Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра інформаційних технологій та систем електронних комунікацій

«Допущено до захисту»
Начальник кафедри інформаційних технологій та систем електронних комунікацій

Олександр ПРИДАТКО
“___” _____20__ року

ДИПЛОМНА РОБОТА МАГІСТРА

на тему: «**Розроблення системи віддаленого моніторингу та фільтрації мережевого трафіку на базі ОС Linux**»

Виконав:
здобувач VI курсу, групи КН-61м
спеціальності 122 «Комп’ютерні науки»
(шифр і назва спеціальності)
Ярослав МАГЕРОВСЬКИЙ
(прізвище та ініціали)
Керівник Юрій БОРЗОВ
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
(ім’я та прізвище)

Львів 2022 рік

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту

Кафедра інформаційних технологій та систем електронних комунікацій
Освітній ступінь магістр
Спеціальність 122 "Комп'ютерні науки"
Освітня програма Комп'ютерні науки

ЗАТВЕРДЖУЮ
Начальник кафедри інформаційних технологій та систем електронних комунікацій

Олександр ПРИДАТКО
"___" _____20__ року

ЗАВДАННЯ
на дипломну роботу

Здобувач Ярослав МАГЕРОВСЬКИЙ
(ім'я, прізвище)

1. Тема Розроблення системи віддаленого моніторингу та фільтрації мережевого трафіку на базі ОС Linux

керівник роботи Юрій БОРЗОВ, к.т.н., доцент
(ім'я, прізвище, науковий ступінь, вчене звання)

затверджені наказом ЛДУ БЖД від "___"_____20___року №_____

2. Термін подання здобувачем роботи _____

3. Початкові дані до роботи

1. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник, Комп'ютерні мережі [навчальний посібник] – Львів, «Магнолія 2006», 2013. – 256 с.
2. OpenFlow Switch Specification Version 1.5.0 (Protocol version 0x06) December 19, 2014, 277 с.
3. Петрик М.Р. Моделювання програмного забезпечення: науково-методичний посібник / М.Р. Петрик, О.Ю. Петрик – Тернопіль : Вид-во ТНТУ імені Івана Пулюя, 2015. – 200 с.
4. Карвинен Теро, Карвинен Киммо, Валтокари Вилле. Делаем сенсоры: проекты сенсорных устройств на базе Arduino и Raspberry Pi. Пер. с анг. – М.: ООО "И. Д. Вильямс", 2015. – 432 с.

4. Зміст дипломної роботи/проекту (перелік питань, які потрібно розробити)

Вступ
Розділ 1. Аналітичний огляд систем моніторингу та фільтрації трафіку
Розділ 2. Технології розробки системи моніторингу та фільтрації трафіку

Розділ 3. Обгрунтування обраного напрямку проектування

Розділ 4. Проектування віддаленої системи моніторингу та фільтрації мережевого трафіку

Висновки

Список використаних джерел

5. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

6. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання дипломної роботи/	Термін виконання етапів роботи	Примітка
1	Аналітичний огляд систем моніторингу та фільтрації трафіку		
2	Технології розробки системи моніторингу та фільтрації трафіку		
3	Обгрунтування обраного напрямку проектування		
4	Проектування віддаленої системи моніторингу та фільтрації мережевого трафіку		

Здобувач _____ Ярослав МАГЕРОВСЬКИЙ
(підпис) (ім'я та прізвище)

Керівник роботи _____ Юрій БОРЗОВ
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Ярослав МАГЕРОВСЬКИЙ. «Розроблення системи віддаленого моніторингу та фільтрації мережевого трафіку на базі ОС Linux». Дипломна робота за спеціальністю 122 «Компютерні науки» складається з текстової частини, що містить 4 розділи, 75 сторінок і містить 39 ілюстрацій, 3 таблиці та 17 джерел.

В даній магістерській кваліфікаційній роботі розроблено систему віддаленого моніторингу та фільтрації мережного трафіку на базі ОС Linux. Система побудована на базі технології SDN (Software Defined Network) і складається з таких компонентів:

- фонового додатку для збору статистики;
- фонового додатку для вузлів фільтрації та моніторингу;
- інтерфейсу командного рядка ;
- мікрокомп’ютера Raspberry Pi.

В даній роботі представлено як апаратну так і програмну складову функціонування системи моніторингу та фільтрації мережевого трафіку.

ABSTRACT

Yaroslav MAGEROVSKYI. "Development of a system for remote monitoring and filtering of network traffic based on the Linux OS". Graduation work on the specialty 122 "Computer Science" consists of a text part containing 4 chapters of 75 pages, 39 illustrations, 3 tables and 17 references.

In this master's thesis, a system of remote monitoring and filtering of network traffic based on the Linux OS was developed. The system is built on the basis of SDN (Software Defined Network) technology and consists of the following components:

- background application for collecting statistics;
- background application for filtering and monitoring nodes;
- command line interface;
- Raspberry Pi microcomputer.

This work presents both the hardware and software components of the network traffic monitoring and filtering system.

ЗМІСТ

ВИСНОВКИ

В магістерській роботі була розроблена система для віддаленого моніторингу та фільтрації мережного трафіку на базі ОС Linux. В ході роботи були розв’язані наступні завдання:

1. Проведено аналіз методів віддаленого доступу, фільтрації та моніторингу мережного трафіку.
2. Обрані технології для реалізації функціоналу системи на основі протоколу OpenFlow.
3. Розроблена архітектура системи та реалізовані основні вузли системи: моніторингу, фільтрації та збору статистики.
4. Розроблео інтерфейс користувача для віддаленого доступу до системи.
5. Проведене тестування функціоналу та продуктивності розробленої системи.

В результаті було реалізовано наступні скрипти:

1. Фоновий додаток для встановлення політик фільтрації згідно правил, визначених користувачем та отримання даних моніторингу системи з OpenFlow комутатора.
2. Фоновий додаток для автоматизованого збору статистики та зберігання її у зручному вигляді для подальшого аналізу.
3. Додаток з інтерфейсом командного рядка для забезпечення загальної конфігурації системи, налаштування політик брандмауера та отримання даних моніторингу системи.

Проведено тестування продуктивності розробленої системи з визначенням пропускної здатності трафіку та “джиттера”. Значення цих параметрів були отримані для Linux комутатора, інтегрованого в ядро ОС Linux, для порівняння зі значеннями системи на базі OpenFlow комутатора.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник, Комп'ютерні мережі [навчальний посібник] – Львів, «Магнолія 2006», 2013. – 256 с.
2. Рамський Ю.С., Олексюк В.П., Балик А.В. Р21 Адміністрування комп'ютерних мереж і систем: Навч. пос. —Тернопіль: Навчальна книга – Богдан, 2010. — 196 с.
3. Андрушко О. А. Аналіз процесів використання Docker для побудови мікросервісів / О. А. Андрушко, Ю. О. Борзов, І. О. Малець, О. В. Придатко // Науковий вісник НЛТУ України: Зб. нак.праць. Львів: НЛТУ, 2017. - №9(27) – С.95-98.
4. M. Gouda and A. Liu, "A model of stateful firewalls and its properties," in DSN, Yokohama, Japan, 2005, 137 с.
5. Y. Bartal, A. Mayer, K. Nissim, and A. Wool, "Firmato: A novel firewall management toolkit," 1999 - 78 с.
6. OpenFlow Switch Specification Version 1.5.0 (Protocol version 0x06) December 19, 2014, 277 с.
7. L. Buttyan, G. Pék, and T. V. Thong, "Consistency verification of stateful firewalls is not harder than the stateless case," Infocommunications Journal, vol. LXIV, 2009 - 33 с.
8. Nick Feamster, Jennifer Rexford, and Ellen Zegura. The Road to SDN: An Intellectual History of Programmable Networks. SIGCOMM Comput. Commun. Rev., 44(2):87– April 2014 - 98 с.
9. Software-Defined Networking and Network Programmability Use Cases for Defense and Intelligence Communities. White Paper, Cisco Inc., January 2014
10. Software-Defined Networking : The New Norm for Networks. White Paper, Open Networking Foundation, April 2012 - 105 с.
11. Карвинен Теро, Карвинен Киммо, Валтокари Вилле. Делаем сенсоры: проекты сенсорных устройств на базе Arduino и Raspberry Pi. Пер. с анг. – М.: ООО "И. Д. Вильямс", 2015. – 432 с.

12. Prydatko O. Informational System of Project Management in the Areas of Regional Security Systems' Development / Prydatko O., Solotvinskyi I., Smotr O., Borzov Y., Didyk O.– Proceedings of the 2018 IEEE 2nd International Conference on Data Stream Mining and Processing, DSMP 2018. Lviv, 2018 (№ статті 8478543). P. 187–192.
13. Python 3.7.3 documentation [Електронний ресурс]; Режим доступу до ресурсу: https://www.python.org/downloads/release/python-373/
14. Click library documentation [Електронний ресурс]; Режим доступу до ресурсу: https://click.palletsprojects.com/en/8.1.x/
15. Bash Reference Manual [Електронний ресурс]; Режим доступу до ресурсу: https://www.gnu.org/software/bash/manual/bash.pdf
16. Raspberry Pi [Електронний ресурс]; Режим доступу до ресурсу: https://www.raspberrypi.com/documentation/computers/os.html
17. Mininet documentation [Електронний ресурс]; Режим доступу до ресурсу: http://mininet.org/walkthrough/