Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Метод оцінки ефективності систем захисту та виявлення несанкціонованого доступу в інформаційних системах
Назва теми

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Комп'ютерна інженерія

КвРКІ. 180296.21.01.01 ПЗ

Виконав: студент 2 курсу, група КІ1м-21-1 _____ Блаута В.В.
Підпис

Керівник к. т. н, доцент кафедри Кб _____ Кльоц Ю.П.
Підпис

Нормоконтролер ст. викладач кафедри Кб _____ Мостовий С.В.
Підпис

До захисту допускаю:
Зав. кафедри Кб, к.т.н., доцент _____ Кльоц Ю.П.
Підпис

7. 12. 2022 р.

Хмельницький, 2022

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КАФЕДРА КІБЕРБЕЗПЕКИ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ПРОГРАМУВАННЯ ТА ЗАХИСТ КОМП`ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ЗАТВЕРДЖУЮ

Зав. кафедри __Ю.П.Кльоц___

_____

"_____" _____2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Блауті Вадиму Віталієвичу

Прізвище, ім'я, по батькові студента

1. Тема роботи Метод оцінки ефективності систем захисту та виявлення несанкціонованого доступу в інформаційних системах

Керівник роботи_____Кльоц Ю.П. кандидат технічних наук, доцент_____

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом № 102 ректора університету додаток №23 від 25.08.2021

2. Строк подання студентом проекту (роботи) на кафедру 20.11.2022

3. Вихідні дані до проекту (роботи) вторгнення в інформаційні системи, методи та засоби виявлення вторгнень, оцінка ефективності_____

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)_____

Вступ. Моніторинг та аналіз сучасних інформаційних систем. Методи і засоби виявлення вторгнень в інформаційну систему. Системи та методи виявлення вторгень в інформаційну систему. Вибір систем виявлення вторгнень на основі аналізу ефективності методів виявлення, що лежать в їх основі. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Загальна характеристика магістерської роботи. Дослідження засобів та методів виявлення вторгнень. Модель корпоративної мережі. Основні положення методу. Алгоритмічна реалізація методу. Апробація методу – вхідні дані. Апробація методу - результати моделювання. Висновки.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завданн
Нормоконтроль	Мостовий С..В. ст. викл. кафедри КБ		

7. Дата видачі завдання «_2_» _____вересня_____ 2022р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи
1	Вибір напряму дослідження та узгодження тематики КРМ з керівником	2.02.2022
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	2.03.2022
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	1.04.2022
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	1.05.2022
5	Робота над науковою публікацією	1.06.2022
6	Уточнення і затвердження теми	1.09.2022
7	Робота над розділом 3 – розробка методу та алгоритмів, їх аналіз	2.09.2022
8	Робота над розділом 4 – апробація запропонованих рішень	1.10.2022
9	Узгодження отриманих результатів; оформлення пояснювальної записки згідно вимог	1.11.2022
10	Оформлення графічної частини	8.11.2022
11	Попередній захист роботи	10.11.2022
12	Захист роботи на засіданні ЕК	8.12.2022

Студент _____ Блаута В.В.
Підпис Ініціали, прізвище

Керівник роботи _____ Кльоц Ю.Г.
Підпис Ініціали, прізвище

чітко визначено об'єкт, предмет та методи

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод оцінки ефективності систем захисту та виявлення несанкціонованого доступу в інформаційних системах

Автор роботи: Блаута Вадим Віталійович

Керівник роботи: к.т.н., доцент Кльоц Ю.П.

Загальний обсяг роботи: 90 сторінок, 17 рисунків, 3 таблиці, 2 додатки, 25 посилань.

ІНФОРМАЦІЙНІ СИСТЕМИ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Метою кваліфікаційної роботи є розроблення методу оцінки ефективності систем захисту та виявлення несанкціонованого доступу та відповідних рекомендацій по вибору таких засобів для підвищення надійності та безпеки функціонування інформаційних систем.

Дана кваліфікаційна робота присвячена питанням аналізу ефективності систем виявлення несанкціонованого доступу та захисту інформаційних систем, розробці відповідного методу та системи. Розроблена система дозволяє виявляти несанкціоноване вторгнення за сигнатурою та за поведінкою, що підвищує надійність функціонування інформаційних систем

ANNOTATION

a qualification work of Blauta Vadym

entitled «Method of evaluating the efficiency of protection systems and detecting unauthorized access in information systems».

Mentor: Ph.D., associate professor Klyots Yurii

Total volume of work: 90 pages, 17 figures, 3 tables, 2 appendices, 25 references.

INFORMATION SYSTEMS, UNAUTHORIZED ACCESS, DETECTION OF INTRUSIONS IN INFORMATION SYSTEMS

The purpose of the qualification work is to develop a method for evaluating the effectiveness of protection systems and detecting unauthorized access and relevant recommendations for choosing such tools to increase the reliability and security of the functioning of information systems.

This qualification work is devoted to the issues of analyzing the effectiveness of systems for detecting unauthorized access and protecting information systems, developing the appropriate method and system. The developed system allows detection of unauthorized intrusion by signature and behavior, which increases the reliability of the functioning of information systems

ЗМІСТ

ВСТУП

Актуальність дослідження.

На сьогодні мережі передачі даних та інформаційно-комунікаційні виступають основою розвитку інформаційного суспільства. Адже саме вони здійснюють передачу, зберігання та обробку інформації. Тому важливим атрибутом функціонування сучасних інформаційно-комунікаційних систем та мереж (ІКСМ) з точки зору по забезпеченню цілісності, конфіденційності та доступності інформаційних ресурсів є захист інформації від несанкціонованого доступу (НСД). Під захистом інформаційного об'єкту розуміється регулярне використання засобів і методів, вживання заходів і здійснення заходів з метою забезпечення комплексної безпеки інформації з метою забезпечення базових властивостей інформаційних ресурсів. На сьогодні розгалужені інформаційні мережі функціонують під керуванням різних операційних систем, на перше місце виходить завдання керування всім розмаїттям захисних механізмів. Базовим підходом до вирішення цієї проблеми є використання систем та методів виявлення НСД. Застосування даних методів та систем унеможливить НСД та зловживання інформаційними ресурсами в сучасних ІКСМ

Мета кваліфікаційної роботи полягає в розробленні методу оцінки ефективності систем захисту та виявлення несанкціонованого доступу та відповідних рекомендацій по вибору таких засобів для підвищення надійності та безпеки функціонування інформаційних систем.

Для досягнення мети роботи необхідно вирішити наступні завдання:

1) провести аналіз інформаційних систем та потоків даних, що в них містяться;

2) провести аналіз найбільш поширених методів та засобів виявлення несанкціонованого доступу до ІС;

3) розробити метод оцінки ефективності систем захисту;

4) реалізувати захист ІС та дослідити його ефективність.

Об'єктом дослідження виступають інформаційні системи та інформаційні потоки в них.

Предметом дослідження є оцінка ефективності методів та засобиів виявлення вторгнень в інформаційні системи

Методи дослідження. Для розв’язання поставлених задач використовуються основні положення методів аналізу даних, імітаційного комп’ютерного моделювання трафіку, математичної статистики..

Наукова новизна одержаних результатів.

У результаті дослідження розв'язано актуальну науково-практичну задачу розроблення методу оцінки ефективності систем захисту та виявлення несанкціонованого в ІС. При цьому одержано такі наукові результати:

1) Проведено аналіз сучасних систем виявлення вторгнень в інформаційних системах. Встановлено, що вони використовують сигнатурний аналіз трафіку.

2) Визначено критерії оцінки ефективності методів та систем захисту від несакціонованого доступу.

3) Розроблено метод оцінки ефективності засобів захисту та на його основі запопоновано вибір таких засобів для інформаційних сивтем.

Апробація роботи. Наукові результати і основні положення кваліфікаційної роботи магістра доповідались і обговорювались на всеукраїнській і міжнародній науково-практичних конференціях.

Публікації. За темою кваліфікаційної роботи опубліковано 1 тези у збірнику наукових праць студентської конференції Університету економіки і підприємництва, 1-2 грудня 2022.

1 АНАЛІЗ ЕВОЛЮЦІЇ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНІ СИСТЕМИ

1.1 Огляд історії розвитку систем виявлення вторгнень

Уявіть, що перед вашим будинком зупинилася дивна людина. Вона обернулася, уважно оглянула околиці, а потім підійшла до дверей і повернула ручку. Двері виявилися замкненими. Вона підійшла до найближчого вікна і спробувала обережно його відкрити. Вікно теж було закрито. Мабуть, ваш будинок в безпеці. Так навіщо ж встановлювати сигналізацію?

Схожі питання часто задають захисникам технології виявлення вторгнень. Навіщо морочити собі голову виявленням вторгнень, якщо вже є міжмережеві екрани, «латки» для операційних систем вчасно встановлюються, і системні адміністратори стежать за тим, щоб у користувачів були розумні паролі? Відповідь дуже проста: тому що в системи як і раніше проникають зловмисники. Точно так же, як іноді люди забувають закрити в будинку вікно, вони забувають коректним чином оновити набір правил на міжмережевому екрані.

Навіть з найдосконалішим захистом комп'ютерні системи не можна назвати абсолютно невразливими. Більшість експертів з комп'ютерної безпеки погоджуються з тим, що створити абсолютно захищену систему ніколи не вдасться. Тому таким актуальним залишається завдання створення методів виявлення вторгнень і систем для виявлення та реагування на комп'ютерні атаки.

Спочатку системні адміністратори виявляли вторгнення, сидячи перед консоллю і аналізуючи дії користувачів. Вони могли помітити атаку, звернувши, наприклад, увагу на те, що користувач, який повинен знаходиться у відпустці, увійшов в систему, причому локально, або надзвичайно активний принтер, який вкрай рідко використовується. Колись, досить ефективна, ця форма виявлення вторгнень була суто орієнтована на конкретні ситуації і не

володіла масштабністю.

На наступному етапі для виявлення вторгнень стали використовуватися журнали реєстрації, які системні адміністратори переглядали в пошуках ознак незвичайних або зловмисних дій. В кінці 70-х і на початку 80-х років адміністратори, як правило, друкували журнали реєстрації на перфорованому папері, які до кінця робочого тижня представляли собою купу висотою в півтора-два метри. Пошук по такому лістингу, безумовно, займав багато часу. При величезній кількості інформації і виключно ручних методах аналізу, адміністратори часто використовували журнали реєстрації як доказ порушення захисту вже після того, як воно сталося. Надія на те, що вдасться виявити атаку в момент її проведення, була вкрай мала.

У міру того, як дискова пам'ять ставала все дешевше, журнали реєстрації стали створювати в електронному вигляді; з'явилися програмні засоби для аналізу зібраних даних. Однак подібний аналіз виконувався дуже повільно і часто вимагав значних обчислювальних ресурсів, так що, як правило, програми виявлення вторгнень запускалися в пакетному режимі, ночами, коли з системою працювало мало користувачів. Більшість порушень захисту як і раніше виявлялися вже постфактум.

На початку 90-х років були розроблені системи виявлення вторгнень в оперативному режимі, які переглядали записи в журналі реєстрації відразу, як тільки вони генерувалися. Це дозволило виявляти атаки і спроби атак в момент їх проведення, що, в свою чергу, дало можливість негайно вживати відповідних заходів, а, в деяких випадках, навіть попереджати атаки.

Найостанніші проекти, присвячені виявленню вторгнень, зосереджуються навколо створення інструментів, які можуть ефективно розвиватися у великих мережах. Це завдання аж ніяк не просте, враховуючи дедалі більшу увагу, яку приділяють питанням безпеки, незліченна кількість нових методів організації атак і безперервні зміни в навколишньому обчислювальному середовищі[1].

1.2 Етапи розвитку СВВ

1.2.1 Початковий період - перші системи

Згідно [2] перші системи виявлення атак призначалися для пошуку проблемних місць в системі захисту і попередження адміністраторів про спроби хакерів скористатися наявністю «дірок» або зробити атаки по типу «відмова в обслуговуванні» (DoS). Зі своєю роботою вони справлялися дуже непогано, але в цьому були свої плюси і мінуси.

У повній відповідності з обіцянками розробників, системи виявлення вторгнень першого покоління давали уявлення про трафік в окремих сегментах мережі і про всі нетипові прояви на підставі аналізу журнальних файлів на хості. Така інформація дозволяла визначити, чи піддавався захист мережі атакам хакерів для отримання доступу до критично важливих мережевих ресурсів. Ці системи встановлювалися в ключових вузлах мережі на рівні міжмережевих екранів, комутаторів, маршрутизаторів, серверів Web, баз даних та інших обслуговуючих пристроїв всередині підприємства. Однак ранні системи виявлення вторгнень видавали велику кількість повідомлень і таким чином породжували величезні обсяги інформації про проходження трафіку через мережу і через системи хоста, нерідко посилаючи помилкові сигнали тривоги, причому в неймовірній кількості. У свою чергу, будучи не в змозі систематизувати і зрозуміти всю цю громаду даних, багато системних адміністраторів просто зводили до мінімуму функції таких систем, а то і зовсім їх відключали.

1.2.2 Другий етап - перехідний період

На думку фахівців з безпеки, колишня концепція побудови системи виявлення атак в значній мірі є збитковою. Для тих, хто дійсно зацікавлений у захисті своїх мережевих ресурсів, сучасний ринок пропонує більш досконалі засоби.

Виробники, наприклад, мають в своєму арсеналі нові розвинені способи виявлення вторгнень, більш ефективні, ніж метод пошуку підозрілого шаблону, званий також методом зіставлення сигнатур найбільш частих типів атак. Реалізований в ранніх системах виявлення атак, саме він був причиною великої кількості помилкових сигналів тривоги.

Крім того, постачальники збільшили продуктивність своїх пристроїв в розрахунку на мережі з пропускною спроможністю 100 Мбіт/с. В даний час вони пропонують більш прості в розгортанні та управлінні спеціалізовані пристрої з IDS, а також почали поставку систем виявлення атак, що поєднують в собі кращі властивості двох основних типів IDS.

Як зауважують в [2], кількість атак на мережеві додатки неухильно зростає. У цій плутанині, для того щоб «загнати хижака в кут», системним адміністраторам необхідно взяти на озброєння різноманітні засоби безпеки, включаючи системи виявлення атак.

Наприклад, некомерційний координаційний центр CERT в 1999 р. отримав повідомлення про 9859 інцидентах, пов'язаних з порушенням безпеки. Це більш ніж в два рази перевищує число інцидентів, зареєстрованих в 1998 р. (яке становить 3734), і майже в п'ять разів перевершує аналогічний показник 1997 року (2134 випадки).

У червні 2001 р CERT повідомив про збільшення кількості спроб вторгнення з використанням програми SubSeven, різновиди «троянського коня», яку хакери намагаються інсталювати на комп'ютерах користувачів для отримання повного контролю над ресурсами системи. CERT пояснює: «Дії SubSeven Trojan Horse нагадують нового «хробака», який здійснює пошук систем, що раніше піддавалися атакам та на які була інстальована SubSeven».

У січні 2001 р. федеральний урядовий центр по захисту національної інфраструктури (National Infrastructure Protection Center, NIPC) попередив про подібну загрозу з боку «хробака» w32-Leaves.worm, основна мета якого - добитися повного контролю з віддаленого комп'ютера над ресурсами зараженої системи, зазвичай за допомогою каналів IRC (Internet Relay Chat).

Однак, за даними організацій, що займаються питаннями безпеки,

найсерйознішою загрозою, що виходить від спільноти хакерів, стали атаки по типу «відмова в обслуговуванні» (DoS) або розподілені атаки по типу «відмова в обслуговуванні» (DDoS), число і різноманітність яких зростає не по днях, а по годинах. За твердженням NIPC, подібні атаки націлені насамперед на пристрої та мережі з виходом в Internet і особливо сайти електронної торгівлі. Розрахунок робиться на виведення з ладу пристрою або мережі за рахунок перевантаженості її трафіком в такій мірі, щоб зовнішні користувачі не могли отримати доступ до цих ресурсів, причому атаки проходять без грубого злому файлів з паролями або крадіжки важливої інформації.

У березні 2001 р. NIPC приступив до вивчення ряду спланованих атак хакерів, зроблених з метою завдати шкоди сайтам електронної торгівлі або інтерактивним банківським сайтам. За інформацією NIPC, 40 компаній з 20 штатів стали жертвами подібних атак, зроблених організованими групами зі Східної Європи (особливо з Росії та України), які використовували лазівки на серверах з встановленими без латок версіями операційних систем Microsoft Windows NT. Отримавши доступ, ця публіка скачувала найрізноманітнішу інформацію приватного характеру - в основному бази даних замовників, а також інформацію про кредитні картки. Зломщики не використали отримані відомості в корисливих цілях, оскільки не мали наміру здійснювати покупки за вкраденими кредитками. Однак їх дії цілком можна класифікувати як приховане вимагання: вони пропонували платні послуги з виправлення систем з невстановленими оновленнями.

1.2.3 Третій етап

На думку Еріка Хеммендінгера, керівника науково-дослідних робіт в області інформаційної безпеки з компанії Aberdeen Group, прийшов час знову звернутися до систем виявлення атак, навіть якщо перший досвід роботи з ними був невдалий. Та й дослідження обсягу цього ринку свідчить про те, що в найближчі роки попит на них буде тільки збільшуватися.

Аналітична компанія Frost & Sullivan, наприклад, прогнозує зростання обсягу продажів цих систем з 62,3 млн доларів в 1999 р до 264,4 млн доларів у 2001 році та до 436,1 млн доларів у 2002 р. Інша аналітична компанія, IDC, малює ще більш вражаючу картину, пророкуючи збільшення продажів систем IDS з 350 млн доларів в 2001 році до 443,5 млн доларів у 2002 р.

Хеммендінгер вважає [2], що повернення системи виявлення атак на передові позиції в чималому ступені пов'язано з останніми розробками: появою спеціалізованих пристроїв, нових методів виявлення вторгнень, вдосконалених засобів управління. Крім того, при гібридному підході моніторинг хостів і мережі здійснюється з однієї консолі. Нарешті, ці сучасні системи можуть справлятися з трафіком високошвидкісних мереж.

Серед компаній-постачальників IDS можна назвати вже непогано зарекомендували себе в цій сфері Cisco Systems, Internet Security Systems (ISS), Intrusion.com, NFR Security, Symantec, а також нещодавно вийшли на цей ринок CyberSafe, Entercept Security Technologies і Enterasys Network.

Американський ринок буквально заполонили численні провайдери керованих послуг захисту (Managed Security Services Provider, MSSP), що пропонують аутсорсинг послуг виявлення вторгнень. Серед них Activis, Exodus Communications, OneSecure, NetSolve, RedSiren Technologies, Riptech і Ubizen.

1.2.4 Четвертий етап - дослідження аномалій

Як уже зазначалося в [2], нові розробки, що визначають розвиток ринку IDS, являють собою вдосконалені засоби спостереження і захисту від небажаних атак, будь то вторгнення в мережу або атаки по типу DoS/DDoS. Безсумнівно, однією з найбільш перспективних є методика виявлення аномальної поведінки мережі, яку все ширше використовують постачальники систем виявлення атак на мережу.

Традиційна система виявлення атак на мережу розпізнає трафік зловмисника шляхом зіставлення його з шаблонами з визначеного набору, а

сама процедура називається «перевіркою сигнатур». Ці системи працюють на зразок пакету антивірусних програм, намагаючись встановити відповідність кожного з надійшовших в мережу пакетів сигнатурам відомих атак, і ефективно відшукують вже відомі сигнатури.

З іншого боку, переваги систем виявлення атак, де застосовується метод пошуку сигнатур, зменшують два принципових недоліки. По-перше, вони не змозі проникнути у вміст зашифрованих пакетів, а тому такі атаки стають невидимими для системи. По-друге, хакери часто видозмінюють сценарій цих атак, після чого перевірка сигнатур втрачає будь-який сенс. Подібно до того, як антивірусний пакет беззахисний перед новим вірусом, поки постачальники не встановлять латки на своє програмне забезпечення, так і розробники системи виявлення вторгнень повинні регулярно оновлювати свої бази даних з сигнатурами. «... І ще невідомо, чи багато хто з них це усвідомлюють», - розмірковує Хеммендінгер.

Система IDS на основі методу виявлення аномалій проводить обстеження пакетів для класифікації та відстеження подій у мережі, щоб встановити відмінності між типовою і нетиповою її поведінкою. Детектори аномальної поведінки аналізують передачу даних між пристроями IP і відрізняють нормальний трафік від підозрілого без будь-якого зіставлення сигнатур.

Як зауважив Чад Робінсон, провідний аналітик в галузі наукових розробок компанії Robert Fransis Group, ці пристрої не піклуються про зміст даних, що передаються по мережі (на відміну від перевірки сигнатур). «Їх цікавить тільки те, як проходив сеанс в мережі, де було встановлено з'єднання, в який час і як швидко. Іншими словами, чи не було за одним підозрілим з'єднанням з будь-яким хостом аналогічного з'єднання з іншим хостом», - пояснює він.

Чак Колоджей, менеджер з питань безпеки Internet компанії IDC, підкреслює, що при налаштуванні системи виявлення аномалій вибір точки відліку набуває визначального значення. На його думку, головна складність полягає в тому, «який трафік прийняти за нормальний, а вже потім визначити відхилення від норми зовсім не складно». Колоджей і інші фахівці вважають,

що метод пошуку сигнатур слід використовувати в поєднанні з методом виявлення аномалій. «Метод аномалій можна порівняти з пошуком сигнатур, і, якщо в процесі неодноразового зняття показань відхилення не виявилося, можна вважати, що аномалія відсутня», - міркує він.

Рішення для аналізу аномальної поведінки мережі постачають такі компанії, як Cisco Systems, Enterasys Networks, Lancope, Intrusion.com, ISS і Resourse Technologies. Район Пакер, віце-президент з розвитку бізнесу в компанії Intrusion.com, заявляє, що продукт SecureNet, що випускається його компанією, - лідер в цій області. Ця система здатна розшифровувати 26 протоколів, включаючи протоколи стека TCP/IP, а також ftp, IRC, NetBIOS, Network News Transfer Protocol (NNTP), POP3, Finger, Rlogin, Remote Procedure Call (RPC), SMTP і Trivial File Transfer Protocol (TFTP).

1.2.5 Пятий етап - підвишення швидкості

В даний час більшість пропонованих систем виявлення атак орієнтується на мережі Ethernet з пропускною спроможністю 100 Мбіт/с. У разі більшої пропускної здатності такі системи не можуть простежити за всіма пакетами в мережі і стають менш ефективними. Коли ж постачальники рішень пропонують використовувати свої системи IDS для мереж з пропускною спроможністю понад 100 Мбіт/с, то, за словами Колоджи, їх продуктам вдається перевіряти лише частину пакетів. «Разом з тим, зустрічаються системи, які взагалі не в змозі працювати в мережах на 100 Мбіт/с», - підкреслює Хеммендінгер.

Колоджи зазначає, що два виробника систем IDS - ISS і Intrusion.com - орієнтуються на гігабітні швидкості. Компанії Cisco і Enterasys стверджують, що їх системи виявлення атак можуть працювати в мережах із пропускною здатністю 100 Мбіт/с.

Ще одна компанія, Top Layer Networks, використовує незвичайний підхід для управління процедурою виявлення вторгнень у високошвидкісних мережевих середовищах. Її система виявлення атак AppSafe 3500 застосовує

процедуру відзеркалювання потоків для копіювання всіх пакетів на конкретний порт AS 3500. Потім кожен порт розподіляє весь потік між окремими системами виявлення атак, підключеними до AS 3500.

Марк Рой, заступник директора з маркетингу компанії Top Layer, стверджує, що його продукт виконує загальний аналіз високошвидкісного гігабітного трафіку і допомагає мережевим адміністраторам скласти політику захисту щодо певних видів трафіку, причому останній може бути спрямований на систему виявлення атак і на міжмережевий екран одночасно. Він бачить в цьому дві безперечні переваги.

По-перше, навантаження стає можливим розподілити між кількома системами IDS - наприклад, направити гігабітний потік на чотири різні системи IDS. В цьому випадку вирішується проблема змінених атак і заторів в мережі під час перевантаження.

По-друге, даний продукт дуже ефективний для припинення атак по типу «відмова в обслуговуванні». «Ми можемо справлятися з 14 найбільш популярними видами атак DoS на рівні пакетів, намагаючись визначити мотиви і спосіб взаємодії між клієнтом і сервером - і таким чином розпізнавати активність, що викликає підозру», - говорить Рой[2].

1.2.6 Шостий етап - апаратні реалізації

Апаратна реалізація системи виявлення вторгнень на мережу - новий етап розвитку засобів забезпечення мережевої безпеки. Раніше програмне забезпечення для моніторингу вторгнень на ПК потрібно було встановити і сконфігурувати. Тепер же пропонуються пристрої, що являють собою програмно-апаратний модуль із заданою конфігурацією.

Система безпеки NetRanger виробництва компанії Cisco була в числі перших подібних пристроїв, і Колоджи з IDC вважає, що з таким продуктом компанія Cisco стане лідером в цій області. Компанії ISS, Intrusion.com і NFR Security також працюють в цьому напрямку.

Новий підхід визначений [2], цікавий з кількох причин. Перш за все, він усуває багато проблем, пов'язаних з інсталяцією і експлуатацією програмних засобів IDS на універсальних комп'ютерах. «Постачальники програмного забезпечення IDS не можуть оптимізувати ці системи для кожного процесора і під кожну версію операційної системи», - стверджує Колоджей.

Апаратна реалізація - це контрольована середа, організована у відповідності зі специфікаціями постачальника, тому програмна частина системи виявлення атак може бути налаштована спеціально для даного застосування. Крім того, вона позбавляє від турбот, пов'язаних з операційною системою, особливо в організаціях, що працюють тільки на платформі Wintel або UNIX.

Нарешті, апаратно реалізовані системи виявлення атак надають підрозділам IT, а також провайдерам послуг стандартні можливості «підключай і працюй» (plug-and-play). Це особливо важливо при розгортанні таких систем у віддалених офісах, де кінцеві користувачі, які не мають великого досвіду, можуть власноруч встановити фізичні з'єднання, залишаючи турботу про налаштування та конфігурації на персонал IT.

1.2.7 Сучасний етап

Постачальники систем IDS пропонують інтегровані рішення, об'єднавши в єдиній платформі управління переваги систем виявлення атак на хост і на мережу. В такому середовищі для отримання дійсної картини активності мережі консоль управління взаємодіє із засобами аналізу трафіку і журнальними файлами, реалізованими в системах виявлення атак на мережу і на хост.

Рон Гула, віце-президент компанії Enterasys по системам IDS, нагадує, що отримання корелюючих даних з опитуваних мережевих пристроїв знижує ймовірність помилки і дозволяє персоналу, відповідального за мережеву безпеку, відстежувати трафік на більш високому рівні. Наприклад, факт

одноразового сканування порту 80 на сервері Web через єдиний маршрутизатор, швидше за все, не привід говорити про здійснювану атаку, але виявлення численних спроб сканувань через кілька маршрутизаторів дозволить стверджувати це з упевненістю.

На думку Гула [2], система для корпоративних мереж Enterasys вельми приваблива для провайдерів керованих послуг безпеки (Managed Security Service Provider, MSSP), коли їм необхідний моніторинг систем виявлення вторгнень не тільки в мережі постачальника, але і в численних мережах замовників. Серед клієнтів Enterasys він називає такі компанії, як RipTech, OneSecure і TrustWave.

1.3 Висновки

Підсумовуючи можна сказати, що хоча за останні роки технологія виявлення вторгнень розвивалася дуже швидко, багато важливих питань досі залишаються відкритими. По-перше, системи виявлення повинні стати більш ефективними, навчившись виявляти широкий діапазон атак з мінімальною кількістю помилкових тривог. По-друге, методи виявлення вторгнень повинні розвиватися з урахуванням зростання розміру, швидкості і динамізму сучасних мереж. Нарешті, необхідні методи аналізу, які підтримують ідентифікацію атак, спрямованих проти мереж в цілому. Навіть в міру того, як захист мереж стає все надійніше, виявлення вторгнень завжди залишиться невід'ємною частиною будь-якої серйозної системи безпеки.

2 МЕТОДИ І ЗАСОБИ ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ

2.1 Поняття системи виявлення вторгнань

Ні для кого не секрет, що кількість направлених на проникнення атак збільшується з кожним днем. Здебільшого це пов'язано не з появою на ринку праці значної кількості ІБ-фахівців, а скоріше з широким проникненням ІТ в наше життя. Зараз кожен більш-менш умілий школяр має уявлення про роботу глобальної мережі, а інструментів для злому інформаційних систем стає все більше. Більш того, багато з них абсолютно безкоштовні і не вимагають від власника навичок використання і глибоких знань. Людей, бездумно використовуючих ці інструменти, так і називають - скрипт-кідді (script kiddie). Ви можете заперечити, що на сторожі мережі завжди встановлено фаєрвол, але будемо чесними: ця система захисту даних, як і всі інші, не позбавлена недоліків і самостійно не може гарантувати повного захисту.

Давайте проведемо паралель із реальним життям. Уявіть собі, що ви купили нову квартиру. І природньо, ви не захочете перевозити туди меблі, що дісталася вам ще від бабусі. Разом з новими меблями ви, як і кожен поважаючий себе ІТ-професіонал, поставите на самому видному місці свій новий комп'ютер, ціна якого дорівнює вашому заробітку за останні кілька місяців. Облаштувавши нове житло, ви захочете його убезпечити і, звичайно ж, замовите найнадійніші двері. В даному прикладі вони і уособлюють фаєрвол. Але одного разу, повернувшись з роботи, ви виявили, що злодії проникли в квартиру через вікно і винесли все, включаючи новий комп'ютер. Ви навіть не могли собі уявити такий розвиток подій, адже ваші апартаменти знаходяться на шістнадцятому поверсі. Так само трапляється і в ІТ. Ваша мережа завжди знаходиться під загрозою. Зловмисники, як і ви, регулярно переглядають бази даних уразливостей і шукають шляхи проникнення в вашу мережу. Іноді ці шляхи можуть бути настільки непередбачуваними, що ви просто не можете собі

такого уявити. У цьому прикладі IDS можна порівняти з сигналізацією. Звичайно, вона не зможе гарантувати стовідсоткового захисту, однак дозволить істотно мінімізувати ризики і можливі збитки[3].

Отже, ми підходимо до головного - що ж являє собою IDS в світі IT?

Система виявлення атак (вторгнень) (англ. Intrusion Detection System, IDS) — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет. Про будь-яку активність шкідливого ПЗ або про порушення типової роботи централізовано збирається інформація SIEM-системою (англ. Security information and event management). SIEM-система обробляє дані отримані від багатьох джерел і використовує методи фільтрування тривог для розрізнення несанкціонованої активності від хибного спрацювання тривоги. Про що оповіщається або адміністратор або операційний центр безпеки[4].

Хоча й IDS, і мережевий екран відносяться до засобів забезпечення інформаційної безпеки, мережевий екран відрізняється тим, що обмежує надходження на хост або підмережу певних видів трафіку для запобігання вторгнень і не відслідковує вторгнення, які відбуваються всередині мережі. IDS, навпаки, пропускає трафік, аналізуючи його і сигналізуючи при виявленні підозрілої активності. Виявлення порушення безпеки проводиться звичайно з використанням евристичних правил та аналізу сигнатур відомих комп'ютерних атак. Система яка розриває з'єднання називається системою запобігання вторгненням (англ. Intrusion Prevention System, IPS) і є однією з видів мережевого екрану на рівні застосунку.

Системи виявлення вторгнень дозволяють виявляти атаки і запобігають їх подальшому розвитку. Кінцевий результат досягається завдяки збору та аналізу даних з різних джерел. Ефективна робота IDS забезпечується завдяки таким технологіям:

- Моніторинг і аналіз активності користувачів і систем. Зазвичай здійснюється шляхом відповідності потоків даних певного набору правил. Використовувані в IDS правила являють собою опис найбільш популярних

векторів атак. Однак навіть невелика зміна в ході проведення атаки дозволяє зловмисникові обійти даний фільтр.

- Перевірка конфігурацій і пошук уразливості ІС.

- Перевірка цілісності критичних даних.

- Статистичний аналіз потоків даних, заснований на математичних моделях відомих атак. Для них не важлива послідовність подій, що ускладнює обхід такої системи. Однак зловмисники можуть навчити такі системи сприймати шкідливий трафік як нормальний.

- Визначення підозрілих дій.

- Використання нейронних мереж для виявлення атак. Дозволяє позбутися недоліків статистичних методів і статичних правил. Зазвичай спочатку нейронні мережі навчають розпізнавати саме нормальний трафік, але вони також можуть навчатися і на атаках зловмисників.

У наш час важко зустріти IDS, в якій був би реалізований тільки один підхід для аналізу даних, - сучасні системи використовують кілька технологій одночасно.

Використання СВВ допомагає досягнути таких цілей:

- виявити вторгнення або мережеві атаки;

- забезпечити належний контроль якості адміністрування, особливо у великих і складних мережах;

- спрогнозувати можливі майбутні атаки і ви-явити вразливості для запобігання їх подальшого розвитку;

- отримати корисну інформацію про проникнення, для відновлення і налаштування конфігурації мережі;

- визначити розташування джерела атаки по відношенню до локальної мережі (зовнішні або внутрішні атаки).

Автори [5] розрізняють IDS між собою не тільки способами обробки даних, а й способами реагування на будь-яку подію. Хоча цей поділ також досить умовний. Виділяють пасивні системи, які тільки попереджають про те, що стався інцидент, і активні, намагаються протидіяти атаці, наприклад, змінюючи конфігурацію фаервола або маршрутизатора.

Деякі системи виявлення вторгнень можуть виявити початок атаки на мережу, причому деякі з них здатні виявляти раніше не відомі атаки. Такі системи називають системами запобігання вторгненням (англ. Intrusion Prevention System, IPS). IPS не обмежуються лише оповіщенням, але й здійснюють різні заходи, спрямовані на блокування атаки (наприклад, розрив з'єднання або виконання скрипту, заданого адміністратором). На практиці досить часто програмно-апаратні рішення поєднують у собі функціональність двох типів систем. Їх об'єднання називають IDPS.

Хоч існує декілька типів IDS, які за розміром варіюються від окремих комп'ютерів до великих мереж, найпоширенішими класифікаціями є системи виявлення вторгнень у мережу (англ. network intrusion detection systems, NIDS) та системи виявлення вторгнень засновані на аналізі хостів (англ. host-based intrusion detection systems, HIDS). Прикладом HIDS буде система, яка відслідковує важливі файли операційної системи, прикладом NIDS буде система, яка аналізує вхідний мережевий трафік. Також можна класифікувати IDS відповідно до методів виявлення загроз: найбільш відомим є виявлення на основі сигнатур (розпізнавання поганих шаблонів, таких як шкідливе ПЗ) та виявлення аномалій (виявлення відхилень від «правильного» трафіку, часто за допомогою машинного навчання)[4,6].

2.2 Архітектура систем виявлення вторгнень

Як і будь-яка система, IDS складається з набору пов'язаних між собою компонентів. Для кращого розуміння подальшого матеріалу розберемо основні складові частини IDS. На рис. 1 зображена архітектура типових систем виявлення вторгнень.

Основними компонентами СВВ є сенсорна підсистема, підсистема аналізу, сховище, консоль управління та модуль реагування.

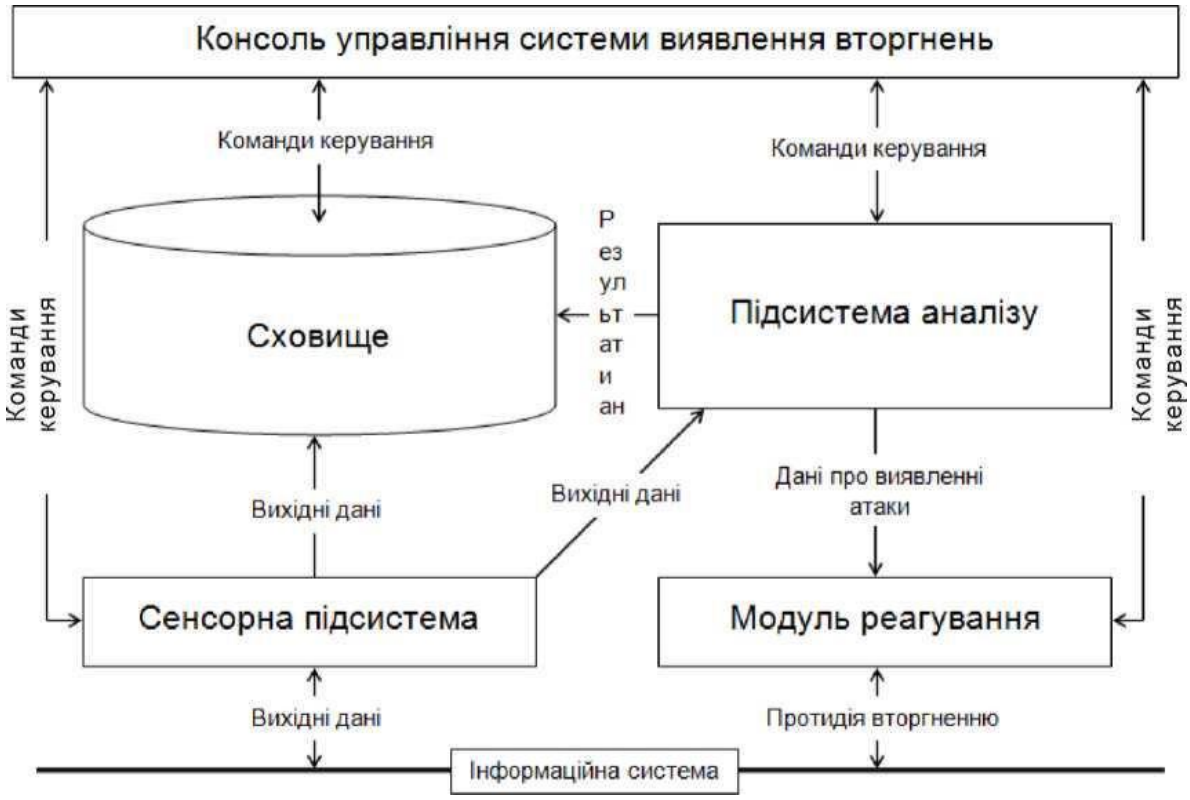


Рисунок 2.1 - Типова архітектура систем виявлення вторгнень

Сенсорна підсистема (модуль стеження, або сенсор), призначена для збору подій, пов'язаних з безпекою мережі або системи, що захищається. Забезпечує стеження за потоком даних. Вона може бути фізично відокремленою від основної системи і перебувати на будь-якому хості в будь-якому сегменті мережі.

Для збору інформації використовуються автономні модулі - датчики. Кількість використовуваних датчиків різна і залежить від специфіки системи, що захищається. Датчики в СВВ прийнято класифікувати за характером інформації, що збирається. Відповідно до загальної структури інформаційних систем виділяють наступні типи:

- датчики додатків - дані про роботу програмного забезпечення системи;
- датчики хоста - функціонування робочої станції системи;
- датчики мережі - збір даних для оцінки мережевого трафіку;
- міжмережеві датчики - містять характеристики даних, що циркулюють між мережами.

Система виявлення вторгнення може включати будь-яку комбінацію з

наведених типів датчиків.

Підсистема аналізу, призначена для виявлення мережевих атак і підозрілих дій. Є основним модулем системи. Здійснює аналіз інформації, отриманої з різних джерел, і, на підставі отриманих результатів і заданих правил, приймає рішення про подальше дії.

Сховище, в якому накопичується база первинних подій і результати аналізу. Містить інформацію, на основі якої аналізується трафік. Це можуть бути і профілі поведінки користувачів, і сигнатури відомих атак, і різні статистичні дані.

Консоль управління, що дозволяє конфігурувати СВВ, спостерігати за станом мережі або інформаційної системи та СВВ, переглядати виявлені підсистемою аналізу інциденти несанкціонованих вторгнень. Зазвичай представлена у вигляді графічного інтерфейсу, що дозволяє управляти всіма компонентами IDS.

Модуль реагування, який встановлений в системах активної протидії відповідає за виконання інструкцій по протидії несанкціонованому вторгненню в мережу або систему[3].

2.3 Класифікація СВВ

Як зазначають Мєшков В.І та Віролайнен В. О. [7], системи виявлення вторгнень можна класифікувати:

1. За характером відповідної реакції:

- пасивні - системи виявлення, в яких після виявлення та розпізнавання підозрілого трафіку, СВВ тільки повідомляє користувача або адміністратора про загрозу;

- активні - системи запобігання, що протистоять вторгненням, шляхом скидання з’єднання або зміна правил Firewall з метою блокування підо зрілого трафіку;

- гібридні, що здійснюють виявлення та протистоять вторгненням в

автоматичному режимі.

2. За методиками аналізу:

- статистичні СВВ - використовує статистичний підхід, після установки «навчаються» адміністратором, який задає політику СВВ, відповідну нормальної активності в мережі - типи трафіку, з'єднання між вузлами, використовувані протоколи і порти. При виявленні аномалій в роботі мережі або статистично значущих відмінностей трафіку від типового в даній мережі, СВВ оповіщає про це адміністратора. Основною проблемою такого підходу є складність в налаштуванні і велика кількість хибнопозитивних тривог у разі некоректно заданих правил.

- сигнатурні СВВ аналізують трафік у мережі або порівнюють пакети з базою даних сигнатур (відомих атрибутів атак). При такому підході основною проблемою є старіння баз сигнатур.

- гібридна СВВ поєднує два і більше підходів для розробки СВВ. Дані від агентів на хостах комбінуються з мережевою інформацією для створення найбільш повного уявлення про безпеку мережі.

3. За рівнем виявленням атак:

- NIDS (англ. Network Intrusrnn Detection Systems). Відстежує вторгнення, перевіряючи мережевий трафік і веде спостереження за декількома хостами. Мережева система виявлення вторгнень отримує доступ до мережевого трафіку, підключаючись до концентратору або комутатору, налаштованому на дублювання портів, або мережевий TAP пристрій. Перевагами NIDS є велике покриття для моніторингу та у зв'язку з цим централізоване управління, також NIDS не впливають на продуктивність і топологію мережі. До недоліків цих систем можна віднести: високу загрузку системи, NIDS потребує додаткового налаштування і функціональності мережевих пристроїв. Системи NIDS не можуть аналізувати зашифровану інформацію і розпізнавати результати атак.

- GrIDS (англ. Graph-Based Intrusion Detection System). Ця система являється удосконаленою версією NIDS. У кожний сегмент LAN встановлюється свій сніфер. Інформація від них збирається разом, аналізується і представляється у виді схеми інформаційних потоків. Усі NIDS не залежать

від типу використовуваної в мережі ОС. Для роботи їм необхідний виділений вузол у контрольованому сегменті і мережевий адаптер, який уміє приймати усі типи пакетів. Логічним вирішенням буде встановлення захищеного з'єднання між NIDS і консоллю управління.

- OIDS (англ. Operational Intrusion Detection Systems). Система спеціалізується на внутрішніх атаках. Ці системи розробили на випадок, якщо зловмиснику вдалося увійти в систему від імені зареєстрованого користувача. Або, коли атака на мережу відбувається зсередини її самої. Система порівнює дії конкретного користувача у даний момент часу з його звичайними діями, і у разі великих розбіжностей видає повідомлення. Простіше кажучи, оцінюється типовість дій (операцій) кожного з користувачів, в той час коли NIDS оцінює типовість трафіку.

- HIDS (англ. Host-based Intrusion Detection System). Ця система працює з інформацією, зібраною всередині одного комп'ютера. Таке розташування дозволяє HIDS аналізувати діяльність з великою вірогідністю і точністю, визначаючи тільки ті процеси і користувачів, які мають відношення до конкретної атаки в ОС. HIDS зазвичай використовують інформаційні джерела двох типів: результати аудиту ОС і системних журналів подій. HIDS мають можливість стежити за подіями локально, відносно хоста, можуть визначати атаки, які не можуть виявити NIDS. HIDS можуть функціонувати в системі, в якій мережевий трафік зашифрований, і система не вимагає додаткової функціональності мережевих пристроїв. До недоліків цієї системи відноситься: висока загрузка системи хоста, мале покриття для моніторингу, не мають централізованого управління і вони можуть бути блокованими деякими DoS-атаками або навіть заборонені.

- ERIDS (англ. External Routing Intrusrnn Detection System). Приклад інноваційної та вузькоспеціалізованої системи. Необхідність її створення була продиктована тим фактом, що крім простого і розподіленого способу збору даних про мережі існують менш тривіальні. Наприклад, зловмисник спочатку здійснює атаку на маршрутизатор, змінює його налаштування так, що він направляє трафік через сегмент, який не контролюється і доступний

атакуючому[8].

2.4 Схеми розташування системи виявлення вторгнень

Тепер, коли ми зрозуміли, як працює IDS і розібралися з основними її компонентами, настав час дізнатися про переваги і недоліки таких систем, а також яким чином здійснюється установка СВВ.

Почнемо з плюсів. Чим же може нам допомогти така система? Отже, IDS може визначити недоліки конфігурації ІС, знайти добре відомі уразливості в установленому ПЗ, визначити початок атаки на вашу мережу, а також аналізувати активність користувачів мережі і відслідковувати зміни в критичних даних.

Однак дана система, як і інші, не позбавлена своїх недоліків. Ось лише деякі з них: вона не може запобігти атаці, що використовує уразливість в мережевих протоколах, втрачає ефективність при великих навантаженнях на мережу, не завжди може правильно аналізувати дані від специфічних або нестандартних ІС, її ефективність знижується в разі атак на пакетному рівні, вона не зможе визначити причину того, що сталося проникнення в автоматичному режимі.

Незважаючи на властиві їй недоліки, така система все одно може дати нам дуже багато. Але для її ефективної роботи необхідна правильна установка IDS в існуючій інфраструктурі. Нижче я наведу список точок, де установка IDS вважається найбільш доцільною (рис. 2.2):

- між вашою і глобальною мережею;
- між DMZ і фаєрволом;
- у віддалених офісах;
- між користувачами і внутрішніми серверами.

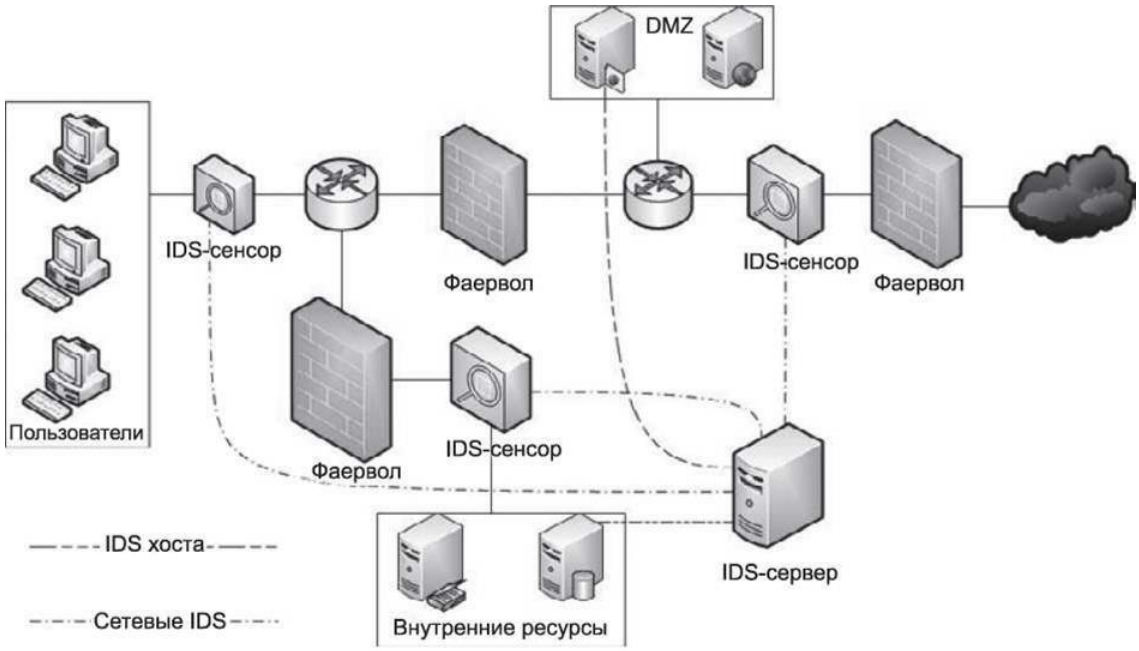


Рисунок 2.2 - Розташування сенсорів системи IDS

Невелике зауваження по даній схемі: різні автори [3] пропонують розміщувати один з сенсорів по-різному. Йдеться про сенсор, що розташований на кордоні з глобальною мережею. Якщо даний сенсор розмістити до фаервола, то можна отримати величезну кількість спрацьовувань і втратиться можливість аналізувати зашифрований трафік. Також на великому потоці даних ефективність IDS знижується, тому варто розміщувати IDS після фаєрвола.

Після того як правильно розташуються всі сенсори, необхідно зробити так, щоб всі дані відправлялися на єдину консоль управління.

Незважаючи на популярність і відмінну роботу IDS, не варто поспішати їх впроваджувати. Після прийняття рішення про встановлення такої системи необхідно детально вивчити логічну схему мережі і зрозуміти, де розмістити сервер, куди встановити мережеві сенсори і які хости потребують встановлення HIDS. Неправильне розміщення компонентів системи може призвести не тільки до великої кількості помилкових спрацьовувань, а й до неможливості аналізу трафіку в принципі.

Уважно проаналізують ризики. Виходячи з отриманої інформації, можна зрозуміти, які дані треба збирати і аналізувати. Машини користувачів будуть більше схильні до таких ризиків, як зараження вірусом, тоді як сервери веб-

додатків варто захищати, наприклад, від SQL-ін'єкцій.

У мережах з високою кількістю трафіку необхідно приділити увагу продуктивності. Безсумнівно, якщо ви не відчуваєте браку в обчислювальних ресурсах проблема продуктивності не буде такою критичною.

Не прагніть активно використовувати всі доступні правила і весь арсенал засобів, спрямованих на запобігання атак. Це загрожує тим, що ви паралізуєте роботу всієї мережі. Починайте впроваджувати поступово, для початку тільки в режимі моніторингу. І лише потім, після збору достатньої кількості даних про роботу системи, можете починати діяти більш активно!

2.5 Системи виявлення вторгнень на хостингах провайдера

Згідно [7] для забезпечення інформаційної безпеки ІТС хостинг провайдера необхідно реалізувати механізми захисту в системі.

Схема мережі хостинг провайдера зображена на рисунку 2.3.

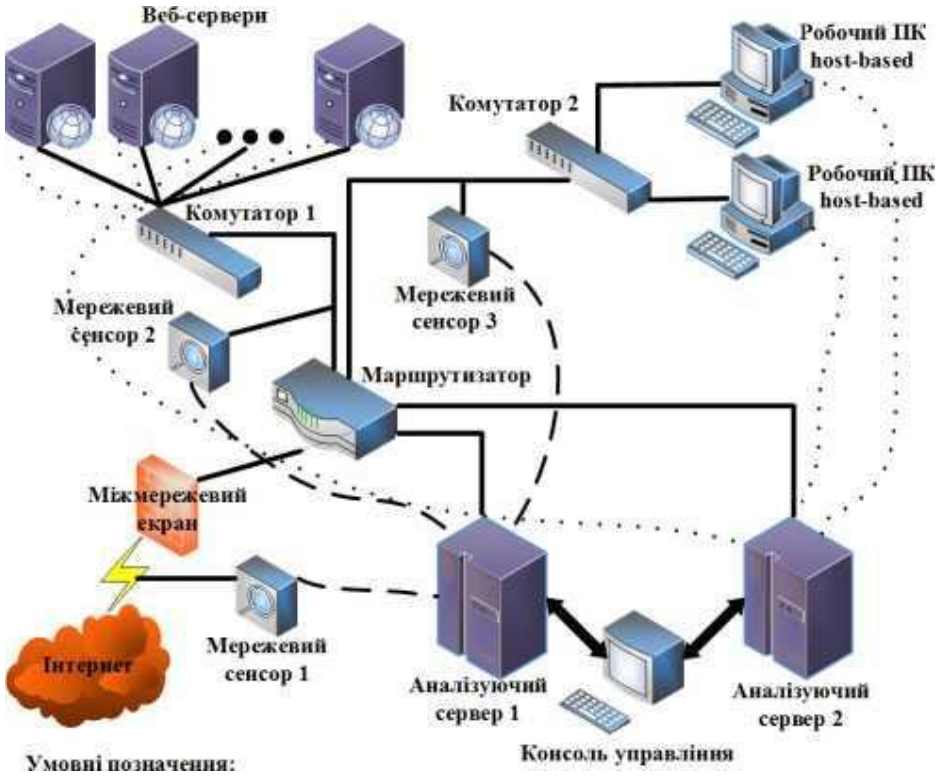


Рисунок 2.3 - Типова мережна схема хостинг провайдера

У мережі хостинг провайдера використовують комбінацію з мережевої та хостової СВВ. Система HIDS розміщується на окремому вузлі і відстежує ознаки атак на даний вузол. Система NIDS знаходиться на окремій системі, яка відстежує мережевий трафік на наявність ознак атак, проведених в підконтрольному сегменті системи.

Існує 5 основних типів сенсорів HIDS:

- аналізатори журналів
- сенсори ознак;
- аналізатори системних викликів
- аналізатори поведінки програм, служб;
- контролери цілісності файлів.

Слід зауважити, що деякі розробники ПЗ пропонують нові функціональні можливості сенсорів HIDS.

При розміщенні сенсорів NIDS необхідно керуватися ще одним ключовим правилом. Якщо в мережі використовуються комутатори замість концентраторів, сенсор виявлення вторгнень не буде правильно працювати, якщо він просто підключений до порту комутатора. Комутатор буде відправляти тільки трафік, спрямований на сенсор, до того порту, до якого підключений сенсор. У випадку з комутованою мережею існують два варіанти використання сенсорів виявлення вторгнень: застосування порту, що відстежує комутатор, або застосування мережевого розгалужувача.

Найбільш популярними системами з відкритим кодом є Snort, Suricata і OSSEC HIDS, з пропрієтарним кодом CATNET і McAfee IPS, Cisco Secure IDS, Dragon IDS.

Для захисту веб-сторінок від несанкціонованого доступу необхідно реалізувати функціональні послуги безпеки інформації згідно НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».

2.6 Висновки

Розглянуто типову структуру системи виявлення несанкціонованого доступу в інформаційну систему. Розглянуто їх класифікацію за різними ознаками. Виділено найбільш характерні місця розташуваня таких систем в інфраструктурі та рекомендації для їх розміщення.

Розглянуто основні моделі та методи, що лежать в основі таких ситем. Дані методи та моделі активно застосовуються у готових апаратних та програмно-апаратних комплексах виявлення та запобігання вторгненням в інформаційну систему.

3 СИСТЕМИ ТА МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІНИХ СИСТЕМАХ

3.1 Розвиток методів бородьби із НСД

Виявлення порушення безпеки проводиться зазвичай з використанням евристичних правил і аналізу сигнатур відомих комп'ютерних атак. Вже в 1984 році Фред Коен заявив, що кожне вторгнення виявити неможливо і ресурси, необхідні для виявлення вторгнень, будуть рости разом зі ступенем використання комп'ютерних технологій.

Найбільш поширеними є, так звані локальні і мережеві «Системи виявлення вторгнень» (СВВ). Локальна СВВ передбачає, що система виявлення встановлюється на кожному окремому комп'ютері. Мережева СВВ збирає пакети, що надходять в мережу через один пристрій і аналізують їх, перш ніж пересилати заданим вузлам. Мережеві СВВ сьогодні вважаються менш ефективними, чим більша кількість вузлів в мережі тим важче стає забезпечення надійної фільтрації пакетів і, як наслідок, захист комп'ютерів в мережі.

Системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на інформаційні системи, як наголошують [9], вже давно застосовуються як один з необхідних рубежів оборони інформаційних систем використовуються для виявлення деяких типів шкідливої активності, яка може негативно вплинути на безпеку комп'ютерної системи. До такої активності відносяться мережеві атаки, що спрямовані проти вразливих сервісів, атаки, які передбачають підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів і черв'яків).

4 листопада 1983 був винайдений перший комп'ютерний вірус. Фред Коен у той час ще аспірант одного з американських університетів, написав першу програму-вірус, яка здатна до саморозмноження та паразитичного поширення

по мережах. На презентації своєї докторської дисертації, яка була присвячена проблемі забезпечення безпеки комп'ютерних систем Коен представив першу програму-вірус. Особливої загрози програма Коена не становила, оскільки експеримент був контрольованим і не мав далекосяжних цілей.

На сьогоднішній день виділяють і рекомендують до застосування, в тому числі, і при побудові системи захисту три групи методів виявлення атак:

- сигнатурні методи;
- методи виявлення аномалій;
- комбіновані методи (використовують спільно алгоритми, визначені в сигнатурних методах і методах виявлення аномалій).

Іншими словами, виявлення порушення безпеки проводиться зазвичай з використанням евристичних правил і аналізу сигнатур відомих комп'ютерних атак.

Серед методів, що використовуються в сучасних СВВ, можна виділити два напрямки: один спрямований на виявлення аномалій в системі, що захищається, а інший - на пошук зловживань. Кожний з цих напрямків має свої переваги і недоліки, тому в більшості існуючих СВВ застосовуються комбіновані рішення, засновані на синтезі відповідних методів. Ідея методів, використовуваних для виявлення аномалій, полягає в тому, щоб розпізнати, чи є процес, що викликав зміни в роботі системи, діями зловмисника.

Виділяють дві групи методів [10]: з контрольованим навчанням («навчання з учителем»), і з неконтрольованим навчанням («навчання без учителя»). Основна відмінність між ними полягає в тому, що методи контрольованого навчання використовують фіксований набір параметрів оцінки і якісь апріорні відомості про значення параметрів оцінки. Час навчання фіксований. У неконтрольованому ж навчанні безліч параметрів оцінки може змінюватися з плином часу, а процес навчання відбувається постійно.

Перейдемо до розгляду конкретних методів виявлення аномалій та зловживань, і здійснимо аналіз ефективності їх використання в конкретних системах за допомогою складання характерних таблиць.

3.2 Методи виявлення аномалій

Метод виявлення аномалій або поведінковий метод базується не на моделях інформаційних атак, а на моделях штатного функціонування (поведінки) ІС. Принцип роботи будь-якого з таких методів полягає в виявленні невідповідності між поточним режимом роботи ІС і режимом роботи, що відповідає штатної моделі даного методу. Будь-яка невідповідність розглядається як інформаційна атака.

Наприклад, якщо система виявлення атак фіксує вхід співробітника компанії в мережу в суботу о 2.30, то це може свідчити про те, що пароль цього користувача вкрадений або підібраний і його зловмисник використовує для несанкціонованого проникнення[11].

Перевага методів даного типу - можливість виявлення нових атак без модифікації або поновлення параметрів моделі. На жаль, створити точну модель штатного режиму функціонування ІС дуже складно.

Серед поведінкових методів найбільш поширені ті, що базуються на статистичних моделях. Такі моделі визначають статистичні показники, що характеризують параметри штатної поведінки системи. Якщо з часом спостерігається певне відхилення даних параметрів від заданих значень, то фіксується факт виявлення атаки. Як правило, в якості таких параметрів можуть виступати рівень завантаження процесора, навантаження на канали зв'язку, штатний час роботи користувачів системи, кількість звернень до мережевих ресурсів і т. д.

Методи виявлення аномалій спрямовані на виявлення невідомих атак і вторгнень. Для СВВ, що захищається на основі сукупності параметрів оцінки формується «образ» нормального функціонування. В сучасних СВВ виділяють кілька способів побудови «образу»:

- накопичення найбільш характерної статистичної інформації для кожного параметра оцінки;
- навчання нейронних мереж значеннями параметрів оцінки;
- представлення за подіями.

Легко помітити, що у виявленні дуже значну роль відіграє безліч параметрів оцінки. Тому в виявленні аномалій одним із головних завдань є вибір оптимальної безлічі параметрів оцінки. Іншим, не менш важливим завданням є визначення загального показника аномальності. Складність полягає в тому, що ця величина повинна характеризувати загальний стан «аномальності» в системі, що захищається[10].

Методи пошуку аномалій наведені в таблицях 3.1 і 3.2.

Таблиця 3.1. Виявлення аномалії - контрольоване навчання («навчання з учителем»)

№	Методи виявлення	Використовується в системах	Опис методу
1	Моделювання правил	W&S	Система виявлення протягом процесу навчання формує набір правил, що описують нормальну поведінку системи. На стадії пошуку несанкціонованих дій система застосовує отримані правила і в разі недостатньої відповідності сигналізує про виявлення аномалії
2	Описова статистика	IDES, NIDES, EMERLAND, JiNao, HayStack	Навчання полягає в зборі простої описової статистики безлічі показників, що захищається системи в спеціальну структуру. Для виявлення аномалій обчислюється «відстань» між двома векторами показників - поточними і збереженими значеннями. Стан в системі вважається аномальним, якщо отримане відстань досить велика.
3	Нейронні мережі	Hyperview	Структура застосовуваних нейронних мереж різна. Але у всіх випадках навчання виконується даними, що представляють нормальну поведінку системи. Отримана навчена нейронна мережа потім використовується для оцінки аномальності системи. Вихід нейронної мережі говорить про наявність аномалії

Таблиця 3.2. Виявлення аномалії - неконтрольоване навчання («навчання без учителя»)

№	Методи виявлення	Використовується в системах	Опис методу
1	Моделювання множини станів	DPEM, JANUS, Bro	Нормальна поведінка системи описується у вигляді набору фіксованих станів і переходів між ними. Де стан являє собою вектор певних значень параметрів вимірювань системи.
2	Описова статистика	MIDAS, NADIR, Haystack, NSM	Аналогічнийвідповідному методув контрольованому навчанні.

3.3 Методи виявлення зловживань

Використання тільки методів виявлення аномалій не гарантує виявлення всіх порушень безпеки, тому в більшості СВВ існує технології розпізнавання зловживань. Виявлення вторгнень-зловживань ґрунтується на прогностичному визначенні атак і подальшим спостереженням за їх появою. На відміну від виявлення аномалії, де образ - це модель нормальної поведінки системи, при виявленні зловживання він необхідний для уявлення несанкціонованих дій зловмисника. Такий «образ» стосовно виявлення зловживань називається сигнатурою вторгнення. Формується сигнатура на основі тих самих вхідних даних, що і при виявленні аномалій, тобто на значеннях параметрів оцінки. Сигнатури вторгнень визначають оточення, умови і спорідненість між подіями, які призводять до проникнення в систему або будь-яким іншим зловживанням. Вони корисні не тільки при виявленні вторгнень, але і при виявленні спроб здійснення незаконних дій. Частковий збіг сигнатур може означати, що в системі, що захищається мала місце спроба вторгнення. Перевага даних методів - висока точність визначення факту атаки, а очевидний недолік - неможливість

виявлення атак, сигнатури яких ще не визначені[9].

Метою другого напрямку (виявлення зловживань) є пошук послідовностей подій, визначених адміністратором безпеки або експертом під час навчання СВВ, як етапи реалізації вторгнення. У теперішній час виділяють лише методи з контрольованим навчанням.

Серед сигнатурних методів виявлення атак найбільш поширений метод контекстного пошуку, який полягає в виявленні у вихідній інформації певної безлічі символів. Так, для виявлення атаки на Web-сервер, що спрямована на отримання несанкціонованого доступу до файлу паролів, проводиться пошук послідовності символів "GET* / etc / passwd" у заголовку HTTP-запиту. Фрагмент "cwd-root" в FTP-сеанс однозначно визначає факт обходу механізму аутентифікації на FTP-сервері і спробі перейти в кореневий каталог FTP-сервера. Іншим прикладом є виявлення аплетів Java в мережевому трафіку на основі шістнадцятирічного фрагмента "CA FE BA BE". Ці ж сигнатури дозволяють виявляти троянських коней, якщо останні використовують стандартні значення портів. Наприклад, троян NetBus визначається по використанню 12345-го і 12346-го портів, а троян BackOrifice - 31337-го порту.

За допомогою контекстного пошуку ефективно виявляються атаки на основі аналізу мережевого трафіку, оскільки даний метод дозволяє найбільш точно задати параметри сигнатури, яку необхідно виявити в потоці вихідних даних.

У ряді СВВ, відповідно до [11] були реалізовані ще два сигнатурних методи: метод аналізу станів і метод, який базується на експертних системах.

Метод аналізу станів або контролю частоти подій заснований на формуванні сигнатури атак у вигляді послідовності переходів інформаційної системи ІС з одного стану в інший. По суті, кожен такий перехід визначається по настанню в ІС певної події, а набір цих подій задається параметрами сигнатури атаки. Ці сигнатури описують ситуації, коли протягом деякого інтервалу часу відбуваються події, число яких перевищує задані заздалегідь показники. Прикладом такої сигнатури є виявлення сканування портів або виявлення атаки SYN Flood. У першому випадку пороговим значенням є число

портів, перевірених в одиницю часу. У другому випадку - число спроб встановлення віртуального з'єднання з вузлом за одиницю часу.

Як правило, сигнатури атак, створені на основі аналізу станів, описуються математичними моделями, що базуються на теорії кінцевих автоматів або мереж Петрі.

На рис. 3.1 показана мережа Петрі, що описує сигнатуру атаки, яка виконує підбір пароля для отримання несанкціонованого доступу до ресурсів ІС. Кожен перехід ІС в новий стан в цій мережі Петрі пов'язаний зі спробою введення пароля. Якщо користувач протягом 1 хв чотири рази поспіль введе неправильний пароль, то метод зафіксує факт здійснення атаки.

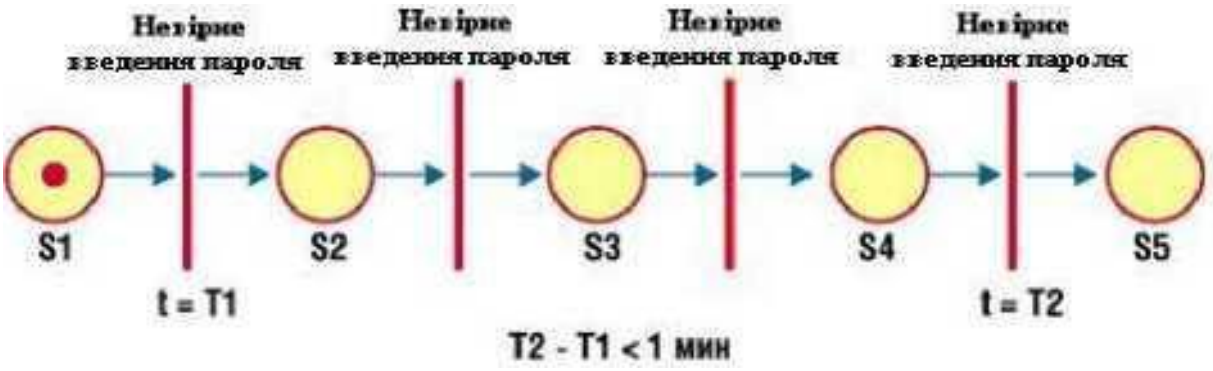


Рисунок 3.1 - Мережа Петрі для фіксації підбору пароля

Методи, що базуються на експертних системах, дозволяють описувати моделі атак на природній мові з високим рівнем абстракції. Експертна система, яку покладено в основу методів цього типу, складається з двох баз даних: фактів і правил. Факти це вихідні дані про роботу ІС, а правила - алгоритми логічних рішень про факт атаки на основі набору фактів. Всі правила експертної системи записуються в форматі "якщо <...>, то <...>". Результуюча база правил повинна описувати характерні ознаки атак, які зобов'язана виявляти СВВ.

Одна з найбільш перспективних сигнатурних груп - методи, які засновані на біологічних моделях. Для їх опису можуть використовуватися генетичні або нейромережеві алгоритми.

Методи пошуку зловживань наведені в таблиці 3.3.

Таблиця 3.3. Виявлення зловживань - контрольоване навчання («навчання з учителем»)

№	Методи виявлення	Використовується в системах	Опис методу
1	Моделювання поведінки (станів)	USTAT, IDIOT	Вторгнення представляється як послідовність станів, де стан - вектор значення параметрів оцінки системи. Необхідна і достатня умова наявності вторгнення - присутність цієї послідовності. Виділяють два основних способи подання сценарію вторгнень: 1) у вигляді простого ланцюжка подій; 2) з використанням мереж Петрі, де вузли - події.
2	Експертні системи	NIDES, EMERLAND, MIDAS, DIDS	Експертні системи являють процес вторгнення у вигляді різного набору правил. Дуже часто використовуються продукційні системи.
3	Моделювання правил	NADIR, HayStack, JiNao, ASAX, Bro	Простий варіант експертних систем.
4	Синтаксичний аналіз	NSM	Системою виявлення виконується синтаксичний розбір з метою виявлення певної комбінації символів, що передаються між підсистемами і системами комплексу, що захищається.

3.4 Методи аналізу трафіку

На відміну від класичних методів виявлення аномалій та зловживань, варто приділити увагу окремо виділеному [12] методу аналізу трафіку. Даний метод, схожий за принципом дії на аномальний, але дозволяє поліпшити захист обчислювальної мережі. На відміну від сигнатурного методу, коли різноманітність загроз іноді просто нереально повністю класифікувати, аналіз поведінки трафіку в мережі більш піддається класифікації, тобто не залежно від того який тип атаки відбувається, види аномалій все ж не так різноманітні.

Варто зазначити, що аналіз трафіку життєво важливий для ефективного управління мережею. Він є джерелом інформації про функціонування корпоративних додатків, яка враховується при розподілі ресурсів, плануванні обчислювальних потужностей, визначенні та локалізації відмов, вирішенні питань безпеки.

Для аналізу трафіку використовують програми аналізатори (сніфери), які можуть виконувати:

- моніторинг мережевих інтерфейсів і мережевого трафіку;
- фільтрацію, тобто вибір будь-якої частини трафіку - аж до конкретного сайту або трафіку з конкретної машини протягом будь-якого зазначеного часу;
- надання графіків активності мережевих з'єднань на основі вибраних фільтрів;
- збір статистики (від години до року) з функцією експорту;
- перегляд статистики віддалених комп'ютерів;
- оповіщення і повідомлення при певному подію;
- можливість запуску як сервісу.

Перераховані можливості можуть бути присутніми в програмах моніторингу не обов'язково в повному обсязі.

Аналіз трафіку, що пройшов через сніффер, дозволяє:

- виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережевого обладнання та каналів зв'язку;
- перехопити будь-який незашифрований (іноді і зашифрований)

призначений для користувача трафік з метою отримання паролів і іншої інформації;

- локалізувати несправність мережі або помилку конфігурації мережевих агентів.

Для аналізу поведінки трафіку в першу чергу потрібно визначити безліч варійованих параметрів мережі, що впливають на її роботу. Зафіксовані значення цих параметрів повинні бути згруповані в підмножини, після чого їх можна використовувати для аналізу.

Передбачається, що показником аномалії в поведінці трафіку є суттєва зміна деяких його характеристик. Причому показники, вибрані для аналізу трафіку, повинні бути досить чутливі до його змін і несправностей, які викликані законним і нешкідливим трафіком, інакше не виключені помилкові спрацювання.

Сучасна мережева інфраструктура настільки велика, що відстежити правильність (безаномальність) руху всієї інформації в ній практично неможливо. Мережевий трафік являє собою складний динамічний процес і є суперпозицією багатьох потоків з множинними взаємозв'язками, які генеруються різними потоками.

Результат досліджень експериментальних даних показав, що трафік сучасних комп'ютерних мереж має особливу структуру, яка проявляє ефект самоподібності. Цей ефект проявляється в тому, що статистичні характеристики трафіку як би «масштабуються» при усередненні значень взятих за різні проміжки часу. Іншими словами, під самоподібністю мається на увазі повторюваність розподілу навантаження в часі при різних масштабах (рис. 3.2)[13].

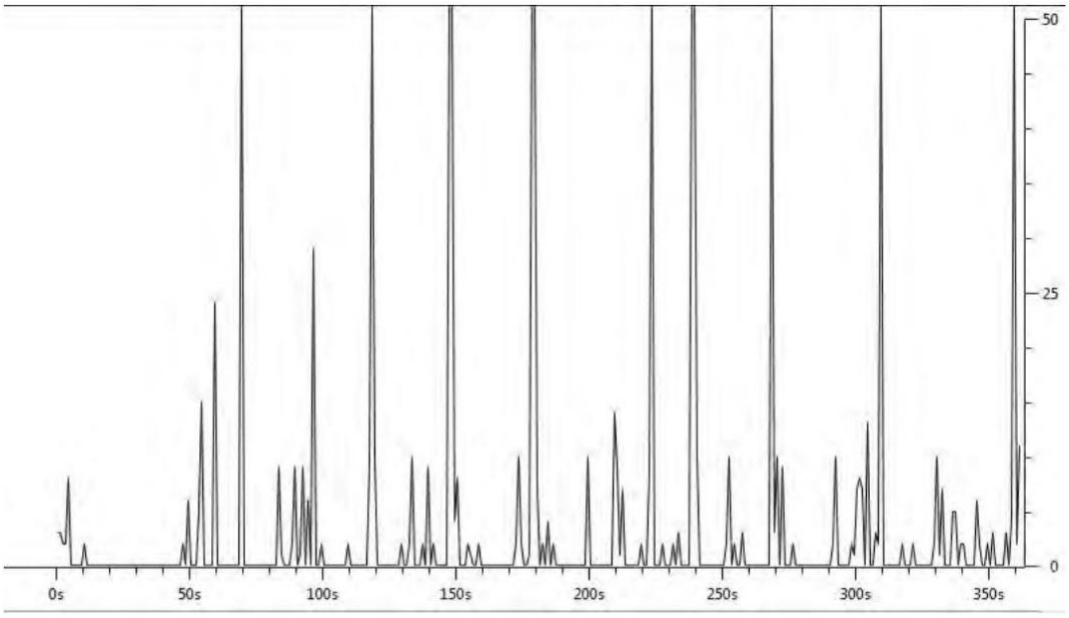


Рисунок 3.2 - Нормальне навантаження трафіку при бездротовому з'єднанні

Поява ефекту самоподібності пов'язано з властивостями TCP/IP протоколу передачі даних, який на сьогоднішній день використовується в комп'ютерних мережах. Мається на увазі особливість передачі даних у вигляді пакетів, які поступають на вузол комутації цілими пачками, а не випадковим чином. Трафік в таких мережах має явно виражений всплесковий характер, що підвищує ймовірність перевантажень в вузлах мережі, які ведуть до переповнення буферів і викликають втрати і/або затримки. Пульсації приводять до перепадів швидкості інформаційних потоків, при яких відношення максимального значення швидкості до мінімального становить десятки разів. Дослідження самоподібності показали, що це явище значно погіршує якість трафіку через мережу.

Для зменшення впливу на нормальне функціонування мережі трафік дублюються на спеціальний сервер, що займається збором трафіку. З пакетів, прийнятих від маршрутизатора, витягується інформація про тип пакету, а також чотири метрики трафіку: загальне число пакетів, число TCP пакетів, UDP пакетів, ARP пакетів в одиницю часу. Обчислюються показники Херста для чотирьох метрик трафіку ітеративним методом оцінки в режимі реального часу. Ці значення використовуються для виявлення аномалій і поновлення моделі нормального трафіку. Поточне обчислене значення показника Херста

порівнюється зі значенням з нормальної моделі поведінки трафіку. Якщо значення виходить за межі допустимого, трафік вважається аномальним. Нормальна модель трафіку будується шляхом аналізу нормальної роботи мережі протягом певного проміжку часу[12].

Модель включає нормальне значення показника Херста і довірчий інтервал, і може бути оновлена при виявленні аномалій. Критерієм оцінки безпеки є рівень ризику, який вираховується методом середньозважених величин, який враховує результати виявлення аномалій від чотирьох метрик трафіку. Рівень ризику надає адміністраторам поточний стан передачі даних в мережі з точки зору безпеки.

3.5 Комбіновані методи

Згідно [9] на стадії вторгнення виявити атаку можна за допомогою як сигнатурних, так і поведінкових методів. Будь-яке вторгнення характеризується певними ознаками, які, з одного боку, можна представити у вигляді сигнатури, а з іншого - описати як якесь відхилення від штатної поведінки ІС. Найбільш ефективно поєднання обох методів, при цьому для отримання необхідних вихідних даних застосовні будь-які (хостової або мережеві) датчики.

Ефективне виявлення атак на етапах атакуючого впливу і розвитку атаки можливо тільки за допомогою поведінкових методів. Оскільки дії порушників залежать від цілей проведеної атаки і фіксованою безліччю сигнатур атак однозначно не визначаються. З огляду на той факт, що на двох останніх стадіях життєвого циклу інформаційної атаки найхарактерніші об'єкти - це хости, в даному випадку найбільш доцільно застосування хостових датчиків.

На основі досліджених даних, можна зробити висновок, що реалізовані в даний час в СВВ методи засновані на загальних уявленнях розпізнавання образів. Відповідно до них для виявлення аномалії формується образ нормального функціонування інформаційної системи. Цей образ виступає як сукупність значень параметрів оцінки. Його зміна вважається проявом

аномального функціонування системи. Після виявлення аномалії і оцінки її ступеня формується судження про природу змін: чи є вони наслідком вторгнення або допустимим відхиленням. Для виявлення зловживань також використовується образ (сигнатура), однак тут він відображає заздалегідь відомі дії атакуючого.

3.6 Висновки

За результатами вище проведеного аналізу і із розрахунком перспективи подальшого впровадження перспективних технологій захисту інформації використання сигнатурного методу та методу виявлення аномалій забезпечують додатковий рівень захисту інформаційної системи, доповнюючи "традиційні" засоби захисту - міжмережеві екрани, криптомаршрутизатори, сервери аутентифікації та ін. Але найперспективнішим методом можна вважати комбінований метод, що використовує спільно алгоритми, визначені в сигнатурних методах і методах виявлення аномалій. Так як, тільки комплексний підхід може значно знизити ризик вторгнення в ІС і виключити втрату цінних даних.

4 ВИБІР СИСТЕМИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ВТОРГНЕННЯ

4.1 Основні характеристики засобів СВВ

Широке використання сучасних засобів захисту від кібератак не гарантує безпеки на належному рівні, оскільки останнім часом:

- зростають атаки, спрямовані на корпоративні системи, публічні, конфіденційні та державні інформаційні ресурси;
- кібератаки, постійно модифікуються, удосконалюються і стають більш регулярними;
- виявлення кібератак класичними засобами захисту не завжди є ефективним;
- частішають випадки здійснення складних атак.

Це також пов’язане з інтенсивним розвитком програмно-апаратних засобів і глобалізації інформаційних мереж та їх повсякденного використання у всіх сферах діяльності суспільства.

Враховуючи результати досліджень [14,15] з подальшим їх узагальненням і відображенням на розширений спектр засобів виявлення зловживань та аномалій розглянемо базові характеристики сучасних СВВ: «Клас кібератак», «Адаптивність», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» та «Підтримка ОС».

Перед початком аналізу розкриємо кожну із зазначених базових характеристик.

«Клас кібератак» — визначає здатність системи виявляти аномалії та зловживання на різних рівнях ІС. Більшість сучасних засобів мають здатність виявляти обидва класи атак (аномалії та зловживання).

«Адаптивність» — дозволяє системі ефективно адаптуватись до нових атак (відсутніх у базі даних сигнатур), наприклад, 0-day та виявляти кібератаки

з незначними модифікаціями.

«Методи виявлення» — множини методів, що використовуються для виявлення атак і складають математичну основу системи. Найбільш поширеними є методи статистичного і кластерного аналізу, контролю зміни подій, графів атак, сигнатурні, динамічні, машинного навчання, поведінкові, евристичні, експертні, нечітких множин тощо.

«Управління системою» — визначає схему управління і його рівень. Управління може здійснюватися централізовано із одного хоста або розподілено із окремих хостів, пов’язаних однією системою. Найбільш оптимальною є організація управління за централізованою схемою з певною множиною центрів, кожний з яких може бути задіяний для управління всією структурою. Централізовані системи реалізують управління всіма засобами (модулями) виявлення аномалій та зловживань з однієї станції, а розподілені реалізують управління окремо, де кожний модуль відповідає за свою функцію.

«Масштабованість» — можливість розширення системи, її адаптивність до різних мережевих структур та долучення нових аналізованих ресурсів мережі.

«Рівень спостереження» — визначає, на якому рівні системи отримуються дані для виявлення кібератак. Застосовуються два рівні отримання даних — мережевий та системний. Сучасні системи, як правило, підтримують обидва рівні спостереження, оскільки саме їх взаємодія дозволяє краще забезпечити захист. Від цієї характеристики залежить швидкість формування первинних даних, їх правильна обробка та отримання точної інформації про поточний стан.

Аналіз трафіку мережі здійснюється за допомогою спеціальних сенсорів (мережевих і системних), що застосовуються у системах виявлення атак та аномалій. Мережеві сенсори аналізують дані на мережевому рівні (зазвичай на основі сигнатурного аналізу) і генерують повідомлення про виявлення кібератак та відправляють їх до модулів управління.

Системні сенсори аналізують журнали реєстрації ОС, додатки та програмні застосунки на можливі аномалії чи загрози і генерують відповідні

повідомлення, які надходять до модулів управління .

«Реакція на кібератаку» — визначає наявність у системі компонентів чи модулів протидії. Тобто, після реєстрації атаки ініціюються дії для редукування подальшого негативного впливу .

«Захищеність» — характеризує наявність власних компонентів системи, які відповідають за її захист від кібератак та зовнішнього негативного інформаційного впливу, а також за стійкість до виходу з ладу та зменшення кількості уразливостей розробки в цілому.

«Підтримка ОС» — характеризує тип ОС (наприклад, Unix, Linux, Windows, MacOS тощо), що підтримує відповідне ПЗ системи.

Далі з урахуванням запропонованих характеристик проаналізуємо властивості відповідних СВВ.

4.2 Мережева СВВ Shadow

Мережева СВВ Shadow (Secondary Heuristic Analysis for Defensive Online Warfare, розробник Naval Surface Warfare Center (військово-морський центр), Вірджинія, США) містить станції-давачі і станції-аналізатори. Перші розташовані на зовнішній стороні міжмережевих екранів, а другі у внутрішньому захищеному сегменті мережі. Станція-давач — це сервер, на якому активізований tcpdump, який записує трафік у файл. Давачі виокремлюють заголовки пакетів і зберігають їх у спеціальному файлі. Станція-аналізатор зчитує цю інформацію, фільтрує її і генерує відповідний журнал. Якщо події ідентифіковані і для них існує стратегія реагування, то попереджувальні повідомлення не генеруються. Давачі використовуються для вилучення пакетів утиліти libpcap, а основний аналіз відбувається в модулі tcpdump, який містить фільтри пакетів, що поділяються на прості та складні (з декількох фільтрів). Фактично система використовує низку фільтрів мовою Perl, сенсори і аналізатори. Також Shadow (рис. 4.1) функціонує на багатьох UNIX-системах, включаючи FreeBSD і Linux та використовує веб-інтерфейс

для відображення інформації. Завдяки гнучкості мови Perl архітектура, що використовується в Shadow є однією з кращих серед мережевих СВВ.

Рисунок 4.1 - Робоче вікно Shadow

Система орієнтована на виявлення зловживань та простих аномалій за допомогою методу контролю станів мережі, який не забезпечує систему в повній мірі можливістю адаптивності до нових кібератак. Shadow має закритий початковий код, а відповідні розширення здійснюються лише розробником. Система давачів та сенсорів дозволяє виявляти кібератаки на основі контролю зміни характеристик мережі за допомогою використання журналів стану та певних програмних фільтрів. Управління системою проводиться розподілено через файли конфігурації на всіх вузлах, де розташовані компоненти системи. Архітектура Shadow дозволяє будувати давачі (розташовані у вузлах мережі для збору інформації і запису у журнал) та аналізатори (аналізують всі події зареєстровані у журналі за допомогою давачів) для виявлення атак на різних рівнях мережі незалежно від її розміру.

Особливості будови даної системи дозволяють виявляти кібератаки лише на мережевому рівні. Для своєї безпеки Shadow використовує протокол SSH, але не містить спеціальних механізмів протидії вторгненням і не є стійкою до можливих спрямованих на неї кібератак. Вона підтримується ОС Kali Linux

(Unix та Linux), є частиною програмного продукту Snort та працює в пасивному режимі для збирання даних про систему[14].

4.3 Arbor Networks Spectrum

Система Arbor Networks Spectrum (розробник компанія Arbor Networks, Массачусетс, США) є високопродуктивним рішенням для аналізу мережевого трафіку, визначення шкоди від інцидентів інформаційної безпеки, виявлення вторгнень за допомогою поєднання статистичного, динамічного та сигнатурного методів аналізу. Основним функціоналом Arbor Networks Spectrum (рис. 4.2) є виявлення DoS і DDoS атак, троянів та їх похідних.

Рисунок 4.2 - Вікно перегляду індикаторів загроз у часі

Arbor може бути розгорнута як пристрій або віртуальне рішення стеження за мережевим трафіком забезпечуючи постійне виявлення кібератак та зменшення їх наслідків. Запатентована в Arbor технологія Cloud Signaling успішно інтегрує цей захист за допомогою хмарних технологій, автоматизуючи ключовий компонент захисту щодо DDoS та скорочуючи час, необхідний для редукування атак. Застосований гібридний багатошаровий ахист є достатньо

ефективним підходом для захисту даних від DDoS, що забезпечує безпеку корпоративних мереж незалежно від того, який тип DDoS-атак на них направлений.

Arbor Networks Spectrum забезпечує:

- швидкий і легкий доступ до величин, що характеризують загрози в мережі та створення архіву трафіку;
- візуалізацію характеристик трафіку та загрози;
- централізоване управління щодо виявлення кібератак;
- постійне поновлення бази даних новими видами потенційних атак;
- масштабованість та простоту використання.

Програмний засіб забезпечує повний перегляд всієї активності в мережі з можливістю аналізу пакетних і потокових даних в режимі реального часу. Саме це дозволяє виявляти аномалії та атаки різного рівня. За допомогою функції ATLAS кожен користувач системи може з легкістю отримувати інформацію про нові кібератаки у глобальній мережі у режимі реального часу, що і забезпечує певний рівень адаптивності даної системи. Крім інформації про кібератаки, користувач отримує оновлену політику безпеки і контрзаходи для попередження атак. Часткова відкритість Arbor Networks Spectrum дозволяє покращувати адаптивність системи до нових кібератак, хоча повне оновлення і удосконалення різних модулів централізовано здійснюється розробниками. Система використовує статистичний, динамічний та сигнатурний методи виявлення атак і має централізоване управління за допомогою зручного інтерфейсу Arbor Spectrum. Гнучкі параметри розгортання системи дозволяють організаціям легко масштабувати та налаштувати даний засіб під потреби своєї мережі. Архітектура Arbor Networks Spectrum дозволяє виявляти атаки на мережевому і системному рівнях. Інтелектуальні схеми роботи і засоби аналізу в режимі реального часу дозволяють службам безпеки розслідувати та підтверджувати відповідні загрози і оперативно вживати необхідних заходів протидії. Система не містить спеціальних механізмів захисту або вони не розкриті розробниками, а також працює на платформі vSphere Hypervisor, яка підтримує ОС Unix, Linux та Windows[16].

4.4 KATA Platform

Система KATA Platform [17] (Kaspersky Anti Targeted Attack Platform, розробка компанії Kaspersky, Росія) орієнтована на розвиток новітніх технологій у сфері корпоративних комп'ютерних мереж і використовується для захисту від комплексних цільових атак будь-якої складності. Рішення KATA Platform інтегрує новітні технології та глобальну аналітику, що дозволяє своєчасно реагувати на цілеспрямовані дії НАС і протидіяти атакам на всіх етапах їх реалізації. Програмний засіб реалізує функції контролю мережевої активності, аналізу поводження об'єктів системи, виявлення комплексних цільових кібератак та аналіз аномалій в комп'ютерних мережах.

Для збору первинної інформації про аномалії в KATA Platform (рис. 4.3) використовуються сенсори (спеціальні агенти), які аналізують IP, веб і e-mail трафік та події на робочих станціях і серверах. Агенти KATA Platform сумісні з іншим програмними засобами захисту і здійснюють мінімальний вплив на продуктивність мережі та комп'ютерів.

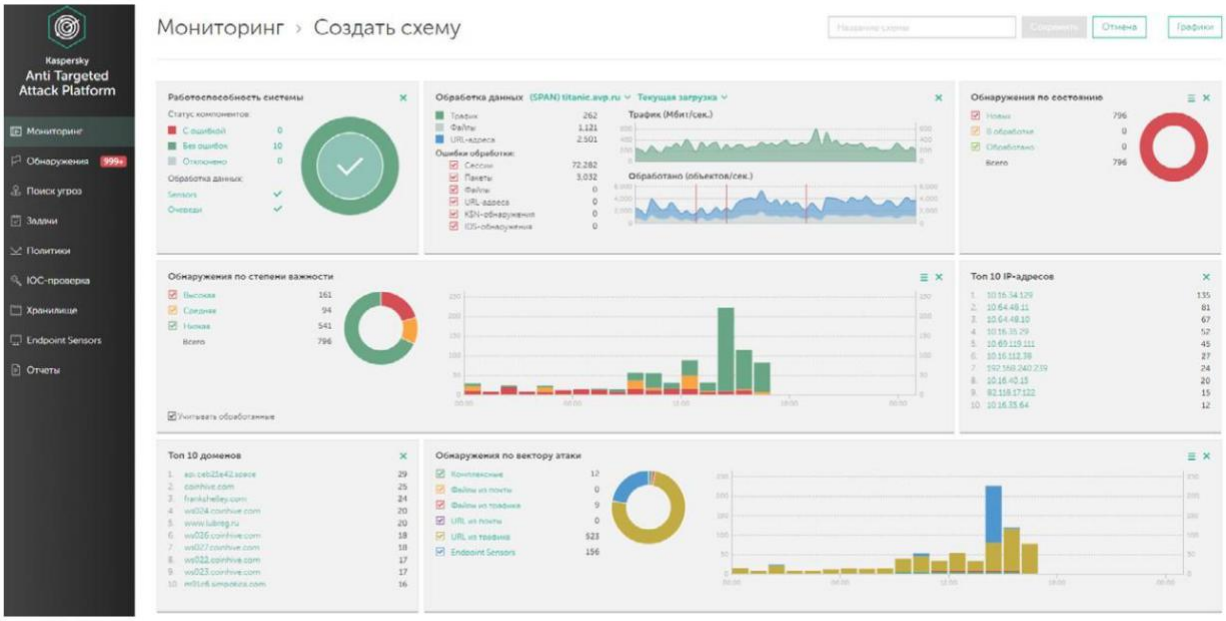


Рисунок 4.3 - Вікно ПЗ Kaspersky Anti Targeted Attack Platform

Функціонування KATA Platform базується на чотирьох етапах і є частиною комплексного стратегічного підходу для створення адаптивної моделі

захисту від нових загроз і реагування на інциденти інформаційної безпеки:

Етап 1 - виявлення:

- постійний моніторинг активностей, які сигналізують про початок атаки;
- викривання уразливостей в системі безпеки і спроб проникнення в мережу;
- викривання інцидентів, оцінка збитку і пріоритизація подальших дій;
- тренінги з розслідування цільових атак;
- звіти про цільові атаки.

Етап 2 - реагування:

- аналіз шкідливого ПЗ;
- оперативна протидія атакам і редукування пов'язаної з ними шкоди;
- протидія інцидентам та їх розслідування;
- проведення глибокої цифрової криміналістики.

Етап 3 - прогнозування:

- тестування на проникнення;
- оцінка рівня захищеності системи;
- оцінка потенційних ризиків для безпеки в поточній інфраструктурі;
- рекомендації щодо удосконалення заходів захисту і усунення уразливостей;
- проактивний захист, який адаптується до нових і невідомих загроз.

Етап 4 - протидія:

- підвищення обізнаності співробітників про актуальні кіберзагрози (навчальні ігри, симуляція загроз тощо);
- тренінги з кібербезпеки для фахівців, що підвищують ефективність протидії цільовим атакам.

KATA Platform здатен виявляти аномалії та комплексні цільові атаки різного роду, а постійне і оперативне оновлення бази даних мережевих загроз та розширення можливостей щодо виявлення кібератак, дозволяє забезпечувати користувачам адаптивність до нових вторгнень. Підтримка та оновлення даного ПЗ реалізується лише розробником. Аналіз цільових атак здійснюється на основі інформації від мережевих сенсорів, робочих станцій і серверів для

створення типових шаблонів поведінки програм. Далі на основі відхилень від цих шаблонів визначається, чи є активність потенційною частиною цільової атаки. Також підозрілі об'єкти, які виявлені в поштовому і інтернет-трафіку передаються сенсорами в «пісочницю», де кожен такий об'єкт аналізується на предмет шкідливої активності, що дозволяє виявляти атаку на ранній стадії.

Система має централізоване та розподілене управління, а також можливості адаптування і масштабування платформи до кількісті вхідного трафіку та архітектури мережі. Особливості будови KATA Platform дозволяють виявляти кібератаки на мережевому і системному рівнях. Також сенсори мережі і робочих станцій дають можливість розташовувати точки контролю в різних сегментах мережі і швидко виявити комплексні загрози. Система оперативно реагує на атаки, що визначені нею у відповідній базі даних та дає можливість проведення цифрової криміналістики[17].

Спеціальні механізми захисту, що містяться в KATA Platform не розкриті розробниками. Система функціонує на основі ОС Unix, Linux, Windows та MacOS.

4.5 Symantec DeepSight

Система Symantec DeepSight (Symantec Deep Sight Threat Management System, розробник компанія Symantec, Каліфорнія, США) дозволяє розширити можливості захисту шляхом забезпечення раннього оповіщення про активні атаки, потенційні загрози, нові уразливі місця, шпигунські програми, рекламне ПЗ, що дає можливість адміністраторам більш точно передбачити і оцінити ступінь ризику, а також визначити пріоритетність інформаційних ресурсів, яким необхідний першочерговий захист від вторгнень. Також наявність розсилки персоніфікованих повідомлень, які доповнені професійним аналізом загроз, узагальненими оцінками і підтримкою вибору дій роблять Symantec DeepSight Threat Management System (рис. 4.4) провідною системою раннього оповіщення про глобальні кібератаки. Система має достатньо розгалужену

інфраструктуру у глобальному кіберпросторі, яка складається з низки мереж honeypot.

За допомогою даної системи, згідно [14], можна аналізувати вхідні потоки даних, що надходять до комп'ютерів через мережу та блокувати загрози до їх реалізації в системі.

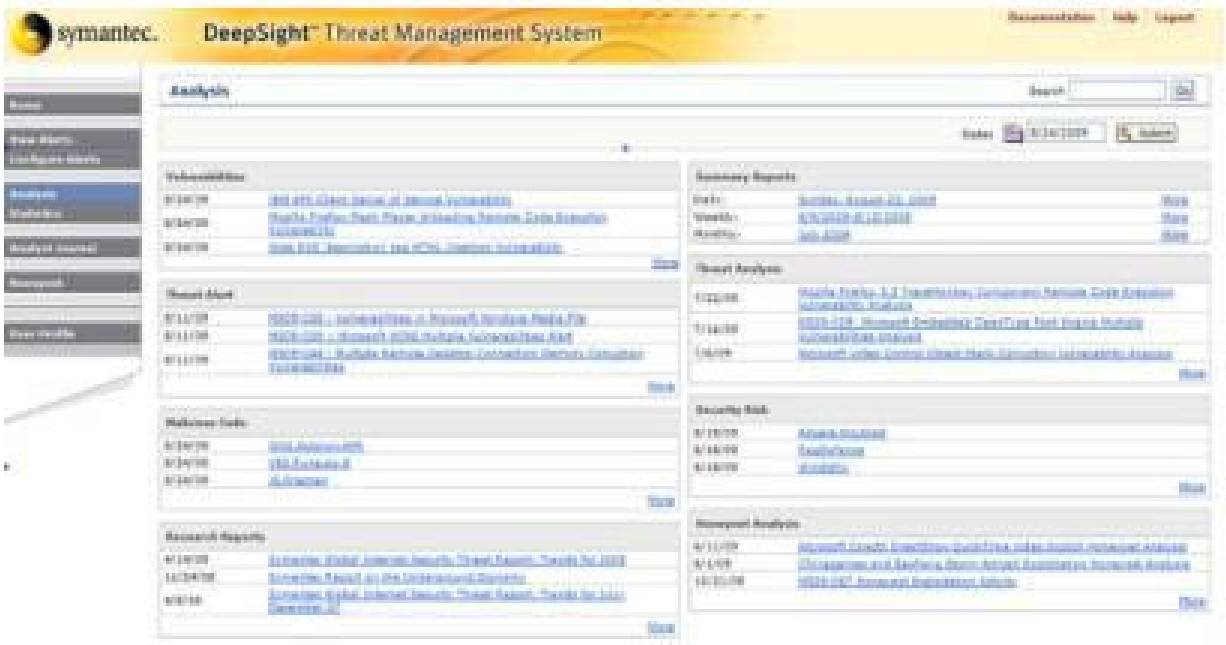


Рисунок 4.4 - Вікно Symantec DeepSight Threat Management System

Серед особливостей роботи даного програмного засобу слід віднести:

- автоматичне визначення пріоритетів серед існуючих загроз та ресурсів системи, що дозволяє оперативно встановити необхідний рівень протидії чи захисту;

- експертний аналіз даних, які збираються з тисяч джерел у глобальному кіберпросторі, включаючи інформацію про активні глобальні атаки;

- постійне збільшення та розширення баз даних існуючих мережевих загроз, через широке поширення даного програмного продукту;

- автоматизований моніторинг комп’ютерних мереж в реальному режимі часу, з можливістю швидкого сповіщення про загрозу;

- аналіз існуючих потенційних загроз в системі та створення базової стратегії їх попередження;

- здійснення управління програмним засобом спеціальними моніторами контролю функціонування в залежності від особливостей системи;

- стратегію редукування наслідків загроз, яка дозволяє забезпечити кращу пріоритетність, розподіл і розгортання персоналу та відповідних ресурсів безпеки;

- точний аналіз, який відповідає вимогам конкретної системи з урахуванням її мережевої структури, особливостей організації та виду діяльності.

Дане ПЗ здатне виявляти атаки і аномалії. Завдяки постійному оновлення бази даних мережевих загроз та розширенню можливостей виявлення кібератак система достатньо легко адаптується до нових видів вторгнень. Підтримка та оновлення Symantec DeepSight здійснюється централізовано розробниками ПЗ. Система використовує експертний, статистичний, динамічний, машинного навчання та сигнатурний методи виявлення кібератак. Залежно від складності побудови системи та мережевої структури, управління може бути централізованим або розподіленим. Система є масштабованою, оскільки має чітку ієрархічну структуру, тобто при розширенні мережі збільшується лише кількість даних для аналізу, які необхідно опрацювати. Зазначена розробка здатна виявляти різного роду кібератаки, які були здійсненні на мережевому рівні, а також в певній мірі аналізувати журнали реєстрації низки програмних засобів та додатків. Symantec DeepSight Threat Management System дозволяє здійснювати завчасне (до нанесення шкоди підприємству) попередження щодо кібератак. Система дозволяє адміністраторам реалізувати превентивні заходи для захисту інфраструктури і компонентів мережі, а також протидіяти втратам продуктивності та нанесенню шкоди репутації компанії. За допомогою автоматизованих сповіщень із заданим пріоритетом на глобальному рівні система формує статистично надійну і дуже детальну інформацію про атаки, можливістю відстеження даних у часі, країни, галузі промисловості та інших параметрів. Існуючі можливості щодо виявлення кібератак, реалізації контрзаходів і використання методів протидії та додаткових джерел довідкової інформації дозволяє системі діяти негайно та ефективно[18].

Symantec DeepSight Threat Management System не містить спеціальних механізмів захисту або вони не розкриті розробниками. Система підтримується ОС Unix, Linux, Windows і MacOS.

4.6 Cisco IPS

Система запобігання вторгнень Cisco IPS (Cisco Intrusion Prevention System, розробка компанії Cisco, США) функціонує в режимі реального часу та забезпечує ідентифікацію і блокування шкідливого трафіку, черв'яків, вірусів, а також запобігання порушенню роботи додатків, інтелектуальне виявлення загроз і захист від них, фільтрацію на основі репутації і глобальні перевірки для запобігання загрозам (рис. 4.5).

Рисунок 4.5 - Моніторинг IPS-давачів з використанням Cisco IPS

Відповідно до [19] Cisco IPS реалізує функцію глибокого пакетного спостереження, яка ефективно протидіє широкому спектру мережевих кібератак. Елемент управління представлений інтегральною системою контролю за загрозою Cisco IOS і доповнений функцією Cisco IOS Flexible Packet Matching. Даний засіб дозволяє ефективно функціонувати комп’ютерній ме-

режі з урахуванням таких чинників:

- контроль доступності мережі (забезпечує мережевий (розподілений) захист від багатьох атак, експлойтів, хробаків та вірусів);

- швидкість виявлення джерела мережевих кібератак та оперативна реалізація контрзаходів;

- гнучкість розгортання та масштабованість (інтерактивне інспектування трафіку за допомогою будь-якої комбінації інтерфейсів локальної мережі та WAN маршрутизатора з налаштованими на протидію визначеним множинам кібератак відповідно до рівня ризику);

- робота з брандмауером Cisco IOS (контроль за функціями безпеки).

Системна архітектура даного програмного засобу складається з чотирьох основних модулів:

- виявлення загроз;

- виявлення мережевих пристроїв (підключень) та неперервний контроль їх роботи;

- комплексного аналізу атак, аномалій та системних подій;

- моніторингу комп'ютерної системи.

Програмний засіб Cisco IOS забезпечує виявлення DoS і DDoS-атак, кібератак на інфраструктуру мережі та нульового дня, моніторинг широкомовних пакетів, виявлення неавторизованих мережевих додатків та захист від шкідливих доменів і IP-адрес. Останні розробки забезпечують:

- спеціалізований захист датацентрів для веб-серверів, баз даних і сховищ;

- безпеку додатків корпоративного класу Oracle, SAP тощо;

- безперервний захист критично важливих серверів від уразливостей ОС додатків;

- зменшення часу на реагування та IT-витрати;

- легкість розгортання і управління (майстер розгортання включає шаблон сигнатур, орієнтований на дата центр).

Даний програмно-апаратний комплекс призначений для виявлення зловживань та аномалій у мережі. Він частково адаптивний до нових кібератак,

оскільки повністю залежний від структури та частоти оновлення бази даних атак. Cisco IPS є закритим програмно-апаратним комплексом з великим спектром налаштувань під особливості мережі і для виявлення вторгнень використовує наявні шаблони сигнатур та певну статистичну інформацію. Управління системою може здійснюватися централізовано або розподілено, залежно від складності побудови мережі. Швидке масштабоване розгортання системи здійснюються за допомогою динамічного управління політиками і установкою необхідних компонент з урахуванням структури та особливості мережі. Даний засіб здійснює безперервний захист критично важливих ресурсів мережі від різного роду уразливостей на рівні ОС та мережі. Cisco IPS дозволяє швидко виявляти джерела мережевих атак та визначати протидію, наприклад, ідентифікувати кібератаку, блокувати її і генерувати відповідне повідомлення. Також система забезпечує захищеність каналів передачі даних про атаку чи аномалію. Cisco IPS працює тільки на FTP і HTTP/HTTPS серверах з ОС Unix, Linux та Windows[14].

4.7 Suricata

Програмний засіб Suricata (розробка компанії Open Information Security Foundation, Бостон, США) має відкритий код, є безкоштовним, швидким, надійним та перспективним засобом виявлення мережевих загроз (рис. 4.6). Він призначений для запобігання та виявлення вторгнень у режимі реального часу, моніторингу мережевої безпеки, автоматичного аналізу та обробки PCAP-файлів.

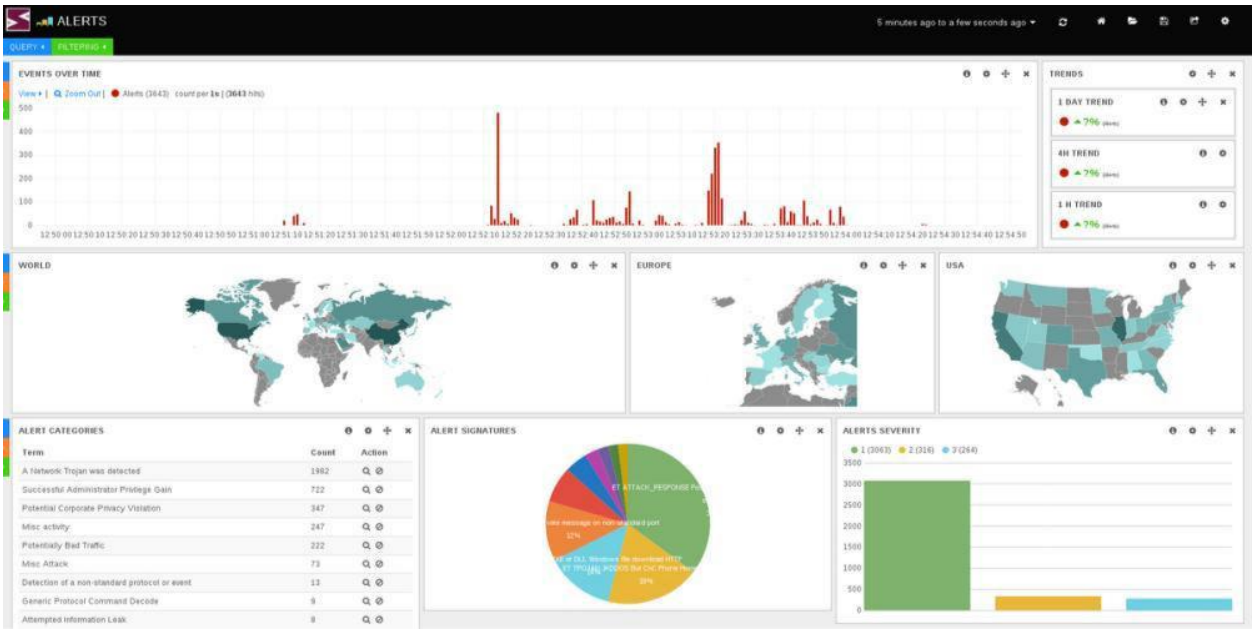


Рисунок 4.6 - Функціональне вікно ПЗ на основі Suricata

Suricata працює на рівні додатків і це дозволяє виявляти загрози, які можуть залишатися непоміченими. Контроль здійснюється на рівні протоколів TLS, ICMP, TCP, UDP, HTTP, FTP та SMB, а також є можливість виявляти спроби вторгнень, що приховуються під звичайними запитами та існує функція вилучення файлів для їх перевірки. Архітектура Suricata дозволяє оптимально розподілити обчислювальне навантаження між декількома ядрами процесора. Наприклад, якщо відеоадаптери більшість часу знаходяться в неактивному режимі, то їх частково можна завантажити певними обчисленнями.

Також як зазначається у [20] програмний засіб здатний виявляти уразливості в режимі реального часу, попереджувати вторгнення в систему, переглядати властивості мережевої безпеки та поєднувати властивості виявлення аномалій і зловживань. Крім того, Suricata має здатність адаптуватись до нових атак, працювати з іншим ПЗ (наприклад, Splunk, SIEM, Kibana тощо), контролювати мережевий трафік (використовуючи сигнатури та розширені правила подібні до Snort) і має потужну підтримку сценаріїв Lua для виявлення складних загроз.

Наявні засоби перевірки HTTP-трафіку засновуються на бібліотеці HTP. Також здійснюється контроль файлів (що передаються з використанням HTTP), розбір стисненого контенту, ідентифікація за URI, cookie, заголовками тощо.

Контент в потоці можна виділяти за допомогою маски і регулярних виразів, а ідентифікація файлів можлива за іменем, типом або контрольною MD5-сумою. Програмний засіб має централізоване управління і швидко виявляє уразливості та атаки завдяки розподіленій роботі між ядрами процесора та потоками. Спостереження за системою відбувається на системному і мережевому рівнях.

Suricata реакція на кібератаку здійснюється оперативно у тому випадку, якщо порушено не менше одного із налаштованих правил, шляхом маркування отриманих пакетів даних, одним із трьох маркерів:

- NF_ACCESS (доступ наданий);
- NF_DROP (доступ заборонений);
- NF_REPEAT (пакети маркуються та повторно направляються на правила брандмауера, який і вирішує подальше призначення відповідного пакету).

Даний програмний засіб є загальнодоступним для всіх користувачів і він не має механізмів захисту. Suricata функціонує на ОС Unix, Linux, Windows та MacOS[15].

4.8 InfoWatch ASAP

Спеціалізований програмно-апаратний комплекс InfoWatch ASAP (InfoWatch Automation System Advanced Protector, розробник компанія InfoWatch, Росія) позиціонує себе як інтелектуальне рішення для виявлення і запобігання кібератак, спрямованих на інформаційну інфраструктуру систем автоматичного управління виробничими і технологічними процесами. Завдяки запропонованому підходу і запатентованим технологіям захисту, рішення має низку переваг перед штатними засобами запобігання вторгнень, які реалізуються виробниками сучасного обладнання[21].

Комплекс InfoWatch ASAP (рис. 4.7) призначений для створення систем безпеки, адаптований до використання в технологічних мережах і здатний виявляти:

- цілеспрямовані атаки на рівні автоматичного управління та введення або виведення даних виконавчими пристроями;

- вторгнення (сигнатурний і статистичний аналіз) та аномалії в характеристиках технологічної ІС;

- команди для зміни налаштувань і мікропрограм технологічного обладнання;

- несанкціоновані підключення до мережі;

- витік інформації щодо стану технологічного процесу;

- уразливості в технологічних ІС.

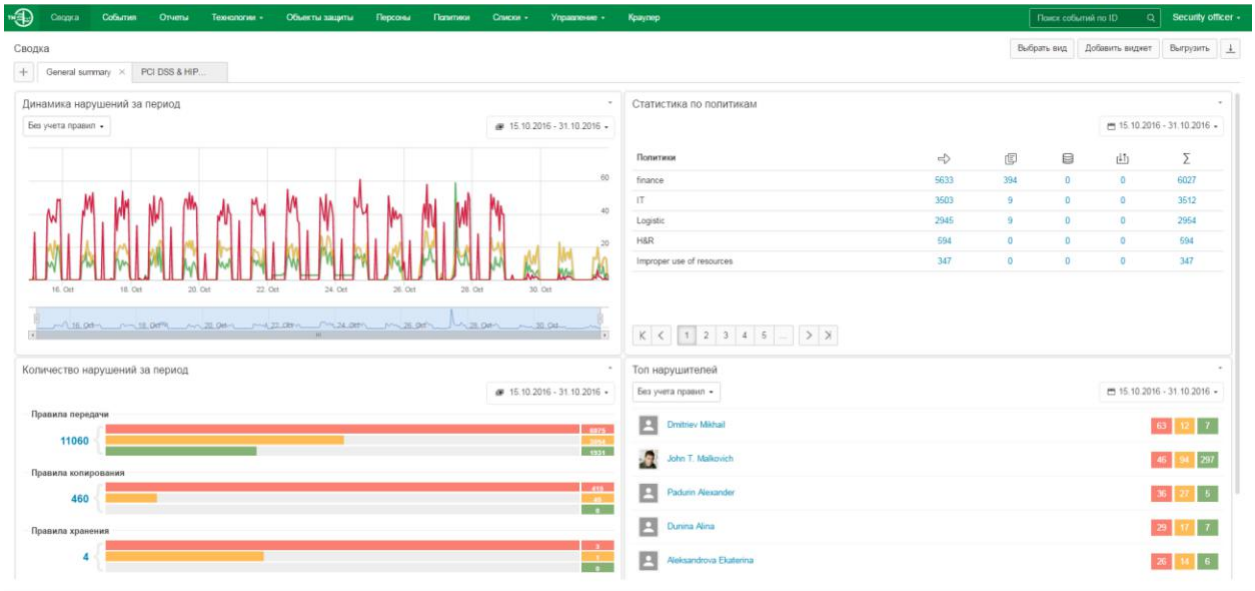


Рисунок 4.7 - Вікно звіту InfoWatch Traffic Monitor

Важливою складовою InfoWatch ASAP є методологічна база, що дозволяє будувати засоби захисту та ефективно протидіяти реально існуючим загрозам. Перевагою комплексу є захист від атак на всіх рівнях, незалежно від точки її виникнення. Комплексом підтримується більше 20 протоколів (з урахуванням галузевої специфіки), а також методологія аудиту та побудова моделі загроз, що забезпечує ефективний захист від кібератак.

Даний програмно-апаратний засіб має модульну архітектуру (основні і допоміжні модулі), що дозволяє легко адаптуватись та масштабуватись в залежності від потреб комп'ютерної мережі.[15]

До основних компонентів InfoWatch ASAP належать модулі:

- міжмережевого екранування;
- моніторингу та аналізу захищеності;
- виявлення і запобігання вторгнень;
- контролю коректності виконання;
- технологічного процесу.

Також до InfoWatch ASAP належать допоміжні компоненти:

- модуль забезпечення мережевої безпеки;
- підсистема аналітики і зберігання даних;
- графічний інтерфейс користувача.

Модульна структура дозволяє InfoWatch ASAP функціонувати в режимах моніторингу, інформування і попередження та виявляти кібератаки і аномалії на різних рівнях мережі (зовнішні і внутрішні атаки на інформаційну структуру підприємства). Постійне оновлення бази даних атак та наявність підсистеми їх моніторингу говорить про умовну адаптивність розробки, а підтримка ПЗ комплексу здійснюється лише його розробниками. InfoWatch ASAP використовує сигнатурний та статистичний методи виявлення вторгнень, а управління здійснюється централізовано за допо-могою адміністраторів. Оскільки даний комплекс в основному орієнтований на внутрішню організацію мережі підприємства і попередження атак внутрішнього сегменту, то він доволі легко адаптується до зазначеної мережі та є легко масштабованим[21].

4.9 Security Onion

Система Security Onion (розробка компанії Security Onion Solutions, США) є безкоштовним і відкритим ПЗ для ОС Linux, яке направлене на виявлення вторгнень, моніторинг стану безпеки підприємств, управління і перегляд системних журналів. Воно містить простий у використанні майстер налаштування розподілених давачів (рис. 4.8 - 4.9) та інтегрує відомі засоби безпеки Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Sguil, Squert,

CyberChef, NetworkMiner тощо[22].

Для ефективного функціонування Security Onion потребує:

- попереджувальні дані (формуються за результатами локального спостереження за допомогою Wazuh та мережевого за допомогою Snort або Suricata);

- дані про активи (спостереження за активами підприємства здійснює Bro);

- повний вміст даних (повний перегляд пакетів даних, що циркулюють, здійснюється завдяки netshifing);

- локальні дані (спостереження за локальними даними здійснюється за допомогою Beats, Wazuh, syslog тощо);

- дані сесії (перегляд сесійних даних відбувається за допомогою Bro);

- дані про транзакцій (дані, що надіслані через http/ftp/dns/ssl переглядаються за участю Bro).

Рисунок 4.8 - Вікно Kibana для перегляду даних підприємства та виявлення НАС

Рисунок 4.9 - Фрагмент процесу аналізу та візуалізації мережевих і локальних попереджень за допомогою Squert

Після встановлення відповідного ПЗ користувач отримує комплексне рішення щодо виявлення вторгнень на мережевому і локальному рівнях. В Security Onion поєднуються різні механізми, наприклад, сигнатурний та аномальний підходи, текстовий і графічний інструментарій тощо. Оскільки функціонал системи достатньо великий, то її основним недоліком є значний часовий ресурс необхідний для налаштування ПЗ. Але для пришвидшення роботи користувач може застосувати спрощений функціонал, для якого використовуються не всі програмні засоби.

Залежно від попередньо встановленого набору інструментів для виявлення вторгнень, вразливостей та інших дій НАС зазначений засіб працює в активному і пасивному режимах. Завдяки використанню в ПЗ різних детекційних методів та засобів (наприклад, Snort, Suricata, Snorby, Bro тощо), які доповнюють один одного, Security Onion містить систему оповіщення про безпеку та виявлення аномалій і шкідливих програм.

Відповідно до засобів аналізу (Kibana, CapME, CyberChef, Squert, ELSA, Sguil), мережевого (Snort, Suricata, Bro, Full Packet Capture) та локального перегляду (Beats, Wazup, Sysmon, Autoruns, Syslog) ПЗ має змогу реагувати на

нові загрози (наприклад, шляхом блокування підозрілої IP адреси, з якої надходить велика кількість незнайомого системі трафіка) та заносити їх в особисту базу даних.

Відповідно до наявних програмних засобів, дане ПЗ здатне зчитувати різні формати даних та інтегруватися в різні системи (наприклад, CapME може переглядати дані аналізу ПЗ Squert та логів і часових відміток ПЗ Kibana; Squert здатне переглядати HTTP логи, що сформовані ПЗ Bro; ELSA може інтегрувати свої рішення в логи програм Bro, NIDS alerts, OSSEC, syslog, а також інтегруватися в веб-браузери Chromium/ Chrome тощо).

Виявлення кібератак на систему відбується за рахунок набору встановлених засобів в ПЗ і засноване на сигнатурних базах даних, статистичних даних та повному контролі змін в системі. Також вбудовані засоби здатні динамічно реагувати на виникнення загроз і їх поведінку.

Управління системою може бути централізоване (наприклад, для Snort, Bro, Suricata тощо) і розподілене (наприклад, для OSSEC), а також є можливість адаптування та масштабування відповідно до потреб окремого користувача чи підприємства.

За допомогою сукупності програмних засобів спостереження за системою відбувається на системному і мережевому рівнях.

Реакція на кібератаку в реальному режимі часу здійснюється тільки у випадку використання в Security Onion відповідного функціоналу, що підтримується необхідним ПЗ із наданого списку. Спеціальні механізми захисту Security Onion не розкриті розробниками, вона підтримується ОС Unix та Linux[15].

4.10 Snort

Snort (розробка компанії Sourcefire, США) на світовому рівні є найпоширенішою безкоштовною мережевою системою виявлення та запобігання вторгнень (рис. 4.10 - 4.11).

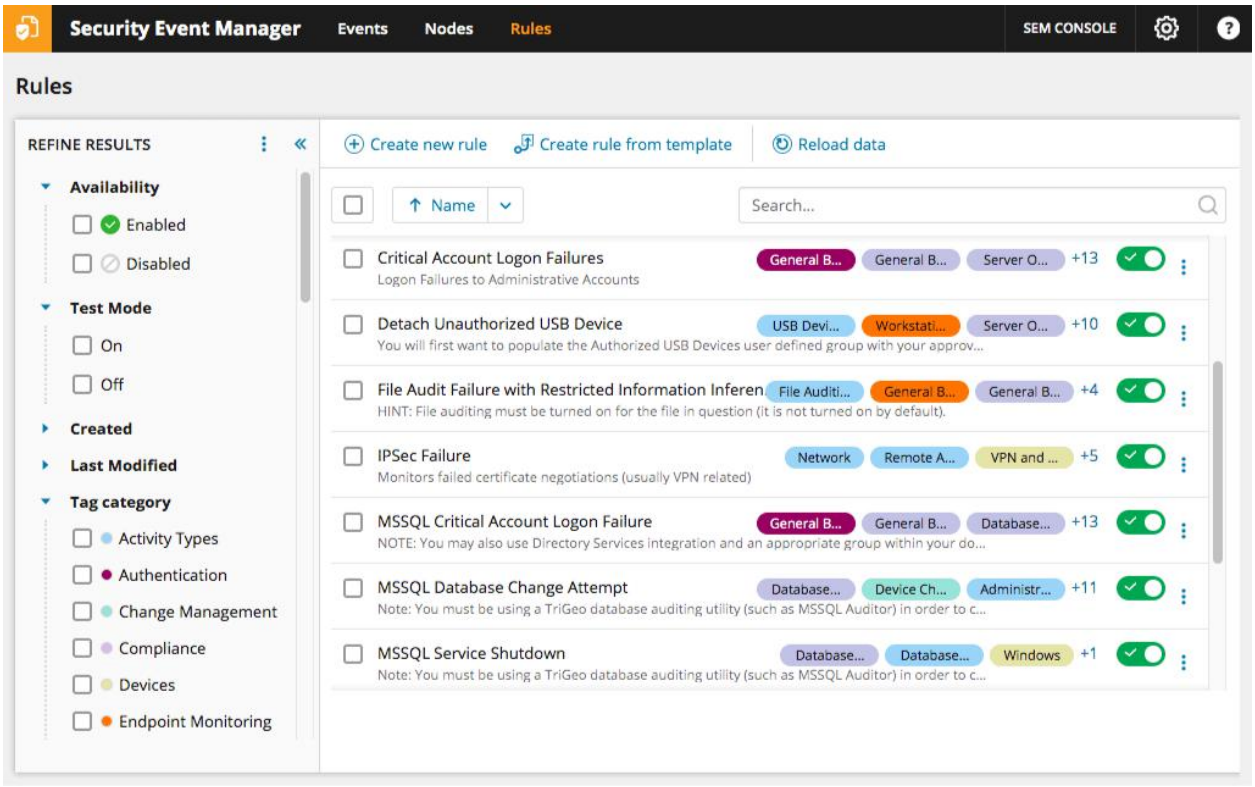


Рисунок 4.10 - Налаштування правил Snort

У структурі Snort виділяють [23] декілька режимів функціонування:

- аналіз пакетів;
- журналювання (протоколювання) пакетів;
- виявлення мережевих вторгнень;
- інші вбудовані можливості.

Архітектура системи розроблена з урахуванням ефективності та швидкості в роботі. Тому вона абсолютно проста і складається з:

- декодера пакетів;
- ядра виявлення;
- підсистеми оповіщення та реагування.

Декодер реалізує набір процедур для послідовної декомпозиції пакетів відповідно до рівнів мережевого стека, тобто прийнятий кадр послідовно перетворюється в пакет, сегмент і блок даних з урахуванням специфічних для даного рівня атрибутів сигнатур. Підтримуються протоколи канального рівня Ethernet, SLIP, PPP та ATM.

Ядро інтегрує існуючі правила в ланцюги, які складають відповідні двомірні послідовності, за якими здійснюється проходження кожного пакету.

Підсистема оповіщення (рис. 4.11) та реагування відповідає за збереження результатів аналізу трафіку в журналах реєстрації Snort або передачу цієї інформації системними службами реєстрації подій ОС.

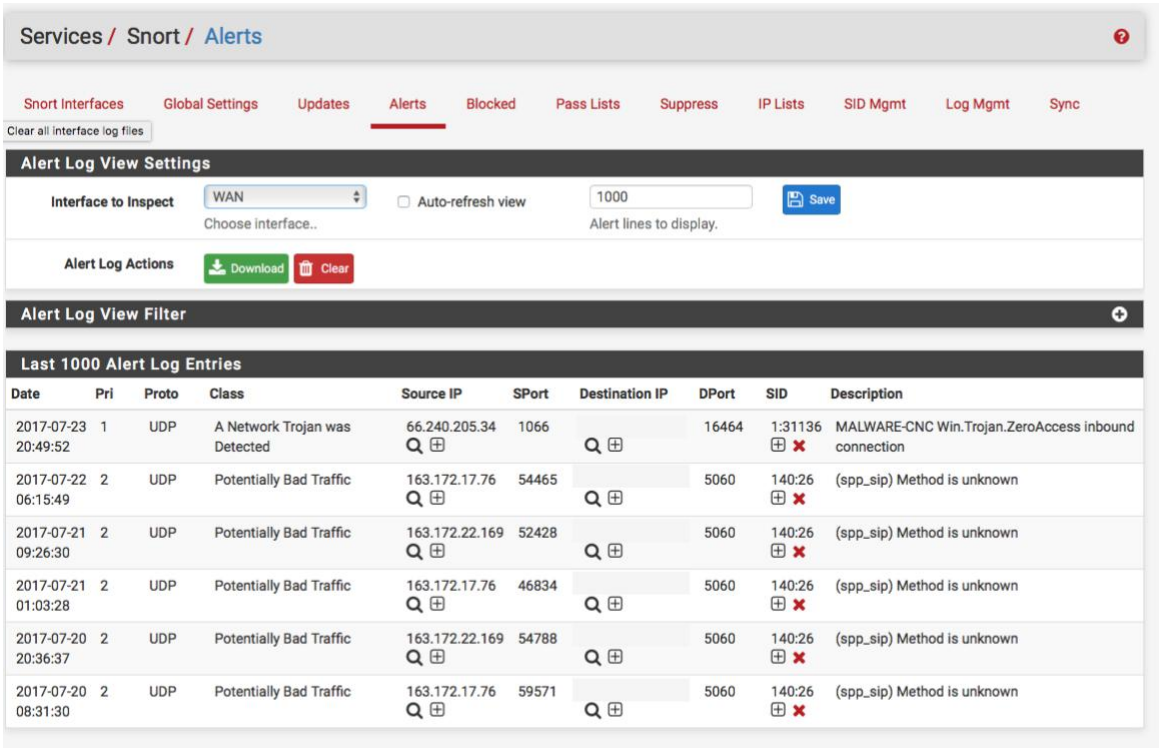


Рисунок 4.11 -Відображення сповіщень Snort

В системі використовується проста мова опису атак, яка повністю є в документації і дозволяє адміністраторам самостійно розширювати базу сигнатур. Кожне правило складається з двох частин - умови його застосування та дії. Крім того, в останніх версіях системи з'явилася спеціальна конструкція мови сигнатур, що дозволяє класифікувати мережевий трафік за ступенем потенційної небезпеки, який визначається експертом, що формує атрибути кібератаки. Також Snort виконує функції протоколювання, аналізу і пошуку за вмістом та широко використовується для активного блокування або пасивного виявлення цілої низки зловживань і аномалій (використовуються засоби інспекції протоколів і механізми виявлення аномалій), наприклад, пов'язаних з атаками на переповнення буфера, прихованим сканування портів, атаками на

веб-додатки, SMB-зондуванням, спробами визначення ОС тощо. Відповідне ПЗ в основному використовується для запобігання проникнення та блокування поточних кібератак.

Система функціонує на основі сигнатурного методу. Це дозволяє швидко виявляти всі задекларовані нею кібератаки. Але через неможливість повноцінного виявлення нових атак у мережі вона не є повністю адаптивною. Система Snort є програмним продуктом з відкритим вихідним кодом, що дозволяє легко змінювати її структуру. Вона здатна виконувати реєстрацію пакетів і в режимі реального часу здійснювати аналіз трафіку в IP-мережах.

Модуль аналізу трафіку базується на основі правил (сигнатур). До ядра виявлення можуть інтегруватися модулі сторонніх розробників (препроцесори) і проводити аналіз на одному з рівнів декомпозиції пакетів. За допомогою таких модулів можна розширити функціональність ядра виявлення та реалізовувати різні методи виявлення. Також до складу Snort був доданий модуль статистичного аналізу, який призначений для виявлення аномалій в мережевому трафіку.

В системі реалізоване централізоване управління за допомогою однієї станції. Оскільки Snort є представником системи з відкритим кодом, то продукт легко масштабувати та змінювати під власні потреби. Система дозволяє ефективно використовувати існуючі та самостійно створювати нові правила (рис. 4.10) для виявлення атак виключно на основі аналізу мережевого трафіку. Підсистема оповіщення та реагування включає базові методи реакції на кібератаку - розрив з'єднання з атакуючим об'єктом чи блокування його.

Механізми захисту в Snort реалізуються протоколом SNMPv2, у якому застосовуються функції шифрування паролів при передачі даних. Програмний засіб Snort працює на ОС Unix, Linux та Windows[15].

4.11 Prelude SIEM

Універсальна система Prelude SIEM (Security Information & Event

Management - управління інформацією про безпеку, розробка США) (рис. 4.12) збирає, нормалізує, сортує, корелює та звітує про всі події, пов'язані з безпекою незалежно від того, що породжує ці події. Також Prelude користується підтримкою інших подібних систем (snort, samhain, ossec, auditd тощо), що дозволяє покращити її функціонування[24].

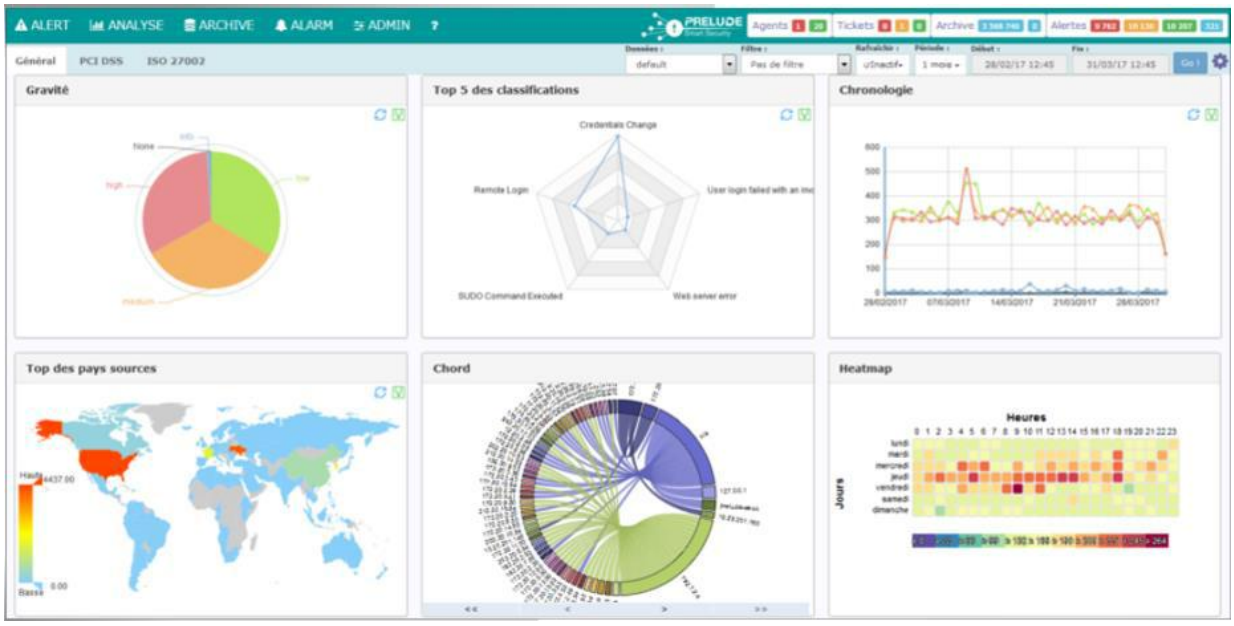


Рисунок 4.12 - Інтерфейс програми Prelude SIEM

Зазначене ПЗ є розподіленою гібридною СВА, яка складається з наступних базових компонент:

- ядро;
- агент;
- модуль кореляції;
- база даних;
- підсистема обміну повідомленнями;
- основний інтерфейс;
- модуль управління.

Ядро системи відповідає за прийом нормалізованих подій (від агентів, модулів кореляції, сторонніх систем або підпорядкованих менеджерів), запис у базу даних та інформування через e-mail. Агент системи працює локально (на одному сервері) та віддалено і здійснює прийом логів від різних систем (через

локальний файл або syslog на UDP-порт), розбирає або нормалізує їх на основі множини правил, що складаються з регулярних виразів, а нормалізовані події направляє ядру. Модуль кореляції підключається до ядра як агент і корелює події, що надійшли до ядра на основі плагінів, реалізованих у вигляді Python-скриптів. База даних зберігає всі події, які обробляються системою. Підсистема обміну повідомленнями включає додаткові ресурси, що безпосередньо підключаються до ядра за підтримки IDMEF (Intrusion Detection Message Exchange Format - спеціальний формат обміну повідомленнями про вторгнення). Основний інтерфейс реалізований на протоколі http і призначений для відображення результатів обробки подій, їх агрегації або фільтрації, виведення статистичної інформації тощо.

Система включає в себе модуль управління, який отримує і обробляє повідомлення сенсорів та генерує можливу реакцію на атаку, наприклад, блокування порушника на мережевому екрані (Net/IP Filter). Агенти реагування (відповідно до згенерованої реакції) реалізують необхідні заходи протидії кібератакам. Додаткові модулі аналізу мережевих даних роблять систему стійкою до некоректних мережевих пакетів на різних рівнях стека та виходу її компонентів з ладу. Це пов'язано з відправкою пакетів з неправильними контрольними сумами, синхронізацією сесій, випадковими відправленнями та іншими діями, що ігноруються.

Згідно [15] система побудована на сенсорах мережевого та вузлового рівнів. Перші аналізують вхідні данні на рівні мережі та генерують повідомлення щодо виявлення атак і відправляють їх модулям управління. Другі аналізують журнали реєстрації ОС та програмних застосунків (сенсори рівня системи), генерують повідомлення про виявлення аномалій і відправляють їх модулям управління. Мережеві сенсори орієнтовані на виявлення зловживань у системі, а вузлові на виявлення аномалій. Prelude заснована на сигнатурному підході, що дозволяє швидко виявляти всі задекларовані у системі атаки. Застосований підхід не ефективний відносно нових загроз, які не відображені у базі даних і тому система не є адаптивною до нових кібератак. Зазначена розробка є системою з відкритим початковим

кодом, що дозволяє її помодульно реконфігурувати. Вона, в основному, використовує метод протоколювання подій та шаблони атак. Управління здійснюється централізовано за допомогою керуючої консолі, якій компоненти системи самі надають ті параметри щодо їх функціонування, які можуть змінюватися. Також управління може здійснюватися через локальні конфігураційні файли на тих вузлах, де встановлені компоненти системи. Вся архітектура відкритої системи Prelude побудована за принципом використання відкритих стандартів. Підсистема обміну повідомленнями IDMEF дозволяє легко масштабувати та адаптувати зазначену розробку під різні потреби, а також інтегрувати її компоненти в системи сторонніх виробників і навпаки. Архітектура Prelude дозволяє адміністратору мережі стежити за активністю на рівні мережі та на рівні окремих вузлів. При розробці системи особливу увагу було приділено питанням безпеки та захищеності. Канали передачі даних шифруються за протоколом SSL, а також використовується спеціалізована бібліотека, яка запобігає класичним помилкам виходу за межі масивів і переповнення буферів. Програмний засіб Prelude працює на ОС Linux.

4.12 Висновки

У розділі були розглянуто вибір засобів виявлення несанкціонованого доступу на основі результатів методу оцінки ефективності засобів запобігання загроз безпеці інформації. Базуючись на результатах дослідження, було приведено практичне застосування апаратного засобу контролю вторгнення IBM ISS, який є системою запобігання вторгнень (IPS) і мережевою системою виявлення вторгнень (IDS) з відкритим вихідним кодом, здатною виконувати реєстрацію пакетів у реальному часі та здійснювати аналіз потоку даних інформаційних системах.

ВИСНОВКИ

Сучасний підхід до побудови ефективних систем виявлення вторгнень і виявлення ознак комп'ютерних атак на інформаційні системи сповнений недоліків і вразливостей, що дозволяють зловмисним діям успішно долати системи захисту інформації. Щоб докорінно змінити дану ситуацію, скоротивши дистанцію відставання в розвитку систем захисту від систем їх подолання, необхідний перехід від пошуку сигнатур атак до виявлення передумов їх виникнення. Крім того, такий перехід повинен сприяти підвищенню ефективності управління інформаційною безпекою та, нарешті, більш конкретних прикладів застосування нормативних та провідних документів, що вже стали стандартами.

На основі викладеного можна зробити висновок про те, що системи виявлення вторгнень все частіше стають важливими елементами інфраструктури мережевої безпеки. СВВ служать механізмами моніторингу та спостереження підозрілої активності. Вони можуть виявити атакуючих, які змогли обійти Firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить подальші кроки щодо запобігання атакам. Однак 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 їх базових характеристик, таких як клас атак, адаптивність, методи виявлення атак, управління системою, масштабованість, рівень спостереження за системою, реакція на атаку, захищеність та підтримувана ОС, 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 починаючи від антивірусного ПЗ, закінчуючи системами виявлення та запобігання вторгненням.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Обнаружение вторжений: краткая история и обзор | Открытые системы. СУБД | Издательство «Открытые системы» [Електронний ресурс] – Режим доступа: URL: https://www.osp.ua/os/2002/07-08/181714

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

3. Корниенко А.А. Системы обнаружения вторжений: современное состояние и направления совершенствования [Інтернет-ресурс]: / А.А. Корниенко, И.М. Слюсаренко. – Режим доступу: http://citforum.ru/security/internet/ids_overview вільний.

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

5. А. Завада, О. Самчишин, В. Охрімчук, "Аналіз сучасних систем виявлення атак і запобігання вторгненням", Інформаційні системи, Житомир: Збірник наукових праць ЖВІ НАУ, Т. 6, № 12, С. 97-106, 2012.

6. М.В. Грайворонський, О.М. Новіков. Безпека інформаційно-комунікаційних систем— 2009.— 608 с.

7. В. І. Мєшков, В. О. Віролайнен, Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах, УДК 004.056+65.012.12, Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ [Електронний ресурс] – Режим доступа: URL: https://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf

8. А. Корченко, С. Ахметова, "Классификация систем обнаружения вторжений", Інформаційна безпека. № 1 (13); № 2 (14). С. 168-175, 2014.

9. 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

10. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования [Електронний ресурс] – Режим доступа: URL: http://citforum.ru/security/internet/ids_overview

11. Лукацкий А. Обнаружение атак. - СПб.: БХВПетербург, 2001. – 624с

12. Т.Н. Шипова, В.В. Босько, И.А. Березюк, Ю.М. Пархоменко, Анализ современных методов обнаружения вторжений в компьютерные системы, УДК 004.7 : 004.31 С.133-137 [Електронный ресурс]. Режим доступа: URL: http://www.hups.mil.gov.ua/periodic-app/article/15262/soi_2016_1_30.pdf

13. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – М.: Горячая линия-Телеком, 2013. – 220 с

14. С. Казмірчук, А.Корченко, Т.Паращук, Аналіз систем виявлення вторгнень, ЗАХИСТ ІНФОРМАЦІЇ, ТОМ 20, №4, ЖОВТЕНЬ-ГРУДЕНЬ 2018, DOI: 10.18372/2410-7840.20.13425, УДК 004.056.53(045), С. 259-276 [Електронный ресурс]. Режим доступу: URL: http://jrnl.nau.edu.ua/inde x.php/ZI/arti cle/ download/13425/18726

15. І.Терейковський, А.Корченко, Т.Паращук, Є.Педченко, Аналіз відкритих систем виявлення вторгнень, DOI: 10.18372/2225-5036.24.13431, УДК 004.056.53(045), 2018, vol. 24, issue 3, С. 201-216

16. Платформа Arbor Networks Spectrum выявляет угрозы безопасности за рекордно быстрое время, [Електронний ресурс]. Режим доступа: URL: http://allta.com.ua/arbor-networks-spectrum

17. Kaspersky Anti Targeted Attack (KATA) Platform, М.: АО Лаборатория Касперского, 2017. [Електронный ресурс]. Режим доступу: URL: https://support.kaspersky.ru/kata

18. Системы раннего оповещения Symantec [Електронный ресурс]. Режим доступа: URL: https://www.cnews.ru/reviews/free/software2005/case/sym antec/index1.

19. Cisco IPS 4500 Series. Описание продукта Cisco IPS 4500. Київ : ТОВ Інфобезпека, 2018. [Електронний ресурс]. Режим доступу: URL: http://www. infobezpeka.com/products/apatnye/Cisco_IPS_450 0_Series/

20. День сурка. Осваиваем сетевую IDS/IPS Suricata — «Хакер» [Електронний ресурс]. Режим доступ: URL: https://xakep.ru/2015/06/28/suri cata-ids-ips-197/

21. ГК InfoWatch | Информационная безопасность в цифровой экономике. [Електронний ресурс]. Режим доступу: URL: https://www.infowatch.ru/

22. Security Onion: дистрибутив Linux для сетевых аудитов | ITIGIC [Електронний ресурс]. Режим доступу: URL: https://itigic.com/ru/security-onion-linux-distribution-for-network-audits/

23. OpenNET: статья - Система обнаружения вторжений на базе IDS Snort (snort ids), [Електронний ресурс]. Режим доступу: URL: https://www.opennet.ru/b ase/ sec/snort_ids.txt.html

24. Prelude SIEM (Intrusion Detection System) – Wikipedia, [Електронний ресурс]. Режим доступу: URL: https://en.wikipedia.org/wiki/Prelude_SIEM_ (Intrusion_Detection_System)

25. Кльоц Ю.П., Петляк Н.С., Блаута В.В. Виявлення аномального трафіку у загальнодоступних комп’ютерних мережах. Збірник наукових праць за матеріалами XIV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2022». Хмельницький – 2022. – 142-145с.

ДОДАТОК А

(обов'язковий)

Копії публікацій

УДК 004.77

Кльоц Ю.П., Петляк Н.С., Блаута В.В.

Хмельницький національний університет

ВИЯВЛЕННЯ АНОМАЛЬНОГО ТРАФІКУ У ЗАГАЛЬНОДОСТУПНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

Розглянуто можливі типи атак та засоби їх виявлення в загальнодоступних комп'ютерних мережах. Визначено необхідність розроблення нових методів та засобів недопущення зловмисних дій щодо третіх осіб зловмисниками, підключеними до загальнодоступних комп'ютерних мереж.

Possible types of attacks and means of their detection in public computer networks are considered. The need to develop new methods and means of preventing malicious actions against third parties by criminals connected to public computer networks was determined.

Із розвитком Інтернету та збільшенням потреб у інформаційних та комп'ютерних технологіях збільшується об'єм трафіку у комп'ютерних мережах. Вони зазнають все більшої кількості мережевих атак, які розвиваються швидкими темпами. Що негативно впливає на функціонування мережі та завдає шкоди у різних державних чи приватних сферах діяльності.

Загальнодоступні комп'ютерні мережі (ЗКМ) переважно використовують у громадських місцях для забезпечення доступу до мережі Інтернет для відвідувачів кафе, торгових центрів тощо. Дана можливість збільшує кількість відвідувачів за рахунок незначних капіталовкладень. Підключення до такої мережі може здійснити будь-яка особа без ідентифікації. Це, в свою чергу, дозволяє зловмиснику додатково приховати себе при виконанні зловмисних дій.

Ідентифікація зловмисного трафіку та аномалій відіграє важливу роль для безпеки. Тому потрібно використовувати системи виявлення вторгнень (СВВ, Intrusion Detection System, IDS), які можуть захистити мережу від існуючих та майбутніх загроз. IDS забезпечують вчасне оповіщення адміністраторів системи.

Відомі системи виявлення вторгнень на основі машинного навчання [1-4] орієнтовані на виявлення атак на корпоративні мережі, та не націлені на виявлення атак, що виходять із ЗКМ та використовують її потужності для атак на третіх осіб.

Розглянемо відомі, поширені типи атак у ЗКМ та опис їх роботи.

Атака на відмову в обслуговуванні (DoS) – це атака, спрямована на надмірне перевантаження комп'ютера або мережі, що робить їх недоступними для

призначених користувачів. DoS-атаки досягають цього, переповнюючи ціль трафіком або надсилаючи їй інформацію, яка викликає збій.

Існує два загальні методи DoS-атак: перевантаження служб або збій служб. До популярних атак належать:

- Атаки переповнення буфера - найпоширеніша DoS-атака. Концепція полягає в тому, щоб відправити на мережеву адресу більше трафіку, ніж система може опрацювати.
- ICMP-флуд - використовує неправильно налаштовані мережеві пристрої, надсилаючи підроблені пакети, які перевіряють пінг на кожному комп'ютері цільової мережі, а не лише на одному конкретному комп'ютері. Ця атака також відома як атака смурфа або пінг смерті.
- SYN flood - надсилає запит на підключення до сервера, але ніколи не завершує рукостискання. Триває, доки всі відкриті порти не будуть переповнені запитами, і жоден з них не стане доступним для підключення законних користувачів.

У порівнянні з аналогічним періодом 2021 року кількість DoS-атак (та DDoS-атак) зросла в 4,5 рази [5].

Злом паролів – це процес використання прикладної програми для визначення невідомого або забутого пароля до комп'ютера чи мережевого ресурсу. Застосовують для того, щоб допомогти зловмиснику отримати несанкціонований доступ до ресурсів.

Зломщики паролів використовують два основні методи визначення правильних паролів: атаки підбір і словник [6].

Паролі часто є слабкою ланкою в кібербезпеці організації чи окремої людини. Фактично, для базових атак на веб-додатки (BWAA) понад 80% зломів можна пояснити викраденими обліковими даними. Середньостатистичний користувач Інтернету має 240 облікових записів, які потребують пароля [7].

Фішинг використовується шахраями, що видають себе за довірених осіб, для виманювання персональних даних. Це може досягатися шляхом проведення масових розсилок електронних листів від імені популярних брендів. Також проявами фішингу можуть бути спливаючі вікна, що з'являються на сайтах, яким довіряють користувачі.

Із статистикою стрімкого розвитку фішингових атак можна ознайомитись у джерелі [8].

Отож, кількість атак та їх характер суттєво збільшилась у порівнянні з попередніми роками [9]. Саме тому слід дбати про безпеку мережі задля своєчасного виявлення вторгнень.

Усі з перерахованих атак виконуються з використанням ресурсів віддалених комп'ютерних систем, які, зазвичай, допомагають приховати зловмисника.

Розглянемо відомі IDS та їх функціональні можливості.

Snort - безкоштовна система виявлення вторгнень, яка дозволяє самостійно та без зусиль писати правила для виявлення атак. Дозволяє захистити певний сегмент локальної мережі від зовнішніх атак з Інтернету. Працює на ОС Windows, Linux та Unix.

Wireshark - це аналізатор мережевих протоколів. Він дозволяє фіксувати та інтерактивно переглядати трафік, що пересилається в комп'ютерній мережі, має багатий і потужний набір функцій і є найпопулярнішим у світі інструментом такого роду. Він працює на більшості комп'ютерних платформ, включаючи Windows, macOS, Linux і UNIX. Професіонали з мереж, експерти з безпеки, розробники та викладачі в усьому світі регулярно використовують його. Він є у вільному доступі у відкритому доступі та випущений під GNU General Public License версії 2 [10].

Інструмент Network Monitor, реалізований у Windows та Microsoft Systems Management Server (SMS), дозволяє виконувати моніторинг мережевого трафіку. Моніторинг можна проводити в реальному часі або, перехопивши і зберігши мережевий трафік, аналізувати його пізніше.

Suricata - це високопродуктивне програмне забезпечення для аналізу мережі та виявлення загроз із відкритим кодом, яке використовується більшістю приватних і державних організацій і впроваджується великими постачальниками для захисту своїх активів [11].

Security Onion класифікується як безкоштовна система виявлення мережевих атак (Network Intrusion Detection System, NIDS), але він також включає функції хостової системи виявлення вторгнень (Host-based intrusion detection system, HIDS). Система створена для операційної системи Linux з акцентом на управління журналами, моніторингом безпеки підприємства та виявлення атак.

Наявні методи навчання IDS не орієнтовані на виявлення атак, що виходять із мережі.

Можливість анонімного підключення до мережі дозволяє підвищити рівень анонімності при проведенні атак на сторонні ресурси. Доцільно розробити нові методи та засоби, що не допускатимуть зловмисних дій користувачів цієї мережі по відношенню до третіх осіб, оскільки відомі системи цього забезпечити не можуть.

Перелік посилань

1. Real-Time DDoS Attack Detection System Using Big Data Approach. Url: https://doi.org/10.3390/su131910743

2. CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques. Url: https://ieeexplore.ieee.org/document/9116932
3. Variational LSTM Enhanced Anomaly Detection for Industrial Big Data. Url: https://ieeexplore.ieee.org/document/9195000
4. Klots, Y., Titova, V., Petliak, N., Cheshun, V., Salem, A.-B.M., Research of the Neural Network Module for Detecting Anomalies in Network Traffic, CEUR Workshop Proceedingsthis, 2022, 3156, pp. 378–389
5. У першому кварталі 2022 року DDoS-атаки б'ють рекорди. Url: https://10guards.com/ua/articles/ddos-attacks-at-an-all-time-high-in-q1-2022/
6. Top cybersecurity statistics, trends, and facts. Url: https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html
7. What is password cracking? Url: https://www.techtarget.com/searchsecurity/definition/password-cracker
8. State of Phishing & Online Fraud. Url: https://boost.bolster.ai/rs/540-RFH-299/images/2021_PhishingandFraudReport-109.pdf
9. Data Breach Investigations Report. Url: https://www.verizon.com/business/resources/T41b/reports/dbir/2022-data-breach-investigations-report-dbir.pdf
10. Wireshark Frequently Asked Questions. Url: https://www.wireshark.org/faq.html#_what_is_wireshark
11. Suricata. Url: https://suricata.io/
12. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Url: https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00077-7

ДОДАТОК Б

(обов’язковий)

Презентація роботи

1

Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

Блаута Вадим Віталійович

Метод оцінки ефективності систем захисту та виявлення несанкціонованого доступу в інформаційних системах

Спеціальність: 123 – Комп’ютерна інженерія

Науковий керівник: кандидат технічних наук, доцент Кльоц Ю.Л.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА МАГІСТЕРСЬКОЇ РОБОТИ

Метою роботи є розроблення методу оцінки ефективності систем захисту та виявлення несанкціонованого доступу та відповідних рекомендацій по вибору таких засобів для підвищення надійності та безпеки функціонування інформаційних систем

Об'єкт дослідження – інформаційні системи та інформаційні потоки в них

Предмет дослідження – оцінка ефективності методів та засобів виявлення вторгнень в інформаційні системи

Задачі дослідження:

1) провести аналіз інформаційних систем та потоків даних, що в них містяться;
2) провести аналіз найбільш поширених методів та засобів виявлення несанкціонованого доступу до ІС;
3) розробити метод оцінки ефективності систем захисту;
4) реалізувати захист ІС та дослідити його ефективність

Методи дослідження базуються на основних положеннях методів аналізу даних, імітаційного комп'ютерного моделювання трафіку, математичної статистики.

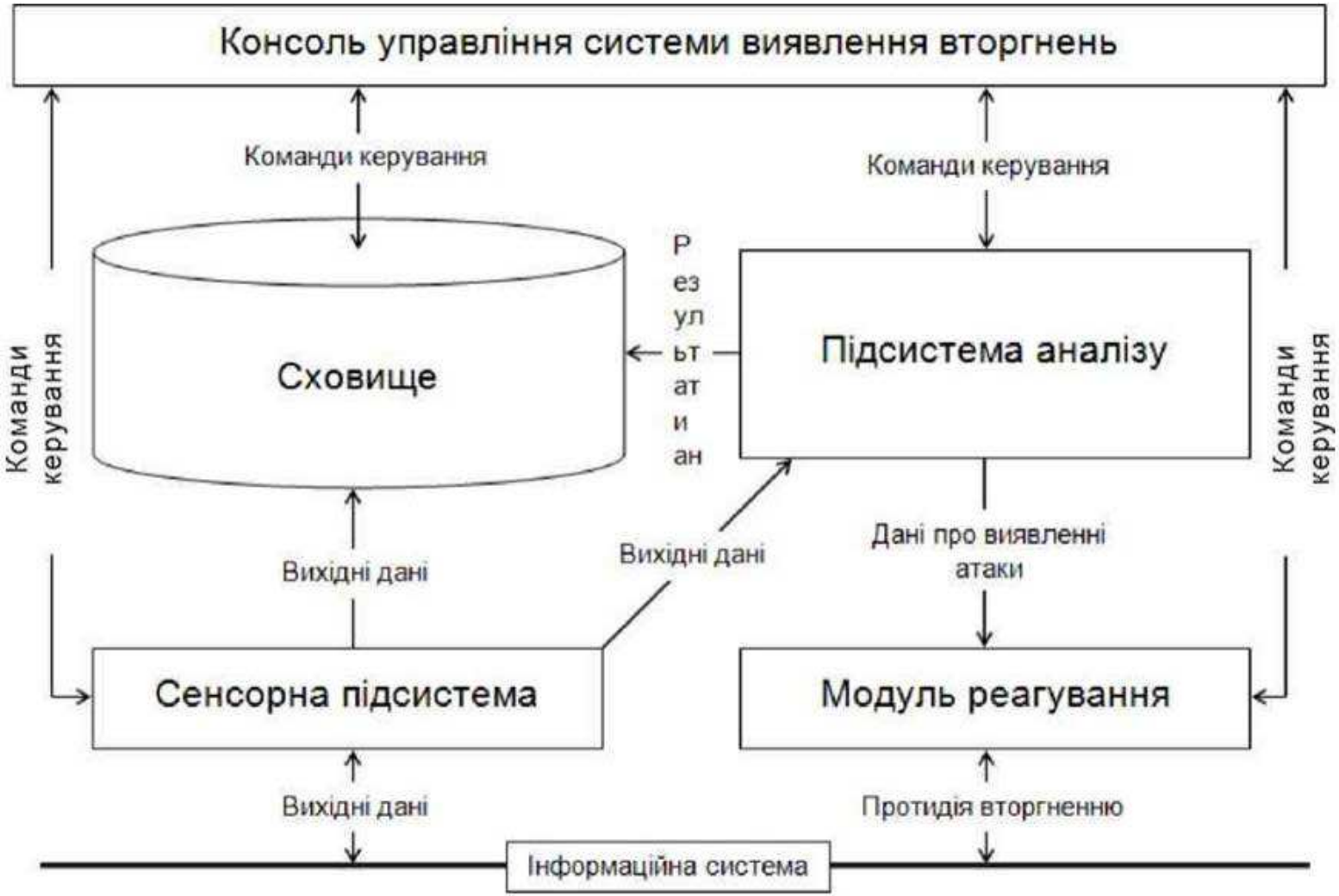
Наукова новизна одержаних результатів:

1. Проведено аналіз сучасних систем виявлення вторгнень в інформаційних системах. Встановлено, що вони використовують сигнатурний аналіз трафіку.
2. Визначено критерії оцінки ефективності методів та систем захисту від несанкціонованого доступу.
3. Розроблено метод оцінки ефективності засобів захисту та на його основі запропоновано вибір таких засобів для інформаційних систем.

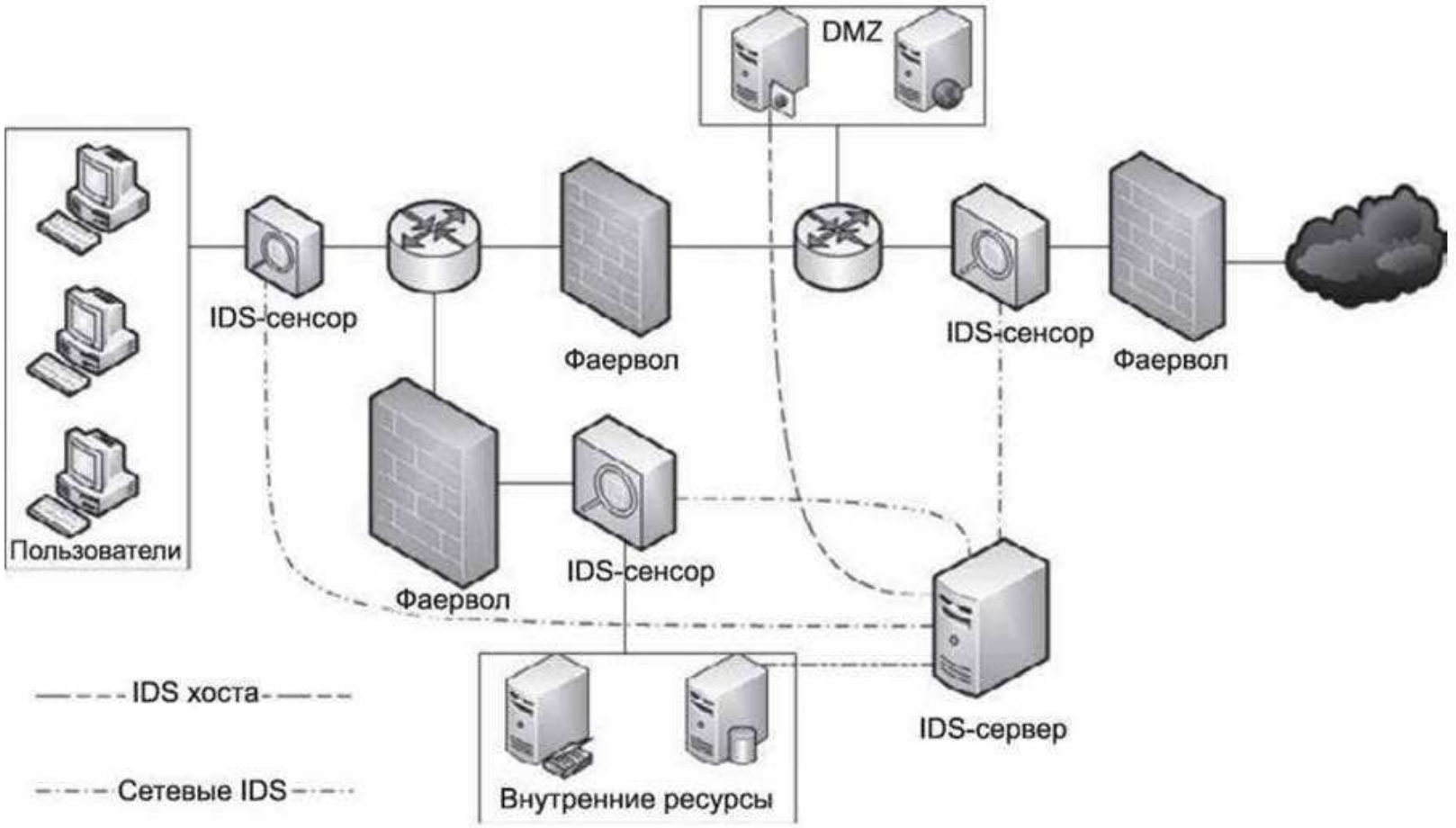
Апробація роботи. Наукові результати і основні положення кваліфікаційної роботи магістра доповідались і обговорювались на всеукраїнській і міжнародній науково-практичних конференціях.

Публікації. За темою кваліфікаційної роботи опубліковано 1 тези у збірнику наукових праць.

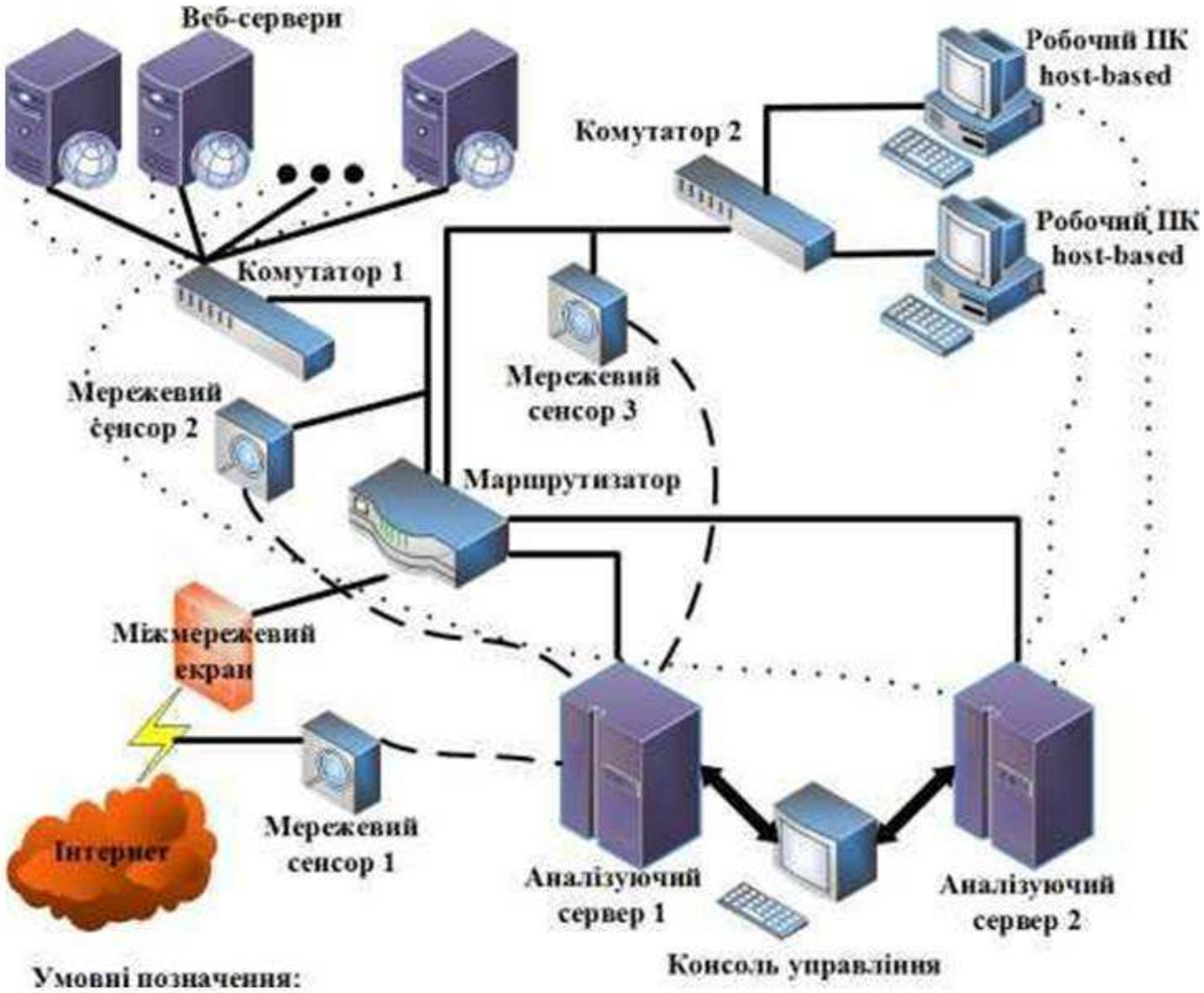
Типова архітектура систем виявлення вторгнень



Розташування сенсорів системи IDS



Типова структура інформаційної системи хостинг провайдера



Виявлення аномалії - контрольоване навчання (навчання з вчителем")

№	Методи виявлення	Використовується в системах	Опис методу
1	Моделювання правил	W&S	Система виявлення протягом процесу навчання формує набір правил, що описують нормальну поведінку системи. На стадії пошуку несанкціонованих дій система застосовує отримані правила і в разі недостатньої відповідності сигналізує про виявлення аномалії
2	Описова статистика	IDES, NIDES, EMERLAND, JiNao, HayStack	Навчання полягає в зборі простої описової статистики безлічі показників, що захищається системи в спеціальну структуру. Для виявлення аномалій обчислюється «відстань» між двома векторами показників - поточними і збереженими значеннями. Стан в системі вважається аномальним, якщо отримане відстань досить велика.
3	Нейронні мережі	Hyperview	Структура застосовуваних нейронних мереж різна. Але у всіх випадках навчання виконується даними, що представляють нормальну поведінку системи. Отримана навчена нейронна мережа потім використовується для оцінки аномальності системи. Вихід нейронної мережі говорить про наявність аномалії

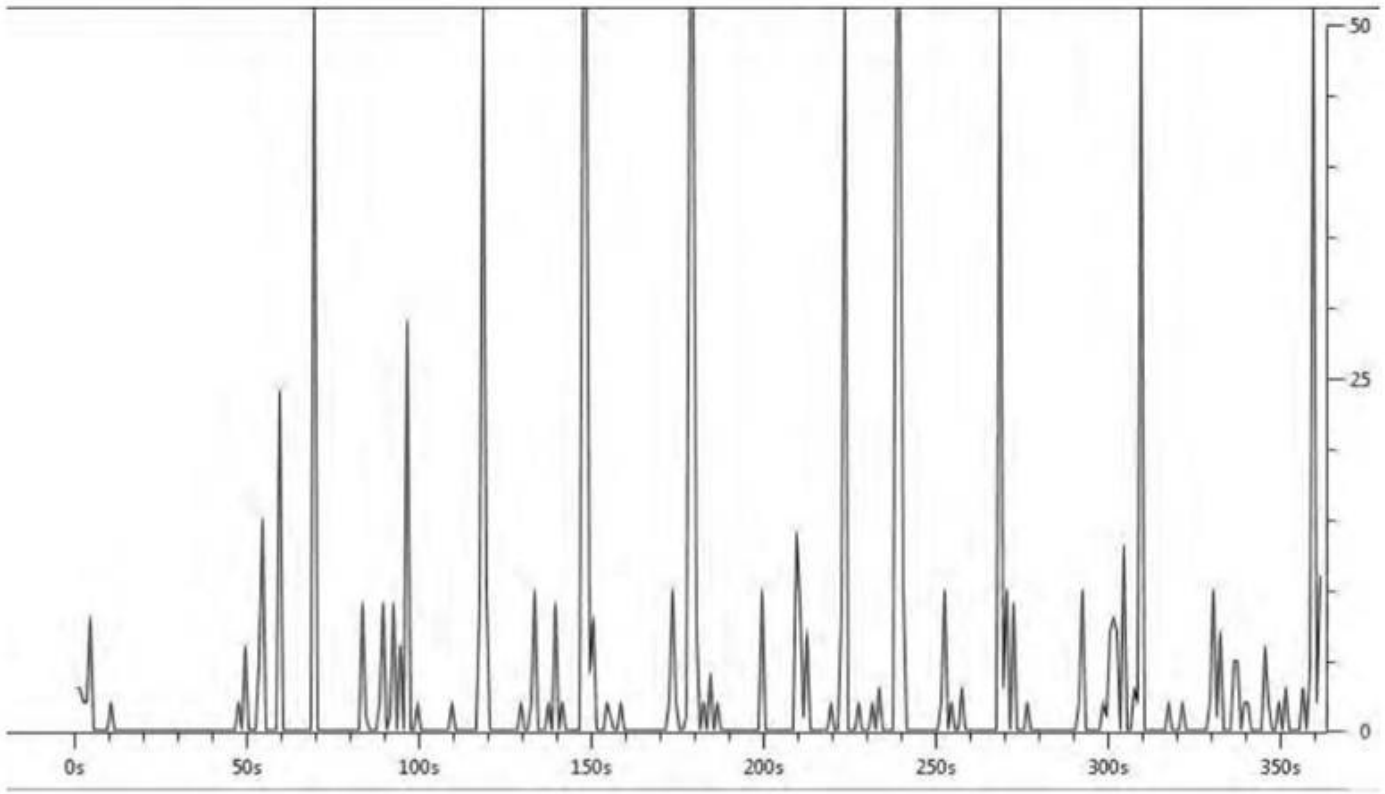
Виявлення аномалій - неконтрольоване навчання (навчання без вчителя")[8]

№	Методи виявлення	Використовується в системах	Опис методу
1	Моделювання множини станів	DPEM, JANUS, Bro	Нормальна поведінка системи описується у вигляді набору фіксованих станів і переходів між ними. Де стан являє собою вектор певних значень параметрів вимірювань системи.
2	Описова статистика	MIDAS, NADIR, Haystack, NSM	Аналогічний відповідному методу в контрольованому навчанні.

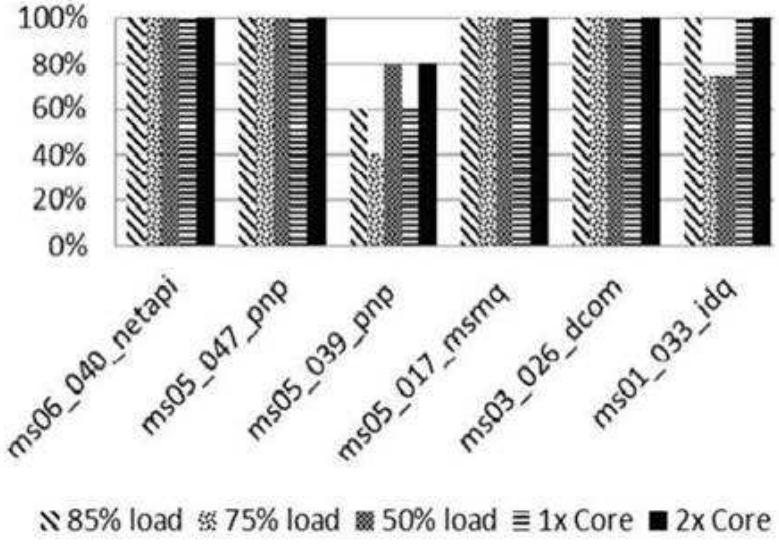
Виявлення зловживань - контрольоване навчання ("навчання з вчителем")

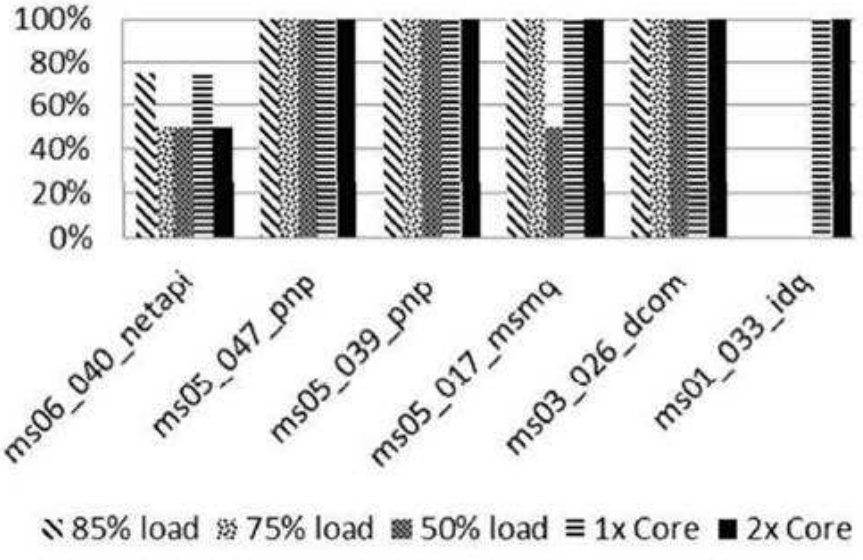
№	Методи виявлення	Використовується в системах	Опис методу
1	Моделювання поведінки (станів)	USTAT, IDIOT	Вторгнення представляється як послідовність станів, де стан - вектор значення параметрів оцінки системи. Необхідна і достатня умова наявності вторгнення - присутність цієї послідовності. Виділяють два основних способи подання сценарію вторгнень: 1) у вигляді простого ланцюжка подій; 2) з використанням мереж Петрі, де вузли - події.
2	Експертні системи	NIDES, EMERLAN D, MIDAS, DIDS	Експертні системи являють процес вторгнення у вигляді різного набору правил. Дуже часто використовуються продукційні системи.
3	Моделювання правил	NADIR, HayStack, JiNao, ASAX, Bro	Простий варіант експертних систем.
4	Синтаксичний аналіз	NSM	Системою виявлення виконується синтаксичний розбір з метою виявлення певної комбінації символів, що передаються між підсистемами і системами комплексу, що захищається.

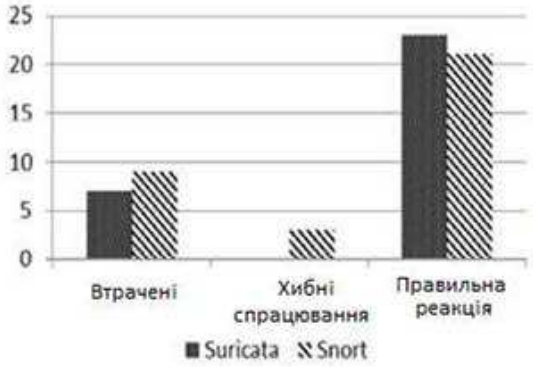
Нормальне навантаження трафіку при бездротовому з'єднанні

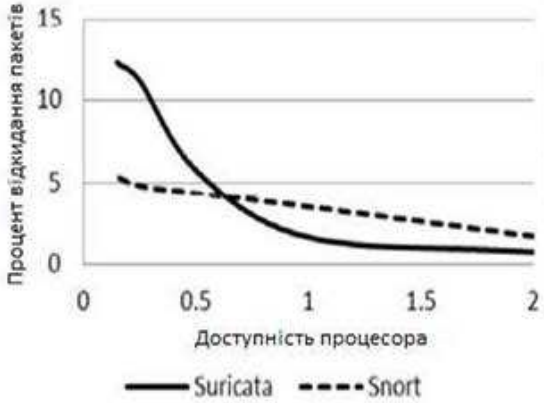


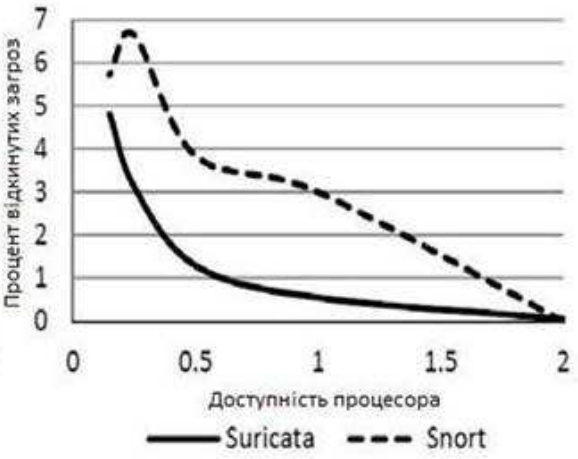
Результати застосування систем виявлення вторгнень











Висновки

1. Проведено аналіз сучасних систем виявлення вторгнень в інформаційних системах. Встановлено, що вони використовують сигнатурний аналіз трафіку.
2. Визначено критерії оцінки ефективності методів та систем захисту від несакціонованого доступу.
3. Розроблено метод оцінки ефективності засобів захисту та на його основі запопоновано вибір таких засобів для інформаційних сивтем.

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод оцінки ефективності систем захисту та виявлення несанкціонованого доступу в інформаційних системах

Автор: Блаута Вадим Віталійович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма:Програмування та захист комп`ютерних систем і мереж

Науковий керівник:Кльоц Ю.П. к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих методів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 12.6% і адресується до 338 першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Ю.П. Кльоц

Завідувач кафедри КбКСМ, гарант ОП _____ Ю.П. Кльоц

Дата: 06.12.2022

5. Негативні сторони роботи В роботі відсутній деталізований опис технічних засобів реалізації методу (програмних або програмно-апаратних).

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження Окремі описи в пояснювальній записці подано стисло, що ускладнює сприйняття матеріалу наукової роботи фахівцями в обраній предметній галузі. Не на всі джерела з переліку є посилання в тексті пояснювальної записки

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «задовільно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Тіщенко Сергій Костянтинович, д.т.н., завідувач кафедри телекомунікаційних медійних та інтелектуальних технологій

« 7 » грудня 2022р. (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Магістр Блаута Вадим Віталійович

Тема Метод оцінки ефективності систем захисту та виявлення несанкціонованого доступу в інформаційних системах

Спеціальність 123 – Комп'ютерна інженерія

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень 12; кількість сторінок записки 90

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі розроблено метод оцінки ефективності систем та засобів виявлення несанкціонованого доступу в інформаційних системах для підвищення надійності та безпеки функціонування систем .

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведено огляд та аналіз сучасних інформаційних систем та захисту даних у них, виконане обгрунтування актуальності теми дослідження і виконана постановка задачі. В другому розділі виконано аналіз моделей та методів, що лежать в основі сучасних засобів виявлення несанкціонованого доступу. В третьому розділі визначено основні положення методу та розроблено систему оцінки ефективності. Четвертий розділ присвячено апробації методу.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну наукову і практичну цінність. Наукова цінність полягає у розробці методу оцінки ефективності засобів виявлення несанкціонованого доступу в інформаційних системах для підвищення надійності та безпеки функціонування систем. Практична цінність результатів дослідження полягає в обґрунтуванні вибору засобів та їх налаштуванню для різноманітних інформаційних систем .

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Блаути Вадима Віталійовича
ПІБ здобувача вищої освіти
студента ФІТ, 2 курсу, групи КІ1м-21-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

5.12.2022
дата

підпис

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

Дата перевірки:
11.12.2022 17:08:04 EET

Дата звіту:
11.12.2022 17:27:32 EET

ID перевірки:
1013269333

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100008300

Назва документа: **Магістерська_Блаута**

Кількість сторінок: 77 Кількість слів: 15271 Кількість символів: 123761 Розмір файлу: 1.19 MB ID файлу: 101302

6.44%
Схожість

Найбільша схожість: 2.29% з джерелом з Бібліотеки (ID файлу: 1009560945)

4.24% Джерела з Інтернету	75	Сторінка 79
2.82% Джерела з Бібліотеки	194	Сторінка 80

3.78% Цитат

Цитати	11	Сторінка 81

Не знайдено жодних посилань

20.5%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 0%)

20.5% Вилучення з Інтернету	1	Сторінка 82

Немає вилучених бібліотечних джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	12

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 3.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 10%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 109348 Название: Метод оцінки ефективності систем захисту та виявлення несанкціонованого доступу в інформаційних системах Добавлено в БД: 2022-12-11 Авторы: Блаута В,В, Руководители: Кльоц Ю.П, Консультанты: Оппоненты:	Символы	Лексемы	Символы	Лексемы
	96889	1501	5369 (6%)	91 (6%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы