ДОДАТОК А

Графічний матеріал атестаційної роботи

АТЕСТАЦІЙНА РОБОТА

Методи та засоби аналізу мережного трафіку

Виконав:
студент гр. СПзм-18-2
Сидоров Д.С.

Керівник:
проф. каф. ЕОМ,
д.т.н. Міхаль О.П.

МЕТА РОБОТИ ТА ЗАВДАННЯ

2

Метою роботи є дослідження методів та засобів аналізу мережного трафіку.

Завдання:

- аналіз існуючих моделей та методів аналізу мережевих пакетів, враховучи особливості передачі данних по мережі (втрата окремих пакетів, стиснення і шифрування даних, вкладене тунелювання);
- розробка аналізатора мережного трафіку з використанням досліджених методів.

Об'єктом дослідження є передача пакетів даних у комп'ютерній мережі.

ОБЛАСТІ ПРАКТИЧНОГО ЗАСТОСУВАННЯ 3

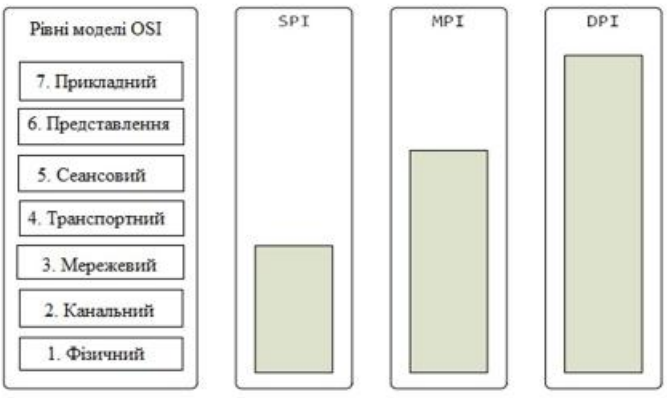
• виявлення проблем в роботі мережі;

• тестування (налагодження) мережевих протоколів;

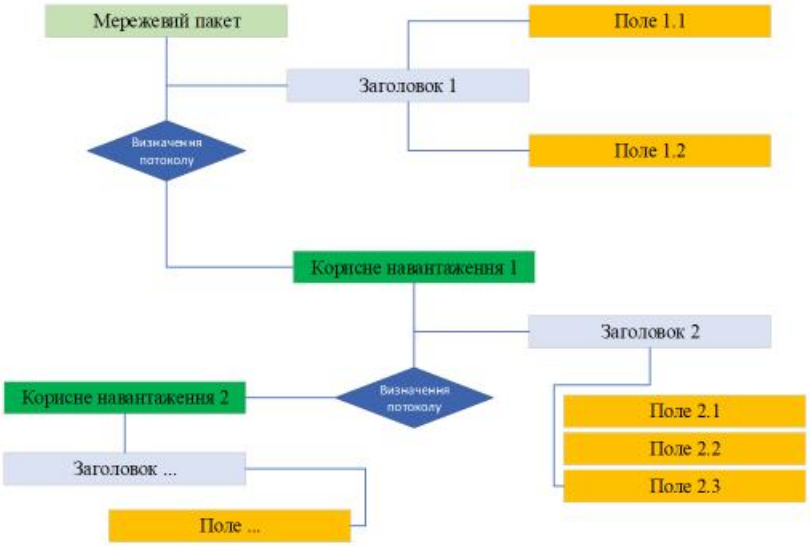
• запобігання мережевих атак;

• класифікація трафіку.

КЛАСИ ПРОВЕДЕНОГО РОЗБОРУ МЕРЕЖЕВИХ ПАКЕТІВ 4



ВИДІЛЕННЯ І РОЗБІР ЗАГОЛОВКІВ ПРОТОКОЛІВ В ПАКЕТІ 5



ФУНКЦІОНАЛЬНІ ВИМОГИ ДО АНАЛІЗАТОРІВ ТРАФІКУ 6

1. Відновлення та подальший розбір потоків даних з урахуванням можливого переупорядкування та / або втрати окремих пакетів.

2. Аналіз вкладених тунелів.

3. Аналіз зашифрованих (модифікованих) даних.

4. Автоматичне визначення протоколу вищого рівня.

5. Локалізація та відтворення помилок розбору.

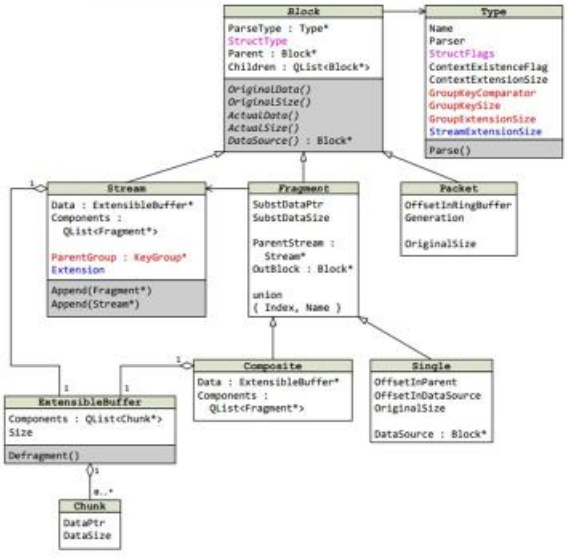
6. Додавання підтримки протоколів без внесення змін до вже існуючих модулів розбору.

7. Переносимість модулів розбору між режимами offline- та online-аналізу.

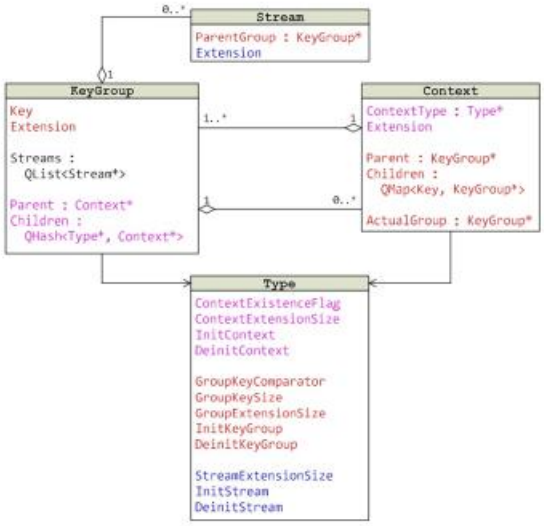
ЗАСОБИ АНАЛІЗУ МЕРЕЖНОГО ТРАФІКУ 7

##	SRC (IP:PORT)	DST (IP:PORT)	Коректне відновлення потоку		
			Wireshark v.2.2.3	Snort v.2.9.7.0	Bro v.2.5
Trace11.pcap					
1	68.142.205.139:80	192.168.0.105:25168	-	-	+
2	68.142.205.139:80	192.168.0.105:25175	-	-	+
3	68.142.205.139:80	192.168.0.105:25180	+	-	+
Trace12.pcap					
4	74.125.19.113:443	192.168.0.105:24044	+	-	+
5	68.142.205.139:80	192.168.0.105:24053	-	-	+
6	68.142.205.139:80	192.168.0.105:24060	+	-	+
7	68.142.205.139:80	192.168.0.105:24089	+	-	+
Trace13.pcap					
8	74.125.224.96:443	24.6.173.220:61960	+	-	+
Trace14.pcap					
9	174.46.74.87:80	192.168.2.7:43542	-	-	+

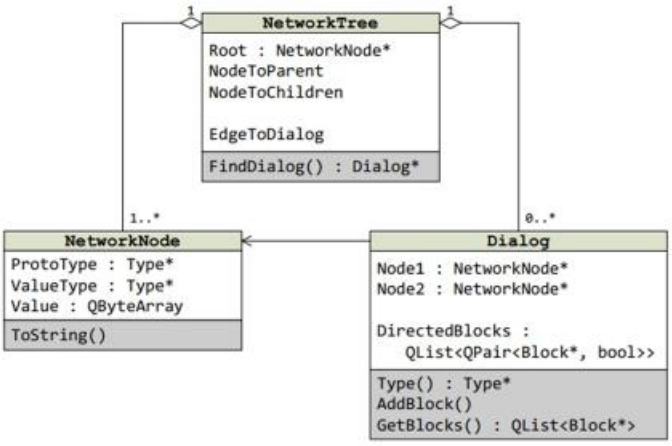
ДІАГРАМА КЛАСІВ ДЛЯ ОПИСУ РОЗІБРАНИХ МЕРЕЖЕВИХ ПАКЕТІВ 8



ДІАГРАМА КЛАСІВ ДЛЯ ОПИСУ ЛОГІЧНИХ З'ЄДНАНЬ 9



ДІАГРАМА КЛАСІВ ДЛЯ ОПИСУ УЧАСНИКІВ МЕРЕЖЕВОГО ОБМІНУ 10

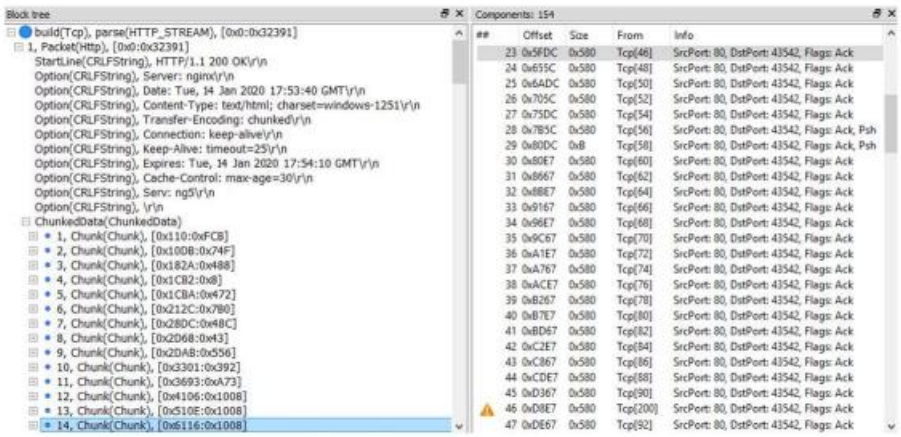


11

АНАЛІЗАТОР ТРАФІКУ

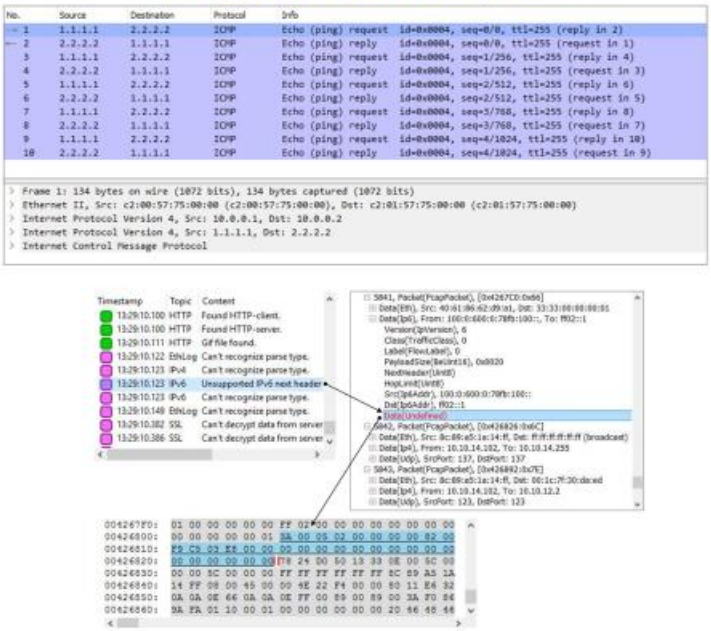
12

РЕЗУЛЬТАТИ РОБОТИ



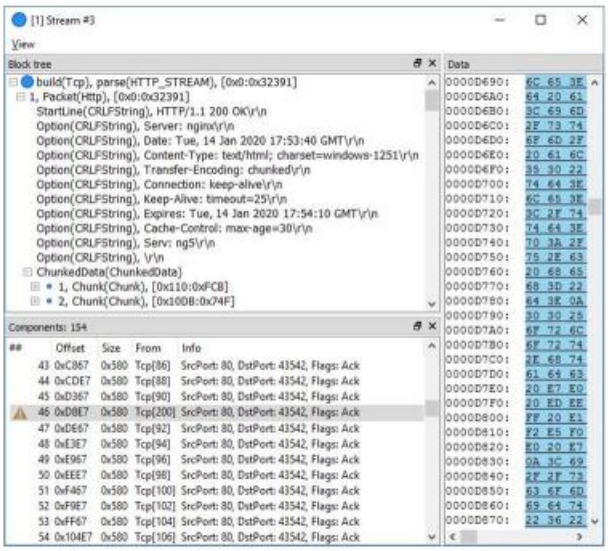
РЕЗУЛЬТАТИ РОБОТИ

13



РЕЗУЛЬТАТИ РОБОТИ

14



15 ВИСНОВКИ

Проведено дослідження методів та засобів аналізу мережного трафіку. Проаналізовано методи відновлення потоків даних для протоколів довільного рівня, в тому числі прикладного, які стійкі до втрат окремих мережевих пакетів, а також їх переупорядкування. Запропонована архітектура системи поглибленого аналізу мережевого трафіку, що дозволяє розробляти і налагоджувати модулі підтримки протоколів на попередньо збереженому трафіку (offline) і згодом використовувати ці модулі в режимі online. Розроблені та реалізовано програмні інструменти для проведення поглибленого аналізу мережевого трафіку в online і offline режимах.