УДК 621.391:004.9 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.174

РОЗРОБКА ДОДАТКУ ДЛЯ АНАЛІЗУ МЕРЕЖНОГО ТРАФІКУ

Чистюк Д.С.
Науковий керівник – к.т.н., доц. Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, каф. IMI,
м. Харків, Україна
e-mail: dmytro.chystiuk@nure.ua

The purpose of the work is to formulate the concept of network traffic analysis, to explore methods of analyzing corporate traffic, working principle of the network traffic analyzer and its advantages. As a result, own traffic analysis application was developed. This application provides real-time visualization of network traffic activity and creation of customized reports in different types of content such as text, graphics, and graphs. These tools will enable many network professionals to create secure, efficient, well designed and performance optimized networks.

У сучасну цифрову епоху мережі відіграють вирішальну роль у функціонуванні організацій будь-якого розміру та типу. Для ефективного керування мережею велике значення має моніторинг. Він є джерелом інформації про функціонування корпоративних додатків, що враховується при розподілі коштів, планування обчислень потужності, виявленні та локалізації відмов, рішень питань безпеки. Відстежуючи мережний трафік на предмет незвичайної активності, спеціалісти з мережної безпеки можуть виявляти та попереджувати різні загрози.

Аналіз мережного трафіку – це процес аналізу активності та доступності мережі, для виявлення незвичайної поведінки об’єктів, яка може вказувати на зловмисну діяльність [1, 2]. Ця операція передбачає відстеження того, які та коли надходять дані у різні частини мережі. Загальні випадки його використання включають:

- збір даних про те, що відбувається в мережі в режимі реального часу та за попередні періоди;
- виявлення зловмисного програмного забезпечення;
- виявлення використання вразливих протоколів і шифрів;
- усунення несправностей повільної мережі;
- покращення внутрішньої видимості та усунення сліпих зон.

Впровадження рішень, які можуть безперервно відстежувати мережний трафік, дає уявлення, необхідні для оптимізації продуктивності мережі, мінімізації поверхні атак, підвищення безпеки та покращення керування ресурсами.

Метою доповіді є дослідження систем аналізу мережного трафіку та розробка власного додатку для аналізу мережного трафіку.

Сьогодні популярними інструментами для аналізу мережних протоколів є аналізатори протоколів (protocol analyzer) та сніфери (sniffer).

Такі пристрої існують в апаратному та програмному вигляді. Аналізатор протоколів на основі апаратного забезпечення використовується в роботі зі складними інтерфейсами протоколів, в той час як програмний аналізатор є менш потужним але простішим та дешевшим в використанні.

Лідером ринку серед додатків для аналізу мережного трафіку є Wireshark [3]. Wireshark – це інструмент із відкритим кодом для моніторинга мережного трафіку та аналізу пакетів, який дає змогу адміністраторам мережі проводити глибокий аналіз трафіку, що переміщується через мережу. Програмне забезпечення дає можливість вивчення деталей трафіку на різних рівнях, починаючи від інформації на рівні підключення до бітів, які складають один пакет. Перехоплення пакетів може надати мережному адміністратору інформацію про окремі пакети, наприклад час передачі, джерело, призначення, тип протоколу та дані заголовка.

В роботі проведено детальний огляд найважливіших функцій Wireshark та виконано розробку власної реалізації програми аналізатора мережного трафіку. Корисна функція, яка надається операторам мого додатку – це наглядне відображення мережних інтерфейсів. Ця функція реалізована для комфортного, зрозумілого, легкого отримання інформації про мережні пристрої. Користувачам більше не треба шукати в параметрах комп'ютера ці відомості, вистачить зайти на сторінку відображення мережних інтерфейсів, де будуть представлені картки з існуючими мережними інтерфейсами, а також їхні короткі описи.

Розроблений додаток своїм функціоналом задовольнить користувачів та за допомогою реалізації різноманітних можливостей, таких як перехоплення мережного трафіку, побудова графіків навантаження мережі, графу ip-адрес, відображення деталей підключених мережевих пристроїв, він може стати конкуренто-спроможним вже на першій ітерації програмного продукту. Варто зазначити, що граф IP-адрес та графік залежності кількості пакетів до IP-адрес не реалізовані в програмному додатку Wireshark, а отже є унікальними функціями розробленого додатку.

Список використаних джерел:

1. Ashtari H. What Is Network Behavior Analysis? Definition, Importance, and Best Practices [Електронний ресурс] / Hossein Ashtari // Spiceworks. – 2022. – Режим доступу до ресурсу: https://www.spiceworks.com/tech/networking/articles/network-behavior-analysis/.

2. Janani A. K. Network Traffic Analysis [Електронний ресурс] / A. K. Janani // Atatus. – 2022. – Режим доступу до ресурсу: https://www.atatus.com/glossary/network-traffic-analysis/.

3. About Wireshark [Електронний ресурс] // Wireshark Foundation. – 2024. – Режим доступу до ресурсу: https://www.wireshark.org/about.html.