Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Метод та засоби виявлення вторгнень на вузли в корпоративних комп'ютерних мережах
Назва теми

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Комп'ютерна інженерія

КРМКІ. 2001102.20.01.08 ПЗ

Виконав: студент 2 курсу, група КІ1м-20-1 Романюк К.І.
Підпис

Керівник проф., д. т. н, професор кафедри Кб Андрощук О.С.
Підпис

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

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

7.12 2021 р.

Хмельницький, 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КАФЕДРА КІБЕРБЕЗПЕКИ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП`ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ПРОГРАМУВАННЯ ТА ЗАХИСТ КОМП`ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П.Кльоц

"01" 09 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Романюку Костянтину Ігоровичу

Прізвище, ім'я, по батькові студента

Тема роботи Метод та засоби виявлення вторгнень на вузли в корпоративних ом'ютерних мережах

Керівник роботи Андрощук О.С,

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

доктор технічних наук, професор

Затверджена наказом № 102 ректора університету додаток №23 від 25.08.2021

2. Строк подання студентом проекту (роботи) на кафедру 20.11.2021

3. Вихідні дані до проекту (роботи) вторгнення в корпоративні мережі, методи та засоби виявлення вторгнень

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

Вступ. Моніторинг та аналіз сучасних корпоративних мереж. Методи і засоби дослідження та аналізу стану мереж. Системи виявлення атак і запобігання вторгнень в корпоративних мережах. Синтез системи захисту інформації на базі системи виявлення вторгнень. Висновки.

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

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання «_2_» _____вересня_____ 2021р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Прим
1	Вибір напряму дослідження та узгодження тематики КРМ з керівником	2.02.2021	
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	2.03.2021	
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	1.04.2021	
4	Робота над розділом 2 – розробка моделей і методів для вирішення поставленої задачі	1.05.2021	
5	Робота над науковою публікацією	1.06.2021	
6	Уточнення і затвердження теми	1.09.2021	
7	Робота над розділом 3 – розробка методу та алгоритмів, їх аналіз	2.09.2021	
8	Робота над розділом 4 – апробація запропонованих рішень	1.10.2021	
9	Узгодження отриманих результатів; оформлення пояснювальної записки згідно вимог	1.11.2021	
10	Оформлення графічної частини	8.11.2021	
11	Попередній захист роботи	10.11.2021	
12	Захист роботи на засіданні ЕК	8.12.2021	

Студент _____ Романюк К.І
Підпис Ініціали, прізвище

Керівник роботи _____ Андрощук О.С.
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод та засоби виявлення вторгнень на вузли в корпоративних комп'ютерних мережах

Автор роботи: Романюк Костянтин Ігорович

Керівник роботи: д.т.н., проф. Андрощук О.С.

Загальний обсяг роботи: 136 сторінок, 32 рисунка, 9 таблиць, 2 додатки, 42 посилання.

КОРПОРАТИВНІ МЕРЕЖІ, ЗАХИСТ ДАНИХ В МЕРЕЖАХ, ВИЯВЛЕННЯ ВТОРГНЕНЬ В МЕРЕЖАХ

Метою кваліфікаційної роботи є розроблення методу та відповідних засобів виявлення вторгнень на вузли в корпоративних комп'ютерних мережах для підвищення надійності та безпеки функціонування мереж.

Дана кваліфікаційна робота присвячена розробці методу та системи виявлення вторгнень у корпоративних мережах із використанням комбінованих підходів. Розроблений система дозволяє виявляти вторгнення як за сигнатурою, так і за поведінкою, що підвищує надійність передачі даних у корпоративних мережах.

7. 12. 2021р.

ANNOTATION

a qualification work of Romanyuk Konstantin

entitled «Method and means of intrusion detection on nodes in corporate computer networks».

Mentor: Ph.D. Androschyk O.

Total volume of work: 136 pages, 32 figures, 9 tables, 2 appendices, 42 references.

CORPORATE NETWORKS, DATA PROTECTION IN NETWORKS, DETECTION OF INVASIONS IN NETWORKS

The purpose of the qualification work is to develop a method and appropriate means of detecting intrusions on nodes in corporate computer networks to increase the reliability and security of networks.

This qualification work is devoted to the development of a method and system for detecting intrusions in corporate networks using combined approaches. The developed system allows to detect intrusions by both signature and behavior, which increases the reliability of data transmission in corporate networks.

7.12.2021р

ЗМІСТ

ВСТУП

Актуальність дослідження. Стрімкий та активний розвиток мережних технологій призводить до появи нових типів атак на корпоративні комп'ютерні мережі. Зростання кількості різноманітних методів вторгнень та їх реалізацій у вигляді атак вимагає необхідності удосконалення наявних технологій та засобів захисту даних у корпоративних комп’ютерних мережах.

Необхідним елементом вирішення сучасних складних завдань з управління системами та об’єктами різного роду виступає використання новітніх інформаційних технологій. Корпоративні комп’ютерні мережі є універсальним інструментом, який дозволяє забезпечити високу ефективність та надійність функціонування різноманітних систем. Паралельно з розвитком комп’ютерних мереж відбувається збільшення кількості користувачів та інформації, яку вони передають. Проте підвищення інтенсивності мережного трафіку може викликати погіршення якості мережевих послуг. Тому виникає необхідність вдосконалення інструментів для моніторингу та аналізу мережного трафіку.

Вивчення проблеми аналізу трафіку відбувається досить давно. Питанню пошуку ефективних рішень за різних умов і обмежень присвячена велика кількість досліджень, в тому числі за останні роки. Такий стан речей пов'язаний з тим, що відбувається швидка зміна мережного ландшафту, а методи і алгоритми, які демонстрували хороші результати в минулому, в нових умовах значно втрачають свою ефективність або не застосовуються більше взагалі.

Серед умов, що мають серйозний вплив на придатність різних методів, можна виділити швидке збільшення обсягу трафіку та смуги пропускання каналу зв'язку. Це означає, що виникає необхідність у пошуку алгоритму, який скорочує обсяг обчислень. В основі механізму виявлення вторгнень в систему лежить припущення про стаціонарність мережного трафіку, тобто під атакою розуміють будь-які відхилення від стаціонарних характеристик мережного трафіку. Звідси випливає, що проблема аналізу трафіку та виявлення вторгнень в корпоративну мережу потребує подальших досліджень.

Мета кваліфікаційної роботи полягає в розробленні методу та відповідних засобів виявлення вторгнень на вузли в корпоративних комп'ютерних мережах для підвищення надійності та безпеки функціонування мереж.

Для досягнення мети роботи необхідно вирішити наступні завдання:

1) провести аналіз корпоративних мереж та мережного трафіку на наявність аномалій, за якими можна визначати факт вторгнення;

2) провести аналіз відомих методів та засобів виявлення атак в мережах;

3) розробити метод виявлення вторгнень у корпоративну мережу;

4) реалізувати захист корпоративних мереж та дослідити його ефективність.

Об’єктом дослідження є захищеність передачі даних в корпоративній мережі

Предметом дослідження є методи та засоби виявлення вторгнень н вузли в корпоративних мережах.

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

Наукова новизна одержаних результатів.

У результаті дослідження розв'язано актуальну науково-практичну задачу розроблення методу виявлення вторгнень в корпоративну мережу. При цьому одержано такі наукові результати:

1) Проведено аналіз існуючих систем виявлення вторгнень IPS/IDS. Виявлено, що системи використовують сигнатурний принцип аналізу трафіку.

2) Розглянуто компоненти, що забезпечують ефективну роботу комп'ютерної мережі, підтримують постійну доступність і високу надійність мережі, а також обґрунтовано необхідність в системах моніторингу та керування.

3) Запропоновано вирішення проблеми захисту інфраструктури корпоративної мережі за допомогою використання IDPS систем.

4) Виявлено, що IDPS система може виконувати всебічний аналіз мережевого трафіку (рівень 7 моделі OSI) при розгортанні центрів обробки

даних на рівні ядра корпоративної мережі або на межі підключення до Інтернету.

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

Публікації. За темою кваліфікаційної роботи опубліковано 1 тези у збірнику наукових праць студентської конференції Університету економіки і підприємництва, 1-2 грудня 2021.

1 МОНІТОРИНГ ТА АНАЛІЗ СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Особливості та модель корпоративних комп’ютерних мереж

Майже в усіх частинах світу не можливо зустріти людину, яка б не користувалась інформаційними технологіями для особистого спілкування чи спілкування по робочих питаннях. Щодня кожен з нас надсилає текстові повідомлення, використовує всесвітню мережу Інтернет для пошуку необхідної інформації на різноманітних пристроях: на смартфоні, на ноутбуці або на планшетному ПК. Інформаційні технології (ІТ) стали повсякденними і загальновживаними та змінюють кожен аспект сучасного життя. Досягнення у здатності передавати та обробляти інформацію у цифровій змінюють економіку та суспільства багатьох країн світу.

Розвиток інформаційних технологій призвів до створення нового відкритого інформаційного суспільства, яке характеризується встановленням інтерактивної мережі між людьми у всіх сферах їх діяльності. Це призвело до появи віртуальних офісів, які дозволили віддаленим працівникам координувати свої дії, розвивати електронну комерцію, створювати нові засоби інформації та ін.

Комп’ютерна мережа (КМ) – це сукупність пов’язаних між собою через канали передавання даних комп’ютерів, що забезпечують користувачів засобами обміну інформацією та колективного використання апаратних, програмних та інформаційних ресурсів [1].

Використання персонального комп’ютера не є доцільним без доступу до мережі інформаційних ресурсів, адже при цьому значно обмежується його функціональність. Такі ресурси можуть бути зосереджені локально (локальна мережа офісу або підприємства) або у глобальних мережах, зокрема Інтернет.

Комп’ютерна мережа складається з наступних складових елементів:

1. Мережне обладнання – це спеціальні пристрої, завданням яких є поєднання комп'ютерного обладнання (або будь-якого іншого, яке має можливість роботи з мережею) в одну або кілька взаємодіючих систем.

2. Лінії зв'язку або лінії передачі даних – це проміжна апаратура і фізичне середовище, по якій передаються інформаційні сигнали (дані). Залежно від фізичного середовища передачі даних лінії зв'язку можна розділити на провідні лінії зв'язку, кабельні, бездротові.

3. Мережеве програмне забезпечення – це програмне забезпечення, що дозволяє організувати роботу користувача в мережі. Воно представлено загальним, системним і спеціальним програмним забезпеченням.

Класифікація КМ здійснюється за наступними ознаками:

1) територіально: локальні, регіональні, глобальні;

2) за топологією: шина, кільце, зірка, змішана топологія;

3) за середовищем передачі: вита пара, коаксіальний кабель, оптоволокно, телефонний кабель, радіозв’язок, супутниковий зв’язок;

4) за методом доступу до середовища передачі: конкурентний, детермінований з опитуванням або маркерним доступом;

5) за технологією: Ethernet, Archnet, Token Ring, FDDI, SNA, Internet та ін.

Комп’ютерні мережі можна умовно розділити на три групи, що є показником їх універсальності та масштабів розповсюдження [2]:

1. Глобальна комп’ютерна мережа Інтернет – всесвітня система об'єднаних комп'ютерних мереж для зберігання і передачі інформації.

2. Мережі Інтранет – локальна або територіально розподілена мережа, закрита від зовнішнього доступу з Internet. Така мережа дозволяє використання публічних каналів зв'язку, що входять в Internet, але при цьому забезпечується захист переданих даних і заходи для припинення проникнення ззовні на корпоративні вузли. Зараз фірми, що займаються електронним бізнесом в Internet мають змішану мережу, в якій підмножина внутрішніх вузлів компанії становить Intranet, а для зовнішніх вузлів (як правило, Web-сервери) запропонований термін Extranet. Прикладами таких мереж є національні мережі науки і освіти, мережі спеціального призначення.

3. Корпоративні комп’ютерні мережі – це мережі, головним призначенням яких є забезпечення функціонування конкретного підприємства, що володіє цією мережею. Користувачами корпоративної мережі є тільки

співробітники даного підприємства. На відміну від мереж операторів зв'язку, корпоративні мережі, в загальному випадку, не надають послуг іншим організаціям або користувачам.

Корпоративна мережа, яка об'єднує локальні мережі відділень корпорації (організації, компанії), є матеріально-технічної базою для вирішення завдань планування, організації та здійснення її виробничо-господарської діяльності. Вона забезпечує функціонування автоматизованої системи управління і системи інформаційного обслуговування корпорації.

З метою забезпечення оптимального доступу до інформації, розміщеної на інформаційних серверах національних або корпоративних мереж, їх інформаційно-технологічні компоненти (телекомунікації) базуються на одному і тому ж принципі на єдиній технологічній платформі. У той же час користувачі національних мереж та мереж компаній автоматично отримуватимуть доступ до глобальної мережі Інтернет.

Основні особливості корпоративних мереж:

1) для роботи використовуються ті ж засоби, що і для локальних мереж загального призначення;

2) відокремлення внутрішньої мережі організації від глобальних мереж за допомогою міжмережевого екрану (ММЕ), доступ до інформації надається лише користувачам внутрішньої мережі;

3) в межах мережі передається інформація офіційна (загальна для всієї організації), групова (захищена, призначається певній групі або відділу), неофіційна (особиста інформація співробітників);

4) наявність централізованої системи управління (ефективністю функціонування, безпекою, життєздатністю) корпоративною мережею.

1.1.1 Властивості корпоративних мереж

Для існуючих корпоративних мереж характерні наступні твердження:

1. Використання розподіленої обчислювальної моделі, хоча останнім часом більшого поширення набуває технологія тонкого клієнта (комп'ютер або програма-клієнт в мережах з клієнт-серверною або термінальною архітектурою,

який переносить всі або більшу частину завдань по обробці інформації на сервер).

2. Додатки невіддільні від відповідних підрозділів компанії, оскільки частина коду програми знаходиться на клієнтській станції.

3. Потрібно одночасно керувати кількома локальними мережами та мати зв’язок між центральною консоллю та консолями управління.

4. Різноманітні способи вираження, зберігання та передачі інформації.

5. Об’єднання даних різного призначення та для різних користувачів в одну базу даних. І навпаки, розташування даних у віддалених мережевих вузлах (наприклад, текстові звіти, що зберігаються на робочих станціях).

6. Абстрагування власника даних від фізичної структури та розташування даних.

7. Участь в автоматизованому процесі обробки інформації для великої кількості різних типів користувачів та працівників. Прямий і одночасний доступ до великої кількості ресурсів (включаючи інформаційні) користувачів різних категорій.

8. Велика різноманітність інформаційно-комунікаційних технологій та програмного забезпечення.

9. Засоби захисту у функціональному обладнанні, що використовується в системі, не має програмно-апаратної підтримки.

Згідно з визначенням корпоративної мережі, її склад, як правило, складається з таких функціональних елементів [4]:

1) робочі місця (абоненти), в одній будівлі або розподілені на певній території;

2) інформаційні сервери компанії використовується для зберігання та обробки інформаційних масивів (баз даних) для різних функціональних цілей. Вони також можуть бути зосереджені або розподілені на великій території;

3) засоби телекомунікації для забезпечення взаємодії між робочими станціями та з інформаційними серверами. Засоби можуть належати компанії (передача або оренда) або загальними (існують поза мережею зв'язку компанії, і компанія використовує їх ресурси). Зазвичай це засоби існуючих

загальнодоступних мереж.

Основною метою побудови корпоративних мереж є забезпечення зв'язку для розподілених бізнес-додатків, таких як:

– мережеві бази даних;

– електронна пошта;

– інформаційні портали;

– IP-телефонія;

– відеоконференції;

– дистанційне навчання.

Для внутрішніх потреб компанії можна використовувати лише одну з служб (телефон, телетекст, відеозв'язок, факс) або поєднати кілька служб з використанням відповідних засобів комунікації.

Залежно від послуг, реалізованих у мережі компанії, можливо доведеться використовувати власні інструменти управління мережею, включаючи інструменти маршрутизації та комутації, що є необхідним для ефективного використання мережевих ресурсів. Засоби управління мережевими елементами можуть бути [5]:

– керовані (власні або додаткові в рамках корпоративної мережі);

– некеровані (мережеве обладнання загальнодоступних мереж).

Необхідні служби мережевої безпеки повинні бути впроваджені в мережу компанії, і інструменти безпеки повинні використовуватися відповідно. У разі виходу з ладу елемента мережі повинні бути передбачені заходи, що забезпечують роботу всієї мережі або її фрагментів.

У корпоративній мережі повинні бути передбачені різні засоби для моніторингу роботи кожного функціонального елемента, а також система збору інформації про помилки та збої, управління ефективністю; управління безпекою. Засоби діагностики корпоративної мережі повинні бути розроблені та впроваджені як під час роботи, так і заздалегідь.

На додаток до цих функціональних елементів, комунікаційна мережа компанії повинна також мати план розвитку, який значною мірою визначає властиві їй функції, особливо з точки зору рівня протоколу взаємодії мережевих

компонентів та можливостей їх інтеграції.

1.1.2 Модель корпоративної мережі

Основним призначенням корпоративної мережі є надання користувачам необхідної інформації незалежно від того, де вони знаходиться, бажано в найкоротші терміни. Система захисту інформації повинна сприяти ефективній реалізації головної функції корпоративної мережі: своєчасного обміну корпоративною інформацією. Іншими словами, замість того, щоб будувати мережу за системою безпеки, система безпеки є додатковим важливим компонентом. Очевидно, що перед створенням моделі системи захисту необхідно визначити модель корпоративної мережі [6]. Приклад такої моделі показано на рисунку 1.1.

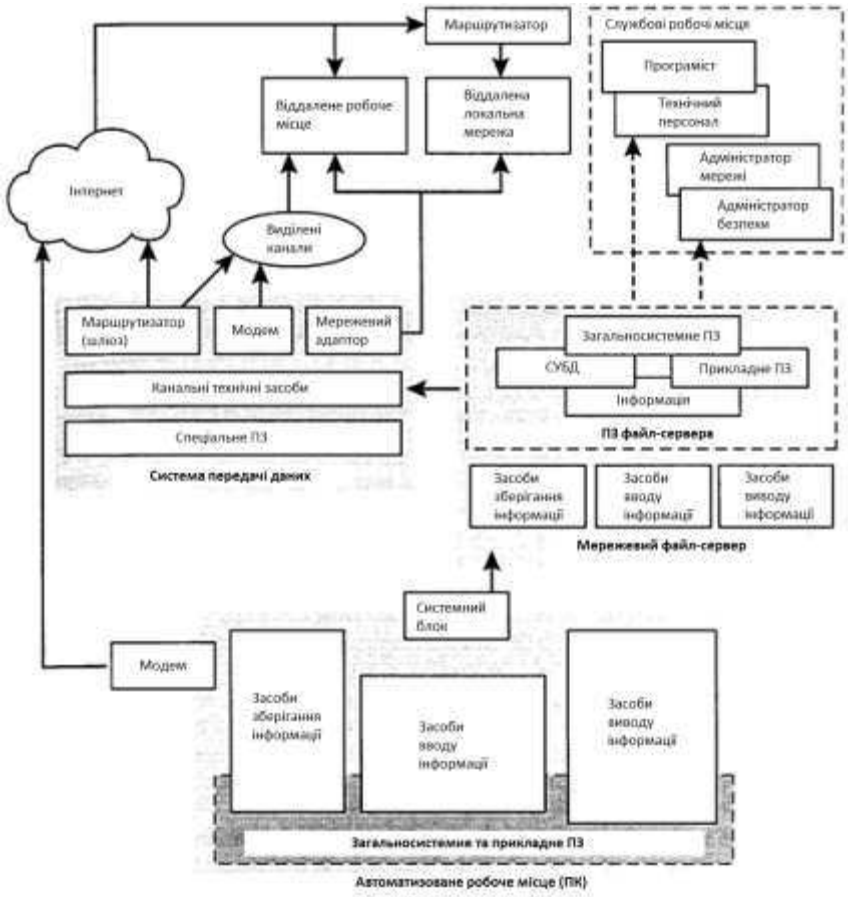


Рисунок 1.1 – Модель корпоративної мережі

Не існує двох однакових мереж, кожна мережа має свій унікальний спосіб. Тому необхідно визначити основні елементи мережі та створити досить спрощену, але відповідну модель корпоративної мережі, яка виконує всі

основні функції та включає весь набір елементів.

На даний час збільшилась кількість кіберзлочинців, метою діяльності яких є збір інформації, що обробляється відповідним програмним забезпеченням у комп'ютерних корпоративних мережах. Основою будь-якої мережі є програмне забезпечення на системному рівні, яке може включати різні операційні системи, програмні оболонки, загальні програми, текстові процесори, редактори та вбудовані програмні пакети, а також системи управління базами даних. Крім того, прикладне програмне забезпечення також використовується для обробки інформації, тобто це програми, створені спеціально для компаній та їх представників для вирішення конкретних проблем.

У процесі обробки інформації задіяне різне технічне обладнання для обробки, зберігання та передачі даних. Інформація може надходити з автоматизованих робочих місць (АРМ) через внутрішні та зовнішні канали зв'язку, може вводитись як з клавіатури, так і з зовнішніх носіїв. Крім того, мережа іноді використовує інформаційні ресурси інших установ та організацій та ресурси глобальних телекомунікаційних мереж. Глобальну телекомунікаційну мережу можна використовувати як засіб передачі інформації споживачам.

Термін "користувач корпоративної мережі" означає особу (організацію), яка має певні права доступу до мережі встановленим чином. В межах своїх повноважень користувачі можуть використовувати загальносистемне та прикладне програмне забезпечення лише для виконання дозволених операцій.

Обробка інформації в мережі здійснюється під наглядом системних адміністраторів, а її захист – під контролем адміністраторів безпеки, які виконують свої функції на спеціальних робочих станціях. Ці станції не завжди надають доступ до оброблюваної інформації, але завжди надають можливість впливати на їх обробку та модернізацію засобів обробки.

1.2 Стан та перспективи розвитку корпоративних мереж

Корпоративна мережа підприємства включає набір конкретних

інформаційних систем. Зазвичай їх поділяють на дві ключові частини: власну інфраструктуру компанії (мережа, організація, програмне забезпечення, телекомунікації та інформація) та функціональні підсистеми, які забезпечують вирішення необхідних завдань у компанії та досягнення запланованих результатів.

Завданням першої частини є забезпечення реалізації функціональної підсистеми, яка повністю визначає ключові особливості успішного використання. Після використання цієї підсистеми протягом багатьох років її основні принципи проектування та вимоги залишаються незмінними.

За нинішніх умов універсальні компоненти базової інфраструктури мають вищий пріоритет. Розвинена інфраструктура може реалізувати різні послуги, необхідні на системному рівні, що значно спрощує робочий процес і підвищує ефективність. Як результат, у процесі розвитку корпоративна мережа пройшла очевидний етап модернізації та отримала багато допоміжних послуг, орієнтованих на вирішення проблем у галузі координації та управління.

Корпоративна мережа являє собою цілісну структуру, що складається із взаємопов’язаних і взаємодіючих рівнів представлених на рисунку 1.2.

Рисунок 1.2 – Ієрархія рівнів корпоративної мережі

Як результат, комп'ютерна мережа компанії – це складна система, яка надає користувачам та програмам ряд корисних служб, професійні додатки на системному рівні з низкою корисних атрибутів та послуг для забезпечення нормальної роботи корпоративних мереж.

В наш час, незалежно від виду бізнесу, IT-інфраструктура компанії є ключовою інфраструктурою. З метою впровадження інформаційних технологій транспортна основа організовується через корпоративну мережу підприємства.

Сучасні корпоративні мережі – це не тільки мережі передачі даних, а й складні системи, які можуть надавати різні послуги з передбачуваними характеристиками.

За допомогою корпоративної мережі ефективно вирішуються такі ключові процеси:

– швидкий доступ до інформації загального інформаційного простору;

– аналіз стану та управління бізнес-процесами за допомогою єдиного аналітичного центру;

– обмін інформацією та документами;

– постійне і автоматичне спостереження та управління ресурсами інформаційно-комунікаційної системи з єдиного центру.

Основною метою проектування корпоративних мереж є визначення параметрів споживачів та виробників інформації, складу апаратного та програмного забезпечення, а також структури та організації продукції відповідно до характеристик інформаційного потоку підприємства, забезпечити основні вимоги для забезпечення якості наданої інформаційної послуги. Мережа обмежена з точки зору проектування, будівництва та витрат на обслуговування. Мережеві інтегратори та адміністратори мережі мають керуватися такими вимогам при проектуванні корпоративних мереж:

– розширюваність: можливість легко інтегрувати окремий мережевий компонент (користувач, комп'ютер, додаток, послуга);

– масштабованість: можливість збільшення кількості вузлів, довжини зв'язків і продуктивності мережевого обладнання та вузлів;

– продуктивність: забезпечення необхідних значень параметрів продуктивності вузлів мережі та каналів зв'язку (час відгуку, швидкість передачі даних, затримка передачі та зміни затримки передачі);

– керованість: забезпечення функції централізованого управління, моніторингу стану мережі та планування розвитку мережі;

– надійність: забезпечення безвідмовної роботи, безпеки мережевих вузлів та каналів зв'язку, відсутності спотворень даних вузла призначення;

– безпека: забезпечення захисту даних від несанкціонованого доступу.

Беручи до уваги масштаби, використання глобальних зв’язків, високий ступінь різноманітності проектування корпоративних мереж, це непростий процес. Поки що не існує універсального методу проектування корпоративних мереж. Тому слід сформулювати деякі типові етапи мережевого проекту.

Інформація, що обробляється в корпоративній мережі, особливо вразлива до атак. Можливість несанкціонованого використання або модифікації даних значно збільшується, і на це так чи інакше впливають:

– збільшення обсягу інформації, що обробляється, передається та зберігається на комп’ютері;

– наявність в базах даних інформації з різною важливістю та конфіденційністю;

– розширення доступу користувачів до інформації, що зберігається в базі даних та ресурсах обчислювальних мереж;

– збільшення кількості віддалених робочих місць;

– використання для спілкування між користувачами Інтернету різних каналів зв'язку у всьому світі;

– автоматизація обміну інформацією між комп’ютерами користувачів.

Процес проектування корпоративної мережі включає наступні кроки, які також показані на рисунку 1.3:

1. Аналіз вимог. На цьому етапі формується основна мета компанії (зменшення виробничого циклу, швидкий прийом замовлень, підвищення продуктивності праці тощо), що може покращити конкурентоспроможність компанії. Аналіз та перевірка існуючих подібних систем

2. Розробка бізнес-моделі компанії. Бізнес-модель або функціональна модель підприємства описує основні, адміністративні та допоміжні бізнес-процеси компанії, інформаційний потік між підрозділами та ієрархічні взаємозв'язки між підрозділами. Являє собою відображення функцій, середовища, інформації виробничої системи та об'єктів, що пов'язують ці функції.

Рисунок 1.3 – Етапи проектування корпоративної мережі

3. Розробка технічної моделі корпоративної мережі (структурний синтез). Модель являє собою сукупність технічних засобів, необхідних для реалізації проекту комп'ютерної мережі. На цьому етапі визначаються технічні параметри мережі: повний функціональний набір необхідного обладнання і програмного забезпечення, визначаються протоколи всіх рівнів OSI для кожної з можливих підмереж, необхідна продуктивність маршрутизаторів, комутаторів і концентраторів, властивості носіїв передачі та інші технічні параметри мережевого обладнання.

4. Розробка фізичної моделі корпоративної мережі (параметричний синтез). Фізична модель являє собою детальний опис технології та програмних засобів, їх кількість, технічні параметри та методи взаємодії. Отже, фізична модель є конкретизацією технічної моделі мережі, в якій присутня конкретна мережа відповідно до технічних параметрів, зазначених у технічній моделі, мережеві пристрої, протоколи та інше обладнання.

5. Моделювання та оптимізація мережі. На цьому етапі для оцінки ефективності виконуються симуляції функціонування комп'ютерної мережі та її оптимізація.

6. Встановлення та налагодження системи. Цей етап включає координацію постачання субпідрядників, встановлення та введення в експлуатацію обладнання, а також навчання персоналу.

7. Тест системи. На цей час повинні бути проведені приймальні випробування, зазначені в контракті з інтегратором.

8. Технічне обслуговування та експлуатація системи. Ця фаза не є має чітко визначені часові межі та представляє собою постійний процес.

Параметри якості корпоративної мережі:

– пропускна здатність мережі: характеризує обсяг інформації, що передається мережею за одиницю часу.

– відповідь на характеристики профілю трафіку: параметр, який характеризує коливання навантаження мережі в залежності від властивостей профілю трафіку.

– кількість спотворених або втрачених пакетів: для протоколу TCP 1-5% втрачених пакетів перебувають у межах норми, межа, при якій мережа практично не працює – 40% втрачених або спотворених пакетів;

– час доставки: тривалість доставки даних (вперед і назад), варіюється від 0 до 2000 мс і може впливати на продуктивність потоку;

– нерівномірність часу доставки пакетів: параметр, який впливає на роботу окремих додатків.

Тому корпоративна мережа – це складна система, що включає тисячі різних компонентів: комп'ютери різних типів, системне та прикладне програмне забезпечення, мережеві адаптери, концентратори, комутатори та маршрутизатори, кабельні системи. Основне завдання - забезпечити, щоб ця громіздка і досить дорога система могла найкращим чином справлятися з обробкою потоків інформації, що циркулює серед працівників компанії, і давала їм можливість приймати своєчасні та раціональні рішення, які забезпечать виживання компанії в умовах високої конкуренції.

Корпоративна мережа є надзвичайно важливою частиною інфраструктури підприємства, без якої неможливе його функціонування. Їх найважливішим завданням є більш ефективне використання ресурсів компанії і, отже, підвищення ефективності роботи за рахунок використання допоміжних послуг.

1.3 Засоби моніторингу і аналізу стану мереж

Моніторинг мережі є важливим практичним завданням. Адміністратори прагнуть підтримувати свою мережу безперебійно. Якщо мережа «падає» хоча б на короткий проміжок часу, продуктивність підприємства погіршується, і (у випадку організацій, які надають державні послуги) здатність надавати основні послуги порушується. Отже, адміністратори повинні контролювати рух мережевого трафіку та ефективність роботи в мережі, переглядати та знаходити лазівки в мережевій безпеці.

Термін моніторинг мережі стосується роботи системи, яка постійно контролює комп'ютерну мережу на предмет повільних або несправних систем та повідомляє адміністратора мережі електронною поштою, телефоном або іншими способами про виявлення проблеми.

Моніторинг корпоративної мережі є важливою IT-функцією, яка може забезпечити економію при підвищенні продуктивності інфраструктури, ефективність роботи працівників та економії витрат.

Множину інструментів для аналізу та діагностики комп'ютерних мереж можна розділити на кілька великих класів.

Агенти систем управління, які підтримують функції одного зі стандартних MIB і надають інформацію через SNMP або CMIP. Для отримання даних від агентів зазвичай потрібна система управління, яка автоматично збирає дані від агентів.

Інтегровані системи діагностики та управління (Embedded systems). Ці системи реалізовані у вигляді програмних та апаратних модулів, які встановлюються в комунікаційних пристроях, а також у вигляді програмних модулів, інтегрованих в операційні системи. Основною відмінністю від

централізованих систем управління є те, що функції діагностики та контролю виконуються лише для одного пристрою. Прикладом цього класу інструментів є багатосегментний модуль управління ретранслятором Ethernet, який реалізує функції автоматичної сегментації портів при виявленні несправностей і призначає порти внутрішнім сегментам ретранслятора та деяким іншим. Як правило, вбудовані модулі управління "за сумісництвом" діють як агенти SNMP, які надають дані про стан пристрою системам управління.

Аналізатори протоколів. Це програмні або апаратно-програмні системи, які, на відміну від систем управління, обмежені лише функціями моніторингу та аналізу трафіку в мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що використовуються в мережах, як правило, кілька десятків. Аналізатори протоколів дозволяють встановити деякі логічні умови для отримання окремих пакетів і здійснити повне декодування отриманих пакетів, тобто вони показують у формі, зрозумілій для фахівця, вміст пакетів протоколів з різними рівнями в кожному з розшифровкою вмісту окремих полів кожного пакету.

Експертні системи. Цей тип системи збирає знання технічних спеціалістів для виявлення причин аномальної роботи мереж та можливих способів приведення мережі в робочий стан. Експертні системи часто реалізуються як окремі підсистеми різних засобів моніторингу та аналізу мережі: систем управління мережею, аналізаторів протоколів, мережевих аналізаторів. Найпростіша версія експертної системи – це контекстно-залежна система довідки. Найскладнішими експертними системами є так звані бази знань з елементами штучного інтелекту. Прикладами таких систем є експертні системи, інтегровані в систему управління Cabletron Spectrum та Network General Sniffer Protocol Analyzer. Завдання експертних систем – проаналізувати велику кількість подій, щоб дати користувачеві короткий діагноз причини відмови мережі.

Обладнання для діагностики та сертифікації кабельних систем. Умовно ці пристрої можна розділити на чотири основні групи: мережеві монітори, пристрої для сертифікації кабельних систем, кабельні сканери та тестери.

Мережеві монітори (їх також називають мережевими аналізаторами) використовуються для тестування різних категорій кабелів. Мережеві монітори також збирають дані про статистичні показники трафіку: середню інтенсивність всього мережевого трафіку, середню інтенсивність потоку пакетів з певним типом помилок тощо. Ці пристрої є найбільш розумними з усіх чотирьох груп пристроїв цього класу, оскільки вони базуються не лише на фізичному, але й працюють на рівні каналу, а іноді і на мережевому рівні.

Пристрої для сертифікації кабелів засвідчують один із міжнародних стандартів кабельної мережі.

Кабельні сканери використовуються для діагностики мідних кабельних систем.

Тестери використовуються для перевірки кабелів на фізичні обриви.

Багатофункціональне портативне обладнання для аналізу та діагностики. З розвитком широкомасштабної технології інтегральних схем стало можливим виготовлення портативних пристроїв, що поєднували функції декількох пристроїв: кабельних сканерів, мережевих моніторів та аналізаторів протоколів.

1.3.1 Аналізатори протоколів

Аналізатор мережевих протоколів є важливою частиною інструментів мережевого адміністрування. Щоб з'ясувати, чому мережевий пристрій працює так, а не інакше, аналізатор протоколів повинен використовуватися для прослуховування трафіку в реальному часі та вилучення даних і протоколів, переданих по мережевому кабелю. Аналізатор мережевих протоколів можна використовувати для вирішення таких завдань:

– виявлення та ідентифікації несанкціонованого програмного забезпечення;

– отримання такої інформації, як базові моделі трафіку та метрики утилізації мережі;

– ідентифікації протоколів, які не використовуються, з метою їх вилучення з мережі;

– генерації трафіку для випробування на проникнення для перевірки

системи захисту;

– роботи з системами виявлення вторгнень (IDS);

– прослуховування трафіку, тобто виявлення несанкціонованого трафіку за допомогою миттєвих повідомлень або бездротової точки доступу;

– вивчення роботи мережі.

Аналізатори протоколів можуть поставлятися як програмне забезпечення або як комбінація програмного та апаратного забезпечення. Апаратний аналізатор протоколів – це незалежний модуль. Аналізатори протоколів використовуються на робочій станції мережі і зазвичай виконують такі завдання:

– перегляд інформації про типи пакетів, що передаються по мережі, щоб можна було визначити точність передачі;

– запит всіх вузлів та перевірка передачі даних від точки до точки між вузлами;

– визначення конфігурації всієї мережі;

– аналіз критичних даних з будь-якого або всіх вузлів і повідомлення лише про незвичні дії на основі визначених користувачем порогових значень;

– перегляд даних про ефективність, таких як обсяг трафіку та обслуговування пакетів;

– надання додаткової інформації про ефективність мережі, продуктивність мережі, потенційні апаратні помилки, проблеми із шумом та проблеми прикладного програмного забезпечення.

Програмне забезпечення аналізатора складається з ядра, що підтримує роботу мережевого адаптера, та програмного забезпечення, що декодує протокол рівня зв'язку, з яким працює мережевий адаптер, а також із найбільш поширених протоколів вищого рівня, таких як IP, TCP, FTP, Telnet, HTTP, IPX, NCP, NetBEUI, DECnet тощо. Деякі аналізатори можуть також включати експертну систему, яка дозволяє повідомляти користувачеві, які експерименти проводити в конкретній ситуації, що можуть означати певні результати вимірювань та як виправити певні типи помилок мережі.

Типові функції. Більшість аналізаторів мережевих протоколів

відображають однакову основну інформацію, принаймні у певній початковій формі. Аналізатор працює на хосту. Коли аналізатор запускається в безладному режимі, драйвер мережевої карти, мережева карта, перехоплють весь трафік, що проходить через них. Аналізатор протоколів перенаправляє захоплений трафік на механізм декодування пакетів, який ідентифікує пакети та розподіляє їх на відповідні рівні ієрархії. Програмне забезпечення аналізатора протоколів перевіряє пакети та відображає інформацію про них на головному екрані у вікні аналізу. Залежно від можливостей конкретного продукту, подана інформація може бути додатково проаналізована та відфільтрована.

Аналіз декодованих пакетів є основним завданням будь-якого аналізатора мережевих протоколів. Аналізатор упорядковує записані пакети за рівнями та протоколами. Найкращі аналізатори пакетів можуть ідентифікувати протокол за його найбільш виразним рівнем – верхнім – і відображати інформацію, яку він перехопив. Цей тип інформації зазвичай відображається у другій області вікна аналізатора. Наприклад, будь-який аналізатор протоколів може виявити TCP-трафік. Хороший аналізатор виявить, що цей трафік надходить із сервера Microsoft Exchange Server, що працює на віддаленому виклику процедур (RPC), і відобразить текст електронного листа. Більшість аналізаторів протоколів розпізнають понад 300 різних протоколів і можуть описувати та декодувати їх за іменами. Чим більше аналізатор здатний декодувати інформацію та відображати її на екрані, тим менше йому потрібно декодувати її вручну.

1.3.2 Мережеві аналізатори

Мережеві аналізатори є еталонними вимірювальними приладами для діагностики та сертифікації кабелів та кабельних систем. Вони можуть вимірювати всі електричні параметри кабельних систем з високою точністю, а також працювати на більш високих рівнях стека протоколів. Аналізатори мережі генерують синусоїдальні сигнали в широкому діапазоні частот, завдяки чому можна виміряти амплітудно-частотну характеристику, а також поперечне наведення, ослаблення та загальне затухання приймаючої пари. Мережевий аналізатор – це великий лабораторний пристрій, яким важко користуватися.

Мережевий аналізатор прослуховує пакети на певному фізичному сегменті мережі. Це дозволяє аналізувати трафік для конкретних моделей, усувати неполадки та виявляти підозрілу активність. Система виявлення вторгнень у мережу – це вдосконалений аналізатор, який порівнює кожен пакет у мережі з базою даних відомих зловмисних шаблонів трафіку.

Мережева статистика. Основні статистичні показники: коефіцієнт використання сегмента, рівень колізій, рівень помилок та рівень широкомовного трафіку. Перевищення цих показників на певні пороги в основному вказує на проблеми в сегменті мережі.

Статистика помилкових кадрів. Дозволяє відстежувати всі помилкові типи кадрів для даної технології. Наприклад, технологія Ethernet характеризується такими типами помилкових кадрів:

1. Короткі кадри. Це кадри, які коротші за дозволену довжину, тобто менше 64 байт. Іноді цей тип кадру поділяють на два класи: лише короткі кадри, які мають правильну контрольну суму, і надто короткі, які не мають правильної контрольної суми. Найбільш вірогідними причинами скорочення кадрів є несправні мережеві карти та їх драйвери.

2. Розширені кадри. Це кадри, які перевищують допустиме значення 1518 байт із хорошою чи поганою контрольною сумою. Розтягнуті кадри є результатом тривалої передачі, яка виникає через несправності мережевого адаптера.

3. Кадри нормального розміру, але з неправильною контрольною сумою і кадри з помилкою вирівнювання межі байта. Кадри з неправильною контрольною сумою є результатом багатьох причин: погані адаптери, перешкоди кабелю, погані контакти, погані ітераційні порти, мости, комутатори та маршрутизатори.

4. Привиди – це результат електромагнітного наведення на кабелі. Мережеві адаптери сприймають їх як кадри, які не мають нормального початку кадру - 10101011. Такі кадри мають довжину більше 72 байт, інакше вони класифікуються як видалені колізії.

Знання процентного розподілу загальної кількості поганих кадрів на

основі їх типу може допомогти адміністратору дізнатись багато нового про можливі причини мережевих проблем. Навіть невеликий відсоток поганих кадрів може значно зменшити корисну пропускну здатність мережі, якщо протоколи працюють з тривалими таймаутами сигналізації під час оновлення спотворених кадрів. У нормально функціонуючій мережі відсоток поганих кадрів не повинен перевищувати 0,01%, тобто не більше 1 поганого кадру на 10000.

Статистика колізій. Цей набір характеристик надає інформацію про кількість і тип колізій, що спостерігаються на сегменті мережі, і дозволяє визначити наявність та місце проблеми. Аналізатори протоколів, як правило, не можуть надати точну картину розподілу загальної кількості зіткнень на основі їх окремих типів, тоді як знання переважаючого типу зіткнень може допомогти зрозуміти причину низької продуктивності мережі.

Розподіл використовуваних мережевих протоколів. Ця статистична група стосується протоколів мережевого рівня. На дисплеї відображається список основних протоколів у відрегульованому порядку відносно відсотка кадрів, що містять пакети цього протоколу, від загальної кількості кадрів у мережі.

Основні відправники. Цю функцію можна використовувати для моніторингу найбільш активних вузлів передачі в локальній мережі. Пристрій можна налаштувати на фільтрацію за однією адресою та пошук списку основних передавачів кадру для цієї станції. Дані відображаються на дисплеї у вигляді графіки разом зі списком основних відправників кадрів.

Основні одержувачі. Ця функція дозволяє контролювати найбільш активні приймачі в мережі. Інформація відображається у форматі, подібному вище.

Основні генератори широкомовного трафіку. Функція виявляє мережеві станції, які генерують більше кадрів з широкомовними та груповими адресами, ніж інші.

Генерація трафіку. Пристрій може генерувати трафік для перевірки роботи мережі з великим навантаженням. Потік даних може генеруватися паралельно з активованими функціями: статистика мережі, статистика кадрів

помилок та статистика колізій.

Користувач може вказати такі параметри генерованого трафіку, як інтенсивність та розмір кадру. Пристрій може автоматично створювати заголовки пакетів IP та IPX для тестування мостів та маршрутизаторів. Оператору потрібно лише ввести адреси джерела та пункту призначення.

Під час тесту користувач може використовувати клавіші курсору для збільшення розміру та частоти рухомих кадрів. Це особливо корисно, коли ви досліджуєте причину проблем із продуктивністю мережі та станів помилок.

Функції аналізу протоколів. Як правило, портативні багатофункціональні інструменти підтримують лише декодування та синтаксичний аналіз ключових протоколів локальної мережі, таких як пакетні протоколи TCP/IP, Novell NetWare, NetBIOS та Banyan VINES.

Деякі багатофункціональні пристрої не можуть декодувати захоплені пакети, наприклад в аналізаторах протоколів замість цього збирається статистика найважливіших пакетів, що вказують на проблеми в мережах. Наприклад, при аналізі протоколів стеку TCP/IP реєструється статистика пакетів ICMP, яку маршрутизатори використовують для інформування кінцевих вузлів про виникнення різних типів помилок. Щоб вручну перевірити наявність мережевих вузлів, пристрої підтримують утиліту IP Ping, а також утиліти NetWare Ping та NetBIOS Ping.

1.4 Висновки

Корпоративні комп’ютерні мережі стали обов’язковим складовим елементом інфраструктури сучасних підприємств та організацій. Без них забезпечення ефективного функціонування технологічних процесів є неможливим. Величезних збитків підприємству можуть завдати відмови і збої в роботі мереж, а тимчасові затримки передачі інформації, або навіть її втрати, можуть не лише порушити важливі технологічні процеси, а й призвести до втрати клієнтів.

Вимоги до комп’ютерних мереж постійно зростають з появою нових більш ємних додатків і компонентів. Аби задовольняти дані вимоги, сучасні

комп’ютерні мережі отримують все складнішу фізичну і логічну топологію та організацію. Концепція взаємодії відкритих систем дозволяє різним мережним компонентам і додаткам різних виробників взаємодіяти один з одним.

Системи моніторингу та управління мережею стають необхідним компонентом у контексті забезпечення мережевої безпеки. Дані системи забезпечують ефективне функціонування комп'ютерних мереж, збереження постійної мережевої готовності і високої надійності.

Мережеві аномалії можуть вплинути на потоки трафіку, призвести до відмов, перевантажень, змін конфігурації. Тому ефективне та своєчасне їх виявлення є основним завданням моніторингу мережевого трафіку.

Тому питання захисту корпоративних мереж є актуальним в умовах ринкової конкуренції, збільшення мережевих загроз та впливу третіх осіб на діяльність компаній. Необхідні рішення, аби забезпечити надійний захист даних, що циркулюють в мережі, недопущення її втрати або витоку, адже це може призвести до негативних технічних та фінансових наслідків.

2 МЕТОДИ І ЗАСОБИ ДОСЛІДЖЕННЯ ТА АНАЛІЗУ СТАНУ МЕРЕЖ

2.1 Методи та моделі дослідження мережевого трафіку

Мережевий трафік – це одиниця обсягу інформації, яка передається через Інтернет протягом певного періоду часу. Крім того, поняття "мережевий трафік" іноді використовується для опису руху потоків даних між різними веб-ресурсами з урахуванням їх географічного розташування та інших конкретних параметрів.

Основною одиницею вимірювання мережевого трафіку є біт, який в секунду визначає обсяг переданих даних. В даний час популярними одиницями обсягу є один кілобіт, один мегабіт і один гігабіт. Для передачі мережевого трафіку можуть використовуватися як дротові, так і бездротові (мобільні) технології.

Сучасні мобільні технології дозволяють обмін даними зі швидкістю приблизно 0,1 мегабіт за секунду (GPRS), до 7,2 мегабіта в секунду (стандарт 3G) і до 1000 мегабіт в секунду, залежно від використовуваного стандарту зв'язку. Друге місце в останньому поколінні мереж LTE (4G).

Крім того, швидкість трафіку по волоконно-оптичних лініях перевищує сто двадцять гігабіт в секунду, що дозволяє сучасним комп’ютерам одночасно виконувати велику кількість задач в мережі.

Трафік поділяється на такі види:

– вхідний (інформація, що надходить в мережу);

– вихідний (інформація, що надходить з мережі);

– внутрішній (в межах певної мережі, найчастіше локальної);

– зовнішній (за межами певної мережі, найчастіше - інтернет-трафік).

2.1.1 Способи аналізу мережевого трафіку

Аналіз мережевого трафіку можна виконати двома способами:

– аналіз трафіку в реальному часі (під час роботи);

– ретроспективний аналіз мережевого трафіку.

Ретроспективний аналіз трафіку передбачає, що весь або деякий трафік спочатку записується на диск, а потім аналізується.

Перехоплюючи мережевий трафік, можливо дізнатися, що відбувається з додатками, користувачами та IT-інфраструктурою, а для визначення часу, коли відбулась та чи інша подія або помилка, виконується запис метричних значень у базу даних. Цим займається переважна більшість систем спостереження. Показники та оцінки можуть допомогти скласти уявлення про те, що сталося в будь-який момент часу.

Дослідження різних типів мережевого трафіку за останні півтора десятиліття показали, що мережевий трафік є самоподібним або фрактальним [9-24]. «Самоподібність» – це властивість процесу збереження своєї поведінки та зовнішніх ознак при розгляді в різних масштабах. Звідси випливає, що методи моделювання та розрахунку використовуваних мережевих систем, які базуються на використанні пуассонівських потоків, не дають повного і точного уявлення про те, що відбувається в мережі.

Крім того, самоподібний трафік має особливу структуру, яка зберігається при багаторазовому масштабуванню. При реалізації зазвичай існує певна кількість викидів при відносно низькому середньому рівні трафіку. Це явище погіршує характеристики (збільшує втрати, затримки пакетів), коли самоподібний трафік проходить через вузли мережі. На практиці це виражається в тому, що пакети не надходять окремо на вузол з великою швидкістю у своєму русі, а наборами, що може призвести до їх втрати через обмежений буфер, розрахований за класичними методами.

2.1.2 Моделі мережевого трафіку

Моделі мережевого трафіку можна використовувати для вирішення гіпотетичних проблем, тоді як вимірювання трафіка відображають лише поточну ситуації. З точки зору ймовірності, відстеження трафіку є реалізацією випадковогопроцесу, тоді як модель трафіку – випадковий процес. Тому моделі руху універсальні. Відстеження трафіку надає інформацію про певне джерело трафіку, але модель трафіку надає інформацію про всі джерела цього типу

трафіку.

Методи концептуального моделювання мережевого трафіку можна концептуально розділити на два класи: аналітичні та імітаційні.

Аналітична модель – це ряд математичних виразів, які формально описують змодельований об’єкт або процес. Такі моделі придатні для теоретичних досліджень. Однак для більшості джерел побудова відповідної аналітичної моделі є надзвичайно складним процесом.

Імітаційна модель – це сукупність алгоритмів, що генерують певну послідовність, властивості якої близькі до реальної послідовності (експериментально вилучені з існуючого об’єкта). Таким чином, ця послідовність може бути, наприклад, мережевим трафіком. Використання імітаційних моделей часто є кращим та зручнішим, ніж використання аналітичних моделей. У той же час імітаційні моделі, як правило, мають вузьку спеціалізацію, і застосування таких моделей вимагає значної роботи для адаптації моделі до нових умов застосування.

Можливі також комбіновані моделі, що поєднують аналітичну та алгоритмічну частини [13].

На сьогодні розроблено багато моделей для імітації фрактального трафіку. Аналіз публікацій про самоподібне моделювання трафіку дозволяє виділити наступні

моделі:

– фрактальний броунівський рух (Fractional Brown Motion – FBM);

– фрактальний гаусівський шум (Fractional Gaussian Noise – FGN) [8,9];

– хаотичні відображення (Chaotic Map – CMAP);

– моделі на основі техніки «динамічного моделювання Маркова» (Dynamic Markov Modelling – DMM) [10,11];

– моделі з використанням нечіткої логіки;

– нейромережеві моделі;

– авторегресивні моделі (Autoregressive Models – AR). Як різновиди таких моделей використовуються моделі ARMA (процес змінного середнього), ARIMA (інтегральний процес змінного середнього) і FARIMA (фрактальний

інтегральний процес змінного середнього);

– фрактальні точкові процеси (Fractal Point Process – FPP);

– ON/OFF – моделі;

– фрактальний рух Леві (Fractional Levi Motion – FLM);

– мультифрактальні моделі (Multifractional – MF);

– вейвлет моделі (Wavelet Models);

– моделі на основі класичних систем масового обслуговування.

Моделі, що використовують нечітку логіку. Побудова нечітких моделей, як правило, базується на конфігурації функцій приналежності відповідно до параметрів нечітких наборів, що використовуються в правилах, на вагах правил та конфігурації операцій. У роботі [14] пропонується використання нечіткої моделі ряду нечітких тенденцій, за допомогою якої можна змоделювати та ефективно прогнозувати функціонування складної технічної системи.

Моделі нейронних мереж. Ці моделі дозволяють вирішити проблему апроксимації функцій різних змінних у навчальній вибірці, розглядаючи часовий ряд у багатовимірному просторі.

Авторегресивні моделі. Часто використовуються для моделювання та прогнозування через властивості довготривалої пам'яті самоподібних процесів. У цих моделях поточне значення сформованого значення обчислюється як зважена сума N попередніх вибірок плюс випадкова величина. Як різноманітність таких моделей використовуються моделі:

– ARMA (змінний середній процес);

– ARIMA (інтегрований змінний середній процес);

– FARIMA (інтегральний фрактальний процес змінного середнього).

До переваг останнього можна віднести можливість гнучкого контролю кореляційної структури (короткострокові та довгострокові залежності, довільний розподіл).

Практично всі ці моделі підходять для моделювання самоподібного трафіку даних у корпоративних мережах з комутацією пакетів. Усі моделі мають високоякісні властивості моделювання, такі як довгострокова залежність, масштабованість, стаціонарність тощо. Однак сучасні дослідження

реалізованих експериментально реалізацій трафіку показують, що властивості трафіку можуть сильно варіюватися і залежати від великої кількості реальних параметрів та налаштувань мережі.

Крім того, були виявлені такі характеристики трафіку, як існування короткочасних залежностей, нестаціонарність та мультифрактальність.

Типовим недоліком моделей мережевого трафіку, що використовуються в даний час, є їхня орієнтація на певний тип трафіку чи мережі та відсутність універсальності, хоча деякі автори підтверджують універсальність розроблених моделей. Крім того, їх практичне застосування призводить до великої кількості досліджень, необхідних для адаптації (навчання) моделі до параметрів конфігурації мережі або параметрів трафіку. Все це дуже ускладнює побудову універсальної моделі, оскільки різноманітність джерел та конфігурацій мережі впливає на її роботу.

Слід зазначити, що прості моделі, такі як FBM, FGN, FPP, FLM, не завжди можуть адекватно описувати реальний трафік, оскільки реальний трафік зазвичай не є суто подібним до себе.

Адекватність фактичного опису трафіку досягається шляхом ускладнення моделей, об'єднання декількох моделей та введення додаткових параметрів.

Звичайно, більш складні моделі вимагають більшої обчислювальної потужності або більше часу для реалізації генерації трафіку. Це не проблема при проведенні індивідуальних експериментів та досліджень, коли час для генерації чергового зворотного відліку руху або всієї реалізації не обмежується. Однак, як тільки виникає проблема з використанням моделі для прогнозування потоку даних для подальшого оптимального управління мережевими ресурсами, фактор складності моделі в реальному часі для даної обчислювальної потужності мережевих вузлів встановлює суворі обмеження на агентів управління.

Прогнози ринку сучасних послуг та реальні статистичні дані операторів вказують на значні відмінності в деяких випадках. На відміну від телефонії, прогностичні оцінки трафіку даних дуже ненадійні. Це свідчить про недостатній розвиток теорії (самоподібного) передбачення мультисервісного

трафіку. З іншого боку, більша частина обчислювальної роботи мережі базується на знанні параметрів трафіку. Тому одним із найактуальніших завдань на сучасному етапі розвитку NGN є розробка нових методів або вдосконалення існуючих методів моделювання та прогнозування трафіку NGN (Next Generation Network).

2.2 Аналіз підходів до вирішення задачі моніторингу трафіку мережевих комунікацій та обробка його результатів

Важко переоцінити роль комп'ютерних мереж у сучасному світі. Розвиток цієї галузі розвивається надзвичайно швидко, намагаючись стримати постійно зростаючий попит на швидке та якісне підключення до глобальної мережі Інтернет. З цієї причини постає необхідність розробити спеціальне програмне забезпечення (sniffers), яке спростить роботу системних адміністраторів при налагодженні мереж і дозволить менш кваліфікованим фахівцям у цій галузі розпочати цей вид роботи.

Нюхачі – це програми, які перехоплюють весь мережевий трафік. Вони корисні для діагностики мережі. Сніфери перемикають мережеву карту в режим PROMISC, тобто отримують всі пакети, що проходять через них [25]. Сніфери можуть перехоплювати всі пакети, а також можуть фільтрувати окремі пакети при відповідних налаштуваннях.

Основним принципом будь-якої мережі є семирівнева модель OSI. Модель OSI, яку іноді називають стеком OSI, являє собою 7-рівневу ієрархію мережі, розроблену Міжнародною організацією стандартизації (ISO). Ця модель по суті містить 2 різні моделі:

– горизонтальна модель на основі протоколів, яка забезпечує механізм взаємодії програм та процесів на різних машинах;

– вертикальна модель на основі послуг, що надаються сусідніми рівнями один одному на одній машині.

У горизонтальній моделі обидві програми потребують спільного протоколу для обміну даними. У сусідніх вертикальних шарах вони обмінюються даними через інтерфейси [26]. На рис. 2.1 показана загальна

схема моделі.

Рисунок 2.1 – Модель OSI

Фізичний рівень (physical layer) – найнижчий рівень, безпосередньо здійснює передачу потоку даних. Протоколи: Bluetooth, IRDA (інфрачервона зв'язок), мідні дроти (вита пара, телефонна лінія), Wi-Fi, і т.д.

Канальний рівень (data link layer) – взаємодія мереж на фізичному рівні. Пристрої канального рівня – комутатори, концентратори і т.п. Типовими представниками на цьому рівні є PPP (Point-to-Point) – це протокол для зв'язку двох комп'ютерів безпосередньо, FDDI (Fiber Distributed Data Interface) – стандарт передає дані на відстань до 200 кілометрів.

Мережевий рівень (network layer) – цей рівень визначає шлях, по якому дані будуть передані. Третій рівень моделі OSI, відповідно на цьому рівні працюють маршрутизатори і використовують протоколи для маршрутизації пакетів (RIP, EIGRP, OSPF).

Транспортний рівень (transport layer) – цей рівень забезпечує надійність передачі даних від відправника до одержувача. На цьому рівні головними є два протоколи: UDP і TCP. UDP протокол (User Datagram Protocol) передає дані без встановлення з'єднання, не підтверджує доставку даних і не робить повтори.

TCP протокол (Transmission Control Protocol), який перед передачею встановлює з'єднання, підтверджує доставку даних, при необхідності робить повтор, гарантує цілісність і правильну послідовність даних при завантаженні.

Сеансовий рівень або рівень сесій (session layer) – організовує сеанс зв'язку між комп'ютерами. Рівень управляє створенням та завершенням сеансу, обміном інформацією, синхронізацією завдань, визначенням права на передачу даних і підтримкою сеансу в періоди не активності додатків.

Представницький рівень або рівень представлення даних (presentation layer) – він перетворює дані у відповідний формат. Цей рівень відповідає за перетворення протоколів та кодування / декодування даних. Запити програм, отримані від прикладного рівня, перетворюються у формат для передачі через мережу, а дані, отримані з мережі, перетворюються у формат, зрозумілий програмам.

Прикладний рівень або рівень додатків (application layer) – це найвищий рівень моделі. Він забезпечує зв'язок призначених для користувача додатків з мережею. Це перегляд веб-сторінок (HTTP), передача і прийом пошти (SMTP, POP3), прийом і отримання файлів (FTP, TFTP), віддалений доступ (Telnet) і т.д.

Багато вчених займаються дослідженнями мережевого трафіку, і спектр дослідницьких областей дуже широкий: це вивчення кореляцій між сигналами [28, 29], заходи щодо вибору параметрів при створенні профілів захисту інформаційних ресурсів [30-32], захисту інформаційних ресурсів при передачі даних через мережі. З урахуванням усіх цих проблем проблема аналізу трафіку мережевого зв'язку залишається актуальною з можливістю аналізу статистичних даних, які система отримує в процесі моніторингу.

Підхід до моніторингу трафіку мережевих комунікацій. Після створення запису системою автоматизації обліку та аналізу трафіку мережевих комунікацій, вона пересилає пакет далі в мережу. Запис проходження пакету повинен містити таку інформацію [28]:

– час запису відносно початку прослуховування;

– IP-адреса відправника пакета;

– номер порту відправника пакета;

– IP-адреса одержувача пакету;

– номер порту одержувача пакета;

– кількість переданих інформаційних байтів;

– тип транспортного протоколу.

Система також повинна дозволити користувачеві вибрати один із існуючих мережевих інтерфейсів у випадку декількох мережевих адаптерів. Кожен з них повинен бути описаний. Крім того, користувач повинен мати можливість призупинити та продовжувати облік пакетів з мережі.

Існує потреба в розробці механізму, за допомогою можна створювати графіки з аналітичною інформацією про стан мережі, коли прослуховування мережі призупинено або повністю зупинено. Система не повинна суттєво впливати на продуктивність мережевої карти і повинна споживати багато процесорного часу.

Основним завданням має бути аналіз та графічне відображення результатів прослуховування з мережевої карти. Основні типи графіків, які потрібно створити:

– кількість пакетів, які були надіслані від вказаної IP-адреси в різний час;

– кількість пакетів, які були надіслані на певну IP-адресу в різний час;

– кількість TCP-пакетів, переданих від вказаної IP-адреси протягом різних періодів часу;

– кількість пакетів UDP, переданих від вказаної IP-адреси протягом різних періодів часу;

– кількість TCP-пакетів, які передавались на певну IP-адресу протягом різних періодів часу;

– кількість пакетів UDP, які передавались на певну IP-адресу протягом різних періодів часу.

Метою системи є відстеження мережевого трафіку, що проходить через певний мережевий інтерфейс. Трафік даних розглядається на основі певних критеріїв, визначених користувачем. Підсистема фільтру мережевого трафіку фактично відхиляє мережеві пакети (кадри), які не цікавлять користувача.

Подальший контроль передається підсистемі зберігання результатів. Тут зберігаються пакети, які відповідають критеріям, встановленим користувачем, перед моніторингом мережевого трафіку. За необхідності ця підсистема може передавати збережені дані до підсистеми обробки результатів, яка аналізує результати моніторингу та відображає графічне зображення свого аналізу. Зв'язок між цими підсистемами відбувається через інтерфейс, який визначає достатню функціональність для виконання завдань, призначених цьому модулю (підсистемі).

Існує кілька аспектів роботи цієї підсистеми. Середовище виконання. Середовище продуктивності. Там, де система працює, повинні бути настільні комп'ютери, здатні до мережевого зв'язку.

Аспекти аналізу трафіку:

– вибір параметрів фільтра. З метою підвищення зручності користування системою користувачеві має надаватися можливість вказувати додаткові параметри фільтра;

– створення аналітичних графіків. Система має формувати діаграми, що відображають навантаження на мережу, а також окрему частку навантаження, яку мережа отримує від однієї точки мережі.

На рис. 2.2 показана схема перетворення даних у системі. Вхідними даними для системи є всі доступні мережеві інтерфейси, які відображаються користувачеві для вибору одного та для налаштування відповідного фільтра для перехоплення мережевих пакетів певного типу.

Ці дані потрібні системі для повернення таблиці з відфільтрованими пакетами, яка, в свою чергу, може бути використана як вхід для створення різних типів графіків. Після отримання сигналу для відстеження та, при необхідності, подальшого уточнення даних користувача, система має створювати діаграму, що відображаєрезультати аналізу відфільтрованого трафіку.

Рисунок 2.2 – Схема перетворення даних в сніфері

Для зручності обслуговування, а також гнучкості системи доцільно забезпечити слабкий зв’язок між компонентами та максимально розрізнити їх. З цих причин систему можна розділити на підсистеми [29]:

– підсистема для перехоплення мережевих пакетів: Дозволяє прослуховувати мережевий інтерфейс і передає дані для обробки наступним підсистемам;

– підсистема фільтрації пакетів перенаправляє пакет до підсистеми зберігання відфільтрованого трафіку залежно від того, чи відповідає він визначеним користувачем критеріям;

– підсистема зберігання відфільтрованого трафіку зберігає дані, отримані користувачем в результаті фільтрації трафіку.

– підсистема обробки інформації, поділена на два компоненти:

1) компонента аналізу отриманих результатів робить висновки відповідно до результатів, отриманих після фільтрування;

2) графічний компонент відображення займається створенням діаграм, що

ілюструють висновки про роботу мережі.

На рис. 2.3 показана загальна структура системи.

Рисунок 2.3 – Структура системи автоматизації обліку та аналізу трафіку мережевих комунікацій

На рис. 2.4 зображена діаграма, що ілюструє варіанти використання системи.

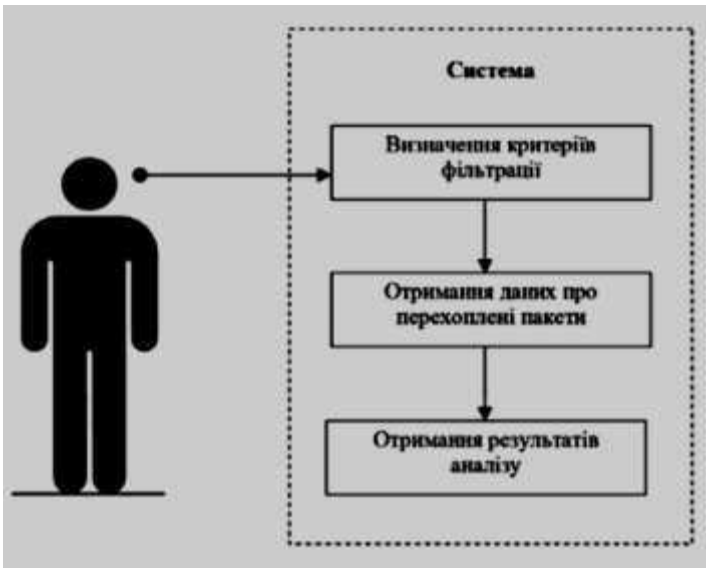


Рисунок 2.4 – Діаграма варіантів використання мережевого аналізатора

На сьогодні існує багато подібних систем перехоплення та аналізу

трафіку, серед них деякі варто розглянути детальніше.

Програма Wireshark використовується для захоплення, реєстрації та аналізу мережевого трафіку, тобто вона є сніфером та аналізатором. За допомогою Wireshark можна виконувати наступні завдання:

– захоплення мережевого трафіку на комп'ютері та обмін захопленими пакетами;

– відображати вміст пакету в структурованому форматі та по суті;

– відбір мережевих пакетів відповідно до гнучких критеріїв;

– аналіз окремих пакетів, сеансів та статистики для декількох пакетів;

– відновлення потоків даних у наборах пакетів.

Ядром Wireshark є бібліотека libpcap або її версія для операційної системи Windows WinPCap. Ці бібліотеки, Wireshark та відповідні програми розробляються у тісній співпраці. Всі вони безкоштовні та кроссплатформенні, код відкритий.

Wireshark перехоплює вхідні пакети, які драйвер надсилає операційній системі, і вихідні пакети, які операційна система надсилає драйверу. Якщо мережева карта перетворює або відкидає деякі пакети, це не враховується у Wireshark.

Tcpdump – це стандартна утиліта для аналізу мережевого трафіку в дистрибутивах Linux. Tcpdump зарекомендував себе як дуже ефективний та надійний інструмент. В результаті багато аналогів в даний час використовують формат tcpdump – libcap як основний формат файлу для читання / запису результатів трасування трафіку.

Коли tcpdump запускається, він автоматично здійснює пошук мережевих інтерфейсів і використовує перший знайдений для аналізу. Тому потрібно звернути увагу на вихідні дані, щоб переконатися, що правильний інтерфейс проаналізований. Якщо ні, то легко вручну налаштувати потрібний інтерфейс. Утиліта може бути дуже корисною, коли служба DNS не працює або працює надто повільно, тобто коли існує ризик втрати пакетів, перш ніж tcpdump зможе їх проаналізувати.

Проект Ettercap – це безкоштовний інструмент захисту мережі з

відкритим кодом для атак "людина посередині" на локальну мережу. Він може бути використаний для аналізу журналів комп'ютерної мережі та перевірки безпеки. Він працює на різних UNIX-подібних операційних системах, включаючи Linux, Mac OS X, BSD і Solaris, а також Microsoft Windows. Може перехоплювати трафік на сегменті мережі, захоплювати паролі та активно перехоплювати протоколи.

Основними особливостями Ettercap є:

– підтримка SSH1: Ettercap – це перша програма, яка може виявити повнодуплексні SSH-з'єднання;

– підтримка SSL: можна прослуховувати захищені дані SSL;

– вставка символів у встановлене з’єднання, щоб підтримувати зв’язок активним;

– фільтрування / відкидання пакетів.

– підтримка плагінів.

– пасивне сканування локальної мережі (без розсилки пакетів) та збір детальної інформації про хости в локальній мережі;

– роз'єднання: у списку з'єднань можливо розірвати певне з'єднання.

2.3 Визначення систем виявлення вторгнень

Система виявлення вторгнень (IDS) – програмне чи апаратне забезпечення, що використовується для виявлення несанкціонованого доступу або несанкціонованого управління комп’ютерною системою чи мережею, переважно через Інтернет.

Інформація про діяльність зловмисного програмного забезпечення або порушення стандартної роботи централізується системою SIEM (англ. Security information and event management). Система SIEM обробляє дані з багатьох джерел і використовує методи фільтрації загроз, щоб розрізнити несанкціоновану активність від хибних спрацьовувань. Про виявлені загрози повідомляється адміністратор або операційний центр безпеки.

Деякі системи виявлення вторгнень (СВВ) можуть виявити початок мережевої атаки, інші можуть виявити раніше невідомі атаки. Такі системи

відомі як системи запобігання вторгненням (IPS). Приклад IPS в мережі показано на рис. 2.5.

IPS не обмежується повідомленнями, вона також вживає різні заходи для блокування атаки (наприклад, вихід із системи або запуск сценарію, вказаного адміністратором). На практиці програмно-апаратні рішення дуже часто поєднують функціональність двох типів систем. Їх асоціації називаються IDPS (IDS і IPS).

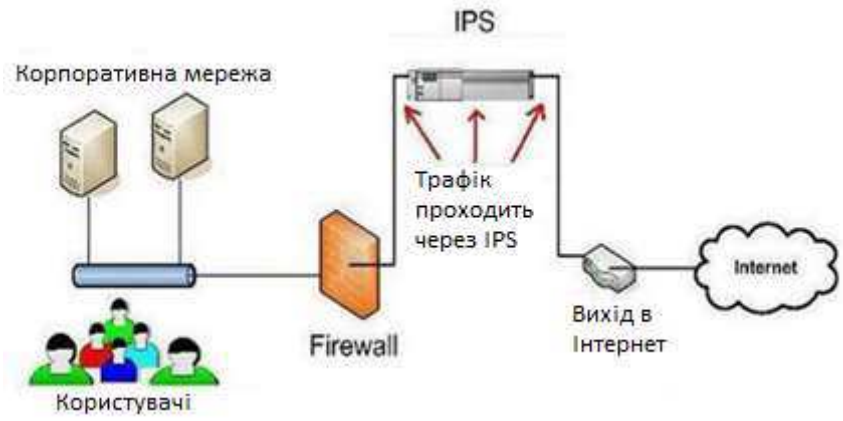


Рисунок 2.5 – Система запобігання вторгнень

Незважаючи на те, що існує кілька типів IDS, за розмірами від окремих комп’ютерів до великих мереж, найпоширенішими класифікаціями є NIDS (системи виявлення вторгнень у мережу) та системи виявлення вторгнень на основі хоста (HIDS). Прикладом HIDS може бути система, яка відстежує важливі файли операційної системи, а прикладом NIDS може бути система, яка аналізує вхідний мережевий трафік. IDS також можна класифікувати за методами виявлення загроз: найбільш відомими є виявлення на основі сигнатур (виявлення неправильних шаблонів як шкідливого програмного забезпечення) та виявлення аномалій (виявлення відхилень від "правильного" трафіку, часто за допомогою машинного навчання).

Розглянемо класичну класифікацію СВВ:

– системи рівня мережі, куди маршрутизатор перенаправляє трафік даних;

– системи рівня хоста, які розпізнають зміни на одному комп'ютері,

наприклад аналіз журналів або мережевої діяльності;

– системи оцінки вразливостей системи.

На основі отриманих даних СВВ повинна визначити, чи існує загроза мережевій безпеці. Основні завдання СВВ:

1) збір даних;

2) інтерпретація отриманих даних;

3) презентація результату.

Відповідно, всі системи можливо позиціонувати за значеннями таких ознак:

– тип зібраних даних;

– методи збору даних;

– метод інтерпретації даних;

– метод подання результату.

Несистемні характеристики можна розглядати як тип реакції на результат:

– інформативний;

– активний.

У першому випадку зацікавлені сторони інформуються. У другому – активні дії, наприклад блокування адрес зловмисника. На цій основі ці системи зазвичай штучно поділяють на IDS та IPS. Будь-які IDS можуть бути включені в IPS.

При моніторингу мережі можуть використовуватися наступні типи даних:

– дані на мережевому вузлі;

– дані рівня мережі.

Типи даних про вузол мережі – це дані, що відносяться до окремого вузла і, частково, до тих, що з ним взаємодіють. Проаналізувавши ці дані, можна виявити факт атаки на даний хост. Зазвичай зручніше збирати ці дані безпосередньо на вузлі, але це не є обов’язковим. Наприклад, мережеві сканери можуть зовні отримувати список відкритих портів на певному вузлі, не маючи можливості виконувати там код.

Цей клас містить дані наступних типів (кожен з яких містить певні

показники):

– мережева активність вузла;

– налаштування мережевого вузла;

– дані щодо файлів (списки, контрольна сума, метадані тощо);

– дані щодо процесів.

Вузлами можуть бути як робочі станції, які не передбачають їх використання в якості серверів, що надають послуги так і сервери.

Хост може бути вразливим для дослідження методів атаки (включаючи додаткове навчання нейронних мереж) та виявлення атакуючих вузлів. Можна припустити, що будь-яка взаємодія з цим вузлом є спробою атаки.

Дані про мережу – це цілісна картина взаємодії мережі. Як правило, повні дані мережі не збираються, оскільки цей процес вимагає великих ресурсів, і вважається, що зловмисник може не знаходитися в мережі або що йому необхідний зв’язок із зовнішнім світом. У цьому випадку IDS аналізує трафік, що протікає через маршрутизатор, для якого маршрутизатор має порт SPAN, з якого трафік перенаправляється на IDS. Однак не виключається можливість збору даних із вузла, на якому запущена IDS, що, в свою чергу, може забезпечити додатковий контроль.

Також можна збирати мережевий трафік на її вузлах. Однак це змушує мережевий адаптер вузла захоплювати весь трафік, який зазвичай не очікується при нормальній роботі.

Можна виділити наступні методи отримання даних у СВВ:

– активний;

– пасивний;

– змішаний (поєднання двох вищезазначених).

За допомогою пасивного виявлення система просто відстежує ситуацію. Більшість IDS використовують цей клас методів. Системи рівня хоста зазвичай також використовують цей клас методів. Наприклад, вони не намагаються видалити системний файл під користувачем і перевірити, що його було видалено, а просто оцінює відповідність прав на цей файл, шаблону у базі даних та видає попередження, якщо відповідності не досягнуто.

При активному методі помилки викликаються деякими відомими та невідомими діями (нечітка система). Далі реакція на ці дії аналізується на основі відомостей у базі. Цей клас методів характерний для сканерів на вразливість.

Можна аналізувати відповіді за допомогою бази даних (наприклад, типові відповіді на типові моделі ін'єкцій SQL) або поведінковий аналіз (реакція цілі та її відповіді на запити). Наприклад, посилка некоректно складеного IP пакета повинна привести до падіння уразливого сервера, після чого він перестане відповідати.

Можливий варіант виявлення ненормальної активності. Наприклад, якщо після відправки 777-байтового пакета ICMP із заповненням 0xDEADBEEF рівень активності мережі різко зростає, а потім зменшується, це аномалія (нормальна ситуація: рівень активності мережі не змінюється).

Переваги активного пошуку вразливості:

– профілактичне виявлення зловмисників;

– перевірка мережі аналогічно атакуючому, що підвищує шанси виявити вразливості.

Недоліки активного пошуку:

– додаткове навантаження на мережу;

– можливість реалізації успішної атаки під час процесу сканування, наприклад DoS деяких сервісів;

– залежність від бази атак, яка з часом стає неактуальною.

Лабораторією "nsslabs" [30] визначено технічні показники, що оцінюються при тестуванні систем IPS / IDS:

– кількість пакетів, оброблених системою за секунду;

– кількість байт в секунду (середній розмір пакета);

– множина протоколів;

– кількість унікальних хостів;

– швидкість встановлення нових з'єднань;

– кількість одночасних з'єднань;

– попереджень за секунду;

– пропускна здатність при передачі TCP, HTTP-трафіку та реалістичне поєднання трафіку з різних протоколів прикладного рівня.

2.4 Аналіз сучасних систем виявлення атак і запобігання вторгненням

Останнім часом інформація, що циркулює в мережах, стала важливим ресурсом, який забезпечує безпеку бізнесу. Можливість несанкціонованого впливу на інформацію розглядається як пряма загроза інтересам компаній. Як результат, системи захисту інформації (СЗІ), особливо антивірусне програмне забезпечення та системи виявлення вторгнень стали невід'ємною частиною корпоративних мереж.

СЗІ – це складне програмне та апаратне забезпечення, яке базується на спеціальних математичних методах та моделях. Висока надійність цих систем досягається шляхом перевірки програмних кодів та перевірки методів і моделей, реалізованих в них. Підтвердження відповідності (верифікація) здійснюється з використанням математичних методів відповідно до критеріїв ефективності СЗІ, визначених на етапі специфікації. Аналіз цих критеріїв з використанням ряду показників дозволяє оцінити якість реалізації окремих елементів та всієї системи.

Слід зазначити, що атаки на ККМ з кожним роком стають все більш досконалими, все більшими та інтенсивнішими. Актуальною є проблема розробки та вдосконалення систем виявлення вторгнень у ККМ, основним завданням яких є виявлення мережевих атак, спроб несанкціонованого доступу та використання мережевих ресурсів. Постійний швидкий розвиток методів та методів руйнівного впливу програмного забезпечення на ККМ вимагає порівняльного аналізу існуючих систем виявлення атак та запобігання вторгненням з метою визначення найбільш ефективних механізмів захисту інформаційних активів.

Насичення ринку інформаційних технологій цими системами робить необхідним для користувача обрати оптимальну систему виявлення атак та запобігання вторгненням. Однак реалізувати це можливо лише на основі аналізу сучасного стану та перспектив їх найближчого розвитку. В даний час

існує велика кількість систем, позиціонованих як IDS або IPS.

На практиці застосовуються різні комбінації атак. Наприклад, зловмисник використовує мережеві сканери для виявлення топології мережі та сканери вразливості для виявлення вразливих хостів. Знайдені на хості уразливості зловмисник використовує для віддаленого виконання коду. Тому СВВ має впровадити механізми виявлення різних типів атак.

Виявлення атаки – процес ідентифікації та реагування на підозрілі дії, спрямовані на комп'ютерні або мережеві ресурси [32], тоді як атака відноситься до будь-якої дії зловмисника, що призводить до загрози через вразливості в комп'ютерній системі [33, 34].

Існує кілька методів класифікації атак. Наприклад, їх поділяють на пасивні та активні, зовнішні та внутрішні, навмисні та ненавмисні. Типовий перелік типів атак на ККМ можна навести наступним чином [34, 35]:

– віддалене проникнення;

– локальне проникнення;

– віддалена відмова в обслуговуванні;

– локальна відмова в обслуговуванні;

– мережеві сканери;

– сканери вразливостей;

– зламники паролів;

– аналізатори протоколів (сніфери);

– збір інформації про характеристики ККМ;

– несанкціонований доступ до інформаційних ресурсів системи;

– підозріла активність;

– системні атаки.

Стандартні засоби захисту інформаційних ресурсів системи (брандмауери, сервери автентифікації, системи обмеження доступу тощо) використовують у своїй роботі одну або дві характеристики типів атак, тоді як спеціалізовані СВВ реалізують майже весь список для виявлення несанкціонованих дій.

Аналіз концептуальних основ побудови сучасних СВВ дозволяє

припустити, що робота будь-якої системи базується на методах визначення аномалій та зловживань. Ці методи засновані на моделях шаблонів (профілів) поведінки.

Методи виявлення аномалій використовуються для виявлення невідомих атак та втручань у ККМ на основі моделей шаблонів нормальної поведінки (ШНП) використовують статистичні методи виявлення, нейронні мережі, теорію масового обслуговування тощо. Вони використовуються для побудови моделей ШНП.

Характерним недоліком моделей ШНП, заснованих на статистичних методах виявлення, є велика кількість хибнопозитивних результатів системи, які можна віднести до помилок першого (пропуск атаки) та другого (хибне спрацювання) роду [41].

В табл. 2.1 наведено основні механізми реалізації різних видів атак [36].

Таблиця 2.1 – Основні механізми реалізації атак

№ з/п	Тип атаки	Механізм реалізації атаки
1	Віддалене проникнення	Віддалений виклик командного рядка шляхом переповнення буфера
2	Аналіз топології мережі	Передача мережних пакетів, що містять запити ECHO_REQUEST
3	Пошук уразливості	Сканування хосту
4	Відмова в обслуговуванні	Передача великої кількості мережних пакетів
5	Злам паролів	Багаторазові спроби аутентифікації в системі
6	Аналіз мережного трафіка	Перемикання мережного інтерфейсу в “режим прослуховування” і перехоплення мережного трафіка
7	Несанкціонована аутентифікація	Порушення прав доступу і незаконне використання ресурсів
8	Шкідливе ПЗ	Приховане встановлення програмних модулів, прихований запуск процесів

Можна виявити або зменшити ризик атак, знаючи характеристики несанкціонованих дій (механізмів атаки), а саме:

– наявність повторюваності деяких подій у системі;

– некоректні або суперечливі поточні процеси та команди;

– використання слабких місць;

– невідповідні параметри мережевого трафіку;

– непередбачувані атрибути;

– додаткові знання порушень.

Найважливіші механізми виявлення вторгнень, визначені для різних класів атак, перераховані в табл. 2.2 [36].

Таблиця 2.2 –Основні механізми виявлення атак

№ з/п	Механізми виявлення атаки	Клас атак, що виявляються
1	Відстеження спроб аутентифікації в системі	Зовнішні (внутрішні) мережні (локальні) активні
2	Відстеження перехоплення мережного трафіка	Зовнішні мережні активні
3	Відстеження мережного трафіка	Зовнішні мережні пасивні
4	Відстеження запуску процесів та звернень до файлової системи й реєстру	Внутрішні локальні активні

Розглянемо переваги та недоліки сучасних систем виявлення атак та запобігання вторгненням. IDS може сповістити про початок мережевої атаки, а деякі з них можуть виявити раніше невідомі атаки. IPS не обмежується сповіщеннями, але також вживає різні заходи для блокування атаки (наприклад, вихід із системи або запуск сценарію, визначеного адміністратором (спеціальна команда)). На практиці програмно-апаратні рішення часто поєднують функціональність двох типів систем, і їх поєднання іноді називають IDPS (IDS та IPS).

Система IDPS виявляє (блокує) спроби злому зловмисником електронного ресурсу та попереджає користувача. IDPS – це поєднання сніфера (модуль для перехоплення мережевого трафіку та збору інформації, який потім може бути використаний як для діагностики, так і для злому мережі), аналізатора та системи сповіщення (блокування). На рис. 2.6 показана загальна схема розміщення системи IDPS в комп’ютерній мережі.

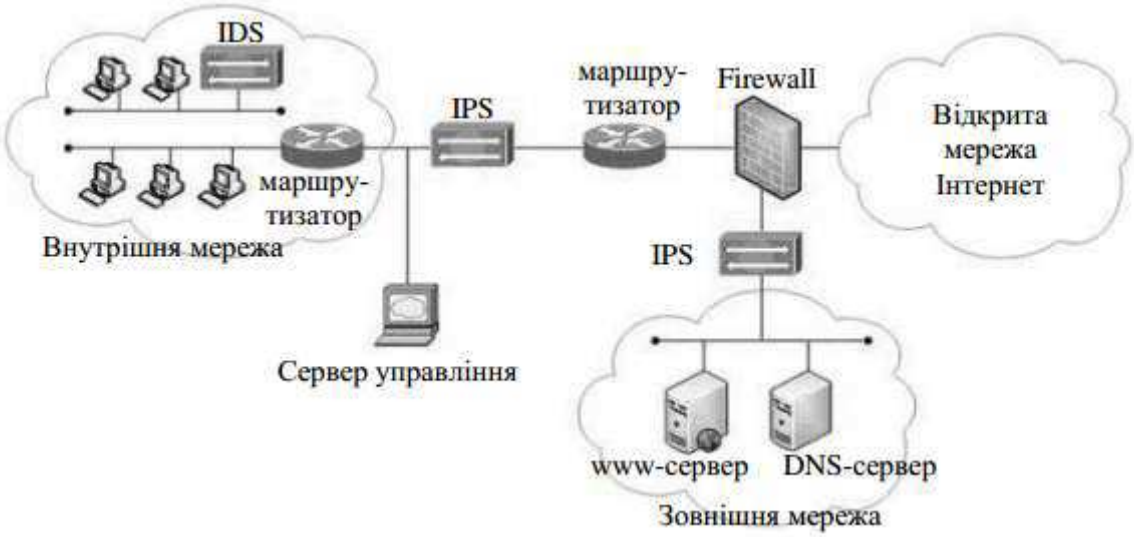


Рисунок 2.6 – Схема розміщення IDPS у комп’ютерній мережі

На рис. 2.6 детектори IDPS (датчики) розташовані у точках входу в сегменти мережі. Сегменти мережі мають як внутрішні, так і зовнішні ресурси. Датчики надсилають звіти про події на сервер моніторингу, який розташований за MME (брандмауер).

Сучасні IDPS можуть контролювати роботу мережевих пристроїв та операційних систем, виявляти несанкціоновані дії та автоматично виконувати функції, визначені адміністратором, такі як:

– повідомлення адміністратора (звукове попередження, електронна пошта, SMS);

– зміна налаштування брандмауера (блокування IP-адреси зловмисника);

– переривання зв’язку TCP, встановленого порушником;

– запуск програми (сценарій), визначену адміністратором;

– внесення інформації про атаку в журнал.

IDPS класифікується кількома способами. Тому метод відповіді розрізняє пасивний та активний IDPS. Пасивні просто реєструють факт нападу, записують дані у файл журналу та генерують попередження. Активні намагаються протидіяти атаці, наприклад, перенастроюючи MME або створюючи списки доступу для маршрутизаторів [37].

Відповідно до методу виявлення вторгнень існують системи, засновані на аналізі сигнатур та пошуку аномалій. Перші порівнюють інформацію про

трафік з базою сигнатур атак. Недоліком таких систем є неможливість реагувати на нові типи невідомих атак. Другі контролюють частоту подій або виявляють статистичні аномалії. Такі системи орієнтовані на виявлення нових типів атак, але їх недоліком є необхідність постійного навчання [37].

Найпопулярнішою класифікацією є IDPS за рівнем виявлення вторгнень. Існують мережевий та системний рівні для виявлення атак. Мережні IDPS (NIDPS) аналізують мережевий трафік для виявлення атак та інших підозрілих дій. Такі системи повинні мати доступ до всього трафіку в сегменті, мати розподілену архітектуру, мати датчики, які збирають інформацію про трафік і надсилають її на консоль управління. Датчики можуть бути програмними та апаратними. Апаратні рішення значно збільшують швидкість, але мають високу вартість. Функціональність таких датчиків майже однакова.

Системи виявлення вторгнень на рівні мережі використовують необроблені мережеві пакети як джерело даних для аналізу. Як правило, NIDPS використовує мережевий адаптер, який працює в режимі прослуховування та аналізує трафік у реальному часі, коли він проходить сегмент мережі. Механізм підтвердження атаки використовує чотири добре відомі методи виявлення сигнатури атаки:

1) узгодження трафіку даних із шаблоном (сигнатурою), виразом або байт-кодом, що ідентифікує підозрілу атаку або підозрілу дію;

2) контроль частоти подій або перевищення порогу;

3) кореляція декількох подій з низьким пріоритетом;

4) виявлення статистичних аномалій.

Якщо виявлено атаку, модуль відповіді видає відповідне повідомлення та попередження та пропонує різноманітні контрзаходи у відповідь на атаку, а також записує сеанс для подальшого аналізу та виявлення атаки.

Окремим сегментом систем виявлення вторгнень мережевого рівня є системи виявлення бездротових вторгнень – WIDS (Wireless Intrusion Detection System), які базуються на датчиках, що виконують функцію збору бездротового трафіку в режимі спостереження при його обробці. Сенсори, як правило, досить інтелектуальні пристрої, що підтримують протоколи TCP / IP і мають

розвинений інтерфейс управління.

Сучасні IDPS системного рівня використовують журнали подій для виявлення атак. Цей процес автоматизований і поєднує в собі складні методи виявлення, засновані на новітніх математичних знаннях. Як правило, IDPS системного рівня контролює систему, події та журнал безпеки або системний журнал. Якщо будь-який із цих файлів змінюється, IDPS порівнює нові записи з сигнатурами атак, щоб перевірити, чи є збіг. Коли це виявляється, система надсилає попередження адміністратору або активує інші зазначені механізми реагування.

IDPS системного рівня постійно розвиваються і поступово поєднують нові методи виявлення. Одним з них є метод перевірки контрольних сум системи ключів та виконуваних файлів через рівні проміжки часу на предмет несанкціонованих змін. Своєчасність реагування на напади безпосередньо залежить від частоти опитування.

Переваги систем виявлення вторгнень мережевого рівня:

1. Відносно низькі експлуатаційні витрати. Це пов’язано насамперед з необхідністю встановлювати датчики лише в ключових точках мережі, щоб контролювати трафік, що циркулює між кількома сегментами мережі. Системи мережевого рівня не вимагають встановлення програмного забезпечення для виявлення вторгнень на кожному окремому хості.

2. Можливість виявлення атак, які ігноруються на системному рівні. IDPS мережевого рівня сканує заголовки мережевих пакетів на підозрілі чи руйнівні дії, тоді як IDPS системного рівня не працює з заголовками пакетів і тому не може виявити певні типи атак. Наприклад, багато мережевих атак, таких як DoS та "фрагментований пакет" (teardrop), можна ідентифікувати лише аналізуючи заголовки пакетів. Крім того, IDPS дозволяє аналізувати вміст тіла даних пакета на рівні мережі для пошуку конкретних команд або синтаксису, які використовуються в конкретних атаках.

3. Великою складністю для зловмисника є видалення слідів його присутності. Мережевий рівень IDPS використовує "живий" трафік для виявлення атаки в режимі реального часу. Проаналізовані дані містять не тільки

інформацію про метод атаки, але також інформацію, яка може допомогти ідентифікувати зловмисника.

4. Здатність розпізнавати і реагувати в режимі реального часу. IDPS мережевого рівня виявляє підозрілі та зловмисні атаки в міру їх виникнення, забезпечуючи швидші сповіщення та відповіді, ніж IDPS системного рівня. Наприклад, зловмисник, що ініціює атаку мережевого рівня DoS на основі TCP, може бути зупинений IDPS мережевого рівня, який надсилає прапорець «скинути» до заголовка пакета TCP, щоб припинити підключення до атакуючого хоста, перш ніж атака заподіє шкоди хосту-жертві. IDPS системного рівня зазвичай розпізнає атаки лише після відповідного запису в журналі та реагує після цього.

5. Можливість виявлення невдалих спроб нападу або підозрілих намірів. Задопомогою мережевої IDPS, встановленої за межами MME, можливо виявити цілеспрямовані атаки на інформаційні ресурси за MME. Системна IDPS не ідентифікує відхилені атаки, які не потрапляють на хост за MME. Це призведе до втрати важливої інформації, яка може бути використана для вдосконалення політики безпеки.

6. Незалежність від операційної системи. IDPS на рівні мережі не залежать від операційної системи, встановленої в захищеній мережі. Системні IDPS вимагає встановлення певних операційних систем для нормальної роботи та отримання необхідних результатів.

Переваги систем виявлення вторгнень системного рівня:

1. Можливість підтвердити успіх або невдачу атаки. Оскільки системна IDPS використовує журнали, що містять інформацію про події, які насправді відбулися, системи цього класу можуть з великою точністю визначити, чи була атака успішною чи ні.

2. Можливість моніторингу конкретного хоста. За допомогою IDPS системного рівня можна контролювати дії користувачів, отримувати доступ до файлів, змінювати права доступу до файлів, спроби встановити нові програми та (або) отримати доступ до привілейованих служб. Наприклад, системна IDPS може контролювати всі дії користувачів щодо входу та виходу з системи та дії,

які вони вживають при підключенні до мережі. Технологія виявлення вторгнень на системному рівні також може контролювати дії, які зазвичай виконує лише адміністратор. IDPS системного рівня може контролювати зміни критичних системних файлів або виконуваних файлів. Спроби перезаписати такі файли або встановлення троянських програм можуть бути виявлені та перервані. Системи мережевого рівня іноді пропускають такий тип атак.

3. Можливість виявлення атак, які не виявляють системи мережевого рівня. IDPS системного рівня може виявляти атаки, яких не можуть інструменти мережевого рівня. Наприклад, атаки на сервер не можуть бути виявлені системами виявлення атак на рівні мережі.

4. Може використовуватися для мереж з шифруванням та комутацією. Оскільки IDPS системного рівня встановлюється на різних хостах у мережі, що захищається, це може вирішити деякі проблеми, що виникають при використанні систем мережевого рівня в комутованих та зашифрованих мережах. Комутація дозволяє управляти великими мережами, такими як декілька сегментів мережі. Як результат, може бути важко визначити найкраще місце для встановлення IDPS на рівні мережі. Виявлення на системному рівні забезпечує більш ефективні операції комутації мережі, оскільки є можливість розміщувати IDPS лише на хостах, які цього потребують. Певні типи шифрування також є проблематичними для систем, щовикористовуються для виявлення атак на рівні мережі. Залежно від того, де застосовується шифрування (канал або учасник), IDPS на рівні мережі може залишатися нечутливим до певних атак.

5. Не потрібно додаткового обладнання. Системна IDPS встановлюється в існуючій мережевій інфраструктурі з урахуванням файлових серверів, веб-серверів та інших використовуваних ресурсів.

Аналіз вищезазначених переваг IDPS мережного та системного рівнів показав, що ці системи ефективно доповнюють одна одну. Тому майбутні покоління IDPS повинні поєднувати інтегровані системи та мережеві компоненти. Синтез цих двох технологій збільшить ефективність мережевого захисту від атак та зловживань, дозволить отримати більш суворі правила

безпеки та більшу гнучкість у роботі мережевих ресурсів.

Сьогодні IDPS представлені на ринку IT-технологій значною кількістю програмних та апаратно-програмних комплексів. Прикладами таких систем є Kerio WinRoute Firewall, Snort, McAfee Entercept, ETrust Intrusion Detection, Symantec ManHunt та інші програмні продукти [39, 40]. Слід зазначити, що розробники IDPS не надають об’єктивного опису своїх переваг та недоліків, що дуже ускладнює користувачеві вибір бажаного продукту. Для вирішення цього питання в даний час розробляється єдиний стандарт для тестування IDPS. Для порівняння IDPS були запропоновані наступні показники [39]:

1. Клас виявлених атак. Цей показник визначає, які класи атак IDPS можна виявити (див. табл. 3.2). Клас атаки складається з чотирьох параметрів <L, R, A, D>, де L – положення об'єкта, що здійснює атаку (воно може бути внутрішнім або зовнішнім щодо системи, що захищається), R – атакований ресурс (ресурси розподіляються за місцем розташування (хост, мережа) та типом (користувацькі ресурси, системи управління базами даних, системні та обчислювальні ресурси), A – цілеспрямований вплив на ресурс (збір інформації) отримання прав користувача або адміністратора, порушення цілісності або ефективності ресурсу, D – ознака розподіленого характеру нападу.

2. Рівень моніторингу системи визначає, на якому рівні система збирає дані для виявлення атаки. Існують джерела хоста та системи. Усередині хоста є ядро та прикладні рівні (HIDS – спостереження на рівні операційної системи одного мережевого хоста; NIDS – спостереження на рівні мережевої взаємодії об'єктів на мережевих хостах; AIDS – спостереження на рівні окремих мережевих хост-додатків; гібридні – поєднання спостерігачів на різних рівнях). Ступінь спостережливості системи залежить від швидкості збору інформації, впливу системи на зібрану інформацію та ймовірності отримання спотвореної інформації.

3. Використаний метод виявлення вторгнень, який є ключовим показником для порівняння IDPS. Існує два класи методів: виявлення аномалій (статистичний аналіз та кластерний аналіз, нейронні та імунні мережі,

експертні системи, біометрія) та виявлення зловживань (аналіз систем станів, графи атак, нейронні та імунні мережі, експертні системи, методи, що ґрунтуються на специфікаціях, сигнатурні методи).

Для порівняльних методів виявлення вторгнень запропоновано наступні показники [40]:

а) ступінь спостереження системи визначає ступінь абстрагування подій, які аналізуються в захищеній системі, а також межі застосування методу виявлення атак у мережах;

б) функція перевірки методу дозволяє оцінити, чи може досвідчений оператор IDPS або експерт відтворити послідовність кроків, щоб вирішити, чи сталася атака (наприклад, передбачається, що сигнатурні методи можна перевірити, а методи кластерні ні). Можливість верифікації дозволяє експертно оцінити правильність методу та його впровадження в будь-який час, навіть під час функціонування IDPS на його основі;

в) адаптивність методу – оцінка стійкості методу до незначних змін у здійсненні атаки, що не змінюють результату атаки. Адаптованість є єдиною головною перевагою "альтернативних" методів виявлення атак над "сигнатурними". Здатність адаптуватися до невідомих атак визначає здатність методу виявляти раніше невідомі атаки;

г) стабільність характеризує незалежність результату методу від захищеної системи: метод повинен забезпечувати вихід для того самого входу. Проблема стійкості особливо гостра із статистичними методами, що використовуються для аналізу абсолютних значень продуктивності та використання ресурсів, які можуть суттєво відрізнятися на різних хостах та в різних мережах;

д) обчислювальна складність – теоретична оцінка складності методу в режимі виявлення без урахування можливих попередніх етапів налаштування та навчання.

4. Масштабованість визначає можливість додавання нових мережевих ресурсів, хостів та каналів даних до аналізу, включаючи можливість управління єдиною розподіленою системою виявлення вторгнень. Також можливе

дистанційне керування IDPS. За допомогою повністю розподіленого управління всіма компонентами IDPS потрібно керувати окремо, а за допомогою повністю централізованого управління всіма компонентами IDPS можна керувати з одного хоста. Адміністративна організація за централізованою схемою вважається кращою і може мати кілька центрів, які можуть динамічно змінюватися.

5. Відкритість визначає наскільки відкритою є система для інтеграції інших методів виявлення вторгнень та сторонніх компонентів та їх поєднання з іншими системами захисту інформації. Вони можуть бути програмними інтерфейсами для підключення додаткових модулів та (або) реалізації стандартів взаємодії мережевих компонентів.

6. Формування адекватну реакцію на напад. Цей показник визначає наявність в системі вбудованих механізмів для адекватної реакції на атаку, а також факт її реєстрації. Прикладами реакцій є: розрив з'єднання з атакуючим об'єктом, блокування зв'язку в ММЕ, відстеження шляху атакуючого об'єкта в систему, що захищається.

7. Безпека визначає ступінь захисту IDPS від атак на його компоненти, включаючи захист інформації, що перебуває в обігу, стійкість до часткового виходу з ладу компонентів, а також наявність слабких місць у компонентах IDPS. Безпека каналів передачі даних між ними, авторизація компонентів в IDPS. Загалом, можна виділити властивості для певної «ідеальної» системи виявлення вторгнень, яка може бути застосована у ККМ:

– розпізнавання всіх класів атак (повна система);

– можливість аналізувати поведінку захищеної ККМ на всіх рівнях: мережа, хост, операційна система та окремі програми;

– адаптація до невідомих атак (адаптивний метод їх виявлення);

– зміна масштабу для мереж різних класів: від локальних мереж класу «домашній офіс» до великих корпоративних мереж з декількома сегментами для централізованого управління всіма компонентами IDPS;

– відкритість;

– вбудовані механізми реагування на вторгнення;

– захищеність від кібератак на компоненти IDPS, включаючи перехоплення або атаки DoS.

2.5 Висновки

Розглянуто основні методи аналізу мережевого трафіку, моделі мережевого трафіку. Дані методи та моделі активно застосовуються у готових апаратних та програмно-апаратних комплексах запобігання вторгненням в комп’ютерну мережу.

Розглянуто приклади систем моніторингу трафіку, таких як сніфери, однак вони мають такі недоліки, як складність використання недосвідченим користувачем, складний інтерфейс, обмеженість використання у різних операційних системах, а також відсутність інструменту виведення графічної інформації щодо стану мережі в певний час. Відсутність графічного представлення інформації ускладнює процес аналізу мережевого трафіку.

Розглянуто поняття систем виявлення та запобігання вторгненням, розглянуто їх види та особливості функціонування. Системи виявлення вторгнень є універсальним інструментом для моніторингу та аналізу мережевого трафіку, в залежності від виду системи вони можуть допомогти користувачу виконувати дії щодо захисту локальної мережі від атак або повідомляти його про підозрілу мережеву активність.

Не існує універсальних вимог щодо вибору IDPS, система має обиратися у відповідності до вимог безпеки у конкретному випадку. Було проведено аналіз систем виявлення атак і запобігання вторгненням, розглянуто їх особливості, відмінності та властивості різних типів подібних систем, також розглянуто механізми реалізації кібератак. Виходячи з отриманих даних, варто зазначити, що СВВ повинні вдосконалюватись та налаштовуватись у відповідності до особливостей функціонування та реалізації ККМ, в якій буде забезпечуватись захист.

3 СИСТЕМИ ВИЯВЛЕННЯ АТАК І ЗАПОБІГАННЯ ВТОРГНЕНЬ В КОРПОРАТИВНИХ МЕРЕЖАХ

3.1 Аналіз методів виявлення вторгнень в комп'ютерну мережу

Один з основних методів виявлення атак на розподілені обчислювальні системи були відібрані для аналізу:

– аналіз сигнатур;

– статистичний аналіз;

– аналіз систем станів;

– графи сценаріїв атак;

– експертні системи;

– методи, засновані на специфікації;

– нейронні мережі;

– імунні мережі;

– груповий аналіз;

– поведінкова біометрія.

Аналіз сигнатур. Сигнатура атаки складається з ряду параметрів системи, низка пов'язаних подій або дій, що призводять до спроби атаки. Метод аналізу сигнатур заснований на порівнянні поточного стану системи зі статусом системи та дій у ній з наявними сигнатурами, які зберігаються у попередньо заповненій базі даних. До переваг методу аналізу сигнатур можна віднести швидкість роботи та низька ймовірність помилки при виявленні атаки через те, що здійснено пошук відповідно до існуючих атак. Недоліком цього методу є неможливість виявлення невідомих атак.

Статистичний аналіз. Для роботи цього методу створюються статистичні профілі системи, що містять набір параметрів і допустимі значення цих параметрів, що відповідають нормальній поведінці системи. Метод статистичного аналізу заснований на виявленні атаки, якщо поведінка захищеної системи відхиляється від статистичного профілю (моделі). До переваг методу можна віднести його адаптивність, тобто можливість виявлення невідомих атак. Недоліками статистичного аналізу є висока ймовірність

помилкових спрацьовувань, а також той факт, що при використанні цього методу зміни в діяльності об'єкта не обробляються, що може призвести як до помилкових спрацьовувань, так і до пропущених атак.

Аналіз систем станів. При використанні цього методу процес роботи захищеної системи описується як ряд станів і переходів між ними. Таким чином, робота системи інтерпретується за допомогою спрямованого графа, як правило, з нескінченною кількістю вершин. Деякі шляхи на графі, що описують зміну стану системи, позначені як недопустимі, кінцевий стан кожного шляху небезпечний для захищеної системи.

Метод аналізу системи станів шукає відомі неприйнятні шляхи у побудованому графі станів захищеної системи. Визначення послідовності переходів, що призводять до небезпечного стану, означає успішне розпізнавання нападу. Недоліком цього методу є неможливість виявити атаку, якщо послідовність системних станів перекривається.

Графи сценаріїв атаки. Метод полягає у створенні графа, який включає всі відомі сценарії атак на основі певної характеристики стану системи. Для того, щоб створити граф сценаріїв атаки, створюється формальний опис захищеної системи та визначається властивість коректності системи. За властивістю коректності можлива поведінка системи поділяється на прийнятну та неприйнятну. Неправильна поведінка системи вважається можливою атакою. Розглянутий метод створює повний набір варіантів неприйнятної поведінки для певної захищеної системи, що забезпечує опис можливих шляхів атаки. Цей метод може бути використаний для пошуку слабких ланок у конструкції системи. Однак через свою високу обчислювальну складність він не застосовується щодо проблеми виявлення вторгнень.

Експертні системи. Використання експертних систем для виявлення атак засноване на описі того, як працює система, у вигляді низки фактів та правил висновку. При введенні даних експертна система отримує дані про події, що спостерігаються в системі, у вигляді фактів. Спираючись на факти та правила, система виявлення та запобігання вторгненню вирішує, чи присутня атака чи ні. У загальному випадку ця група методів має дуже високі обчислювальні

зусилля, оскільки можна спостерігати повний перебір великої кількості альтернатив.

Методи, засновані на специфікаціях. Цей метод заснований на описі обмежень щодо забороненої поведінки об'єктів у захищеній системі у вигляді специфікацій атаки. Специфікація може включати обмеження щодо завантаження ресурсів, перелік заборонених операцій та спосіб їх роботи, а також час доби, коли застосовуються певні обмеження. Дотримання специфікацій вважається атакою. Основним недоліком є еволюція специфікацій.

Нейронні та імунні мережі. Проблему виявлення вторгнень можна розглядати як проблему розпізнавання зразків або проблему класифікації, тому для її вирішення використовуються нейронні або імунні мережі. При використанні імунних мереж система імітує негативний механізм відбору, генеруючи раніше невідомі сигнатури, які порівнюються зі звичайним профілем. Метод нейронної мережі, у свою чергу, характеризується поданням захищеної системи та зовнішніх об'єктів, які взаємодіють з нею у вигляді траєкторій у певному числовому просторі атрибутів. Як метод виявлення зловживань нейронні мережі навчаються на прикладах атак кожного класу, а потім використовуються для визнання належності спостережуваної поведінки до одного з класів атак.

Груповий аналіз. Суть цієї групи методів полягає у розподілі набору властивостей спостережуваних векторів системи на кластери, серед яких виділяються кластери з нормальною поведінкою. Кожен конкретний метод кластерного аналізу використовує власну метрику, щоб оцінити, чи належить системний вектор властивостей до одного з кластерів чи перевищує межі відомих кластерів. Метод кластерного аналізу по суті такий самий, як і метод статистичного аналізу.

У табл. 3.1 наведено результати порівняльного аналізу методів ідентифікації різних класів атак.

Оскільки число нових, раніше невідомих атак з кожним роком збільшується, адаптивні методи виявлення вторгнень є найкращими. З

результатів аналізу, наведених у табл. 3.1 випливає, що розглянуті адаптивні методи виявлення вторгнень включають: статистичний аналіз, графи сценаріїв атак, експертні системи, нейронні мережі, імунні мережі, кластерний аналіз та біометричну поведінку.

Таблиця 3.1 – Результати аналізу методів виявлення вторгнень

Методи	Рівень спостереження	Верифікація	Адаптивність	Стійкість	Обчислювальна складність
Аналіз сигнатур	Хост, мережа, додатки	Так	Ні	Глобальна	O(log n)
Статистичний аналіз	Хост, мережа	Ні	Так	Локальна	O(n)
Аналіз систем станів	Хост, мережа, додатки	Так	Ні	Локальна	O(n)
Графи сценаріїв атак	Хост, мережа, додатки	Так	Так	Локальна	NP
Експертні системи	Хост, мережа	Так	Так	Глобальна	NP
Методи засновані на специфікаціях	Мережа	Так	Ні	Локальна	O(log n)
Нейронні мережі	Хост, мережа, додатки	Так	Так	Локальна	O(n)
Імунні мережі	Хост, мережа	Ні	Так	Локальна	O(n)
Кластерний аналіз	Хост, мережа, додатки	Ні	Так	Локальна	O(n)
Поведінкова біометрія	Хост	Ні	Так	Локальна	O(n)

Методи, засновані на побудові графів сценаріїв атак та експертних системах практично не використовуються в існуючих системах виявлення та запобігання вторгненню через великі обчислювальні зусилля, залучені до їх реалізації. Методи виявлення вторгнень, засновані на використанні імунних мереж та поведінкової біометрії також не використовуються у готових рішеннях через складність їх реалізації. Методи засновані на нейронних мережах володіють адаптивністю та низькою обчислювальною складністю, однак для виявлення невідомих типів атак постає потреба у формуванні тестового набору для навчання системи. Некоректний навчальний набір може призвести до неефективної роботи СВВ. З інших методів адаптивного виявлення вторгнень метод статистичного аналізу та аналогічний по суті метод

кластерного аналізу мають непогану ефективність, хоча присутня ймовірність помилково позитивних результатів.

3.2 Використання статистичних методів виявлення вторгнень

Аналіз статистичних характеристик аномальних вторгнень передбачає обчислення для кожного нового набору даних значень статистичного аналізу таких статистичних характеристик:

– вибіркове середнє

$$\mathrm{m_i}=\frac{1}{\mathrm{n}}\sum_{j=i}^{i+n}S_j \tag{3.1}$$

де S – показник активності мережевого трафіка;

– вибіркова дисперсія

$$\mathrm{D}=\frac{1}{\mathrm{n\text{-}1}}\sum_{j=i}^{i+n}(S_j m_i)^2 \tag{3.2}$$

– коефіцієнт асиметрії

$$K_\alpha=\frac{\frac{1}{\mathrm{n}}\sum_{j=i}^{i+n}(S_j m_i)^3}{D^3} \tag{3.3}$$

– коефіцієнт ексцесу

$$K_e=\frac{\frac{1}{\mathrm{n}}\sum_{j=i}^{i+n}(S_j m_i)^4}{D^4}-3 \tag{3.4}$$

– контрексцес

$$K_o=\frac{1}{\sqrt{\eta}} \tag{3.5}$$

де η – параметр ексцесу

Для зіставлення розподілів, сформованих для кожної статистичної характеристики, використовується критерій згоди Пірсона, який характеризує існування лінійної залежності між двома розподілами

$$r_{xy}=\frac{\sum_{i=1}^{m}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{m}(x_i-\bar{x})^2\sum_{i=1}^{m}(y_i-\bar{y})^2}}=\frac{cov(x,y)}{\sqrt{s_x^2 s_y^2}} \tag{3.6}$$

Мережева атака являє собою збільшення неоднорідності мережевої активності, при якій заражені пристрої кардинально змінюють поведінку

вхідного мережевого трафіку, що в свою чергу відбивається на статистичних показниках.

При черговому порівнянні з еталонними значеннями статистичних характеристик детектується аномалія поведінки мережевого трафіку і робиться припущення про наявність мережевої атаки.

На прикладі атаки типу HTTP-flood (початок атаки: 12 секунд, довжина статистичного аналізу: 45 секунд, момент обновлення статистичних даних: 57 секунд) розглянуто поведінку представлених статистичних характеристик.

Як видно на рис. 3.1, в момент здійснення атаки показник вибіркового середнього починає лінійно зростати і досягає свого максимуму і перестає зростати в момент повного оновлення значень статистичного аналізу, починаючи з моменту атаки.

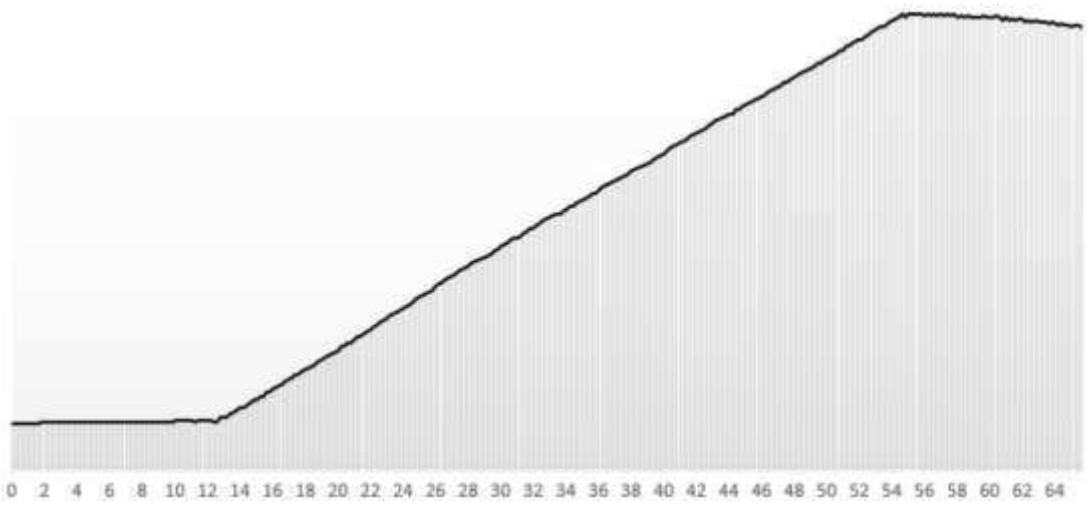


Рисунок 3.1 – Розподіл значень вибіркового середнього

Показник вибіркової дисперсії починає квадратично зростати, досягає свого максимуму і починає також зменшуватися до середнього показника між значенням «в момент атаки» і повного оновлення даних статистичного аналізу (рис. 3.2).

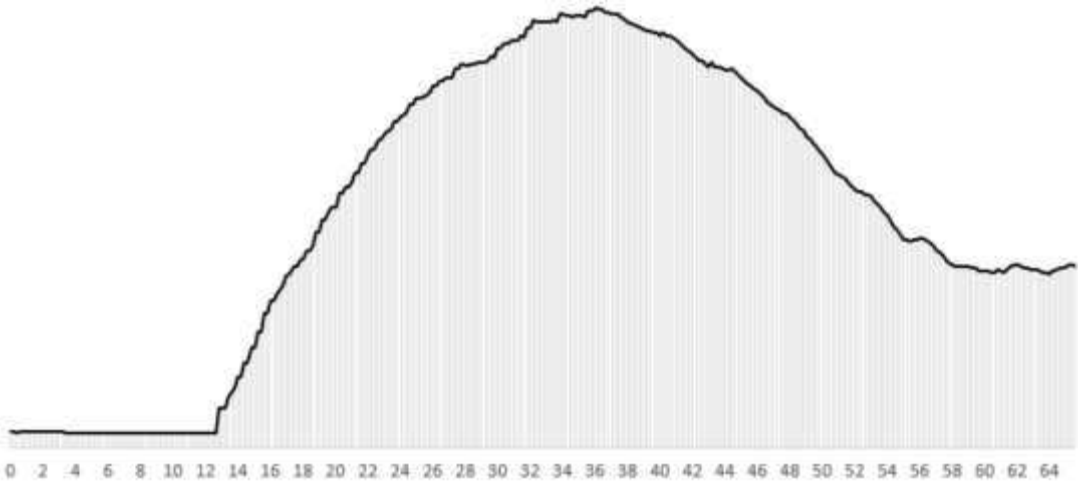


Рисунок 3.2 – Розподіл значень вибіркової дисперсії

Як видно на рис. 3.3, в момент здійснення атаки показник коефіцієнта асиметрії різко досягає свого максимуму, а потім демонструє експоненціальне зменшення і досягає свого мінімуму до моменту повного оновлення даних статистичного аналізу.

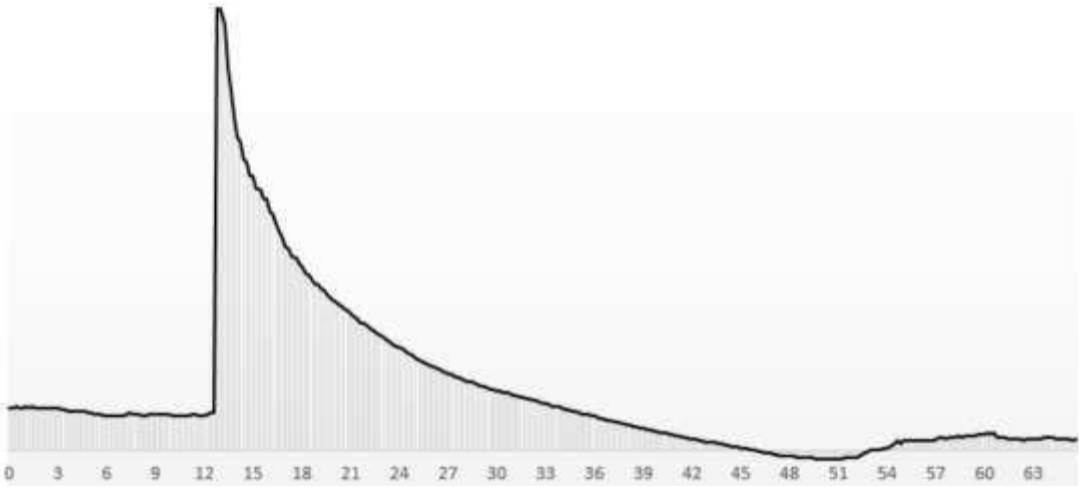


Рисунок 3.3 – Розподіл значень коефіцієнта асиметрії

Як видно на рис. 3.4, в момент здійснення атаки показник коефіцієнта контрексцесу різко зменшується і досягає свого мінімуму, потім спостерігається квадратичне зростання, досягнення максимуму і поступове відновлення до початкового значення.

Для оцінки розподілу статистичних параметрів повинна бути реалізована функція розрахунку коефіцієнта кореляції Пірсона. Оскільки розподіл

формується для кожної статистичної характеристики, яка у разі мережевої атаки є одним із відомих типів розподілу випадкової величини, найважливішим моментом у статистичному аналізі є правильне порівняння сформованого розподілу з одним із відомих.

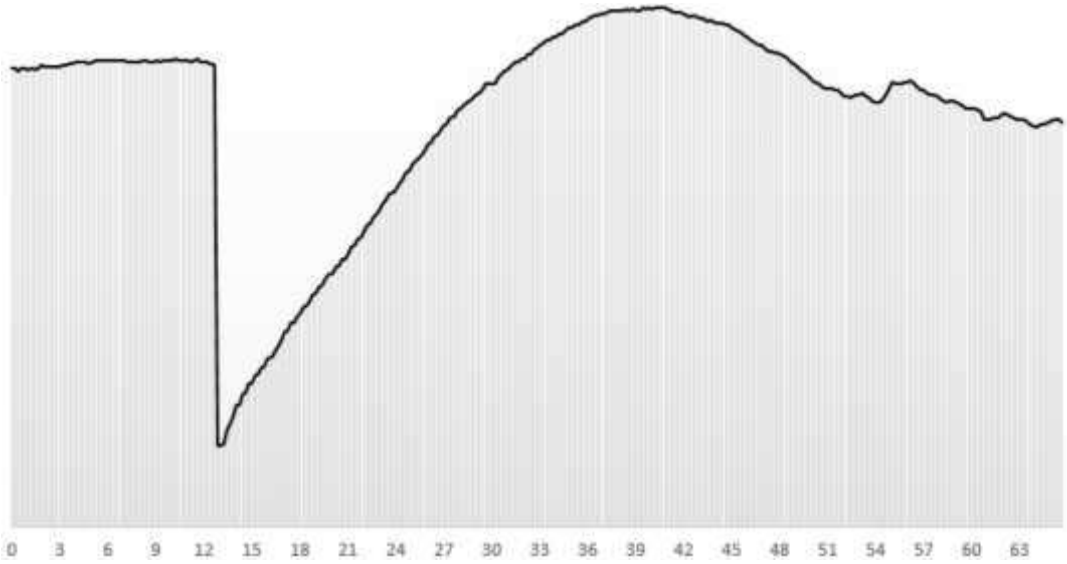


Рисунок 3.4 – Розподіл значень коефіцієнта контрексцесу

Розподіл значень дисперсії під час атаки HTTP-flood (рис. 3.5).

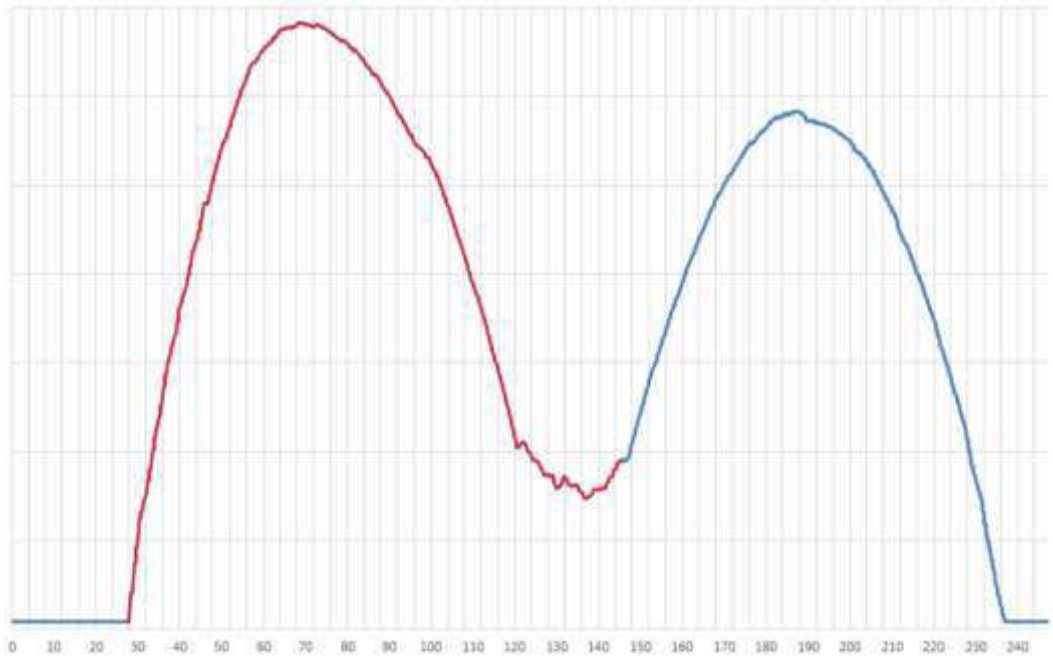


Рисунок 3.5– Розподіл значень вибіркової дисперсії

Атака на мережу розпочалася через 28 секунд після початку і закінчилася на 147, атака на мережу була виявлена через 120 секунд, через 92 секунди після початку атаки. Коефіцієнт кореляції Пірсона для даного розподілу r_{xy}= 0,9141, з чого випливає, означає що обрана ділянка на 91% корелює з прикладом нормального розподілу, що говорить про наявність мережевої атаки.

Аналізуючи отримані результати можна зробити висновок про ефективність статистичних методів при виявленні мережевих атак.

3.3 Обґрунтування вибору систем виявлення вторгнень

На ринку продуктів та послуг з інформаційної безпеки можна знайти широкий спектр будь-яких систем, починаючи від невеликих програмних проектів із вихідним кодом і закінчуючи системами захисту інформації від відомих виробників. У той же час виробники деяких продуктів захисту інформації роблять наступне: вони встановлюють додаткові модулі, які виконують функції IDS, у продукт захисту інформації, який виконує роль брандмауера. Як правило, вони мають меншу функціональність і продуктивність, оскільки не є повноцінною незалежною системою.

Проведено порівняльну оцінку систем IDS, які зараз доступні на ринку інформаційної безпеки, які є загальнодоступними або які можна придбати у виробника. Результати наведені в табл. 3.2.

Таблиця 3.2 – Порівняльний аналіз існуючих СВВ

Назва	ПЗ/ПАК	Тип сенсора	Спосіб збору даних	Аналіз результатів	Повнота документації	Вартість
1	2	3	4	5	6	7
KFSensor	ПЗ	HIDS	Сигнатурний	Ні	Ні	Платно
OSSEC HIDS	ПЗ	HIDS	Сигнатурний	Ні	Так	0
Snort	ПЗ	NIDS	Сигнатурний	Ні	Так	0
Suricata	ПЗ	HIDS/NIDS	Сигнатурний	Ні	Так	0
EasyIDS	ПЗ	NIDS	Сигнатурний	Ні	Ні	0
Bro	ПЗ	NIDS	Сигнатурний	Ні	Так	0
Cisco IPS	ПАК	NIDS/HIDS	Сигнатурний, евристичний	Так	Так	Платно

Продовження таблиці 3.2

1	2	3	4	5	6	7
ViPNet IDS	ПАК	NIDS/ HIDS	Сигнатурний, евристичний	Так	Так	Платно
McAfee IPS	ПЗ/ПАК	NIDS/ HIDS/ APIDS	Сигнатурний, евристичний	Так	Так	Платно
Open Source Tripwire	ПЗ	NIDS/ HIDS	Сигнатурний	Ні	Так	0
IBM ISS Proventia IPS	ПЗ/ ПАК	NIDS/ HIDS/ APIDS	Сигнатурний, евристичний	Так	Так	Платно
OSSIM	ПЗ	HIDS	Сигнатурний, евристичний	Так	Так	Платно

Апаратно-програмні комплекси мають власні системи для аналізу даних та результатів роботи. Однак такі системи можуть мати велику вартість, що є проблематичним для застосування їх у ККМ невеликих компаній та підприємств.

Програмне забезпечення на безкоштовній основі не має власної бази аналізу та власного графічного інтерфейсу. Однак для реалізації цих функцій можна використовувати сторонні програми.

Як приклад, розглянуто безкоштовні програмні комплекти для виявлення вторгнень: Snort, Suricata, EasyIDS, Bro, Openwind Tripwire. На тлі цих IDS виділяються Snort та Suricata, оскільки вони є свого роду стандартом для подібних систем. Suricata є більш гнучким, ніж Snort. Однак багато постачальників розробляють і впроваджують IDS на основі системи Snort, але не приховують цього, навпаки, відкрито заявляють про це. До таких постачальників належать Source Fire, Cisco та інші.

3.4 Аналіз ефективності Snort і Suricata, інструментів виявлення і запобігання вторгнення

Snort – це безкоштовне програмне забезпечення з відкритим кодом, яке ліцензовано GPL. Розроблена в 1998 році однією з найвідоміших особистостей у галузі кібербезпеки, автором багатьох книг Мартіном Роше. Основною причиною створення цієї системи IDS була відсутність на той час інструменту

безпеки, який здатен ефективно сповіщати про атаки, і в той же час був би безкоштовним [17].

Snort може виявити:

– поганий трафік;

– використання експлойтів (ідентифікація Shell code);

– сканування системи (порти, операційна система, користувачі тощо);

– атаки на такі послуги, як Telnet, FTP, DNS тощо;

– DoS / DDoS-атаки;

– атаки, пов'язані з веб-серверами (cgi, php, frontpage, iss та ін.);

– атаки на бази даних SQL, Oracle тощо;

– атаки через протоколи SNMP, Net Bios та ICMP;

– атаки на SMTP, imap, pop2, pop3;

– різні Back doors;

– веб-фільтри (порнографія).

Принцип роботи Snort показано на рис. 3.6.

Рисунок 3.6 – Принцип роботи Snort

Схема роботи включає:

– бібліотеку libpcap;

– декодер пакетів;

– препроцесор;

– детектор;

– нормативну базу;

– модулі виведення інформації.

Бібліотека libpcap дозволяє перехоплювати пакети, що надходять на мережеву карту до того, як вони потраплять в стек протоколів. На основі цієї бібліотеки створюються програми для моніторингу і тестування мережі, такі як Snort, а також сніфери, наприклад, WireShark [18].

Після перехоплення пакет потрапляє в декодер, його завдання полягає в тому, щоб з протоколів канального рівня, таких як Ethernet або 802.11, декапсулювати дані мережевого і транспортного рівня (IP, TCP, UDP, ICMP).

Препроцесор готує дані протоколів транспортного і мережного рівнів для подальшої обробки їх детектором. У Snort присутнє налаштування препроцесорів і їх правил, що дозволяє в загальному випадку збільшити швидкодію системи [21].

Детектор проводить аналіз даних, що надійшли шляхом пошуку в пакетах певних правил, сигнатур, що знаходяться в базі. Самі правила складаються з опису правила, сигнатури, опису загрози і реакції при виявленні [21].

Після аналізу даних Snort виводить необхідну інформацію (Log, Alert) в потрібних форматах.

Snort здатна працювати в трьох режимах:

– режим сніфер (просто перехоплює і виводить на екран перехоплені дані);

– режим реєстратора пакетів (перехоплює дані і реєструє їх у відповідних файлах);

– режим системи виявлення вторгнень (перехоплює дані і виробляє їх аналіз, при цьому автоматично включається реєстрація пакетів, якщо в налаштуваннях не вказано іншого).

Barnyard2 є інтерпретатором з відкритим вихідним кодом для двійкових файлів, створюваних Snort.

Стандартний спосіб запису подій, передбачений в Snort, консоль або у файл досить ресурсномісткий. В кращому випадку події Snort повинні зберігатися в базі даних MySQL.

PulledPork – це скрипт, який буде завантажувати, комбінувати, встановлювати та оновлювати правила для Snort з різних джерел. Існує кілька

наборів правил, які може завантажувати PulledPork. Його можна налаштувати для завантаження безкоштовного набору правил спільноти Snort, без створення безкоштовного облікового запису Snort.org.

BASE (Basic Analysis and Security Engine) – базовий двигун аналізу і безпеки. Дана програма потрібна для візуалізації детектованих атак.

Як і Snort, Suricata складається з декількох модулів (захоплення, збору, декодування, виявлення і виведення), за замовчуванням до декодування захоплений трафік йде одним потоком, це оптимально з точки зору детектування, але більше навантажує систему. На відміну від Snort, в Suricata можна налаштуваннями перевизначати поведінку трафіку і одним налаштуванням розділити потоки відразу після захоплення, а іншим – вказати, як будуть розподілятися потоки по процесорам.

Це дає широкі можливості для оптимізації обробки трафіку на конкретному обладнанні в конкретній мережі.

У Suricata підтримується вилучення та перевірка переданих по HTTP файлів, розбір стисненого контенту, можливість ідентифікації по URI, cookie, заголовкам, user-agent, тілу запиту і відповіді. Цю можливість Suricata в деяких мережах використовують для протоколювання HTTP-трафіку без детектування. Контент в потоці можна виділяти за маскою і за допомогою регулярних виразів, ідентифікація файлів можлива по імені, типу або контрольною MD5-сумою.

Підтримується декодування IPv6, в тому числі і тунелі IPv4-in-IPv6, IPv6-in-IPv6, Teredo та інші. Модульне компонування движка дає можливість швидко підключити новий елемент для захоплення, декодування, аналізу або обробки пакетів.

Для перехоплення трафіку використовується кілька інтерфейсів – NF Queue, IPF Ring, Lib Pcap, IPFW, AF_PACKET, PF_RING. Режим Unix Socket дозволяє автоматично аналізувати PCAP-файли, попередньо захоплені іншою програмою (сніфером, наприклад).

Критичне порівняння проводиться між системами виявлення та запобігання вторгненням Suricata та Snort.

Показниками, що використовуються для вимірювання ефективності

систем виявлення та запобігання вторгнень, повинні бути: швидкість виявлення атак, помилкові спрацьовування. Обмеження потужності є несправністю, як тільки система виявлення та запобігання вторгнень досягне граничної потужності, пакети відкидаються, і тому шкідливий вміст не виявляється.

Для кількісної оцінки метрик, що використовуються для оцінки точності системи виявлення та запобігання вторгненню, можна використати наступні: охоплення (кількість атак, які можна виявити), ймовірність помилкових спрацьовувань, ймовірність виявлення резистивних атак, здатність обслуговувати канал з високою пропускною здатністю і ємністю. Що стосується продуктивності, вона має ряд компонентів, і тому не є метрикою. У табл. 3.3 наведено деякі показники, що відображають ємність.

Необхідно реєструвати такі показники: байти в секунду, пакети в секунду та кількість мережевих атак. Крім того, для кожної системи виявлення та запобігання вторгненню в мережу зменшено кількість втрачених пакетів, також були записані фактичні тригери, помилкові спрацьовування, негативні тригери та загальна кількість тривог. Нарешті, хост відстежує використання центрального процесора та пам'яті, постійне зберігання, пропускну здатність інтерфейсу та статистику файлів підкачки.

Таблиця 3.3 – Оцінка потенціалу

Показник, що перевіряється	Використання ресурсів
Пакетів в секунду	Цикли CPU, пропускна здатність інтерфейсів, пропускна здатність шини
Байт в секунду (середній розмір пакета)	Цикли CPU, пропускна здатність інтерфейсів, пропускна здатність шини
Протоколи	Цикли CPU і пропускна здатність шини
Кількість унікальних хостів	Розмір пам'яті, цикли CPU, пропускна здатність шини
Кількість нових з'єднань в секунду	Цикли CPU і пропускна здатність шини
Кількість одночасних з'єднань	Розмір пам'яті, цикли CPU, пропускна здатність шини
Попередження в секунду	Розмір пам'яті, цикли CPU, пропускна здатність шини

Тестовий стенд налаштований у віртуальному середовищі, що сприяє

мобільності та безпеці експерименту. Це було необхідно для частого повторення та реконфігурації експериментальних випробувань.

VMware Workstation 15 була використана як платформа для віртуалізації, багато в чому завдяки хорошій продуктивності вводу-виводу та жорсткого диска порівняно з іншими засобами віртуалізації. В якості операційної системи було обрано 32-розрядну Ubuntu 18.04 LTS. Ubuntu регулярно оновлюється і має хорошу базу спільнот. Це також найпопулярніша операційна система Linux.

За замовчуванням апаратна конфігурація для системи виявлення та запобігання вторгнень в мережу становила 2,8 ГГц чотирьохядерним процесором Intel Xeon (E5462) з 4-ядерною 3 ГБ DDR2 800 МГц повністю буферованою пам'яттю. Кожна система також мала максимальний об’єм жорсткого диска 20 ГБ. Мережевий трафік передавався окремо для кожної системи. Система, що використовується для відтворення мережевого трафіку, використовує одне ядро та 1 Гб оперативної пам'яті. VMware хост операційної системи, що використовує 2 Гб оперативної пам'яті і 1 ядро, що перешкоджає хосту з якого виробляє на випробувальному стенді.

Snort і Suricata були налаштовані на роботу з однаковими правилами. Suricata використовує різні класифікації конфігурації Snort, яка використовує 134 декодери та 174 правила препроцесора. Ідентичні методи реєстрації, які називаються Barnyard, MySQL та AcidBase, використовувались як для систем виявлення вторгнень в мережі, так і для систем запобігання. Версії Snort та Suricata були v2.9.8.3 та v4.1.2 відповідно.

Обидві системи використовували набір правил VRT Snort v2.9.8.3 у поєднанні з набором правил для нових загроз. Після того, як усі правила були завантажені, визначення правил були завантажені в Suricata 11039 порівняно з 11065 в Snort. Ця розбіжність пов’язана з тим, що Suricata не може проаналізувати деякі правила VRT.

При виборі мережевого трафіку для тестування систем для виявлення та запобігання вторгненню в мережу є певні особливості. По-перше, атакуючий трафік можна використовувати окремо або з додаванням контекстного фонового трафіку. Якщо використовується фоновий трафік, це може бути

реальною або імітованою поведінкою. Якщо це реальна поведінка, її можна залишити недоторканою або, навпаки, дезінфікувати, тобто дані користувача та інформацію про IP-адресу буде видалено.

Для тестування було корисно і бажано використовувати реальний мережевий трафік у фоновому режимі. Однак повторення експериментів із трафіком у реальному часі було б непередбачуваним через його динаміку. Було обрано використання трафіку, захопленого з файлу pcap. Це сприяло їх обробці системою виявлення та попередження вторгнення мережі в автономному режимі, дозволяючи відтворювати в мережі з різною швидкістю, використовуючи TCPReplay. Крім того, усунуто всі ризики для критично важливих мереж.

Існує багато джерел тестового трафіку для завантаження, але, на жаль, їх часто дезінфікують. Це робить їх непридатними для оцінки NIDPS, яка робить глибокий аналіз пакетів. Існують такі інструменти, як TCPdump Randomiser, які додають будь-яке корисне навантаження до очищення даних. Однак реалістичність таких змінених даних стає сумнівною. Контекстний злом також забезпечує джерела для захоплення трафіку, хоча зміст трафіку не задокументовано. Тому його потрібно визначити заздалегідь перед використанням. Наприклад, деякі атаки зазнали невдачі, а інші – успіху. На основі цих питань було вирішено зафіксувати фоновий трафік із задіяних веб-серверів та серверів додатків. Потім це було поєднано з керованим трафіком, створеним за допомогою Metasploit Framework. Metasploit Framework містить загалом 587 модулів, які можна використовувати для атаки даних, які генеруються у великих кількостях.

Використовуваний трафік було зафіксовано для запуску атак Metasploit на комп'ютері під керуванням Microsoft Windows 2000. Windows 2000 було обрано як найбільш підходящий Metasploit для цієї операційної системи порівняно з іншими.

Велика кількість служб і додатків перестали працювати і встановлюються там, щоб дозволити якомога більше атак. На жаль, не всі з них можна отримати. Атаки, перелічені в таблиці 3.4, реєструються за допомогою Wireshark.

Захоплений і фоновий і атакуючий тип трафіку. Частина програми Wireshark, Edicap, була використана для зміни часової позначки використовуваного трафіку та співвіднесення її з трафіком у фоновому режимі. У цій дії вони були об’єднані в хронологічному порядку, щоб атакуючий трафік перемістився на другий план.

Таблиця 3.4 – Вивчення атак

Код	Ім’я	Опис
ms03_026_dcom	Microsoft RPCDCOM Interface Overflow	Модуль використовуваного стеку переповнення буфера в службі RPCSS
ms05_039_pnp	Microsoft Server Service NetpwPathCanonicalize Overflow	Стек переповнення буфера в службі Windows Plug and Play
ms05_047_pnp	Microsoft Plug and Play Service Registry Overflow	Стек переповнення буфера в службі Windows PnP. Причина перезавантажень.
ms06_040_netapi	Microsoft Server Service NetpwPathCanonicalize Overflow	Стек переповнення буфера в NetApi32 CanonicalizePathName () використовуючи функцію NetpwPathCanonicalize RPC виклик служби Server
ms05_017_msmq	Microsoft Message Queueing Service Path Overflow	Використовуваний стек переповнення буфера в RPC інтерфейсі в службі Microsoft Message Queueing
ms01_033_idq	Microsoft IIS5.0 IDQ Path Overflow	Використовуваний стек переповнення буфера в IDQ ISAPI обслуговування для Microsoft Index Server

Продуктивність NIDPS тісно пов'язана з продуктивністю системи центрального процесора. Отже, Snort та Suricata повинні завантажувати центральний процесор, щоб оцінити їх роботу в стресових умовах.

VMware використовувався для зменшення кількості логічних та фізичних ядер. Самі ядра зазнавали напруги, створюючи потоки, які створювали регульовані та вимірювані навантаження. Це було зроблено за допомогою cpulimit, який генерує налаштування робочого навантаження центрального процесора і дозволяє загальному навантаженню кожного потоку обмежити відсоток потужності центрального процесора.

І Snort, і Suricata дозволяють внутрішнє відтворення файлів pcap. Це робиться з максимально можливою швидкістю для NIDPS і забезпечує хорошу оцінку продуктивності системи. Однак цей метод не враховує максимальні швидкості без втрат (MLFR). Тому TCPReplay використовувався для перевірки

швидкості трафіку, що дозволяє проводити стрес-тести під навантаженням на мережу.

Відстежувались такі ресурси: використання центрального процесора, використання пам’яті, опір пропускної здатності пам'яті та пропускна здатність мережі. Це було зроблено за допомогою інструмента командного рядка Linux dstat.

Пропускна здатність збільшується, і MLFR NIDPS впливає як на використання центрального процесора, так і на пропускну здатність трафіку. Тому експеримент був розроблений, щоб надати дані про те, як кожна система може впоратися з більшою пропускною здатністю в умовах високої напруги процесора.

Атакуючий трафік даних маршрутизувався через обидві NIDPS з різними конфігураціями процесора. Сюди входять: 2-ядерна конфігурація ядра процесора, 1 ядро, навантаження 50% та 75%. Здатність NIDPS читати пакети вимірювалась, як і точність попереджень, з особливою увагою приділялись помилково негативні результати. Тестовий трафік було перенаправлено в середовище за допомогою TCPReplay, помноженого на 40. Він відтворюється в 40 разів швидше, ніж при захопленні. Цей результат призвів до відтворення смуги пропускання 3,1 Мбіт / с, а кількість скинутих пакетів досягла 2%. Це забезпечило можливість завершення експериментів вчасно, безпосередньо перед втратою пакетів.

Кожного разу, коли запускалося тестування, реєструвались початок і кінець трафіку запуску NIDPS. Це було гарною відправною точкою для аналізу системи попередження та статистики. Інформація про попередження видавалася для кожного тестового запуску та реєструвалась за допомогою acidbase, також відомого як вихідний файл unified2, який архівується для подальшого використання. Статистика продуктивності NIDPS закрита, записана, кількість генерованих сповіщень, кількість оброблених пакетів та їх відношення до оброблюваних мережевих протоколів. Трафік проходив через хости 192.168.16.2 та 192.168.16.128, але був позначений як небажаний трафік.

Для визначення точності використаний контроль попереджень. Ці

попередження, отримані без системи стресів, використовувались як еталон. Відхилення від базової лінії в умовах стресу показувало зміни в точності виявлення. У табл. 3.5 наведено кількість типів попередження, що генеруються під час нападу на кожну NIDPS. На рис. 3.7 показані попередження Suricata на кожен експлоїт у всіх конфігураціях, але деякі попередження втрачені, що призводить до зменшення діапазону виявлення.

Таблиця 3.5 – Попередження згенеровані Snort і Suricata

Попередження	Snort	Suricata
ms05_040_pnp	4	4
ms05_047_pnp	1	1
ms05_039_pnp	1	6
ms03_026_dcom	1	2
ms01_033_1dq	2	4
ms05_017_msmq	2	3

На рис. 3.8 показано провальні попередження Snort на ms01_033_idq. Ці помилкові негативні результати обумовлені надмірним навантаженням.

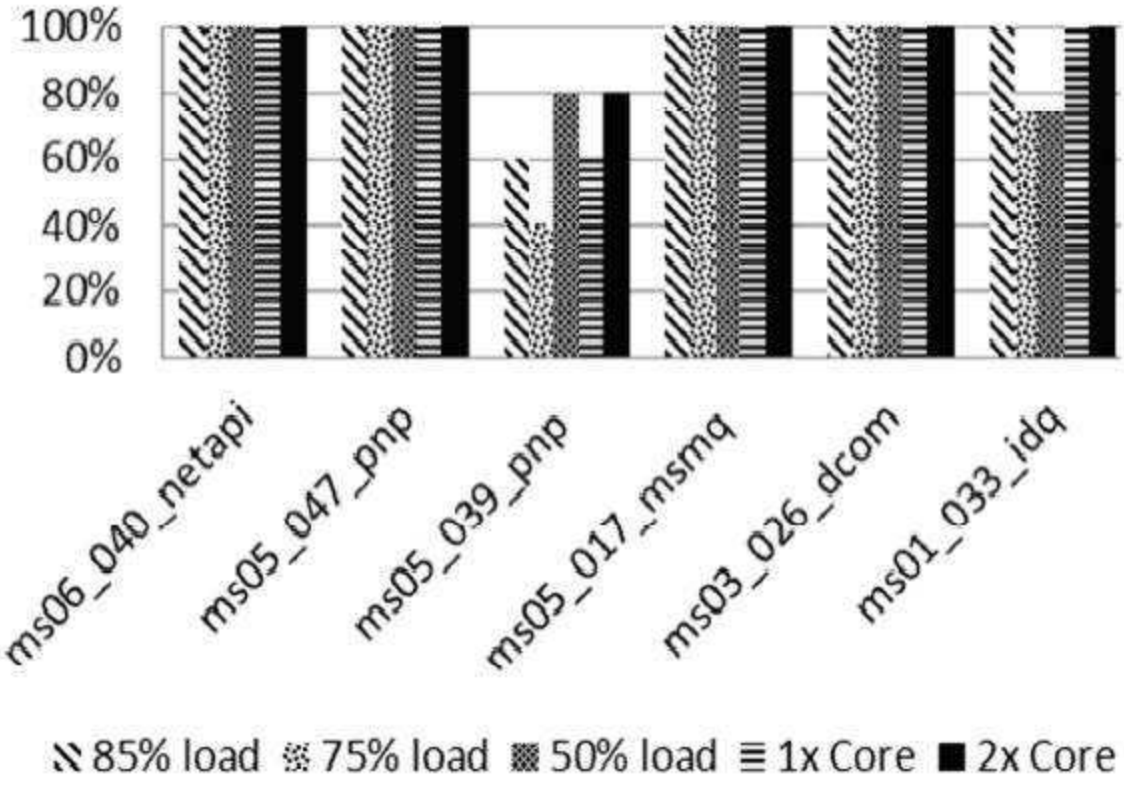


Рисунок 3.7 – Попередження у Suricata

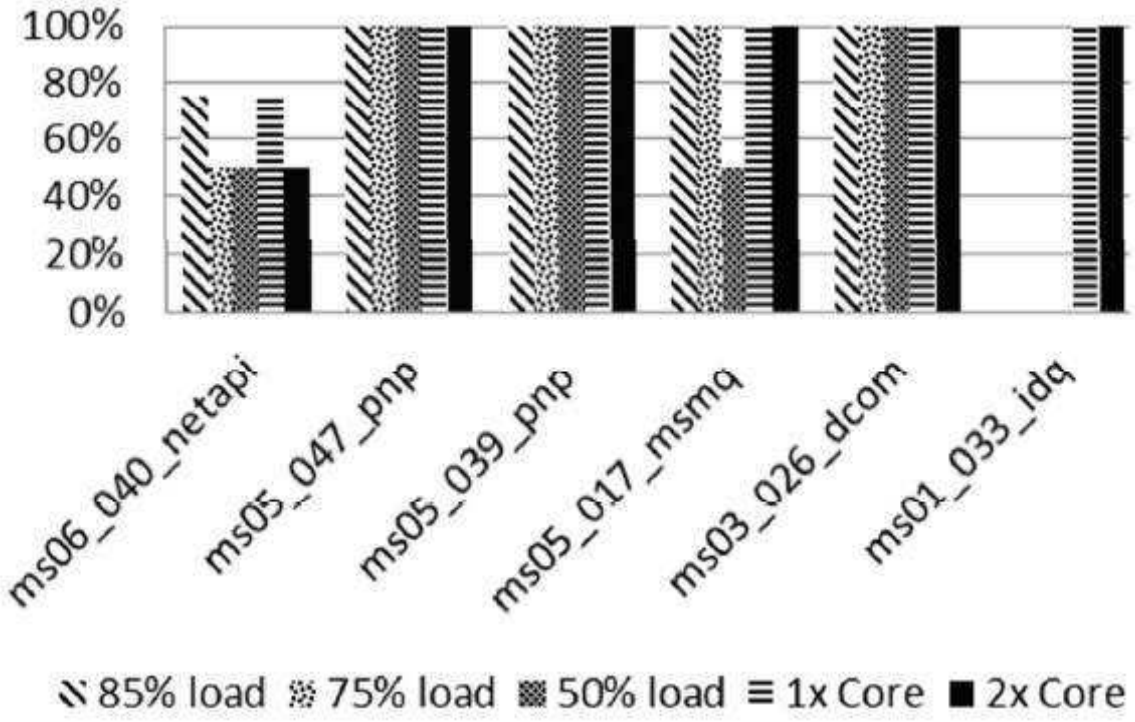


Рисунок 3.8 – Попередження у Snort

На рис. 3.9 показано кількість хибнопозитивних та справді позитивних результатів для обох NIDPS порівняно з кількістю втрачених попереджень для кожної системи.

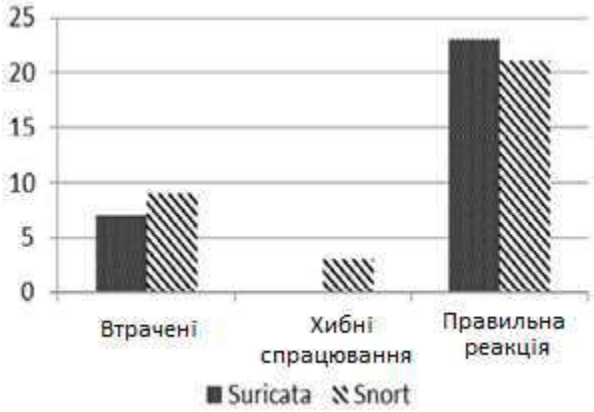


Рисунок 3.9 – Точність вимірювання атак

Помилково негативні результати можуть призвести до викидання пакетів. Рис. 3.10 показує кількість відхилених пакетів Snort та Suricata як міру доступності центрального процесора. Хоча відсоток падіння Snort в основному лінійний, продуктивність Suricata значно зменшується лише в тому випадку,

якщо ресурси центрального процесора зменшуються до одного ядра. На рисунку 3.11 показано, як зменшується кількість ядер та використання центрального процесора, вплив помилкових негативних результатів на обидві системи.

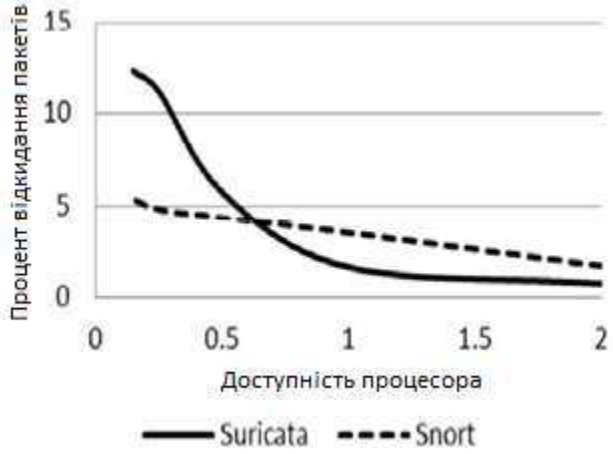


Рисунок 3.10 – Графік втрати пакетів в 3,2 Мб/с

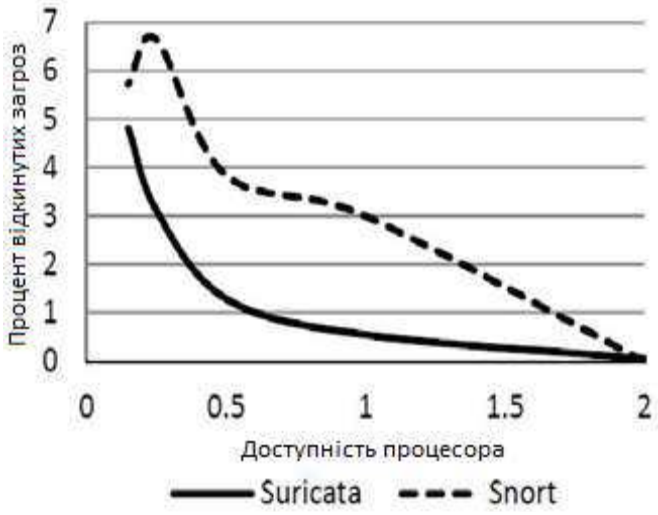


Рисунок 3.11 – Графік помилкових відкинутих попереджень

На рисунку 3.12 показано взаємозв'язок між використанням процесора та пропускною здатністю мережі для Suricata та Snort. Він показує, як збільшується використання центрального процесора щодо пропускної здатності мережі. Така поведінка найбільш помітна, коли працює Suricata. Snort поводиться подібним чином у значно менших масштабах.

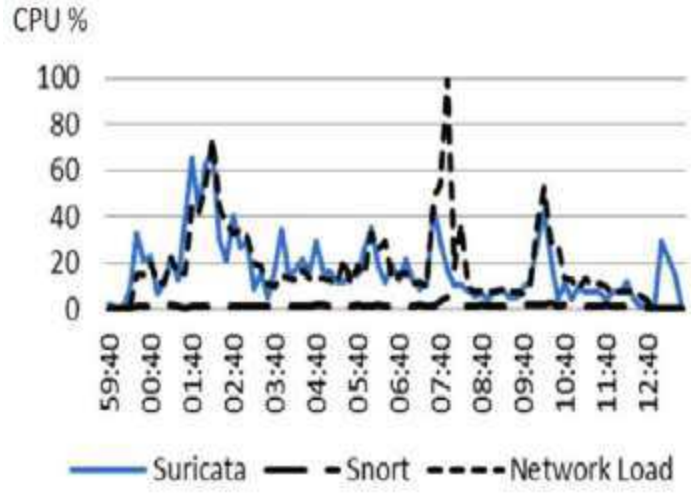


Рисунок 3.12 – Пропускна здатність мережі і використання CPU для одного ядра

При використанні двоядерних процесорів, Suricata має меншу швидкість відкидання, ніж Snort. Щоб з’ясувати, чому обидві системи були оцінені за здатність використовувати обидва ядра. Щоб з'ясувати, чому обидві системи були оцінені по їх здатності використання обох ядер. Рис. 3.13 і 3.14 показують як Snort і Suricata (відповідно), використовують двоядерні процесори.

Рис. 3.13 показує, що Suricata використовує 2 ядра рівномірно, в порівнянні зі Snort, у якого більш нестійке балансування навантаження. На рис. 3.14 це узгоджується з очікуваним, завдяки багатопотоковій архітектурі Suricata.

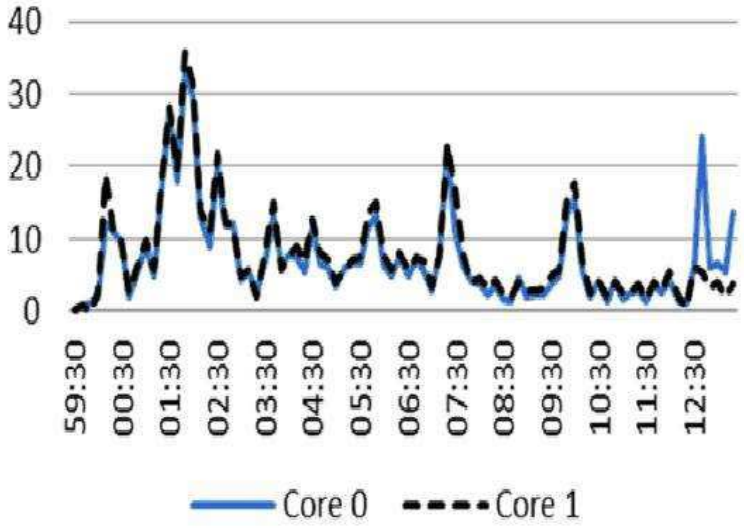


Рисунок 3.13 – Використання Suricata двох ядер

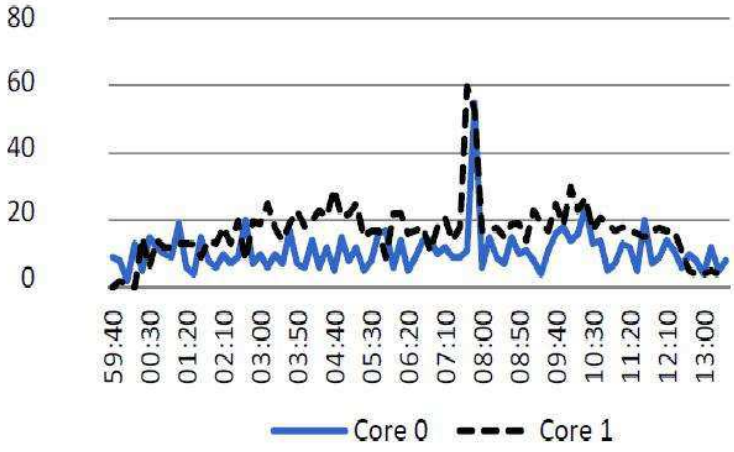


Рисунок 3.14 – Використання Snort двох ядер

Обидва NIDPS можуть обробляти трафік автономно, отримуючи файл pcap і обробляючи його максимально. Це було зроблено для визначення швидкості, з якою обидві системи можуть обробляти трафік. Тест проводився для обох NIDPS, використовуючи один і той же файл pcap. Час, необхідний для кожної системи, показаний на рис. 3.15.

Додаткові ядра не покращили час обробки Snort, хоча продуктивність Suricata зросла на 220% при використанні 4 ядер порівняно з одним. Знову ж, як очікувалося, завдяки багатопотоковій архітектурі Suricata.

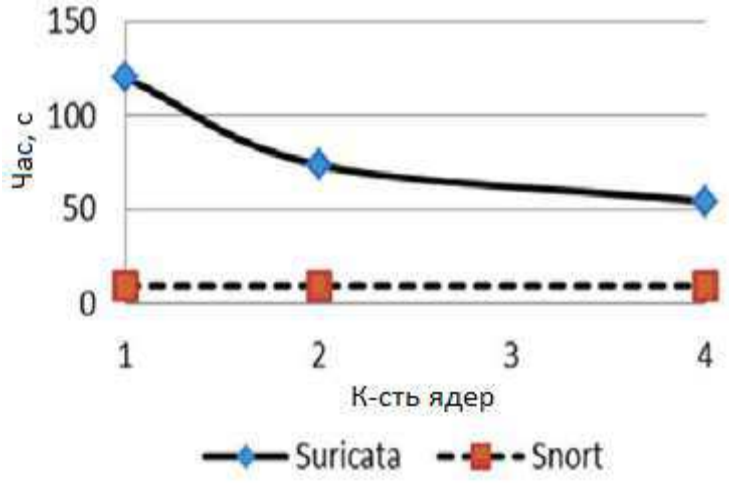


Рисунок 3.15 – Час обробки pcap файлу

Можливо, найважливішим показником оцінки IDPS є точність. Це

розглядалося як покриття атаки системи, помилковий позитивний, помилковий негативний, потенційний, і здатність обробляти великий трафік, тобто з великою пропускною здатністю.

Розробники Suricata заявили, що їх основним напрямком діяльності в удосконаленні NIDPS є підвищення точності. З Suricata спостерігається більша точність, ніж у Snort, звідси можна зробити висновок, що вони мали певний успіх. Це видно на рис. 3.7, 3.8 та 3.9, включаючи дані, які показують, що Snort не спромігся попередити про експлойт ms01_033_idq, коли центральний процесор мав менше 50% навантаження. Частково це пов'язано з тим, що Snort менше контролює функціонування оповіщень під час атаки, ніж Suricata (два проти чотирьох). Snort не зміг попередити ms01_033_idq двома правилами з набору правил VRT, ідентифікаторами 1245 та 1244. Suricata був успішним, і ці сповіщення спрацьовували.

Suricata має високі вимоги до обробки, саме тому він досягає більших експлуатаційних можливостей, ніж Snort. Пояснення великої кількості пакетів, які були відкинуті під навантаженням. Для порівняння, Snort має набагато нижчі системні вимоги, тому він не може працювати з втратою пакетів при максимальному навантаженні системи. Рис. 3.10 показує відсоток втрачених пакетів, який різко збільшується, коли ресурси CPU зменшуються на завантаженому ядрі. Пропорційне співвідношення між відхиленими пакетами та помилково негативними результатами показано на рис. 3.9 в обох системах. При роботі в багатоядерній конфігурації Suricata показує менше втрат пакетів, ніж Snort. Рис. 3.13 та 3.14 показують, що Suricata використовує наявні ядра більш рівномірно. Тести в автономному режимі показують, що Suricata набагато повільніша за Snort. Хоча Suricata використовує багатоядерну систему більш чітко, ніж Snort, (див. рис. 3.10, 3.11 та 3.15). З огляду на це, можна сказати, що Suricata має кращу масштабованість. Однак, якщо Snort отримує хороші результати пропускної здатності, рекомендується запускати кілька екземплярів Snort на декількох ядрах. Це може запропонувати таку ж масштабованість, як Suricata, але з додатковими витратами на обробку однопотокових додатків на декількох ядрах.

3.5 Висновки

Було проаналізовано методи виявлення вторгнень в комп’ютерну мережу. Результати показують, що найкращим рішенням можуть бути статистичні методи та методи, засновані на апараті нейронних мереж при відповідній навчальній вибірці.

Було перевірено твердження ефективності статистичного методу щодо питання виявлення вторгнення в ККМ. Оскільки воно є вірним, даний метод може використовуватись в системах виявлення вторгнень. Було проведено аналіз СВВ за різними критеріями, для подальшого дослідження обрано СВВ Snort та Suricata.

В результаті аналізу функціонування СВВ можна зробити висновок, що Suricata має вищу точність, ніж Snort. Частково це за рахунок підвищення навантаження на центральний процесор. Результати показали, що при більш рівномірно розподілених ядрах Suricata може бути більш масштабованим та ефективним за наявності декількох ядер. Однак через підвищені потреби в ресурсах Suricata точність повинна зменшуватися при використанні Suricata з одним ядром.

4 СИНТЕЗ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

4.1 Методи оцінки загроз інформаційної безпеки

4.1.1 Аналіз наявних методів

Аналіз загроз інформаційної безпеки дає змогу виділити складові елементи сучасних загроз – їх джерела та рушійні сили, способи і наслідки реалізації. Аналіз важливий для одержання всієї необхідної інформації про інформаційні загрози для визначення потенційної величини збитку (як матеріальної, так і нематеріальної) і прийняття необхідних заходів протидії.

Для аналізу загроз інформаційної безпеки використовуються три основні методи:

1) пряма експертна оцінка;

2) статистичний аналіз;

3) факторний аналіз.

Пряма експертна оцінка - це метод експертних оцінок, що заснований на заданні параметрів загроз експертами. Експерти визначають переліки параметрів, що характерні для загрози інформаційної безпеки, і дають суб’єктивні коефіцієнти важливості кожного параметра.

Статистичний аналіз – це аналіз інформаційних загроз на основі накопичених статистичних даних про різноманітні інциденти інформаційної безпеки, зокрема, про частоту виникнення загроз певного типу, їх джерела та причини успішної або неуспішної реалізації. Наприклад, інформація про частоту появи загрози інформаційній безпеці дає змогу визначити ймовірність її виникнення за певний часовий інтервал. Для ефективного застосування статистичного методу потрібна наявність достатньо великої бази даних про інциденти. Необхідно відмітити ще одну вимогу - при використанні об’ємних баз даних необхідно мати інструменти для узагальнення даних і виявлення в базі вже відомої інформації.

В основі факторного аналізу лежить виявлення факторів, які з певною ймовірністю ведуть до реалізації загроз та тих чи інших негативних наслідків.

До таких факторів відносять наявність привабливих для злочинців інформаційних активів, уразливості інформаційних систем, високий рівень вірусної активності в зовнішньому середовищі, тощо. Оскільки на сучасні інформаційні системи вплив мають безліч факторів, то зазвичай використовується багатофакторний аналіз.

При проведенні аналізу загроз інформаційній безпеці найбільш ефективне застосування комплексу різних аналітичних методів. Це значно підвищує точність та достовірність оцінки.

Найбільш вдалим рішенням є створення моделі загроз, що може бути описана різними способами. Найчастіше використовується табличне представлення моделі загроз, проте також популярні способи математичного опису та використання наочних схем.

4.1.2 Аналіз інформаційних загроз приватного підприємства

Оскільки в інформаційних системах приватних підприємств обертається інформація з обмеженим доступом, то відносно неї існують загрози.

Однією із важливих процедур здійснення оцінки захищеності інформації є проведення оцінки інформаційних загроз. Вихідними даними для такої оцінки загроз виступає модель загроз. Модель загроз безпеці необхідна для визначення вимог до системи захисту. Без використання моделі загроз неможливо побудувати прийнятну (з точки зору грошових витрат) систему захисту інформації, що забезпечує потрібний рівень інформаційної безпеки. При такому підході в систему захисту включаються тільки ті засоби захисту, які направлені на нейтралізацію актуальних загроз.

Модель загроз повинна стати відправною точкою для проектування майбутніх систем захисту, чи прийняття рішення про захищеність системи. Тому вдало складена модель загроз дозволяє надійно захистити інформацію і зробити мету прийнятих нормативних документів реальною. З іншого боку, погано або поверхнево розроблена модель загроз зробить всю подальшу роботу марною, не дасть змоги вірно скласти технічне завдання на розробку системи захисту, призведе до необґрунтованих витрат на захист.

Відповідно до діючих державних нормативних документів формування

моделі загроз є необхідною умовою для розробки системи захисту інформації. Згідно з НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», модель загроз – це абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Роботи зі створення моделі загроз безпеки інформації повинні проводитися у відповідності з такими документами:

– Постанова КМУ від 16.02.98 №180 «Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах».

– НД ТЗІ 1.6-003-2004 «Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації»;

– ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт.»;

– НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»;

– НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»;

Модель загроз формується і затверджується відповідно до даних методичних документів, і може бути переглянута на основі:

– періодичного аналізу та оцінки загроз інформаційної безпеки з врахуванням особливостей і змін конкретної інформаційної системи;

– заходів по контролю за дотриманням вимог до забезпечення інформаційної безпеки при обробці даних в інформаційній системі.

Розробка моделі загроз інформаційній безпеці має базуватися на наступних засадах:

1) Безпека інформації при її циркуляції в ІС забезпечується системою захисту інформації.

2) Засоби захисту не можуть забезпечити захист інформації від дій, які виконуються в рамках наданих суб'єкту повноважень (наприклад, система

захисту не може забезпечити захист інформації від розкриття особами, яким надано право на доступ до цієї інформації). Тому потрібно використовувати організаційні заходи разом з технічними засобами.

3) При формуванні моделі загроз необхідно враховувати не тільки загрози, здійснення яких порушує безпеку інформації, а й загрози, що створюють умови для появи прямих загроз або непрямих погроз.

4) Інформація обробляється і зберігається в ІС з використанням деяких інформаційних технологій і технічних засобів, що є об'єктами захисту різного рівня, атаки на які створюють прямі або непрямі загрози інформації.

Для розробки моделі загроз потрібно послідовно виконати такі кроки:

1) провести категоріювання об'єкту;

2) розглянути логічну послідовність процесу порушення інформаційної безпеки;

3) провести ідентифікацію всіх складових моделі загроз та їх зіставлення;

4) дослідити усі зіставлені складові та зробити висновок про їх актуальність;

5) оформити результати висновків згідно із шаблоном.

Розробка моделі загроз здійснюється на підставі детального аналізу атрибутів. У випадку побудови моделі загроз, атрибутами виступають загрози, їх джерела та вразливості.

В таблиці 4.1 представлено аналіз загроз інформаційній безпеці згідно наведеного переліку.

Таблиця 4.1 – Аналіз інформаційних загроз

№	Вид загрози	Ймовір-ність	Що порушує	Рівень збитків	Вразливості
1	2	3	4	5	6
1	Крадіжка а) інформації; б) засобів доступу (ключі, паролі).	Висока	К	Високий	Відсутність засобів захисту інформації від несанкціонованого доступу

Продовження таблиці 4.1.

1	2	3	4	5	6
2	Підміна (модифікація) а) ОС; б) систем управління базами даних; в) програмного забезпечення; г) інформації (даних); д) паролів.	Висока	Ц	Високий	Відсутність засобів виявлення несанкціонованого підключення до КМ; Недостатній мережевий моніторинг.
3	Знищення а) програмного забезпечення (ОС, СУБД, ПЗ) б) інформації в) паролів та ключової інформації.	Висока	Д	Високий	Відсутність засобів виявлення мережевого вторгнення, відсутність засобів протидії мережевим атакам.
4	Порушення нормальної роботи а) швидкості обробки інформації; б) пропускної здатності каналів зв'язку; в) об'ємів оперативної пам'яті; г) об'ємів вільного дискового простору;	Висока	Д	Середній	Недостатня захищеність мережі проти атак зловмисників; Неправильне налаштування програмного забезпечення.
5	Порушення встановлених правил доступу	Висока	К,Ц,Д	Середній	Вразливості робочих станцій та серверного ПЗ внаслідок їх недосконалого налаштування.
6	Порушення нормальної роботи а) швидкості обробки інформації; б) пропускної здатності каналів зв'язку;	Середній	Ц,Д	Середній	Помилки при управлінні складними системами Помилки при експлуатації технічних засобів Порушення режиму експлуатації технічних засобів
7	Порушення нормальної роботи в наслідок пожежі	Низька	Ц,Д	незначний	Порушення режиму охорони і захисту

При класифікації рівнів збитку внаслідок реалізації загрози виділимо наступні:

– критичний – інформація може бути видалена чи змінена без можливості відновлення (в даному випадку втрати організації будуть дуже великі);

– високий – інформація втрачає певні властивості, але може бути відновлена (втрати підприємства в цьому випадку менші, ніж внаслідок повної втрати або неможливості відновлення інформації);

– середній – інформація втрачає деякі властивості, але може бути відновлена в прийнятні терміни і з мінімальними втратами;

– незначний – частина інформації втрачає деякі зі своїх властивостей, які можливо відновити в найкоротший термін (крім конфіденційності).

У класифікації ступенів ймовірності здійснення загрози виділимо наступні:

– висока – прогнозується здійснення загрози декілька разів на місяць;

– середня – настання загрози декілька разів на рік;

– низька – ймовірність настання загрози до одного разу на рік.

Враховуючи вищевикладене, можна зробити висновок, що впровадження заходів по зменшенню ймовірності проведення атак на інформаційну систему приватного підприємства, є виправданим кроком, оскільки це є запобіжним заходом по відношенню до всіх критичних загроз інформаційної мережі.

4.2 Вибір профілю захищеності

Відповідно до НД ТЗІ 2.5-005-99, автоматизована система, що забезпечує функціонування підприємств, являє собою АС ІІІ класу, тобто розподілений багатокористувацький багатомашинний комплекс, який обробляє інформацію різних типів конфіденційності.

Автоматизована система - це організаційно-технічна система, яка об’єднує ОС, фізичне середовище, персонал і інформацію. Відповідно до НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу” стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати захисний комплекс обчислювальної системи, щоб задовольняти вимоги по захищеності інформації, що обробляється в даній системі. На базі типових умов функціонування і класу системи оберемо наступний стандартний

профіль захищеності: 3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}.

Це стандартний функціональний профіль захищеності для АС класу ІІІ з підвищеними вимогами по забезпеченню конфіденційності, цілісності й доступності інформації, яка обробляється в мережі. В профіль включено наступні вимоги:

1) КД-2 - Довірча конфіденційність. Ця послуга застосовується для розмежування доступу користувачів до захищених об’єктів і дає змогу користувачу керувати потоками інформації в системі від захищених об’єктів, що належать його домену, до інших користувачів. Ця послуга реалізовується лише у разі необхідності та як доповнення до послуги КА-2, що визначає основний механізм розмежування доступу до конфіденційної інформації.

2) КВ-1 - Конфіденційність при обміні. Ця послуга забезпечує конфіденційність інформації з обмеженим доступом, яка передається по незахищеним каналам за межами інформаційної системи. Реалізується за допомогою створення VPN-каналу або за допомогою механізму сесій, що існує в апаратних засобах контролю вторгнення після аутентифікації користувача у базі даних.

3) КО-1 - Повторне використання об’єктів. Дозволяє забезпечити коректність повторного використання спільних об’єктів, гарантуючи, що в разі, виділення об'єкту новому користувачу або процесу, він не міститиме інформації, яка залишилась від використання його попереднім користувачем або процесом. Політика повторного використання об’єктів, що реалізується захисним комплексом, стосується тільки тих об’єктів системи, що містять конфіденційну інформацію та ресурси яких розподіляються між користувачами та процесами, які виконуються в системі.

4) ЦД-1 - Довірча цілісність. Ця вимога задіюється для захисту інформації від несанкціонованої модифікації й дає змогу користувачам будь-якої категорії керувати інформаційними потоками в АС від інших користувачів до захищених об’єктів, що належать його домену. Реалізується такий підхід апаратними засобами контролю вторгнення за допомогою встановлення права доступу до

захищених об’єктів, які повинні задаватись при їх створенні чи ініціалізації. На етапі розробки потрібно чітко визначити та вказати, до якої інформації повинні мати доступ клієнтські додатки.

5) ЦВ-1 - Цілісність при обміні. Ця вимога забезпечує цілісність інформації з обмеженим доступом, яка передається по незахищеним каналам за межами інформаційної системи. Реалізується шляхом створення VPN-каналу.

6) ЦО-1 - Відкат. Ця послуга дає можливість відмінити окрему операцію або послідовність операцій й повернути захищений об’єкт, з яким маніпулював користувач, до попереднього стану.

7) ДР-1 - Використання ресурсів. Ця послуга дозволяє керувати використанням послуг та ресурсів користувачами. Адміністратор безпеки або уповноважений користувач встановлює обмеження на використання окремим користувачем або процесом обсягів обчислювальних ресурсів системи. Запити на зміну обмежень обробляються тільки в тому випадку, якщо вони надходять від адміністраторів.

8) ДВ-1 - Відновлення після збоїв. В політиці відновлення після збоїв повинна бути визначена й задокументована множина типів відмов і переривань обслуговування системи чи окремих її компонентів, після яких можливо повернутись у відомий захищений стан без порушення вимог політики безпеки. Для кожної з відмов необхідно чітко вказати рівні відмов, у разі перевищення яких необхідна повторна інсталяція системи.

9) НР-2 - Реєстрація/аудит. Вимога реєстрації дозволяє контролювати небезпечні дії для системи відносно об’єктів і процесів, що існують в системі і стосуються захищених об’єктів, зі сторони користувача будь-якої категорії. Адміністратор безпеки і уповноважені користувачі повинні мати у своєму розпорядженні засоби перегляду і аналізу журналу реєстрації, а ситема захисту повинна забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

10) НИ-2 - Ідентифікація та автентифікація. Вони дозволяють визначити й перевірити особу будь-якого користувача, що намагається отримати доступ до системи або до захищених об’єктів, та повинні гарантувати, що доступ може

бути надано тільки авторизованому користувачеві. Користувач отримує дозвіл на виконання будь-яких дій тільки після його автентифікації на підставі введеного пароля.

11) НК-1 - Достовірний канал. Ця вимога гарантує користувачеві будь-якої категорії можливість взаємодії безпосередньо з засобами захисту, а також те, що жодна взаємодія користувача з системою не може бути змінена іншим користувачем або процесом. Послуга має визначати перелік вимог до механізму встановлення надійного зв'язку між користувачем і захисним комплексом. Достовірний канал повинен використовуватись як для початкової ідентифікації, такі для автентифікації. Зв'язок, що використовує даний канал, повинен ініціюватись тільки користувачем.

12) НО-2 - Розподіл обов'язків. Дозволяє розмежувати повноваження користувачів через визначення категорій користувачів. Для кожної категорії визначені певні функції (ролі). Вимога направлена на зменшення потенційних збитків від навмисних або помилкових дій користувачів та на обмеження авторитарності керування системою.

13) НЦ-2 - Цілісність захисних засобів. Визначає межу здатності захисної системи захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. При цьому повинен бути визначений механізм для контролю цілісності елементів, що входять до складу захисних засобів. У випадку виявлення порушень цілісності одного із своїх компонентів КЗЗ повинен повідомити адміністратора безпеки або уповноваженого користувача та перевести систему до стану, при якому заборонена обробка конфіденційної інформації. Повернення системи до нормального функціонування можливе лише після відновлення відповідності компоненту КЗЗ еталону і тільки адміністратором безпеки або уповноваженим користувачем.

14) НТ-2 - Самотестування. Дає змогу засобам захисту виконати перевірку й на підставі неї гарантувати коректне функціонування та цілісність функцій системи, які забезпечені захистом. До складу засобів необхідно включити набір тестових процедур, що буде достатній для оцінки правильності виконання в системі всіх критичних функцій для забезпечення безпеки

конфіденційної та технологічної інформацій. При цьому сам КЗЗ повинен бути здатним контролювати виконання таких функцій. Тести мають виконуватися на етапі ініціалізації КЗЗ за ініціативи адміністратора безпеки або уповноважених користувачів. У випадку не коректного виконання одного із тестів засоби захисту повинні перевести систему в стан, при якому заборонена обробка конфіденційної інформації взагалі, або в стан, при якому заборонена обробка конфіденційної інформації з використанням послуг безпеки. Повернення системи до нормального стану функціонування можливе за умови відновлення працездатності КЗЗ і повторного виконання повного набору тестів.

15) НВ-1 - Автентифікація при обміні. Забезпечує автентифікацію обох сторін процесу обміну перед початком передаванням інформації з обмеженим доступом. Така дія реалізовується завдяки ПЗ, яке відповідає за створення VPN-каналу.

Для отримання необхідного рівня безпеки і для виконання критеріїв профілю захищеності в організації рекомендується використовувати апаратні засоби контролю вторгнення.

4.3 Вибір засобів контролю вторгнення

Системи для контролю вторгнень, що використовують в приватних підприємствах, можна розділити на дві категорії:

– апаратні засоби;

– програмне забезпечення.

Розглянемо кожну категорію окремо та оберемо засоби, на основі яких буде проведено аналіз ефективності.

4.3.1 Апаратний комплекс Stonegate IPS

Stonegate IPS – це апаратний комплекс, який забезпечує активний захист від вторгнень. В основі Stonegate IPS лежать різні методи виявлення вторгнень, а саме: технологія декодування протоколів, що не мають сигнатур; сигнатурний аналіз; аналіз аномалій протоколів; аналіз поведінки конкретних вузлів; виявлення статистичних відхилень у потоці даних; кореляційний аналіз подій, які відбуваються. Stonegate IPS поєднує режими IDS та IPS для різних сегментів

мережі, що дає змогу проводити контроль підмереж із застосуванням різноманітних політик безпеки. Для здійснення контролю на рівні VLAN існує можливість логічного поділу фізичного інтерфейсу на підрівні.

Рішення Stonegate IPS має велику кількість сертифікатів визнаних міжнародних організацій з інформаційної безпеки, таких як ICSA Labs і Common Criteria, та має сертифікат ISO.

4.3.2 Програмно-апаратний комплекс Snort

Snort – програмно-апаратний комплекс, що забезпечує активний захист від вторгнень. Цей комплекс здатний аналізувати потік даних у реальному масштабі часу та IP-пакети, що ввійшли в мережу.

Snort може аналізувати протоколи та використовуватись для виявлення різноманітних атак типу переповнення буферу, прихованого перегляду портів, CGI нападу, SMB нападу, визначення OS, та інших. Snort використовує гнучку систему правил для опису інформаційного потоку, який повинен бути пропущений або заблокований. Snort здатний реагувати на атаки в реальному масштабі часу, додаючи результати подій або в системний звіт syslog, або у файл, що визначений користувачем, або у вигляді WinPopup-повідомлення клієнтам Windows, які використовують Samba client.

4.3.3 Апаратний комплекс IBM ISS Proventia

IBM ISS Proventia – це апаратний комплекс, який забезпечує активний захист від вторгнень мережу. IBM ISS Proventia складається з аналізатора подій, який дозволяє обробляти інформацію з декількох сенсорів та виконувати кореляцію подій між ними. Система виявлення і запобігання вторгнень IBM ISS Proventia сконфігурована для виявлення розподілених в часі атак, специфічних атак, які використовують слабкі місця в поштових системах, систем ERP, для запобігання поширенню і використанню шкідливого ПЗ, витоку інформації з використанням пірінгових мереж та іншого. Містить унікальні механізми аналізу дій користувачів у мережі та аналізу аномальної активності.

IBM ISS Proventia має сертифікат ISO, сертифікацію проведено у ДССЗ та

ЗІ.

4.3.4 Програмна система Rule-based IDS

Rule-based IDS – це програмна система виявлення вторгнення, розроблена для сімейства ОС Linux. Вона має наступні можливості:

– виявлення і запобігання атак в реальному часі в прозорому для користувачів режимі (продуктивність одного пристрою більше 10 Гбіт/с);

– здійснення кластеризації та можливість плавного нарощування продуктивності;

– містить широкий список сигнатур атак (по змісту, по контексту мережевих пакетів та за іншими ознаками);

– можливість обробки фрагментованого мережного потоку даних;

– можливість виявлення спроб тунелювання трафіку, підтримка IPv6;

– інспекція всередині SSL/TLS;

– можливість боротьби з (D)DoS-атаками.

В таблиці 4.2 представлена характеристика проаналізованих апаратно-програмних засобів для контроля вторгнення в мережі приватних підприємств згідно з обраними критеріями.

Таблиця 4.2 – Таблиця апаратно-програмних засобів контрою вторгнення в корпоративні мережі

Назва	Реалізація	Продуктивність	Споживання ресурсів	Складність налаштування
Stonegate	Апаратна	170Mb/s	<5%	Середня
Snort	Програмна	95Mb/s	25%	Мала
IBM ISS Proventia	Апаратна	230Mb/s	<5%	Мала
Rule-based ID System	Програмна	75Mb/s	20%	Висока

Аналіз апаратних та програмних продуктів за ефективністю контролю вторгнення для інформаційно-телекомунікаційних систем комерційних підприємств показав, що самими ефективними виявились апаратні продукти. Це досягається тим, що вони практично не впливають на споживання ресурсів системи, оскільки є окремими засобами, що самостійно фільтрують мережний

потік даних. Наступні дослідження ефективності засобів контролю вторгнення будуть проводитись для апаратних засобів, які мають ряд переваг над програмними, а саме:

– простота розгортання і використання;

– розміри і енергоспоживання;

– продуктивність;

– надійність.

4.4 Аналіз ефективності апаратних засобів контролю вторгнення

Для здійснення оцінки ефективності апаратних засобів контролю вторгнення в корпоративні мережі необхідно визначити основні критерії оцінки.

За результатами першого етапу складається перелік засобів контролю вторгнення, у якому зазначаються усі продукти аналізованого типу і їх виробники. При наявності або відсутності сертифіката у засобах захисту в таблиці порівняння проставляється "1" або "0" відповідно.

На другому етапі для відбору засобів контролю вторгнення з попереднього переліку використовується факторний аналіз. У факторному аналізі використовуються вагомі характеристики засобів, ваговий коефіцієнт характеристики, ступінь відповідності продукту – опису характеристики. Перелік характеристик визначається на підставі всіх властивостей засобів захисту інформації, що пов’язані з функціональними та системними можливостями, з можливостями по керуванню і моніторингу. При цьому враховуються тільки такі властивості, для яких можна дати відповідь "є" або "немає", а також такі, для яких можна експертним шляхом вибрати значення з діапазону від 0 до 1. Ваговий коефіцієнт кожної окремої характеристики визначає, наскільки вона важлива для реалізації. Він може приймати такі значення: 1 – дуже важлива; 0,5 – важлива; 0 – не важлива.

Те, наскільки продукт відповідає необхідним системним можливостям або характеристикам, визначає ступінь відповідності продукту. В факторній таблиці позиції матриці заповнювались логічними значеннями «0» або «1»

відповідно при відсутності або наявності в системі можливості або якості, представленою характеристикою. Якщо ступінь відповідності характеристиці у різних засобів може бути оцінений, то застосовувалась градація значень параметра цієї характеристики, який може приймати значення від 0 до 1.

Кількісні показники, що включались у факторну таблицю, приводились до нормального вигляду. Показники характеристик, для яких найкращими є максимальні значення, обчислюються відповідно до формули 4.1:

$$П_n = \frac{C_n}{C_{\max}}, \tag{4.1}$$

де $П_n$ – нормований кількісний показник характеристики n-го засобу контролю вторгнення;

C_n – значення показника характеристики n-го засобу контролю вторгнення,

$C_{\max}$ – максимальне значення показника характеристики з усіх аналізованих засобів контролю вторгнення.

Показники характеристик, для яких найкращими є мінімальні значення, обчислювані за формулою 4.2:

$$П_n = 1 - \frac{C_n}{C_{\max}}, \tag{4.2}$$

де $П_n$ – нормований кількісний показник характеристики n-го засобу контролю вторгнення;

C_n – значення показника характеристики n-го засобу контролю вторгнення,

$C_{\max}$ – максимальне значення показника характеристики з усіх аналізованих засобів контролю вторгнення.

Наприклад, якщо вартість 1-го, 2-го, 3-го і 4-го засобів захисту інформації дорівнює відповідно 300, 350, 400 і 450 грн, то буде дорівнювати 450 грн, а

нормовані значення показників для всіх коштів: 1 – 0,4 = 0,6; 1 – 0,6 = 0,4; 1 – 0,8 = 0,2 і 1 – 1 = 0.

Після заповнення факторної таблиці проводиться оцінка і отримання значень показників ефективності захисту аналізованого типу.

Показник ефективності апаратних засобів контролю вторгнення розраховувався за формулою 4.3:

$$E_n = \frac{\sum_m Z_n X_m}{M}, \tag{4.3}$$

де E_n – показник ефективності n-го засобу контролю вторгнення;

Z_n – показник наявності властивості у n-го засобу контролю вторгнення, що приймає значення від 0 до 1;

X_n – ваговий коефіцієнт m-го властивості засобу контролю вторгнення, що приймає значення від 0 до 10;

n – порядковий номер (індекс) засобу контролю вторгнення у матриці факторної таблиці;

m – порядковий номер (індекс) характеристики властивості матриці факторної таблиці;

M – загальна кількість характеристик засобу контролю вторгнення.

4.5 Практичне застосування IBM ISS

Розглянемо апаратний засіб IBM ISS, який являє собою систему запобігання вторгнень (IPS) і мережну систему виявлення атак (IDS) з відкритим вихідним кодом, що здатна виконувати реєстрацію пакетів у реальному часі та здійснювати аналіз потоків даних в мережах.

IBM ISS здійснює протоколювання, пошук по вмісту, аналіз, а також широко застосовується для активного блокування або пасивного виявлення атак і зондувань, таких як переповнення буфера, стелс-сканування портів, атаки на веб-додатки, SMB-зондування і спроби визначення ОС. Програмне забезпечення в основному використовується для запобігання проникнень та

блокування атак, якщо вони є.

4.5.1 Загальний принцип функціонування IBM ISS

Система виявлення вторгнень IBM ISS може виступати в якості як вузлової, так і мережної системи за способом моніторингу, в залежності від параметрів установки. В основному вона захищає визначений сегмент локальної мережі від зовнішніх атак. На рисунку 4.1. подано схему мережі із встановленою IBM ISS в ній. Система виявлення атак, виділена червоним прямокутником, працює як вузлова, інша – як мережна. Припустимо, що хтось відправляє пакет через мережу Інтернет. Після цього пакет потрапляє на маршрутизатор і далі передається в потрібну підмережу. Пройшовши через маршрутизатор, пакет пропускається чи блокується міжмережним екраном. Міжмережний екран – це комплекс апаратних і програмних засобів, який здійснює контроль і фільтрацію пакетів, що проходять через нього, у відповідності із заданими правилами. Тут необхідно зауважити, що міжмережний екран, зазвичай, поєднується із функціями маршрутизатора, але також вони можуть співіснувати як окремі пристрої.

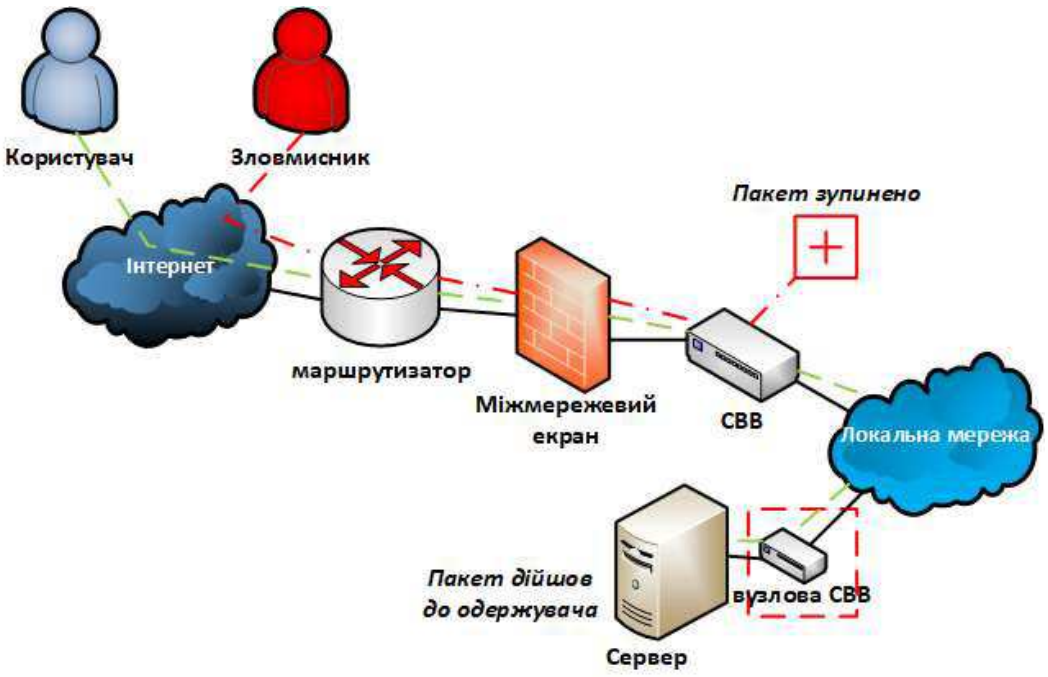


Рисунок 4.1 – Мережа із встановленою IBM ISS

Після цього пакет потрапляє на комп'ютер із ситемою IBM ISS, яка

контролює підмережу. IBM ISS переглядає, чи не підпадає пакет під якесь із правил, що існує в її базі. Якщо такого правила не існує, то пакет передається далі адресату, в іншому випадку IBM ISS передає на міжмережний екран відповідні команди. Команди можуть бути двох видів: система дозволяє передавати пакет отримувачу; система забороняє передавати пакет отримувачу.

Існує також і інший підхід, при якому мережні пакети з Інтернету потрапляють спочатку на міжмережний екран, а вже потім до системи виявлення вторгнень.

При роботі IBM ISS в якості вузлової системи виявлення втргнень вона буде захищати лише один вузол. Для цього вона повинна мати відповідні налаштування.

4.5.2 Архітектура IBM ISS

Розглянемо функціональні блоки, з яких складається IBM ISS. На рисунку 4.2 зображено компоненти, які входять до складу IBM ISS.

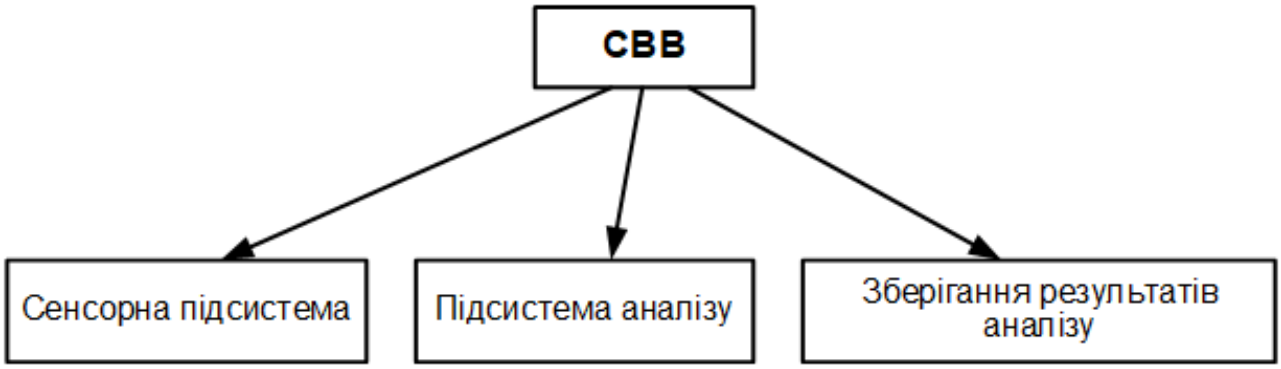


Рисунок 4.2 – Підсистеми IBM ISS

Сенсорна підсистема – це підсистема, яка займається збором подій, що пов’язані з безпекою системи.

Підсистема аналізу – це підсистема, що використвується для виявлення атак та підозрілих дій, що грунтуються на основі даних сенсорної підсистеми.

Підсистема зберігання результатів аналізу – це підсистема, яка забезпечує накопичення подій і результатів аналізу.

Система IBM ISS містить в своєму складі сніфер пакетів, який перехоплює всі пакети в підмережі. На рисунку 4.3 зображено принцип

проходження даних через IBM ISS, які отримані сніфером.

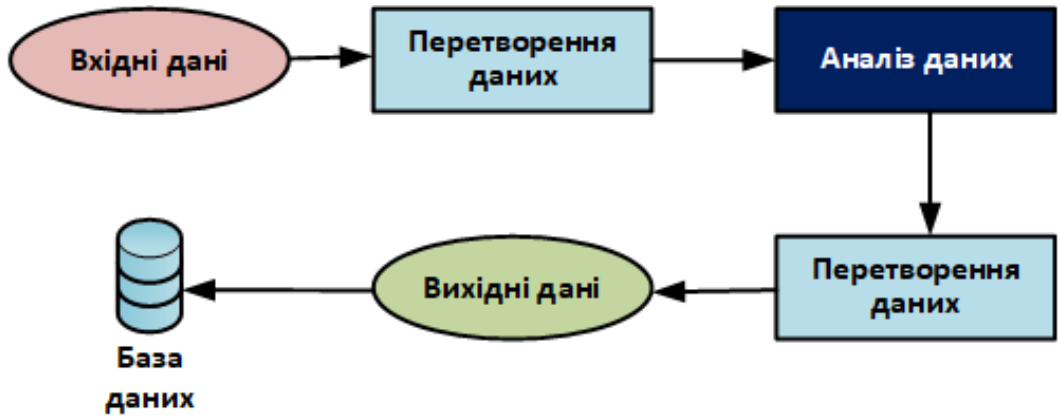


Рисунок 4.3 – Проходження даних через IBM ISS

Проходження даних через IBM ISS відбується наступним чином:

1) здійснюється перетворення даних до придатного для аналізу вигляду. Це перетворення виконується за допомогою декодера;

2) проводиться аналіз даних за допомогою відповідних блоків програми;

3) відбувається перетворення одержаних результатів до прийнятного для людини вигляду;

4) зберігаються вихідні дані у базі даних.

4.5.3 Проведення експериментів

Для проведення експерименту по застосуванню системи IBM ISS нам необхідно кілька комп’ютерів, що об’єднані у мережу. Ключовою особливістю є те, що необхідно мати одночасний доступ до декількох комп'ютерів із цієї мережі. Для цього було прийнято рішення земулювати віртуальну обчислювальну мережу.

На сучасному ринку безліч програмних продуктів, створених спеціально для вирішення подібних завдань. Лідерами серед компаній, що займаються розробкою продуктів віртуалізації, є VMware, Parallels, Sun Microsystems. За допомогою даних програм можна земулювати обладнання реального комп’ютера. Створена в цьому середовищі машина називається віртуальною машиною. Віртуальна машина захоплює не всі ресурси комп’ютера відразу, користувач може самостійно їх обмежувати. Наприклад, при створенні

віртуальної машини користувач вказує об’єм оперативної пам’яті, відео-пам’яті та жорсткого диска. На створений віртуальний комп’ютер можна встановити будь-яке програмне забезпечення і працювати з ним зі своєї базової операційної системи.

Для моделювання комп’ютерної мережі було розроблено декілька віртуальних машин, на них встановлено операційні системи та проведено об’єднання віртуальних комп’ютерів у локальну мережу.

Структура експериментальної комп’ютерної мережі наведена на рисунку. 4.4. Три комп’ютери з’єднані між собою та розташовані в одній підмережі. Через хост-машину вони також мають доступ в Інтернет.

Рисунок 4.4 – Структура експериментальної комп’ютерної мережі

4.5.4 Режими запуску IBM IS

IBM ISS може бути запущений в чотирьох режимах:

1) сніфер – просто читає пакети з мережі і відображає їх на екрані у вигляді потоку даних в консолі. Для запуску цього режиму застосовуються команди:

./isort -v – на екран виводяться тільки IP і TCP/UDP/ICMP заголовки пакетів, які програма перехопила в мережі;

./isort -vd – на відміну від попереднього випадку ключ d забезпечує виведення на екран пакетних даних;

./isort -dev – ключ е забезпечує додатковий вивід даних на канальному рівні.

2) пакетне журналювання – відбувається читання пакетів з мережі і їх запис на диск у лог-файл. Відрізняється від режиму "сніфер" тільки тим, що виведення даних здійснюється не на екран, а у файл. Запуск IBM ISS у цьому режимі виконується аналогічно, як і в режимі "сніфер", але з додаванням ключа -l, після якого необхідно вказати шлях до каталогу, де будуть зберігатися лог-файли. Якщо ж зазначеного каталогу не існує, то запуск програми буде завершено з помилкою. Нижче наведено приклад:

./isort -dev -l /usr/local/var/logs/isort;

./isort -dev -l /home/user/logs -h 192.168.1.0/24

./isort -l /home/user/logs -b – запис даних в бінарний лог-файл;

./isort -dv -r packet.log – читання бінарного файлу для подальшого аналізу.

3) мережна система виявлення вторгнень – IBM ISS аналізує мережний потік даних і виконує певні дії, в залежності від виду атак.

./isort -dev -c /usr/local/etc/snort/snort.conf

4) inline – режим роботи спільно з міжмережним екраном iptables. Для того, щоб запустити в цьому режимі, необхідно додати додатковий ключ Q:

./isort -GDc ../etc/drop.conf -l /var/log/isort

Перед запуском у цьому режимі необхідно впевнитись, що програму було встановлено з підтримкою такого режиму. Після цього необхідно налаштувати міжмережний екран для взаємодії з IBM ISS.

4.5.5 Конфігурування системи виявлення вторгнень IBM ISS

Три типи змінних можуть бути визначені в СВВ IBM ISS: var; portvar; ipvar. Дані ключові слова призначені для присвоєння зазначеним нами змінним значень. Синтаксис у них однаковий, відмінність полягає в тому, що var/portvar/ipvar використовуються для різних типів даних:

<var | portvar | ipvar> <назва_змінної> <значення_змінної>

Слово var використовується для присвоєння змінній шляху до файлу або каталогу та для призначення змінній IP-адреси. Ключове слово ipvar

застосовується до змінних для визначення IP-адрес, але тільки з підтримкою IPv6. Ключове слово portvar використовується для задання змінних з номерами портів. Наведемо фрагмент файлу конфігурації snort.conf.

var RULE_PATH /usr/local/etc/isort/rules – зазначення розташування директорії з правилами.

var HOME_NET [192.168.1.0/24,!192.168.1.23] – зазначення діапазону IP-адрес, які будемо захищати. При цьому виключено одну IP-адресу. Якщо вказати IP-адресу своєї машини, тоді IBM ISS буде використовуватись як вузлова система.

var EXTERNAL_NET any – вибір IP-адрес, від яких будемо захищати мережу. В даному випадку від усіх адрес.

portvar_HTTP_PORTS [80,2301,3128,7777,7779,8000,8008,8028, 8080,8180,8888,9999]

portvar FTP_PORTS 21

portvar SMB_PORTS [139,445]

portvar SSH_PORTS 22

У попередніх чотирьох прикладах визначаємо порти. Тут теж може використовуватись заперечення, як і у випадку з IP-адресами. Для вказівки послідовності портів, запис виглядає так: [12:17,1024:].

За допомогою ключового слова include можна підключати додаткові файли з налаштуваннями. В даному випадку ми підключили кілька правил:

include $RULE_PATH/ftp.rules

include $RULE_PATH/ssh.rules

Правила складаються з заголовка і опціонального поля. Опції розміщені в круглих дужках. Загальний синтаксис таких правил:

<дія_програми> <протокол> <ip-адреси> <порт> <напрям дії правила> <ip-адреси> <порт> (опції).

До дій програми належить:

1) alert – вивести відповідне повідомлення, а потім записати дані пакета в лог-файл;

2) log – просто записати дані пакета в лог-файл;

3) pass – ігнорувати пакет.

Протоколи з якими працює IBM ISS

1) tcp;

2) udp;

3) icmp;

4) ip.

У полі IP-адреси можуть зазначатись як діапазон IP-адрес, так і окремі адреси. В полі порт можна вказати будь-який порт в діапазоні від 1 до 65535.

Напрямки дії правила можуть бути двох видів:

1) В одну сторону, позначається "->".

2) В обидві сторони, позначається "<>".

4.5.6 Сигнатурні правила

Визначення атак по сигнатурах досить відома практика. У перших версіях IBM ISS тільки за цим принципом і визначались атаки. Розглянемо як працює таке виявлення. Візьмемо будь-який файл, наприклад sunset.jpg і відкриємо його у шістнадцятковому редакторі (рисунок 4.5).

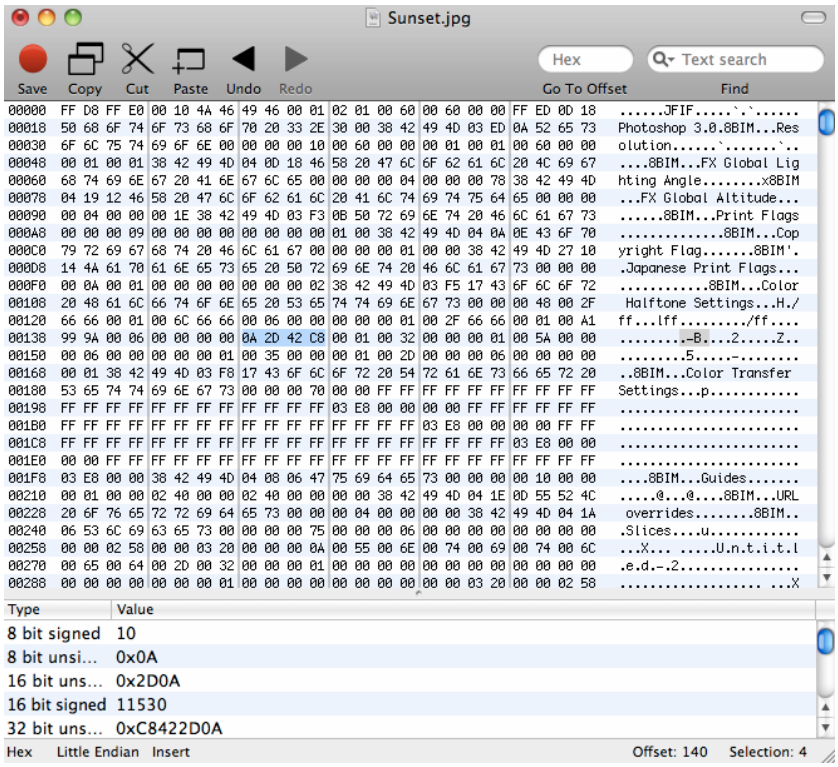


Рисунок 4.5 – Шістнадцятковий редактор

В цей файл у будь-яке місце вставимо нашу сигнатуру, на малюнку вона виділена і являє собою 4-байтову послідовність: 0A 2D 42 C8.

Напишемо своє правило: IBM ISS всі файли з такою сигнатурою перехоплював і зберігав відповідне попередження. Правило буде виглядати так:

alert tcp any any -> $HOME_NET $SMB (msg:"SMB attack!";

content: "|0A 2D 42 C8|"; sid: 1000004; rev:2;).

Дане правило додамо в файл local.rules, який знаходиться в директорії з різними правилами.

Потім по протоколу SMB відправляємо наш модифікований файл sunset.jpg. У результаті система видає нам повідомлення, яке показано на рисунку 4.6.

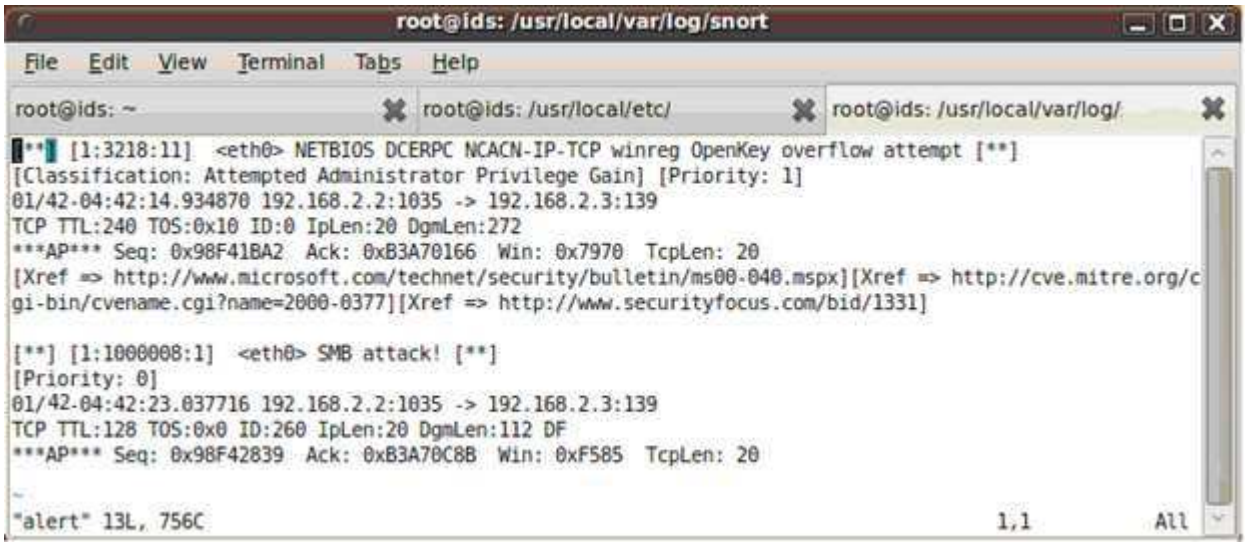


Рисунок 4.6 – Відповідні дії системи на модифікований файл

З цього випливає висновок, що IBM ISS із легкістю виявляє сигнатури у файлах. Так, у будь-який файл зловмисник може вмонтувати свій шкідливий код і передавати його, а користувачі ні про що не підозрюють.

4.5.7 Аномальні правила

Розглянемо одне з існуючих аномальних правил. Припустимо, що зловмисник вирішив виявити вразливість комп’ютерів мережі шляхом сканування їх портів. Популярною утилітою з такими можливостями є Nmap.

Вона призначена для сканування IP-мереж із будь-якою кількістю об’єктів. Nmap використовує безліч різних методів сканування. Для перевірки працездатності системи виявлення вторгнень скористаємось цим програмним засобом. Проскануємо комп’ютер із IP-адресою 192.168.2.3 FIN методом. Для цього введемо команду nmap -sF 192.168.2.3 (рисунок 4.7).

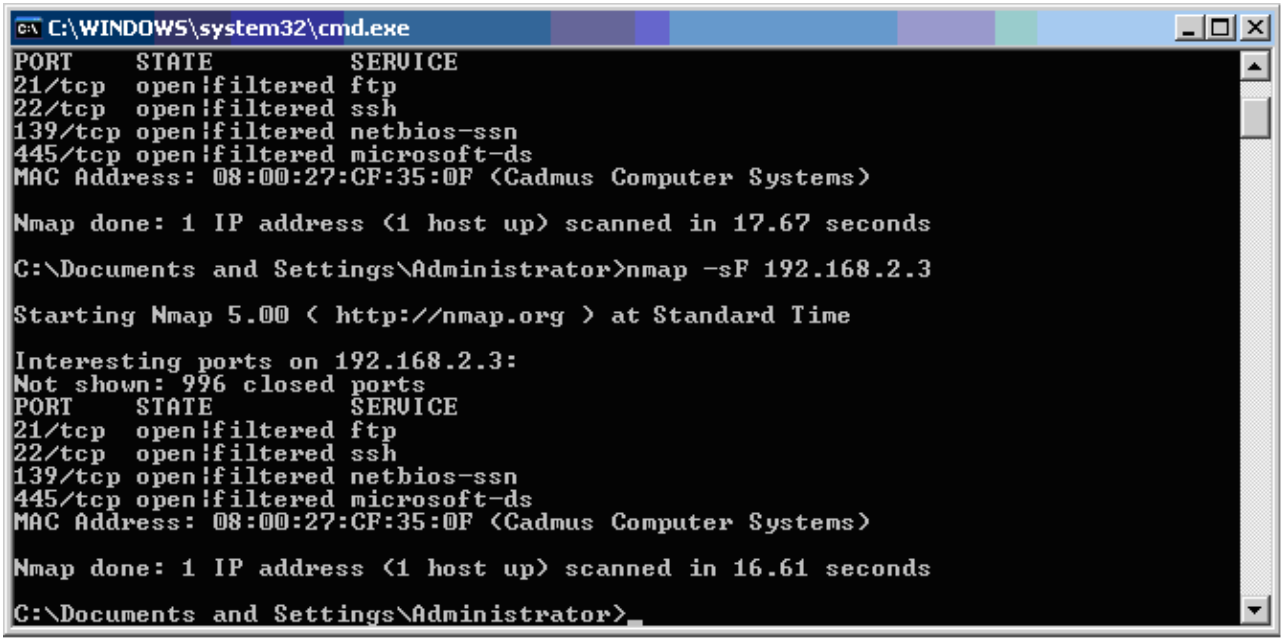


Рисунок. 4.7 – Сканування портів за допомогою nmap 5.0

Після проведених дій звернемось до комп’ютера, що сканувався, і перевіримо, чи виявила IBM ISS "неправильну" активність з боку іншого комп’ютера. Після перегляду файлу alert з попередженнями (рисунок 4.8) бачимо, що було зафіксувоно сканування портів із зазначенням IP-адреси машини. Також у цьому файлі вказана адреса в інтернет із докладним описом атаки. Правила, що відповідають за виявлення атак, пов’язаних зі скануванням портів, зберігаються у файлі scan.rules.

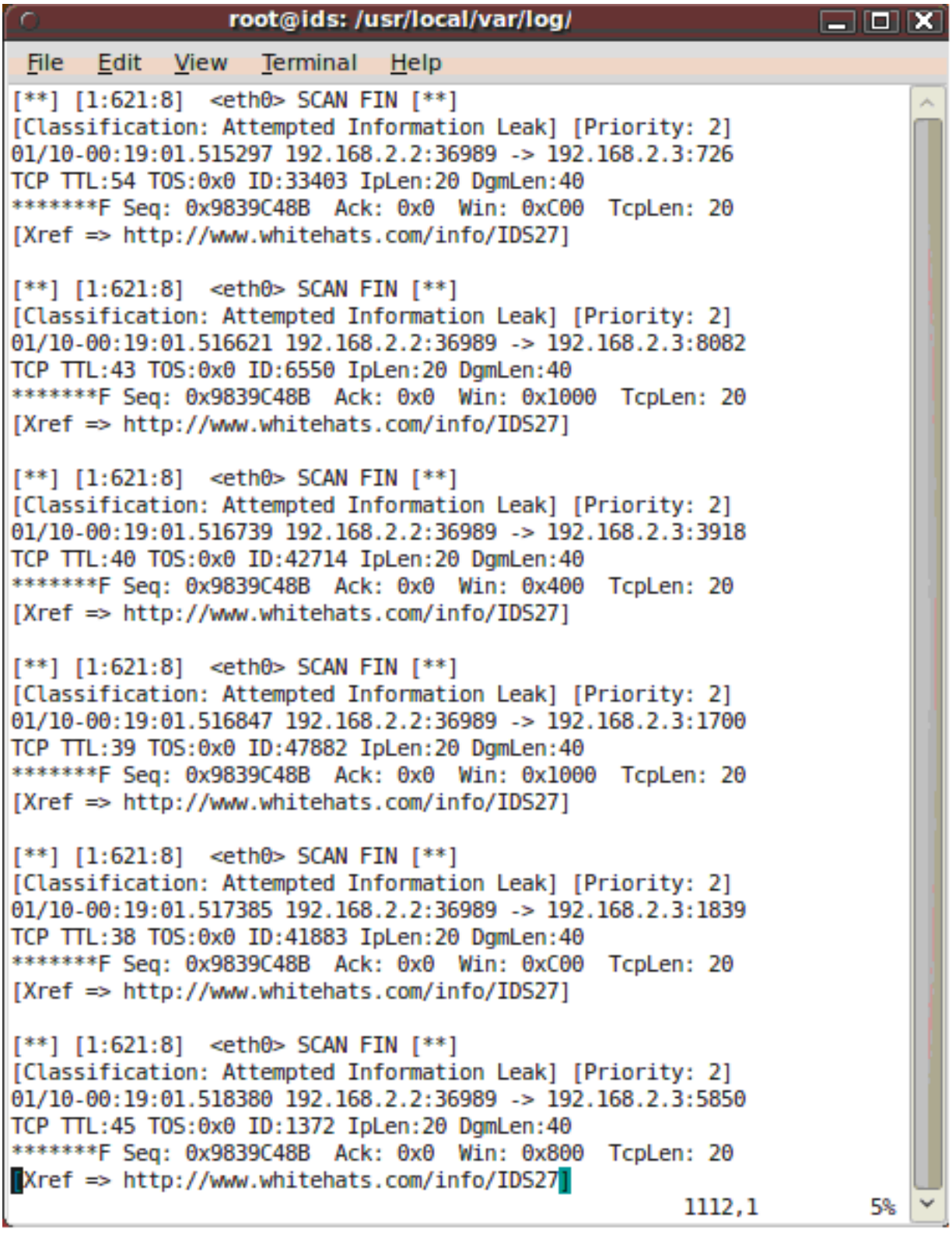


Рисунок 4.8 – Відповідні дії СВВ на сканування портів

4.6 Висновки

У розділі були наведені методи оцінки загроз безпеці інформації, проведено аналіз інформаційних загроз підприємства, на основі якого був проведений вибір засобів контролю вторгнення та проведений аналіз

ефективності апаратних засобів контролю вторгнення для корпоративних мереж. Грунтуючись на отриманих результатах, було приведено практичне застосування апаратного засобу контролю вторгнення IBM ISS, який є системою запобігання вторгнень (IPS) і мережевою системою виявлення вторгнень (IDS) з відкритим вихідним кодом, здатною виконувати реєстрацію пакетів у реальному часі та здійснювати аналіз потоку даних в корпоративних мережах.

ВИСНОВКИ

Проведено аналіз існуючих систем виявлення вторгнень IPS/IDS. Виявлено, що системи використовують сигнатурний принцип аналізу трафіку.

Розглянуто компоненти, що забезпечують ефективну роботу комп'ютерної мережі, підтримують постійну доступність і високу надійність мережі, а також обґрунтовано необхідність в системах моніторингу та керування.

Запропоновано вирішення проблеми захисту інфраструктури корпоративної мережі за допомогою використання IDPS систем.

Виявлено, що IDPS система може виконувати всебічний аналіз мережевого трафіку (рівень 7 моделі OSI) при розгортанні центрів обробки даних на рівні ядра корпоративної мережі або на межі підключення до Інтернету.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 4-е изд. / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2010. – 944 с.: ил.

2. Спортак М. Компьютерные сети и технологии / М. Спортак, Ф. Паппас и др.: Пер. с англ. – К.: ООО «ТИД», 2002. – 736 с.

3. Биячуев Т.А. Безопасность корпоративных сетей / Т.А. Биячуев, под ред. Л.Г. Осовецкого. – СПб.: СПб ГУ ИТМО, 2004. – 161 с.

4. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – Саратов: Профобразование, 2017. – 702 с.

5. Корячко В.П. Корпоративные сети: технологии, протоколы, алгоритмы / В.П. Корячко, Д.А. Перепелкин. – М.: Гор. линия-Телеком, 2013. – 219 с.

6. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК Пресс, 2002. – 656 с.

7. Методи аналізу та моделювання безпеки розподілених інформаційних систем: навч. посіб. / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. – Чернігів: Чернігівський національний технологічний університет, 2016. – 254 с.

8. Горев А.И., Симаков А.А. Обеспечение Информационной Безопасности / А.И. Горев, А.А. Симаков. – М.: ИЛ, 2016. – 494 с.

9. Taqqu M., Willinger W., Sherman R. Proof of a fundamental result in self–similar traffic modeling / M. Taqqu, W. Willinger, R. Sherman // Computer Communication Review. – 1997. – Vol. 27(2). – p. 5 – 23.

10. Leland W., Taqqu M., Willinger W., Wilson D. On the self–similar nature of Ethernet traffic / W. Leland, M. Taqqu, W. Willinger, D. Wilson // IEEE/ACM Transactions on Networking. – 1994. – Vol. 2(1). – p. 1 – 15.

11. Paxon V., Floyd S. Wide-area traffic: The failure of Poisson modeling. / V. Paxon, S. Floyd // IEEE/ACM Transactions on Networking. – 1995. – Vol. 3. – p. 226 – 244.

12. Feldmann A., Gilbert A.C., Willinger W. Data Networks as Cascades:

Investigating the multifractal nature of Internet WAN traffic. / A. Feldmann, A.C. Gilbert, W. Willinger // ACM SIGCOM. – 1998. – p. 42 – 55.

13. Шелухин О.И., Тенякишев А.М., Осин А.В. Фрактальные процессы в телекоммуникациях / О.И. Шелухин, А.М. Тенякишев, А.В. Осин. – М.: Радиотехника, 2003. – 480 с.

14. Шелухин О.И., Осин А.В., Смольский С.М. Самоподобие и фракталы. Телекоммуникационные приложения / О.И. Шелухин, А.В. Осин, С.М. Смольский. – М.: ФИЗМАТЛИТ, 2008. – 368 с.

15. Цыбаков Б.С. Модель телетрафика на основе самоподобного случайного процесса / Б.С. Цыбаков // Радиотехника. – 1999. – Вып. 5. – С. 24 – 31.

16. Петров В.В. Структура телетрафика и алгоритм обеспечения качества обслуживания при влиянии эффекта самоподобия: автореф. дис. канд. тех. наук / Петров В.В. – М., 2004. – 19 с.

17. Ложковский А.Г. Модель мультисервисного трафика и метод расчета параметров QoS при его обслуживании / А.Г. Ложковский // Радиотехника. – 2009. – Вып. 157. – С. 48 – 52.

18. Добровольский Е.В., Нечипорук О.Л. Имитационное моделирование источников нагрузки в сетях передачи данных с коммутацией пакетов / Е.В. Добровольский, О.Л. Нечипорук // Наукові праці ОНАЗ ім. О.С. Попова. – 2000. – № 3. – С. 19 – 23.

19. Добровольский Е.В., Нечипорук О.Л. Моделирование сетевого трафика с использованием контекстных методов / Е.В. Добровольский, О.Л. Нечипорук // Наукові праці ОНАЗ ім. О.С. Попова. – 2005. – № 1. – С. 24 – 32.

20. Росляков А.В., Криштофович А.Ю. Математическое описание автомодельного трафика / А.В. Росляков, А.Ю. Криштофович // 4-я Международная конференция DSPA. – 2002. – С. 25 – 31.

21. Маркин Ю.В., Падарян В.А., Тихонов А.Ю.. Программная инфраструктура для глубокого анализа сетевого трафика. / Ю.В. Маркин, В.А. Падарян, А.Ю. Тихонов // Материалы 24-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». –

Санкт-Петербург, 29 июня – 02 июля 2015. – С. 87 – 89.

22. Шелухин О.И., Сакалема Д.Ж., Филипова А.С. Обнаружение вторжении в компьютерные сети. Сетевые аномалии / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филипова. – М.: Горячая линия-телеком, 2013. – 220 с.

23. Галицкий, А.В. Защита информации в сети – анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – М.: ДМК Пресс, 2016. – 615 с.

24. Нестеренко В.А. Статистические методы обнаружения нарушений безопасности в сети / В.А. Нестеренко // Информационные процессы. – 2006. – № 3. – С. 208 – 217.

25. Зоріна Т.І. Системи виявлення і запобігання атак в комп'ютерних мережах / Т.І. Зоріна // Вісник східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15 (204) ч.1. – С. 48 – 54.

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

27. Запечников С.В. Информационная безопасность открытых систем: учебник для вузов. В 2-х томах / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М., 2008. – Т. II: Средства защиты в сетях. – 558 с.

28. Обзор систем обнаружения вторжений [Інтернет-ресурс]. Режим доступу: http://www.connect.ru вільний.

29. Субач І.Ю., Фесьоха В.В. Модель виявлення аномалій в інформаційно – телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу / І.Ю. Субач, В.В. Фесьоха // Збірник наукових праць ВІТІ. – 2017. – № 3. – С. 21 – 24.

30. Бондарев В. В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства: учебное пособие / В. В. Бондарев. – М.: Издательство МГТУ им. Н. Э. Баумана, 2017. – 225 с.

31. Уилсон Э., Мониторинг и анализ сетей. Методы выявления неисправностей / Э. Уилсон. – М.: Лори, 2002. – 350 с.

32. TCPDUMP/LIBPCAP public repository [Інтернет-ресурс] / Web-сайт: tcpdump; Режим доступу http://www.tcpdump.org, вільний.

33. Snort [Інтернет-ресурс] / Web-сайт: snort; Режим доступу http://www.snort.org, вільний.

34. Wireshark [Інтернет-ресурс] / Web-сайт: wireshark; Режим доступу http://www.wireshark.org, вільний.

35. Лукацкий А. В. Предотвращение сетевых атак: технологи и решения / А. В. Лукацкий. – СПб.: Экспресс Электроника, 2006. – 268 с.

36. Норткат С., Новак Д., Обнаружение арушений безопасности в сетях, 3-е изд. / С. Норткат, Д. Новак. – М.: Лори, 2003. – 447 с.

37. Информационная безопасиость [Інтернет-ресурс]. – Режим доступу: http://www.data.com/lab_tests/intrusion.html, вільний.

38. Критерии сравнения систем обнаружения атак [Інтернет-ресурс]. – Режим доступу: http://inf-bez.ru/?p=480, вільний.

39. Критерии сравнения методов обнаружения атак [Інтернет-ресурс]. – Режим доступу: http://inf-bez.ru/7ps478, вільний.

40. Ленков С. В. Методы и средства защиты информации: в 2 т. / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко, под ред. В. А. Хорошко. – К.: Арый, 2008. – Т.2: Информационная безопасность. – 344 с.

41. Анализаторы сетевых протоколов [Інтернет-ресурс]. – Режим доступу: http://www.osp.ru/win2000/2004/06/177125, вільний.

42. Шиндер Д. Основы компьютерных сетей [пер. с англ.] / Д. Шиндер – М.: изд. дом “Вильямс”, 2002. – 656 с.

ДОДАТОК А

(обов'язковий)

Копії публікацій

АНАЛІЗ ЕФЕКТИВНОСТІ ІНСТРУМЕНТІВ ВИЯВЛЕННЯ І ЗАПОБІГАННЯ ВТОРГНЕННЯ НА ВУЗЛИ В КОРПОРАТИВНІЙ МЕРЕЖІ

Романюк Костянтин Ігорович,

студент групи КІ1м-20-1.,

Науковий керівник: Андрощук О.С.

д.т.н, професор,професор кафедри кібербезпеки ХНУ

Критичне порівняння проводиться між системами виявлення та запобігання вторгненням Suricata та Snort [1,4].

Показниками, що використовуються для вимірювання ефективності систем є: швидкість виявлення атак, помилкові спрацьовування [2].

Для кількісної оцінки метрик, що використовуються для оцінки точності системи виявлення та запобігання вторгненню, можна використати наступні: охоплення (кількість атак, які можна виявити), ймовірність помилкових спрацьовувань, ймовірність виявлення резистивних атак, здатність обслуговувати канал з високою пропускною здатністю і ємністю [2]. Що стосується продуктивності, вона має ряд компонентів, і тому не є метрикою. У табл. 1 наведено деякі показники, що відображають ємність.

Таблиця 1

Оцінка потенціалу

Показник, що перевіряється	Використання ресурсів
Пакстів в ескунду	Цикли CPU, пропускна здатність інтерфейсів, пропускна здатність шини
Байт в секунду (середній розмір пакета)	Цикли CPU, пропускна здатність інтерфейсів, пропускна здатність шини
Протоколи	Цикли CPU і пропускна здатність шини
Кількість унікальних хостів	Розмір пам'яті, цикли CPU, пропускна здатність шини
Кількість нових з'єднань в секунду	Цикли CPU і пропускна здатність шини
Кількість одночасних з'єднань	Розмір пам'яті, цикли CPU, пропускна здатність шини
Попередження в секунду	Розмір пам'яті, цикли CPU, пропускна здатність шини

Необхідно реєструвати такі показники: байти в секунду, пакети в секунду та кількість мережевих атак. Крім того, для кожної системи виявлення та

запобігання вторгненню в мережу зменшено кількість втрачених пакетів, також були записані фактичні тригери, помилкові спрацьовування, негативні тригери та загальна кількість тривог. Нарешті, хост відстежує використання центрального процесора та пам'яті, постійне зберігання, пропускну здатність інтерфейсу та статистику файлів підкачки.

Тестовий стенд налаштований у віртуальному середовищі, що сприяє мобільності та безпеці експерименту. Це було необхідно для частого повторення та реконфігурації експериментальних випробувань.

VMware Workstation 15 була використана як платформа для віртуалізації, багато в чому завдяки хорошій продуктивності вводу-виводу та жорсткого диска порівняно з іншими засобами віртуалізації. В якості операційної системи було обрано 32-розрядну Ubuntu 18.04 LTS. Ubuntu регулярно оновлюється і має хорошу базу спільнот. Це також найпопулярніша операційна система Linux.

За замовчуванням апаратна конфігурація для системи виявлення та запобігання вторгнень в мережу становила 2,8 ГГц чотирьохядерним процесором Intel Xeon (E5462) з 4-ядерною 3 ГБ DDR2 800 МГц повністю буферованою пам'яттю. Кожна система також мала максимальний об’єм жорсткого диска 20 ГБ. Мережевий трафік передавався окремо для кожної системи. Система, що використовується для відтворення мережевого трафіку, використовує одне ядро та 1 Гб оперативної пам'яті. VMware хост операційної системи, що використовує 2 Гб оперативної пам'яті і 1 ядро, що перешкоджає хосту з якого виробляє на випробувальному стенді.

Snort і Suricata були налаштовані на роботу з однаковими правилами. Suricata використовує різні класифікації конфігурації Snort, яка використовує 134 декодери та 174 правила препроцесора. Ідентичні методи реєстрації, які називаються Barnyard, MySQL та AcidBase, використовувались як для систем виявлення вторгнень в мережі, так і для систем запобігання. Версії Snort та Suricata були v2.9.8.3 та v4.1.2 відповідно.

Обидві системи використовували набір правил VRT Snort v2.9.8.3 у поєднанні з набором правил для нових загроз.

Для тестування було використано реальний мережевий трафік у фоновому режимі [3]. Однак повторення експериментів із трафіком у реальному часі було б непередбачуваним через його динаміку. Було обрано використання трафіку, захопленого з файлу pcap. Це сприяло їх обробці системою виявлення та попередження вторгнення мережі в автономному режимі, дозволяючи відтворювати в мережі з різною швидкістю, використовуючи TCPReplay. Крім того, усунуто всі ризики для критично важливих мереж. Використовуваний трафік було зафіксовано для запуску атак Metasploit на комп'ютері під керуванням Microsoft Windows 2000. Windows 2000 було обрано як найбільш підходящий Metasploit для цієї операційної системи порівняно з іншими.

Атаки, перелічені в таблиці 2, реєструються за допомогою Wireshark [5]. Частина програми Wireshark, Edicap, була використана для зміни часової позначки використовуваного трафіку та співвіднесення її з трафіком у фоновому режимі. У цій дії вони були об'єднані в хронологічному порядку, щоб атакуючий трафік перемістився на другий план.

Таблиця 3.4

Вивчення атак

Код	Ім'я	Опис
ms03_026_dcom	Microsoft RPCDCOM Interface Overflow	Модуль використовуваного стеку переповнення буфера в службі RPCSS
ms05_039_pnp	Microsoft Server Service NetpwPathCanonicalize Overflow	Стек переповнення буфера в службі Windows Plug and Play
ms05_047_pnp	Microsoft Plug and Play Service Registry Overflow	Стек переповнення буфера в службі Windows PnP. Причина перезавантажень.
ms06_040_netapi	Microsoft Server Service NetpwPathCanonicalize Overflow	Стек переповнення буфера в NetApi32 CanonicalizePathName () використовуючи функцію NetpwPathCanonicalize RPC виклик служби Server
ms05_017_msmq	Microsoft Message Queueing Service Path Overflow	Використовуваний стек переповнення буфера в RPC інтерфейсі в службі Microsoft Message Queueing
ms01_033_idq	Microsoft IIS5.0 IDQ Path Overflow	Використовуваний стек переповнення буфера в IDQ ISAPI обслуговування для Microsoft Index Server

Відстежувались такі ресурси: використання центрального процесора,

використання пам’яті, опір пропускної здатності пам'яті та пропускна здатність мережі. Це було зроблено за допомогою інструмента командного рядка Linux dstat.

Кожного разу, коли запускалося тестування, реєструвались початок і кінець трафіку запуску NIDPS. Трафік проходив через хости 192.168.16.2 та 192.168.16.128, але був позначений як небажаний трафік.

Для визначення точності використаний контроль попереджень. Ці попередження, отримані без системи стресів, використовувались як еталон. Відхилення від базової лінії в умовах стресу показувало зміни в точності виявлення. У табл. 3 наведено кількість типів попередження, що генеруються під час нападу на кожну NIDPS. На рис. 1 показані попередження Suricata на кожен експлоїт у всіх конфігураціях, але деякі попередження втрачені, що призводить до зменшення діапазону виявлення.

Таблиця 3.5

Попередження згенеровані Snort і Suricata

Попередження	Snort	Suricata
ms05_040_pnp	4	4
ms05_047_pnp	1	1
ms05_039_pnp	1	6
ms03_026_dcom	1	2
ms01_033_1dq	2	4
ms05_017_msmq	2	3

На рис. 2 показано провальні попередження Snort на ms01_033_idq. Ці помилкові негативні результати обумовлені надмірним навантаженням.

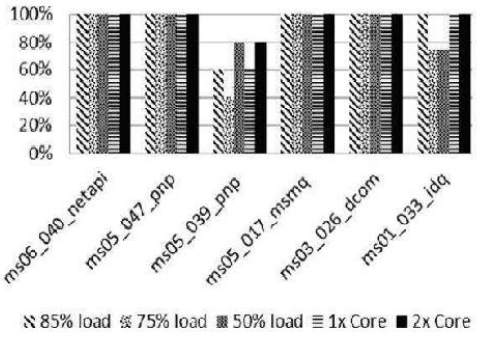


Рис 1 – Попередження у Suricata

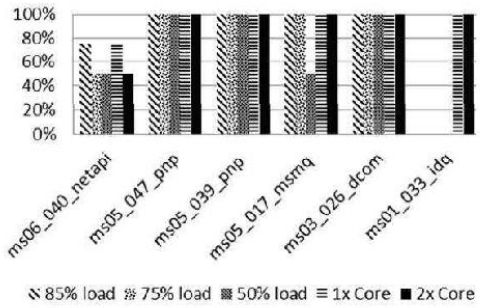


Рис 2 – Попередження у Snort

У Suricata спостерігається більша точність, ніж у Snort Частково це пов'язано з тим, що Snort менше контролює функціонування оповіщень під час атаки, ніж Suricata (два проти чотирьох). Snort не зміг попередити ms01_033_idq двома правилами з набору правил VRT, ідентифікаторами 1245 та 1244. Suricata був успішним, і ці сповіщення спрацьовували.

Suricata має високі вимоги до обробки, саме тому він досягає більших експлуатаційних можливостей, ніж Snort. Snort має набагато нижчі системні вимоги, тому він не може працювати з втратою пакетів при максимальному навантаженні системи. При роботі в багатоядерній конфігурації Suricata показує менше втрат пакетів, ніж Snort. Suricata використовує наявні ядра більш рівномірно. Тести в автономному режимі показують, що Suricata набагато повільніша за Snort. Хоча Suricata використовує багатоядерну систему більш чітко, ніж Snort. З огляду на це, можна сказати, що Suricata має кращу масштабованість. Однак, якщо Snort отримує хороші результати пропускної здатності, рекомендується запускати кілька екземплярів Snort на декількох ядрах. Це може запропонувати таку ж масштабованість, як Suricata, але з додатковими витратами на обробку однопотокових додатків на декількох ядрах.

Список використаних джерел

1. Обзор систем обнаружения вторжений [Інтернет-ресурс]. Режим доступу: http://www.connect.ru вільний.

2. Критерии сравнения систем обнаружения атак [Інтернет-ресурс]. – Режим доступу: http://inf-bez.ru/?p=480, вільний.

3. Paxon V., Floyd S. Wide-area traffic: The failure of Poisson modeling. / V. Paxon, S. Floyd // IEEE/ACM Transactions on Networking. – 1995. – Vol. 3. – p. 226 – 244.

4. Snort [Інтернет-ресурс] / Web-сайт: snort; Режим доступу http://www.snort.org, вільний.

5. Wireshark [Інтернет-ресурс] / Web-сайт: wireshark; Режим доступу http://www.wireshark.org, вільний.

ДОДАТОК Б

(обов’язковий)

Презентація роботи

1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА МАГІСТЕРСЬКОЇ РОБОТИ

Метою роботи є розроблення методу та відповідних засобів виявлення вторгнень на вузли в корпоративних комп'ютерних мережах для підвищення надійності та безпеки функціонування мереж

Об’єкт дослідження **– захищеність передачі даних в корпоративній мережі.**

Предмет дослідження **– методи та засоби виявлення вторгнень н вузли в корпоративних мережах.**

Задачі дослідження:

1) **провести аналіз корпоративних мереж та мережного трафіку на наявність аномалій, за якими можна визначати факт вторгнення;**
2) **провести аналіз відомих методів та засобів виявлення атак в мережах;**
3) **розробити метод виявлення вторгнень у корпоративну мережу;**
4) **реалізувати захист корпоративних мереж та дослідити його ефективність**

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

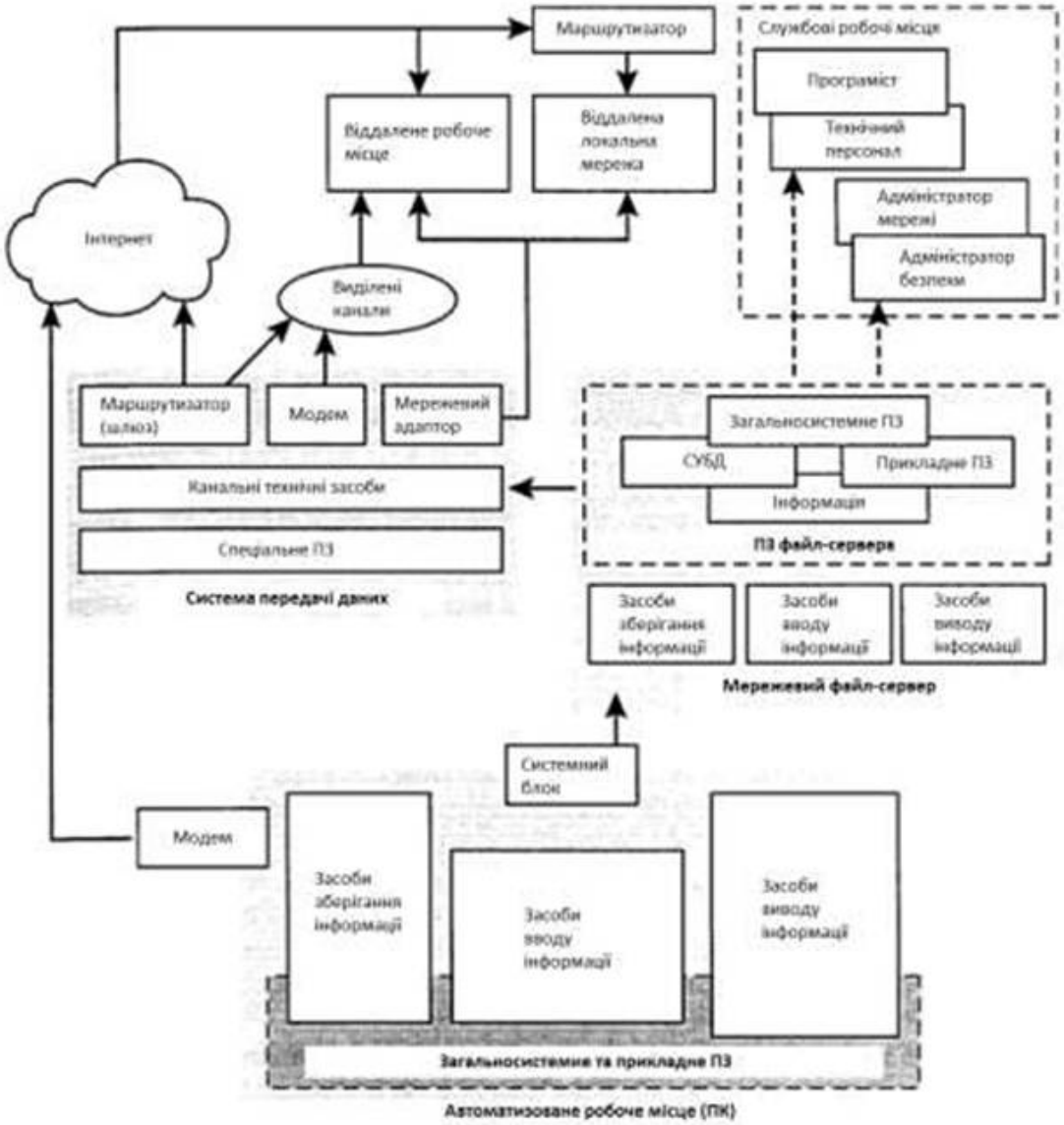
Наукова новизна одержаних результатів:

1. Проведено аналіз існуючих систем виявлення вторгнень IPS/IDS. Виявлено, що системи використовують сигнатурний принцип аналізу трафіку.
2. Розглянуто компоненти, що забезпечують ефективну роботу комп'ютерної мережі, підтримують постійну доступність і високу надійність мережі, а також обґрунтовано необхідність в системах моніторингу та керування.
3. Запропоновано вирішення проблеми захисту інфраструктури корпоративної мережі за допомогою використання IDPS систем.
4. Виявлено, що IDPS система може виконувати всебічний аналіз мережевого трафіку (рівень 7 моделі OSI) при розгортанні центрів обробки даних на рівні ядра корпоративної мережі або на межі підключення до Інтернету.

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

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

Модель корпоративної мережі

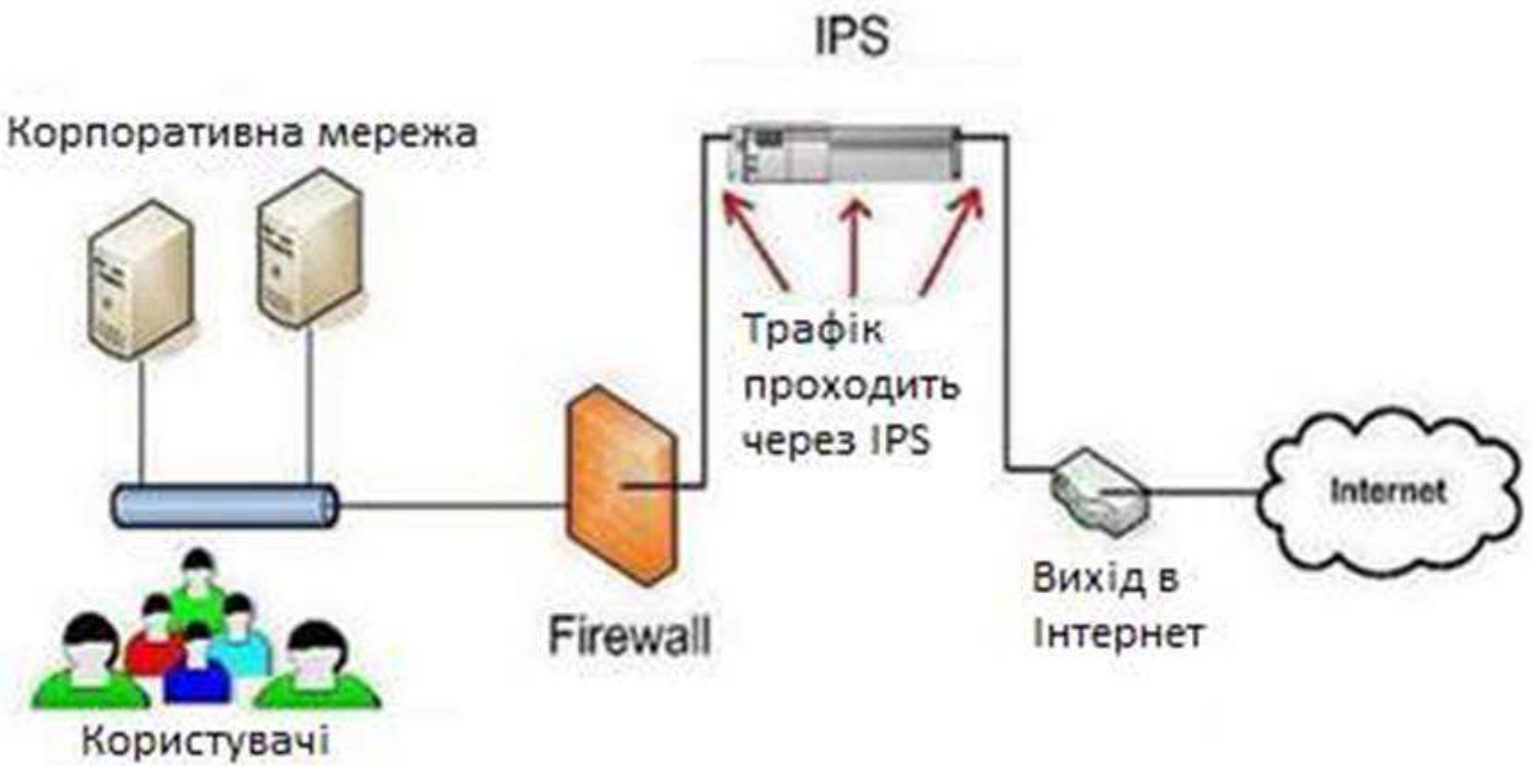


Ієрархія рівнів корпоративної мережі

Структура системи автоматизації обліку та аналізу трафіку мережних комунікацій

5

Структура системи запобігання вторгнень



Основні механізми реалізації атак

№ з/п	Тип атаки	Механізм реалізації атаки
1	Віддалене проникнення	Віддалений виклик командного рядка шляхом переповнення буфера
2	Аналіз топології мережі	Передача мережних пакетів, що містять запити ECHO_REQUEST
3	Пошук уразливості	Сканування хосту
4	Відмова в обслуговуванні	Передача великої кількості мережних пакетів
5	Злам паролів	Багаторазові спроби аутентифікації в системі
6	Аналіз мережного трафіка	Перемикання мережного інтерфейсу в “режим прослуховування” і перехоплення мережного трафіка
7	Несанкціонована аутентифікація	Порушення прав доступу і незаконне використання ресурсів
8	Шкідливе ПЗ	Приховане встановлення програмних модулів, прихований запуск процесів

Основні механізми виявлення атак

№ з/п	Механізми виявлення атаки	Клас атак, що виявляються
1	Відстеження спроб аутентифікації в системі	Зовнішні (внутрішні) мережні (локальні) активні
2	Відстеження перехоплення мережного трафіка	Зовнішні мережні активні
3	Відстеження мережного трафіка	Зовнішні мережні пасивні
4	Відстеження запуску процесів та звернень до файлової системи й реєстру	Внутрішні локальні активні

Результати аналізу методів виявлення вторгнень

Методи	Рівень спостереження	Верифікація	Адаптивність	Стійкість	Обчислювальна складність
Аналіз сигнатур	Хост, мережа, додатки	Так	Ні	Глобальна	O(log n)
Статистичний аналіз	Хост, мережа	Ні	Так	Локальна	O(n)
Аналіз систем станів	Хост, мережа, додатки	Так	Ні	Локальна	O(n)
Графи сценаріїв атак	Хост, мережа, додатки	Так	Так	Локальна	NP
Експертні системи	Хост, мережа	Так	Так	Глобальна	NP
Методи засновані на специфікаціях	Мережа	Так	Ні	Локальна	O(log n)
Нейронні мережі	Хост, мережа, додатки	Так	Так	Локальна	O(n)
Імунні мережі	Хост, мережа	Ні	Так	Локальна	O(n)
Кластерний аналіз	Хост, мережа, додатки	Ні	Так	Локальна	O(n)
Поведінкова біометрія	Хост	Ні	Так	Локальна	O(n)

Порівняльний аналіз існуючих СВВ

Назва	ПЗ/ПАК	Тип сенсора	Спосіб збору даних	Аналіз результатів	Повнота документації	Вартість
1	2	3	4	5	6	7
KFSensor	ПЗ	HIDS	Сигнатурний	Ні	Ні	Платно
OSSEC HIDS	ПЗ	HIDS	Сигнатурний	Ні	Так	0
Snort	ПЗ	NIDS	Сигнатурний	Ні	Так	0
Suricata	ПЗ	HIDS/NIDS	Сигнатурний	Ні	Так	0
EasyIDS	ПЗ	NIDS	Сигнатурний	Ні	Ні	0
Bro	ПЗ	NIDS	Сигнатурний	Ні	Так	0
Cisco IPS	ПАК	NIDS/HIDS	Сигнатурний, евристичний	Так	Так	Платно
ViPNet IDS	ПАК	NIDS/ HIDS	Сигнатурний, евристичний	Так	Так	Платно
McAfee IPS	ПЗ/ПАК	NIDS/ HIDS/ APIDS	Сигнатурний, евристичний	Так	Так	Платно
Open Source Tripwire	ПЗ	NIDS/ HIDS	Сигнатурний	Ні	Так	0
IBM ISS Proventia IPS	ПЗ/ ПАК	NIDS/ HIDS/ APIDS	Сигнатурний, евристичний	Так	Так	Платно
OSSIM	ПЗ	HIDS	Сигнатурний, евристичний	Так	Так	Платно

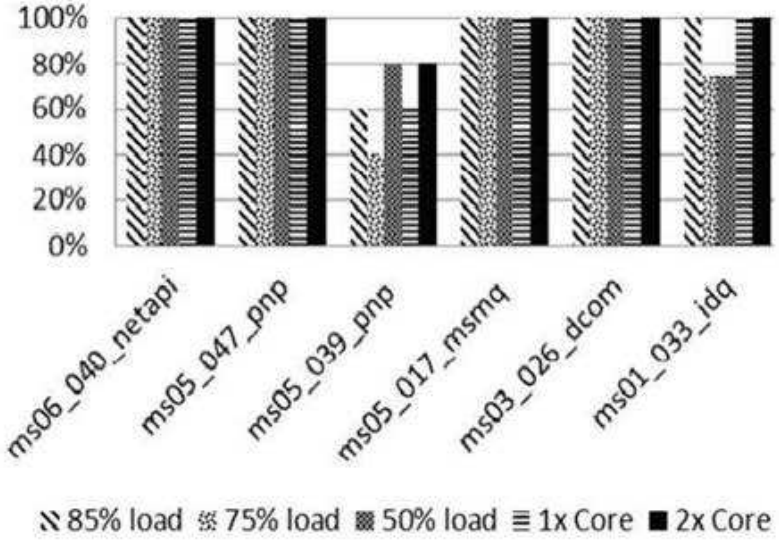
Види атак

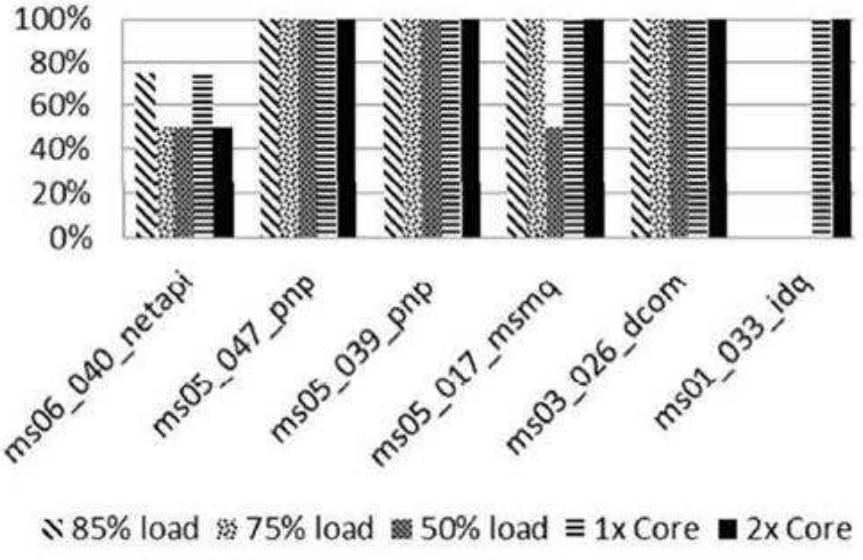
Код	Ім'я	Опис
ms03_026_dcom	Microsoft RPCDCOM Interface Overflow	Модуль використовуваного стеку переповнення буфера в службі RPCSS
ms05_039_pnp	Microsoft Server Service NetpwPathCanonicalize Overflow	Стек переповнення буфера в службі Windows Plug and Play
ms05_047_pnp	Microsoft Plug and Play Service Registry Overflow	Стек переповнення буфера в службі Windows PnP. Причина перезавантажень.
ms06_040_netapi	Microsoft Server Service NetpwPathCanonicalize Overflow	Стек переповнення буфера в NetApi32 CanonicalizePathName () використовуючи функцію NetpwPathCanonicalize RPC виклик служби Server
ms05_017_msmq	Microsoft Message Queueing Service Path Overflow	Використовуваний стек переповнення буфера в RPC інтерфейсі в службі Microsoft Message Queueing
ms01_033_idq	Microsoft IIS5.0 IDQ Path Overflow	Використовуваний стек переповнення буфера в IDQ ISAPI обслуговування для Microsoft Index Server

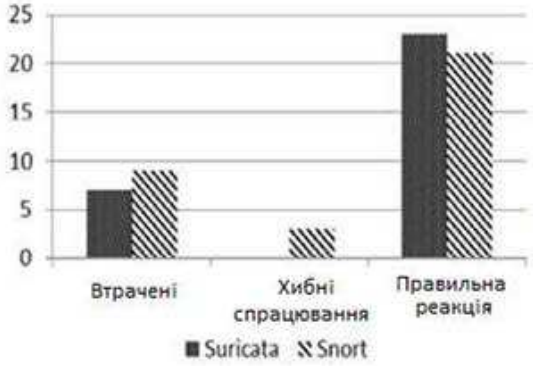
Попередження згенеровані Snort і Suricata

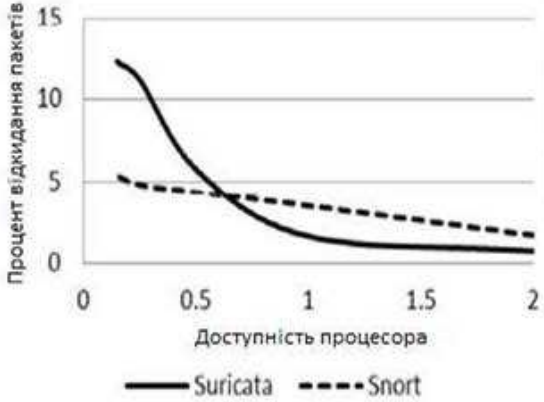
Попередження	Snort	Suricata
ms05_040_pnp	4	4
ms05_047_pnp	1	1
ms05_039_pnp	1	6
ms03_026_dcom	1	2
ms01_033_idq	2	4
ms05_017_msmq	2	3

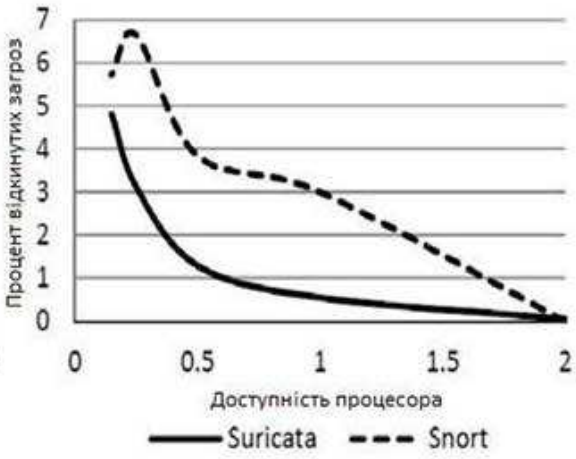
Результати застосування систем виявлення вторгнень



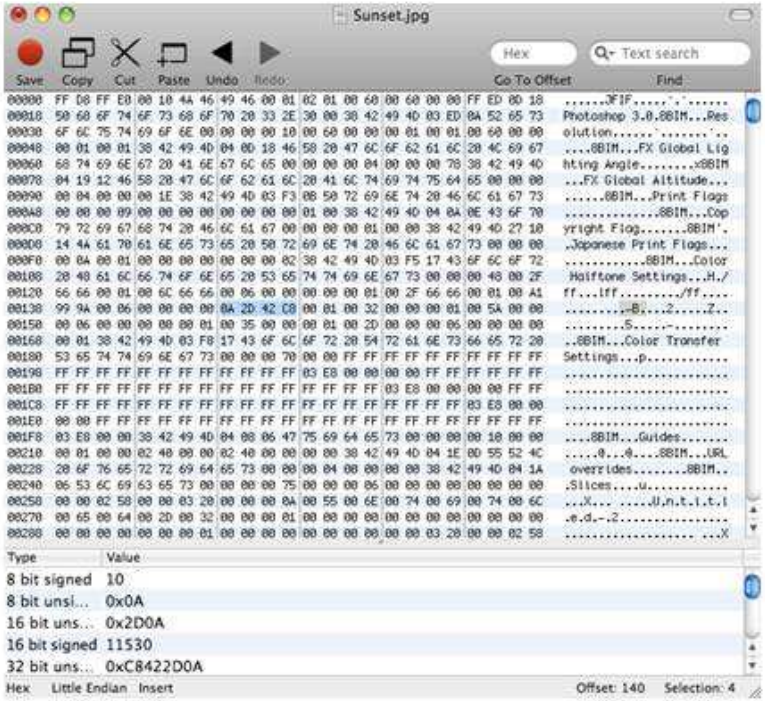


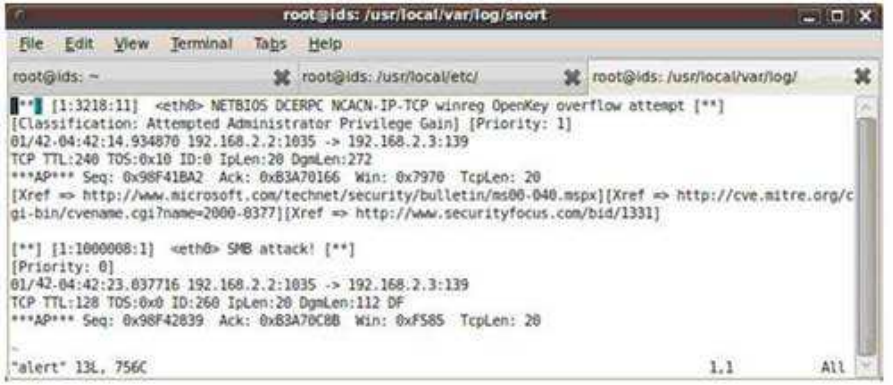


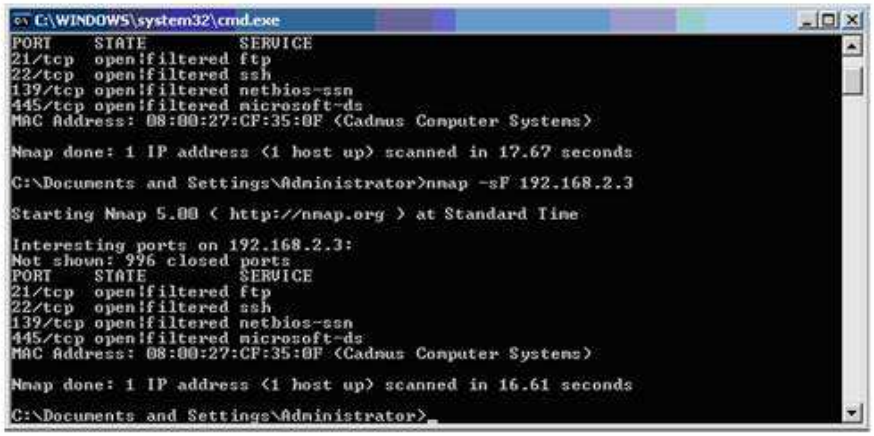




Результати застосування систем виявлення вторгнень







Висновки

1. Проведено аналіз існуючих систем виявлення вторгнень IPS/IDS. Виявлено, що системи використовують сигнатурний принцип аналізу трафіку.
2. Розглянуто компоненти, що забезпечують ефективну роботу комп'ютерної мережі, підтримують постійну доступність і високу надійність мережі, а також обґрунтовано необхідність в системах моніторингу та керування.
3. Запропоновано вирішення проблеми захисту інфраструктури корпоративної мережі за допомогою використання IDPS систем.
4. Виявлено, що IDPS система може виконувати всебічний аналіз мережевого трафіку (рівень 7 моделі OSI) при розгортанні центрів обробки даних на рівні ядра корпоративної мережі або на межі підключення до Інтернету.