Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Захист інформаційно-телекомунікаційної системи з використанням IDS (IPS) - технологій»

Виконавець: студентка IV курсу, групи КБ-42

_____ **Ірина ЧЕРНЯВКА**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Юрій ЩЕБЛАНІН	

Нормоконтроль	Сергій ДАКОВ	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентові **КБ-42** (група) **Чернявці Ірині Юріївній** (прізвище ім'я по-батькові)

Тема дипломної роботи Захист інформаційно-телекомунікаційної системи з використанням IDS (IPS) - технологій

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Інформаційно-телекомунікаційні системи, протоколи зв'язку, засоби мережевого захисту , технології захисту інформаційно-телекомунікаційних систем

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Нормативно-правова база у сфері захисту інформаційно-телекомунікаційних систем, проведення аналізу основних загроз для телекомунікаційних систем, проведення аналізу систем виявлення вторгнень та розробка рекомендацій щодо їх вибору

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Поєднання системи виявлення та система запобігання

вторгнень, формування рекомендацій щодо їх вибору.

5.ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ініціали, прізвище)

Завдання прийняла до виконання _____ (підпис) Ірина ЧЕРНЯВКА (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021 – 27.01.2022	*виконано*
2	Аналіз літератури	28.01.2022 – 11.02.2022	*виконано*
3	Огляд системи виявлення вторгнень	12.02.2022 – 24.02.2022	*виконано*
4	Збір відомостей щодо системи запобігання вторгненням	25.02.2022 – 24.03.2022	*виконано*
5	Аналіз класифікації IDS – технологій	25.03.2022 – 07.04.2022	*виконано*
6	Дослідження основних вразливостей IDS (IPS) – технологій	08.04.2022 – 20.04.2022	*виконано*
7	Визначення важливих факторів при виборі рішення IDS (IPS)	21.04.2022 – 05.05.2022	*виконано*
8	Дослідження рекомендації щодо оцінки системи виявлення вторгнень	06.05.2022 – 20.05.2022	*виконано*
9	Формування рекомендацій щодо вибору IDS (IPS) – технологій	21.05.2022 – 01.06.2022	*виконано*
10	Оформлення пояснювальної записки	02.06.2022 – 06.06.2022	*виконано*
11	Підготовка до захисту	07.06.2022 – 13.06.2022	*виконано*

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ініціали, прізвище)

Завдання прийняла до виконання _____ (підпис) Ірина ЧЕРНЯВКА (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 61 сторінок основного тексту, 2 таблиці та 7 рисунків. Список використаних джерел містить 36 найменування і займає 3 сторінок.

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння;

Об'єктом дослідження є процес захисту інформаційно-телекомунікаційної системи від кібератак.

Предметом дослідження є використання можливостей IDS (IPS) – технологій для захисту інформаційно-телекомунікаційної системи.

У роботі проаналізована існуюча література з теорії систем виявлення та запобігання вторгненням, виконаний аналіз документів, порівняння, вивчення та узагальнення вітчизняної і зарубіжної практики з теми IDS (IPS) – технологій, розроблено рекомендації щодо вибору IDS (IPS) – технологій.

Результати досліджень можуть застосовуватися в області інформаційної безпеки, які дають можливість розробникам і користувачам обрати ефективний, найбільш вдалий та дієвий спосіб захисту інформації, яка циркулює в інформаційно-телекомунікаційних системах.

Ключові слова: атака, кібератака, вторгнення, загроза, система виявлення вторгнень, система запобігання вторгненням, безпека інформаційно-телекомунікаційної системи.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

DoS	–	Denial Of Service
GAN	–	Generative Adversarial Network
HIDS	–	Host-Based Intrusion Detection System
HIPS	–	Host-Based Intrusion Prevention Sysytem
HTTP	–	Hypertext Transfer Protocol
IDS	–	Intrusion Detection Sysytem
IP	–	Internet Protocol
IPS	–	Intrusion Prevention Sysytem
ISO	–	International Organization for Standardization
IT	–	Information Technology
NGIPS	–	Next Generation Intrusion Prevention System
NIDS	–	Network Intrusrnn Detection Systems
NIPS	–	Network-Based Intrusion Prevention Sysytem
OSI	–	Open System Interconnection
PIDS	–	Perimeter Intrusion Detection System
R2L	–	Root To Local
SIEM	–	Security Information And Event Management
TCP	–	Transmission Control Protocol
U2R	–	User To Root
UDP	–	User Datagram Protocol
VM	–	Virtual Machine
VMIDS	–	Virtual Machine-Based Intrusion Detection System
ІКТ	–	Інформаційно-комунікаційні технології
ПЗ	–	Програмне забезпечення
СВВ	–	Система виявлення вторгнень
ЦП	–	Центральний процесор
ШІ	–	Штучний інтелект

ЗМІСТ

ВСТУП

Актуальність роботи зумовлюється тим, що системи виявлення вторгнень в наш час стали одним з основних інструментів для захисту від атак.

Завдяки широкому використанню технологій підприємства будь-якого розміру отримали значну користь від використання Інтернету та технічних ресурсів. З іншого боку, віртуальні загрози безпеки стають дедалі зростаючою проблемою. А допомогти нам може система виявлення вторгнень (IDS) - це мережеві пристрої або програмне забезпечення, яке покращує безпеку комп'ютерних мереж, виявляючи атаки в режимі реального часу. Система виявлення вторгнень просто відстежує мережевий трафік і попереджає адміністратора мережі про будь-які незвичайні дії. Це дуже схоже на домашню сигналізацію, яка подає сигнал, якщо зловмисник спробує проникнути у вікно або двері.

Метою роботи є розробка рекомендацій щодо вибору IDS (IPS) – технологій захисту інформаційно-телекомунікаційної системи, для її досягнення було визначено наступні *завдання*:

- провести аналітичний огляд систем виявлення та запобігання вторгненням;
- провести аналіз класифікації IDS – технологій;
- встановити особливості атак за допомогою штучного інтелекту;
- визначення найбільш важливих факторів при виборі рішення IDS або IPS**;**
- розробка рекомендації щодо оцінки системи виявлення вторгнень;
- використання програмного забезпечення провідних рішень IDS та IPS - технологій.

Об'єктом дослідження є процес захисту інформаційно-телекомунікаційної системи від кібератак.

Предметом дослідження є використання можливостей IDS (IPS) – технологій для захисту інформаційно-телекомунікаційної системи.

Методи дослідження дипломної роботи:

- аналіз документів;

- порівняння;
- вивчення та узагальнення вітчизняної і зарубіжної практики.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ IDS (IPS) – ТЕХНОЛОГІЙ

1.1 Дослідження поняття IDS

IDS, IPS (Intrusion Detection System, Intrusion Prevention System), системи виявлення та запобігання вторгненням – це мережеві пристрої, які підвищують безпеку комп’ютерних мереж шляхом виявлення (IDS) або виявлення та блокування атак (IPS) у режимі реального часу. В ієрархії захисту ІКТ-інфраструктури вони повинні розташовуватися як наступні — після брандмауера — системи захисту. IDS використовується для моніторингу та сповіщення про загрози та інциденти безпеки. У свою чергу, IPS вживає додаткових заходів, щоб зупинити атаку, мінімізувати її наслідки або активно реагувати на порушення безпеки. Поведінку двох цих систем ми можемо побачити на рисунку 1.1. [1]. Таким чином, дані рішення дають змогу підвищити рівень безпеки комп’ютерних мереж за рахунок посилення контролю зв’язку між мережами різного ступеня довіри. Ефективна система захисту на основі IDS/IPS повинна враховувати специфіку діяльності компанії, оцінювані джерела загроз комп'ютерної мережі, і на цій основі приймати рівень рішення, що випливає з аналізу ризиків.

Система IPS використовує багаторівневий аналіз і механізми безпеки, такі як аналіз протоколів, виявлення аномалій у мережевому трафіку або кореляції подій. Він також дозволяє створювати власні правила на основі порівняння моделей атак.

Система IDS зазвичай працює як сніфер (комп'ютерна програма, завданням якої є перехоплення та аналіз даних, що надходять у мережу), виявляючи спробу порушення безпеки та інформуючи брандмауер про місцезнаходження (IP-адресу) зловмисника. Як наслідок, брандмауер блокує пакети з заданої адреси, які беруть участь у атаці.

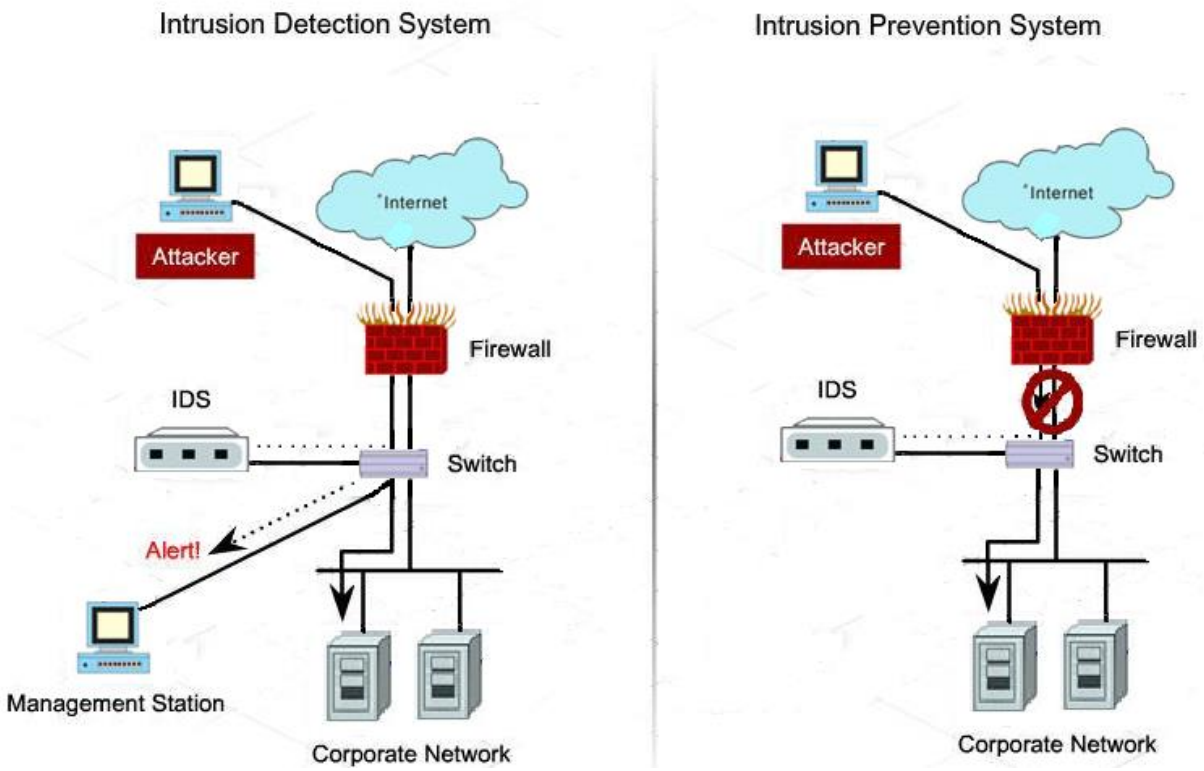


Рисунок 1.1 - Поведінка системи виявлення вторгнення (ліворуч), поведінка системи запобігання вторгнення (праворуч)

Виявлення вторгнень — це процес моніторингу та виявлення спроб несанкціонованого доступу до системи або маніпуляцій. Система ідентифікації збирає та аналізує інформацію з різних областей комп’ютера або мережі для виявлення можливих порушень безпеки, які включають як вторгнення (атака ззовні організації), так і зловживання (атака зсередини організації).

Система виявлення вторгнень (IDS) є ще одним інструментом в арсеналі комп'ютерної безпеки адміністратора мережі. Він перевіряє всю вхідну та вихідну мережеву активність. IDS ідентифікує будь-який підозрілий шаблон, який може вказувати на атаку на систему, і діє як перевірка безпеки всіх транзакцій, які відбуваються в системі та поза нею.

Системи виявлення IDS використовуються для підвищення безпеки мережі як зсередини, так і ззовні. Перевага систем IDS полягає в тому, що їх можна використовувати для аналізу мережевого трафіку.

Методи виявлення, що використовуються в IDS [2]:

- виявлення аномалій (anomalny detection);

- виявлення підпису (signature detection);
- цільовий моніторинг (target monitoring);
- невидиме зондування (invisible probing);
- виявлення на основі медового горщика (honey pot).

Виявлення аномалій — це виявлення нестандартних моделей поведінки. Зберігається набір стандартних випадків використання системи. Усі події, що відхиляються від цієї схеми, класифікуються як потенційно небезпечні.

Метод виявлення аномалій можна класифікувати за різними критеріями, котрі представлені на рисунок 1.2.

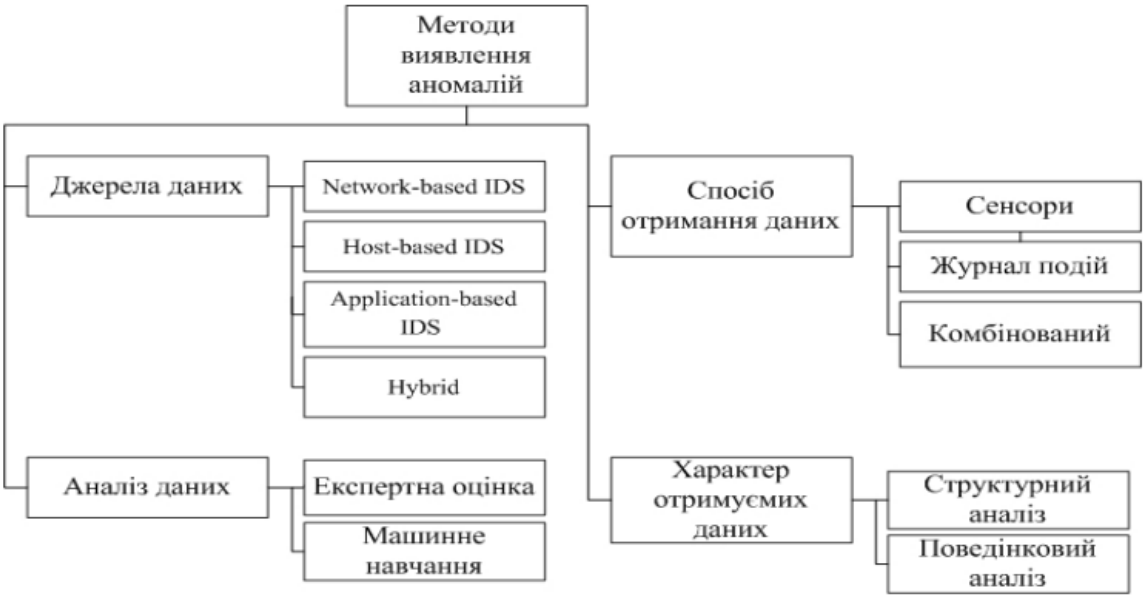


Рисунок 1.2 - Класифікація методів виявлення аномалій

IDS на основі статистичних аномалій встановлює базову лінію продуктивності, використовуючи звичайні оцінки мережевого трафіку. Потім він аналізує поточну активність мережевого трафіку до цієї базової лінії, щоб визначити, чи знаходиться вона в межах базових параметрів. Якщо вибірковий трафік виходить за межі базових параметрів, буде спрацьовано тривогу.

Системи виявлення аномалій використовують інший підхід до виявлення шкідливого вмісту. Замість відбитків пальців відомих атак вони будують модель «нормальної» поведінки для певної системи. Після створення цієї моделі «нормальної поведінки» інструмент може шукати все, що не відповідає його

моделі (аномалія). Якщо модель добре навчена, будь-які аномалії повинні бути нападами [3].

IDS на основі підпису

Мережевий трафік перевіряється на наявність попередньо налаштованих і визначених моделей атак, відомих як сигнатури. Сьогодні багато атак мають різні ознаки. У належній практиці безпеки колекція цих підписів повинна постійно оновлюватися, щоб пом’якшити виникаючі загрози [4].

Виявлення сигнатур зберігає набір небажаних моделей поведінки, щоб виявити дії зловмисників, подібні до них. Ці шаблони є підписами.

Алгоритм на основі сигнатур порівнює активність мережі з відомими атаками. Після того, як зловмисне програмне забезпечення або інший шкідливий вміст було ідентифіковано та проаналізовано, з нього витягуються унікальні функції, щоб створити відбиток пальця цієї конкретної атаки [3].

Стратегії виявлення на основі сигнатур мають дуже низький рівень хибнопозитивного виявлення, але можуть виявляти лише відомі атаки. Розгортання рішень, які використовують обидві стратегії, у поєднанні створює надійніше рішення з кращим виявленням загроз, ніж ізольовано будь-який підхід.

Цільовий моніторинг заснований на тому, що система перевіряє, чи не були змінені певні файли не санкціоновано. Порівняння файлів здійснюється за допомогою хешування (хеш-функція) і порівняння хешування [4].

Невидиме зондування виявляє зловмисників, які атакують вашу систему протягом тривалого періоду часу. Щоб виявити підозрілу поведінку, цей метод поєднує виявлення аномалій із виявленням сигнатур.

Виявлення на основі меду використовує сервер-замінник. Це дає можливість ізолювати атаки від реальних систем. Він дає змогу аналізувати типи вхідних атак і шаблони шкідливого трафіку. Цей метод корисний для виявлення поширених атак на мережеві ресурси та внесення необхідних виправлень на основі цього для захисту цих ресурсів [5].

Типи тривог, що генеруються системою IDS:

- помилкові тривоги:

o помилковий позитив: звичайний, нормальний мережевий трафік ініціює дію підпису;

o помилковий негатив: незаконний мережевий трафік не запускає дію, пов'язану з підписом, атака не виявляється;

- справжні тривоги:

o справжній позитив: незаконний мережевий трафік ініціює дію, пов'язану з підписом, виявляється атака;

o справжній негатив: нормальний, нормальний мережевий трафік не запускає дію підпису, звичайний трафік не викликає тривогу.

1.2 Аналіз класифікації IDS технологій

Для цілей роботи з IT існує чотири основних типи IDS [6]:

- Система виявлення вторгнень в мережу (NIDS);
- Система виявлення вторгнень на базі хоста (HIDS);
- Система виявлення вторгнення по периметру (PIDS);
- Система виявлення вторгнень на основі VM (VMIDS).

1.2.1 IDS на основі хосту (HIDS)

HIDS складається з агента на хості, який ідентифікує вторгнення, аналізуючи системні виклики, журнали програм, модифікації файлової системи (двійкові файли, файли паролів, бази даних можливостей, списки контролю доступу тощо) та інші дії та стан хоста. У HIDS датчики зазвичай складаються з програмного агента. Деякі IDS на основі програм також є частиною цієї категорії. Прикладом HIDS є OSSEC.

Системи виявлення вторгнень також можуть бути специфічними для системи за допомогою спеціальних інструментів і медіа. У випадку фізичної безпеки будівлі IDS визначається як система сигналізації, призначена для виявлення несанкціонованого проникнення.

HIDS може бути хорошим додатковим рішенням до мережевої програми IDS від ISO, оскільки надає додаткові можливості виявлення в результаті доступу до локальної операційної системи та файлової структури. HIDS може забезпечити додаткове виявлення шляхом встановлення агентів на системах, що контролюються. Центральний сервер керування зазвичай контролює програмне забезпечення агента через мережу, яке підтримує конфігурацію агента, як визначено адміністратором HIDS, і збирає події з програмного забезпечення агента. На основі зібраних подій центральний сервер HIDS може співвідносити дії з усіх своїх хостів, які контролюються, на основі попередньо визначених сигнатур і налаштованих правил, щоб створювати попередження про підозрілу або зловмисну поведінку. Зібрані події також можна надіслати в програмне забезпечення кореляції журналів (наприклад, програму кореляції журналів ISO) для подальшого аналізу.

Деякі з додаткових можливостей виявлення включають:

- виявлення на рівні файлу:

  - перевірка цілісності файлів включає періодичне генерування дайджестів повідомлень або інших криптографічних контрольних сум для критичних файлів, порівняння їх із контрольними значеннями та виявлення відмінностей. Перевірка цілісності файлу може лише згодом визначити, що файл уже змінено, наприклад, замінено системний двійковий файл троянським конем або руткітом;

  - перевірка атрибутів файлів — це періодична перевірка атрибутів важливих файлів, таких як право власності та дозволи, на наявність змін. Як і перевірка цілісності файлу, вона може визначити лише після факту, що відбулася зміна;

  - спроби доступу до файлу. Агент із прокладкою файлової системи може контролювати всі спроби отримати доступ до критичних файлів, таких як системні двійкові файли, і зупиняти підозрілі спроби. Агент має набір політик щодо доступу до файлів, тому агент порівнює ці політики з характеристиками поточної спроби, включно з тим, який користувач або програма намагається отримати доступ до кожного файлу, і який тип доступу було запитано (читання, запис, виконати). Це може бути використано для запобігання встановленню деяких форм шкідливого програмного забезпечення, наприклад руткітів і троянських коней, а також для

запобігання багатьом іншим видам шкідливої діяльності, що включає доступ до файлів, їх зміну, заміну або видалення;

- аналіз коду:

  - моніторинг системних викликів. Агент знає, які програми та процеси мають викликати які інші програми та процеси чи виконувати певні дії. Наприклад, агент може розпізнати процес, який намагається перехопити натискання клавіш, наприклад кейлоггер. Агенти також можуть обмежувати, які драйвери можна завантажувати, що може запобігти встановленню руткітів та іншим атакам;

  - списки програм і бібліотек. Агент може контролювати кожну програму та бібліотеку, які користувач або процес намагаються завантажити, і порівнювати цю інформацію зі списками авторизованих і неавторизованих програм і бібліотек. Це можна використовувати не тільки для обмеження, які програми та бібліотеки можна використовувати, але й для того, які їх версії можна використовувати;

- моніторинг конфігурації:

  - деякі агенти можуть контролювати поточну конфігурацію мережі хоста та виявляти зміни в ній. Зазвичай відстежуються всі мережеві інтерфейси на хості, включаючи дротові, бездротові, віртуальну приватну мережу і модем. Прикладами значних змін конфігурації мережі є переведення мережевих інтерфейсів у безладний режим, використання додаткових портів TCP або UDP на хості або використання додаткових мережевих протоколів, наприклад, протоколів без IP. Ці зміни можуть свідчити про те, що хост уже зламано і налаштовується для використання в майбутніх атаках або для передачі даних [7].

Системи HIDS збирають та аналізують дані на комп’ютері (хості), на якому реалізована ця система. Зібрані дані можна проаналізувати локально або на спеціально призначеному для цієї мети комп’ютері.

Додаток HIDS може бути реалізацією, завданням якої є збір системних журналів і журналів програм з інших комп’ютерів. У разі великих мереж це рішення неефективне і незручне. Однією із запропонованих систем збору журналів є IBM Tivoli.

Вихідний код деяких функцій не включено, але їх відносно легко відтворити, тому в цьому просто немає потреби. Для зацікавлених автор надасть повний вихідний код електронною поштою.

K-Means Clustering є відносно простим алгоритмом для класифікації даних [2].

1.2.2. IDS на основі мережі (NIDS)

NIDS — це незалежна платформа, яка ідентифікує вторгнення, досліджуючи мережевий трафік і відстежує декілька хостів. Системи виявлення вторгнень в мережу отримують доступ до мережевого трафіку, підключаючись до мережевого концентратора, мережевого комутатора, налаштованого на дзеркальне відображення портів, або мережевого крана [4]. У NIDS датчики розміщуються в точках заглушення в мережі для моніторингу, часто в демілітаризованій зоні або на кордонах мережі. Датчики фіксують весь мережевий трафік і аналізують вміст окремих пакетів на наявність шкідливого трафіку. Прикладом NIDS є Snort.

NIDS працює шляхом перевірки пакетів, надісланих у комп’ютерній мережі. Пакети аналізуються, а потім класифікуються з точки зору правильності. Комп’ютерна мережа, оснащена NIDS, характеризується підвищеною стійкістю до зовнішніх атак. Такі системи дуже добре справляються з несанкціонованим доступом. Обмеженням використання систем NIDS є мережі, в яких передача зашифрована або дуже швидка (понад 80 Мбіт/с). Тоді аналіз надісланого вмісту стає неповним. Прикладом такого рішення IDS є пристрій Cisco IDS-4215.

Рішенням, яке усуває це обмеження, є використання гібридної системи, що складається з HIDS і NIDS. Прикладом такого рішення є розподілена мережа агентів (клієнтське програмне забезпечення), в якій агенти обмінюються інформацією один з одним [4].

1.2.3 Система виявлення вторгнення по периметру (PIDS)

Виявляє та визначає місця спроб вторгнення на периметр огорож критичної інфраструктури. Використовуючи або електроніку, або більш досконалу технологію опто- волоконного кабелю, встановлену на огорожі по периметру, PIDS виявляє порушення на паркані. Якщо вторгнення виявлено та розцінено системою як спроба вторгнення, спрацьовує сигнал тривоги [8].

1.2.4 Система виявлення вторгнень на основі VM (VMIDS)

VMIDS виявляє вторгнення за допомогою моніторингу віртуальної машини. Використовуючи це, ми можемо розгорнути систему виявлення вторгнень із моніторингом віртуальної машини. Це найновіший тип, який все ще розробляється [8]. Немає необхідності в окремій системі виявлення вторгнень, оскільки за допомогою неї ми можемо контролювати загальну діяльність.

1.3 Дослідження поняття IPS технологій

Особливістю системи IPS є те, що, крім того, що вона виявляє атаки на системи ІКТ (як у випадку системи IDS), вона запобігає їх здійсненню. Дана система дозволяє відстежити і зареєструвати спроби несанкціонованої мережевої активності і опційно блокувати атаки в режимі реального часу. Схема роботи мережі з використанням системи запобігання вторгнень зображена на рисунку 1.3 [9].

За топологією системи IPS поділяються на мережеві рішення, у тому числі засновані на пасивному зонді, підключеному до порту моніторингу комутатора, що аналізує всі пакети в даному сегменті мережі, і вбудовані - із зондом, розміщеним між двома сегментами мережі, не має IP-адрес і працює в режимі прозорого мосту, пересилаючи всі пакети в мережі.

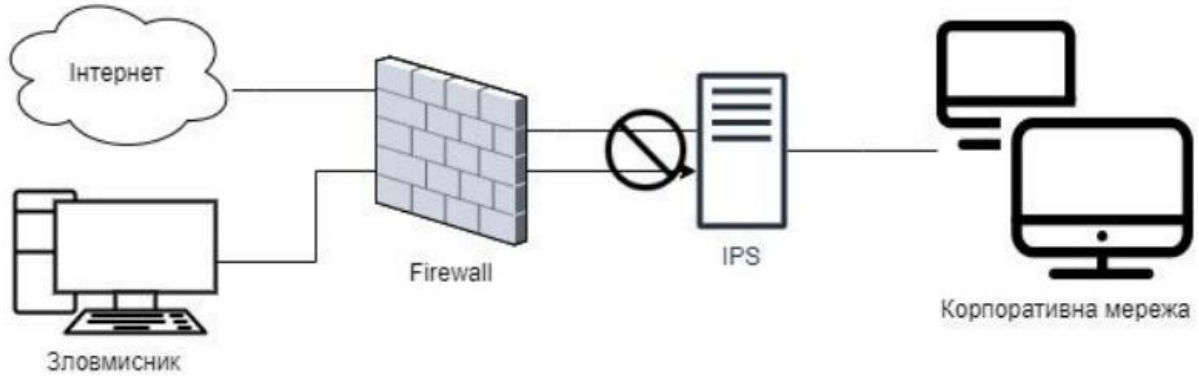


Рисунок 1.3 – Схема роботи мережі з використанням системи запобігання вторгнень

З технічної сторони IPS значною мірою є поєднанням IDS з системою брандмауера.

Датчики IPS порівнюють мережевий трафік із сигнатурами. Сигнатури мають три характерні ознаки: тип сигналу, тригер і дію.

IPS-системи можуть бути у двох варіантах:

- мережевий IPS (NIPS);
- IPS на основі хосту (HIPS).

1.3.1. IPS на основі хоста

HIPS — це програмний агент, встановлений в операційній системі під захистом. Він забезпечує виявлення та захист від атак. Він не вимагає спеціального обладнання.

Характеристики HIPS:

- призначений для системи, на якій він встановлений;
- записує інформацію про атаки, здійснені зловмисником;
- шифрування передачі даних не обмежує роботу системи;

Обмеження HIPS:

- відсутність можливості кореляції подій при спостереженні окремих агентів;
- кожному агенту потрібна ліцензія;

- відсутність програмного забезпечення (агента) для деяких програмних платформ, представлених постачальником системи.

1.3.2. Мережевий IPS

У випадку з технологією NIPS, датчики підключаються до сегментів мережі, і один датчик може контролювати кілька комп'ютерів. Розширення мережі не впливає на ефективність захисту доданих пристроїв, які були представлені без додаткових датчиків. Ці датчики є мережевими пристроями, пристосованими для запобігання проникненню певного типу.

Характеристики мережі IPS:

- рентабельний (один датчик може захистити велику мережу);
- забезпечувати аналіз трафіку під час атак на нижніх рівнях моделі ISO / OSI,
- є незалежною операційною системою;
- мають багато варіантів виявлення;
- невидимі в мережі (IP не призначено).
- Обмеження мережі IPS (продуктивність):
- може бути перевантажений мережевим трафіком;
- можуть бути відмінності між мережевим трафіком, який сприймається IPS та отриманим цільовим;
- не працювати в зашифрованій мережі.

1.3.3. Типи підписів

Типи підписів:

- атомний;
- композитні.

Атомарні підписи мають прості форми. Вони містять опис окремого пакета, активності та події. Вони не вимагають зберігання інформації про стан («горизонт

подій») в IPS. Ці підписи легко ідентифікувати. Складені підписи часто називають державними. Вони визначають послідовність дій на кількох хостах. Підпис такого типу повинен містити інформацію про його статус.

1.4 Порівняння системи виявлення вторгнень з брандмауером

Хоча обидва вони стосуються безпеки мережі, система виявлення вторгнень (IDS) відрізняється від брандмауера тим, що брандмауер дивиться назовні, щоб запобігти вторгненням. Брандмауери обмежують доступ між мережами, щоб запобігти вторгненням і не сигналізують про атаку зсередини мережі. IDS оцінює підозрюване вторгнення, коли воно відбулося, і сигналізує про тривогу.

IDS також відстежує атаки, які відбуваються зсередини системи. Традиційно цього досягають шляхом вивчення мережевих комунікацій, визначення евристики та шаблонів (часто відомих як сигнатури) поширених комп’ютерних атак та вжиття заходів для попередження операторів. Система, яка розриває з'єднання, називається системою запобігання вторгненням і є іншою формою брандмауера прикладного рівня .

Що таке брандмауер?

Брандмауер – це пристрій, встановлений між внутрішньою мережею організації та іншою частиною мережі. Він призначений для пересилання одних пакетів і фільтрації інших. Наприклад, брандмауер може фільтрувати всі вхідні пакети, призначені для певного хоста або конкретного сервера, наприклад HTTP, або його можна використовувати для заборони доступу до певного хосту або служби в організації.

Брандмауери — це набір інструментів, які контролюють потік трафіку між мережами. Розміщений на рівні мережі та тісно співпрацюючи з маршрутизатором, він фільтрує всі мережеві пакети, щоб визначити, чи пересилати їх до місця призначення.

1.5 Безпека IDS і IPS технологій

Основними етапами в галузі безпеки передачі даних є: побудова комп'ютерних мереж, впровадження структури Інтернету в мережу, поширення антивірусних і антиспамових систем, впровадження технології брандмауера і, нарешті, складні методи захисту передачі даних між мережами, таких як IDS і IPS.

Безпека інфраструктури ІКТ може бути виражена формулою:

Безпека = Видимість + Контроль

Щоб забезпечити належний рівень безпеки для інфраструктури ІКТ, її слід одночасно контролювати та контролювати. Це забезпечується поєднанням технологій IDS та IPS. Технологія IDS забезпечує видимість, яка включає пасивний моніторинг мережі, зберігання подій і звітування. Наочність має вирішальне значення в процесі прийняття рішень адміністратором мережі щодо безпеки. Він дозволяє створювати політики безпеки на основі реальних даних, які можна виміряти.

Другим елементом формули вище є контроль. За контроль відповідає технологія IPS, яка забезпечує активний моніторинг мережі та дозволяє застосовувати політику безпеки в мережі ІКТ, встановлену адміністратором мережі.

Захист IDS

Захист компонентів IDS дуже важливий, оскільки IDS часто є мішенню зловмисників, які хочуть запобігти IDS від виявлення атак або хочуть отримати доступ до конфіденційної інформації в IDS, наприклад, конфігурації хостів та відомих вразливостей. IDS складаються з кількох типів компонентів, включаючи датчики або агенти, сервери керування, сервери баз даних, консолі користувача та адміністратора та мережі керування. Операційні системи та програми всіх компонентів повинні повністю оновлюватися, а всі програмні компоненти IDS мають бути захищені від загроз. Конкретні захисні дії особливого значення включають:

- підтримка операційних систем і програм повністю оновленими з останніми версіями від постачальника програмного забезпечення;

- створення окремих облікових записів для кожного користувача та адміністратора IDS;
- обмеження доступу до мережі до компонентів IDS;
- забезпечення належного захисту комунікацій керування IDS, наприклад їх шифрування або передачі через фізичну або логічно окрему мережу;
- періодично створюйте резервні копії налаштувань конфігурації та перед застосуванням оновлень, щоб переконатися, що наявні налаштування не будуть випадково втрачені [7].

Адміністратор мережевої безпеки повинен виконувати різні запобіжні заходи та ініціативи, щоб захистити мережу від зовнішніх або внутрішніх атак. Деякі з них:

- часто оновлюйте базу антивірусних сигнатур;
- налаштуйте брандмауер, щоб відфільтрувати ip-адресу зловмисника;
- подайте звуковий сигнал або відтворіть файл .wav як індикацію;
- змусити пакет tcp fin або rst примусово розірвати з’єднання;
- збережіть файл трасування необроблених пакетів для подальшого аналізу;
- збережіть інформацію про атаку (ip-адреса зловмисника, ip-адреса жертви, мітка часу);
- надішліть повідомлення адміністратору про атаку.

Адміністратори повинні підтримувати безпеку компонентів IDS на постійній основі, включаючи перевірку, що компоненти функціонують належним чином, моніторинг компонентів на предмет проблем безпеки, виконання регулярних оцінок вразливостей, відповідне реагування на вразливості в компонентах IDS, а також тестування та розгортання IDS оновлення.

Симптоми на вторгнення

Вторгнення в систему:

- помилка системи ідентифікації дійсного користувача;
- активний доступ до невикористаних логінів;
- вхід у неробочий час;
- новий обліковий запис користувача створено автоматично;

- зміни системного програмного забезпечення або файлів конфігурації;
- системні журнали видаляються;
- продуктивність системи різко знизилася;
- незвичайне відображення графіки, спливаючих вікон;
- система раптово виходить з ладу та перезавантажується без втручання користувача.

Вторгнення в файли:

- ідентифікація невідомих файлів і програм у вашій системі;
- зміни прав доступу до файлу;
- непояснені зміни розміру файлу;
- ідентифікація присутності дивного файлу в системних каталогах;
- відсутні файли.

Вторгнення в мережу:

- ідентифікація повторних спроб увійти з віддалених місць;
- раптове збільшення споживання пропускної здатності;
- повторні перевірки існуючих служб;
- довільні дані журналів у файлах журналів.

Висновки за розділом 1

Цей розділ проілюстрував важливість IDS та її різних типів. IDS відстежує хости на предмет змін в системі або виловлює мережеві пакети з дроту, шукаючи шкідливий вміст. Адміністратори безпеки повинні подумати про використання комбінацій HIDS і NIDS, як із виявленням сигнатур, так і з механізмами на основі аномалій.

IDS можна налаштувати виключно як пристрої моніторингу та виявлення або брати участь як вбудований пристрій і запобігати загрозам. Його найбільшими недоліками є велика кількість помилкових спрацьовувань і зусилля по технічному

обслуговуванню, необхідні для підтримання актуальності та тонкої настройки підписів.

У цьому розділі надано детальний огляд IDS та брандмауерів та їх ролі у захисті корпоративної мережі. Існує чотири основних типи брандмауерів: фільтрація пакетів, шлюзи програм, шлюзи рівня каналів та інші брандмауери. Хоча деякі передбачили кінець брандмауера, його стратегічне розташування в мережі робить його незамінним інструментом для захисту активів. Належні методи безпеки передбачають, що між будь-якими двома мережами з різними вимогами безпеки слід розгортати брандмауери.

Також ми розглянули безпеку IDS (IPS) – технологій. Щоб підтримувати надійну позицію безпеки, багато організацій використовують системи IPS і IDS для моніторингу мережевого трафіку. Майте на увазі, що багато атак спрямовані на використання відомих пробілів у програмному забезпеченні безпеки або затримок у завершенні оновлення системи. З цієї причини важливо, щоб системи безпеки працювали на повну потужність, використовуючи останні випуски.

РОЗДІЛ 2
ВРАЗЛИВОСТІ IDS (IPS) – ТЕХНОЛОГІЙ

2.1 Аналіз атак за допомогою штучного інтелекту

Штучний інтелект (ШІ) пройшов довгий шлях за дуже короткий період часу. Алан Тьюринг, перший вчений-комп'ютерник, опублікував першу роботу про можливості машин, які можуть мислити, у 1950 році. Менш ніж за століття люди створили машини та програми, які можуть обчислювати й осягати дуже великі обсяги даних, щоб вивчати та імітувати вчинки самих людей.

Люди, підприємства та уряди дуже покладаються на цю нову технологію, навіть не усвідомлюючи цього. Одним з зростаючих секторів ШІ є безпека. Системи виявлення вторгнень (IDS) — це системи, що використовуються для захисту мереж або систем від шкідливого трафіку. ШІ за своєю природою динамічний зі своєю здатністю до навчання, тому він ідеально підходить для цієї програми, щоб він міг навчатися та розвиватися. Завдяки цьому ШІ добре виявляє хороший і шкідливий інтернет-трафік, оскільки він не дотримується визначеного набору правил, а замість цього динамічно створює власні.

Системи виявлення вторгнень (IDS) відіграють велику роль у захисті цієї інформації, збереженої в мережі або системі, а ШІ інтегрується в IDS через низький рівень обслуговування та здатність залишатися в курсі останніх атак. Через швидкий розвиток ШІ потреба у підвищенні надійності цих систем була знехтувана, і поточні дослідження розглядають шляхи покращення IDS [10].

Нова технологія під назвою Generative Adversarial Network (GAN) намагається атакувати будь-які системи машинного навчання за допомогою ШІ. Атаки, які генерує GAN на системи машинного навчання, сплутають або обманюють алгоритм, виробляючи вихід, відмінний від очікуваного.

Рисунок 2.1 нижче є хорошим прикладом того, як GAN заплутує систему машинного навчання. Він приймає вхідні дані та змінює його, щоб він все ще

здавався оригіналом. Будь-яка людина, подивившись на ці два зображення, переконається, що вони обидва кішки. Вони обидва мають загострені вуха, вуса, форму обличчя, шерсть тощо. Але для системи машинного навчання, де вона аналізує зображення на більш глибокому, нижчому рівні, ці двоє дуже відрізняються. Той, що ліворуч, має набагато більше деталей, що збиває з пантелику систему машинного навчання, оскільки вона не бачить так багато шерсті і кольорів. Разом з цим зображення праворуч є набагато зрозумілішим, що або переконає систему машинного навчання, що зображення зліва занадто детальне, щоб бути кішкою, або зображення праворуч не має достатньо деталей, щоб бути кіт, хоча для людини це одне й те саме.

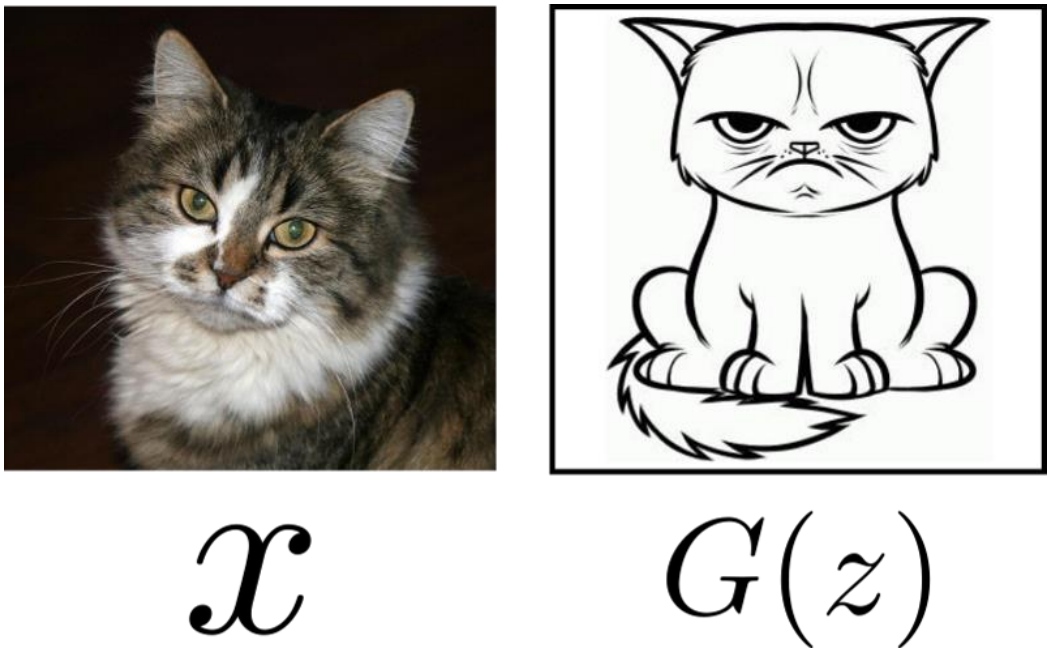


Рисунок 2.1 - Зображення котів

Атака на будь-яку IDS, засновану на машинному навчанні, містить три основні характеристики, які показують, яким це буде атака, тому вона потрапляє до одного з восьми окремих класів атак. Слід зазначити, що позитивне вважається шкідливим, а негативне — нормальним. Нижче наведено три різні класи, кожен із яких містить дві різні характеристики:

Вплив:

- причинні атаки впливають на навчання з контролем над даними навчання (змінити навчальний процес);
- дослідницькі атаки спричиняють відмову в обслуговуванні (DoS) (використовують наявні слабкі сторони), як правило, з помилковими спрацьовуваннями (відхиляють правильний вхід).

Порушення безпеки:

- атаки на цілісність компрометують активи через помилкові негативи (приймає шкідливий вхід);
- атаки доступності спричиняють відмову в обслуговуванні, як правило, через помилкові спрацьовування (відхилення правильного введення даних).

Специфіка:

- цільові атаки зосереджені на певному екземплярі (дозволяють певному вхідному сигналу пройти);
- невибіркові атаки охоплюють широкий клас випадків (пропускає багато речей).

Атака може брати одну характеристику для кожної категорії, і ніколи не візьме обидві з однієї категорії, оскільки обидві суперечать один одному. Залежно від типу IDS, який ви атакуєте, тип атаки, яку створить GAN, буде відрізнятися. Наприклад, IDS, заснований на послідовності (на основі правил), буде підданий атакам Exploratory Integrity, де специфічність не має значення. Атака Exploratory Integrity зосереджена на заповненні системи за допомогою помилкових негативів, що дозволяє шкідливому трафіку проникнути в систему. Обман IDS на основі послідовності включає надсилання масової кількості вхідних даних, кожен із дещо іншим наміром, щоб спробувати виконати всі правила, встановлені IDS. Мета може полягати в тому, щоб надіслати один зловмисний вхід або кілька, і це вирішуватиме поганий актор.

На рівні OSI відбувається багато різних атак, основні типи котрих показано на рисунку 2.2.

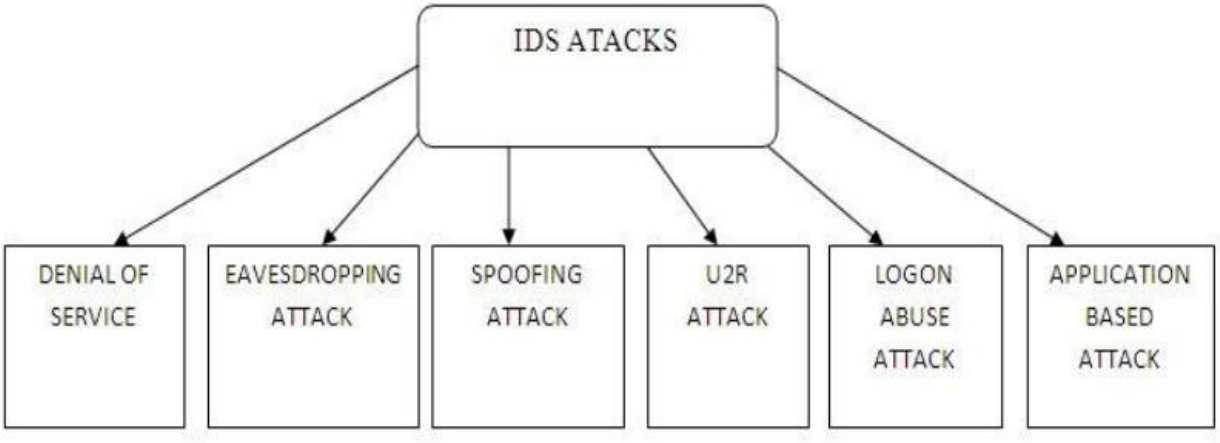


Рисунок 2.2 – Типи атак на систему

Ці атаки потім об’єднуються в 4 типи атак: «Відмова в обслуговуванні» (DoS), «Зондування», «User-to-root» (U2R) і «Root-to-Local» (R2L). Ці типи атак зосереджені на різних результатах, де намір кожної атаки показано нижче:

DoS — це атака, яка намагається закрити потік трафіку до та з цільової системи. IDS переповнений ненормальним обсягом трафіку, який система не може впоратися, і вимикається, щоб захистити себе. Це запобігає відвідуванню мережі звичайного трафіку. Прикладом цього може бути онлайн-роздрібний продавець, який переповнений онлайн-замовленнями в день великого розпродажу, і оскільки мережа не може обробити всі запити, вона закриється, не дозволяючи клієнтам-платникам купити що-небудь.

Зондування або спостереження — це атака, яка намагається отримати інформацію з мережі. Мета тут — діяти як злодій і вкрасти важливу інформацію, будь то особиста інформація про клієнтів чи банківська інформація.

U2R — це атака, яка починається зі звичайного облікового запису користувача і намагається отримати доступ до системи або мережі як суперкористувач (root). Зловмисник намагається використати вразливості в системі, щоб отримати root-права/доступ.

R2L — це атака, яка намагається отримати локальний доступ до віддаленої машини. Зловмисник не має локального доступу до системи/мережі і намагається «зламати» свій шлях до мережі.

У цих широких категоріях існує безліч різних форм комп’ютерних атак. Короткий зміст цих атак з коротким поясненням, характеристиками та прикладами представлено в таблиці 2.1.

Таблиця 2.1

Класи комп’ютерних атак

Види атаки	**Пояснення**
Переповнення буфера	Атакує межі буфера і перезаписує область пам'яті.
Черв'як	Відтворюється на локальному хості або через мережу.
Троянський	Програми виглядають привабливими та справжніми, але в них вбудований зловмисний код.
Відмова в обслуговуванні (DoS)	Подія безпеки, яка порушує роботу мережевих служб. Це починається з примусового скидання на цільових комп'ютерах. Користувачі більше не можуть підключитися до системи через недоступність послуги.
Сценарії загального інтерфейсу шлюзу (CGI)	Зловмисник використовує сценарії CGI для створення атаки, надсилаючи неправомірні дані на веб-сервер.

продовження табл.1.2

Фізичний напад	Прагне атакувати фізичні механізми комп'ютерної системи.
Атака паролем	Прагне зламати пароль протягом короткого часу, і це помічається послідовністю помилок входу.
Збір інформації	Збирає інформацію або знаходить слабкі місця в комп'ютерах або мережах за допомогою обнюхування чи пошуку.
Атака користувача до кореня (U2R)	Спочатку кіберзлочинець отримує доступ як звичайний користувач, а потім переходить на суперкористувача, що може призвести до використання декількох вразливостей системи.
Атака віддаленого до локального (R2L)	Кіберзлочинець надсилає пакети у віддалену систему, підключившись до мережі, не маючи облікового запису в системі.
Зонд	Визначення дійсних IP-адрес шляхом сканування мережі для збору пакетів даних хосту.

2.2 Методи ухилення від системи виявлення вторгнень

Методи ухилення від системи виявлення вторгнень є модифікації, внесені в атаки для запобігання виявлення вторгненням система виявлення (IDS). Багато опублікованих методів ухилення модифікують мережеві атаки. У статті 1998 року «Вставка, ухилення

та відмова в обслуговуванні: вислизання від виявлення мережевих вторгнень» популяризувалося ухилення від IDS та обговорювалися як методи ухилення, так і області, у яких правильна інтерпретація була неоднозначною залежно від цільової комп'ютерної системи. Програми fragroute та fragrouter реалізують методи ухилення, що обговорюються у статті. Багато сканерів веб-вразливостей, таких як Nikto, Whker та Sandcat, також включають методи обходу IDS.

Більшість IDS були модифіковані для виявлення або навіть скасування основних методів ухилення, але ухилення від IDS (і протидія ухилення від IDS) все ще є активним полем.

Заплутування коду

Від IDS можна обійти шляхом обфускації або кодування корисного навантаження таким чином, щоб цільовий комп'ютер розгорнув назад, а IDS - ні. Таким чином, зловмисник може використати кінцевий хост без попередження IDS.

Кодування та шифрування

Протоколи прикладного рівня, такі як HTTP, допускають кілька кодувань даних, які інтерпретуються як те саме значення. Наприклад, рядок «cgi-bin» в URL може бути закодований як «% 63% 67% 69% 2d% 62% 69% 6e» (тобто у шістнадцятковому форматі). Веб-сервер розглядатиме їх як один і той же рядок і діятиме відповідно до них. IDS повинна знати всі можливі кодування, які приймають її кінцеві вузли, щоб зіставити мережевий трафік із відомими шкідливими сигнатурами.

Атаки на зашифровані протоколи, такі як HTTPS , не можуть бути прочитані IDS, якщо IDS не має копії закритого ключа, використовуваного сервером для шифрування зв'язку. IDS не зможе порівняти зашифрований трафік із підписами, якщо це не буде враховано.

Поліморфізм

IDS на основі сигнатур часто шукають загальні шаблони атак, щоб порівняти шкідливий трафік із сигнатурами. Щоб виявити атаки переповнення буфера, IDS може шукати докази слайдів NOP, які використовуються для ослаблення захисту рандомізації макету адресного простору [11].

Щоб приховати свої атаки зловмисники можуть використовувати поліморфний шелл-код для створення унікальних шаблонів атак. Цей метод зазвичай включає кодування корисного навантаження будь-яким чином (наприклад, операцію XOR для кожного байта з 0x95), а потім розміщення декодера перед корисним навантаженням перед її відправкою. Коли ціль виконує код, вона запускає декодер, який перезаписує корисне навантаження у вихідну форму, яку потім виконує ціль.

Поліморфні атаки не мають єдиної сигнатури, що робить їх дуже складними для заснованих на сигнатурі IDS, і навіть IDS на основі аномалій, для виявлення. Shikata ga nai («нічого не поробиш») - популярний поліморфний кодувальник у структурі Metasploit, який використовується для перетворення шкідливих шелл-коду у складний для виявлення поліморфний шелл-код з використанням адитивного зворотного зв'язку XOR.

Вставка та ухилення

Зловмисники можуть ухилятися від IDS, створюючи пакети таким чином, що кінцевий хост інтерпретує ці атаки правильно, в той час як IDS або неправильно інтерпретує атаку, або визначає, що трафік є безпечним надто швидко.

Фрагментація та невеликі пакети

Один з основних методів - розділити корисне навантаження атаки на кілька невеликих пакетів, тому IDS повинна повторно зібрати потік пакетів для виявлення атаки. Простий спосіб поділу пакетів - їх фрагментування, але зловмисник може також створювати пакети з невеликими корисними даними. Інструмент ухилення від "усів" називає створення пакетів з невеликим корисним навантаженням "з'єднанням сеансів".

Саме по собі невеликі пакети не обходитимуть IDS, які повторно збирають потоки пакетів. Однак невеликі пакети можуть бути додатково змінені, щоб ускладнити повторне складання та виявлення. Один із способів ухилення - зробити паузу між відправкою частин атаки в надії, що IDS закінчиться за тайм-аутом раніше, ніж це зробить цільовий комп'ютер. Другий метод ухилення полягає в тому, щоб відправляти пакети не по порядку, що збиває з пантелику прості збирачі пакетів, але не цільовий комп'ютер.

Фрагменти, що перекриваються, і сегменти TCP

Інший спосіб ухилення - це створення серії пакетів з порядковими номерами TCP, налаштованими на перекриття. Наприклад, перший пакет включатиме 80 байтів корисного навантаження, але порядковий номер другого пакета буде 76 байтів після початку першого пакета. Коли цільовий комп'ютер повторно збирає потік TCP, він повинен вирішити, як обробляти чотири байти, що перекриваються. Деякі операційні системи будуть використовувати старі дані, деякі - нові дані. Якщо IDS не збирає TCP таким же чином, як ціль, нею можна маніпулювати, щоб або пропустити частину корисного навантаження атаки, або побачити безпечні дані, вставлені в шкідливе корисне навантаження, порушивши сигнатуру атаки. Цей метод також можна використовувати із фрагментацією IP аналогічним чином.

Невизначеність протоколу

Деякі методи обходу IDS включають навмисне маніпулювання протоколами TCP або IP таким чином, щоб цільовий комп'ютер обробляв інакше, ніж IDS. Наприклад, покажчик терміновості TCP по-різному обробляється у різних операційних системах. Якщо IDS не обробляє ці порушення протоколу відповідно до своїх кінцевих хостів, вона вразлива для методів вставки та обходу, аналогічних згаданим раніше.

Атаки з низькою пропускною здатністю

Атаки які розподілені за тривалим періодом часу або з великою кількістю вихідних IP-адрес, такі як повільне сканування nmap може бути важко виділити на тлі легкого трафіку. Онлайн-програма для злому паролів

Що перевіряє один пароль для кожного користувача кожен день, буде виглядати майже так само, як звичайний користувач, який неправильно ввів свій пароль.

Відмова в обслуговуванні

Через те, що пасивні IDS за своєю суттю (на відміну від), запускають атаку відмови в обслуговуванні проти IDS в мережі, це реальний спосіб обійти його захист. Зловмисник може досягти цього, використовуючи помилку в IDS, споживаючи всі обчислювальні ресурси IDS або навмисно ініціюючи велику кількість попереджень, щоб замаскувати фактичну атаку.

Перевантаження ЦП

Пакети, захоплені IDS, зберігаються в буфері ядра, доки ЦП не буде готовий їх обробити. Якщо ЦП перебуває під високим навантаженням, він може обробляти пакети досить швидко, і це буфер заповнюється. Нові (і, можливо, шкідливі) пакети відкидаються, оскільки буфер заповнений.

Зловмисник може вичерпати ресурси ЦП IDS декількома способами. Наприклад, системи виявлення вторгнень на основі сигнатур використовують алгоритми зіставлення із зразком для зіставлення вхідних пакетів із сигнатурами відомих атак. Природно, зіставлення деяких сигнатур потребує більших обчислювальних витрат, ніж інші. Скориставшись цим фактом, зловмисник може відправляти спеціально створений мережевий трафік, щоб змусити IDS використовувати максимальну кількість процесорного часу, наскільки це можливо, для виконання свого алгоритму зіставлення зі зразком для трафіку. Ця атака з алгоритмічною складністю може перевантажити IDS із відносно невеликою смугою пропускання.

IDS, яка також відстежує зашифрований трафік, може витрачати більшу частину ресурсів свого процесора на розшифровку вхідних даних.

Вичерпання пам'яті

Щоб відповідати певним сигнатурам, IDS потрібно підтримувати стан , пов'язаний зі з'єднаннями, які вона відстежує. Наприклад, IDS повинен підтримувати «керуючі блоки TCP» (TCB), блоки пам'яті, які відстежують інформацію, таку як порядкові номери, розміри вікон та стану з'єднання (ESTABLISHED, RELATED, CLOSED тощо) Для кожного TCP-з'єднання , контрольований IDS. Коли вся оперативна пам'ять (RAM) IDS витрачена, вона змушена використовувати віртуальну пам'ять на жорсткому диску, що набагато повільніше, ніж RAM. що призводить до проблем з продуктивністю та відкидання пакетів, аналогічних ефектам виснаження ЦП.

Якщо IDS не є збирачем сміття TCB правильно і ефективно, зловмисник може вичерпати пам'ять IDS, запустивши велику кількість TCP-з'єднань дуже швидко. Подібні атаки можуть бути виконані шляхом фрагментації великої кількості пакетів на більшу кількість менших пакетів або надсилання великої кількості невпорядкованих сегментів TCP.

Втома оператора

Згенеровані попередження IDS повинні діяти, щоб вони мали будь-яку цінність. Зловмисник може знизити доступність IDS, придушивши оператора-людини надмірною кількістю попереджень, посилаючи великі обсяги шкідливого трафіку, призначеного для генерації попереджень в IDS. Потім зловмисник може виконати справжню атаку, використовуючи звуковий сигнал як прикриття. Для цього були створені інструменти «палиця» та «соплі». Вони генерують велику кількість попереджень IDS, відправляючи сигнатури атак по мережі, але не запускають попередження в IDS, які підтримують контекст протоколу програми [4].

Висновки за розділом 2

IDS піддається багатьом типам атак, оскільки в кожному типі атаки є багато підкласів. Зростає ідея IDS на основі машинного навчання, де IDS може самостійно навчитися класифікувати різні атаки. Ось чому потенціал створення GAN для протидії IDS настільки великий: GAN створений, щоб обдурити системи машинного навчання. Це виявиться чудовим активом у тестуванні надійності IDS і може привести систему безпеки до нової ери, піднявши IDS на новий рівень.

IDS допомагає контролювати мережу. Але вони не блокують і не вирішують всі проблеми. Їм не вдається виявити нове підозрюване вторгнення, оскільки нове шкідливе програмне забезпечення не відображає шаблон попередньої незвичайної поведінки.

Були розглянуті основні способи обходу СВВ, отже з’явилася можливість побудувати метод, завдяки якому ми зможемо краще для себе зрозуміти, яку саме системи виявлення вторгнень обрати.

РОЗДІЛ 3

РЕКОМЕНДАЦІЇ ЩОДО ВИБОРУ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

3.1 Аналіз важливих факторів при виборі рішення IDS або IPS

Вибір, розміщення та обслуговування систем виявлення вторгнень (IDS) ґрунтуються на вимогах та поточній інфраструктурі компанії. Один продукт може добре працювати для однієї компанії і вийти з ладу для наступної. Вибір, як правило, є найскладнішим рішенням, оскільки продукти повинні відповідати вимогам бізнесу, правильно функціонувати в межах передбаченої мережевої інфраструктури та підтримуватися поточним персоналом.

Організації можуть вибирати з різноманітних недорогих і потужних рішень IDS та IPS, які відповідають різноманітним потребам – від стартапів із обмеженим бюджетом до глобальних підприємств. Деякі з них будуть окремими рішеннями, а інші будуть функціями, доданими до інших продуктів безпеки.

Важливі фактори при виборі рішення IDS або IPS:

IDS чи IPS? На основі хоста чи мережі? Автономний чи інтегрований? Вибір того, що використовувати, має ґрунтуватися на унікальних потребах та ресурсах організації. Бюджет, кадри, IT-середовище, толерантність до ризиків і бізнес-стратегії – все це відіграє певну роль у визначенні того, яке рішення найкраще підходить.

Також важливо мати на увазі, що параметри системи запобігання вторгненню не завжди є вибором «або/або». Для досягнення комплексного виявлення та запобігання загрозам може знадобитися розгортання як хостової, так і мережевої системи виявлення та запобігання вторгненням або запуск кількох систем IDS на рівні мережі, щоб скористатися перевагами їхніх різних переваг.

Іншим важливим фактором є здатність організації впоратися з результатами рішення. Системи IDS можуть бути дуже недорогими, оскільки вони звільняють тягар реагування на попередження на людський талант у команді безпеки.

Рішення IPS можуть поглинути частину цього тягаря, оскільки багато типів сповіщень можна просто автоматично обробляти інструментом. Однак групам із IT-безпеки все одно доведеться досліджувати та скасувати потенційні помилкові спрацьовування, а також досліджувати сповіщення про аномалії, які не призвели до автоматизованих дій.

Деякі рішення будуть вузькоспеціалізованими для певних цілей, таких як бездротові мережі. Інші інструменти будуть хмарними та намагатимуться охопити середовища корпоративного рівня, що складаються з кількох мереж, хмарних ресурсів тощо. «Правильний» IDS або IPS буде тим, що відповідає вашим потребам у сфері IT та безпеки прямо зараз і в найближчому майбутньому.

У практичному сенсі багато інструментів поєднують функції як IDS, так і IPS з деякими, які називають себе рішеннями IDPS (IDS та IPS) або інструментами наступного покоління IPS (NGIPS). Оскільки інструменти стають все більш складними, ми також повинні подумати, чи потрібні нашій організації сторонні експерти, щоб правильно встановити та налаштувати ці пристрої для нашого середовища.

3.2 Рекомендації щодо оцінки системи виявлення вторгнень

Оскільки ми працюємо над багатошаровими стратегіями кіберзахисту, а розмова переходить до систем моніторингу мережі та виявлення вторгнень (IDS), існує тенденція розглядати ці інструменти як частину застарілого посібника. Це має сенс, IDS є одним з найбільш зрілих інструментів в арсеналі, тим не менш, він залишається важливим будівельним блоком для поглибленої оборони, а сучасний підхід до технології IDS може принести більшу цінність, ніж будь-коли раніше.

Існує багато міркувань щодо вибору IDS, отже, було б корисно перерахувати кілька найбільш застосовних для широкої спільноти. Ось чотири важливі міркування щодо вибору IDS:

1) Автономна IDS проти вбудованої системи;

Багато брандмауерів та маршрутизаторів постачаються з певною формою IDS із коробки з ліцензією на програмне забезпечення, яку можна активувати. Для організацій з обмеженим технічним досвідом це може бути достатнім рішенням, яке пропонує додатковий захист.

Однак поєднання цих граничних пристроїв накладає навантаження на ці численні функції на одну частину апаратного забезпечення, яке може не масштабуватися так ефективно, як спеціально створені пристрої. Крім того, системи IDS, вбудовані в брандмауер, є частиною типової жорсткої оболонки зі стратегією м'якого липкого центру. Якщо зловмисне програмне забезпечення проскакує в фішинговому електронному листі або флеш-накопичувачі, IDS на периметрі більше не допоможе.

Після того, як противник вийшов за межі брандмауера, ми не можемо розраховувати на вихідний командний і контрольний трафік, який видасть свою позицію. Сучасні загрози-вимагачі не потребують допомоги, щоб поширюватися по всій мережі, і дуже важливо стежити за трафіком між тими системами, які мають найбільше значення.

Автономний IDS може розташовуватися у внутрішній мережі як частина багатошарового захисту, забезпечуючи видимість всередині підприємства навколо пріоритетних активів, де зараз, ймовірно, відбудеться боротьба. Його можна налаштувати з більшим ступенем витонченості та деталізації. З розділеними мережами можна ввімкнути запобігання чи блокування, щоб захистити конфіденційні дані, не заважаючи законному мережевому трафіку.

2) З відкритим кодом проти закритого;

Як відкрите програмне забезпечення, так і власницьке програмне забезпечення мають сильні та слабкі сторони. Власне програмне забезпечення, як правило, має достатньо ресурсів, і ці постачальники прагнуть своєчасно публікувати оновлення. Це зазвичай коштує значних бюджетних витрат, але забезпечує підтримку на рівні підприємства та когось, до кого можна звернутися, якщо справи підуть на перекосяк.

Традиційний кейс для програмного забезпечення з відкритим вихідним кодом є нижчим, оскільки воно не має ліцензійних зборів. Всупереч поширеній думці, ці інструменти також добре підтримуються.

У багатьох випадках «наукових проектів» із відкритим кодом проблема полягає в тому, що їх важко масштабувати, оскільки часто мало вбудованої підтримки для розгортань на рівні підприємства; важко керувати, коли політика змінюється від однієї частини організації до іншої; і неможливо підтримувати, коли розробник з відкритим кодом йде, щоб переслідувати інші інтереси.

Існують також гібридні підходи до цих двох моделей. Запатентовані рішення, створені на основі проектів і спільнот із відкритим кодом. Ці гібридні об'єкти прагнуть об'єднати найкраще з обох світів – добре оснащені, масштабовані та підтримувані продукти, підтримані цілим відкритим вихідним кодом спільноти користувачів і розробників. У разі успіху ці гібридні рішення можуть принести величезну цінність при значному зниженні вартості.

3) Підвищення цінності через інтеграцію;

Занадто багато підприємств мають багато інструментів, які не взаємодіють один з одним. Наприклад, опитування галузевих аналітиків показало, що більшість компаній, що надають фінансові послуги, мають 25 або більше , а деякі мають більше 100.

IDS наступного покоління має легко інтегруватися з наявними інструментами в портфелі безпеки для підтримки конкретних робочих процесів, які потрібні організації.

Однієї інтеграції недостатньо, оскільки лише те, що інструмент може передавати дані, не робить ці дані цінними. Наприклад, передача сповіщень IDS разом із будь-яким іншим пристроєм генерування журналів у мережі до інструменту керування інформацією та подіями безпеки (SIEM) і сподіваючись, що він чарівним чином виплесне інформацію, є хибним підходом. Якщо дані не підтримують жодного із запитань, які ставить програма безпеки, то вони просто створюють шум і накладні витрати для тих, хто повинен їх просіяти.

4) Тільки після підписів;

Традиційно IDS базується на сигнатурах і, хоча ефективний у визначенні раніше спостережуваних загроз, мало попереджає про ті загрози, які раніше не були помічені. Щоб подолати цю прогалину, індустрія безпеки досягла певних успіхів у розробці методик поведінкової аналітики та аналітики великих даних для виявлення аномальних і потенційно шкідливих мережевих активностей, а також для попередження захисників про загрози до того, як вони вкоренилися або поширилися. через середовище.

Сучасний підхід до IDS використовуватиме ці покращені аналітичні механізми для надання контексту журналам і попередженням, створеним рішенням. У разі атаки цей контекст має вирішальне значення для швидкого вжиття заходів і надання захисникам мережі інструментів, необхідних для швидкого стримування та усунення загроз. У руках досвідчених мисливців за загрозами та служб реагування на інциденти це може означати різницю між добре стриманим інцидентом або неконтрольованим порушенням.

3.3 Порівняння провідних рішення IDS та IPS

AIDE

Advanced Intrusion Detection Environment (AIDE) — це система виявлення вторгнень з відкритим вихідним кодом (HIDS) для Unix, Linux і Mac OS. Цей спеціалізований інструмент зосереджений на дуже важливій ніші перевірки цілісності файлів, але не пропонує ширшого виявлення шкідливих програм або атак [12].

Плюси:

- відкрите джерело;
- працює на системах MacOS і *nix;
- перевіряє цілісність файлів;
- може націлюватися на певні каталоги для моніторингу або виключати певні файли;
- інтегрується з іншими інструментами.

Мінуси:

- необхідно отримати від комерційного постачальника (наприклад, Red Hat) або через консультанта для підтримки;
- менш часті оновлення;
- дуже специфічна ніша (цілісність файлу) не виявляє багатьох типів атак;
- захищає лише той пристрій, на якому він встановлений.

BluVector

Удосконалене рішення BluVector для виявлення загроз, яке раніше відоме як Cortex, а тепер належить Comcast, використовує штучний інтелект (ШІ) як доповнення до існуючого стека безпеки. ШІ виявляє без файлове зловмисне програмне забезпечення та загрози нульового дня і розроблено, щоб ставати потужнішим, чим довше він знаходиться в середовищі [10].

Плюси:

- on premise;
- створено на основі надійних технологій Suricata і Zeek;
- інтегрується з іншими інструментами;
- відкрита платформа – дані легко доступні;
- бере дані з кількох каналів Intel і пісочниць;
- запатентований алгоритм машинного навчання розширює можливості;
- широке покриття MITER ATT&CK, не використовує технологію підпису;
- вбудований помічник налаштування для легкого зменшення помилкових спрацьовувань.

Мінуси:

- потрібні локальні ресурси, не створені для підтримки хмари;
- відсутність опублікованої вартості ліцензії ускладнює порівняння з іншими рішеннями.

Check Point Quantum IPS

Check Point вбудовує свій Quantum IPS у свої рішення брандмауера наступного покоління (NGFW) для сканування пакетів, що проходять через

пристрій. Цей пристрій може замінити безліч інших пристроїв (брандмауери, VPN тощо) і забезпечує функціональність як IDS, так і IPS [13].

Плюси:

- інтегрована продуктивність IPS до 15 Гбіт/с;
- детальні та настроювані звіти;
- виявлення вразливостей для HTTP, POP, IMAP, SMTP тощо;
- політики можна налаштувати за постачальником, продуктом, протоколом, типом файлу та роком загрози;
- оновлення кожні дві години через шлюз безпеки;
- вбудований антивірус, анти-бот і пісочниця;
- блокує тунелювання DNS, атаки без сигнатур, відомі CVE;
- використовує як сигнатуру, так і виявлення аномалій.

Мінуси:

- продається лише як обладнання (безпечний шлюз);
- немає підтримки сторонніх (хмарних, віддалених) ресурсів, які не перенаправлені через шлюз;
- внутрішній мережевий трафік має маршрутизуватися через шлюз для захисту.

Cisco NGIPS

Cisco продає свій продукт Secure IPS як систему запобігання вторгненню наступного покоління (NGIPS) з понад 35 000 вбудованих правил IPS і широкими можливостями для виявлення та блокування аномального трафіку. Захищений IPS може бути інтегрований з іншими пристроями Cisco або розгорнутий як автономний IPS [14].

Плюси:

- можна розгорнути як апаратне забезпечення або у віртуальній машині;
- виявлення безфайлових загроз;
- вбудований аналіз безпеки DNS, IP та URL-адрес;
- аналіз загроз і оцінка;

- пісочниця файлів;
- інтегрує Snort 3.0;
- використовує сигнатуру та виявлення аномалій.

Мінуси:

- деякі клієнти скаржаться на те, що інтерфейс може бути більш зручним;
- для розшифрування SSL потрібно багато пам’яті та потужності ЦП;
- ціна залежить від типу продукту, кількості ліцензованих років та рівня підтримки;
- більш дороге рішення.

Fail2Ban

Fail2Ban — це IPS з відкритим вихідним кодом, призначений для виявлення підозрілих або шкідливих IP-адрес і реагування на них на основі моніторингу файлів журналів. Аналітики можуть поєднувати «фільтри» (правила виявлення) з автоматичними діями по виправленню, щоб сформувати «в’язницю» [15].

Плюси:

- відкритий вихідний код і доступний безкоштовно;
- працює на системах *nix та MacOS;
- аналіз файлу журналу для виявлення підозрілих подій (наприклад, повторні невдалі спроби входу);
- автоматичне блокування підозрілих/шкідливих IP-адрес;
- ефективний проти атак грубої сили та відмови в обслуговуванні (DoS);
- заблоковані IP-таблиці можна передавати на брандмауери та інші пристрої безпеки.

Мінуси:

- фокусується на повторюваних шкідливих діях з однієї IP-адреси (може пропустити DDoS-атаки);
- занадто жорстка політика може заборонити легальних користувачів;
- немає платної підтримки;
- немає зручного графічного інтерфейсу користувача;

- блокує лише IP-адреси, не виявляє та не блокує інші типи атак.

Fidelis Network

Продукт Network IPS від Fidelis Cybersecurity аналізує мережевий трафік для обчислення ризику всіх активів і зв’язку в мережі. Інструмент інтегрується з іншими інструментами Fidelis, які захищають інші активи, такі як кінцеві точки, хмарні програми та контейнери [16].

Плюси:

- використовує базу знань MITER ATT&CK для виявлення загроз і реагування на них;
- може розшифровувати та аналізувати зашифрований мережевий трафік;
- підтримує хмару та локальну мережу;
- відстежує тіньове розгортання IT;
- інтегрується з іншими рішеннями безпеки;
- частина розширеного рішення для виявлення та реагування (XDR);
- пропонує можливості пісочниці;
- визначає захоплення облікового запису, інсайдерську загрозу та хакерську діяльність;
- вбудований сканер OCR для сканування зображень і вкладень PDF для електронних листів;
- цілодобова глобальна підтримка по телефону та в інтернеті;
- 15-денна безкоштовна пробна версія.

Мінуси:

- складні вимоги до конфігурації;
- більш дороге рішення [17].

Hillstone Networks

Hillstone Networks пропонує високошвидкісні спеціалізовані пристрої для мережевих IPS і брандмауерів наступного покоління. Починаючи з 2006 року, обладнання Hillstone IPS було встановлено понад 20 000 клієнтів і пропонує цілий ряд приладів для задоволення різноманітних потреб [18].

Плюси:

- 13 000 вбудованих підписів, користувацькі підписи та виявлення аномалій;
- можливості пісочниці для розслідування;
- можливості виявлення від рівня 3 до рівня 7;
- програма обізнана;
- опції захисту від спаму та блокування URL-адрес;
- хмарне управління розподіленими пристроями.

Мінуси:

- пропозиції лише для техніки;
- приладу потрібно буде оновити, щоб пристосуватись до зростання;
- більш дороге рішення.

Kismet

Рішення Kismet з відкритим вихідним кодом перевіряє бездротовий трафік і може діяти як інструмент керування або бездротовий інструмент IDS. Kismet працює з більшістю карт Wi-Fi, пристроями Bluetooth та іншим обладнанням [19].

Плюси:

- безкоштовне рішення з відкритим кодом;
- спеціаліст з бездротових мереж та пристроїв;
- підтримує Linux, OSX і Windows 10 (обмежено);
- викриває несанкціоновані точки доступу;
- розширена підтримка плагінів для веб-інтерфейсу користувача та покращення функціональності.

Мінуси:

- може бути повільним для пошуку в мережах;
- обмежена підтримка Windows;
- обмежена підтримка клієнтів;
- нішеві пропозиції з обмеженими можливостями для виявлення або блокування інших атак;

NSFOCUS

NSFOCUS, що базується в Санта-Кларі та Пекіні, пропонує рішення IPS наступного покоління з пропускною здатністю до 20 Гбіт/с [20].

Плюси:

- варіанти відповіді включають: блокування, перехід, сповіщення, карантин і захоплення;
- захищає від веб-оболонки, XSS, ін’єкції SQL та шкідливих URL-адрес;
- 9000+ сигнатур загроз і розширене виявлення аномалій;
- категорії політик IPS і складних політик паролів;
- аналіз трафіку, управління пропускною здатністю та дані Netflow про вхідний та вихідний трафік;
- захищає від різноманітних розподілених атак DoS (DDoS);
- можна інтегрувати з каналами загроз.

Мінуси:

- не перевіряє SSL-пакети;
- відгуків не так багато;
- розгорнуто переважно в Азії [21].

OpenWIPS-NG

OpenWIPS-NG — це система запобігання бездротовим вторгненням з відкритим вихідним кодом, яка може виявляти та блокувати вторгнення в бездротову мережу на основі датчика. Датчик пересилає інформацію на сервер із механізмом аналізу, який виявляє шаблони вторгнення, щоб видавати попередження або вживати заходів [22].

Плюси:

- дуже гнучкий і безкоштовний інструмент;
- особливо зосереджено на бездротових мережах;
- легкий інтерфейс командного рядка.

Мінуси:

- працює тільки на Linux;

- кожна установка підтримує лише один датчик;
- не підходить для початківців або не підходить для потреб підприємства.

OSSEC

OSSEC означає безпеку на базі хостів з відкритим кодом (незважаючи на відсутність букви H в акронімі). OSSEC і більш надійне рішення OSSEC+ захищають хости, аналізуючи системні файли на наявність ознак зловмисної активності. Компанія Atomicorp випустила комерційну версію [23].

Плюси:

- з відкритим кодом і безкоштовно;
- моніторинг реєстру Windows;
- виявлення підвищення привілеїв MacOS;
- відстежує контрольні суми файлу журналу для виявлення несанкціонованого доступу;
- широко використовується – понад 500 000 щорічних завантажень.

Мінуси:

- обмежена підтримка Windows;
- крута крива навчання;
- захист орієнтований на системні файли і не захищає від інших типів атак [24].

Palo Alto Networks

Palo Alto Networks пропонує IPSдля великих компаній, які шукають підтримку з комерційним рішенням. Їхня мережа IPS починається від 9 509,50 доларів і може бути розгорнута як апаратне забезпечення, програмне забезпечення (віртуальні машини чи контейнери), як хмарна служба або інтегрована в брандмауери наступного покоління [25].

Плюси:

- постійно оновлювані профілі захисту від загроз;
- блокує шкідливі сайти;
- кілька захисних пізній, що поєднують характерний та аномальний аналіз;

- блокує неправильно сформовані пакети, повторну збірку TCP, дефрагментацію IP і атаки C2;
- може застосовувати правила Snort і Suricata;
- хмарний варіант;
- інтегрує захист від уразливостей, виявлення шкідливих програм і шпигунських програм;
- може сканувати зашифрований трафік.

Мінуси:

- більш дорогий варіант;
- відсутність видимості деталей аналізу файлів;
- користувачі скаржаться на те, що деякі конфігурації мають занадто складні етапи реалізації;
- деякі користувачі скаржаться на рівень підтримки.

Sagan

Sagan — це IPS з відкритим кодом на базі хоста, який зосереджений на аналізі журналів. Незвичайним аспектом програмного забезпечення є те, що, хоча його можна встановити лише на Unix, Linux або MacOS, воно може приймати дані журналу з Windows або з мережевих інструментів IDS, таких як Snort. Sagan також інтегрується з брандмауерами, щоб блокувати IP-адреси від виявлених зовнішніх зловмисників [26].

Плюси:

- з відкритим кодом і безкоштовно;
- сумісний з Snort, Snorby, BASE та іншими;
- може завантажувати файли журналів з Windows, Zeek і Suicata;
- кілька сторонніх інтеграцій;
- легка, високопродуктивна, багатопотокова архітектура;
- аналіз журналу в режимі реального часу;
- функція IP-локатора, яка показує географічне розташування IP-адреси.

Мінуси:

- важко встановити та правильно налаштувати;
- крута крива навчання (багато функцій).

Samhain

Samhain Design Labs з Німеччини виробляє безкоштовне рішення IDS на базі хостів, яке можна запускати на багатьох хостах і використовувати для подачі в центральне сховище моніторингу. Samhain примітний тим, що він використовує стеганографію, щоб приховати свою присутність на хост-комп'ютері, що робить ймовірність того, що зловмисники не зможуть вимкнути його моніторинг [27].

Плюси:

- безкоштовно;
- працює в системах MacOS, Unix і Linux;
- шукає руткіт-віруси, шахрайські права доступу користувачів, приховані процеси;
- перевіряє цілісність журналу;
- легкий і може приховувати його присутність, щоб запобігти вимкненню зловмисниками.

Мінуси:

- автоматично не блокує та не усуває атаки;
- застарілий інтерфейс, складний у використанні;
- менша спільнота, ніж більш популярні інструменти з відкритим кодом;
- безкоштовна версія з відкритим кодом не підтримується;
- недоступно для Windows.

Security Onion

Security Onion — це Linux IDS, який може контролювати як хост, так і мережу. Рішення з відкритим вихідним кодом включає в себе аспекти Snort, Suricata, Zeek та інших популярних інструментів безпеки з відкритим кодом за панеллю візуалізації Kibana [28].

Плюси:

- дистрибутив Linux з відкритим кодом;

- інтегрує ряд популярних інструментів IDS;
- перевіряє файли журналу хосту та мережевий трафік;
- може виконувати живий аналіз мережевого трафіку та зберігати пакети у файлі;
- використовує аналіз сигнатур і аномалій.

Мінуси:

- багато автономних інструментів, що перекриваються;
- без автоматизації дій;
- деякі інтерфейси не є зручними для користувача.

Snort

Snort, мабуть, найвідоміший і найпопулярніший IPS. Його надзвичайно велика база прихильників привела до того, що його формати правил були прийняті як широко використовуваний стандарт, а багато інших інструментів IDS та IPS створено для сумісності з ним [29].

Плюси:

- з відкритим кодом і безкоштовно;
- встановлюється на Linux, Unix або MacOS, але підтримує аналіз Windows;
- велика бібліотека попередньо створених правил виявлення;
- сніфер, реєстратор пакетів, виявлення вторгнень;
- аналіз сигнатур і аномалій;
- глибока видимість мережевого трафіку;
- підтримується Cisco;
- базові правила можна завантажити, розширений доступ до нових правил доступний за окрему плату.

Мінуси:

- нестабільні оновлення;
- покладаючись на підтримку громади;
- дуже складний із стрімким навчанням.

SolarWinds SEM

SolarWinds Security Event Manager (SEM) — це платний інструмент аналізу IPS та журналів, створений на основі Snort і розроблений для корпоративних середовищ. Він доступний як послуга передплати від 2525 доларів США і вище, а довічні ліцензії доступні від 4485 доларів США [30].

Плюси:

- працює на Windows;
- підтримує файли журналів Windows, MacOS, Unix і Linux;
- збирає та аналізує дані мережі та хосту;
- інтегрується з Snort для аналізу мережі;
- понад 700 вбудованих правил для кореляції подій;
- контроль цілісності файлів;
- зручний інтерфейс;
- функції звітності про відповідність та криміналістичного аналізу;
- сповіщеннями можна керувати як правилами з настроюваними параметрами відповіді;
- може працювати як рішення для вторгнення в систему безпеки та керування подіями (SIEM).

Мінуси:

- функція щільна і потребує часу для навігації та встановлення;
- платне оновлення до безкоштовного інструменту;
- потрібні деякі оновлення вручну, а оновлення може бути складним.

Suricata

Suricata розроблена як альтернатива Snort. Він сумісний з форматами файлів Snort, правилами тощо, а також є безкоштовною опцією. Він включає в себе функції, недоступні в Snort, наприклад, аналіз мережевого трафіку на рівні програми (що дозволяє виявляти шкідливий вміст, поширений на кілька пакетів). Творець Zeek також пропонує пристрій, який поєднує в собі функції Suricata і Zeek [31].

Плюси:

- з відкритим кодом і безкоштовно;

- збір даних на прикладному рівні;
- може відстежувати кілька протоколів, таких як TLS, HTTP і SSL;
- глибока видимість мережевого трафіку;
- інтеграція з рядом сторонніх інструментів;
- підтримка сценаріїв Lua;
- зручний інтерфейс;
- паралельна обробка з підтримкою графічного процесора;
- використовує аналіз сигнатур і аномалій.

Мінуси:

- менша спільнота підтримки;
- вбудовані сценарії можуть бути складними у використанні;
- важкий процесор.

Trellix Network Security (McAfee + FireEye)

Деталі щодо продукту безпеки мережі Trellix можуть змінитися найближчим часом, оскільки платформа розширеного виявлення та реагування (XDR) компанії створюється на основі платформи безпеки мережі McAfee (NSP) і продуктів мережевої безпеки FireEye. У липні 2021 року відбулася серія злиття компаній, брендів і технологій, але оригінальні продукти все ще можна знайти на веб-сайтах окремих компаній [32].

Плюси:

- захист від ботів, розподіленої відмови в обслуговуванні (DDoS), програм-вимагачів та багатьох інших атак;
- блокує шкідливі сайти та завантаження;
- захищає хмарні та локальні пристрої;
- IPS FireEye було розгорнуто як частина рішення з безпеки мережі та криміналістичної експертизи;
- технологія FireEye зосереджена на виявленні аномалій, а McAfee — на виявленні сигнатур;
- запуск на фізичних або віртуальних пристроях;

- можливості пісочниці;
- виявляйте та блокуйте зловмисне програмне забезпечення, фішинг, експлойти, зворотні виклики команд і контролю (C2) і ботнети.

Мінуси:

- помилкові результати для виявлення шкідливих сайтів;
- негативно впливає на продуктивність мережі;
- ціни будуть незрозумілими, поки старі продукти не будуть припинені.

Trend Micro (IPS)

Рішення Trend Micros IPS доступне як фізичний або віртуальний пристрій для розгортання в локальних мережах, приватних або загальнодоступних хмарах [33].

Плюси:

- включає антивірусні сигнатури Trend Micro, а також машинне навчання;
- можливість пісочниці для розслідування;
- розгортається з правилами та політикою безпеки, щоб блокувати поточні та попередні загрози;
- використовує глибоку перевірку пакетів, аналіз шкідливих програм, репутацію URL-адрес і репутацію загроз;
- застосовує як аналіз сигнатур, так і аналіз аномалій;
- сканує вхідний, вихідний та бічний трафік.

Мінуси:

- поки що не інтегрується з іншими продуктами IPS або TrendMicro (DBI, IWSVA тощо);
- автоматичне застосування правил може порушити бізнес-процеси;
- більш дорогий варіант.

Vectra Cognito

Платформа Vectra Cognito IPS застосовує штучний інтелект для аналізу трафіку з джерел загальнодоступних хмар, програмного забезпечення як послуги (SaaS), ідентифікаційної інформації користувачів, мереж і EDR для виявлення та блокування зловмисних атак [34].

Плюси:

- надає результати у добре відомому форматі Zeek;
- інтегрується з різними засобами безпеки;
- витягуватиме дані з різних кінцевих точок ;
- пропонує потужну підтримку хмар і контейнерів (Kerberos);
- в основному використовується виявлення аномалій.

Мінуси:

- більш дорогий варіант;
- не має гнучкого географічного розташування для обробки даних;
- використовуйте власний формат журналу;
- може генерувати багато помилкових спрацьовувань, якщо неправильно налаштовано або неправильно налаштовано.

Zeek (AKA: Bro)

Zeek, раніше відомий як Bro, є надзвичайно потужним IDS, орієнтованим на мережу. Вбудована підтримка сценаріїв Zeek дає змогу налаштовувати та налаштовувати автоматичні відповіді на виявлені загрози.Творець Zeek пропонує попередньо запаковані фізичні або віртуальні пристрої Zeek як Corelight зі зручними графічними інтерфейсами, сценаріями та додатковою підтримкою [35].

Плюси:

- Zeek з відкритим кодом доступний безкоштовно;
- працює на системах MacOS і *nix;
- глибока видимість мережевого трафіку;
- інтегрована реєстрація трафіку;
- завдання забезпечують індивідуальну автоматизацію;
- відстежуйте трафік SNMP і відстежуйте активність FTP, DNS і HTTP;
- виконує аналіз на прикладному рівні для більш широкого аналізу;
- застосовує як сигнатуру, так і виявлення аномалій.

Мінуси:

- крута крива навчання вимагає глибоких знань SIEM та IDS;
- безкоштовна версія з відкритим кодом не підтримується;
- недоступно для Windows.

ZScalar Cloud IPS

IPS-рішення ZScalar фіксує весь трафік, незалежно від того, чи працює користувач на місці чи віддалено та підключається до локальних даних або хмарних ресурсів SaaS [36].

Плюси:

- підтримує всі типи ресурсів: локальні дані, хмарні дані, додатки SaaS;
- розширюване дозване рішення, яке зростає або зменшується за потреби;
- може розшифрувати SSL-трафік;
- необмежена ємність;
- немає обладнання для покупки чи програмного забезпечення для керування;
- групи безпеки можуть вивчити сповіщення IPS і отримати доступ до бібліотеки загроз Zscaler, щоб отримати докладнішу інформацію;
- підтримує iOS, macOS, Android, Windows, деякі Linux;
- підтримує мобільні пристрої.

Мінуси:

- пропонується лише як ліцензія SaaS;
- може підтримуватися не всі ОС;
- може додати затримку до продуктивності мережі;
- глобальна інсталяція та вирівнювання спеціального додатка можуть бути складними та тривалими.

Висновки за розділом 3

У даному розділі було запропоновано найважливіші фактори для вибору системи виявлення вторгнень, вони не можуть бути однаковими для всіх так як для

системи можуть використовуватися в різних компаніях, організаціях з різними сферами діяльності, бюджетом та масштабом.

Також були розроблені рекомендації оцінки систем виявлення вторгнень, так як в теперішній час їх є багато, тому я виділила чотири найважливіші, на мою думку, міркування щодо вибору IDS.

Було створено порівняльну характеристику різних рішень IDS та IPS, було визначено їх плюси та мінуси, застосування, що значно полегшить вибір системи.

ВИСНОВКИ

У роботі було проведено аналіз сучасних систем виявлення та запобігання вторгненням, їх класифікацію, та визначили що система виявлення вторгнень - це мережеві пристрої або програмне забезпечення, яке покращує безпеку комп'ютерних мереж, виявляючи атаки в режимі реального часу. Система виявлення вторгнень просто відстежує мережевий трафік і попереджає адміністратора мережі про будь-які незвичайні дії. IPS — це інструмент безпеки мережі, який постійно контролює мережу на наявність шкідливої діяльності та вживає заходів, щоб запобігти її, включаючи звітування, блокування або видалення, коли це сталося. Вона є більш досконалою, ніж IDS, яка просто виявляє зловмисну активність, але не може вжити заходів проти неї, крім попередження адміністратора.

Також дізналися що існує чотири основних типи IDS: система виявлення вторгнень в мережу (NIDS), система виявлення вторгнень на базі хоста (HIDS), система виявлення вторгнення по периметру (PIDS), система виявлення вторгнень на основі VM (VMIDS).

Також після дослідження особливостей атак за допомогою штучного інтелекту та інших класів атак, стало зрозуміло що є великий потенціал створення GAN для протидії IDS, він створений, щоб обдурити системи машинного навчання. Отже це стане хорошим тестуванням надійності IDS і підніме її на новий рівень.

Згодом визначення найбільш важливих факторів при виборі рішення IDS або IPS, дало розуміння що одного універсального засобу, який дозволив би захистити систему не існує і доводиться вже обирати програми моніторингу під конкретні потреби.

Проведений аналіз програмних засобів систем виявлення вторгнень за рахунок дослідження їх базових характеристик, таких як клас атак, адаптивність, методи виявлення атак, управління системою, масштабованість, рівень спостереження за системою, реакція на атаку, захищеність, підтримувана ОС та опис їх перевага і недоліків, а також розробка рекомендації щодо оцінки системи виявлення

вторгнень, дає можливість для розробників і користувачів обрати ефективний, найбільш вдалий та дієвий спосіб захисту інформації, яка циркулює в ІТС. Враховуючи це, власник ІТС має можливість обрати, відповідно до свого бюджету, необхідні механізми захисту системами виявлення та запобігання вторгненням.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sistemas de Detecção de Intrusão [Електронний ресурс]. – Режим доступу: https://www.gta.ufrj.br/grad/16_2/2016IDS/conceituacao.html

2. Studia i Materiały Informatyki Stosowanej, Tom 4, № 7, 2012 ст. 16-21, 166-170.

3. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему / В. В. Бєрковський, О. С. Безсонов // Системи управління, навігації та зв'язку. - 2017. - Вип. 3. - С. 57-62. - [Електронний ресурс] – Режим доступу: URL: http://nbuv.gov.ua/UJRN/suntz_2017_3_17

4. Maciej Szmit, Marek Gusta, Mariusz Tomaszewski 101 zabezpieczeń przed atakami w sieci komputero-wej, Helion 2005. – p. 497-524.

5. Системы выявления атак обретают второе дыхание - Журнал сетевых решений/LAN - Издательство «Открытые системы» [Електронний ресурс] – Режим доступа: URL: https://www.osp.ru/lan/2002/10/135318

6. Система обнаружения вторжений [Електронний ресурс]. - Режим доступу: URL: http://ru.wikipedia.org/wiki/Система_обнаружения_ вторжений

7. NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS).

8. Скабцов Н., Аудит безопасности информационных систем. — СПб.: Питер, 2018. — 252-256 с.

9. Яцків В.В., Драчук М. Ф., Боднар В.М, Система запобігання вторгнень на основі машинного навчання. – Тернопіль, 2019. – 1-2 с.

10. ЄРОХІН С. Д. Штучний інтелект для інформаційної безпеки. В:2020 Системи генерування та обробки сигналів у сфері бортового зв'язку.IEEE, 2020.с.1-4.

11. Spectrogram: A Mixture-of-Markov-Chains Model for Anomaly Detection in Web Traffic [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://academiccommons.columbia.edu/doi/10.7916/D8891G6G.

12. Сміт, Кеті Л. AIDE - Розширене середовище виявлення вторгнень . Тихоокеанська північно-західна національна лабораторія (PNNL), Річленд, штат Вашингтон (США), 2013.

13. Quantum Intrusion Prevention System (IPS) - Check Point Software [Електронний ресурс]. – Режим доступу: https://www.checkpoint.com/quantum/intrusion-prevention-system-ips/.

14. Cisco Secure IPS - Cisco [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/security/ngips/index.html

15. Fail2ban - Wikipedia [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Fail2ban.

16. Fidelis Network - Integrity Partners [Електронний ресурс]. – Режим доступу: https://integritypartners.pl/produkty/fidelis-network/.

17. Fidelis Network - NDR - Fidelis Cybersecurity [Електронний ресурс]. – Режим доступу: https://fidelissecurity.com/platforms/network/.

18. Innovative and Accessible Cybersecurity Solutions - Hillstone Networks [Електронний ресурс]. – Режим доступу: https://www.hillstonenet.com/.

19. Kismet - Kismet [Електронний ресурс]. – Режим доступу: https://www.kismetwireless.net/.

20. Home - NSFOCUS [Електронний ресурс]. – Режим доступу: https://nsfocusglobal.com/.

21. NSFOCUS On-Premises Defenses - SecureCraft Asia [Електронний ресурс]. – Режим доступу: https://www.securecraftasia.com/nsfocus-on-premises-defenses/.

22. Sharkfest ’12 - Wireshark Developer and User Conference [Електронний ресурс]. – Режим доступу: https://sharkfestus.wireshark.org/sharkfest.12/presentations/A-6_Open_WIPS-ng.pdf.

23. OSSEC - World's Most Widely Used Host Intrusion Detection System - HIDS [Електронний ресурс]. – Режим доступу: https://www.ossec.net/.

24. OSSEC – integralność systemów plików i danych – open Audit [Електронний ресурс]. – Режим доступу: https://www.open-audit.eu/ossec-integralnosc-systemow-i-danych/.

25. Palo Alto Networks - systemy NGFW, bezpieczeństwo endpoint, bezpieczeństwo chmury - CC Otwarte Systemy Komputerowe [Електронний ресурс]. – Режим доступу: https://www.cc.com.pl/pl/prods/paloaltonetworks/home.php.

26. Open Source - Quadrant Information Security [Електронний ресурс]. – Режим доступу: https://quadrantsec.com/sagan_log_analysis_engine/.

27. Samhain Labs - samhain [Електронний ресурс]. – Режим доступу: https://la-samhna.de/samhain/.

28. Security Onion Solutions [Електронний ресурс]. – Режим доступу: https://securityonionsolutions.com/.

29. Snort - Network Intrusion Detection & Prevention System [Електронний ресурс]. – Режим доступу: https://www.snort.org/.

30. Security Event Manager - View Event Logs Remotely | SolarWinds [Електронний ресурс]. – Режим доступу: https://www.solarwinds.com/security-event-manager.

31. Home - Suricata [Електронний ресурс]. – Режим доступу: https://suricata.io/.

32. Network Security - Trellix [Електронний ресурс]. – Режим доступу: https://www.trellix.com/en-us/platform/network-security.html.

33. Enterprise Intrusion Prevention (IPS) Software & Solutions - Trend Micro [Електронний ресурс]. – Режим доступу: https://www.trendmicro.com/en_us/business/products/network/intrusion-prevention.html

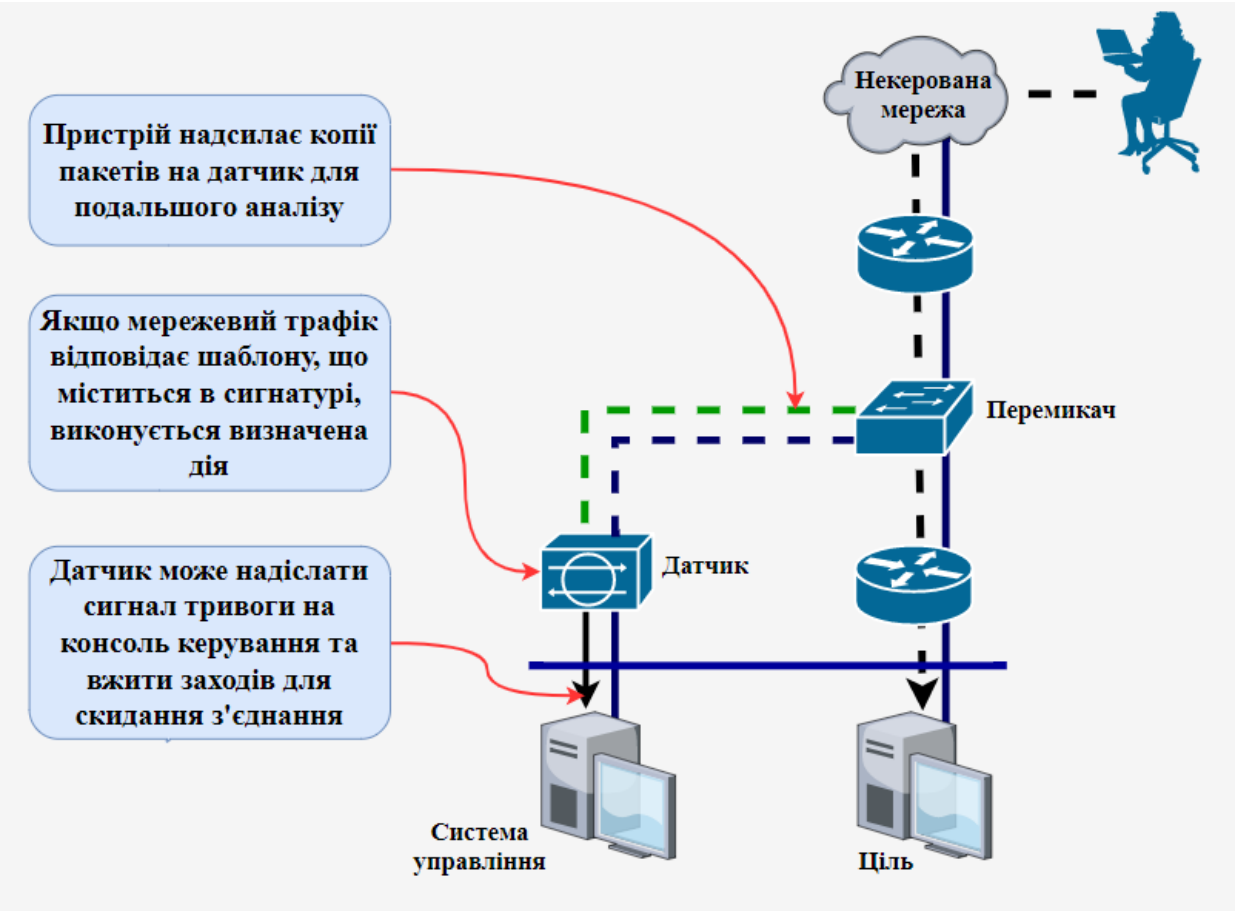
34. Network Threat Detection & Response Platform - Vectra AI [Електронний ресурс]. – Режим доступу: https://www.vectra.ai/products/platform.

35. The Zeek Network Security Monitor [Електронний ресурс]. – Режим доступу: https://zeek.org/.

36. Intrusion Prevention Service - Zscaler Cloud IPS [Електронний ресурс]. – Режим доступу: https://www.zscaler.com/technology/cloud-ips.

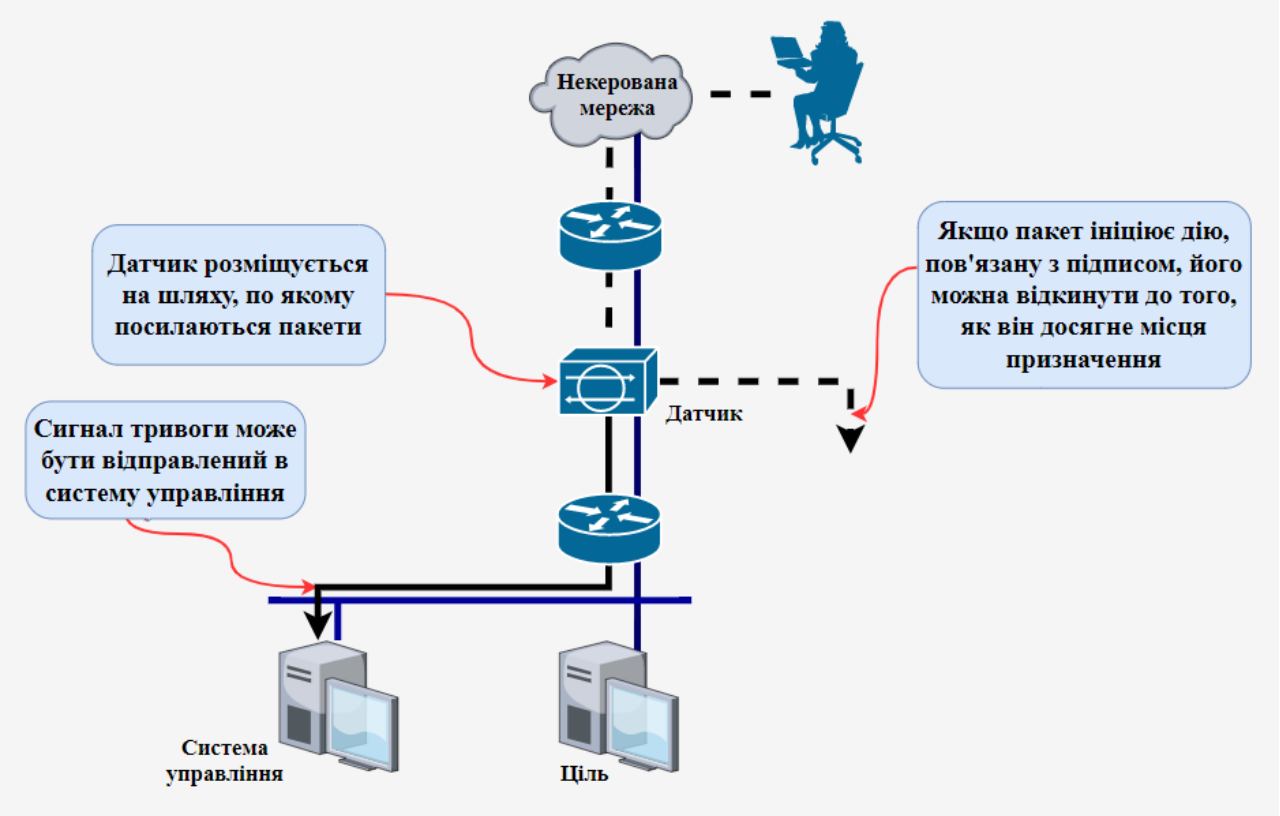
ДОДАТОК А

Архітектура типової IDS



ДОДАТОК Б

Архітектура типової IPS



ДОДАТОК В
ПОРІВНЯННЯ ПАРАМЕТРІВ IDS ТА IPS

Назва	IDS/IPS і хост/мережа	Підтримувані платформи	Виявлення	Ціна
AIDE	IDS, хост	Unix, Linux і Mac OS	Перевірка цілісності файлу (тільки)	Безкоштовно*
BluVector	IDS, мережа	Не визначено	Широке виявлення загроз	Недоступний
Check Point Quantum IPS	IDS, IPS, Мережа	Прилад	Широке виявлення загроз	1500 доларів США на рік
Cisco NGIPS	IPS, мережа	Прилад, VMware	Широке виявлення загроз	1280 доларів США на рік
Fail2Ban	IDS, IPS, хост	Unix, Linux і Mac OS	Виявляє потенційно шкідливі IP-адреси	Безкоштовно
Fidelis Network	IDS, IPS, Мережа	Не визначено	Широке виявлення загроз	$78 000+ на рік залежно від пропускної здатності ГБ та днів зберігання
Hillstone Networks	IDS, IPS, Мережа	Прилад	Широке виявлення загроз	Безстрокова ліцензія на основі користувачів і функціональності

Продовження табл.1.1

Kismet	IDS, мережа	Linux, OSX, Windows 10 (обмежено)	Тільки бездротові IDS	Безкоштовно
NSFOCUS	IDS, IPS, Мережа	Не визначено	Широке виявлення загроз	Недоступний
OpenWIPS-NG	IDS, IPS, Мережа	Linux	Бездротові мережі	Безкоштовно
OSSEC	IDS, IPS, хост	Unix, Linux, MacOS, Windows	Моніторинг системних файлів	безкоштовно*
Palo Alto Networks	IDS, IPS, Мережа	Прилад, Контейнер, ВМ	Широке виявлення загроз	$9 509,50+
Sagan	IDS, IPS, хост	Unix, Linux, MacOS	Аналіз лог-файлів, блокування IP	Безкоштовно
Samhain	IDS, хост	Linux, Unix, MacOS	Перевірка цілісності файлів, аналіз файлів журналу, виявлення руткітів	Безкоштовно
Security Onion	IDS, мережа, хост	Лише для Linux	Широке виявлення загроз	Безкоштовно*

Продовження табл.1.1

Snort	IDS, IPS, Мережа	Linux, Unix, MacOS	Широке виявлення загроз	Безкоштовно, $399+ за підписку на правила
SolarWinds SEM	IDS, IPS, Мережа, Хост	Windows, Linux, Unix, MacOS	Широке виявлення загроз	2525 доларів США+
Suricata	IDS, IPS, Мережа	Windows, Linux, Unix, MacOS	Широке виявлення загроз	Безкоштовно
Trellix (McAfee + FireEye)	IDS, IPS, Мережа	Прилад або програмне забезпечення	Широке виявлення загроз	10 995 доларів США+
Trend Micro	IDS, IPS, Мережа	Прилад або програмне забезпечення	Широке виявлення загроз	Недоступний
Vectra Cognito	IDS, IPS, Мережа, Хмара	Прилад або програмне забезпечення	Широке виявлення загроз	$10 000+, на основі IP-адрес
Zeek (AKA: Bro)	IDS, мережа	Windows, Linux, Unix, MacOS	Широке виявлення загроз	Безкоштовно*
ZScalar Cloud IPS	IDS, IPS, Мережа, Хмара	Windows, MacOS, деякі Linux, Android,	Широке виявлення загроз	Пропонує різні рівні: Бізнес, Трансформація,

		iOS		ELA

*Підтримка або попередньо завантажені пристрої доступні від сторонніх постачальників за окрему плату