**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Лабораторная работа № 1**

на тему «Технологии использования МЭ и СОВ»

|  |
| --- |
| Выполнил: студент группы ВКБ43 |
| Ковалев Данил Петрович |
| (Фамилия, имя, отчество) |
| Проверил: доцент |
| Решетникова Ирина Витальевна |
| (Фамилия, имя, отчество) |

## **Цель:**

* Изучить особенности функционирования межсетевого экрана и средства обнаружения вторжений;
* Применить на примере задач технологии использования МЭ и СОВ.

## Ход выполнения работы:

### **Задание № 1.**

### Разделить сеть 192.168.1.0/24 на подсети, согласно таблице:

Для выполнения задания разбиение на подсети будет производиться на основе равномерного разделения сетей.

Определим, какое количество бит нам необходимо использовать для разбиения сети 192.168.1.0/24 на 4 подсети .

Следовательно, для разбиения сети на подсети нам потребуется занять 2 бита из адресного пространства сети.

Определим общее количество устройств, которые можно подключить к данным подсетям. На каждую подсеть из 8 бит адресного пространства останется 6 бит для адресации устройств, то есть

Следовательно, ко всей сети мы сможем подключить В вычислении вычитались 2 адреса – один является широковещательным, второй – сетевой (нулевой) адрес.

Нулевые адреса определяются множеством комбинаций единиц на старших занятых битах адресного пространства сети, приведу вычисления ниже.

Широковещательными же являются адреса незанятого адресного пространства, биты которых равны единице. На основе полученных данных можно составить таблицу. Результаты представлены на таблице 1.

Таблица - разделение сети 192.168.1.0/24 на подсети

|  |  |  |  |
| --- | --- | --- | --- |
|  | Адрес подсети  Маска подсети | Диапазон адресов | Широковещательный адрес |
| Подсеть № 1 | 192.168.1.0/24  255.255.255.192 | 192.168.1.1 –  192.168.1.62 | 192.168.1.63 |
| Подсеть № 2 | 192.168.1.64/24  255.255.255.192 | 192.168.1.65 –  192.168.1.126 | 192.168.1.127 |
| Подсеть № 3 | 192.168.1.128/24  255.255.255.192 | 192.168.1.129 –  192.168.1.190 | 192.168.1.191 |
| Подсеть № 4 | 192.168.1.192/24  255.255.255.192 | 192.168.1.193 –  192.168.1.254 | 192.168.1.255 |

### **Задание № 2.**

Проанализировать IP-пакеты в сети, заданной схемой:

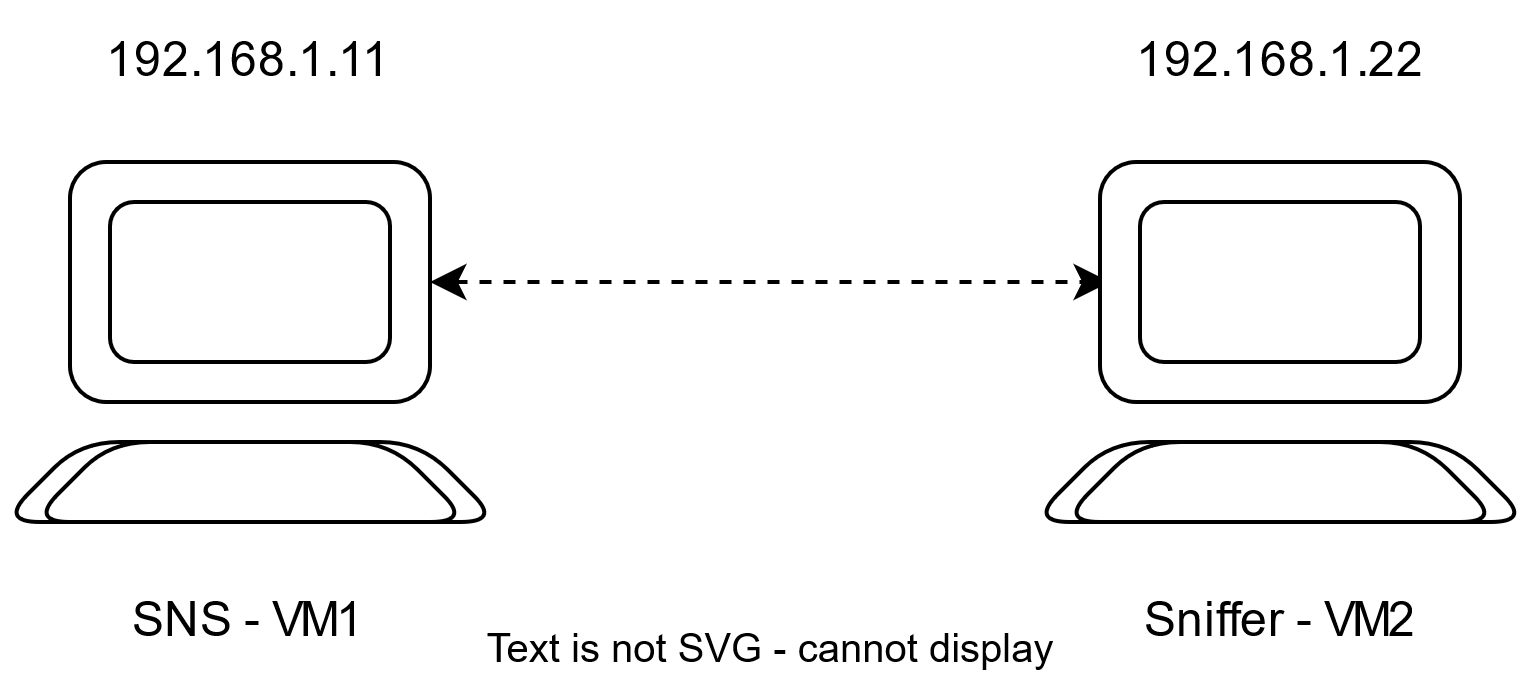


Рисунок 1 - схема сети 192.168.1.0 с имеющимися в ней устройствами SNS - VM1 и Sniffer - VM2

Для создания виртуальных машин будем использовать систему контейнеризации – Docker. Для создания двух виртуальных машин использовалась конфигурация, которая представлена ниже на рисунке 2.

В задании не указана необходимость в создании виртуальных машин на основе платформы Windows, и лабораторная не обязывает специально пользоваться Wireshark для анализа трафика. В следствии этого, мы будем использовать alpine linux для создания легковесной машины – sns-vm1, а в случае прослушивания будем использовать готовую сборку – nicolaka/netshoot, которая содержит консольную утилиту tshark.

Можно также обратить внимание, чтобы были заданы фактические IP контейнеров, которые связываются в общую Docker сеть.

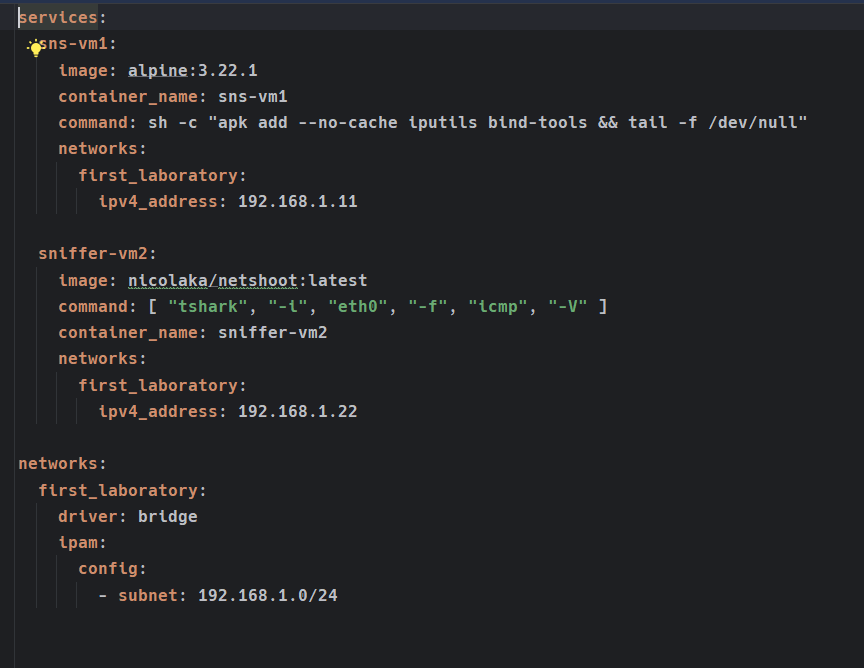


Рисунок 2 – docker compose для выполнения лабораторной

Попробуем теперь посмотреть из-под sns-vm1 видно ли хост sniffer-vm2. Для этого воспользуемся командой, которая представлена на рисунке 3. Можно убедиться, что хост 192.168.1.11 прекрасно видно, что означает, что устройства видят друг друга.

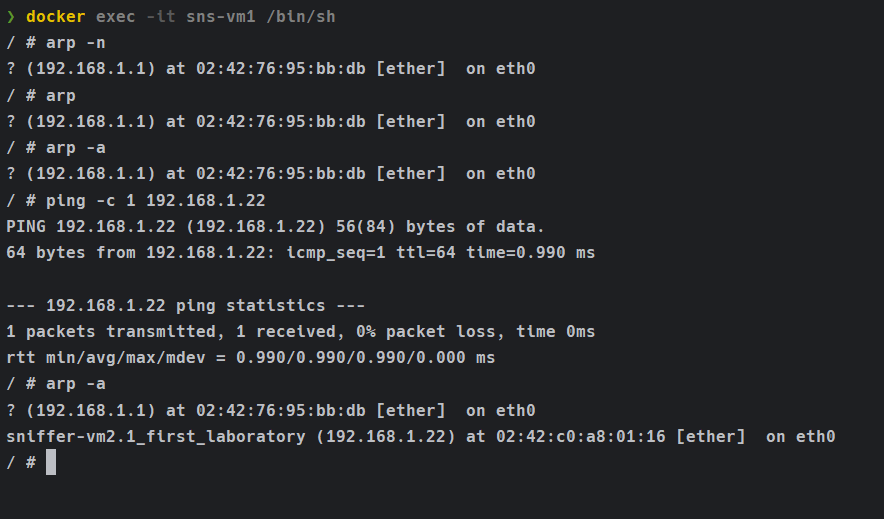


Рисунок 3 – таблица arp для sns-vm1

Посмотрим на более подробный вывод на хост, используя другие инструменты. Результат представлен на рисунке 4.

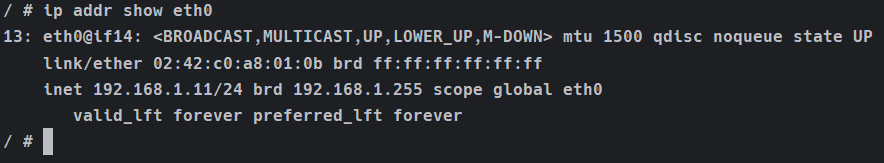


Рисунок 4 – более подробная информация по arp

Попробуем теперь произвести перехват пакетов. Для этого на Sniffer-VM2 с самого старта уже запущен сниффер с помощью утилиты t-shark. Мы попробуем отправить 1 пакет и посмотреть его содержимое. Результаты представлены на рисунках 5 и 6.

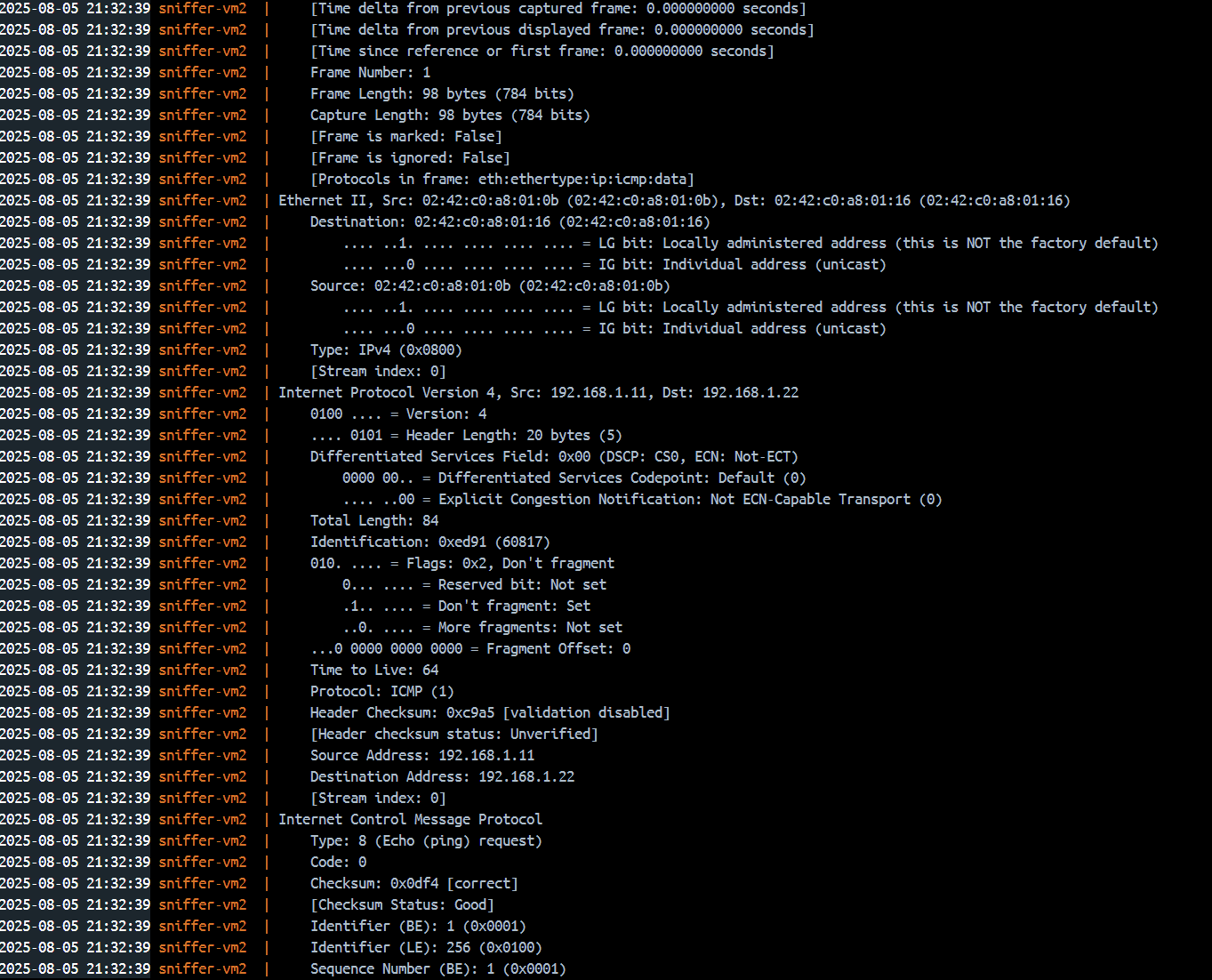


Рисунок 5 – информация о пакетах ч.1.

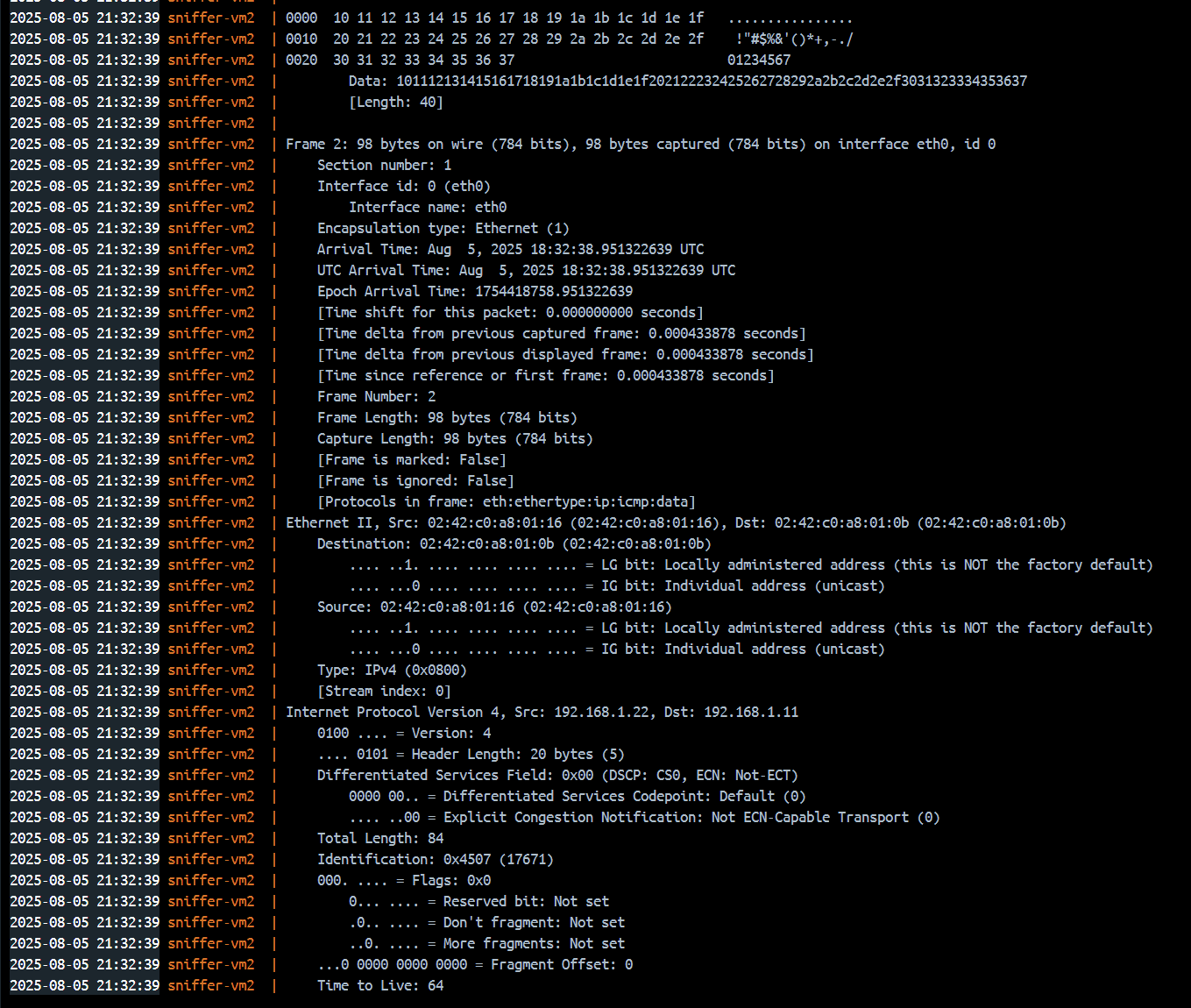


Рисунок 6 – информация о пакетах ч.2.

Проведем анализ полученных данных и что получилось. Можно увидеть, что у нас используются протоколы в фрейме: ICMP, IP, ETH, Ethertype, data. Есть длина пакета (frame length), есть описание MAC адресов. можно заметить, что соединение осуществлено по протоколу IPv4, отправителем является хост 192.168.1.11, получателем является хост 192.168.1.22. Пакет соответствует протоколу ICMP, предназначенный для отправки сообщений.

## Вывод:

В данной лабораторной работе были изучены технологии применения МЭ и СОВ, а также на конкретных примерах были разобраны особенности разделения подсетей, установки соединения между хостами сети, отправка и перехват пакетов, а также анализ полученных данных.