Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра Електронних обчислювальних машин
(повна назва)

# КВАЛІФІКАЦІЙНА РОБОТА

## Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи та засоби моніторингу корпоративної комп'ютерної мережі
(тема)

Виконав:
студент II курсу, групи СПзм-21-1
Гребеннік К.В.
(прізвище, ініціали)

Спеціальність
123 – Комп’ютерна інженерія
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма
Системне програмування
(повна назва освітньої програми)

Керівник: доц. Ткачов В.М.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ Коваленко А.А.
(підпис) (прізвище, ініціали)

2023 р.

Харківський національний університет радіоелектроніки

Факультет Навчально-науковий центр заочної форми навчання

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

# ЗАВДАННЯ

## НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Гребенніку Кирилу Валентиновичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи та засоби моніторингу корпоративної комп'ютерної мережі

затверджена наказом по університету від " 24 " березня 2023 р. № 60 СТз

2. Термін подання студентом роботи до екзаменаційної комісії 17 травня 2023 р.

3. Вхідні дані до роботи 1) моделі та методи моніторингу мультисервісних мереж;
2) сучасні вимоги до мережних показників;
3) перелік використаних програмних та апаратних засобів: ОС Windows 10, MATLAB Zabbix, Multi Router Traffic Grapher

4. Перелік питань, що потрібно опрацювати у роботі
1) аналіз сучасного стану проблеми
2) огляд технологій управління перевантаженням та середньою затримкою
3) аналіз моделі моніторингу мережного трафіку
4) вибір програмних та апаратних засобів реалізації
5) проведення експериментальних досліджень
6) висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Слайдів презентації – 20 шт

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1 )

| Найменування розділу | Консультант (посада, прізвище, ім'я, по батькові) | Позначка консультанта про виконання розділу | |
|---|---|---|---|
| | | підпис | дата |
| | | | |
| | | | |

## КАЛЕНДАРНИЙ ПЛАН

| № | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Огляд літератури за темою роботи | 29.03.23-05.04.23 | |
| 2 | Вибір та обґрунтування методики дослідження | 06.04.23-16.04.23 | |
| 3 | Вибір інструментальних засобів | 17.04.23-29.04.23 | |
| 4 | Проведення експериментів | 30.04.23-04.05.23 | |
| 5 | Оформлення матеріалів кваліфікаційної роботи | 04.05.23-10.05.23 | |
| 6 | Подання кваліфікаційної роботи керівникові | 11.05.23-12.05.23 | |
| | та попередній захист | | |
| 7 | Подання кваліфікаційної роботи на | 13.05.23-17.05.23 | |
| | рецензування | | |
| | | | |
| | | | |
| | | | |

Дата видачі завдання 27 березня 2023 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Ткачов В.М.
(підпис) (посада, прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 89 сторінок, 15 рисунків., 3 таблиці., 1 додаток, 26 джерел.

МЕТОДИ І ЗАСОБИ МОНІТОРИНГУ ТРАФІКУ, ЛОКАЛЬНА МЕРЕЖА КОРПОРАТИВНОГО РІВНЯ, ВИЯВЛЕННЯ ПОДІЙ, ВЕЙВЛЕТ-АНАЛІЗ, SNMP, CWT, ZABBIX

Метою кваліфікаційної роботи є аналіз методів та засобів моніторингу мережного трафіку у корпоративній мережі. Детально розглянуто методи моніторингу корпоративних мереж, які націлені на збереження безпеки даних та працездатності мереж

Також проведено аналіз корпоративної мережі із застосуванням вейвлет перетвореннь з метою покращення ситеми моніторингу та своєчасного виявлення загроз та реагування на них. Приділено увагу темам виявлення раптових подій в системах моніторингу, та виявлення поштових хробаків за допомогою аналізу DNS запитів. Для моделювання та експериментальних обчислень використано вейвлет-аналіз, а саме дискретне та неперевне вейвлет перетворення, статистичні алгоритми кластеризації, численні методи та інші методи математичного аналізу.

# ABSTRACT

Master’s thesis: 89 pages, 15 figures, 3 tables, 1 application, 26 sources.

TRAFFIC MONITORING METHODS AND TOOLS, CORPORATE-LEVEL LOCAL NETWORK, EVENT DETECTION, WAVELET ANALYSIS, SNMP, CWT, ZABBIX, EMAIL WORMS DETECTION.

The purpose of the qualification work is to analyze the methods and the means of monitoring network traffic in the corporate network. The methods of monitoring corporate networks, which are aimed at preserving data security and network performance, are considered in detail

An analysis of the corporate network was also carried out using wavelet transformations in order to improve monitoring systems and timely detection of threats and response to them. Attention is paid to the topics of detection of sudden events in monitoring systems and detection of mail worms using DNS query analysis. Wavelet analysis, namely discrete and continuous wavelet transformation, statistical clustering algorithms, multiple methods and other methods of mathematical analysis were used for modeling and experimental calculations.

ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ATM (Asynchronous Transfer Mode) – режим асинхронної передачі;

SMTP (Simple Mail Transfer Protocol) – комунікаційний протокол для пересилання електронної пошти;

HTTP (HyperText Transfer Protocol) – протокол передачі даних;

IMAP (Internet Message Access Protocol) – протокол доступу до інтернет-повідомлень;

NMS (Network Management System) – система управління мережею;

API (Application Programming Interface) – інтерфейс прикладного програмування;

AS (Application Server) – сервер додатків;

POP3 (Post Office Protocol Version 3) – поштовий офісний протокол;

CWT (Continuous Wavelet Transform) – безперервне вейлветне перетворення;

SNMP (Simple Network Management Protocol) – протокол керування мережами зв'язку;

TAP (Test Access Port) – апаратний пристрій, який дозволяє пропускати мережевий трафік від портів A до B;

IPMI (Intelligent Platform Management Interface) – інтерфейс керування інтелектуальною платформою;

JMX (Java Management Extensions) – розширення для управління;

LDAP (lightweight directory access protocol) – полегшений протокол доступу до директорій;

RFC (Request for Comments) – інформаційні документи Інтернету, що містять технічні специфікації та стандарти;

ASN.1 (Abstract Syntax Notation One) – мова для опису абстрактного синтаксису даних;

STFA (Short-Time Fourier Analysis) – швидкий аналіз Фур’є;

IDS (Intrusion Detection System) – Система виявлення вторгнень;

XSS (Cross-site scripting) – тип вразливості інтерактивних інформаційних систем у вебі;

DPI (Deep Packet Inspection) – технологія перевірки та фільтрації пакетів за змістом;

IETF (Internet Engineering Task Force) – відкрита міжнародна спільнота інженерів, учених, мережевих спеціалістів і провайдерів;

DoS (denial-of-service attack) – напад на комп'ютерну систему;

DDoS (distributed denial-of-service attack) – розподілений напад на комп'ютерну систему;

NIC (network interface controller) – мережева карта;

LAN (Local Area Network) – локальна мережа;

Pcap (Packet Capture) – інтерфейс прикладного програмування (API) для захоплення мережевого трафіку;

SCADA (Supervisory Control And Data Acquisition) – програмний пакет, призначений для розробки в реальному часі систем збору, обробки, відображення та архівування інформації про об'єкт моніторингу або управління;

FPGA (Field-Programmable Gate Array) – напівпровідниковий пристрій, який налаштовується виробником;

ICMP (Internet Control Message Protocol) – протокол повідомлень для управління;

RDA (Remote Data Access) – віддалений доступ до даних;

DWT (Discrete wavelet transform) – це будь-яке вейвлет-перетворення, для якого вейвлети дискретно відбираються.

# ВСТУП

З роками комп’ютерні мережі стають все більш важливими для людського суспільства. Комп’ютерні мережі широко використовуються всюди – від невеликих організацій, шкіл і підприємств до корпорацій, установ уряду, військових організацій і можуть поширюватися на міжконтинентальні дослідницькі та академічні установи. Це пов’язано з тим, що більшість організацій мають високий ступінь залежності від комп’ютерних мереж, збої або неправильні налаштування мережі призведуть до великих збитків, знижують продуктивність установ і підприємств і, як наслідок, зменшують їхні доходи.

Природа комп’ютерної мережі – це складна конструкція як апаратного, так і програмного забезпечення. Комп’ютерну мережу можна описати як систему, де відбувається багато взаємодій між апаратними пристроями, такі як маршрутизатори, мости, концентратори та канали зв’язку, а також протоколи керування та координація цих пристроїв. Коли велика кількість мережевих пристроїв з’єднана між собою для компенсації комп’ютерної мережі, дуже ймовірно, що деякі з мережевих компонентів можуть вийти з ладу, може знадобитися оптимізація конфігурації для поточної мережі, або просто потребувати ремонту. Крім того, деякі мережеві ресурси можуть використовуватися понад встановлений ліміт, що спричиняє вузькі місця в мережі.

Завдання мережевого адміністратора – стежити за мережею, щоб запобігти або відновити її після нещасних випадків і підтримувати здоровий стан та повноцінне функціонування для мережі та кожного її пристрою. Оскільки комп’ютерні мережі виросли як за розмірами, так і за складністю, тому завдання управління та підтримки нормального функціонування мережі стало більш важливим. Отже, мережевому менеджеру необхідно мати спеціальні інструменти з метою моніторингу, контролю та керування

мережею. У наступних параграфах висвітлено концепції моніторингу мережі, представлено та обговорено моніторинг продуктивності мережі. Різноманітні показники продуктивності мережі представлені та досліджені нижче.

Комп’ютерні мережі об’єднують мільйони комп’ютерів і користувачів комп’ютерів у всьому світі. Мережа має стати інфраструктурою для багатьох програм, які впливають на наше повсякденне життя. Дуже важливо, щоб комп'ютерна мережа потрібно правильно управляти. Менеджмент мережі вимагає моніторингу. Моніторинг мережі – це набір механізмів, які дозволяють адміністраторам мережі знати миттєвий стан і довгострокові тенденції розвитку комплексу. Моніторинг та вимірювання мережі стало важливіше в сучасній складній мережі. У минулому адміністратори могли контролювати лише кілька мережевих пристроїв або менше сотні комп'ютерів. Пропускна здатність мережі була лише 10 або 100 Мбіт/с; однак тепер адміністратори повинні мати справу не тільки з високошвидкісною дротовою мережею (більше 10 Гбіт/с і мережею ATM (режим асинхронної передачі), а також із бездротовими мережами. Їм потрібна більш складна архітектура, інструменти моніторингу та аналізу трафіку для підтримки, стабільність і доступність мережевої системи, наприклад для виправлення проблеми з мережею вчасно, або щоб уникнути збою мережі, щоб забезпечити міцність безпеки мережі та покращити рішення для мережевого планування. Внутрішня мережа –локальна мережа (LAN) і моніторинг охоплюють апаратне забезпечення, програмне забезпечення, віруси, шпигунське програмне забезпечення, уразливості, такі як бекдори та діри в безпеці, а також інші аспекти, які можуть порушити цілісність мережі.

Моніторинг мережі є складним і вимогливим завданням, є важливою частиною роботи мережевого адміністратора. Мережеві адміністратори постійно прагнуть підтримувати плавність функціонування своїх мереж. Якщо мережа не працює навіть за невеликий проміжок часу, продуктивність всередині компанії знизиться, а у випадку відділів державної служби здатність надавати основні послуги буде скомпрометовано. Щоб бути

ініціативними, а не реактивним, адміністратори повинні стежити за рухом трафіку та продуктивністю у всій мережі та перевіряти безпеку так, щоб порушення в мережі не відбувалися. Коли відбувається збій мережі, агенти моніторингу повинні виявляти, ізолювати та усувати несправності в мережі та можливо, відновити несправність. Як правило, агенти повинні попередити адміністраторів про усунення проблем протягом хвилини. При стабільній роботі мережі адміністратори залишаються постійно стежити, чи є загроза зсередини або із зовнішньої мережі. Крім того, вони повинні регулярно перевіряти продуктивність мережі, якщо мережеві пристрої перевантажені.

В даній роботі буде розглянуто найпоширеніші методи та засоби моніторингу корпоративної мережі. Розглянуто службові протоколи передачі даних, які застосовуються у середовищах для моніторингу, також приділено увагу методам по виявленню і усуненню загроз безпеки мереж. Показані приклади аналізу трафіку корпоративної мережі за допомогою вейвлет (хвилькових) перетворень.

# 1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА, ПАРАМЕТРИ І ПРИНЦИПИ МОНІТОРИНГУ ТРАФІКУ У МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ

## 1.1 Термінологічна основа, загальні особливості і принципи моніторингу корпоративних мереж

Моніторинг мережі – це використання системи, яка постійно відстежує комп’ютерну мережу на наявність повільних або несправних компонентів і сповіщає адміністратора мережі (через електронну пошту, SMS або інші сигнали тривоги) у разі збоїв або інших проблем. Моніторинг мережі є підзадачею керування мережею.

У той час як система виявлення вторгнень відстежує мережеві загрози ззовні, система мережевого моніторингу відстежує мережу на наявність проблем, спричинених перевантаженням або збоями серверів, мережевих підключень або інших пристроїв.

Наприклад, щоб визначити статус веб-сервера, програмне забезпечення для моніторингу може періодично надсилати HTTP-запит для отримання сторінки. Для серверів електронної пошти тестове повідомлення може бути надіслано через SMTP і отримано через IMAP або POP3.

Зазвичай вимірюваними показниками є час відповіді, доступність і безвідмовна робота, хоча показники узгодженості та надійності починають набирати популярності. Широко розповсюджене додавання пристроїв оптимізації глобальної мережі негативно впливає на більшість інструментів мережевого моніторингу, особливо коли мова йде про вимірювання точної наскрізної затримки, оскільки вони обмежують видимість часу затримки в обидва кінці.

Помилки запиту статусу, наприклад, коли не вдається встановити з’єднання, вичерпано час очікування або неможливо отримати документ чи повідомлення, зазвичай призводять до виконання дії від системи

моніторингу. Ці дії відрізняються; резидентному системному адміністратору може бути надіслано тривогу (через SMS, електронну пошту тощо), можуть бути активовані автоматичні системи перемикання збоїв, щоб усунути проблемний сервер з роботи, доки його не можна буде відремонтувати тощо.

Системи моніторингу мережі включають програмні та апаратні засоби, які можуть відстежувати різні аспекти мережі та її роботу, такі як трафік, використання пропускної здатності та час безвідмовної роботи.

Мережеві адміністратори покладаються на системи моніторингу мережі, які допомагають їм швидко виявляти збої пристрою чи з'єднання або проблеми, наприклад вузькі місця трафіку, які обмежують потік даних. Здатність виявляти проблеми поширюється на частини мережі, які традиційно знаходяться за межами їх демаркації. Ці системи можуть сповіщати адміністраторів про проблеми електронною поштою або текстовими повідомленнями та надавати звіти за допомогою мережевої аналітики.

Протоколи – це набори правил і вказівок для пристроїв у мережі для обміну даними один з одним. Мережеве обладнання має використовувати протоколи для передачі даних. Системи моніторингу мережі використовують протоколи для виявлення проблем із продуктивністю мережі та звітування про них.

Моніторинг мережі буває активним чи пасивним. Пасивний моніторинг мережі зчитує дані з лінії зв'язку, без впливу на трафік. Активний моніторинг мережі додає можливість змінити дані в рядку. Пасивний моніторинг мережі існує в кількох формах. Просто моніторинг може бути легким для оцінки вручну, оскільки сума даних, що відстежуються та створюються, невелика. Крім того, чим більше даних збирається, тим технологічніше середовище вимагається для коректного збереження та обробки даних. Тому різні способи проведення мережевого моніторингу конкурують один з одним, як кожен має різні компроміси, направлені на різні цілі, середовища і користувачів. На рисунку 1.1 показана загальна архітектура мережевого

моніторингу.

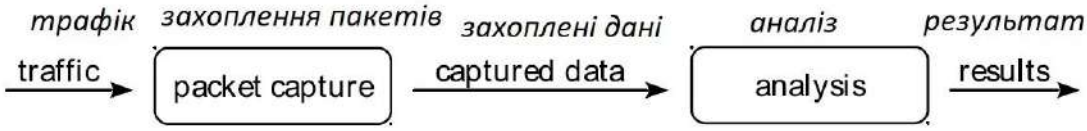


Рисунок 1.1 – Загальна архітектура мережевого моніторингу

Процес моніторингу мережі складається з двох основних кроків, дублювання трафіку та аналізу трафіку.

### 1.1.1 Дублювання трафіку

Дублювання може відбуватися в одному з двох режимів; вбудований або дзеркальний [1]. У режимі дзеркалювання портів можливість дублювання вже є вбудованою функцією маршрутизатора (router) або комутатора (switch). Існує кілька способів віддзеркалення трафіку; дзеркалювання портів, TAP (Test Access Port) і TAP-подібне налаштування з використанням обхідних мережевих карт (NICs). Наступні підрозділи описують кожен спосіб.

Дзеркальні порти мають два недоліки. По-перше, якщо сумарна пропускна здатність трафіку більша, ніж може дзеркальний порт передати, дзеркальний порт стає перевантаженим і втрачає пакети. Повнодуплексний трафік передається в одному напрямку через дзеркальний порт. Це майже вдвічі перевищує пропускну здатність на один порт для двох портів, що обслуговуються комутатором, і навіть більше якщо обслуговується більше двох портів. По-друге, більшість комутаторів не мають достатньо обчислювальної потужності, щоб впоратися з обома завданнями:

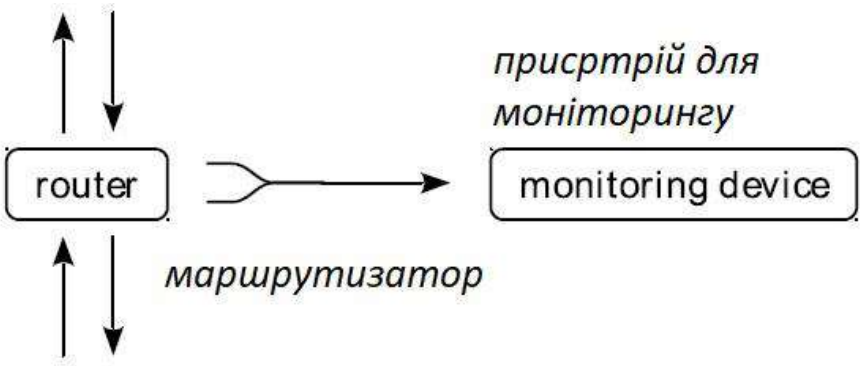


Рисунок 1.2– Принципова схема дзеркалювання портів

перемикання та дзеркалювання. Основною функцією перемикача є пріоритет, і дзеркалювання може не працювати належним чином під час періодів пікового трафіку

Дзеркалювання портів – це функція, яка зазвичай доступна в корпоративно-орієнтованих мережевих комутаторах та маршрутизаторах, трафік, що проходить через вибрані порти комутатора або маршрутизатора віддзеркалено на інший вибраний порт. Порт, який використовується для виведення дубльованого трафіка зазвичай називається дзеркальним портом або SPAN (Switched Port Analyzer) порт (аналізатор комутованих портів). На рисунку 1.2 показаний принцип дзеркалювання портів. Обидва напрямки трафіку пристрою, який перебуває під моніторингом, передаються в одному напрямку через дзеркальний порт.

Пасивні мідні порти (TAP) підключаються безпосередньо до лінії. Оскільки пасивні порти не живляться, відключення живлення не може внести несправність на лінію. Недолік пасивної мідної лінії (TAP) полягає в тому, що вона підтримує лише з’єднання зі швидкістю 10 Мбіт/с і 100 Мбіт/с. Пасивний зв'язок спотворює сигнал таким чином, що неможливо підключити Gygabit Ethernet пасивно. Патент NetOptic представляє метод, який використовує активний гігабітний TAP, оснащений конденсаторами для підтримки зв'язку, поки перемикаються вбудовані обхідні реле (рисунок 1.3).

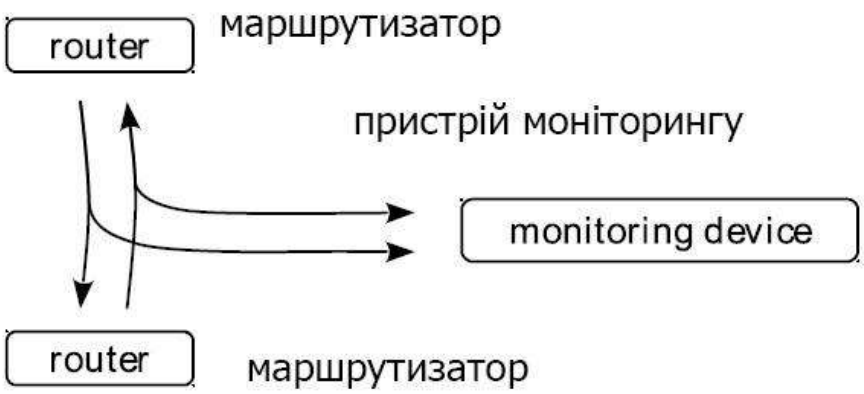


Рисунок 1.3 – Дзеркалювання трафіку за допомогою тестового порту доступу (TAP)

Активні мідні TAP функціонують подібно до пасивних, як описано в попередньому абзаці. Сигнал, який проходить через TAP ретранслюється та подвоюється (дублюється) без спотворень, за винятком незначних затримок, спричинених електронною схемою.

Пасивні оптичні TAP відводять деякий відсоток оригінального сигналу на дзеркальний вихід. Перевага пасивних TAP тому, що немає втрат потужності. Недоліком є той факт, що сигнал в лінії ослаблений самою технологією TAP.

Налаштування за допомогою карти мережевого інтерфейсу (NIC) інтегрується віддзеркалення трафіку з аналізом трафіку. Як показано на рисунку 1.4, спостережувана лінія розділена. Обидва кінці в розколі є підключений до двох інтерфейсів NIC. NIC встановлено в комп'ютер. Інтерфейси налаштовані в програмному забезпеченні як мережевий міст. Виконуючи роль моста, лінія розриву продовжує функціонувати належним чином. Через комп'ютер дозволяє стежити за трафіком. Ця збірка розміщена у вбудованому режимі, подібно до TAP.

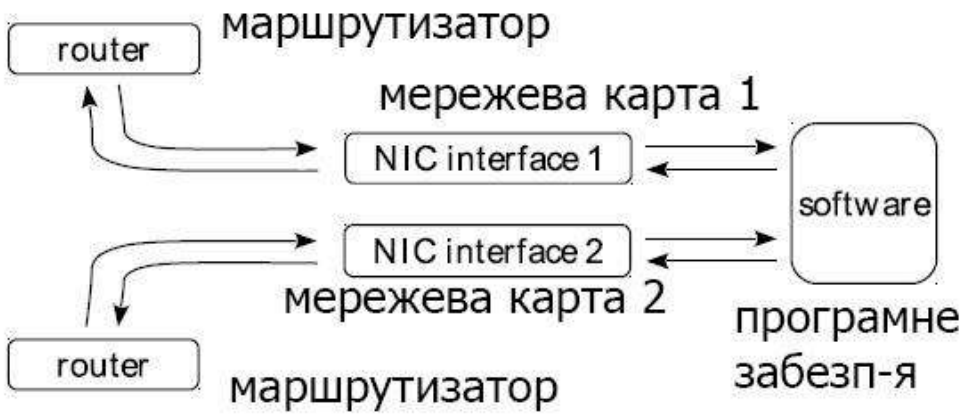


Рисунок 1.4 – Вбудоване дзеркалювання з використанням двох інтерфейсів мережевої карти

Дзеркалювання за допомогою NIC можливе за допомогою звичайних споживчого рівня NIC. Це створює точку відмови. Як тільки програмне забезпечення або апаратний збій, лінія більше не підключена. Існують спеціалізовані, так звані обхідні NIC, як показано на рисунку 1.5. Обхідні мережеві карти мають можливість обходити два мережі інтерфейси, коли виникає збій; наприклад, збій програмного забезпечення або втрата потужності.

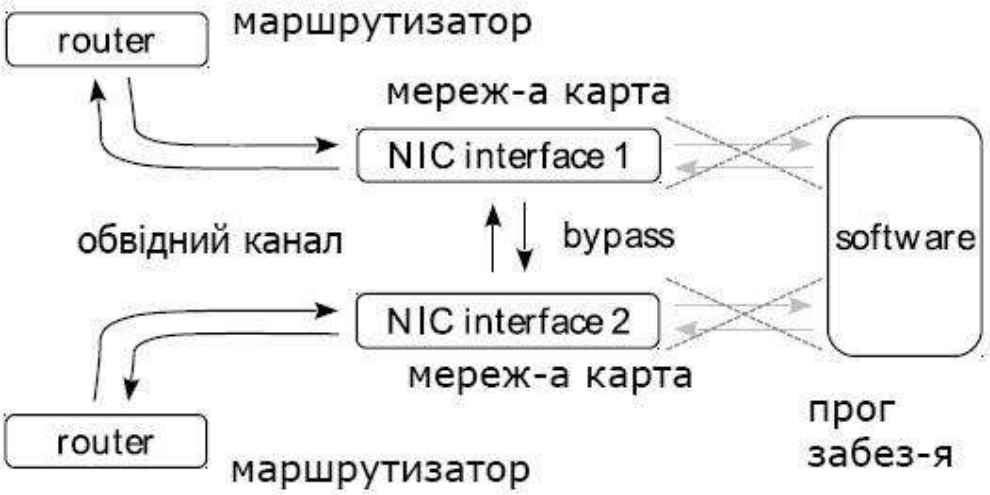


Рисунок 1.5 – Обхідна мережева карта в режимі обходу (bypass) перекриває з’єднання обладнання, щоб не розірвати з’єднання

Недоліком є те, що комп’ютер заблоковано в певному місці, і його неможливо перемістити без переривання з'єднання.

### 1.1.2 Захват пакетів

Перехоплення пакетів має три значення без певного порядку. По-перше, це інтерактивний підхід до моніторингу мережі. По-друге, захоплення пакетів – це файл трасування пакетів. По-третє, це акт захоплення пакетів з мережевого каналу. Захоплення може бути збережено у файлі або прочитано безпосередньо за допомогою аналізатора мережевого трафіку у реальному часі.

Перехоплення пакетів як метод дублювання пакетів. Мережевий трафік фіксується з точки спостереження. Це є не обов'язково, щоб захоплення було часовим і просторовим, все залежить від подальшого аналізу, оскільки отримані дані можуть бути збережені у файл. Це може бути тимчасовий файл як частина всього процесу моніторингу мережі або його можна зберегти у файл для подальшого використання. Зібрані дані такі ж, як і раніше на лінії. Процес захоплення пакетів може бути як ручний, так і автоматичний.

Перехоплення пакетів як підхід до моніторингу мережі. Підхід до моніторингу мережі захоплення пакетів складається з двох основних кроків; спочатку створюється файл захоплення пакетів і по-друге, виконання аналізу мережевого трафіку на файл захоплення пакетів. Захоплення пакетів як підхід до моніторингу мережі може бути як в ручному, так і в автоматичному режимі. Використовується автоматизований підхід для запису та аналізу поведінки шкідливих програм. Додатковий ручний аналіз вибраних захоплень пакетів від автоматизованої системи також можливий.

Рівень 3 моделі OSI зазвичай використовується для того, щоб трафік розглядається як серія IP-пакетів. Знятий трафік в потім це представлення

можна переглядати, шукати в ньому або фільтрувати Також можна відфільтрувати пакети перед захопленням трасування пакета.

Використовується як графічний інтерфейс користувача (GUI), так і інтерфейс командного рядка (CLI). У деяких налаштуваннях автоматизація через можливий сценарій дій. Це лише задумано як допомога для людини-користувача і не призначена для реалізації як складна автоматизована система. Система виявлення вторгнень (IDS) можна вважати складним автоматизованим система. У контексті аналізу захоплення пакетів навіть IDS-подібна сценарна функціональність все ще призначена для окремих осіб інтерактивний аналіз.

Доступність повних мережевих даних для безкоштовного перегляду та пошуку є неперевершеним серед усіх архітектурних підходів, згаданих в цьому підрозділі. Величезна перевага – інтерактивність і доступ до будь-якої частини даних трафіку. Користувач може шукати дуже специфічні артефакти без необхідності програмувати щось і не будучи обмежений більш автоматизованим програмним забезпеченням. Це корисно для роботи з новими моделями трафіку, такими як нові шкідливі програми або невідомі комунікаційні протоколи. Інтерактивність однак, стає недоліком в тому випадку, коли шаблон уже відомий, і робота є повторюваною та автоматизованою. Підхід не масштабується, тому пошук стає обтяжливим у великих обсягах даних.

PCAP є широко використовуваним форматом файлів для зберігання захопленого трафіку. Tshark і tcpdump – приклади програмного забезпечення, що працюють через CLI. Wireshark є приклад програмного забезпечення з графічним інтерфейсом користувача.

### 1.1.3 Докладний аналіз пакетів (Deep Packet Inspection)

Захоплення трафіку та подальший аналіз можуть бути окремими процесами як у часі, так і в просторі або їх можна інтегрувати, як один конвеєр

процесу, як показано на рисунку 1.6. Засобом захоплення пакетів може служити джерелом файлу PCAP для подальший аналізу на основі DPI

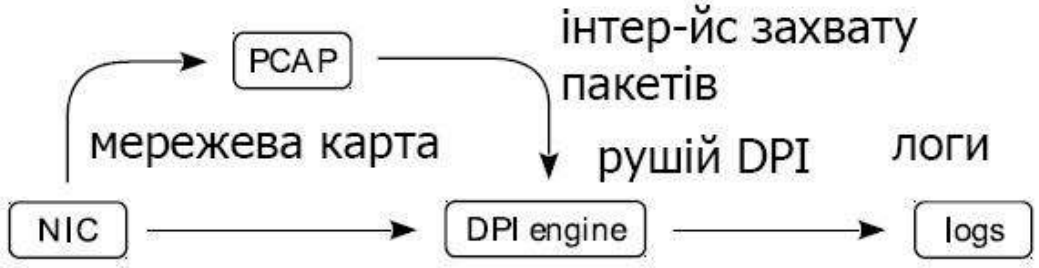


Рисунок 1.6 – Засіб захвату пакетів, заснований на DPI

Існує два основних типи аналізу на основі DPI; зіставлення паттернів та аналіз подій. Обидва використовуються в різних IDS/IPS (Системи виявлення вторгнень/запобігання вторгненням системи).

Зіставлення паттернів (Pattern Matching) Зіставлення паттернів – це метод DPI, який передбачає пошук через повні дані мережі для відомих послідовностей байтів або для збігів регулярного виразу. Принцип дії такого методу показано на рисунку 1.7. Пошук можна обмежити певними частинами пакетів або до певних пакетів.


Рисунок 1.7 – Принцип роботи методу зіставлення паттернів

Відносна простота є перевагою цього підходу, тому це популярний тип DPI. Описувати шукані дані за допомогою послідовностей байтів або регуля-

рних виразів часто просто. Однак ця сила стає проблемою, коли треба шукати шаблони, які неможливо чи можливо описати за допомогою регулярних виразів. Якщо дані мають бути декодовані перед подальшим зіставленням шаблону та декодуванням, а функціональні можливості ще не вбудовані в систему безпеки мережі монітора, зазвичай неможливо створити регулярний вираз для того, щоб виконати декодування. Стиснення може служити як приклад такого декодування необхідного перед виконанням, власне операції зіставлення паттернів.

Складну логіку прийняття рішень, також неможливо використовувати просто регулярні вирази. Приклад завдання; сповіщення про прострочений SSL сертифікати для з'єднань HTTPS, що надходять із указаного список IP-адрес і нікуди більше. Перекладаючи виявлення даних сертифіката SSL у регулярних виразах може бути неможливим. Перевірка наявності конкретного сертифіката належить до списку може призвести до складного регулярного виразу. Навіть якщо першу проблему вирішує SSL декодер, другий ще стоїть. Ще один крок далі, якщо список сигналів динамічно змінюється під час виконання, перетворення алгоритму регулярного виразу взагалі стає неможливим. Прикладом цього може бути виявлення на основі порогового значення, наприклад, сповіщення про хости, які отримують більше 10 помилок DNS на годину. Сучасний мережевий трафік відстежує за шаблоном відповідний метод DPI, як правило, декодує найбільш використовувані протоколи.

Підхід зіставлення паттернів є повільним порівняно з підходом спостереження потоку, який пояснюється в наступному підрозділі. Конкретна реалізація відповідності шаблону для 10 Гбіт/с вимагає апаратного прискорення за допомогою FPGA. На противагу цьому, а здійснення спостереження за потоком без апаратного забезпечення прискорення обробляє 40 Гбіт/с. У порівнянні з подієвим заснований підхід у наступному підрозділі, зіставлення шаблонів підхід також досить спрощений.

Існують численні алгоритми зіставлення шаблонів. Алгоритми зіставлення паттернів у контексті мережі моніторингу описані Дж. Келлі [2]. Крім

алгоритмів, є пакети програмного забезпечення для зіставлення паттернів, готові до використання, вбудовані в інше програмне забезпечення: Flex і MultiFast.

Snort і Suricata є програмними реалізаціями шаблону DPI. Ngrep – утиліта командного рядка для зіставлення паттернів у трасувальних файлах захоплених пакетів.

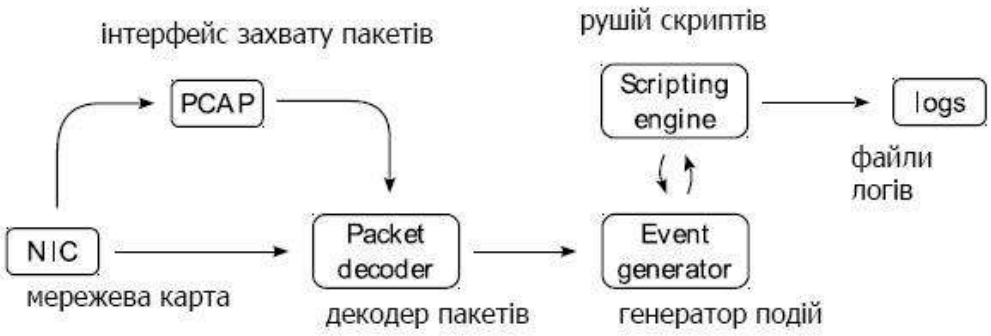


Рисунок 1.8 – Принцип роботи методу DPI з аналізом подій

Подійний аналіз. У попередньому підрозділі описано випадки, коли зіставлення паттернів явно недостатньо. Його нездатність виконати декодування або кілька етапів прийняття рішення розглядається в архітектурному підході аналіз на основі подій. У підході DPI з подієвим аналізом, як показано на рисунку 1.8, пакети обробляються в події, які у свою чергу обробляються скриптами. Скрипти можуть реалізувати складні алгоритми обробки та додавання нових, пов’язаних з DPI функціональностей.

### 1.1.4 Спостереження за потоком (Flow Observation)

Підхід, що відрізняється від описаних у попередніх розділах – це спостереження за потоком. Зміст пакетів не аналізуються, крім інформації із заголовка пакета. Ця інформація агрегується в потоки. RFC 7011 надає таке визначення потоку: «Потік – це набір пакетів або кадрів, що передаються через

Точку спостереження в мережі протягом певного інтервалу часу. Всі пакети, що належать до певного потоку, мають набір загальних властивостей».

В процесі спостереження формується п’ять потоків загального призначення, незалежних один від одного: IP-адреса джерела, IP-адреса призначення, IP-порт джерела, IP-порт призначення, протокол рівня 4.

Архітектура потокового спостереження складається так, що в процесі моніторингу мережевого трафіку підхід зберігає службову інформацію про 5 потоків мережевого трафіку, кількість переданих байтів, пакети і флаги протоколу рівня 4, проте не аналізує і не зберігає основний трафік.

Завдяки тому, що над основним трафіком не проводиться ніяких маніпуляцій, підхід потокового спостереження має ряд переваг. Оскільки основний трафік не аналізується, процес потокового спостереження відбувається швидше, ніж вищезгадані підходи мережевого моніторингу, якщо порівнювати на однаковому апаратному забезпеченні.

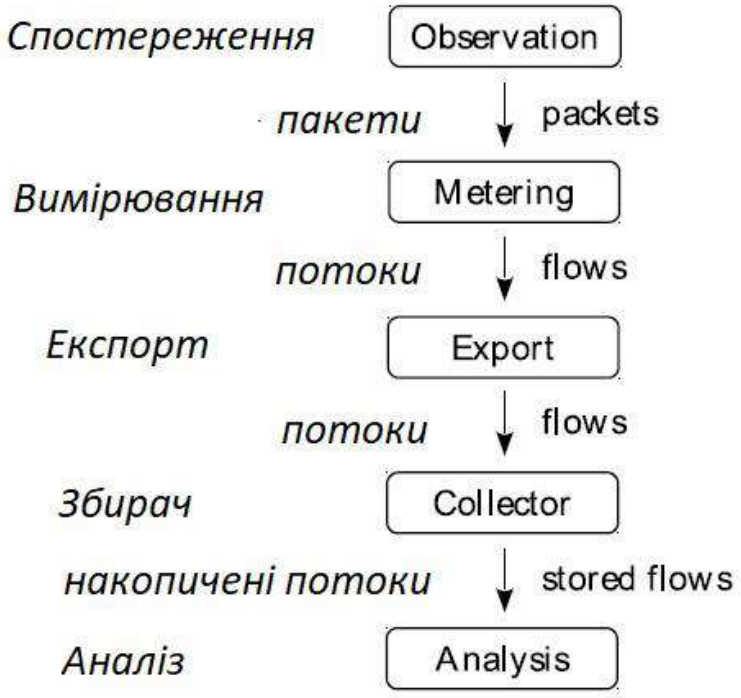


Рисунок 1.9 – Архітектура потокового спостереження

Крім того, порівняно з підходом захвату пакетів, основні дані не зберігаються, тобто потрібно зберігати набагато менше даних. Це також позитивно відзначається із законами про збереження даних, так як не зберігання основного потоку даних не може призвести до витоку персональної або корпоративної інформації.

На рисунку 1.9 показана архітектура спостереження за потоком. Після спостереження, пакети надсилаються до процесу вимірювання. Вимірювальний процес ідентифікує потоки та підраховує їх статистику. З цього моменту вихідні пакети не обробляються. Процес вимірювання надсилає інформацію про потоки до процесу експорту через певний період часу. Облік і процеси експорту зазвичай знаходяться разом у зонді мережі. Процес експорту надсилає остаточну інформацію про потік до збирача для зберігання і подальшої обробки.

Існує два помітні формати для передачі потокової інформації; NetFlow, розроблений CISCO та IPFIX (розроблено IETF). Частина існуючого потоку

програмного забезпечення експортерами є nProbe, softflowd, YAF та FlowMon; обрані колектори потоку nProbe, nfdump, flowd, IPFIXcol і SiLK.

Таблиця 1.1 показує порівняння між підходами моніторингу та представляє плюси та мінуси кожного підходу.

Таким чином, враховуючи пакети даних і потік мережевого трафіку інформації, адміністратори можуть зрозуміти поведінку мережі, наприклад, використання програми та мережі, використання мережих ресурсів, аномалії мережі та вразливі місця безпеки. мережевий трафік спочатку дублюється, а потім аналізується. Підсумовуючи, було розглянуто два способи дублювання трафіку; віддзеркалення портів і TAP. Існує три підходи до аналізу трафіку; захоплення пакетів, переважно автоматизована глибока перевірка пакетів і потік спостереження. Кожен підхід має свої сильні сторони та недоліки.

Таблиця 1.1– Порівняння підходів до моніторингу корпоративних мереж

| Підхід моніторингу | Переваги і недоліки | |
|---|---|---|
| Дзеркалювання портів | За | -Доступне широко у комутаторах |
| | Проти | -Ненадійний зв’язок |
| Тестовий порт доступу | За | -Надійний на високих швидкостях |
| | Проти | -Дорогий, вимагає роз’єднання при встановленні |
| Захват пакетів | За | - Безперешкодний доступ до повних мережевих даних протягом аналізу |
| | Проти | - Переважно ручний аналіз<br>- Не масштабується до високих швидкостей і великого розмір захоплених даних |
| Зіставлення паттернів | За | - Проста розробка правил виявлення<br>- Добре масштабується до високих швидкостей |
| | Проти | - Не всі дані можна описати шаблонами або регулярними виразами |
| Подієвий аналіз пакетів | За | - Добре масштабується до високих швидкостей |
| | Проти | - Вимагає більш складної реалізації ніж відповідність шаблону DPI<br>- Розробка правил вимагає від розробника дізнайтеся значно більше про DPI реалізації, ніж для зіставлення шаблонів |

Продовження таблиці 1.1

| Підхід моніторингу | Переваги і недоліки | |
|---|---|---|
| Потокове спостереження | За | - Конфіденційність – пакетні дані не використовуються<br>- Добре масштабується до високих швидкостей |
| | Проти | - Зберігає лише агреговані метадані про трафік<br>- Обмежені можливості аналізу даних |

## 1.2 Протоколи передачі даних SNMP, LDAP

Протокол керування мережею (SNMP) – це стандартний протокол Інтернету для збору й упорядкування інформації про керовані пристрої в IP-мережах і для зміни цієї інформації для зміни поведінки пристрою. Пристрої, які зазвичай підтримують SNMP, включають кабельні модеми, маршрутизатори, комутатори, сервери, робочі станції, принтери тощо.

SNMP широко використовується в управлінні мережею для моніторингу мережі. SNMP надає керуючі дані у вигляді змінних на керованих системах, організованих у інформаційній базі керування (MIB), яка описує стан і конфігурацію системи. Ці змінні потім можна дистанційно запитувати (і, за деяких обставин, маніпулювати) за допомогою керування програмами.

Було розроблено та розгорнуто три важливі версії SNMP. SNMPv1 є оригінальною версією протоколу. Останні версії, SNMPv2c і SNMPv3, мають покращену продуктивність, гнучкість і безпеку.

SNMP є компонентом Internet Protocol Suite, як це визначено спільнотою IETF. Він складається з набору стандартів для керування мережею, включаючи протокол прикладного рівня, схему бази даних і набір об’єктів даних.

### 1.2.1 Огляд і базові концепції

У типовому використанні SNMP один або кілька адміністративних комп’ютерів, які називаються менеджерами, виконують завдання моніторингу або керування групою хостів або пристроїв у комп’ютерній мережі. Кожна керована система виконує програмний компонент, який називається агентом, який повідомляє інформацію через SNMP менеджеру.

Мережа, керована SNMP, складається з трьох ключових компонентів:

- керовані пристрої;
- агент – програмне забезпечення, яке працює на керованих пристроях;
- станція керування мережею (NMS) – програмне забезпечення, яке працює на диспетчері.

Керований пристрій — це мережевий вузол, який реалізує інтерфейс SNMP, що забезпечує односпрямований (лише читання) або двонаправлений (читання та запис) доступ до інформації вузла. Керовані пристрої обмінюються інформацією про вузли з NMS. Керовані пристрої, які іноді називають елементами мережі, можуть бути будь-якими типами пристроїв, включаючи, але не обмежуючись, маршрутизатори, сервери доступу, комутатори, кабельні модеми, мости, концентратори, IP-телефони, IP-відеокамери, комп’ютерні хости та принтери.

Агент – це програмний модуль для керування мережею, який знаходиться на керованому пристрої. Агент має локальні знання інформації про керування та перекладає цю інформацію у форму, специфічну для SNMP, або з неї.

Станція керування мережею виконує програми, які відстежують і контролюють керовані пристрої. NMS забезпечують основну частину ресурсів обробки та пам'яті, необхідних для керування мережею. Одна чи декілька NMS можуть існувати в будь-якій керованій мережі (рисунок 1.10).

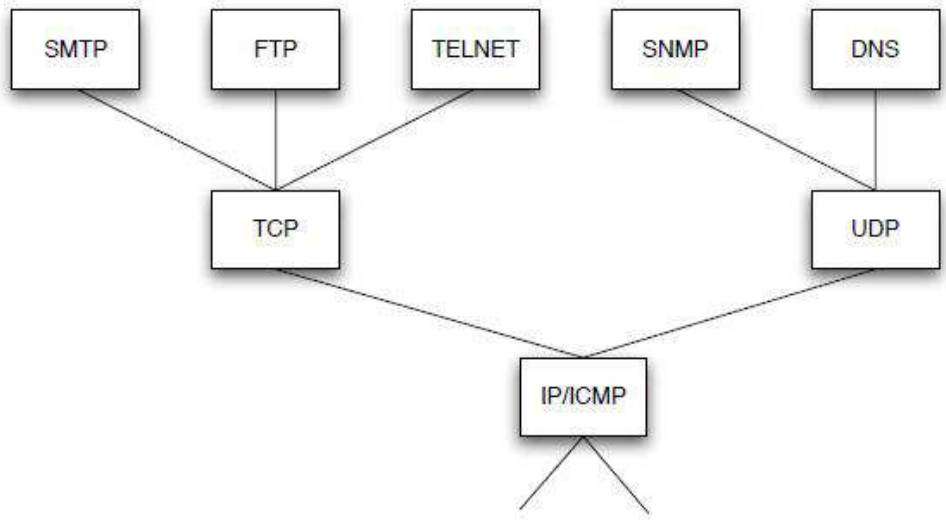


Рисунок 1.10 – SNMP – протокол прикладного рівня

Змінні, доступні через SNMP, організовані в ієрархії. Ці ієрархії та інші

Агенти SNMP надають дані керування в керованих системах як змінні. Протокол також дозволяє виконувати завдання активного керування, такі як зміни конфігурації, шляхом дистанційної модифікації цих змінних. Змінні, доступні через SNMP, організовані в ієрархії. Сам SNMP не визначає, які змінні має пропонувати керована система. Натомість SNMP використовує розширюваний дизайн, який дозволяє програмам визначати власні ієрархії. Ці ієрархії описуються як інформаційна база управління (MIB). MIB описує структуру даних керування підсистемою пристрою; вони використовують ієрархічний простір імен, що містить ідентифікатори об’єктів (OID). Кожен OID ідентифікує змінну, яку можна прочитати або встановити через SNMP. MIB використовує нотацію, визначену структурою управлінської інформації версії 2.0 (SMIv2, RFC 2578), підмножиною ASN.1

SNMP працює на прикладному рівні набору протоколів Інтернету. Усі повідомлення SNMP транспортуються через протокол UDP (User Datagram

Protocol). Агент SNMP отримує запити на UDP-порт 161. Менеджер може надсилати запити з будь-якого доступного вихідного порту на порт 161 агента. Відповідь агента надсилається назад до вихідного порту диспетчера. Менеджер отримує повідомлення (Traps і InformRequests) на порт 162. Агент може генерувати повідомлення з будь-якого доступного порту. У разі використання з безпекою транспортного рівня або безпекою транспортного рівня датаграм запити надходять на порт 10161, а повідомлення надсилаються на порт 10162.

SNMPv1 визначає п’ять основних протокольних блоків даних (PDU). Два інші PDU, GetBulkRequest і InformRequest, були додані в SNMPv2, а PDU звіту додано в SNMPv3.

### 1.2.2 Протокол LDAP

LDAP – це відкритий, нейтральний до постачальника галузевий стандартний протокол додатків для доступу та підтримки інформаційних служб розподіленого каталогу через мережу Інтернет-протоколу (IP). Служби каталогів відіграють важливу роль у розробці додатків внутрішньої мережі та Інтернету, дозволяючи обмінюватися інформацією про користувачів, системи, мережі, служби та програми по всій мережі. Як приклад, служби каталогів можуть надавати будь-який організований набір записів, часто з ієрархічною структурою, як-от корпоративний каталог електронної пошти. Так само телефонний довідник – це список абонентів із зазначенням адреси та номера телефону.

Будь-який запис у каталозі LDAP складається з одного або декількох атрибутів і володіє унікальним / розрізняльним ім'ям (DN - англ. Distinguished Name). Унікальне ім'я може виглядати, наприклад, наступним чином: «cn = Іван Петренко, ou = Співробітники, dc = example, dc = com». Унікальне ім'я складається з одного або декількох відносних унікальних імен

(RDN – англ. Relative Distinguished Name), розділених комою. Відносне унікальне ім'я має вигляд ІмяАтрибута = значення. На одному рівні каталогу не може існувати двох записів з однаковими відносними унікальними іменами. В силу цієї структури унікального імені записи в каталозі LDAP можна легко уявити у вигляді дерева.

Запис може складатися тільки з тих атрибутів, які визначені в описі класу запису (object class), які, у свою чергу, об'єднані в схеми (schema). У схемі визначено, які атрибути є для даного класу обов'язковими, а які – необов'язковими. Також схема визначає тип і правила порівняння атрибутів. Кожен атрибут запису може зберігати кілька значень.

Як правило, каталог LDAP реалізується згідно з моделлю X.500: він складається із дерева записів, кожне з яких складається із множини іменованих атрибутів зі значеннями. Деякі зі служб підтримують складнішу модель «ліс», але більшість мають лише один початковий запис.

Залежно від обраної моделі, LDAP-каталог часто віддзеркалює різноманітні політичні, географічні, та (або) організаційні регіони. Встановлені LDAP-системи схиляються до використання доменних імен (DNS) для структурування найвищих рівнів ієрархії. На нижчих рівнях в каталозі можуть бути записи, які відповідають людям, організаційним підрозділам, принтерам, документам, групам людей, або будь чому іншому, що представляє даний запис, або множину записів в каталозі.

Остання версія протоколу – LDAPv3. Стандарт LDAPv3 визначено в низці документів IETF, як описано в RFC 4510.

## 1.3 Загальні особливості, підходи та методи моніторингу трафіку в мережах

### 1.3.1 Підходи моніторингу: активний і пасивний моніторинг

Підходи моніторингу продуктивності мережі можна розділити на пасивний та активний, а також комбінований моніторинг. У техніці пасивного моніторингу мережевий трафік може спостерігатися за допомогою пристроїв моніторингу, але не можуть бути змінені жодним чином. Висновки щодо продуктивності мережі зроблені на основі зібраної інформації. Цієї інформації може бути недостатньо, щоб дозволити адміністратору робити висновки. З іншого боку, активний моніторинг передбачає введення невеликих пакетів даних у мережевий трафік з метою виробництва та збору необхідної інформації для вимірювання конкретних параметрів мережі.

Перевага активного моніторингу полягає в тому, що введений пакет даних контролюється та може бути змінений для вимірювання необхідної продуктивності мережі інформації. Таким чином, багато результатів отримуються швидше в порівнянні до техніки пасивного моніторингу. Недолік активного моніторингу полягає в тому, що навантаження на мережу збільшується завдяки додаванню тестових пакетів.

Активний метод моніторингу більше підходить для мереж з високою швидкістю передачі даних, де додавання деякого навантаження в мережу не викликає проблем із затримкою пакетів. Однак він небажаний для мереж з низькою швидкістю передачі даних, де пропускна здатність потрібна для ефективної передачі пакетів.

## 1.4 Загальна характеристика методів моніторингу корпоративної комп'ютерної мережі

### 1.4.1 Методи моніторингу мережі

IT-фахівці використовують різноманітні методи моніторингу мережі. Методи розгортаються через рішення моніторингу мережі, які автоматично виявляють і реагують на проблеми безпеки та продуктивності.

Виявлення вторгнень (Intrusion Detection): виявлення вторгнень

контролює локальні мережі на предмет несанкціонованого доступу хакерів. Цей метод можна реалізувати вручну, однак більшість IT-спеціалістів вважають за краще використовувати програму виявлення вторгнень, яка автоматично виявляє віруси та зловмисне програмне забезпечення. Програми виявлення вторгнень створюють звіти після перевірки системи, щоб можна було вирішити будь-які проблеми.

Перегляд пакетів (Packet Sniffing): аналізатор пакетів – це програма, яка перевіряє кожен пакет інформації, що проходить через мережу. Метою сніфера пакетів є виявлення несанкціонованого програмного забезпечення для моніторингу мережі, яке можуть встановити хакери для стеження за бізнес-діяльністю та інформаційними процесами.

Сканування вразливостей (Vulnerability Scanning): Сканер вразливостей періодично скануватиме мережу на наявність уразливостей і слабких місць, які відкривають потенціал для використання. Цей метод відрізняється від виявлення вторгнення, оскільки він виявляє слабкі місця до того, як відбулася атака. Виявлення вторгнень визначає несанкціонований доступ після того, як хакер зламав мережу.

Брандмауер моніторингу (Firewall Monitoring): брандмауери контролюють трафік, який надходить і виходить з мережі. Моніторинг брандмауера відстежує діяльність брандмауера, щоб переконатися, що процес перевірки вхідних і вихідних з’єднань працює належним чином і безпечно.

Тестування на проникнення (Penetration Testing). Тест на проникнення, розмовно відомий як pentest або етичне хакерство, це санкціонована імітована кібератака на комп’ютерну систему, яка виконується для оцінки безпеки системи; це не слід плутати з оцінкою вразливості. Перевірка виконується для виявлення слабких сторін (також відомих як уразливості), включно з можливістю неавторизованого доступу до функцій і даних системи, а також сильних сторін, що дозволяє повноцінно оцінити ризики бути завершеним.

#### 1.4.1.1 Виявлення вторгнень

Система виявлення вторгнень (IDS; також система запобігання вторгненням або IPS) — це пристрій або програмне забезпечення, яке відстежує мережу або системи на наявність зловмисної активності або порушень політики. Про будь-яке вторгнення або порушення зазвичай повідомляється або адміністратору, або збирається централізовано за допомогою системи керування інформацією та подіями безпеки (Security Information and Event Management – SIEM). Система SIEM поєднує виходи з кількох джерел і використовує методи фільтрації тривог, щоб відрізнити зловмисну активність від помилкових тривог.

Типи IDS варіюються від окремих комп'ютерів до великих мереж. Найпоширенішими класифікаціями є системи виявлення вторгнення в мережу (NIDS) і системи виявлення вторгнення на основі хоста (HIDS). Система, яка відстежує важливі файли операційної системи, є прикладом HIDS, тоді як система, яка аналізує вхідний мережевий трафік, є прикладом NIDS. Також можна класифікувати IDS за методом виявлення. Найвідоміші варіанти – це виявлення на основі сигнатур (розпізнавання поганих шаблонів, наприклад зловмисного програмного забезпечення) та виявлення на основі аномалій (виявлення відхилень від моделі «хорошого» трафіку, яка часто покладається на машинне навчання). Іншим поширеним варіантом є виявлення на основі репутації (розпізнавання потенційної загрози за балами репутації). Деякі продукти IDS мають здатність реагувати на виявлені вторгнення. Системи з можливостями реагування зазвичай називають системами запобігання вторгненням. Системи виявлення вторгнень також можуть служити певним цілям, доповнюючи їх спеціальними інструментами, такими як використання honeypot для залучення та визначення характеристик шкідливого трафіку.

Системи запобігання вторгненням можна класифікувати на чотири

різні типи:

- мережева система запобігання вторгненням (NIPS): контролює всю мережу на наявність підозрілого трафіку шляхом аналізу активності протоколу;
- система запобігання бездротовому вторгненню (WIPS): перевіряйте бездротову мережу на наявність підозрілого трафіку шляхом аналізу протоколів бездротової мережі;
- аналіз поведінки мережі (NBA): аналізує мережевий трафік, щоб виявити загрози, які створюють незвичайні потоки трафіку, наприклад атаки розподіленої відмови в обслуговуванні (DDoS), певні форми зловмисного програмного забезпечення та порушення політики;
- система запобігання вторгнень на основі хоста (HIPS): встановлений програмний пакет, який відстежує підозрілу активність на одному хості шляхом аналізу подій, що відбуваються на цьому хості.

Більшість систем запобігання вторгненням використовують один із трьох методів виявлення: на основі сигнатур, на основі статистичних аномалій та аналіз протоколу з урахуванням стану.

Виявлення на основі сигнатур: IDS на основі сигнатур відстежує пакети в мережі та порівнює їх із попередньо налаштованими та визначеними шаблонами атак, відомими як сигнатури.

Виявлення на основі статистичних аномалій: IDS, яка базується на аномаліях, відстежуватиме мережевий трафік і порівнюватиме його зі встановленою базовою лінією. Базовий рівень визначає, що є «нормальним» для цієї мережі – яка пропускна здатність зазвичай використовується та які протоколи використовуються. Однак він може викликати хибно-позитивний сигнал тривоги для законного використання пропускної здатності, якщо базові лінії не налаштовані правильно. Ансамблеві моделі, які використовують коефіцієнт кореляції Метьюза для ідентифікації несанкціонованого мережевого трафіку, отримали точність 99,73%.

Виявлення аналізу стану протоколу: цей метод визначає відхилення

станів протоколу шляхом порівняння спостережуваних подій із «попередньо визначеними профілями загальноприйнятих визначень доброякісної активності».

Правильне розміщення систем виявлення вторгнень є критичним і залежить від мережі. Найпоширеніше розміщення – за брандмауером, на межі мережі. Ця практика забезпечує IDS високу видимість трафіку, що надходить у вашу мережу, і не отримуватиме жодного трафіку між користувачами в мережі. Край мережі – це точка, в якій мережа підключається до екстранету. Ще одна практика, яку можна реалізувати, якщо доступні додаткові ресурси, – це стратегія, за якої технік розміщує свій перший IDS у точці найвищої видимості, а залежно від доступності ресурсу розміщує інший у наступній найвищій точці, продовжуючи цей процес, доки всі точки мережі охоплені.

Якщо IDS розміщено за межами мережевого брандмауера, його основною метою буде захист від шуму з Інтернету, але, що більш важливо, захист від типових атак, таких як сканування портів і картографування мережі. IDS у цій позиції відстежуватиме рівні з 4 по 7 моделі OSI та базуватиметься на сигнатурах. Це дуже корисна практика, оскільки замість показу фактичних зламів мережі, які пройшли через брандмауер, будуть показані спроби зломів, що зменшує кількість помилкових спрацьовувань. IDS у цій позиції також допомагає зменшити кількість часу, необхідного для виявлення успішних атак на мережу.

Іноді IDS з більш розширеними функціями буде інтегровано з брандмауером, щоб мати можливість перехоплювати складні атаки, що проникають у мережу. Приклади розширених функцій включають кілька контекстів безпеки на рівні маршрутизації та режимі мосту. Все це, у свою чергу, потенційно знижує вартість і складність експлуатації.

Інший варіант розміщення IDS – у реальній мережі. Вони виявлять атаки або підозрілу активність у мережі. Ігнорування безпеки в мережі може спричинити багато проблем, це або дозволить користувачам створювати

ризики безпеці, або дозволить зловмиснику, який уже зламався в мережу, вільно блукати. Інтенсивна безпека інтрамережі ускладнює навіть хакерам у мережі маневрувати та підвищувати свої привілеї.

Шум (у обробці сигналу шум – це загальний термін для небажаних модифікацій, яких сигнал може зазнати під час захоплення, зберігання, передачі, обробки або перетворення) може серйозно обмежити ефективність системи виявлення вторгнень. Погані пакети, згенеровані через помилки програмного забезпечення, пошкоджені дані DNS і локальні пакети, які втекли, можуть створити значно високий рівень помилкових тривог.

Нерідкі випадки, коли кількість реальних атак значно нижча за кількість помилкових тривог. Кількість реальних атак часто настільки нижча за кількість помилкових тривог, що справжні атаки часто пропускають та ігнорують.

Багато атак спрямовані на певні версії програмного забезпечення, які зазвичай є застарілими. Бібліотека сигнатур, що постійно змінюється, потрібна для пом’якшення загроз. Застарілі бази даних сигнатур можуть зробити IDS вразливим до нових стратегій.

Для IDS на основі сигнатур буде затримка між виявленням нової загрози та її підписом, застосованим до IDS. Протягом цього часу затримки IDS не зможе ідентифікувати загрозу. Він не може компенсувати слабкі механізми ідентифікації та автентифікації або слабкі місця в мережевих протоколах. Коли зловмисник отримує доступ через слабкі механізми автентифікації, IDS не може запобігти зловмиснику від будь-яких зловживань.

Зашифровані пакети не обробляються більшістю пристроїв виявлення вторгнень. Таким чином, зашифрований пакет може дозволити вторгнення в мережу, яке не буде виявлено, доки не відбудуться більш значні вторгнення в мережу.

Програмне забезпечення для виявлення вторгнень надає інформацію на основі мережевої адреси, пов’язаної з IP-пакетом, надісланим у мережу. Це

корисно, якщо мережева адреса, що міститься в IP-пакеті, точна. Однак адреса, яка міститься в IP-пакеті, може бути підробленою або зашифрованою.

Через природу систем NIDS і потребу в них аналізувати протоколи під час їх захоплення системи NIDS можуть бути сприйнятливі до тих самих атак на основі протоколу, до яких можуть бути вразливі мережеві хости. Недійсні дані та атаки на стек TCP/IP можуть призвести до збою NIDS.

Заходи безпеки в хмарних обчисленнях не враховують варіацію потреб користувачів щодо конфіденційності. Вони забезпечують однаковий механізм безпеки для всіх користувачів, незалежно від того, чи є вони компаніями чи окремими особами.

Найперша попередня концепція IDS була окреслена в 1980 році Джеймсом Андерсоном з Агентства національної безпеки та складалася з набору інструментів, призначених для допомоги адміністраторам у перегляді журналів аудиту. Журнали доступу користувачів, журнали доступу до файлів і журнали системних подій є прикладами журналів аудиту.

Фред Коен зазначив у 1987 році, що неможливо виявити вторгнення в кожному випадку, і що ресурси, необхідні для виявлення вторгнень, зростають разом із обсягом використання. [4]

### 1.4.1.2 Перегляд пакетів

Аналізатор пакетів, також відомий як прослуховувач пакетів (packet sniffer), аналізатор протоколів або мережевий аналізатор – це комп’ютерна програма або комп’ютерне обладнання, наприклад пристрій захоплення пакетів, який може перехоплювати та реєструвати трафік, що проходить через комп’ютерну мережу або частину мережі. Перехоплення пакетів – це процес перехоплення та реєстрації трафіку. Коли потоки даних проходять по мережі, аналізатор фіксує кожен пакет і, якщо необхідно, декодує необроблені дані пакета, показуючи значення різних полів у пакеті, і аналізує його вміст відповідно до відповідних RFC або інших специфікацій.

Аналізатор пакетів, який використовується для перехоплення трафіку в бездротових мережах, називається бездротовим аналізатором або аналізатором WiFi. Хоча аналізатор пакетів також можна називати мережевим аналізатором або аналізатором протоколів, ці терміни також можуть мати інші значення. Технічно аналізатор протоколу може бути ширшим, загальнішим класом, який включає аналізатори/аналізатори пакетів. Однак ці терміни часто використовуються як синоніми.

На початку 1990-х років він широко використовувався хакерами для захоплення логінів і паролів користувачів, які передаються незашифрованими або слабко зашифрованими в ряді мережевих протоколів. Широке поширення концентраторів дозволило без особливих зусиль перехоплювати трафік у великих сегментах локальної мережі практично без ризику бути виявленим.

Сніфери використовуються як для хороших, так і для руйнівних цілей. Аналіз трафіку, що пройшов через сніффер, дозволяє:

- виявлення паразитного, вірусного і кільцевого трафіку, наявність якого підвищує завантаження мережевого обладнання і каналів зв'язку (тут сніфери малоефективні, як правило, для цих цілей використовують збір різної статистики серверами і активною мережею. обладнання та їх подальший аналіз);

- виявляти в мережі шкідливе та несанкціоноване програмне забезпечення, наприклад, мережеві сканери, флудери, троянські програми, клієнти піринговых мереж та інше (зазвичай це робиться за допомогою спеціалізованих сніфферів – моніторів мережевої активності).

- перехоплювати будь-який незашифрований (а іноді зашифрований) трафік, призначений для користувача, щоб отримати паролі та іншу інформацію;

- локалізація несправності мережі або помилки конфігурації мережевих агентів (для цього системні адміністратори часто використовують сніфери).

Оскільки в «класичному» сніфері аналіз трафіку виконується вручну, використовуючи лише прості засоби автоматизації (аналіз протоколів, відновлення TCP-потоку), він підходить для аналізу лише невеликих його обсягів. Найпоширеніші сніфери: Wireshark, Allegro Network Multimeter, Capsa Network Analyzer, Charles Web Debugging Proxy, Carnivore (software), CommView, dSniff, EndaceProbe Packet Capture Platform, ettercap, Fiddler, Kismet, Lanmeter, Microsoft Network Monitor, NarusInsight, NetScout Systems nGenius Infinistream, ngrep, Network Grep, OmniPeek, Omnipliance by Savvius та багато інших.

Перехоплення пакетів може використовуватися для виконання ордера правоохоронних органів на прослуховування всього мережевого трафіку, створеного особою. Постачальники послуг Інтернету та провайдери VoIP у Сполучених Штатах повинні дотримуватися положень Закону про підтримку зв’язку для правоохоронних органів. Використовуючи захоплення та зберігання пакетів, телекомунікаційні оператори можуть забезпечити необхідний за законом безпечний і окремий доступ до цільового мережевого трафіку та можуть використовувати той самий пристрій для цілей внутрішньої безпеки. Збір даних із системи оператора без ордера є незаконним через закони про перехоплення. Використовуючи наскрізне шифрування, зв’язок може бути конфіденційним від операторів зв’язку та судових органів.

#### 1.4.1.3 Сканування вразливостей

Оцінка вразливості – це процес визначення, ідентифікації та класифікації прогалин у безпеці систем інформаційних технологій. Зловмисник може використати вразливість, щоб порушити безпеку системи. Деякі ві-домі вразливості: уразливість автентифікації, уразливість авторизації та вразливість перевірки введення.

Перш ніж розгортати систему, вона спочатку повинна пройти серію

оцінок вразливості, які гарантують, що система збірки захищена від усіх відомих ризиків безпеки. Коли виявляється нова вразливість, системний адміністратор може знову виконати оцінку, виявити, які модулі є вразливими, і почати процес виправлення. Після виправлення можна запустити іншу оцінку, щоб переконатися, що вразливості справді усунено. Цей цикл оцінки, виправлення та повторної оцінки став стандартним методом для багатьох організацій для вирішення проблем безпеки.

Основною метою оцінки є виявлення вразливостей у системі, але звіт про оцінку повідомляє зацікавленим сторонам, що система захищена від цих уразливостей. Якщо зловмисник отримав доступ до мережі, що скла-дається з уразливих веб-серверів, можна з упевненістю припустити, що він також отримав доступ до цих систем. Завдяки звіту про оцінку адміністратор безпеки зможе визначити, як сталося вторгнення, ідентифікувати скомпрометовані активи та вжити відповідних заходів безпеки, щоб запобігти критичному пошкодженню системи [6].

Залежно від системи оцінка вразливості може мати багато типів і рівнів.

Оцінка хосту. Оцінка хосту шукає вразливості на системному рівні, такі як незахищені дозволи на файли, помилки на рівні програми, встановлення бекдорів і троянських програм. Для цього потрібні спеціалізовані інструменти для операційної системи та пакетів програмного забезпечення, що використовуються, на додаток до адміністративного доступу до кожної системи, яку потрібно перевірити. Оцінка хоста часто дуже дорога з точки зору часу, і тому використовується лише для оцінки критичних систем. Такі інструмен-ти, як COPS і Tiger, популярні в оцінці хостів.

Оцінка мережі. Під час оцінки мережі оцінюють мережу на відомі вразливості. Він знаходить усі системи в мережі, визначає, які мережеві служби використо-вуються, а потім аналізує ці служби на потенційну вразливість. Цей процес не вимагає жодних змін у конфігурації систем, що

оцінюються. На відміну від оцінки хоста, оцінка мережі вимагає невеликих обчислювальних витрат і зусиль.

#### 1.4.1.4 Брандмауер моніторингу

Міжмережевий екран, мережевий екран, брандмауер, брандмауер, брандмауер (англ. Firewall, firewall) – загальна назва фізичних пристроїв або програмних додатків, налаштованих на дозвіл, заборону, шифрування, передачу мережевого трафіку між областями різної безпеки мережі відповідно до з бажаним набором правил безпеки [7].

Брандмауер може бути у вигляді окремого пристрою (так званого маршрутизатора або роутера), або програмного забезпечення, яке встановлюється на персональний комп'ютер або проксі-сервер. Простий і дешевий брандмауер може не мати такої гнучкої системи налаштування правил фільтрації пакетів і трансляції адрес вхідного і вихідного трафіку (функція переадресації).

Залежно від активних підключень, які контролюються, брандмауери поділяються на:

- stateless – без збереження стану (проста фільтрація), які не відстежують поточні з'єднання (наприклад, TCP), а фільтрують потік даних виключно на основі статичних правил;

- stateful (фільтрація з урахуванням контексту), з моніторингом поточних з'єднань і пропусканням тільки таких пакетів, які відповідають логіці та алгоритмам відповідних протоколів і програм. Ці види брандмауерів дозволяють більш ефективно боротися з різними DDoS-атаками і вразливістю деяких мережевих протоколів.

Щоб задовольнити вимоги широкого кола користувачів, існує три типи брандмауерів: мережевий рівень, рівень додатків і рівень підключення. Кожен із цих трьох типів має свій підхід до безпеки мережі.

Брандмауер мережевого рівня представлений екрануючим

маршрутизатором. Він контролює лише інформаційні дані пакетної служби мережевого та транспортного рівнів моделі OSI. Недоліком таких маршрутизаторів є те, що ще п'ять рівнів залишаються неконтрольованими. Нарешті, адміністратори, які працюють із екранованими маршрутизаторами, повинні знати, що більшість пристроїв фільтрації пакетів не мають механізмів аудиту та сигналізації. Іншими словами, маршрутизатори можуть бути атаковані та відбити їх велику кількість, навіть не проінформувавши адміністраторів.

Брандмауер на рівні програми також відомий як проксі-сервер. Брандмауери прикладного рівня встановлюють певне фізичне розділення між локальною мережею та Інтернетом, тому вони відповідають найвищим вимогам безпеки. Однак, оскільки програма повинна аналізувати пакети та приймати рішення про контроль доступу до них, брандмауери на рівні програми неминуче знижують продуктивність мережі, тому швидші комп’ютери використовуються як проксі-сервери.

Брандмауер рівня підключення подібний до брандмауера прикладного рівня тим, що вони обидва є проксі-серверами. Різниця полягає в тому, що брандмауери прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби, наприклад FTP або HTTP. Натомість брандмауери рівня підключення підтримують велику кількість протоколів.

#### 1.4.1.5 Тестування на проникнення

Тест на проникнення (тест на проникнення, pentesting) – метод оцінки безпеки комп'ютерної системи або мережі шляхом часткової імітації дій зовнішніх зловмисників (які не мають авторизованого доступу до системи) і внутрішніх зловмисників (які мають певний авторизований доступ рівня) [8]. Цей процес передбачає активний аналіз системи на наявність будь-якої потенційної вразливості, яка може виникнути внаслідок неправильної

конфігурації системи, відомих і невідомих дефектів апаратного та програмного забезпечення або операційних помилок у процедурних чи технічних заходах протидії. Цей аналіз виконується з точки зору потенційного зловмисника та може включати активне використання вразливостей.

Проблеми безпеки, виявлені під час тесту на проникнення, представлені власнику системи. Ефективний тест на проникнення поєднує цю інформацію з точною оцінкою потенційного впливу на організацію та окреслює межі технічних і процедурних контрзаходів для зменшення ризиків.

У процесі зазвичай визначаються цільові системи та конкретна ціль, потім переглядається доступна інформація та вживаються різні засоби для досягнення цієї мети. Об’єктом тесту на проникнення може бути біла скринька (про яку тестеру заздалегідь надається фонова та системна інформація) або чорна скринька (про яку надається лише основна інформація, якщо така є, крім назви компанії). Тест на проникнення в сірий ящик є комбінацією обох (де аудитору надаються обмежені знання про ціль). Тест на проникнення може допомогти виявити вразливість системи для атаки та оцінити, наскільки вона вразлива.

Про проблеми безпеки, які виявляє тест на проникнення, слід повідомляти власнику системи. Звіти про тестування на проникнення також можуть оцінити потенційний вплив на організацію та запропонувати контрзаходи для зменшення ризику.

Британський національний центр кібербезпеки описує тестування на проникнення як: «Метод отримання впевненості в безпеці IT-системи шляхом спроби порушити частину або всю безпеку цієї системи, використовуючи ті самі інструменти та методи, що й зловмисник».

Цілі тесту на проникнення відрізняються залежно від типу схваленої діяльності для будь-якої конкретної взаємодії, причому головна мета зосереджена на пошуку вразливостей, якими може скористатися зловмисник,

і інформуванні клієнта про ці вразливості разом із рекомендованими стратегіями пом’якшення.

Тести на проникнення є складовою повного аудиту безпеки. Наприклад, стандарт безпеки даних індустрії платіжних карток вимагає тестування на проникнення за регулярним графіком і після зміни системи. Тестування на проникнення також може підтримувати оцінку ризиків, як зазначено в NIST Risk Management Framework SP 800-53.

Існує кілька стандартних структур і методологій для проведення тестів на проникнення. Серед них Посібник з методології тестування безпеки з відкритим кодом (OSSTMM), Стандарт виконання тестування на проникнення (PTES), Спеціальна публікація NIST 800-115, Структура оцінки безпеки інформаційної системи (ISSAF) і Посібник з тестування OWASP. CREST, некомерційна професійна організація для індустрії технічної кібербезпеки, надає свій стандарт CREST Defensible Penetration Test, який надає промисловості вказівки щодо комерційно обґрунтованої діяльності під час проведення тестів на проникнення.

Методологія гіпотези недоліків – це техніка системного аналізу та прогнозування проникнення, у якій список гіпотетичних недоліків у системі програмного забезпечення складається шляхом аналізу специфікацій і документації до системи. Список гіпотетичних недоліків потім розставляється за пріоритетністю на основі оціненої ймовірності того, що недолік дійсно існує, і на основі легкості його використання в міру контролю або компромісу. Список пріоритетів використовується для керування фактичним тестуванням системи.

Існують різні типи тестування на проникнення, залежно від цілей організації, які включають: мережу (зовнішню та внутрішню), бездротову мережу, веб-додаток, соціальну інженерію та перевірку виправлення.

До середини 1960-х рр. зростаюча популярність комп’ютерних систем із розподілом часу, які зробили ресурси доступними через лінії зв’язку, створила нові проблеми безпеки. Як пояснюють вчені Дебора Рассел і Г. Т.

Гангемі старший, «1960-ті ознаменували справжній початок ери комп’ютерної безпеки».

У червні 1965 року, наприклад, кілька провідних американських експертів з комп’ютерної безпеки провели одну з перших великих конференцій з системної безпеки, яку організував державний підрядник System Development Corporation (SDC). Під час конференції хтось зазначив, що один співробітник SDC зміг легко підірвати різні системні засоби захисту, додані до комп’ютерної системи розподілу часу AN/FSQ-32 SDC. У надії, що подальше вивчення безпеки системи буде корисним, учасники попросили «...дослідження проводити в таких сферах, як порушення захисту системи з розділеним часом». Іншими словами, учасники конференції ініціювали один із перших офіційних запитів на використання комп’ютерного проникнення як інструменту вивчення системної безпеки.

На Об'єднаній комп'ютерній конференції навесні 1967 року багато провідних комп'ютерних спеціалістів знову зустрілися, щоб обговорити питання безпеки системи. Під час цієї конференції експерти з комп’ютерної безпеки Вілліс Вер, Гарольд Петерсен і Рейн Терн, усі з корпорації RAND, і Бернард Пітерс з Агентства національної безпеки (АНБ) використовували фразу «проникнення» для опису атаки на комп’ютер. система. У своїй статті Вейр посилався на військові системи розподілу часу з дистанційним доступом, попереджаючи, що «слід передбачити навмисні спроби проникнення в такі комп’ютерні системи». Його колеги Петерсен і Терн поділяли те саме занепокоєння, зазначивши, що системи онлайн-комунікації «...вразливі до загроз приватності», включаючи «навмисне проникнення». Бернард Пітерс з АНБ висловив те ж саме, наполягаючи на тому, що комп’ютерний ввід і вихід «...можуть надати великі обсяги інформації проникливій програмі». Під час конференції проникнення комп’ютерів було офіційно визначено як головну загрозу онлайн-комп’ютерним системам.

Загроза, яку становило проникнення до комп’ютерів, була наступним чином окреслена у великій доповіді, організованій Міністерством оборони

США (DoD) наприкінці 1967 року. По суті, чиновники DoD звернулися до Вілліса Уера, щоб він очолював робочу групу експертів з АНБ, ЦРУ, Міністерства оборони, науковим колам і промисловості для офіційної оцінки безпеки комп'ютерних систем із розподілом часу. Спираючись на численні документи, представлені під час об'єднаної комп'ютерної конференції навесні 1967 року, цільова група значною мірою підтвердила загрозу безпеці системи, яку становило проникнення комп'ютерів. Спочатку доповідь Вейра була засекречена, але багато провідних комп'ютерних експертів країни швидко визначили це дослідження як остаточний документ з комп'ютерної безпеки. Джеффрі Р. Йост з Інституту Чарльза Беббіджа нещодавно описав звіт Вера як «...на сьогоднішній день найважливіше та ґрунтовне дослідження технічних та операційних питань, що стосуються захищених обчислювальних систем того часу». Фактично, У доповіді Ware ще раз підтверджується головна загроза, яку представляє проникнення до комп'ютерів для нових онлайнових комп'ютерних систем розподілу часу.

Для тестування на проникнення доступний широкий спектр інструментів оцінки безпеки, включаючи безкоштовне та комерційне програмне забезпечення.

Існує кілька дистрибутивів операційних систем, спрямовані на тестування на проникнення. Такі дистрибутиви зазвичай містять попередньо упакований і налаштований набір інструментів. Тестеру проникнення не потрібно шукати кожен окремий інструмент, що може збільшити ризик ускладнень, таких як помилки компіляції, проблеми залежностей і помилки конфігурації. Крім того, придбання додаткових інструментів може бути непрактичним у контексті тестувальника.

Серед відомих прикладів ОС тестування на проникнення:

- BlackArch на основі Arch Linux;
- BackBox на основі Ubuntu;
- Kali Linux (замінено BackTrack у грудні 2012 р.) на основі Debian;
- ОС Parrot Security на основі Debian;

- Pentoo на основі Gentoo;
- WHAX на основі Slackware.

Багато інших спеціалізованих операційних систем полегшують тестування на проникнення – кожна більш-менш присвячена певній області тестування на проникнення.

Кілька дистрибутивів Linux містять відомі вразливості ОС і додатків, і їх можна розгортати як цілі для практики. Такі системи допомагають новачкам у сфері безпеки випробувати новітні інструменти безпеки в лабораторних умовах. Приклади включають Damn Vulnerable Linux (DVL), OWASP Web Testing Environment (WTW) і Metasploitable.

Процес тестування на проникнення можна спростити в наступні п'ять етапів.

Етап 1. Розвідка: акт збору важливої інформації про цільову систему. Ця інформація може бути використана для кращої атаки на ціль. Наприклад, пошукові системи з відкритим кодом можна використовувати для пошуку даних, які можна використати в атаці соціальної інженерії.

Етап 2. Сканування: використовує технічні інструменти, щоб розширити знання зловмисника про систему. Наприклад, Nmap можна використовувати для пошуку відкритих портів.

Етап 3. Отримання доступу: використовуючи дані, зібрані на етапах розвідки та сканування, зловмисник може використовувати корисне навантаження для використання цільової системи. Наприклад, Metasploit можна використовувати для автоматизації атак на відомі вразливості.

Етап 4. Підтримка доступу: підтримка доступу вимагає виконання кроків, пов’язаних із можливістю постійного перебування в цільовому середовищі, щоб зібрати якомога більше даних.

Етап 5. Приховування слідів: зловмисник повинен очистити будь-які сліди компрометації системи жертви, будь-який тип зібраних даних, журнальних подій, щоб залишитися анонімним.

Після того, як зловмисник скористався однією вразливістю, він може

отримати доступ до інших машин, тому процес повторюється, тобто вони шукають нові вразливості та намагаються їх використати. Цей процес називається обертанням (pivoting).

Правові операції, які дозволяють тестувальнику виконати незаконну операцію, включають неекрановані команди SQL, незмінені хешовані паролі в проектах, видимих для джерела, людські відносини та старі хешування або криптографічні функції. Одного недоліку може бути недостатньо, щоб активувати критично серйозний експлойт. Майже завжди потрібне використання кількох відомих недоліків і формування корисного навантаження таким чином, щоб це виглядало як дійсна операція. Metasploit надає бібліотеку Ruby для типових завдань і підтримує базу даних відомих експлойтів.

Під час роботи в умовах обмеженого бюджету та часу фаззинг є поширеною технікою, яка виявляє вразливі місця. Він спрямований на отримання необробленої помилки через випадковий вхід. Тестер використовує випадковий вхід для доступу до менш часто використовуваних шляхів коду. Добре проторені кодові шляхи зазвичай не містять помилок. Помилки корисні, оскільки вони або надають більше інформації, як-от збої HTTP-сервера з повним відстеженням інформації, або їх можна використовувати безпосередньо, як-от переповнення буфера.

Наприклад,  веб-сайт має 100 полів для введення тексту. Деякі з них уразливі до SQL-ін’єкцій у певних рядках. Надсилання випадкових рядків до цих полів на деякий час, потрапить на шлях коду з помилками. Помилка проявляється як пошкоджена HTML-сторінка, наполовину відтворена через помилку SQL. У цьому випадку лише текстові поля розглядаються як вхідні потоки. Проте програмні системи мають багато можливих вхідних потоків, таких як файли cookie та дані сеансу, потік завантажених файлів, канали RPC або пам’ять. Помилки можуть статися в будь-якому з цих вхідних потоків. Мета тесту – спочатку отримати необроблену помилку, а потім зрозуміти недолік на основі невдалого тесту. Тестувальники створюють

автоматизований інструмент для перевірки свого розуміння недоліку, доки він не буде правильний. Після цього може стати очевидним, як упакувати корисне навантаження, щоб цільова система ініціювала його виконання. Якщо це неможливо, можна сподіватися, що інша помилка, створена фаззером (fuzzer), принесе більше плодів. Використання фаззера економить час, не перевіряючи відповідні шляхи коду там, де експлойти малоймовірні.

У той час як тестування на проникнення зосереджується на атаках на програмне забезпечення та комп'ютерні системи з самого початку – наприклад, сканування портів, перевірка відомих дефектів у протоколах і програмах, що працюють у системі, встановлення виправлень – етичний злом (ethical hacking) може включати й інші речі. Повномасштабний етичний хак може включати електронний лист до співробітників із запитом про пароль, нишпоріння в корзинах та інших сховищах службових бінарних даних (executive dustbins), як правило, без відома та згоди цілей. Лише власники, генеральні директори та члени правління (зацікавлені сторони), які звернулися з проханням про перевірку безпеки такого масштабу, знають про перевірку. Щоб спробувати відтворити деякі з руйнівних методів, які може застосувати справжня атака, етичні хакери можуть організувати клонування тестових систем або організувати злом пізно вночі, коли системи менш критичні. У останніх випадках ці хакерські атаки зберігаються протягом тривалого періоду (дні, якщо не тижні, тривалого проникнення людини в організацію). Деякі приклади включають залишення USB/флеш-накопичувачів із прихованим програмним забезпеченням автозапуску в громадському місці, ніби хтось загубив маленький диск, а нічого не підозрюючий працівник знайшов його та забрав.

Деякі інші методи їх виконання включають:

- криміналістика дисків і пам'яті;
- DoS-атаки.

Такі фреймворки, як:

- Metasploit;

- Network Security;
- Reverse engineering.

Сканери безпеки, такі як:

- Burp Suite;
- Nessus;
- W3af;
- тактика соціальної інженерії;
- навчальні платформи;
- дослідження вразливості.

Ці методи виявляють використання відомих вразливостей безпеки та намагаються уникнути безпеки, щоб отримати доступ до захищених зон. Вони можуть зробити це, приховавши «задні двері» програмного забезпечення та системи, які можна використовувати як посилання на інформацію або доступ, до якого може захотіти отримати неетичний хакер, також відомий як «чорний капелюх» або «сірий капелюх».

Підводячи підсумок, слід зазначити, що незалежно від конфігурації сервера, розподілу прав повністю захистити себе від впровадження подібного роду вразливостей неможливо. Найбільш оптимальним рішенням є фільтрація даних, які передає користувач. Це те, що програмісти повинні враховувати при написанні сценаріїв, при використанні даних методів вирішення завдань [13].

## 1.5 Основні засоби (механізми) моніторингу трафіку в мережах рівня корпоративної LAN

Тема моніторингу продуктивності мережі має велике значення – більшість мережевих дослідницьких груп розробили власні засоби вимірювання продуктивністі мереж. У цьому розділі представлені деякі з найбільш відомих інструментів, доступних для мережевих вимірювань. Їх мета – вимірювання загальних показників продуктивності мережі, таких як

час затримки RTT, пропускна здатність, втрата пакетів тощо.

### 1.5.1 Пінг-програма (Ping)

Програма ping, написана Майком Муссом, є діагностичним інструментом для обстеження чи доступний інший хост чи ні. Пінг (англ. Packet Inter-Network Groper, PING) – службова комп'ютерна програма, призначена для перевірки з'єднань в мережах на основі TCP/IP.

Вона відправляє запити (англ. Echo-Request) протоколу ICMP зазначеному вузлу мережі й фіксує відповіді (англ. Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати двосторонні затримки у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв.

Вона надсилає запити протоколу ICMP (Echo-Request) до вказаного вузла мережі та записує відповіді (Echo-Reply). Час між відправкою запиту і отриманням відповіді (RTT, від англ. Round Trip Time) дозволяє визначити двосторонні затримки в маршруті і частоту втрати пакетів, тобто побічно визначити завантаженість каналів передачі даних. і проміжні пристрої.

Повна відсутність відповідей ICMP також може означати, що віддалений вузол (або один із проміжних маршрутизаторів) блокує ехо-відповідь ICMP або ігнорує ехо-запит ICMP.

Програма ping є одним з основних інструментів діагностики в мережах TCP/IP і входить до складу всіх сучасних мережевих операційних систем. Функція ping також реалізована в деяких вбудованих операційних системах маршрутизаторів, доступ до результатів ping для таких пристроїв за допомогою протоколу SNMP визначається стандартами (English Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations) [14].

### 1.5.2 Програма Traceroute

В обчислювальній техніці traceroute і tracert – це діагностичні команди комп’ютерної мережі для відображення можливих маршрутів (шляхів) і вимірювання затримок передавання пакетів через мережу Інтернет-протоколу (IP). Історія маршруту записується як час проходження пакетів, отриманих від кожного наступного хоста (віддаленого вузла) на маршруті (шляху); сума середнього часу в кожному стрибку є мірою загального часу, витраченого на встановлення з'єднання. Traceroute продовжує роботу, якщо всі (зазвичай три) надіслані пакети не втрачаються більше двох разів; тоді з’єднання втрачається, і маршрут неможливо оцінити. Ping, з іншого боку, обчислює лише остаточний час у зворотному напрямку від пункту призначення.

Для Інтернет-протоколу версії 6 (IPv6) інструмент іноді має назву traceroute6 і tracert6.

Команда traceroute доступна в багатьох сучасних операційних системах. У Unix-подібних системах, таких як FreeBSD, macOS і Linux, він доступний як інструмент командного рядка. Traceroute також доступний у графічному вигляді в macOS у пакеті мережевих утиліт; ці утиліти застаріли після випуску macOS Big Sur.

Microsoft Windows і ReactOS надають програму під назвою tracert, яка виконує ту саму функцію трасування маршруту. Операційні системи на базі Windows NT також забезпечують PathPing, який поєднує в собі функції ping і tracert. Версія ReactOS була розроблена Гедом Мерфі та ліцензована під GPL.

В Unix-подібних операційних системах traceroute надсилає за замовчуванням послідовність пакетів протоколу дейтаграм користувача (UDP) із номерами портів призначення в діапазоні від 33434 до 33534; реалізації traceroute, що постачаються з Linux, FreeBSD, NetBSD, OpenBSD, DragonFly BSD і macOS, включають опцію використання пакетів ICMP Echo Request (-I) або будь-яких довільний протокол (-P), такий як UDP, TCP з використанням пакетів TCP SYN або ICMP.[10]

У Windows tracert надсилає пакети ICMP Echo Request, а не UDP-пакети, які traceroute надсилає за замовчуванням.

Значення часу життя (TTL), також відоме як обмеження стрибків (hop limit), використовується для визначення проміжних маршрутизаторів, які проходять до пункту призначення. Traceroute надсилає пакети зі значеннями TTL, які поступово зростають від пакета до пакета, починаючи зі значення TTL одиниці. Маршрутизатори зменшують значення TTL пакетів на одиницю під час маршрутизації та відкидають пакети, значення TTL яких досягло нуля, повертаючи повідомлення про помилку ICMP ICMP Time Exceeded. Для першого набору пакетів перший маршрутизатор отримує пакет, зменшує значення TTL і відкидає пакет, оскільки тоді він має нульове значення TTL. Маршрутизатор надсилає повідомлення ICMP Time Exceeded назад до джерела. Наступному набору пакетів надається значення TTL, що дорівнює двом, тому перший маршрутизатор пересилає пакети, а другий маршрутизатор відкидає їх і відповідає ICMP Time Exceeded. Продовжуючи таким чином, traceroute використовує повернуті повідомлення ICMP Time Exceeded для створення списку маршрутизаторів, через які проходять пакети, доки не буде досягнуто пункту призначення, і повертає повідомлення ICMP Destination Unreachable, якщо використовуються UDP-пакети, або повідомлення ICMP Echo Reply, якщо ICMP Echo використовуються повідомлення.

## 1.6 Огляд найбільш вживаних програм моніторингу комп'ютерних систем і мереж

Ринок програмного забезпечення для моніторингу мережі настільки переповнений інструментами, що вибрати буває важко. Комплексні інструменти моніторингу мережі дають можливість керувати своїми пристроями та переконатися, що вони доступні, коли це потрібно. Серед них найбільш вживаними можна назвати SolarWinds Network Performance

Monitor, Auvik, Nagios Core, Checkmk, Domotz, Zabbix та багато інших.

### 1.6.1 Огляд системи моніторингу на прикладі програми Zabbix

Zabbix – це програмний інструмент із відкритим вихідним кодом для моніторингу IT-інфраструктури, такої як мережі, сервери, віртуальні машини та хмарні служби. Zabbix збирає та відображає основні показники системи.

Zabbix розроблено в основному як інструмент моніторингу IT-інфраструктури. Нові функції зазвичай випускаються кожні шість місяців для основних версій і кожні 1,5 року для версій LTS.

Zabbix, випущений на умовах GNU General Public License версії 2, є безкоштовним програмним забезпеченням, яке не вимагає додаткової ліцензії для використання будь-якої з його функцій. Незважаючи на те, що Zabbix є програмним забезпеченням з відкритим вихідним кодом, це програмний продукт для закритої розробки, розроблений компанією Zabbix LLC, розташованою в Ризі, Латвія.

На початку своєї історії Zabbix описували як простий у налаштуванні порівняно з іншими рішеннями моніторингу. Однак пізніше деякі вважали, що потрібна значна кількість ручного налаштування. Проте як продукт із відкритим вихідним кодом Zabbix зосереджується на використанні існуючих інструментів і функцій, а також власних рішень для досягнення масштабованого рішення моніторингу.

Перша стабільна версія, 1.0, була випущена в 2004 році. Оскільки перша стабільна версія була випущена як 1.0, у версії Zabbix використовувалися проміжні номери версій для позначення основних випусків. Кожен незначний випуск реалізує багато нових функцій, тоді як випуски рівня змін здебільшого містять виправлення помилок.

Схема нумерації версій Zabbix з часом змінилася. У той час як перші дві стабільні гілки були 1.0 і 1.1, після 1.1 було вирішено використовувати непарні номери для версій розробки та парні номери для стабільних версій. У

результаті 1.3 слідував за 1.1 як оновлення розробки, яке було випущено як 1.4.

Zabbix може підтримувати кілька високопродуктивних агентів (zabbix-agent) практично для всіх платформ (рисунок 1.11);

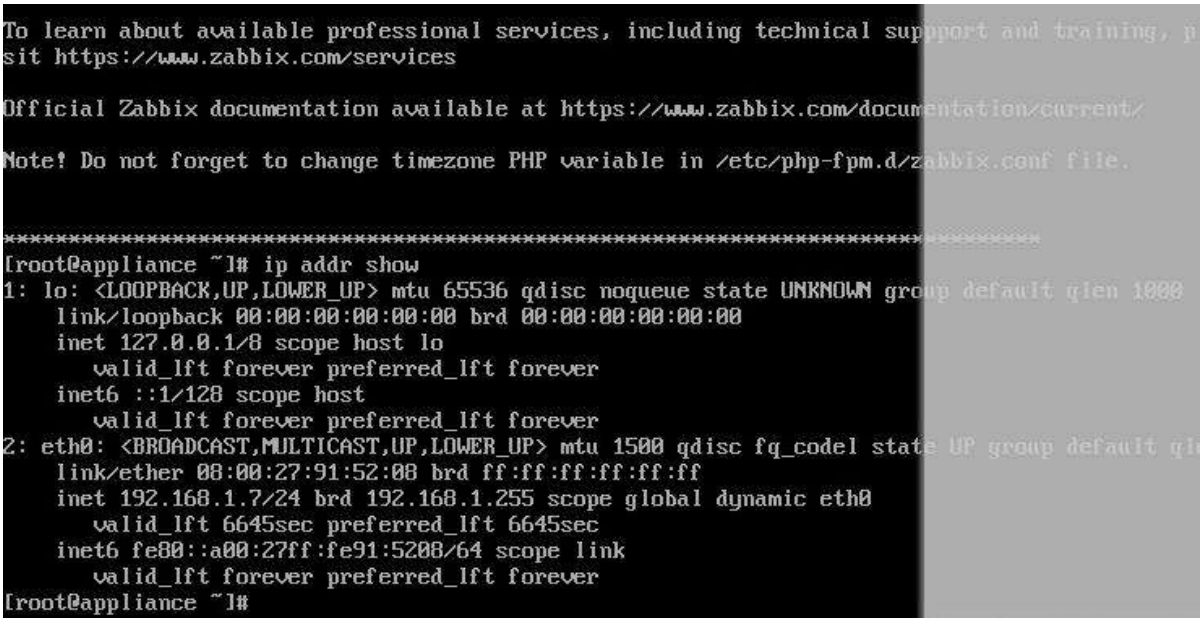


Рисунок 1.11 – Конфігурування zabbix-агента у програмі віртуалізації VirtualBox Oracle

# 2 АНАЛІЗ ТРАФІКУ МЕРЕЖІ КОРПОРАТИВНОЇ LAN

## 2.1 Постановка завдання до проведення аналізу

Актуальність теми роботи. Постійний моніторинг мережі та пристроїв допомагає вирішувати не лише серйозні збої, але й уповільнення. Раннє усунення несправностей забезпечує безперервність роботи та мінімальний час простою або його відсутність, а також переваги моніторингу мережі, такі як:

- виявлення проблем будь-де в мережі. Моніторинг і оцінка мережі – це спосіб швидко виявити проблему в мережі. Моніторинг продуктивності мережі може показати причину та джерело проблеми з мережею, де та коли вона виникла. Він також може сказати, хто повинен це виправити. Коли мережа активно відстежується, можна виявити будь-які зміни продуктивності, які можуть бути проблемними для користувачів, ще до того, як вони відбудуться;

- краще використання IT-ресурсів. Збій у мережі вбиває продуктивність. Щоб це виправити, IT-менеджеру з недостатніми ресурсами доведеться відволікати увагу від одного критично важливого для бізнесу проекту до іншого без попередження чи підготовки. Ключова перевага систем моніторингу мережі полягає в тому, що вони зменшують ручну роботу IT-команд. Це повертає IT-відділу дорогоцінний час, який замість цього можна виділити на важливіші проекти.

Надання історичних і вихідних даних. За наявності базових даних інструменти моніторингу мережі можуть постійно й автоматично порівнювати дані. У разі зниження продуктивності вам надсилається сповіщення, і ви можете негайно вирішити проблему. Зібрані дані дають точку порівняння для визначення оптимальної продуктивності мережі або виявлення низької продуктивності. Це також дозволяє вирішувати проблеми

з мережею через минулі події. Отже, важливим завданням в галузі інформаційних технологій є покращення характеристик моніторингу мереж за допомогою [16].

Метою роботи є огляд засобів аналізу та покращення властивостей корпоративної мережі.

Задачі, які потрібно вирішити у ході даної магістерської роботи полягають у наступному:

- аналіз даних моніторингу мереж прогнозування трафіку в комп’ютерних мережах;

- обґрунтування використання засобів аналізу та моделювання трафіку комп’ютерних мереж;

Об’єктом дослідження даної магістерської роботи є аналіз даних, отриманих в результаті моніторингу комп’ютерних мереж.

Предметом дослідження є методи та засоби аналізу трафіку комп’ютерних мереж для забезпечення якості обслуговування.

Наукова новизна роботи полягає в наступному:

- запропонований метод аналізу трафіку виявлення раптових подій у мережевих комп'ютерних вимірюваннях за допомогою вейвлет-аналізу;

- уточнення алгоритму виявлення вірусних «хробаків» електронної пошти за допомогою вейвлет-аналізу потоків запитів DNS, за рахунок використання іншої техніки стиснення даних.

Практична цінність результатів дослідження: Результати, отримані в ході виконання цієї дипломної роботи, можуть бути використані у програмних продуктах для моніторингу показників систем та мереж, а також використовуваних для захисту мережевих ресурсів від мережевих вторгнень.

## 2.2 Виявлення подій під час вимірювання (моніторингу) комп’ютерної мережі

Моніторинг і вимірювання різних показників мереж високої швидкості та високої потужності виробляють величезну кількість інформації протягом тривалого періоду часу. Ці показники описують стан і продуктивність мережі в термінах використання, перевантаження, втрачених пакетів тощо та допомагають операторам ідентифікувати потенційні проблеми. Щоб зібрані дані моніторингу були корисними для адміністраторів, ці вимірювання необхідно проаналізувати та обробити, щоб виявити цікаві характеристики такі, як раптові зміни. Виявлення таких характеристик у великих обсягах даних є нелегким завданням і цікавлять дослідників мережі протягом багатьох років. Зміни в мережах викликають зміни в їх продуктивності, і це повторно відображені в зібраних вимірюваннях. Ці зміни можуть виникнути через зміна навантаження в мережі, несправність або планові зміни в інфраструктурі. Автоматизований інструмент для аналізу даних і етапів виявлення змін зменшить витрати, необхідні для навчання та утримання людських ресурсів. Запропонований алгоритм можна застосувати до сигналів затримки мережі та швидкості передачі даних. Отримано експериментальні результати які дозволяють перевірити, наскільки добре застосований метод виявляє зміни в сигналах. Загальна методологія виявлення подій у мережі передбачає використання історичні дані для оцінки середнього значення та дисперсії, а потім узагальнення події за межами третього стандартного відхилення як аномальні. Однак слід брати до уваги змінний характер мережі в часі. Продуктивність мережі змінюється залежно від часу дня, дня тижня або пори року. Таким чином, для правильної роботи системи виявляти аномалії, він повинен адаптуватися до динамічної природи мережі. У цьому розділі вейвлети використовуються для адаптації до середовища, що змінюється в часі мережі та виявляти будь-які різкі зміни, включені в вимірювання взяті з цієї мережі. Нижче обговорені переваги вейвлетів у розділі 2.3 та зробили вейвлети відповідним інструментом для виявлення раптових подій у мережевих комп'ютерних вимірюваннях [17].

## 2.3 Вейвлети і вейвлет-аналіз

Подібно до STFA, вейвлет-аналіз є віконним методом але з різним розміром вікна. Зазвичай вейвлет-аналіз використовує довге вікно на низьких частотах і коротке вікно на високих частотах, іншими словами, на низьких частотах часова роздільна здатність погана, але частотна роздільна здатність висока. На високих частотах часова роздільна здатність висока, але частотна роздільна здатність погана. Таким чином, висока частота може бути локалізована в часі домен точніше, ніж низька частота. З іншого боку, низький частота може бути розташована в частотній області точніше, ніж висока частота.

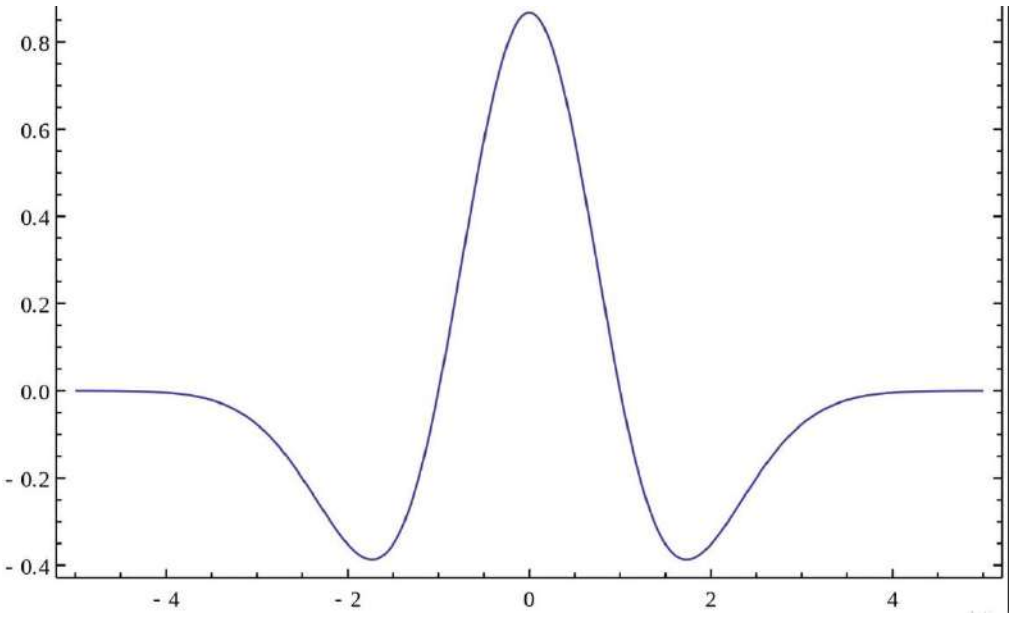


Рисунок 2.1 – Графік функції вейвлет-перетворення типу «Мексиканський капелюх»

Вейвлет- перетворення для вейвлет-аналізу є еквівалентом синусоїди для аналізу Фур'є. Вейвлет – це хвиля ефективно обмеженої тривалості, яка має середнє значення нуль. У порівнянні з синусоїдою, вейвлет нерегуляр-

ний, різкий і обмеженого розміру, а не передбачуваний, плавний і нескінченний (рисунок 2.1).

### 2.3.1 Безперервне вейвлетне перетворення

Подібно до безперервного перетворення Фур'є, можна визначити Безперервне вейвлетне перетворення – Continuous Wavelet Transform (CWT) як сума за весь час сигналу, помноженого на масштабовані, зміщені ($shift$) версії вейвлет-функції $\varphi$. Ця сума призводить до набору вейвлет-коефіцієнтів, які є функцією масштабу $scale$ та положення.

$$C_{scale,shift} = \int_{-\infty}^{\infty} f(t) \times \varphi(scale, shift, t)dt \qquad (2.1)$$

Щоб отримати коефіцієнти CWT, виконуються такі кроки: 1. Вибирається вейвлет, який порівнюється з аналізованим сигналом у відправній точці. 2. Генерується коефіцієнт, який вказує, наскільки вейвлет подібний до відповідної частини досліджуваного сигналу. Чим вище значення, чим більше коефіцієнт, тим вище подібність між двома сигналами. 3. Вейвлет зсувається вправо і виконуються кроки 1 і 2 поки весь сигнал не буде досліджено. 4. Вейвлет масштабується, і кроки 1-3 повторюються. 5. Кроки 1-4 повторюються для кожної шкали. Коли помножиться кожен із коефіцієнтів на вказані масштабовані і зміщену версію вейвлета створюються складові компоненти вейвлета вихідного сигналу [18].

### 2.3.2 Виявлення раптових подій у мережевих комп'ютерних вимірюваннях за допомогою вейвлет-аналізу.

Моніторинг і вимірювання різних показників високої швидкості та високої потужності мережі виробляють величезну кількість інформації протя-

гом тривалого періоду часу. Ці показники описують стан і продуктивність мережі в термінах використання, перевантаження, втрачених пакетів тощо та допомагають операторам ідентифікувати потенційні проблеми. Щоб зібрані дані моніторингу були корисними для адміністраторів, ці вимірювання необхідно проаналізувати та обробити, щоб виявити цікаві характеристики, такі як раптові зміни. Виявлення таких характеристик у великих обсягах даних є нелегким завданням і цікавить дослідників мережі протягом багатьох років.

Оскільки детальні коефіцієнти насправді є змінами середнього значення, ці коефіцієнти з великою величиною виявляють зміну вихідного сигналу. Щоб відфільтрувати ці коефіцієнти, які мають достатньо велику величину, і зробити висновок про зміну у вихідному сигналі, потрібен поріг. Для цього завдання поріг заснований на універсальній системі Донохо-Джонстона. Для кожного рівня декомпозиції поріг перемасштабується залежною від рівня оцінкою рівня шуму $\sigma_{lvl}$. Таким чином, поріг, залежний від рівня, має такий вигляд:

$$T_{lvl} = \sigma_{lvl} \times \sqrt{2 \times log_e n} \tag{2.2}$$

Де $n$ – кількість загальних коефіцієнтів вейвлет-області та $\sigma_{lvl}$ є стандартним відхиленням шуму, що залежить від рівня. Як пропонує [19], середнє абсолютне відхилення використовується як надійна оцінка шуму для стандартного відхилення.

$$\sigma_{lvl} = \frac{median(|cDetail_{lvl}|)}{0.6745} \tag{2.3}$$

де *cDetail* – коефіцієнти деталізації для рівня *lvl.*

Для цієї частини аналізу вейвлет Хаара використовувався як базовий аналіз. Блок-схема представлена нижче на рисунку 2.1. Після нанесення вейвлет-аналіз досліджуваного сигналу, поріг (оцінюється як описаний вище)

застосовувався на кожному рівні. Цей крок фільтрує всі коефіцієнти які не представляють значних змін. Для реалізації методики, використовувалися MATLAB і Wavelet toolbox [20].

Запропонована процедура виявляє аномалії досліджуваної затримки і сигнали швидкості передачі даних. На наступних рисунках оригінальний перевірений сигнал зображено зверху, а виявлені зміни – знизу. Значущі коефіцієнти, отримані після порогового значення, описаного вище, нормалізуються, а потім відображаються на графіку в часі, який вони представляють. На рисунку 2.2 показано сигнал швидкості передачі даних із чотирма випадками значної зміни. Усі зміни виявлено та нанесено на графік. Третя зміна сигналу триває довше, ніж решта. Однак це також повторно на графіку з високими значеннями виявлення на часовій осі на відрізку 600 – 630 (рисунок 2.3).


Рисунок 2.1 – Блок-схема алгоритму Хаара

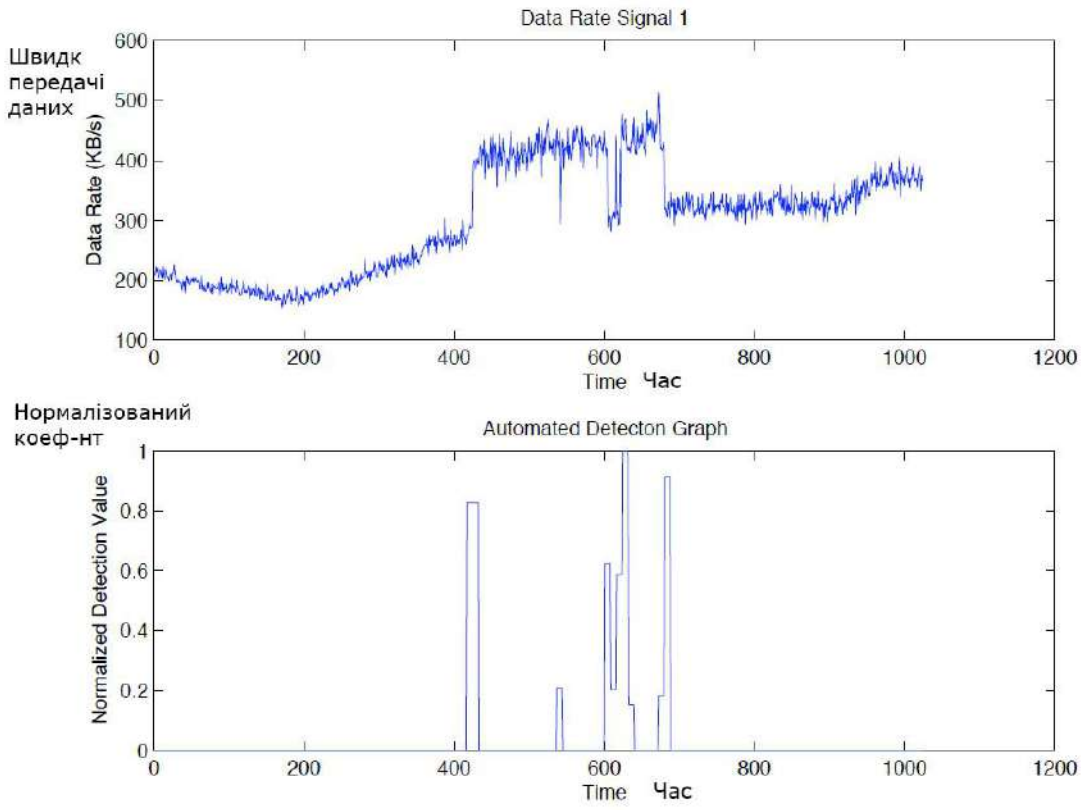


Рисунок 2.2 – Виявлення змін у сигналі при швидкості передачі даних 1

У цьому підрозділі використовується аналіз сигналу на основі вейвлет-перетворення порогу, запропонований Донохо-Джонстоном [21] для виявлення різких змін вимірювання комп'ютерної мережі, такі як затримка та швидкість передачі даних. Сигнали перевірені були з реальних комп'ютерних мереж, а не з інструментів моделювання. Адаптивна за часом характеристика вейвлет-аналізу робить його придатним інструментом для дослідження середовища, що змінюється в часі, наприклад комп'ютерні мережі. Крім того, вейвлет-аналіз може виконувати локальний аналіз і забезпечують як частотну, так і часову роздільну здатність, необхідні для процедур виявлення аномалії. Це було б неможливо з глобальним представленням, отриманим з аналізу Фур'є.

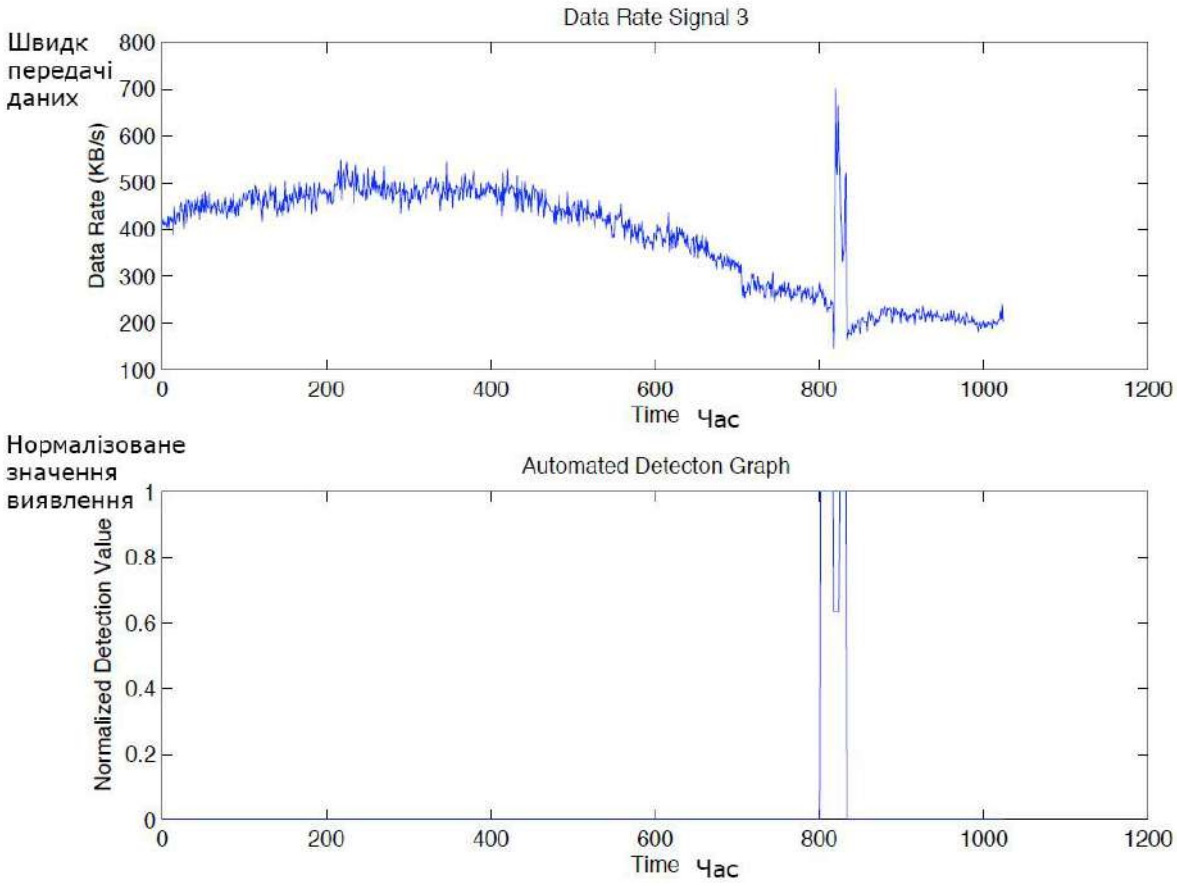


Рисунок 2.3 – Виявлення змін у сигналі при швидкості передачі даних 2

Після використання можливостей аналізу вейвлетів із різною роздільною здатністю, універсальне порогове значення застосовується для фільтрації тих коефіцієнтів із достатньо великим значенням, щоб вказати значну зміну вихідного сигналу. Для того, щоб визначити якомога точніше положення зміни, скануються коефіцієнти прогресивним шляхом від найбільшого до найменшого масштабу. Тривалість аномалії також вказується алгоритмом [22]. Час розрахунку алгоритму не є проблемою для онлайн реалізації алгоритму виявлення аномалії. Це тому, що коли аналіз швидкості передачі даних або сигналу затримки, де кожна вибірка є за секунду, а достатньо кількох мілісекунд часу обробки. Для фіксування такого сигналу скажімо, для 1024 точок вимірювання знадобиться 1024 секунди. Таким чином, достатньо вікна сканування приблизно 17 хвилин для повного аналізу та виявлення.

# 3 ВИЯВЛЕННЯ ВІРУСНИХ «ХРОБАКІВ» ЕЛЕКТРОННОЇ ПОШТИ ЗА ДОПОМОГОЮ ВЕЙВЛЕТ-АНАЛІЗУ ПОТОКІВ ЗАПИТІВ DNS

## 3.1 Постановка проблеми

Інтернет-хробаки сьогодні є одними з основних оперативних викликів безпеки, зі спалахами зараженнями черв’яків пов’язані величезні грошові втрати. Надалі терміном «хробак» (червяк) використовуватиметься, щоб охопити кожну шкідливу програму, яка поширюється через комп'ютерну мережу незалежно від взаємодії людини потрібен (вірус) чи ні (хробак). На основі їх розмноження, хробаки поділяються на скануючі (на основі експлойтів) і топологічні [23]. Черв'яки-сканери використовують вразливість, щоб заразити машину користувача, а потім поширити за адресами вибрати з простору IP-адрес. Топологічні черви покладаються головним чином на соціальній інженерії для зараження комп’ютера користувача та використовувати інформацію, яку вони збирають з машини, для поширення серед соціальних контактів. Соціальна інженерія – це вид вторгнення, що сильно залежить від взаємодії людини, що передбачає переслідування користувачів з метою порушення нормальної безпеки.

Ресурсні записи DNS – записи про відповідність імені і службової інформації в системі доменних імен. Оскільки користувачі стають все більш обізнаними про загрозу електронної пошти складність механізмів захисту хробаків збільшується, автори хробаків стають все більш занепокоєними про збільшення рівня їх зараження. Тому, для того, щоб швидкість хробаків досягнула рівня епідемії, вони їх споряджають агресивними методами збирання списків з багатьма адресами електронної пошти.

Суть експериментального обчислення становить три кроки. По-перше, підтверджується гіпотеза про те, що потоки запитів DNS діляться на два канонічні профілі. По-друге, перевіряються два профілі та показано, що один

відповідає неінфікованим машинам користувачів і інший – на машини, заражені різними поштовими хробаками. На цьому етапі оцінюється загальна точність даного методу на здатність виявляти різні черв'яки електронної пошти. По-третє оцінюється точність методу для незалежного виявлення кожного черв’яка електронної пошти.

Дані для аналізу взяті з реальної мережі, яка представляє собою ізольований комп'ютерний кластер, в якому були запущені 71 найпоширеніші програм черв’яків. В кластері було відтворено роботу реальної мережі, для чого було злито трафік DNS запитів сервера доменних імен, який обслуговував щоденно від 350 до 500 користувачів, із зараженим черв’яками трафіком DNS запитів.

## 3.2 Вейвлет-перетворення та стиснення даних

Для даного аналізу використовується дискретне вейвлетне перетворення (DWT), яке апроксимує часовий ряд суперпозицією базису функції. Ці базисні функції утворюються шляхом розширення і трансляції базисної вейвлет-функції. DWT представлення за своєю суттю має багатороздільну здатність і дозволяє одночасний аналіз часу та частоти, оскільки він перетворює часові ряди на коефіцієнти, локалізовані в часі. Це дозволяє відстежувати зміни в характеристиках часу рядів в певному масштабі як функція часу. Крім того, для часових рядів, які зазвичай зустрічаються на практиці, багато з коефіцієнтів дорівнюють нулю або дуже малі, що дозволяє ефективне стиснення. Крім загальних переваг DWT, ще два фактори мотивують його використання. По-перше, DWT застосована для аналізу нестаціонарних сигналів, тобто сигналів, частотний зміст яких змінюється в часі; і по-друге, це добре працює при стисненні розріджених часових рядів. DWT застосовується незалежно до кожного часового ряду матриця часових рядів з використанням алгоритму піраміди Маллата – базовий метод, доступний у будь-якому статистичному програмному забезпеченні. Алгоритм Маллата розкладає p довжину

– з p є ступенем двох часових рядів до p вейвлет-коефіцієнтів у розкладі $log_2 p$ рівнів, де кожен рівень відповідає діапазону частот. Тому після нанесення DWT на кожну лінію часу матриці серій, отримується матриця вейвлет-коефіцієнтів n × p.

Щоб зменшити розмірність вейвлет-коефіцієнтів матриці, застосовується техніка стиснення, яка вибирає невелика підмножина вейвлет-коефіцієнтів, які забезпечують високу дискримінаційну силу між часовими рядами та хорошою кластеризацією. Для цілей стиснення вейвлет-коефіцієнти часто нормалізуються, що означає, що коефіцієнти при нижчій роздільній здатності мають більшу вагу, ніж коефіцієнти при вищій роздільній здатності. Зберігаючи k найбільших коефіцієнтів у терміни абсолютного нормалізованого значення, дає для даного бюджету коефіцієнтів k оптимальне вейвлет-представлення в термінах помилки суми квадратів [24]. Ще одна добре відпрацьована техніка пропонує зберегти перші k коефіцієнтів, які описують низькочастотні особливості часового ряду. Mörchen [25] порівнює ці дві методики, які застосовуються незалежно для кожного часового ряду з двома методами, застосовними до набору n часових рядів. Ці прийоми застосовуються безпосередньо до матриці вейвлет-коефіцієнтів. Перший зберігає k стовпців матриці, яка має найбільшу середню в квадраті елементів вартість; тоді, як другий для даного k є n × k найбільшим коефіцієнтом матриці вейвлет-коефіцієнтів. Збереження перших k вейвлет-коефіцієнтів або k стовпців матриці вейвлет-коефіцієнтів, які мають найбільше середнє значення поелементне квадратне значення створює вектор ознак n × k матриця, з k << p. Тоді як два інших компресійні методи створюють векторну матрицю ознак n × p із n × k ненульових елементів. На практиці використовується одна техніка стиснення.

## 3.3 Загальне виявлення хробаків електронної пошти

Для оцінки використовуються хибнонегативні та хибнопозитивні

результати. Хибнопозитивний результат – це помилка у двійковій класифікації, коли результат тесту неправильно вказує на наявність захворювання (наприклад, захворювання, коли хвороба відсутня), тоді як помилково негативний результат є протилежною помилкою, коли результат тесту неправильно вказує на відсутність умови, коли вона фактично є. Це два типи помилок у двійковому тесті, на відміну від двох типів правильного результату (істинно позитивний і істинно негативний). Вони також відомі в медицині як хибнопозитивний (або хибнонегативний) діагноз, а в статистичній класифікації як хибнопозитивний (або хибнонегативний) помилка

Вони є також відомими в медицині як хибно позитивний (та хибно негативний) діагноз, та в статистичній класифікації як істинно позитивна (та істинно негативна) помилка. У цьому контексті хибнонегативні та хибнопозитивні ставки стосуються виявлення різних черв’яків електронної пошти, а не виявлення окремо для кожного електронного хробака, який представлено пізніше. Тому помилкові негативні результати виникають, коли не вдається виявити деякі з 71 черв'яків електронної пошти, тоді як трапляються помилкові спрацьовування коли діяльність неінфікованого користувача визначається як підозріла.

## 3.4 Експериментальна оцінка та результати обчислення

У таблиці 3.1 показується правила зупинки значення k, техніка стиснення та середнє значення (над десятьма наборами даних) і стандартне відхилення відсотка черв’яків електронної пошти для яких правила зупинки вказують, що двокластерна схема є найкращою кластеризацією. У таблиці FC, LC, BKC, і BCO стосується збереження перших k коефіцієнтів, найбільшого k, які мають найбільші середньоквадратичні значення та найбільші n×k коефіцієнти матриці вейвлет-коефіцієнтів відповідно. Для, наприклад, значення

100 у першій верхній лівій клітинці таблиці дорівнює інтерпретувати таким чином:

Таблиця 3.1 – Значення $\mu$ та стандартне відхилення $\sigma$ для чотирьох систем стиснення даних при значенні коефіцієнта k=4, k=8

| | | k=4 | | | | k=8 | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | C. | D. | S. | DB | C. | D. | S. | DB |
| FC | $\mu$ | 100 | 93.3 | 97.5 | 92.4 | 100 | 94.8 | 99.5 | 94.2 |
| | $\sigma$ | 0 | 13.6 | 3 | 13.4 | 0 | 11.2 | 1 | 11.1 |
| LC | $\mu$ | 100 | 98 | 98.6 | 95.4 | 100 | 98.8 | 99.1 | 97.5 |
| | $\sigma$ | 0 | 2.7 | 2.6 | 10.4 | 0 | 2.1 | 1.9 | 7.5 |
| ВКС | $\mu$ | 100 | 97.0 | 98 | 94.9 | 100 | 96.3 | 98.9 | 98.8 |
| | $\sigma$ | 0 | 5.9 | 1.9 | 9.9 | 0 | 9.7 | 1.8 | 11.0 |
| ВСО | $\mu$ | 100 | 97.9 | 98.9 | 97.6 | 100 | 98 | 99.2 | 97.7 |
| | $\sigma$ | 0 | 3.8 | 2.3 | 3.8 | 0 | 3.7 | 1.7 | 3.7 |

Таблиця 3.2 – Значення $\mu$ та стандартне відхилення $\sigma$ для чотирьох систем стиснення даних при значенні коефіцієнта k=16, k=32

| | | k=16 | | | | k=32 | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | C. | D. | S. | DB | C. | D. | S. | DB |
| FC | $\mu$ | 100 | 98.7 | 99.7 | 95.6 | 100 | 96.5 | 99.9 | 96.2 |
| | $\sigma$ | 0 | 1.7 | 0.6 | 9.9 | 0 | 9.7 | 0.4 | 9.7 |
| LC | $\mu$ | 100 | 99.1 | 99.2 | 97.3 | 100 | 99 | 99.1 | 97.4 |
| | $\sigma$ | 0 | 1.8 | 1.7 | 7.5 | 0 | 1.9 | 1.8 | 6.7 |
| ВКС | $\mu$ | 100 | 96.1 | 97.9 | 95.6 | 100 | 96.6 | 98.3 | 95.3 |
| | $\sigma$ | 0 | 9.6 | 2.8 | 9.6 | 0 | 8.3 | 1.9 | 8.3 |
| ВСО | $\mu$ | 100 | 98 | 99.2 | 97.8 | 100 | 98.1 | 99.3 | 97.9 |
| | $\sigma$ | 0 | 3.7 | 1.5 | 3.7 | 0 | 3.5 | 1.3 | 3.6 |

зв’язок показує, що в середньому для наборів даних двокластерна схема є найкращою кластеризацією для всіх – тобто 100% – перевірених черв’яків електронної пошти, коли перші чотири коефіцієнти на часовий ряд зберігаються. У таблиці показується, що всі чотири правила зупинки демонструють явне домінування двокластерної схеми над будь-яким іншим результатом кластеризації. Це означає, що індекси розкривають лише два відмінних основні сукупності існують у векторній матриці ознак. В зокрема, збереження найбільших n×k коефіцієнтів перевершує інші методи стиснення, оскільки для кожного k усі правила вказують на те, що в середньому понад 97% email черв’яків існують точно два канонічні профілі [26]. Тому надалі, надається перевага виключно цій техніці стиснення (рисунок 3.1).

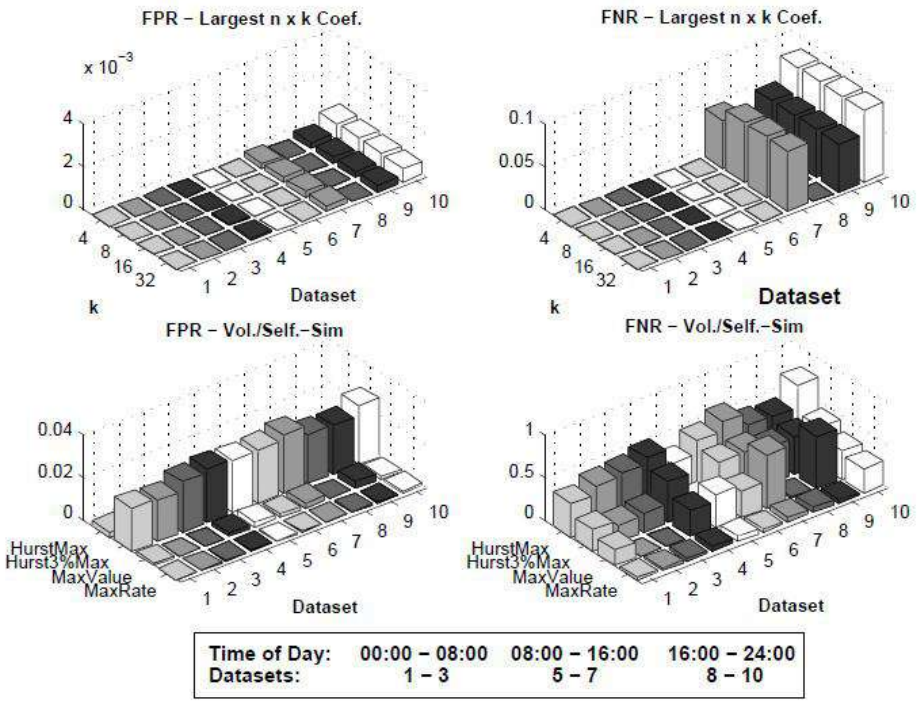


Рисунок 3.1 – Частота хибнопозитивних (FPR) і хибнонегативних (FNR) вибірок різних поштових хробаків з різними наборами даних (верхні графіки) і порівняння даного методу із методами, які висвітлюють виключно по обсягу або самоподібності DNS трафіку (нижні графіки)

Другий метод на основі порогового значення обсягу, позначається MaxValue, виявляє, що заражена email-хробаком машина користувача, яка генерує максимальну кількість запитів вимірюється в 15-секундному діапазоні часу. Третій спосіб натхненний результатами в [26], які показують, що атака шаблонного сканування хробаків є самоподібною. Це свідчить про те, що електронна пошта, заражена хробаком, генерує DNS-трафік, який має найвищий ступінь самоподібності. Для вимірювання ступеня самоподібності оцінюється параметр H за допомогою непараметричної оцінки.

Таким чином, на основі вищевикладеного, знятих даних в результаті експериментів, та виконаних обчислень можна зробити висновки, що заявлений метод виявлення вірусів може бути використаний для виявлення активності електронного хробака у відправника, швидше, ніж в одержувача листів домену. Це означає, що він більш ефективніший, ніж подібні методи, засновані на самоподібності вірусу або накопиченні обсягу запитів.

# ВИСНОВКИ

У ході виконання кваліфікаційної роботи проведено аналіз загальних принципів і особливостей, засобів та методів моніторингу корпоративної комп'ютерної мережі, які за своїм рівнем топологічної і архітектурної організації відносяться до локальних корпоративних мереж і є найбільш поширеним класом мереж.

У процесі проведеного аналізу розглянута термінологічна основа, загальні особливості, принципи функціонування, методи моніторингу корпоративної комп'ютерної мережі. Відзначено деякі підходи моніторингу корпоративної комп'ютерної мережі, такі як дублювання трафіку, зіставлення паттернів, глибокий аналіз пакетів, захват пакетів, потокове спостереження, та проведено порівняльний аналіз між цими підходами із зазначенням переваг та недоліків.

Показано, що найпростіші рішення для корпоративних мереж є підходи дзеркалювання портів, та захват пакетів, проте вони досить ненадійні, придатні для захвату відносно невеликих обсягів трафіку і вимагають здебільшого ручного аналізу даних.

Також приділено увагу і детально розглянуто методи моніторингу корпоративних мереж, які націлені на збереження безпеки даних та працездатності мереж. Докладно описано наступні методи: виявлення вторгнень, сканування вразливостей, перегляд пакетів, брандмауер моніторингу, тестування на проникнення. Всі ці методи мають свої особливості, переваги та недоліки, описані у відповідному розділі. Варто відмітити, що для ефективної і безпечної роботи корпоративної мережі потрібно застосувати хоча б один з цих методів.

Виходячи з вищевикладеного, а також відповідно до вимог в технічному завданні головний акцент проведеного в роботі аналізу вирішено було

зробити в напрямку аналізу даних моніторингу мережі за допомогою вейвлет перетворень.

В роботі розглянуті особливості аналізу трафіку в корпоративних мережах, із застосуванням вейвлет перетвореннь. Вона включає в себе наступні компоненти:

- виявлення подій під час моніторингу комп'ютерної мережі;

- виявлення вірусних «хробаків» електронної пошти за допомогою вейвлет-аналізу потоків запитів DNS.

В рамках виявлення подій під час моніторингу, виявлення різких змін вимірювання комп'ютерної мережі, такі як затримка та швидкість передачі даних. Сигнали перевірені були з реальних комп'ютерних мереж, а не з інструментів моделювання. Адаптивна за часом характеристика вейвлет-аналізу робить його придатним інструментом для дослідження середовища, що змінюється в часі, наприклад комп'ютерних мереж.

Стиснення відстежуваних даних про продуктивність роботи мережі є привабливим варіантом для зменшення вимог до тривалого зберігання. Однак підбір підходящого механізму стиснення – доволі складне завдання. Умовно без втрат для цієї мети використовувалися алгоритми стиснення, однак це так загальновизнано, що більш високий ступінь стиснення досягається за допомогою втрат алгоритму. Звичайно, вони не можуть підтримувати ідеальну регенерацію оригіналу даних. Проте, якщо важливі та значущі елементи оригіналу даних зберігаються, стиснення з втратами стає дуже доречним. Робота, описана в даній дипломній роботі, розглядає це питання і пропонує використання вейвлет-перетворення як перший крок у стисненні часового ряду вимірювання затримки або використання. Використання вейвлет-перетворення таким чином описаний у кваліфікаційній роботі дозволяє отримати корисне подальше стиснення над конкуруючими алгоритмами без втрат, водночас забезпечуючи контрольоване погіршення сигналу. Деградація гарантує, що важливі характеристики вихідних даних зберігаються. Крім того, крім високого ступеня стиснення і хорошої реконструкції якості сигна-

лу, було досліджено кілька факторів стисненого сигналу щоб визначити дію стиснення на них.

В рамках виявлення вірусних «хробаків» електронної пошти потоків запитів DNS для корпоративної мережі, був проведений аналіз із застосуванням дискретного вейвлетного перетворення (DWT), статистичних алгоритмів кластеризації,

Поштові черв'яки та пов'язаний із ними спам залишаються одною з головних проблем оперативної безпеки, яка викликає серйозні грошові втрати. У цій роботі показано, що рівень потоку характеристик потоків DNS-запитів неінфікованих машин користувачів мають багато однакових канонічних дій, в той час як більшість хробаків електронної пошти покладаються на схожі методи поширення, генерування трафіку DNS із загальними шаблонами. Представлено метод, який базується на неконтрольованому навчанні та аналіз часових рядів і використовує вейвлет-перетворення для виявлення активності електронного хробака у відправника, швидше, ніж в одержувача листів домену. Результати експериментів показують, що метод є придатний для отримання надійних поведінкових знань, які є необхідним кроком для автоматичного адаптованого коригування дії. Майбутня робота потребує вивчення ефективності методу через дані запитів DNS з інших мережевих середовищ, і можливо, замість вейвлетів використовуватимуться інші (більш актуальні) часові ряди. Крім того, є перспектива у вивченні контрзаходів, які можна активно застосовувати одноразово виявлено машину, заражену поштовим хробаком, щоб перешкодити таким атакам, як обмеження швидкості DNS-відповідей зараженим пристроєм користувача.

Методика такого розрахунку і його результати можуть служити для застосування у спеціалізованому програмному забезпеченні для моніторингу мереж.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Jakub Svoboda, Ibrahim Ghafir, Vaclav Prenosil.: Network Monitoring Approaches: An Overview. International Journal of Advances in Computer Networks and Its Security – IJCNS. Volume 5: Issue 2 [ISSN : 2250-3757], 2015.

2. Worrall, A.; Carter, B.;Widley, G.: Network monitor and method. 2008 [cit. 2015-04-21], URL, http://www.google.com/patents/US7411946

3. Кучерявий Е.А. Управління трафіком і якість обслуговування в мережі Інтернет. – СПб .: Наука і Техніка, 2004. – 336 с.

4. Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі: принципи, технології, протоколи. – СПб .: Пітер, 2003. – 864 с.

5. A. Feldmann, A. C. Gilbert, W. Willinger, and T. G. Kurtz. The changing nature of network traffic: Scaling phenomena. ACM Computer Communication Review, 28(5–29), 1998. 2.4.4, 6.5

6. Ashok Erramilli, Onuttom Narayan, and Walter Willinger. Experimental queueing analysis with long-range dependent packet traffic. IEEE/ACM Transactions on Networking, 4(2):209–223, 1996. 2.4.4

7. Frank Feather, Daniel P. Siewiorek, and Roy A. Maxion. Fault detection in an ethernet network using anomaly signature matching. In Proceedings of the Conference on Communications Architectures, Protocols and Applications, San Francisco, CA, USA, Sep 13-17 1993. ACM. 8.1.

8. M. Misiti, Y. Misiti, G. Oppenheim, and J. Poggi. Matlab wavelet toolbox. Technical report, The MathWorks, Inc., 1997-2004. (document), 3.2, 3.3.1, 3.3.2, 3.3.2, 3.3.2, 3.4, 3.3.4, 3.6, 3.3.4, 3.4.1, 3.4.2, 3.4.2, 3.4.3, 3.4.3, 3.4.4, 3.5, 4.2.1, 6.3.1, 6.4, 8.2.1, 8.3

9. V. Paxson, “Bro: a system for detecting network intruders in real-time,” Comput. Networks, vol. 31, no. 23-24, pp. 2435–2463, 1999.

10. Tobi Oetiker. Multi router traffic grapher. Website. Available on http://oss.oetiker.ch/mrtg/. Page last visited 30/03/2023. 2.2.5.

11. Gerla, M. Flow Control: A Comparative Survey [Текст] / Mario Gerla, Leonard Kleinrock // IEEE Transactions on Communications. – 1980. – vol. 28 (4) – pp. 553 – 574.

12. Романов А.І. Телекомунікаційні мережі й управління. - К .: Видавничо-поліграфічний центр «Київський університет», 2003. - 247 с.

13. Вовченко В. В., Степанов И. О. Організаційні проблеми захисту інформації. – К.: Академія, 2003 .- 48-65с.

14. Стєклов В.К., Беркман Л.Н. Проектування телекомунікаційніх мереж - К .: Техніка 2002 - 392с.

15. Вільям Столлінгс Комп'ютерні системи передачі даних. - М .: Видавничий дім «Вільямс», 2002. - 928 с.

16. Patrice Abry, Richard Baraniuk, Patrick Flandrin, Rudolf Riedi, and Darryl Veitch. Multiscale nature of network traffic. IEEE Signal Processing Magazine, 19(3):28 – 46, May 2002. 3.5

17. P. Barford, J. Kline, D. Plonka, and A. Ron. A signal analysis of network traffic anomalies, 2002. 3.5

18. Ashok Erramilli, Onuttom Narayan, and Walter Willinger. Experimental queueing analysis with long-range dependent packet traffic. IEEE/ACM Transactions on Networking, 4(2):209 - 223, 1996. 2.4.4

19. James F. Kurose and Leith W. Ross. Computer Networking: A Top-Down Approach Featuring the Internet. Pearson/Addison Wesley, second edition, 2003. 1.1, 1.2, 1.3, 1.4.1, 1.4.1, 1.4.1, 1.4.1, 1.4.1, 1.4.2, 1.4.4, 1.4.6

20. Seong Soo Kim, A. L. Narasimha Reddy, and Marina Vannucci. Detecting traffic anomalies using discrete wavelet transform. In Hyun-Kook Kahng, editor, ICOIN, volume 3090 of Lecture Notes in Computer Science, pages 951{961. Springer, 2004. 3.5, 8.1

21. K. Ishibashi, T. Toyono, H. Matsuoka, K. Toyama, M. Ishino, C. Yoshimura, T. Ozaki, Y. Sakamoto, and I. Mizukoshi, “Measurement of dns traffic caused by ddos attacks,” in SAINT ’05: Proc. of the 2005 Symposium on Applications and the Internet Workshops. Los Alamitos, CA, USA: IEEE

Computer Society, 2005, pp. 118–121.

22. Polly Huang, Anja Feldmann, and Walter Willinger. A nonintrusive, wavelet-based approach to detecting network performance roblems. In Proceedings of the ACM SIGCOMM Internet Measurement Workshop, pages 213–227, November 1-2 2001.

23. N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, “A taxonomy of computer worms,” in WORM ’03: Proc. of the 2003 ACM workshop on Rapid malcode. New York, NY, USA: ACM, 2003, pp. 11–18

24. G. Ganger, G. Economou, and S. Bielski, “Self-securing network interfaces: What, why and how,” Computer Science Department, Carnegie Mellon University, Tech. Rep. CMU-CS-02-144, 2002

25. F. Mörchen, “Time series feature extraction for data mining using dwt and dft,” Dept. of Maths and CS, Philipps-U. Marburg, Tech. Rep. No. 33, 2003.

26. E. Stollnitz, T. Derose, and D. Salesin, Wavelets for computer graphics: theory and applications. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1996