НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
В.о. завідувача кафедри

_____ **Микола ГРАЙВОРОНСЬКИЙ**
(підпис)

«_____»_____2021 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною программою «Системи, технології та математичні методи кібербезпеки»
спеціальності: 125 «Кібербезпека»

на тему: Класифікація і таксономія аномалій в аспекті кібербезпеки і захисту інформації_____

_____

_____

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ___ФБ-73_____
(шифр групи)

_____Біла Ольга Павлівна _____ _____
(прізвище, ім'я, по батькові) (підпис)

Керівник _к.е.н. доцент кафедри ІБ Ткач Володимир Миколайович__ _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ - 2021 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Микола ГРАЙВОРОНСЬКИЙ
(підпис)
«___»_____2021 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Білої Ольги Павлівни
(прізвище, ім'я, по батькові)

1. Тема роботи Класифікація і таксономія аномалій в аспекті кібербезпеки і захисту інформації, керівник роботи Ткач Володимир Миколайович, к.е.н. доцент кафедри інформаційної безпеки, затверджені наказом по університету від « » _____ 2021 р. №

2. Термін подання здобувачем вищої освіти роботи 07 червня 2021 р.

3. Вихідні дані до роботи Попередні дослідження та інша література на тему класифікації аномалій в кіберпросторі.

4. Зміст роботи Огляд існуючих класифікацій аномалій, дослідження зв'язку аномалій із загрозами, огляд існуючих проблем побудови універсальних систем виявлення аномалій, проведення аналізу аномальної поведінки, використовуючи HTTP трафік, побудова власних схем класифікацій.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) Класифікація і таксономія аномалій в аспекті кібербезпеки і захисту інформації — презентація.

6. Дата видачі завдання 01.03.2021

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	01.03.2021	Виконано
2	Опрацювання літератури	10.03.2021	Виконано
3	Аналіз існуючої таксономії загроз	25.03.2021	Виконано
4	Побудова моделі зв’язку аномалій з загрозами	15.04.2021	Виконано
5	Аналіз аномальної поведінки системи, використовуючи HTTP трафік	30.04.2021	Виконано
6	Аналіз аномалій в розрізі методів IDS	10.05.2021	Виконано
7	Побудова схем класифікації	15.05.2021	Виконано
8	Оформлення графічної та текстової частини	25.05.2021	Виконано
9	Оформлення дипломного проекту	28.05.2021	Виконано

Здобувач вищої освіти _____ Ольга БІЛА
(підпис) (Власне ім’я, ПРІЗВИЩЕ)

Керівник роботи _____ Володимир ТКАЧ
(підпис) (Власне ім’я, ПРІЗВИЩЕ)

РЕФЕРАТ

Обсяг роботи 53 сторінки, 7 ілюстрацій, 3 таблиці, 30 джерел літератури.

Об’єктом дослідження стали аномалії та системи виявлення аномалій в кіберпросторі.

Предметом дослідження особливості виникнення аномалій в мережі, складності детектування аномальної поведінки, аналіз існуючої класифікації аномалій для побудови таксономії.

Метою даної роботи є складання класифікації аномалій з різних сторін, знаходження зв’язку аномалій з атаками, аналіз мережевих і немережевих аномалій, огляд аномалій з боку методів та технік їх детектування для побудови таксономії, яка буде корисною в наступних дослідженнях атак і конструювань IDS.

Подальше використання матеріалів дослідження планується у вивченні більш глибоко методів детектування аномалій для розробки систем, здатних виявляти окремі категорії аномалій, в розгляді технічної можливості реалізації IDS за наведеним концептуальним фреймворком для аналізу HTTP трафіку.

Результати роботи доповідалися на:

Інновації науки XXI століття, LXVI Міжнародна науково-практична інтернет-конференція – м. Дніпро, 17 травня 2021 року.

Ключові слова: аномалія, IDS, система виявлення аномалій, атака, набір даних, таксономія, загроза, машинне навчання, методи виявлення аномалій.

ABSTRACT

The volume of work 53 pages, 7 illustrations, 3 tables, 30 sources of literature.

The object of the study were anomalies and systems for detecting anomalies in cyberspace.

The subject of the study is the peculiarities of the occurrence of anomalies in the network, the complexity of detecting anomalous behavior, the analysis of the existing classification of anomalies in order to build a taxonomy.

The aim of this work is to classify anomalies from different angles, to find the connection of anomalies with attacks, analysis of network and non-network anomalies, review of anomalies by methods and techniques of their detection to build a taxonomy that will be useful in future studies of IDS constructions, dealing with specific types of attacks.

Further use of research materials is planned in the studying of deeper methods of detecting anomalies for the development of systems capable of detecting certain categories of anomalies; in considering the technical feasibility of implementing IDS according to the conceptual framework for HTTP traffic analysis.

The results were reported on:

Innovations of Science of the XXI Century, LXVI International Scientific and Practical Internet Conference - Dnipro, May 17, 2021.

Keywords: anomaly, IDS, anomaly detection system, attack, data set, taxonomy, threat, machine learning, anomaly detection methods.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IDS – Intrusion Detection System

HIDS – Host-Based Intrusion Detection System

NIDS - Network Intrusion Detection System

HTTP – The Hypertext Transfer Protocol

HTTPS – The Hypertext Transfer Protocol over SSL(Secure)

СВА – система виявлення аномалій

OSI Model – The Open Systems Interconnection model

DNS – Domain Name System

XSS – Cross-Site Scripting

R2L – Root to Local

U2R – User to Root

DoS – Denial of Service (attacks)

ML – Machine Learning

ВСТУП

Оскільки світ постійно розвивається і стає залежним від використання автоматизованих складних систем, безпека пристроїв, систем та мереж стає як ніколи необхідною. Як окремі користувачі, так і бізнеси стикаються з загрозами, кількість яких зростає щодня. Щоб якось призупинити і бути в змозі контролювати вплив загроз на систему, дослідники розробляють різні комплексні рішення щодо детектування аномалій. Проте існуючі рішення часто не спрацьовують при спробі адаптуватись до постійно-мінливої архітектури застосунків.

Згідно останнім тенденціям з'являються нові типі атак, так звані приховані атаки. В цьому випадку до цільового сервісу отримують доступ комп'ютери, що є підконтрольні атакуючому цілком правомірно та за допомогою ресурсоємних операцій завантажують канал (атака погіршення якості) або в певний момент «вибухають» беззмістовним трафіком, що ставить перед системами захисту нові нетривіальні задачі виявлення і протидії. Стає вже більше вживаним термін «кібернетичний тероризм», що містить загрозу для Інтернет інфраструктури певної держави. Оскільки єдиного комплексного методу захисту від атакуючої діяльності досі немає, питання надійності і захищеності мережі Інтернет стає більш загальним, ніж втрат доходів бізнесу, а стосується загроз національної безпеки.

Загалом, через еволюцію розвитку комп'ютерних мереж з кожним роком згідно The Global State of Information Security Survey помічається зростання числа інцидентів [1].

Розглядаючи ситуацію на теперішній час і беручи до уваги пандемію, що почалась 2020 року, згідно даним NETSCOUT Threat Intelligence кількість denial-of-service (DDoS) атак зросла на 20% за рік і за останні шість місяців 2020 року на 22% [2]. Отож, зараз адміністраторам мережі доводиться

поратись із великою кількістю спроб вторгнень як зі сторони окремих осіб, що мають зловмисні наміри, так само зі сторони потужних ботнетів. Для цього застосовується система спеціалізованих алгоритмів та методів для виявлення відомих та невідомих атак, а також методи знаходження аномальної активності.

Аномалія - відступ або ухилення від правила, тому аномальним називають все, що відступає або відрізняється від правильного або нормального [3].

Аномалії в більшості випадків є початковою стадією атак, тому існують цілі системи виявлення аномалій (СВА). СВА «знають», якою має бути нормальна поведінка контрольованої мережі, і реагують на відхилення від профілю нормальної активності. СВА використовують різноманітні підходи виявлення аномалій, але не існує загальноприйнятної методики

Основні підходи до виявлення аномалій діляться на дві широкі категорії: з участю людини (переважно на основі правил) та на основі машинного навчання (переважно без нагляду).

Приклад першого підходу: якщо кількість спроб авторизації перевищує порогове значення або передається більше порогового числа байтів протягом певного періоду – то така поведінка може вважатись аномальною. Тоді як правила сформульовані експертами з безпеки корисні, вони неефективні проти атаки нульового дня. Крім того, ці правила може бути важко підтримувати. З іншого боку, підходи на основі машинного навчання, розроблені із використанням величезної кількості даних, зібраних на сучасних підприємствах стали найкращим вибором для виявлення аномалій безпеки.

Загалом виявлення аномалій - це надважливе завдання аналізу даних, що має на меті дослідити нестандартні неочікувані дані з заданого набору даних.

Знайти аномалії непросто. Шаблони поведінки комплексної системи, які можна вважати «нормальними», різні в кожному домені, більшість із часом змінюються, і властиві їм варіації породжують шум, який часто може приховати фактичні аномалії. В більшості випадків аномалії - це не просто окремі точки даних, а вони виникають із кількох точок даних, що взаємодіють між собою. Отож, існує потреба класифікації та структуризації аномалій, досліджені їх відношення до атак. Наявність класифікації і таксономії може допомогти розробляти більш ефективні системи виявлення втручань для знаходження аномалій в системі, щоб запобігти реалізації атаки до того моменту, як вона встигне завдати значної шкоди системі.

1 КЛАСИФІКАЦІЯ АНОМАЛІЙ НА ОСНОВІ ЗВ'ЯЗКУ «АНОМАЛІЯ-ЗАГРОЗА»

1.1 Типи аномалій

Важливим аспектом виявлення аномалії є характер аномалії. Існують три типи аномалій, що з'являються не тільки в кіберпросторі, але й що стосується будь-якої системи [4].

- *point anomaly* – тип аномалії, коли певний екземпляр даних відрізняється від нормальної шаблонної поведінки. Наприклад, якщо користувач намагається отримати доступ до обмеженого серверу. До СВА, що стосуються point anomaly, відноситься значна частина методів, а саме: класифікації, кластеризації, статистичні, та ін.
- *contextual anomaly* – тип аномалії, коли екземпляр даних поводиться аномально у певному контексті. Кожний окремий екземпляр має розглядатись спираючись на наступні атрибути: *contextual* (визначає положення або позицію в загальному датасеті), *behavioral* (якщо подія не залежить від положення).

Подібний приклад можна знайти в домені виявлення шахрайства з кредитною карткою. Контекстним атрибутом у домені кредитної картки може бути час придбання. Припустимо, що людина зазвичай має щотижневий рахунок за покупки в 100 доларів, за винятком Різдвяного тиждень, коли вона досягне 1000 доларів. Якщо буде нова покупка в 1000 доларів за тиждень у липні це розглядається як контекстуальна аномалія, оскільки вона не відповідає нормальній поведінці людини в контексті часу [5].

- *collective anomalies* – тип аномалій, що принципово відрізняється від попередніх тим, що стосується групи екземплярів. Можливий такий випадок, коли окремо той, чи інший екземпляри не будуть мати

аномальну поведінку, а разом – поводитись аномально. Розглянемо наступну послідовність подій на хості:

smtp-mail, http-web, http-web, ftp, smtpmail, http-web, **ssh, buffer-overflow, ftp**, http-web, …

Виокремлені дії відносяться до відомої атаки віддаленою машиною з копіюванням даних з хосту на віддалений пункт призначення через ftp. Потрібно зазначити, що point anomaly та collective anomalies можуть бути перетворені на contextual anomaly шляхом включення контекстної інформації.

1.2 Огляд таксономії загроз

В рамках виділення зв'язку «атака - аномалія» важливо визначити класифікацію загроз, яка дозволить детальніше розібрати з різних сторін категорії атак, як вони поражають систему і завдають збитки організаціям. Представлена таксономія загроз буде мати класифікацію за наступними критеріями, використовуючи найбільш типові категорії та підкатегорії атак:

- OSI Model – по рівням

- тип загроз – активна або пасивна.

За типом загроз класифікація пояснюється детальніше таким чином [6]:

- Пасивна: атаки напрямлені на колекціонування або викрадення інформації через пасивне знаходження даних в процесі комунікації (target – source).
- Активна: атаки використовують спосіб спілкування для надсилання даних / запитів, що можуть завдати шкоди цільовій системі.

Однак деякі атаки не можна розглядати активні або пасивні, поки не стане відомо про їх використання. Приклад цього випадку - це SQL injection, якщо вона використовується для запиту даних із бази даних, то вона пасивна.

Проте, якщо вона використовується для зміни даних, видалення таблиць або зв’язків в таблиці, тоді атаку можна розглядати як активну.

Таксономія загроз [7]:

1. Application layer

- DoS/ DDoS: HTTP Flood (active)
  Amplification (active)
  Buffer overflow (active)
- Man-in-the-Middle: Man-in-the-browser (active / passive)
- Impersonate: Unauthorized access (active)
  Cloning (active)
- DNS: DNS Spoofing (active)
- Malware: Trojans (active)
  Worm (active)
  Virus (active)
  Adware (passive)
  Spyware (passive)
  Ransomware (active)
- Code injection: SQL-injection (active / passive)
  Cross Site Scripting (active / passive)
  Shellcode (active / passive)
- Fingerprinting (active)
- Misconfiguration (active)
- Drive-by Download (active)
- Masquerade (active)
- Phishing (active)
- L2R (active)
- U2R (active)
- Repudiation

- Fraud (active)
- Brute Force: SSH (active / passive)
  FTP (active / passive)

2. Presentation layer

- DoS/ DDoS: Flood: SSL (active)
- Man-in-the-middle: Monitor (passive)
  Replay (active)
- VLAN Hooping: Heartbleed (active / passive)
- Fake Certificate (active)

3. Session

- Session Hijacking (active)

4. Transport

- DoS / DDoS: Flood: Smurf (active)
  UDP Flood (active)
  SYN Flood (active)
- Packet Forging (active)
- nonTor traffic (active / passive)

5. Network

- DoS / DDoS: Flood: ICMP Flood (active)
  Protocol exploit: Teardrop (active)
  Malformed packets: Ping of Death (active)
- Impersonate: Spoofing: IP Spoofing (active)
- Scanning / Enumeration: TCP (passive)
  UDP (passive)
- Probing (passive)

6. Data Link

- Impersonate: Spoofing: ARP Spoofing (active)
- MAC Spoofing (passive)

- VLAN Hooping: Switch Spoofing (active)
  Double Tagging (active)

7. Physical

- Backdoor (active)
- Misconfiguration (active)
- Physical Damage (active)

Основна ціль побудови таксономії загроз – це допомога в побудові IDS, що можуть виявити якомога більше категорій атак, а саме використовуючи асоціацію загроз із OSI моделлю для досягнення вищої точності та зменшення кількості false positives спрацьовувань IDS та покращення датасетів, які використовують IDS.

1.3 Дослідження зв’язку аномалій з загрозами

У багатьох випадках аномалії та атаки здаються не пов’язаними, або, принаймні, аномалії можуть правомірно траплятись в доброякісному русі. Наприклад, в деяких випадках атаки переповнення буфера, які використовують погано написані програми, що використовують функції C, такі як gets () або strcpy (), щоб записати в буфер (масив символів фіксованого розміру) без перевірки довжини введення. Зазвичай атака міститиме довгий рядок, який переповнює буфер і перезаписує адресу зворотного зв'язку в стеку цільової машини. Коли виконувана функція повертається, вона переходить до адреси, наданої зловмисником, як правило, до рядка машинного коду, що постачається як частина тієї самої атакуючого рядка. Код виконується з рівнем привілеїв цілі (часто root), як правило, щоб відкрити shell або встановити backdoor. Очікується, що атака переповнення буферу буде генерувати аномалії у вигляді довгих рядків виконуваного коду, де зазвичай зустрічаються короткі рядки тексту. Однак може недоставати відповідних атрибутів для виявлення цього типу аномалій, тоді допомагає щось інше, що робить атаку стійкою.

Наприклад, використання рідко-вживаних або написаних із помилками ключових слів в ncftp і sendmail, коли більшість клієнтів використовують великі регістри.

Навіть коли аномалія пов'язана з атакою, можливо не отримати чіткої відповіді про деталі атаки і як вона реалізується. Наприклад, *portsweep* та *queso* – виявлені як ідентичні аномалії, проте мають різний зміст у собі. [8]

Особливості деяких популярних атак:

1. Denial of Service (DoS).

Це спроба завдати шкоди, зробивши недоступною цільову систему, наприклад веб-сайт або додаток, для звичайних кінцевих користувачів. Зазвичай зловмисник генерують велику кількість пакетів або запитів, які в результаті перенавантажують роботу цільової системи.

На сьогоднішній день існує досить багато різних видів атак на відмову, кожна з яких використовує певну особливість побудови мережі або вразливості програмного забезпечення. Наприклад, атаки можуть здійснюватися шляхом безпосередньої пересилки великої кількості пакетів (SYN, UDP, ICMP flood), використання проміжних вузлів (Smurf, Fraggle), передачі занадто довгих пакетів (Ping of Death), некоректних пакетів (Land) або великої кількості трудоємних запитів [9, 10].

У випадку DoS-атаки здійснюючи пересилку великої кількості пакетів (flooding) надсилання великої кількості запитів до веб-сервера є незвичною поведінкою, але надсилання одного запиту є законним. Отже, ми можемо розглянути DoS-атаку як collective anomaly. Як було зазначено в розділі 1.1, коли окремо той, чи інший екземпляри не будуть мати аномальну поведінку, а разом – поводитись аномально.

2. Probe

Протягом атаки здійснюється збір інформації про цільову мережу або окремі хости, загалом для розвідувальних цілей. Розвідувальні напади є частими способами збору інформації про типи та кількість підключених машин до мережі, що включає різні типи встановленого програмного забезпечення та / або додатків, які використовується на хості. Probe вважається першим кроком у фактичній атаці компрометації хоста або мережі. Хоча особливої шкоди probe не завдає, ця атака вважається серйозною загрозою для корпорацій. Це може надати корисну інформацію для зловмисників для запуску майбутньої руйнівної атаки.

Оскільки probe не завжди завдає шкоди, а скоріше має певний намір у розвідуванні інформації, атака probe відноситься до contextual anomaly.

3. User to Root (U2R)

В ході реалізації цієї атаки зловмисник прагне отримати незаконний доступ до акаунту адміністратора. Застосовуючи методи соціальної інженерії або відслідковування паролю різними способами, зловмисник може отримати доступ до звичайного облікового запису користувача, а потім скористатися деякою вразливістю, щоб отримати привілей суперкористувача.

(Більшість з U2R атак (що network-based IDS зазвичай пропускає) виявляються, оскільки зловмисник завантажує шкідливу програму за допомогою FTP серверу, який зазвичай використовується лише для завантажень) – user behavior

4. Remote to User (R2U or R2L)

Атака відбувається, коли зловмисник без певного рівню доступу користувача (адміністратора) отримує можливість виконувати код локально. Найчастіше зловмисник використовує метод спроб і помилок вгадати пароль за допомогою автоматизованих сценаріїв, brute force тощо. Є також деякі складні атаки, завдяки яким

зловмисник встановлює інструмент прослуховування для захоплення пароля перед проникненням у систему.

Метою U2R та R2L атак є маніпулювання або зловживання важливими ресурсами системи.

Для того, щоб відслідкувати закономірності та подібності в класах атак будемо розглядати наступні датасети: IX, KD, NK, UN.

Такі атаки к Shellcode або Exploit мають на меті пошкодити систему одиничними запитами чи діями: отже, очікується, що вони генерують *point* або *contextual* аномалії. Натомість атаки, які надсилають жертві кілька запитів, генерують окремі аномалії, що мають спільні характеристики, тобто *collective* аномалії. Розрізнення атак, що породжують точкові аномалії, або контекстні аномалії, не є тривіальним: зокрема, воно вимагає розуміння того, чи атаки діють лише у конкретних сценаріях (контексті), і як вони впливають на ціль (жертву) [11].

Більш детально, атаки Probing, Reconnaissance , та Analysis attacks (наприклад, PortScan) спрямовані на сканування системних інтерфейсів або мережевих пристроїв з метою визначення вразливостей. Ця діяльність містить в собі надсилання багатьох запитів ping або arp, які не з'являються під час нормальних умов роботи системи, створюючи колективні аномалії. Інші атаки, як Fuzzers та Bruteforce, спрямовані на подання даних системі, щоб або заблокувати її, або отримати несанкціонований доступ. Подібним чином у випадку DoS-атаки здійснюючи пересилку великої кількості пакетів (flooding) надсилання великої кількості запитів до веб-сервера є незвичною поведінкою, але надсилання одного запиту є законним. Отже, ми можемо розглянути DoS-атаку як collective anomaly. Як було зазначено в розділі 1.1, коли окремо той, чи інший екземпляри не будуть мати аномальну поведінку, а разом – поводитись аномально. В окремих випадках (надсилаючи неправильно сформовані пакети) DoS-атаку можна вважати point аномалією.

Інші атаки можна розглядати як contextual аномалії. Їх об’єднує зловживання системними вразливостями для завдання шкоди. Наприклад, Shellcode або Backdoor виконують програмні скрипти коду; Worms та Malware встановлюють шкідливе ПО; R2L U2R змінюють або отримують дозволи (привілеї) користувача системи (в багатьох випадках – суперкористувача) шляхом виконання дій на машині жертви. Такі атаки повинні якомога швидше пошкодити систему, приховуючи також свою діяльність, щоб уникнути виявлення та блокування антивірусами. Припускається, що вони генерують контекстні аномалії, впливаючи на систему за короткий проміжок часу без значних відповідних коливань значень ознак. Наприклад, worm може мати на меті сканувати систему на наявність паролів і відправляти їх до якогось віддаленого сховища, або змінювати облікові дані для доступу VPN або SSH на машині: надсилання даних або зміна дозволів самі по собі не є аномалією, але вони є аномальними у конкретному контексті. З іншого боку, атаки U2R та R2L є специфічними і складними в реалізації, порівняно з іншими типами атак. Тому ці атаки можуть розглядатись як point аномалія. Також оскільки атака probe не завжди завдає шкоди, а скоріше має певний намір у розвідуванні специфічної інформації, вона може відноситись до contextual anomaly [10].

Визначення колективних аномалій зазвичай більш легка процедура, тому що можна виділити наступне правило: «Якщо повторювальні дії, що відступають від нормальної поведінки системи, з'являються в наступних точках даних, ми можемо однозначно стверджувати, що така атака проявляється як колективна аномалія». В іншому випадку вивчення наборів даних для диференціації точкових та контекстних аномалій вимагає більших зусиль, бо не складає досить не тривіальну задачу для аналітиків.

Наведена схема на рисунку 1.1 визначає зв’язок аномалій з атаками і є частиною таксономії аномалій, яка буде представлена надалі. Проте треба мати

на увазі, що в залежності від конкретного випадку точкова або колективна аномалія може бути контекстною.

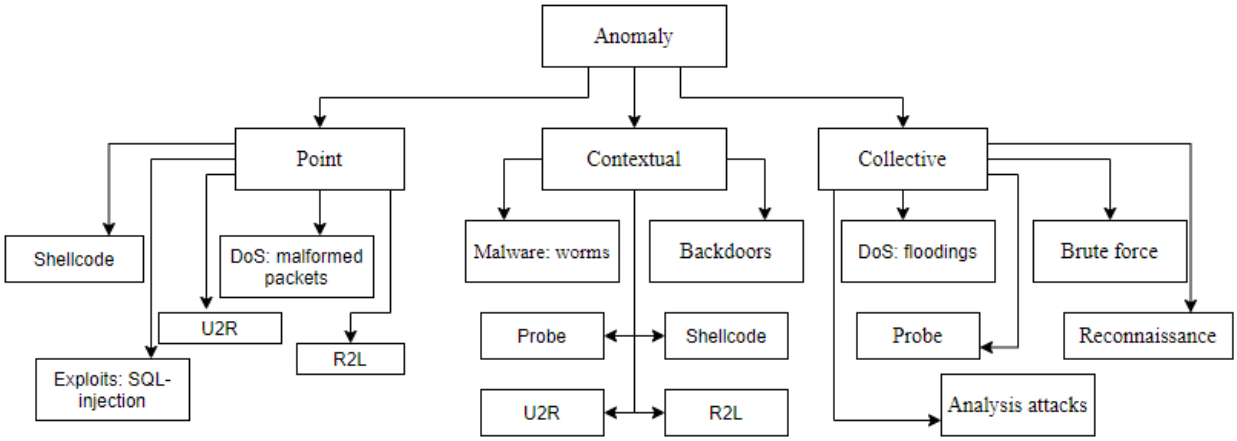

Рисунок 1.1 – Зв’язок аномалій з атаками

1.4 Характеристика мережевих аномалій в аспекті джерела виникнення

Можна виділити 5 основних джерел виникнення аномальної поведінки системи в мережі [7].

1) Network – targeted anomalies

З групи мережевих атак можна виділити атаки, які викликають аномальну поведінку мережевого трафіку в корпоративній мережі і націлені на виведення роботи всієї мережі з ладу. Мережеві аномалії можна також класифікувати, розділивши на дві основні групи: *програмно-апаратні відхилення* і *проблеми безпеки*. (Рис. 2.2.1.)

Програмно-апаратні відхилення можна розділити на: апаратні несправності, помилки програмного забезпечення, помилки конфігурації, порушення продуктивності обладнання; в той час як проблеми безпеки можна розділити на: сканування, вірусну активність, експлуатацію вразливостей,

атаки на відмову від обслуговування, мережеві модифікатори та аналізатори трафіку [12].

Типові приклади програмно-апаратних відхилень - це збої в роботі файлового сервера, network paging, шторми трансляцій (broadcast storms), babbling node, та transient congestion [7]. Наприклад, збої файлового сервера, такі як збій веб-сервера, може статися, коли збільшується кількість ftp-запитів до цього сервера. Помилки network paging виникають, коли прикладна програма переростає ліміт пам’яті робочої станції і починає використовувати пам’ять файлового серверу мережі. Ця аномалія може не вплинути на окремого користувача але впливає на інших користувачів мережі, викликаючи дефіцит пропускної здатності мережі. Broadcast storms стосуються ситуацій, коли широкомовні пакети використовуються до тих пір, поки не вийде з ладу мережа. Babbling node стається тоді, коли вузол надсилає невеликі пакети в нескінченному циклі, щоб перевірити наявність така інформація, як звіти про стан. Congestion за короткий час стається за наявності «гарячих точок» в мережі як результат відповідної несправності каналу або надмірного навантаження на той момент в мережі. У деяких випадках можуть виникати проблеми з програмним забезпеченням в якості мережевих аномалій, такі як помилка впровадження протоколу. Наприклад, помилка прийняття протоколу в супер сервері (inetd) призводить до зменшення доступу до мережі, що, в свою чергу, впливає на навантаження на мережевий трафік. Помилки програмного забезпечення компонентів інформаційної системи можуть спричинити припинення надання сервісів, порушення працездатності як окремих компонентів, так і цілої системи.

Друга основна категорія аномалій мережі - це проблеми, пов’язані з безпекою. Атаки відмови в обслуговуванні та вторгнення в мережу - приклади таких аномалій. Атака на відмову в обслуговуванні трапляється, коли послуги, пропоновані мережею, захоплені зловмисною особою. Сторона, що порушила,

могла вимкнути важливу службу, таку як сервер доменних імен (DNS) і спричинити віртуальне відключення мережі. Для цієї події аномалія може характеризуватися дуже низькою пропускна здатність. У разі вторгнення в мережу, зловмисники можуть викрасти пропускну здатність мережі, затопивши мережу непотрібним трафіком. Мережеве сканування проводиться для того, щоб провести аналізу топології мережі і виявлення доступних для атаки сервісів. Найчастіше скануються цілі підмережі, що виражається в наявності в атакований мережі безлічі пакетів з однієї IP адреси сканера по безлічі IP адрес досліджуваної підмережі. Аналізатори трафіку (сніфери) призначені для перехоплення і аналізу мережевого трафіку. У найпростішому випадку для цього проводиться перехід мережевого адаптера апаратного комплексу в прослуховуючий режим і потоки даних в сегменті, до якого він підключений, стають доступні для подальшого вивчення. Вірусна мережева активність є результатом спроб поширення комп'ютерних вірусів і черв'яків, використовуючи мережеві ресурси. Встановлений вірус може використовувати як одну так і декілька уразливостей в мережевій прикладний службі [12].

Найчастіші атаки, пов’язані із мережевими аномаліями це: DoS/DDoS, broadcast storms, network paging, file server errors, babbling node, transient congestion, scanning / enumeration, packet forging.

2) Host – related anomalies

Host – related атаки націлені на конкретні хости або системи шляхом запуску зловмисного програмне забезпечення для компрометації або пошкодження функціональних можливостей системи. Більшість атак хосту класифікуються за категоріями шкідливих програм: віруси, рекламне програмне забезпечення, шпигунське програмне забезпечення, троянські програми.

3) Software – related anomalies

Прикладами software– related аномалій може бути діяльність, пов’язана із такою атакуючою поведінкою, як Code injection та Cross-site scripting (XSS). Підроблені сертифікати сервера є тривожним знаком, що слід враховувати при аналізі комунікацій, оскільки вони можуть ввести в оману браузер / користувача, думаючи, що зв’язок безпечний. Це може призвести до появи фішингових веб-сайтів, які виглядають законно. Більше того, вони могли використовуватись як підґрунтя здійснення інших атак, таких як Man-in-the Middle.

4) Physical-related anomalies

Фізичні атаки є результатом спроби загартування мережевого обладнання (вузлів або інших пристроїв) або його конфігурації. Це може включати зміну конфігурацій і введення backdoors (тобто The Evil Maid).

5) Human-related anomalies

Остання категорія мережевих атак заснована на діях людини. Фішинг - це одна форма атаки «людиною», де зловмисник використовує електронні листи або інші електронні повідомлення або послуги з метою отримання облікових або конфіденційних даних. Коли користувач намагається отримати вищі привілеї, це вважається атака людини типу User to Root та R2L. Human-related атаки також можуть включати викрадення сесії, ці атаки засновані на отриманні зловмисником доступу через активний сеанс для доступу до файлів cookie та токенів.

На рисунку 1.2 схематично зображена демонстрація джерел виникнення аномальної поведінки із прикладами аномальної поведінки.

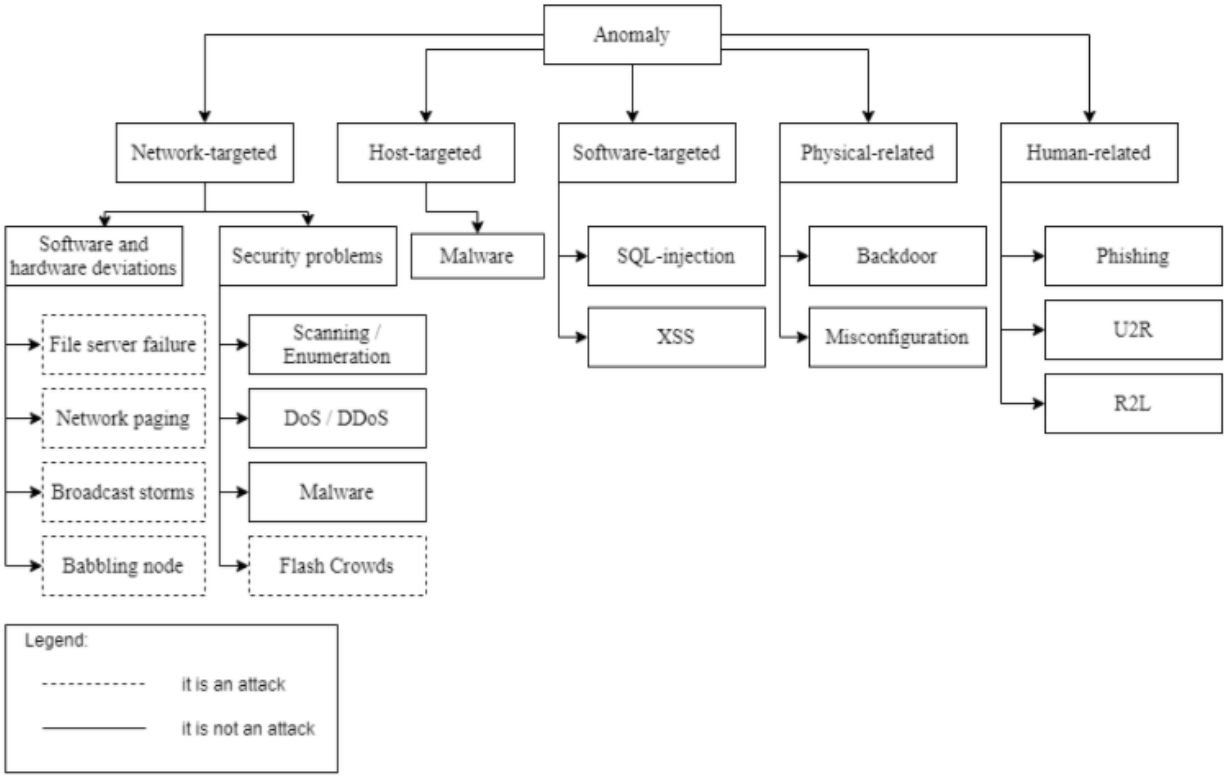

Рисунок 1.2 – Характеристика аномалій в контексті джерел (цілей) виникнення

1.5 Огляд схеми виявлення аномалій (мережевих та немережевих)

Основний підхід по виявленню аномалій це побудова профілю організації (нормальної активності) по певним параметрам. Опис роботи алгоритму виявлення аномалій наведений на рисунку 1.3 [13].

Аналізованими даними для прийняття рішення щодо наявності аномальних екземплярів для того чи іншого випадку є трафік. Він може бути як мережевим так і немережевим, в залежності від системи і цілей моніторингу. Для мережі трафік це набір пакетів, зазвичай фрагменованих на рівні IP. Дані збираються за певний проміжок часу для подальшої нормалізації, щоб визначити ознаки, за якими буде побудований профіль активності. Заданий набір ознак порівнюється із ознаками нормальної діяльності системи,

визначеними попередньо. Якщо наявна значуща різниця порівнювальних параметрів тоді трафік рахується аномальним, в іншому випадку відбувається корегування шаблону нормальної поведінки і ця діяльність переходить в штатний режим мережі [13]. Алгоритм перевірки на відповідність поточних даних від шаблонних зазвичай комплексний і не такий простий, як здається на перший погляд, тому що від точності результатів може залежати майбутнє як інформаційної системи, так і організації в цілому.

Рисунок 1.3 - Алгоритм дії системного профілю

Принцип моніторингу немережевих аномалій не відрізняється від мережевих. В залежності від певних особливостей компанії, програм, якими вона користується, типом операційної системи, тощо відбувається категоризація та складання шаблону нормальної активності. В таблиці 1.1

наведені групи окремих випадків, які потребують уваги (наведений приклад на операційній системі Windows).

Таблиця 1.1 – Характеристика немережевих аномалій

Windows: підозрілі мережеві комунікації	Для того, щоб виявити спілкування процесів з зовнішніми IP адресами, що зазвичай відрізняється (профіль мережевої активності)
Windows: елементи запуску	Для того щоб виявити невідомі ознаки (елементи) запуску (профіль елементів запуску)
Windows: заплановані завдання	Для того щоб виявити невідомі заплановані завдання (профіль запланованих завдань)
Windows: запущені процеси	Для того, щоб виявити: - Діяльність невідомих дивних процесів; - Процес із невідомими шляхами; - Процеси із нестандартними хешами;
Windows: прослуховування портів	Для того, щоб виявляти невідомі процеси, що відкривають та прослуховують порти
Windows: etc / hosts	Для того, щоб виявляти підозрілі зміни etc / hosts файлів
Windows: cmd.exe та powershell.exe процеси	Для того, щоб виявляти аномальні процеси, що запускають cmd.exe та powershell.exe процес
Windows: загрузка драйверів	Для того, щоб моніторити всі драйвери, що завантажені із підозрілих сайтів
Windows: загрузка модулів	Для того, щоб моніторити всі модулі, що завантажені із підозрілих сайтів
Windows: сервіси	Для того, щоб виявляти нові сервіси або зміни в існуючих
Windows: батьківські та дочірні процеси	Для того, щоб виявляти батьківські та дочірні процеси

Наприклад підозрілі ініціації Інтернет-з’єднань від певних процесів. Збирається таблиця по процесам кожний раз коли ініціюється нове Інтернет-зє’єднання і відбувається порівняння із профілем нормальної активності. Для випадку моніторингу процесів, що відкривають порти, схема працює таким чином: є список портів які часто відкриваються і є список портів, що відкриваються рідко. Якщо був відкритий порт, що належить списку «рідких» портів – спрацьовує попередження (так можна визначити хто і навіщо відкривав порт незапланово). Перевіряється який процес запустив модуль та хеши модулів.

Тобто на основі різної службової інформації, що дає нам ОС будуються профілі організацій з певними виключеннями для випадків (профіль організації для кожної компанії свій).

Висновки до розділу 1

Для характеристики аномалій була проаналізована поведінка категорій атак, які детектуються більшістю IDS для трьох основних категорій аномалій. Враховуючи характеристики найбільш популярних атак, їх відношення до певного типу аномалії та джерела виникнення допоможе скласти прозору картину розуміння появи загроз в кіберпросторі. Наголошена збіжність при фіксуванні нестандартних подій при складанні профілю організації для мережевих і немережевих аномалій також допомагає побачити частину процесу захисту інформаційних систем від атакуючих дій зловмисників.

2 ХАРАКТЕРИСТИКА АНОМАЛІЙ, ВИКОРИСТОВУЮЧИ АНАЛІЗ HTTP ТРАФІКУ

Існуюча методологія виявлення втручань в систему та аномалій досі незріла в області безпеки веб-додатків. Системи виявлення в більшості використовуються як пристрій мережевої безпеки, проте проектування веб-IDS вимагає іншого підходу, ніж традиційний мережевий IDS для обробки нестандартної поведінки, пов'язаною з веб-додатками.

Зловмисники використовують як правило протоколи HTTP / HTTPS для використання вразливостей веб-додатків. Hypertext Transfer Protocol (HTTP) [14] - це протокол відповіді на запит, призначений для забезпечення зв'язку між клієнтом та сервером, а HTTPS [15] забезпечує безпечне та зашифроване з'єднання. Коли трафік HTTPS спостерігається з точки зору IDS, одним суттєвим недоліком є те, що шифрування зав'язує очі мережевим системам виявлення. Якщо розглядати IDS як систему на основі Host-Based (HIDS) та на основі Network-Based (NIDS) в залежності від того, чи вони працюють на рівні додатків або на Інтернет-рівні моделі TCP / IP. NIDS відстежує мережеві пакети, і використовуючи протокол HTTPS пакетні дані існують у зашифрованому вигляді, який система детектування не може перевірити. Однак ці системи можуть перевіряти трафік HTTPS, якщо мати доступ до приватного ключа сертифіката SSL. З іншого боку, HIDS не стикається з жодною проблемою у роботі з трафіком HTTPS, оскільки вони захищають кінцеві точки, де зашифрована інформація дешифрується назад у звичайну форму.

Основна роль систем виявлення полягає у розкритті і перевірці значень, наданих у полях заголовка та параметрах запиту. Перевірка відбувається в сенсі проведення порівняння поточних значень запиту із ознаками, які будуть

визначені в ході цієї роботи, що вважаються аномальними при дії зловмисних програм.

2.1 Концептуальний фреймворк IDS/IPS системи для аналізу HTTP трафіка

Для проведення аналізу HTTP трафіку треба зазначити як саме аналізуються запити в IDS / IPS системах. Як приклад можна навести ідеалізовану картину концептуального фреймворку, що наведений у [16]. Основні частини фреймворку:

- Структура запропонованого IPS використовує гібридний підхід виявлення для використання можливостей як сигнатур, так і методів виявлення на основі аномалій. Методологія виявлення сигнатур допомагає визначити жорсткі правила як для білого, так і для чорного списку вже відомого вмісту, а методологія виявлення аномалій розширює знання системи про нормальну поведінку.
- Представлена структура відповідає модульній архітектурі, де вся система розділена на п’ять компонентів, а саме: препроцесор, детектор, захисник, реєстратор та контролер відповіді.
- IPS зберігає конфігурацію та поведінкові профілі кожного веб-додатка відповідно до його бізнес-логіки, щоб зрозуміти його структуру, функціональні можливості та операції. Пояснюються етапи конфігурації та побудова поведінкових профілів разом із компонентами фреймворку.
- IPS також включає функцію offloading SSL для шифрування та дешифрування трафіку SSL. Він отримує як HTTP, так і HTTPS-запити, розшифровує вміст, якщо запит є HTTPS, перевіряє вміст і пересилає нешкідливі запити на сервер у форматі HTTP. Подібним чином IPS отримує відповіді HTTP від веб-сервера, обробляє вміст, шифрує вміст для зв'язку HTTPS і, нарешті, відправляє його клієнту. Компонент «препроцесор»

обробляє дешифрування, тоді як компонент «контролер відповіді» забезпечує шифрування.

Саме аналіз трафіку відбувається в модулі препроцесору, що має назву «конструктор даних». Відбувається підготовка даних до формату, який буде використовуватися компонентом «детектор» для аналізу запитів. Конструктор даних зчитує необроблений вміст HTTP-запиту та структурує його на кілька полів, які слід дослідити для розпізнавання підозрілих запитів, таких як вихідна IP-адреса, позначка часу запиту, метод HTTP, запитувана URL-адреса, заголовки HTTP, файли cookie, дані запитів POST та GET.

2.2 Визначення аномальної поведінки, використовуючи HTTP запити (трафік)

Використовуючи більшість досліджень в сфері зловмисної діяльності аналізуючи HTTP трафік, було виявлено такі головні відмінності між шкідливим трафіком і трафіком браузера [17]:

- Наявність 0–3 заголовків
- Відсутність User-Agent заголовку
- Нестандартні значення User-Agent заголовку
- Non-ASCII символи в payload
- Присутність POST request без Referer header
- Присутність GET з payload
- Значення Host header відрізняється від домену
- Нестача значень заголовків, таких як Accept, Accept-Encoding, Accept-Language, Referer, Connection

Визначення аномальної поведінки, використовуючи HTTP запити (трафік), що може бути потенційною загрозою, які зазначені вище в наведеній таксономії:

1) Нестандартне значення User-Agent заголовків може свідчити про діяльність таких атак, як XSS, DoS, SQL-injection.

Прикладом цього є старий відомий експлоіт проти сервера SHOUTcast. Сервер вийде з ладу, коли в заголовку HTTP-запиту буде зроблено дуже довгий (4 КБ) запит. Ще один приклад - сервер потокової передачі Darwin (використовуючи агент користувача довшим за 255 символів, спричинить відмову в обслуговуванні). [18]

2) Зберігання чутливої інформації в cookie може свідчити про XSS, Session hijacking, Session spoofing, Session fixation.

У більш широкому розумінні зловживання файлами cookie може означати будь-які маніпуляції файлами cookie, як правило, націленими на файли cookie сеансу. Ідентифікатор сеансу - найцінніший фрагмент даних, що зберігається у файлах cookie додатків, оскільки він відкриває шлях до викрадення сесії та пов'язаних з ним атак. Незалежно від використовуваного атакуючого методу (XSS, Session hijacking, Session spoofing, Session fixation), успішне поглинання сесії може мати згубні наслідки. Залежно від цільового сайту або програми, зловмисники можуть мати змогу викрасти конфіденційну інформацію користувача, таку як облікові дані або особисту інформацію, або виконати небажану інформацію про операції, такі як переказ коштів або додавання нового облікового запису користувача для подальшого доступу [19].

3) Багаточисленні спроби автентифікації в маленькому проміжку часу (приблизно 0,5 секунд), додатково присутнє зростання номеру порту

говорить про використання автоматизованого інструменту – можлива реалізація атаки Brute Force [20].

4) Багаточисленні запити (більше 10) веб-сторінок одного веб-застосунку в маленькому проміжку часу (менше 1 секунди), зроблених з однієї адреси. Це говорить про використання автоматизованого інструменту (вручну це відтворити за такий малий час неможливо). Також присутнє зростання номер порту із кожним новим запитом, і наявність багатьох “404 Not Found” говорить про використання спеціального списку слів для запиту найпоширеніших каталогів з веб-сайту. Ці дії свідчать про можливу дію атаки Spydering [20].

5) Невірно сформовані запити в наповненні поля Referer (GET query); або відсутність кодування або фільтрації (перевірки) в mutillidae у запиті POST – діяльність атаки SQL-injection.

Атака SQL Injection зазвичай використовує поле введення у веб-формі, до якого не застосовані певні обмеження валідації. Частини операторів SQL подаються у поле веб-форми, які потім переходять до сервера баз даних, де вони обробляються. Прикладом такої атаки може бути скидання вмісту бази даних у загальнодоступний файл або назад до самого виводу веб-сайту [21].

6) Відсутність кодування в mutillidae у запиті POST, наявність знаків скрипту ‘<>’ які будуть декодовані з ASCII в шістнадцяткову систему – свідчить про можливість реалізації атак XSS, Command Injection, SQL injection, BeEF, Unvalidated Redirects.

У випадку наявності декодованих знаків скрипту ‘<>’ програмне забезпечення таке як Suricata та Snort здатне виявляти та перекодувати ці символи. Command injection не так поширене у веб-програмах, як SQL-injection. При command injection зловмисник вводить команди операційної системи через веб-застосунок. Цей тип атаки може бути дуже потужним, якщо

веб-програма вразлива і особливо тоді, якщо команди можна запускати з правами супекористувача [20].

7) Наявність специфічних кодованих символів в URL у заголовках відповіді в полі “location”може свідчити про атаку Double Encoding [20].

В наведеній таблиці можна побачити конкретні символи, які слід перевіряти на наявність атаки кодувати атаки Double Encoding. Оскільки це найпоширеніші набори символів, які використовуються для атаки на веб-застосунок можна зменшити ризик експлуатації.

Таблиця 2.1 – Символи двойного кодування

Double encoding symbols	
.	%252E
\	%255C
/	%252F
<	%253C
>	%253E

8) Наявність Non-ASCII символів in the payload свідчить про аномальний трафік. Згідно аналізу, представленому у [17] – такі категорії атак, як Banker, Downloader, Spambot у більш ніж 50% випадках містять non-ASCII символи у payload. Також менш розповсюджено використання non-ASCII символів для атак категорій Bruteforce, Keylogger, PUA/Adware, Ransomware, та Trojan.

9) Кількість заголовків суттєво перевищує нормальну кількість (1-3).

Аналіз, проведений у [22] показує, що зловмисне програмне забезпечення іноді не включає User-Agent або його довжина значення, як правило, менше 90 байт. Крім того, шкідливе програмне забезпечення, як

правило, надсилає 1–3 заголовки в запитах, а шкідливі програми зазвичай надсилають більше 9 заголовків.

Висновки до розділу 2

Дослідив концепт аналізу HTTP трафіку в IDS / IPS системах і розглянувши найкращий випадок застосування фреймворку, в якому представлено як саме відбувається перевірка значень полях заголовка та параметрах запиту, що є найбільш вразливими місцями, можна виділити групи аномальної поведінки. Наведена таблиця 2.2 об’єднує різні типи аномальної поведінки, пов’язаної із HTTP трафіком і групує відповідно до категорій атак

Таблиця 2.2 - Характеристика аномалій згідно аналізу HTTP трафіку

Аномальна поведінка	Можливий тип атаки
Не стандартне значення в полі User-Agent header.	XSS, DoS, SQL-injection
Зберігання чутливої інформації в cookie.	XSS, Session hijacking, Session spoofing, Session fixation
Повторювальні спроби логіну в проміжку часу (менше 0.5 секунд), номеру порту постійно збільшується.	Brute Force
Багато запитів націлених на різні сторінки одного web-додатку, зроблених з однакового IP адресу за час (менше 1 секунди).	Spydering
Присутність великої кількості "404 Not Found" помилкових результатів зпитів за час (менше 1 секунди).	Spydering
Присутність неправильно форматованого запросу, деякі символи '<>' закодовані з ASCII до hexademical.	XSS, Command Injection, SQL injection, Unvalidated redirects

Продовження таблиці 2.2

Присутність специфічно закодованих символів (як %252E, %252F, %255C, %253C, %253E).	Double encoding
Non-ASCII символи в playload.	Ransomware, Spambot
Кількість заголовків суттєво перевищує нормальну кількість (1-3).	Malware

3 КЛАСИФІКАЦІЯ АНОМАЛІЙ НА ОСНОВІ МЕТОДУ ЇХ ВИЯВЛЕННЯ В АСПЕКТІ КАТЕГОРІЙ АТАК

3.1 Класифікація IDS

IDS - це системи, побудовані для моніторингу та аналізу мережевого трафіку та / або системи для виявлення аномалій, втручань або порушень конфіденційності. Коли виявляється вторгнення, очікується, що IDS:

(a) реєструє інформацію, що стосується вторгнення,

(b) спрацьовують попередження (alerts)

(c) відповідно до попереджень застосовуються певні заходи / корективи

IDS можна класифікувати на три категорії відповідно до виду підозрілої активності, що спостерігається [23]:

1. IDS на основі хостів (HIDS) - це агент, встановлений на окремих хостах, який аналізує їх діяльність: файли, процеси, системні журнали тощо.
2. Мережеві IDS (NIDS) зазвичай використовує сенсори (датчики) в різних точках мережі. Аналіз трафіку проводиться або сенсором (датчиком), або віддалено за допомогою центрального контролера. NIDS є більш масштабованими та крос-платформними, ніж HIDS, саме тому вони широко розповсюджені для захисту даних в IT компанії.
3. IDS на основі додатків (application-based IDSs) - це особливий тип HIDS, призначений для моніторингу конкретного додатка. IDS на основі додатків аналізують взаємодію між користувачами та додатками: виконання чи модифікації файлів, журнали, авторизації та інші типи діяльності.

З іншого боку, IDS можна класифікувати згідно методу виявлення: signature-based, anomaly-based, hybrid [23].

1. Signature-based: Першими були розроблені IDS на основі сигнатур, що будуються з попередньо виявлених атак. Головною перевагою цього методу є висока точність детектування відомих атаки.

2. Anomaly-based. За допомогою цього методу відбувається порівняння певних закономірностей в трафіку з наперед визначеною «нормальною» або «очікуваною» поведінкою системи. Будь-яке відхилення буде вважатись потенційною атакою і буде спрацьовувати попередження (alarm). *Точність систем на основі аномалій при виявлення атак нульового дня, метаморфічних та поліморфних, тощо є кращою порівняно з IDS на основі підпису.*

3. Гібридне виявлення поєднує signature-based та anomaly-based рішення для усунення слабких сторін кожної категорії.

Anomaly-based IDS можна класифікувати на підкатегорії на основі правила: аномальну поведінку потрібно відрізняти від нормальної поведінки. Наразі існує багато рішень щодо того, який метод детектування аномалій краще використовувати (рис. 3.1) [7].

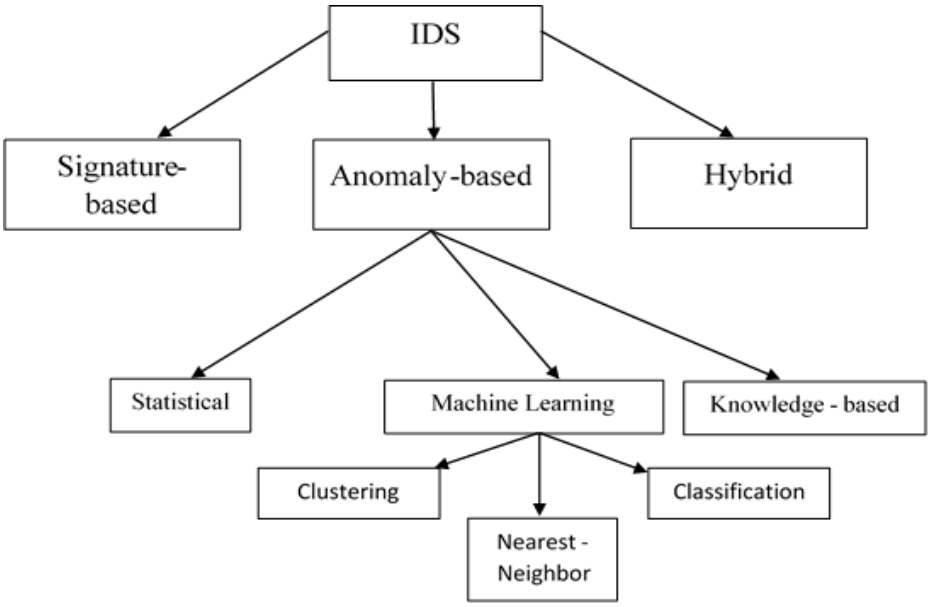

Рисунок. 3.1 – Методи детектування аномалій

За допомогою переважно signature-based IDS використовують набори даних (датасети), які допомагають ідентифікувати ту чи іншу загрозу. Набори даних можуть бути як реальними (тобто дані є зчитані з мережевих налаштувань), так і синтетичними (тобто дані з модельованого трафіку). Однак, оскільки мережі зазнають постійних змін, в наборах даних, що доступні на теперішній час, бракує real-life характеристик, що з'являються останнім часом. Досліджуючи датасети, що використовуються signature-based IDS, були знайдені таки атаки: DoS, DDoS, Fraud, Backdoor, R2L, Code-injection, Heartbleed, U2L, Worm, Probing, Enumeration, nonTor traffic. Знайдені лише 12 типів атак говорять про певні обмеження IDS проти широкого кола атак і атак нульового дня. Існує потреба у створенні розширюваних наборів даних, які можуть бути використані для навчання моделей машинного навчання, що використовуються для виявлення аномалії. Використовуючи розширювані набори даних разом з використанням ML, виявлення атаки нульового дня може бути інтегроване в IDS на основі аномалій.

Як зазначено вище, класифікація anomaly-based IDS має розбиття на категорії. Використовуючи дослідження [7] можна розглянути частоту використання різних IDS на основі аномалій. Категорія, що належить методам машинного навчання займає більше 70%, статистичні методи близько 20% і решта належить іншим категоріям, в тому числі і knowledge-based. Звідси можна зробити висновок, що anomaly-based IDS на основі машинного навчання є найбільш популярним у використанні.

3.2 Приклади детектування аномалій на основі машинного навчання

Anomaly-based IDS для здійснення моніторингу подій і відповідного реагування на відхилення від нормальної поведінки спочатку необхідно «навчити». Процес «навчання» залежить від певного обраного методу

знаходження аномалій (в широкому сенсі застосовуючи технології машинного навчання існують дві категорії: supervised та unsupervised). Для оцінки результату, використовуються або оцінки, або мітки. Для систематизованого представлення процесу роботи «системи виявлення аномалій» (СВА) в ході цього дослідження є наведений фреймворк (рис. 3.2) [24].

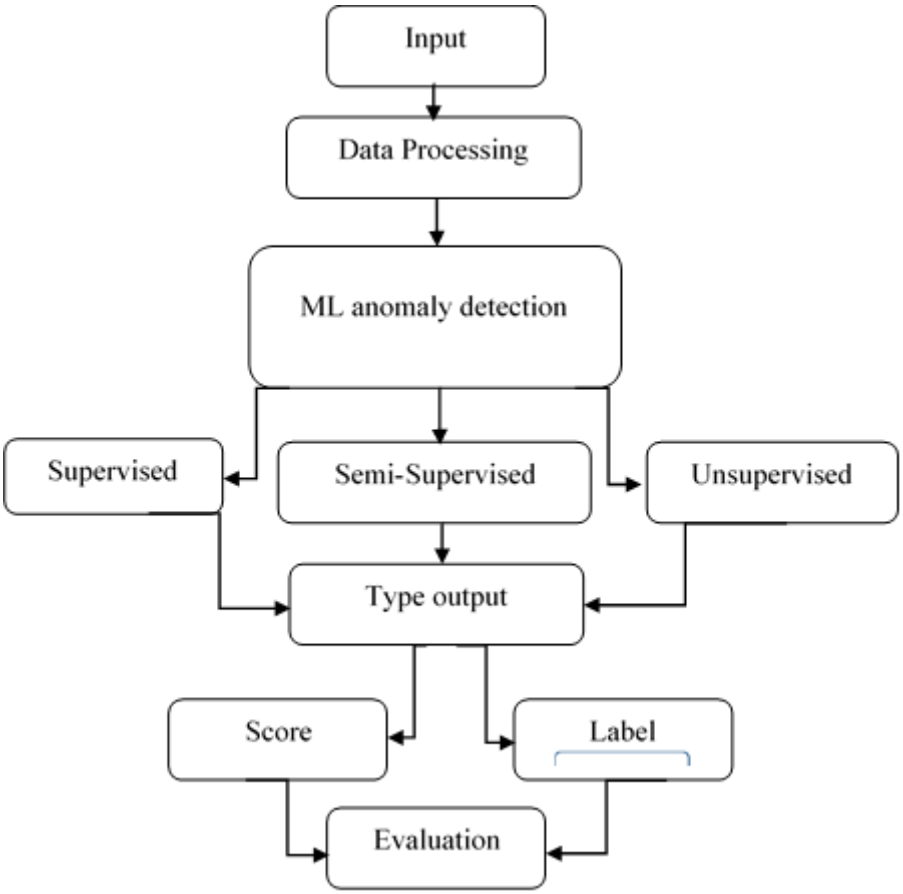

Рисунок. 3.2 – Схема фреймворку СВА із використанням машинного навчання

Методи виявлення аномалій з використання машинного навчання можуть бути представлені в трьох способах: контрольований (supervised), напівконтрольований (semi-supervised) і неконтрольований(unsupervised).

1) supervised: алгоритми машинного навчання «навчають» функцію відображення за допомогою міток в навчальних наборах, де кожен екземпляр навчального набору позначений одним із станів у S.

2) semi-supervised: алгоритми машинного навчання, в яких екземпляри з навчального набору мають мітки лише для нормального класу і не вимагають міток для класу аномалій.

3) unsupervised: алгоритми машинного навчання «навчають» функцію відображення з навчального набору даних без використання міток.

Алгоритми класифікації та кластеризації як правило застосовуються для point та collective аномалій [24].

Research Article Adaptive Anomaly Detection Framework Model Objects in Cyberspace Hasan Alkahtani, Theyazn H. H. Aldhyani , and Mohammed Al-Yaari

Для гарантії ефективної роботи IDS / IPS треба враховувати два фактори. По-перше, виявлення вторгнень повинно забезпечувати сумісні та доречні результати виявлення. По-друге, IDS повинні мати можливість справлятись із «ворожим середовищем» (тобто під спробами реалізацій атак). Оскільки присутня тенденція збільшення атакуючих спроб завдати шкоди інформаційним системам, інструменти IDS стають нездатними для захисту комп’ютерів та програм. Отже, потрібен надійний підхід, який здатний виявляти нові атаки, необхідний для створення надійних IDS. Машинне навчання забезпечує «навчання» для виявлення нових атак. Для вивчення використовуються методи машинного навчання, що обробляють звичайну поведінку на комп’ютері та виявляють аномальну, яка відхиляється від звичайної, як вторгнення.

Розглянемо як ключову атаку DoS / DDoS, на прикладі якої будуть наведені різні алгоритми IDS по детектуванню аномальної поведінки. Для цього насамперед потрібно наголосити про обмеженість наборів даних, які використовуються дослідниками при тестуванні того чи іншого алгоритму.

Основні датасети для машинного навчання [6]:

- KDD Cup’99 Dataset

- NSL-KDD Dataset
- ISCX Dataset
- CICIDS2017 Dataset
- CICIDS2018 Dataset

Найбільш відомий набір даних в сфері застосування IDS це KDD Cup’99 Dataset. Він досі використовується в останніх експериментах та обстеженнях і існував ще до випуску оновленого NSL-KDD. Набір даних містить такі атаки: DoS (відмова в обслуговуванні), R2L (несанкціонований доступ з віддаленого), U2R (несанкціонований доступ до суперкористувацьких / кореневих функцій) та Probing (збір інформації про мережу).

Наступний набір даних це NSL-KDD (2009), який був створений для вирішення проблем у наборі даних KDD Cup 99, оскільки була наявність надлишкових записів у наборах поїздів та дублікати в тестових наборах. Атаки, що детектуються такі ж, як і в KC.

Набір даних ISCX (2012) був створений Канадським інститутом кібербезпеки в контрольованому середовищі на основі реалістичної мережі та трафіку для відображення реальних наслідків атак над мережею та відповідних реакцій робочих станцій. Моделюються чотири різні сценарії атак: infiltration, відмова HTTP в обслуговуванні, розподілена відмова в обслуговуванні за допомогою бот-мережі IRC та спроби авторизації SSH brute-force.

Датасети CICIDS2017 та CICIDS2018 також розроблені Канадським інститутом кібербезпеки, проте більш новітніші і здатні покривати більш ширший діапазон можливих атак. Набір даних CICIDS2017 містить найсучасніші поширені атаки, які нагадують справжні реальні дані (PCAP). Він також включає результати аналізу мережевого трафіку за допомогою CICFlowMeter з позначеними потоками на основі часової позначки, джерела та IP-адреси, порти джерела та призначення, протоколів та атак. Створення

реалістичного фонового трафіку було нашим головним пріоритетом у створенні цього набору даних. До реалізованих атак належать Infiltration, Brute Force FTP / SSH, DoS / DDoS, Heartbleed, Web Attack, Botnet та DDoS [6].

Далі будуть коротко описані найбільш вживані методи IDS на основі машинного навчання для детектування DoS атак.

Традиційні методи машинного навчання як Support Vector Machine (SVM) та K-Nearest Neighbor (K-NN) залишаються надійними для виявлення аномалій в сфері кібербезпеки, в тому числі DoS / DDoS атак.

Концепт SVM методу лежить у використанні функції ядра. Популярні варіанти функції ядра - лінійна, поліноміальна і сигмоїдальна. За допомогою функції прийняття рішення, що базується на функції ядра можна класифікувати набір даних у два класи.

Інший популярний метод класифікації в машинному навчанні це K-Nearest Neighbor, в якому відбувається вимірювання відстані між різними значеннями ознак. K-NN алгоритм потрібен щоб знайти K значень, близьких до значень у навчальному наборі даних, та якщо більшість із цих значень K належать до певного одного класу, тоді вхідний екземпляр буде відноситись до цієї категорії.

Більш детально про дослідження методів класифікації при виявленні класу DoS атак можна прочитати у [25].

Для детектування DoS атак також застосовують алгоритми кластеризації, а саме k-means. У кластеризації алгоритм навчання знаходить подібність між екземплярами для побудови кластерів (тобто груп екземплярів). Одна з переваг методів кластеризації перед статистичними методами полягає в тому, що вони не покладаються на будь-який відомий раніше розподіл даних. Але методи, засновані на машинному навчанні, вимагають тривалого періоду навчання, і тому це може викликати труднощі.

K-means алгоритм, заснований на ітеративному переміщенні, що розділяє набір даних на кластери, локально мінімізуючи середню квадратну відстань між точками даних кластера та центрами кластера. Проте він має недоліки, такі як:

1) вибір k-значення (число кластеризації) складно оцінити;

2) початкові центри кластеризації алгоритму вибираються випадковим чином, і вибір центру має великий вплив на результати кластеризації;

3) алгоритму потрібно постійно коригувати класифікацію вибірки до зближення цільової функції, бо коли великий обсяг даних, складність часу алгоритму є також великою.

Згідно деяким дослідженням [25] краще застосовувати MF-CKM метод детектування, що відноситься до semi-supervised алгоритмів машинного навчання. Його перевага над K-means в використанні невеликої кількості даних з мітками для обмеження вибору початкових центральних точок та підвищення швидкості збіжності та точності класифікації алгоритму.

Також при виявленні DoS / DDoS атак є ефективним інший метод кластеризації: MCADET (або HCADET): Multi-stage Clustering based Collective Anomaly Detection. В цьому методі використовується дисперсія екземплярів даних у створених багатоступеневих кластерах щоб мати змогу диференціювати колективно аномальний кластер від нормального. Однак, дисперсія не завжди може враховувати колективні аномалії і вибираючи багатоступінчасті кластери, можливе виникнення великих false negatives. Тому є доречним включення параметру Hurst (H), оскільки значення H для атаки DoS зазвичай має тенденцію бути значно меншим, ніж в нормальному трафіку. У запропонованому HCADET підході, створені кластери оцінюються відповідно до їх H значення параметра для виявлення колективної аномалії.

Запропоновані методи детектування аномальної поведінки при виявленні DoS / DDoS атак представлені у рис.3.3 і можуть бути представлені в більш ширшому діапазоні, окрім основних наведених методів, оскільки існує велика кількість досліджень і ця кількість постійно збільшується разом із розвитком технологій.

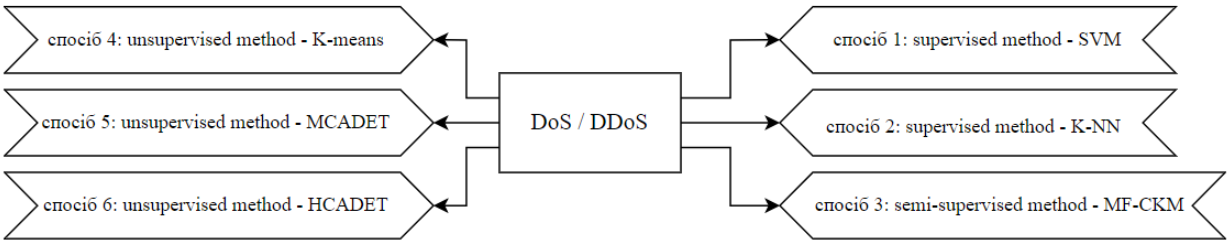

Рисунок 3.3 – Методи детектування аномальної поведінки DoS / DDoS атак

Аналогічним чином були розглянуті дослідження по IDS, проведені для виявлення таких типів атак, як Bruce Force, Probing, R2L, U2R (рис 3.4).

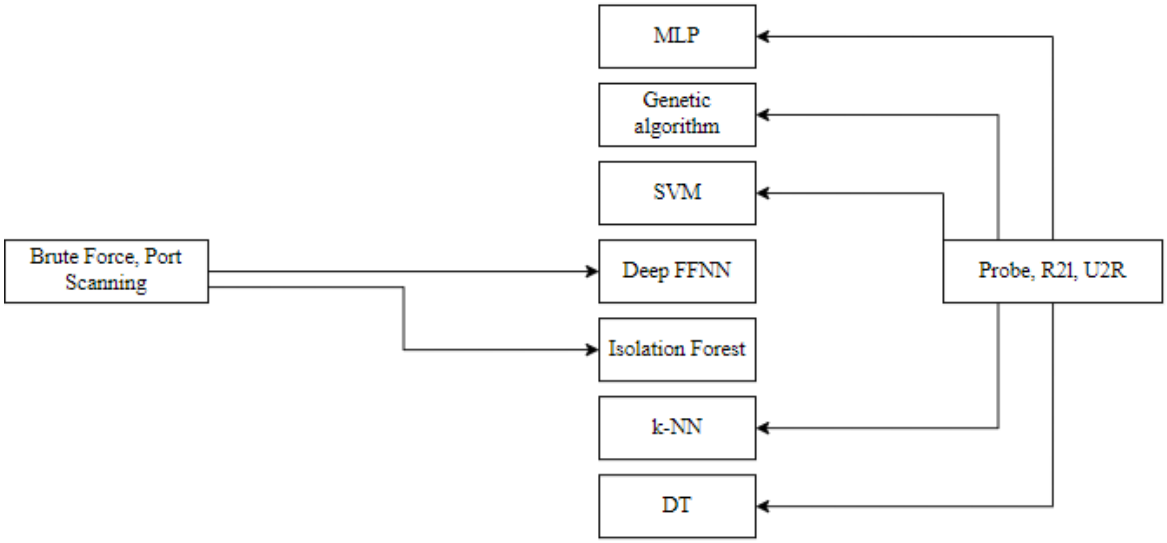

Рисунок 3.4 – Методи детектування аномальної поведінки інших відомих типів атак

Далі будуть коротко описані найбільш вживані методи IDS на основі машинного навчання для детектування вище зазначених атак на рисунку 3.5.

Multi-layer Perceptron (MLP): є одним з найбільш популярних класифікаторів загальних функцій, ефективність якого проявляється коли він

має справу з декількома областями застосування, наприклад часовий ряд, класифікаційні та регресійні проблеми та ін. Етап тестування може бути реалізований протягом короткого періоду часу. З іншого боку, фаза навчання, як правило, виконується за тривалий проміжок часу. Алгоритм MLP може бути реалізований за допомогою різних функції передачі, наприклад сигмоїдна, лінійна та гіперболічна. Кількість результатів або очікуваних класів та кількість приховані рівнів є важливими конструктивними елементами реалізації алгоритму MLP [26]. Технологія FeedForward Neural Network (FFNN) схожа за принципом MLP. Переваги цього підходу це прискорення швидкості конвергенції, а також посилювання глобального пошук [27].

Генетичний алгоритм (GA) найчастіше застосовують як надійну технологію, засновану на машинному навчанні, для проектування IDS. GA функціонує на ряді можливих рішень, використовуючи принцип виживання найсильніших, з метою створення кращих наближень для вирішення певної проблеми, з якою стикається GA [28].

Для підходу дерев ізоляції зазначимо ще раз, що зазвичай аномальними екземплярами є ті об’єкти, значення їх атрибутів сильно відрізняються від звичайних екземплярів і їх легше розділити, ніж звичайні екземпляри. У процесі ізоляції вони також знаходяться ближче до кореня і легше поділяються, ніж звичайні екземпляри. Для того, щоб полегшити ефекти, що імпортуються випадковою характеристикою в процесі побудови ізоляційних дерев, обчислюється середня глибина екземпляра в «лісі», який складається з декількох дерев ізоляції, і використовуємо середню глибину як аномальну оцінку екземпляра. Чим нижчий бал має екземпляр, тим вища ймовірність аномалії [29].

Дерева рішень можуть аналізувати дані та виявляти значущі характеристики в мережі, що вказують на зловмисну діяльність. Це може додати цінності багатьом системам безпеки в режимі реального часу шляхом

аналізу великого набору даних для виявлення вторгнень. Дерева рішень можуть розпізнавати тенденції та закономірності, які підтримують подальше розслідування, розвиток сигнатур нападу та інші види моніторингу. Головною перевагою використання дерев рішень в порівнянні з іншими класифікаційними методами полягає в тому, що вони забезпечують широкий набір правил, які легко зрозуміти, та можуть бути легко інтегровані з використанням технологій реального часу без особливих зусиль [30].

Висновки до розділу 3

Були проведений огляд різних методів виявлення аномалій, що можуть бути потенційними атаками. Було зазначено що існують певні обмеження існуючих датасетів для побудови IDS систем і їх якісної роботи моніторингу. Набори даних в більшості націлені на знаходження таких категорій атак, як DoS / DDoS, U2R, L2R, Probing. В контексті цих атак були побудовані схеми, що відповідають найбільш популярним методам детектування незвичної поведінки (в більшості – методи машинного навчання). Окремо було розглянуто DoS / DDoS атаку, як одну із атак, що може завдати невичерпної шкоди компаніям.

ВИСНОВКИ

В цій роботі було наголошено про важливість детектування аномалій в кіберпросторі, були оговорені існуючі проблеми і обмеження, з якими стискаються розробники IDS систем для забезпечення безпеки організацій, а саме:

1. Відсутність загальноприйнятої методики виявлення аномалій;

Наприклад, техніка виявлення вторгнень у дротовій мережі може бути мало корисною у бездротовій мережі.

2. Дані можуть містити шум, який, як правило, є фактичною аномалією.
3. Відсутність загальнодоступного маркованого набору даних, який буде використовуватися для виявлення аномалій мережі.

Отож, розвиток IDS систем це актуальний напрямок проведення досліджень і класифікація аномалій є змістовною в цьому контексті.

Однією з основних задач було дослідження взаємозв’язку аномалій із атаками, класифікація аномалій в аспекті джерела виникнення атаки та аналіз аномальної поведінки HTTP трафіку. Ці три пункти є основою для таксономії аномалій (ієрархічна структура класифікації в різних сторін), яка є змістовною і корисною для кіберпростору і простору інформаційної безпеки. Аналізуючи аномалії, притаманні HTTP трафіку, були згадані категорії атак, що належать OWASP top 10, а саме це різні варіації Injection (SQL-injection), наявність Broken Authentication (можливість реалізації Brute Force), тощо. Основна ціль складання таксономії аномалій – це допомога в побудові майбутніх IDS, що можуть виявити більше атак, що належать тієї и іншій категорії, а саме використання асоціації аномалій із OSI моделлю, асоціації аномалій із джерелом атак та класифікації аномалій за змістом HTTP трафіку допомагає в досягненні вищої точності та зменшення кількості помилково позитивних

спрацьовувань IDS та покращення наборів, які використовують IDS. В розрізі немережевих аномалій був розглянутий профіль нормальної активності, процес його створення і класифікація фіксування аномалій в межах прикладів груп на операційній системі Windows.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1) Top Ten Industries Under Attack [Електронний ресурс] / Режим доступу: https://www.netscout.com/blog/top-ten-industries-under-attack
2) The Global State of Information Security Survey 2015 [Електронний ресурс] //— 2015. — Режим доступу: http://www.pwc.com
3) Єфрон І.А., Брокгауз Ф.А. Енциклопедичний словник / [Електронний ресурс] // — 2015. — Режим доступу: http://fshq.ru/anz_slovar_brokgauza/slovar 239.html
4) Mohiuddin Ahmed, Abdun Naser Mahmood, Jiankun Hu. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. — 2016.
5) C. Varun, B. Arindam, K. Vipin. Anomaly Detection: A Survey [Електронний ресурс] / — 2007. — Режим доступу: https://www.researchgate.net/publication/220565847_Anomaly_Detection_A_Survey
6) On the educated selection of unsupervised algorithms via attacks and anomaly classes [Електронний ресурс] / T.Zoppi, A. Ceccarelli, L. Salani, A. Bondavalli // Journal of Information Security and Applications. – 2020. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S2214212619307975
7) A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems [Електронний ресурс] / H.Hanan, B. David, B. Ethan, S. Amar // IEEEAccess. – 2020. – Режим доступу до ресурсу: https://rke.abertay.ac.uk/ws/portalfiles/portal/23654523/Hindy_ATaxonomyOfNetworkThreatsAndTheEffectOfCurrentDatasets_Published_2020.pdf
8) Mahoney M. Learning Nonstationary Models of Normal Network Traffic for Detecting Novel Attacks [Електронний ресурс] / M. Mahoney, C. Philip //

Department of Computer Sciences Florida Institute of Technology – Режим доступу до ресурсу: https://cs.fit.edu/~mmahoney/paper4.pdf

9) Андон П. І. ПРОТИДІЯ АТАКАМ НА ВІДМОВУ В МЕРЕЖІ ІНТЕРНЕТ: КОНЦЕПЦІЯ ПІДХОДУ [Електронний ресурс] / П. І. Андон, О. П. Ігнатенко // Інститут програмних систем НАН України – Режим доступу до ресурсу: https://core.ac.uk/download/pdf/38468722.pdf
10) Ahmed M. Detecting Rare and Collective Anomalies in Network Traffic Data using Summarization [Електронний ресурс] / Mohiuddin Ahmed // School of Engineering and Information Technology The University of New South Wales Australia. – 2016. – Режим доступу до ресурсу: http://unsworks.unsw.edu.au/fapi/datastream/unsworks:42253/SOURCE02?view=true
11) Malware & Exploit Attacks Explained [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://newtecservices.ie/malware-exploit-attacks-explained/
12) Модель реагування на мережеві атаки. Модель мережевої безпеки. Класифікація мережевих атак. Відмова в обслуговуванні [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://remzhuk.ru/uk/model-reagirovaniya-na-setevye-ataki-model-setevoi/
13) Кожевникова, И. С. Анализ методов обнаружения аномалий для обнаружения сканирования портов / И. С. Кожевникова. // Молодой ученый. [Електронний ресурс]. — 2017. — № 14 (148). — С. 31-34. — Режим доступу до ресурсу: https://moluch.ru/archive/148/41829/
14) R. Fielding, J. Gettys, J. Mogul et al., “Hypertext transfer protocol--HTTP/1.1,” No. RFC 2616, 1999
15) F. Callegati, W. Cerroni, and M. Ramilli, “Man-in-the-Middle Attack to the HTTPS Protocol,” IEEE Security & Privacy, vol. 7, no. 1, pp. 78–81, 2009

16) Agarwal N. A Closer Look at Intrusion Detection System for Web Applications [Електронний ресурс] / Nancy Agarwal // Security and Communication Networks. – 2018. – Режим доступу до ресурсу: https://www.hindawi.com/journals/scn/2018/9601357/

17) Białczak P. Characterizing Anomalies in Malware-Generated HTTP Traffic [Електронний ресурс] / Piotr Białczak // Security and Communication Networks. – 2020. – Режим доступу до ресурсу: https://www.hindawi.com/journals/scn/2020/8848863/#sec6.1

18) Manners D. The User Agent Field: Analyzing and Detecting the Abnormal or Malicious in your Organization [Електронний ресурс] / Darren Manners // SANS Institute Information Security Reading Room. – 2021. – Режим доступу до ресурсу: https://www.sans.org/reading-room/whitepapers/malicious/user-agent-field-analyzing-detecting-abnormal-malicious-organization-33874

19) Banach Z. Understanding Cookie Poisoning Attacks [Електронний ресурс] / Zbigniew Banach. – 2021. – Режим доступу до ресурсу: https://www.netsparker.com/blog/web-security/understanding-cookie-poisoning-attacks/

20) Sarokaari N. How to identify malicious HTTP Requests [Електронний ресурс] / Niklas Sarokaari // SANS Institute Information Security Reading Room. – 2021. – Режим доступу до ресурсу: https://www.sans.org/reading-room/whitepapers/detection/identify-malicious-http-requests-34067

21) Siemons F. SQL Injection Analysis [Електронний ресурс] / Frank Siemons // Infosec. – 2016. – Режим доступу до ресурсу: https://resources.infosecinstitute.com/topic/sql-injection-analysis/

22) Montoro R. HTTP Header Hunter - Looking for malicious behavior into your http header traffic [Електронний ресурс] / Rodrigo Montoro – Режим доступу до ресурсу: http://2011.video.sector.ca/video/39786962

23) Anomaly-Based Network Intrusion Detection Using Machine Learning [Електронний ресурс] // — 2020. — Режим доступу: https://tel.archives-ouvertes.fr/tel-02988296/document

24) Mohiuddin Ahmed, Abdun Naser Mahmood, Jiankun Hu. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. — 2016.

25) Alkahtani H. Adaptive Anomaly Detection Framework Model Objects in Cyberspace [Електронний ресурс] / Hasan Alkahtani. – 2020. – Режим доступу до ресурсу: https://www.researchgate.net/publication/347816570_Adaptive_Anomaly_Detection_Framework_Model_Objects_in_Cyberspace

26) Almseidin M. Evaluation of Machine Learning Algorithms for Intrusion Detection System [Електронний ресурс] / M. Almseidin, A. Maen, S. Kovac – Режим доступу до ресурсу: https://arxiv.org/ftp/arxiv/papers/1801/1801.02330.pdf

27) GA-FFNN: An Intelligent Classification Approach for Signature-based IDS [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://medium.com/swlh/ga-ffnn-an-intelligent-classification-approach-for-signature-based-ids-b18a8dd2158d

28) Improving Intrusion Detection Using Genetic Algorithm [Електронний ресурс] – Режим доступу до ресурсу: https://scialert.net/fulltext/?doi=itj.2013.2167.2173#:~:text=Genetic%20Algorithm%20(GA)%20is%20most,machine%20learning%20for%20designing%20IDS.&text=GA%20functions%20on%20a%20number,particular%20problem%20GA%20is%20facing.

29) Ding Z. An Anomaly Detection Approach Based on Isolation Forest Algorithm for Streaming Data using Sliding Window [Електронний ресурс] / Zhiguo Ding // IFAC Proceedings Volumes. – 2013. – Режим доступу до

ресурсу: https://www.sciencedirect.com/science/article/pii/S1474667016314999

30) Decision Tree Based Algorithm for Intrusion Detection [Електронний ресурс] // 2016 – Режим доступу до ресурсу: https://www.researchgate.net/publication/318673949_Decision_Tree_Based_Algorithm_for_Intrusion_Detection