УДК 004.056

Я.В. Максименко

Модуль моніторингу мережі

Вінницький національний технічний університет

Анотація. *В даній роботі описано як аналізувати мережевий трафік. Запропоновано та розроблено засіб для моніторингу трафіку, реалізований мовою програмування Python.*

Ключові слова: *аналіз, моніторинг, трафік, Python, мережа..*

Abstract*. In this paper describes how to analyze network traffic. A tool for traffic monitoring implemented in the Python programming language has been proposed and developed.*

Keywords*: analysis, monitoring, traffic, Python, network.*

Вступ

Проблема інформаційної безпеки останнім часом виходить на новий, відкритий загальнодоступний рівень. Новітні технології відкривають нові можливості для зловмисників, які намагаються вкрасти різного роду інформацію користувачів персональних комп'ютерів, мобільних пристроїв та інших систем. Тому розробка нових підходів та систем для захисту інформації з використанням існуючих або нових аналізаторів трафіку є актуальною у сучасному інформаційному світі [1].

Аналізатор трафіку, або мережевий сніфер - програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів мережі [2].

Аналізуючи існуючі програмні продукти, основною відмінністю розробленого аналізаторуа є низьке навантаження на систему.

Результати дослідження

За результатами роботи створеного аналізатора передбачається величезна кількість пакетів, тобто сегментів даних, які відправляються з одного пристрою на інший через мережу. Практично усі мережеві сніфери дозволяють проводити аналіз декодованих пакетів мережі. Сніфер розподіляє перехоплені пакети по рівнях і протоколах [3].

Деякі з відомих аналізаторів пакетів здатні розпізнавати протокол і відображати перехоплену інформацію. Наприклад, будь-який сніфер здатний розпізнавати протокол TCP, а сучасні мережеві сніфери визначають, яким саме застосунком створювався

розпізнаваний трафік. Тому актуальним є застосування фільтрів, що могли б відсіювати пакети за критеріями сформованими користувачем в розробленому сніфері. Це дозволить спростити процес аналізу трафіку та виділити необхідний трафік для подальшого його аналізу.

А саме, пропонується такий фільтр, що включав би в себе можливість модифікації трафіку в реальному часі та підтримував графічний інтерфейс вибору користувача. Перевагами такого програмного застосунку є простота у використанні, незавантаженість пристрою та можливість у відповідний момент модифікувати трафік [4].

Блок-схема аналізатора

Розроблений програмний засіб виконує функції обробки вхідних пакетів, після-обробки даних та обробки пакетів обраним фільтром, закриття сніфера та черги.

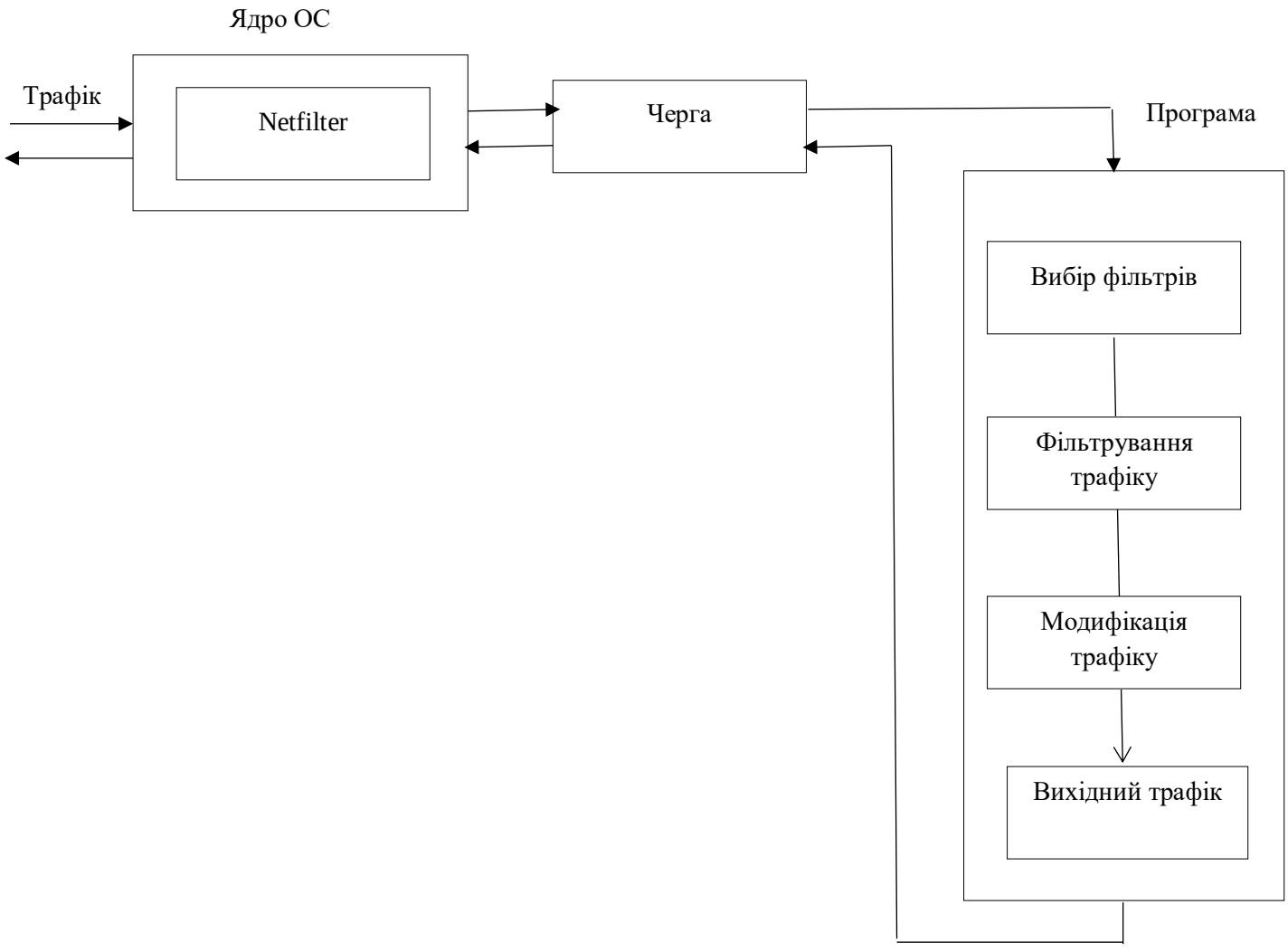

Рисунок 1 – Рух трафіка через сніфер

Трафік з мережі надходить на netfilter, пакети пропускаються через ланцюжки. Ланцюжок є впорядкованим списком правил, а кожне правило має критерії. Коли пакет

проходить через комп'ютер, система netfilter перенаправляє його в ланцюжок, аналізатор трафіка перевіряє чи відповідає пакет потрібним критеріям, то в такому випадку, трафік надходить на модуль створеного додатка filter.py, виконує функції обробки вхідних пакетів, після-обробки усіх даних, а тоді надходить на модуль підміни трафіку, що виконує потрібну дію. Якщо пакет не підходить, то система перенаправляє його без змін.

Висновки

В результаті виконання роботи розроблено аналізатор трафіка, що реалізовує функції перехоплення, фільтрування та аналізу мережевих пакетів та складається із власного модуля, що відповідає за перехоплення, обробку, після-обробку. Для реалізації фільтрів обрано інтерпретовану об'єктно-орієнтовану мову програмування Python. Розроблений застосунок встановлюється на ОС Linux Ubuntu.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Shunquan Tan and Bin Li. Best of open source in networking – IEEE Signal Processing Letters Vol 19, No. 6, 2012, pages 336-339.
2. What Is a Packet Analyzer? - Garland Technology [Електронний ресурс]. – Режим доступу до ресурсу: URL: https://www.garlandtechnology.com/blog/what-is-a-packet-analyzer – Назва з екрану.
3. What Is A Packet Sniffer and How Does It Work? [Електронний ресурс]. – Режим доступу до ресурсу: URL: https://heimdalsecurity.com/blog/what-is-a-packet-sniffer/ – Назва з екрану.
4. J. Fridrich et al. "Wireshark 1.2.6". Wireshark 1.2.6 Review & Rating.– J. Fridrich, M. Goljan, R. Du / IEEE Multimedia Magaz., Special Issue on Security 22–28, 2013.

Максименко Ярослав Вікторович – студент групи 2БС-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м.Вінниця, e-mail: subwofer2017@gmail.com

Maksymenko Yaroslav V.— Department of Information Techologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, email : subwofer2017@gmail.com.

Шелепало Галина Василівна — к. фіз.-мат. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Shelepalo Halyna V. — PhD (Eng), Associated Professor of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine..