МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра комп'ютерних інформаційних технологій

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____Аліна САВЧЕНКО

"____"_____2021 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
"МАГІСТРА"

ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ
"ІНФОРМАЦІЙНІ УПРАВЛЯЮЧІ СИСТЕМИ ТА ТЕХНОЛОГІЇ"

Тема: "Модель системи виявлення вторгнень для інтелектуальних середовищ"

Виконавець: Сторощук Олександр Андрійович

Керівник: доцент Моденов Юрій Борисович

Нормоконтролер: _____ Ігор РАЙЧЕВ

Київ — 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії

Кафедра Комп'ютерних інформаційних технологій

Галузь знань, спеціальність, освітньо-професійна програма: 12 "Інформаційні технології", 122 "Комп'ютерні науки", "Інформаційні управляючі системи та технології"

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Аліна САВЧЕНКО
«____»_____2021р.

ЗАВДАННЯ

на виконання дипломної роботи студента

студента Сторощука Олександра Андрійовича

1. **Тема роботи:** «Модель системи виявлення вторгнень для інтелектуальних середовищ» затверджена наказом ректора від 12.10.2021 за № 2228/ст.
2. **Термін виконання роботи:** з 12.10.2021 р. по 31.12.2021 р.
3. **Вихідні дані до роботи:** дослідити основні поняття та завдання сучасних систем виявлення вторгнень для інтелектуальних середовищ, проаналізувати сучасні системи виявлення вторгень.
4. **Зміст пояснювальної записки**: сучасні системи виявлення вторгнень, аналіз та впровадження комплексної моделі системи виявлення вторгнень в інтелектуальне середовище.
5. **Перелік обов'язкового ілюстративного матеріалу:** слайди, презентація.

6. Календарний план-графік

№ з/п	Завдання	Термін виконання	Підпис керівника
1.	Отримання завдання на дипломну роботу та побудова графіку виконання роботи.	12.10.2021 - 15.10.2021	Виконано
2.	Пошук, огляд та аналіз літературних джерел	16.10.2021 – 28.10.2021	Виконано
3.	Обґрунтування рішення	29.10.2021 – 30.10.2021	Виконано
4.	Збір інформації	01.11.2021 – 07.11.2021	Виконано
5.	Аналіз основних понять та завдань сучасних систем виявлення та запобігання вторгнень	08.11.2021 – 14.11.2021	Виконано
6.	Аналіз існуючих систем виявлення вторгнень та програмного забезпечення для інтелектуальних середовищ	15.11.2021 – 20.11.2021	Виконано
7.	Порівняння існуючих систем виявлення вторгнень для інтелектуальних середовищ	21.11.2021 – 28.11.2021	Виконано
8.	Реалізація системи виявлення вторгнень та програмного забезпечення	29.11.2021 – 09.12.2021	Виконано
9.	Оформлення і друг пояснювальної записки	10.12.2021 – 12.12.2021	Виконано
10.	Оформлення презентації	13.12.2021 – 16.12.2021	Виконано
11.	Отримання рецензій від опонентів	17.12.2021	Виконано

7. **Дата видачі завдання:** 12.10.2021р.

Керівник дипломної роботи Юрій МОДЕНОВ

Завдання прийняв до виконання Олександр СТОРОЩУК

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальним обсягом складає 71 сторінку, має 17 рисунків, 3 таблиці. Список використаних джерел містить 39 найменувань і займає 4 сторінки.

Метою роботи є проектування моделі системи виявлення вторгнень для інтелектуальних середовищ.

В дипломній роботі розглянуто проблеми забезпечення захисту інтелектуальних середовищ. Проаналізовані основні поняття та завдання сучасних систем виявлення вторгнень. В ході аналізу існуючих систем виявлення та запобігання вторгнень були виявлені певні недоліки, а саме: в системі Snort було виявлено відсутність можливості багатопотокової обробки, нативної підтримки IP версії 6; в системі Bro виявлено складність в налаштуванні та використанні, та підтримку лише ОС Linux.

Було реалізовано модульну систему виявлення вторгнень SELKS. Розроблено покрокову інструкцію для налаштування мережевого маршрутизатора, робочих станції, мобільних пристроїв користувачів, комутаторів та точок доступу.

Ключові слова: СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ, ІНТЕЛЕКТУАЛЬНЕ СЕРЕДОВИЩЕ, «ІНТЕРНЕТ РЕЧЕЙ», ІНФОРМАЦІЙНА БЕЗПЕКА, РОЗУМНИЙ БУДИНОК.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ	–	Програмне забезпечення
ІТ	–	Інформаційні технології
ПК	–	Персональний комп’ютер
СВВ	–	Система виявлення вторгнень
ОС	–	Операційна система
IoT	–	«Інтернет речей»(Internet of Things)
WSN	–	Бездротова сенсорна мережа
CoAP	–	Протокол обмеженого застосування

ВСТУП

Актуальність. Розумні будинки є одним з найбільш перспективних застосувань нової технології Інтернету речей (IoT).

Зі зростанням кількості пристроїв, пов'язаних з Інтернетом речей, таких як розумні термостати, розумні холодильники, розумні динаміки, розумні лампи і розумні замки, розумні будинки обіцяють зробити наше життя простіше і комфортніше. Однак більш широке впровадження таких інтелектуальних пристроїв призводить до збільшення потенційних ризиків для безпеки і порушень домашньої конфіденційності.

Для подолання таких ризиків системи виявлення вторгнень представлені в якості відповідних інструментів, які можуть забезпечити захист на мережевому рівні для інтелектуальних пристроїв, розгорнутих в домашніх умовах. Ці системи відстежують мережеву активність підключених до розумного будинку пристроїв і фокусуються на попередженні про підозрілу або шкідливу активність. Вони також можуть боротися з виявленими аномальними діями, перешкоджаючи самозванцям у доступі до пристроїв жертв. Однак використання таких систем в контексті розумного будинку може бути складним через апаратні обмеження пристроїв, які можуть обмежити їх здатність протистояти існуючим і виникаючим векторам атак.

Економічні звіти підтверджують, що ринок підключених домашніх пристроїв стає найбільшим сегментом Інтернету речей з сімома мільярдами пов'язаних інтелектуальних пристроїв в 2018 році, що становить 26% світового ринку пристроїв Інтернету речей. Крім того, в 2019 році кількість домовласників з інтелектуальними системами зросла майже до 150 мільйонів розумних домовласників по всьому світу. Основними причинами широкого впровадження такої технології є комфорт, зручність, безпека, а також економія енергії і витрат.

Метою є проектування моделі системи виявлення вторгнень для інтелектуальних середовищ.

Для досягнення цієї мети необхідно розв’язати такі **задачі**:

1. Проаналізувати основні поняття та завдання сучасних систем виявлення вторгнень;
2. Провести аналіз та порівняння існуючих систем виявлення вторгнень для інтелектуальних середовищ;
3. Реалізувати систему виявлення вторгнень для інтелектуальних середовищ.

Об’єкт дослідження – процеси проектування моделі системи виявлення вторгнень.

Предмет дослідження – системи виявлення вторгнень для інтелектуальних середовищ.

Для досягнення поставленої мети необхідно проаналізувати особливості таких систем для захисту мереж, їх функціональні можливості, переваги та недоліки. Крім того сформувати належний підхід, щодо розгортання реального зразка системи. Тобто дослідити методи захисту інтелектуальних середовищ та зупинитися на найбільш ефективних способах виявлення вторгнень.

Основними науковими результатами роботи є:

- *отримала подальший розвиток* система виявлення вторгнень для інтелектуальних середовищ, яка за рахунок спеціального налаштування моніторингу та поведінкових фільтрів дозволяє вчасно відстежувати та попереджувати потенційні інциденти домашньої конфіденційності.

Практична цінність роботи полягає у тому, що на базі запропонованої системи виявлення вторгнень розроблено покрокову інструкцію для налаштування мережевого маршрутизатора, робочих станцій, мобільних пристроїв користувачів, комутаторів та точок доступу. Крім того, отримані результати будуть корисними для інших мережевих інфраструктур державного та приватного сектору.

РОЗДІЛ 1. СУЧАСНІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ СЕРЕДОВИЩ

1.1. Інтернет речей, інтелектуальні середовища та їх особливості

Неймовірні досягнення в повсякденному використанні електронних послуг і додатків призвели до масових досягнень в телекомунікаційних мережах і появи концепції Інтернету речей (IoT). Інтернет речей - це зростаюча комунікаційна парадигма, в якій пристрої служать об'єктами або" речами", здатними сприймати навколишнє середовище, з'єднуватися один з одним і обмінюватися даними через Інтернет. До 2022 року один трильйон IP-адрес або об'єктів буде підключений до Інтернету через мережі IoT. Парадигма Інтернету речей останнім часом використовується для створення інтелектуальних середовищ, таких як розумні міста і розумні будинки, з різними областями додатків і пов'язаними з ними послугами.

Мета розробки таких інтелектуальних середовищ полягає в тому, щоб зробити життя людини більш продуктивною і комфортною за рахунок вирішення проблем, пов'язаних з умовами життя, споживанням енергії та промисловими потребами. Ця мета безпосередньо відображена в значному зростанні доступних сервісів і додатків на основі Інтернету речей в різних мережах. Наприклад, розумне місто Падуя в Італії є успішним прикладом розумного міста, заснованого на системі Інтернету речей.

Інтелектуальні середовища складаються з датчиків, які працюють разом для виконання операцій. Бездротові датчики, технології бездротового зв'язку та IPv6 сприяють розширенню інтелектуальних середовищ.

Такі середовища різноманітні: від розумних міст і розумних будинків до розумного охорони здоров'я та розумних послуг. Інтеграція систем Інтернету речей та інтелектуальних середовищ робить інтелектуальні об'єкти більш ефективними. Однак системи Інтернету речей схильні до різних атак на безпеку, таким як атаки типу "відмова в обслуговуванні" (DOS) і розподілені атаки типу "відмова в обслуговуванні" (DDoS). Такі атаки можуть завдати значної шкоди службам Інтернету речей і додаткам інтелектуального середовища в мережі Інтернету речей. Отже, забезпечення безпеки систем Інтернету речей стало серйозною проблемою. Наприклад, в п'ятницю, 21 жовтня 2016 року, по всій території США була запущена серія DDoS-атак, в ході яких використовувалися уразливості безпеки в системах Інтернету речей. Ці атаки вплинули на пристрої Інтернету речей, веб-сайти та онлайн-сервіси, такі як Twitter, Netflix і PayPal.

Парадигма Інтернету речей

Концепція Інтернету речей була розроблена з моменту заснування Центру автоматичної ідентифікації в Массачусетському технологічному інституті (MIT) в 1999 році. Центр автоматичної ідентифікації створив номер електронного коду продукту (EPC), який залежить від радіочастотної ідентифікації (RFID), у 2003 році. Це стало найважливішою технологією Інтернету речей. Однак Інтернет речей - це усталена парадигма, і вона визначається кількома способами з різних точок зору.

Інститут інженерів електротехніки та електроніки (IEEE) визначає IoT як набір елементів з датчиками, які утворюють мережу, підключену до Інтернету.

Міжнародний союз електрозв'язку (MCE) визначає Інтернет речей в трьох вимірах як мережу, доступну в будь-якому місці, в будь-який час, чим завгодно і ким завгодно.

Європейський інститут телекомунікаційних стандартів (ETSI) замість того, щоб використовувати вираз "Інтернет речей (IoT)", визначає міжмашинний зв'язок (M2M) як автоматизовану систему зв'язку, яка приймає рішення і обробляє операції з даними без прямого втручання людини.

Проект з координації та підтримки глобальної діяльності та стандартизації, пов'язаної з RFID (CASAGRAS), створив нову концепцію Інтернету речей, яка охоплює дві точки зору: з'єднання фізичних об'єктів з віртуальними об'єктами через глобальну мережу без будь-якого втручання людини в максимально можливій мірі і неймовірне збільшення додатків Інтернету речей в традиційних мережах через масштаби маркетингу Інтернету речей.

Більш того, Cisco, промислова організація, працює над технологією Інтернету речей під назвою Інтернет всього (IoE). Cisco узагальнила концепцію IoE як мережу, що складається з людей, даних, речей і процесів. Таким чином, інформація і дії створюються в цій мережі і передаються через неї.

Архітектури систем Інтернету Речей

Що стосується проектування Інтернету Речей, IEEE працює над проектом (IEEE P2413) для визначення архітектурної структури Інтернету речей. Мета цього проекту - описати домени Інтернету Речей і різні додатки в цих доменах. Ця архітектура Інтернету Речей розділена на три рівні: рівень додатків, рівень мереж і передачі даних та рівень датчиків.

Загальна архітектура Інтернету Речей розділена на п'ять рівнів:

- Рівень сприйняття - це апаратний рівень, що складається з датчиків і фізичних об'єктів різних форм. Ці апаратні елементи забезпечують ідентифікацію, збір, зберігання та обробку інформації. Інформація, що виводиться з цього рівня, відправляється на наступний рівень (мережевий рівень) для передачі в систему обробки.
- Мережевий рівень - це рівень передачі, який передає інформацію від фізичних об'єктів або датчиків в систему обробки по захищених лініях з використанням зв'язку система. Ця система зв'язку може бути як дротовою, так і бездротовою і може бути заснована на різних технологіях, в залежності від фізичного об'єкта або компонентів датчика. Інформація, що виводиться з цього рівня, відправляється на наступний рівень (рівень проміжного програмного забезпечення).

- Рівень проміжного програмного забезпечення - відповідає за управління службами на пристроях Інтернету речей для створення з'єднань між пристроями Інтернету речей, що надають одну і ту ж послугу. Крім того, рівень проміжного програмного забезпечення зберігає інформацію, що надходить з мережевого рівня, в базі даних для полегшення прийняття рішень на основі операцій обробки інформації.
- Прикладний рівень - відповідає за глобальне управління додатками Інтернету речей. Рівень застосування залежить від інформації, оброблюваної на рівні проміжного програмне забезпечення. Крім того, рівень додатків залежить від специфіки різних реалізованих додатків Інтернету речей, таких як додатки для інтелектуальної промисловості, будівель, міст і охорони здоров'я.
- Бізнес-рівень – також відповідає за глобальне управління додатками Інтернету речей, а також за управління послугами на пристроях Інтернету речей. Бізнес-рівень створює бізнес-модель, яка залежить від інформації, оброблюваної на прикладному рівні, і від аналізу результатів цих операцій обробки інформації.

Ці рівні охоплюють три домени, а саме домен додатків, мережевий домен і фізичний домен; таким чином, Інтернет речей може бути налаштований відповідно до потреб різних інтелектуальних середовищ. Домен додатків охоплює управління і використання; мережевий домен відповідає за передачу даних; фізичний домен відповідає за збір інформації.

Хмарні обчислення та Інтернет речей

Системи Інтернету речей з'єднують величезну кількість пристроїв і датчиків, обмінюючись величезним обсягом даних і підтримуючи величезну кількість послуг. Управління і аналіз цих даних пред'являють певні особливі вимоги, такі як потужна обробка, масивне зберігання і високошвидкісні мережеві можливості.

Хмарні обчислення забезпечують високу обчислювальну потужність, величезну ємність сховища і настроювані ресурси з можливостями віртуалізації

для управління великими обсягами даних, зібраних в інтелектуальних середовищах на основі Інтернету речей.

Завдяки інтеграції систем хмарних обчислень та інтелектуальних середовищ на основі Інтернету речей, до інтелектуальних речей можна легко отримати доступ і управляти ними в будь-який час і в будь-якому місці, а також надавати більш якісні послуги за допомогою моделі Інтернету речей.

Однією з важливих проблем при використанні системи хмарних обчислень для Інтернету речей є синхронізація між різними постачальниками хмарних обчислень. Друге завдання полягає в забезпеченні сумісності між загальними середовищами хмарних сервісів і вимогами Інтернету речей. Проблеми безпеки є основним чинником, що перешкоджає впровадженню хмарних обчислень підприємствами та державними організаціями.

Таким чином, здатність дотримуватися необхідних обмежень безпеки для задоволення потреб Інтернету речей на платформі хмарних обчислень є життєво важливою вимогою. Одним з можливих варіантів є надійне і ефективне рішення для забезпечення безпеки, таке як системи виявлення вторгнень(СВВ). Крім того, стандартизація, вдосконалення та управління розгортанням систем Інтернету речей і їх підключенням до хмари є додатковими проблемами, які слід брати до уваги.

Проблеми безпеки в інтелектуальних середовищах на основі Інтернету Речей

Безпека систем Інтернету речей є серйозною проблемою у зв'язку зі збільшенням числа сервісів і користувачів в мережах Інтернету Речей.

Інтеграція систем Інтернету Речей та інтелектуальних середовищ робить інтелектуальні об'єкти більш ефективними. Однак наслідки вразливостей безпеки Інтернету речей дуже небезпечні в критично важливих інтелектуальних середовищах, що використовуються в таких областях, як медицина і промисловість. В інтелектуальних середовищах на основі Інтернету Речей без надійних систем безпеки додатки і сервіси будуть піддаватися ризику. Конфіденційність,

цілісність і доступність є трьома важливими концепціями безпеки додатків і послуг в інтелектуальних середовищах на основі Інтернету речей; таким чином, для вирішення цих проблем інформаційна безпека в системах Інтернету Речей вимагає більшої уваги до досліджень. Наприклад, розумні будинки на базі Інтернету Речей стикаються з проблемами безпеки та конфіденційності, які охоплюють всі рівні архітектури Інтернету Речей.

Створення інтелектуальних середовищ в реальному світі стикається з двома помітними перешкодами: безпекою систем Інтернету Речей і складністю і сумісністю середовищ Інтернету речей.

Атаки, такі як DOS-або DDoS-атаки на мережі Інтернету Речей, впливають на служби Інтернету Речей і, отже, впливають на послуги, що надаються інтелектуальними середовищами.

Дослідники вивчають проблеми безпеки IoT з різних точок зору, однією з яких є вразливість комунікаційних протоколів Інтернету Речей. Це дослідження зосереджується на системах виявлення вторгнень для парадигми Інтернету Речей, незалежно від будь-якого конкретного протоколу; таким чином, це дослідження зосереджується на проблемах безпеки, з якими стикаються системи Інтернету Речей, на основі визначення IEEE та загальної архітектури IoT.

Проблеми безпеки в системах Інтернету Речей пов'язані з проблемами безпеки, що виникають на різних рівнях IoT. Фізичні пошкодження, апаратні збої і обмеження потужності - це проблеми, з якими доводиться стикатися на фізичному рівні. DOS-атаки, перехоплення, атаки на шлюзи і несанкціонований доступ є проблемами, що відносяться до мережевого рівня. Атаки шкідливого коду, уразливості додатків і програмні помилки - це проблеми, з якими доводиться стикатися на прикладному рівні.

Проблеми, пов'язані з безпекою будь-якої системи Інтернету Речей, можна розділити на чотири типи: автентифікація і фізичні загрози, ризики конфіденційності, проблеми з цілісністю даних і проблеми конфіденційності.

- Проблеми, пов'язані з автентифікацією, і фізичні загрози є першими проблемами, які впливають на систему Інтернету Речей. Рівень сприйняття включає в себе безліч пристрої, таких як датчики, які залежать від власних систем безпеки; таким чином, вони схильні до фізичних атак.

- Ризики, пов'язані з конфіденційністю, виникають між IoT пристроями і шлюзами на мережевому рівні. Обмеженість ресурсів низькорівневих пристроїв в системах Інтернету Речей створює непряму проблему щодо конфіденційності передачі даних в мережах.

- Третій клас проблем безпеки стосується цілісності даних між службами і додатками. Проблеми з цілісністю даних виникають, коли атаки з підміною або перешкоди впливають на систему Інтернету речей. DOS-атаки, DDoS-атаки і зондуючі атаки - це довільні атаки, які можуть завдати шкоди додаткам і службам IoT.

- Проблеми четвертого типу пов'язані з конфіденційністю. Конфіденційність інформації є важливим аспектом безпеки в системах Інтернету речей. Різні компоненти використовують різні типи технологій ідентифікації об'єктів; таким чином, кожен об'єкт має свою власну ідентифікаційну мітку, яка містить особисту інформацію, інформацію про місцезнаходження та переміщення. Управління та моніторинг додатків і сервісів в системі Інтернету Речей означають, що конфіденційність інформації піддається ризику; наприклад, використання системи, заснованої на методі глибокої перевірки пакетів, для довірених операцій в системі вважається порушенням конфіденційності інформації. Будь-який нав'язливий доступ до системи управління без дозволу загрожує конфіденційності інформації користувачів Інтернету речей.

1.2. Основні поняття та завдання сучасних систем виявлення вторгнень в інтелектуальних середовищах.

Кількість шкідливого трафіку збільшується, і нові загрози створюються щодня. Загрози стають дедалі серйознішими та складнішими.

Внутрішні загрози та організовані кіберзлочинці, які шукають конфіденційну інформацію, таку як номер соціального страхування та банківські рахунки, є однією з найбільших проблем сьогодні. Такі загрози посилюються, і компаніям потрібні інструменти для цього аби не допускати компрометації їх системи.

В результаті зросла потреба в захисті конфіденційної інформації користувачів. Організації почали прагнути зберегти конфіденційність, цілісність і доступність своїх мережевих ресурсів, і для захисту від мережевих вторгнень був використаний ряд методів.

Однак навіть незважаючи на те, що ці заходи забезпечують певний рівень безпеки, вони були визнані недостатніми з цілого ряду причин:

Використання мережевого екрану(брандмауер). Мережевий екран - це апаратне або програмне рішення, яке використовується для забезпечення дотримання політики безпеки в приватній мережі. Він в основному використовується для керування трафіком в приватній мережі.

Класифікація брандмауера. Те, як брандмауер забезпечує більший захист, залежить від самого брандмауера та політики, налаштованої на ньому.[6] Основними доступними сьогодні технологіями брандмауера є:

- Апаратний брандмауер. Апаратний брандмауер є кращим, коли брандмауер потрібен на більш ніж одній машині. Апаратний брандмауер забезпечує додатковий рівень безпеки фізичної мережі. Недоліком такого підходу є те, що якщо один брандмауер порушений, усі машини, які він обслуговує, вразливі.
- Брандмауер програмного забезпечення. Програмний брандмауер - це другий рівень безпеки і захищає мережу від шкідливих програм, хробаків та вірусів та вкладень електронної пошти. Він схожий на будь-яку іншу програму і може бути налаштований на основі мережевих вимог. Програмний брандмауер

можна налаштувати для включення антивірусних програм та блокування сайтів та зображень.

- Брандмауер фільтрування пакетів. Фільтр брандмауера фільтрування пакетів мережевого або транспортного рівнів. Він забезпечує мережеву безпеку шляхом фільтрації мережевих комунікацій на основі інформації, що міститься в заголовку TCP / IP кожного пакету. Брандмауер вивчає ці заголовки та використовує інформацію, щоб вирішити, чи приймати та спрямовувати пакети до місця призначення або відмовити пакет, скидаючи їх. Брандмауер фільтрування пакетів - це маршрутизатор, який використовує таблицю фільтрації, щоб вирішити, які пакети потрібно відкинути.
- Брандмауер проксі. Встановлення проксі-комп'ютера між клієнтом та корпоративним комп'ютером. Коли клієнтський процес користувача надсилає повідомлення, брандмауер проксі запускає серверний процес для отримання запиту. Сервер відкриває пакет на рівні програми та підтверджує, чи запит легітимний чи ні. Якщо він легітимний, сервер діє як клієнтський процес і відправляє повідомлення на реальний сервер, інакше повідомлення відкидається. Таким чином запити зовнішніх користувачів фільтруються на основі вмісту на рівні додатків.
- Шлюзи додатків. Ці брандмауери аналізують інформацію про рівень додатків для прийняття рішень щодо передачі пакетів чи ні. Шлюзи додатків виступають посередником для таких додатків, як електронна пошта, FTP, Telnet, HTTP тощо. Шлюз додатків перевіряє зв'язок, автентифікуючи користувача для передачі пакетів. При необхідності він також може виконувати функцію перетворення даних.
- Шлюзи рівня мікросхем. Шлюзи рівня мікросхеми працюють на рівні сеансів моделі OSI або TCP рівня TCP / IP. Вони пересилають дані між мережами, не перевіряючи їх. Він блокує вхідні пакети на носії, але дозволяє трафіку проходити через себе. Інформація, що передається віддаленим комп'ютерам через неї, схоже, походить з шлюзу. Шлюзи рівня мікросхеми функціонують шляхом передачі TCP-з'єднань від надійної мережі до ненадійної мережі. Це означає,

що прямий зв’язок між клієнтом і сервером ніколи не відбувається. Основна перевага шлюзу рівня мікросхем полягає в тому, що він надає послуги для багатьох різних протоколів і може бути адаптований для обслуговування ще більшої різноманітності комунікацій.

- Державна інспекція пакетів (SPI).

Однак це всього лише список дозволених і заборонених правил, тому вони не завжди можуть мати можливість виявляти вторгнення. Мережевий екран, автентифікація користувачів, шифрування даних і віртуальні приватні мережі (VPN) забезпечують певний рівень безпеки, але вони обмежені тим, що не можуть забезпечити захист від шкідливих кодів, внутрішніх атак або незахищених модемів. Тому вони будуть ефективні тільки як одна з доступних ліній оборони.

Криптографія. Вона приховує інформацію від неавторизованих користувачів, однак цей метод ускладнює визначення того, чи мала місце будь-яка атака. Як правило, управління ключами - це непросте завдання. Криптосистеми можуть потребувати спеціальних систем управління ключами. Це, в свою чергу, вимагатиме спеціалізованого обладнання або конфігурації. В іншому випадку хакери матимуть змогу отримати доступ до цих ключів і зламати систему.

Забезпечення фізичної безпеки мережевого сайту або серверів. Однак вони обмежені тим, що фізична безпека не може забезпечити практичне рішення для зловмисників, які використовують сеанси Telnet для отримання доступу до мережі.

Ідентифікація. Метод, який використовується для перевірки користувачів мережевого ресурсу. Ефективність цього послаблюється тим фактом, що багато хто досі використовують «прості для злому паролі», в той час як деякі користувачі або не надійні, або просто недбало ставляться до своїх паролів, тому багато з них можуть бути легко отримані неавторизованими користувачами.

Антивіруси. Багато організацій також намагались використовувати антивіруси, однак це може не дати інформації про те, чи було вторгнення чи ні. Окрім цього, антивіруси також вимагають частих оновлень.[11]

Брандмауер та антивірус, які використовуються разом, забезпечують певний захист, але питання, чи цього достатньо. Хакери можуть пройти брандмауер, а комп’ютери можуть бути заражені, перш ніж антивірусна програма виявить це. Компанії потребують певного програмного та апаратного забезпечення, яке відстежує мережу на предмет шкідливого трафіку, і зупиняє її, перш ніж це завдає шкоди. Саме через це підприємства звертаються до систем виявлення вторгнень.

Організація, підприємство чи розумний будинок з інтелектуальним середовищем, що інтегрує технологію Інтернету речей, вважається складною системою, оскільки вона може складатись з різних продуктів різних компаній, заснованих на різних технологіях, які не мають загальної універсальної мови. Тому стандартизація є ще одним важливим аспектом безпеки в системах IoT.

Створення стандартної архітектури Інтернету речей на основі єдиної стандартної технології для всіх постачальників і виробників підвищить сумісність функцій безпеки всіх об'єктів і датчиків в системі Інтернету Речей.

Успіх цієї інтеграції буде залежати від співпраці між компаніями у створенні універсального стандарту. Така стандартизація значно полегшить безпеку мережі Інтернету Речей.

Проте, підключення інтелектуальних пристроїв, таких як освітлення, побутова техніка та замки, створює величезні ризики для інформаційної безпеки. Всі звіти з безпеки попереджають, що більше 80% підключених пристроїв "розумного будинку" уразливі для широкого спектру атак.

Недавнє дослідження, проведене фірмою з кібербезпеки Avast, підтверджує, що два з п'яти розумних домашніх господарств уразливі для кібератак. Використання хакерами таких незахищених пристроїв може привести до потенційних шкод різних масштабів, таких як перемикання системи безпеки для розблокування дверей, або злам розумної духовки до тих пір, поки вона не перегріється і не спалить будинок дотла.

В інших випадках мережа розумного будинку заражена програмою-вимагачем, яка вимагає, щоб домовласник заплатив, щоб відновити доступ до домашньої мережі. Навіть проста розумна лампочка може бути використана хакерами

для отримання більш широкого доступу до мережі "Розумний будинок" і завдати потенційної фізичної шкоди.

Одне успішне проникнення в один або кілька кінцевих пристроїв може загрожувати безпеці всієї системи і завдати шкоди її додаткам і сервісам, особливо з промислової точки зору. Таким чином, реалізація надійного механізму безпеки в системі Інтернету речей залежить від рівня безпеки окремих пристроїв, що, в свою чергу, залежить від факторів потужності і пам'яті. Отже, вважається, що обмеження потужності і пам'яті створюють непрямі проблеми безпеки в системах Інтернету Речей. Для вирішення цих проблем потрібні полегшені рішення для забезпечення безпеки і полегшені методи шифрування і дешифрування. Ці рішення і методи повинні бути застосовні в різних доменах Інтернету речей і повинні задовольняти вимогам безпеки, не впливаючи на якість обслуговування.

Важливе значення має і захист мережевої інфраструктури. Адже при виникненні надзвичайної ситуації велика ймовірність втрати не тільки самого обладнання, але й інформації. Багато таких аварій і катастроф загрожують цілісності самого бізнесу. Вони є передбачуваними з певним відсотком ймовірності.

Існує так зване «гаряче запасне обладнання», яке готове миттєво включитися в роботу при аварійній ситуації. Наприклад, можна дублювати найважливіші дані занесенням їх на спеціально призначену базу. А ось холодне - являє собою пристрої, які можна оперативно підготувати до виконання тих чи інших завдань. Це може бути набір не підключених серверів, на яких встановлено все необхідне для роботи ПЗ мережевої інфраструктури. Таким чином, можна без проблем і дуже швидко переключитися з несправного обладнання і продовжити роботу.

Дуже важливим питанням також є і конфігурування та підтримка мережевої інфраструктури. Адже з кожним роком потужність серверів і швидкостей збільшується. Це тягне за собою необхідність своєчасного і професійного обслуговування, а також потребу в оперативному вирішенні поточних і перспективних завдань.

Саме через всі вище вказані критерії та фактори багатьом компаніям та підприємствам доводиться звертатися до систем виявлення вторгнень.

Моніторинг та аналіз інформації користувача, мереж і сервісів за допомогою пасивного збору та аналізу трафіку є корисними інструментами для управління мережами і своєчасного виявлення вразливостей в системі безпеки.

Для цього існують СВВ - інструменти моніторингу даних про трафік для виявлення та захисту від вторгнень, що загрожують конфіденційності, цілісності та доступності інформаційної системи.

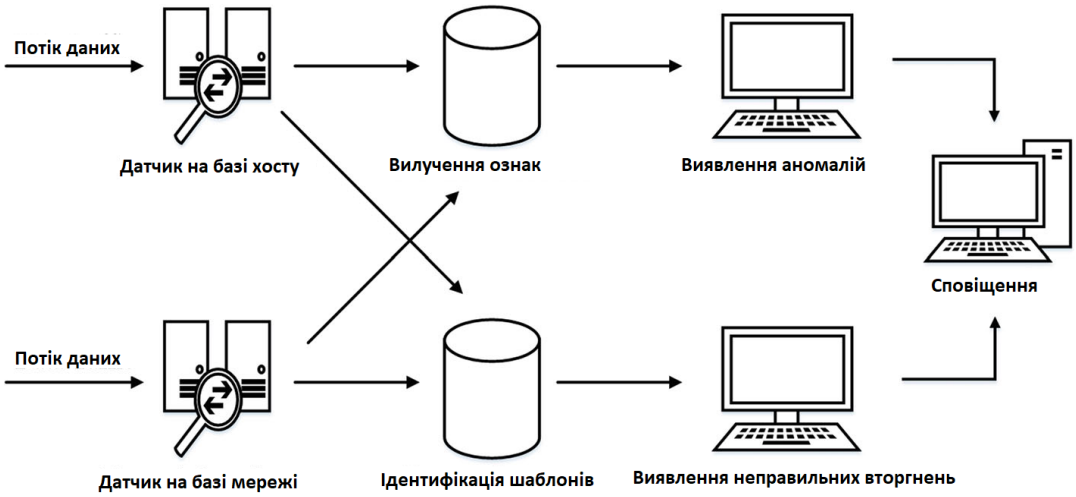

Рис. 1.1. Операції Системи Виявлення Вторгнень

Операції СВВ можна розділити на три етапи:

- Перший етап - це етап моніторингу, який спирається на мережеві або хостові датчики.
- Другий етап - це етап аналізу, який ґрунтується на методах вилучення ознак або методах ідентифікації шаблонів.
- Заключний етап - це етап виявлення, який грунтується на виявленні аномалій або неправильних вторгнень.

Система виявлення вторгнень фіксує копію трафіку даних в інформаційній системі, а потім аналізує цю копію для виявлення потенційно небезпечних дій.

Є два способи налаштування СВВ. Один - це виявлення вторгнень на основі хоста, а другий - це мережеве виявлення вторгнень.

Мережева СВВ працює наступним чином:

Рис. 1.2. Принцип роботи мережевої СВВ

Технології виявлення вторгнень не роблять систему абсолютно безпечною. Як правило, СВВ мають структуру, як вказано на Рис. 1.3:

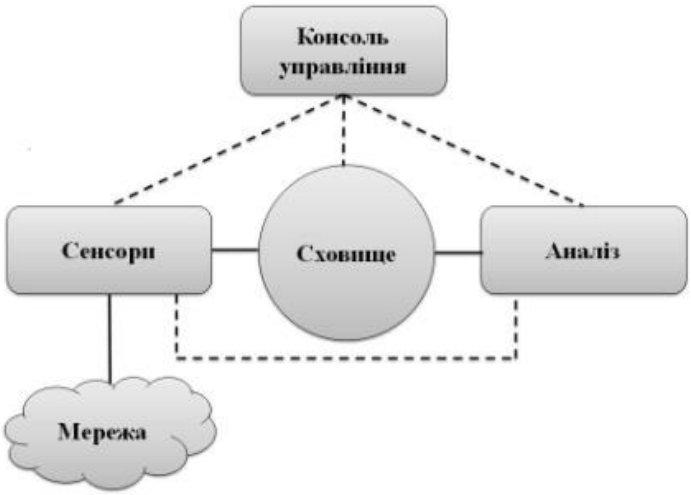

Рис. 1.3. Структура СВВ

1.3. Класифікація існуючих систем виявлення вторгнень для інтелектуальних середовищ

1.3.1. Узагальнена класифікація СВВ

Реалізація системи виявлення вторгнень залежить від середовища.

Вузлова, або Хостова, СВВ (англ. Host-based Intrusion Detection System, HIDS). Така система призначена для реалізації в одній системі і захисту цієї системи від вторгнень або шкідливих атак, які можуть завдати шкоди її операційній системі або даним.

Хостова СВВ відстежує характеристики одного хоста та події, що відбуваються в ньому, в пошуках підозрілої діяльності. Це вимагає певного ПЗ, яке знаходиться в системі та контролює мережевий трафік, системний журнал, процеси, доступ до файлів та їх модифікацію та конфігурацію або зміни системи.[18] Він записує будь-які дії, які він виявляє, у захищену базу даних і перевіряє, чи відповідають події будь-якому зловмисному запису подій, переліченому в базі знань. Деякі з основних переваг хостових СВВ наступні:

- Перевірка атаки: хостова СВВ використовує журнали, які містять фактично події, що відбулися. Система має також можливість знати, чи була вдалою атака чи ні. Цей тип виявлення є більш точним і створює менше помилкових попереджень.
- Моніторинг важливих компонентів. Хостова СВВ відстежує ключові компоненти, наприклад, виконувані файли, конкретні DDL та реєстр NT. Все це може завдати шкоди хосту або мережі.[14]
- Специфічна активність системи. Система виявлення відстежує діяльність користувачів та доступ до файлів. Він контролює процедуру виходу з системи чи входу в систему та моніторить її на основі поточної політики. Він також відстежує доступ до файлу, наприклад, відкриття файлу, що не використовується спільно.
- Переключені та зашифровані середовища. СВВ, що базуються на хості, забезпечують більшу видимість у чисто переключеному середовищі, розміщуючи на необхідній кількості критичних хостів. Шифрування - це складна проблема для мережевих СВВ, але не є основною проблемою для хостових СВВ. Якщо у відповідного хоста є аналіз на основі журналу, шифрування не матиме впливу на те, що входить до файлів журналу.
- Виявлення майже в режимі реального часу. Хостова СВВ покладається на аналіз журналу, який не є справжнім аналізом у реальному часі. Але він може виявити та реагувати, як тільки журнал записується та порівнюється з активними сигнатурами атаки.[14]

Хостові СВВ можуть функціонувати в системі, в якій мережевий трафік зашифрований, і система не вимагає додаткової функціональності мережевих пристроїв. До недоліків цієї системи відноситься: високе завантаження системи хоста, мале покриття для моніторингу, відсутність централізованого управління і те, що вони можуть бути блокованими деякими DoS-атаками або навіть заборонені.[7]

Протокольні СВВ (англ. Protocol-based IDS, PIDS) - така СВВ, яка відслідковує та аналізує протоколи зв’язку із пов'язаними системами або користувачами. Для веб-сервера цей тип системи зазвичай контролює протоколи HTTP та HTTPS. При використанні HTTPS система виявлення вторгнень повинна розташовуватися на цьому інтерфейсі, щоб переглядати пакети HTTPS, перш ніж вони будуть зашифровані та відправлені в мережу.

Мережева СВВ (англ. Network Intrusion Detection System, NIDS). Мережева СВВ відстежує мережевий трафік для певного сегменту мережі. Вони аналізують діяльність мережі та протоколу додатків, щоб виявити будь-яку підозрілу активність.[25] Мережева СВВ, як правило, сидить в мережі, і аналізує мережеві пакети, вишукуючи загрози. Він отримує всі пакети в певному сегменті мережі, включаючи комутовані мережі. Вона ретельно реконструює потоки руху, аналізуючи їх на закономірності зловмисної поведінки. Вони оснащені засобами для реєстрації своєї діяльності та звітування або сигналізації про сумнівні події. Основні переваги мережевих СВВ:

- Виявлення та реагування в реальному часі: мережева СВВ виявляє атаки в режимі реального часу, як тільки вони відбуваються, і забезпечує швидшу реакцію. Наприклад, якщо хакер ініціював DoS-атаку на основі TCP, СВВ може перервати з'єднання, надіславши скидання TCP.
- Виявлення зловмисного вмісту: мережеві СВВ видаляють та замінюють підозрілу частину атаки. Наприклад, якщо в електронному листі заражене вкладення, СВВ видаляє заражений файл і дозволяє отримати чисту електронну пошту.

- Докази притягнення до відповідальності: мережева СВВ контролює трафік у реальному часі, і якщо атака виявлена та захоплена, хакер не може вилучити докази. Оскільки захоплений напад має в собі дані, а також інформацію про його ідентифікацію, яка допомагає притягнення до кримінальної відповідальності.

Перевагами NIDS є також 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: високе завантаження системи, NIDS потребує додаткового налаштування і функціональності мережевих пристроїв. Системи NIDS не можуть аналізувати зашифровану інформацію і розпізнавати результати атак.

СВВ на основі прикладних протоколів (англ. Application Protocol-based IDS, APIDS) - це система (або агент), яка контролює та аналізує дані, що передаються за допомогою специфічних протоколів. Наприклад, на веб-сервері з базою даних SQL СВВ буде відслідковувати вміст команд SQL, що надсилаються на сервер.

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.

1.3.2. Класифікація СВВ за методиками аналізу.

Статистичні СВВ. СВВ на основі статистики будує модель розподілу для нормального профілю поведінки, а потім виявляє малоймовірні події та позначає їх як потенційні вторгнення. Статистична СВВ по суті враховує статистичні показники, такі як медіана, середнє значення, вибірка і стандартне відхилення пакетів. Іншими словами, замість того, щоб перевіряти трафік даних, кожен пакет контролюється. Статистична СВВ застосовується для виявлення будь-якого типу відмінностей у теперішній поведінці від нормальної поведінки.[3]

Основною проблемою такого підходу є складність в налаштуванні і велика кількість хибно позитивних тривог у разі некоректно заданих правил.

Сигнатурні СВВ (метод аналізу сигнатур).

Розберемо спершу, що таке сигнатура. У термінології комп'ютерної безпеки сигнатура - це типовий слід або зразок, пов’язаний зі шкідливою атакою на комп'ютерну мережу чи систему. Ця закономірність може представляти собою послідовність байтів у мережевому трафіку. Він також може мати форму несанкціонованого виконання програмного забезпечення, несанкціонованого доступу до мережі, несанкціонованого доступу до каталогу або аномалій у користуванні мережевими привілеями.

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. Цей метод було вперше застосовано для розпізнавання вторгнень.

Працює він наступним чином: серед мережевих мереж Інтернет-трафік шукаються певні шаблони або рядки, які використовувались для виконання певних атак.

Ключовим в цьому способі є те, що він захищає лише від відомих атак, оскільки неможливо розпізнати нові атаки за допомогою цього методу. Програмні рішення, засновані на методі аналізу підписів (сигнатур), оновлюються за принципом антивірусного ПЗ: є оновлення самого програмного продукту, а крім того, оновлюється база даних сигнатур. Оновлення цієї бази безпосередньо впливає на безпеку системи, тому що з оновленням система може виявити нові, раніше невідомі типи атак.

Цей метод також використовується в Протокольних СВВ, для перевірки, чи правильно було використано синтаксис певного протоколу.

1.3.3. Основні вимоги до системи виявлення вторгнень для інтелектуальних середовищ

Цілісність, конфіденційність та доступність є трьома важливими факторами в системах Інтернету речей. У більшості випадків додатки, що використо-

вують модель Інтернету речей, вважаються життєво важливими, такими як промислові та медичні програми. З одного боку, ці програми можуть бути додатками реального часу; таким чином, затримка в мережі і затримка безпосередньо впливають на їх продуктивність.

З іншого боку, такі атаки, як DOS, DDoS, зондування та атаки RPL, можуть погіршити зручність використання цих додатків. Таким чином, проблеми безпеки можна вважати небезпечною для життя проблемою, наприклад, в системах електронної охорони здоров'я. Отже, в мережах Інтернету речей потрібні потужні заходи безпеки. Такий механізм безпеки повинен захищати мережу Інтернету речей і її ресурси, не впливаючи на продуктивність системи або конфіденційність користувачів.

Крім того, інтелектуальні середовища на основі Інтернету речей складаються з широкого спектру пристроїв, датчиків і об'єктів Інтернету речей від різних постачальників і засновані на різних платформах Інтернету речей. Таким чином, проблеми сумісності перешкоджають появі технології Інтернету речей у великих масштабах. При розробці СВВ для інтелектуальних середовищ на основі Інтернету речей необхідно враховувати питання сумісності та стандартизації.

Також, мережі Інтернету речей страждають від проблем з енергоефективністю; таким чином, необхідна полегшена система СВВ, що вимагає лише невеликої кількості обчислювальних операцій. У HIDS Інтернету речей повинні одночасно виконувати необхідні обчислювальні операції для ідентифікаторів і для служб Інтернету речей.

Таким чином, при проектуванні HIDS необхідно враховувати енергоресурси і час автономної роботи. Через обмеження по потужності і пам'яті систем Інтернету речей споживання енергії, час обробки і накладні витрати на продуктивність СВВ є важливими показниками продуктивності. Таким чином, ці показники необхідно враховувати при розробці систем виявлення вторгнень для інтелектуальних середовищ на основі Інтернету речей. Ці питання слід приділяти більше уваги дослідженням HIDSS для таких середовищ.

Конфіденційність - ще один важливий фактор в системах Інтернету речей. Методи глибокої перевірки пакетів вважаються порушенням конфіденційності. Тому такі методи та інші методи з аналогічними характеристиками небажані.

Крім того, блокування звичайних пакетів даних впливає на програми та служби Інтернету речей. Цей ефект дуже шкідливий, особливо для життєво важливих додатків і додатків реального часу, таких як промислові та медичні програми. Тому впровадження інтелектуальної системи без глибокої перевірки пакетів вимагає впевненості в тому, що операції в системі Інтернету речей допоможуть запобігти будь-якому несанкціонованому доступу до об'єктів Інтернету речей, тим самим допомагаючи вирішити проблему конфіденційності користувачів.

Для застосування в життєво важливих додатках і додатках реального часу потрібна нова конструкція IDS з дуже низьким FPR і дуже високою точністю виявлення, оскільки традиційні СВВ можуть не задовольнити ці вимоги.

Розміщення систем виявлення вторгнень також є серйозною проблемою, яку необхідно враховувати при розробці СВВ будь-якого типу, будь то NIDS або HIDS. Розміщення СВВ в мережі Інтернету речей вплине на загальну ефективність системи.

Існує дві основні стратегії розміщення системи виявлення вторгнень: централізована і розподілена.

Централізована стратегія забезпечує перевагу централізованого управління, але також може призвести до перевантаження системної обробки, що може вплинути на якість обслуговування в мережі Інтернету речей.

Розподілена стратегія має переваги в скороченні обсягу відстежуваного трафіку і збільшенні пропускної здатності. Однак впровадження СВВ в різних регіонах мережі Інтернету речей є складним завданням через пов'язані з цим проблеми управління.

Нарешті, існує потреба як в нормальних, так і в аномальних базах даних, які були б актуальними і інтегрованими з додатками і службами Інтернету речей. Ці бази даних будуть дуже корисні для тестування різних типів СВВ і методів в

середовищі Інтернету речей. Здатність виконувати успішні та значущі порівняння систем виявлення вторгнень залежатиме саме від цих баз даних.

1.3.4. Недоліки СВВ.

Щодня вигадуються нові атаки на певний тип ПЗ. СВВ може дізнатися про ці атаки та почати на них реагувати лише після отримання нової бази відомих атак. Ефективність СВВ безпосередньо залежить від своєчасного оновлення бази даних. Також необхідно вчасно оновлювати ПЗ, оскільки оновлення можуть містити виправлення, що забезпечують захист від певних типів атак.

У випадку СВВ на основі методу виявлення підписів (сигнатур) існує певний проміжок часу між виявленням конкретної атаки та оновленням бази даних сигнатур, що дозволить виявити цю атаку. Протягом цього періоду часу СВВ не в змозі виявити цю атаку.

«Гучна» мережа також може значно знизити ефективність системи СВВ через велику кількість помилкових позитивних результатів. Шумна мережа - це мережа, в якій циркулюють пакети, які не відповідають вимогам певних зазначених протоколів (такі пакети можуть з’являтися через помилки ПЗ).

Зашифровані пакети не обробляються більшістю СВВ. Тобто зашифровані пакети можуть бути використані для цілеспрямованої атаки, проте атака не буде виявлені.

Хоча СВВ можуть виявити підозрілу активність, це не означає, що вони захистять від слабких вимог автентифікації або використання слабких і застарілих протоколів. Якщо доступ отриманий через слабку систему автентифікації, зловмисник може здійснити багато шкідливих дій, які не будуть розпізнані СВВ, наприклад, вони можуть скопіювати конфіденційну документацію, до якої має доступ обліковий запис, який вони скомпрометували.

1.3.5. Основні типи потенційних атак на інтелектуальні середовища

Завданням СВВ є оцінка впливу певної команди на систему, тому атаки полягають у генерації команди, для якої СВВ не може оцінити точний вплив на стан системи.

Деякі команди досить гнучкі і їх вплив на систему може залежати від багатьох факторів, не всі нюанси можна враховувати в СВВ.

Можна також використовувати незвичне поєднання команд, яке також не було враховано СВВ.

Атака на СВВ в першу чергу спрямована на їхню:

- Доступність - завдання полягає у формуванні такої кількості потенційних користувачів атаки, що система не зможе їх обробити або вимкне СВВ;
- Точність - генерування великої кількості помилкових позитивних результатів;
- Надійність - не виявлення атак за допомогою СВВ.

Основні типи атак та методи обходу СВВ:

- **Відмова в обслуговуванні** (англ. Denial of Service, DoS). Запуск атаки відмови в обслуговуванні на систему СВВ є можливим методом обходу одного з механізмів захисту мережі.[13] Зловмисник може досягти цього, використовуючи помилки в СВВ, споживаючи всі обчислювальні ресурси в системі або навмисно запускаючи велику кількість повідомлень, щоб замаскувати фактичну атаку. Варіації цієї атаки показані нижче:

Виснаження процесора: пакети, захоплені IDS, зберігаються в основному буфері до тих пір, поки процесор не буде готовий обробити їх. Якщо процесор знаходиться під великим навантаженням, він не зможе обробляти пакети достатньо швидко, і цей буфер переповнюється. Після цього нові (і, можливо, шкідливі) пакети неможливо помістити у заповнений буфер.

Втома оператора: повідомлення, що були створені за допомогою СВВ, мають попереджати про початок атаки. Зловмисник може зменшити "доступність" СВВ, перевантаживши оператора людини необмеженою кількістю сповіщень, надсилаючи велику кількість "шкідливого" трафіку, призначеного для генерації

сповіщення від СВВ. Потім зловмисник може здійснити фактичну атаку, використовуючи попереджувальний шум у якості прикриття.

- **Ухилення** (англ. Evasion). Обхід пристрою інформаційної безпеки для того, щоб доставити експлойт, атаку або іншу форму шкідливого ПЗ в цільову мережу або систему без виявлення. Цей тип атаки зазвичай використовують задля протидії мережевим СВВ, але також можуть використовуватися для обходу брандмауерів і аналізу шкідливих програм.[17]
- **Слабкість порівняння вже існуючих шаблонів** (англ. Pattern Matching Weakness). Система перевіряє вміст кожного пакету на відповідність з моделями атаки, що вже внесені в оновлену базу даних, і попередження генерується, якщо вони відповідають.

Цей підхід є проблематичним, оскільки не всі вхідні дані повинні бути однаковими, щоб використовувати однакову вразливість. Іншими словами, одна і та ж атакуюча команда може мати різні варіації.

- **Шифрування й тунелювання** (англ. Encryption and Tunneling). СВВ не перевірятиме трафік системи, через яку проходить встановлене злочинцями зашифроване з’єднання (тунель) із системою. Найбільш відомими прикладами тунелю є SSH, SSL та IPSec. За умови, що не надано ключів дешифрування, мережева СВВ не матиме засобів для перевірки трафіку.
- **Фрагментація атаки на невеликі пакети** (англ. Fragmentation). Розподіл навантаження на невеликі пакети. Простий спосіб атаки полягає в фрагментації, але також можна створити пакети з невеликими навантаженнями. Основними методами даної атаки є пауза між відправленнями менших пакетів та відправлення пакетів у недостовірному порядку, що в даному випадку може ввести в оману прості СВВ.
- **Сніфинг**. Це процес моніторингу та захоплення всіх пакетів, що проходять через дану мережу, за допомогою відповідних інструментів. Це форма "прослуховування дротів телефону" та ознайомлення з розмовою. Він також називається прослуховуванням, застосованим до комп'ютерних мереж. Усі в тому ж фізичному місці можуть підключитися до мережі за допомогою кабелю

Ethernet або підключитися бездротово до цієї мережі та отримати доступ до загального трафіку. Можна проаналізувати таку конфіденційну інформацію з мережі:

- Трафік електронної пошти
- FTP-паролі
- Веб-трафік
- Конфігурацію маршрутизатора
- Сеанси чату
- DNS-трафік

1.4. Висновки до розділу 1

У першому розділі дипломної роботи були отримані такі результати:

Проведено аналіз основних понять, завдань та видів сучасних систем виявлення вторгнень, у результаті якого встановлено, що:

- Брандмауер та антивірус, які використовуються разом, забезпечують певний захист, але цього, зазвичай, недостатньо. Хакери можуть пройти брандмауер, а комп’ютери можуть бути заражені, перш ніж антивірусна програма виявить це;
- Для якомога ефективнішого захисту інтелектуальних середовищ на базі Інтернету Речей рекомендується використовувати мережеві СВВ, деякі з яких знаходяться у вільному доступі.

Було проаналізовано основні типи потенційних атак на інтелектуальні середовища, а також недоліки систем виявлення вторгнень.

РОЗДІЛ 2. АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

2.1. Загальний опис систем виявлення вторгнень для мережевих інфраструктур

Виявлення вторгнень було вперше представлене на комерційному ринку два десятиліття тому як система SNORT, і швидко стало ключовим моментом кібербезпеки. Мережева СВВ (NIDS) здійснює моніторинг трафіку на усі та з усіх пристроїв в стратегічних точках мережі для виявлення атак (вторгнень), які пройшли через мережевий брандмауер.[15] У своєму першому втіленні мережева СВВ використовувала механізми виявлення на основі зловживань (шаблонів і сигнатур) або на основі аномалії (шаблони) для аналізу проходження трафіку та відповідності трафіку до бібліотеки відомих атак. Після того, як напад був ідентифікований, команді кібербезпеки надсилалось попередження.[4]

Незважаючи на те, що технологія продовжує відігравати ключову роль на більшості підприємств, мережева система виявлення вторгнень вийшла з обороту з двох ключових причин:

- Двигуни, засновані на правилах, що використовуються для виявлення, були передані в брандмауер нового покоління (NG-FW), що робить економічно вигідним для деяких організацій розгортання об'єднаної можливості;
- Загрози суб'єктів вміють виконувати атаки, що ухиляються від підписів / правил / зразків, використовуваних як традиційною мережевою системою виявлення вторгнень, так і об'єднаним брандмауером нового покоління.

Типи мережевих атак, які повинні бути вирішені мережевими СВВ нового покоління, включають:

- Зловмисні програми. Зловмисне ПЗ - це шкідливе ПЗ, створене для "зараження" або заподіяння шкоди цільовій системі з будь-якої кількості причин. Ці причини охоплюють простий доступ до облікових даних та крадіжку даних до зриву або знищення системи або даних. Сьогодні, за оцінками, 30% шкідливих програм здатні уникати традиційних технологій на основі підписів. Більшість організацій вирішили це через впровадження технологій виявлення та реагування на кінцеві точки. У відносно однорідних середовищах з твердим контролем над кінцевою точкою, кінцеві точки контролю можуть бути адекватними. Для організацій, що мають масив клієнтських та серверних технологій, обмеження частоти виправлення та оновлення, пристрої Інтернету Речей, над якими обмежений контроль, стратегічно розгорнута мережева СВВ нового покоління виступає в якості основного захисту від “невідомих” шкідливих програм.
- Черви. Форма саморозповсюдження зловмисного ПЗ, яка не потребує взаємодії з користувачем. Наприклад, WannaCry націлив на широку вразливість Windows для зараження машини. Після зараження зловмисне програмне забезпечення перемістилося збоку, заразивши інших вразливих хостів. Після зараження цілі можна вжити будь-яку кількість дій, таких як тримання пристрою для викупу, видалення файлів користувачів або ОС, крадіжка облікових даних або сканування мережі на предмет вразливості.
- Веб-атаки. Під час веб-атаки публічні сервіси, такі як веб-сервери та сервери баз даних, безпосередньо націлені з різних причин: знеструмити веб-сервер, викрасти або іншим чином маніпулювати даними або створити стартовий майданчик для додаткових атак.
- Сканувальні атаки. Скани, як правило, використовуються як засіб для збору розвідки. У цьому випадку суб'єкти погроз використовують різноманітні інструменти для зондування систем для кращого розуміння цілей, наявних та

експлуатованих уразливих місць. Мережева СВВ нового покоління, що керує мережевим брандмауером, здатна виявляти ці зонди і видавати блокові запити на мережевий брандмауер.

- Брутфорс(атака грубої сили). Нападник намагається розкрити пароль для системи чи послуги шляхом спроб та помилок. Оскільки ця форма або атака вимагає часу для виконання, суб'єкти погроз часто використовують програмне забезпечення для автоматизації спроб злому пароля. Ці паролі можна використовувати для будь-якої кількості цілей, включаючи модифікацію системних установок, крадіжку даних, фінансовий злочин тощо. Мережева СВВ нового покоління, що керує мережевим брандмауером та / або перебуває в стратегічних точках мережі, здатна виявляти брутфорс та видавати блокові запити мережевого брандмауера.
- Атаки відмови в обслуговуванні. Також відомі як розподілені атаки відмови в обслуговуванні (DDoS), DDoS-атаки намагаються перекрити свою ціль - як правило, веб-сайт або сервери DNS - за рахунок потоку трафіку. У цьому випадку мета - уповільнити або збити систему. Мережева СВВ нового покоління, що керує мережевим брандмауером, здатна виявляти DDoS-атаки та видавати блокові запити на мережевий брандмауер.

Найпопулярнішим брендом у сфері СВВ нового покоління є CISCO. Саме вони пропонують перший в своїй галузі адаптивний, орієнтований на загрозу брандмауер нового покоління (NGFW), розроблений для нової ери загроз і сучасного захисту від зловмисного ПЗ(Табл. 2.2). Cisco ASA(Adaptive Security Appliance - Пристосувальний Прилад Безпеки) з сервісами FirePOWER забезпечує інтегрований захист від загрози для всього континууму атаки - до, під час та після атаки.

Cisco ASA з сервісами FirePOWER використовує комплексний підхід до захисту від загрози, зменшення капітальних та експлуатаційних витрат та адміністративної складності(Табл. 2.1). Він плавно інтегрується з існуючим IT-середовищем, робочим потоком та мережею. Сімейство приладів є високомасштаб-

ним, працює на швидкостях з багатогігабайтними системами та забезпечує стабільну та надійну безпеку через відділення, Інтернет-мережі та центри обробки даних як у фізичному, так і у віртуальному середовищі.[4][5]

Таблиця 2.1

Особливості та переваги мережевих СВВ нового покоління

Особливості мережевої СВВ нового покоління	Переваги
Брандмауер нового покоління	Перший в галузі брандмауер, орієнтований на загрозу; забезпечує функціональність брандмауера ASA, розширений захист від загрози та розширене виявлення та усунення порушень у поєднанні в одному пристрої
Розширений захист від зловмисного ПЗ	Виявлення, блокування, відстеження, аналіз та виправлення для захисту підприємства від цілеспрямованих та стійких атак зловмисного ПЗ
Повна контекстуальна обізнаність	Застосування політики на основі повної видимості користувачів, мобільних пристроїв, клієнтських додатків, зв'язку між віртуальними машинами, вразливості, загроз та URL-адрес
Управління додатками та фільтрування URL-адрес	Контроль на рівні додатків (над додатками, геолокаціями, користувачами, веб-сайтами) та здатність застосовувати правила використання та адаптування даних на основі спеціальних програм та URL-адрес
Цільовий, масштабований	Високомасштабна архітектура приладів безпеки, яка працює на швидкостях до багатьох Гб/с; послідовна та міцна безпека для малого офісу, філій, Інтернет-Інтернету та центрів обробки даних у будь-якому фізичному та віртуальному середовищі
Управління на пристрої	Спрощує вдосконалене управління захистом від загроз для малого та середнього бізнесу з малим розміщенням

Колективна розвідка безпеки (CSI)	Неперевершена безпека та дані веб-репутації забезпечують розвідку про загрози та захист безпеки в режимі реального часу

Таблиця 2.2

Оцінка СВВ нового покоління Cisco

Оцінка систем виявлення вторгнень нового покоління Cisco				
Категорії	Найкращий показник	Дуже добре	Добре	Непогано
Продуктивність безпеки				
Ціна				
Реалізація				
Управління				
Підтримка				
Хмарні технології				

Таким чином, ми можемо дійти до висновку, що задля досягнення найбільшого результату та найвищого ККД системи, потрібно заплатити чималих грошей, що є найбільшим мінусом та не дозволяє заволодіти системою на рівні СВВ Cisco.

Тому, в такому випадку, залишається звертатись до СВВ з відкритим кодом, які постійно модифікуються завдяки общині користувачів, зацікавлених у постійному розвитку цієї технології.

Так як СВВ були винайдені в середині 1980-х років, було розроблено безліч різних систем, різних методів виявлення шкідливого трафіку, різних алгоритмів та інших підходів. СВВ використовують два різних підходи для виявлення шкідливого трафіку: виявлення на основі сигнатур і виявлення аномалій.

Виявлення на основі сигнатур - це коли СВВ використовує базу даних з сигнатурами відомого шкідливого трафіку, і порівнює ці сигнатури з трафіком і бачить, чи є якісь збіги. Якщо ці сигнатури збігаються з будь-яким трафіком в мережі, створюються попередження.

Виявлення аномалій дозволяє виявити статистичні аномалії в мережевому трафіку. Ідея виявлення аномалій полягає у створенні "базової лінії", яка визначає, який вид трафіку вважається нормальним, в той час як трафік, що знаходиться поза цією базовою лінією, розглядається як шкідливий трафік, або ж «аномалії», і створюються попередження.

Зараз існує чимало СВВ з відкритим кодом у вільному доступі - ACARM-ng, AIDE, Bro, Snort, Suricata, OSSEC, Prelud Hybrid IDS, Samhain, Fail2Ban, Security Onion - та більшість з них постійно модифікуються задля досягнення кращого результату у захисті обладнання та конфіденційних даних. Розглянемо перелік найбільш популярних з них, а саме: Suricata, Snort та Bro.

Багато досліджень показують, що саме ці три мережеві СВВ є найбільш ефективними і стають де-факто галузевим стандартом для систем виявлення вторгнень. Основним внеском цієї роботи є порівняння продуктивності цих трьох систем на основі деяких істотних характеристик, включаючи точність, використання процесора і оперативної пам'яті.

Порівнюючи Suricata, Snort та Bro, потрібно вирішити, яку інформацію ми можемо порівняти. Є багато речей, які можна порівняти, наприклад вихідні журнали, сигнали тривоги, конфігурація, набір правил, налаштування і тестове середовище, тощо.

Bro

Bro - це NIDS на базі Unix з відкритим вихідним кодом і пасивний аналізатор мережевого трафіку [35]. Спочатку він був розроблений в 1994 році Верном Паксоном і перейменований в Zeek в кінці 2018 року.

Bro працює інакше, ніж Snort і Suricata, через свою спрямованість на мережевий аналіз. Він працює як NIDS, пасивно відстежуючи мережевий трафік і виявляючи підозрілу активність. Крім того, сценарії політики Bro написані на власній мові сценаріїв Bro, який не покладається на традиційне виявлення сигнатур. Крім того, Suricata і Snort знаходяться під ліцензією GNU GPL, підтримують трафік IPv6, а їх установка і розгортання прості. Навпаки, Bro знаходиться під ліце-

нзією BSD, не підтримує трафік IPv6, та установка системи може бути утруднена. Насправді, Bro складніше і вимагає більше часу для розгортання і розуміння.

Крім того, Snort і Suricata можуть працювати на всіх операційних системах (наприклад, Linux, Mac OS X, FreeBSD, OpenBSD, UNIX і Windows) і не обмежуватися повністю обладнаною серверною апаратною платформою, тоді як Bro обмежується UNIX-подібними операційними системами, що перешкоджає їх переносимості. Як Snort і Suricata, Bro також використовує методи вторгнення на основі сигнатур і аномалій для виявлення незвичайної поведінки мережі [7, 31].

Snort

Протягом багатьох років Snort (розроблений та підтримується SourceFire) фактично є стандартом для систем виявлення / запобігання вкрапленню з відкритим кодом (IDS / IPS). Його двигун поєднує в собі переваги сигнатур, протоколів та перевірки на основі аномалії і став найбільш широко розгорнутою IDS / IPS у світі. Як фактичний стандарт для СВВ, Snort є надзвичайно цінним інструментом. Цю утиліту Linux легко розгортати і її можна налаштувати для контролю вашого мережевого трафіку на предмет спроб вторгнення, реєстрації їх та вжиття визначених дій при виявленні спроби вторгнення. Це один з найбільш широко розгорнутих інструментів СВВ, який також може виступати у якості СЗВ.

Метод роботи даної СВВ доволі простий: після потрапляння до Snort, пакет послідовно проходить через декодери, препроцесори, і лише після цього він потрапляє в детектор, який починає застосовувати правила. Завдання декодерів зводиться до "витягування" даних мережевого та транспортного рівня (IP, TCP, UDP) з протоколів рівня передачі даних (Ethernet, 802.11, токенове кільце тощо).

Suricata

Нещодавно з'явився Suricata, новий і менш розповсюджений продукт, розроблений Фондом відкритої інформаційної безпеки (OISF), і він здається справді перспективним. Suricata – СВВ з відкритим кодом, заснована розробниками, які працювали над СЗВ-версією Snort. Він також заснований на сигнатурах, але інтегрує революційні методи. Цей двигун вбудовує нормалізатор та парсер HTTP

(бібліотека HTP), який забезпечує дуже вдосконалену обробку потоків HTTP, що дозволяє зрозуміти трафік на 7-му рівні моделі OSI. Основна відмінність Suricata від Snort - це можливість використовувати графічний процесор у режимі СВВ, більш досконала система СЗВ, багатопоточність, як результат високої продуктивності, що дозволяє обробляти трафік до 10 Гбіт на звичайному обладнанні та багато іншого, в т.ч. повна підтримка формату правил Snort.

Системою Suricata постійно користується спільнота задля її модифікації, та однією з кращих таких модифікацій є система SELKS від Stamus Networks. Її особливість полягає в дружелюбному для користувачів інтерфейсі, та досить інтуїтивно зрозумілим функціоналом. Завантажити дану систему можна напряму з офіційного сайту лише декількома натисками.

Рис. 2.1. Приклад роботи системи SELKS у режимі СВВ

Snort і Suricata можуть бути використані з певними однаковими правилами, але так не робиться. Система Snort налаштована на використання правил підписника, знайдених за адресою snort.org, в той час як Suricata використовує набір правил з ресурсу Emerging Threats.

2.2. Експериментальні модифікації систем виявлення вторгнень направлені на захист інтелектуальних середовищ

Через проблеми безпеки, з якими стикаються системи Інтернету речей, методи, які можуть активно виявляти нові атаки, найбільш підходять для захисту мереж Інтернету речей. Таким чином, потрібна надійна система ідентифікації, що здатна виявляти нові атаки в інтелектуальних середовищах на основі Інтернету речей.

Відповідно до рекомендацій, що містяться в недавніх оглядах СВВ для систем Інтернету речей, основну увагу приділимо особливостям всіх методів систем виявлення вторгнень для Інтернету речей, які можуть бути застосовані в інтелектуальних середовищах. Системи Інтернету речей вимагають особливих заходів безпеки з особливими характеристиками, які не пропонуються традиційними системами виявлення вторгнень.

У 2011 році, Лю та ін. запропонували штучний імунний ідентифікатор для мереж Інтернету речей. Ця система може адаптуватися до середовища Інтернету речей і автоматично вивчати нові атаки. Система заснована на машинному навчанні і сигнатурної моделі.

Прийнятий підхід до машинного навчання розроблений на основі механізмів штучних імунних систем. Метою системи є підвищення безпеки мережі Інтернету речей; таким чином, це мережа СВВ. Ця система володіє двома основними функціями: самоадаптацією до нових умов і самонавчанням новим атакам.

У 2013 році, Касінатаном та його командою було запропоновано СВВ, яка виявляє DoS-атаки на основі 6LoWPAN в мережах Інтернету речей. Вони запропонували архітектуру виявлення DOS, яка складається з зонда СВВ, менеджера захисту DOS та ідентифікатора Suricata. Вони розробили цю систему на основі вивчення вразливостей, присутніх в WSNS на основі IP. IDS Suricata працює на головному комп'ютері; таким чином, перевага цієї системи в тому, що вона може

вирішити проблему енергоспоживання, тим самим заощаджуючи енергоресурси в WSNS.

Окрім того, Касінатан запропонував вдосконалену СВВ для виявлення DoS-атак на основі 6LoWPAN в мережах Інтернету речей. Ця система залежить від архітектури виявлення DOS; її основними новими елементами є менеджер частотної гнучкості (FAM) і система управління інцидентами і подіями безпеки (SIEM). Ці елементи разом створюють систему моніторингу, яка може контролювати великі мережі.

У 2014 році, Джун і Чі запропонували СВВ, інтегровану з технологією комплексної обробки подій (CEP). Перевагою технології CEP є здатність ідентифікувати складні закономірності за допомогою обробки даних в режимі реального часу. Архітектура системи для обробки подій складається з блоку фільтрації подій, блоку бази даних подій, блоку CEP і блоку механізму дій. Система залежить від моделі обробки подій, яка використовує підхід моделі правил для виявлення вторгнень. Основні особливості цієї системи полягають в тому, що вона працює в режимі реального часу і демонструє високу продуктивність при виявленні вторгнень в систему Інтернету речей з використанням механізму обробки подій.

У тому ж році, Кріммлінг і Пітер запропонували експериментальну модель мережевої СВВ, яка залежить від машинного навчання для виявлення вторгнень на основі аномалій і сигнатур. Системна платформа призначена для інтелектуальних додатків громадського транспорту, що використовують CoAP. Основними особливостями цієї системи є її застосовність до додатків CoAP і її залежність від полегшеного алгоритму.

Сурендар і Умамакесварі запропонували у 2016 році системи виявлення вторгнень на основі обмежень для мереж Інтернету речей з використанням 6LoWPAN. Ця система підтримує ефективність з точки зору показників QoS при виявленні атак на воронки. Система ізолює шкідливі вузли і відновлює мережу без цих вузлів. Ця СВВ є системою на основі специфікації, який залежить від

поведінкових правил і використовує підхід моделі протоколу. Основні особливості цієї системи полягають в тому, що вона виявляє провальні атаки, зберігає QoS і ізолює шкідливі вузли.

Більш того, Бостані і Шейхан [84] запропонували гібридні ідентифікатори для мереж Інтернету речей з використанням 6LoWPAN для виявлення декількох атак RPL. Ця система залежить від модулів виявлення вторгнень на основі специфікацій, що виконують функції агентів IDS, у вузлах маршрутизатора і модуля виявлення вторгнень на основі аномалій, що виконує функції основних IDS, в кореневому вузлі. Основними особливостями цієї системи є скорочення кількості комунікаційних повідомлень через відсутність додаткових керуючих повідомлень або вузлів моніторингу в конструкції IDS і її застосовності до великомасштабних мереж.

Гарсія-Фонтом було запропоновано мережеву СВВ для WSN, які залежать від підходу машинного навчання та моделі підпису. Вони використовували механізм виявлення на основі сигнатур і механізм виявлення на основі аномалій для підвищення швидкості виявлення. Система призначена для того, щоб допомогти адміністраторам розумного міста виявляти вторгнення з використанням систем виявлення вторгнень і схеми класифікації атак. Метою системи є виявлення вторгнень в WSN в різних середовищах розумного міста. Головною особливістю цієї системи є її застосовність до великомасштабних бездротових сенсорних мереж.

Фу Вай в 2017 році запропонував мережеву СВВ, яка залежить від виявлення аномалій на основі сигнатур і протоколів. Запропонована структура СВВ орієнтована на виявлення атак на мережі Інтернету речей без шкоди для неоднорідності такої мережі. Метод виявлення залежить від порівняння абстрактних потоків дій у пакетах даних з трьома базами даних на основі інформації про тип протоколу для кожного пакета. Ці бази даних являють собою бібліотеку стандартних протоколів, бібліотеку ненормальних дій і бібліотеку звичайних дій. Запропонований підхід складається з монітора подій, бази даних подій, аналізатора

подій та блоку реагування. Цей підхід забезпечує єдиний метод виявлення вторгнень для мереж Інтернету речей, заснований на теорії автоматів. Основними особливостями цієї системи є класифікація атак на три категорії і розробка інструментів графічного інтерфейсу (GUI) для графічного представлення абстрактних потоків дій і виявлення можливих вторгнень.

У 2018 році Амурі, Алапарті та Моргера запропонували CBB, засновану на підході моделі протоколу і машинному навчанні. Ця система складається з двох етапів виявлення. На першому етапі, а саме при локальному виявленні, дані про поведінку мережі збираються спеціальними аналізаторами для створення набору правильно класифікованих екземплярів (CCI) з використанням підходу контрольованого навчання, заснованого на деревах рішень. На другому етапі, а саме при глобальному виявленні, CCI збираються супервузлами для створення заснованих на часі профілів, званих накопиченими показниками коливань, для шкідливих і нормальних вузлів окремо. Основними особливостями цієї системи є її низька обчислювальна складність і низькі вимоги до ресурсів.

У тому ж році було запропоновано модель мережевої системи виявлення вторгнень, яка залежить від ймовірності відкидання пакетів (PDP) в пристроях Інтернету речей для моніторингу шлюзів і виявлення шкідливих шлюзів. Система використовує підхід статистичної моделі для виявлення вторгнень на основі аномалій з використанням тесту відношення правдоподібності для виявлення шкідливих шлюзів, які порушують зв'язок між пристроями Інтернету речей і точками доступу. Одним з недоліків цієї системи є те, що вона може виявляти тільки шкідливі витоку, які впливають на пакети низхідної лінії зв'язку; вона не враховує шкідливі витоку, які впливають на пакети висхідної лінії зв'язку з пристроїв Інтернету речей. Основні особливості цієї системи полягають в тому, що вона заснована на теоретичних основах замість того, щоб вимагати навчальних даних, і що вона може виявляти шкідливі шлюзи в режимі реального часу.

У 2015 році на 34-й конференції IEEE було запропоновано надлегкий підхід до виявлення аномалій глибоких пакетів, який може бути реалізований на

невеликих пристроях Інтернету речей. Система розроблена з урахуванням залежності від побітової AND операції і використовує підхід моделі корисного навантаження для виявлення вторгнень на основі аномалій. Основними особливостями цієї системи є її низька затримка, висока пропускна здатність і надлегка вага.

Інженер Рам Мохан запропонував модель хостової СВВ, яка залежить від виявлення аномалій на основі сигнатур і правил. Система використовує традиційну техніку, засновану на сигнатурах, у поєднанні з виявленням вторгнень на основі правил Snort. Таким чином, система може виявляти відомі атаки з використанням бази даних сигнатур і невідомі атаки з використанням правил SNORT. Основною проблемою цієї системи є конфіденційність, оскільки система використовує метод глибокої перевірки пакетів для виявлення атак. Основними особливостями цієї системи є її простота і здатність до самонавчання.

На IEEE конференції у 2013 році було підтверджено, що загроза атак в системах Інтернету речей впливає не тільки на обчислювальне середовище, але і на життя людей і економіку. З цієї причини було запропоновано СВВ на основі обчислювального інтелекту для систем бездротового зв'язку та Інтернету речей. Вони запропонували трирівневу архітектуру як основу інтелектуальної IDS, придатної для бездротових мереж; ця архітектура складається з блоку зберігання інформації, блоку обчислювального аналізу та оптимізації, а також блоку кластеризації та звітності про вторгнення. Ця система заснована на підході машинного навчання для виявлення вторгнень на основі аномалій.

Підхід до машинного навчання, що застосовується в цій СВВ, заснований на парадигмі «swarm intelligence» (SI), яка являє собою особливий тип парадигми обчислювального інтелекту (CI). Система націлена на IP-адреси для виявлення атак; таким чином, у неї є недолік - вона не може бути застосована в регіонах VPN, які не використовують протокол TCP/IP. Головною особливістю цієї системи є її здатність працювати як в якості мережевої СВВ, так і хостової.

Таким чином, дослідивши дані експериментальні моделі СВВ для інтелектуальних середовищ ми визначили основні рекомендації, які повинні бути враховані при проектуванні, моделюванні та створенні СВВ для інтелектуального середовища, такі як необхідність потужної і легкої системи з відповідною стратегією розміщення, яка не робить негативного впливу на цілісність, конфіденційність і доступність середовища Інтернету речей.

2.3. Порівняльний аналіз обраних систем виявлення вторгнень

Задля визначення найпродуктивнішої СВВ було проведено аналіз раніше зазначених СВВ та виявлено наступні особливості кожної з них:

Bro

Bro - це система виявлення мережевих вторгнень з відкритим вихідним кодом (NIDS), що складається з багаторівневої модульної архітектури, що лежить в основі мережевого рівня в семирівневій моделі ISO-OSI. Це незалежний від платформи фреймворк.

Bro пасивно відстежує вхідні пакети і вишукує шкідливі дії. Такі дії, як багаторівневий аналіз, накладання політики, поведінковий контроль і виявлення, орієнтоване на політику, виконуються Bro, і він спостерігає за атаками після перетворення мережевого трафіку в належний семантичний формат для виконання механізму порівняння.

Є багато суттєвих переваг використання Bro:

- Він ефективно збирає дані з мереж зі швидкістю 1 Гбіт/с і може працювати з великою ефективністю в високошвидкісний середовище;
- За допомогою цієї структури створюються більш складні і складні підписи;
- Він має гнучкість для налаштування функцій.

Однак у системи Bro є деякі обмеження, такі як

- Помірна складність і вимагає більше часу для розгортання;

- Він не має графічного інтерфейсу користувача (GUI) і сумісний тільки з ОС Linux.

Suricata

Suricata - це СВВ з відкритим кодом, розроблений Фондом відкритої інформаційної безпеки (англ. Open Information Security Foundation, OISF). Suricata вважається однією з найшвидших СВВ, оскільки вона заснована на багатопотокових методах, які використовуються при виявленні. Крім того, дана система використовує як сигнатури, так і методи виявлення на основі аномалії. Вона спрямована на заміну Snort шляхом подолання його розвитку та архітектурних обмежень. Як результат, ця СВВ впроваджує нові функції, такі як паралелізм та підтримка у своїх реалізаціях.

Від самого початку Suricata працює в багатопотоковому режимі, що дозволяє оптимально використовувати декілька процесорів. До випуску версії 1.3 були деякі проблеми зі масштабованістю, наприклад, кількість ядер більше чотирьох не давала пришвидшення тестів. Тепер усі проблеми вирішені, і Suricata працює досить ефективно з 24 і більше процесорами. Крім того, Suricata може використовувати обчислення на стороні GPU (CUDA і OpenCL, опція збірки - -enable-cuda). В результаті цього СВВ спокійно справляється зі звичайним обладнанням із потоками до 10 Гбіт/с.

Як і Snort, Suricata складається з декількох модулів (захоплення, збирання, декодування, виявлення та виведення), за замовчуванням перед декодуванням захоплений трафік йде одним потоком, це оптимально з точки зору виявлення, але він завантажує систему більше. Але на відміну від налаштувань Snort, ви можете змінити цю поведінку і буквально використовувати одне налаштування в конфігурації, щоб розділити потоки відразу після захоплення, а іншою - вказати, яким чином потоки будуть розподілятися між процесорами. Це надає широкі можливості оптимізувати обробку трафіку на конкретному обладнанні в певній мережі.

Існують розроблені інструменти для перевірки трафіку HTTP на основі бібліотеки HTP, створеної автором ModSecurity Іваном Ристіком. Він підтримує вилучення та перевірку файлів, переданих через HTTP, аналіз стисненого вмісту, можливість ідентифікації за допомогою cookie, заголовків, користувальницького агента, органу запиту та відповіді. Ця функція Suricata, до речі, використовується в деяких мережах для запису HTTP-трафіку без виявлення. Вміст у потоці можна вибрати за маскою, використовуючи регулярні вирази, ідентифікація файлів можлива за іменем, типом або контрольною сумою MD5.

З самого початку підтримується декодування IPv6, включаючи тунелі IPv4-в-IPv6, IPv6-в-IPv6, Teredo та деякі інші. Модульне компонування двигуна дає можливість швидко підключити новий елемент для захоплення, декодування, аналізу або обробки пакетів. Для перехоплення трафіку використовується кілька інтерфейсів - NFQueue, IPFRing, LibPcap, IPFW, AF_PACKET, PF_RING. Режим Unix Socket дозволяє автоматично аналізувати файли PCAP, раніше захоплені іншою програмою (наприклад, sniffer).

Отже, Suricata - це більш швидка система, ніж Snort, здатна максимально використати можливості сучасних процесорів та графічних процесорів, при цьому повністю сумісна із Snort за правилами та умовами. Щоправда, є один мінус - велика кількість налаштувань і недостатньо зрозуміла документація з деяких питань. Хоча після першого встановлення система працює нормально і з налаштуваннями за замовчуванням, не буде великою проблемою провести тонке налаштування даної СВВ.

Snort

Snort – один з найвідоміших на даний момент інструмент в галузі, який використовується для аналізу пакетів, ведення журналів та виявлення вторгнень. Він був створений Cisco і може бути встановлений у Windows, а також у більшості дистрибутивах Linux.

Поєднання трьох його різних режимів дозволяє використовувати його як СВВ, так і СЗВ. Якщо ви використовуєте Snort лише як аналізатор пакетів, він

надає вам можливість живого зчитування пакетів мережі. Для лістингу пакетів він записує дані пакета у файл як журнали. Він може виявляти атаки такі як переповнення буфера, сканування портів, CGI-атаки, SMB-зонди та спроби фальсифікації службових даних авторизації. Він використовує різні методології (так звані "правила") для виявлення вторгнень. Ці правила по-різному працюють на виявлення на основі підписів, виявлення фактичної вразливості, а не експлуатування чи унікальний фрагмент даних. По суті, Snort використовує "відомий поганий" або "підозрюваний поганий" підхід, коли мова йде про виявлення вторгнення.

Під час використання Snort правила застосовуються до мережевого трафіку. Є змога завантажити деякі з цих правил, що називаються "базовими полісами" з веб-сайту Snort, або навчитися самостійно користуватися Snort і написати свої. На веб-сайті спільноти Snort також є люди, які можуть допомогти вам писати та завантажувати правила, розроблені іншими користувачами Snort.

Snort також працює з супутніми програмами, які називаються Snorby, BASE, Squil і Anaval. Усі вони призначені для більш глибокого аналізу даних, які збирає Snort, що може компенсувати деякі недоліки в програмному забезпеченні Snort. Однак для її ефективного використання потрібна ресурсоємка конфігурація, яка може не підходити для тих, хто не знайомий з таким програмним забезпеченням. Оновити свої правила також може бути досить складно, оскільки це потрібно робити вручну або за допомогою сценарію.

2.4. Експерименти перевантаження обраних систем виявлення вторгнень

Як згадувалося раніше, безпека розумних будинків стає складною темою, в якій експерти з безпеки та домашньої автоматизації намагаються підтримувати баланс між високими вимогами до безпеки розумного будинку та обмеженнями апаратного забезпечення підтримуючих інфраструктур. В цілому, ці середовища страждають від властивих їм апаратних обмежень, які обмежують їх здатність

реалізовувати комплексні заходи безпеки і підвищують їх схильність атакам вразливостей.

Щоб вибрати відповідні рішення для забезпечення безпеки, необхідно вивчити ці апаратні обмеження і переконатися, що вони не вплинуть на продуктивність цих рішень при захисті пристроїв, пов'язаних з розумним будинком. У світлі цього ми прагнемо в цих експериментах вивчити обрані нами системи виявлення вторгнень - Snort 3.0, Suricata 3.0.1 і Bro 2.5, щоб знайти найоптимальніший варіант для розумних будинків з точки зору споживання ресурсів і точності виявлення. Більш конкретно, ми вивчили продуктивність цих СВВ в режимі реального часу при моніторингу мережевого трафіку в реальному часі.

Інформація про продуктивність центрального процесора і оперативної пам'яті буде записана, проаналізована і порівняна.

Оцінка продуктивності кожної СВВ проводитиметься для 20 зразків шкідливого трафіку PCAP, що генерується різними типами атак.

Ті ж шкідливі файли pcap використовувалися для моніторингу ресурсів, що використовуються трьома системами, при аналізі трафіку та генерації попереджень. Для оцінки продуктивності трьох СВВ інформація, записана під час виконання шкідливих зразків PCAP, включає використання ЦП і оперативної пам'яті. TCPreplay використовується для відтворення шкідливих файлів PCAP в мережевих СВВ. У Таблиці 2 показані зразки шкідливого трафіку PCAP, використані в експериментах завантаженості визначених раніше систем виявлення вторгнень.

Таблиця 2.3

Список PCAP шкідливих файлів використаних в експерименті

#ID	Тип шкідливого ПЗ в PCAP	Розмір PCAP
#1	Malspam traffic	1.03MB
#2	Necurs Botnet Malspam	448 KB
#3	Payment Slip Malspam	3.0 MB

#4	MedusaHTTP malware	669 kB
#5	Adwind Malspam	1.7 kB
#6	KainXN EK	1.93 MB
#7	Cyber Ransomware	584 KB
#8	Locky-malspam-traffic	285 KB
#9	Facebook Themed Malspam	1.4 MB
#10	BOLETO Malspam infection traffic	2.4 MB
#11	Pizzacrypt	254.4 KB
#12	BIZCN Gate Actor Nuclear	0.98 MB
#13	Fiesta Ek	1.52 MB
#14	Nuclear EK	2 MB
#15	Fake-Netflix-login-page-traffic	768 KB
#16	URSNIF Infection with DRIDEX	2.5 MB
#17	Dridex Spam trafic	999 KB
#18	Brazil malware spam	12.7 MB
#19	Info stealer that uses FTP to exfiltrate data	1.4 MB
#20	Hookads-Rig-EK-sends-Dreambot	595 KB

Використання оперативної пам'яті.

На рисунку 2.2 порівнюються результати щодо швидкості використання оперативної пам'яті для кожного зразка шкідливого ПЗ для трьох систем виявлення вторгнень: Snort, Suricata і Bro. З отриманих результатів ми також можемо зробити ті ж висновки щодо завантаженості ЦП; СВВ Snort дає найвищі показники використання оперативної пам'яті для більшості зразків PCAP. Результати знаходяться в діапазоні від 60% до приблизно 80%. У той час як найвищі показники були зафіксовані для зразків № 4, № 13 і № 19.

У системі Suricata були зафіксовані відносно нижчі показники, ніж в Snort, в діапазоні від 20% до приблизно 40%.

У той час як Bro був найкращою ідеєю з точки зору використання оперативної пам'яті, зафіксувавши найнижчі показники для більшості тестів (від 20% приблизно до 34%). Як і в тестах процесора, також спостерігається, що тип шкідливого трафіку робить істотний вплив на використання оперативної пам'яті для трьох IDSS.

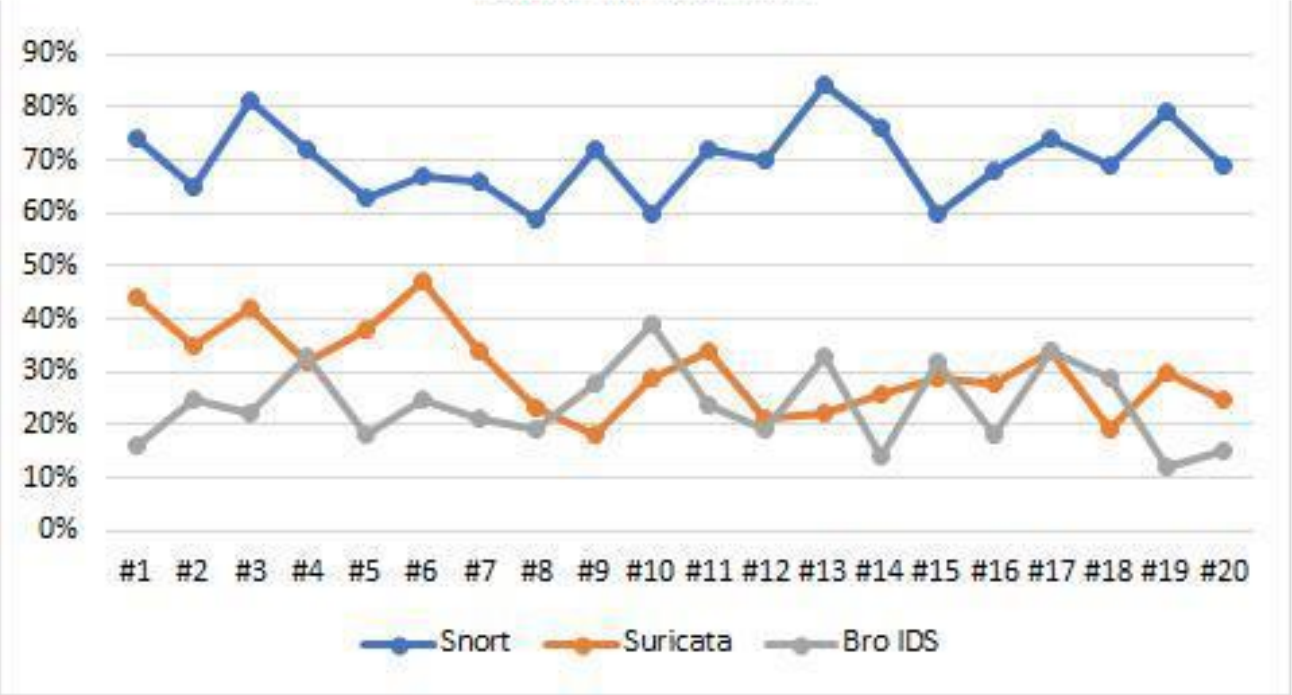

Рис. 2.2. Завантаження оперативної пам’яті під час експерименту

Завантаження процесора

На малюнку 2.3 порівнюються результати по швидкості завантаження ЦП для кожного зразка шкідливого ПЗ для трьох СВВ: Snort, Suricata і Bro.

З отриманих результатів видно, що система Snort зафіксувала найвищі показники завантаження ЦП для більшості зразків PCAP, від 60% до 70%. У той час як Suricata і Bro зафіксували відносно нижчі показники для тих же тестів на атаку шкідливими програмами.

Завантаження ЦП для обох СВВ коливається від 20% до 40%, однак Suricata дає більш низькі показники для більшості тестів в порівнянні з Bro і Snort. Також простежується, що тип шкідливого трафіку робить істотний вплив на завантаження ЦП, кожна СВВ дає різні показники завантаження ЦП для однієї

і тієї ж тестової атаки, оскільки вони діють абсолютно по-різному для кожної атаки.

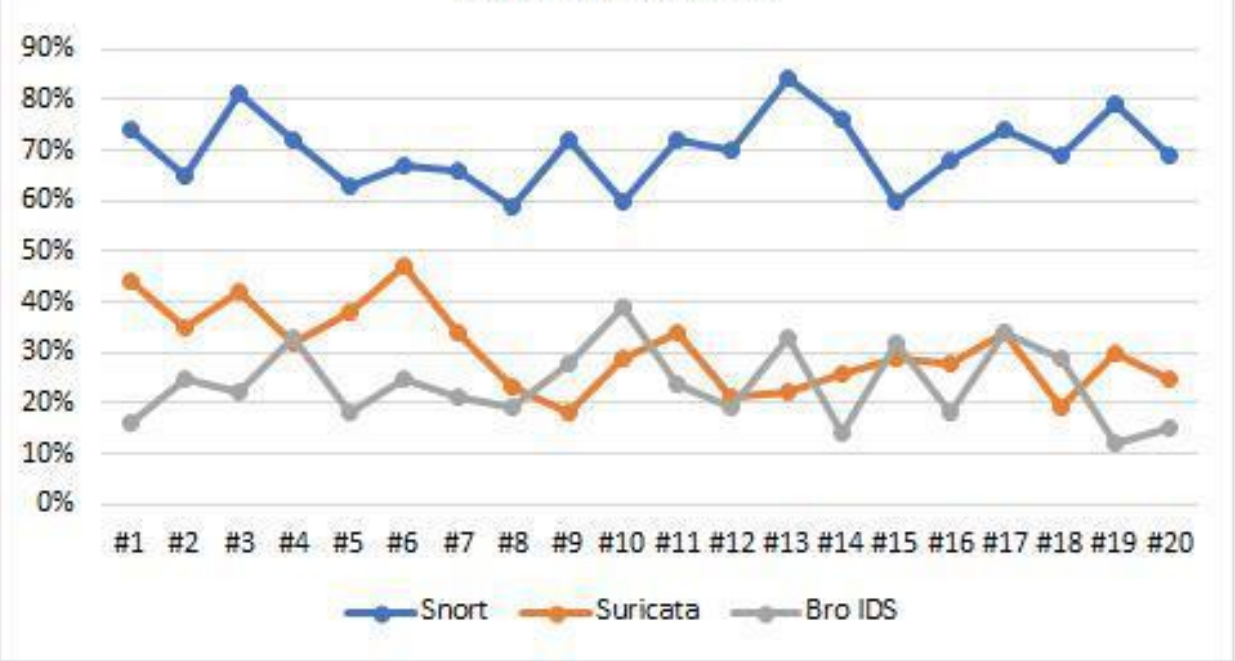

Рис. 2.3. Завантаження ЦП під час експерименту

2.5. Висновки до розділу 2

У другому розділі дипломної роботи було проаналізовано принципи та основні особливості функціонування систем виявлення вторгнень: Bro, Snort та Suricata. Всі вони на сьогоднішній день є найбільш розвиненими та здатні забезпечувати певний рівень безпеки інтелектуального середовища на базі Інтернету Речей.

Проте система виявлення вторгнень Bro, як один з масштабних першовідкривачів цього стеку технологій, нині є дещо застарілою, більш складною та важчою у використанні, адже вона може використовуватись виключно на ОС Linux.

Щодо Snort, ця система досі може забезпечувати належний рівень безпеки в інфраструктурах довільного масштабу та рівня складності архітектури. Проте, саме цьому ПЗ властива неактуальність протоколів, таких як відсутність можливості багатопотокової обробки та нативна підтримка IPv6.

Suricata, будучи від самого початку сучасним ПЗ з відкритим вихідним кодом та неабиякою підтримкою компанії Stamus Networks[31], має більший функціонал та здатність до модульного використання, зокрема більш глибокий та прискорений аналіз мережевих журналів операційних систем з одночасним моніторингом мережевого трафіку в реальному часі, підтримкою сучасних протоколів таких як IPv6 та можливістю аналізу пакетів на 7 рівні моделі OSI.

РОЗДІЛ 3. ВПРОВАДЖЕННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖУ ІНТЕЛЕКТУАЛЬНОГО СЕРЕДОВИЩА

3.1 Опис реалізації системи виявлення вторгнень в мережу інтелектуального середовища

Для демонстрації і розгляду можливостей системи виявлення вторгнень SELKS, мною було впроваджено дану систему в мережу, яка складається з:

- Мережевого маршрутизатора MikroTik;
- Робочі станції користувачів(ноутбуки, ПК);
- Мобільні пристрої користувачів;
- Точки доступу Ubiquiti;
- Та серверу на базі обладнання HP.

1. Почнемо зі встановлення програмного комплексу SELKS

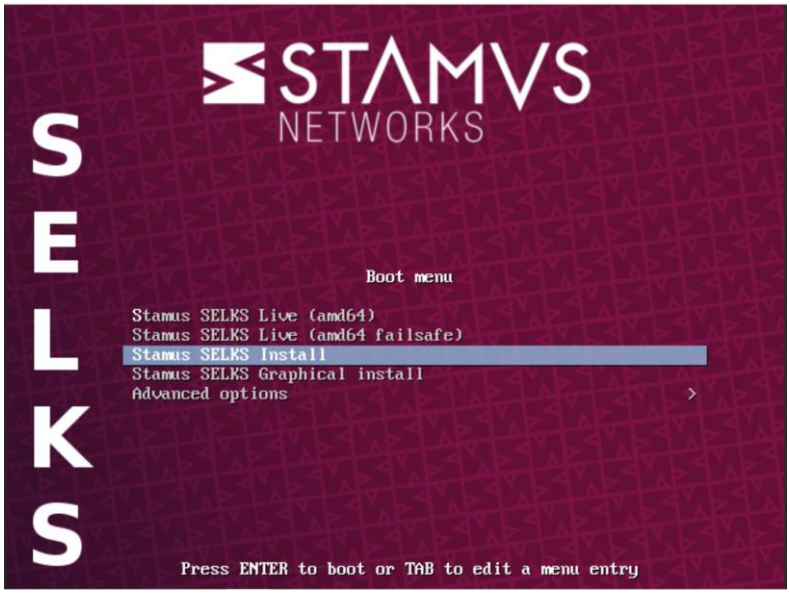

Рис. 3.1. Початкове меню інсталятора Системи Виявлення Вторгнень SELKS від Stamus Networks

2. Визначимо всі необхідні параметри локалізації, та дочекаємось завантаження утиліти розмітки дисків:

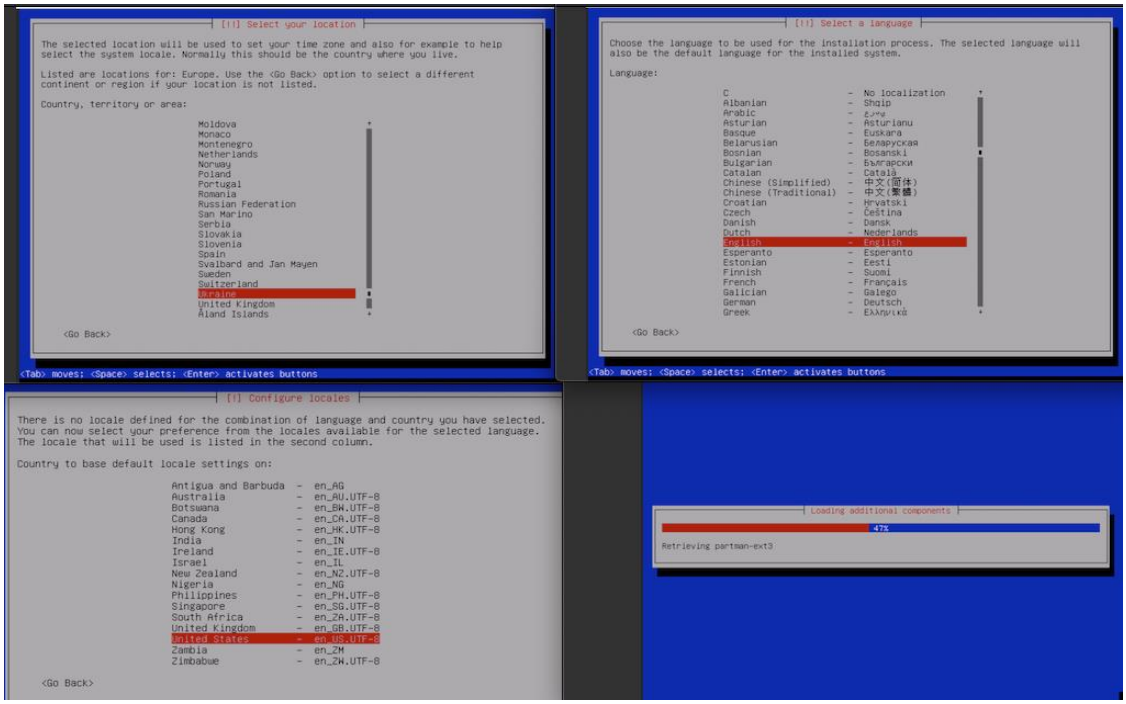

Рис. 3.2. Налаштування параметрів локалізації та ініціалізація утиліти розмітки дисків

3. Після завантаження утиліти розмітки, встановимо необхідні параметри:

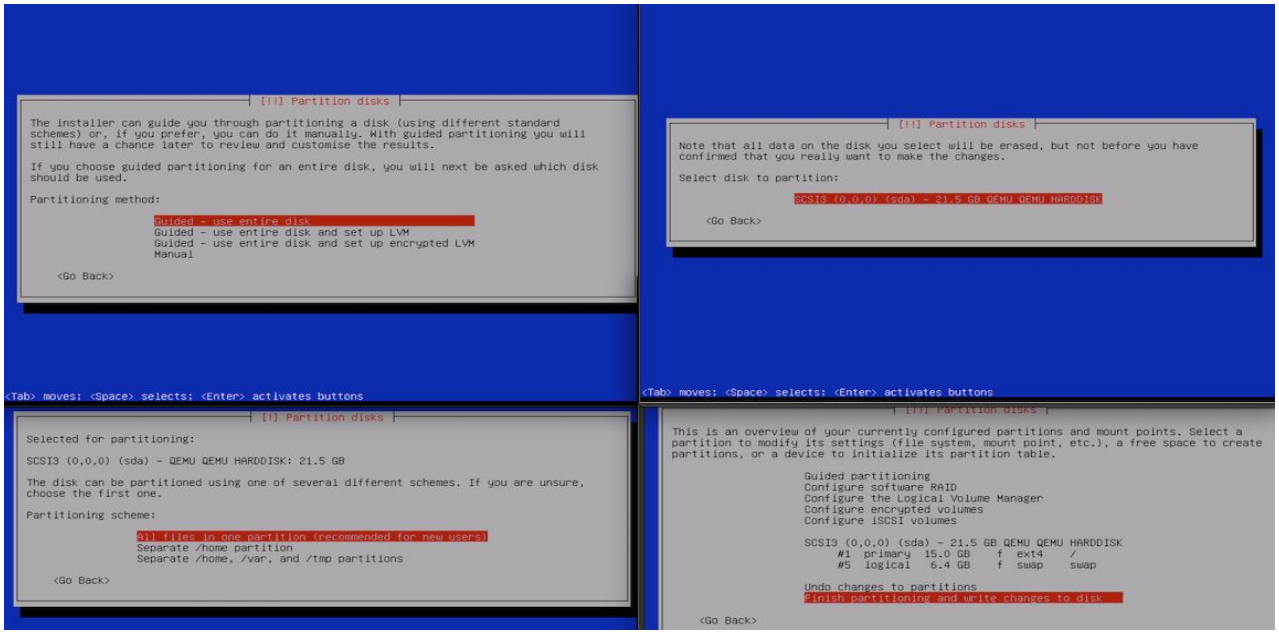

Рис. 3.3. Встановлення параметрів дискового простору.

4. Дочекаємось копіювання всіх необхідних даних, після чого налаштуємо параметр Master Boot Record, для коректного завантаження системи:

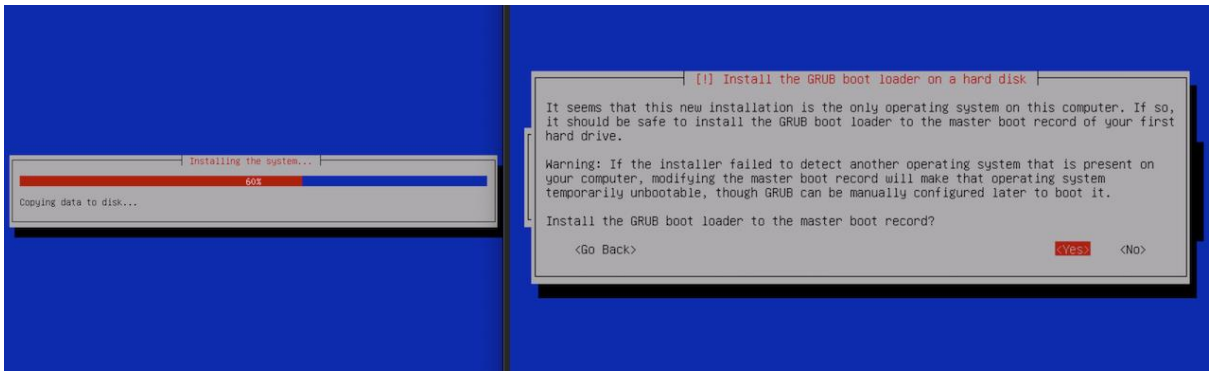

Рис. 3.4. Налаштування параметру Master Boot Record.

5. Після встановлення всіх необхідних пакетів, перезавантажимо сервер-пробу SELKS. Після завершення завантаження, авторизуємось за допомогою SSH на сервері та звіримо мережеві параметри отримані сервером з параметрами на мережевому обладнанні:

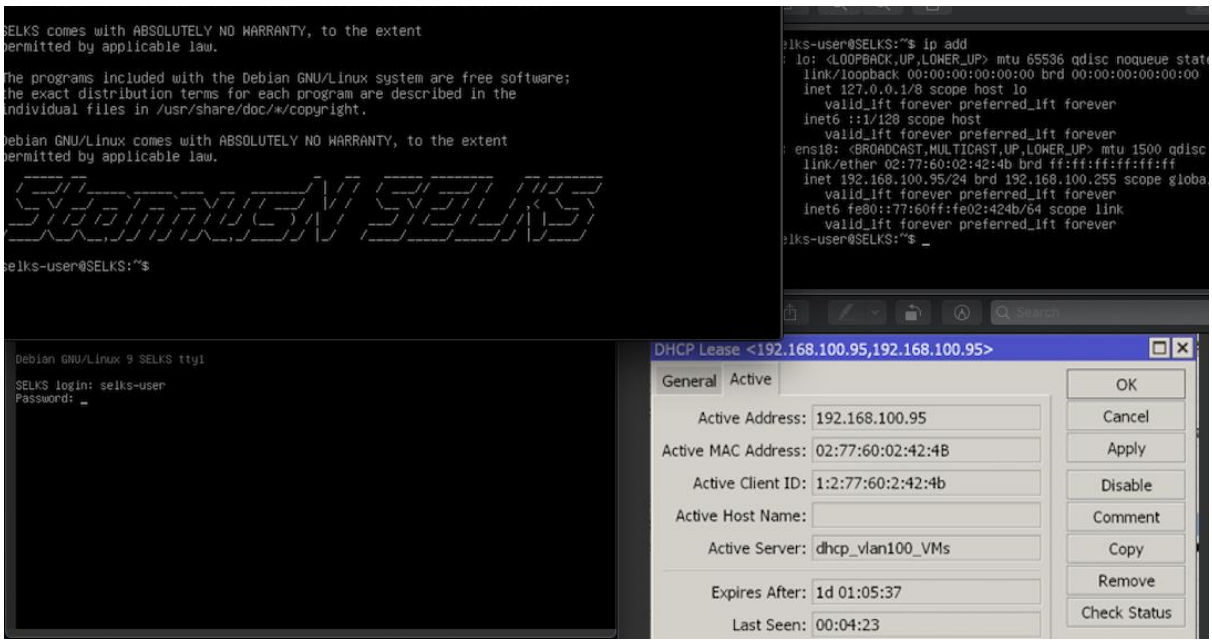

Рис. 3.5. Авторизація на сервер SELKS.

6. Параметри вірні, тож наступним кроком буде дублювання всього трафіку з нашого мережевого пристрою на інтерфейс-слухач сервера. Лістинг команди наведено на рисунку:

Рис. 3.6. Дублювання трафіку на інтерфейс-слухач.

7. Повернемось до командного рядку сервера, та встановимо всі необхідні оновлення ПЗ:

Рис. 3.7. Завантаження необхідних оновлень ПЗ.

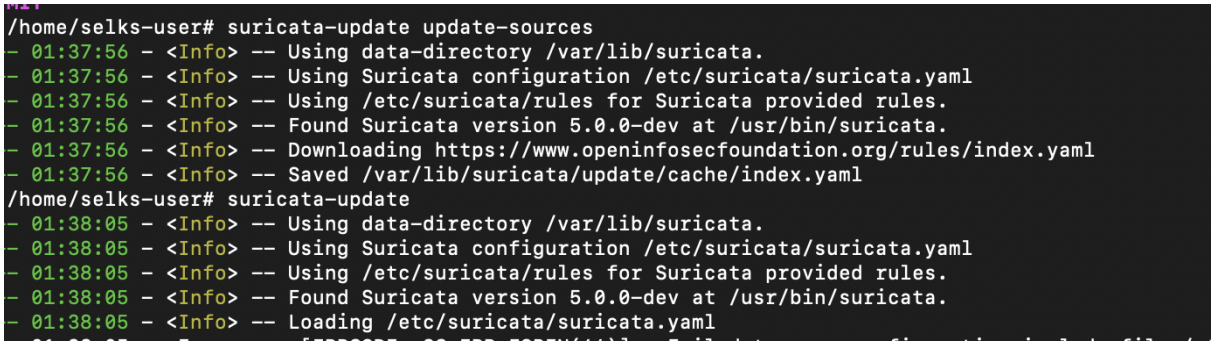

Рис. 3.8. Інсталяція завантажених оновлень ПЗ.

8. А також встановимо базовий набір правил виявлення та баз сигнатур, за допомогою команд, лістинг яких наведено нижче:

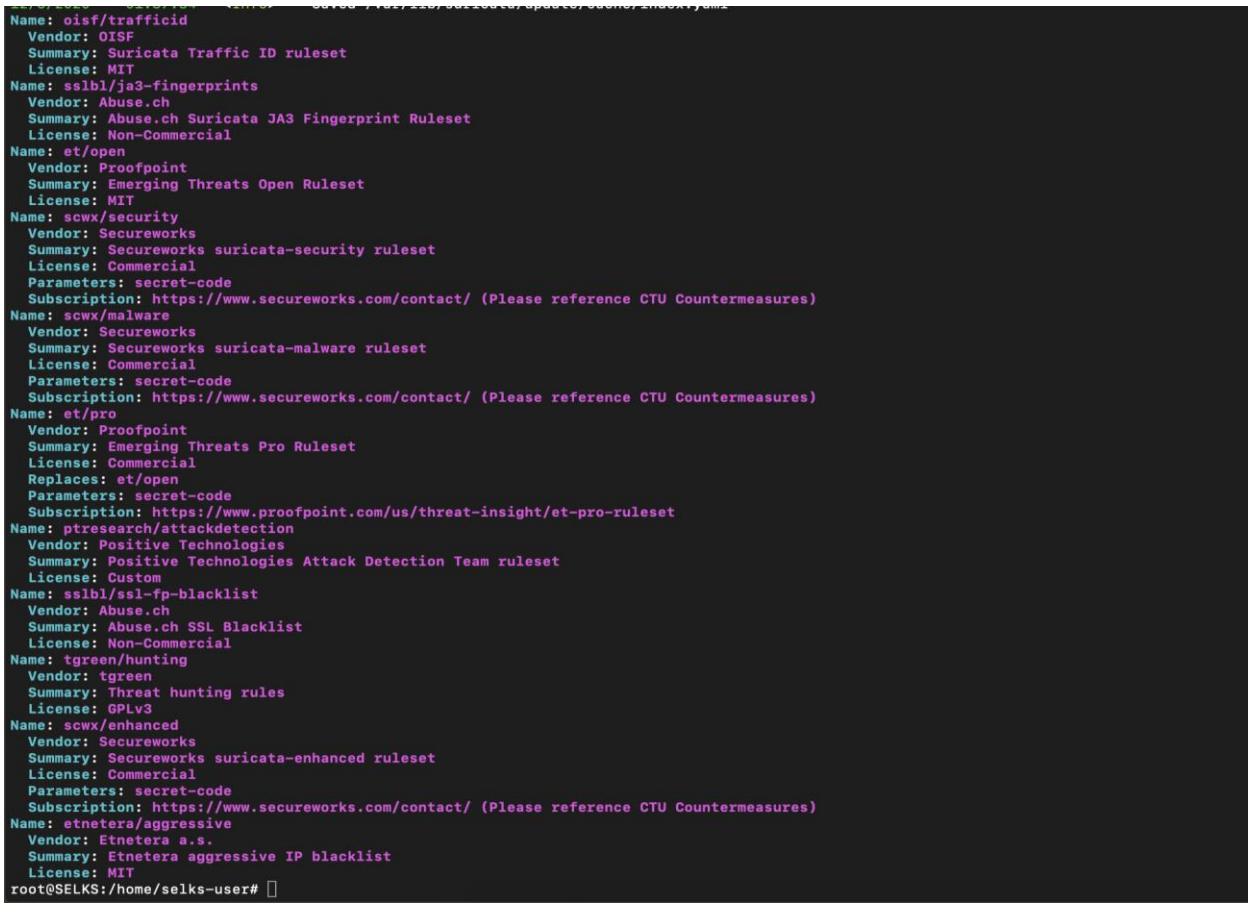

Рис. 3.9. Встановлення базових правил виявлення та баз сигнатур.

9. Після цього перезапустимо наш сервер вже в режимі активного прослуховування та аналізу трафіку, що надходить з мережевого обладнання:

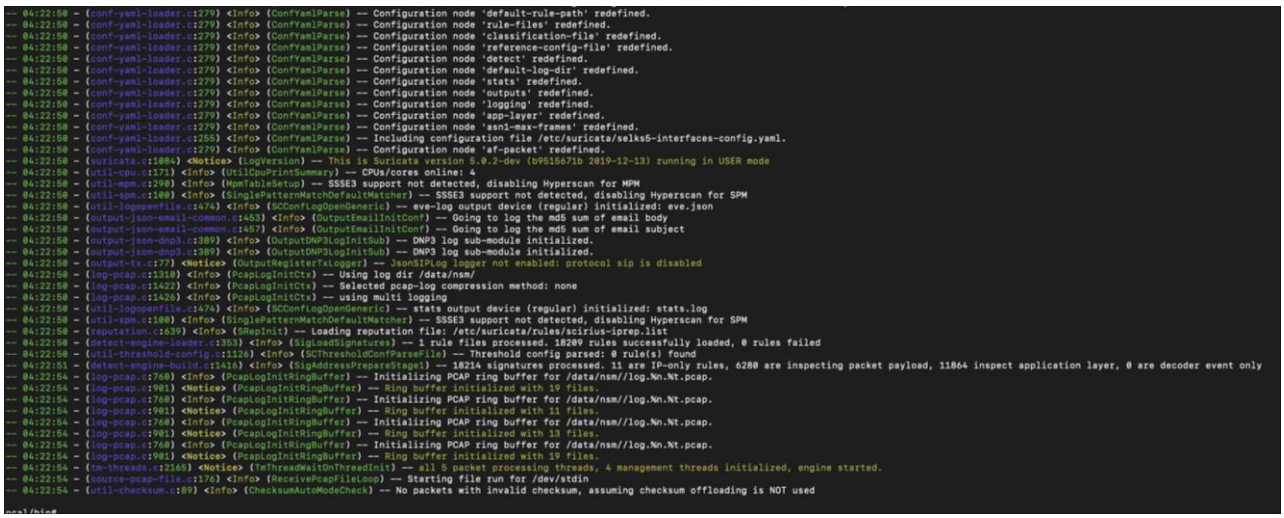

Рис. 3.10. Результат запуску серверу в режимі активного прослуховування та аналізу трафіку.

10. На цьому базове налаштування моніторингу внутрішнього мережевого трафіку -- завершено.

11. Наступним кроком, ми перейдемо до веб-інтерфейсу СВВ і використавши попередньо встановлені дані авторизації -- авторизуємось:

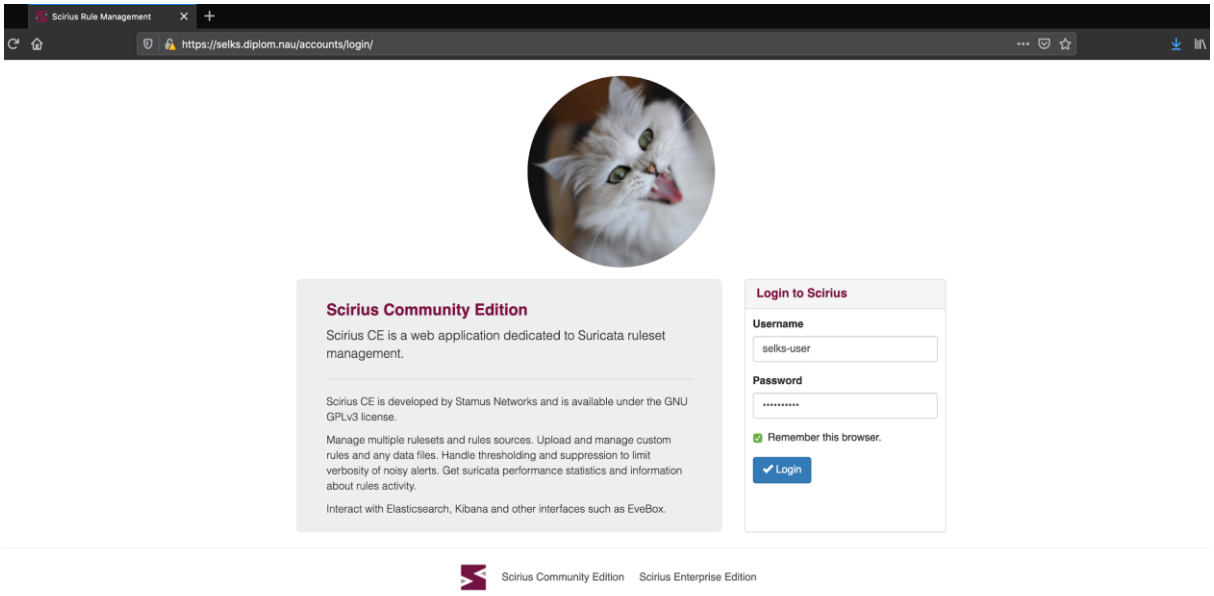

Рис. 3.11. Веб-інтерфейс СВВ. Меню авторизації в систему.

12. На зображеннях нижче можна помітити, що система вже проаналізувавши трафік в нашій мережі, надає детальну статистику стосовно подій на які варто звернути увагу, а також дані в режимі реального часу(кількість завантажених файлів на даний момент):

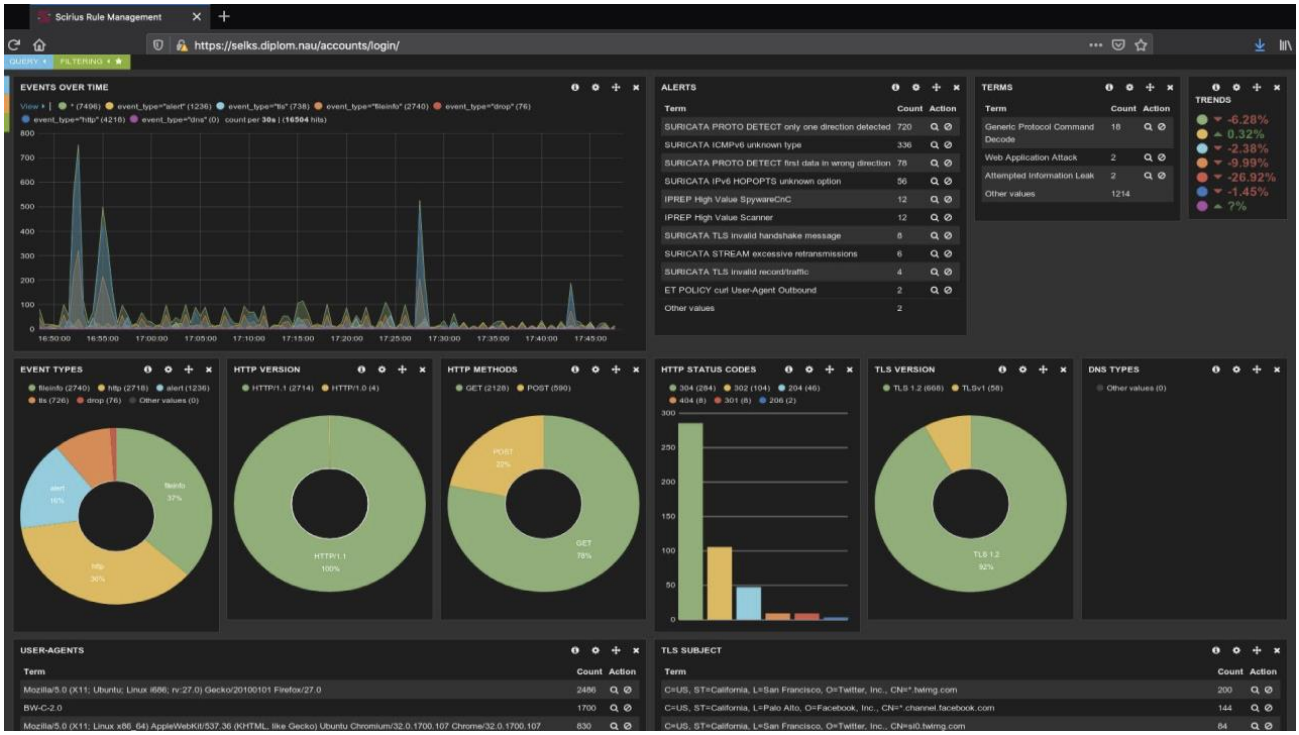

Рис. 3.12. Детальна статистика системи після аналізу трафіку.

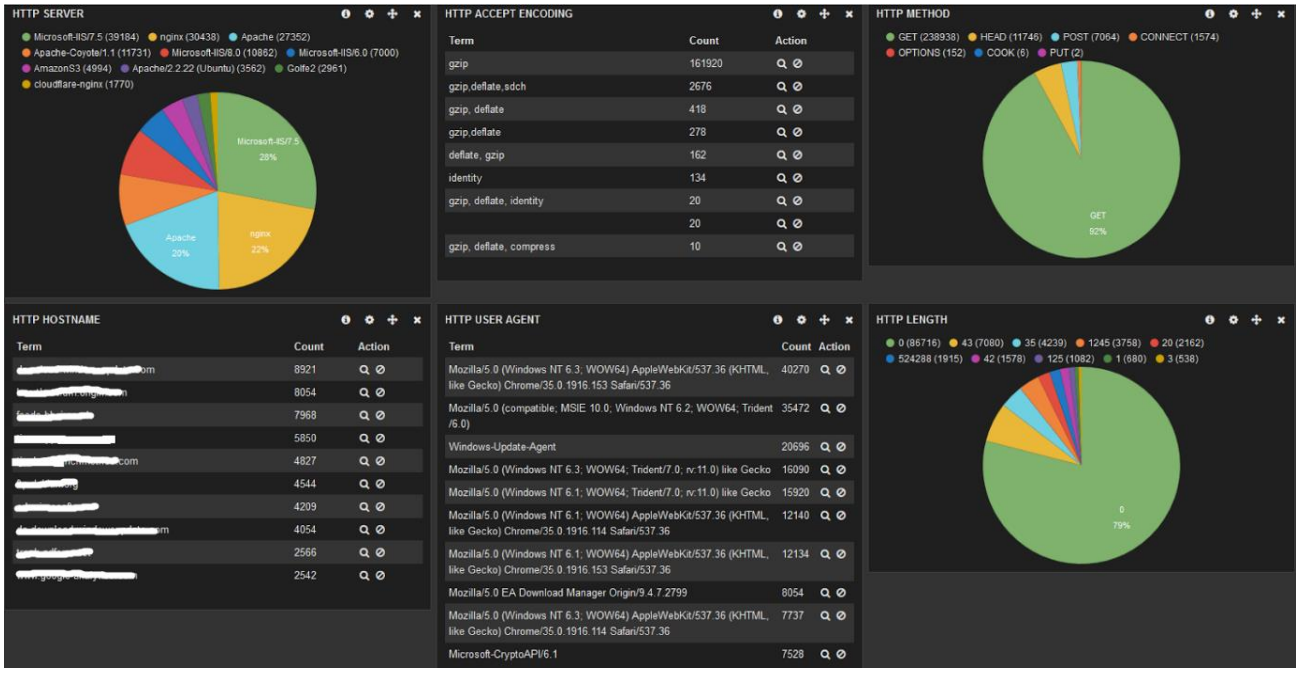

Рис. 3.13. Відображення даних мережевого трафіку в режимі реального часу.

3.2 Додаткові налаштування моделі системи виявлення вторгень для інтелектуальних середовищ

У міру того як наша залежність від Інтернету речей і технологій "розумного будинку" буде рости, користувачам буде необхідно розширювати свої методи забезпечення кібербезпеки. Окрім налаштування мережевої системи виявлення вторгнень, варто зробити наступні покращення вашого інтелектуального середовища, щоб захистити ваші особисті дані і конфіденційність, при цьому насолоджуючись усім, що можуть запропонувати ваші гаджети для розумного будинку:

- В першу чергу забезпечити безпеку мережі, а саме мережевого маршрутизатора. Впевнитись в його безпеці можна шляхом зміни паролю на роутері на більш складний, з використанням символів верхнього та нижнього регістрів, цифр та спеціальних символів. Не менш важливе регулярне оновлення паролю кожні кілька місяців/півроку задля задання більшого рівня безпеки.
- Також важливо запевнитись в тому, що пристрої Інтернету Речей, включаючи смартфони, є надійно захищеними. В цьому випадку ми можемо звернутись до комерційних та безкоштовних додатків-сканерів, які аналізують усі пристрої, що підключені до вашої мережі, наприклад Kaspersky IoT Scanner. Такі додатки аналізують усі підключення до мережі, перевіряє відкриті/закриті порти кожного пристрою, та надсилає користувачу сповіщення про те, які вразливі сторони пристроїв є на даний момент. Саме таким чином ви зможете захистити себе від потенційного потрапляння пристроїв інтелектуального середовища у відкритий доступ(приклад – ресурс Shodan, який дозволяє отримати доступ у режимі реального часу до малозахищенних пристроїв по всьому світу)
- Для перевірки пристроїв у мережі на вразливість можна також використати ПЗ - BlueBorne Vulnerability Scanner, який є безкоштовним і перевіряє усі пристрої в мережі на вразливості BlueBorne, котра може дозволити зловмисникам отримати доступ до всіх пристроїв, або влаштувати атаку лише через те, що у когось в системі може бути увімкнутий Bluetooth модуль.

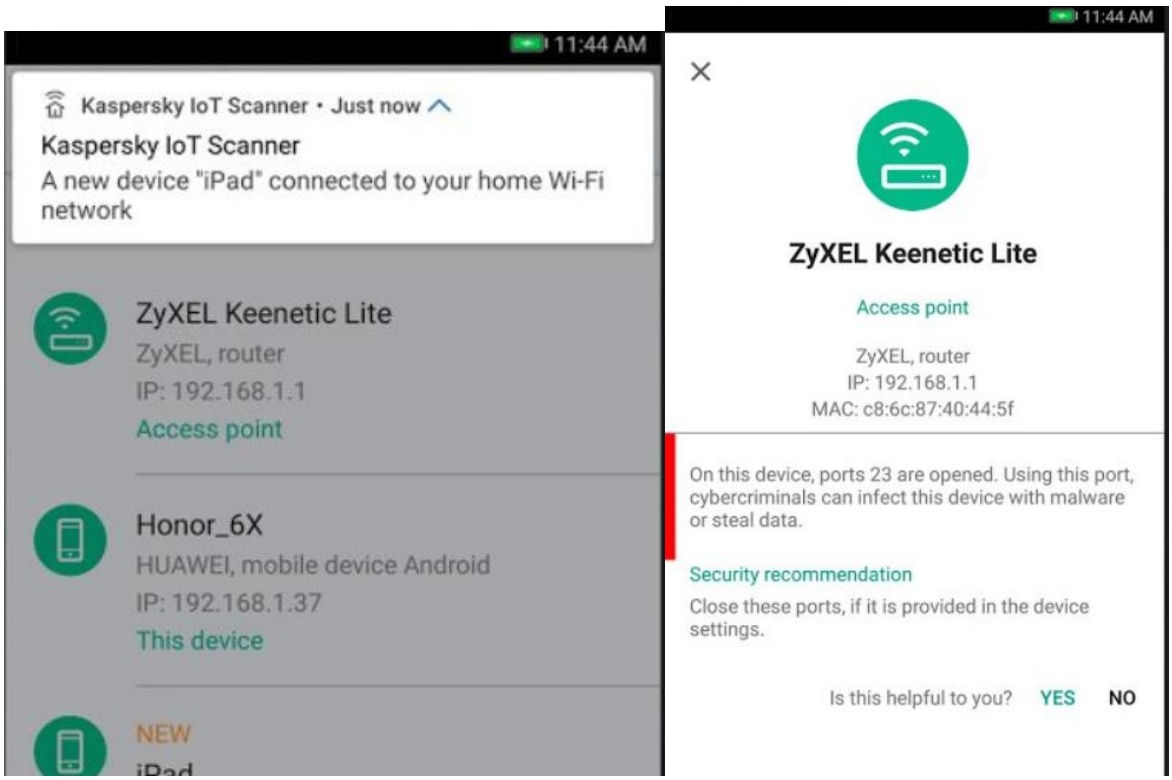

Рис. 3.14. Приклад вікна додатку Kaspersky IoT Scanner.

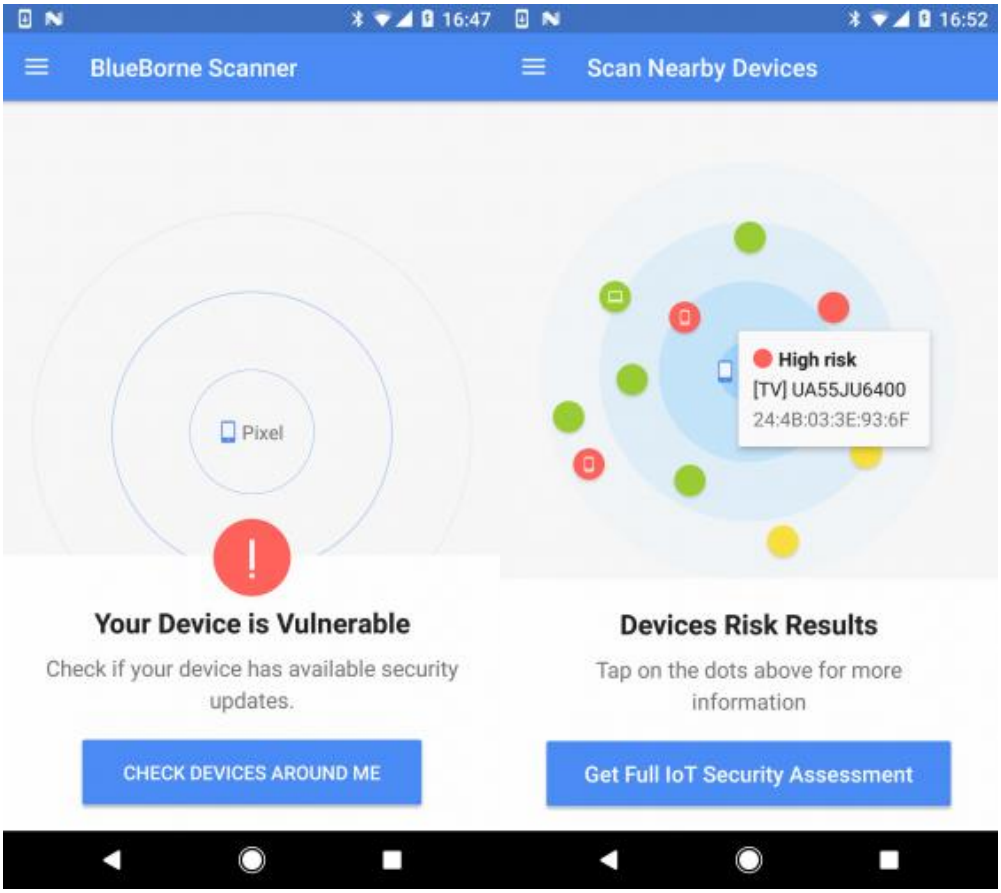

Рис. 3.15. Приклад вікна додатку BlueBorne Vulnerability Scanner.

- Обов’язковим фактором підвищення безпеки інтелектуального середовища є мультифакторна автентифікація на пристроях де це є можливим.
- У випадку якщо ви користуєтесь голосовим асистентом – найкращим варіантом буде зміна активаційного слова на щось, що знаєте лише ви та ваша родина/люди з якими ви проживаєте. Таким чином потенційний зловмисник не зможе отримати доступу до вашого голосового асистенту.
- Перевіряйте дозволи які надаються додаткам на ваших пристроях, все що може мати доступ до зміни налаштувань мережевого маршрутизатора потенційно може бути небезпечним для безпеки інтелектуального середовища.
- Також, для забезпечення відсутності фізичного втручання на житлову територію, наприклад «розумні міста», можна звернутись до комерційного рішення, що може надати система Kaspersky Antidrone – вона встановлюється окремо, в режимі реального часу відстежує невідомі літальні апарати на заданій відстані, слідкує за ними, та може в один клік надіслати радіосигнал, який знешкоджує будь які невідомі апарати, які потенційно можуть стежити та відслідковувати всю інфраструктуру інтелектуального середовища.

3.3 Висновки до розділу 3

В третьому розділі було спроектовано та реалізовано модель системи виявлення вторгнень в мережі інтелектуального середовища.

В якості вибору програмного забезпечення для реалізації проекту було віддано перевагу на користь ПЗ SELKS. Обґрунтування вибору програмного комплексу проводилося з урахуванням: функціональних характеристик, можливостей конфігурації, ресурсовартості, тощо.

Проведена реалізація захисту мережі є достатньою, щоб запобігти втручанню в адміністративний сектор мережі, що складається з мережевого маршрутизатора MikroTik, робочих станції користувачів, мобільних пристроїв користувачів, точки доступу Ubiquiti та серверу на базі обладнання HP.

Для того щоб підвищити ефективність системи аналізу та запобіганню вторгнень у мережу, мною були проведені наступні роботи:

- Встановлено останні оновлення програмного комплексу SELKS;
- Налаштовано моніторинг трафіку усієї мережі, а не окремих її частин;
- Запрограмовано найпоширеніші поведінкові фільтри для аналізу мережевих подій;
- Налаштовано інтуїтивно зрозумілий інтерфейс користувача для зручного нагляду і відстеження потенційних інцидентів мережевої безпеки.

ВИСНОВКИ

Результатом виконання дипломної роботи є розроблена система виявлення вторгнень для інтелектуальних середовищ, яка за рахунок спеціального налаштування моніторингу трафіку та поведінкових фільтрів дозволяє вчасно відстежувати та попереджувати потенційні інциденти мережевої безпеки.

У процесі виконання роботи отримані такі результати:

1. Були проаналізовані основні поняття та завдання сучасних систем виявлення вторгнень. В ході аналізу було виявлено, що брандмауер та антивірус, які використовуються разом, забезпечують певний захист, але цього, зазвичай, замало, тому варто звернутись до представників систем виявлення вторгнень.

2. Проведено порівняльний аналіз існуючих систем виявлення вторгнень для інтелектуального середовища. В ході аналізу методів були виявлені недоліки систем Bro та Snort, які суттєво занижують ефективність систем виявлення вторгнень у інтелектуальному середовищі.

3. Було розроблено систему виявлення вторгнень для інтелектуальних середовищ. На базі запропонованої системи виявлення вторгнень розроблено покрокову інструкцію для налаштування мережевого маршрутизатора, робочих станцій, мобільних пристроїв користувачів, та точок доступу. Також, були надані рекомендації щодо додаткових перевірки та захисту інтелектуального середовища від потенційних вразливостей. Крім того, отримані результати будуть корисними для інших інфраструктур державного та приватного сектору.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Beekman D., New York Daily News “Hackers hit companies like Nasdaq, 7-Eleven for $300 million, prosecutors says” [Електронний ресурс] // Режим доступу: World Wide Web. – URL: https://www.nydailynews.com/news/national/russians-ukrainian-charged-largest-hacking-spree-u-s-history-article-1.1408948

2. Analysis of Intrusion Detection Systems (IDS) [Електронний ресурс] // Режим доступу: World Wide Web. – URL: https://ukdiss.com/examples/intrusion-prevention-security.php

3. Survey of intrusion detection systems: techniques, datasets and challenges // https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7

4. Rosiek T., “What is a Next Generation Network Intrusion Detection System?” [Електронний ресурс] // Режим доступу: World Wide Web. – URL: https://www.bluvector.io/next-generation-network-intrusion-detection-system/

5. Cisco Firepower NGFW [Електронний ресурс] // Режим доступу: World Wide Web. – URL: https://www.cisco.com/c/en/us/support/security/firepower-ngfw/series.html

6. Network Design [Електронний ресурс] // Режим доступу: World Wide Web. – URL: https://resources.infosecinstitute.com

7. Essays, UK. Analysis of Intrusion Detection Systems (IDS), November, 2018

8. А. Мустафаев, "Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика", Вопросы безопасности, № 2. С. 1-7, 2016.

9. Lewis T. “IDS vs. IPS: How Each System Works and Why You Need Them” [Електронний ресурс] // Режим доступу: World Wide Web. – URL: https://www.lbmc.com/blog/ids-vs-ips/

10. В. Литвинов, "Аналіз систем та методів виявлення несанкціонованих вторгнень у комп’ютерні мережі", Математичні машини і системи, № 1, С.

31-40, 2018.

11. А. Браницкий, А. Котенко, "Анализ и классификация методов обнаружения сетевых атак", Тр. СПИИРАН, № 2 (45), С. 207-244, 2016.

12. Краткий анализ решений в сфере СОВ и разработка нейросетевого детектора аномалий в сетях передачи данных, 2018. [Электронный ресурс] // Режим доступа: https://habr.com/post/358200

13. Д. Даниленко, О. Смірнов, Є. Мелешко, "Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі", Системи озброєння і військова техніка, Х.: Харк. нац. ун-т Повітряних Сил ім. І. Кожедуба, № 1, С. 92-100, 2012.

14. А. Корниенко, И. Слюсаренко, "Системы и методы обнаружения вторжений: современное состояние и направления совершенствования", 2009. [Электронный ресурс] // Режим доступа: http://citforum.ru/security/internet/ids_overview/

15. R. Patel, A. Thakkar, A. Ganatra, "A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems", International Journal of Soft Computing and Engineering (IJSCE), vol. 2, no. 1, pp. 265-260, 2012.

16. Al-Sakib Khan Pathan, The State of the Art in Intrusion Prevention and Detection, 2014, 516 p. [Електронний ресурс] // Режим доступу: http://docshare03.docshare.tips/files/20579/205795770.pdf

17. К. Носенко, О. Півторак, Т. Ліхоузова, "Огляд систем виявлення атак в мережевому трафіку", Адаптивні системи автоматичного управління, К : НТУУ КПІ, № 1 (24), С. 67-75, 2014.

18. Amrit Pal Singh, Manik Deep Singh, "Analysis of Host-Based and Network-Based Intrusion Detection System", I. J. Computer Network and Information Security, vol. 8, pp. 41-47, 2014.

19. В. Мєшков, В. Віролайнен, "Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах", Проблеми безпеки інформації в інформаційно-комунікаційних системах, Д.: НТУУ КПІ РТФ, 2015. С. 4. [Електронний ресурс] // Режим доступу:

http://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf

20. С. Гриняев, Системы обнаружения вторжений, № 10, 2001. [Электронный ресурс] // Режим доступа: https://www.bytemag.ru/articles/detail.php?ID=6563

21. E Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas, "An implementation of intrusion detection system using genetic algorithm", International Journal of Network Security & Its Applications (IJNSA), Sylhet, Vol. 4, no. 2, pp. 109-120, 2012.

22. O. Lawal, "Analysis and Evaluation of Network-Based Intrusion Detection and Prevention System in an Enterprise Network Using Snort Freeware", African Journal of Computing & ICT, Ibadan, Vol. 6, no. 2, pp. 169-184, 2013.

23. S. Cooper, 11 Top Intrusion Detection Tools for 2018. [Електронний ресурс] // Режим доступу: World Wide Web. – URL: https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

24. Т. Зоріна, "Системи виявлення і запобігання атак в комп'ютерних мережах", Вісник східноукраїнського національного університету імені Володимира Даля, № 5 (204), С. 48-52, 2013.

25. Liu Hua Yeo, Understanding modern intrusion detection systems: a survey, 2017. [Електронний ресурс] // Режим доступу: World Wide Web. – URL: https://arxiv.org/ftp/arxiv/papers/1708/ 1708.07174.pdf

26. Д. Гамаюнов, Р. Смелянский, "Современные некоммерческие средства обнаружения атак", Программные системы и инструменты. Тематический сборник. М. : Ф-т ВМиК МГУ, С. 20, 2002.

27. Е. Явтуховский, "Анализ систем обнаружения вторжений на основе интеллектуальных технологий", Технические науки: теория и практика: материалы III Междунар. науч. конф., С. 27-30, 2016.

28. В.І. Мєшков, В.О. Віролайнен «Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах»

29. Tereykovsky I., Korchenko A., Parashchuk T., Pedchenko Y., Open intrusion detection systems analysis // Ukrainian Scientific Journal of Information

Security, 2018, vol. 24, issue 3, pp. 201-216.

30. Stamus Networks | SELKS [Електронний ресурс] // Режим доступу: World Wide Web. – URL: https://www.stamus-networks.com/scirius-open-source

31. Ray PP (2018) A survey on Internet of Things architectures. J King Saud Univ Comput Inform Sci 30(3):291–319

32. Khan R, Khan S, Zaheer R, Khan S (2012) Future internet: The internet of things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology. IEEE, Islamabad. pp 257–260

33. Liu X, Zhao M, Li S, Zhang F, TrappeW(2017) A security framework for the internet of things in the future internet architecture. Future Internet 9(3)

34. Liu C, Yang J, Chen R, Zhang Y, Zeng J (2011) Research on immunity-based intrusion detection technology for the internet of things. In: 2011 Seventh International Conference on Natural Computation, vol. 1. IEEE, Shanghai. pp 212–216

35. Minerva R, Biru A, Rotondi D (2015) Towards a definition of the Internet of Things (IoT). Technical report, IEEE, Internet of Things

36. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor 17(4):2347–2376

37. Ahmed E, Yaqoob I, Gani A, Imran M, Guizani M (2016) Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wirel Commun 23(5):10–16

38. Schaffers H, Komninos N, Pallot M, Trousse B, Nilsson M, Oliveira A (2011) Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. Springer, Berlin

39. Kumar S, Vealey T, Srivastava H (2016) Security in internet of things: Challenges, solutions and future directions. In: 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa. pp 5772–5781