ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення та блокування мережевих вторгнень у корпоративну мережу організації на прикладі Suricata»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дмитро СИРОТЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
СИРОТЕНКО Дмитро
(прізвище, ім'я)

Керівник доктор філософії СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API - Application Programming Interface

DNS - Domain Name System

DoS - Denial of Service

DDoS - Distributed Denial of Service

FTP - File Transfer Protocol

HTTP - HyperText Transfer Protocol

HTTPS - HyperText Transfer Protocol Secure

ICMP - Internet Control Message Protocol

IDS - Intrusion Detection System

IPS - Intrusion Prevention System

IP - Internet Protocol

JSON - JavaScript Object Notation

LAN - Local Area Network

NAT - Network Address Translation

Nmap - Network Mapper

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

VM - Virtual Machine

VPN - Virtual Private Network

YAML - YAML Ain’t Markup Language

ВСТУП

Актуальність дослідження. У сучасних умовах розвитку інформаційних технологій корпоративні мережі зазнають постійного впливу з боку зовнішніх та внутрішніх загроз інформаційній безпеці. Зростання кількості мережевих сервісів, використання хмарних технологій, віртуалізації, а також активне застосування віддаленого доступу суттєво ускладнюють процеси захисту інформаційних ресурсів організацій.

Особливу небезпеку становлять атаки на мережевому рівні, зокрема мережеве сканування, спроби несанкціонованого доступу, розвідка мережевої інфраструктури та інші дії, що передують цілеспрямованим атакам. У зв'язку з цим зростає потреба у впровадженні систем виявлення та запобігання вторгненням, здатних здійснювати глибокий аналіз мережевого трафіку та своєчасно реагувати на підозрілу активність.

Одним із перспективних рішень у сфері мережевої безпеки є система Suricata, яка належить до класу IDS/IPS та поєднує можливості сигнатурного аналізу, високої продуктивності й гнучкого налаштування правил. Використання Suricata в корпоративних мережах дозволяє не лише фіксувати факти порушення безпеки, але й активно блокувати мережеві атаки в режимі реального часу. Проте ефективність такої системи безпосередньо залежить від коректності її налаштування, адаптації до конкретної мережевої інфраструктури та правильного формування правил виявлення загроз.

Вищезазначене обумовлює актуальність теми даної кваліфікаційної роботи, основний зміст якої полягає у дослідженні можливостей та практичних аспектів використання системи Suricata для забезпечення захисту інформації в корпоративних мережах.

Об'єкт дослідження – Об'єктом дослідження є процес забезпечення інформаційної безпеки корпоративної мережі.

Предмет дослідження – Предметом дослідження є методи та засоби

виявлення і запобігання мережевим вторгненням у корпоративних мережах з використанням системи Suricata.

Мета роботи – Метою дипломної роботи є дослідження та практична реалізація системи захисту корпоративної мережі на основі Suricata, а також розробка рекомендацій щодо її впровадження та використання для підвищення рівня інформаційної безпеки.

Наукові завдання:

дослідити сучасні загрози інформаційній безпеці корпоративних мереж;

проаналізувати принципи функціонування систем виявлення та запобігання вторгненням;

розглянути існуючі рішення класу IDS/IPS та їх особливості;

дослідити архітектуру та функціональні можливості системи Suricata;

реалізувати тестовий стенд корпоративної мережі та налаштувати систему Suricata.

провести експериментальні дослідження з виявлення та блокування мережевих атак

розробити практичні рекомендації щодо впровадження Suricata в корпоративному середовищі

Методи дослідження – аналіз наукової та технічної літератури з питань інформаційної безпеки, вивчення експлуатаційної документації систем IDS/IPS, моделювання мережевих атак у тестовому середовищі, експериментальні дослідження роботи системи Suricata, а також аналіз та узагальнення отриманих результатів.

Практичне значення одержаних результатів: Отримані результати можуть бути використані фахівцями з кібербезпеки для підвищення ефективності виявлення та запобігання мережевим атакам у реальних умовах експлуатації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції “Актуальні проблеми кібербезпеки”, яка відбулася 29 жовтня 2025 в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1. Дослідження проблеми захисту інформації в корпоративних мережах

У сучасних умовах розвитку цифрової економіки корпоративні мережі стають фундаментом функціонування більшості організацій, незалежно від сфери їх діяльності. Вони забезпечують не лише передачу даних, а й підтримку ключових бізнес-процесів, взаємодію між підрозділами, інтеграцію з партнерськими сервісами, доступ до хмарних платформ та інфраструктурних рішень. Водночас стрімке зростання обсягів інформації, що циркулює в таких мережах, та підвищення цінності даних для бізнесу роблять корпоративні мережі привабливою ціллю для кіберзлочинців. Це зумовлює підвищення вимог до забезпечення їх захищеності та актуалізує дослідження проблеми безпеки корпоративних інформаційних систем [1].

Проблема захисту інформації в корпоративних мережах полягає не лише у протидії зовнішнім загрозам, але й у комплексному управлінні внутрішніми ризиками [5], що охоплюють технічні, організаційні та людські фактори. Сучасні мережі характеризуються високою динамічністю, гетерогенністю та відкритістю, що створює умови для появи численних векторів атаки. Зловмисники використовують широкий спектр інструментів: від елементарного підбору паролів до складних багаторівневих APT-кампаній, що включають соціальну інженерію, експлуатацію вразливостей нульового дня, приховане проникнення в мережу та використання легітимних протоколів і служб для маскування шкідливої активності.

Одним із ключових викликів, що постають перед сучасними корпоративними мережами, є зростання складності їхніх топологій [9]. Якщо раніше корпоративна інфраструктура зазвичай була централізованою та мала чітко визначені межі, то сьогодні більшість організацій використовує віддалені робочі місця, мобільні пристрої, хмарні додатки та зовнішні API-сервіси. Це призводить до розширення

периметра безпеки, розмивання його кордонів і збільшення кількості точок доступу, які необхідно контролювати. Наявність розподілених філій, VPN-каналів, гібридних хмарних середовищ і IoT-компонентів ускладнює застосування традиційних методів захисту та потребує переходу до адаптивних моделей безпеки.

Корпоративні мережі функціонують у середовищі, де обсяги трафіку постійно зростають, а набір використовуваних протоколів розширюється. Наявність у мережі високошвидкісних потоків даних, таких як відеоконференції, потокове передавання медіаконтенту, операції з великими масивами даних, транзакції в реальному часі, ускладнює оперативний аналіз трафіку без зниження продуктивності. Крім того, значна частина сучасного мережевого трафіку є зашифрованою, що унеможливлює його простий аналіз за допомогою традиційних методів глибокої інспекції пакетів без розшифрування. Відповідно, заходи безпеки повинні орієнтуватися не лише на аналіз вмісту пакетів, а й на поведінкові та статистичні характеристики трафіку [10].

Суттєвою загрозою для корпоративних мереж є також експлуатація системних і програмних вразливостей. Незважаючи на наявність регулярних оновлень, у великих інфраструктурах часто залишаються застарілі або неправильно налаштовані компоненти, які можуть бути використані зловмисниками для проникнення в мережу або отримання привілейованого доступу. Багато атак здійснюються шляхом автоматизованого сканування інтернет-простору на наявність відкритих портів, сервісів або систем із відомими експлойтами. Така активність може залишатися непоміченою без спеціалізованих засобів аналізу трафіку.

Особливо небезпечною є тенденція до використання зловмисниками легітимних інструментів адміністрування та комунікацій - так званих «living-off-the-land» технік. У цьому випадку вторгнення практично не створює ознак, характерних для класичних атак, і тому не фіксується традиційними антивірусами або фаєрволами. Наприклад, зловмисник може використовувати стандартні командлети PowerShell, внутрішні протоколи, сервери віддаленого доступу або навіть штатні бізнес-процеси компанії для розповсюдження шкідливої активності.

Людський фактор залишається одним із найкритичніших аспектів проблеми захисту корпоративних мереж. Помилки персоналу, нехтування правилами інформаційної безпеки, недостатній рівень обізнаності щодо сучасних загроз, використання слабких або повторюваних паролів, випадкове відкриття шкідливих вкладень електронної пошти - усе це створює додаткові ризики для безпеки. Навіть найскладніші технічні засоби не здатні гарантувати повний захист за умов відсутності культури безпеки серед працівників [2].

Слід зазначити, що забезпечення безпеки корпоративних мереж ускладнюється також необхідністю підтримки продуктивності та безперебійної роботи систем. У багатьох випадках запровадження більш жорстких заходів захисту (наприклад, глибокої інспекції пакетів, аналізу всіх HTTP-сесій або постійного моніторингу внутрішнього трафіку) може призвести до збільшення затримок, надмірного споживання ресурсів або зниження доступності сервісів. Тому організації змушені шукати компроміс між рівнем безпеки і продуктивністю мережі.

У відповідь на розвиток кіберзагроз організації все частіше використовують багаторівневі підходи до забезпечення кібербезпеки, що поєднують периметровий захист, сегментацію мережі, аналіз логів, системи SIEM, політики доступу Zero Trust та інші інструменти. Водночас особливу роль у цьому комплексі відіграють системи виявлення та запобігання вторгненням, які забезпечують глибокий аналіз мережевого трафіку та здатні виявляти як відомі, так і нові види атак.

Системи IDS/IPS дозволяють здійснювати моніторинг пакетів у режимі реального часу, виявляти ознаки небажаної активності, блокувати або сповіщати про підозрілі дії та реагувати на інциденти відповідно до визначених політик. Вони застосовують різні методи аналізу, включаючи сигнатурний, поведінковий, статистичний і гібридний. Завдяки поєднанню різних підходів такі системи можуть забезпечити високий рівень точності та оперативності виявлення загроз.

У контексті корпоративних мереж особливої уваги заслуговує система Suricata, яка поєднує можливості IDS/IPS та мережевого моніторингу. Вона здатна працювати в умовах високої пропускної здатності, використовувати

багатопотокову архітектуру, аналізувати метадані протоколів, застосовувати сигнатури правил та визначати аномалії у поведінці трафіку. Suricata підтримує розширені можливості парсингу протоколів, інтеграцію з SIEM-системами, збором статистики, автоматизацію реагування та режим активного блокування.

Важливість систем на кшталт Suricata зумовлена тим, що вони здатні забезпечити захист у ситуаціях, коли інші засоби безпеки виявляються недостатніми. Наприклад, фаєрвол не зможе виявити складну атаку в межах легітимного HTTPS-з'єднання, антивірус не зреагує на експлуатацію мережевої вразливості, а сегментація мережі не запобігатиме розповсюдженню трафіку, подібного до легітимного. У таких випадках саме IDS/IPS стає критично важливим елементом багаторівневого захисту.

Таким чином, дослідження проблеми захисту інформації в корпоративних мережах показує, що забезпечення безпеки є багатокомпонентним, комплексним процесом, що включає технічні, організаційні та поведінкові аспекти. Його ефективність залежить від узгодженої роботи всіх складових системи, своєчасного реагування на інциденти, постійного моніторингу трафіку та здатності адаптуватися до нових типів загроз. З огляду на це системи IDS/IPS, зокрема Suricata, набувають особливої значущості, оскільки дозволяють оперативно виявляти вторгнення, аналізувати поведінкові закономірності трафіку та запобігати атакам на ранніх етапах їх розвитку. Саме вони стають ключовим елементом стратегії кібербезпеки корпорацій у сучасних умовах [3].

1.2. Аналіз сучасних кіберзагроз та уразливостей у корпоративному середовищі

Сучасні корпоративні мережі є складними, багатокомпонентними інформаційними системами, які об'єднують різні типи обладнання, програмного забезпечення, серверні інфраструктури, локальні та віддалені підрозділи організації. З одного боку, це забезпечує високу гнучкість та ефективність бізнес-процесів, а з іншого - створює нові точки вразливості та розширює поверхню

можливих атак. Цифровізація бізнесу, перехід до хмарних сервісів, активне використання мобільних робочих місць і збільшення кількості IoT-пристроїв значно підвищили складність корпоративного ландшафту безпеки. У таких умовах кількість кіберінцидентів не лише зростає, але й змінюється за характером - атаки стають багатовекторними, тривалими в часі, добре спланованими і часто орієнтованими на конкретну організацію або окремі її підрозділи.

Одним із ключових чинників, що впливає на формування сучасного середовища загроз, є глобальна взаємопов'язаність корпоративних мереж. Багато компаній, прагнучи зменшити витрати та підвищити ефективність, активно використовують сервіси віддаленої обробки даних, сервіси SaaS, PaaS, IaaS, а також різноманітні хмарні інструменти. У результаті дані компанії часто розпорошені між локальними серверами та зовнішніми дата-центрами, а доступ до них здійснюється через численні канали бездротового та дротового зв'язку. Це збільшує залежність організації від безпеки сторонніх платформ і створює ситуацію, коли компрометація одного хмарного середовища може спричинити кризу у всій корпоративній інфраструктурі.

Однією з найхарактерніших сучасних загроз залишаються атаки на рівні мережевої взаємодії, що використовують вразливості стандартних протоколів. Наприклад, протокол ARP, який застосовується для прив'язки IP-адрес до фізичних адрес MAC, не передбачає механізмів автентифікації. Зловмисник може надсилати фальшиві ARP-повідомлення з метою зміни таблиць відповідності в мережі, що дає змогу перехоплювати трафік, проводити MITM-атаки, перенаправляти користувачів або інфікувати їхні пристрої шкідливим програмним забезпеченням. Подібні вразливості є і в протоколі DNS, який не має вбудованої перевірки достовірності записів, що дозволяє використовувати техніки DNS-spoofing та DNS-cache poisoning. У таких випадках користувачів перенаправляють на підроблені веб-ресурси, де вони вводять конфіденційні дані, не підозрюючи про фальсифікацію.

Значну загрозу становлять атаки типу DoS та DDoS, метою яких є виведення з ладу серверів або мережевої інфраструктури шляхом перевантаження їх кількістю

запитів. Оскільки сучасні підприємства значною мірою залежать від онлайн-сервісів, навіть короткочасна недоступність ресурсу може призвести до фінансових збитків, репутаційних втрат і зриву операційної діяльності. В останні роки атаки DDoS набули особливо великого масштабу завдяки використанню ботнетів, що складаються з інфікованих пристроїв користувачів, серверів та IoT-обладнання. Ці ботнети можуть налічувати сотні тисяч вузлів, що робить атаки надзвичайно потужними та складними для нейтралізації традиційними засобами.

Окремим напрямом загроз є швидке поширення різноманітного шкідливого програмного забезпечення. Найбільш небезпечними серед них є програми-вимагачі, які шифрують файли на робочих станціях і серверах, після чого зловмисники вимагають викуп за їх розблокування. Різновиди таких атак здатні швидко поширюватися мережею, вражаючи сотні пристроїв протягом кількох хвилин. Особливо небезпечними є цілеспрямовані атаки на великі компанії, коли зловмисники попередньо вивчають інфраструктуру, підбирають точку входу та атакують системи, що містять найбільш цінні дані. У багатьох випадках ransomware викликає тривалі простої бізнесу, втрату комерційної інформації, руйнацію баз даних та значні фінансові збитки.

На додаток до програм-вимагачів, велике розповсюдження отримали троянські програми, які створюють бекдори, крадуть креденціали або забезпечують повноцінний віддалений доступ до системи. Деякі трояни працюють у прихованому режимі роками, передаючи інформацію зловмисникам або дозволяючи їм здійснювати приховані мережеві операції. Часто такі шкідливі програми маскуються під легітимні процеси операційної системи, що значно ускладнює їх виявлення без застосування спеціалізованих засобів моніторингу мережевого трафіку.

Окремої уваги потребує проблема фішингових атак - однієї з найефективніших форм соціальної інженерії. Сучасні фішингові кампанії набули високого рівня персоналізації: зловмисники досліджують структуру компанії, імена співробітників, характер внутрішньої комунікації, особливості робочого середовища. У результаті листи можуть виглядати абсолютно легітимними,

оскільки в них використані справжні назви відділів, реальні підписи менеджерів або навіть внутрішні документи. Атаки spear phishing, спрямовані на окремих співробітників із доступом до важливої інформації, особливо небезпечні, адже вони використовують індивідуальний підхід і психологічні прийоми.

Важливим джерелом загроз залишається внутрішній фактор. Незалежно від рівня технічного захисту, людина залишається найслабкішою ланкою будь-якої системи безпеки. У корпоративних мережах істотні ризики становлять випадкові помилки співробітників, такі як відкриття заражених файлів, використання слабких паролів, неправильне налаштування серверів або передача конфіденційної інформації через незахищені канали. Крім цього, можливі і навмисні дії внутрішніх працівників - крадіжка даних, саботаж, встановлення шкідливих програм або змова з третіми сторонами. Внутрішні атаки часто найскладніше виявити, оскільки працівники мають легітимний доступ до мережі, знають її структуру та можуть приховувати свої дії, використовуючи адміністративні привілеї.

Розвиток корпоративної IT-інфраструктури постійно породжує нові типи уразливостей. Наприклад, неправильна сегментація мережі призводить до того, що зловмисник, отримавши доступ до одного вузла, може легко переміститися до інших частин системи. Використання застарілого мережевого обладнання або пристроїв зі слабким програмним забезпеченням створює можливості для експлуатації відомих уразливостей, які роками залишаються невиправленими. І навіть коли компанія впроваджує сучасні рішення, такі як VPN, сервери віртуалізації або системи хмарного зберігання, вони часто залишаються неправильно налаштованими або використані без належного контролю доступу, що відкриває нові можливості для атак.

У сучасному корпоративному середовищі надзвичайно великою стала кількість IoT-пристроїв: датчики, камери відеонагляду, принтери, системи контролю доступу. Багато з них виробляються без належного рівня безпеки, мають стандартні паролі, старі прошивки або відсутність механізмів оновлення. Зловмисники можуть використовувати такі пристрої для отримання доступу до внутрішньої мережі або як частину ботнетів для DDoS-атак.

Таким чином, сучасні кіберзагрози (Таблиця 1.1.) характеризуються масштабністю, високою технічною складністю, прихованістю та адаптивністю. Кіберзлочинці використовують багатокрокові атаки, комбінують експлойти, соціальну інженерію та шкідливе ПЗ, а також застосовують інструменти для обходу систем захисту та уникнення виявлення. Корпоративні мережі потребують комплексного підходу до безпеки, що включає моніторинг трафіку, аналіз поведінки систем, оперативне виявлення аномалій та впровадження таких рішень, як сучасні IDS/IPS-системи.

Таблиця 1.1.

Класифікація основних загроз корпоративних мереж

Тип загрози	Джерело загрози	Характеристика загрози	Можливі наслідки
Мережеві атаки	Зовнішній порушник	Сканування портів, експлуатація вразливостей протоколів, DoS/DDoS-атаки	Порушення доступності сервісів, зниження продуктивності мережі
Шкідливе програмне забезпечення	Зовнішній порушник	Ransomware, троянські програми, бекдори	Втрата або шифрування даних, компрометація систем
Соціальна інженерія	Зовнішній порушник	Фішинг, spear phishing, підробка службових повідомлень	Компрометація облікових даних, несанкціонований доступ
Внутрішні загрози	Внутрішній користувач	Зловживання привілеями, помилки персоналу, навмисні дії	Витік інформації, порушення цілісності даних
Атаки на IoT-пристро	Змішане джерело	Використання слабких паролів, застарілих прошивок	Проникнення в мережу, участь у ботнетах
MITM та DNS-атаки	Зовнішній порушник	Підміна трафіку, перехоплення даних	Крадіжка конфіденційної інформації

Саме тому актуальним є використання Suricata - універсального, адаптивного та високопродуктивного інструменту для аналізу мережевого трафіку, який здатен своєчасно виявляти загрози та блокувати атаки.

1.3. Аналіз існуючих підходів до виявлення та запобігання мережевим

вторгненням

Проблематика виявлення та запобігання мережевим вторгненням є однією з найважливіших у сфері сучасної кібербезпеки, оскільки корпоративні мережі стають дедалі складнішими, а кіберзагрози - більш агресивними, інтелектуальними та динамічними. Злочинці активно застосовують автоматизовані інструменти, шифрування, методи обходу систем безпеки, а також розподілені та багатокрокові атаки. Тому розробка ефективних підходів до виявлення й блокування вторгнень є основою побудови надійної системи захисту корпоративного середовища.

На ранніх етапах розвитку кібербезпеки основним методом протидії небажаному трафіку був класичний міжмережевий екран, який виконував фільтрацію пакетів на основі статичних правил. Проте з часом стало очевидно, що просте порівняння заголовків пакетів не дозволяє виявляти складні атаки, такі як SQL-ін’єкції, експлуатація уразливостей, розповсюдження шкідливих програм або сканування внутрішніх сервісів. Саме тоді було сформовано концепцію систем виявлення вторгнень, які дозволяють здійснювати аналіз трафіку на більш глибокому рівні. Згодом, із розвитком технологій, IDS-системи трансформувалися в IPS - системи запобігання вторгнень, які не лише фіксували шкідливу активність, але й могли блокувати її в режимі реального часу.

Сьогодні всі підходи до виявлення мережевих атак можна умовно поділити на кілька основних напрямів: сигнатурний аналіз, статистичний та аномалійний аналіз, поведінковий аналіз, кореляція подій, застосування машинного навчання та гібридні методи. Кожен із цих підходів використовується у сучасних системах IDS/IPS, але ступінь їхньої ефективності залежить від характеру мережевої архітектури, типів трафіку та ризиків, властивих конкретному корпоративному середовищу [12].

Сигнатурний метод залишається однією з найбільш точних технік для виявлення атак, які вже були класифіковані фахівцями. Він ґрунтується на використанні бази сигнатур - структурованих описів атак або характерних ознак, що містять шаблони трафіку, регулярні вирази, бінарні сигнатури або характерні

послідовності байтів. Цей підхід широко реалізований у Snort, Suricata та інших популярних системах. Його точність і зрозумілий механізм роботи є незаперечними перевагами. Однак швидкість розвитку кіберзлочинності, часті модифікації коду шкідливих програм і наявність нових векторів атак значно знижують ефективність сигнатурного аналізу в умовах реального часу. Крім того, сигнатурні методи не здатні виявляти атаки, які здійснюються вперше або мають мінімальні відмінності від легітимного трафіку.

Аномалійний аналіз став відповіддю на обмеження сигнатурних методів. Він передбачає побудову моделі “нормальної” поведінки мережі, після чого аналізуються будь-які відхилення від цього профілю. Наприклад, збільшення обсягу вихідного трафіку, нетипові запити DNS, нехарактерне зростання кількості з'єднань або різкі зміни в активності користувачів можуть свідчити про приховану атаку. Такий підхід здатний виявляти нові типи загроз, включаючи атаки нульового дня, ботнет-активність і lateral movement - рух зловмисника мережею після початкового проникнення. Проте складність і динамічність корпоративних мереж призводять до великої кількості хибних спрацювань. Для коректної роботи аномалійного аналізу необхідні значні обчислювальні ресурси та ретельне налаштування.

Поведінковий аналіз став важливим компонентом сучасних рішень безпеки, особливо в контексті внутрішніх загроз. Цей підхід не обмежується аналізом пакетів, а розглядає логічні дії користувача: підключення до серверів, які він раніше не використовував, доступ до незвичних директорій, спроби модифікації системних файлів, нетипові операції з великими обсягами даних тощо. Поведінковий аналіз забезпечує можливість виявляти інсайдерські атаки, компрометацію облікових даних та триваючі приховані атаки. Водночас складність нормальної поведінки у великих організаціях вимагає ретельної адаптації моделі до специфіки бізнес-процесів.

Окреме місце займає кореляція подій, яка використовується у таких системах, як SIEM. SIEM-платформи збирають дані з різних джерел - мережевого обладнання, серверів, робочих станцій, систем контролю доступу, хмарних сервісів

та додатків. Кореляційний аналіз дозволяє виявляти складні, багаторівневі атаки, які складаються з кількох дій, що окремо можуть виглядати нешкідливо. Наприклад, підвищення прав доступу після підозрілого входу, а потім масове копіювання даних може свідчити про атаки типу Data Exfiltration. Хоча SIEM-системи є потужним інструментом, їхнє впровадження потребує високого рівня експертизи і значних ресурсів [14].

Сучасні підходи активно включають методи машинного навчання. Завдяки алгоритмам класифікації, кластеризації та нейронним мережам системи безпеки стають здатними самостійно виявляти закономірності, які складно або неможливо описати вручну. Алгоритми навчаються на великих масивах даних і здатні розпізнавати складні патерни атак, приховані взаємозв'язки та нетипову поведінку. Проте використання ML-технологій може бути ризикованим без належного налаштування: неправильні дані для навчання або упередженість моделі можуть призводити до некоректних результатів.

У сучасному корпоративному середовищі все більшого поширення набувають гібридні підходи (рисунок 1.1), які поєднують сигнатурний, аномалійний, поведінковий аналізи та ML-моделі. Комбінація методів дозволяє компенсувати недоліки окремих підходів. Наприклад, сигнатурні правила точно виявляють відомі атаки, а аномалійні механізми помічають нові загрози. Поведінковий аналіз контролює внутрішню активність, а кореляційні механізми виявляють складні багатокрокові інциденти.

Серед інструментів, які реалізують гібридний підхід, важливе місце займає Suricata. Ця система здатна одночасно аналізувати трафік на високих швидкостях, застосовувати сигнатурний аналіз, виявляти аномалії, аналізувати протоколи на рівні додатків, працювати з потоковими файлами та інтегруватися з SIEM-рішеннями. Можливість роботи у режимах IDS та IPS, підтримка багатопотоковості та сучасних форматів журналів робить Suricata одним із найефективніших рішень для побудови систем виявлення та запобігання вторгненням у корпоративних мережах [9].

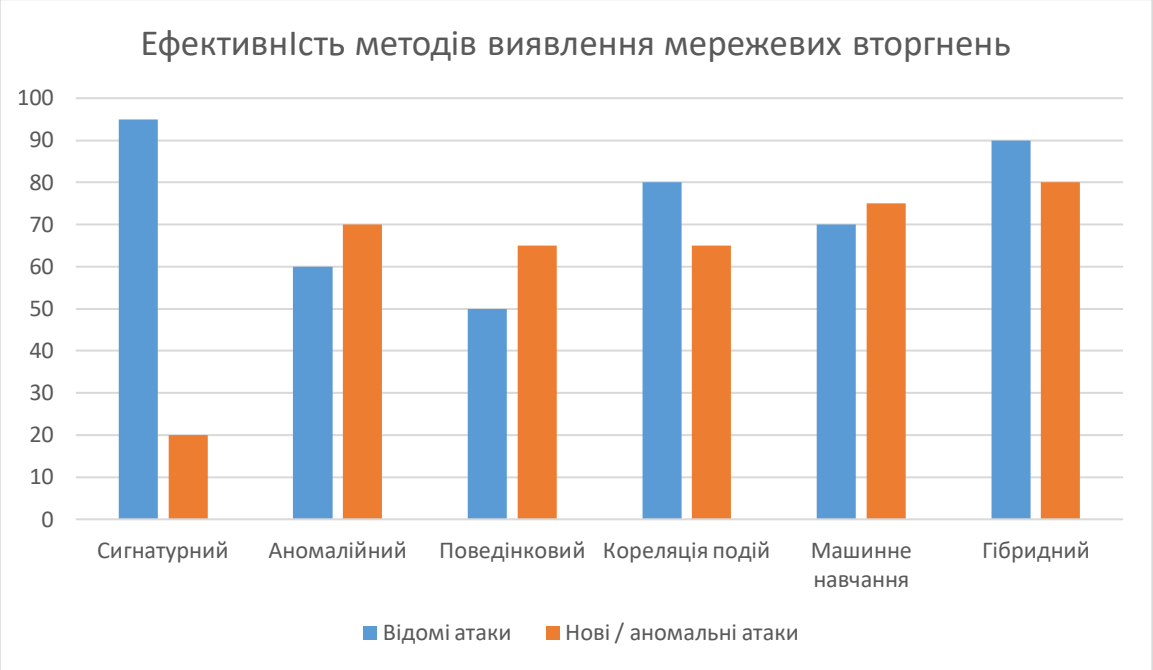

Рис. 1.1. Сорівняння ефективності методів виявлення мережевих вторгнень

Саме тому аналіз підходів до захисту від вторгнень логічно переходить до дослідження можливостей та архітектури Suricata, що розглядатиметься у наступному розділі.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ І БЛОКУВАННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ НА БАЗІ SURICATA

2.1. Призначення та основні функції системи Suricata

Система Suricata є одним із провідних інструментів сучасної кібербезпеки для виявлення та запобігання мережевим вторгненням у корпоративних мережах. Вона поєднує високу продуктивність, багаторівневий аналіз мережевого трафіку, масштабованість та можливості інтеграції з іншими компонентами систем безпеки, що робить її ефективним засобом захисту інформаційної інфраструктури. Основна мета використання Suricata полягає у забезпеченні комплексного захисту від широкого спектра кіберзагроз, включаючи відомі та нові атаки, шкідливе програмне забезпечення, фішингові кампанії, атаки типу DDoS, внутрішні загрози, експлуатацію вразливостей мережевого обладнання та програмного забезпечення, а також складні багатокрокові інциденти.

Suricata була розроблена для роботи у великих корпоративних та дата-центрових мережах, де обсяг трафіку може перевищувати сотні гігабіт на секунду. Високопродуктивна багатопотокова архітектура дозволяє обробляти тисячі одночасних підключень, не знижуючи точність аналізу. Паралельна обробка пакетів забезпечує можливість ефективного використання сучасних багатоядерних процесорів, що критично важливо для великих корпоративних мереж, де навіть короткі затримки в обробці трафіку можуть призвести до збоїв у роботі бізнес-додатків або втрати критичних даних. Suricata підтримує роботу на різних операційних системах, включаючи Linux, Windows та BSD, що забезпечує гнучкість при впровадженні у гетерогенних корпоративних середовищах.

Основні функції Suricata охоплюють комплексний аналіз мережевого трафіку на декількох рівнях. Система здатна виконувати сигнатурний аналіз, аномалійний та поведінковий аналіз, а також глибокий протокольний аналіз (рисунок 1.2.). Сигнатурний аналіз дозволяє виявляти відомі атаки за допомогою бази сигнатур,

яка постійно оновлюється через репозиторії Emerging Threats та інші джерела. Це забезпечує швидке реагування на нові загрози та підтримку високої точності виявлення відомих атак, таких як сканування портів, експлуатація відомих вразливостей, поширення шкідливих програм або несанкціоновані спроби доступу до критичних ресурсів.

Рис. 2.1. Види аналізу

Аномалійний аналіз у Suricata дозволяє виявляти загрози, що раніше не були класифіковані, та складні багатокрокові атаки. Цей підхід передбачає побудову базового профілю мережевої активності, який включає нормальний обсяг трафіку, типи протоколів, характер використання портів, частоту запитів та взаємодію між пристроями. Будь-які відхилення від цього профілю, наприклад, нехарактерний обсяг даних, нетипові протокольні комбінації або раптові підключення до невідомих ресурсів, можуть свідчити про потенційну загрозу. Аномалійний аналіз особливо ефективний для виявлення складних атак, внутрішніх загроз та прихованої активності шкідливого програмного забезпечення [5], включно з ботнет-мережами та рухом зловмисника у внутрішній мережі.

Поводінковий аналіз доповнює сигнатурний та аномалійний підходи, фокусуючись на поведінці користувачів та системних об’єктів. Suricata здатна відстежувати нетипові дії, такі як спроби доступу до критичних серверів,

модифікація системних файлів або робота з великою кількістю конфіденційних даних, що не відповідає типовим сценаріям діяльності. Такий аналіз є важливим для запобігання інсайдерських атак та компрометації облікових даних.

Однією з ключових функцій Suricata є підтримка режиму IPS, який дозволяє не лише виявляти загрози, а й блокувати їх у реальному часі. Завдяки можливості інтеграції з мережею через фаєрволи, TAP-порти або inline-моніторинг, система може оперативно зупиняти шкідливий трафік, відключати компрометовані сесії або блокувати конкретні IP-адреси. Це особливо важливо для корпоративних мереж, де навіть короткочасне проникнення може призвести до значних фінансових втрат, порушення роботи бізнес-процесів або витоку конфіденційної інформації.

Suricata підтримує детальний аналіз протоколів високого рівня, включаючи HTTP, TLS, DNS, SMTP, FTP, SMB та інші. Це дозволяє виявляти складні атаки на рівні додатків, наприклад SQL-ін’єкції, XSS, підробку HTTP-запитів або аномалії у TLS-з’єднаннях. Декодування протоколів у реальному часі дає змогу ідентифікувати атаки навіть у випадках, коли шкідливий трафік маскується під легітимні запити або зашифрований контент, що значно підвищує рівень захисту корпоративної мережі.

Ще однією суттєвою перевагою Suricata є інтеграція з платформами SIEM та SOC. Система може генерувати детальні журнали подій у форматах, сумісних із SIEM-платформами, включаючи JSON, EVE та стандартні syslog-формати [9]. Це забезпечує можливість централізованого збору даних, кореляції подій, аналізу трендів та прогнозування потенційних атак. Інтеграція з SIEM дозволяє аналітикам SOC швидко реагувати на інциденти, відстежувати ескалацію загроз та здійснювати аудит безпеки корпоративної мережі.

Suricata також підтримує масштабованість і гнучкість розгортання. Вона може працювати у невеликих локальних мережах, великих офісах з сотнями користувачів або масштабних дата-центрах з тисячами підключень. Можливість багатопотокової обробки, розподіленого розгортання та балансування навантаження дозволяє збільшувати продуктивність без втрати точності виявлення. Крім того, Suricata підтримує різні режими роботи: пасивний IDS для

моніторингу, активний IPS для блокування атак і гібридний режим, що поєднує обидва підходи.

Важливим аспектом є здатність системи працювати з зашифрованим трафіком. Suricata може аналізувати TLS/SSL-з'єднання, виконувати класифікацію протоколів, розпізнавати аномальні сценарії та виявляти підозрілу активність у шифрованому потоці даних. Це особливо актуально в сучасних корпоративних мережах, де більшість трафіку передається через HTTPS або інші захищені канали.

Завдяки поєднанню сигнатурного, аномалійного та поведінкового аналізу, підтримці режимів IDS/IPS, багатопотоковості, інтеграції з SIEM та аналізу протоколів високого рівня, Suricata є універсальним і високоефективним інструментом для захисту корпоративних мереж від сучасних кіберзагроз. Вона дозволяє організаціям впроваджувати багаторівневу систему безпеки, контролювати мережевий трафік, оперативно реагувати на інциденти та знижувати ризик компрометації інформаційних ресурсів.

2.2. Основні компоненти архітектури системи Suricata та принципи її роботи

Архітектура системи Suricata розроблена з урахуванням вимог сучасних корпоративних мереж, де обсяг трафіку, швидкість його обробки та складність мережевих протоколів можуть досягати високих значень. Головна мета архітектури - забезпечити одночасно високу продуктивність, точність виявлення загроз, масштабованість та можливість інтеграції з іншими компонентами безпеки. Suricata поєднує в собі традиційні підходи до виявлення атак на основі сигнатур, аномалійний та поведінковий аналіз, а також глибокий аналіз протоколів на рівні додатків. Висока ефективність системи досягається завдяки багатопотоковій обробці, модульній архітектурі та підтримці паралельного аналізу трафіку.

Архітектура Suricata складається з кількох основних компонентів, кожен із яких виконує конкретні функції, спрямовані на виявлення та запобігання мережевих загроз. До основних компонентів належать:

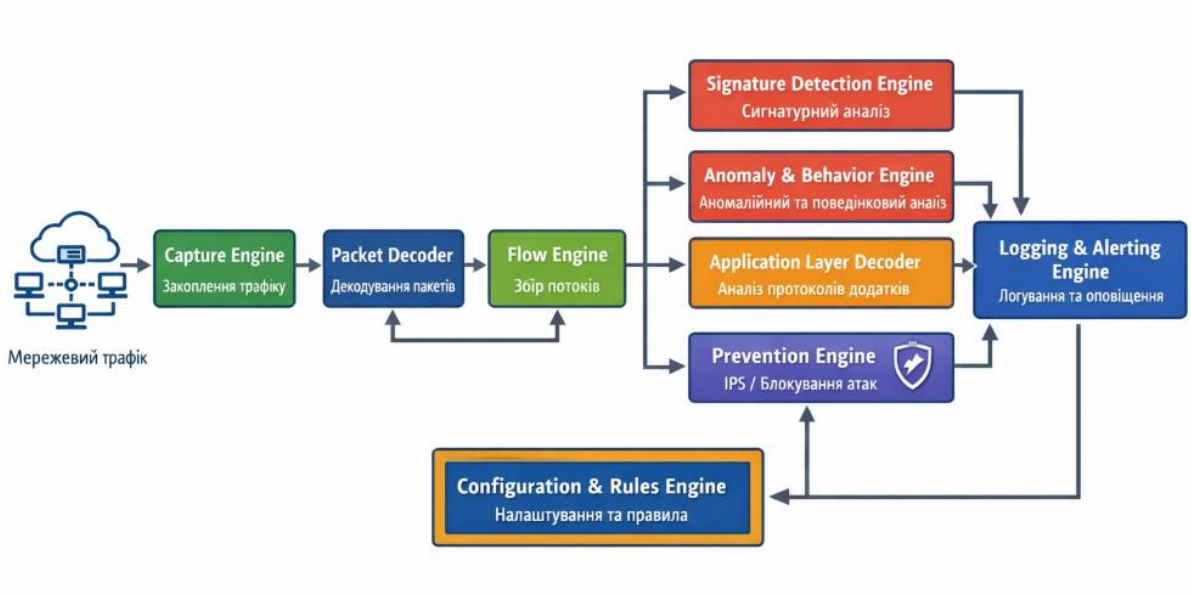

Рис. 2.2. Модульна архітектура Suricata

Мережевий інтерфейс та модуль захоплення трафіку. Цей компонент відповідає за прийом та збереження всього мережевого трафіку, що надходить до системи. Suricata підтримує роботу з різними типами мережевих інтерфейсів, включно з Ethernet, Wi-Fi та віртуальними інтерфейсами у хмарних середовищах. Модуль захоплення трафіку здійснює первинну фільтрацію пакетів, відкидаючи дублікати та пакети, що не відповідають критеріям аналізу. Завдяки цьому зменшується навантаження на систему та підвищується швидкість обробки.

Декодер пакетів. Декодер є критично важливим елементом архітектури, оскільки забезпечує правильне розпізнавання протоколів на всіх рівнях мережевої взаємодії. Suricata підтримує широкий спектр мережевих протоколів - TCP, UDP, ICMP, HTTP, TLS, DNS, SMTP, FTP, SMB та інші. Декодер аналізує заголовки пакетів і визначає, до якого протоколу належить кожен пакет, після чого передає дані для подальшого аналізу. На цьому етапі відбувається первинна класифікація пакетів та підготовка їх до глибшої обробки, включно з визначенням сегментації та повторної збірки потоків даних.

Модуль збору потоків. Flow Engine відповідає за збір та обробку мережевих потоків. Потік визначається як серія пакетів, що належать до одного з’єднання між двома вузлами мережі. Модуль збирає пакети в цілісні потоки, що дозволяє проводити аналіз на рівні сесій, а не лише окремих пакетів. Це особливо важливо

для виявлення складних атак, таких як багатоетапні ін’єкції, DDoS-атаки або компрометація внутрішніх серверів, де шкідливі дії можуть бути розподілені по кількох пакетах або сеансах.

Модуль сигнатурного аналізу. Сигнатурний двигун є серцем традиційного IDS. Він порівнює мережеві потоки з базою сигнатур, що включає відомі шаблони атак. Suricata використовує формат правил, сумісний із Snort, що дозволяє легко імпортувати готові сигнатури та додавати власні. База сигнатур оновлюється регулярно, що забезпечує своєчасне реагування на нові загрози. Сигнатурний модуль може аналізувати пакети на рівні протоколів, заголовків і корисного навантаження, дозволяючи виявляти як відомі атаки, так і спроби використання відомих вразливостей у програмному забезпеченні.

Модуль аномалійного та поведінкового аналізу. Цей компонент відповідає за виявлення нових, невідомих загроз. Він аналізує відхилення від нормальної поведінки мережевої інфраструктури, включно з частотою з’єднань, обсягом переданих даних, нетиповими протоколами або нестандартною активністю користувачів. Поведінковий аналіз дозволяє виявляти інсайдерські атаки, підозрілу активність облікових записів та складні сценарії компрометації, що не підпадають під відомі сигнатури.

Модуль логування та інтеграції з SIEM. Suricata забезпечує детальне журналювання всіх подій, що дозволяє проводити кореляцію інцидентів, аудит та аналіз безпеки. Логи можуть генеруватися у форматах EVE JSON, syslog або CSV, що робить їх сумісними з більшістю SIEM-систем, таких як Splunk, ELK Stack або Graylog. Цей модуль також відповідає за генерацію оповіщень у режимі реального часу, що дозволяє аналітикам SOC швидко реагувати на потенційні загрози.

Модуль IPS та блокування атак. У режимі IPS Suricata не лише виявляє загрози, але й активно блокує їх у реальному часі. Вона може розривати сесії, блокувати IP-адреси або конкретні потоки даних через інтеграцію з фаєрволами та мережевим обладнанням. Ця функція критично важлива для корпоративних мереж, де затримка у реагуванні навіть на короткий час може призвести до витоку конфіденційної інформації або порушення бізнес-процесів.

Модуль аналізу протоколів високого рівня. Suricata здатна виконувати глибокий аналіз протоколів додатків, таких як HTTP, SMTP, DNS, FTP, SMB, TLS та інших. Це дозволяє виявляти складні атаки на рівні додатків, включно з SQL-ін’єкціями, підробкою запитів, аномальним використанням API або шкідливою активністю в зашифрованих потоках. Модуль декодує пакети, збирає корисне навантаження та передає його на подальший аналіз іншими двигунами системи.

Модуль розширення та налаштування. Suricata підтримує детальне налаштування правил і профілів роботи, що дозволяє адаптувати систему під специфіку конкретної корпоративної мережі. Модуль дозволяє визначати пріоритети правил, режим роботи IDS/IPS, обробку хибнопозитивних спрацювань та інтеграцію з зовнішніми джерелами правил.

Принцип роботи Suricata базується на багатопоточному паралельному обробленні мережевого трафіку. Кожен пакет спочатку надходить у модуль захоплення, потім декодується і направляється у Flow Engine для збору сесій. Після цього потоки аналізуються сигнатурним і аномалійним двигунами, а результати передаються у модуль логування та оповіщення. У режимі IPS додатково виконується блокування атакуючих пакетів та сесій.

Архітектура Suricata дозволяє реалізувати масштабовані багаторівневі системи захисту, де різні модулі можуть працювати на окремих серверах або віртуальних середовищах, а дані з різних точок мережі централізовано аналізуються у SIEM. Це дозволяє організаціям реалізувати ефективний моніторинг трафіку, оперативне реагування на інциденти та гнучке налаштування системи під власні потреби.

Архітектура Suricata спроектована таким чином, щоб забезпечувати ефективну обробку великих обсягів трафіку у реальному часі без втрати точності виявлення загроз. Один із ключових механізмів, що забезпечує це - мультипоточність. Suricata може розподіляти обробку пакетів між декількома ядрами процесора, що дозволяє одночасно аналізувати тисячі потоків і збільшувати продуктивність системи майже пропорційно кількості доступних обчислювальних ресурсів. Механізм багатопоточності реалізований у вигляді декількох робочих

потоків: окремі потоки відповідають за захоплення та декодування пакетів, інші - за збір потоків та сигнатурний аналіз, ще інші - за логування та генерацію оповіщень. Такий поділ дозволяє уникнути «вузьких місць» у системі та забезпечує стабільну роботу навіть при пікових навантаженнях.

Flow Engine у Suricata є одним із ключових компонентів для коректного виявлення складних атак. Потоки визначаються як серії пакетів, що належать до однієї сесії TCP, UDP або ICMP, а також специфічних протоколів високого рівня. Flow Engine збирає пакети у сесії, визначає порядок їх надходження, перевіряє контрольні суми та забезпечує повторну збірку сегментованих пакетів. Цей підхід дозволяє виявляти атаки, які поширюються через кілька пакетів або навіть через різні підключення до серверів. Наприклад, SQL-ін’єкція, яка надсилається по шматках даних через кілька TCP-пакетів, буде виявлена саме завдяки Flow Engine.

Сигнатурний модуль Suricata реалізує паралельне порівняння потоків із базою правил, що дозволяє швидко визначати відомі загрози. Система підтримує як статичні, так і динамічні сигнатури, включаючи сигнатури Emerging Threats та власні правила адміністратора. Кожне правило описує умови, за яких трафік вважається підозрілим або шкідливим, включаючи специфікацію протоколу, портів, IP-адрес та ключових слів у пакеті. Suricata застосовує оптимізовані алгоритми пошуку та порівняння, що дозволяє обробляти великий обсяг правил без значного зниження продуктивності.

Аномалійний та поведінковий аналіз у Suricata реалізований як додатковий рівень контролю, який доповнює сигнатурний аналіз. Цей механізм дозволяє системі виявляти атаки нульового дня, а також складні багатоступеневі інциденти. Наприклад, якщо користувач раптово починає надсилати великі обсяги даних на зовнішні сервери або звертається до нетипових портів і служб, система генерує оповіщення. Поведінковий аналіз також інтегрується з Flow Engine, що дозволяє відстежувати активність на рівні сесій та виявляти аномалії у взаємодії між вузлами мережі.

Важливим аспектом архітектури є механізм інтеграції з SIEM та іншими системами безпеки. Suricata генерує події у форматі JSON, який містить детальну

інформацію про джерело та призначення пакету, протокол, тип атаки, час події, а також контекст мережевої сесії. Ці дані можуть бути відправлені до централізованої платформи для подальшого аналізу, кореляції інцидентів та аудиту. Таке рішення дозволяє аналітикам SOC проводити багаторівневий аналіз подій, відстежувати тенденції атак та прогнозувати потенційні загрози, що є критично важливим для корпоративних мереж із великою кількістю користувачів та розгалуженою топологією.

Модуль IPS Suricata дозволяє здійснювати активне блокування атак у режимі реального часу. Система може розривати сесії TCP, блокувати IP-адреси джерел атаки, фільтрувати підозрілі потоки та взаємодіяти з фаєрволами для обмеження доступу. Це дозволяє оперативно реагувати на атаки та мінімізувати шкоду, завдану інформаційним ресурсам компанії. Інтеграція з inline-фаєрволами або мережевими TAP-портами забезпечує можливість безпосереднього контролю трафіку без його затримки.

Suricata також забезпечує аналітичні можливості щодо протоколів високого рівня, включаючи HTTP, SMTP, DNS, FTP, SMB та TLS. Модуль декодування протоколів розпізнає заголовки та корисне навантаження, визначає нетипові або шкідливі запити, проводить аналіз шифрованого трафіку та інтегрується з сигнатурним і аномалійним двигунами для комплексного виявлення атак. Це дозволяє виявляти складні атаки на рівні додатків, включно з ін’єкціями, підробкою запитів, аномальним використанням API та шкідливим завантаженням файлів.

Масштабованість Suricata дозволяє реалізувати розподілену обробку трафіку у великих мережах. Можна розгортати декілька екземплярів системи на різних сегментах мережі та збирати дані централізовано для кореляції подій. Це дозволяє організаціям забезпечувати моніторинг на всіх рівнях мережевої інфраструктури та зменшувати ризик пропуску атак через локальні вузькі місця.

Окрему увагу варто приділити гнучкості конфігурації. Suricata дозволяє налаштовувати правила для конкретних підмереж, серверів, груп користувачів, визначати пріоритети для різних типів атак, а також задавати поведінку системи при хибнопозитивних спрацюваннях. Це дозволяє адаптувати систему під

специфіку корпоративного середовища, забезпечуючи баланс між точністю виявлення та швидкістю роботи мережі.

У практичному використанні Suricata показує високу ефективність у захисті корпоративних мереж. Вона дозволяє виявляти атаки на ранніх етапах, запобігати розповсюдженню шкідливого програмного забезпечення, контролювати активність користувачів та забезпечувати аудит мережевої безпеки. Завдяки багаторівневій архітектурі, модульності та інтеграції з зовнішніми системами, Suricata стає ключовим елементом сучасної системи кіберзахисту корпоративної мережі.

Suricata реалізує комплексну обробку мережевих подій у режимі реального часу, що дозволяє ефективно виявляти і блокувати атаки, навіть якщо вони мають складну або приховану структуру. Після того, як пакет або потік пройшов через декодер і Flow Engine, наступним етапом є аналіз за правилами IDS/IPS. Кожне правило визначає умови, при яких трафік вважається підозрілим або шкідливим. Правила включають специфікацію протоколу, IP-адреси джерела і призначення, порти, ключові слова у корисному навантаженні та типи сесій. Suricata дозволяє комбінувати умови за логічними операторами «і» та «або», що дає змогу створювати складні правила для багатоступеневих атак.

Механізм кореляції потоків і пакетів дозволяє системі об’єднувати розрізнені події в єдину інцидентну картину. Наприклад, атака типу «розподілена SQL-ін’єкція» може складатися з десятків або сотень пакетів, які поодинці не викликають підозри. Flow Engine збирає ці пакети у потоки, а сигнатурний та аномалійний модулі аналізують послідовність подій. У разі виявлення підозрілої активності система генерує оповіщення або блокує потік у режимі IPS. Такий підхід забезпечує високу точність виявлення складних атак, які складно розпізнати при аналізі окремих пакетів.

Для підвищення продуктивності Suricata використовує оптимізацію обробки правил. Правила структуруються у дерева або хеш-таблиці, що дозволяє швидко визначати, які правила застосовуються до конкретного пакету. Модуль потоків забезпечує ефективне повторне використання зібраної інформації, а багатопоточна архітектура дозволяє обробляти одночасно тисячі потоків без зниження швидкості

системи. Крім того, Suricata підтримує класифікацію правил за пріоритетами, що дозволяє обробляти критичні сигнатури першими та забезпечувати пріоритетне реагування на серйозні загрози.

У корпоративних мережах Suricata може працювати у гібридному режимі IDS/IPS, де частина системи виконує пасивний моніторинг, а частина - активне блокування атак. Це дозволяє балансувати між швидкістю реакції та мінімізацією хибнопозитивних спрацювань. Наприклад, нові правила або експериментальні сигнатури можна спершу тестувати у пасивному режимі, відстежуючи їх ефективність, а після підтвердження надійності переводити у активний IPS.

Suricata забезпечує також декодування та аналіз зашифрованого трафіку, що є критично важливим у сучасних корпоративних мережах, де більшість трафіку передається через HTTPS. Система може витягувати інформацію про сертифікати, протоколи шифрування та інші атрибути, що дозволяє виявляти підозрілі з’єднання та аномальні шаблони поведінки навіть у шифрованих потоках. Поєднання цієї функції з сигнатурним і поведінковим аналізом дозволяє виявляти складні атаки типу MITM, SSL Stripping або підробку сертифікатів.

Особливу увагу в архітектурі Suricata приділено логуванню та інтеграції з зовнішніми системами. Всі події, виявлені системою, можуть бути збережені у форматах EVE JSON, syslog або CSV. JSON-формат містить детальну інформацію про джерело та призначення трафіку, тип протоколу, застосоване правило, оцінку загрози та контекст сесії. Ці дані можуть передаватися до SIEM, де відбувається кореляція подій, побудова графів атак, створення дашбордів і прогнозування потенційних загроз. Завдяки цьому аналітики SOC отримують повну картину мережевої активності та можуть оперативно реагувати на інциденти, відстежувати багаторівневі атаки та проводити аудит безпеки.

Suricata також підтримує масштабовану багаторівневу інфраструктуру, де кілька екземплярів системи можуть бути розгорнуті на різних сегментах мережі або у хмарних середовищах. Кожен екземпляр обробляє локальний трафік і передає події до центрального агрегатора для аналізу. Такий підхід дозволяє організаціям реалізовувати централізовану систему моніторингу для великих корпоративних

мереж, зменшуючи ризик пропуску атак через локальні вузькі місця та забезпечуючи стійкість до відмов компонентів.

У практичних сценаріях використання Suricata дозволяє ефективно виявляти та блокувати різноманітні види атак:

- Сканування портів і розвідку мережі - модуль сигнатурного аналізу виявляє спроби сканування та передає інформацію в лог та SIEM.

- Атаки типу DoS/DDoS - Flow Engine аналізує обсяги трафіку та частоту з'єднань, а IPS-модуль блокує підозрілі потоки.

- Використання відомих вразливостей - сигнатурний модуль порівнює пакети з базою сигнатур експлойтів, виявляючи атаки на сервери та прикладне ПО.

- Внутрішні загрози та компрометація користувачів - поведінковий модуль відстежує нетипову активність, наприклад спроби доступу до критичних ресурсів або витік конфіденційних даних.

- Атаки на рівні додатків - аналіз протоколів високого рівня дозволяє виявляти SQL-ін'єкції, XSS, підробку HTTP-запитів та інші складні сценарії.

Suricata дозволяє гнучко налаштовувати систему під потреби конкретної організації, визначати пріоритети правил, обмежувати хибнопозитивні спрацювання, налаштовувати логування та оповіщення, а також інтегруватися з фаєрволами та іншими компонентами безпеки для активного блокування атак.

Таким чином, архітектура Suricata є модульною, масштабованою та гнучкою, що дозволяє ефективно виявляти і блокувати відомі та невідомі загрози, здійснювати глибокий аналіз мережевого трафіку, забезпечувати інтеграцію з SIEM та SOC, а також підтримувати високу продуктивність навіть у великих корпоративних мережах. Всі ці особливості роблять Suricata одним із найефективніших інструментів для захисту корпоративних інформаційних ресурсів.

2.3. Порядок функціонування системи Suricata під час виявлення мережевих атак

Функціонування системи Suricata у корпоративних мережах базується на комплексному, багаторівневому підході до виявлення загроз, що включає захоплення мережевого трафіку, його аналіз на рівні пакетів і потоків, застосування правил IDS/IPS та інтеграцію з системами централізованого моніторингу. Основною метою Suricata є оперативне виявлення та блокування атак, що може відбуватися як на рівні окремих мережевих пакетів, так і на рівні сесій або складних поведінкових патернів.

Перший етап роботи системи - захоплення мережевого трафіку. Suricata підтримує інтеграцію з різними мережевими інтерфейсами, включно з фізичними Ethernet-портами, TAP-портами, SPAN-портами та віртуальними мережевими адаптерами у хмарних середовищах. Модуль захоплення пакує отримані дані у внутрішні структури для подальшого аналізу та виконує первинну фільтрацію, відкидаючи дублікати, некоректні пакети або трафік, який не підлягає моніторингу відповідно до налаштувань адміністратора. Такий підхід дозволяє зменшити навантаження на систему та оптимізувати обробку великих обсягів трафіку.

Наступний етап - декодування та класифікація пакетів. Декодер Suricata розпізнає тип протоколу, визначає заголовки і корисне навантаження, а також визначає сегментацію пакетів для подальшого аналізу. На цьому етапі відбувається розпізнавання TCP/UDP-сесій, обробка ICMP-пакетів та визначення протоколів високого рівня, таких як HTTP, DNS, SMTP, TLS, FTP або SMB. Коректне декодування критично важливе для точного виявлення атак, оскільки неправильне визначення протоколу або структури пакету може призвести до пропуску шкідливого трафіку.

Після декодування пакетів Flow Engine формує потоки даних, що належать до однієї сесії або з’єднання. Потоки збираються за джерелом та призначенням, портами та протоколом, після чого передаються на сигнатурний і аномалійний аналіз. Потоковий підхід дозволяє системі виявляти багатоступеневі атаки, де шкідлива активність розподілена між кількома пакетами або сесіями. Наприклад, атака на базу даних через розбиті SQL-запити або DDoS-атака з багатьох джерел буде правильно ідентифікована завдяки агрегованому аналізу потоків.

Після формування потоків даних Suricata переходить до сигнатурного аналізу, який є основним інструментом для виявлення відомих мережевих атак. Модуль сигнатурного аналізу порівнює пакети та потоки з базою правил IDS/IPS. Кожне правило описує умови, при яких трафік вважається підозрілим або шкідливим. Правила можуть містити деталі протоколу, IP-адресу джерела та призначення, порти, специфічні значення заголовків, ключові слова у корисному навантаженні, а також різноманітні логічні комбінації. Такий підхід дозволяє точно ідентифікувати відомі атаки, наприклад спроби експлуатації вразливостей у веб-серверах, SMTP-сервісах, базах даних або внутрішніх корпоративних застосунках.

Для підвищення ефективності, Suricata використовує оптимізовані алгоритми пошуку та порівняння, які дозволяють швидко обробляти великі бази правил навіть у середовищах із високим трафіком. Система застосовує паралельне порівняння пакетів із сигнатурами, класифікує правила за пріоритетами та забезпечує пріоритетне реагування на критичні загрози. Така оптимізація особливо важлива для корпоративних мереж із великою кількістю користувачів та серверів, де затримка в обробці навіть кількох мілісекунд може бути критичною для безпеки.

Паралельно із сигнатурним аналізом, Suricata виконує аномалійний та поведінковий аналіз. Цей механізм дозволяє виявляти нові, невідомі загрози або складні атаки нульового дня, які не мають конкретних сигнатур. Поведінковий двигун аналізує обсяги трафіку, частоту з’єднань, нетипові запити, використання портів, а також незвичайну активність облікових записів. Наприклад, якщо користувач раптово починає надсилати великі обсяги даних на зовнішні сервери або отримує доступ до ресурсів, до яких раніше не мав доступу, система генерує оповіщення. Інтеграція аналізу потоків із поведінковим двигуном дозволяє виявляти атаки, які розподілені по багатьох пакетах і сесіях.

Наступним етапом є обробка подій та генерація оповіщень. Коли модулі виявляють потенційно шкідливий трафік, інформація про інцидент фіксується у форматі EVE JSON або інших лог-файлах, сумісних із SIEM. Логи містять деталі події: IP-адресу джерела та призначення, протокол, застосоване правило, оцінку загрози, час події та контекст сесії. Ці дані дозволяють аналітикам SOC проводити

кореляцію подій, відстежувати багаторівневі атаки, прогнозувати потенційні загрози та проводити аудит безпеки.

У режимі IPS Suricata не лише виявляє загрози, а й виконує їх активне блокування. Механізм блокування може включати розрив TCP-сесій, блокування IP-адрес джерел атак, фільтрацію підозрілих потоків та взаємодію з фаєрволами. Це дозволяє оперативно реагувати на атаки та мінімізувати потенційну шкоду, запобігаючи розповсюдженню шкідливого ПЗ, витоку конфіденційної інформації або порушенню критичних бізнес-процесів. Механізм IPS інтегрується із багатопоточними потоками обробки трафіку, що забезпечує високу продуктивність і низьку затримку.

Важливим аспектом є аналіз протоколів високого рівня. Suricata здатна декодувати HTTP, SMTP, DNS, FTP, SMB, TLS та інші протоколи, що дозволяє виявляти атаки на рівні додатків, включно з SQL-ін’єкціями, XSS, підробкою HTTP-запитів та шкідливими файлами. Декодер протоколів передає дані сигнатурному та аномалійному двигунам, забезпечуючи багаторівневий контроль і точне виявлення складних атак.

Масштабованість системи дозволяє реалізувати розподілену обробку трафіку: кілька екземплярів Suricata можуть працювати на різних сегментах корпоративної мережі, обробляючи локальний трафік і передаючи події до центрального агрегатора для кореляції та аналізу. Це забезпечує централізоване управління безпекою у великих мережах і зменшує ризик пропуску атак через локальні вузькі місця.

Suricata також підтримує гнучку конфігурацію правил IDS/IPS, що дозволяє адаптувати систему під специфіку конкретної організації. Можна задавати пріоритети правил, визначати обмеження на хибнопозитивні спрацювання, налаштовувати логування та оповіщення для різних сегментів мережі, груп серверів або окремих користувачів. Така конфігурація дозволяє забезпечити баланс між точністю виявлення загроз та ефективністю роботи мережі.

У реальному корпоративному середовищі функціонування Suricata відбувається за комплексним сценарієм, який включає кілька етапів обробки

трафіку та реагування на загрози. Перш за все, пакети трафіку надходять на модуль захоплення, де відбувається первинна фільтрація та підготовка для подальшого аналізу. Пакети, що пройшли цей етап, направляються до декодера протоколів, який визначає їх тип, сегментацію та специфіку протоколу. Це дозволяє Suricata коректно розпізнавати TCP/UDP-сесії, ICMP-повідомлення та високорівневі протоколи, такі як HTTP, DNS, SMTP, TLS, FTP і SMB.

Після декодування відбувається агрегація пакетів у потоки, яка забезпечує цілісність сесійного аналізу. Потоки можуть складатися з десятків або сотень пакетів, що належать до одного з'єднання або дії користувача. Flow Engine контролює порядок пакетів, перевіряє контрольні суми, обробляє повторно сегментовані пакети та формує повні потоки для подальшого аналізу. Саме на цьому етапі система здатна виявляти багатопакетні та багатоступеневі атаки, наприклад, SQL-ін'єкції, DDoS-атаки або внутрішні витоки даних, які розподілені по кількох сесіях.

Далі потоки направляються на сигнатурний та поведінковий аналіз. Сигнатурний модуль порівнює трафік із базою правил, де кожне правило описує умови для виявлення конкретної атаки. При цьому Suricata використовує оптимізовані алгоритми пошуку і порівняння для роботи з великою кількістю правил, що дозволяє забезпечити високу продуктивність навіть при обробці трафіку гігабітних мереж. Аномалійний і поведінковий модуль аналізує нетипові патерни активності, включаючи частоту запитів, обсяги переданих даних, доступ до нестандартних портів та використання нетипових протоколів. Такий підхід дозволяє виявляти атаки нульового дня, внутрішні загрози та складні багатоступеневі сценарії компрометації.

Suricata забезпечує оперативне оповіщення та логування, що є критично важливим для корпоративних мереж. Події зберігаються у форматі EVE JSON, syslog або CSV і можуть передаватися до централізованих SIEM-систем, таких як Splunk, ELK Stack або Graylog. Логи містять деталі: IP-адресу джерела і призначення, протокол, застосоване правило, оцінку загрози, час події, контекст сесії та тип потоку. Це дозволяє аналітикам SOC виконувати кореляцію подій,

побудову графів атак, моніторинг трендів та прогнозування потенційних загроз.

У режимі IPS Suricata виконує активне блокування атак. При виявленні загрози система може розривати TCP-сесії, блокувати IP-адреси атакуючих вузлів, фільтрувати підозрілі потоки та взаємодіяти з фаєрволами або мережевим обладнанням для обмеження доступу. Наприклад, у випадку DDoS-атаки модуль IPS здатний блокувати потоки від конкретних джерел, не впливаючи на легітимний трафік, завдяки інтеграції з Flow Engine та поведінковим алгоритмам, що визначають аномальні патерни.

Suricata дозволяє використовувати сценарії роботи на рівні правил для різних сегментів мережі.

Приклади таких сценаріїв включають:

- Виявлення сканування портів:

alert tcp any any -> 192.168.1.0/24 any (msg:"Port scan detected"; flags:S; threshold:type threshold, track by_src, count 20, seconds 60; sid:1000001; rev:1;)

Це правило визначає спроби сканування TCP-портів, коли одна IP-адреса робить більше 20 спроб протягом хвилини.

- Блокування спроб SQL-ін’єкції:

drop tcp any any -> 192.168.1.100 80 (msg:"SQL Injection Attempt"; content:"UNION SELECT"; nocase; sid:1000002; rev:1;)

У режимі IPS Suricata блокує пакет із підозрілим SQL-запитом, що дозволяє запобігти компрометації веб-сервера.

- Виявлення підозрілих з’єднань до зовнішніх серверів

alert udp any any -> any 53 (msg:"Suspicious DNS query"; content:"maliciousdomain.com"; sid:1000003; rev:1;)

Це правило виявляє підозрілі DNS-запити, що можуть свідчити про активність шкідливого ПЗ.

Suricata дозволяє комбінувати сигнатурні правила з поведінковими алгоритмами, що забезпечує багаторівневий захист. Наприклад, поведінковий модуль може виявляти аномальні обсяги трафіку на нестандартних портах, а сигнатурний - перевіряти конкретний тип пакету на наявність відомої експлойт-

активності.

Масштабованість та модульність Suricata дозволяють організаціям розгортати систему у розподіленому режимі, де декілька екземплярів обробляють локальний трафік, а центральний агрегатор корелює події. Це знижує навантаження на окремі вузли та забезпечує повний контроль над безпекою корпоративної мережі.

В цілому, порядок функціонування Suricata можна представити як послідовність етапів:

1. Захоплення трафіку з мережевого інтерфейсу.
2. Декодування пакетів і визначення протоколів.
3. Формування потоків і обробка сесій.
4. Сигнатурний та аномалійний аналіз.
5. Генерація логів та оповіщень у реальному часі.
6. Активне блокування атак у режимі IPS.
7. Інтеграція з SIEM для централізованого аналізу та кореляції подій.

Такий підхід забезпечує повний контроль над мережею, швидке реагування на загрози та захист корпоративних ресурсів від широкого спектру атак, включно з внутрішніми загрозами та складними зовнішніми атаками.

3 ТЕХНОЛОГІЯ РЕАЛІЗАЦІЇ СИСТЕМИ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ ВТОРГНЕНЬ У КОРПОРАТИВНІЙ МЕРЕЖІ

3.1. Проєктування архітектури системи Suricata для корпоративної мережі

Метою даного підрозділу є розробка та обґрунтування тестового стенду для дослідження роботи системи виявлення та запобігання мережевим вторгненням Suricata у корпоративному середовищі. Стенд використовується для моделювання типових мережевих атак та аналізу реакції IDS/IPS у контрольованих умовах.

Для забезпечення відтворюваності експерименту та мінімізації апаратних витрат було обрано підхід віртуалізації, що дозволяє моделювати корпоративну мережу без використання фізичного обладнання.

Для реалізації тестового середовища було використано платформу віртуалізації Oracle VirtualBox. У середовищі віртуалізації розгорнуто дві віртуальні машини на базі операційної системи Ubuntu Server: сервер моніторингу з установленою системою Suricata та сервер-імітацію порушника (attacker), призначений для генерації мережевих атак.

Рис. 3.1. Початок встановлення серверу Suricata

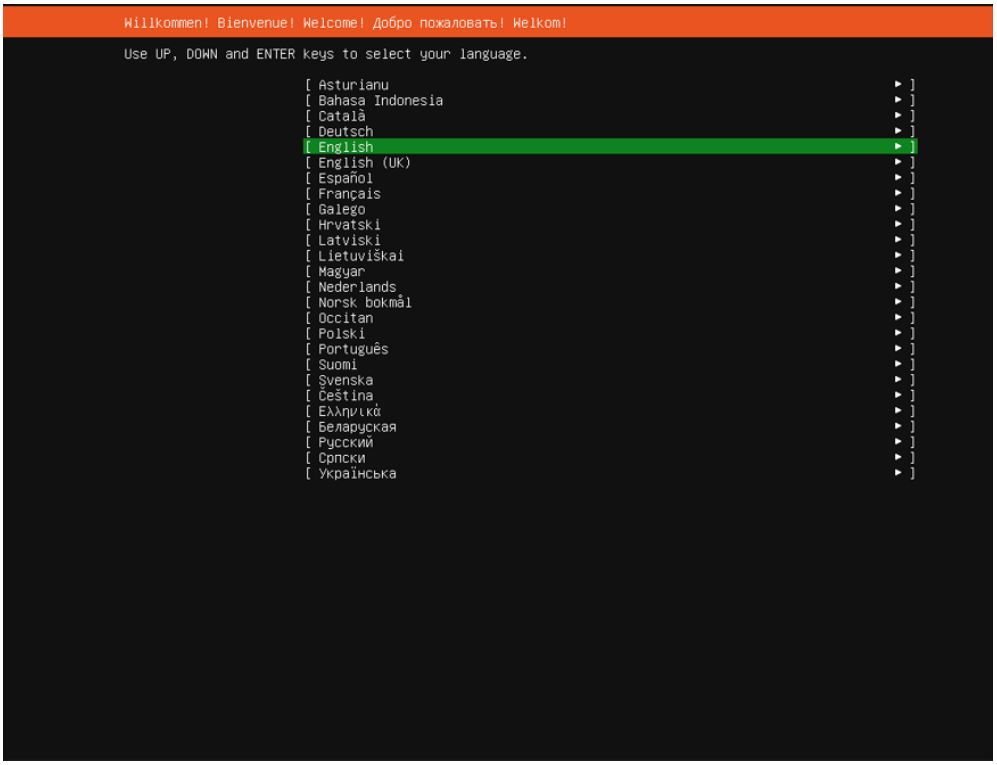

Рис. 3.2. Перший етап встановлення серверу Suricata

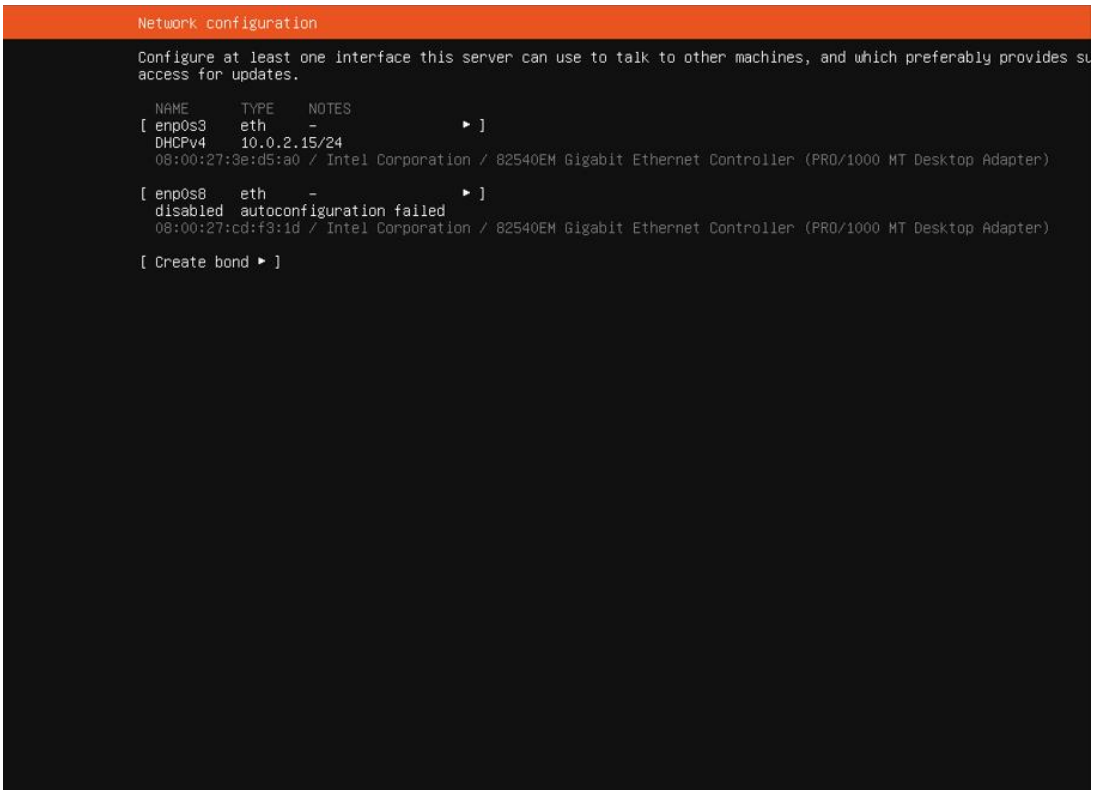

Рис. 3.3 Другий етап встановлення серверу Suricata

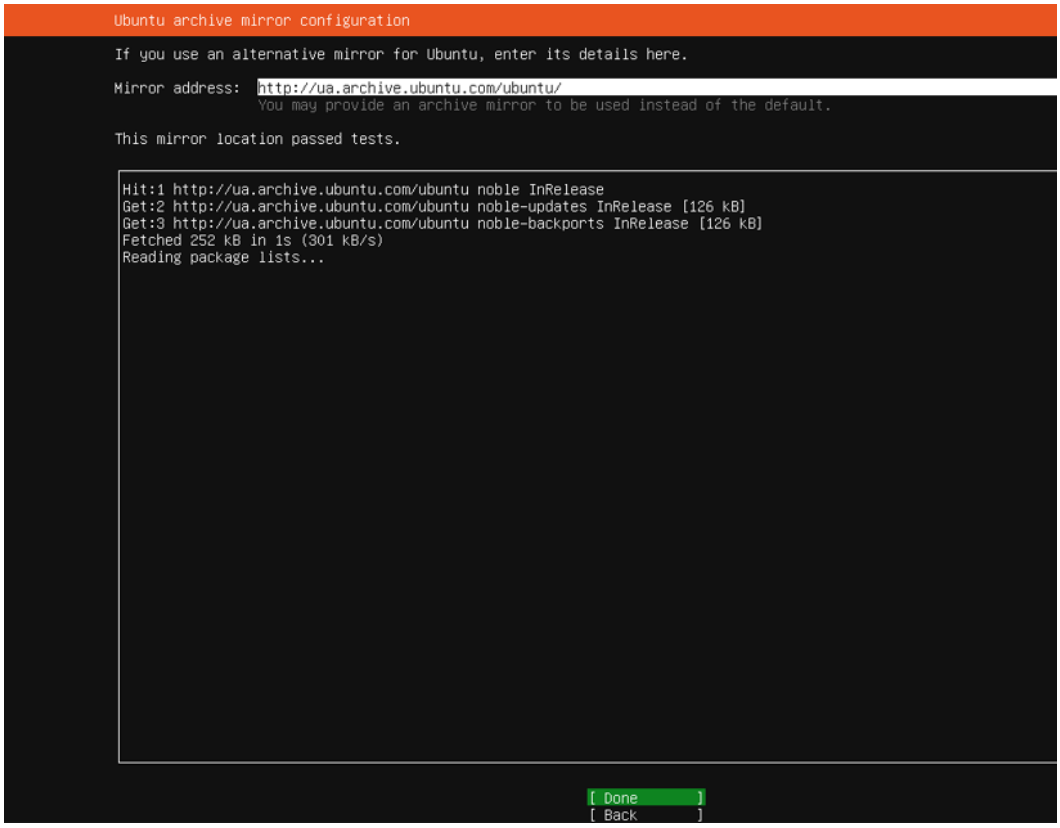

Рис. 3.4. Третій етап встановлення серверу Suricata

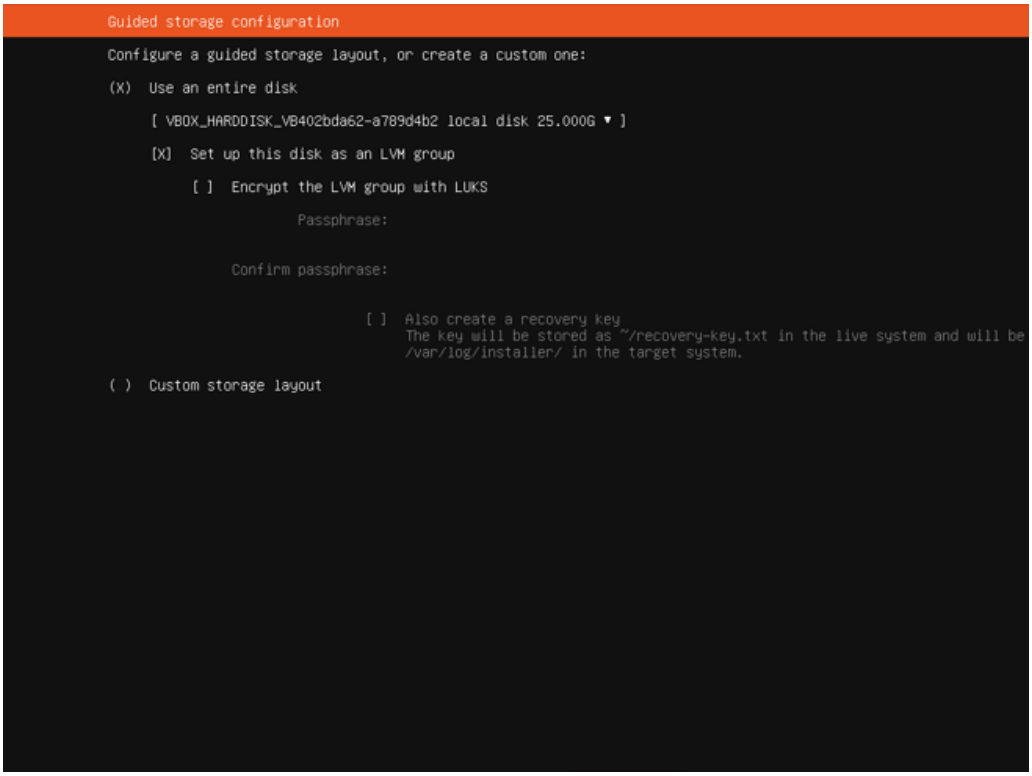

Рис. 3.5. Четвертий етап встановлення серверу Suricata

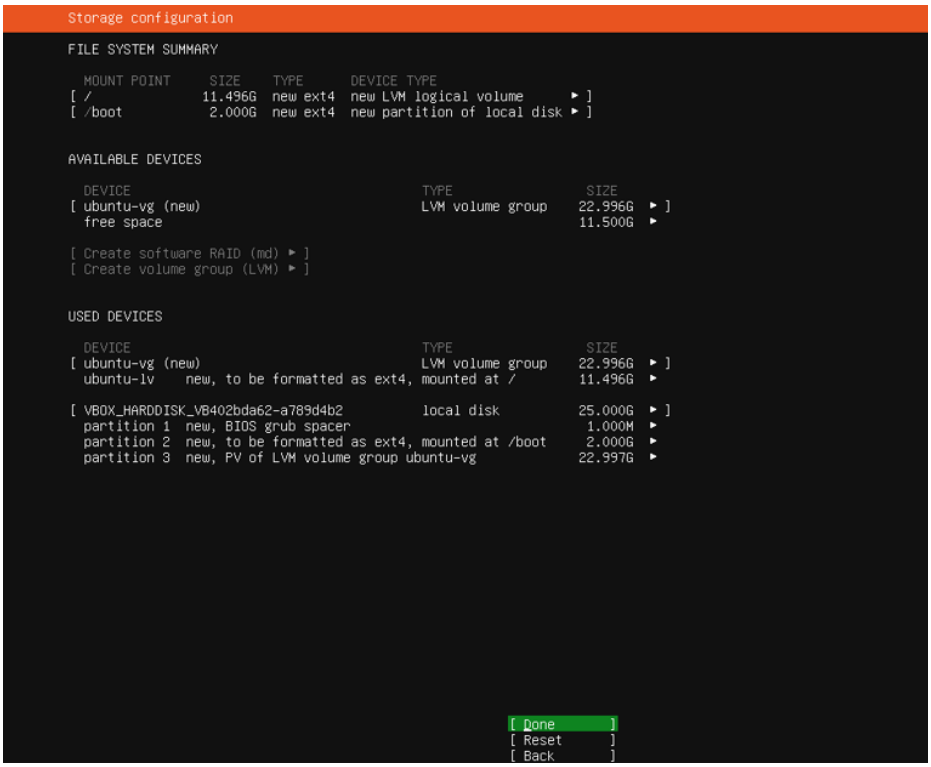

Рис. 3.6. П’ятий етап встановлення серверу Suricata

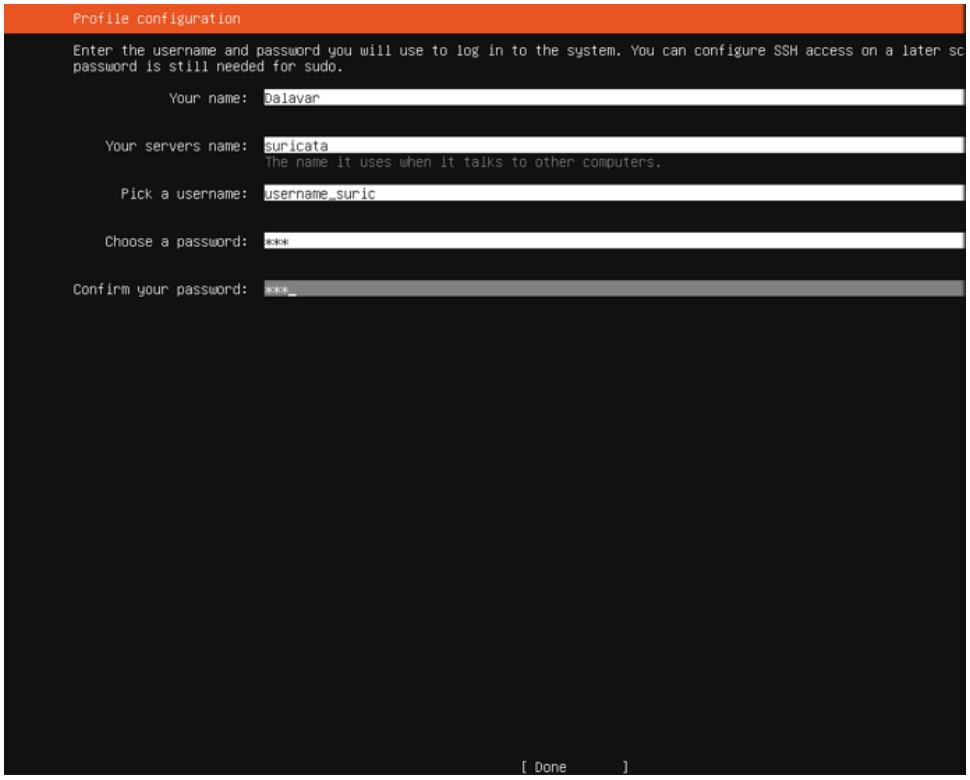

Рис. 3.7. Шостий етап встановлення серверу Suricata

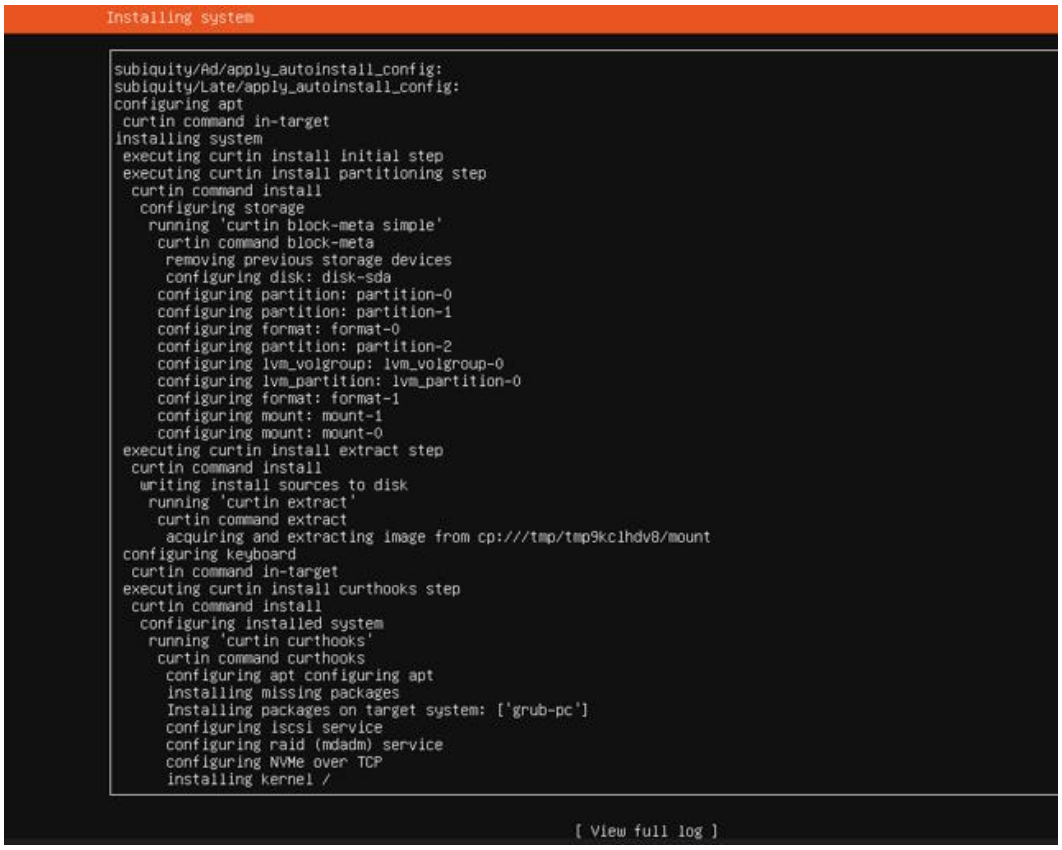

Рис. 3.8. Сьомий етап встановлення серверу Suricata

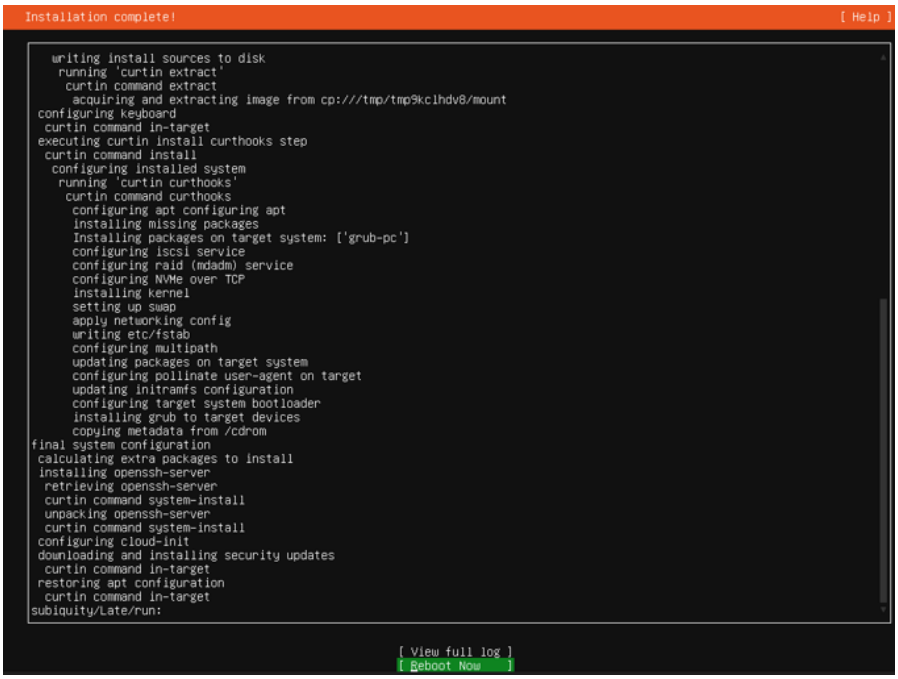

Рис. 3.9. Восьмий етап встановлення серверу Suricata

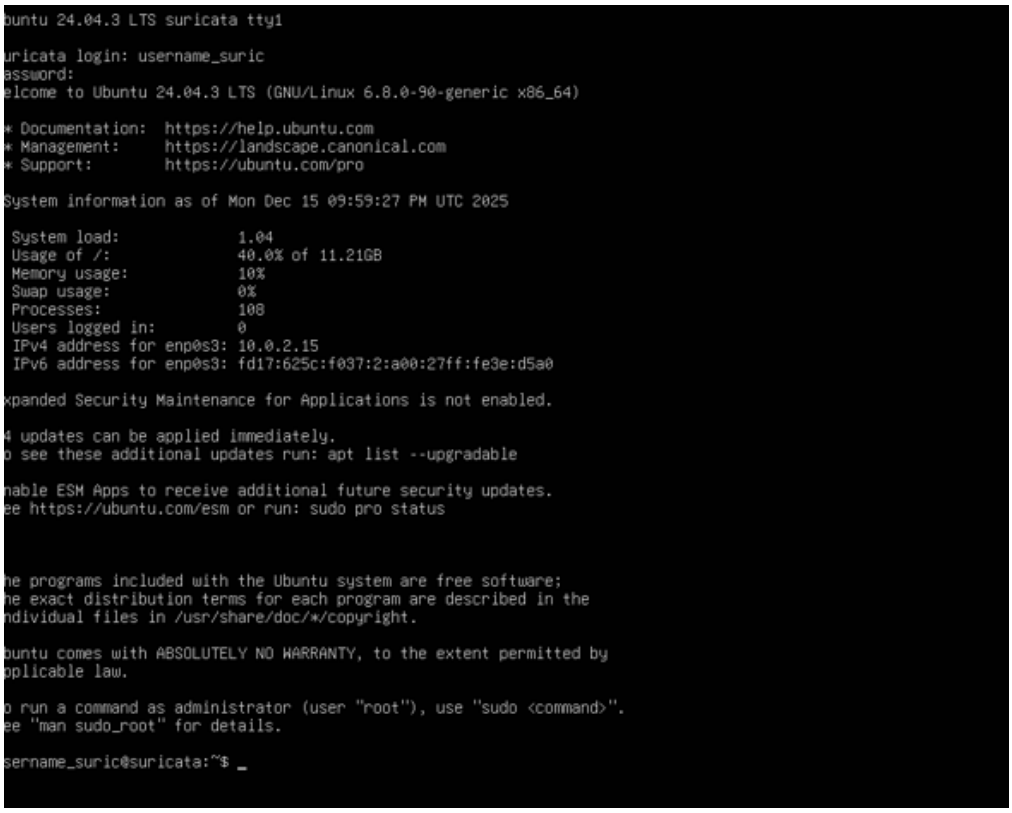

Рис. 3.10. Дев’ятий етап встановлення серверу Suricata

За таким самим принципом було завантажено та встановлено другий сервер-атакер.

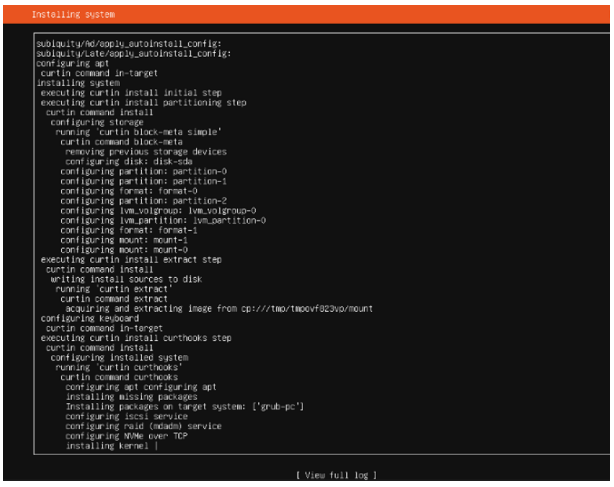

Рис. 3.11. Налаштування та встановлення серверу-атакера

Після успішного встановлення серверів було налаштовано локальну мережу між двома серверами під назвою “corp_net”.

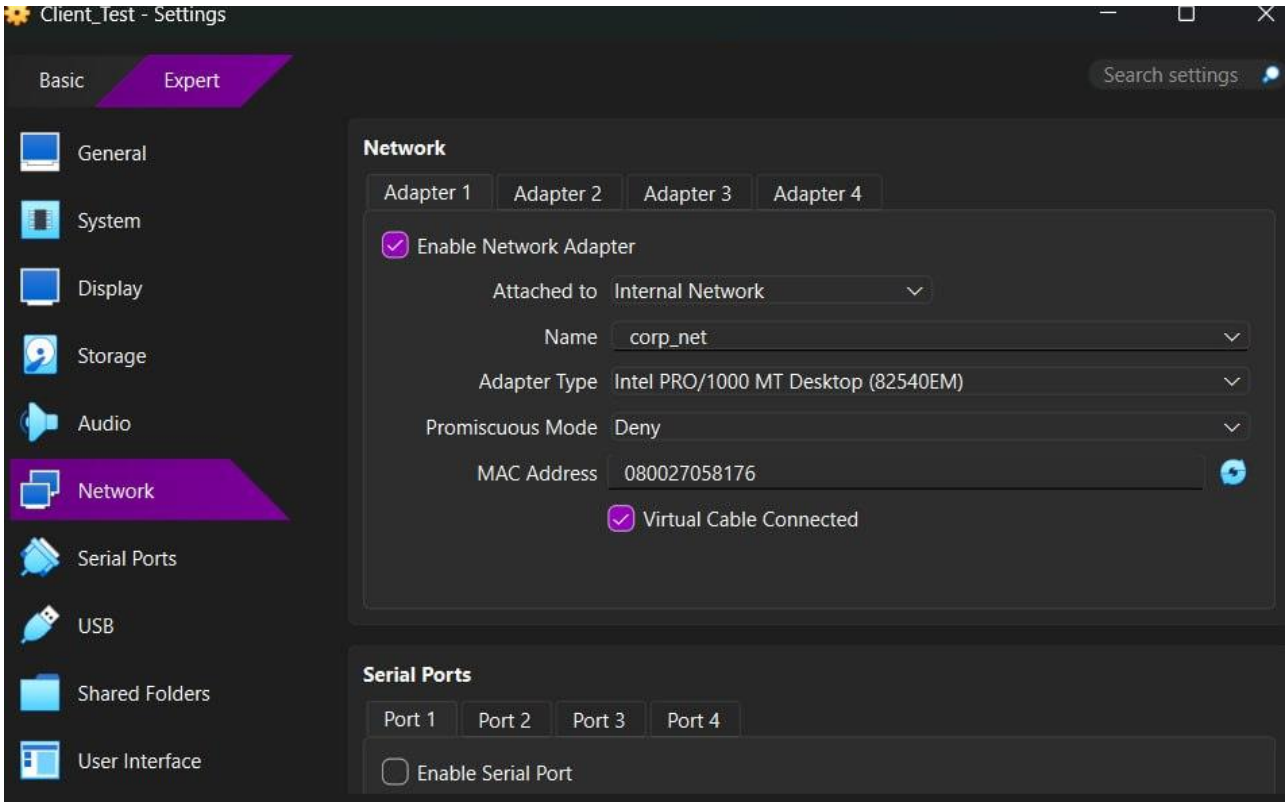

Рис. 3.12. Налаштування локальної мережі для сервера-атакера

Наступним етапом було запущено сервер Suricata для подальшого налаштування мережі.

В середені серверу відкрито мережеву конфігурацію серверу Suricata командою “sudo nano /etc/netplan/00-installer-config.yaml”

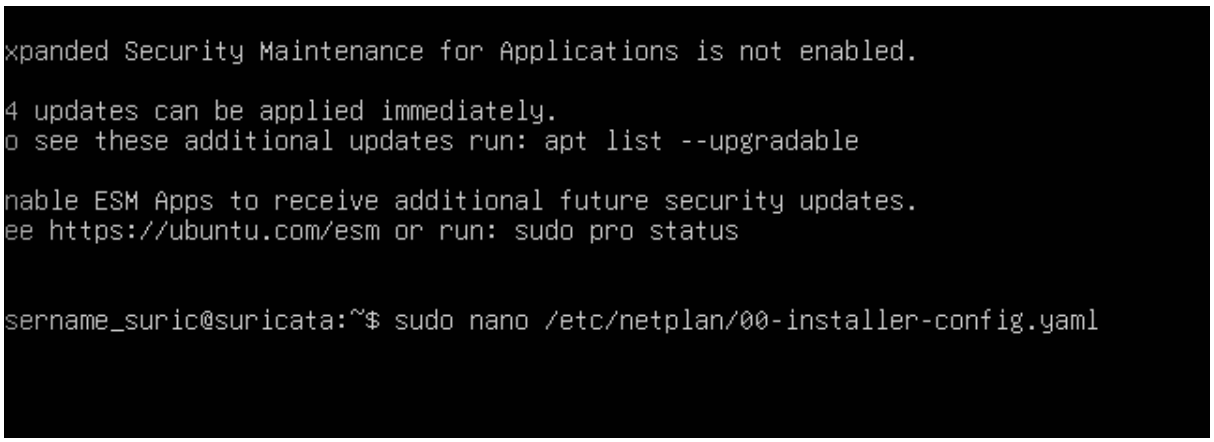

Рис. 3.13. Відкриваємо мережеву конфігурацію

Нашим завданням на даний момент буде видача особистих ip адрес для кожного серверу, для цього спочатку командою “ip a” передевляємося базові ip які буди встановлені на сервері.

```
username_suric@suricata:~$ ls /etc/netplan/
50-cloud-init.yaml
username_suric@suricata:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3e:d5:a0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86030sec preferred_lft 86030sec
    inet6 fd17:625c:f037:2:a00:27ff:fe3e:d5a0/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86378sec preferred_lft 14378sec
    inet6 fe80::a00:27ff:fe3e:d5a0/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:cd:f3:1d brd ff:ff:ff:ff:ff:ff
username_suric@suricata:~$ _
```

Рис. 3.14. Мережеві виходи серверу Suricata

Після цього відкриваємо файл мережевої конфігурації серверу Suricata та виставляємо особистий ip “192.168.1.1/24”

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      addresses: [192.168.1.1/24]
      optional: true_
```

Рис. 3.15. Мережева конфігурація серверу Suricata

Командою “ip a” перевіряємо чи змінився ip у сервера Suricata

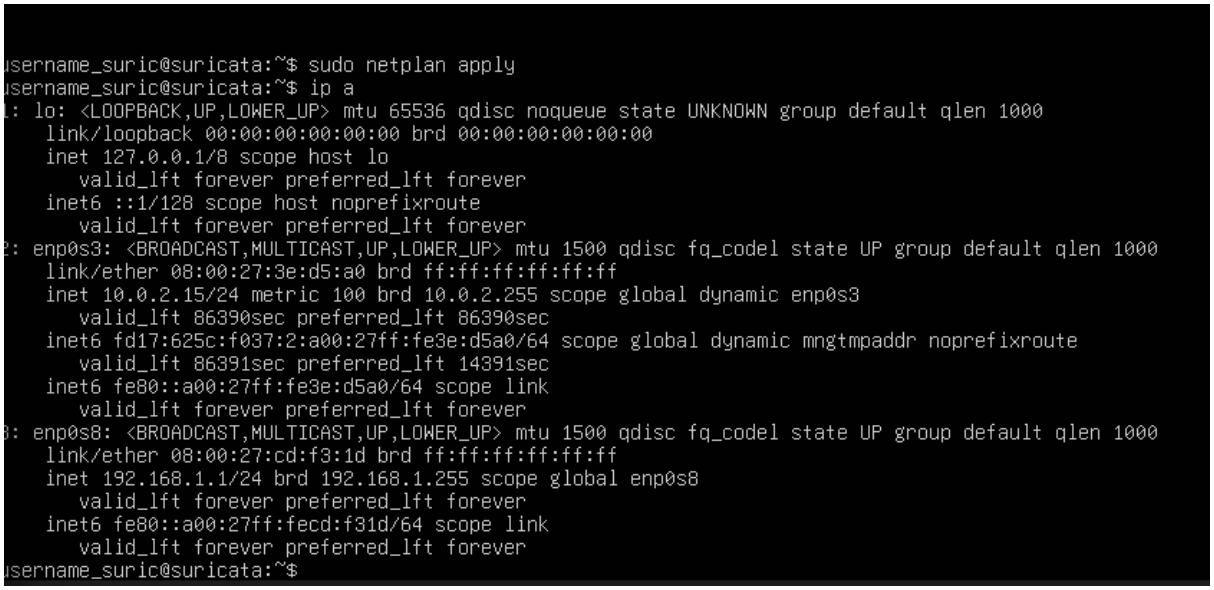

Рис. 3.16. Мережеві виходи серверу Suricata

Таку саму процедуру проводимо на сервері-атакері та даємо йому ip “192.168.1.10/24”

Рис. 3.17. Мережева конфігурація сервера-атакера

Командою “sudo netplan apply” ми застосовуємо зміни та перевіряємо їх командою “ip a”

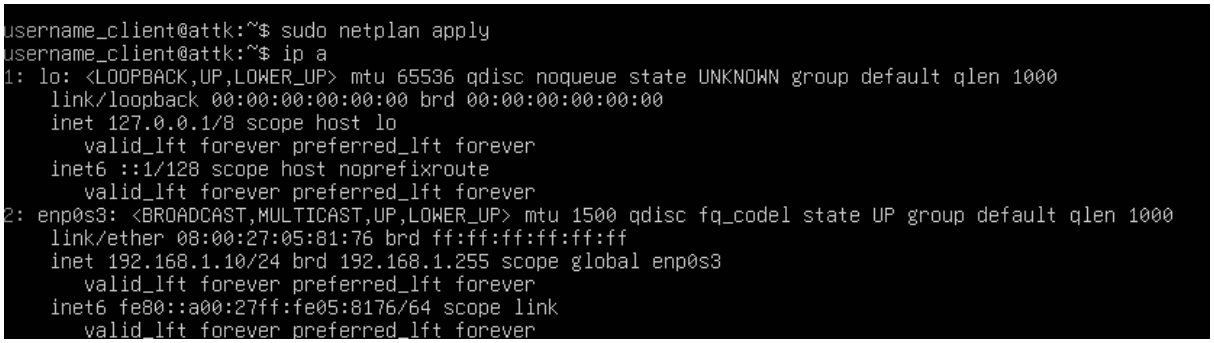

Рис. 3.18. Мережеві виходи сервера-атакера

Проводимо перевірку серверім методом пінгування один одного командою “ping <ip>”

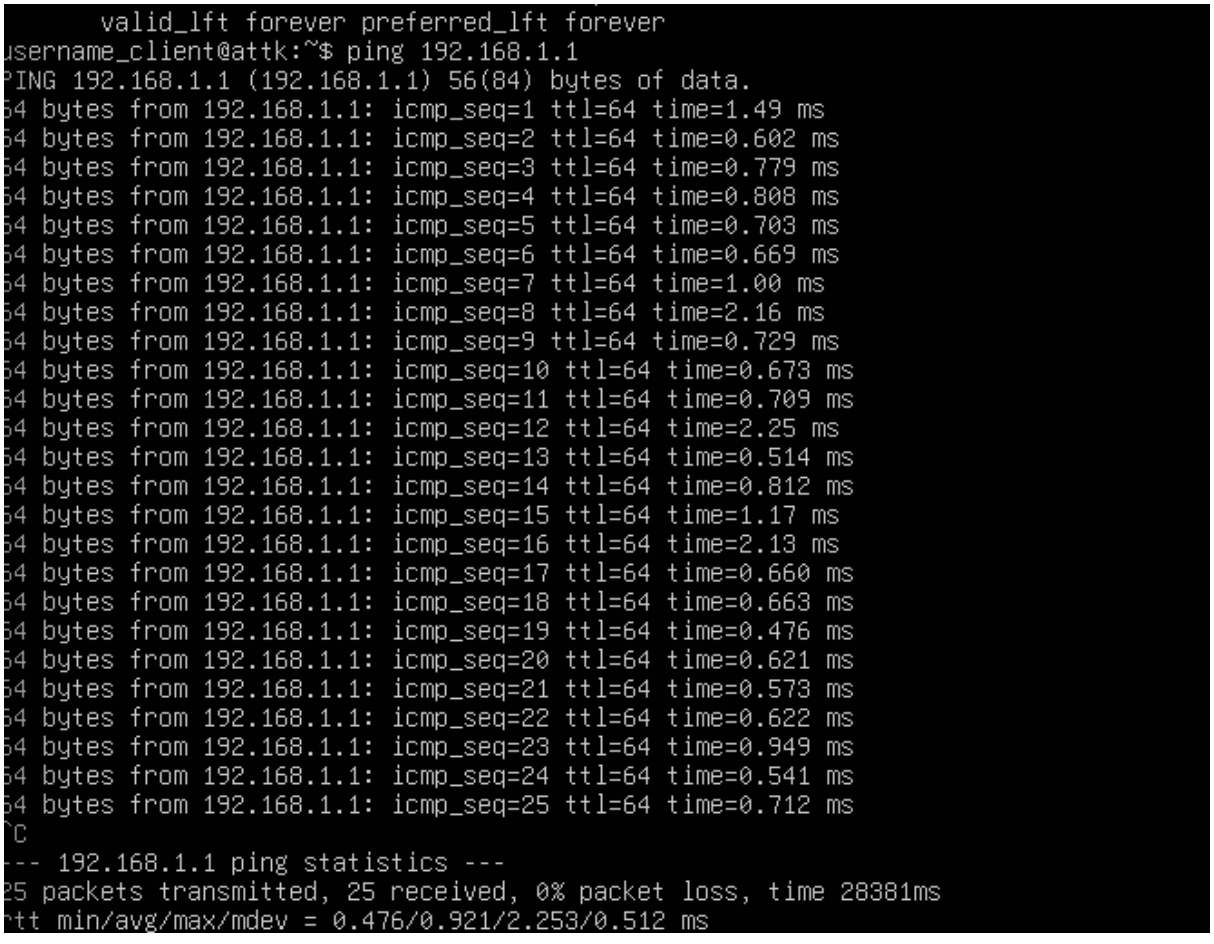

Рис. 3.19. Пінгування серверу Suricata

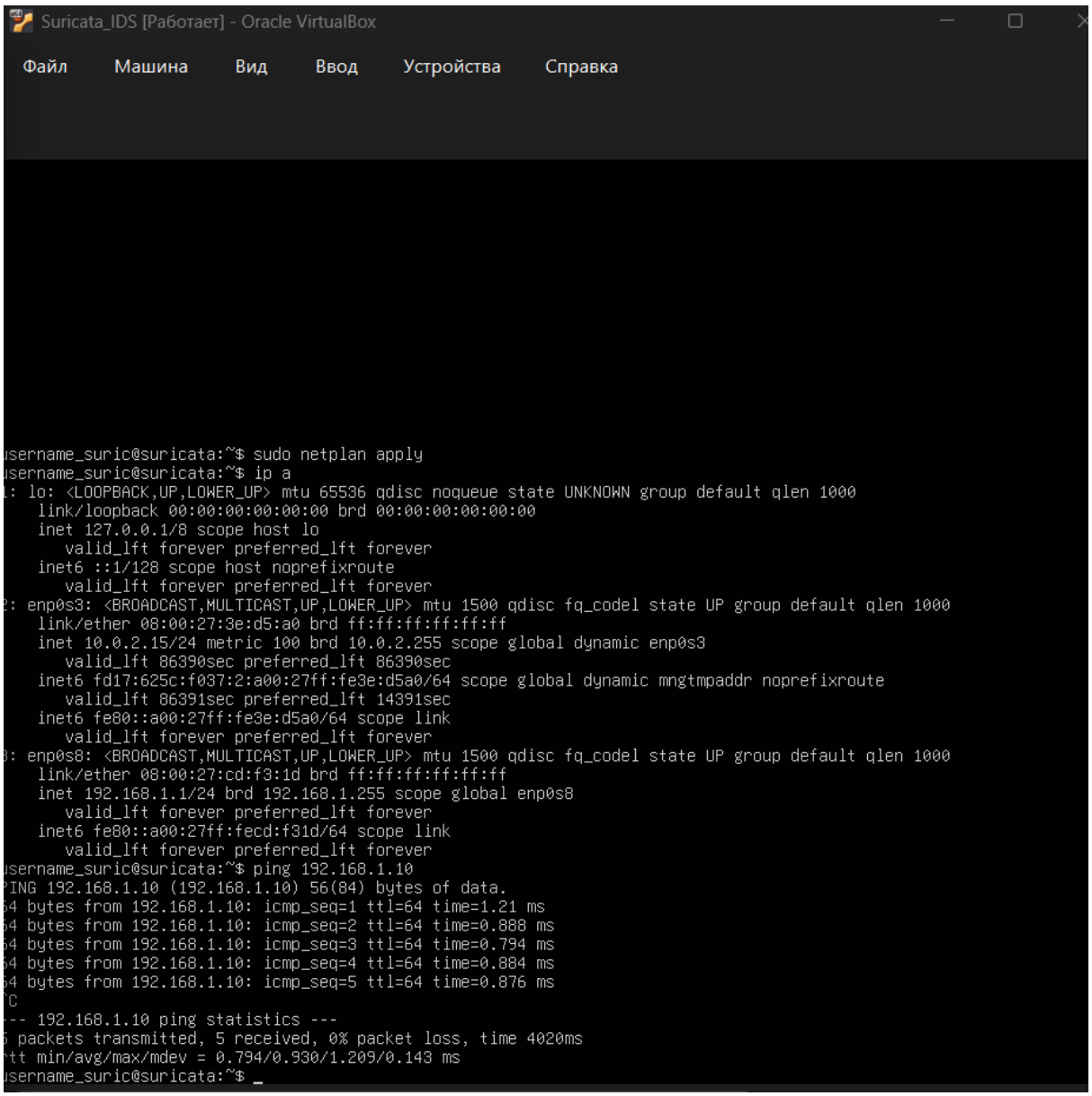

Рис. 3.20. Пінгування сервера-атакера

Завершальним етапом перед встановленням Suricata буде оновлення пакетів за допомогою команди “sudo apt update”

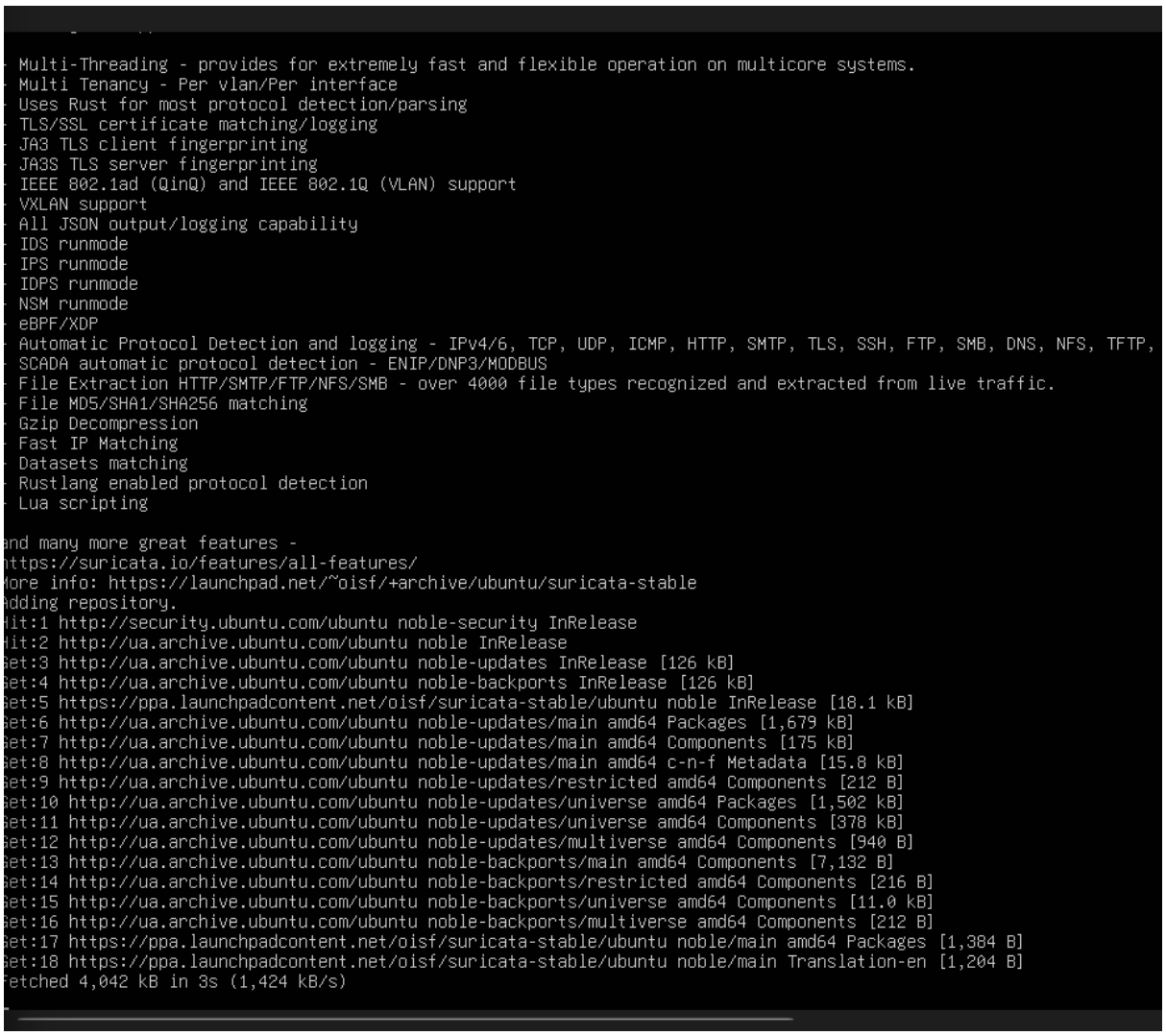

Рис. 3.21. Оновлення списку пакетів

Переходимо до встановлення самої Suricata. На сервері Suricata прописуємо “sudo apt install suricata -y”

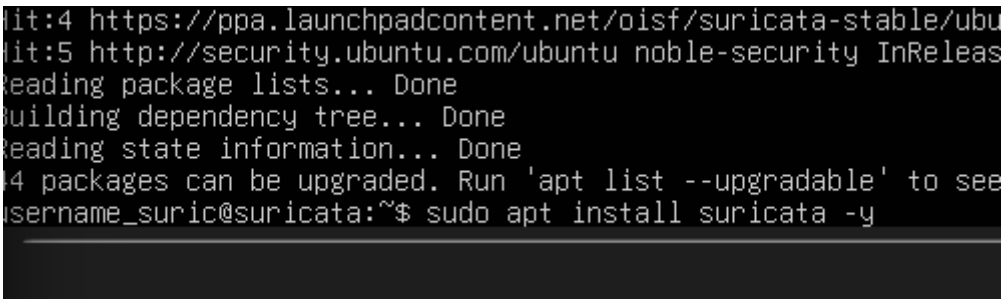

Рис. 3.22. Встановлення Suricata

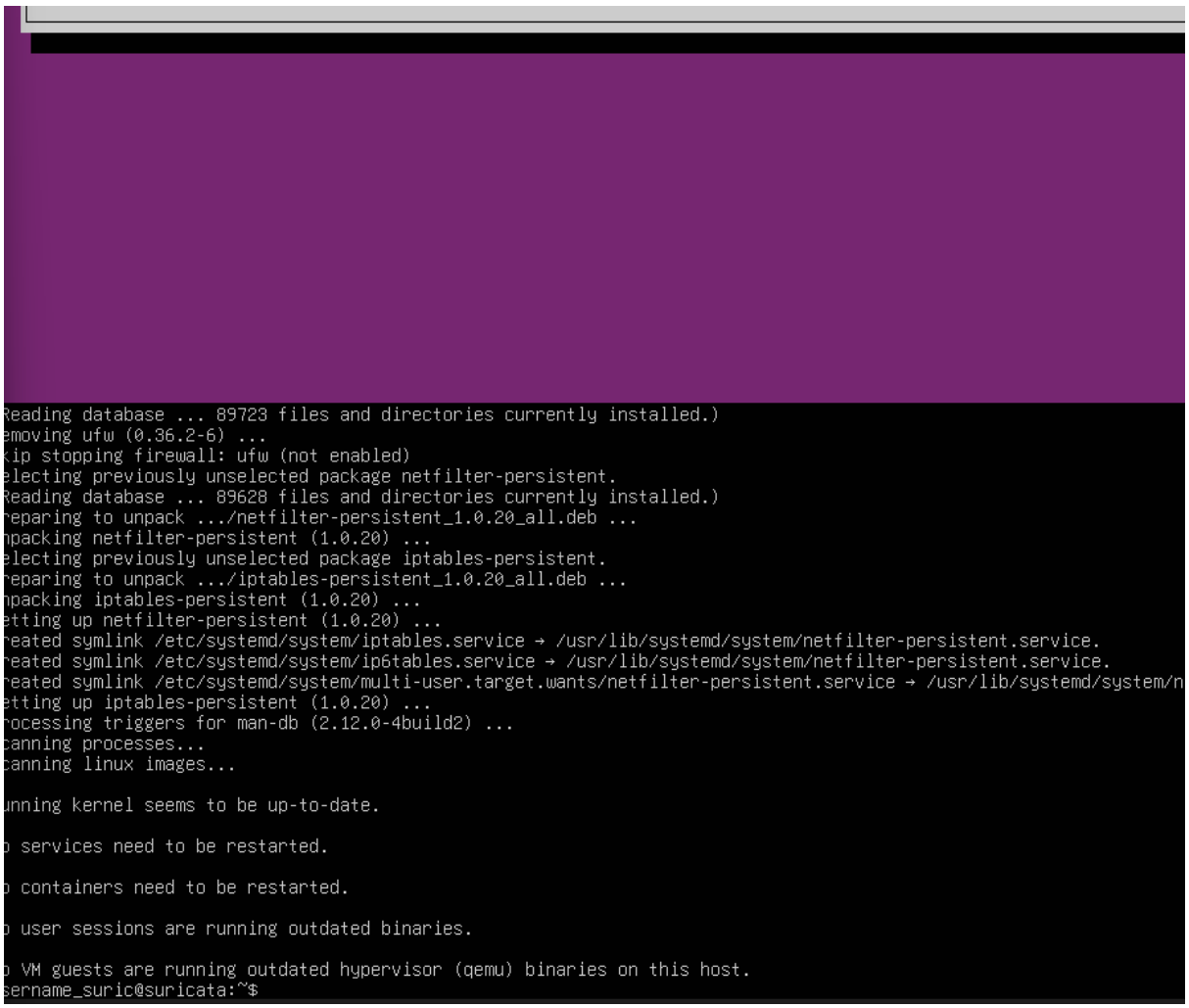

Рис. 3.23. Встановлення Suricata

Після успішного встановлення Suricata перевіряємо її версію за допомогою команди “suricata -V”

Рис. 3.24. Перевірка версії Suricata

3.2. Налаштування правил IDS/IPS та механізмів блокування атак у Suricata

Переходимо до налаштування правил IDS/IPS. Першим етапом буде налаштування конфігураційного файлу Suricata. Відкриваємо на сервері Suricata конфігураційний файл командою “sudo nano /etc/suricata/suricata.yaml”

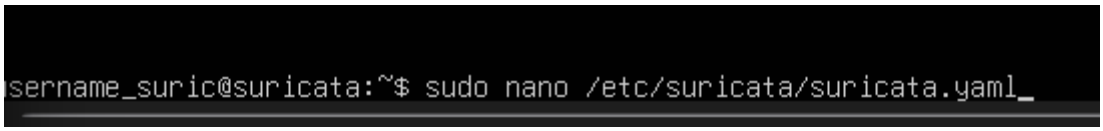

Рис. 3.25. Відкриття головного конфігураційного файлу Suricata

В розділі af -packet міняємо -interface на enp0s8 це наша локальна мережа

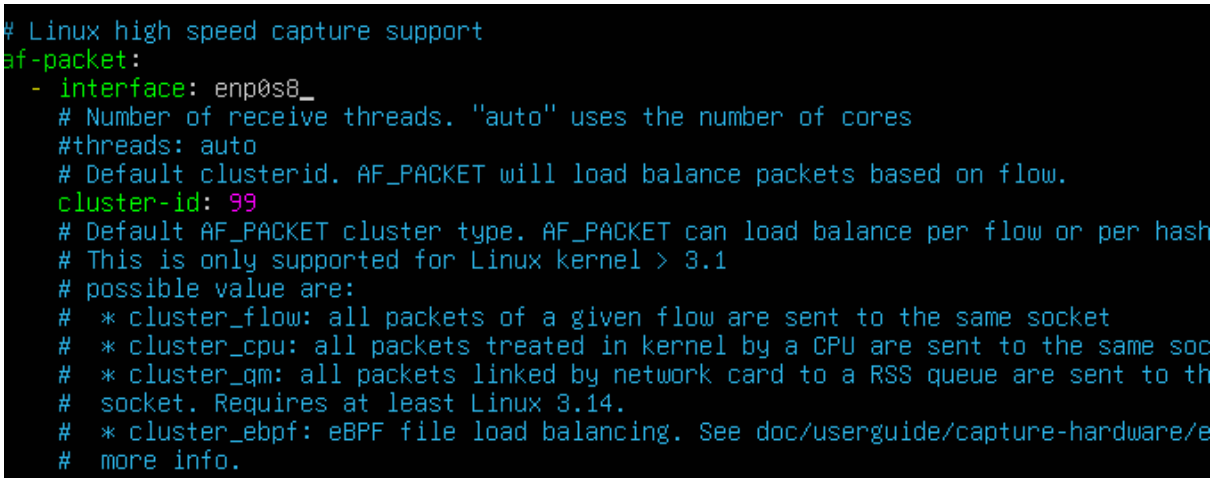

Рис. 3.26. Налаштування головного конфігураційного файлу Suricata

Оновлюємо правила Suricata після налаштування головного конфігураційного файлу

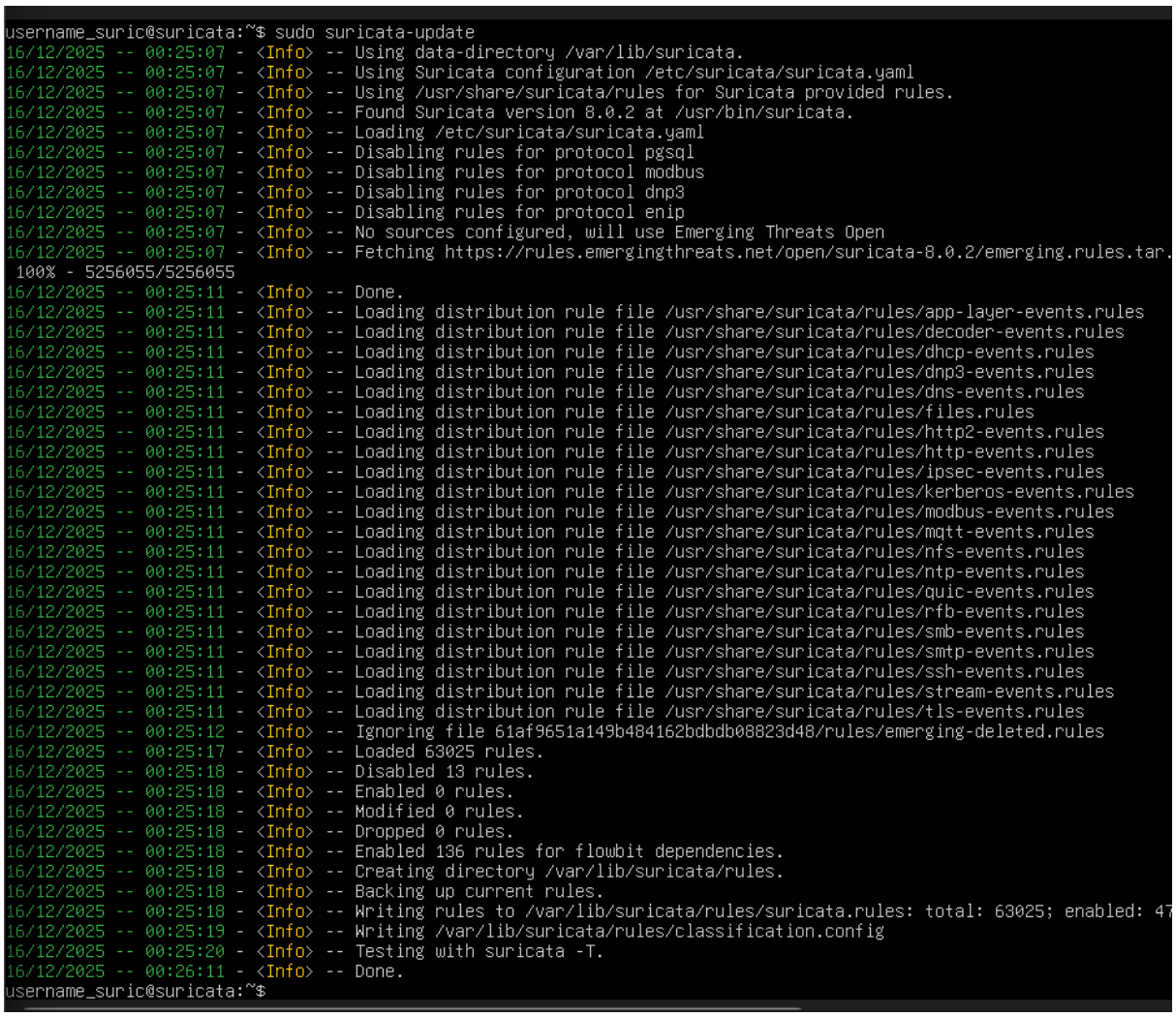

Рис. 3.27. Оновлення правил Suricata

Перевіряємо конфігураційний файл за допомогою команди “sudo suricata -T -c /etc/suricata/suricata.yaml -i enp0s8”

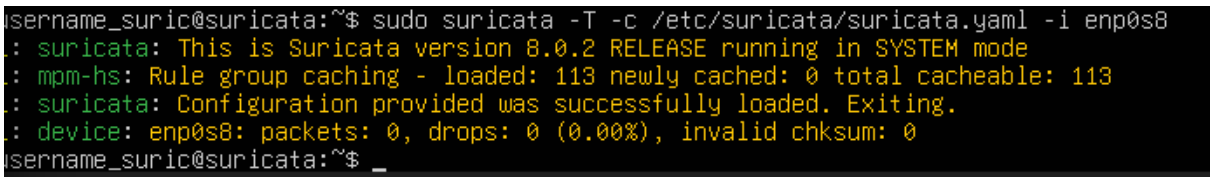

Рис. 3.28. Перевірка конфігураційного файлу Suricata

Оновлюємо та перевіряємо статус Suricata командами “enable suricata”, “start suricata”, “status suricata”.

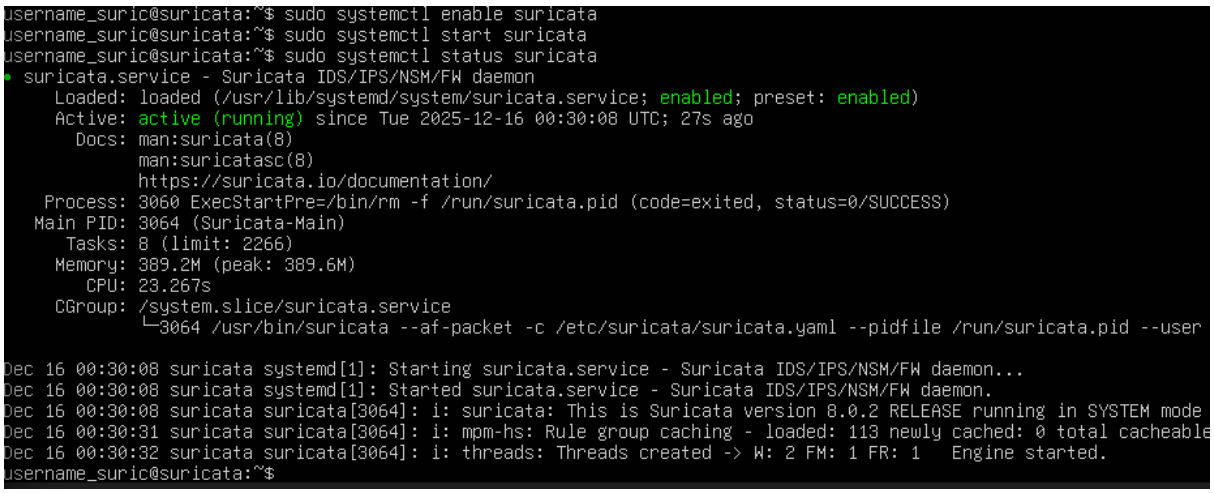

Рис. 3.29. Перевірка статусу Suricata

Переходимо до створення простого правила для виявлення пінгів на сервер. Відкриваємо головний конфігураційний файл та в пункті rule-files вписуємо назву локального файлу правил local.rules

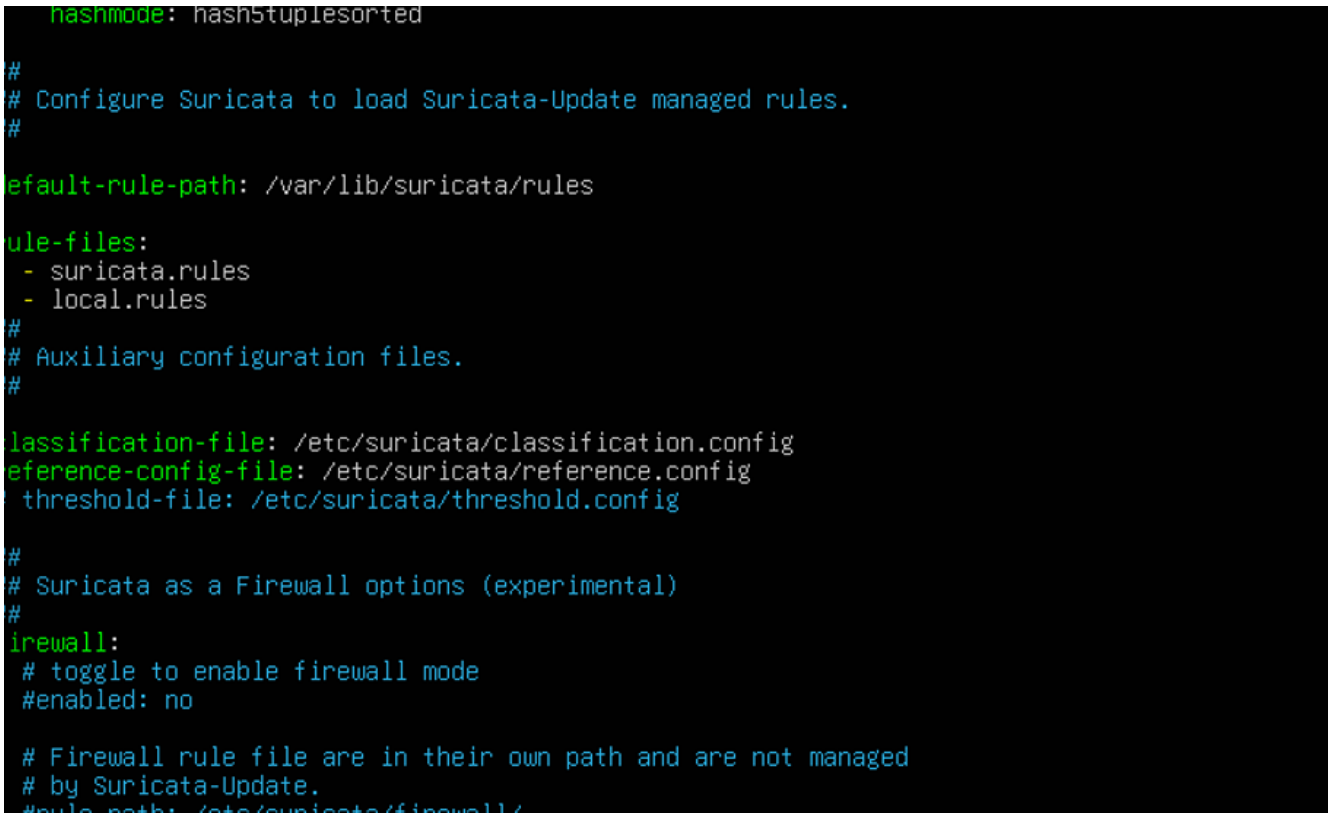

Рис. 3.30. Налаштування головного конфігураційного файлу Suricata

Відкриваємо редактор локальних правилю.

Рис. 3.31. Відкриття головного конфігураційного файлу Suricata

Пишемо просте правило виявлення пінгування та видачу алерту.

Рис. 3.32. Написання правила для Suricata

З серверу-атакера проводимо пінгування серверу Suricata

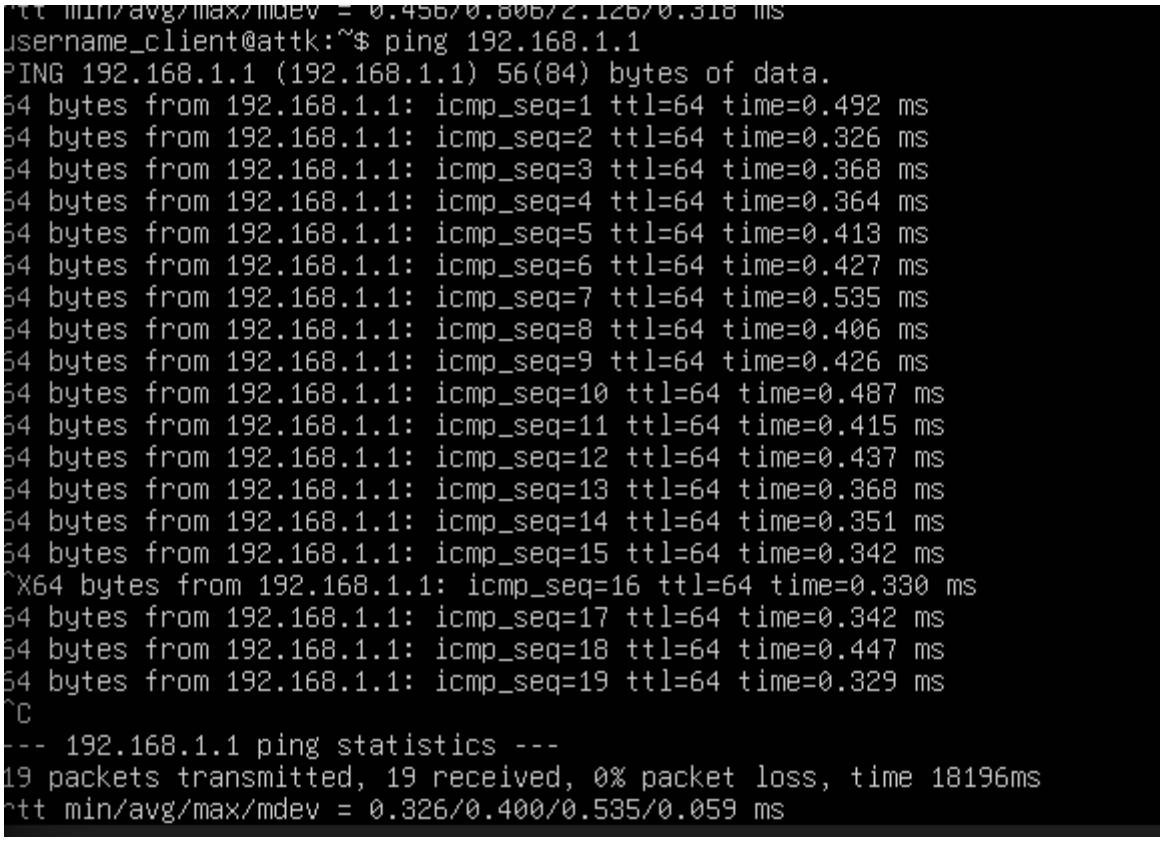

Рис. 3.33. Пінгування серверу Suricata

Підтверджуємо спрацювання алерту Suricata в файлі fast.log

Рис. 3.34. Спрацювання алерту

Для наступного етаму роботи нам треба серверу-атакеру видати доступ до інтернету для завантаження NMAP. Для цього переходимо до налаштувань мережі атакера в налаштуваннях VirtualBox та для другого адаптера даємо доступ до NAT.

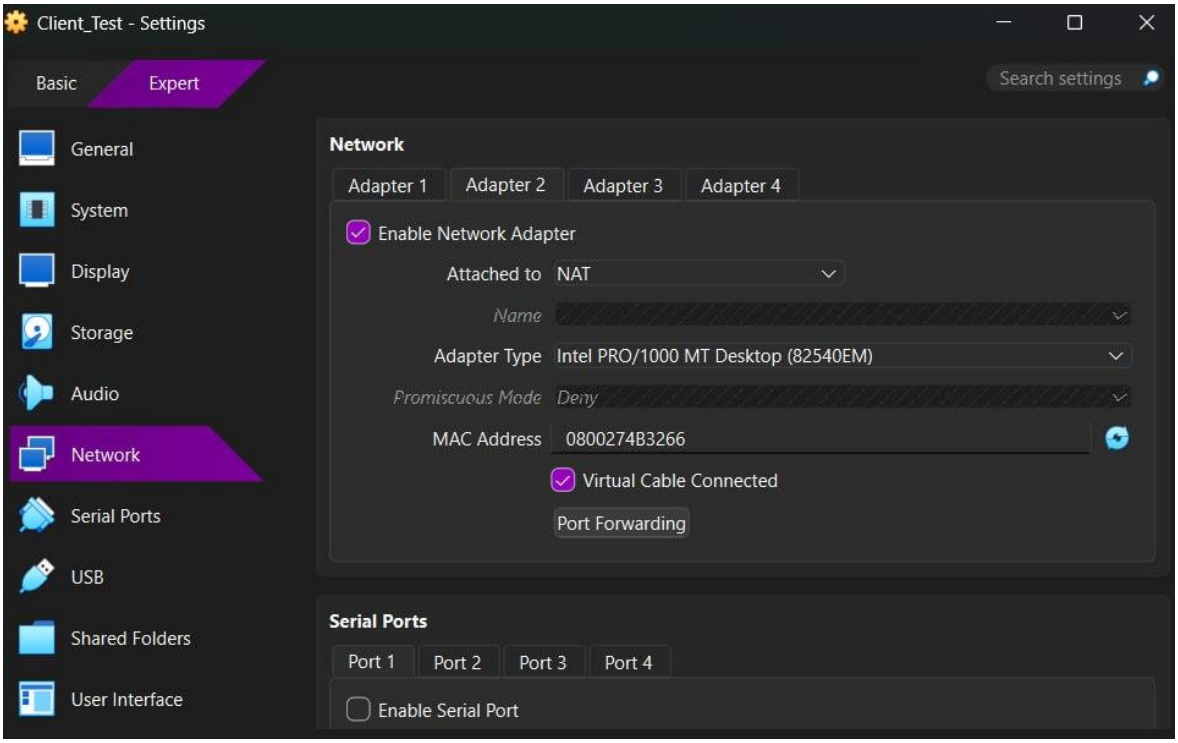

Рис. 3.35. Налаштування мережі атакера

Оновлюємо список пакетів на атакері.

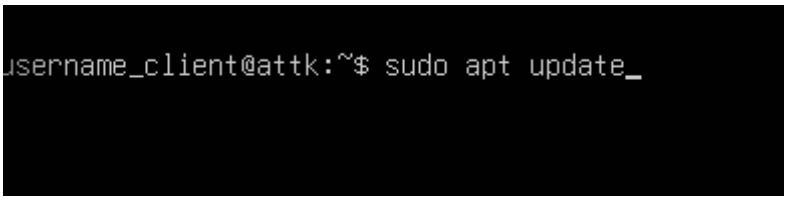

Рис. 3.36. Оновлення списку пакетів

Спробуємо встановити NMAP.

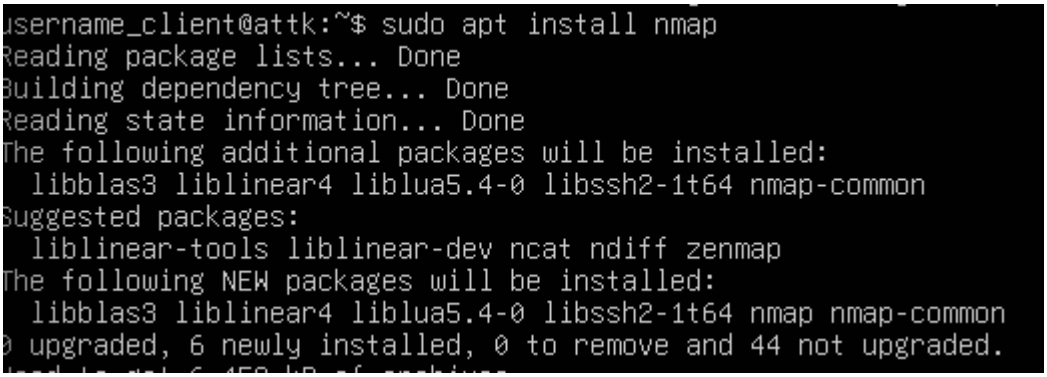

Рис. 3.37. Встановлення NMAP

Невдача. Переходимо до мережевих конфігурацій серверу-атакера. Даємо доступ enp0s8 до dhcp4.

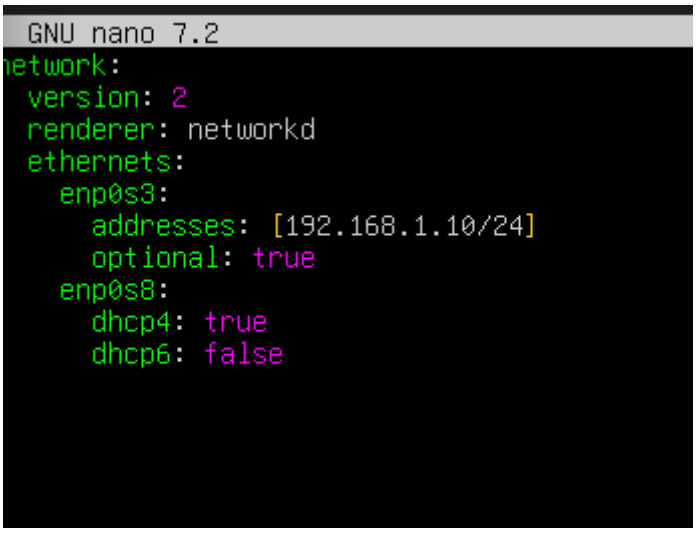

Рис. 3.38. Мережева конфігурація серверу-атакера

Після успішної заміни застосовуємо нові налаштування мережі.

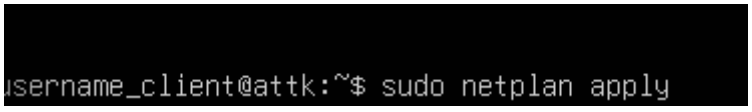

Рис. 3.39. Застосування мережевих налаштуваль

Перевіряємо мережу атакера.

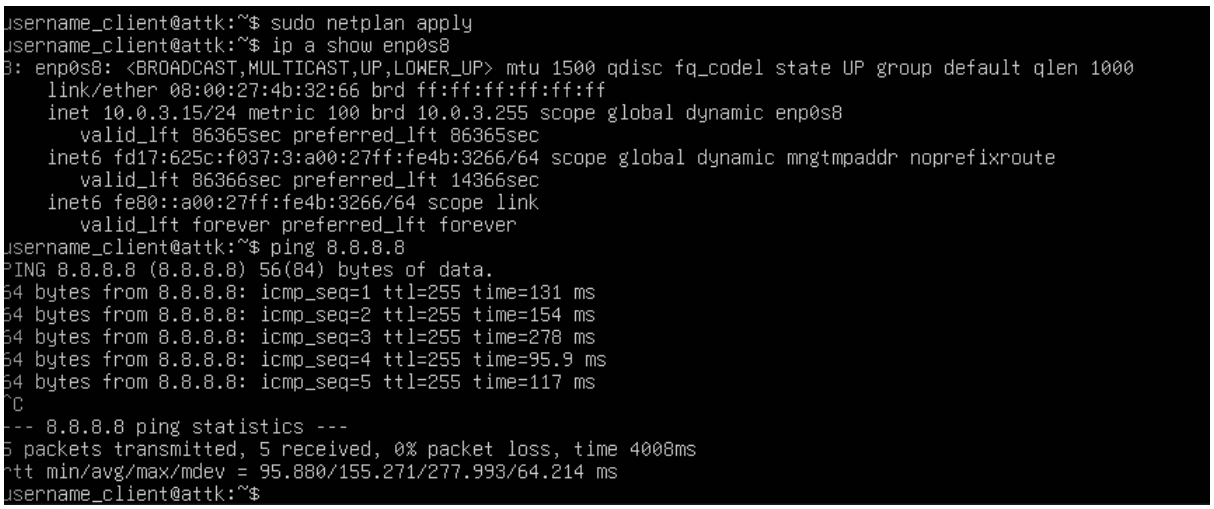

Рис. 3.40. Перевірка мережі атакера

Після перевірки мережі проводимо оновлення списку пакетів.

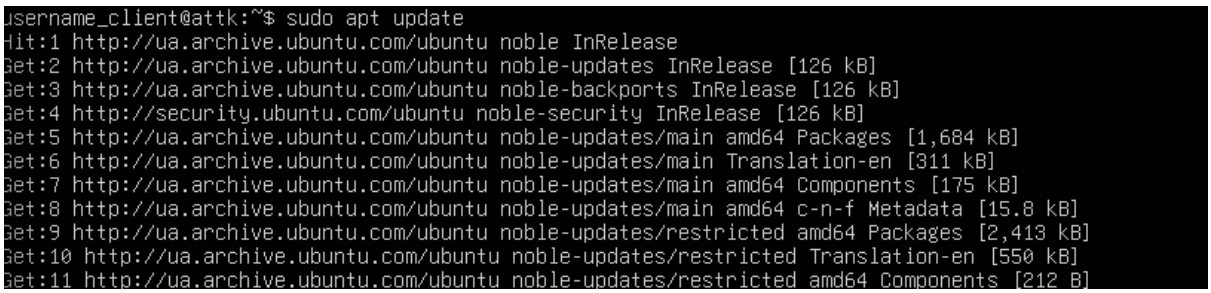

Рис. 3.41. Оновлення списку пакетів

Проводимо встановлення NMAP

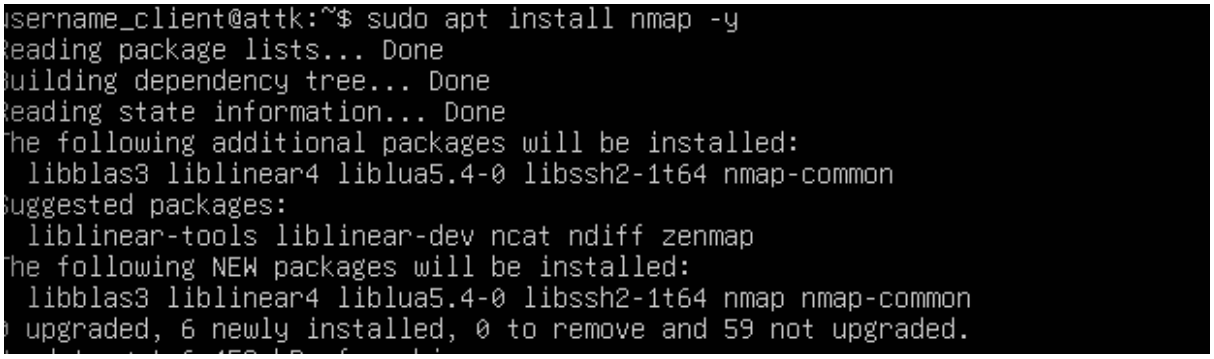

Рис. 3.42. Встановлення NMAP

Перевіряємо версію NMAP

Рис. 3.43. Версія NMAP

На сервері Suricata пишемо правило виявлення NMAP.

Рис. 3.44. Написання правила

Після написання правила проводимо перевірку конфігураційного файлу на помилки.

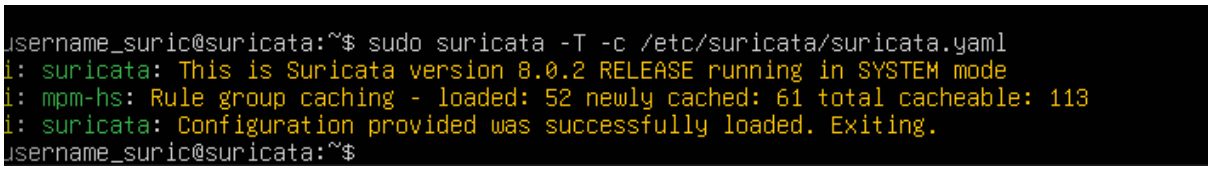

Рис. 3.45. Перевірка конфігураційного файлу Suricata

Перевіряємо статус Suricata

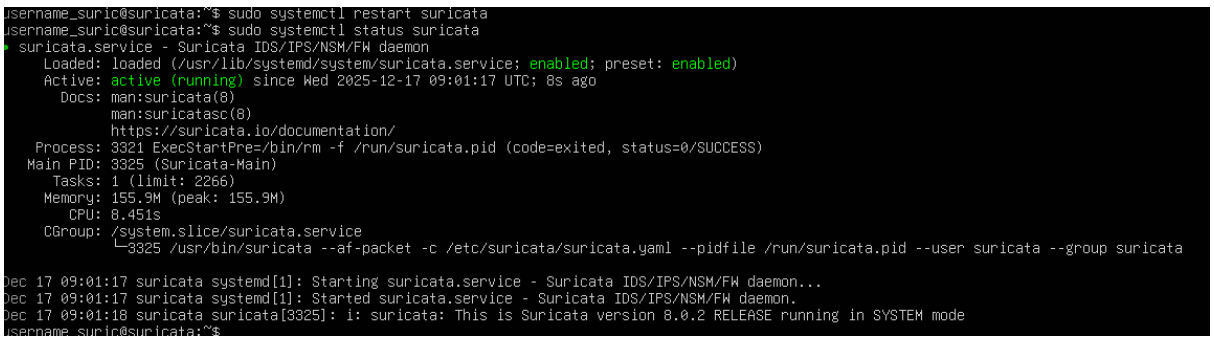

Рис. 3.46. Статус Suricata

На сервері-атакері проводимо швидке сканування портів за допомогою NMAP.

Рис. 3.47. Швидке сканування портів

Перевіряємо спрацювання Suricata.

Рис. 3.48. Алерт NMAP

Окрім класичного TCP SYN-сканування, інструмент Nmap підтримує альтернативні методи порт-сканування, такі як FIN-scan, NULL-scan та XMAS-scan. Дані типи сканування використовують нестандартні комбінації TCP-прапорців з метою обходу міжмережевих екранів та систем безпеки.

- FIN-scan — передача TCP-пакетів лише з прапорцем FIN
- NULL-scan — передача TCP-пакетів без встановлених прапорців
- XMAS-scan — використання одночасно прапорців FIN, PSH та URG

Подібні типи трафіку є нетиповими для легітимних з’єднань і можуть бути ефективно виявлені за допомогою сигнатурного аналізу в Suricata. Наявність таких механізмів детекції дозволяє значно підвищити рівень захищеності мережі та своєчасно виявляти приховані спроби розвідки.

Для налаштування IPS заходимо в налаштування конфігураційного файлу Suricata, перевіряємо налаштування af -packet.

```
# Linux high speed capture support
af-packet:
  - interface: enp0s8
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
    # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
    # This is only supported for Linux kernel > 3.1
    # possible value are:
    #  * cluster_flow: all packets of a given flow are sent to the same socket
    #  * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket
    #  * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
    #  socket. Requires at least Linux 3.14.
    #  * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardware/ebpf-xdp.rst for
    #  more info.
    # Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on system
    # with capture card using RSS (requires cpu affinity tuning and system IRQ tuning)
    # cluster_rollover has been deprecated; if used, it'll be replaced with cluster_flow.
    cluster-type: cluster_flow
    # In some fragmentation cases, the hash can not be computed. If "defrag" is set
    # to yes, the kernel will do the needed defragmentation before sending the packets.
    defrag: yes
    # Lock memory map to avoid it being swapped. Be careful that over
```

Рис. 3.49. Налаштування конфігураційного файлу Suricata

Після перевірки af -packet спускаємось вниз та розкоментовуємо розділ -drop та активовуємо його.

```
        #force-hash: [md5]
    - drop:
        enabled: yes
        alerts: yes       # log alerts that caused drops
    #    flows: all        # start or all: 'start' logs o
    #                      # per flow direction. All logs
```

Рис. 3.50. Налаштування конфігураційного файлу Suricata

Проводимо перевірку статусу Suricata.

```
username_suric@suricata:~$ sudo suricata -T -c /etc/suricata/suricata.yaml
i: suricata: This is Suricata version 8.0.2 RELEASE running in SYSTEM mode
i: mpm-hs: Rule group caching - loaded: 113 newly cached: 0 total cacheable: 113
i: suricata: Configuration provided was successfully loaded. Exiting.
username_suric@suricata:~$ sudo systemctl restart suricata
username_suric@suricata:~$ sudo systemctl status suricata
● suricata.service - Suricata IDS/IPS/NSM/FW daemon
     Loaded: loaded (/usr/lib/systemd/system/suricata.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-12-17 09:38:11 UTC; 8s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata.io/documentation/
    Process: 3414 ExecStartPre=/bin/rm -f /run/suricata.pid (code=exited, status=0/SUCCESS)
   Main PID: 3418 (Suricata-Main)
      Tasks: 1 (limit: 2266)
     Memory: 150.9M (peak: 151.1M)
        CPU: 8.367s
     CGroup: /system.slice/suricata.service
             └─3418 /usr/bin/suricata --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/suricata.pid --user suricata --group suricata

Dec 17 09:38:11 suricata systemd[1]: Starting suricata.service - Suricata IDS/IPS/NSM/FW daemon...
Dec 17 09:38:11 suricata systemd[1]: Started suricata.service - Suricata IDS/IPS/NSM/FW daemon.
Dec 17 09:38:11 suricata suricata[3418]: i: suricata: This is Suricata version 8.0.2 RELEASE running in SYSTEM mode
username_suric@suricata:~$
```

Рис. 3.51. Перевірка статусу Suricata

Змінюємо правило суріката так що б воно не просто видавало алерт а ще й

блокувало атаку.

Рис. 3.52. Написання правила для Suricata

Проводимо перевірку конфігураційного файлу на момент помилок.

Рис. 3.53. Перевірка конфігураційного файлу

Проводимо очистку фаст логу. Після цього запускаємо читання в реальному часі.

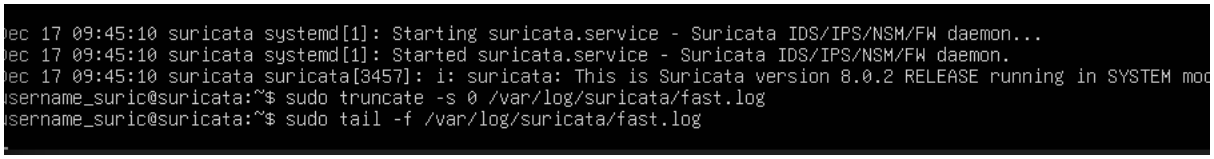

Рис. 3.54. Перевірка фаст логу

Проводимо атаку та бачимо успішне блокування.

Рис. 3.55. Спрацювання блокування

3.3 Рекомендації щодо впровадження системи Suricata в корпоративному середовищі

На основі виконаної практичної частини доцільно рекомендувати

використання системи Suricata як ефективного інструменту виявлення та запобігання мережевим вторгненням у корпоративному середовищі. Впровадження Suricata доцільно здійснювати на окремому сервері або мережевому вузлі, який має доступ до трафіку корпоративної мережі та достатні обчислювальні ресурси для аналізу пакетів у режимі реального часу. Особливу увагу слід приділяти коректному налаштуванню мережевих інтерфейсів і логічному розмежуванню внутрішніх та зовнішніх сегментів мережі, що забезпечує правильне визначення змінних типу HOME_NET і підвищує точність роботи правил виявлення.

У процесі впровадження рекомендовано починати експлуатацію Suricata в режимі IDS, що дозволяє накопичити статистику спрацювань, проаналізувати характер мережевого трафіку та мінімізувати кількість хибнопозитивних сповіщень. Після етапу тестування та оптимізації правил доцільним є переведення системи в режим IPS, що забезпечує активне блокування підозрілої мережевої активності, зокрема мережевого сканування та спроб несанкціонованого доступу, подібних до атак, змодельованих у межах практичного дослідження.

Окремої уваги потребує налаштування та підтримка актуальності правил Suricata. Рекомендується регулярно виконувати оновлення сигнатур за допомогою інструменту suricata-update, а також доповнювати стандартний набір правил власними користувацькими правилами, розміщеними у файлі local.rules. Такий підхід дозволяє адаптувати систему до специфіки конкретної корпоративної мережі та забезпечити виявлення характерних для неї загроз, включно з активним мережевим скануванням і нетиповою поведінкою вузлів.

Для підвищення ефективності реагування на інциденти безпеки рекомендовано налаштовувати централізоване логування та аналіз подій, зокрема шляхом використання детальних журналів у форматі JSON. Це дає змогу інтегрувати Suricata з іншими засобами моніторингу та управління інформаційною безпекою, а також спрощує подальший аналіз інцидентів і формування звітності. Практичні результати дослідження підтверджують, що коректно налаштована система Suricata здатна ефективно виявляти та блокувати підозрілу мережеву

активність, що робить її доцільним компонентом комплексної системи захисту корпоративних мереж

У результаті впровадження технології IDS/IPS на базі Suricata підвищився рівень захищеності корпоративної мережі, зокрема було забезпечено:

- своєчасне виявлення мережевих атак та аномальної активності;
- автоматичне блокування частини атак у режимі IPS;
- зменшення ризику несанкціонованого доступу до мережевих ресурсів;
- покращення контролю за мережевим трафіком та подіями інформаційної безпеки;
- можливість централізованого журналювання та аналізу інцидентів.

Отримані результати підтверджують доцільність використання системи Suricata як ефективного засобу підвищення рівня інформаційної безпеки корпоративних мереж та можливість її застосування в реальних умовах з обмеженими фінансовими витратами.

ВИСНОВКИ

У процесі виконання дипломної роботи було досліджено основні підходи до забезпечення захисту інформації в корпоративних мережах та проаналізовано сучасні загрози інформаційній безпеці, що виникають у процесі експлуатації мережевої інфраструктури. У теоретичній частині роботи розглянуто принципи функціонування систем виявлення та запобігання вторгненням, класифіковано основні типи мережевих атак та визначено місце систем класу IDS/IPS у загальній архітектурі захисту корпоративних мереж.

У межах практичної частини дипломної роботи було розгорнуто тестовий стенд на базі двох віртуальних серверів під управлінням операційної системи Ubuntu Server, що дозволило змоделювати типове корпоративне мережеве середовище. Було налаштовано локальну мережу між серверами, забезпечено доступ до мережі Інтернет, присвоєно статичні IP-адреси та перевірено коректність мережевої взаємодії. На одному з серверів встановлено та налаштовано систему Suricata, яка використовувалась для аналізу мережевого трафіку та виявлення підозрілої активності.

У ході експериментальних досліджень реалізовано та протестовано набір правил Suricata, зокрема прості правила для виявлення ICMP-запитів і складніші правила для фіксації мережевого сканування за допомогою утиліти Nmap. Проведено моделювання атаки з боку машини-атакера та проаналізовано спрацювання системи в режимах IDS та IPS. Отримані результати підтвердили можливість ефективного виявлення та блокування підозрілих мережевих дій за умови коректного налаштування конфігураційного файлу та правил системи.

На основі результатів практичної реалізації було розроблено рекомендації щодо впровадження системи Suricata в корпоративному середовищі, які охоплюють питання поетапного введення системи в експлуатацію, оптимізації правил, оновлення сигнатур та організації моніторингу подій безпеки. Зроблено висновок, що використання Suricata як складової комплексної системи захисту

дозволяє підвищити рівень інформаційної безпеки корпоративної мережі, забезпечити своєчасне виявлення мережевих атак і зменшити ризики несанкціонованого доступу до інформаційних ресурсів.

Загалом результати дипломної роботи підтверджують доцільність застосування відкритих систем IDS/IPS у корпоративних мережах та демонструють практичну можливість їх ефективного використання для захисту інформації за умови правильного налаштування та регулярного адміністрування.

ПЕРЕЛІК ПОСИЛАНЬ

1. Захист інформації в корпоративних інформаційних системах : навчальний матеріал. Національний університет харчових технологій. URL: https://dspace.nuft.edu.ua/server/api/core/bitstreams/e19e9fdf-e7d6-4ac0-bd52-05b434b5a35a/content.

2. Козак В. М., Шелудько Н. В. Аналіз сучасних загроз інформаційній безпеці корпоративних мереж. Вісник Національного університету «Львівська політехніка». 2017. № 878. С. 99–105. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6630/17-99-105.pdf.

3. Hidden Risks of Information Security and Data Protection in Accounting and Payroll Services. PS-BPO Blog. URL: https://ps-bpo.com/blog/hidden-risks-of-info-security-and-data-protection-in-accounting-and-payroll-services/.

4. What Are the Biggest Security Risks for a Company. Secfix. URL: https://www.secfix.com/post/what-are-the-biggest-security-risks-for-a-company.

5. Cyber Security Threats. DataGuard. URL: https://www.dataguard.com/cyber-security/threats/.

6. Corporate Cybersecurity: The Challenges, the Risks, and Good Practice. Oodrive Blog. URL: https://www.oodrive.com/blog/security/corporate-cybersecurity-the-challenges-the-risks-and-good-practice/.

7. Жуков С. М., Коваленко О. В. Аналіз систем виявлення та запобігання мережевим вторгненням. Збірник наукових праць НУПП. URL: https://journals.nupp.edu.ua/sunz/article/view/2562.

8. Сучасні підходи до забезпечення інформаційної безпеки корпоративних мереж : наукова стаття. Харківський національний університет радіоелектроніки. URL: https://openarchive.nure.ua/server/api/core/bitstreams/381a4953-9306-4362-a6d1-e7199f2f425a/content.

9. Suricata Features. Open Information Security Foundation. URL: https://suricata.io/features/.

10. Suricata Documentation. Open Information Security Foundation. URL: https://docs.suricata.io/en/suricata-8.0.2/.

11. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf.

12. HPE. What is IDS/IPS? HPE Glossary. URL: https://www.hpe.com/us/en/what-is/ids-ips.html?utm_source=chatgpt.com.

13. PurpleSec. Intrusion Detection Vs Prevention Systems: What's the Difference? URL: https://purplesec.us/learn/intrusion-detection-vs-intrusion-prevention-systems/?utm_source=chatgpt.com.

14. NIST. Intrusion Detection and Prevention Systems | CSRC/NIST. URL: https://csrc.nist.gov/pubs/book-section/2010/10/intrusion-detection-and-prevention-systems/final?utm_source=chatgpt.com.

15. Corelight. IDS vs. IPS: What Are the Differences, and Do You Need Both? URL: https://corelight.com/resources/glossary/ids-vs-ips?utm_source=chatgpt.com.