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

**КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технологія захисту корпоративної мережі на основі SNORT IDPS»**

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*

_____ Артем ТИМОФЄЄВ
*(підпис)*

Виконав: здобувач вищої освіти групи БСДМ-63
ТИМОФЄЄВ Артем
*(прізвище, ім'я)*

Керівник д.ф., МАРЧЕНКО Віталій
*(науковий ступінь, вчене звання, прізвище, ім'я)*

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

Київ 2024

**ЗМІСТ**

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IDS - Intrusion Detection System

IPS - Intrusion Prevention System

IDPS - Intrusion Detection and Prevention System

DPI - Deep Packet Inspection

IAM - Identity and Access Management

EDR - Endpoint Detection and Response

NGFW - Next-Generation Firewall

SOAR - Security Orchestration, Automation, and Response

TCP - Transmission Control Protocol

NIDPS - Network-Based Intrusion Detection and Prevention System

# ВСТУП

*Актуальність дослідження*. У цифрову епоху дані стали одним із найцінніших активів компаній, а їх втрата або компрометація може призвести до значних фінансових втрат, пошкодження репутації та порушення правових норм. Технології виявлення та запобігання вторгненням (IDPS), зокрема SNORT, є ефективними інструментами, що дозволяють своєчасно ідентифікувати та нейтралізувати загрози. Відкритий код і гнучкість SNORT роблять його доступним і універсальним рішенням для широкого спектра корпоративних мереж. Завдяки можливостям інтеграції з іншими системами безпеки, налаштуванню правил відповідно до потреб організації та підтримці великої спільноти користувачів, SNORT стає важливим елементом сучасної кібербезпеки. Дослідження цієї теми дозволяє визначити оптимальні підходи до розгортання та налаштування SNORT IDPS у корпоративному середовищі, забезпечити гнучкість і масштабованість системи захисту, а також розробити рекомендації для її ефективного використання. Це дослідження спрямоване на зміцнення кібербезпеки компаній шляхом мінімізації ризиків, підвищення рівня захищеності даних та зниження впливу кібератак на бізнес-процеси.

*Об'єкт дослідження* – реагування на загрози як складова частина безпеки корпоративної мережі.

*Предмет дослідження* – методи та засоби захисту корпоративної мережі.

*Мета роботи* – дослідження методів та розроблення рекомендацій щодо захисту корпоративної мережі.

*Наукові завдання:*

*Методи дослідження* – опрацювання експлуатаційної документації інформації, міжнародні стандарти, практичне випробування.

*Практичне значення одержаних результатів* полягає в розробці технології захисту корпоративної мережі на основі SNORT IDPS.

*Апробація результатів.* Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

# 1 АНАЛІЗ НЕОБХІДНОСТІ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

## 1.1. Аналіз проблеми захисту корпоративної мережі

Корпоративні мережі стали серцем діяльності сучасних організацій. Вони забезпечують зручність комунікації, обмін інформацією та доступ до бізнес-ресурсів. Однак разом із розвитком технологій зростають і ризики, пов’язані з їх захистом. Тема безпеки корпоративних мереж є не просто актуальною, а критично важливою, адже будь-яка вразливість може призвести до серйозних наслідків: витоку даних, фінансових втрат чи навіть повної зупинки діяльності компанії. Проблема захисту корпоративної мережі охоплює три основні аспекти: зовнішні загрози, внутрішні ризики та технічні недоліки. Зовнішні загрози включають кібератаки, такі як DDoS, фішингові атаки та шкідливе програмне забезпечення. Внутрішні ризики часто пов'язані з людським фактором: співробітники можуть випадково надати доступ до мережі зловмисникам або самі стати інсайдерами. А технічні недоліки, наприклад, застаріле програмне забезпечення чи неправильно налаштовані мережеві пристрої, створюють сприятливе середовище для атак. Сучасні методи захисту корпоративних мереж різноманітні. Вони включають як технічні рішення, так і організаційні заходи. Використання міжмережевих екранів, VPN і систем виявлення вторгнень допомагає знизити ризики зовнішніх атак. Багатофакторна автентифікація та шифрування даних стають стандартами для забезпечення безпеки доступу до мережі.

Проте одних технологій недостатньо – важливу роль відіграє навчання персоналу основам кібергігієни, адже навіть найдосконаліший захист може бути зламаний через людську помилку. Однією з ключових проблем є те, що багато компаній недооцінюють важливість кібербезпеки. Відсутність регулярних аудитів, економія на безпекових рішеннях або ігнорування необхідності оновлення систем – це основні причини, через які організації залишаються вразливими. Ба більше, сучасні загрози стають дедалі складнішими: зловмисники використовують штучний інтелект для автоматизації атак, цілеспрямовані атаки часто важко

відрізнити від легітимного трафіку, а захист хмарних середовищ залишається для багатьох організацій нерозв’язаним завданням. Захист корпоративної мережі можна порівняти з оборонною фортецею, де кожен елемент грає важливу роль у стримуванні загроз. Але сучасний світ кібербезпеки вимагає не просто міцних стін – він вимагає гнучкості, адаптивності та передбачливості. Загрози еволюціонують, і корпорації, які не готові змінюватися, залишаються уразливими перед новими викликами. Однією з ключових проблем є те, що в багатьох організаціях захист мережі будується "реактивно", а не "проактивно". Це означає, що заходи впроваджуються лише після інциденту, замість того, щоб попереджати його. Наприклад, статистика показує, що значна частина атак відбувається через використання застарілого програмного забезпечення, в якому зловмисники легко знаходять вразливості. Але замість регулярного оновлення систем, багато компаній відкладають ці процеси, мотивуючи це зупинкою бізнес-процесів. Як результат – компрометація даних і величезні витрати на відновлення після атак.

Ще одна проблема – недостатній акцент на людському факторі. Більшість кібератак починаються з фішингових листів, у яких зловмисники обманюють працівників, змушуючи їх надати доступ до корпоративних систем. Найслабша ланка в будь-якій системі безпеки – це людина. Попри це, багато організацій не приділяють достатньо уваги навчанню своїх співробітників. Регулярні тренінги та імітації атак, як от фішингові кампанії, могли б значно знизити ризики. Складність сучасних корпоративних мереж також є викликом. Інтеграція хмарних рішень, використання віддаленого доступу, робота з підрядниками – усе це створює додаткові точки входу для зловмисників. Більшість традиційних методів захисту, таких як простий міжмережевий екран, більше не здатні забезпечити належний рівень безпеки. Потрібен новий підхід, зокрема впровадження концепції *Zero Trust*. Ця модель передбачає, що не можна довіряти жодному пристрою чи користувачу, навіть якщо вони знаходяться всередині мережі. Доступ надається лише за чіткими правилами, з урахуванням контексту: місцезнаходження, рівня авторизації, поведінкових факторів. Особливу увагу заслуговує і захист даних у хмарних середовищах. Зростання популярності таких сервісів, як Microsoft Azure, AWS та

Google Cloud, створює нові ризики. Багато компаній переконані, що провайдери хмарних послуг повністю відповідають за безпеку даних. Але насправді хмарна безпека працює за моделлю спільної відповідальності: провайдер відповідає за інфраструктуру, але за безпеку самих даних відповідає клієнт. Це вимагає впровадження додаткових засобів шифрування, контролю доступу та моніторингу. Не можна забувати і про кіберзлочинців, які постійно вдосконалюють свої методи. Сьогодні атаки часто автоматизовані, а зловмисники використовують штучний інтелект для знаходження вразливостей у системах. Це створює нові виклики для організацій, які мають адаптуватися до таких умов, використовуючи ті ж самі технології – автоматизацію процесів моніторингу, поведінковий аналіз та предиктивну аналітику. [1]

Підсумовуючи, можна сказати, що аналіз проблеми захисту корпоративної мережі виходить далеко за межі технічних рішень. Це стратегічне завдання, яке вимагає міждисциплінарного підходу, постійного вдосконалення процесів та активної участі всіх рівнів організації – від технічного персоналу до топменеджменту. Тільки системний підхід, заснований на сучасних технологіях, організаційних змінах і навчанні, може гарантувати надійний захист корпоративної мережі у світі, де загрози стають дедалі складнішими. Отже, проблема захисту корпоративної мережі є багатогранною і потребує системного підходу. Ефективний захист має базуватися на трьох основах: впровадження сучасних технологій, розробка чіткої стратегії безпеки та постійне навчання персоналу. Лише поєднання цих елементів дозволить зменшити ризики і забезпечити надійний захист для бізнесу.

Безпека є головною проблемою для більшості організацій, і багато керівників стурбовані кіберзагрозами. Це побоювання не безпідставне: 70% організацій, які зіткнулися з порушенням системи безпеки, повідомляють про значні або дуже значні збої в бізнесів результат.

Захист організації є критично важливим, але часто складним завданням. Команди безпеки повинні збирати, підтримувати, керувати та адаптувати складні середовища, використовуючи численні інструменти та служби від різноманітних

часто конкуруючих постачальників. Кількість пропозицій збільшується щороку, тому команди повинні постійно досліджувати, оцінювати та інтегрувати нові продукти в міру того, як змінюється ландшафт безпеки.

Крім того, серйозність і вартість порушень безпеки продовжують зростати. Витрати через втрату бізнесу та реагування на порушення у 2024 році зросли майже на 11% порівняно з попереднім роком. А середня вартість витоку даних у 2024 році підскочила до 4,88 млн доларів США з 4,45 млн доларів США у 2023 році.

Завдання, пов’язані з безпекою, можуть бути трудомісткими, виснажливими та схильними до помилок, коли потрібне втручання людини. Команди безпеки переповнені та не мають достатнього персоналу, а кількість організацій, які стикаються з критичною нестачею кваліфікованих працівників служби безпеки, зросла до 53% у 2024 році порівняно з 42% у 2023 році. Середня вартість злому, пов’язана з високим рівнем нестачі навичок безпеки підскочив до 5,74 млн доларів США в 2024 році з 5,36 млн доларів США в 2023 році, що на 7,1% збільшення.

Проте впровадження рішень на основі автоматизації та штучного інтелекту зростає. Кількість організацій, які активно використовують штучний інтелект безпеки та автоматизацію, зросла до 31% у 2024 році. Скрізь, де застосовують штучний інтелект та автоматизацію, вони прискорюють роботу з виявлення та локалізації порушень. Широке використання штучного інтелекту та автоматизації в ключових сферах безпеки — запобігання, виявлення, розслідування та реагування — скоротило середній час виявлення та локалізації порушень даних на 33% для реагування та на 43% для запобігання у 2024 році. Широка автоматизація та використання ШІ є також доведено, що середні витрати на злом значно нижчі порівняно з організаціями, які не використовують ці технології в ключових сферах безпеки.

### 1.2. Аналіз та класифікація загроз корпоративної мережі

Загрози корпоративної мережі постійно змінюються під впливом розвитку технологій і зростання складності мережевих систем. Вони можуть бути спрямовані на викрадення конфіденційної інформації, порушення роботи систем,

знищення даних або компрометацію корпоративної репутації. Загрози виникають як через технічні вразливості, так і через людський фактор. Наприклад, навіть найсучасніша система безпеки може бути скомпрометована через помилкові дії співробітників, такі як відкриття фішингового листа або використання слабких паролів. Тому розуміння загроз потребує системного підходу, який включає як технічні, так і організаційні аспекти. У сучасному цифровому світі корпоративні мережі є серцем функціонування організацій. Вони забезпечують доступ до критично важливих ресурсів, комунікацію між співробітниками, зберігання даних та управління бізнес-процесами.

Однак разом із широкими можливостями зростає і спектр загроз, які можуть порушити нормальне функціонування мережі. Для того щоб забезпечити надійний захист, необхідно глибоко розуміти природу цих загроз та класифікувати їх відповідно до різних критеріїв. Загрози корпоративної мережі постійно змінюються під впливом розвитку технологій і зростання складності мережевих систем. Вони можуть бути спрямовані на викрадення конфіденційної інформації, порушення роботи систем, знищення даних або компрометацію корпоративної репутації. Загрози виникають як через технічні вразливості, так і через людський фактор. Наприклад, навіть найсучасніша система безпеки може бути скомпрометована через помилкові дії співробітників, такі як відкриття фішингового листа або використання слабких паролів. [2] Тому розуміння загроз потребує системного підходу, який включає як технічні, так і організаційні аспекти.

Таблиця 1.1

Класифікація загроз корпоративної мережі

| | | |
|---|---|---|
| За джерелом | Зовнішні | Хакерські атаки |
| | | Шкідливе ПЗ |
| | | Фішинг |
| | Внутрішні | Інсайдерські атаки |
| | | Помилкові дії співробітників |
| | | Використання незахищених пристроїв |
| За методом дії | Мережеві атаки | Перехоплення даних |
| | | DNS-спуфінг |
| | | Сканування портів |
| | Загрози на рівні даних | Шифрувальники |
| | | Викрадення даних |
| | Програмні загрози | Віруси |
| | | Трояни |
| | | Руткіти |
| | Соціальна інженерія | Фішинг |
| | | Претекстинг |
| | | Baiting |
| За впливом на систему | Загрози конфіденційності | Викрадення персональних або корпоративних даних |
| | | Несанкціонований доступ до баз даних |
| | Загрози цілісності | Пошкодження або спотворення даних |
| | | Саботаж через внесення змін до програмного забезпечення |
| | Загрози доступності | Блокування доступу до ресурсів |
| | | Пошкодження мережевої інфраструктури |

Приклади загроз у корпоративних мережах (добавить под каждый подтип свою угрозу)

1. Ransomware-атаки

У 2021 році атака шифрувальника DarkSide паралізувала роботу Colonial Pipeline, що призвело до масштабної енергетичної кризи в США. Зловмисники вимагали викуп у криптовалюті, погрожуючи знищенням даних.

2. DDoS-атаки

Атака на сервери Amazon Web Services у 2020 році стала однією з найбільших у світі. Вона тривала понад три дні, перевантажуючи сервери масивним трафіком.

3. Соціальна інженерія

У 2020 році кіберзлочинці викрали облікові дані кількох співробітників Twitter, отримавши доступ до акаунтів знаменитостей, з яких публікували шахрайські оголошення.

Аналіз та класифікація загроз корпоративної мережі є фундаментальними кроками для побудови ефективної системи кіберзахисту. Загрози стають дедалі складнішими, і традиційні підходи більше не є достатніми. Необхідно впроваджувати новітні технології, розвивати культуру безпеки серед працівників та постійно вдосконалювати методи захисту. [3] Лише інтегрований підхід забезпечить стабільність і безпеку корпоративної мережі у сучасних умовах.

### 1.3. Типи критичних даних та наслідки атак

Критичні дані корпоративної мережі – це основа будь-якої організації, її найцінніший актив у цифрову епоху. Це інформація, без якої бізнес не може функціонувати, розвиватися чи ефективно конкурувати на ринку. Втрата або компрометація таких даних може завдати непоправної шкоди – від фінансових збитків до повного знищення репутації. Уявіть, що дані – це кровоносна система будь-якої організації. Без них компанія не може функціонувати, приймати рішення чи обслуговувати клієнтів. Саме тому захист критичних даних є настільки важливим, а їх втрата або компрометація може стати справжньою катастрофою.

Корпоративні мережі є не тільки платформами для обміну інформацією та обслуговування бізнес-процесів, але й містять величезну кількість критичних даних, які становлять значну цінність для організацій. Ці дані можуть бути ключем до фінансового благополуччя компанії, її конкурентоспроможності на ринку, а також до довіри клієнтів і партнерів. Однак зростаючі кіберзагрози змушують організації приділяти особливу увагу захисту цих даних. Витоки, викрадення чи знищення критичної інформації можуть спричинити не тільки фінансові втрати, а й серйозні репутаційні та юридичні наслідки. [4]

У цьому розділі буде розглянуто основні типи критичних даних, що зберігаються в корпоративних мережах, та потенційні наслідки їх компрометації. Кожен тип даних має свої особливості, рівень чутливості та вимоги до захисту, тому важливо детально зрозуміти, яка інформація є найбільш вразливою до атак. Крім того, важливим аспектом є наслідки таких атак: як вони можуть вплинути на фінансовий стан, репутацію компанії, а також на її здатність виконувати операційні функції. Розуміння цих аспектів допоможе розробити ефективну стратегію захисту та забезпечити надійну безпеку корпоративної мережі.

Критичні дані в корпоративних мережах мають різний характер і класифікуються за кількома важливими параметрами, які визначають підходи до їхнього захисту. Три основні аспекти, які потрібно враховувати, це **конфіденційність**, **доступність** і **цілісність**. Кожен із цих аспектів відіграє ключову роль у побудові ефективної системи кіберзахисту.

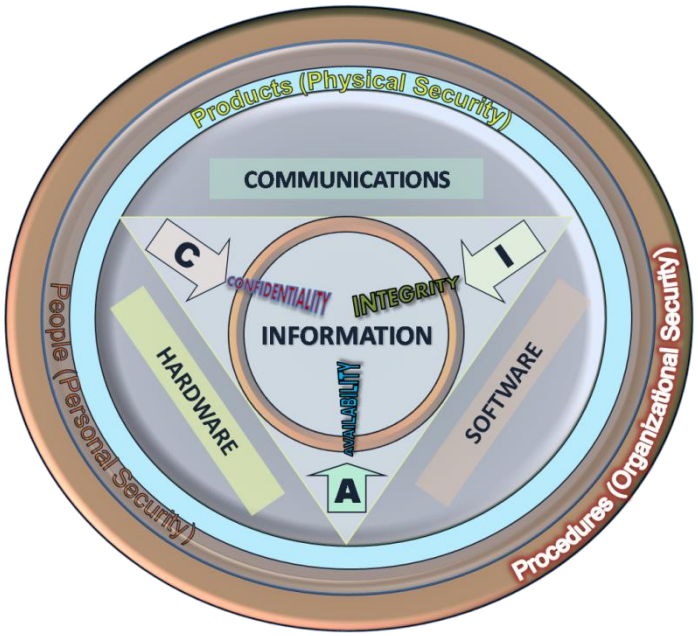



Рис. 1.1 - Основи інформаційної безпеки

**1. Конфіденційність**

Конфіденційність критичних даних означає, що до них мають доступ лише уповноважені особи. Основна мета – запобігти несанкціонованому доступу, розголошенню чи використанню інформації. Типи даних, для яких конфіденційність є пріоритетною:

- **Персональні дані**: Імена, адреси, фінансова інформація клієнтів чи співробітників. Порушення конфіденційності таких даних може призвести до фінансових втрат, репутаційних збитків та судових позовів.
- **Комерційні та стратегічні дані**: Бізнес-плани, маркетингові стратегії, технічна документація, інноваційні розробки. Розголошення цих даних може бути використане конкурентами, що поставить компанію у невигідне становище.
- **Юридичні документи**: Контракти, ліцензії, судові матеріали. Їхня компрометація може спричинити правові наслідки.

Методи забезпечення конфіденційності:

- Шифрування даних на всіх етапах обробки.

- Обмеження доступу за допомогою ролей (role-based access control, RBAC).
- Впровадження багатофакторної аутентифікації.

**2. Доступність**

Доступність даних означає, що критична інформація завжди має бути доступною для уповноважених користувачів, особливо у критичних моментах. Втрата доступності може зупинити бізнес-процеси і завдати значної шкоди.

Дані, для яких доступність є критично важливою:

- **Операційні дані**: Інформація, необхідна для функціонування виробничих ліній, систем управління запасами чи логістичних процесів. Перерви у доступі до цих даних можуть призвести до зупинки роботи підприємства.
- **Фінансова інформація**: Дані, необхідні для проведення транзакцій, підготовки звітності чи прийняття фінансових рішень. Їхня недоступність може викликати затримки у платежах, порушення контрактів або втрату довіри партнерів.
- **Системні журнали (лог-файли)**: Їх відсутність у критичний момент може ускладнити аналіз інцидентів безпеки або відновлення систем.

Методи забезпечення доступності:

- Впровадження систем резервного копіювання та відновлення (backup and recovery).
- Використання кластерних систем і мережевих резервів.
- Захист від DDoS-атак, які спрямовані на блокування доступу до систем.

**3. Цілісність**

Цілісність даних означає, що інформація залишається точною, повною і незмінною, якщо зміни не були санкціоновані. Порушення цілісності може спричинити спотворення даних, яке вплине на процес прийняття рішень або навіть на репутацію компанії.

Типи даних, для яких цілісність є основною вимогою:

- **Фінансова звітність**: Невідповідність даних у фінансових документах може викликати підозру в шахрайстві чи ненадійності компанії.

- **Юридичні документи**: Некоректність або зміни у контрактах, договорах чи ліцензіях можуть призвести до юридичних суперечок.
- **Операційні дані**: Зміна інформації про виробничі процеси може призвести до збоїв у роботі або дефектів у продукції.

Методи забезпечення цілісності:

- Використання контрольних сум (checksums) для перевірки цілісності файлів.
- Системи журналювання, які відстежують усі зміни в даних.
- Захист від внутрішніх загроз, включаючи розмежування доступу і моніторинг дій співробітників. [5]

**Різноманітність критичних даних у контексті корпоративної мережі**

У корпоративних мережах критичні дані охоплюють широкий спектр інформації, від стратегічно важливих до операційно необхідних. Їх різноманітність вимагає диференційованого підходу до захисту, залежно від того, який аспект – конфіденційність, доступність чи цілісність – є пріоритетним.

Наприклад, у фінансових транзакціях найбільше значення має конфіденційність і цілісність даних. У виробничих системах акцент робиться на доступності, адже навіть короткочасний збій може спричинити серйозні наслідки. Водночас, юридичні дані вимагають високого рівня цілісності, оскільки будь-які зміни можуть мати довгострокові наслідки. [6]

Глибоке розуміння різноманітності критичних даних дозволяє побудувати більш детальну та структуровану систему захисту інформації в корпоративній мережі. У дипломній роботі це знання може бути використане для розробки рекомендацій з побудови ефективної стратегії кібербезпеки, що враховує специфіку даних компанії та потенційні загрози.

Крім того, дослідження цих аспектів допоможе обґрунтувати вибір технологій захисту та проілюструвати важливість комплексного підходу до безпеки даних у сучасному цифровому середовищі. [7]

**Висновки до розділу 1**

Аналіз необхідності захисту корпоративної мережі демонструє, наскільки критичним є забезпечення інформаційної безпеки в сучасному бізнес-середовищі. Усі аспекти корпоративних даних – від їх конфіденційності до доступності та цілісності – грають вирішальну роль у стабільній роботі організації. Втрата контролю над цими аспектами може спричинити фінансові збитки, репутаційні втрати, юридичні проблеми або навіть повне припинення діяльності.

Критичні дані, які включають фінансову інформацію, комерційні стратегії, персональні дані співробітників і клієнтів, операційні показники та юридичну документацію, є об’єктом підвищеної уваги з боку зловмисників. Кібератаки, спрямовані на ці дані, не лише компрометують їхню конфіденційність, але й загрожують доступності важливих бізнес-процесів і цілісності інформації. Особливу небезпеку становлять складні атаки, такі як DDoS, фішинг, програмне забезпечення-вимагач та інші методи, що еволюціонують у відповідь на сучасні захисні механізми.

Однією з ключових проблем у захисті корпоративної мережі є необхідність дотримання балансу між забезпеченням доступності даних для співробітників і мінімізацією ризику їх компрометації. Це вимагає впровадження багаторівневих систем захисту, які включають шифрування, багатофакторну аутентифікацію, системи моніторингу та аналізу мережевої активності, а також регулярне оновлення політик і технологій безпеки. [8]

Важливим є також розуміння, що кібербезпека – це не лише технічна, але й організаційна задача. Навчання персоналу, регулярне тестування систем безпеки, розробка планів реагування на інциденти – усе це є невід’ємними компонентами комплексної стратегії захисту корпоративної мережі.

Таким чином, захист корпоративної мережі є не просто технічною необхідністю, а стратегічним завданням, яке визначає стійкість і довговічність бізнесу. Глибоке розуміння природи критичних даних, їхньої різноманітності та можливих наслідків атак дозволяє організації не лише реагувати на загрози, але й проактивно запобігати їм, забезпечуючи стабільний розвиток у цифровому світі. [9]

# 2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

## 2.1. Методи та засоби захисту корпоративної мережі

Сучасні корпоративні мережі є основою функціонування бізнесу, забезпечуючи обмін даними, доступ до ресурсів та інтеграцію з глобальними інформаційними системами. Водночас вони залишаються мішенню для численних кіберзагроз, які постійно еволюціонують, набуваючи дедалі складніших форм.

Для забезпечення стійкості корпоративної мережі необхідно впроваджувати комплексний підхід до її захисту, який включає різноманітні методи і засоби, орієнтовані на запобігання атакам, виявлення загроз і нейтралізацію їх наслідків. У цьому підрозділі розглядаються основні технології та інструменти, що застосовуються для захисту корпоративних мереж, зокрема системи виявлення і запобігання вторгнень, фільтрація трафіку, сегментація мережі, а також перспективні підходи, що базуються на штучному інтелекті та автоматизації процесів. [10]

Комплексний аналіз доступних рішень дозволяє побудувати ефективну модель захисту, яка відповідає потребам сучасних підприємств і мінімізує ризики, пов’язані з інформаційною безпекою.

Захист корпоративної мережі передбачає впровадження різноманітних методів і засобів, які забезпечують конфіденційність, цілісність та доступність даних. Існує цілий ряд технологій, інструментів і методів захисту.

**Методи захисту**

**1. Фільтрація трафіку**

Один із ключових методів захисту корпоративної мережі, спрямований на контроль і моніторинг даних, які проходять через мережу. Основна мета фільтрації – забезпечити, щоб лише дозволений і безпечний трафік потрапляв до мережевих ресурсів, запобігаючи проникненню шкідливого коду або несанкціонованого доступу.

- **Міжмережеві екрани (Firewall)**: Обмежують доступ до мережі, блокуючи небезпечний або неавторизований трафік. Бувають апаратними, програмними та гібридними.
- **Системи глибокої перевірки пакетів (DPI)**: Аналізують вміст трафіку, виявляючи шкідливий вміст у реальному часі.

Ці інструменти дозволяють мінімізувати ризики, пов'язані з атаками, контролюючи потоки даних і забезпечуючи стабільність корпоративної мережі.

**2. Сегментація мережі**

Метод розділення корпоративної мережі на менші, логічно або фізично ізольовані сегменти. Мета цього підходу – обмежити поширення загроз, підвищити безпеку та оптимізувати управління трафіком.

- **Віртуальні локальні мережі (VLAN)**: Поділяють мережу на сегменти, зменшуючи ризик поширення атак у випадку компрометації однієї з зон.
- **Мережі з нульовою довірою (Zero Trust Networks)**: Реалізують суворий контроль доступу до всіх сегментів мережі незалежно від внутрішнього або зовнішнього походження трафіку.

Сегментація дозволяє зменшити ризик компрометації всієї мережі, ізолюючи критичні ресурси та обмежуючи вплив можливих атак.

**3. Контроль доступу**

Контроль доступу є ключовим елементом захисту корпоративної мережі, який забезпечує доступ до ресурсів лише авторизованим користувачам і пристроям.

- **Системи управління доступом (IAM)**: Визначають, хто і до яких ресурсів має доступ. Включають багатофакторну аутентифікацію (MFA) та динамічний контроль доступу.
- **Network Access Control (NAC)**: Аналізують і контролюють пристрої, що підключаються до мережі, перевіряючи відповідність політикам безпеки.

Ефективний контроль доступу знижує ризик несанкціонованого проникнення та втрату даних, забезпечуючи захист від внутрішніх і зовнішніх загроз.

**4. Моніторинг і аналітика**

Моніторинг і аналітика є важливими компонентами захисту корпоративної мережі, що забезпечують постійний нагляд за її станом, виявлення загроз і реагування на інциденти.

- **Системи управління інформацією та подіями безпеки (SIEM)**: Збирають, аналізують і корелюють події з різних джерел для виявлення загроз.
- **Системи аналізу поведінки користувачів і пристроїв (UEBA)**: Виявляють аномальну поведінку, яка може свідчити про кібератаку.

Ці інструменти дозволяють не лише виявляти потенційні атаки, але й проактивно запобігати їм, мінімізуючи вплив на бізнес.

**5. Шифрування даних**

Шифрування даних є важливим методом захисту конфіденційної інформації в корпоративній мережі, що гарантує її захист від несанкціонованого доступу, навіть якщо дані будуть перехоплені.

- Захищає дані під час передачі (протоколи TLS, IPsec) і зберігання (шифрування дисків, баз даних).
- Реалізація криптографічних стандартів (AES, RSA) для гарантування конфіденційності.

Шифрування гарантує конфіденційність, навіть якщо зловмисники отримають доступ до зашифрованих даних, забезпечуючи їх незрозумілість без відповідного ключа дешифрування.

**6. Резервне копіювання та відновлення**

Резервне копіювання та відновлення є критично важливими для забезпечення безпеки даних у корпоративній мережі. Ці процеси гарантують, що у разі втрати або пошкодження даних можна відновити важливу інформацію без значних втрат.

- Регулярне створення резервних копій важливих даних із зберіганням у безпечних і географічно віддалених місцях.
- Використання інструментів для швидкого відновлення після збоїв або атак, таких як програмне забезпечення для резервного копіювання (Acronis, Veeam).

Процес відновлення передбачає швидке повернення даних до робочого стану після інцидентів, таких як атаки з використанням шкідливого ПЗ або відмови

обладнання, що допомагає мінімізувати час простою та зберегти бізнес-операції. [11]

**Засоби захисту**

**1. Антивірусні системи та системи боротьби зі шкідливим ПЗ**

Антивірусні системи та системи боротьби зі шкідливим ПЗ є важливими інструментами для захисту корпоративних мереж від вірусів, троянів, руткітів та інших шкідливих програм. Вони здійснюють моніторинг, виявлення та нейтралізацію загроз, що можуть спричинити шкоду даним або компрометувати безпеку мережі.

- Використовуються для виявлення та нейтралізації шкідливих програм (McAfee, Symantec, Kaspersky).
- Системи захисту кінцевих точок (Endpoint Detection and Response, EDR) забезпечують додатковий рівень моніторингу.

Ці системи допомагають знижувати ризик зараження корпоративної мережі, попереджаючи її від атак через інфіковані файли чи шкідливі програми.

**2. Системи виявлення та запобігання вторгнень (IDPS)**

Системи виявлення та запобігання вторгнень (IDPS) є критичними компонентами захисту корпоративних мереж, що поєднують функції моніторингу, виявлення загроз і запобігання атакам у реальному часі. IDPS аналізує мережевий трафік або активність на кінцевих точках, щоб виявити аномалії або спроби зловмисного доступу.

- **SNORT** – система IDS/IPS, яка аналізує пакети в реальному часі та забезпечує гнучкість у налаштуванні правил для виявлення вторгнень.

Багато людей знають 1998 як рік виходу Windows 98, але це був також час, коли Martin Roesch вперше випустив у світ Snort. Хоча тоді Snort не був справжнім IDS, зараз все змінилося. завдяки величезному внеску до IT-спільноти.

Важливо відзначити, що Snort не має графічного інтерфейсу або простий у використанні адміністративної консолі, хоча до цього були створені багато інших інструментів з відкритим вихідним кодом, такі як BASE і Sguil Ці утиліти мають веб-інтерфейс для запитів і аналізу попереджень, що надходять від Snort IDS.

- **Suricata** – потужна система для аналізу мережевого трафіку, що забезпечує виявлення загроз, моніторинг і аналіз з можливістю роботи як IDS/IPS.

Що можна використовувати окрім Snort? Звичайно ж, Suricata. Хоча її архітектура відрізняється від Snort, вона поводиться так само, як і ця програма, і може використовувати ті ж сигнатури. Що чудово, так це те, що Suricata має ще більший функціонал. Вона здатна багато на що, правду кажучи.

Існують і сторонні інструменти з відкритим вихідним кодом, у яких є веб-інтерфейс для запитів та аналізу попереджень, що надходять від ідентифікаторів Suricata.

- **Bro/Zeek** – система для аналізу мережевих подій, що спеціалізується на виявленні аномалій і забезпеченні моніторингу для виявлення зловмисної активності.

Bro була перейменована на Zeek наприкінці 2018 року і іноді згадується в статтях як BroIDS або non-Zeek-IDS. Вона трохи відрізняється від Snort та Suricata. У якомусь сенсі Bro це і сигнатура, і ідентифікатор аномалії. Її механізм аналізу перетворює захоплений трафік на серію подій. Подія може бути ім'ям користувача FTP, підключенням до веб-сайту або ще. Потужність системи полягає в інтерпретаторі сценаріїв політики. Цей механізм політики має власну мову (Bro-Script) і може виконувати деякі універсальні завдання. [12]

Якщо користувач є аналітиком і запитує: «Як я можу автоматизувати частину своєї роботи?», тоді це той самий інструмент, який він шукав. Людина хоче завантажити файли та надіслати їх на аналіз шкідливих програм. Інструмент повідомить його, якщо виявлено проблему, а потім внесе джерело до чорного списку і вимкне комп'ютер користувача. Шаблони використання мережі можна відстежувати після того, як він зв'язався з IP-адресою з бази даних.

Якщо користувач не аналітик, йому буде складно. Оскільки інструмент був розроблений як експеримент, він спочатку не фокусувався на таких речах, як GUI, зручність його використання та простота установки. Він не має власного графічного інтерфейсу, але є сторонні інструменти з відкритим вихідним кодом, доступні для

отримання запитів та аналізу попереджень, що надходять від Bro-IDS. Наприклад, ELK stack.

- **SnortSam** – розширення для SNORT, яке дає змогу автоматично реагувати на загрози, блокуючи їх через міжмережеві екрани.

Модуль, який інтегрується зі SNORT для автоматичного блокування зловмисного трафіку. Його головна функція полягає у швидкому реагуванні на виявлені загрози, додаючи правила блокування до міжмережевих екранів у реальному часі. SnortSam підтримує широкий спектр фаєрволів, таких як Cisco ASA, Check Point, iptables тощо. Працюючи разом із SNORT, SnortSam отримує інформацію про потенційні загрози через сигнатури або аномалії трафіку, а потім передає команди блокування на фаєрвол. Це дозволяє миттєво запобігти подальшому розповсюдженню шкідливої активності в мережі. SnortSam є ефективним інструментом для покращення роботи IDS, оскільки додає до неї функціонал активного реагування, забезпечуючи додатковий рівень захисту для корпоративної мережі.

- **OSSEC** – система виявлення вторгнень, яка зосереджена на моніторингу логів і забезпеченні автоматичного реагування на загрози в реальному часі.

В області повнофункціональних інструментів з відкритим кодом є тільки OSSEC. Хороша новина полягає в тому, що OSSEC дуже хороша, що вона робить.

OSSEC працює практично на будь-якій операційній системі і включає клієнт-серверну архітектуру управління та ведення журналів, що дуже важливо. Локальні HIDS можуть бути скомпрометовані в той же час, що і ОС, необхідно щоб інформація про безпеку та криміналістику залишила хост і була збережена в іншому місці якнайшвидше, щоб уникнути будь-якого роду фальсифікації, які б запобігли виявленню. [13]

Архітектура клієнт-сервер OSSEC включає цю стратегію шляхом доставки попереджень і журналів на централізований сервер, де аналіз і повідомлення можуть відбуватися навіть у тому випадку, якщо хост-система відключена або скомпрометована. Ще однією перевагою архітектури клієнт-сервер є можливість

централізованого керування агентами з одного сервера. Оскільки кількість розгортань може змінюватись від однієї до декількох тисяч установок, здатність вносити глобальні зміни з центрального сервера має вирішальне значення для адміністратора.

Під час обговорення OSSEC (та інших HIDS) часто виникає питання щодо встановлення програмного забезпечення на критично важливих серверах. Слід зазначити, що установка OSSEC надзвичайно легка (установник важить менше 1 МБ), і більшість аналізу фактично відбувається на сервері, що означає, що OSSEC займає трохи місця на хості. OSSEC також має можливість відправляти журнали ОС на сервер для аналізу та зберігання, що особливо корисно на машинах Windows, які не мають власних та кросплатформових механізмів ведення журналу. [14]

- **Cisco Firepower**: Пропонує виявлення та блокування загроз із інтегрованими функціями управління.

Платформа для забезпечення мережевої безпеки, яка інтегрує різноманітні засоби захисту в одному рішенні. Вона забезпечує багаторівневий захист корпоративних мереж, поєднуючи функції міжмережевого екрану (NGFW), системи виявлення та запобігання вторгнень (IPS), контролю додатків, захисту від шкідливого ПЗ та інструменти для аналізу загроз.

Ключовою особливістю Cisco Firepower є її здатність забезпечувати глибокий огляд трафіку завдяки використанню сучасних технологій аналізу. Вона не лише виявляє загрози, але й автоматично реагує на них у реальному часі. Система підтримує адаптивний підхід до безпеки: з кожною новою атакою вона вдосконалюється за рахунок інтеграції з хмарними сервісами для аналізу загроз, такими як Cisco Talos.

Firepower дозволяє сегментувати мережу, забезпечувати шифрування даних і застосовувати політики безпеки на основі ролей користувачів. Завдяки зручному інтерфейсу адміністратори можуть легко налаштовувати правила та моніторити безпеку мережі. Це робить Cisco Firepower ідеальним вибором для організацій, які прагнуть надійного і масштабованого захисту.

Ці інструменти є ефективними у боротьбі з кіберзагрозами та забезпечують необхідний рівень безпеки для корпоративних мереж.

**3. Системи запобігання витокам даних (DLP)**

Системи запобігання витокам даних (DLP) призначені для захисту конфіденційної інформації в корпоративних мережах, запобігаючи її несанкціонованому розповсюдженню або витоку. [15] DLP-системи контролюють і аналізують потік даних, виявляючи спроби передачі або доступу до чутливих даних, таких як персональні дані, фінансова інформація чи корпоративні секрети.

- Забезпечують контроль і захист конфіденційної інформації від несанкціонованого доступу, передачі чи копіювання. Приклади: Symantec DLP, McAfee Total Protection for Data Loss Prevention.

Ці системи допомагають компаніям захистити свою інформацію, знижуючи ризики витоку даних і відповідальність за порушення конфіденційності.

**4. Захист веб-додатків (WAF)**

Захист веб-додатків (WAF, Web Application Firewall) — це система безпеки, яка забезпечує захист веб-додатків від різноманітних атак, таких як SQL-ін'єкції, кросс-сайтні скрипти (XSS), атаки типу "відмова в обслуговуванні" (DoS) та інші загрози, орієнтуючись на захист прикладних рівнів.

- Web Application Firewall (WAF) захищає веб-додатки від таких загроз, як SQL-ін'єкції, XSS-атаки. Популярні рішення: Cloudflare WAF, Imperva.

WAF є ефективним інструментом для захисту веб-додатків на прикладному рівні, що дозволяє знизити ризики експлуатації вразливостей додатків і забезпечити їх безпеку в реальному часі.

**5. Системи захисту електронної пошти**

Системи захисту електронної пошти призначені для запобігання кіберзагрозам, пов'язаним з електронною поштою, таких як спам, фішинг, віруси та шкідливе ПЗ. Вони допомагають захистити корпоративну пошту від несанкціонованих доступів, витоків даних і атак через електронні повідомлення.

- Захищають від фішингових атак і шкідливих вкладень. Засоби: Mimecast, Proofpoint, Microsoft Defender for Office 365.

Ці системи забезпечують безпечну комунікацію через електронну пошту, знижуючи ризики витоків даних і захищаючи від загроз.

**6. Захист від DDoS-атак**

Захист від DDoS-атак (атаки відмови в обслуговуванні з розподіленим навантаженням) спрямований на запобігання перенавантаженню мережі або серверів корпоративної мережі шляхом великої кількості фальшивих запитів, що надходять одночасно з різних джерел.

- Використання спеціалізованих платформ (Cloudflare, Akamai, Arbor Networks) для аналізу та нейтралізації великих обсягів шкідливого трафіку.

Ці заходи допомагають зберегти доступність корпоративних сервісів і мереж у разі великих атак, знижуючи ризики простоїв і збитків.

**7. Платформи оркестрації та автоматизації безпеки (SOAR)**

Платформи оркестрації та автоматизації безпеки (SOAR) використовуються для автоматизації процесів реагування на інциденти, оркестрації між різними засобами безпеки та покращення ефективності операцій з кібербезпеки. SOAR платформи допомагають знижувати час реакції на загрози та забезпечувати кращу координацію між командами безпеки.

- Інструменти типу Splunk Phantom або Palo Alto Cortex дозволяють автоматизувати реагування на загрози, зменшуючи час на їх ліквідацію.

SOAR платформи допомагають оптимізувати діяльність безпекових команд, зменшуючи ручну працю та час на реагування на інциденти, тим самим покращуючи загальний рівень безпеки в корпоративній мережі.

**Перспективні технології захисту**

Перспективні технології захисту корпоративних мереж зосереджені на використанні новітніх досягнень у галузі кібербезпеки для боротьби з дедалі складнішими загрозами. Ці технології обіцяють підвищення ефективності, швидкості та масштабованості захисту.

- **Штучний інтелект і машинне навчання**: Використовуються для прогнозування та виявлення нових видів атак. Інструменти, як Darktrace, аналізують поведінку в мережі в реальному часі.

- **Мережева віртуалізація та ізоляція**: Застосування SDN (Software-Defined Networking) для більш гнучкого управління мережевими політиками.
- **Блокчейн для захисту даних**: Використання децентралізованих підходів для гарантії цілісності та автентичності даних, застосування технологій блокчейн для захисту від фальсифікації даних і забезпечення прозорості в управлінні доступом.

Ці технології дозволяють адаптуватися до нових викликів кібербезпеки і забезпечити високий рівень захисту в умовах швидко змінюваного цифрового середовища.

### 2.2. Архітектура SNORT IDPS

Архітектура SNORT IDPS (Intrusion Detection and Prevention System) складається з кількох ключових компонентів, які забезпечують виявлення, аналіз і запобігання вторгненням у мережу. SNORT є модульною системою, що дозволяє налаштовувати її для різних завдань і середовищ, роблячи її універсальним інструментом для захисту мережі. Побудована на модульному принципі, який забезпечує її універсальність, гнучкість і масштабованість. Ця архітектура дозволяє ефективно інтегрувати різні функціональні компоненти, кожен з яких виконує чітко визначену роль у процесі виявлення та запобігання вторгнень. Завдяки такій структурі SNORT може адаптуватися до різних потреб і сценаріїв використання — від моніторингу невеликих локальних мереж до забезпечення безпеки розгалужених корпоративних систем.

Архітектура включає кілька основних елементів, таких як модуль перехоплення трафіку, який відповідає за отримання даних із мережі; попередня обробка, де відбувається аналіз і нормалізація трафіку; та ядро аналізу, яке працює на основі набору правил і сигнатур. Кожен із цих компонентів тісно пов’язаний із системою правил, що постійно оновлюється, та забезпечує можливість точного виявлення відомих загроз, таких як атаки за сигнатурами, і аналіз аномалій, які можуть сигналізувати про нові або невідомі загрози.

Модульність архітектури дозволяє розширювати функціональність SNORT через інтеграцію додаткових інструментів і плагінів. Наприклад, система може бути налаштована для роботи в якості простого аналізатора трафіку, а також як комплексне рішення для запобігання вторгнень, яке автоматично блокує шкідливу активність. Це досягається завдяки можливості поєднувати SNORT із міжмережевими екранами, антивірусними системами, SIEM-платформами та іншими рішеннями.

SNORT забезпечує різноманітні режими роботи, що відповідають потребам різних користувачів. Наприклад, у режимі перехоплення система просто відображає пакети мережевого трафіку, дозволяючи адміністраторам переглядати його в реальному часі. У режимі журналювання дані записуються у вигляді логів для подальшого аналізу, що є корисним для розслідування інцидентів або проведення аудиту. Найпотужнішим є режим виявлення та запобігання вторгнень, який об’єднує можливості аналізу трафіку в реальному часі, виявлення загроз і миттєвого реагування. [16]

Архітектура SNORT підтримує високу продуктивність і ефективність завдяки використанню сучасних алгоритмів аналізу трафіку та оптимізації обробки даних. Відкрита природа системи дозволяє спільноті розробників і користувачів постійно вдосконалювати її компоненти, додаючи нові можливості та покращуючи продуктивність. Завдяки цьому SNORT залишається одним із найпоширеніших і найпотужніших рішень для забезпечення мережевої безпеки, яке використовується як у невеликих організаціях, так і у великих корпораціях.

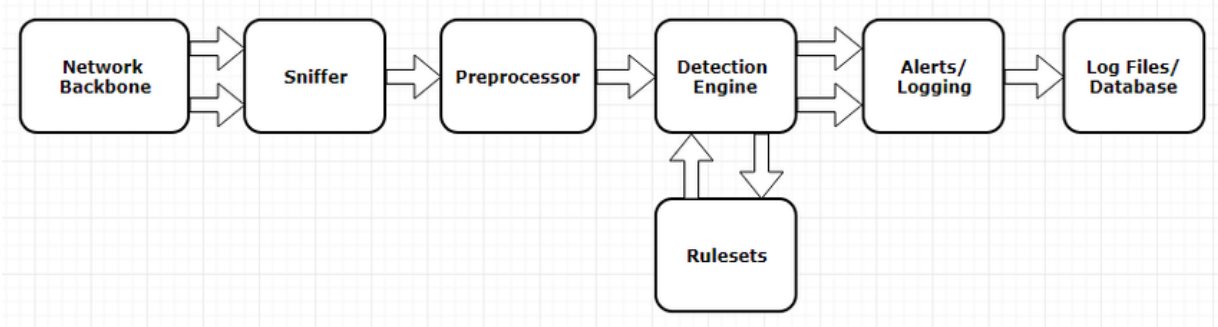



Рис.2.1 - Архітектура SNORT

**Основні компоненти архітектури SNORT :**

**Sniffer-модуль (Пакетний захоплювач)**

Цей модуль відповідає за перехоплення мережевого трафіку. Він копіює пакети, які проходять через мережевий інтерфейс, і передає їх для подальшої обробки. Використовуються бібліотеки, такі як libpcap, для ефективного збору трафіку.

**Модуль попередньої обробки (Preprocessors)**

Після перехоплення трафіку він проходить попередню обробку. Цей етап включає:

- Нормалізацію трафіку: усунення різних аномалій, які можуть вплинути на подальший аналіз.

- Фрагментацію пакетів: збір даних, розділених на кілька частин, для кращого аналізу.

- Виявлення сесій: групування пакетів у контекст користувацьких сесій. Попередньо оброблений трафік стає більш структурованим і зручним для аналізу.

**Модуль аналізу та виявлення загроз (Detection Engine)**

Це ядро системи SNORT. Модуль використовує набір правил і сигнатур для перевірки кожного пакета:

**- Сигнатурний аналіз**: Порівняння пакета із шаблонами атак.

**- Аналіз аномалій**: Виявлення відхилень від нормального трафіку.

**- Stateful Inspection**: Врахування контексту і стану сесій для більш точного виявлення загроз. Результат роботи цього модуля — сповіщення про виявлені загрози або прийняття рішення про блокування.

**База правил (Rules Database)**

Правила SNORT описують, як ідентифікувати потенційні загрози. Вони складаються з умов (наприклад, сигнатур атак) і дій (сповіщення, блокування тощо). База правил регулярно оновлюється спільнотою та розробниками для врахування нових типів атак.

**Модуль обробки результатів (Output Plugins)**

Цей модуль відповідає за запис і передачу результатів аналізу:

- Генерація сповіщень (в реальному часі чи в логах).

- Інтеграція з іншими системами (наприклад, SIEM).

- Збереження даних у різних форматах (текстові файли, бази даних, syslog тощо).

**Переваги архітектури SNORT**

1. **Модульність**

Кожен компонент працює незалежно, що дозволяє легко додавати нові функції чи оновлювати існуючі.

2. **Гнучкість**

SNORT можна налаштовувати для роботи у невеликих локальних мережах або масштабованих корпоративних середовищах.

3. **Відкритий код**

SNORT — це програмне забезпечення з відкритим кодом, що робить його доступним для розширення та налаштування під специфічні потреби.

4. **Широка підтримка спільноти**

Активна спільнота користувачів і розробників забезпечує регулярне оновлення правил і швидке реагування на нові загрози.

**Обмеження архітектури SNORT**

1. **Високі вимоги до ресурсів**

При великому обсязі трафіку можуть виникати затримки через необхідність обробки великої кількості правил.

2. **Потреба в експертних знаннях**

Для ефективного налаштування і підтримки SNORT потрібен досвід у кібербезпеці.

Архітектура SNORT IDPS забезпечує потужний, масштабований і гнучкий захист корпоративних мереж. Завдяки модульному підходу та активній спільноті, SNORT залишається одним із найпопулярніших рішень для виявлення та запобігання вторгненням у мережу. [17] Його інтеграція з іншими системами безпеки робить його незамінним компонентом сучасної стратегії кіберзахисту.

## 2.3. Призначення та функції SNORT IDPS

SNORT — це потужна система виявлення вторгнень (IDS) і система запобігання вторгненням (IPS) з відкритим кодом, яка забезпечує аналіз мережевого трафіку в реальному часі та реєстрацію пакетів даних. SNORT використовує мову на основі правил, яка поєднує методи перевірки аномалій, протоколів і сигнатур для виявлення потенційно зловмисної активності.

Використовуючи SNORT, мережеві адміністратори можуть виявляти атаки відмови в обслуговуванні (DoS) і розподілені атаки DoS (DDoS), атаки на загальний інтерфейс шлюзу (CGI), переповнення буфера та невидиме сканування портів. SNORT створює низку правил, які визначають зловмисну мережеву активність, ідентифікують шкідливі пакети та надсилають сповіщення користувачам.

Мова правил SNORT визначає, який мережевий трафік потрібно збирати та що має відбуватися, коли він виявляє шкідливі пакети. [18] Це значення нюхання можна використовувати так само, як сніфери та системи виявлення мережевих вторгнень для виявлення зловмисних пакетів або як повне мережеве IPS-рішення, яке відстежує мережеву активність, виявляє та блокує потенційні вектори атак.

**Особливості SNORT**

Існують різні функції, які роблять SNORT корисним для мережевих адміністраторів для моніторингу їхніх систем і виявлення зловмисної активності. До них належать:

- Монітор трафіку в реальному часі

SNORT можна використовувати для моніторингу трафіку, який надходить і виходить з мережі. Він відстежуватиме трафік у режимі реального часу та видаватиме сповіщення користувачам, коли виявлятиме потенційно шкідливі пакети чи загрози в мережах Інтернет-протоколу (IP).

- Протоколювання пакетів

SNORT дозволяє реєструвати пакети в режимі реєстратора пакетів, що означає, що він записує пакети на диск. У цьому режимі SNORT збирає кожен пакет і записує його в ієрархічний каталог на основі IP-адреси хост-мережі.

- Аналіз протоколу

SNORT може виконувати аналіз протоколу, який є процесом мережевого аналізу, який фіксує дані на рівнях протоколу для додаткового аналізу. Це дає змогу адміністратору мережі додатково досліджувати потенційно зловмисні пакети даних, що має вирішальне значення, наприклад, у специфікації протоколу стека протоколу керування передачею/IP (TCP/IP).

- Відповідність вмісту

SNORT порівнює правила за протоколом, таким як IP і TCP, потім за портами, а потім за тими з вмістом і без. Правила, у яких є вміст, використовують збіг кількох шаблонів, що підвищує продуктивність, особливо коли мова йде про такі протоколи, як протокол передачі гіпертексту (HTTP). Правила, які не мають змісту, завжди оцінюються, що негативно впливає на продуктивність.

- Відбитки ОС

Відбитки операційної системи (ОС) використовують концепцію, згідно з якою всі платформи мають унікальний стек TCP/IP. За допомогою цього процесу SNORT можна використовувати для визначення платформи ОС, яка використовується системою, яка звертається до мережі.

- Можна встановити в будь-якому мережевому середовищі

SNORT можна розгорнути на всіх операційних системах, включаючи Linux і Windows, і як частину всіх мережевих середовищ.

- Відкритий код

Як частина програмного забезпечення з відкритим вихідним кодом, SNORT є безкоштовним і доступним для всіх, хто хоче використовувати IDS або IPS для моніторингу та захисту своєї мережі.

- Правила легко реалізувати

Правила SNORT легко впроваджувати та забезпечувати роботу моніторингу та захисту мережі. Його мова правил також є дуже гнучкою, а створювати нові

правила досить просто, що дозволяє мережевим адміністраторам відрізняти звичайну активність в Інтернеті від аномальної чи зловмисної активності.

**Режими SNORT**

Є три різні режими, у яких можна запускати SNORT, які залежатимуть від прапорів, які використовуються в команді SNORT.

- Сніффер пакетів

Режим аналізу пакетів SNORT означає, що програмне забезпечення читатиме IP-пакети, а потім відображатиме їх користувачеві на консолі.

- Логер пакетів

У режимі реєстратора пакетів SNORT реєструватиме всі IP-пакети, які відвідують мережу. Тоді адміністратор мережі може побачити, хто відвідував його мережу, і отримати уявлення про ОС і протоколи, які вони використовували.

- NIPDS (Система виявлення та запобігання вторгненню в мережу)

У режимі NIPDS SNORT реєструватиме лише пакети, які вважаються шкідливими. Він робить це за допомогою попередньо встановлених характеристик шкідливих пакетів, які визначені в його правилах. Дії, які виконує SNORT, також визначаються правилами, встановленими адміністратором мережі. [19]

**Основні функції SNORT**

**Підписне виявлення (Signature-Based Detection)**

Snort використовує бібліотеку правил для аналізу мережевого трафіку. Ці правила створені для виявлення специфічних шаблонів поведінки, характерних для атак. Наприклад, відомі шаблони DoS-атак або експлуатації конкретних вразливостей.

**Аномальне виявлення (Anomaly-Based Detection)**

Хоча ця функція менш поширена в Snort, вона може бути інтегрована для розпізнавання аномальної активності на основі аналізу базової поведінки мережі. Це корисно для виявлення нових, ще невідомих загроз.

**Передобробка даних (Preprocessor)**

Передобробники дозволяють декодувати мережеві пакети, перевіряти протоколи та створювати умови для більш глибокого аналізу.

**Журналювання та звітування**

Усі події, які система вважає підозрілими, логуються у вигляді звітів. Це спрощує аналіз інцидентів, виявлення тенденцій і планування заходів безпеки.

**Інтеграція та розширюваність**

Snort підтримує інтеграцію з багатьма іншими інструментами, такими як SnortSam, SIEM-платформи або аналітичні системи. Це робить її частиною більшої екосистеми захисту.

**Для чого використовуються правила SNORT?**

Правила, визначені в SNORT, дозволяють програмному забезпеченню виконувати низку дій, які включають:

- Виконання аналізу пакетів

SNORT можна використовувати для аналізу пакетів, який збирає всі дані, які передаються в мережу та з неї. [20] Збір окремих пакетів, які надходять до та від пристроїв у мережі, дозволяє детально перевірити, як передається трафік.

- Налагодження мережевого трафіку

Після реєстрації трафіку SNORT можна використовувати для налагодження шкідливих пакетів і будь-яких проблем конфігурації.

- Створення сповіщень

SNORT генерує сповіщення для користувачів, як визначено в діях правил, створених у файлі конфігурації. Щоб отримувати сповіщення, правила SNORT мають містити умови, які визначають, коли пакет слід вважати незвичайним або зловмисним, ризики використання вразливостей і можуть порушувати політику безпеки організації або становити загрозу для мережі.

- Створення нових правил

SNORT дозволяє користувачам легко створювати нові правила в програмному забезпеченні. Це дозволяє мережевим адміністраторам змінювати те, як вони хочуть, щоб перетворення SNORT працювало для них, і процеси, які воно має виконувати. Наприклад, вони можуть створювати нові правила, які вказують SNORT запобігати бекдор-атакам, шукати певний вміст у пакетах, показувати мережеві дані, вказувати, яку мережу контролювати, і друкувати сповіщення на консолі.

- Розрізняти звичайну діяльність в Інтернеті та зловмисну діяльність

Використання правил SNORT дає змогу мережевим адміністраторам легко відрізнити звичайну очікувану активність в Інтернеті від усього, що виходить за межі норми. SNORT аналізує мережеву активність у реальному часі, щоб виявити шкідливу активність, а потім генерує сповіщення для користувачів.

**Переваги SNORT**

- Відкритість та безкоштовність: Snort — це програмне забезпечення з відкритим вихідним кодом, яке можна використовувати без ліцензійних обмежень.
- Гнучкість: Завдяки розширюваності Snort можна адаптувати до потреб будь-якої мережі.
- Широка підтримка спільноти: Постійне оновлення правил та рекомендацій.

**Висновки до розділу 2**

Було розглянуто основні методи та засоби захисту корпоративної мережі, які забезпечують її стабільне функціонування та захист від зовнішніх і внутрішніх загроз. Особливу увагу було приділено технології SNORT IDPS, як одній із ключових систем для виявлення та запобігання вторгнень. Дослідження показали, що інтеграція таких рішень дозволяє організаціям ефективно реагувати на сучасні виклики у сфері кібербезпеки.

Розгляд методів захисту, зокрема, фільтрації трафіку, сегментації мережі, контролю доступу, шифрування даних, резервного копіювання, а також засобів виявлення загроз, таких як антивірусні системи та IDPS, дозволяє сформувати комплексний підхід до захисту мережевої інфраструктури. Це забезпечує конфіденційність, цілісність та доступність інформації, що є критично важливим для ефективного функціонування корпоративних мереж.

Особливу увагу було приділено сучасним технологіям, як-от захист веб-додатків (WAF), системам запобігання витокам даних (DLP), платформам

оркестрації та автоматизації безпеки (SOAR) та іншим інноваційним рішенням, які забезпечують багаторівневий захист мережі. Також було досліджено перспективні напрями розвитку, включаючи інтеграцію із системами на основі штучного інтелекту, що дозволяє вдосконалити процеси моніторингу та аналізу загроз.

Таким чином, другий розділ підтвердив необхідність використання комплексного підходу до захисту корпоративних мереж. [21] Поєднання традиційних методів із сучасними інноваціями дозволяє створювати стійкі та ефективні системи безпеки, які здатні забезпечити стабільну роботу організацій у швидко змінюваних умовах кіберзагроз.

# 3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ SNORT IDPS

## 3.1. Розгортання та налаштування технології захисту корпоративної мережі на основі SNORT IDPS

Розгортання та налаштування технології захисту корпоративної мережі на основі SNORT IDPS є ключовим етапом у створенні ефективної системи кібербезпеки. Цей процес передбачає встановлення програмного забезпечення, його адаптацію до потреб конкретної мережі та інтеграцію з існуючою інфраструктурою. Важливість правильної конфігурації SNORT обумовлена його здатністю оперативно виявляти та запобігати загрозам, мінімізуючи ризики для даних і систем підприємства. У цьому підрозділі буде розглянуто основні кроки розгортання системи, починаючи з підготовки середовища, налаштування правил та тестування, і закінчуючи оптимізацією для забезпечення високої продуктивності.

Для цієї роботи було використано операційну систему Ubuntu.

Для встановлення SNORT потрібно ввести команду *sudo apt-get install snort -y*

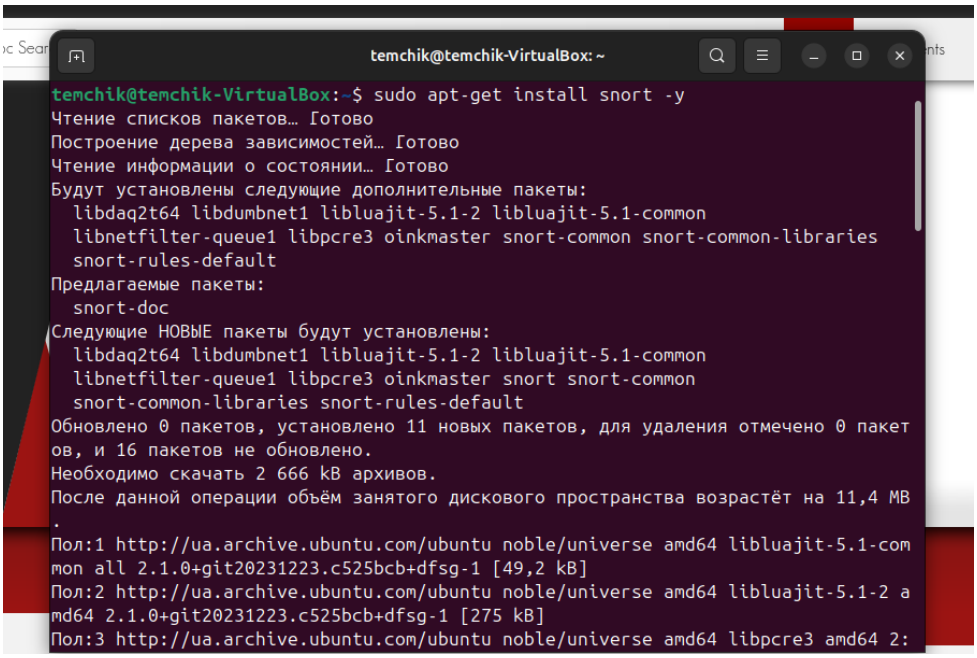



Рис.3.1 Встановлення SNORT

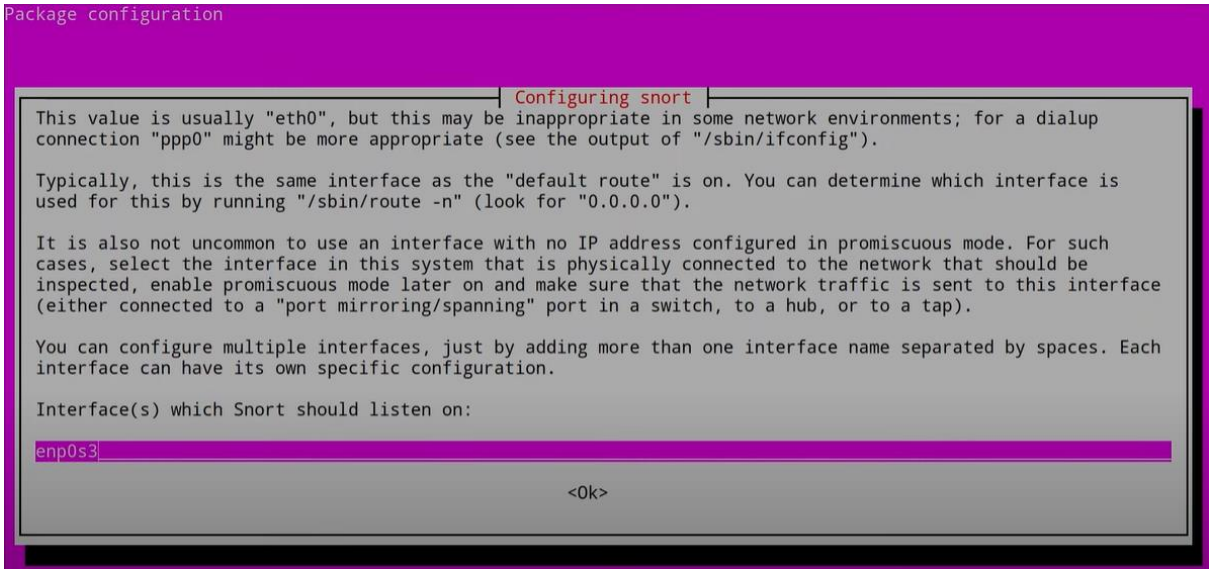



Рис.3.2 Вибір інтерфейсу

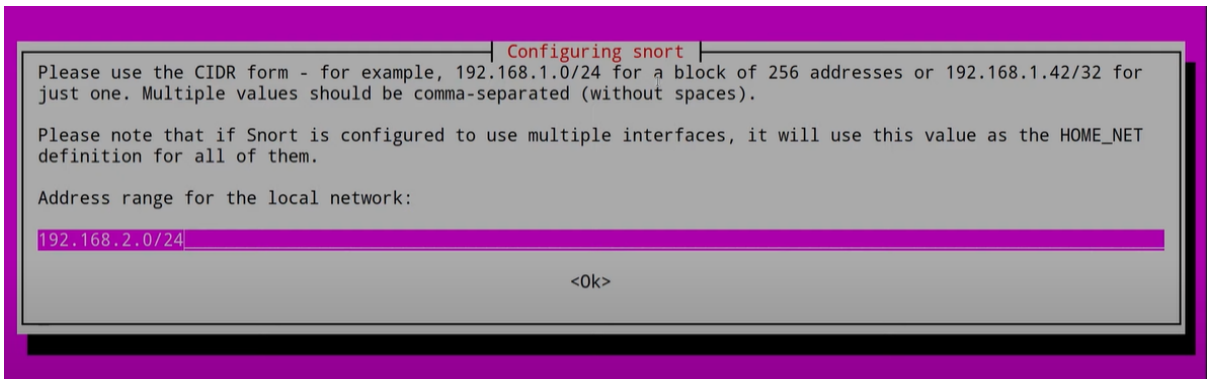



Рис.3.3 Вибір фактичного діапазону мережі

Після цього перевіряємо чи встановилась програма

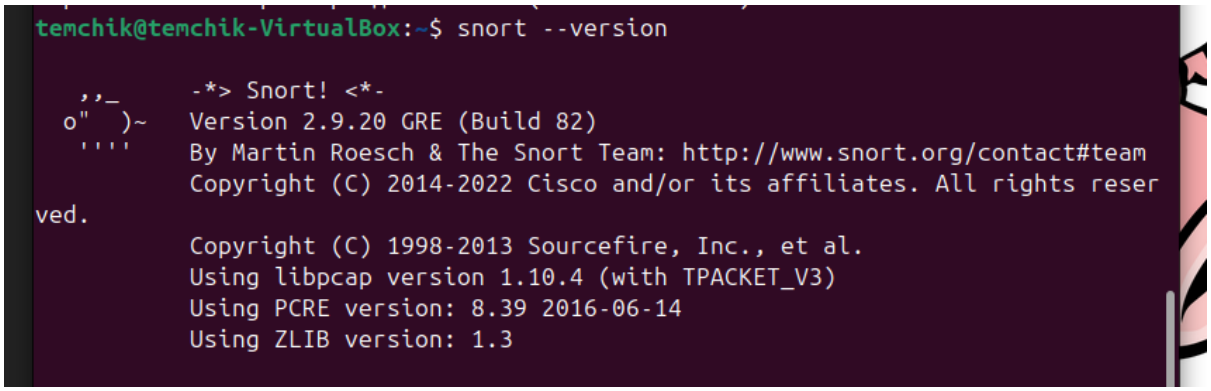



Рис.3.4 Показ версії SNORT

Встановлено версію SNORT 2.9.20 (Build 82).

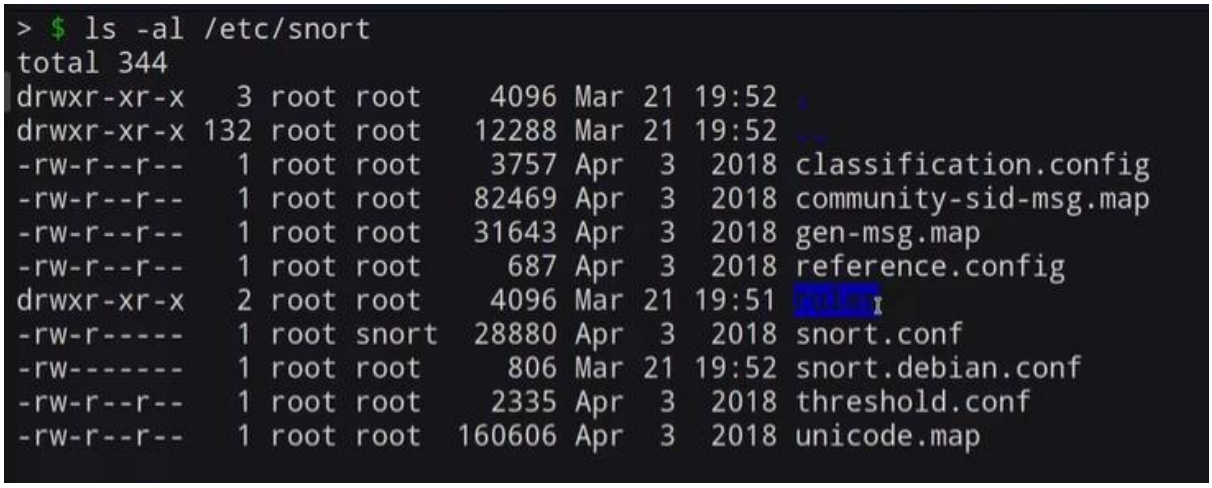


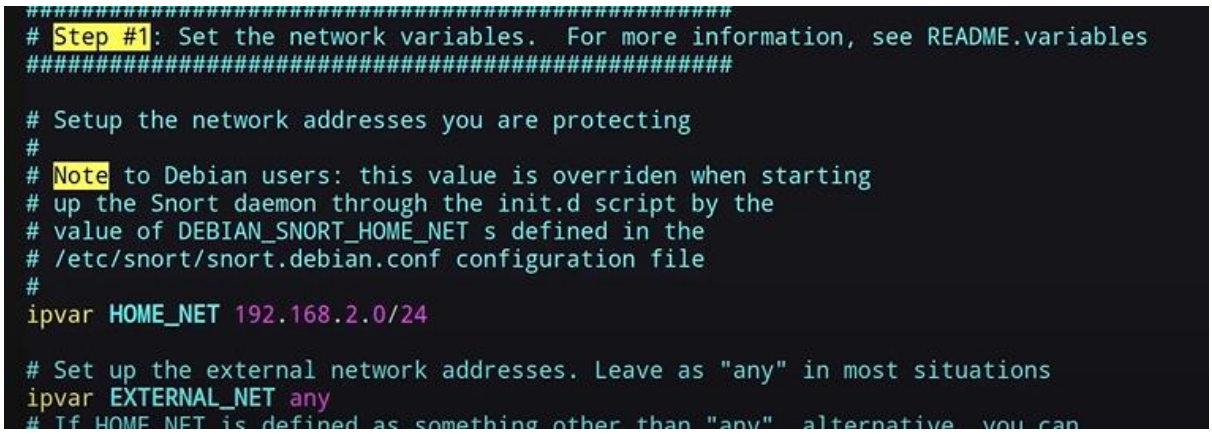

Рис.3.5 Перевірка файлового наповнення

Попередньо SNORT запакований із кількома правилами спільноти та декількома правилами розробленими самими SNORT. Найважливіший файл в конфігурації є snort.conf, це ядро функціоналу.

Після вводу команди *sudo vim /etc/snort/snort.conf* з'являється файл конфігурації.

Перший розділ – розділ індексів у файлі конфігурації, він охоплює процес налаштування мережевих змінних, потім ми зможемо налаштувати декодер базового виявлення, двигун, перепроцесори, вихідні плагіни, набір правил тощо.

Тепер найважливіші параметри будуть на першому кроці, де ми встановлюємо мережеві змінні. Прокручуємо до змінної IP (HOME_NET)? Де ми вказуємо фактичну мережу, яку хочемо контролювати




Ри.3.6 Налаштування контрольованої мережі

В параметрі EXTERNAL_NET залишаємо any тому що ми не хочемо обмежувати змінну певною мережею, бо атаки та вторгення можуть надходити з будь-якої мережі.

У файлі local.rules знаходяться правила які ми самостійно можемо використовувати та змінювати, тому наразі він порожній.

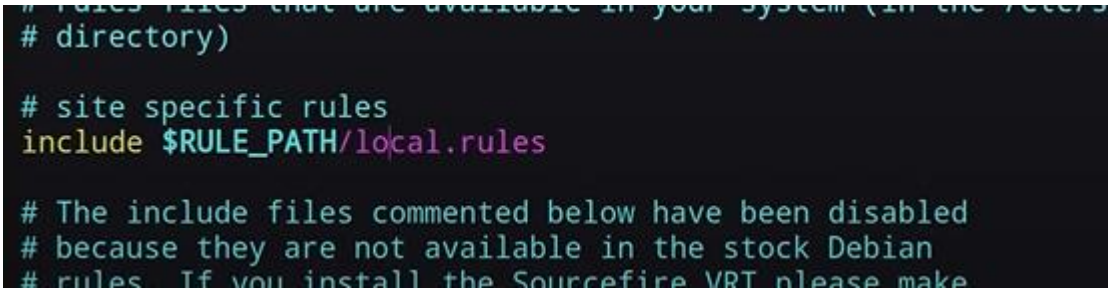



Рис.3.7 Файл з правилами

Після запуску SNORT запускає два файли, що дозволяє нам розмежувати особисті правила та правила написати SNORT. Це дуже комфортно, бо ми можемо організовувати свої правила, наприклад DDoS, DNS, DoS, SQL-Injector та інші.

Нам потрібна перевірка чи якісь зміни які ми робили є дійсними, і чи є взагалі якісь синтаксичні помилки, тому треба вказати команду *sudo snort -T -i enp3s0 -c /etc/snort/snort.conf*

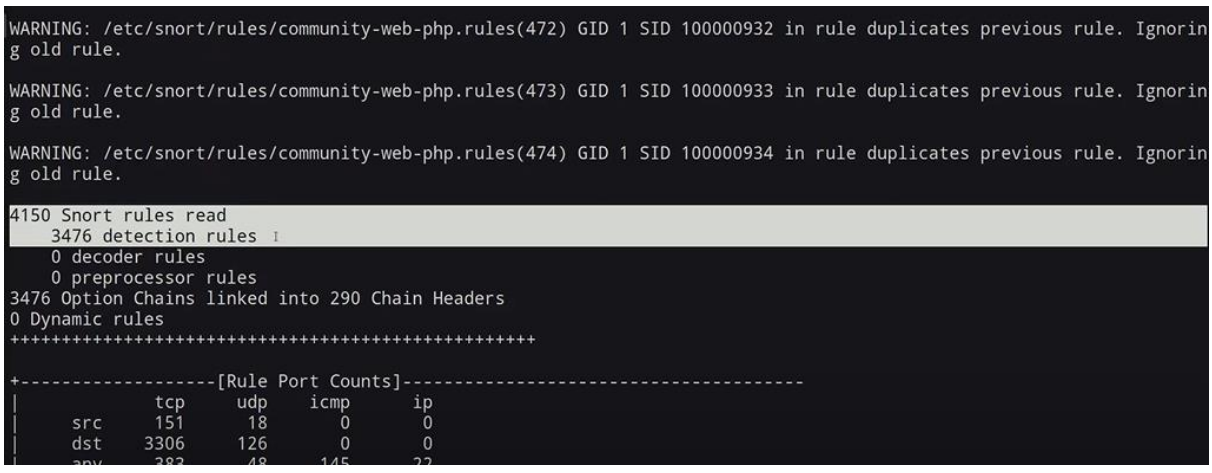



Рис.3.8 Перевірка правил

Загалом 4150 правил SNORT та 3476 правил виявлення.

### 3.2. Технологія захисту корпоративної мережі на основі SNORT IDPS

Почнемо з відкриття пустого файлу local.rules командою *sudo vim /etc/snort/local.rules*


Рис.3.9 Конфігураційний файл local.rules

Прописуємо *alert icmp any any -> $HOME_NET any (msg:"ICMP Ping Detected"; sid:100001; rev:1;)*

Нам потрібно, щоб видавало сповіщення (alert icmp) з будь якої мережі та будь-якого порту (any any) що приходить у нашу мережу ($HOME_NET) з нашим портом (any) і видавало повідомлення (msg), далі вказуємо ідентифікатор підпису (sid), потім ми можемо вказати версії для певних правил. Тепер ми можемо робити інші правила.

Важливим параметром є alert-mode.

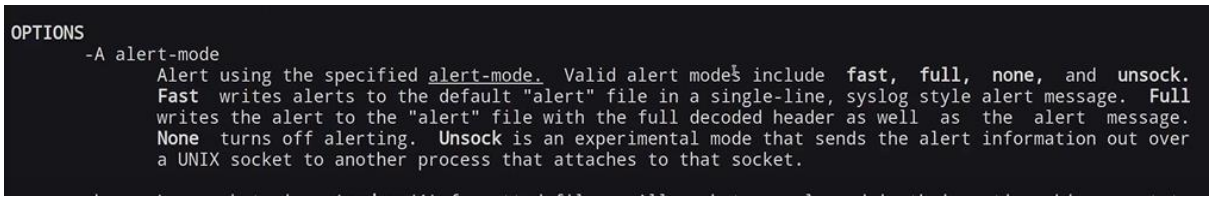



Рис.3.10 Показ моду


Рис.3.11 Команда для початку роботи зі сповіщеннями

Запускаємо віртуальну машину Linux та прописуємо команду для перевірки ping 192.168.2.157. Повертаємось в Ubuntu SNORT та бачимо сповіщення.

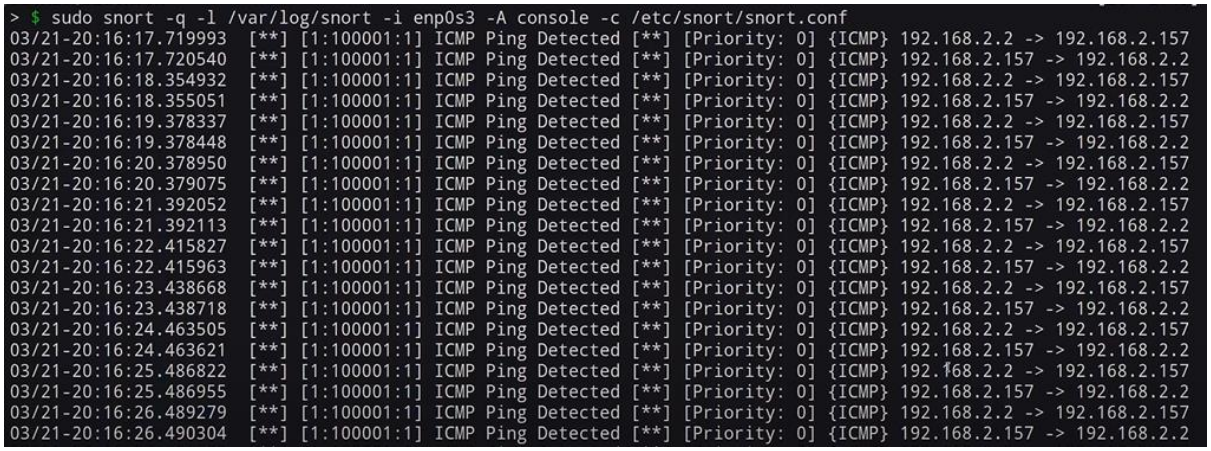



Рис.3.12 Сповіщення безпеки SNORT

Бачимо виявлення пінгу та основі створеного нами правила.

Тепер напишемо правило для з’єднань SSH, оскільки це може бути дуже важливим для моніторингу в мережі. Повертаємось в local.rules та прописуємо правило та не забуваємо що SSH працює на TCP, будемо вибирати конкретний порт 22, оскільки правило не працюватиме

*alert tcp any any -> $HOME_NET 22 (msg:”SSH Authentication Attempt”; sid:100002; rev:1)*

Виходимо з Ubuntu та заходимо в Linux для перевірки правила. Спробуйте побачити з точки зору захисника, як виглядає ця мережева активність і якщо ми

написали правила для цього, то ми повинні мати можливість виявити що робиться в мережі, це суть виявлення вторгнень і аналізу мережевого трафіку. У випадку виявлення вторгнень у мережу ми налаштовуємо наш аналіз мережевого трафіку, щоб ідентифікувати та автоматизувати процес виявлення вторгнень або загроз. Тому знов запускаємо SNORT та вписуємо команду *sudo snort -q -l /var/log/snort -I enp0s3 -A console -c /etc/snort/snort.conf*

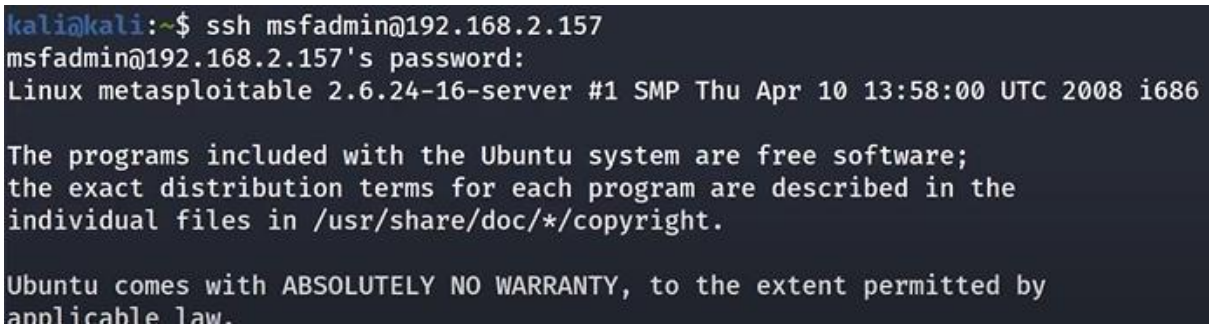



Рис.3.13 Запуск перевірки другого правила

Перемикаємо назад і бачимо, що ми отримуємо сповіщення та правило працює.

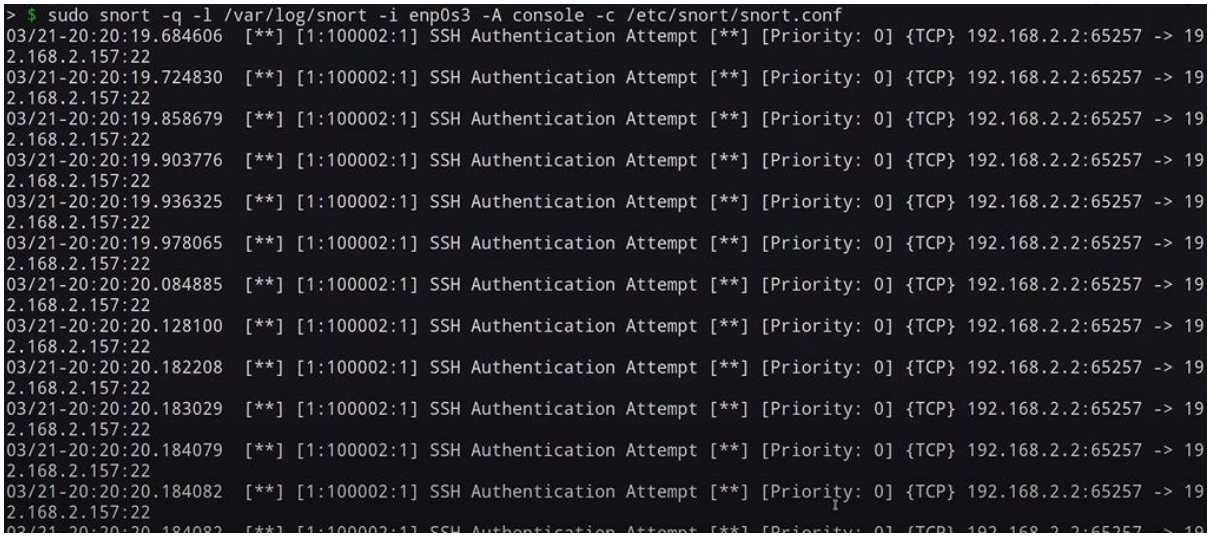



Рис.3.14 Сповіщення про авторизацію від другого правила

За допомогою сайту http://www.cyb3rs3c.net/ ми можемо генерувати правила. Спробуємо створити правило 100003 автентифікації FTP для нашої мережі 192.168.2.157 з окремим портом 21 за допомогою SNORPY.


Рис.3.15 Інтерфейс SNORPY

Зупиняємо SNORT за допомогою команди quit та вставляємо скопійоване правило *alert tcp any any -> 192.168.2.157 21 ( msg:"FTP Authentication Attemp On MS2"; sid:100003; rev:1 )*

Знов запускаємо SNORT з командою *sudo snort -q -l /var/log/snort -I enp0s3 -A console -c /etc/snort/snort.conf* та автентифікуємось за допомогою Kali.

```
kali@kali:~$ ftp 192.168.2.157 21
Connected to 192.168.2.157.
220 (vsFTPd 2.3.4)
Name (192.168.2.157:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Рис.3.16 Спроба автентифікації FTP


Рис.3.17 Сповіщення третього правила

### 3.3. Розроблення рекомендацій щодо застосування технології захисту корпоративної мережі на основі SNORT IDPS

Корпоративні мережі, що забезпечують безперервну діяльність компаній, зберігання та обробку великих обсягів конфіденційної інформації, перебувають під постійною загрозою атак. У таких умовах актуальність застосування технологій, що забезпечують надійний захист інформаційної інфраструктури, є надзвичайно високою. Одним із найбільш ефективних інструментів захисту є система виявлення та запобігання вторгнень SNORT IDPS, яка пропонує потужний функціонал для моніторингу мережі, виявлення аномалій і протидії загрозам.

**Попередній аналіз інфраструктури**

Рекомендації щодо впровадження технології SNORT IDPS повинні починатися з аналізу поточного стану мережевої інфраструктури. Проведення повного аудиту дозволяє визначити слабкі місця мережі, критичні вузли та потенційні вектори атак. Увагу слід звернути на топологію мережі, розподіл ресурсів і розташування серверів та інших ключових елементів. Важливим етапом є класифікація сегментів мережі залежно від їхньої важливості та чутливості даних, що передаються.

- Інвентаризація інфраструктури

Визначення всіх елементів мережі: серверів, клієнтських пристроїв, маршрутизаторів, комутаторів, точок доступу.

Оцінка характеристик обладнання: потужності, пропускної здатності, наявних оновлень.

Документування топології мережі, включаючи схеми підключень і маршрутизації.

- Аналіз мережевого трафіку

Моніторинг обсягів і характеру трафіку, що циркулює в мережі.

Ідентифікація пікових навантажень та критичних точок пропуску трафіку.

Виявлення потенційних вузьких місць, які можуть обмежити продуктивність SNORT IDPS.

- Аудит безпеки

Перевірка існуючих політик безпеки та механізмів захисту.

Оцінка наявності вже впроваджених систем безпеки, таких як брандмауери, VPN, або антивірусні програми.

Визначення вразливих сегментів мережі, які можуть стати об’єктом атак.

- Виявлення критичних активів

Ідентифікація ключових елементів інфраструктури, таких як сервери баз даних, файлові сховища, поштові сервери.

Визначення конфіденційної інформації або ресурсів, які потребують максимального рівня захисту.

- Аналіз загроз

Виявлення типових атак, які раніше мали місце в мережі, наприклад, DDoS, фішингові атаки, експлойти.

Оцінка ризиків, пов’язаних із використанням застарілого обладнання чи ненадійного ПЗ.

Врахування галузевих особливостей, які можуть впливати на рівень загроз.

- Вимоги до продуктивності

Оцінка навантаження, яке буде створене SNORT IDPS на наявну інфраструктуру.

Визначення необхідності масштабування обладнання чи мережевих ресурсів.

- Інструменти для попереднього аналізу

- Пакетні аналізатори (Packet Sniffers): Wireshark, Tcpdump.
- Мережеві сканери: Nmap, Nessus, OpenVAS.
- Інструменти моніторингу: Zabbix, Nagios, SolarWinds.

Результати аналізу

Попередній аналіз дозволяє:

- Сформувати чітке уявлення про мережеву інфраструктуру.
- Ідентифікувати всі активи, які потребують захисту.
- Визначити необхідні налаштування SNORT IDPS, зокрема правила фільтрації трафіку, розташування сенсорів, потреби в ресурсах.

Ретельно проведений попередній аналіз допомагає знизити кількість помилок під час налаштування SNORT IDPS, мінімізувати ризики пропуску атак і забезпечити стабільну роботу мережі. Це етап, який створює фундамент для ефективного впровадження системи захисту, адаптованої до потреб конкретної організації.

**Вимоги до апаратного та програмного забезпечення**

Для ефективної роботи SNORT IDPS важливо забезпечити відповідність апаратної бази вимогам системи. Зокрема, сервери, на яких розгортається система, повинні мати багатоядерні процесори, які дозволяють обробляти великі обсяги трафіку в реальному часі, а також оперативну пам’ять обсягом не менше 4-8 ГБ. Використання швидкісних мережевих адаптерів дозволяє знизити затримки під час моніторингу трафіку. На рівні операційної системи рекомендується обирати стабільні платформи Linux (Ubuntu, CentOS), які забезпечують гнучкість налаштувань і надійну підтримку.

1. Апаратні вимоги

SNORT IDPS є гнучким рішенням, яке може працювати як на мінімальному обладнанні для малих мереж, так і на високопродуктивних серверах для великих підприємств. Основні апаратні вимоги включають:

-Процесор:

Для невеликих мереж достатньо сучасного процесора із двома ядрами (наприклад, Intel i3 або AMD Ryzen 3).

Для середніх і великих мереж рекомендується використовувати серверні процесори із багатоядерною архітектурою (Intel Xeon, AMD EPYC), які можуть обробляти великий обсяг трафіку в реальному часі.

-Оперативна пам’ять (RAM):

Для базової роботи SNORT мінімально необхідно 4 ГБ оперативної пам’яті.

Для великих мереж із високим рівнем навантаження рекомендується не менше 16-32 ГБ.

-Накопичувач (HDD/SSD):

Обсяг дискового простору залежить від вимог до зберігання журналів (логів) та баз даних.

Рекомендовано використовувати SSD для пришвидшення доступу до даних, з мінімальним обсягом 250 ГБ для малих мереж і від 1 ТБ для великих інфраструктур.

-Мережева карта (NIC):

Гігабітні або швидші мережеві карти (1 Gbps або 10 Gbps) є критично важливими для аналізу мережевого трафіку в реальному часі.

Для великих мереж можуть знадобитися спеціалізовані NIC із підтримкою віддзеркалення портів (port mirroring).

-Додаткове обладнання:

У складних інфраструктурах може бути доцільним використання виділених серверів для бази даних правил або моніторингу трафіку.

2. Програмні вимоги

SNORT є кросплатформним рішенням і підтримує встановлення на різних операційних системах. Програмні вимоги можна розділити на основне та допоміжне ПЗ:

-Операційна система:

Linux (рекомендуються дистрибутиви Ubuntu, CentOS, RHEL або Debian).

Підтримується також Windows, але для виробничих середовищ частіше обирають Linux через його надійність і налаштовуваність.

-Залежності:

Libpcap — для захоплення мережевого трафіку.

DAQ (Data Acquisition Library): SNORT використовує DAQ для інтеграції з мережевими інтерфейсами.

PCRE (Perl Compatible Regular Expressions): бібліотека для підтримки розширених правил.

-Менеджери правил:

Snorby, BASE або Squil для управління правилами та перегляду логів.

-Додаткове ПЗ:

Barnyard2: використовується для обробки логів.

MySQL/PostgreSQL: бази даних для зберігання інформації про атаки.

Apache/Nginx: для веб-інтерфейсу моніторингу.

3. Мережеві вимоги

-Трафік:

Пропускна здатність залежить від обсягу аналізованого трафіку. Для великих мереж із інтенсивним трафіком (понад 10 Гбіт/с) може знадобитися масштабування інфраструктури.

-Інтеграція:

SNORT можна інтегрувати з іншими системами, такими як SIEM (Security Information and Event Management) або брандмауери.

4. Рекомендації

Провести попередній аналіз інфраструктури перед визначенням вимог до обладнання.

Залишити запас потужності апаратного забезпечення для подальшого масштабування.

Забезпечити регулярне оновлення як операційної системи, так і самого SNORT.

5. Мінімальні вимоги для навчальних середовищ

-Для тестування або навчальних цілей можна використовувати віртуальні машини з мінімальними ресурсами:

2 ядра процесора.

2 ГБ оперативної пам’яті.

20 ГБ дискового простору.

-Мережевий інтерфейс із доступом до віртуальної або фізичної мережі.

**Налаштування базових правил**

Одним із ключових етапів розгортання SNORT IDPS є налаштування правил виявлення загроз. База правил SNORT оновлюється регулярно, що дозволяє системі вчасно реагувати на нові типи атак. Проте стандартні правила часто потребують адаптації до конкретної мережі, що дозволяє зменшити кількість хибнопозитивних спрацювань. Наприклад, у мережах із специфічним трафіком варто налаштовувати виключення для законних, але нетипових пакетів.

1. Формат правил SNORT

Правила SNORT пишуться в текстових файлах і складаються з двох основних частин:

- Заголовок правила — визначає основні параметри, такі як протокол, IP-адресу джерела та призначення, порти та напрямок трафіку.
- Опції правила — містять додаткові умови для виявлення загроз, такі як сигнатури атак, дані про зміст пакету, маркери часу тощо.

Приклад базового правила:

*alert tcp any any -> 192.168.1.0/24 80 (msg:"HTTP traffic detected"; sid:100001; rev:1;)*

Це правило сповіщає про HTTP-трафік, що надходить до мережі 192.168.1.0/24.

2. Категорії базових правил

Базові правила поділяються за типами атак і загроз, серед яких:

- Мережеві атаки: сканування портів, DoS/DDoS.
- Протокольні порушення: аномалії в роботі TCP, UDP, ICMP.
- Атаки на додатки: SQL-ін'єкції, XSS.
- Виявлення шкідливого ПЗ: сигнатури вірусів або троянів.

3. Основні файли для правил

SNORT використовує кілька ключових файлів:

- snort.conf — головний конфігураційний файл, де вказується шлях до правил і основні параметри налаштування.
- Файли правил, наприклад: local.rules, community.rules, emerging-threats.rules.
  - Local.rules — для локально визначених правил, які створює користувач.
  - Community.rules — попередньо налаштовані правила спільноти

4. Налаштування файлу snort.conf

У конфігураційному файлі необхідно:

1. Визначити шляхи до файлів правил:

*include $RULE_PATH/local.rules*

*include $RULE_PATH/community.rules*

2. Налаштувати змінні для мережевих сегментів:

*var HOME_NET 192.168.1.0/24*

*var EXTERNAL_NET any*

3. Активувати або деактивувати певні категорії правил залежно від потреб.

5. Створення власних правил

Для забезпечення гнучкості SNORT дозволяє створювати власні правила у файлі local.rules. Наприклад:

Виявлення спроб доступу до заборонених портів:

*alert tcp any any -> any 22 (msg:"SSH access attempt"; sid:100002; rev:1;)*

Виявлення передачі даних із ключовими словами:

*alert tcp any any -> any any (content:"password"; nocase; msg:"Sensitive data leakage"; sid:100003; rev:1;)*

6. Тестування та налагодження

1. Перевірка правил на помилки:

*snort -T -c /etc/snort/snort.conf*

2. Аналіз логів після запуску SNORT у тестовому режимі:

*snort -A console -q -c /etc/snort/snort.conf -i eth0*

7. Рекомендації щодо налаштування

- Використовуйте попередньо налаштовані правила з офіційного джерела (Snort.org) або Emerging Threats.
- Регулярно оновлюйте правила для забезпечення актуальності.
- Оптимізуйте правила для уникнення помилкових спрацювань (false positives).
- Використовуйте пріоритезацію для критичних правил із високим рівнем загрози.

Налаштування базових правил SNORT дозволяє адаптувати систему під конкретні вимоги мережі, забезпечуючи ефективний захист та реагування на кіберзагрози.

**Інтеграція з іншими системами безпеки**

Для досягнення максимальної ефективності SNORT IDPS необхідно інтегрувати з іншими інструментами захисту, такими як SIEM (системи управління подіями безпеки) та платформи автоматизації (SOAR). Завдяки такій інтеграції можна забезпечити централізоване управління інцидентами та прискорити реагування на загрози. Наприклад, SIEM дозволяє об’єднати логи з різних систем і на основі аналітики виділяти найбільш критичні загрози.

1. Інтеграція з SIEM-системами

Системи управління інформацією та подіями безпеки (SIEM) збирають і корелюють дані з різних джерел, зокрема SNORT:

- Мета: Централізація даних про загрози та автоматизація аналітики.
- Процес: Логи SNORT передаються в SIEM через syslog, де обробляються для створення інцидентів безпеки.
- Переваги:
  - Краща видимість загроз у масштабах всієї мережі.
  - Побудова кореляційних правил для виявлення складних атак.

Приклади SIEM-систем: Splunk, IBM QRadar, ArcSight.

2. Інтеграція з фаєрволами та NGFW

SNORT може взаємодіяти з фаєрволами для автоматичного блокування виявлених загроз:

- NGFW (Next-Generation Firewall): Забезпечують додатковий аналіз трафіку, що доповнює SNORT.
- Інтеграція: Через API або механізми автоматичного оновлення списків блокувань (наприклад, IP-адрес).
- Результат: Миттєве блокування підозрілих IP-адрес і трафіку.

3. Взаємодія зі системами запобігання витокам даних (DLP)

DLP-системи контролюють передачу конфіденційної інформації в мережі:

- SNORT допомагає виявляти аномалії або підозрілий трафік.
- DLP аналізує його зміст для запобігання витокам.
- Приклад: Поєднання правил SNORT із політиками DLP для блокування файлів із чутливими даними.

4. Інтеграція з платформами SOAR

Платформи оркестрації та автоматизації безпеки (SOAR) дозволяють автоматизувати дії після виявлення загрози:

- Процес: Дані з SNORT передаються в SOAR для автоматичного створення відповідних сценаріїв реагування (наприклад, ізоляції пристрою).
- Переваги:
  - Автоматизація рутинних задач.
  - Зниження часу реакції на інциденти.

5. Інтеграція з антивірусними системами та EDR

Endpoint Detection and Response (EDR) розширює можливості SNORT до рівня кінцевих пристроїв:

- SNORT фіксує мережеві аномалії, а EDR перевіряє файли або процеси на кінцевих точках.
- Виявлені загрози можуть бути автоматично ліквідовані на пристроях.

6. Використання спільно з WAF

Веб-аплікаційні фаєрволи (WAF) та SNORT утворюють потужний захист від атак на веб-додатки:

- WAF аналізує HTTP/HTTPS трафік, а SNORT додає можливості для виявлення аномалій та вторгнень у більш широкому спектрі протоколів.

- Результат: Покращена безпека веб-ресурсів.

7. Інтеграція через SnortSam

SnortSam — це інструмент, який дозволяє SNORT блокувати підозрілий трафік у реальному часі:

- Принцип: Передача інформації від SNORT до різних фаєрволів для внесення змін до правил фільтрації трафіку.
- Сумісність: SnortSam працює з багатьма популярними мережевими пристроями.

8. Рекомендації для інтеграції

- Використовуйте центральні системи логування, щоб забезпечити простоту передачі даних.
- Проводьте регулярні тести інтеграцій для перевірки їх коректності.
- Забезпечте відповідність стандартам і політикам інформаційної безпеки, інтегруючи SNORT із іншими системами.

Інтеграція SNORT IDPS із суміжними системами робить корпоративну мережу більш захищеною та стійкою до сучасних кіберзагроз, забезпечуючи всебічний і багаторівневий підхід до безпеки.

**Моніторинг та тестування**

Одним із важливих етапів є організація постійного моніторингу роботи системи. SNORT IDPS генерує великий обсяг журналів подій, які потрібно регулярно аналізувати. Проведення періодичних тестів, таких як пентестинг, допоможе виявити слабкі місця в налаштуваннях системи або нові вектори атак. Окрім цього, важливою є перевірка швидкості реакції системи на потенційні загрози в умовах високого навантаження.

1. Моніторинг системи SNORT IDPS

Моніторинг — це безперервний процес спостереження за станом мережі та роботою системи. Його основна мета — забезпечити стабільну роботу системи та вчасне виявлення аномалій.

Основні аспекти моніторингу:

Аналіз журналів (логів): SNORT генерує докладні журнали подій, які містять інформацію про виявлені загрози, зібраний трафік і реакцію системи.

- Необхідно перевіряти журнали на предмет помилкових спрацьовувань (FPR) або пропущених загроз (FNR).
- Логи інтегруються в SIEM для централізованого аналізу.

Використання інструментів візуалізації: Застосування інструментів, таких як Kibana, Splunk, або спеціалізованих рішень, дозволяє створювати дашборди для моніторингу активності в реальному часі.

Автоматичні сповіщення: Налаштування сповіщень (email, SMS) для реагування на критичні події, такі як виявлення спроб вторгнення.

Ресурсний моніторинг: Постійний контроль за навантаженням на сервер, де розгорнуто SNORT, щоб уникнути збоїв через перевантаження.

2. Тестування SNORT IDPS

Тестування забезпечує перевірку працездатності системи та її здатність виявляти потенційні загрози.

Етапи тестування:

Первинне тестування після розгортання: Перевірка правильності встановлення, конфігурації правил і сумісності з іншими компонентами мережі.

Тестування на виявлення загроз:

- Використання інструментів, таких як Metasploit, Kali Linux, або спеціалізованих тестових пакетів для симуляції атак.
- Перевірка, чи система коректно фіксує та реагує на інциденти.

Аналіз помилкових спрацьовувань:

- Виявлення і усунення проблем із надмірно чутливими або некоректними правилами.
- Оптимізація фільтрації трафіку для зниження кількості помилкових спрацьовувань (FPR).

Планові тести безпеки: Проведення регулярних тестів для перевірки відповідності системи новим загрозам і актуальності правил.

3. Інструменти для моніторингу та тестування

- Wireshark: Аналіз мережевого трафіку.
- Snort Report: Генерація звітів про виявлені події.
- Metasploit Framework: Симуляція реальних атак для перевірки надійності системи.
- Nmap: Перевірка доступності вузлів мережі та пошук уразливостей.

4. Рекомендації щодо організації моніторингу та тестування

- Налаштуйте розклад регулярних перевірок і аналізу системи.
- Забезпечте достатній рівень автоматизації для обробки журналів і тестування.
- Регулярно оновлюйте правила та сигнатури для актуалізації захисту.
- Інтегруйте SNORT з іншими інструментами, такими як SIEM і платформи SOAR, для комплексного аналізу.

Ефективний моніторинг та регулярне тестування є запорукою працездатності SNORT IDPS і забезпечують високий рівень захисту корпоративної мережі.

**Навчання персоналу**

Не менш важливим є навчання персоналу, який працюватиме з SNORT IDPS. Співробітники мають бути обізнані щодо принципів роботи системи, особливостей налаштування правил і способів реагування на сповіщення. Регулярні тренінги та семінари допоможуть підтримувати високий рівень кваліфікації команди, що дозволить зменшити ризики, пов’язані з людським фактором.

1. Цілі навчання

- Ознайомлення з основами кібербезпеки: Загальні поняття безпеки мережі, типи атак, принципи роботи мережевих систем захисту.
- Робота зі SNORT: Вивчення архітектури, налаштування та оптимізації системи.
- Інцидент-менеджмент: Реакція на виявлені загрози та аналіз журналів.

2. Основні компоненти навчання

Теоретичний блок:

- Основи роботи SNORT IDPS.
- Принципи фільтрації трафіку та створення правил.

- Методи інтеграції SNORT з іншими системами (SIEM, SOAR).

Практичний блок:

- Розгортання системи на реальному або тестовому середовищі.
- Симуляція атак (наприклад, за допомогою Metasploit) для виявлення помилок у налаштуваннях.
- Аналіз логів і створення власних правил для SNORT.

Безперервне навчання:

- Ознайомлення з оновленнями та новими сигнатурами загроз.
- Курси підвищення кваліфікації з використанням практичних кейсів.

3. Методи навчання

- Тренінги: Проводяться індивідуально або для груп персоналу з використанням симуляцій і практичних завдань.
- Онлайн-курси та сертифікації: Відомі платформи, такі як Coursera, Cybrary, або сертифікати Cisco, надають курси з кібербезпеки, які охоплюють SNORT.
- Внутрішні воркшопи: Регулярні зустрічі для обговорення нових кіберзагроз та обміну досвідом.
- Навчання через інциденти: Аналіз реальних випадків атак на мережу та вивчення кроків їх усунення.

4. Рекомендації для ефективного навчання

- Різнорівнева підготовка: Забезпечити базові знання для всіх працівників та поглиблене навчання для IT-фахівців.
- Складання сценаріїв: Використовувати реальні або змодельовані сценарії атак для практичних занять.
- Моніторинг ефективності: Оцінювати знання персоналу через тести, сертифікацію або проведення "червоних командних" навчань.
- Мотивація: Надавати працівникам сертифікати або інші винагороди для стимулювання участі у програмах навчання.

5. Результати навчання

- Забезпечення розуміння принципів роботи SNORT IDPS та можливостей його налаштування.

- Зниження часу реагування на загрози.
- Збільшення ефективності захисту корпоративної мережі завдяки кваліфікованому персоналу.

Постійне навчання співробітників не лише підвищує ефективність роботи SNORT IDPS, але й дозволяє адаптувати систему до змінних умов кіберзагроз.

**Забезпечення гнучкості та масштабованості**

SNORT IDPS є системою, що легко адаптується до змін у мережевій інфраструктурі. У великих корпоративних мережах варто впроваджувати декілька сенсорів із використанням балансувальників навантаження, що дозволить забезпечити безперебійну роботу навіть при значному збільшенні обсягу трафіку. У випадку розширення мережі додавання нових сенсорів не потребує суттєвих змін у вже існуючій конфігурації.

1. Архітектура та масштабованість

SNORT IDPS базується на модульній архітектурі, яка дозволяє:

- Легко додавати нові компоненти, такі як додаткові сенсори чи системи аналізу логів.
- Використовувати балансування навантаження за допомогою кластеризації або інтеграції з проксі-серверами.
- Здійснювати розгортання в різних середовищах: від невеликих офісних мереж до великих корпоративних інфраструктур із кількома підмережами.

2. Підтримка гнучких правил

SNORT дозволяє використовувати:

- Параметризовані правила: Їх можна адаптувати до специфічних умов мережі.
- Автоматичне оновлення: Підтримка актуальних сигнатур атак через регулярні оновлення баз правил.
- Індивідуальні налаштування: Створення правил відповідно до унікальних потреб підприємства.

3. Інтеграція з іншими рішеннями

Забезпечення масштабованості також включає інтеграцію SNORT з:

- SIEM-системами (наприклад, Splunk): Для централізованого моніторингу та аналізу подій.
- Технологіями автоматизації (SOAR): Для автоматичного реагування на інциденти.
- Хмарними сервісами: Використання SNORT у хмарних середовищах для захисту гібридної інфраструктури.

4. Підтримка багатоплатформного середовища

SNORT IDPS підтримує роботу на різних платформах, таких як Linux, Windows і Unix-системи, що робить його придатним для різноманітних мережевих інфраструктур.

5. Використання віртуалізації

Масштабованість забезпечується через:

- Розгортання SNORT у віртуальних середовищах (VMware, Hyper-V, Docker), що дозволяє гнучко адаптуватися до змінних ресурсів.
- Розподіл навантаження між декількома віртуальними інстанціями.

6. Прогнозоване розширення

Для забезпечення масштабованості слід:

- Враховувати прогнозований ріст трафіку та збільшення кількості користувачів.
- Проводити регулярний аудит ресурсів для оновлення обладнання або програмного забезпечення.

7. Автоматизація

Автоматизація налаштувань та інтеграція з іншими системами дозволяє мінімізувати час на розгортання та забезпечити динамічне оновлення правил без зупинки системи.

Забезпечення гнучкості та масштабованості SNORT IDPS є основою для її довгострокового використання в корпоративній мережі. Завдяки модульній архітектурі, автоматизації та інтеграції з іншими системами, SNORT здатна адаптуватися до змін і зберігати високу ефективність в умовах еволюції кіберзагроз.

**Постійне вдосконалення**

Останнім етапом є впровадження процесу постійного вдосконалення системи. SNORT IDPS, як і будь-яка технологія, вимагає адаптації до нових викликів. Регулярне оновлення бази правил, впровадження нових функцій та тестування забезпечують підтримку високого рівня безпеки.

**Висновки до розділу 3**

У розділі 3 були детально розглянуті основні етапи розгортання та налаштування технології захисту корпоративної мережі на основі SNORT IDPS. Кожен з цих етапів є важливим для створення стабільної та ефективної системи, здатної протистояти сучасним кіберзагрозам. Ретельний попередній аналіз інфраструктури, що включає оцінку топології мережі та конфігурації серверів, є першим кроком у впровадженні цієї технології. Цей етап дозволяє створити точну картину поточних умов і підготувати систему до адаптації під конкретні потреби підприємства.

Після завершення аналізу, важливим є налаштування апаратного та програмного забезпечення. Це забезпечує стабільну роботу SNORT IDPS, гарантує її високу продуктивність та здатність швидко реагувати на потенційно небезпечні загрози. Налаштування базових правил виявлення загроз дозволяє побудувати ефективний захист від атак, забезпечуючи швидку і точну фільтрацію шкідливого трафіку. Цей етап визначає основний рівень безпеки системи та дозволяє автоматизувати більшість процесів.

Важливою частиною побудови надійної системи захисту є інтеграція SNORT IDPS з іншими системами безпеки. Це включає використання таких рішень, як SIEM, DLP та інші. Взаємодія між цими компонентами дозволяє створити єдину мережу безпеки, що гарантує більш ефективний моніторинг та реагування на кіберінциденти. Завдяки такій інтеграції організація може швидко відреагувати на будь-які спроби вторгнення, забезпечуючи захист на всіх етапах взаємодії з мережею.

Моніторинг і тестування є необхідними складовими постійної перевірки ефективності системи. Це дозволяє не лише підтвердити її працездатність, а й виявити можливі слабкі місця, які потребують додаткової уваги та вдосконалення.

Регулярний аналіз результатів тестувань допомагає підтримувати систему в актуальному стані, відповідно до сучасних загроз.

Невід'ємною частиною впровадження є навчання персоналу, адже без належного розуміння системи з боку працівників неможливо досягти ефективного застосування. Персонал має бути підготовлений до роботи з SNORT IDPS, здатний оперативно реагувати на сигнали системи та здійснювати необхідне налаштування.

Важливою перевагою технології є її гнучкість і масштабованість. Це дозволяє організації адаптувати систему до зростаючих потреб та вимог. Наприклад, зі збільшенням трафіку або змінами в мережі можна коригувати налаштування SNORT IDPS, що гарантує ефективний захист незалежно від масштабів організації.

Не менш важливою є постійна робота над вдосконаленням системи. Системи безпеки повинні постійно оновлюватися, щоб не лише ефективно захищати від відомих загроз, а й протистояти новим, що постійно з'являються. Це дозволяє підтримувати високу ступінь безпеки в умовах швидко змінюваного кіберсередовища.

Загалом, запропонована технологія на основі SNORT IDPS є потужним інструментом для забезпечення надійного захисту корпоративної мережі. Завдяки інтеграції з іншими системами безпеки, гнучкості та постійному вдосконаленню, вона дозволяє успішно захищати дані і ресурси організації від будь-яких кіберзагроз, гарантуючи стабільну і ефективну роботу мережі навіть у найскладніших умовах.

# ВИСНОВКИ

Захист корпоративної мережі є надзвичайно важливою складовою для забезпечення безпеки інформаційних систем та даних підприємств. Актуальність цієї теми зростає в умовах постійного розвитку технологій і збільшення кількості кіберзагроз. Підприємства та організації повинні постійно адаптувати свої стратегії безпеки до нових викликів, щоб запобігти втратам важливої інформації та знизити ризик впливу зовнішніх і внутрішніх атак.

Протягом аналізу проблеми захисту корпоративних мереж було розглянуто різноманітні підходи та технології, серед яких важливе місце займають системи виявлення та запобігання вторгненням (IDPS). Зокрема, система SNORT є одним із найбільш поширених і ефективних рішень для забезпечення безпеки мережі завдяки її здатності детектувати різноманітні типи атак у реальному часі.

В результаті проведеного аналізу та розробки теми "Технологія захисту корпоративної мережі на основі SNORT IDPS", можна зробити кілька важливих висновків. По-перше, технологія SNORT IDPS є ефективним інструментом для захисту корпоративних мереж від кіберзагроз, забезпечуючи належний рівень безпеки завдяки виявленню та блокуванню атак на різних етапах їх здійснення. SNORT IDPS використовує потужні методи аналізу трафіку та виявлення аномалій, що дозволяє оперативно реагувати на потенційні загрози та знижувати ризик успішних кібератак.

Процес налаштування та інтеграції SNORT IDPS у корпоративну мережу потребує детального попереднього аналізу інфраструктури, що включає вивчення топології мережі та наявних систем безпеки. Це дозволяє визначити оптимальні параметри для налаштування SNORT та забезпечити ефективну взаємодію з іншими системами безпеки, такими як SIEM, DLP та антивірусні рішення. Крім того, важливим етапом є тестування та моніторинг роботи системи після впровадження, що допомагає виявляти потенційні проблеми та покращувати налаштування для більш ефективного захисту.

Ще одним важливим аспектом є навчання персоналу, який працює з SNORT IDPS. Адекватна підготовка працівників забезпечує правильне реагування на інциденти безпеки та ефективне використання можливостей системи. Підтримка високого рівня обізнаності співробітників щодо кіберзагроз є необхідною для забезпечення ефективного функціонування технології захисту.

Завдяки своїй гнучкості та масштабованості, SNORT IDPS може бути адаптований до потреб будь-якої організації, забезпечуючи захист як малих підприємств, так і великих корпорацій. Важливим є постійне вдосконалення системи, зокрема оновлення баз даних правил і підвищення рівня інтеграції з іншими інструментами безпеки. Впровадження таких технологій дозволяє підприємствам значно знизити ризик атак і забезпечити надійний захист своїх інформаційних систем.

Загалом, вивчення різноманітних методів і засобів захисту мереж підтверджує, що забезпечення надійного захисту корпоративних мереж потребує інтегрованого підходу, що включає використання різних технологій у поєднанні з постійним моніторингом і оновленням систем безпеки.

Отже, запровадження технології захисту на основі SNORT IDPS є важливим кроком до підвищення рівня безпеки корпоративних мереж. Це дозволяє значно зменшити вплив кіберзагроз і зберегти цінні дані та ресурси підприємства в безпеці.

## ПЕРЕЛІК ПОСИЛАНЬ


1. Fuchsberger, Andreas. "Intrusion Detection Systems and Intrusion Prevention Systems." Information Security Technical Report 10, no. 3 (January 2005): 134–39. http://dx.doi.org/10.1016/j.istr.2005.08.001. (дата звернення: 05.10.2024).

2. Kaur, Harpreet. "NETWORK INTRUSION DETECTION AND PREVENTION ATTACKS." INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY 2, no. 3 (June 30, 2012): 21–23. http://dx.doi.org/10.24297/ijct.v2i3a.2669. (дата звернення: 05.10.2024).

3. Wang, Lidong. "Big Data in Intrusion Detection Systems and Intrusion Prevention Systems." Journal of Computer Networks 4, no. 1 (August 26, 2017): 48–55. http://dx.doi.org/10.12691/jcn-4-1-5. (дата звернення: 09.10.2024).

4. Afzal, Shehroz, and Jamil Asim. "Systematic Literature Review over IDPS, Classification and Application in its Different Areas." STATISTICS, COMPUTING AND INTERDISCIPLINARY RESEARCH 3, no. 2 (December 31, 2021): 189–223. http://dx.doi.org/10.52700/scir.v3i2.58. (дата звернення: 15.10.2024).

5. Stefanova, Zheni Svetoslavova. "Machine Learning Methods for Network Intrusion Detection and Intrusion Prevention Systems." Scholar Commons, 2018. https://scholarcommons.usf.edu/etd/7367. (дата звернення: 14.10.2024).

6. Abdulazeez, M. B. "Intrusion detection and prevention systems in the cloud environment." Thesis, University of Liverpool, 2017. http://livrepository.liverpool.ac.uk/3009224/.(дата звернення: 15.10.2024).

7. Toxen, Bob. Real-world Linux security: Intrusion, prevention, detection, and recovery. Upper Saddle River, NJ: Prentice Hall, 2001. (дата звернення: 15.10.2024).

8. Planning for the future of cyber attack attribution: Hearing before the Subcommittee on Technology and Innovation, Committee on Science and Technology, House of Representatives, One Hundred Eleventh Congress, second session, July 15, 2010. Washington: U.S. G.P.O., 2010. (дата звернення: 15.10.2024).

9. Garbis, Jason, and Jerry W. Chapman. "Intrusion Detection and Prevention Systems." In Zero Trust Security, 117–26. Berkeley, CA: Apress, 2021. http://dx.doi.org/10.1007/978-1-4842-6702-8_8. (дата звернення: 23.10.2024).

10. Mukhopadhyay, Indraneel, Kirit Sankar Gupta, Diptarshi Sen, and Piyali Gupta. "Heuristic Intrusion Detection and Prevention System." In 2015 International Conference and Workshop on Computing and Communication (IEMCON). IEEE, 2015. http://dx.doi.org/10.1109/iemcon.2015.7344479. (дата звернення: 23.10.2024).

11. Hurd, Steven A., and Elliot P. Proebstel. Characterizing and Improving Distributed Intrusion Detection Systems. Office of Scientific and Technical Information (OSTI), November 2007. http://dx.doi.org/10.2172/1139982. (дата звернення: 03.11.2024).

12. Martins, Daniel MourÃo. "A Strategy for Detection Systems and Intrusion Prevention Based on Free Software." Universidade Federal do CearÃ, 2012. http://www.teses.ufc.br/tde_busca/arquivo.php?codArquivo=8923. (дата звернення: 03.11.2024).

13. Red Hat - We make open source technologies for the enterprise. URL: https://www.redhat.com/rhdc/managed-files/ma-security-automation-ebook-1349512OM-202408-en.pdf (дата звернення: 05.11.2024).

14. What is an intrusion detection and prevention system (IDPS)?. Red Hat - We make open source technologies for the enterprise. URL: https://www.redhat.com/en/topics/security/what-is-an-IDPS. (дата звернення: 05.11.2024).

15. Pharate, Abhishek, Harsha Bhat, Vaibhav Shilimkar, and Nalini Mhetre. "Classification of Intrusion Detection System." International Journal of Computer Applications 118, no. 7 (May 20, 2015): 23–26. http://dx.doi.org/10.5120/20758-3163. (дата звернення: 12.11.2024)

16. Deshpande, Apoorva. "A Review on Intrusion Detection System using Artificial Intelligence Approach." SMART MOVES JOURNAL IJOSCIENCE 4, no. 8 (August 5, 2018): 6. http://dx.doi.org/10.24113/ijoscience.v4i8.153. (дата звернення: 12.11.2024)

17. Al, Tobi Amjad Mohamed. "Anomaly-based network intrusion detection enhancement by prediction threshold adaptation of binary classification models." Thesis, University of St Andrews, 2018. http://hdl.handle.net/10023/17050. (дата звернення: 20.11.2024)

18. Zoghi, Zeinab. "Ensemble Classifier Design and Performance Evaluation for Intrusion Detection Using UNSW-NB15 Dataset." University of Toledo / OhioLINK, 2020. http://rave.ohiolink.edu/etdc/view?acc_num=toledo1596756673292254. (дата звернення: 20.11.2024)

19. Herrero, Alvaro. Mobile Hybrid Intrusion Detection: The MOVICAB-IDS System. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. (дата звернення: 01.12.2024)

20. Abraham, Ajith, and Ravi Jain. "Soft Computing Models for Network Intrusion Detection Systems." In Classification and Clustering for Knowledge Discovery, 191–207. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005. http://dx.doi.org/10.1007/11011620_13. (дата звернення: 01.12.2024)

21. Shang-fu, Gong, and Zhao Chun-lan. "Intrusion detection system based on classification." In 2012 IEEE International Conference on Intelligent Control, Automatic Detection and High-End Equipment (ICADE). IEEE, 2012. http://dx.doi.org/10.1109/icade.2012.6330103. (дата звернення: 09.12.2024)

**ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)**