МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА ─ Российский технологический университет»

РТУ МИРЭА

Институт информационных технологий (ИИТ)
Кафедра инструментального и прикладного программного обеспечения (ИиППО)

ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ

по дисциплине «Технологии передачи данных»

Лабораторная работа № 2

Студент группы *ИВБО-07-21, Стока Иван Павлович*
(подпись)

Преподаватель *Рогов И.Е.*
(подпись)

Отчет представлен «___»_____2023 г.

Москва 2023 г.

СОДЕРЖАНИЕ

ХОД РАБОТЫ

Шаг 1 UgraCTF

Для нахождения ключа необходимо отфильтровать все протоколы HTTP, после чего отследить путь протоколов, где в последнем запросе находим ячейку с данными (data). Там представлен код в системе HEX. Рассматриваем байт пакеты данной ячейки и получаем необходимый ключ (Рисунок 1).

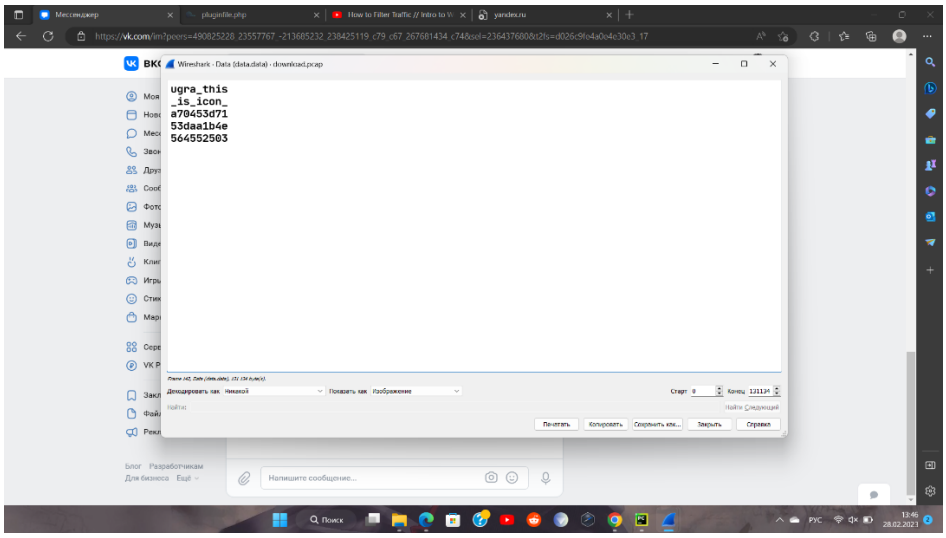

Рисунок 1 – Ключ

Проводится проверка правильности ключа (Рисунок 2).

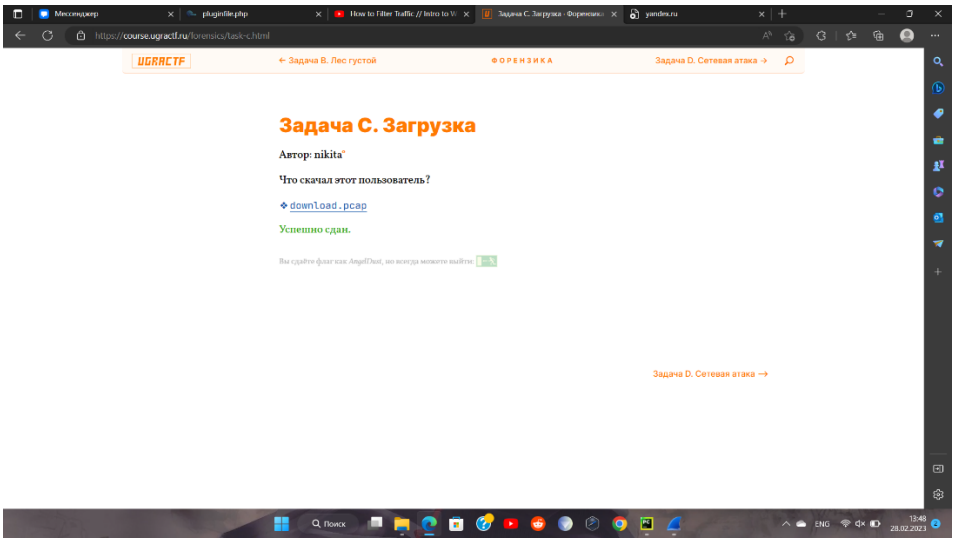

Рисунок 2 – Проверка правильности ключа

Шаг 2 UgraCTF

Необходимо сделать фильтр по HTTP протоколам, далее извлекаются по одной букве данные, приносившиеся запросами с text/html информацией. По итогу получаем ключ: ugra_pcap_with_trash_6eebc1fec68e6db. Проводится проверка правильности ключа (Рисунок 3).

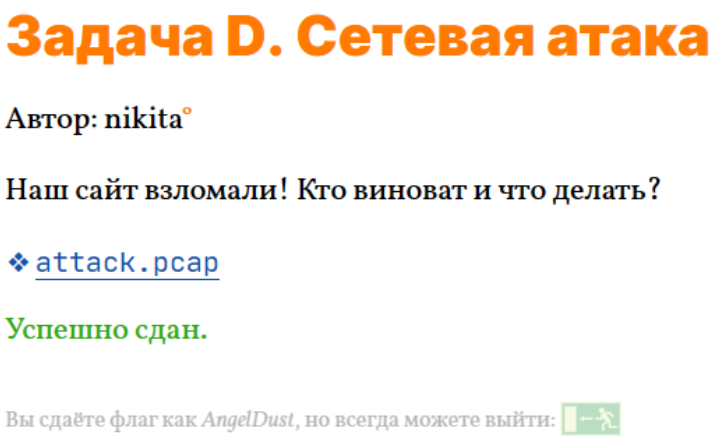

Рисунок 3 – Проверка правильности ключа

Шаг 3 FreeHackQuest

Проводится фильтрация TELNET протоколов. При проходе по запросам находится логин, пароль, а также ключ (Рисунок 4).

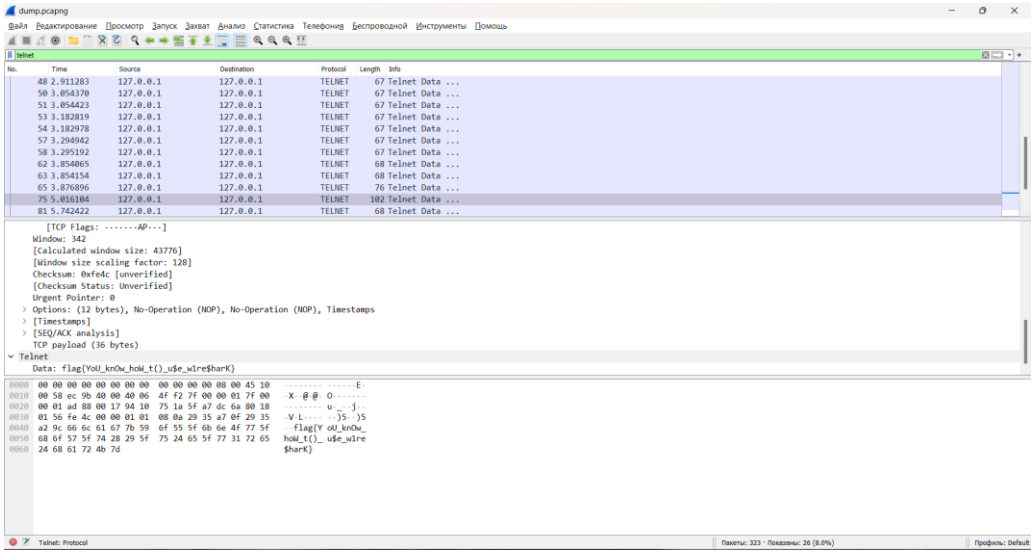

Рисунок 4 – Ключ

Проводится проверка правильности ключа (Рисунок 5).

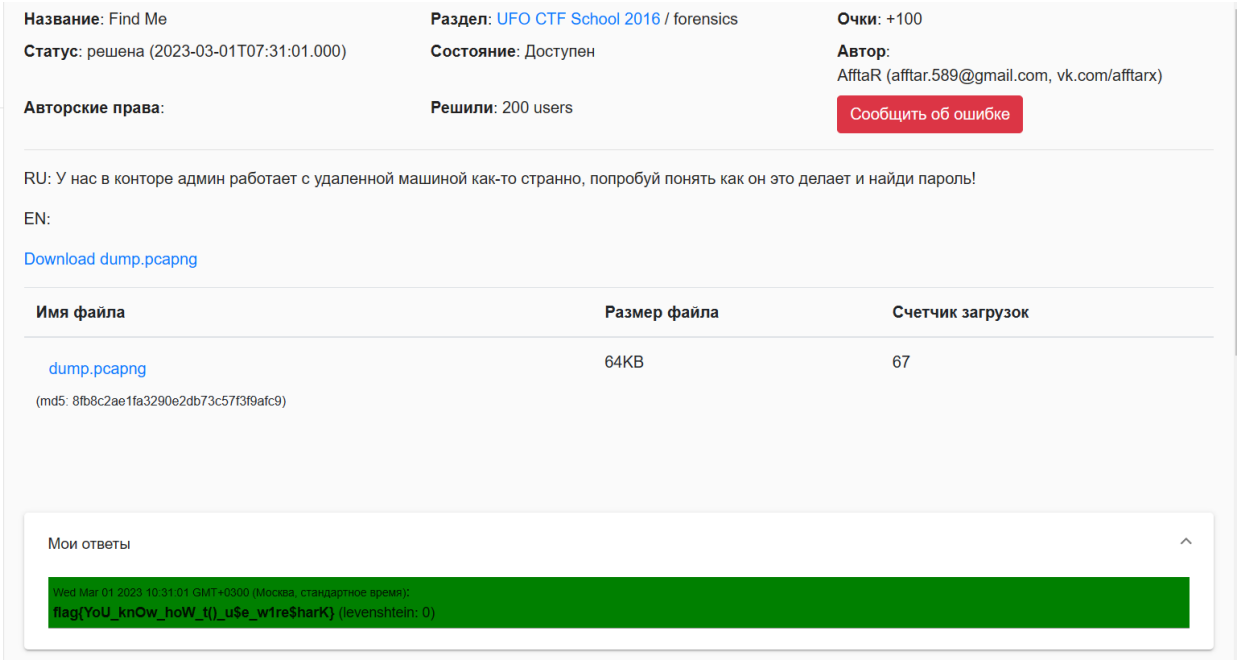

Рисунок 5 – Проверка правильности ключа

Шаг 4 FreeHackQuest

Проверяется через фильтр, существование в данных протоколов строки FLAG, используя команду data contains “FLAG”. По данному запросу выдаётся протокол типа ICMP с флагом, записанном в HEX системе (Рисунок 6).

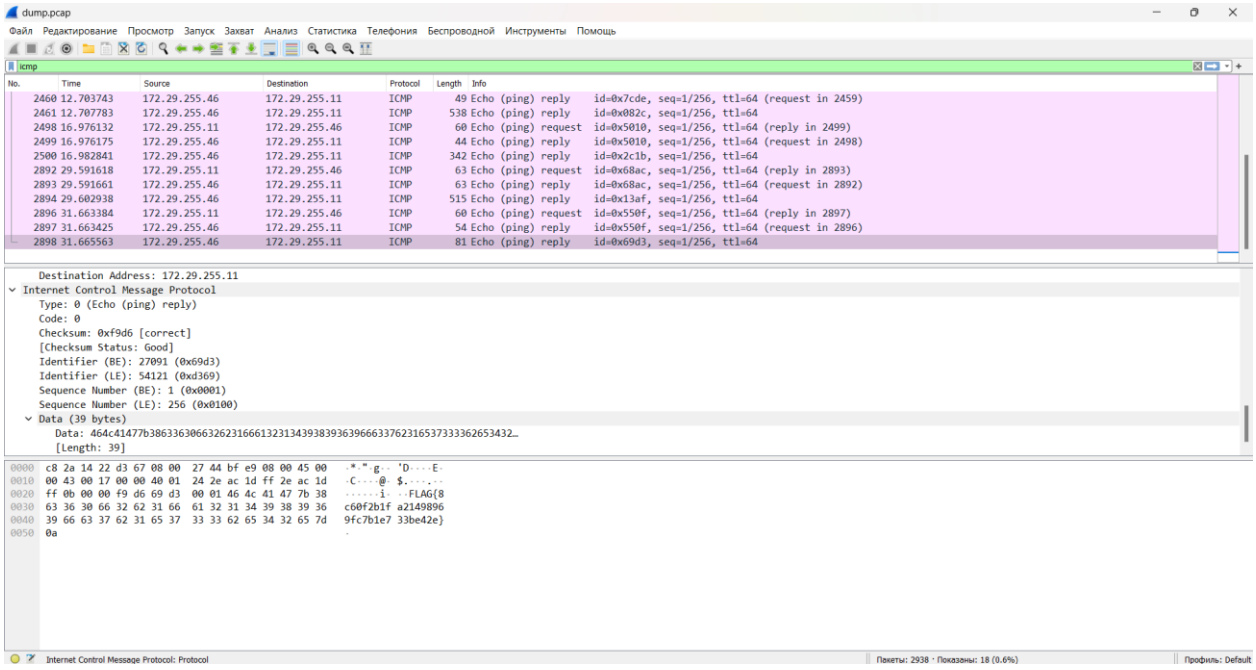

Рисунок 6 – Ключ

Проводится проверка правильности ключа (Рисунок 7).

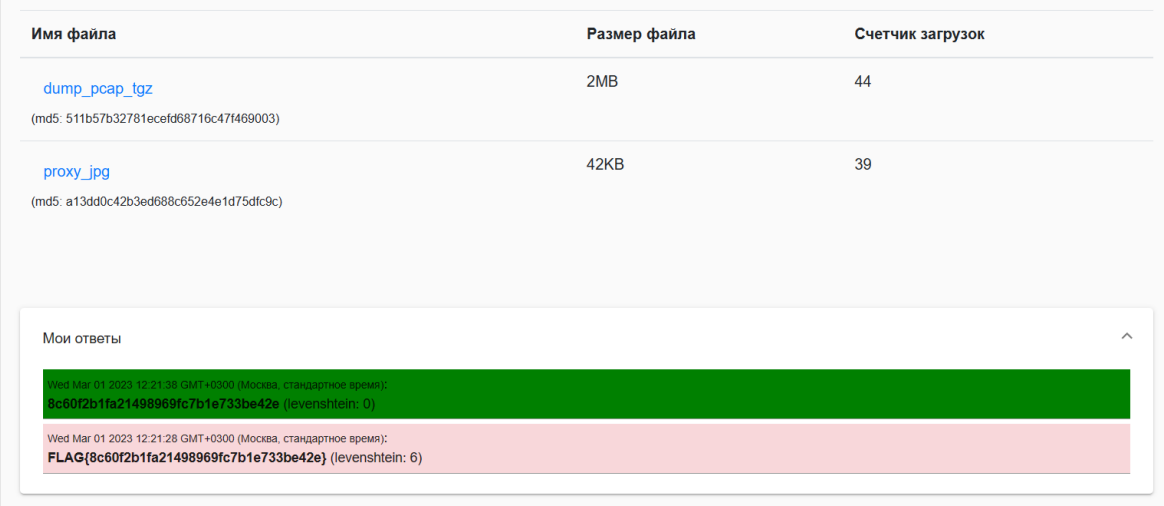

Рисунок 7 – Проверка правильности ключа

Шаг 5 PicoCTF

Делается фильтр по HTTP протоколам, выделяются запросы, возвращающие данные в text/html формате, по итогу находится закодированный флаг, который надо декодировать, в конечном итоге находится нужный ключ (Рисунок 8-9).

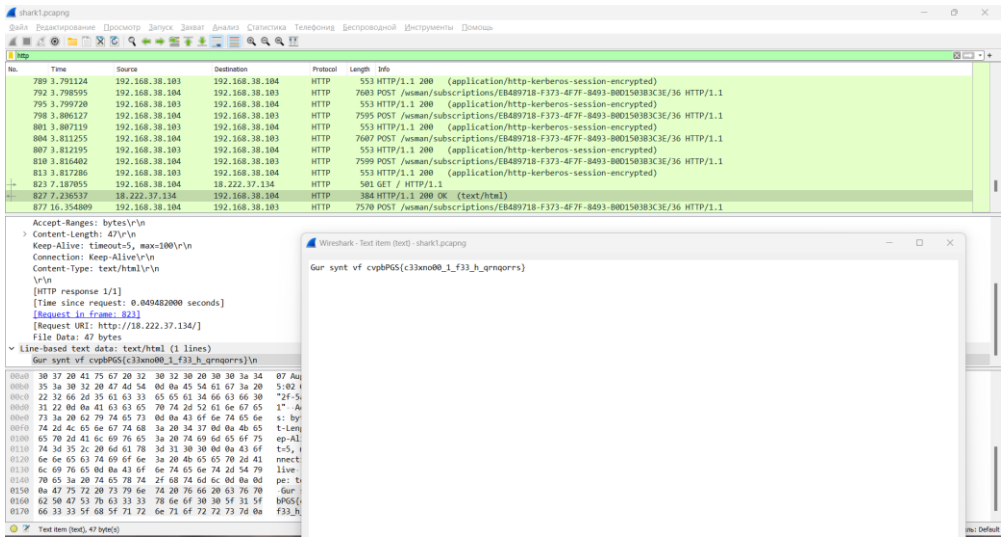

Рисунок 8 – Закодированный ключ

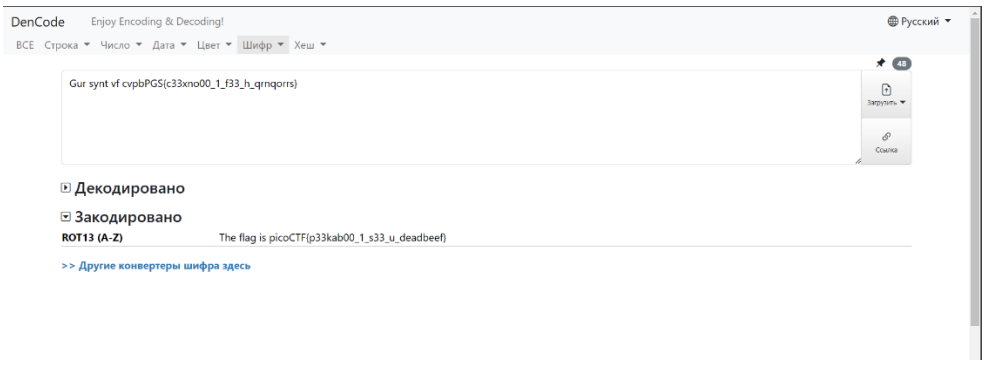

Рисунок 9 – Декодирование ключа

Проводится проверка правильности ключа (Рисунок 10).

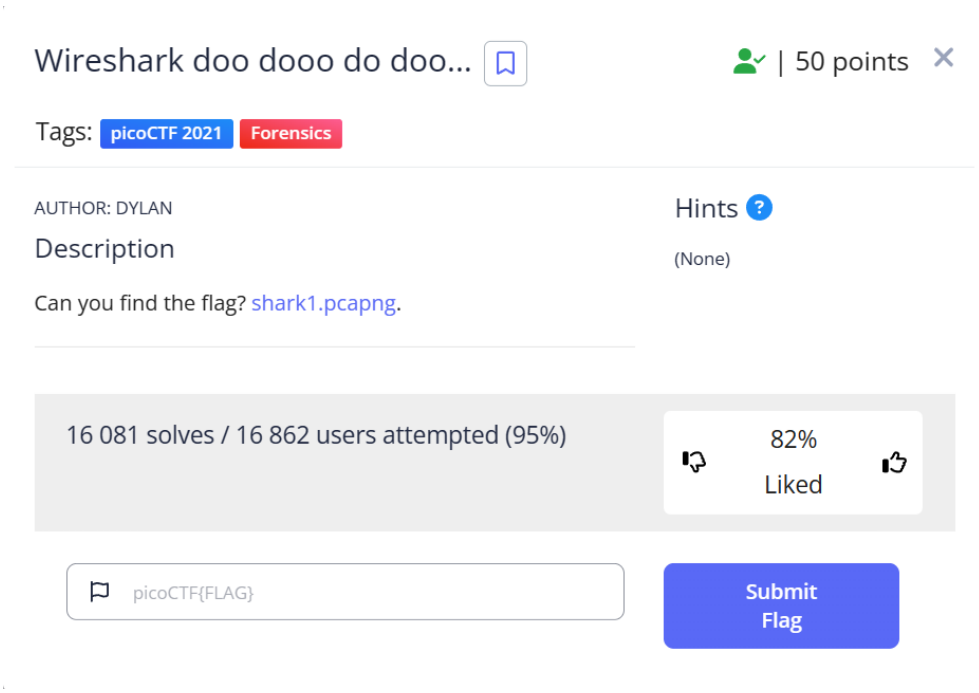

Рисунок 10 – Проверка правильности ключа

ЗАКЛЮЧЕНИЕ

В данной практической работе был изучен функционал программы Wireshark, отслеживающей трафик сети, на примере пентестов.

СПИСОК ИСТОЧНИКОВ

1. Олифер В.Г., Олифер В.А. Компьютерной сети. – 2-е изд. – Санкт-Петербург: Питер, 2021. – 1008 с.

2. Мастер класс по использованию Wireshark // youtube URL: https://www.youtube.com/watch?v=OU-A2EmVrKQ&list=PLW8bTPfXNGdC5Co0VnBK1yVzAwSSphzpJ (дата обращения: 01.03.2023).