається сервер із системою моніторингу (наприклад, Security Onion).

Крок 2. Налаштування SPAN на комутаторі Cisco (як приклад).

1. Увійдіть у режим конфігурації: Підключіться до комутатора через SSH або консольний кабель і перейдіть у режим конфігурації: enable configure terminal.

2. Налаштуйте вихідний SPAN порт. Вихідний порт – це порт, куди буде надсилатися скопійований трафік для моніторингу. Наприклад, якщо ваш сервер моніторингу підключений до порту GigabitEthernet0/10, ви налаштуєте його наступним чином:

monitor session 1 destination interface GigabitEthernet0/10.

3. Виберіть порти для моніторингу. Визначте порти, трафік з яких ви хочете моніторити. Наприклад, якщо ви хочете моніторити трафік з портів GigabitEthernet0/1 та GigabitEthernet0/2, виконайте таку команду:

monitor session 1 source interface GigabitEthernet0/1 monitor session 1 source interface GigabitEthernet0/2

4. Вихід з режиму конфігурації. Після того як ви налаштували SPAN, вийдіть з режиму конфігурації:

end

5. Перевірка налаштувань. Перевірте, чи правильно налаштований SPAN порт:

show monitor session 1

Крок 3. Налаштування SPAN на комутаторах інших виробників.

На різних комутаторах (наприклад, HP, Juniper, Mikrotik або Netgear) налаштування SPAN може відрізнятись, але концепція залишається подібною.

Розглянемо приклад для Mikrotik.

1. Налаштуйте порт, який буде моніторити трафік: Наприклад, якщо ви хочете моніторити трафік з порту 2 на порт 3: /interface ethernet switch set mirror-source=ether2 mirror-target=ether3

Крок 4. Підключення Security Onion для моніторингу.

1. Підключення до SPAN порту. Після налаштування SPAN порту на комутаторі підключіть сервер із Security Onion до порту, який був призначений для моніторингу. Важливо, щоб цей порт був налаштований тільки на прийом трафіку, оскільки його призначення – лише отримувати віддзеркалений трафік для аналізу.

2. Налаштування мережевого інтерфейсу на Security Onion:

− На сервері Security Onion налаштуйте мережевий інтерфейс для прийому трафіку, який надходить через SPAN порт.

− Це може бути окремий інтерфейс, який не має IP-адреси, але отримує всі пакети для аналізу. У системах на базі Linux це можна зробити за допомогою таких команд:

sudo ifconfig eth1 up

де eth1 – це інтерфейс, підключений до SPAN порту.

3. Моніторинг трафіку:

− після налаштування SPAN портів сервер Security Onion почне отримувати копії мережевого трафіку з портів, які ви вказали для моніторингу;

− тепер Security Onion зможе аналізувати трафік в реальному часі, використовуючи такі інструменти, як **Zeek**, **Suricata** або **Wireshark** для виявлення аномалій і загроз.

Крок 5. Тестування налаштувань.

1. Перевірте, чи отримує сервер трафік: Використовуйте інструменти, такі як tcpdump або Wireshark [42] для перевірки, чи сервер Security Onion отримує трафік через SPAN порт:

sudo tcpdump -i eth1

Аналіз трафіку в Security Onion. В інтерфейсі Security Onion ви зможете бачити деталі отриманого трафіку. Для перевірки роботи SPAN можна переглядати лог файли або використовувати Kibana для візуалізації трафіку.

3.3 Збір і аналіз трафіку за допомогою Security Onion

Основними компонентами, що відповідають за аналіз трафіку, є Zeek (Bro) та Suricata, які забезпечують глибокий аналіз мережевих подій.

Крок 1. Налаштування Security Onion для збору трафіку.

1. Підключення до мережевого інтерфейсу. Важливо переконатися, що інтерфейс, підключений до порту SPAN, налаштований на отримання

мережевого трафіку. Наприклад, якщо інтерфейс називається eth1, увімкніть його:

sudo ifconfig eth1 up

2. Налаштування мережевого інтерфейсу для аналізу. Security Onion зазвичай налаштований так, що інтерфейс для аналізу не має IP-адреси, оскільки його роль полягає лише в прийомі трафіку для аналізу, а не в обміні даними з іншими вузлами.

3. Активація збору трафіку. Під час початкового налаштування Security Onion ви вибираєте мережеві інтерфейси, які будуть використовуватися для моніторингу. Переконайтеся, що ваш інтерфейс для аналізу трафіку (той, який підключений до SPAN-порту) правильно вибраний для моніторингу.

Крок 2. Збір трафіку.

1. **Zeek** виконує пасивний аналіз трафіку, збирає метадані та генерує лог-файли про сесію кожного підключення (HTTP, DNS, SSL, FTP тощо).

Після збору трафіку Zeek генерує журнали в /nsm/bro/logs, які містять різноманітну інформацію про активність у мережі, наприклад:

- логи HTTP-запитів;
- логи сесійного часу для підключень;
- логи DNS-запитів;

2. Suricata є системою глибокого аналізу трафіку, яка використовує базу підписів для виявлення загроз. Вона аналізує трафік в реальному часі, порівнюючи його з набором правил і відомих сигнатур атак.

Suricata може також створювати файли PCAP для збереження повних копій трафіку для подальшого аналізу.

3. Збереження логів і сесій. Логи і файли PCAP, зібрані системою, можна знайти в директоріях /nsm/bro/logs для Zeek та /nsm/suricata для Suricata.

Файли PCAP також можна використовувати для аналізу в інших інструментах, таких як Wireshark [42] або для ручного розбору пакетів.

Крок 3. Аналіз трафіку.

1. Kibana для візуалізації та аналізу. Kibana є інструментом візуалізації та пошуку в Elastic Stack, який надає інтерфейс для зручного пошуку та аналізу мережевого трафіку, журналів, подій.

Для перегляду зібраного трафіку та подій у Kibana перейдіть до веб-інтерфейсу Security Onion і виберіть панелі, які містять метадані мережевих подій, таких як HTTP, DNS, SSL.

Приклад пошуку активності в Kibana:

− перевірка всіх HTTP запитів у мережі:

event.dataset: «zeek.http»;

− пошук підозрілих DNS-запитів:

event.dataset: «zeek.dns»;

2. Sguil для моніторингу подій. Sguil є інструментом для інтерактивного моніторингу подій безпеки в режимі реального часу. Він інтегрований з Suricata та Zeek і дозволяє легко переглядати підозрілі сесії та глибше аналізувати мережеві події.

Використовуйте Sguil для виявлення активностей, які можуть вказувати на можливі атаки або аномальні дії у вашій мережі.

3. Zeek для аналізу. Zeek генерує лог-файли для кожного типу трафіку, що проходить через мережу. Аналіз цих логів дозволяє виявляти аномальні активності, такі як:

− підозрілі HTTP-запити;

− незвичайна активність DNS;

− SSL сесії з незвичних джерел.

Необхідно використовувати Zeek-cut для витягання потрібної інформації з логів:

zeek-cut <ім’я поля> < ім’я_файлу_лога

Крок 4. Виявлення та реагування на загрози.

1. Виявлення загроз з Suricata:

− Suricata може генерувати попередження про загрози на основі аналізу трафіку. Це можуть бути спроби вторгнення, сканування портів або інші шкідливі дії;

− попередження можна переглядати у Kibana або в **Sguil**, де вони будуть виводитись у реальному часі.

2. Інтерактивний аналіз подій. Після виявлення підозрілої активності можна детально переглянути сесії в Kibana або Sguil. Також можна завантажити і проаналізувати повні копії трафіку (PCAP) за допомогою Wireshark [42] або інших інструментів.

3. Автоматизація реагування. Security Onion дозволяє автоматизувати реагування на деякі загрози, використовуючи попередньо налаштовані правила. Ви можете додавати власні правила для Suricata або Zeek для більш точного налаштування виявлення аномалій.

Крок 5. Оптимізація та налаштування правил.

1. Налаштування правил Suricata:

− Suricata використовує підписані правила для виявлення загроз. Важливо регулярно оновлювати ці правила, щоб захистити вашу мережу від нових загроз.

− Для оновлення бази правил виконайте: sudo so-rule-update.

2. Налаштування правил Zeek. Можна створювати свої власні сценарії для Zeek, що дозволяють автоматизувати специфічний аналіз мережевого трафіку або виявлення певних загроз.

3.4 Виявлення та аналіз кіберзагроз

Security Onion – це комплексне рішення для виявлення, моніторингу та аналізу кіберзагроз, яке використовує комбінацію відкритих інструментів для

мережевої безпеки. Завдяки інтеграції таких рішень, як Zeek, Suricata, Elastic Stack (ELK), Sguil та інших, Security Onion дозволяє детально виявляти та аналізувати кіберзагрози в реальному часі. Далі розглянемо процес виявлення та аналізу загроз на основі даних, зібраних Security Onion.

Підходи до виявлення загроз. Security Onion використовує два основні підходи для виявлення загроз:

- на основі підписів (signature-based detection): Виявлення загроз на основі відомих патернів атак, описаних у підписах (правилах). Цей підхід реалізовано в Suricata;
- на основі поведінки (behavioral-based detection): Аналіз трафіку та подій для виявлення аномальних або підозрілих дій, що можуть бути ознакою нових або невідомих загроз. Такий аналіз реалізовано в Zeek (Bro).

Виявлення загроз за допомогою Suricata.

Suricata – це система виявлення загроз (IDS/IPS), яка працює на основі підписів. Вона порівнює мережевий трафік з відомими шаблонами атак і генерує попередження, коли виявляє збіг.

Налаштування правил. Suricata використовує базу правил, яка містить сигнатури відомих атак, таких як спроби сканування портів, експлойти або підозрілі з'єднання. Правила Suricata можна налаштувати під специфічні потреби мережі або використовувати загальні правила, доступні в інтернеті.

Приклад виявлення атаки на основі правил. Suricata може виявити спробу експлуатації вразливості на вебсервері, використовуючи відповідну підпис:

alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:»WEB_SERVER Exploit Attempt»; flow:to_server,established; content:»/exploit»; nocase; sid:100001; rev:1

Якщо трафік відповідає правилу, Suricata генерує попередження, яке можна переглянути в інтерфейсі Kibana або Sguil.

Оновлення та керування правилами. Suricata дозволяє постійно оновлювати базу правил, щоб підтримувати актуальність виявлення нових

загроз. Це можна робити автоматично або вручну через команду: sudo so-rule-update

Виявлення загроз за допомогою Zeek (Bro).

Zeek (Bro) виконує більш глибокий аналіз трафіку, зосереджуючись на поведінкових аспектах. Він не просто порівнює трафік із підписами, а й створює лог-файли про кожну сесію та тип протоколу. Це дозволяє виявляти аномалії та загрози, які можуть залишитися непоміченими іншими інструментами.

1. Аналіз мережевого трафіку. Zeek – це потужний інструмент, який спеціалізується на аналізі всіх видів мережевих сесій, тобто тих «розмов», які відбуваються між комп'ютерами через мережу. Він може працювати з такими популярними протоколами, як HTTP (те, що ви використовуєте для перегляду сайтів), DNS (який відповідає за пошук адрес в Інтернеті), SSL (забезпечує захищене з'єднання) та FTP (передача файлів).

Zeek не просто дивиться на трафік, а збирає дуже детальну інформацію про кожне підключення. Наприклад, він може побачити, який сайт відкривали, які файли передавали, чи були використані захищені з'єднання і як саме.

Це дуже корисно для виявлення підозрілих подій. Наприклад.

Якщо SSL-з'єднання (зазвичай захищене) використовує дивний сертифікат, який не відповідає відомим стандартам, це може бути ознакою атаки або шкідливого програмного забезпечення.

Якщо хтось (або щось) постійно надсилає незвичайні запити до DNS-сервера, це може означати, що пристрій заражено, і він намагається зв'язатися з командним сервером ботнету (це як головний комп'ютер, який керує вірусами на заражених пристроях).

Таким чином, Zeek допомагає не просто спостерігати за мережею, а й глибше зрозуміти, що відбувається «за лаштунками», навіть якщо ви не експерт у мережевих технологіях.

2. Оповіщення про аномалії. Zeek генерує оповіщення, коли знаходить підозрілу активність, таку як:

- незвичайно тривалі з’єднання;
- DNS-запити до відомих шкідливих доменів;
- підозрілі активності FTP або HTTP-запитів.

Наприклад, якщо було виявлено підозрілий DNS-запит, він запише це в лог і відобразить у Kibana або іншому інтерфейсі для аналізу.

3. Детальний аналіз логів. Zeek зберігає логи про всі протоколи і сесії, які можна використовувати для глибшого аналізу. Це можуть бути логи про HTTP-запити, SSL-сертифікати, DNS-запити тощо.

Наприклад, логи HTTP можуть містити інформацію про заголовки запитів, адреси і параметри, що дозволяє ідентифікувати шкідливі дії: zeek-cut host uri status_code < zeek_http.log

Візуалізація та аналіз даних за допомогою Elastic Stack (Kibana). Elastic Stack у Security Onion використовується для зберігання, пошуку та візуалізації даних про події безпеки. За допомогою Kibana можна аналізувати дані зібраного трафіку та подій.

1. Візуалізація даних у Kibana. Kibana дозволяє створювати дашборди для моніторингу різних типів подій. Наприклад, можна створити панелі для перегляду HTTP-запитів, DNS-запитів або SSL-сесій.

Також можна створювати графіки та звіти для виявлення тенденцій у мережевому трафіку, таких як збільшення кількості запитів до певного хоста або підозрілої активності в певний час.

2. Аналіз попереджень у Kibana. Всі попередження, згенеровані Suricata або Zeek, автоматично відображаються у Kibana. Вони можуть містити детальну інформацію про тип атаки, IP-адреси, порти та інші дані.

За допомогою Kibana можна виконувати гнучкий пошук за ключовими словами або фільтрами, наприклад:

event.module: «suricata» AND event.dataset: «alert» AND source.ip: «192.168.1.10»

3. Виявлення аномалій. Використовуючи потужні можливості фільтрації та пошуку, Kibana дозволяє швидко знаходити аномалії в

мережевих даних, наприклад підозрілі запити до зовнішніх серверів або нетипову активність з певних IP-адрес.

Реагування на інциденти через Sguil.

Sguil є інструментом для моніторингу інцидентів у режимі реального часу, інтегрованим у Security Onion. Він дозволяє легко переглядати та аналізувати події безпеки, включаючи попередження від Suricata і Zeek.

Перегляд попереджень. Sguil надає інформацію про події в режимі реального часу, що дозволяє оперативно реагувати на потенційні загрози. Він відображає попередження з інформацією про атаку, джерело, мету та тип загрози.

Аналіз трафіку. За допомогою Sguil можна завантажувати та аналізувати повні копії трафіку (PCAP-файли), щоб дослідити, як саме проходила атака або яка саме активність є підозрілою.

Реагування на загрози. Security Onion може автоматично реагувати на деякі загрози за допомогою вбудованих механізмів захисту, блокуючи певний трафік або сповіщаючи адміністраторів про критичні події.

Оптимізація правил і налаштувань. Адаптація правил Suricat. Ви можете редагувати правила Suricata для кращого виявлення загроз у конкретному середовищі. Наприклад, якщо ваша мережа має унікальні патерни трафіку, можна створити правила для виявлення аномалій саме в цих патернах.

Налаштування політик Zeek. За допомогою сценаріїв Zeek можна налаштувати більш гнучкі політики безпеки, що будуть автоматично виявляти загрози на основі поведінкових моделей у мережі.

ВИСНОВКИ

У результаті проведеного дослідження було успішно реалізовано систему виявлення інцидентів кібербезпеки на основі Security Onion. Налаштування цієї системи на платформі Proxmox дозволило створити гнучку та ефективну віртуалізацію компонентів, необхідних для моніторингу мережевого трафіку. Завдяки окремому віртуальному маршрутизатору на базі Ubuntu, до якого підключені інші віртуальні машини, вдалося організувати ефективний збір та аналіз даних.

Спеціально налаштований SPAN порт забезпечив можливість контролювати трафік з різних джерел, що підключаються до маршрутизатора. Це дозволило Security Onion здійснювати моніторинг і виявлення потенційних загроз у реальному часі. Використання Debian 12 у якості базової операційної системи для розгортання рішення забезпечило стабільність та продуктивність.

Загалом, результати дослідження підтвердили ефективність системи Security Onion у виявленні інцидентів кібербезпеки, а також підтвердили можливість реалізації подібних рішень у віртуалізованих середовищах. Вдосконалення та подальші дослідження в цій галузі можуть суттєво підвищити рівень кібербезпеки в організаціях.

Подальший розвиток системи виявлення інцидентів кібербезпеки з використанням Security Onion та її інтеграція в мережеві архітектури можуть відкрити нові можливості для підвищення ефективності моніторингу та захисту інформаційних систем.

Основні напрямки подальших досліджень.

1. Автоматизація процесів виявлення загроз. Впровадження механізмів машинного навчання та штучного інтелекту для автоматизації аналізу трафіку та виявлення аномалій. Це дозволить зменшити людський фактор і підвищити швидкість реагування на інциденти.

2. Інтеграція з іншими системами безпеки. Розширення можливостей системи шляхом інтеграції з іншими рішеннями, такими як системи управління інформацією та подіями безпеки (SIEM), що дозволить зібрати та проаналізувати дані з різних джерел в одному інтерфейсі.

3. Розвиток віртуалізації та хмарних технологій. Використання хмарних рішень для розгортання Security Onion може забезпечити більшу гнучкість і масштабованість системи, а також спростити її управління та оновлення.

4. Покращення користувацького інтерфейсу. Розробка більш інтуїтивно зрозумілого та зручного для користувача інтерфейсу, що спростить взаємодію з системою та дозволить швидше отримувати потрібну інформацію.

5. Навчання та підвищення обізнаності. Проведення тренінгів та семінарів для спеціалістів у сфері кібербезпеки, щоб підвищити їхні навички у використанні системи Security Onion та виявленні інцидентів.

6. Дослідження нових загроз. Постійний моніторинг еволюції загроз у кіберпросторі та адаптація системи до нових методів атак. Це включає в себе розробку нових алгоритмів виявлення та реагування на загрози.

Ці перспективи розвитку свідчать про високий потенціал системи Security Onion та її здатність адаптуватися до змінюваного ландшафту кібербезпеки. Їх реалізація допоможе організаціям покращити захист своїх інформаційних систем та ефективніше реагувати на кіберзагрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ozkan-Okay, M., Samet, R., Aslan, Ö., & Gupta, D. (2021). A comprehensive systematic literature review on intrusion detection systems. *IEEE Access*, *9*, 157727-157760.

2. Mohammadi, M., Rashid, T. A., Karim, S. H. T., Aldalwie, A. H. M., Tho, Q. T., Bidaki, M., … & Hosseinzadeh, M. (2021). A comprehensive survey and taxonomy of the SVM-based intrusion detection systems. *Journal of Network and Computer Applications*, *178*, 102983.

3. Garuba, M., Liu, C., & Fraites, D. (2008, April). Intrusion techniques: Comparative study of network intrusion detection systems. In *Fifth International Conference on Information Technology: New Generations (itng 2008)* (pp. 592-598).

4. Albasheer, H., Md Siraj, M., Mubarakali, A., Elsier Tayfour, O., Salih, S., Hamdan, M., … & Kamarudeen, S. (2022). Cyber-attack prediction based on network intrusion detection systems for alert correlation techniques: a survey. *Sensors*, *22*(4), 1494.

5. Mulyanto, M., Faisal, M., Prakosa, S. W., & Leu, J. S. (2020). Effectiveness of focal loss for minority classification in network intrusion detection systems. *Symmetry*, *13*(1), 4.

6. Installing Security Onions. [Електронний ресурс]. – Режим доступу: https://medium.com/@imrannajmiie/installing-security-onions-92ba10b349ad

7. Network Configuration. [Електронний ресурс]. – Режим доступу: https://github.com/security-onion-solutions/security-onion/wiki/NetworkConfiguration

8. About Security Onion [Електронний ресурс]. – Режим доступу: https://docs.securityonion.net/en/2.4/about.html

9. ChangingIPAddress [Електронний ресурс]. – Режим доступу: https://github.com/security-onion-solutions/security-onion/wiki/ChangingIPAddress

10. Install Proxmox VE on Debian 12 Bookworm [Електронний ресурс]. – Режим доступу: https://pve.proxmox.com/wiki/Install_Proxmox_VE_on_Debian_12_Bookworm

11. Ubuntu documentation [Електронний ресурс]. – Режим доступу: https://docs.ubuntu.com/

12. Create a Ubuntu VM in Proxmox and setup networking [Електронний ресурс]. – Режим доступу: https://www.snel.com/support/ubuntu-vm-in-proxmox-and-networking-setup/

13. WireGuard installer [Електронний ресурс]. – Режим доступу: https://github.com/angristan/wireguard-install

14. Some Unofficial WireGuard Documentation [Електронний ресурс]. – Режим доступу: https://github.com/pirate/wireguard-docs

15. Configure Catalyst Switched Port Analyzer (SPAN): Example [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html

16. Setting Up a SPAN and Linux Bridge for a Network Sensor [Електронний ресурс]. – Режим доступу: https://medium.com/@LDS_Cyber/setting-up-a-span-and-linux-bridge-for-a-network-sensor-1f29024400a8

17. SecurityOnion on Proxmox [Електронний ресурс]. – Режим доступу: https://docs.securityonion.net/en/2.4/proxmox.html

18. Configuring networks UBUNTU 22.04 [Електронний ресурс]. – Режим доступу: https://ubuntu.com/server/docs/configuring-networks

19. WireGuard Guide [Електронний ресурс]. – Режим доступу: https://github.com/mikeroyal/WireGuard-Guide

20. SPAN Ports and OT Continuous Monitoring: Securing Otherwise Insecure Network Traffic [Електронний ресурс]. – Режим доступу: https://www.automation.com/en-us/articles/may-2024/span-ports-ot-continuous-monitoring-security

21. Proxmox Virtual Environment [Електронний ресурс]. – Режим доступу: https://www.proxmox.com/en/proxmox-virtual-environment/overview

22. Proxmox download [Електронний ресурс]. – Режим доступу: https://www.proxmox.com/en/downloads

23. Linux Container [Електронний ресурс]. – Режим доступу: https://pve.proxmox.com/wiki/Linux_Container

24. Security Onion tools [Електронний ресурс]. – Режим доступу: https://www.cisa.gov/resources-tools/services/security-onion#:~:text=Security%20Onion%20includes%20Elasticsearch%2C%20Logstash,and%20many%20other%20security%20tools.

25. SecurityOnion Software [Електронний ресурс]. – Режим доступу: https://securityonionsolutions.com/software

26. Network Configuration on Proxmox [Електронний ресурс]. – Режим доступу: https://pve.proxmox.com/wiki/Network_Configuration

27. Configuring the network on Proxmox VE on the High Grade, Scale & Advance ranges [Електронний ресурс]. – Режим доступу: https://help.ovhcloud.com/csm/en-dedicated-servers-proxmox-network-hg-scale?id=kb_article_view&sysparm_article=KB0043913

28. How to Install Proxmox (Server Virtualization) on Debian 12 [Електронний ресурс]. – Режим доступу: https://www.tecmint.com/install-proxmox/

29. Proxmox VE Installer on Debian 12 Bookworm [Електронний ресурс]. – Режим доступу: https://github.com/mathewalves/Proxmox-Debian12

30. Proxmox Bibliography [Електронний ресурс]. – Режим доступу: https://github.com/mathewalves/Proxmox-Debian12

31. SecurityOnion SSH [Електронний ресурс]. – Режим доступу: https://github.com/Security-Onion-Solutions/security-onion/wiki/SSH

32. OpenVPN [Електронний ресурс]. – Режим доступу: https://openvpn.net/community-resources/

33. OpenWRT [Електронний ресурс]. – Режим доступу: https://openwrt.org/docs/start

34. Ipsec [Електронний ресурс]. – Режим доступу: https://docs.strongswan.org/docs/latest/howtos/ipsecProtocol.html

35. OpenSwitch [Електронний ресурс]. – Режим доступу: https://docs.openvswitch.org/en/latest/

36. ZeroTier [Електронний ресурс]. – Режим доступу: https://docs.zerotier.com/

37. Vmware vSphere [Електронний ресурс]. – Режим доступу: https://docs.vmware.com/en/Vmware-vSphere/index.html

38. XenServer [Електронний ресурс]. – Режим доступу: https://docs.xenserver.com/en-us/xenserver/8

39. SolarWinds Network Performance Monitor (NPM) [Електронний ресурс]. – Режим доступу: https://documentation.solarwinds.com/en/success_center/npm/content/npm_documentation.htm

40. PRTG Network Monitor [Електронний ресурс]. – Режим доступу: https://www.paessler.com/manuals/prtg

41. Nagios [Електронний ресурс]. – Режим доступу: https://www.nagios.org/documentation/

42. Wireshark [Електронний ресурс]. – Режим доступу: https://www.wireshark.org/docs/

ДОДАТОК А

Копії публікацій



ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В'ЯЧЕСЛАВА ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2024)

науково-практична конференція
молодих вчених, аспірантів та студентів

26–28 серпня 2024
Тернопіль

ЗМІСТ

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

УДК 004.056.5

Алладін МАБРОУК

Західноукраїнський національний університет

СИСТЕМА ВИЯВЛЕННЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ SECURITY ONION

Вступ. Кожен рік кіберзагрози стають дедалі складнішими, число атак на комп'ютерні мережі неухильно збільшується, тим самим створює нові виклики для системних адміністраторів та фахівців з інформаційної безпеки, тож тепер їхнє завдання не лише запобігти можливим атакам, але й уміти швидко виявити і проаналізувати загрози, аби мінімізувати шкоду від потенційних ризиків. В таких умовах стає особливо важливо використовувати ефективні інструменти для моніторингу та аналізу мережевого трафіку.

Один з таких інструментів це Security Onion, він пропонує потужний набір засобів виявлення, моніторингу та аналізу інцидентів мережевих трафіків. Завдяки Security Onion можна збирати і аналізувати інформацію про активність у мережі, які допомагають виявляти атаки на ранніх етапах, щоб швидше реагувати. SecurityOnion дозволяє організаціям будувати надійні механізми захисту, які знижують ризики й підвищують рівень безпеки мережевих ресурсів.

Мета: розкрити процес виявлення та аналізу кіберзагроз за допомогою системи Security Onion.

Основні етапи роботи Security Onion

Security Onion - це дистрибутив Linux, розроблений для виявлення вторгнень, моніторингу безпеки мережі та управління журналами.

Security Onion складається з кількох основних етапів (рисунок 1), кожен з яких відповідає за виконання окремих завдань у процесі моніторингу кібербезпеки.

1. Sensor - слідкує за мережевим трафіком і фіксує події, які відбуваються в мережі. Система отримує дані з різних джерел, таких як мережеві пристрої, сервери чи інші елементи інфраструктури. В результаті, збирається вся інформація про активність в мережі, що допомагає аналізувати потенційні загрози чи аномалію. Основні типи зібраних даних включають:

- журнали подій (Syslog), які містять записи про діяльність систем та інциденти безпеки;
- мережевий трафік, включаючи пакети даних, які можуть бути перевірені на наявність аномальної активності.

2. Обробка та фільтрація трафіку. Після збору дані направляються для обробки за допомогою інструментів, таких як Suricata та Zeek. Ці інструменти виконують наступні функції:

- Suricata аналізує мережеві пакети та шукає підозрілі шаблони, що можуть вказувати на атаки;
- Zeek здійснює аналіз мережевих сесій, виділяючи деталі про HTTP-запити, FTP-сеанси, DNS-запити тощо.

Таким чином, на цьому етапі відбувається початкове виявлення загроз через аналіз мережевого трафіку, що дозволяє виявити можливі інциденти кібербезпеки.

3. Генерація попереджень (Alerts). Якщо оброблені дані містять підозрілу активність, Security Onion створює попередження, яке записується в систему та відображається аналітикам. Попередження формуються в базі даних Elasticsearch, що дозволяє швидко та ефективно здійснювати пошук і фільтрацію інформації про загрози. Попередження можуть включати:

- інформацію про тип загрози (наприклад, DDoS-атака, спроба несанкціонованого доступу тощо);
- відомості про джерело і ціль атаки, що дозволяє оперативно реагувати на загрозу.

4. Аналіз та візуалізація даних. Аналітики кібербезпеки використовують Kibana та інші інструменти для візуалізації та пошуку за даними. Цей етап є важливим для ідентифікації тенденцій та детального аналізу кожного інциденту. Візуалізація даних допомагає швидко виявляти аномалії і спрощує процес аналізу, що дозволяє:

- швидко ідентифікувати джерела загроз;
- оцінювати, як певні події впливають на загальну безпеку мережі.

5. Зберігання даних (Storage Nodes). Всі зібрані та оброблені дані зберігаються на спеціальних серверах. Це важливо для детального розслідування минулих інцидентів і формування профілів загроз. Збереження даних дозволяє:

- проводити ретроспективний аналіз для виявлення схожих інцидентів;
- оцінювати поведінку кіберзлочинців і визначати нові тактики, техніки і процедури, що використовуються під час атак.

6. Планування та управління інцидентами. Необхідно спланувати процес на реагування інцидентів для миттєвої реакції загроз, цей процес допомагає:

- швидко реагувати на інцидент та зупинити загрозу;
- зменшити час на відновлення після інциденту.

7. Індексація даних в Elasticsearch. Компонент seraElasticsearch Index відіграє важливу роль у зберіганні та індексації даних про безпеку, що надходять з різних джерел. Його основні завдання включають:

- збирання даних: Отримання інформації з різних систем моніторингу та безпеки, таких як IDS/IPS, мережевий трафік і журнали подій;
- індексація в Elasticsearch: Дані індексуються для того, щоб їх можна було швидко знайти та проаналізувати. Це дозволяє зберігати велику кількість інформації та ефективно працювати з нею;
- зберігання та пошук: Індексовані дані зберігаються в Elasticsearch, що забезпечує швидкий доступ до них через пошукові запити. Це допомагає оперативно знаходити необхідні відомості за конкретними параметрами, такими як час або тип події;
- візуалізація та аналіз: Дані, що зберігаються в Elasticsearch, можна візуалізувати у Kibana, що полегшує їх аналіз і виявлення можливих інцидентів безпеки.

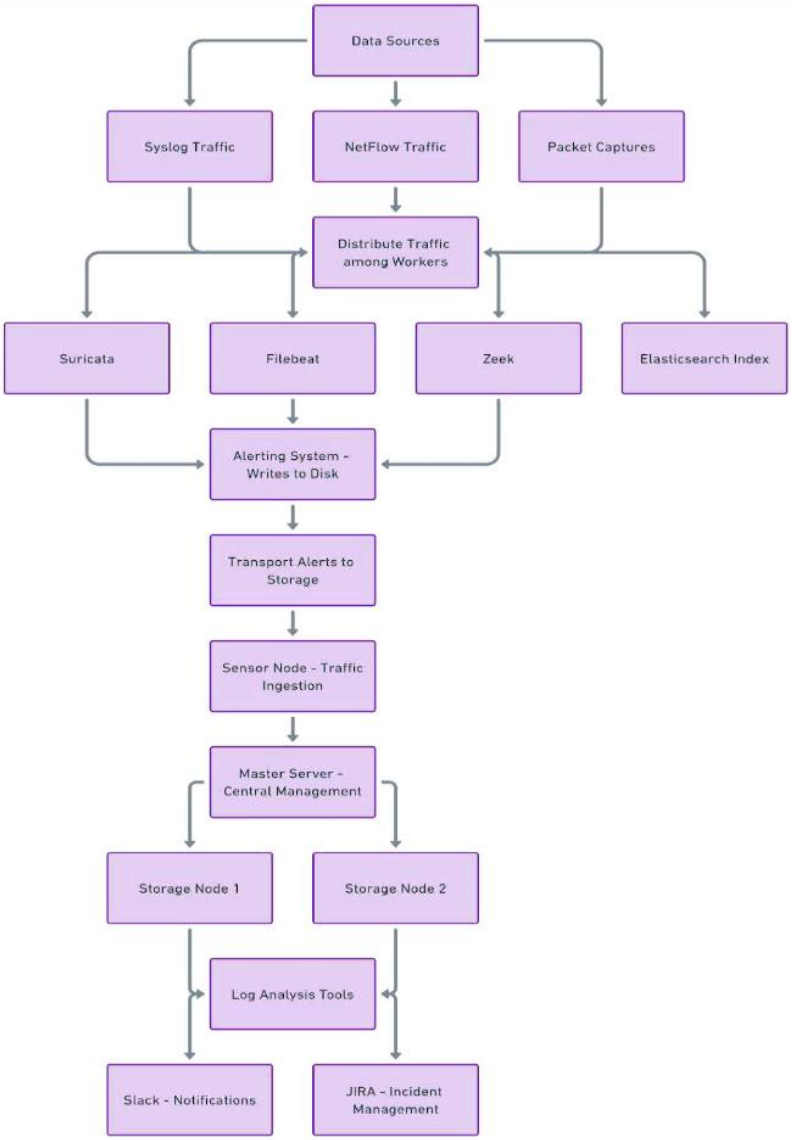

Рисунок 1 - Архітектура компонента в SecurityOnion

Висновок. Security Onion надає все необхідне для забезпечення моніторингу трафіку, надаючи системним адміністраторам та фахівцям інформаційної безпеки інструменти для швидкого виявлення та реагування на загрози. Це рішення допомагає організаціям забезпечити високий рівень безпеки у своїх мережевих ресурсів, запобігаючи та аналізуючи інциденти кібербезпеки в реальному часі та в довгостроковій перспективі. Завдяки структуруванню даних та їх візуалізації, система SecurityOnion є ефективним інструментом для забезпечення захисту в умовах сучасних кіберзагроз.

Перелік використаних джерел.

1. Security Onion Documentation [Електронний ресурс]. - Режим доступу: https://docs.securityonion.net/en/2.4/

2. Elastic Architecture [Електронний ресурс]. - Режим доступу: https://github.com/security-onion-solutions/security-onion/wiki/Elastic-Architecture

ГРОМАДСЬКА ОРГАНІЗАЦІЯ
«КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»

30 листопада 2024
Тернопіль

УДК 004.056.5

Алладін МАБРОУК

Західноукраїнський національний університет

РОЗГОРТАННЯ SECURITY ONION НА БАЗІ ГІПЕРВІЗОРА PROXMOX

Вступ. Кожна компанія, незалежно від сфери діяльності та розміру, може стикнутися з кіберзагрозами з різних джерел: хакерів, шахраїв, конкурентів або навіть через необережність персоналу.

Щоб мінімізувати ризики, пов’язані з кіберзагрозами, компанії повинні впроваджувати комплексні системи безпеки. Одним з ефективних інструментів для цього є Security Onion, який забезпечує проактивне виявлення кіберзагроз шляхом постійного моніторингу мережевого трафіку..

Мета: розкрити процес введення в експлуатацію Security Onion та подальшого налаштування.

1. Основні етапи використання Security Onion

SecurityOnion - це дистрибутив Linux, спеціально розроблений для моніторингу мережевого трафіку та збереження логів для подальшого аналізу.

Вимоги до системи. Для стабільної роботи SecurityOnion необхідне потужне обладнання. Мінімальні вимоги включають:

- 16 ГБ оперативної пам'яті;
- 4 процесорних ядра;
- 200 ГБ жорсткого диску;
- 2 мережевих адаптери.

Для великих мереж вимоги можуть бути суттєво вищими.

Вибір гіпервізора. Для спрощення управління та масштабування рекомендується встановлювати SecurityOnion у віртуальній машині під управлінням гіпервізора Proxmox.

2. Особливості Proxmox

Proxmox Virtual Environment (Proxmox VE) - це високопродуктивний і гнучкий гіпервізор з відкритим кодом, заснований на Debian GNU/Linux. Він призначений для керування віртуальними машинами (VM) та контейнерами LXC, забезпечуючи ефективне використання серверних ресурсів та централізоване управління.

1. Керування віртуальними машинами та контейнерами. Proxmox VE дозволяє створювати, керувати та мігрувати як віртуальні машини (базовані на KVM), так і контейнери LXC з єдиного веб-інтерфейсу. Це забезпечує гнучкість у виборі рівня ізоляції та оптимізації ресурсів.

2. Кластеризація. Proxmox VE підтримує створення кластерів, що дозволяє розподіляти навантаження між декількома фізичними серверами, підвищуючи доступність та масштабованість.

3. Зберігання.Гнучка система зберігання даних, що підтримує різні типи сховищ, включаючи iSCSI, NFS та локальні диски.

4. Мережеве управління. Вбудовані інструменти для керування мережевими інтерфейсами та створення віртуальних мереж.

5. Бек-ап та відновлення. Прості інструменти для створення резервних копій віртуальних машин та контейнерів, а також їх відновлення.

6. Автоматизація. Підтримка сценаріїв на основі QMAPI для автоматизації рутинних задач.

7. Веб-інтерфейс. Інтуїтивно зрозумілий веб-інтерфейс для керування всіма аспектами системи.

8. Безпека. Підтримка шифрування даних, аутентифікації за допомогою LDAP та інших методів для забезпечення безпеки.

Proxmox має ряд переваг:

- відкритий код. Безкоштовний доступ до коду та гнучкість у налаштуванні;
- продуктивність. Висока продуктивність завдяки використанню KVM та LXC;
- масштабованість; Легко масштабується від невеликих до великих середовищ;
- гнучкість. Підтримує різні типи віртуальних машин та контейнерів;
- спільнота. Велика та активна спільнота користувачів та розробників.

Proxmox VE відрізняється від інших гіпервізорів (наприклад, VMware , Microsoft Hyper-V) більш низькими вимогами до апаратного забезпечення, відкритим кодом та гнучкістю налаштувань. Він є відмінним вибором для компаній, які цінують свободу вибору та прагнуть оптимізувати витрати на інфраструктуру.

Налаштування мережі. Для забезпечення ефективного моніторингу необхідно налаштувати мережевий трафік. Рекомендується використовувати віртуальну машину з Ubuntu 22.04, встановлену в Proxmox, в якості маршрутизатора. На цьому маршрутизаторі слід налаштувати:

- WireGuard для створення безпечного тунелю;
- SPAN-порт для копіювання мережевого трафіку з інших пристроїв на SecurityOnion.

Висновок. SecurityOnion є потужним інструментом для моніторингу мережевої безпеки. Однак, він вимагає значних ресурсів і ретельної конфігурації. Відкритий код Proxmox його висока продуктивність та значний набір функцій роблять його одним з найпопулярніших гіпервізорів на сьогоднішній день. Використання Proxmox спрощує управління системою, а налаштування мережі за допомогою WireGuard і SPAN-порту забезпечує ефективний збір даних для аналізу.

Перелік використаних джерел.

1. Proxmox on Debian 12 [Електронний ресурс]. - Режим доступу: https://pve.proxmox.com/wiki/Install_Proxmox_VE_on_Debian_12_Bookworm

2. SecurityOnion documentation [Електронний ресурс]. - Режим доступу: https://docs.securityonion.net/en/2.4/

3. Linux Contaiter [Електронний ресурс]. - Режим доступу: https://pve.proxmox.com/wiki/Linux_Container