ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 4 (2), 2024

https://doi.org/10.23939/ictee2024.02.060

РОЗРОБЛЕННЯ МОДЕЛІ СИСТЕМИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ КІБЕРЗАГРОЗАМ ІЗ ПІДТРИМКОЮ ТА ОНОВЛЕННЯМ ПРАВИЛ ВИЯВЛЕННЯ АТАК

А. Голдій [ORCID: 0009-0002-4177-7281], **О. Шпур** [ORCID: 0000-0001-8156-8017], **А. Масюк** [ORCID: 0000-0003-2020-138X]

Національний університет "Львівська політехніка", вул. С. Бандери, 12, Львів, 79013, Україна

Відповідальний за рукопис: А. Голдій (e-mail: andrii.y.holdii@lpnu.ua)

(Подано 15 червня 2024)

Стаття присвячена проблемі захисту даних в інформаційно-комунікаційних системах в умовах зростання обсягів трафіку та кількості кіберзагроз, що робить необхідним покращення ефективності систем протидії вторгненням. Розглянуто різновиди систем виявлення вторгнень (IDS) та систем запобігання вторгнень (IPS), їхні переваги та недоліки. Проаналізовано методи виявлення загроз, серед яких сигнатурні методи, методи виявлення аномалій та методи на основі машинного навчання. Особлива увага приділяється методам виявлення атак на основі вмісту трафіку. Проведено порівняння ефективності різноманітних комерційних та відкритих рішень, таких як Snort і Suricata, з точки зору їхньої архітектури, продуктивності та точності. Основною пропозицією є доповнення системи Suricata додатковим модулем Intelligent Threat Detector (ITD), що базується на методах машинного навчання. Модуль ITD інтегрований у основний модуль Suricata і виконує глибокий аналіз трафіку та виявлення аномалій. Такий підхід дозволяє знизити навантаження на систему виявлення, підвищуючи продуктивність обробки вхідного трафіку і забезпечуючи високий рівень безпеки. Запропоноване рішення забезпечує багаторівневий підхід до захисту мережі, де первинна фільтрація здійснюється Suricata, а глибокий аналіз — ITD. Система може перехоплювати мережеві пакети для аналізу інформації, будуючи функції обробки на основі обраних даних для визначення можливості вторгнення. Додатково, інтеграція модуля ITD дозволяє адаптувати систему до нових та невідомих загроз у реальному часі, модуль постійно навчається на основі нових даних, що забезпечує безперервне покращення точності виявлення та реагування на загрози. Розміщення системи після фаєрволу допомагає знизити навантаження на систему виявлення, забезпечуючи ефективне використання ресурсів багатопроцесорних систем та зменшення помилкових спрацьовувань.

Ключові слова: *IPS, IDS, виявлення атак, розподілені системи, балансування навантаження, автоматичне масштабування.*
УДК: 621.391

1. Вступ та постановка проблеми

У сучасному цифровому світі щоденно генерується величезний обсяг даних, тому захист конфіденційності та цілісності інформації стає завданням критичної важливості. Особливої актуальності захист даних набуває у комерційних сферах, де втрата чи компрометація «чуттєвої» чи особистої інформації може нести великі економічні втрати. Проблема може стосуватися як

зберігання так і передавання даних по інформаційних мережах, коли існує ризик перехоплення та перегляду інформації третіми сторонами. Іншою проблемою можна назвати використання соціально-інженерних методів, коли зловмисники намагаються отримати доступ до даних, обманюючи користувачів, персонал або використовуючи слабкі місця в системах безпеки.

Сучасними популярними системами, які постійно вдосконалюються для боротьби з кіберзагрозами можна назвати системи вивлення вторгнень (Intrusion Detection System – IDS) та системи запобігання вторгення (Intrusion detection system – IPS). Головною відмінністю між цими системами є те, що IDS використовують для моніторингу трафіку мережі, формування звітів та надсилання сповіщень про підозрілі події в інформаційно-комунікаційній системі, а IPS дозволяє в режимі реального часу автоматично реагувати на зловмисні дії залежно від налаштувань. Водночас, обидві системи можуть використовувати однакові методи моніторингу та виявлення.

Комплексним рішенням у питанні виявлення та запобігання вторгнень є комбінація обох принципів в одну систему IDPS, яка відстежує мережевий трафік та шукає ознаки атак, таких як аномальні пакети, сканування портів та спроби проникнення, а також може автоматично блокувати підозрілий трафік, запобігаючи вторгненням в мережу (рис 1).

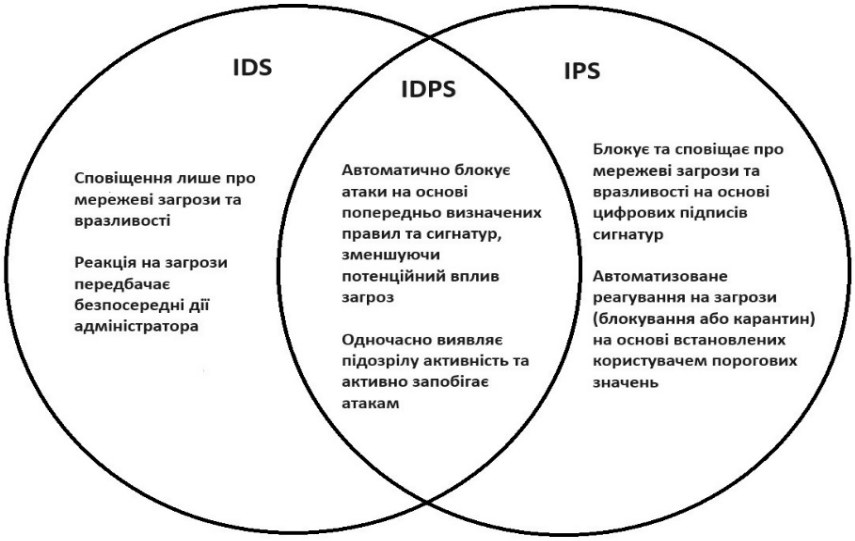

Рис 1. Функції систем виявлення та запобігання вторгень

Однак, традиційні методи IDPS можуть бути недостатньо ефективними у виявленні вторгнень, оскільки вони схильні до хибно позитивних і хибно негативних результатів. Хибно позитивні результати можуть призвести до того, що адміністратори мережі витрачатимуть час і ресурси на розгляд помилкових тривог, а хибно негативні результати можуть дозволити зловмисникам проникнути в систему непоміченими [1].

2. Аналіз особливостей реалізації систем IDPS та способи їх удосконалення

Системи виявлення та запобігання вторгнень активно збирають та зберігають велику кількість даних, що стосуються виявлених подій у мережі. Отримані дані можна використовувати для підтвердження правомірності сповіщень, розслідування інцидентів та встановлення зв'язків між подіями, виявленими IDPS, та іншими джерелами реєстрації подій [4].

В залежності від методів збору та обробки даних, а також від стратегій реакції на виявлені події, можлива різноманітність класифікації систем. Наприклад, деякі системи можуть базуватися на мережевому моніторингу та реагувати на аномалії в трафіку, в той час як інші можуть аналізувати локальні дані хостів та виявляти підозрілі активності на рівні окремих пристроїв. Крім того, існують системи, які поєднують обидва підходи та кореляцію даних з різних джерел для покращення точності

виявлення та зменшення помилкових тривог. Такий різноманітний підхід до класифікації систем допомагає забезпечити більш ефективний захист мережі від потенційних загроз [3-4].

Хост-орієнтовані системи моніторингу. Системи, які вивчають характеристики окремого хосту та події, що відбуваються в ньому, на предмет виявлення підозрілої активності. Наприклад, хост-орієнтована система може відслідковувати мережевий трафік, системні журнали, запущені процеси, активність програм, доступ та зміни в файлах, а також зміни в конфігурації системи. Такі системи встановлюються на критичних вузлах, таких як сервери, що доступні публічно, а також сервери, що містять конфіденційну інформацію, для забезпечення їхньої безпеки та захисту від потенційних загроз.

Мережево-орієнтовані системи моніторингу. Такі системи використовують для аналізу мережевого трафіку для конкретних сегментів мережі або окремих пристроїв з метою виявлення будь-яких підозрілих активностей. Для цього вони виконують глибоку перевірку мережевих та прикладних протоколів, щоб виявити відхилення від звичайної активності та потенційні загрози безпеці. Розгортають мережево-орієнтовані системи на кордонах мережі, серверах приватних мереж, серверах віддаленого доступу.

Гібридні системи. Інструменти, які можуть одночасно використовувати як хост-орієнтовані, так і мережево-орієнтовані системи. Це дозволяє поєднувати переваги обох підходів та забезпечувати більш повне охоплення мережевих загроз інформаційній системі.

Аналізатори поведінки мережі (Network Behavior Analysis – NBA). Досліджує мережевий трафік для виявлення загроз, які породжують незвичайні потоки трафіку, такі як розподілені атаки відмови обслуговування (DDoS), певні форми шкідливих програм та порушення політики безпеки. Системи NBA найчастіше використовують для моніторингу потоків внутрішніх мереж, а іноді розгортають і там, де вони можуть відслідковувати потоки між внутрішніми мережами організації та зовнішнім середовищем [4].

Вагомим фактором для вдосконалення систем виявлення та запобігання вторгненням є аналіз методів та моделей захисту, які охоплюють широкий спектр підходів, включаючи як традиційні, так і інноваційні рішення.

Сигнатурні методи (Signature-Based Methods), представляють собою традиційний підхід, який базується на веденні баз даних з сигнатурами, які містять зразки шкідливих поведінок, наприклад, відомі вразливості, шкідливі скрипти чи специфічні кодові послідовності. При виявленні системою моніторингу трафіку, який відповідає одному з цих підписів, вона ідентифікує його як потенційну загрозу і вживає заходів, таких як повідомлення адміністратора або блокування трафіку [1-4].

Одне із останніх досліджень [2] пропонує кілька вдосконалень для системи виявлення вторгнень на основі сигнатур та аномалій. Система використовує дерево рішень для виявлення відомих атак і нейронну мережу ResNet50 для виявлення аномалій. Отримані результати показали, що запропонована система досягає точності 98,98% для виявлення вторгнень. Поєднання методів виявлення сигнатур та аномалій – це перспективний підхід, який має потенціал для підвищення ефективності виявлення вторгнень. Однак заявлена точність була отримана на основі двох наборів даних, які не обов'язково є репрезентативними для реального світу. Крім того, відсутність порівняльних оцінок з іншими системами виявлення вторгнень ускладнює оцінку фактичної ефективності системи. Для того, щоб оцінити фактичну ефективність системи, її необхідно порівняти з іншими системами виявлення вторгнень, які використовують різні методи, а також в реальному середовищі, щоб оцінити її вплив на продуктивність мережі.

Методи виявлення аномалій (Anomaly-Based Methods). Такі методи аналізують поведінку мережі, формуючи базу того, що вважається нормальною мережевою активністю, враховуючи різноманітні метрики, включаючи пропускну здатність, протоколи, порти та інше. Після виявлення підозрілої активності, яка відхиляється від базового профілю, система позначає її як аномальну що може вказувати на кібератаку.

Ефективним способом покращення роботи сучасних систем виявлення вторгнень є використання машинного навчання [3] з класифікацією вхідних даних у певні класи, такі як

«доброякісні» або «атака». Для класифікації використовують різні алгоритми машинного навчання, такі як дерева ухвалення рішень (Decision tree), Extra-Trees, SVM тощо.

Методи виявлення атак на основі вмісту (Content-Based Attack Detection Methods). Ці методи можуть використовувати різні техніки для аналізу вмісту, включаючи сигнатури, ключові слова, відхилення від типового шаблону та інші евристичні методи. Вони можуть також використовувати алгоритми машинного навчання для виявлення складних атак, які можуть бути важко визначити за допомогою традиційних методів. Таким чином, вони аналізують конкретний вміст мережевих пакетів або даних для виявлення характеристик атак, таких як SQL-ін'єкції, крос-сайт скриптінг тощо та можуть бути корисними для виявлення нових та невідомих атак, а також атак, які не мають сигнатур. Методи виявлення на основі вмісту з технологіями машинного навчання дозволяють виявляти фальшиві акаунти у соціальних мережах [5]. Використання ієрархічної структури мережі глибокого машинного навчання для кращого аналізу багатовимірної інформації про особливості користувачів дозволяє підвищити точність виявлення таких акаунтів [6].

3. Системи виявлення та протидії вторгненням

На ринку кібербезпекових рішень існує широкий спектр комерційного програмного забезпечення для виявлення та запобігання вторгненням, які можуть бути інтегровані в системи безпеки організацій. Важливо враховувати не лише функціональні можливості цих систем, а й їхню сумісність з існуючим інфраструктурним середовищем підприємства. Для невеликих компаній Unified Threat Management (UTM) може бути оптимальним рішенням через його зручність та доступність за ціною. Однак, великі компанії, які мають потужну мережу, можуть вибрати мережеві брандмауери нового покоління (NGFW) для більшого контролю та розширених можливостей управління.

Окрім комерційних рішень, системи IDPS з відкритим вихідним кодом, відкривають широкі можливості для співпраці у розвитку і адаптації до унікальних потреб компаній. Їхня гнучкість та спроможність виявляти навіть найскладніші загрози робить їх популярними серед тих, хто цінує якість та ефективність за доступну ціну. Загалом, вибір безпекових рішень повинен базуватися на унікальних потребах та можливостях кожної конкретної компанії, а також враховувати її масштаби та бюджетні обмеження. Прикладом систем з відкритим вихідним кодом є Snort і Suricata.

Snort – це одна з найпопулярніших систем виявлення вторгнень, яка активно використовується для моніторингу мереж і виявлення аномальних дій та загроз на основі аналізу мережевого трафіку і відповідності його зразків патернам атак. Система використовує набір правил, які визначають характеристики потенційних загроз і діють у випадку їх виявлення. Snort може працювати в режимі реального часу, що дозволяє оперативно реагувати на потенційні загрози. Крім того, Snort підтримує різні режими роботи, включаючи режими мережевого моніторингу, пакетний режим та режим з виведенням повідомлень. Це дає можливість використовувати Snort не лише для виявлення загроз, а й для аналізу мережевого трафіку та подальших дій. Проте важливо зазначити, що система може бути обмеженою у виявленні раніше не відомих атак або тих, що не відповідають визначеним правилам [7].

Вхідні пакети системи Snort спочатку проходять через декодери і препроцесори, а потім потрапляють в детектор для застосування правил. Декодери отримують дані мережевого та транспортного рівнів (IP, TCP, UDP) з протоколів канального рівня, наприклад, Ethernet. Препроцесори готують ці дані для застосування правил, контролюють стан, відновлюють сесії та нормалізують протоколи. Правильно налаштовані препроцесори можуть значно покращити продуктивність системи та зменшити кількість надлишкових даних, які потрапляють до детектора. Крім того, завдяки архітектурним особливостям, до Snort можна додати власний препроцесор.

Перед відправкою в детектор формуються пакети, до яких потім застосовуються правила. Самі правила містять опис трафіку, сигнатури атак, опис загрози та реакцію на виявлення загрози [8,10].

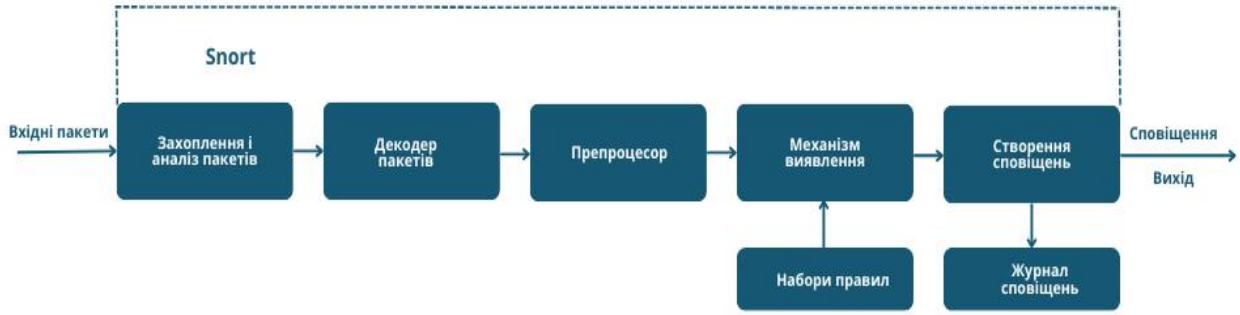

Рис. 2 Архітектура системи Snort

Snort довгий час був провідною системою виявлення та попередження вторгнень. Але зі зростанням багатоядерних процесорів, складності мережевих середовищ та збільшенням трафіку, система стикнулася з труднощами в адаптації до нових умов. Хоча Snort додав підтримку IPv6, інспектування рівня додатків та інші функції, він залишався однопотоковою системою, що обмежувало його швидкість і ефективність у високонавантажених середовищах. Це призвело до пошуку альтернативних рішень, здатних більш ефективно відповідати на нові виклики сучасних мереж.

Suricata – це ще одна потужна система виявлення та запобігання вторгненням з відкритим вихідним кодом, яка набула широкої популярності в сфері кібербезпеки. Її можливість використання багатопотоковості дозволяє ефективно обробляти пакети мережного трафіку в реальному часі, що пришвидшує процес роботи.

Рис.3 Архітектура системи Suricata

Однією з головних переваг Suricata є підтримка багатьох різних протоколів, включаючи TCP, UDP, ICMP, HTTP, SSL і багато інших. Система може виявляти і аналізувати широкий спектр мережевого трафіку, включаючи захищені SSL з'єднання. Suricata також відома своїм механізмом розпізнавання зразків, який використовує різноманітні правила і сигнатури для виявлення відомих атак та аномалій в мережевому трафіку. Вона також підтримує різні режими роботи, включаючи режим мережевого моніторингу і режим виявлення вторгнень, що дозволяє налаштовувати систему під конкретні потреби мережі [9,10].

У Suricata існують два режими IPS: NFQ і AF_PACKET. В NFQ IPS режимі процес відбувається наступним чином: пакет потрапляє до iptables, де правила направляють його до черги NFQUEUE. Після цього пакети можуть бути оброблені на рівні користувача, на якому працює Suricata. Потім Suricata застосовує правила, визначені користувачем, і приймає один із трьох вердиктів: NF_ACCEPT, NF_DROP або NF_REPEAT. Пакети, що отримали вердикт NF_REPEAT, можуть бути помічені і повернуті на початок поточної таблиці iptables, що дозволяє значно впливати на їх подальшу обробку.

Основна різниця між Snort і Suricata полягає в багатопотоковості Suricata, яка дозволяє їй ефективно використовувати кілька ядер процесора одночасно. Це призводить до ефективного балансування навантаження та можливість обробляти більші обсяги даних, що робить Suricata більш продуктивною. Suricata є сумісною з більшістю розробок Snort. Формат виведення подій у JSON спрощує інтеграцію з різними сторонніми інструментами, включаючи системи моніторингу та візуалізації логів, наприклад таких як Kibana [9,10].

Однією з ключових особливостей Suricata є можливість роботи з рівнем дадатків моделі OSI, що дозволяє їй виявляти шкідливі програми. На відміну від Snort, правила в Suricata не вимагають суворої прив'язки до номерів портів, достатньо вказати протокол та дію, і модулі Suricata самі розберуться з трафіком, навіть якщо використовується нестандартний порт.

У порівнянні з Snort, Suricata пропонує більше можливостей для розширення та конфігурації завдяки своїй архітектурі. Однак це може стати недоліком для початківців через велику кількість налаштувань та іноді не найвичерпнішу документацію. Таким чином, вибір між Snort і Suricata залежить від вимог конкретного середовища та рівня досвіду користувача [9,10].

У роботі [11] було запропоновано побудувати IDPS-систему, яка поєднує багато методів виявлення вторгнень, зокрема виявлення аномалій, засноване на сигнатурах, та перевірку за правилами. Ця IDPS-система була розроблена на основі Snort і поєднувала до трьох методів для досягнення максимальної ефективності. Крім того, було використано ряд алгоритмів для генерації вибірки сигналів на основі атак, виявлених системою виявлення аномалій, яка, в свою чергу, відповідала правилам Snort.

Інше дослідження [12] вивчало прискорення обробки в IDPS-системі Snort шляхом створення апаратного модуля для перетворення PCRE на FPGA. Кожне правило Snort перетворювалось на регулярний вираз, специфічний для PCRE. Оскільки система обробляє велику кількість правил, швидкість роботи безпосередньо впливає на ефективність обробки трафіку. Дослідники розробили модель, яка використовує апаратні можливості Virtex-4 LX200 FPGA для перетворення регулярних виразів.

Враховуючи особливості реалізації систем виявлення вторгнень та аналіз існуючих механізмів збору та обробки даних необхідна реалізації IPS, яка б мала можливість виявляти вторгнення незалежно від способу аналізу мережевого трафіку та дозволяла автоматично блокувати підозрілий трафік, що дозволить мінімізувати шкідливий вплив атак у мережі.

4. Розроблення моделі IDPS із підтримкою та оновленням правил виявлення атак

Перевагою систем виявлення вторгнень з відкритим вихідним кодом є їх здатність скоротити витрати на ліцензійне програмне забезпечення. Також система повинна підтримувати єдину базу даних, де регулярно оновлюються шаблони та правила для виявлення нових методів вторгнення. Система має досліджувати та спостерігати за роботою в нормальних умовах, щоб фіксувати параметри для подальшого виявлення відхилень. При цьому необхідно врахувати місце розташування системи виявлення і запобігання вторгнень для забезпечення ефективного захисту інформаційних ресурсів, що дозволить не лише вчасно виявляти і блокувати потенційні загрози, але й впливатиме на продуктивність мережі, знижуючи навантаження на інші елементи інфраструктури і сприятиме точнішій обробці трафіку.

Місце розташування системи IDPS значною мірою залежить від специфічних потреб типу мережі, зважаючи на на унікальні вимоги до безпеки, типу трафіку та навантаження. Для мереж, що мають високий рівень взаємодії з Інтернетом, важливо забезпечити максимальний захист від зовнішніх загроз. В такому випадку розміщення IDPS необхідно робити на вхідному шлюзі, що дозволить виявляти та блокувати загрози ще на етапі входу трафіку в мережу. Для великих організацій або мереж з високим рівнем сегментації, розміщення систем IDPS у внутрішній частині мережі дозволить аналізувати трафік між сегментами, що забезпечить виявлення та запобігання внутрішніх загроз, таких як скомпрометовані пристрої або користувачі. У випадку захисту мереж, що містять критичні системи або сервери, необхідно забезпечити захист саме цих елементів. При

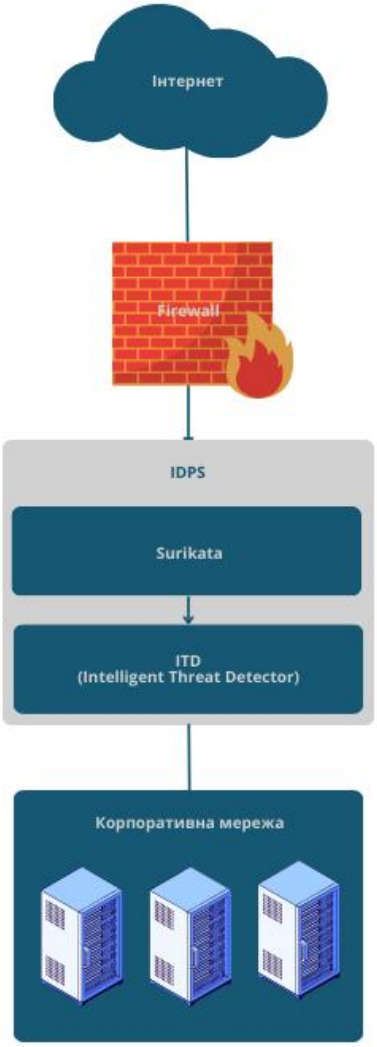

Рис. 4. Узагальнена схема мережі з системою IDPS

цьому застосовують хостові IDPS, які встановлюються безпосередньо на серверах або критичних системах, що дозволить захистити найважливіші елементи мережі.

Для мереж, де важливо забезпечити баланс між продуктивністю і безпекою, системи IDPS розташовують після брандмауера, який виконує первинну фільтрацію трафіку, а IDPS – поглиблений аналіз відфільтрованого трафіку. При такому підході знижується навантаження на систему виявлення та запобігання вторгненням, підвищуючи загальну продуктивність опрацювання вхідного трафіку і забезпечуючи при цьому високий рівень безпеки.

Пропонована інтелектуальна система IDPS складається з двох частин: основа системи заснована на IDS з відкритим вихідним кодом і блок машинного навчання для автоматичної підтримки та оновлення правил виявлення атак. Система може перехоплювати мережеві пакети для аналізу інформації, будуючи функції обробки на основі обраних даних для визначення можливості вторгнення.

Перший модуль використовує Suricata для виконання початкової функції фільтрації пакетів, діючи як самодостатня система IDS.

Модуль машинного навчання інтегрований в основний модуль, що використовує рішення під назвою IDT (Intelligent Threat Detector) на основі методів машинного навчання. Основний модуль здійснюватиме фільтрацію верхнього рівня, видаляючи пакети, які вважаються небезпечними згідно з наборами правил, наданими IDS-пристроєм.

Система повинна обробляти кожен вхідний пакет, тому необхідно визначити властивості, які потрібно передати в блок машинного навчання для подальшої обробки. Великий обсяг вхідного мережевого трафіку може призвести до різкого зростання навантаження на систему виявлення та протидії вторгненням, що підвищує вимоги до її продуктивності та оптимізації роботи для забезпечення безперебійної обробки трафіку в реальному часі.

Для підвищення швидкості обробки пакетів пропонується використовувати багатопроцесорну систему з інтеграцією машинного навчання та паралельним аналізом пакетів. Її основою буде використання модуля Intelligent Threat Detector (ITD), що дозволить підвищити ефективність і точність виявлення загроз. ITD, заснований на методах машинного навчання для аналізу мережевого трафіку, дозволить виявляти більш складні та нові загрози, які можуть залишатися непоміченими при використанні традиційних правил IDS, адаптуючись до нових загроз на основі постійно оновлюваних даних, підвищуючи точність виявлення. Вхідними даними для модуля ITD будуть пакети мережевого трафіку, що пройшли первинну фільтрацію через Suricata, але потребують глибшого аналізу. Suricata виконує базову фільтрацію трафіку, використовуючи правила і сигнатури, та відбирає підозрілі пакети для подальшого аналізу.

Перевагою є те, що багатопроцесорна архітектура дозволяє розподілити обробку трафіку між кількома процесорами. Це дає можливість паралельно виконувати фільтрацію трафіку за допомогою Suricata та аналіз загроз за допомогою ITD, що має підвищити загальну пропускну здатність системи. Кожен процесор зможе одночасно обробляти окремий потік даних, що зменшує час реакції на загрози.

Крім того, багатопроцесорна система з ITD забезпечить масштабованість і гнучкість, що дозволить додавати нові процесори для обробки зростаючого обсягу трафіку, що дозволяє системі

швидко адаптуватися до змін в обсязі трафіку та складності загроз. Ця архітектура також підтримує рівномірний розподіл навантаження між процесорами, що запобігає виникненню вузьких місць в обробці даних і знижує затримки.

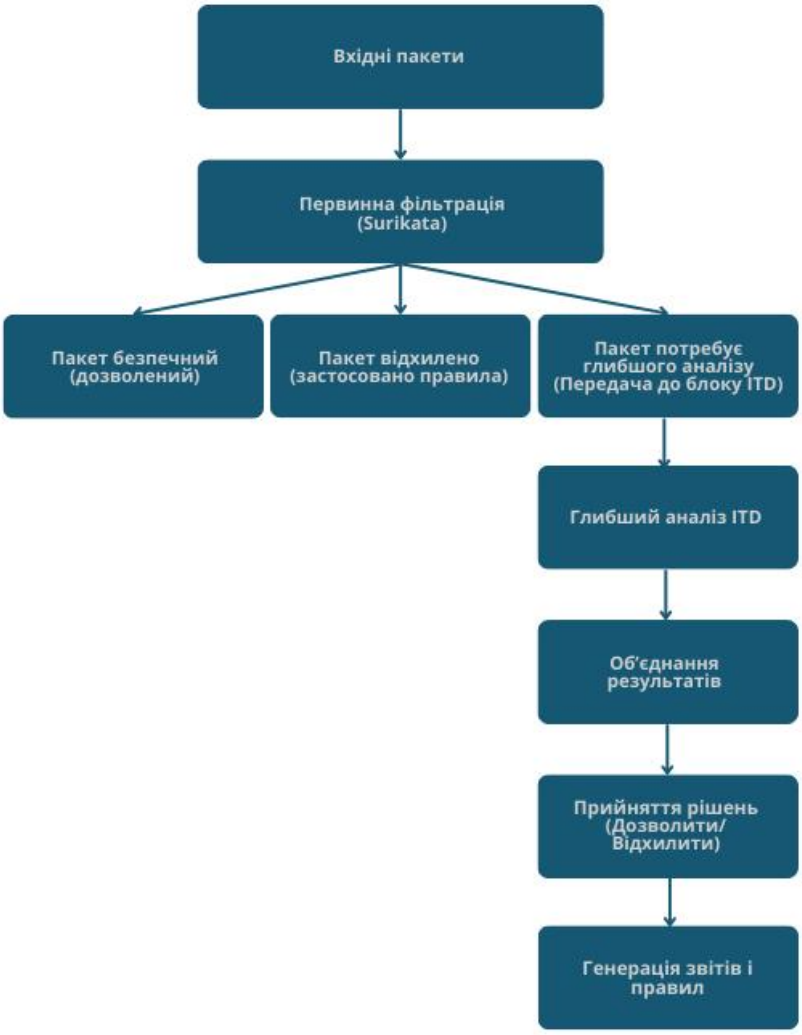

Рис.5 Пропонована модель системи IDPS

Модуль ITD також сприятиме підвищенню надійності системи. У випадку відмови одного з процесорів, інші зможуть продовжувати роботу, забезпечуючи безперервну обробку трафіку. При цьому варто забезпечити резервування та балансування навантаження для додаткової стабільність і надійності системи.

Робота такої системи матиме наступну послідовність: мережеві пакети, які надходитимуть до системи спрямовуються до компонента, який здійснюватиме розподіл між процесорами для паралельної обробки. При цьому варто використовувати балансування потоків для рівномірного навантаження на процесори з використанням можливих методів і технологій, наприклад, розподілу трафіку на основі хешування, що дозволить розподіляти пакети на основі певних характеристик, таких як IP-адреса,порт або протокол. Інший спосіб можна застосувати балансування на основі черг, які формуються в порядку надходження пакетів і реалізузується за допоогою програмного або апаратного балансувальника, який керує чергами пакетів і спрямовує їх до відповідних процесорів.

Крім того, можна застосувати способи динамічного балансування або балансування на рівні ядра операційної системи. У першому випадку, динамічні алгоритми балансування можуть враховувати поточне завантаження процесорів і перенаправляти трафік до менш завантажених

процесорів, що дозволять системі адаптуватися до змін у трафіку в режимі реального часу. У випадку балансування на рівні ядра розподіл обчислювальних ресурсів буде здійснюватися вбудованими механізмами операційної системи між доступними ядрами, однак такий підхід зазвичай базується на зальних алгоритмах, що може мати обмежену гнучкість для використання в системах виявлення та протидії вторгенням.

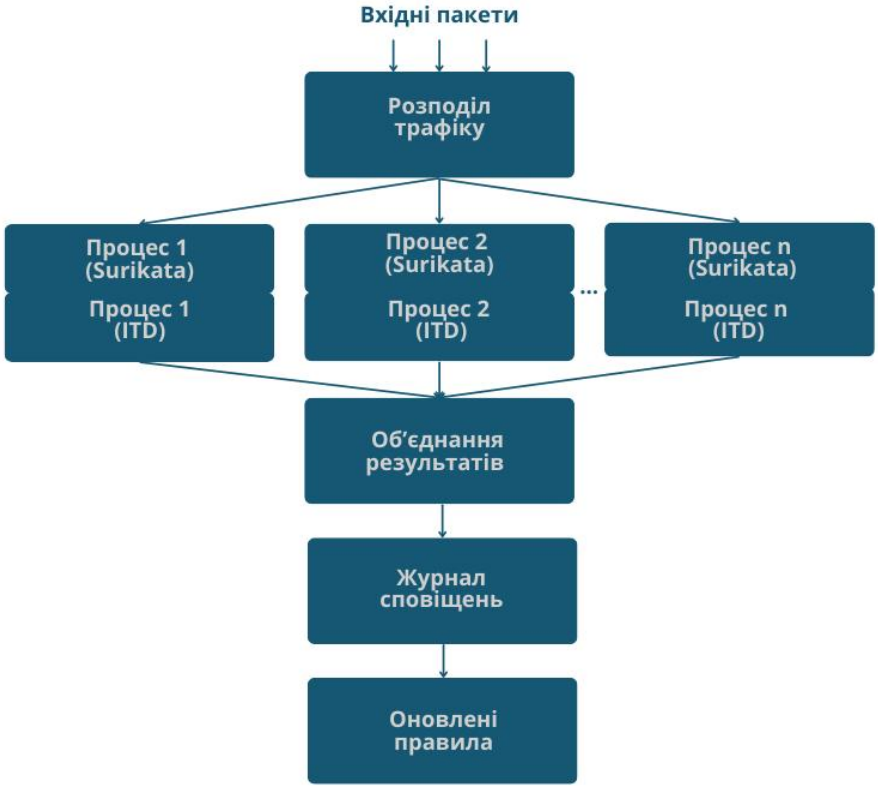

Рис.6 Блок-схема багатопроцесорної обробки пакетів

Після розподілу навантаження кожен процесор виконуватиме первинну фільтрацію пакетів за допомогою Suricata паралельно з іншими процесорами відповідно до схеми: Процес_1(Suricata), Процес_2(Suricata)… Процес_n(Suricata). Результати обробки кожного процесу Syricata надходимуть на відповідний процесор для опрацювання ITD, такий алгоритм вибрано для збереження контексту обробки даних і уникнення додаткових витрат на передачу даних між різними процесорами. Реалізація такого алгоритму може бути здійснена через спільну пам'ять, що дозволить кільком процесорам одночасно мати доступ до одного й того самого блоку пам'яті, використання черги повідомлень, з збереженням у оперативній пам'яті або на диску, при можливості кожного процесу додавати дані до черги або отримувати їх. У випадку необхідності максимальної продуктивності при обробці мережевого трафіку у реальному часі, оптимальним підходом може бути поєднання методів черг повідомлень для надійної синхронізації та спільної пам'яті для високошвидкісного обміну даними, оскільки процесори зможуть читати і записувати дані з мінімальними затримками.

Процес взаємодії Suricata та Intelligent Threat Detector базуватиметься на на можливостях обох систем для аналізу мережевого трафіку та прийняття рішень. Після перехоплення пакету Suricata аналізує його вміст, визначаючи тип протоколу, наприклад, TCP, UDP, ICMP, HTTP, SSL тощо. Цей крок дозволяє системі використовувати відповідні правила для конкретного типу трафіку. Далі, Suricata порівнює перехоплені пакети з наборами правил та сигнатур, щоб виявити потенційно небезпечні пакети, фільтрація пакетів відбувається в режимах IPS – NFQ та AF_PACKET. Якщо

пакет відповідатиме певному правилу або сигнатурі, Suricata маркує його як підозрілий, таке маркування може включати додавання метаданих до пакету або встановлення певної мітки або прапорця, який вказує на необхідність глибшого аналізу.

Intelligent Threat Detector, отримавши дані від Suricata, опрацьовує їх з використанням моделей машинного навчання та інтелектуальних алгоритмів виявлення складних загроз та аномалій. Результати аналізу ITD, наприклад як, оцінка ризику, тип загроз та рекомендовані дії повертаються до Suricata або центральної системи, використовуючи вищевказані методи синхронізації та координації доступу до спільної пам’яті.

В запропонованій моделі Suricata виконує первинну фільтрацію пакетів, і модуль ITD проводить глибокий аналіз підозрілих пакетів, після чого, отримані результати потрібно об'єднати та передати для прийняття рішень. Таку функцію здійснюватиме центральна система із збереженням даних у спільній пам’яті. Центральна система, отримавши результати аналізу здійснює журналювання, внесення змін до політик безпеки, оповіщення та приймання рішень про дії з підозрілим трафіком на основі результатів ITD.

Прогнозованим результатом інтеграції методів машинного навчання для аналізу трафіку та виявлення аномалій є підвищення продуктивності завдяки паралельній обробці, забезпечення швидкого виявлення і реакції на загрози, ефективне використання ресурсів багатопроцесорних систем.

Висновок

Модернізація систем виявлення та протидії загрозам є важливим аспектом безпеки у сучасних мережах. Традиційні методи, що базуються на правилах і сигнатурах, стають менш ефективними перед складними та динамічними загрозами, які постійно еволюціонують. Додавання модулів машинного навчання до існуючих IDPS систем, значно підвищує їх здатність виявляти і протидіяти новим та невідомим загрозам.

У даній роботі пропонується розроблення моделі системи виявлення та протидії кіберзагрозам із підтримкою та оновленням правил виявлення атак. Особливістю даної системи є можливість виявляти вторгнення незалежно від способу аналізу мережевого трафіку та автоматично блокувати підозрілий трафік, що дозволить мінімізувати шкідливий вплив атак у мережі. Пропонована інтелектуальна система IDPS складається з двох частин: основа системи заснована на IDS з відкритим вихідним кодом і блок машинного навчання для автоматичної підтримки та оновлення правил виявлення атак. Система може перехоплювати мережеві пакети для аналізу інформації, будуючи функції обробки на основі обраних даних для визначення можливості вторгнення. Перший модуль використовує Suricata для виконання початкової функції фільтрації пакетів, діючи як самодостатня система IDS. Модуль машинного навчання інтегрований в основний модуль, що використовує рішення під назвою IDT (Intelligent Threat Detector) на основі методів машинного навчання. Основний модуль здійснюватиме фільтрацію верхнього рівня, видаляючи пакети, які вважаються небезпечними згідно з наборами правил, наданими IDS-пристроєм. Система повинна обробляти кожен вхідний пакет, тому необхідно визначити властивості, які потрібно передати в блок машинного навчання для подальшої обробки.

Для підвищення швидкості обробки пакетів пропонується використовувати багатопроцесорну систему з інтеграцією машинного навчання та паралельним аналізом пакетів. Її основою буде використання модуля Intelligent Threat Detector (ITD), що дозволить підвищити ефективність і точність виявлення загроз. ITD, заснований на методах машинного навчання для аналізу мережевого трафіку, дозволить виявляти більш складні та нові загрози, які можуть залишатися непоміченими при використанні традиційних правил IDS, адаптуючись до нових загроз на основі постійно оновлюваних даних, підвищуючи точність виявлення. Крім того, можна застосувати способи динамічного балансування або балансування на рівні ядра операційної системи. Процес

взаємодії Suricata та Intelligent Threat Detector базуватиметься на на можливостях обох систем для аналізу мережевого трафіку та прийняття рішень. Після перехоплення пакету Suricata аналізує його вміст, визначаючи тип протоколу, наприклад, TCP, UDP, ICMP, HTTP, SSL тощо. Intelligent Threat Detector, отримавши дані від Suricata, опрацьовує їх з використанням моделей машинного навчання та інтелектуальних алгоритмів виявлення складних загроз та аномалій. Результати аналізу ITD, наприклад як, оцінка ризику, тип загроз та рекомендовані дії повертаються до Suricata або центральної системи, використовуючи вищевказані методи синхронізації та координації доступу до спільної пам'яті. В запропонованій моделі Suricata виконує первинну фільтрацію пакетів, і модуль ITD проводить глибокий аналіз підозрілих пакетів, після чого, отримані результати потрібно об'єднати та передати для прийняття рішень.

Крім того, розташування системи після фаєрволу допомагає знизити навантаження на систему виявлення, підвищуючи загальну продуктивність опрацювання вхідного трафіку і забезпечуючи при цьому високий рівень безпеки. Такий підхід дозволяє ефективно управляти трафіком, відсівати відомі загрози на ранньому етапі і направляти підозрілий трафік на глибший аналіз.У підсумку, модернізація IDPS систем із додаванням модуля ITD є необхідним кроком для забезпечення надійного захисту мережі від сучасних кіберзагроз.

Список використаних літературних джерел

[1] *Adeleke O. (2020). Intrusion detection: issues, problems and solutions. In 3rd International Conference on Infȯormation and Computer Technologies (ICICT). IEEE. 2020 pp. 397-402, https://doi.org/10.1109/ICICT50521.2020.00070*

[2] *Advanced Signature-Based Intrusion Detection System *Asma Shaikh1 and Preeti Gupta21aAmity University Maharashtra, Mumbai Maharashtra India, Marathwada MitraMandal College of Engineering, Pune , January 2023, https://doi.org/ 10.1007/978-981-19-1844-5_24*

[3] *Fosić, I., Žagar, D., Grgić, K. & Križanović, V. 2023. Anomaly detection inNetFlow network traffic using supervised machine learning algorithms. Journal ofIndustrial Information Integration, 33, art.number:100466. https://doi.org/10.1016/j.jii.2023.100466.*

[4] *Indraneel Mukhopadhyay, Mohuya Chakraborty, Satyajit Chakrabarti, «A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems», Journal of Information Security, 2011, 2, 28-38, https://doi.org/10.4236/jis.2011.21003*

[5] *M. Al-Qurishi, M. Alrubaian, S. M. M. Rahman, A. Alamri and M. M. Hassan, "A prediction system of sybil attack in social network using deep-regression model", Future Gener. Comput. Syst., vol. 87, pp. 743-753, Oct. 2018.*

[6] *Tianyu Gao, Jin Yang, Wenjun Peng, Luyu Jiang, Yihao Sun ,Fangchuan Li "A Content-Based Method for Sybil Detection in Online Social Networks via Deep Learning", IEEE Access (Volume: 8), Pages: 38753 – 38766, February 24, 2020, https://doi.org/10.1109/ACCESS.2020.2975877*

[7] *https://www.snort.org/*

[8] *SNORT Users Manual [Електронний ресурс] – Режим доступу до ресурсу:http://manual-snort-org.s3-website-us-east-1.amazonaws.com/*

[9] *https://docs.suricata.io/en/latest/what-is-suricata.html*

[10] *Т. Коробейнікова, О. Цар, Аналіз сучасних відкритих систем виявлення та запобігання вторгнень, Міжнародний науковий журнал «Грааль науки», №27, с. 317-325, 2023, https://doi.org/10.36074/grail-of-science.12.05.2023.050*

[11] *Yu-Xin Ding, Min Xiao, Ai-Wu Liu, Research and implementation on snort-based hybrid intrusion detection system, IEEE publiser, ISBN: 978-1-4244-3702-3, 2009.*

[12] *Abhishek Mitra, Walid Najjar, Laxmi Bhuyan, Compiling PCRE to FPGA for accelerating SNORT IDS, ANCS '07 Proceedings of the 3rd ACM/IEEE Symposium on Architecture for networking and communications systems, Pages 127-136, 2007.*

[13] *Vasiliadis G., Antonatos S., Polychronakis M., Markatos E. P., Ioannidis S. Gnort: High Perfomance Network Intrusion Detection Using Graphics Processors, Heraklion, Crete, Greece, 2008.*

DEVELOPMENT OF A MODEL OF A CYBER THREATS DETECTION SYSTEM WITH SUPPORT AND UPDATE OF ATTACK DETECTION RULES

Andriy Holdii, Olha Shpur, Andriy Masyuk

Lviv Polytechnic National University, S. Bandery Str., 12, 79013, Lviv, Ukraine

The article addresses the issue of data protection in information and communication systems amid the growing volume of traffic and the increasing number of cyber threats, necessitating improvements in the effectiveness of intrusion detection and prevention systems. Various types of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), their advantages, and disadvantages are considered. The methods of threat detection are analyzed, including signature-based methods, anomaly detection methods, and machine learning-based methods. Special attention is paid to methods of attack detection based on traffic content. The effectiveness of various commercial and open-source solutions, such as Snort and Suricata, is compared in terms of their architecture, performance, and accuracy. The main proposal is to enhance the Suricata system with an additional module called the Intelligent Threat Detector (ITD), which is based on machine learning methods. The ITD module is integrated into the main Suricata module and performs deep traffic analysis and anomaly detection. This approach helps reduce the load on the detection system, improving the processing performance of incoming traffic and ensuring a high level of security. The proposed solution provides a multi-level approach to network protection, where initial filtering is carried out by Suricata, and deep analysis is performed by ITD. The system can intercept network packets for information analysis, building processing functions based on selected data to determine the possibility of intrusion. Additionally, the integration of the ITD module allows the system to adapt to new and unknown threats in real time, as the module continuously learns from new data, ensuring continuous improvement in detection accuracy and response to threats. Placing the system behind the firewall helps reduce the load on the detection system, ensuring efficient use of multiprocessor system resources and reducing false positives.

Keywords: *IPS, IDS, attack, distributed systems, load balancing, detection*