Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Створення системи інтерактивного навчання з кібербезпеки з використанням симуляційних середовищ"

Виконав: студент VI курсу, групи СБм-61

Спеціальності:
125 Кібербезпека та захист інформації
(шифр і назва напряму підготовки, спеціальності)
Ворона Максим Сергійович
підпис (прізвище та ініціали)

Керівник Деркач М. В.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Вороні Максиму Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Створення системи інтерактивного навчання з кібербезпеки з використанням симуляційних середовищ

Керівник роботи Деркач Марина Володимирівна,
кандидат технічних наук, доцент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «20» 11 2024 року № 4/7-1112

2. Термін подання студентом завершеної роботи 12.12.2024

3. Вихідні дані до роботи Гіпервізор XEN, Security Onion, Kali Linux та Ubuntu Linux

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз існуючих симуляційних середовищ для навчання з кібербезпеки та їх можливостей.
Розробка архітектури симуляційного середовища на основі гіпервізора XEN (XCP-NG).
Налаштування компонентів Security Onion, зокрема IDS Suricata, Zeek, та ELK Stack.
Моделювання різних типів кіберзагроз. Проведення тестування системи виявлення вторгнень у реалістичних сценаріях. Оцінка ефективності системи виявлення вторгнень.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Актуальність дослідження. Мета, об'єкт, предмет дослідження.
Наукова новизна та практичне значення.
Завдання дослідження.
Типи атак. Схема симуляційного середовища.
Елементи симуляційного середовища.
Тестування компонентів симуляційного середовища.
Тест IDS Suricata. Атака типу SYN flood. Виявлення сигнатури "вірусу".
Атака типу brute-force. Відображення статистики сповіщень в Kibana.
Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 20.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.09 – 22.09	Виконано
2.	Підбір джерел для аналізу в галузі дослідження	25.09 – 10.10	Виконано
3.	Опрацювання джерел в галузі дослідження	11.10 – 15.10	Виконано
4.	Налаштування симуляційного середовища	16.10 – 25.10	Виконано
5.	Моделювання кіберзагроз та оцінка ефективності системи Security Onion	25.10 - 30.10	Виконано
6.	Оформлення розділу «Огляд предметної області»	30.10 – 05.11	Виконано
7.	Оформлення розділу «Елементи симуляційного середовища»	06.11 – 10.11	Виконано
8.	Оформлення розділу «Тестування та оцінка ефективності симуляційного середовища»	11.11 – 25.11	Виконано
9.	Виконання завдання до підрозділу «Охорона праці та безпека в надзвичайних ситуаціях»	26.11-01.12	
10.	Оформлення кваліфікаційної роботи	02.12 – 10.12	Виконано
11.	Нормоконтроль	08.12 – 10.12	Виконано
12.	Перевірка на плагіат	12.12 – 14.12	Виконано
13.	Попередній захист кваліфікаційної роботи	20.12 – 15.12	Виконано
14.	Захист кваліфікаційної роботи	23.12.2024	

Студент _____ Ворона М. С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Деркач М. В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Створення системи інтерактивного навчання з кібербезпеки з використанням симуляційних середовищ // ОР «Магістр» // Ворона Максим Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2024 // С. 85, рис. – 35, табл. – - , кресл. – 18, додат. – 1.

Ключові слова: Security Onion, DDoS, IDS, Suricata, XEN, ELK, Cybersecurity.

У кваліфікаційній роботі магістра розроблено інтерактивну симуляційну систему для навчання з кібербезпеки, яка базується на використанні гіпервізора першого типу XEN та платформи Security Onion. Система дозволяє моделювати реальні сценарії кіберзагроз, аналізувати наслідки атак та розробляти оптимальні методи захисту. У першому розділі роботи проведено огляд існуючих симуляційних середовищ для навчання з кібербезпеки, таких як Check Point Cyber Range, Cyberbit Range, RangeForce та інших. Досліджено можливості гіпервізорів для створення ефективних віртуальних середовищ. Описано різні типи кіберзагроз. У другому розділі представлено архітектуру розробленого симуляційного середовища. Описано налаштування гіпервізора XEN (XCP-NG) та розгортання ключових компонентів: віртуального маршрутизатора MikroTik CHR, серверів Ubuntu Linux та Kali Linux, а також платформи Security Onion з інтегрованими інструментами Suricata, Zeek та Kibana. У третьому розділі здійснено моделювання різних типів атак та тестування системи виявлення вторгнень Suricata, яка успішно виявила та зареєструвала аномальну активність. За допомогою Kibana було візуалізовано зібрані дані, що дозволило провести детальний аналіз інцидентів та оцінити ефективність налаштованих правил.

Результати дослідження підтверджують, що розроблена симуляційна система є ефективним інструментом для навчання та дослідження в галузі кібербезпеки.

ABSTRACT

Creation of an interactive cybersecurity training system using simulation environments // Thesis of educational level "Master"// Maksym Vorona // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-61 // Ternopil, 2024 // P. 85, figs. 35, tables -, drawings 18, added. 1.

Keywords: Security Onion, DDoS, IDS, Suricata, XEN, ELK, Cybersecurity.

In the master's thesis was developed an interactive simulation system for cybersecurity training based on the XEN hypervisor of the first type and the Security Onion platform. The system allows to simulate real-life cyber threat scenarios, analyse the consequences of attacks and develop optimal protection methods. The first section of the paper reviews existing simulation environments for cybersecurity training, such as Check Point Cyber Range, Cyberbit Range, RangeForce, and others. The capabilities of hypervisors for creating effective virtual environments were investigated. Different types of cyber threats were described. The second section presents the architecture of the developed simulation environment. It also describes the configuration of the XEN hypervisor (XCP-NG) and the deployment of key components: the MikroTik CHR virtual router, Ubuntu Linux and Kali Linux, as well as the Security Onion platform with integrated Suricata, Zeek and Kibana tools. In the third section, various types of attacks were simulated and the Suricata intrusion detection system was tested, which successfully detected and logged anomalous activity. Kibana was used to visualise the collected data, which allowed for a detailed analysis of incidents and evaluation of the effectiveness of the configured rules.

The results of the study confirm that the developed simulation system is an effective tool for training and research in the field of cybersecurity.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IDS	—	Intrusion Detection System
DoS	—	Denial of Service
DDoS	—	Distributed Denial of Service
OSI	—	Open Systems Interconnection
TCP	—	Transmission Control Protocol
UDP	—	User Datagram Protocol
ICMP	—	Internet Control Message Protocol
HTTP	—	Hypertext Transfer Protocol
DNS	—	Domain Name System
BIND	—	Berkeley Internet Name Domain
MITM	—	Man-in-the-Middle
MDR	—	Monitoring, Detection, and Response
CHR	—	Cloud Hosted Router
IPS	—	Intrusion Prevention System
LAN	—	Local Area Network
WAN	—	Wide Area Network
DHCP	—	Dynamic Host Configuration Protocol
SSH	—	Secure Shell
NAT	—	Network Address Translation
ARP	—	Address Resolution Protocol

ВСТУП

Актуальність теми. Розвиток інформаційних технологій супроводжується зростанням кількості та складності кіберзагроз, які стають серйозною проблемою. В умовах зростаючої складності атак та вдосконалення методів захисту актуальним є створення інтерактивних навчальних систем для підготовки фахівців з кібербезпеки. Інтерактивні симуляційні середовища дозволяють моделювати реальні сценарії атак, досліджувати їх наслідки та ефективність захисних механізмів. Одним із перспективних рішень у цій галузі є використання Security Onion – потужної платформи для моніторингу, виявлення та аналізу кіберзагроз.

Мета і задачі дослідження. Метою роботи є створення системи інтерактивного навчання з кібербезпеки, заснованої на симуляційних середовищах, що дозволяє ефективно моделювати кіберзагрози, аналізувати наслідки атак і розробляти оптимальні методи захисту.

Для досягнення цієї мети необхідно вирішити такі задачі:

- провести огляд існуючих симуляційних середовищ для навчання з кібербезпеки;
- дослідити можливості гіпервізорів для створення симуляційних середовищ;
- описати типи атак, їх наслідки та методи захисту;
- проаналізувати функціональні можливості Security Onion, включаючи ELK Stack, IDS Suricata, Zeek, CyberChef;
- реалізувати систему інтерактивного навчання на основі гіпервізора першого типу та Security Onion;
- провести тестування системи з використанням реальних сценаріїв атак.

Об’єкт дослідження. Процес навчання з кібербезпеки із застосуванням симуляційних середовищ.

Предмет дослідження. Інтерактивна система навчання з кібербезпеки, побудована з використанням Security Onion для навчання методам виявлення кіберзагроз та їх аналізу.

Наукова новизна одержаних результатів кваліфікаційної роботи. Наукова новизна роботи полягає в удосконаленні підходів до навчання з кібербезпеки шляхом створення інтерактивної симуляційної системи, що базується на Security Onion. Запропонована система дозволяє реалізувати реалістичні сценарії атак і їх аналіз у реальному часі, що покращує якість підготовки фахівців.

Практичне значення одержаних результатів. Розроблена система може бути використана у вищих навчальних закладах та навчальних центрах для підготовки спеціалістів з кібербезпеки. Система дозволяє моделювати різні види атак та навчати ефективним методам захисту.

Апробація результатів магістерської роботи. Основні результати дослідження були представлені на VII міжнародній науково-практичній конференції «Основи сучасних наукових досліджень» (Цюріх, Швейцарія, 13 грудня 2024 р).

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд існуючих симуляційних середовищ для навчання з кібербезпеки

Кіберзагрози стають дедалі складнішими, що вимагає якісної підготовки фахівців із кібербезпеки. Одним із ключових елементів такої підготовки є використання симуляційних середовищ, які дозволяють студентам і професіоналам моделювати реальні сценарії атак, аналізувати наслідки, розробляти та тестувати засоби захисту в безпечному навчальному середовищі.

Симуляційні середовища забезпечують можливість вивчення широкого спектру атак, таких як DDoS, SQL-ін'єкції, фішинг, а також дозволяють відпрацьовувати налаштування засобів захисту, наприклад, систем IDS/IPS [1][2] та брандмауерів. Це робить їх ефективним інструментом для розвитку практичних навичок і стратегічного мислення в умовах, наближених до реальних.

На ринку доступні різноманітні комерційні рішення для симуляційних середовищ, призначених для навчання та підвищення кваліфікації фахівців з кібербезпеки. Ці платформи надають можливість моделювати реалістичні сценарії кібератак, відпрацьовувати методи захисту та реагування на інциденти в безпечному та контрольованому середовищі.

Check Point Cyber Range - це інтерактивна платформа для навчання кібербезпеки, розроблена компанією Check Point Software Technologies. Вона надає користувачам можливість зануритися в реалістичні сценарії кібератак, відпрацьовувати навички захисту та реагування на інциденти в безпечному та контрольованому середовищі. Платформа використовує елементи гри, що робить процес навчання захоплюючим та інтерактивним. Учасники можуть брати участь у місіях та квестах, що сприяє розвитку творчого мислення та командної роботи. Користувачі стикаються з реальними проблемами кібербезпеки, що дозволяє відпрацьовувати навички в умовах, максимально наближених до реальних. Це включає виявлення та нейтралізацію загроз, аналіз вразливостей та впровадження заходів захисту. Платформа адаптується до рівня

знань та потреб користувачів, що робить її придатною як для новачків, так і для досвідчених фахівців. Вона підтримує як індивідуальне навчання, так і групові заняття, сприяючи розвитку командних навичок. Check Point Cyber Range працює на основі хмарних технологій, що забезпечує доступність з будь-якої точки світу та спрощує процес розгортання та оновлення платформи.

Cyberbit Range - це передова платформа для навчання та моделювання в галузі кібербезпеки, яка надає можливість відтворювати реалістичні сценарії кібератак у безпечному середовищі [3]. Вона дозволяє фахівцям з кібербезпеки відпрацьовувати навички виявлення, реагування та нейтралізації загроз, використовуючи реальні інструменти та методи. Платформа підтримує широкий спектр сценаріїв, від базових до складних, що охоплюють різні типи атак, включаючи DDoS, SQL-ін'єкції, фішинг та інші. Cyberbit Range інтегрується з комерційними засобами безпеки, такими як SIEM-системи та брандмауери, що дозволяє користувачам працювати з інструментами, які вони використовують у своїй повсякденній діяльності. Платформа також підтримує моделювання атак на хмарні середовища, що забезпечує підготовку до захисту сучасних інфраструктур. Крім того, Cyberbit Range надає можливість оцінювати ефективність команд, відстежувати прогрес та виявляти прогалини у знаннях, що сприяє підвищенню загальної готовності до кіберзагроз. Завдяки своїй гнучкості та масштабованості, платформа підходить для використання як у великих організаціях, так і в навчальних закладах, забезпечуючи високий рівень підготовки фахівців з кібербезпеки.

RangeForce - це хмарна платформа для інтерактивного навчання кібербезпеки, яка надає користувачам можливість розвивати практичні навички через реалістичні симуляції та лабораторні роботи [4]. Платформа пропонує широкий спектр навчальних модулів, що охоплюють різні аспекти кібербезпеки, включаючи роботу з реальними інструментами, такими як, брандмауери та інші засоби захисту. Користувачі можуть відпрацьовувати навички виявлення та реагування на атаки в живих середовищах, що сприяє глибшому розумінню реальних загроз. RangeForce також підтримує командні тренування, допомагаючи розвивати комунікаційні та лідерські навички, а також

покращувати управління часом під час інцидентів. Платформа дозволяє створювати індивідуальні плани навчання, адаптовані до конкретних ролей, рівнів підготовки та ризиків, що забезпечує цілеспрямований розвиток навичок. Завдяки хмарній інфраструктурі, RangeForce легко розгортається та інтегрується в існуючі процеси навчання, надаючи доступ до актуальних загроз та методів захисту. Платформа також пропонує аналітичні інструменти для відстеження прогресу та оцінки готовності команд до реальних кіберзагроз. Завдяки своїй гнучкості та масштабованості, RangeForce підходить як для індивідуального навчання, так і для корпоративних програм підвищення кваліфікації фахівців з кібербезпеки.

IBM X-Force Cyber Range - це передова платформа для навчання та підготовки фахівців у сфері кібербезпеки, розроблена компанією IBM [5]. Вона надає можливість зануритися в реалістичні сценарії кібератак, що дозволяє учасникам відпрацьовувати навички виявлення, реагування та нейтралізації загроз у безпечному та контрольованому середовищі. Платформа використовує симуляції, які охоплюють технічні, лідерські та комунікаційні аспекти, сприяючи розвитку комплексних навичок у сфері кібербезпеки. IBM X-Force Cyber Range пропонує різні формати навчання: на спеціалізованих об'єктах у Кембриджі (Массачусетс), Вашингтоні (округ Колумбія), Оттаві (Канада) та Бангалорі (Індія); на місці у клієнта; а також у віртуальному форматі, що дозволяє організаціям з усього світу брати участь у тренуваннях. Платформа також інтегрується з іншими послугами IBM, такими як X-Force Threat Intelligence Services та X-Force Red Offensive Security Services, що забезпечує комплексний підхід до підготовки та захисту від кіберзагроз.

Cisco Cyber Range - це інтерактивна платформа, розроблена компанією Cisco, яка надає можливість навчання та підготовки фахівців у сфері кібербезпеки через реалістичні симуляції кібератак [6]. Платформа дозволяє користувачам відпрацьовувати навички виявлення, реагування та нейтралізації загроз у безпечному та контрольованому середовищі. Cisco Cyber Range використовує методологію, що передбачає поступове ускладнення навчальних сценаріїв: від ознайомлення з інструментами та техніками до застосування їх у

реальних сценаріях атак. Протягом курсу учасники проходять через різні етапи. На завершальному етапі учасники беруть участь у комплексному сценарії атаки, де відпрацьовують командну роботу. Платформа також інтегрує реальні тактики, техніки та процедури зловмисників, що забезпечує автентичний досвід для користувачів. Cisco Cyber Range фокусується на методологіях та техніках, незалежних від конкретних інструментів, що дозволяє учасникам застосовувати набуті знання у різних середовищах та з різними технологіями. Платформа також сприяє розвитку командної взаємодії та покращенню технічних навичок, необхідних для ефективного реагування на інциденти.

Міжнародний союз електрозв'язку (ITU) використовує платформу Cyber Ranges для проведення кібернавчань та підвищення кваліфікації фахівців у сфері кібербезпеки. Cyber Ranges - це передова симуляційна платформа, яка надає можливість моделювати реалістичні сценарії кібератак та відпрацьовувати навички реагування на інциденти в безпечному середовищі [7]. Платформа підтримує масштабовані симуляційні середовища з реалістичним трафіком та атаками, що базуються на актуальній інформації про загрози. Вона дозволяє учасникам досліджувати, аналізувати та розробляти ефективні стратегії пом'якшення наслідків атак. Cyber Ranges також забезпечує можливість оцінки політик, планів та процедур, сприяючи підвищенню готовності до реальних кіберзагроз. Платформа використовується ITU для проведення кібернавчань, які включають динамічні сесії з нарощування потенціалу, семінари з захисту критичної інфраструктури, розробки кіберстратегій та міжнародних дискусій на теми кібербезпеки. Під час навчань учасники стикаються з серією високоефективних атак, розроблених експертами ITU на платформі Cyber Ranges, що дозволяє відпрацьовувати навички розслідування, аналізу та розробки стратегій реагування.

Project Ares - це інтерактивна платформа для навчання кібербезпеки, розроблена компанією Circadence [8]. Вона поєднує елементи гри з реалістичними кіберсценаріями, що дозволяє користувачам відпрацьовувати навички виявлення, реагування та нейтралізації загроз у безпечному середовищі. Платформа пропонує широкий спектр навчальних модулів, включаючи базові

лабораторії для освоєння основних інструментів та технік, а також спеціалізовані місії, що моделюють складні атаки, такі як ботнети, фішинг та програми-вимагачі. Project Ares використовує реалістичні мережеві середовища та віртуальні машини, що дозволяє користувачам працювати з автентичними інструментами, такими як Linux, Windows, PowerShell та Wireshark. Платформа також включає вбудовані підказки та поради, що підтримують навчальний процес та допомагають користувачам досягати поставлених цілей. Project Ares інтегрується з хмарною інфраструктурою Microsoft Azure, що забезпечує масштабованість та доступність для користувачів з різних куточків світу. Платформа підходить як для індивідуального навчання, так і для командних тренувань, сприяючи розвитку навичок співпраці та комунікації. Використання Project Ares допомагає студентам та професіоналам підготуватися до реальних викликів у сфері кібербезпеки, надаючи практичний досвід та підвищуючи впевненість у своїх навичках.

Симуляційні платформи можуть бути швидко оновлені для відображення новітніх загроз та вразливостей, що забезпечує актуальність навчального процесу та підготовку до сучасних викликів у сфері кібербезпеки. Практичний досвід, отриманий у симуляційних середовищах, сприяє розвитку критичного мислення, навичок прийняття рішень у стресових ситуаціях та здатності швидко адаптуватися до нових загроз. Крім того, такі середовища надають можливість об'єктивно оцінювати рівень підготовки фахівців, проводити сертифікаційні іспити та визначати області, що потребують додаткового навчання.

1.2 Використання гіпервізорів для створення симуляційних середовищ

Гіпервізори є важливим інструментом для створення віртуальних середовищ, які дозволяють ефективно моделювати і симулювати реальні умови для навчання, тестування або розробки. У контексті симуляційних середовищ для кібербезпеки, гіпервізори використовуються для створення віртуальних машин, які можуть імітувати інфраструктуру реальних мереж та систем, що дає

змогу проводити різноманітні сценарії атак і відпрацювання методів захисту без ризику для реальних систем.

Існує два основних типи гіпервізорів: гіпервізори типу 1 (bare-metal) та гіпервізори типу 2 (hosted) [9,10,11]. Гіпервізори типу 1 - це гіпервізори, які працюють безпосередньо на апаратному забезпеченні хост-системи, без необхідності запускати операційну систему як проміжний шар між апаратним забезпеченням і віртуальними машинами (див. рисунок 1.1).

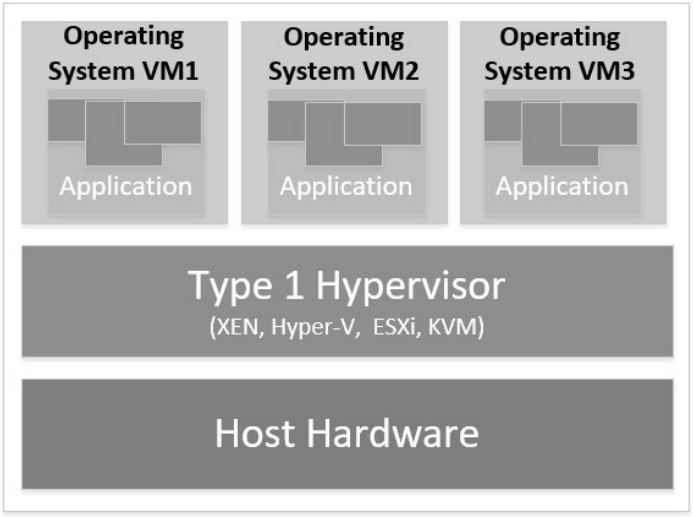

Рисунок 1.1 – Схема гіпервізора типу 1

Це забезпечує високу ефективність і більшу безпеку порівняно з гіпервізорами типу 2, оскільки вони працюють безпосередньо з апаратними ресурсами та не залежать від ОС хоста. Гіпервізори типу 1 управляють фізичними ресурсами, такими як процесор, пам'ять і сховище, і надають ці ресурси кільком віртуальним машинам. Вони мають повний контроль над всіма операціями, що здійснюються на апаратному рівні, що дозволяє їм забезпечувати кращу ізоляцію між віртуальними машинами та зменшувати ймовірність витоків даних чи зловживань із боку зловмисників.

Гіпервізори типу 1 є більш ефективними, оскільки працюють безпосередньо на фізичному апаратному забезпеченні і можуть краще розподіляти ресурси, що забезпечує більшу продуктивність віртуальних машин. Вони також надають кращу ізоляцію між віртуальними машинами, що забезпечує вищий рівень безпеки. Це особливо важливо в умовах, коли система має обробляти чутливі або

критичні дані, оскільки зменшується ризик того, що порушення в одній віртуальній машині вплине на інші. Окрім того, гіпервізори типу 1 підтримують великі інфраструктури, такі як дата-центри або хмарні платформи, що робить їх ідеальними для масштабованих середовищ.

Ці гіпервізори використовуються для віртуалізації серверів та створення інфраструктур, що потребують високої надійності, безпеки та продуктивності. Вони є основою для таких рішень, як VMware vSphere [12], Microsoft Hyper-V [13], XenServer [14] і KVM [15], що широко застосовуються в корпоративних середовищах та дата-центрах.

Гіпервізори типу 2 - це гіпервізори, які працюють поверх операційної системи хоста (див. рисунок 1.2).

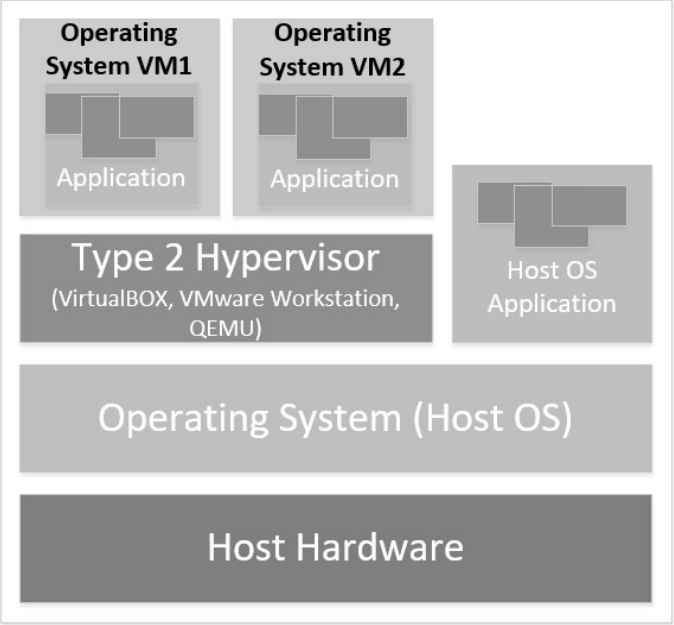

Рисунок 1.2 – Схема гіпервізора типу 2

Вони функціонують як додатки на вже існуючій операційній системі. Це означає, що гіпервізор типу 2 залежить від операційної системи хоста для доступу до апаратних ресурсів, що може знижувати ефективність порівняно з гіпервізорами типу 1.

Гіпервізори типу 2 є більш зручними для використання в середовищах, де не потрібно забезпечувати високу продуктивність або масштабованість, ідеально підходять для персональних комп'ютерів або невеликих серверів, де

користувачам не потрібна складна інфраструктура. Вони дозволяють створювати віртуальні машини, запускати різні операційні системи на одному комп'ютері і працювати в ізольованих середовищах без необхідності виділяти окремі фізичні ресурси для кожної операційної системи.

Гіпервізори типу 2 дозволяють користувачам запускати віртуальні машини на звичайних комп'ютерах, що робить їх зручними для тестування програмного забезпечення або навчання. Популярними прикладами гіпервізорів типу 2 є VMware Workstation, Oracle VirtualBox та Parallels Desktop. Однак, оскільки ці гіпервізори працюють через операційну систему хоста, вони можуть мати певні обмеження у використанні системних ресурсів, порівняно з гіпервізорами типу 1, які безпосередньо працюють з апаратним забезпеченням.

Використання гіпервізорів типу 1 в симуляційних середовищах є одним з найбільш ефективних підходів для створення масштабованих, безпечних і продуктивних віртуальних середовищ. Гіпервізори типу 1 працюють безпосередньо на фізичному апаратному забезпеченні, що дозволяє їм забезпечувати високий рівень продуктивності та безпеки, що є критично важливим для симуляційних середовищ, де відтворюються складні сценарії атак, мережеві взаємодії або тестуються нові технології.

У симуляційних середовищах гіпервізори типу 1 дозволяють створювати кілька ізольованих віртуальних машин, які можуть працювати на одному фізичному сервері. Це дає змогу моделювати різноманітні мережеві інфраструктури, зокрема для тестування різних сценаріїв кіберзагроз, атаки на мережу, перевірки налаштувань безпеки, а також відпрацювання методів захисту в умовах реальної експлуатації. Використання гіпервізорів типу 1 дозволяє максимально ефективно використовувати апаратні ресурси, оскільки вони працюють безпосередньо з ними, що підвищує швидкість і знижує затримки в порівнянні з гіпервізорами типу 2.

Такі гіпервізори ідеально підходять для побудови великих віртуальних лабораторій, де необхідно відтворювати реальні інфраструктури з кількома серверами, клієнтами, брандмауерами, комутаторами і маршрутизаторами. Вони можуть бути використані для створення тестових середовищ, де моделюються

різноманітні типи атак, включаючи DDoS, атаки на мережеву інфраструктуру, зломи систем та інші кіберзагрози. У такому середовищі фахівці з кібербезпеки можуть перевіряти свої стратегії захисту, налаштовувати системи моніторингу та захисту від вторгнень, а також тестувати реакцію на реальні загрози.

Використання гіпервізорів типу 1 також важливе для симуляцій навчання, оскільки дозволяє створювати різноманітні варіанти сценаріїв для тренувань з кібербезпеки без ризику для реальних систем. Віртуальні машини можуть бути швидко налаштовані і видалені, що робить їх ідеальними для динамічних середовищ, де потрібно часто змінювати конфігурації або сценарії.

Гіпервізори типу 1 дозволяють також здійснювати глибокий контроль за ресурсами, включаючи CPU, пам'ять, сховище та мережеві ресурси, що дає можливість симулювати сценарії високих навантажень і тестувати стійкість систем до великих обсягів трафіку або складних атак. Це забезпечує не тільки ефективність, але й надійність тестових середовищ, що критично важливо для реалістичних симуляцій і навчань у кібербезпеці.

1.3 Типи атак та методи їх виявлення і запобігання

Атаки на доступність, конфіденційність та цілісність разом формують ключові загрози інформаційній безпеці [16].

1.3.1 Атаки на доступність

Атаки на доступність спрямовані на порушення нормального функціонування інформаційних систем, мереж чи сервісів, унаслідок чого легітимні користувачі не можуть отримати доступ до ресурсів. Цей тип атак є однією з ключових загроз для організацій, оскільки він здатний паралізувати бізнес-процеси, призводячи до фінансових втрат та зниження довіри клієнтів.

До цього типу атак належать атаки типу DoS та DDoS [17]. Атака відмови в обслуговуванні здійснюється шляхом перенавантаження системи або мережі запитами, які система не може обробити. Наприклад, масові запити до веб-

сервера, що перевищують його обчислювальні потужності, призводять до збою. Розподілені атаки відмови в обслуговуванні реалізуються за допомогою великої кількості зламаних пристроїв (ботнетів), які синхронно надсилають запити до цільової системи [18]. Це ускладнює виявлення джерела атаки та її нейтралізацію.

Атаки на доступність можуть відбуватися на різних рівнях моделі OSI, залежно від того, які частини комунікаційної інфраструктури атакують зловмисники. Ці атаки спрямовані на порушення роботи систем або ресурсів, використовуючи слабкі місця конкретного рівня.

На фізичному рівні атаки пов'язані з пошкодженням апаратного забезпечення або фізичної інфраструктури. Це можуть бути фізичні пошкодження кабелів, відключення електроживлення, саботаж мережевого обладнання, таких як маршрутизатори, комутатори або точки доступу. Зловмисники також можуть використовувати засоби радіочастотного перешкоджання для блокування роботи бездротових мереж (Wi-Fi, Bluetooth).

Методи запобігання включають фізичний захист обладнання, резервне живлення (UPS) та використання екранів для захисту від радіоперешкод.

Атаки на канальному рівні можуть включати MAC-flood [19]. Її суть полягає у перевантаженні таблиці комутатора (CAM-таблиці) великою кількістю підроблених MAC-адрес (див. рисунок 1.3).

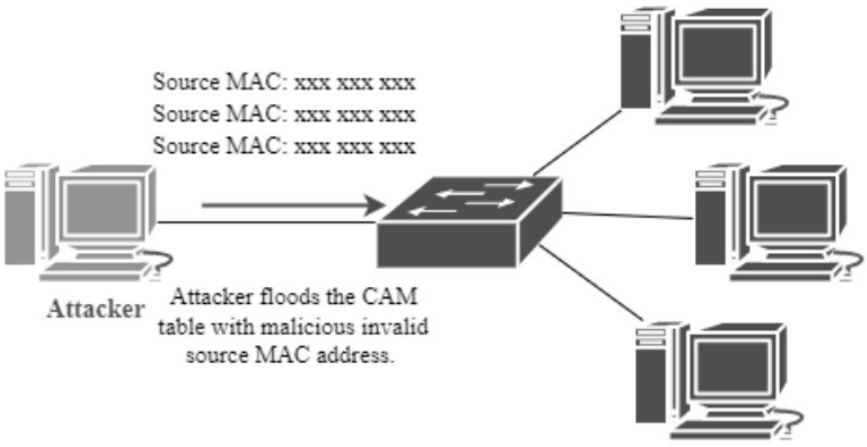

Рисунок 1.3 – Атака типу MAC-flood

Коли таблиця перевантажена, комутатор переходить у режим хабу і починає пересилати всі кадри на всі порти, що значно знижує продуктивність мережі і може бути використано для перехоплення трафіку.

Інший приклад - ARP-spoofing, де зловмисник підміняє ARP-відповіді у мережі [20] (див. рисунок 1.4).

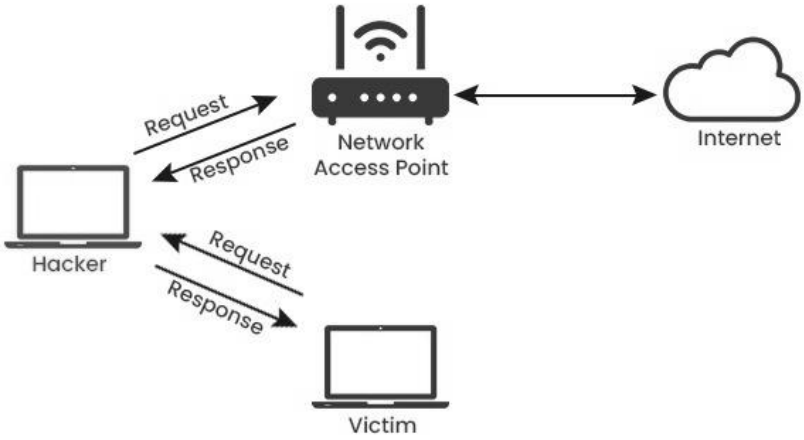

Рисунок 1.4 – Атака типу ARP-spoofing

У результаті пристрої починають асоціювати IP-адресу зловмисника із MAC-адресою іншого пристрою. Це дозволяє атакуючому перехоплювати або модифікувати мережевий трафік, порушуючи комунікацію між пристроями.

Запобігання включає використання механізмів Port Security, обмеження кількості MAC-адрес на порт та впровадження захищених протоколів ARP (Dynamic ARP Inspection).

Атаки на мережевому рівні спрямовані на порушення функціонування протоколів маршрутизації або блокування мережевих ресурсів. Основна мета таких атак - погіршити роботу мережі, порушити маршрутизацію даних, вивести ресурси з ладу.

ICMP Flood - це тип атаки DoS, який спрямований на перевантаження цільової системи великим обсягом ICMP-пакетів (зазвичай ICMP Echo Request) [21]. Протокол ICMP є частиною мережевого рівня та використовується для діагностики мережевих проблем і надсилання службових повідомлень. Атаки ICMP Flood експлуатують цей протокол, генеруючи великий обсяг ICMP Echo Request (Ping) запитів до цільової системи або мережі (див. рисунок 1.5).

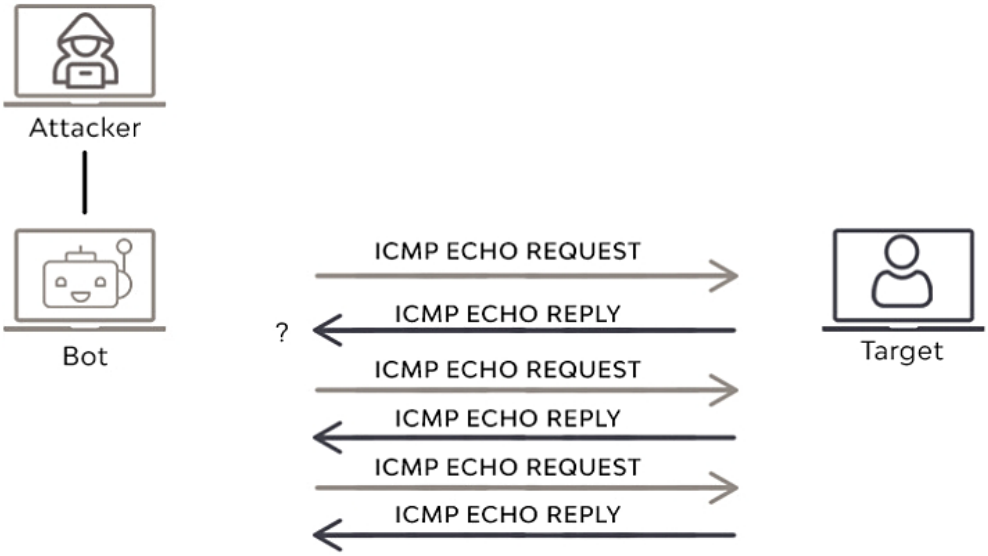

Рисунок 1.5 – Атака типу ICMP Flood

Система змушена обробляти велику кількість ICMP-запитів і формувати відповідні відповіді (ICMP Echo Reply), що вимагає значних обчислювальних потужностей. Великий обсяг ICMP-пакетів перевантажує мережу, роблячи її недоступною для легітимних користувачів. Для запобігання застосовують фільтрацію трафіку, використання чорних списків, обмеження пропускної здатності для запобігання перевантаження.

IP Spoofing - це техніка, за допомогою якої зловмисник змінює IP-адресу джерела в заголовку IP-пакета, щоб приховати своє справжнє місцезнаходження або видавати себе за інший пристрій [22] (див. рисунок 1.6).

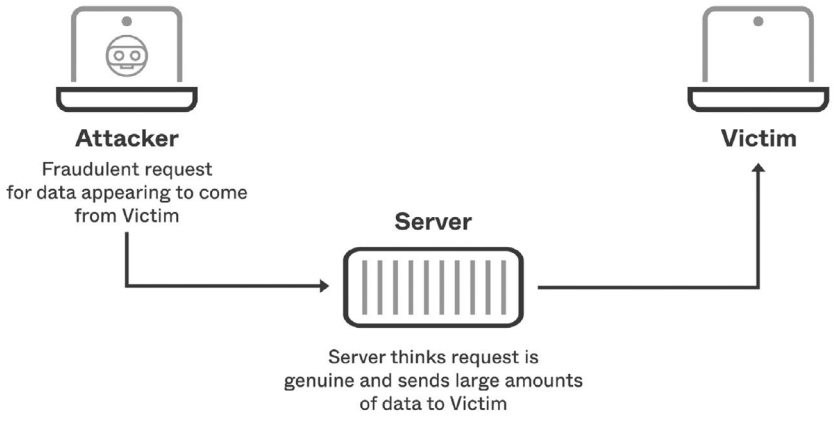

Рисунок 1.6 – Атака типу IP Spoofing

Ця техніка часто використовується для здійснення атак або обходу засобів безпеки. При передачі даних у мережі кожен IP-пакет містить адресу джерела і адресу призначення. Зловмисник змінює адресу джерела, підставляючи вигадану чи легітимну IP-адресу замість своєї. Це створює ілюзію, що трафік походить від іншого джерела. Для запобігання IP Spoofing застосовуються методи, такі як фільтрація вихідного трафіку, коли маршрутизатори перевіряють відповідність вихідної IP-адреси дійсному маршруту. IDS/IPS-системи допомагають виявляти підроблені IP-адреси. Ефективний захист включає моніторинг аномального трафіку, аналіз мережевих потоків та налаштування мережевих політик для обмеження доступу тільки для довірених IP-адрес.

Транспортний рівень моделі OSI відповідає за передачу даних між вузлами та забезпечення надійності цієї передачі. Основними протоколами цього рівня є TCP та UDP. Атаки на цьому рівні спрямовані на порушення роботи цих протоколів, перевантаження ресурсів чи отримання несанкціонованого доступу до даних.

Однією з найпоширеніших атак є TCP SYN Flood, при якій зловмисник надсилає великий обсяг запитів на встановлення з'єднання (SYN-пакетів), але не завершує тристоронній рукостиск (TCP handshake) [23] (див. рисунок 1.7).

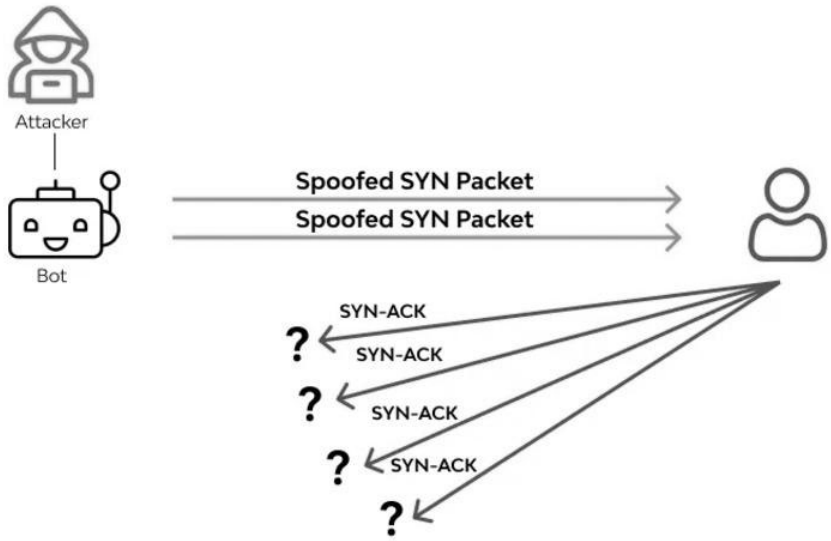

Рисунок 1.7 – Атака типу TCP SYN Flood

Це залишає сервер із напіввідкритими з'єднаннями, що призводить до вичерпання ресурсів сервера, роблячи його недоступним для легітимних користувачів.

Інший варіант - UDP Flood, де зловмисник надсилає велику кількість UDP-пакетів на випадкові порти цільового пристрою, змушуючи його перевіряти порти та надсилати ICMP-повідомлення про недосяжність [24] (див. рисунок 1.8).

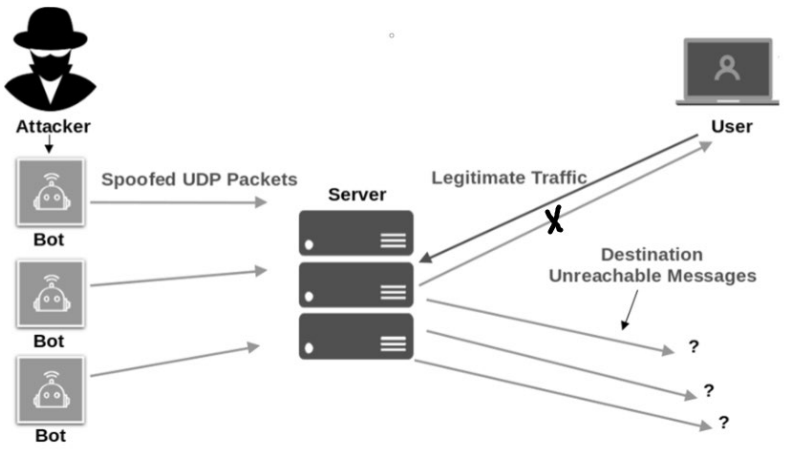

Рисунок 1.8 – Атака типу UDP Flood

Оскільки UDP є безстановий протокол, який не встановлює з'єднання і не перевіряє статус, ця атака може бути особливо ефективною для викликання перевантаження системи, оскільки пристрій, отримавши UDP-пакет, спробує відповісти на нього або перевірити, чи відкритий відповідний порт.

Кожен UDP-пакет, що надсилається на випадковий порт цільового сервера або маршрутизатора, змушує пристрій перевіряти, чи є відповідна служба, що відповідає на цей порт. Якщо сервіс не доступний, пристрій зазвичай надсилає ICMP-повідомлення "destination unreachable" назад. Оскільки на сервері чи маршрутизаторі можуть бути відкриті багато портів, що спричиняють велику кількість оброблених запитів, це перевантажує ресурси сервера та мережу.

UDP Flood може мати великий негативний вплив на сервери, що обробляють велику кількість пакетів, зокрема на ті, що мають обмежені ресурси для обробки

великих обсягів трафіку. Ці атаки можуть знизити продуктивність системи, а в деяких випадках навіть призвести до повної недоступності мережі або сервісу.

Методи запобігання UDP Flood включають фільтрацію непотрібного UDP-трафіку на маршрутизаторах і брандмауерах, використання IDS для моніторингу підозрілої активності, обмеження кількості UDP-пакетів, що можуть бути оброблені на порт, а також використання DDoS-захисту від сторонніх провайдерів.

У випадку TCP Reset Attack зловмисник надсилає підроблені TCP RST-пакети для примусового завершення активних сеансів зв'язку, порушуючи передачу даних між сторонами [25].

Для захисту від атак на транспортному рівні використовуються такі методи, як впровадження механізмів SYN Cookies для запобігання TCP SYN Flood, налаштування таймаутів для з'єднань, а також використання фільтрації трафіку за допомогою брандмауерів. IDS/IPS-системи допомагають ідентифікувати аномальну активність у мережі.

На прикладному рівні атаки є найбільш поширеними та багатогранними. Прикладами є, коли зловмисники надсилають велику кількість HTTP запитів, що перевантажують сервер [26] (див. рисунок 1.9).

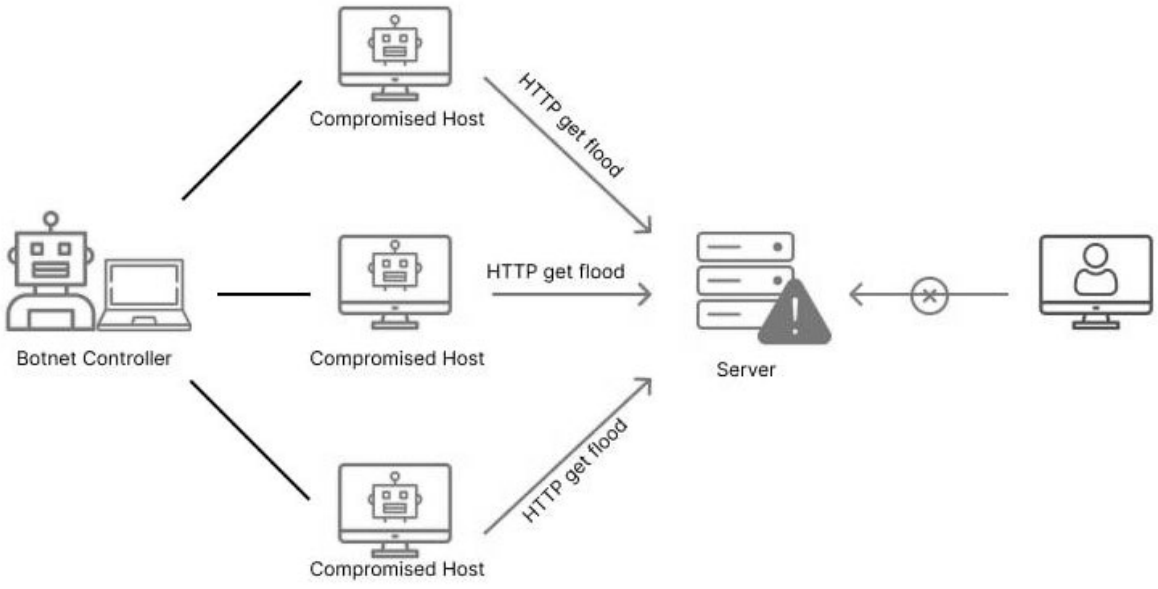

Рисунок 1.9 – Атака типу HTTP Flood

Методи запобігання включають впровадження веб-аплікаційних брандмауерів (WAF), використання CAPTCHAs для перевірки активності користувачів, а також постійний моніторинг роботи серверів.

Іншим прикладом є атаки на специфічні сервіси, наприклад, DNS Amplification, які використовують вразливості DNS для генерації масивного трафіку [27] (див. рисунок 1.10).

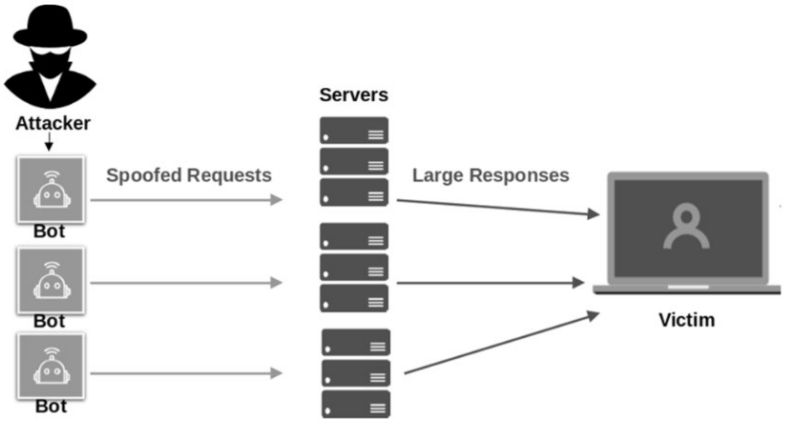

Рисунок 1.10 – Атака типу DNS Amplification

У цьому випадку зловмисник підробляє адресу джерела запиту, спрямовуючи його на відкритий DNS-сервер, який відповідає значно більшим обсягом даних, ніж запит, на адресу жертви. Це дозволяє зловмисникові значно збільшити обсяг трафіку, що надсилається на жертву, в результаті чого ресурс жертви може бути перевантажений, що призводить до його недоступності для легітимних користувачів. Під час атаки DNS-сервер відповідає на запит великими пакетами даних, що перевантажують сервери жертви і можуть спричинити відмову в обслуговуванні.

Зловмисник генерує DNS-запит з підробленою IP-адресою жертви, на яку сервер відповідає великим обсягом даних, часто в багато разів більшим за обсяг самого запиту. Цей трафік несе великі навантаження на сервери і мережу жертви, що робить їх недоступними. Оскільки DNS-сервери часто не перевіряють джерело запиту, вони можуть бути використані для цих атак, що робить їх вразливими.

Захист від таких атак включає обмеження рекурсивних запитів на публічних DNS-серверах, фільтрацію трафіку, використання обмежень на максимальний розмір відповіді, застосування анти-DDoS рішень, таких як сервіси від Cloudflare або Akamai, а також постійний моніторинг трафіку для виявлення аномальних запитів.

1.3.1 Атаки на конфіденційність

Атаки на конфіденційність спрямовані на несанкціонований доступ до чутливої або особистої інформації з метою її викрадення, модифікації або знищення. Конфіденційність забезпечує, щоб тільки уповноважені особи мали доступ до певної інформації, тому атаки на конфіденційність можуть мати серйозні наслідки, включаючи витік особистих даних, фінансову шкоду та втрату довіри до організацій.

Фішинг - це атака, коли зловмисники намагаються викрасти конфіденційну інформацію, видаючи себе за надійні джерела. Зазвичай атака відбувається через електронну пошту, SMS або соціальні мережі. Зловмисники надсилають повідомлення, що виглядають як офіційні запити, і просять користувача навести чутливі дані, такі як логіни, паролі, номери кредитних карт або інші особисті відомості. Витік даних це випадок, коли організація або система втрачає контроль над чутливою інформацією, яка потрапляє до рук зловмисників. Витік може статися через слабкі місця в системах безпеки, в тому числі через злами, неправильне зберігання або передавання даних. Кібератаки, такі як SQL-ін'єкції або вразливості в програмному забезпеченні, можуть бути використані для отримання доступу до великих обсягів даних, включаючи особисту інформацію. Спостереження за трафіком - це випадок, коли зловмисник перехоплює дані, які передаються між двома сторонами. Це може відбуватися через техніку MITM, де зловмисник знаходиться між двома пристроями, що обмінюються даними, і перехоплює або змінює інформацію. Спостереження за трафіком може бути використано для збору чутливих даних, таких як паролі, номери кредитних карт або інші особисті дані. Крадіжка ідентифікації - ця атака полягає у використанні

викрадених персональних даних для здійснення несанкціонованих дій, таких як отримання кредитів, відкриття банківських рахунків або навіть вчинення кримінальних дій під чужим ім'ям. Зловмисники можуть використовувати крадену інформацію, щоб обдурити фінансові установи, державні органи або компанії, що надають послуги. Скріпт-атаки і ін'єкції - атаки, що використовують вразливості у веб-додатках, такі як Cross-Site Scripting (XSS) або SQL-ін'єкції, дозволяють зловмисникам виконувати шкідливі сценарії або запити на сервері. Ці атаки можуть бути використані для отримання доступу до конфіденційної інформації, яка зберігається в базах даних, таких як імена користувачів, паролі або інші чутливі дані. Шпигунські програми - це тип шкідливого програмного забезпечення, яке встановлюється на пристрої жертви без її відома з метою збору конфіденційної інформації, такої як активність в Інтернеті, натискання клавіш, паролі або фінансові дані. Це може бути використано для подальшого викрадення інформації та порушення конфіденційності.

Атаки на конфіденційність можуть мати серйозні наслідки як для окремих користувачів, так і для організацій. Витік особистих або фінансових даних може призвести до фінансових втрат, крадіжки особистої ідентичності, а також до порушення конфіденційності на рівні компанії або урядових установ. Для організацій це може включати в себе значну шкоду репутації, юридичні наслідки та фінансові санкції.

Шифрування даних використовується для захисту переданої інформації між користувачем і сервером. Шифрування забезпечує конфіденційність навіть у випадку перехоплення трафіку. Багатофакторна автентифікація є важливим елементом захисту, додаючи додатковий рівень безпеки при доступі до чутливої інформації. Фільтрація спаму та шкідливих листів допомагає запобігти отриманню фішингових листів або інших шкідливих повідомлень. Навчання користувачів щодо важливості конфіденційності даних допомагає розпізнавати фішинг та інші загрози. Регулярне оновлення програмного забезпечення забезпечує закриття вразливостей, які можуть бути використані для атак. Захист від шпигунських програм включає використання антивірусного програмного забезпечення для виявлення та видалення шпигунських програм.

1.3.3 Атаки на цілісність

Атаки на цілісність спрямовані на порушення правильності, точності та повноти даних. Цей тип атак має на меті змінити або пошкодити інформацію таким чином, щоб її не можна було вірно інтерпретувати або використати. Цілісність є однією з основних складових інформаційної безпеки, і атаки на цілісність можуть мати серйозні наслідки, оскільки вони впливають на достовірність даних, що використовуються для прийняття рішень, фінансових операцій або управління системами.

Однією з основних атак на цілісність є маніпуляція даними, де зловмисники змінюють інформацію або її частину з метою її вигоди. Це може включати зміни в фінансових звітах, маніпулювання транзакціями, фальсифікацію результатів голосування або зміну даних у базах даних. Такі зміни можуть бути як прихованими, так і явними, що ускладнює виявлення атак і може призвести до значних негативних наслідків, таких як неправомірне використання ресурсів або шкода репутації організації.

Ще однією технікою, яка використовується для порушення цілісності даних, є ін'єкція SQL. В цьому випадку зловмисник вводить шкідливі SQL-запити в поля для введення даних на веб-сайті або в додатку. Це дозволяє йому маніпулювати базою даних, видаляти або змінювати дані, що може серйозно порушити цілісність інформації в організації. Наприклад, зловмисник може змінити кількість на рахунках, змінити ціни або навіть вилучити з бази даних чутливу інформацію.

Атаки на зміну даних під час їхнього транспортування також можуть порушувати цілісність. В таких випадках зловмисники можуть здійснювати атаки MITM [28], де вони перехоплюють комунікацію між двома сторонами і змінюють передані дані. Це може включати зміну змісту повідомлень або переспрямування їх у невірне місце. Такі атаки є особливо небезпечними, коли передаються чутливі або критично важливі дані, які можуть бути змінені без відома відправника чи отримувача.

Додатково до цього існують атаки на системи резервного копіювання, де зловмисники намагаються змінити або знищити резервні копії важливих даних. Це робить їх відновлення неможливим або створює ризики для відновлення даних після атаки або катастрофи.

Методи захисту від атак на цілісність включають використання криптографії для забезпечення непідробності даних, таких як хеш-функції та цифрові підписи, які дозволяють перевірити, чи не були змінені дані. Використання журналів змін та систем контролю доступу дозволяє відстежувати зміни, що були внесені в систему, і, у разі необхідності, швидко відновлювати оригінальні дані. Важливим методом є також регулярне оновлення програмного забезпечення та систем, оскільки багато атак на цілісність базуються на вразливостях, які можна запобігти через своєчасні оновлення.

Атаки на цілісність можуть завдати значної шкоди, адже навіть незначні зміни в даних можуть призвести до великих фінансових або репутаційних втрат. Тому важливо реалізувати комплексні заходи безпеки для забезпечення цілісності інформації в усіх системах і процесах.

1.4 Висновки до розділу 1

В першому розділі було розглянуто важливість симуляційних середовищ для навчання в галузі кібербезпеки, що дозволяють ефективно моделювати різноманітні сценарії атак і відпрацьовувати методи захисту. Описано використання гіпервізорів типу 1 для створення симуляційних середовищ. Показано їх можливості щодо забезпечення високої продуктивності, безпеки та ефективного використання ресурсів для моделювання реалістичних мережевих інфраструктур. Розглянуто типи атак, їхні методи виявлення та запобігання, що є важливою складовою навчання з кібербезпеки. Проведено огляд існуючих комерційних платформ, таких як Check Point Cyber Range, Cyberbit Range, RangeForce, IBM X-Force Cyber Range, Cisco Cyber Range та інших, які використовуються як симуляційні середовища. Показано їхню роль у підготовці фахівців для протидії реальним кіберзагрозам.

РОЗДІЛ 2 ЕЛЕМЕНТИ СИМУЛЯЦІЙНОГО СЕРЕДОВИЩА

2.1 Схема симуляційного середовища

Використання симуляційного середовища для навчання з кібербезпеки та дослідження кіберзагроз і методів захисту є важливим інструментом для підготовки фахівців та вдосконалення стратегій захисту від сучасних кіберзагроз. Такі середовища дозволяють моделювати реальні умови кібернападів, відпрацьовувати відповідні реакції на інциденти та тестувати різноманітні методи захисту без ризику для реальних систем і даних.

Симуляційні середовища створюють можливість для безпечного тестування нових технологій, стратегій захисту та засобів моніторингу. Вони дозволяють вивчати широкий спектр атак, таких як DDoS, фішинг, SQL-ін'єкції, а також тренувати навички виявлення, аналізу та нейтралізації загроз. Кібернапади можуть бути відтворені в симульованому середовищі з реалістичними параметрами трафіку та поведінкою зловмисників, що забезпечує глибше розуміння їхніх механізмів та наслідків.

Завдяки таким середовищам фахівці можуть отримати практичний досвід у використанні реальних інструментів безпеки, таких як системи IDS/IPS, брандмауери, системи для моніторингу мереж, а також засоби для боротьби з конкретними типами атак. Вони також допомагають розробляти, тестувати і вдосконалювати стратегії для захисту від кіберзагроз, що особливо важливо у світі, де кіберзагрози стають дедалі складнішими та більш витонченими.

Симуляційні середовища також можуть використовуватись для оцінки готовності організацій до кіберзагроз, тренування персоналу в реалістичних умовах та удосконалення процедур реагування на інциденти. Це дозволяє визначити прогалини в знаннях і навичках учасників, а також оптимізувати процедури безпеки, щоб краще відповідати на майбутні кіберзагрози.

На рисунку 2.1 показано схему симуляційного середовища на основі гіпервізора XEN.

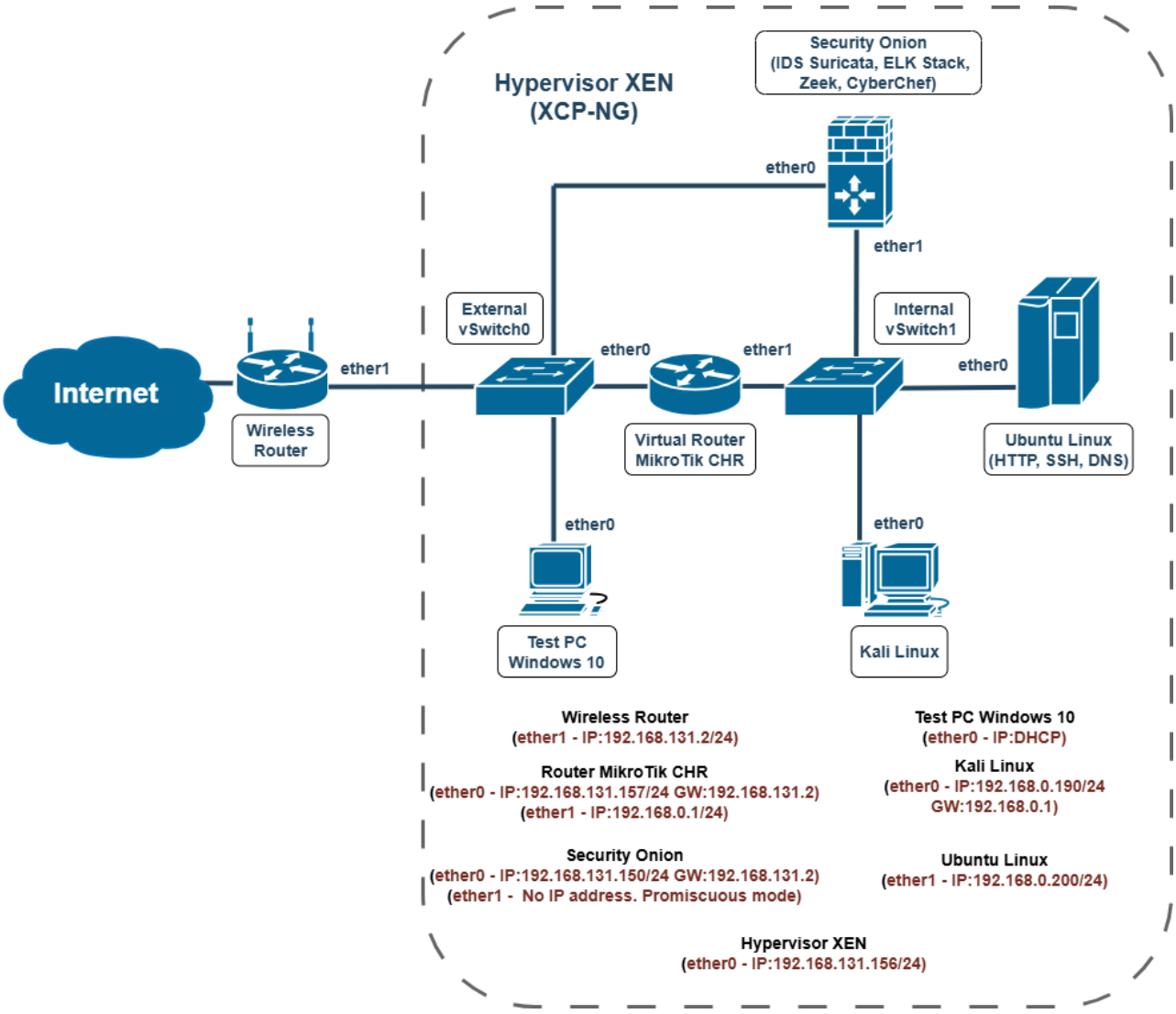

Рисунок 2.1 – Архітектура симуляційного середовища

На схемі представлено архітектуру симуляційного середовища, яке базується на гіпервізорі XEN (XCP-NG) для моделювання та дослідження кіберзагроз. Це середовище використовується для виявлення, аналізу та запобігання кіберзагрозам, а також для навчання з кібербезпеки.

Гіпервізор XEN є гіпервізором типу 1 (bare-metal), який керує всіма віртуальними машинами та ресурсами в системі. Він забезпечує ізоляцію та управління апаратними ресурсами для створення симуляційного середовища.

Wireless Router виконує функцію підключення симуляційного середовища до Інтернету. Має IP-адресу 192.168.131.2/24 на інтерфейсі ether1. Відповідає за надання доступу до глобальної мережі через зовнішній шлюз.

Virtual Router MikroTik CHR – це віртуальний маршрутизатор, який забезпечує управління внутрішньою мережею симуляційного середовища. Має два мережевих інтерфейси:

- ether0, який відповідає за підключення до зовнішньої мережі з IP-адресою 192.168.131.157/24 і шлюзом 192.168.131.2;
- ether1, який відповідає за підключення внутрішньої мережа з IP-адресою 192.168.0.1/24.

Security Onion- це платформа для моніторингу, аналізу та реагування на кіберзагрози. Вона включає IDS Suricata, ELK Stack, Zeek і CyberChef. Має такі інтерфейси:

- ether0 - підключення до зовнішньої мережі з IP-адресою 192.168.131.150/24 і шлюзом 192.168.131.2;
- ether1 - немає IP-адреси, працює в режимі promiscuous для перехоплення трафіку.

Kali Linux: Інструмент для тестування на проникнення та моделювання атак. Віртуальна машина підключена до внутрішньої мережі через ether0 з IP-адресою 192.168.0.190/24 та шлюзом 192.168.0.1.

Ubuntu Linux це сервер, який забезпечує сервіси HTTP, SSH і DNS для тестування. Віртуальна машина підключена до внутрішньої мережі через ether0 з IP-адресою 192.168.0.200/24.

Test PC Windows 10 – це робоча станція для керування симуляційним середовищем. IP-адресу отримує через DHCP. Використовується для тестування доступності сервісів та аналізу мережевих атак.

Мережеві комутатори: External vSwitch0 та Internal vSwitch1 забезпечують зв'язок між віртуальним маршрутизатором MikroTik CHR, Security Onion, Wireless Router та підключенням внутрішніх компонентів симуляційного середовища, включаючи Ubuntu Linux, Kali Linux і Test PC Windows 10.

Інтернет-з'єднання здійснюється через Wireless Router і Virtual Router MikroTik CHR, які забезпечують доступність глобальної мережі для симуляційного середовища.

Security Onion аналізує трафік між усіма компонентами та виявляє можливі атаки. Інтерфейс у режимі promiscuous дозволяє перехоплювати весь трафік внутрішньої та зовнішньої мережі.

Kali Linux виконує роль інструменту для моделювання атак, таких як DDoS, SQL-ін'єкції або фішинг, спрямованих на Ubuntu Linux чи інші системи.

Ubuntu Linux забезпечує тестові сервіси, які є об’єктами для атак з боку Kali Linux або зовнішнього трафіку.

Test PC Windows 10 використовується для керування симуляційним середовищем та для перевірки доступності ресурсів, тестування мережевих з'єднань і аналізу роботи безпекових рішень.

Основні можливості схеми:

- моделювання реальних атак та виявлення кіберзагроз;
- перевірка ефективності захисних систем, таких як IDS Suricata, та аналіз загроз за допомогою ELK Stack і Zeek;
- навчання та тестування фахівців з кібербезпеки у реалістичних умовах;
- моделювання мережевих інфраструктур та перевірка їх стійкості до атак;
- можливість масштабування для додавання нових компонентів, тестування додаткових сценаріїв та інтеграції з іншими системами.

Загальна архітектура симуляційного середовища забезпечує комплексну інфраструктуру для дослідження різних типів кіберзагроз, моделювання атак та відпрацювання методів їх нейтралізації. Ця архітектура створює можливості для відтворення складних сценаріїв атак, таких як DDoS, SQL-ін'єкції або атаки типу MITM, одночасно надаючи безпечне середовище для тестування стратегій реагування та захисту. Розширюваність системи дозволяє додавати нові компоненти або модифікувати існуючі, забезпечуючи універсальність і адаптивність середовища до змінюваних кіберзагроз.

2.2 Складові симуляційного тестового середовища

2.2.1 Платформа віртуалізації XCP-NG

Платформа віртуалізації XCP-NG працює на базі гіпервізора типу 1 XEN [29]. Вона встановлюється безпосередньо на апаратне забезпечення і забезпечує високу продуктивність, безпеку та ефективне управління ресурсами для створення та роботи віртуальних машин. XEN є однією з найбільш відомих платформ з відкритим кодом, яка використовується як в корпоративних середовищах, так і в симуляційних навчальних лабораторіях. Гіпервізор XEN дозволяє створювати ізольовані віртуальні машини, які можуть працювати з різними операційними системами, такими як Linux, Windows чи BSD, на одному фізичному сервері. Завдяки безпосередньому доступу до апаратних ресурсів, таких як CPU, пам'ять і диски, XEN забезпечує мінімальні затримки та максимальну продуктивність віртуальних машин.

Гіпервізор XEN використовує апаратну підтримку віртуалізації, надану сучасними процесорами з технологіями, такими як Intel VT-x і AMD-V. Ці технології дозволяють гіпервізору розділяти апаратні ресурси, такі як процесор, пам'ять, мережеві інтерфейси та диски, між кількома віртуальними машинами, забезпечуючи їхню повну ізоляцію. Завдяки цьому кожна віртуальна машина отримує доступ до виділених їй ресурсів так, ніби вона працює на окремому фізичному сервері. Апаратна віртуалізація в XEN дозволяє одночасно використовувати паравіртуалізацію та повну віртуалізацію. Паравіртуалізація є ефективним підходом, який використовує модифіковані операційні системи для більш ефективного управління ресурсами, тоді як повна віртуалізація дозволяє запускати немодифіковані операційні системи безпосередньо на гіпервізорі. Це забезпечує високу гнучкість XEN у підтримці різних сценаріїв використання.

Архітектура XEN забезпечує ізоляцію віртуальних машин одна від одної, що робить систему більш захищеною від потенційних загроз. Платформа підтримує велику кількість віртуальних машин, дозволяючи створювати складні симуляційні середовища або корпоративні серверні ферми. Завдяки підтримці як паравіртуалізації, так і повної віртуалізації, XEN може запускати оптимізовані для віртуального середовища операційні системи, а також стандартні ОС без модифікацій.

У галузі кібербезпеки XEN використовується для створення симуляційних лабораторій, які дозволяють моделювати реалістичні сценарії кіберзагроз. Він дозволяє розгортати віртуальні машини для серверів, клієнтських систем, мережевих пристроїв і систем моніторингу, таких як Security Onion. Завдяки цьому забезпечується можливість розгортання багатошарових мережевих середовищ із різними рівнями доступу, моделювання складних атак, таких як DDoS, MITM, SQL-ін'єкції, тестування стратегій захисту, а також відпрацювання навичок реагування на кіберінциденти.

Гіпервізор XEN є ключовим компонентом для побудови ефективного симуляційного середовища, забезпечуючи гнучкість, надійність та безпеку, необхідні для дослідження кіберзагроз і навчання фахівців із кібербезпеки.

На рисунку 2.2 представлено інтерфейс управління гіпервізором XEN.

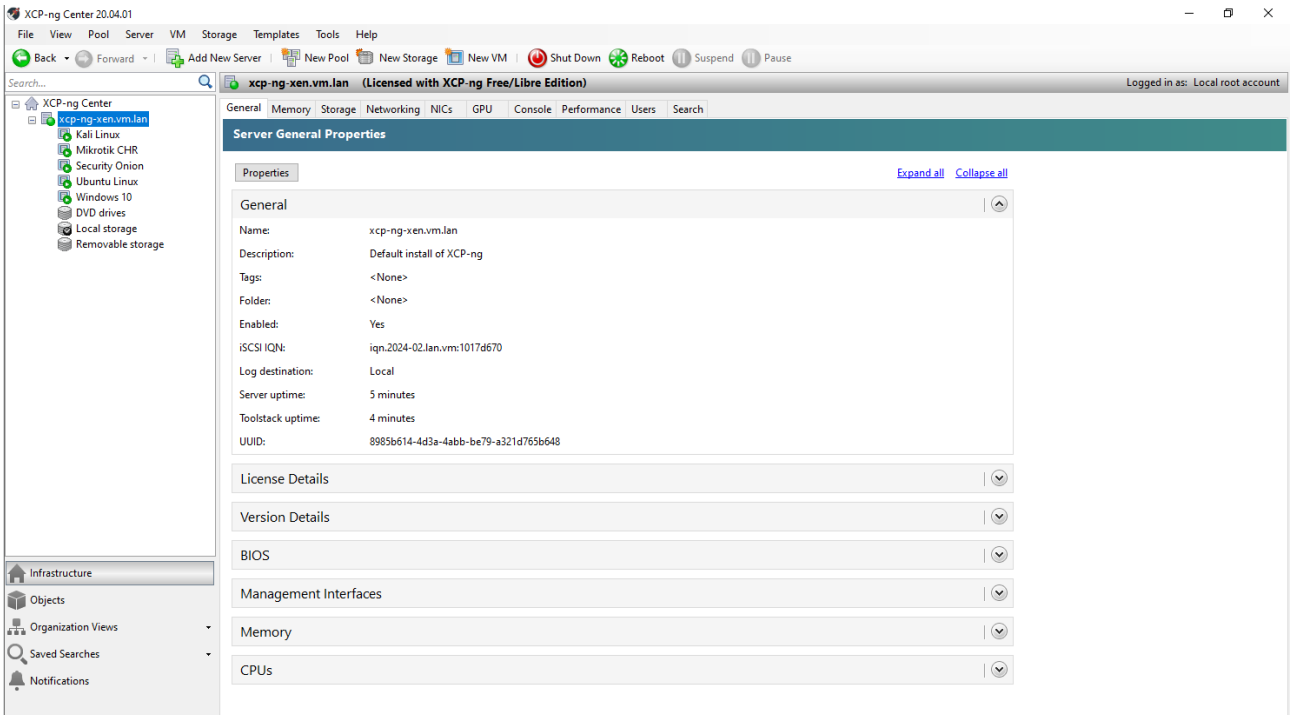

Рисунок 2.2 – Центр керування платформою віртуалізації XCP-NG основі XEN

XCP-ng Center забезпечує зручний графічний інтерфейс для управління інфраструктурою віртуалізації, що робить його ефективним інструментом для роботи в симуляційних середовищах кібербезпеки.

2.2.2 Віртуальний маршрутизатор MikroTik CHR

Маршрутизатор MikroTik CHR є віртуалізованою версією маршрутизатора від MikroTik, яка працює на різних гіпервізорах, таких як XCP-ng, VMware, Hyper-V або інших платформах віртуалізації [30]. Це рішення забезпечує повний функціонал фізичних маршрутизаторів MikroTik, дозволяючи використовувати його в віртуальних середовищах для побудови ефективної мережевої інфраструктури. MikroTik CHR використовується для маршрутизації, управління потоками трафіку та забезпечення захисту в мережах, що робить його важливим компонентом симуляційних середовищ кібербезпеки. Він підтримує такі можливості, як маршрутизація IP-трафіку, перетворення адрес (NAT), використання брандмауера для захисту мережі, управління якістю сервісу (QoS), налаштування VPN для захищеного доступу, а також моніторинг і аналіз мережевого трафіку.

У представленому симуляційному середовищі MikroTik CHR виконує ключову роль маршрутизатора, що з'єднує зовнішню мережу Інтернет із внутрішньою інфраструктурою. Цей маршрутизатор виконує функції розподілу трафіку між внутрішньою мережею та Інтернетом, використовуючи NAT для захисту приватних IP-адрес та забезпечення безпечного виходу в глобальну мережу.

MikroTik CHR є потужним інструментом для побудови складних симуляційних середовищ, що дозволяє моделювати реалістичні сценарії кіберзагроз, тестувати ефективність захисних систем та розробляти нові стратегії реагування. Завдяки своїй гнучкості та широкій функціональності він забезпечує високий рівень продуктивності у віртуальному середовищі.

На рисунку 2.3 показано інтерфейс WinBox, клієнтської програми для управління маршрутизаторами MikroTik, зокрема віртуальним маршрутизатором MikroTik CHR.

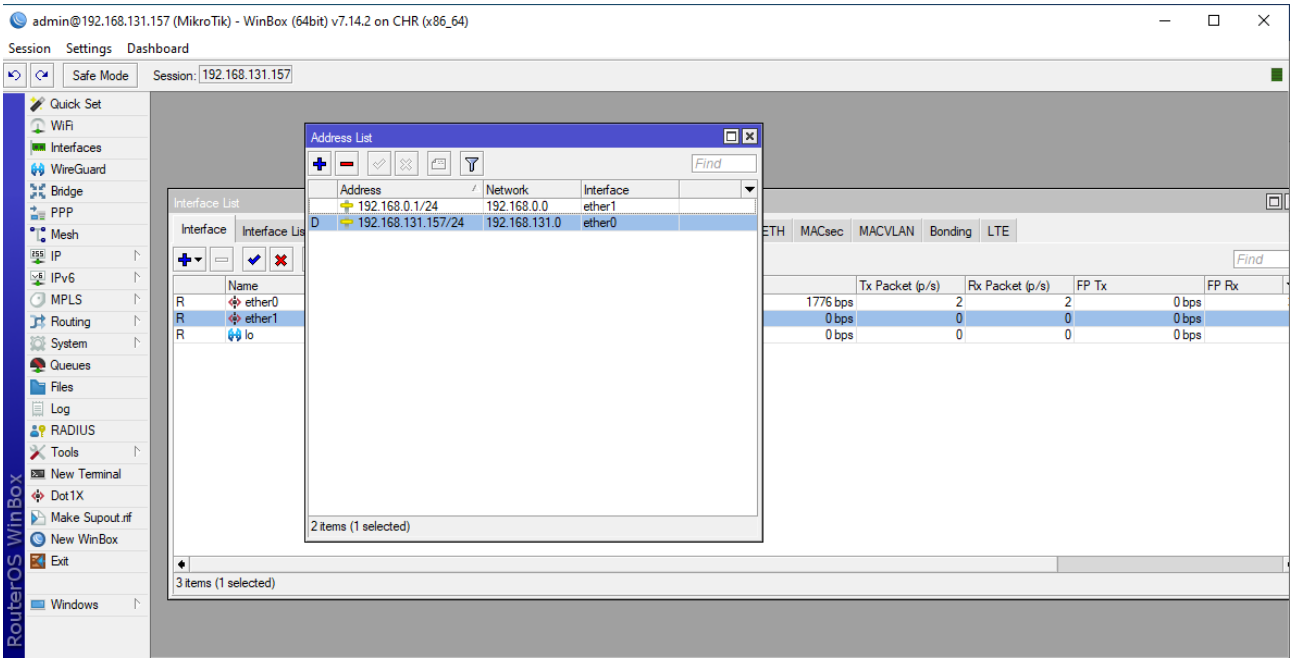

Рисунок 2.3 – Інтерфейс WinBox програми управління віртуальним маршрутизатором MikroTik CHR

У цьому випадку відображено налаштування мережевих інтерфейсів та IP-адрес, які використовуються в симуляційному середовищі.

MikroTik CHR використовується як центральний маршрутизатор для управління трафіком між внутрішньою мережею (LAN) і зовнішньою мережею (WAN). Інтерфейс ether0 забезпечує з'єднання з Інтернетом через Wireless Router, тоді як ether1 забезпечує зв'язок із внутрішніми компонентами симуляційного середовища, такими як Security Onion, Kali Linux і Ubuntu Linux.

Маршрутизатор виконує функції NAT для трансляції адрес між внутрішньою та зовнішньою мережею, а також забезпечує маршрутизацію трафіку.

2.2.3 Операційна системи Ubuntu Linux

Операційна система Ubuntu Linux є однією з найпопулярніших і широко використовуваних дистрибутивів Linux, яка базується на Debian [31]. Її ключовими особливостями є зручність використання, стабільність, висока продуктивність і багатофункціональність. Ubuntu активно використовується для

серверів, робочих станцій, розробки програмного забезпечення, а також у симуляційних середовищах, включаючи навчання з кібербезпеки.

Ubuntu Linux підтримує широкий спектр інструментів і служб, які забезпечують її універсальність у різних сценаріях. Вона надає стабільне серверне середовище для хостингу веб-додатків, баз даних, поштових серверів, а також інших критично важливих служб. У кібербезпекових симуляційних середовищах Ubuntu Linux зазвичай використовується для розгортання серверів і служб, які слугують об'єктами для тестування атак або дослідження вразливостей.

У контексті симуляційного середовища, Ubuntu Linux може бути налаштована для надання таких послуг, як HTTP, SSH та DNS. Наприклад, HTTP-сервер на основі Apache чи Nginx забезпечує хостинг веб-ресурсів для моделювання атак, таких як SQL-ін'єкції чи XSS (Cross-Site Scripting). Сервіс SSH використовується для безпечного віддаленого доступу до системи, а DNS-сервер може бути використаний для моделювання атак на рівні доменних імен, таких як DNS spoofing чи DNS amplification. Також дані сервіси можуть бути використані для моделювання DDoS атак або тестування механізмів перевірки сигнатур в системі IDS.

Ubuntu Linux є надійним інструментом у симуляційних середовищах для моделювання атак, відпрацювання методів захисту, а також тестування надійності інфраструктури в умовах реальних кіберзагроз. Вона забезпечує стабільність, продуктивність і широкий спектр можливостей для навчання та досліджень у сфері кібербезпеки.

На рисунку 2.4 представлено список активних служб операційної системи Ubuntu Server, отриманий за допомогою команди `service --status-all | grep +`.

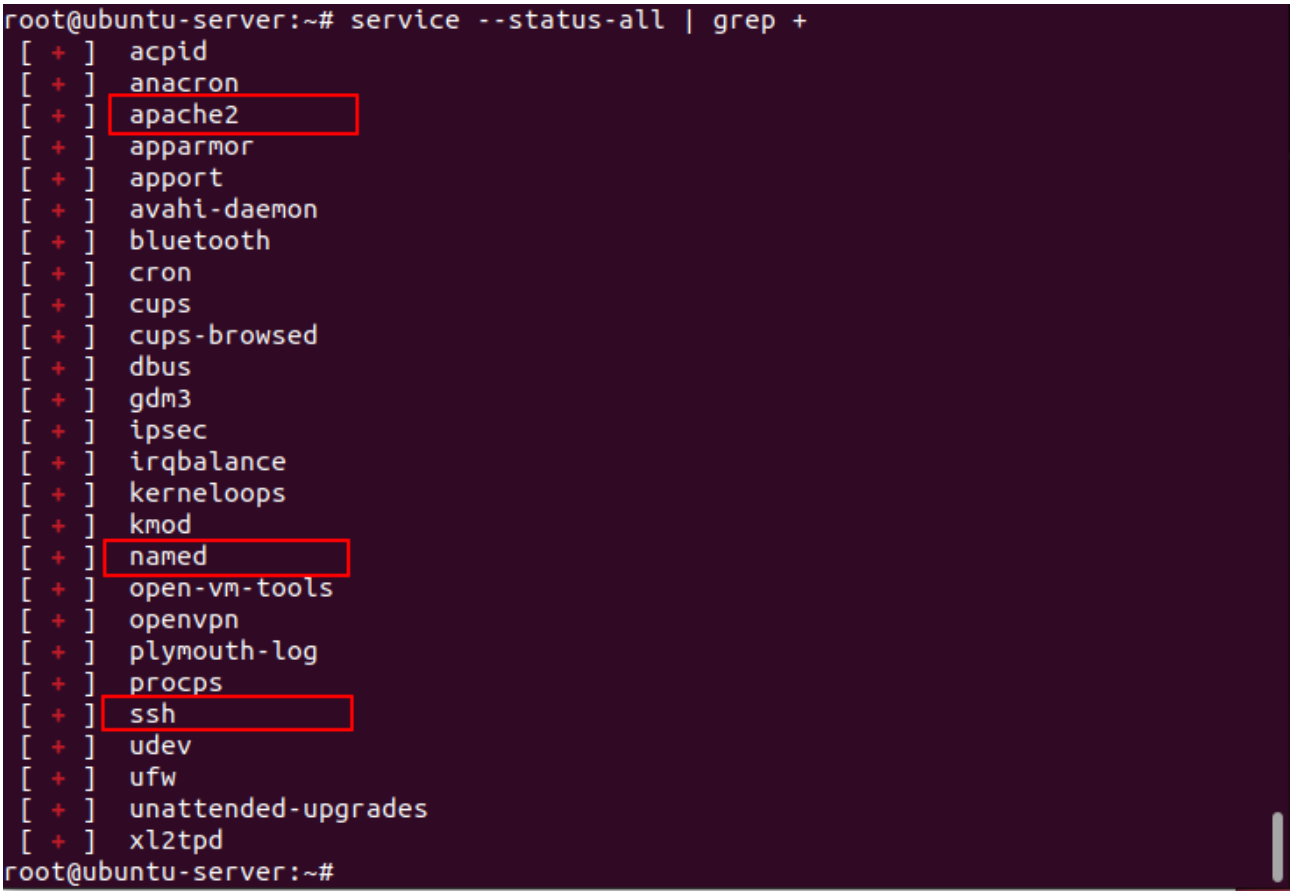

Рисунок 2.4 – Список активних сервісів в Ubuntu Linux

Ця команда відображає всі запущені служби, які мають позначення `[ + ]`, що означає їхній активний стан.

Служба веб-сервера Apache є важливим компонентом у симуляційних середовищах для моделювання атак, таких як SQL-ін'єкції чи атаки на веб-додатки. У цьому випадку Apache2 працює, забезпечуючи доступність HTTP-сервісів. Служба DNS-сервера є частиною програмного забезпечення BIND. Вона використовується для розв’язування доменних імен у відповідні IP-адреси. У симуляційних середовищах DNS-сервери можуть бути об'єктом для моделювання атак, таких як DNS Spoofing або DNS Amplification. Служба OpenSSH забезпечує захищений доступ до сервера через протокол SSH. Вона використовується для віддаленого адміністрування та управління системою. У симуляційних середовищах SSH може бути об'єктом для моделювання атак на авторизацію (brute-force) або експлуатації вразливостей у протоколі.

Цей сервер, базуючись на Ubuntu, виконує кілька функцій у симуляційному середовищі. Служба Apache2 забезпечує доступність веб-сервісів для тестування

атак на веб-додатки. DNS-сервер (named) відповідає за розв'язування доменних імен, що може бути об'єктом для аналізу кіберзагроз на мережевому рівні. Служба SSH забезпечує безпечний доступ для адміністраторів, одночасно даючи можливість тестувати методи захисту від атак на віддалений доступ. Завдяки цим активним службам сервер може ефективно виконувати роль тестового середовища для моделювання загроз.

На рисунку 2.5 наведено результат виконання команди ip addr, яка відображає налаштування мережевих інтерфейсів на сервері Ubuntu.

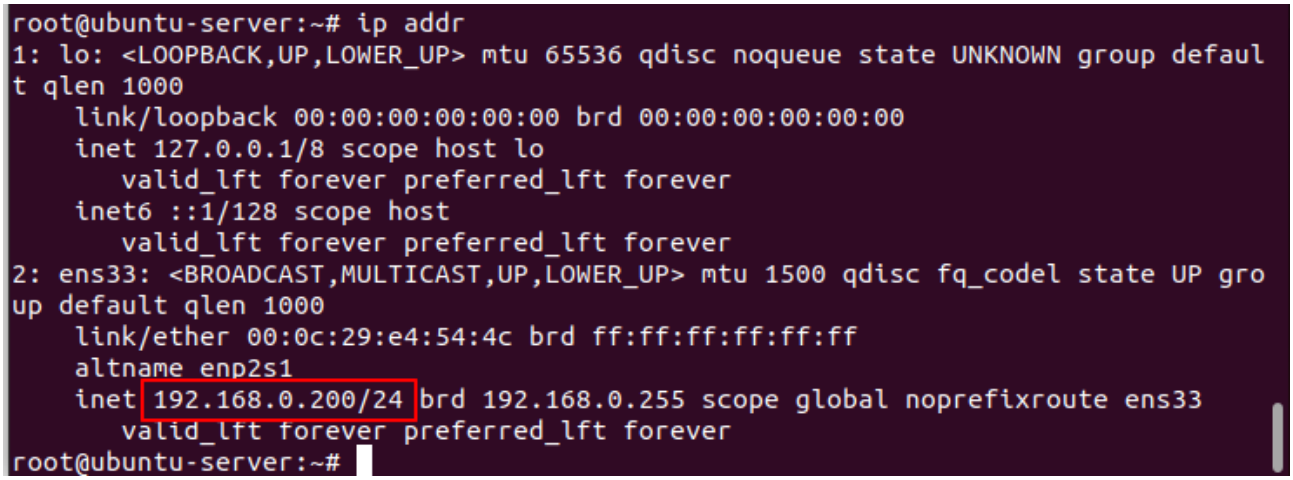

Рисунок 2.5 – Налаштування мережевих інтерфейсів в Ubuntu Linux

Мережевий інтерфейс ens33 з IP-адресою 192.168.0.200/24 є частиною внутрішньої мережі симуляційного середовища, до якої підключені інші компоненти, такі як Kali Linux, Security Onion та маршрутизатор MikroTik CHR. Ця адреса використовується для доступу до серверу Ubuntu, на якому розгорнуті служби, такі як HTTP, DNS та SSH.

Сервер з цією конфігурацією буде об'єктом для тестування атак у симуляційному середовищі. Наприклад, атакуюча система на Kali Linux може виконувати сканування мережі для виявлення активних IP-адрес, спроби доступу через SSH або моделювати атаки на HTTP-сервер, запущений на Ubuntu. Конфігурація інтерфейсу відповідає вимогам симуляційного середовища, забезпечуючи підключення до внутрішньої мережі та можливість для інших компонентів взаємодіяти із сервером.

2.2.4 Операційна система Kali Linux

Kali Linux є спеціалізованим дистрибутивом операційної системи Linux, заснованим на Debian, який розроблений для тестування на проникнення, аналізу вразливостей, цифрової криміналістики та забезпечення інформаційної безпеки [32]. Ця операційна система широко використовується фахівцями з кібербезпеки, дослідниками і в навчальних середовищах для моделювання атак, аналізу захисних механізмів та перевірки стійкості систем до сучасних кіберзагроз. Kali Linux включає великий набір інструментів, які дозволяють виконувати завдання, пов'язані з тестуванням безпеки, аналізом мережі, пошуком вразливостей, а також моделюванням складних атак, таких як DDoS, SQL-ін'єкції, ARP-spoofing і багато інших. Система підтримує широкий спектр завдань, включаючи аудит безпеки веб-додатків, перевірку безпеки бездротових мереж, аналіз мережевого трафіку та виявлення вразливих точок у мережевих протоколах і системах.

У симуляційних середовищах Kali Linux забезпечує платформу для моделювання реалістичних атак, перевірки ефективності захисних систем і тестування відповідності безпекових стратегій сучасним загрозам. Вона використовується для атак на сервери й мережі, перевірки механізмів реагування на інциденти та моделювання сценаріїв у реальних умовах. Наприклад, Kali Linux може бути налаштована для запуску атак на веб-сервери, що працюють на Ubuntu Linux, або для перевірки стійкості IDS/IPS-систем до аномальної активності в мережі. Операційна система інтегрує всі необхідні інструменти, які дозволяють виконувати ці завдання з високою точністю та ефективністю.

Kali Linux підтримує різні середовища для роботи, включаючи графічний інтерфейс і командний рядок, що дозволяє легко адаптувати її для різних сценаріїв використання. Вона може бути встановлена як на фізичних комп'ютерах, так і у віртуальних або хмарних середовищах, що забезпечує її гнучкість і масштабованість. Постійні оновлення системи і додавання нових інструментів забезпечують актуальність її використання для сучасних завдань кібербезпеки. Завдяки своїй функціональності, гнучкості та широкій підтримці безпекових інструментів Kali Linux залишається одним із найпотужніших

інструментів для тестування безпеки, навчання і дослідження в галузі кібербезпеки.

На рисунку 2.6 показано мережеві налаштування Kali Linux.

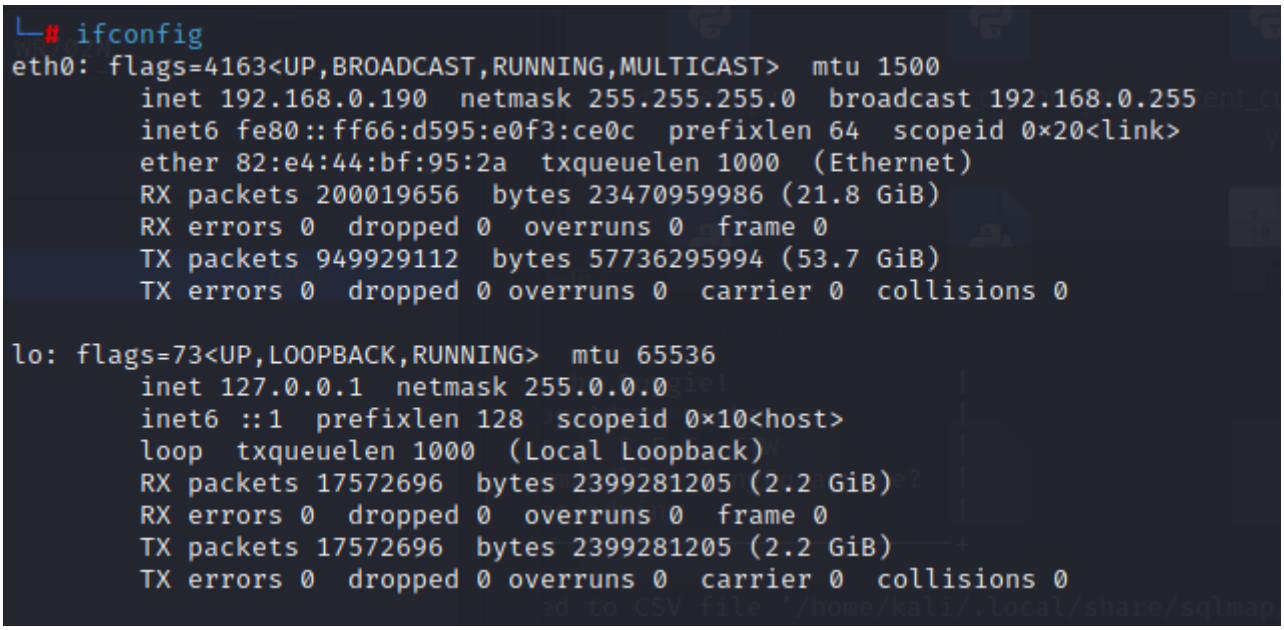

Рисунок 2.6 – Мережеві налаштування Kali Linux

2.2.5 Платформа Security Onion

Security Onion - це безкоштовна та відкрита платформа для моніторингу, виявлення та реагування на кіберзагрози (MDR). Вона поєднує в собі широкий спектр інструментів для аналізу мережевого трафіку, виявлення аномалій, збору журналів і розслідування інцидентів. Security Onion є потужним рішенням для організацій, які прагнуть посилити свою безпеку та забезпечити оперативне реагування на кіберзагрози [33].

Платформа інтегрує популярні інструменти, такі як IDS Suricata, Zeek, Elastic Stack (ELK: Elasticsearch, Logstash, Kibana), CyberChef та інші. Suricata забезпечує виявлення атак на основі аналізу сигнатур, Zeek займається аналізом і генерацією логів мережевого трафіку, а Elastic Stack дозволяє зберігати, обробляти і візуалізувати дані для проведення розслідувань. CyberChef є універсальним інструментом для аналізу даних та розшифрування інформації.

Security Onion підтримує кілька ключових функцій, включаючи IDS, аналіз журналів, моніторинг кінцевих точок, збір даних із мережі в режимі реального часу та проведення розслідувань після інцидентів. Ці функції забезпечують повний цикл виявлення та реагування на загрози. Платформа дозволяє створювати централізовану систему моніторингу, яка об'єднує мережеві, серверні та кінцеві точки в єдину захисну інфраструктуру.

У симуляційних середовищах Security Onion використовується для аналізу кіберзагроз і відпрацювання методів захисту. Наприклад, у симуляційній мережі вона може моніторити трафік між компонентами, такими як Kali Linux і Ubuntu Linux, виявляючи аномальну активність або атаки, такі як ARP-spoofing, DDoS чи SQL-ін'єкції. Security Onion дозволяє не лише виявляти загрози, а й досліджувати їх, використовуючи Kibana для візуалізації даних або Suricata для детального аналізу пакетів. Вона також надає інструменти для кореляції даних і автоматизації виявлення загроз.

Security Onion легко інтегрується в різні середовища завдяки гнучкості налаштувань і підтримці сучасних стандартів мережевого моніторингу та виявлення вторгнень. Вона може бути розгорнута як у фізичних, так і у віртуальних середовищах, забезпечуючи адаптивність до різних інфраструктур. Завдяки своїй функціональності та доступності Security Onion стала важливим інструментом у сфері кібербезпеки, який використовується для підготовки фахівців, розслідування інцидентів і підвищення загального рівня безпеки організацій.

На рисунку 2.7 показано налаштування мережевих інтерфейсів і таблицю маршрутизації системи Security Onion.

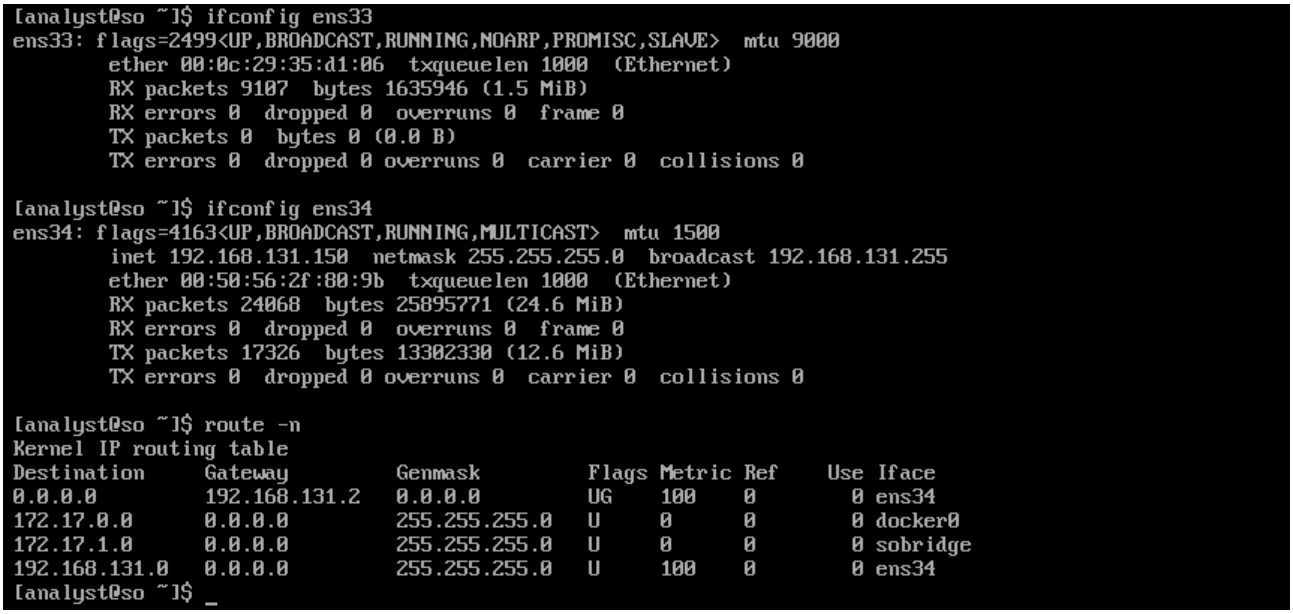

Рисунок 2.7 – Мережеві налаштування Security Onion

Інтерфейс ens33 знаходиться в активному стані (UP) і працює в режимі promiscuous, що дозволяє перехоплювати весь мережевий трафік. Обсяг отриманих даних становить 1635946 байтів, а передача даних відсутня. Це свідчить про його використання для моніторингу мережевого трафіку.

Інтерфейс ens34 також знаходиться в активному стані і має IP-адресу 192.168.131.150 з маскою підмережі 255.255.255.0. Це інтерфейс керування.

У таблиці маршрутизації представлено шлюз за замовчуванням 192.168.131.2, який використовується для маршрутизації всього вихідного трафіку через інтерфейс ens34. Локальна мережа 192.168.131.0/24 також використовує цей інтерфейс для комунікацій. Крім того, налаштовані маршрути для віртуальних мереж Docker (172.17.0.0) і sobridge (172.17.1.0), які призначені для ізольованих контейнерів.

Конфігурація інтерфейсів демонструє, що ens33 виконує функції моніторингу, характерні для систем виявлення загроз, таких як Suricata і Zeek, які аналізують мережевий трафік. Інтерфейс ens34, у свою чергу, виконує роль основного інтерфейсу для обміну даними в мережі та маршрутизації через шлюз. Таке налаштування забезпечує ефективне виявлення і аналіз кіберзагроз, а також підтримку мережевих комунікацій у симуляційному середовищі.

2.3 Тестування компонентів симуляційного середовища

Тестування мережі та компонентів симуляційного середовища є ключовим етапом перевірки його працездатності, ефективності взаємодії між компонентами та відповідності поставленим завданням. Цей процес включає оцінку роботи мережевої інфраструктури, функціональності серверів, налаштувань маршрутизаторів.

Першочерговим етапом є перевірка мережевої інфраструктури. Використовуючи інструменти, такі як ping та traceroute, тестується зв'язок між компонентами симуляційного середовища, такими як MikroTik CHR, Ubuntu Linux, Kali Linux та Security Onion. Перевіряється доступність усіх вузлів, правильність маршрутизації і стабільність з'єднання. Наступним етапом є перевірка серверів і служб, розгорнутих на Ubuntu Linux. Це включає тестування HTTP-сервісе, DNS-сервера та SSH-доступу.

На рисунку 2.8 показано результати тестування симуляційного середовища, де в розділі "Network Tree" відображається структура мережі та стан її компонентів.

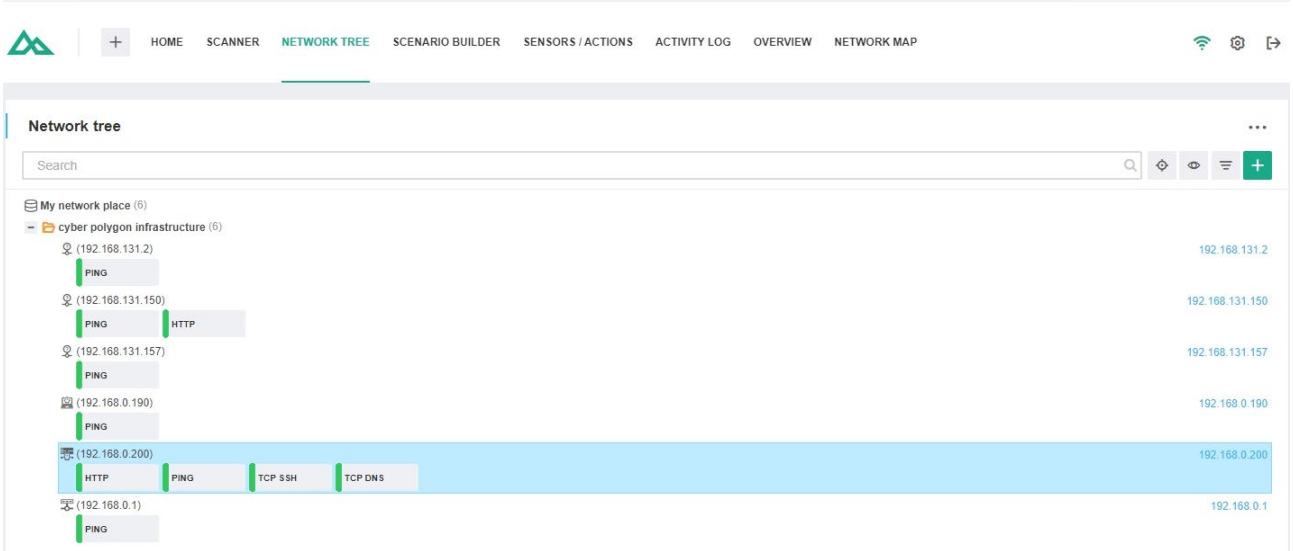

Рисунок 2.6 – Тестування доступності хостів та сервісів лабораторного середовища

Кожен вузол перевірений за допомогою команд, таких як ping, які забезпечують тестування доступності. Сервіси HTTP, SSH та DNS вказують на

те, що вузли готові до виконання різноманітних функцій у симуляційному середовищі, таких як моделювання веб-атак, атак на віддалений доступ або тестування налаштувань DNS-сервера.

Доступність усіх зазначених сервісів свідчить про стабільність і функціональність мережевої інфраструктури симуляційного середовища. Це дозволяє використовувати середовище для моделювання кібератак, аналізу захисних механізмів і навчання фахівців у сфері кібербезпеки. Наявність працюючих сервісів також підтверджує коректну конфігурацію мережі та її компонентів, що є основою для проведення подальших тестувань і досліджень.

2.4 Висновки до розділу 2

В другому розділі було розглянуто архітектуру та основні компоненти симуляційного середовища для навчання з кібербезпеки і дослідження кіберзагроз. Описано структуру симуляційного середовища, яке базується на гіпервізорі XEN (XCP-NG), що забезпечує ізоляцію і управління апаратними ресурсами для роботи віртуальних машин. Проаналізовано роль ключових компонентів середовища, таких як маршрутизатор MikroTik CHR, сервери Ubuntu Linux та Kali Linux, а також платформи моніторингу Security Onion, яка поєднує інструменти для аналізу трафіку, виявлення та розслідування кіберзагроз.

Описано функціональність кожного з компонентів та їх роль у моделюванні реальних кіберзагроз і тестуванні захисних систем. Розглянуто переваги використання гіпервізора XEN для створення масштабованого, безпечного і продуктивного симуляційного середовища. Окремо акцентовано увагу на можливостях Security Onion як платформи для аналізу мережевого трафіку та виявлення загроз за допомогою інструментів Suricata, Zeek та ELK Stack.

Проведено тестування компонентів симуляційного середовища, включаючи перевірку доступності серверів та працездатності сервісів, таких як HTTP, SSH та DNS. Результати тестування підтвердили коректність налаштувань і стабільність роботи середовища, що забезпечує можливість його використання

для моделювання реалістичних атак, навчання фахівців та дослідження ефективності стратегій захисту.

Результатом другого розділу є створення повноцінної інфраструктуру, яка дозволяє досліджувати різні типи кіберзагроз, аналізувати їх наслідки та відпрацьовувати методи нейтралізації у безпечних і контрольованих умовах.

РОЗДІЛ 3 ТЕСТУВАННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ СИМУЛЯЦІЙНОГО СЕРЕДОВИЩА

3.1 Налаштування та тестування компонентів середовища

Налаштування компонентів та тестування симуляційного середовища є важливим етапом для перевірки його працездатності, ефективності та відповідності поставленим завданням. У контексті навчання з кібербезпеки це дозволяє оцінити, наскільки точно середовище може імітувати реальні сценарії атак, підтримувати аналіз мережевого трафіку та надавати інструменти для виявлення й нейтралізації загроз.

Під час тестування симуляційного середовища було проведено моделювання типових атак, таких як DDoSta атаки на вебдодатки. У процесі тестування оцінювалась здатність компонентів середовища, таких як Security Onion, Ubuntu Linux та Kali Linux, взаємодіяти та реагувати на ці загрози. Security Onion забезпечує аналіз трафіку і виявлення аномалій, використовуючи IDS Suricata і Zeek, тоді як Kibana і Elasticsearch дозволяють візуалізувати результати та досліджувати зібрані дані.

Одним із ключових етапів тестування є перевірка точності виявлення атак системою IDS. Генерувався тестовий трафік з Kali Linux, який містить відомі сигнатури атак, а потім проводилась перевірка, чи були вони успішно виявлені Suricata. Також здійснюється тестування реакції системи на аномальний трафік і спроби проникнення, щоб переконатися, що середовище адекватно реагує і реєструє події.

Після завершення тестування аналізувались журнали подій і результати візуалізації. Це дозволило оцінити, чи коректно працюють всі компоненти і чи відповідає середовище очікуваним параметрам. Таким чином, тестування симуляційного середовища забезпечує його надійність і готовність до використання для навчання, досліджень і відпрацювання практичних навичок у сфері кібербезпеки. Результати тестування дозволяють підтвердити

ефективність системи та забезпечити її здатність імітувати реальні загрози й оцінювати методи їхнього нейтралізування.

Налаштування компонентів Security Onion включає в себе декілька важливих етапів для забезпечення ефективної роботи цієї платформи моніторингу, аналізу та реагування на кіберзагрози. Security Onion інтегрує потужні інструменти, такі як Suricata, Zeek, Elastic Stack, CyberChef і потребує детальної конфігурації для коректного функціонування в симуляційному середовищі.

Спочатку платформа була розгорнута на віртуальній машині з використанням гіпервізора XCP-NG. Security Onion отримала два мережевих інтерфейси: ether0, налаштований для підключення до зовнішньої мережі з IP-адресою 192.168.131.150/24, і ether1, який працює в режимі promiscuous для моніторингу та збору трафіку внутрішньої мережі.

На етапі інсталяції було обрано режим конфігурації, що включає всі компоненти платформи: IDS Suricata, Zeek, Kibana, Elasticsearch, Logstash, CyberChef та інші. Suricata була налаштована для виявлення атак на основі сигнатур та правил. Zeek був конфігурований для генерації логів про активність у мережі, що включає підключення, HTTP-запити, DNS-запити та інші події. Це забезпечує глибокий аналіз мережевого трафіку для виявлення аномальної поведінки або потенційних загроз.

Наступним етапом стало налаштування Elasticsearch для зберігання логів, зібраних Suricata і Zeek, та Kibana для візуалізації цих даних. У Kibana були створені панелі для моніторингу мережевої активності, аналізу виявлених загроз і перегляду статистики атак. Logstash був налаштований для попередньої обробки даних перед їхнім зберіганням в Elasticsearch.

Додатково була встановлена та налаштована Suricata для аналізу трафіку, що перехоплюється інтерфейсом ether1. Suricata забезпечує автоматичне оновлення бази сигнатур для забезпечення актуальності виявлення загроз [34]. Було створено правила для моніторингу трафіку на портах, які використовуються HTTP, SSH, DNS та іншими сервісами, що працюють у симуляційному середовищі.

CyberChef, як частина Security Onion, був налаштований для аналізу даних, таких як журнали атак або мережеві з'єднання. Цей інструмент використовується для декодування та дешифрування інформації, аналізу логів і дослідження інцидентів.

На рисунку 3.1 показано результат виконання команди `sudo so-status`, яка відображає статус всіх контейнерів і сервісів, що працюють у системі Security Onion.

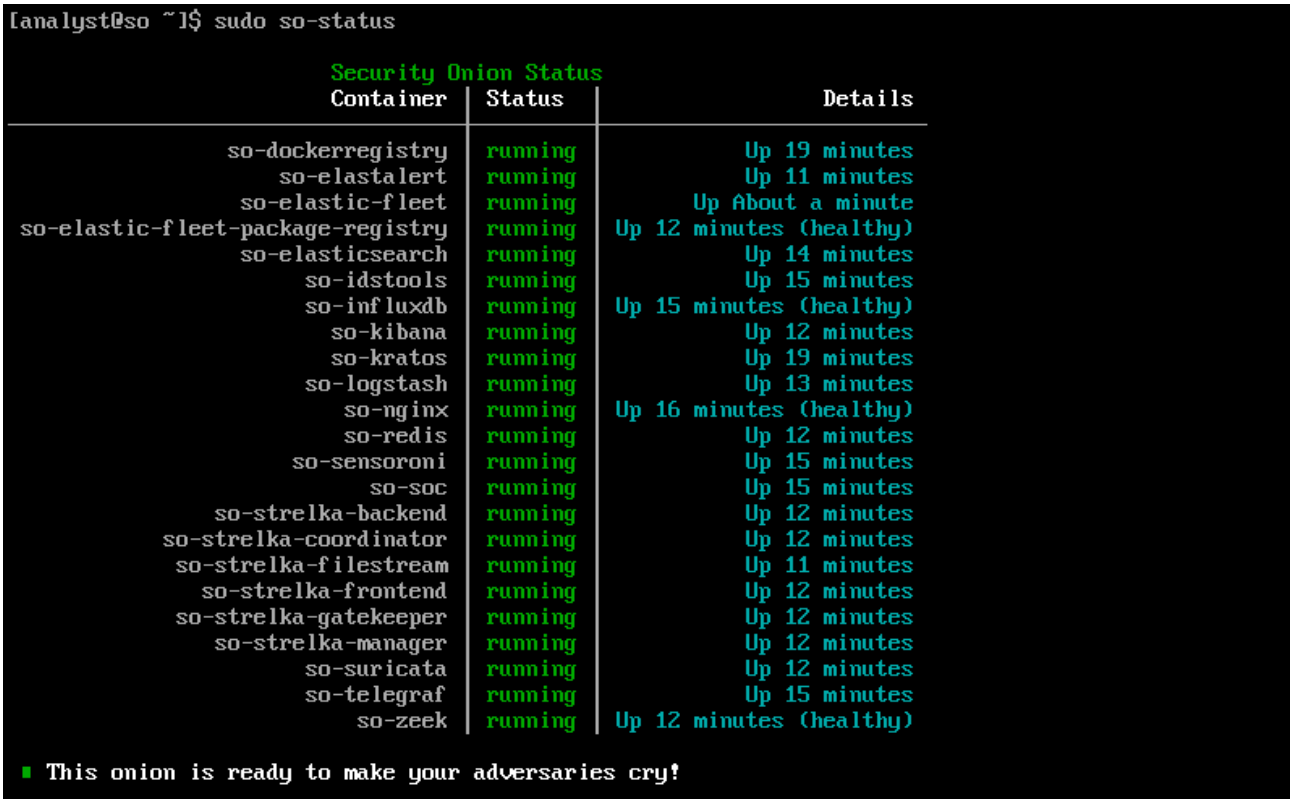

Рисунок 3.1 – Статус контейнерів і сервісів в Security Onion

Ця команда надає інформацію про стан і час роботи кожного компонента, який є частиною платформи.

Працюють наступні сервіси:

- so-dockerregistry –локальний реєстр контейнерів Docker, який використовується для зберігання і управління контейнерами;
- so-elasticsearch – основний компонент Elastic Stack, що забезпечує зберігання, пошук і аналітику зібраних даних;
- so-kibana – веб-інтерфейс для візуалізації даних і побудови аналітичних панелей на основі інформації, зібраної Elasticsearch;

- so-logstash – інструмент для збору, обробки і пересилання даних до Elasticsearch;
- so-suricata – система виявлення вторгнень (IDS), яка аналізує мережевий трафік і виявляє потенційні загрози;
- so-zeek – інструмент аналізу мережевого трафіку, який генерує журнали про різні типи мережевої активності;
- so-redis – база даних, що використовується для кешування та зберігання даних у реальному часі;
- so-nginx – веб-сервер, який забезпечує взаємодію з веб-інтерфейсами платформи;
- so-strelka (backend, coordinator, frontend) – компонент для аналізу файлів і виявлення загроз у файловому потоці.
- so-telegraf – інструмент для збору метрик системи й моніторингу продуктивності;
- so-sensoroni – компонент, який відповідає за збір даних із сенсорів мережевого трафіку.

Всі компоненти перебувають у стані running, що означає їхню активну роботу. Security Onion з усіма активними компонентами є повноцінною платформою для моніторингу, виявлення та реагування на кіберзагрози. У симуляційному середовищі вона використовується для аналізу трафіку, генерованого іншими системами, такими як Kali Linux і Ubuntu Linux. Suricata й Zeek виконують функції аналізу мережевого трафіку та виявлення загроз, Kibana забезпечує візуалізацію даних для розслідувань, а Elasticsearch зберігає всі журнали для подальшого аналізу. Завдяки цим компонентам Security Onion дозволяє ефективно проводити навчання, досліджувати реальні кіберзагрози і відпрацьовувати стратегії захисту.

На рисунку 3.2 представлено інтерфейс платформи Security Onion, зокрема розділ налаштувань правила виявлення Suricata під назвою GPL ATTACK_RESPONSE id check returned root.

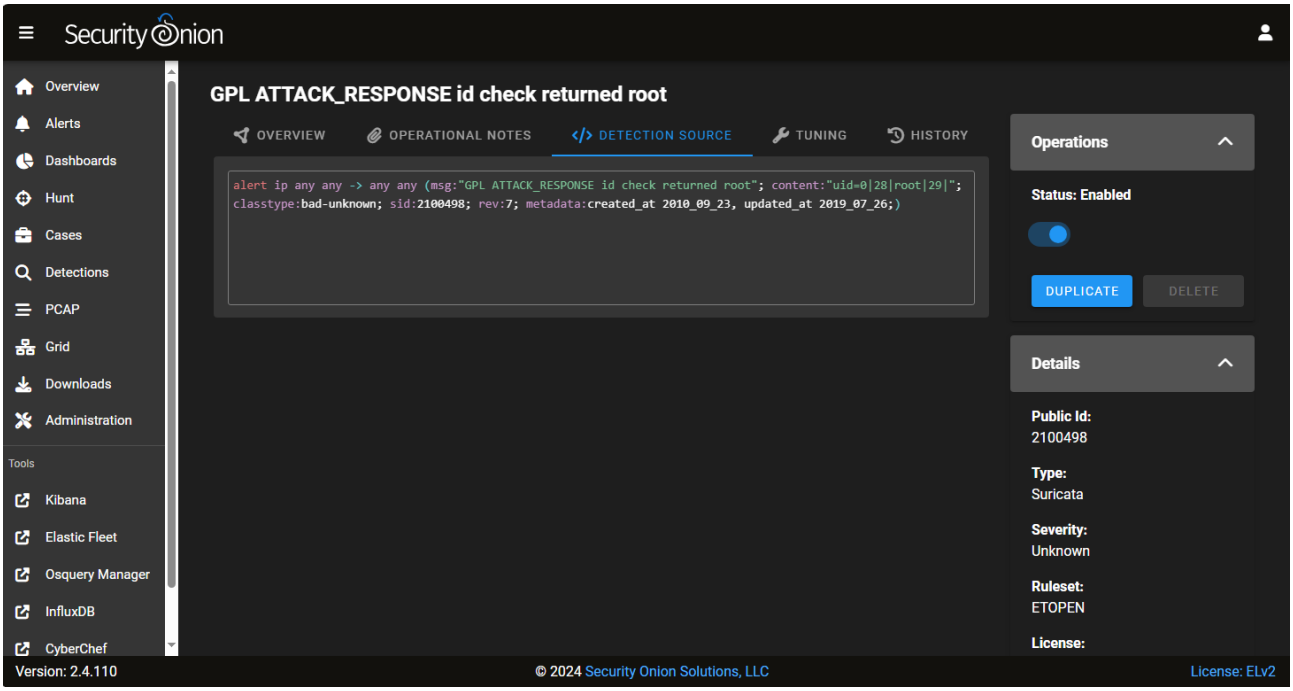

Рисунок 3.2 – Правило перевірки коректної роботи IDS Suricata

Це стандартне правило, яке створене для виявлення мережевого трафіку, який містить результати виконання команди id, що повертає інформацію про поточного користувача. Якщо результат вказує на обліковий запис root (uid=0), це може свідчити про те, що зловмисник отримав привілейований доступ до системи. Таке правило застосовується для моніторингу реакцій на команди або запити, які можуть бути використані під час атак, наприклад, коли зловмисник намагається отримати підтвердження успішного злому або привілеїв адміністратора.

На рисунку 3.3 показано налаштування правила в системі виявлення вторгнень Suricata, яке інтегроване в платформу Security Onion. Правило має назву "SYN Flood Alert" і використовується для виявлення атак типу SYN Flood, що належать до категорії DDoS-атак.

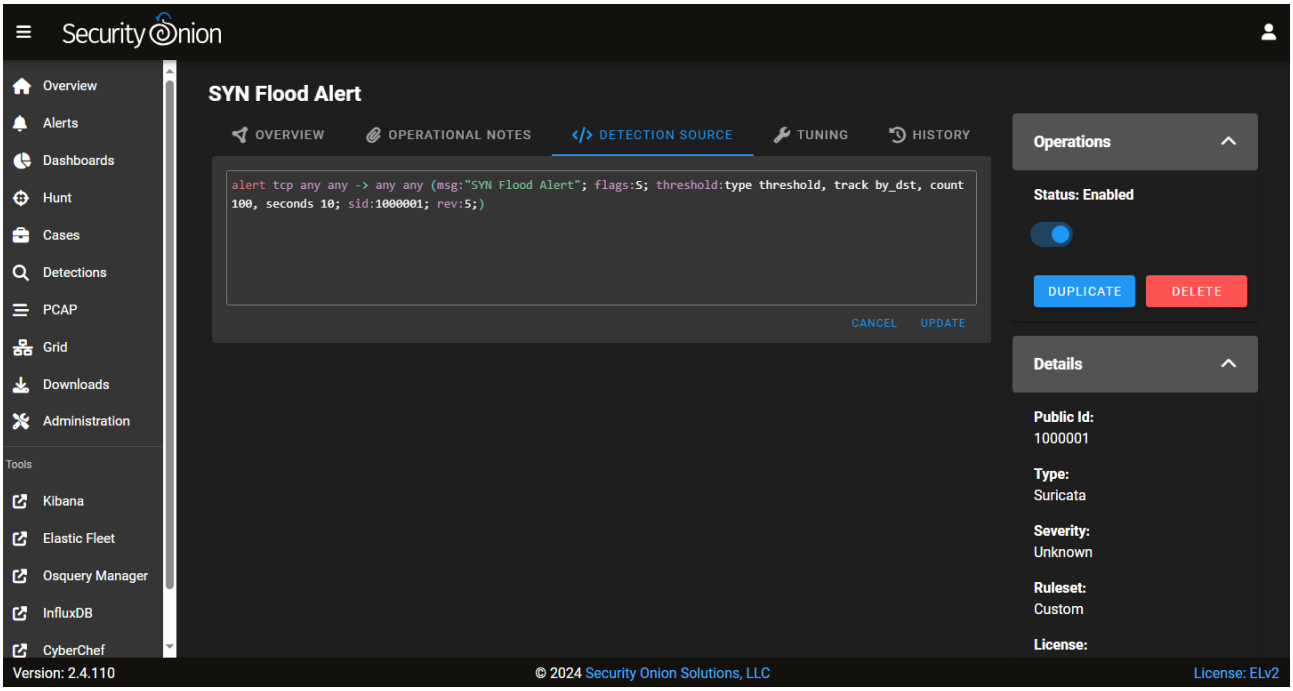

Рисунок 3.3 – Правило IDS Suricata для виявлення SYN Flood атаки

У вихідному коді правила вказано, що воно реагує на TCP-з'єднання, у яких встановлений прапорець S (SYN).

Правило налаштоване з використанням порогового обмеження, яке дозволяє визначати потенційні загрози на основі певної кількості подій. Тип порогу визначено як threshold, відстеження ведеться за напрямком by_dst (за адресою призначення), з кількістю подій, що дорівнює 100, протягом 10 секунд. Це означає, що якщо одна IP-адреса призначення отримує понад 100 SYN-запитів у зазначений часовий інтервал, спрацьовує тривога.

Ідентифікатор правила sid становить 1000001, а його ревізія позначена як rev:5. Це дозволяє однозначно ідентифікувати правило в системі, що є корисним для його подальшого налаштування та оновлення. У правій частині інтерфейсу відображено статус правила, який встановлений як Enabled, що підтверджує його активність. Також зазначено, що правило належить до користувацького набору (Ruleset: Custom).

Це правило є частиною системи моніторингу, що дозволяє ідентифікувати аномальну активність, характерну для DDoS-атак. Security Onion із таким правилом забезпечує можливість виявлення загроз і оперативного реагування на

них, дозволяючи адміністраторам мережі аналізувати трафік і блокувати шкідливі дії в реальному часі.

На рисунку 3.4 показано налаштування тестової сигнатури в системі виявлення вторгнень Suricata. Правило має назву "The signature of the virus has been detected" і використовується для виявлення конкретного вмісту в мережевому трафіку, що відповідає сигнатурі “вірусу”.

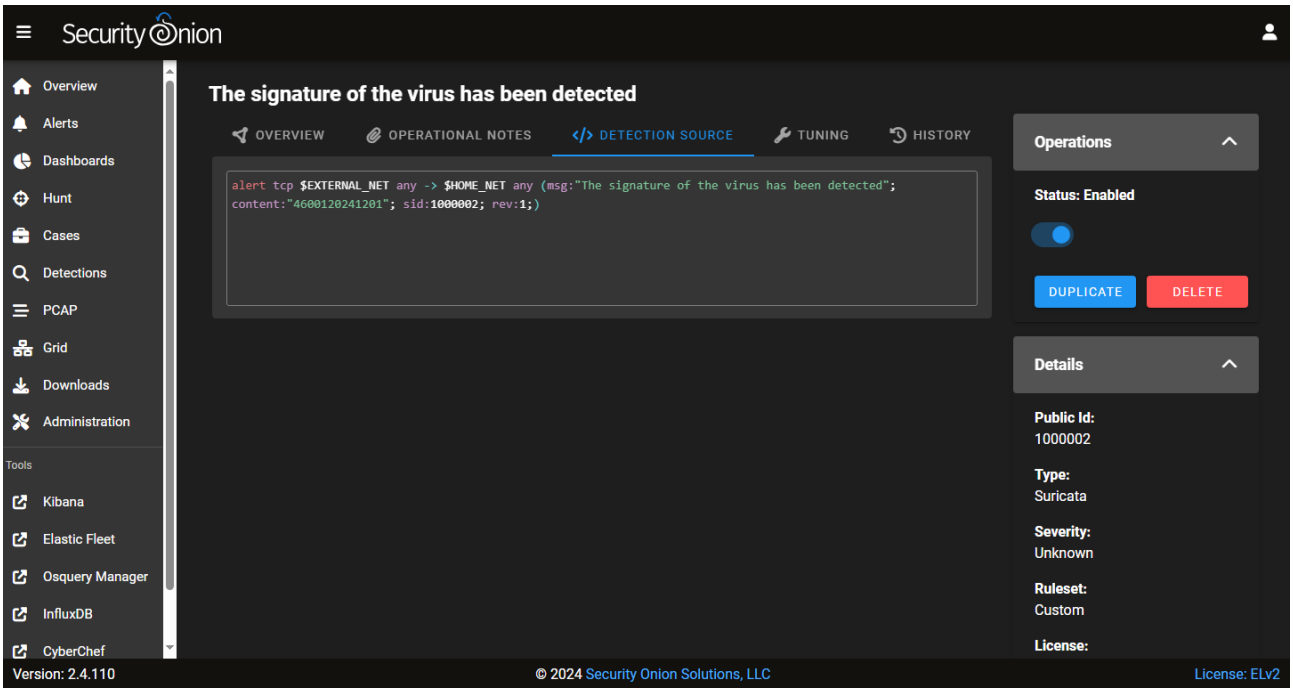

Рисунок 3.4 – Правило IDS Suricata для виявлення сигнатури в мережевому трафіку

Правило налаштоване для аналізу TCP-з'єднань між зовнішньою мережею $EXTERNAL_NET та внутрішньою мережею $HOME_NET. Відповідне правило генерує тривогу за наявності у трафіку вмісту "4600102041201". Ідентифікатор правила sid становить 1000002, а його ревізія позначена як rev:1. Це дозволяє легко відстежувати і керувати правилом у системі.

Статус правила позначений як Enabled, що свідчить про його активну роботу. Усі налаштування, включаючи назву, опис та параметри, створені вручну в межах набору правил Custom. Ця сигнатура слугує демонстрацією можливості створення та тестування користувацьких правил для виявлення загроз у мережевому середовищі. Правило дозволяє ефективно перевіряти роботу IDS

Suricata та аналізувати, як система реагує на певні сигнатури в реальному трафіку.

Правило під назвою "ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack" спрямована на виявлення можливих атак грубої сили через SSH (див. рисунок 3.5).

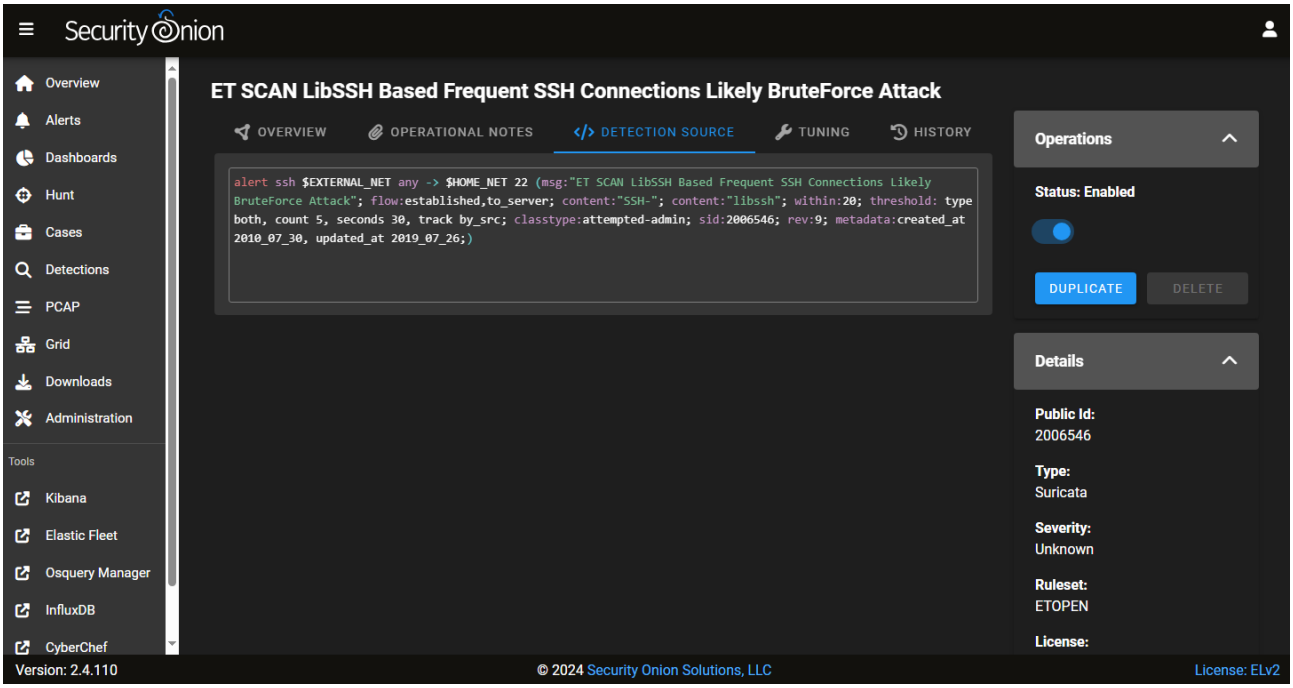

Рисунок 3.5 – Правило IDS Suricata для виявлення brute force атаки

Правило аналізує трафік з зовнішньої мережі $EXTERNAL_NET до внутрішньої мережі $HOME_NET на порт 22 (SSH). У сигнатурі використано ключові параметри: перевірка встановленого з'єднання через параметр flow:established,to_server;, пошук специфічного вмісту "SSH-" і "libssh", а також визначення частоти запитів. Для виявлення підозрілої активності задається поріг threshold:type both, count 5, seconds 30, track by_src;, який активується при 5 підключеннях протягом 30 секунд з одного джерела.

Сигнатура має ідентифікатор sid:2006546 і належить до класу attempted-admin, що вказує на спроби адміністративного доступу. Статус сигнатури позначено як Enabled, що означає її активну дію в мережі. Правило належить до набору ETOPEN, створеного для аналізу загальнодоступних загроз.

Ця сигнатура є прикладом використання Suricata для виявлення специфічних атак у реальному часі. Вона дозволяє швидко реагувати на спроби атаки грубої сили, забезпечуючи захист внутрішньої інфраструктури.

На рисунку 3.6 показано правило для виявлення атаки типу DNS Query Flood.

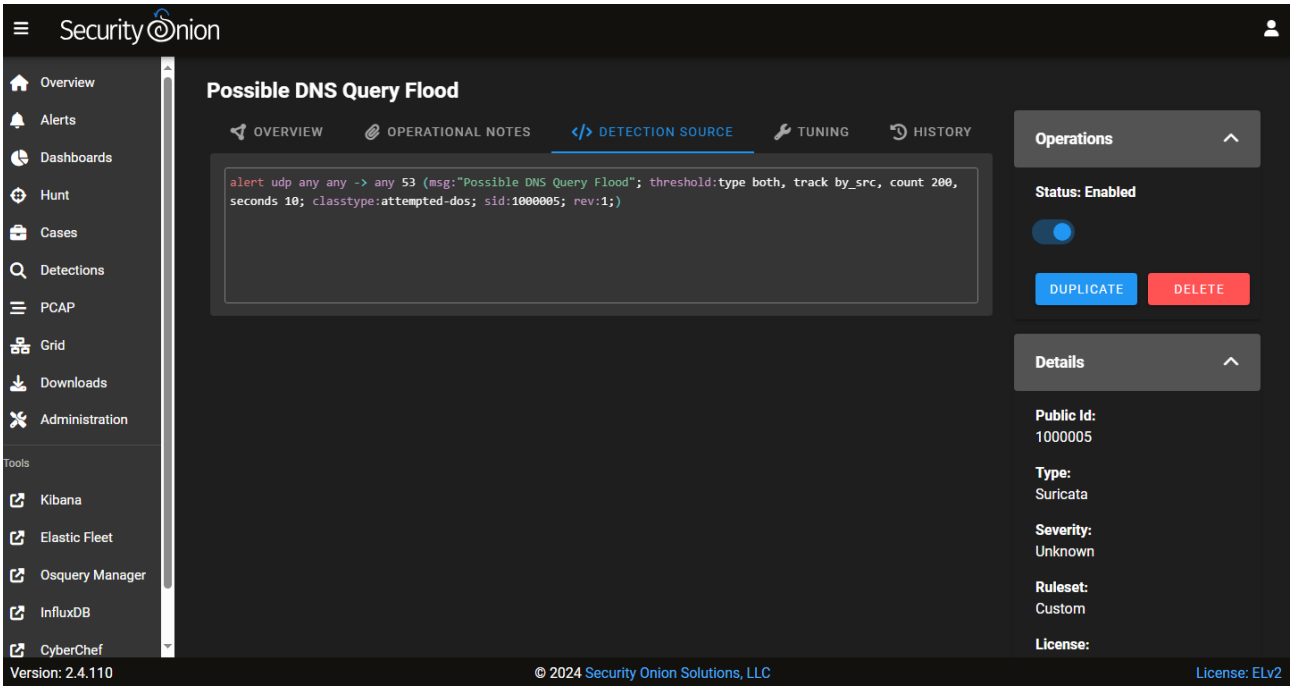

Рисунок 3.6 – Правило IDS Suricata для виявлення DNS Query Flood атаки

Це парвило налаштовує систему Suricata на аналіз мережевого трафіку для виявлення аномальної поведінки, яка характерна для перевантаження серверів DNS. Сигнатура працює з використанням протоколу UDP, аналізуючи трафік, що проходить через порт 53, який є стандартним для DNS-запитів. Умови її спрацьовування визначаються кількістю запитів, що надходять від одного джерела. Якщо протягом 10 секунд від одного джерела надходить 200 DNS-запитів, сигнатура активується, оскільки така активність може свідчити про атаку типу DNS Flood [35].

Сигнатура містить кілька важливих елементів. Вона налаштована на відстеження трафіку, який направляється на порт 53, та аналізує запити з метою виявлення перевищення порогу у 200 запитів за 10 секунд. Повідомлення "Possible DNS Query Flood" генерується у разі спрацьовування сигнатури, що

дозволяє ідентифікувати джерело аномальної активності, оцінити обсяг трафіку та визначити можливі загрози. Ідентифікатор сигнатури SID 1000005 забезпечує її унікальність у системі.

На рисунку 3.7 показано правило для виявлення можливої спроби використання DNS-тунелювання.

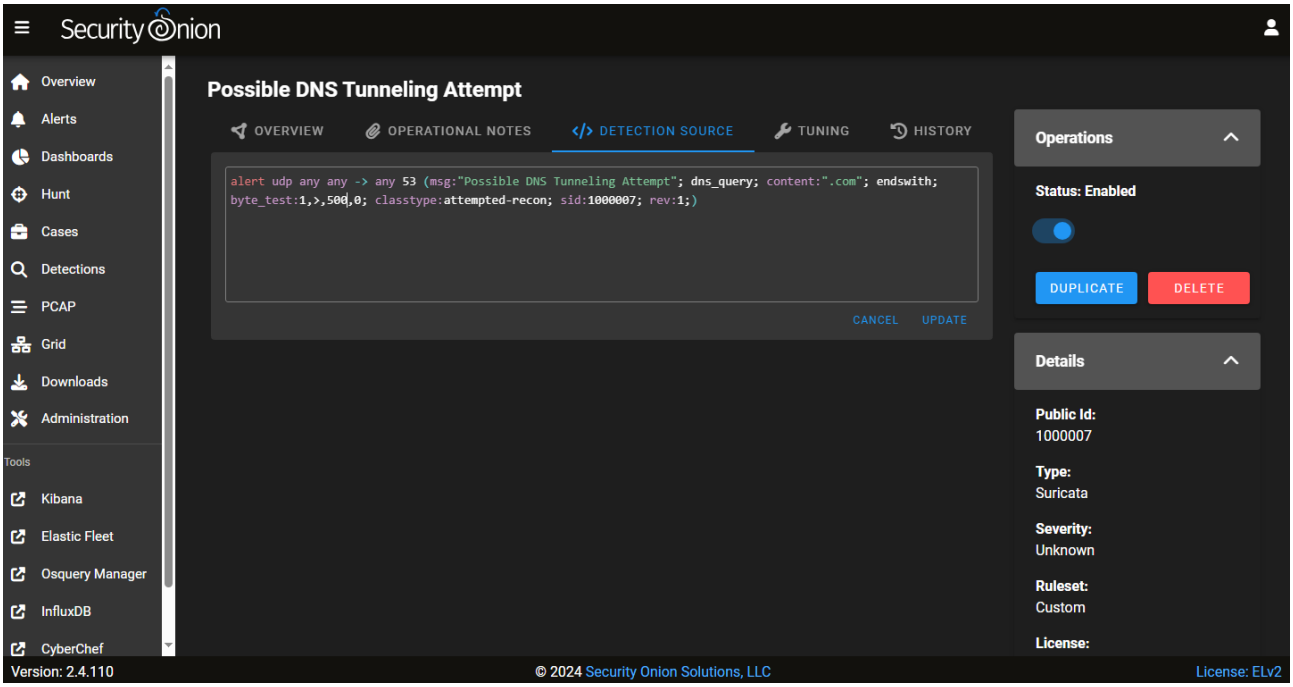

Рисунок 3.7 – Правило IDS Suricata для виявлення DNS-тунелювання

Це правило створене для системи виявлення вторгнень Suricata, призначена для виявлення можливих спроб використання DNS-тунелювання, що є одним із методів обходу традиційних заходів безпеки. Сигнатура аналізує DNS-запити, які відправляються через протокол UDP на порт 53 (порт, який зазвичай використовується для DNS-трафіку). Правило працює для будь-яких UDP-запитів від будь-якої IP-адреси та порту до будь-якої IP-адреси на порт 53. У разі активації правило генерує повідомлення, яке попереджає про можливу спробу DNS-тунелювання. Правило фокусується на DNS-запитах і перевіряє, чи закінчується запит доменним іменем із закінченням ".com". Вона також перевіряє розмір корисного навантаження DNS-запиту, щоб визначити, чи перевищує цей розмір 500 байт, що може свідчити про аномальну активність, пов'язану з тунелюванням. Аномальний розмір запиту часто є індикатором використання

DNS для передавання нехарактерних даних. Сигнатура класифікує виявлену активність як спробу розвідки, надаючи можливість для її подальшого аналізу.

Унікальний ідентифікатор сигнатури дозволяє ідентифікувати її в системі та використовувати для управління й відстеження.

Таким чином, Security Onion була налаштована як платформа для аналізу мережевого трафіку та реагування на загрози в симуляційному середовищі.

3.2 Моделювання кіберзагроз та оцінка ефективності системи

Моделювання кіберзагроз є важливим етапом у дослідженні ефективності захисних систем і вдосконаленні стратегій кібербезпеки. Цей процес передбачає створення реалістичних сценаріїв атак із використанням різних методів, таких як DDoS, brute-force атаки та атаки на веб-додатки. У представленому симуляційному середовищі ключовими компонентами для моделювання кіберзагроз є Security Onion, Kali Linux і сервер Ubuntu Linux.

Для моделювання кіберзагроз використовується підхід, що поєднує тестування атак із різноманітними сценаріями. Атакуюча система Kali Linux генерує шкідливий трафік або виконує атаки на сервер Ubuntu Linux. Використовуючи інструменти Kali Linux, можна реалізовувати різноманітні типи атак: мережеве сканування, brute-force SSH, DDoS та інші.

Security Onion, у свою чергу, забезпечує моніторинг мережевого трафіку, реєстрацію журналів та виявлення атак за допомогою Suricata та Zeek. Завдяки цьому можна аналізувати результати атак, визначати слабкі місця системи та оцінювати ефективність налаштованих механізмів захисту.

Оцінка ефективності системи виявлення вторгнень базується на аналізі логів, візуалізації даних у Kibana, а також на реєстрації спрацювань сигнатур. Наприклад, для атаки типу SYN Flood, UDP Flood або brute-force в системі Security Onion створені спеціальні правила, які аналізують кількість запитів, їх частоту та аномалії в трафіку. Правила налаштовуються так, щоб вони фіксували як відомі типи атак (з використанням сигнатурного методу), так і аномалії (поведінковий підхід).

3.2.1 Тест IDS Suricata

Для перевірки працездатності системи IDS Suricata можна скористатися спеціальними тестовими ресурсами. Один із таких ресурсів - `testmynids.org`, який надає можливість генерувати трафік, що відповідає певним сигнатурам атак. Зокрема, звернення до `http://testmynids.org/uid/index.html` повертає відповідь, яка містить рядок `uid=0(root)`, що відповідає сигнатурі з ID 2100498 у правилах Emerging Threats. Це дозволяє перевірити, чи правильно налаштована Suricata для виявлення подібних атак.

На рисунку 3.8 показано результати звернення до тестового ресурсу.

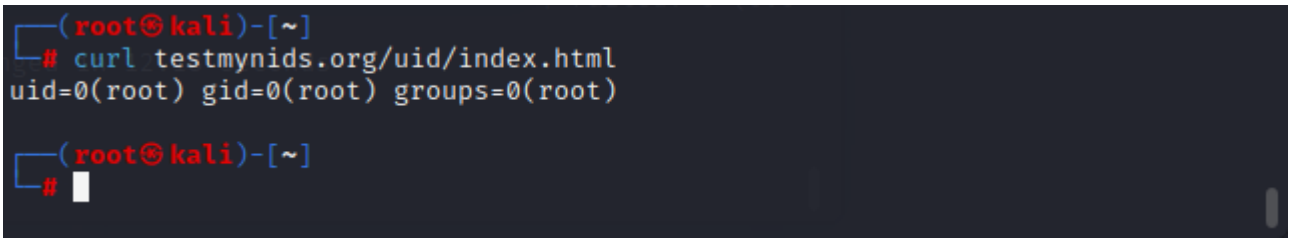

Рисунок 3.8 – Результати звернення до тестового ресурсу.

Результати тесту свідчать про те, що підключення до ресурсу успішно виконано, а виявлення рядка `uid=0(root)` може бути використано для діагностики працездатності IDS. Якщо Suricata налаштована коректно, цей тест допоможе перевірити правильність її конфігурації та роботу правил для виявлення подібних активностей у мережі.

На рисунку 3.8 показано результат роботи системи виявлення вторгнень Suricata у платформі Security Onion при виявленні звернення на тестовий ресурс.

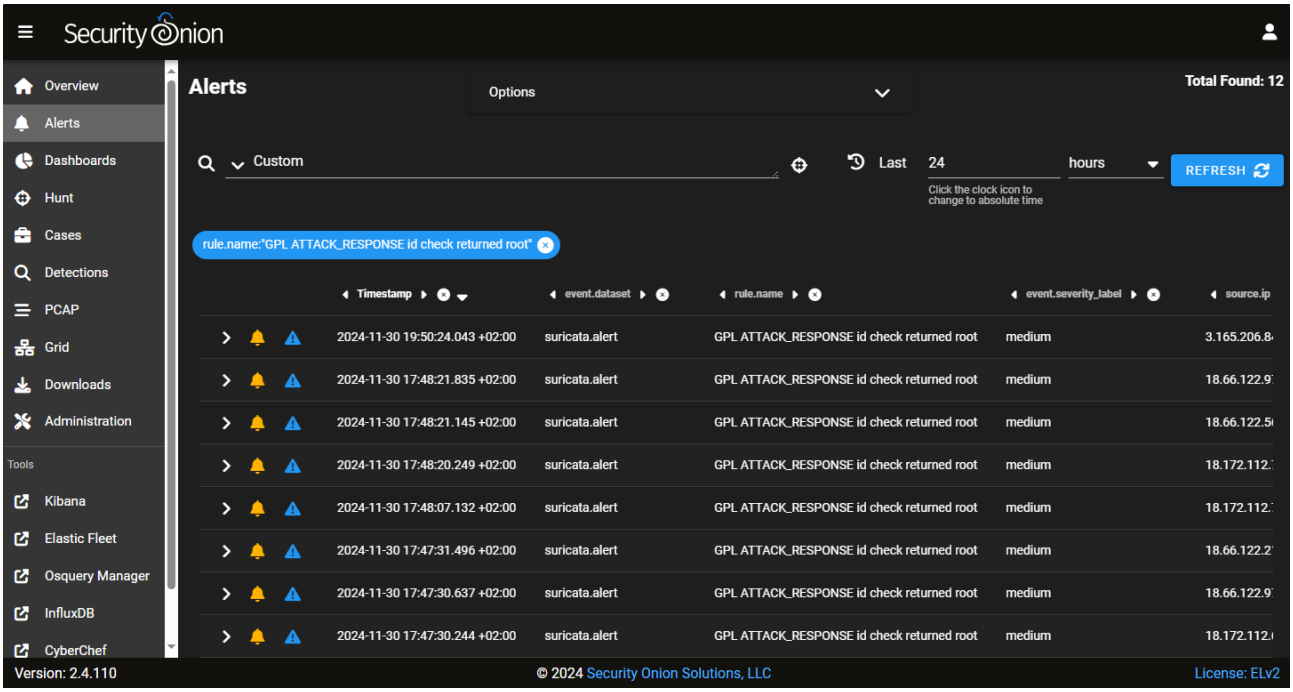

Рисунок 3.9 – Результати виявлення звернення до тестового ресурсу.

Виявлені сповіщення стосуються правила "GPL ATTACK_RESPONSE id check returned root," яке спрацювало у відповідь на тестовий HTTP-запит, ініційований з Kali Linux за допомогою команди curl testmynids.org/uid/index.html. Це правило активувалось, коли у мережевому трафіку виявилась відповідь, що містила рядок uid=0(root).

3.2.2 Атака типу SYN flood

Kali Linux дозволяє вивчити поведінку системи під час SYN flood атаки та оцінити ефективність засобів виявлення й запобігання. SYN flood є атакою на рівні транспортного протоколу TCP, яка спрямована на перевантаження сервера великою кількістю запитів на встановлення з'єднань (SYN-запитів), залишаючи їх незавершеними. У результаті сервер витрачає свої ресурси на очікування відповіді, що може призвести до його недоступності.

На рисунку 3.10 представлено приклад виконання команди для моделювання SYN flood атаки за допомогою утиліти hping3 у Kali Linux.

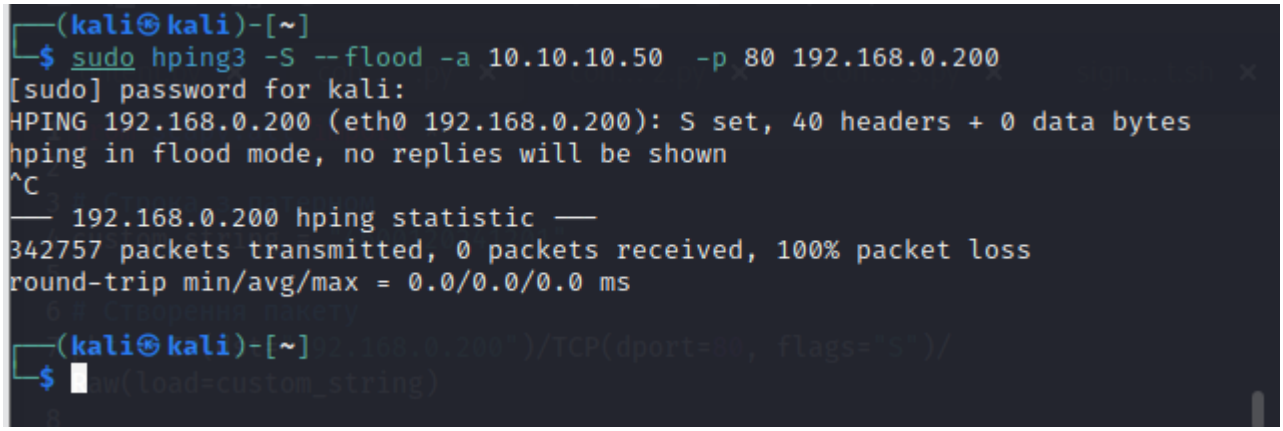

Рисунок 3.10 – Моделювання SYN flood атаки

Під час виконання команди утиліта hping3 згенерувала 342757 SYN-пакетів, які були спрямовані на вказаний сервер. Жоден пакет не отримав відповіді, що свідчить про втрачені пакети (100% packet loss), що є типовою поведінкою для SYN flood атаки.

На рисунку 3.11 показано результати роботи системи IDS Suricata в Security Onion після моделювання SYN flood атаки за допомогою утиліти hping3 на Kali Linux. У вкладці "Alerts" відображено спрацювання сигнатури "SYN Flood Alert", яка була попередньо налаштована в Suricata для виявлення атак цього типу.

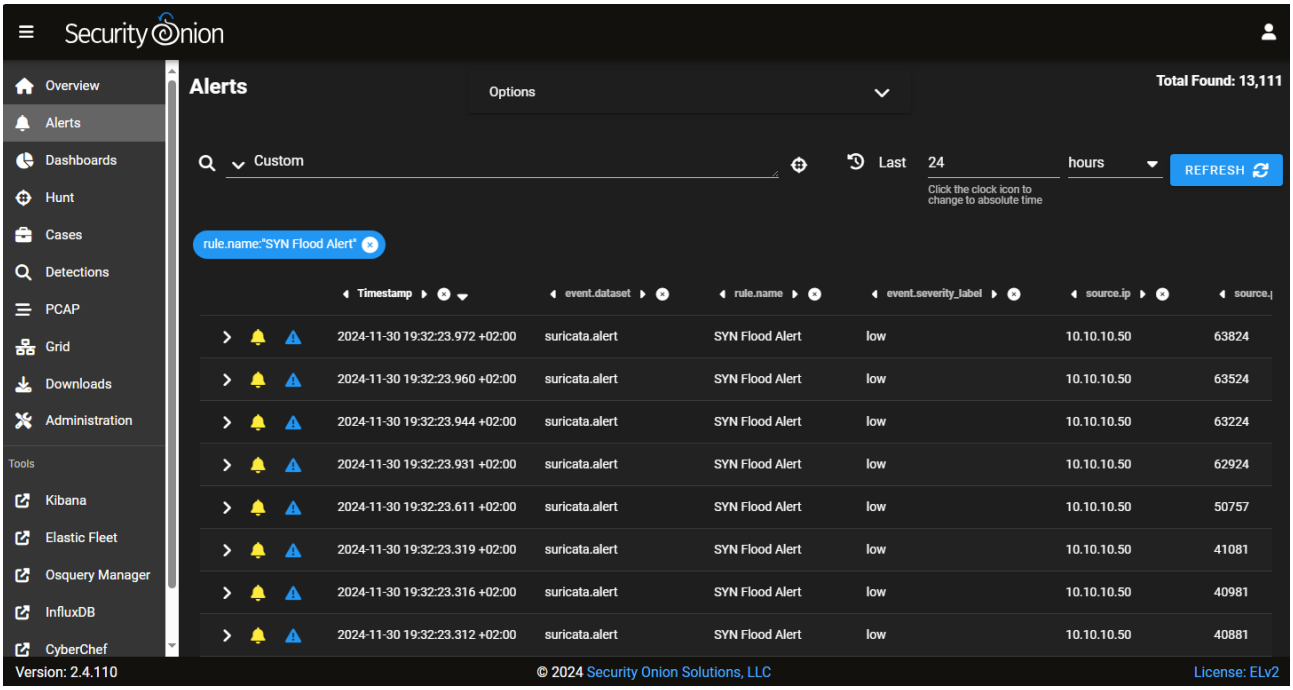

Рисунок 3.11 – Виявлення SYN flood атаки

Виявлення атаки дозволило отримати інформацію про трафік (зокрема IP-адреси джерела й цілі, тип пакетів, порт тощо) та дало можливість вжити відповідних заходів для нейтралізації загрози.

3.2.3 Виявлення сигнатури “вірусу”

Для перевірки ефективності правила виявлення сигнатури "вірусу" в системі Suricata було створено відповідне правило (див пункт 3.1).

Це правило активується, коли в TCP-трафіку, що надходить із зовнішньої мережі $EXTERNAL_NET до внутрішньої мережі $HOME_NET, виявляється сигнатура "4600120241201". Сигнатура може бути частиною корисного навантаження TCP-пакета, яке вказує на можливий шкідливий вміст або активність.

На рисунку 3.12 показано результат виконання команди для моделювання передачі даних із сигнатурою "4600120241201" за допомогою hping3.

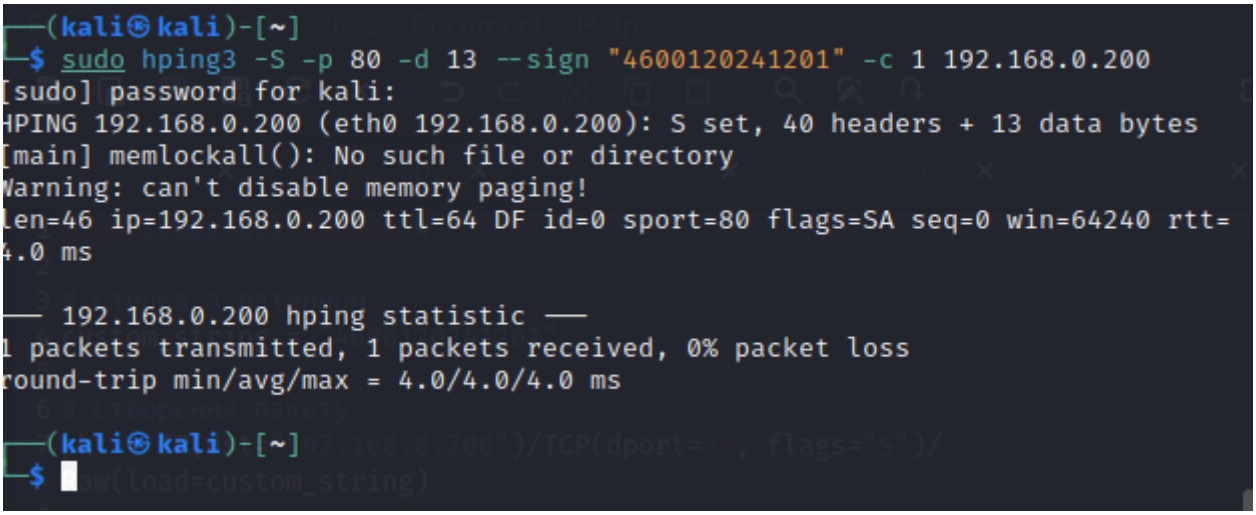

Рисунок 3.12 – Передача даних із сигнатурою “вірусу”

Цей тест підтверджує, що SYN-пакет із заданим підписом "4600120241201" був успішно доставлений до сервера. Система Suricata, розгорнута на платформі Security Onion, обробила цей трафік і зафіксувала подію та відобразила її в журналі сповіщень (див. рисунок 3.13).

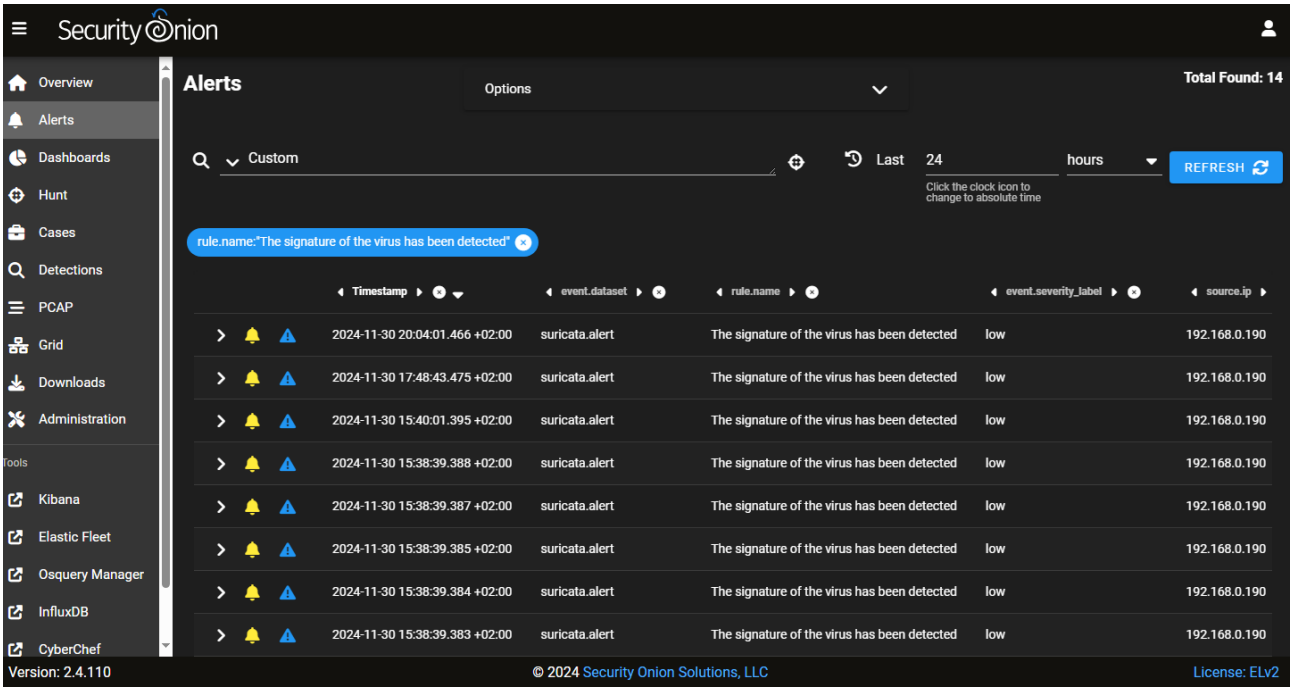

Рисунок 3.13 – Виявлення сигнатури “вірусу”

На рисунку представлено журнал сповіщень платформи Security Onion, в якому зафіксовані події, пов’язані з виявленням сигнатури "The signature of the virus has been detected". Ці події були зареєстровані системою Suricata на основі раніше налаштованого правила IDS. Ці дані підтверджують, що система Suricata успішно виявила специфічний трафік із заданою сигнатурою. Це свідчить про правильне налаштування системи та коректну роботу механізму виявлення.

3.2.4 Атака типу brute-force

Для моделювання атаки brute-force було використано інструмент Hydra в kali Linux. Ця програма створює багаторазові спроби авторизації на сервер SSH, використовуючи комбінації логіна та паролів.

На рисунку 3.14 показано виконання атаки типу brute-force на сервер SSH, розгорнутий в Ubuntu Linux.

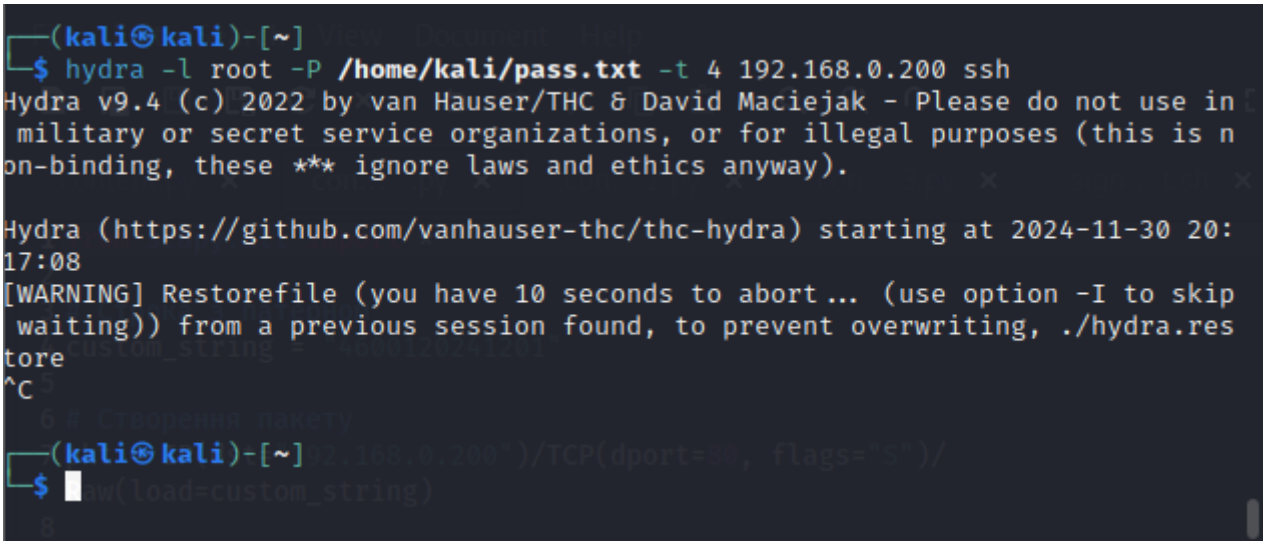

Рисунок 3.14 – Моделювання brute-force атаки

Інструмент Hydra використовується для автоматизованого перебору паролів у мережевих сервісах, таких як SSH. У цій команді вказано, що буде використовуватися логін "root", список паролів зберігається у файлі /home/kali/pass.txt, і атака здійснюється з використанням 4 потоків одночасно.

Ця спроба brute-force атаки створює мережевий трафік, який фіксується системою виявлення вторгнень Suricata, розгорнутою в середовищі Security Onion. У журналі подій Suricata має з'явитися запис, відповідний сигнатурі:

На рисунку 3.15 представлено результат спрацювання правила в системі виявлення вторгнень Suricata. Подія пов’язана з атакою типу brute-force на SSH-сервер.

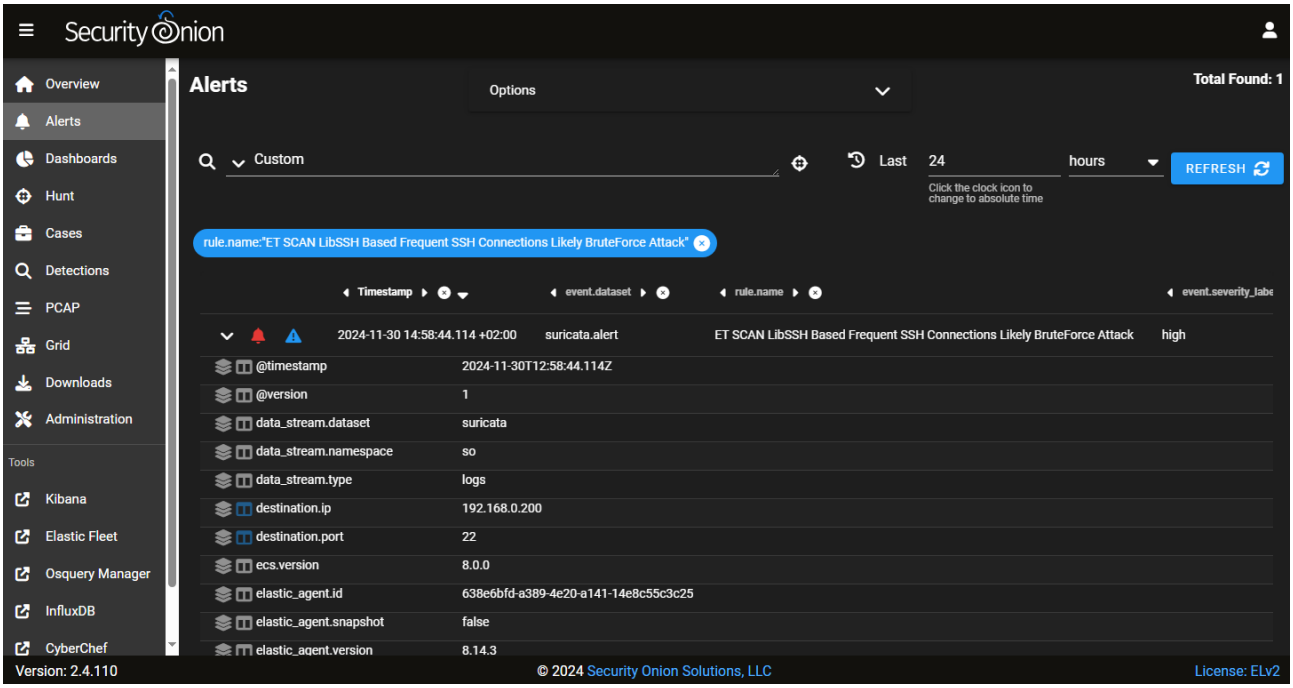

Рисунок 3.15 – Виявлення brute-force атаки

Suricata зафіксувала декілька підключень до порту 22 з IP-адреси атакуючої машини в межах короткого проміжку часу. В Alert Viewer Security Onion видно, що було створено подію з високим рівнем важливості (high severity).

Ця подія демонструє, що система виявлення Suricata успішно зафіксувала аномальну активність у мережі, яка характерна для атак brute-force на SSH-сервіси [36]. Це підтверджує коректну роботу правила, ефективність налаштувань Suricata та готовність середовища Security Onion для виявлення потенційних загроз.

3.2.5 DNS Query Flood атака та DNS Tunneling

Атака типу DNS Query Flood була змодельована з використанням інструменту hping3 (див. рисунок 3.16).

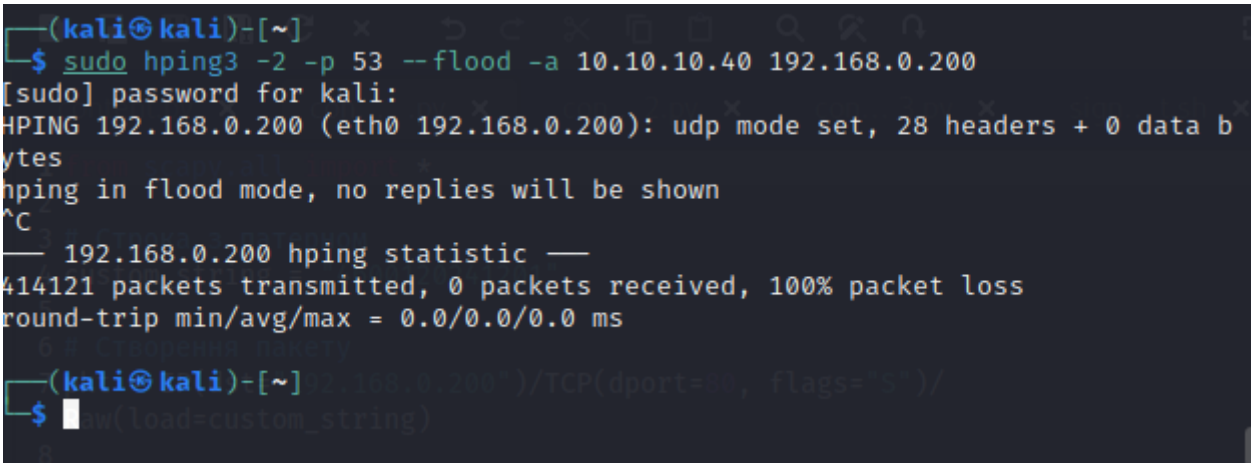

Рисунок 3.16 – Моделювання DNS Query Flood атаки

Ця команда генерує великий обсяг UDP-запитів на порт 53 цільового сервера 192.168.0.200, підробляючи IP-адресу джерела як 10.10.10.40. Метою такої атаки є перевантаження DNS-сервера великою кількістю запитів, що може призвести до відмови в обслуговуванні.

На рисунку 3.17 зображено інтерфейс системи Security Onion, який демонструє спрацювання сигнатури "Possible DNS Query Flood".

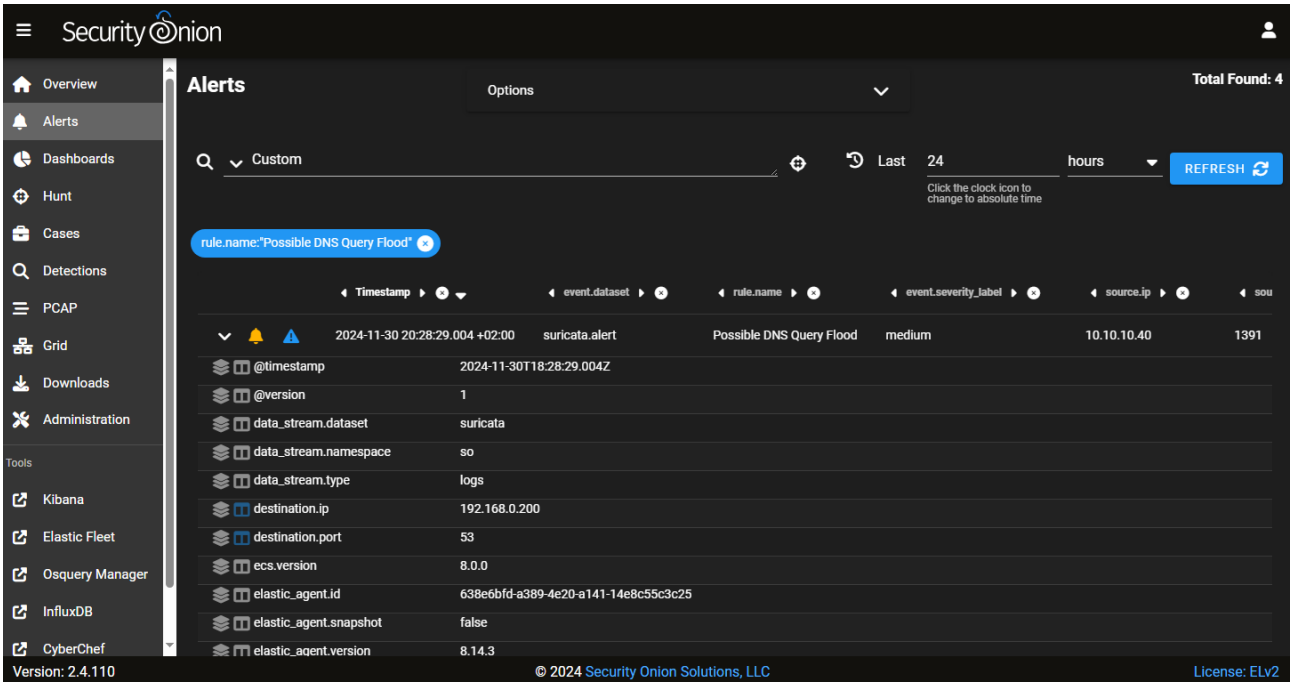

Рисунок 3.17 – Виявлення DNS Query Flood атаки

Ця подія була зафіксована системою виявлення вторгнень Suricata, що є частиною платформи. Атака типу DNS Query Flood виявлена на основі аналізу

великої кількості запитів до DNS-сервера за короткий проміжок часу. Джерело атаки ідентифіковане за IP-адресою 10.10.10.40, а цільовий DNS-сервер має IP-адресу 192.168.0.200, порт 53.

Система вказує, що рівень загрози цієї події оцінюється як середній (medium), що свідчить про потенційно шкідливу активність, яка може бути направлена на перевантаження серверу або створення відмови в обслуговуванні. Ця подія підтверджує коректну роботу правила Suricata, яке аналізує частоту запитів і генерує відповідне сповіщення, якщо поріг у 200 запитів за 10 секунд перевищено.

На рисунку 3.18 показано результат виконання команди nslookup, спрямованої на перевірку запиту до DNS-сервера за IP-адресою 192.168.0.200 для доменного імені 1234567890example-malicious.com.

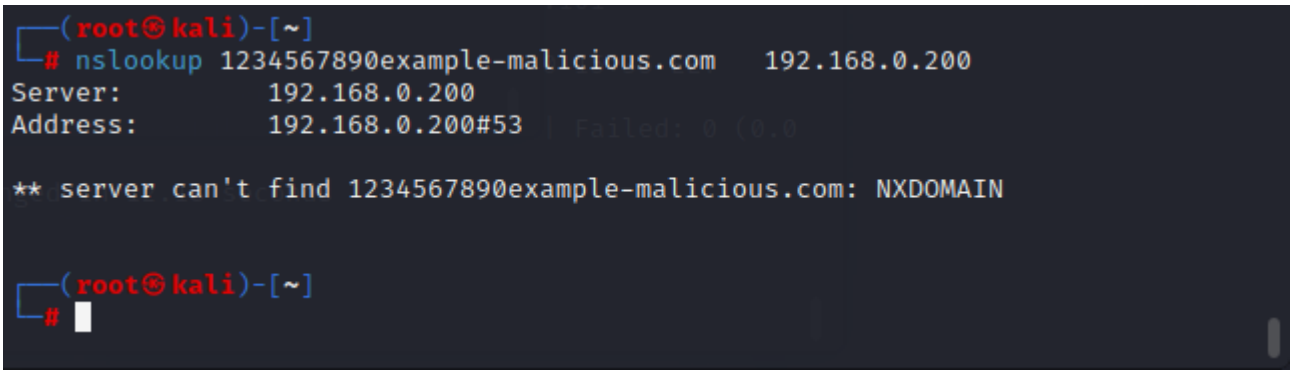

Рисунок 3.18 – Моделювання DNS Query Flood атаки

Ця команда була виконана для перевірки роботи правила "Possible DNS Tunneling Attempt", налаштованого в IDS Suricata. Відповідь NXDOMAIN свідчить про те, що запитаний домен не зареєстрований у DNS-системі, але сам факт запиту відображений у журналах Suricata для подальшого аналізу (див. рисунок 3.19).

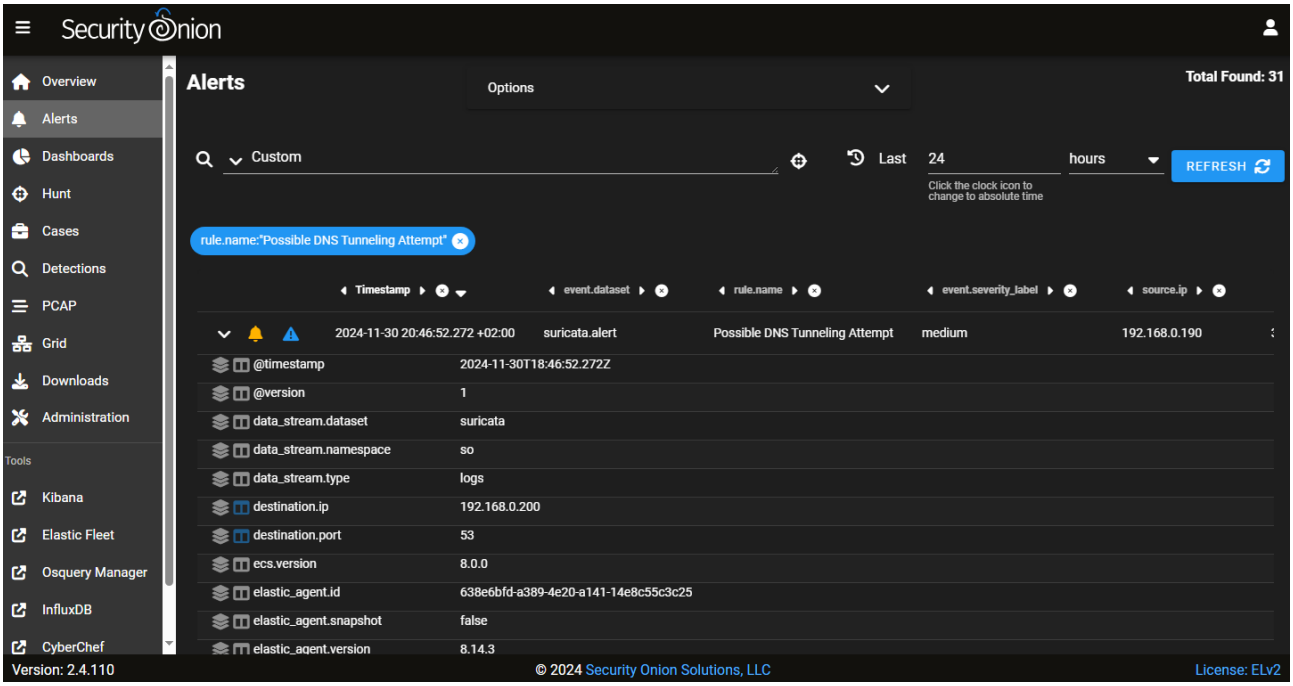

Рисунок 3.17 – Виявлення DNS Tunneling

На рисунку представлено спрацювання сигнатури "Possible DNS Tunneling Attempt" у системі виявлення вторгнень Suricata. Це спрацювання зафіксовано в журналі сповіщень, і його рівень серйозності визначено як "medium".

Сигнатура була активована внаслідок аналізу DNS-запиту, спрямованого на сервер за адресою 192.168.0.200, порт 53. Запит відбувся від джерела з IP-адресою 192.168.0.190.

Цей запис підтверджує, що система IDS Suricata успішно ідентифікувала потенційну спробу DNS тунелювання. Використання сигнатури дозволяє фіксувати підозрілий трафік, який відповідає характеристикам, типових для таких атак. Це важливий крок у перевірці ефективності налаштування системи виявлення вторгнень у симуляційному середовищі, орієнтованому на кіберзахист.

Отримані результати підтверджують здатність Security Onion до виявлення та реагування на кіберзагрози, дозволяючи своєчасно вживати необхідних заходів для мінімізації наслідків атак. Даний результат демонструє, що платформа Security Onion може ефективно реагувати на події такого типу, що є ключовим елементом для навчання та тестування в симуляційному середовищі.

3.3 Відображення статистики сповіщень Kibana

У Kibana, інтегрованій із Security Onion, можна детально переглядати сповіщення, згенеровані системою IDS Suricata. Це дозволяє провести поглиблений аналіз виявлених інцидентів. Відображення таких сповіщень у Kibana підтверджує факт виявлення підозрілої активності.

Через Kibana користувачі можуть аналізувати всі доступні метадані інциденту, включаючи джерело атаки, цільову IP-адресу, використаний порт, часові мітки та рівень серйозності сповіщення [37]. Це спрощує дослідження інцидентів і дозволяє швидко оцінити масштаб потенційної загрози. Інтеграція Kibana з Security Onion є ключовим інструментом для розслідування інцидентів і перевірки роботи правил, налаштованих у Suricata.

На рисунку 3.18 представлено інтегрований дашборд Kibana, який відображає дані, зібрані платформою Security Onion.

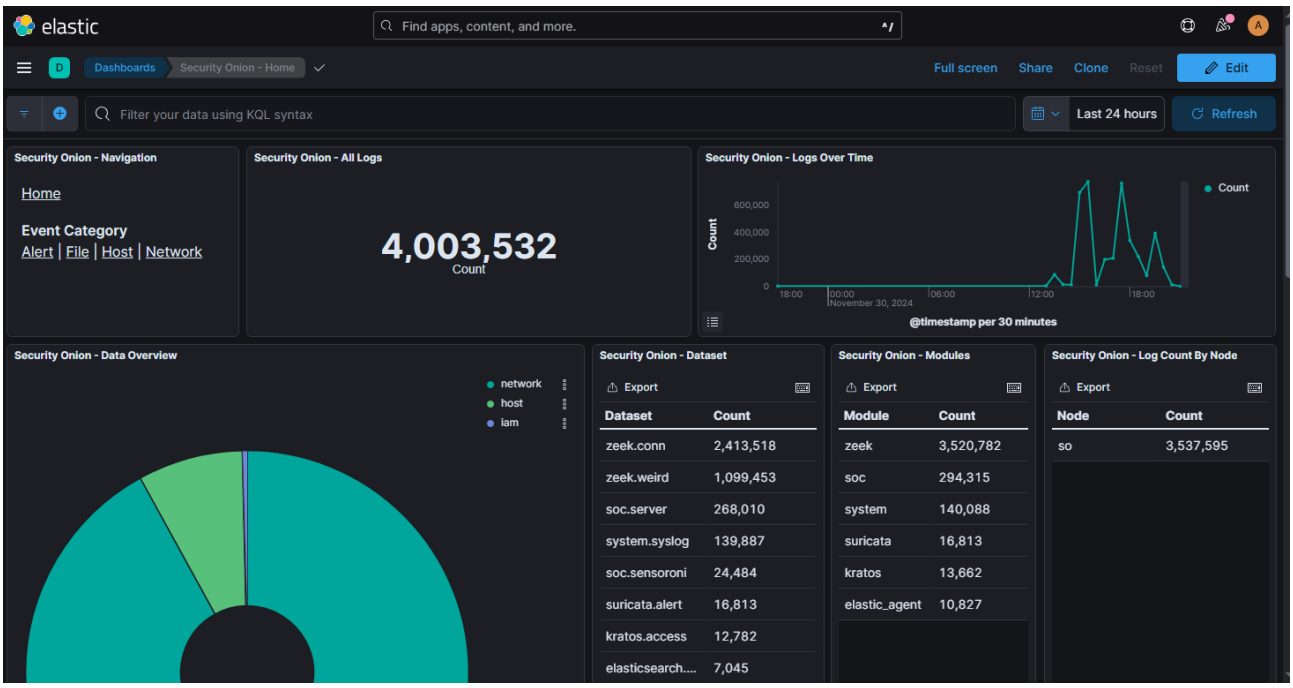

Рисунок 3.18 – Дашборд Kibana

Дашборд надає візуалізацію зібраних журналів і подій у мережі за останні 24 години. Центральний показник відображає загальну кількість логів (4,003,532), що дає розуміння обсягу мережевого трафіку та активності.

У верхньому правому куті видно графік, який демонструє динаміку логів у часі. Ця інформація допомагає ідентифікувати пікові періоди активності або потенційних атак. У розділі "Dataset" наведено різні джерела логів, серед яких найбільшу кількість становить трафік Zeek.conn (2413518), що вказує на значну активність мережевих підключень. У розділі "Modules" зазначено кількість записів, згенерованих різними модулями. Модуль Zeek є провідним із понад 3.5 млн записів, що свідчить про його важливу роль у моніторингу мережі. Інші модулі, такі як Suricata (16813 записів), вказують на кількість спрацювань сигнатур для потенційних загроз. Розділ "Log Count By Node" відображає кількість логів, зібраних кожним вузлом платформи Security Onion. Зокрема, вузол "so" обробив понад 3.5 млн записів, що свідчить про його ефективність у зборі та обробці даних.

Цей дашборд дозволяє адміністраторам безпеки отримувати швидкий доступ до ключових метрик та аналізувати виявлені загрози, використовуючи дані з таких інструментів, як Zeek, Suricata та інші компоненти Security Onion.

На рисунку 3.19 відображено аналіз сповіщень Suricata за останні 24 години.

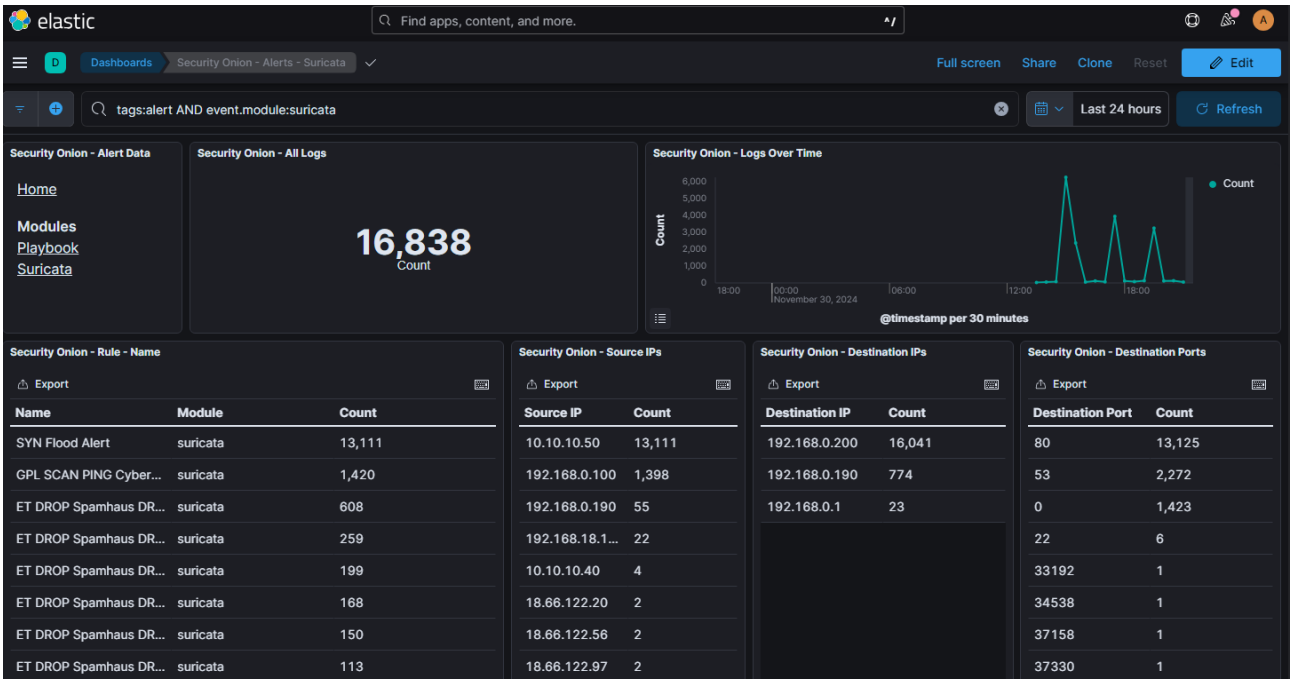

Рисунок 3.19 – Аналіз сповіщень Suricata в Kibana

Загальна кількість спрацювань правил Suricata становить 16,838, що свідчить про значну активність в мережі підчас атаки. Основна частина подій пов'язана зі спрацюванням правила "SYN Flood Alert," яке зафіксувало 13111 повідомлень. На графіку видно пікові періоди активності, що дозволяє аналізувати час найбільш інтенсивних атак. Серед джерел IP-адрес найбільшу активність демонструє IP 10.10.10.50 з 13,111 подіями. Основною ціллю атак є Ubuntu Linux з IP-адресою 192.168.0.200. Переважна кількість атак спрямована на порт 80.

Kibana є незамінним інструментом для моніторингу та аналізу мережевої активності в рамках системи безпеки на основі Security Onion. Завдяки інтеграції з Suricata, Zeek та іншими компонентами платформи, Kibana дозволяє візуалізувати великі обсяги даних про події в мережі, надаючи чітке уявлення про джерела загроз, цілі атак та їхні характеристики. Її дашборди забезпечують оперативний доступ до статистики, як-от кількість подій, типи атак, IP-адреси джерел і цілей, а також інформацію про найчастіше атаковані порти. Завдяки можливостям виявлення пікових періодів активності, Kibana сприяє ефективному розподілу ресурсів для реагування на загрози та дозволяє виявляти закономірності атак.

Використання Kibana значно підвищує ефективність системи моніторингу та реагування на кіберзагрози, полегшуючи аналіз подій і прийняття рішень у реальному часі. Це є важливим компонентом сучасної системи кіберзахисту, яка дозволяє забезпечити оперативне виявлення та нейтралізацію загроз.

3.4 Висновки до розділу 3

У третьому розділі було проведено тестування та оцінку ефективності симуляційного середовища для моделювання кіберзагроз і аналізу роботи системи виявлення вторгнень. Було виконано налаштування компонентів середовища, таких як Security Onion, Suricata, Zeek, Kibana, а також Kali Linux і Ubuntu Linux. Особливу увагу приділено перевірці коректності роботи правил

IDS Suricata, що дозволило виявити потенційні загрози, зокрема DDoS-атаки, brute-force, DNS Flood, DNS тунелювання та інші типи шкідливої активності.

У процесі тестування здійснювалися моделювання реальних сценаріїв атак із використанням таких інструментів, як hping3 та hydra. Виявлення атак та аналіз мережевого трафіку підтвердили ефективність роботи платформи Security Onion. Усі компоненти, включаючи Suricata, Zeek та Elasticsearch, успішно взаємодіяли, забезпечуючи зберігання, обробку та візуалізацію даних. Результати тестування показали, що налаштовані правила IDS Suricata здатні ефективно виявляти як відомі атаки за сигнатурами, так і нові загрози за допомогою аналізу аномальної поведінки.

Таким чином, проведене тестування продемонструвало високу ефективність симуляційного середовища для навчання, дослідження та вдосконалення кіберзахисту. Використання Security Onion у поєднанні з інтегрованими інструментами забезпечує комплексний підхід до моніторингу, аналізу та реагування на кіберзагрози, що робить це середовище незамінним для підготовки фахівців із кібербезпеки та тестування стратегій захисту.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою роботи є створення системи інтерактивного навчання з кібербезпеки, заснованої на симуляційних середовищах. Дані середовища розгортаються на серверному обладнанні, яке розміщене в приміщення спеціального типу. При роботі з даними системами потрібно забезпечити дотримання вимог з охорони праці, техніки безпеки та протипожежної безпеки при використанні ПК.

Основними регламентуючими нормативними документами охорони праці користувачів комп'ютерів є:

– НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями»;

– ДСанПіН 3.3-2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»;

– НАПБ А.01.001-2004 «Правила пожежної безпеки в Україні».

Вимоги до приміщень, згідно з [38][39], щодо розташування робочого місця передбачають виконання наступних вимог:

– мінімальна площа, яка виділяється на одне робоче місце повинна становити мінімум 6,0 м2, при об'ємі – мінімум 20,0 м3;

– розташування робочих місць користувачів ПК заборонено у цокольних або підвальних приміщеннях.

При організації робочих місць у НПАОП 0.00-7.15-18 передбачано наявність природного і штучного освітлення. Зазвичай, природне освітлення поступає у приміщення через вікна та світлові прорізи і забезпечує коефіцієнт освітленості на рівні не менше 1,5%. Орієнтація вікон – на північ або північний схід. Штучне освітлення забезпечують відповідні джерела, наприклад, люмінесцентні лампи. Приміщення з комп'ютерною технікою не повинні межувати з будівлями, де рівень шуму чи вібрації перевищує визначені допустимі значення. Покриття підлоги повинне бути матовим з коефіцієнтом відбиття 0,3-0,5. Для внутрішнього оздоблення приміщень слід використовувати

дифузно-відбивні матеріали з коефіцієнтами відбиття для стелі 0,7-0,8, для стін 0,5-0,6 [38].

У приміщеннях, де організовано робочі місця користувачів ПК, повинні бути забезпечені аптечками першої медичної допомоги. Вологе прибирання у таких приміщеннях є обов'язковим кожного дня.

Щодо ергономічної організації робочого місця, то воно також повинно відповідати вимогам, наведеним у [38][39]. Конструкція робочого місця повинна забезпечити підтримання оптимальної робочої пози. У відповідності до НПАОП 0.00-7.15-18, обладнання і організація робочого місця працюючих з ЕОМ мають забезпечувати відповідність конструкції всіх елементів робочого місця та їх взаємного, розташування ергономічним вимогам з урахуванням характеру і особливостей трудової діяльності.

Висота робочого столу з ПК повинна бути виконана в діапазоні 680...800 мм, а ширина і глибина – 600...1400 мм і 800..1000 мм відповідно. Стіл також повинен мати достатній простір для ніг, що забезпечить зручну осанку користувача. Стілець на робочому місці користувача ПК повинен бути підйомно-поворотним, регульованим за висотою, за кутом і за нахилом сидіння та спинки [38].

Екран комп'ютера повинен бути розміщений на відстані 600...700 мм від очей користувача. Розташування монітору має забезпечувати зручність зорового спостереження у вертикальній площині під кутом +30 градусів до нормальної лінії погляду працівника [38].

Електромережі штепсельних з'єднань та електророзеток для живлення ПК потрібно виконувати за магістральною схемою. При організації робочих місць електромережу штепсельних розеток для живлення ПК у центрі приміщення прокладають у каналах або під знімною підлогою в металевих трубах або гнучких металевих рукавах [38].

Щодо безпеки при роботі з ПК, щодня перед початком роботи необхідно очищати монітор від пилу та інших забруднень. Після закінчення роботи з ПК, він та периферійні пристрої повинні бути відключені від електричної мережі. У разі виникнення певної аварійної ситуації необхідно негайно відключити ПК від

електричної мережі. Не допускається виконувати обслуговування, ремонт та налагодження ПК безпосередньо на робочому місці [38].

Основні вимоги до пожежної безпеки вказані в НАПБ А.01.001-2004 «Правила пожежної безпеки в Україні». Згідно з [38], на та під приміщеннями, в яких розміщені ЕОМ, а також у суміжних із ними приміщеннях не дозволяється розташування приміщень категорій А та Б за вибухопожежною небезпекою.

Фальшпідлога у приміщеннях з ЕОМ має бути з негорючих матеріалів або матеріалів груп горючості Г1, Г2 з межею вогнестійкості не менше 0,5 години. Простір під нею слід розділяти негорючими діафрагмами на відсіки площею не більше 250 м2. Діафрагми повинні мати межу вогнестійкості не менше 0,75 год. Звукопоглинаюче облицювання стін та стель цих приміщень слід виготовляти з негорючих матеріалів або матеріалів груп горючості Г1, Г2. Персональні комп'ютери після закінчення роботи повинні відключатися від мережі. Не рідше одного разу на квартал необхідно очищати від пилу агрегати та вузли, кабельні канали та простір між підлогами [39].

Приміщення повинні бути забезпечені первинними засобами пожежогасіння, а саме вогнегасниками, що використовуються для локалізації і ліквідації пожеж у їх початковій стадії розвитку.

Вогнегасники слід встановлювати у легкодоступних та помітних місцях (коридорах, біля входів або виходів з приміщень тощо), а також у пожежонебезпечних місцях, де найбільш вірогідна поява осередків пожежі. При цьому необхідно забезпечити їх захист від попадання прямих сонячних променів та безпосередньої (без загороджувальних щитків) дії опалювальних та нагрівальних приладів.

Вибір типу та необхідна кількість вогнегасників визначається відповідно до Типових норм належності вогнегасників, затверджених наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 02.04.2004 № 151.

У кваліфікаційній роботі розроблено метод захисту серверів від атак. Дослідження в роботі вимагали взаємодії людини з серверним обладнанням, тому важливим та актуальним було провести аналіз основних вимог до

приміщень та робочих місць з ПК, що дозволило забезпечити комфортні і безпечні умови праці адміністраторів систем.

4.2 Фактори ризику і можливі порушення здоров’я користувачів комп’ютерної мережі

Велика кількість людей проводить багато часу за комп’ютером, що збільшує ризики та можливі негативні наслідки для здоров’я. Довге сидіння за комп’ютером призводить до різних проблем із здоров’ям. Найпоширенішими причин погіршення стану здоров’я є порушення постави та біль у спині [40]. Неправильна постава, яка зумовлена внаслідок погано організованого робочого місця або неправильно підібраного комп’ютерного стільця, це може спричинити хронічні болі у спині, шиї та плечах. Також поширена проблема із зап’ястям та кистями, наприклад синдром зап’ястного каналу, який виникає через повторюванні рухи, наприклад використання миші чи клавіатури [40]. Ще одним серйозним ризиком, пов’язаним із тривалим використанням комп’ютера, є проблеми зі здоров’ям очей. Проведення надто тривалого часу перед екраном може призвести до таких симптомів, як погіршенням зору або напруження очей, яке характеризується сухістю, свербінням, подразненням і втомою очей. Робота за комп'ютером часто пов'язана з високим рівнем стресу, особливо в умовах коли терміни стислі, а вимоги високі. Це може призвести до вигоряння, депресії та інших психологічних проблем. Крім того, ізоляція, яка часто супроводжує роботу вдома або в невеликих кабінетах, може вплинути на соціальне та емоційне самопочуття.

Також важливо розглянути вплив на якість сну та загальне фізичне здоров'я. Багато користувачів комп'ютерів скаржаться на порушення сну, що може бути пов'язано з надмірним впливом на світлові екрани перед сном. Це світло пригнічує вироблення мелатоніну, гормону сну, заважаючи людям засинати та підтримувати здоровий цикл сну. Використання спеціальних програм або окулярів для блокування синього світла є важливим для тих, хто регулярно працює з комп'ютерами ввечері. Фізична неактивність, яка часто супроводжує

довготривалу роботу за комп'ютером, також є фактором ризику для ряду хронічних захворювань, серцево-судинні захворювання та діабет другого типу. Недостатня фізична активність призводить до уповільнення метаболізму, що може спричинити набір ваги і зниження загальної фізичної форми. Це підвищує ризик розвитку серцевих захворювань.

Залежність від Інтернету та соціальних медіа є ще однією проблемою, з якою стикаються користувачі комп'ютерних мереж. Ця залежність може призвести до зниження продуктивності, соціальної ізоляції та погіршення психічного здоров'я. Важливо встановлювати межі та регулярно проводити час без використання електронних пристроїв.

Для зменшення цих ризиків існують різні стратегії. По-перше, важливо правильно організувати робоче місце. Ергономічні крісла, належно розташовані монітори та клавіатури, підставка для ніг, регулярні перерви для руху та розтяжки можуть значно знизити ризик мускул скелетних проблем. Крім того, використання спеціальних окулярів або застосування програм, що знижують синє світло від екранів, можуть допомогти зменшити втому очей [40].

Що стосується психологічного здоров'я, важливо забезпечити баланс між роботою та особистим життям, включаючи регулярні перерви, хобі, соціальну взаємодію та вправи на свіжому повітрі. Також корисною може бути практика медитації для зниження рівня стресу.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи магістра було здійснено розробку інтерактивної симуляційної системи для навчання з кібербезпеки, заснованої на використанні гіпервізора першого типу XEN та платформи Security Onion. У процесі роботи було досліджено існуючі симуляційні середовища, проаналізовано можливості гіпервізорів для створення ефективних віртуальних середовищ, а також розглянуто типи кіберзагроз та методи їх виявлення і запобігання.

У першому розділі проведено огляд сучасних симуляційних платформ, таких як Check Point Cyber Range, Cyberbit Range, RangeForce, IBM X-Force Cyber Range та інших. Встановлено, що використання симуляційних середовищ є ключовим елементом у підготовці фахівців з кібербезпеки, оскільки вони дозволяють моделювати реальні сценарії атак та відпрацьовувати методи захисту в безпечних умовах. Розглянуто різні типи атак на доступність, конфіденційність та цілісність, а також методи їх виявлення та запобігання.

У другому розділі розроблено архітектуру симуляційного середовища, яке базується на гіпервізорі XEN (XCP-NG). Описано основні компоненти середовища: віртуальний маршрутизатор MikroTik CHR, сервери Ubuntu Linux та Kali Linux, а також платформу Security Onion, яка інтегрує інструменти Suricata, Zeek та ELK Stack для моніторингу та аналізу мережевого трафіку. Проведено налаштування та тестування компонентів середовища, що підтвердило їхню коректну роботу та готовність до моделювання кіберзагроз.

У третьому розділі здійснено моделювання різних типів кіберзагроз, таких як DDoS-атаки, brute-force, DNS Flood та інші. Проведено тестування системи виявлення вторгнень Suricata, яка успішно виявила та зареєструвала аномальну активність. За допомогою Kibana було візуалізовано зібрані дані, що дозволило провести детальний аналіз інцидентів та оцінити ефективність налаштованих правил. Результати тестування підтвердили здатність системи оперативно реагувати на кіберзагрози та забезпечувати високий рівень безпеки.

Результати дослідження підтверджують, що розроблена симуляційна система є ефективним інструментом для навчання та дослідження в галузі кібербезпеки.

Вона дозволяє:

- моделювати реальні сценарії атак та аналізувати їх наслідки;
- відпрацьовувати методи виявлення та нейтралізації кіберзагроз;
- підвищувати практичні навички фахівців з кібербезпеки;
- оцінювати ефективність захисних механізмів у реальному часі.

Практичне значення одержаних результатів полягає в можливості використання розробленої системи у навчальних закладах та тренінгових центрах для підготовки спеціалістів з кібербезпеки. Система є масштабованою та може бути адаптована під різні сценарії та потреби, що робить її універсальним інструментом для навчання та дослідження.

Поставлені в роботі цілі та задачі були досягнуті. Розроблена система демонструє ефективність у виявленні та аналізі кіберзагроз, що підтверджує її придатність для використання у навчальних та дослідницьких цілях. Результати дослідження можуть бути використані для подальшого розвитку методів навчання та підвищення рівня захисту інформаційних систем від сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is intrusion detection systems (IDS)? How does it work? | fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system (date of access: 03.12.2024).
2. What is an intrusion prevention system (IPS)? | fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/what-is-an-ips (date of access: 04.11.2024).
3. Cyber range. Cyberbit. URL: https://www.cyberbit.com/platform/cyber-range/ (date of access: 02.12.2024).
4. Platform | cybersecurity training platform team readiness. RangeForce Cloud-Based Cyber Range | Cybersecurity Training. URL: https://www.rangeforce.com/platform (date of access: 02.12.2024).
5. X-Force cyber range | IBM. IBM - United States. URL: https://www.ibm.com/services/xforce-cyber-range (date of access: 02.12.2024).
6. Cisco: software, network, and cybersecurity solutions. Cisco. URL: https://www.cisco.com/c/dam/global/en_au/solutions/security/pdfs/cyber_range_aag_v2.pdf (date of access: 02.12.2024).
7. CYBER RANGES: cybersecurity exercises for training and capability development. CYBER RANGES. URL: https://www.cyberranges.com/ (date of access: 02.12.2024).
8. Gamified cybersecurity training solutions by Circadence. Circadence Corporation. URL: https://circadence.com/ (date of access: 02.12.2024).
9. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56. https://doi.org/10.31891/2219-9365-2024-79-7

10. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220. https://doi.org/10.31891/2219-9365-2024-80-26
11. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146. https://doi.org/10.62731/mcnd-24.05.2024.001
12. VMware vsphere | virtualization platform. VMware by Broadcom - Cloud Computing for the Enterprise. URL: https://www.vmware.com/products/cloud-infrastructure/vsphere (date of access: 03.12.2024).
13. Introduction to Hyper-V on Windows. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/ (date of access: 03.12.2024).
14. XenServer - secure, reliable, and high-performance virtualization platform. XenServer. URL: https://www.xenserver.com/ (date of access: 03.12.2024).
15. What is KVM?. Red Hat - We make open source technologies for the enterprise. URL: https://www.redhat.com/en/topics/virtualization/what-is-KVM (date of access: 03.12.2024).
16. Types of network attacks against confidentiality, integrity and avilability. Free Networking tutorials, System Administration Tutorials and Security Tutorials - omnisecu.com. URL: https://www.omnisecu.com/ccna-security/types-of-network-attacks.php (date of access: 12.11.2024).
17. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.
18. How do layer 3 DDoS attacks work? | L3 DDoS. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/layer-3-ddos-attacks/ (date of access: 12.11.2024).

19. MAC flooding attack. InfosecTrain. URL: https://www.infosectrain.com/blog/mac-flooding-attack/ (date of access: 03.12.2024).
20. Tymoshchuk, D., & Yatskiv, V. (2024). SLOWLORIS DDOS DETECTION AND PREVENTION IN REAL-TIME. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.
21. Ping (ICMP) flood DDoS attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/ (date of access: 12.11.2024).
22. What is IP spoofing? URL: https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/ (date of access: 12.11.2024).
23. Демчук, В., Тимощук, В., & Тимощук, Д. (2023). ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК. Collection of scientific papers «SCIENTIA», (November 24, 2023; Kraków, Poland), 130-130.
24. Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD АТАК НА DNS СЕРВЕР. Матеріали конференцій МНЛ, (3 листопада 2023 р., м. Вінниця), 177-178.
25. What is TCP reset attack (RST)?. Wallarm | Integrated App and API Security Platform. URL: https://www.wallarm.com/what/what-is-syn-spoofing-or-tcp-reset-attack (date of access: 03.12.2024).
26. HTTP flood attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/ (date of access: 04.11.2024).
27. DNS amplification attack. URL: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/ (date of access: 04.11.2024).
28. Lindemulder G., Kosinski M. What Is a Man-in-the-Middle (MITM) Attack? | IBM. IBM - United States. URL: https://www.ibm.com/think/topics/man-in-the-middle (date of access: 12.11.2024).

29. XCP-ng documentation | XCP-ng Documentation. XCP-ng documentation | XCP-ng Documentation. URL: https://docs.xcp-ng.org/ (date of access: 03.12.2024).
30. Cloud hosted router, CHR - routeros - mikrotik documentation. MikroTik Routers and Wireless - Support. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/18350234/Cloud+Hosted+Router+CHR (date of access: 02.12.2024).
31. Official ubuntu documentation. URL: https://help.ubuntu.com/ (date of access: 03.12.2024).
32. Kali docs | kali linux documentation. Kali Linux. URL: https://www.kali.org/docs/ (date of access: 03.12.2024).
33. Security Onion Documentation 2.4 documentation. URL: https://docs.securityonion.net/en/2.4/about.html#security-onion (date of access: 02.12.2024).
34. Suricata User Guide – Suricata 8.0.0-dev documentation. URL: https://docs.suricata.io/en/latest/ (date of access: 03.12.2024).
35. What is a DNS flood? | DNS flood DDoS attack. Cloudflare. URL: https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/ (date of access: 04.11.2024).
36. What is a brute force attack? | definition, types & how it works. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/brute-force-attack (date of access: 03.12.2024).
37. Kibana: explore, visualize, discover data | elastic. Elastic. URL: https://www.elastic.co/kibana (date of access: 03.12.2024).
38. Tymoshchuk, D., Yasniy, O., Maruschak, P., Iasnii, V., & Didych, I. (2024). Loading Frequency Classification in Shape Memory Alloys: A Machine Learning Approach. Computers, 13(12), 339.
39. Катренко Л.А., Катренко А.В. Охорона праці в галузі комп'ютинґу. Львів: Магнолія-2006. 2012. 544 с.

40. Шкідливий вплив персонального комп’ютера на здоров’я людини. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/21370/5363.pdf (дата звернення: 16.12.2023).
41. Як захиститися від синього світла на телефоні та ПК: простий алгоритм. URL: https://my.ua/news/cluster/2023-05-03-iak-zakhistitisia-vid-sinogo-svitla-na-telefoni-ta-pk-prostii-algoritm (дата звернення: 16.12.2023).

Додаток А Публікація

IVFWKI | European Scientific Platform

ΛΌΓΟΣ

DER SAMMLUNG WISSENSCHAFTLICHER ARBEITEN

ZU DEN MATERIALIEN DER
VII INTERNATIONALEN WISSENSCHAFTLICH-PRAKTISCHEN KONFERENZ

«GRUNDLAGEN DER MODERNEN WISSENSCHAFTLICHEN FORSCHUNG»

Zürich,
Schweiz

13. Dezember
2024

Zürich, Schweiz
«BOLESWA Publishers»

Ukraine
«UKRLOGOS Group»

2024

UDC 082:001
G 90

G 90 **Grundlagen der modernen wissenschaftlichen Forschung**: der Sammlung wissenschaftlicher Arbeiten **«ΛΌΓΟΣ»** zu den Materialien der VII internationalen wissenschaftlich-praktischen Konferenz, Zürich, 13. Dezember, 2024. Zürich-Vinnytsia: BOLESWA Publishers & UKRLOGOS Group LLC, 2024.

ISBN 978-617-8312-11-4
ISBN 978-2-8315-3467-1 (PDF)
DOI 10.36074/logos-13.12.2024

«UKRLOGOS Group» LLC, Ukraine
«BOLESWA Publishers», Schweizerische Eidgenossenschaft

Es werden Thesen von Berichten und Artikeln von Teilnehmern der VII internationalen wissenschaftlich-praktischen Konferenz «Grundlagen der modernen wissenschaftlichen Forschung», am 13. Dezember, 2024 in Zürich vorgestellt.

The conference is certified by Euro Science Certification Group (**Certificate № 22571 dated February 14, 2024**);

The conference is also included in the catalog of International Scientific Conferences by ResearchBib; and registered by State Scientific Institution «Ukrainian institute of scientific and technical expertise and information» in the database «Scientific and technical events of Ukraine» (**Certificate № 103 dated 5 January 2024**).

Bibliografische Beschreibungen der Konferenz Tagungsband sind von Google Scholar, CrossRef, OpenAIRE, OUCI, Scilit, Semantic Scholar, Mendeley, WarldCat und ORCID werden indiziert.

UDC 082:001

ISBN 978-617-8312-11-4
ISBN 978-2-8315-3467-1 (PDF)

Grundlagen der modernen
wissenschaftlichen Forschung

ABSCHNITT 18.
INFORMATIONSTECHNOLOGIEN UND –SYSTEME

DOI 10.36074/logos-13.12.2024.048

SECURITY ONION PLATFORM AS A TOOL FOR DETECTING AND ANALYSING CYBER THREATS

Vitaliy Tymoshchuk[1], Maksym Vorona[2], Andrii Dolinskyi[3], Viktoriia Shymanska[4]
Scientific supervisor: Dmytro Tymoshchuk[5]

1. First-level student of higher education
Faculty of Applied Information Technologies and Electrical Engineering
Ternopil Ivan Puluj National Technical University, UKRAINE
ORCID ID: 0009-0007-2858-9434

2. Second-level student of higher education
Faculty of Computer Information Systems and Software Engineering
Ternopil Ivan Puluj National Technical University, UKRAINE

3. Third-level student of higher education
Faculty of Computer Information Systems and Software Engineering
Ternopil Ivan Puluj National Technical University, UKRAINE
ORCID ID: 0009-0003-4230-0183

4. First-level student of higher education
Faculty of Computer Information Systems and Software Engineering
Ternopil Ivan Puluj National Technical University, UKRAINE

5. Senior lecturer at the Department of Cyber Security
Ternopil Ivan Puluj National Technical University, UKRAINE
ORCID ID: 0000-0003-0246-2236

Abstract. *The article discusses the use of the Security Onion platform for modelling cyber threats and evaluating the effectiveness of intrusion detection systems (IDS). Experiments have been conducted to simulate various types of attacks, such as SYN flood, brute-force, DNS flood, and DNS tunnelling, using Kali Linux tools. The results of attack detection using Suricata IDS are analysed and the data are visualised in Kibana. The results of the study demonstrate the effectiveness of using Security Onion as a comprehensive solution for monitoring, analysing, and responding to cyber threats.*

Introduction. The growing complexity and number of cyber threats requires effective tools to monitor, detect and respond to potential attacks. Intrusion

detection systems have become an integral part of cybersecurity strategy, providing the ability to identify and analyse suspicious activity on the network. However, to evaluate the effectiveness of such systems, it is necessary to simulate real cyber threats in a controlled environment. The Security Onion platform is a powerful tool that integrates a number of open source solutions for network traffic monitoring, anomaly detection, and incident analysis [1]. It combines Suricata IDS [2][3], Zeek network analyser [4], ELK (Elasticsearch, Logstash, Kibana) stack [5] and other tools, making it an effective solution for researching and implementing cybersecurity strategies.

The purpose of this article is to study the capabilities of the Security Onion platform for modelling various types of cyber threats and evaluating the effectiveness of intrusion detection systems. As part of the study, a series of experiments were conducted to simulate attacks, analyse their detection, and visualise the results.

Main part. This study used a comprehensive approach to modelling cyber threats and evaluating the effectiveness of IDSs using the Security Onion platform. A realistic laboratory environment was created to reproduce various types of attacks and analyse the system's response to them [6][7][8]. The lab environment consisted of three main components: the Security Onion platform, the Kali Linux attack system [9], and the Ubuntu Linux target server [10]. Security Onion acted as a threat monitoring and detection system, combining Suricata tools for network traffic analysis and Zeek for in-depth analysis of network behaviour. Kali Linux was used as a platform for attack simulation [11][12][13], providing a wide range of tools for generating malicious traffic. Ubuntu Linux was used as the target server for the attacks (Figure 1).

The configuration of the network interfaces was important to ensure the correct functioning of the test environment. Two network interfaces were configured in Security Onion. The first interface was used for management. This interface provided communication with other network components and access to administration tools. The second interface operated in promiscuous mode and was designed to capture all network traffic. This allowed Suricata to analyse the traffic without interfering with its transmission.The Kali Linux attack system was configured to simulate various types of attacks. The Ubuntu Linux server was configured with HTTP, SSH, and DNS services that were used as potential attack targets. This made it possible to simulate real-world scenarios where the server provides standard network services and can be vulnerable to different types of threats.

The Suricata and Zeek tools integrated into Security Onion were used to analyse network traffic and detect attacks. Suricata was configured using standard rules as well as additional rules created specifically for this study.

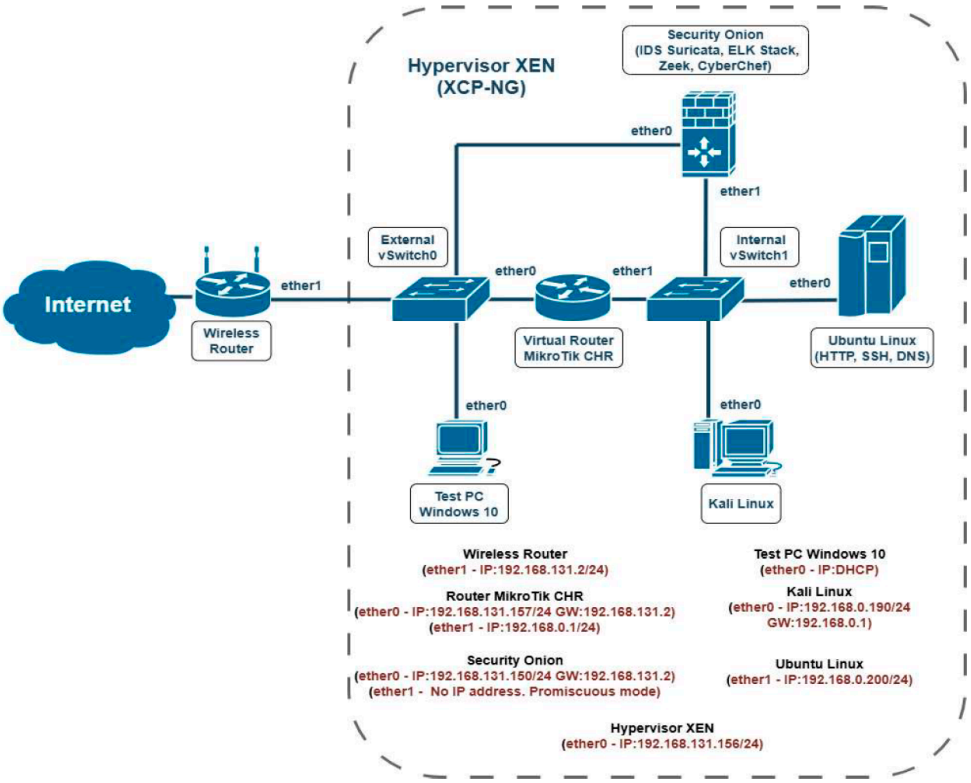

Fig. 1. **Laboratory testing environment**

Cyber threats were modelled by performing a series of experiments, each of which corresponded to a specific type of attack. The SYN flood attack [14] was modelled using hping3. The goal was to test whether Suricata could detect this attack and generate the appropriate alerts.

Figure 2 shows the Alerts tab in the Security Onion, which demonstrates the detection of a SYN Flood attack.

To detect specific threats, we created a custom rule in Suricata that responded to the transmission of a specific signature in traffic. This allowed us to test the system's ability to detect non-standard malicious elements in traffic and demonstrated the possibility of extending the rules to meet security needs. A brute-force attack [15] was simulated using hydra, which made multiple authentication attempts to an SSH server with different passwords. Suricata was configured to detect a large number of failed attempts to connect to the SSH port in a short period of time, which is typical for such attacks. The DNS attack simulation

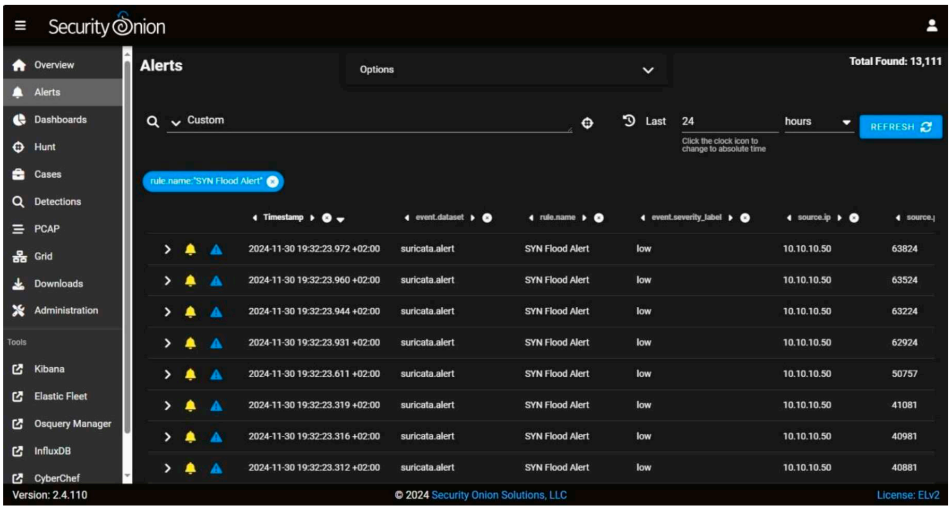

Fig. 2 **Detection of a SYN Flood attack in Suricata IDS**

included generating a large number of DNS queries to the DNS server [16] and making queries with long and atypical domain names to simulate DNS tunnelling.

The ELK stack (Elasticsearch, Logstash, Kibana) was used to store and analyse the collected data. Traffic analysed by Suricata was transferred to Elasticsearch, which provided efficient storage and quick search capabilities. Kibana was used to visualise data, create dashboards, and perform analytics (Figure 3).

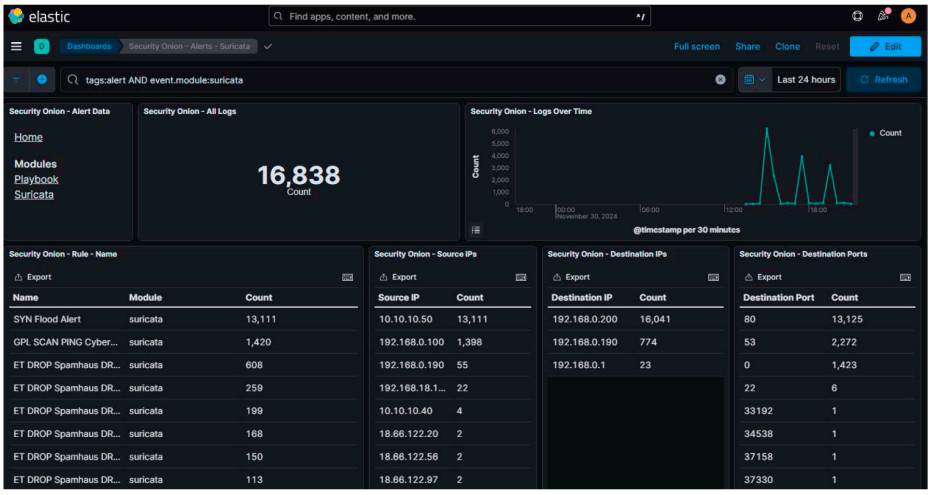

Fig. 3. **Visualisation of notifications in Kibana**

Discussion. The experiments provided important insights into the capabilities and limitations of the Security Onion platform for modelling cyber threats and evaluating IDS effectiveness. The integration of various open-source tools within Security Onion, such as Suricata, Zeek and Kibana, offers a comprehensive framework for monitoring, detecting and analysing network activity. The Suricata IDS has been proven to be effective in detecting a wide range of cyber threats using both signature and behavioural analysis. The successful identification of known attacks underlines the reliability of Suricata's predefined rules and signatures. In addition, the ability to create custom rules, as demonstrated by the detection of a specific 'virus' signature, underlines Suricata's flexibility in adapting to new threats and the specific needs of the organisation. The use of Kali Linux as an attack platform allowed us to realistically simulate the actions of attackers. Kibana's role in data visualisation and analysis proved to be extremely valuable. The ability to create customised dashboards and visualise large data sets helped identify trends in network traffic.

Experiments show that Security Onion, when properly configured and managed, can effectively detect and analyse a wide range of cyber threats. The integration of multiple tools within a single platform simplifies the deployment and management of network security monitoring solutions. The findings from this study contribute to a better understanding of IDS capabilities and improve network security in different environments.

Conclusions. The study demonstrates that the Security Onion platform is an effective tool for modelling cyber threats and evaluating intrusion detection systems. The integration of components such as Suricata, Zeek, and the ELK stack provides a comprehensive approach to monitoring, analysing, and responding to potential attacks. Experimental results confirm that configured Suricata IDS rules are able to effectively detect various types of attacks. Kibana's data visualisation facilitates in-depth incident analysis.

REFERENCES:

[1] Security Onion Documentation (n.d.). https://docs.securityonion.net/en/2.4/about.html#security-onion
[2] What is intrusion detection systems (IDS)? How does it work? | fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system
[3] Suricata User Guide — Suricata 8.0.0-dev documentation. (n.d.). Suricata User Guide — Suricata 8.0.0-dev documentation. https://docs.suricata.io/en/latest/
[4] The zeek network security monitor. (n.d.). Zeek. https://zeek.org/
[5] Elastic stack: (ELK) elasticsearch, kibana & logstash. (n.d.). Elastic. https://www.elastic.co/elastic-stack

[6] **ТИМОЩУК, Д.**, & **ЯЦКІВ, В.** (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56. https://doi.org/10.31891/2219-9365-2024-79-7

[7] **Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145**-146. https://doi.org/10.62731/mcnd-24.05.2024.001

[8] **ТИМОЩУК Д., ЯЦКІВ В., ТИМОЩУК В., & ЯЦКІВ Н (2024).** INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215–220. https://doi.org/10.31891/2219-9365-2024-80-26

[9] Kali docs | kali linux documentation. (n.d.). Kali Linux. https://www.kali.org/docs/

[10] Official ubuntu documentation. (n.d.). Official Ubuntu Documentation. https://help.ubuntu.com/

[11] **Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD АТАК НА DNS СЕРВЕР. Матеріали конференцій МНЛ, (3 листопада 2023 р., м. Вінниця), 177**-178.

[12] **Демчук, В., Тимощук, В., & Тимощук, Д. (2023). ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК. Collection of scientific papers «SCIENTIA», (November 24, 2023; Kraków,** Poland), 130-130.

[13] Tymoshchuk, D., & Yatskiv, V. (2024). SLOWLORIS DDOS DETECTION AND PREVENTION IN REAL-TIME. Collection of scientific papers **«ΛΌГОΣ»**, (August 16, 2024; Oxford, UK), 171-176. https://doi.org/10.36074/logos-16.08.2024.036

[14] SYN flood attack. Cloudflare. (n. d.) https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

[15] What is a brute force attack? | definition, types & how it works. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/brute-force-attack

[16] UDP flood attack. Cloudflare. (n.d.). https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/