Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационный технологий и управления

Кафедра интеллектуальных информационных технологий

Дисциплина: «Средства и методы защиты информации в  
интеллектуальных системах»

Лабораторная работа №8 по теме:  
«Наблюдение за стеком TCP/IP»

Студент гр. 121702

Заломов Р.А.

Проверил:

Сальников Д.А.

Минск 2023

**Тема**

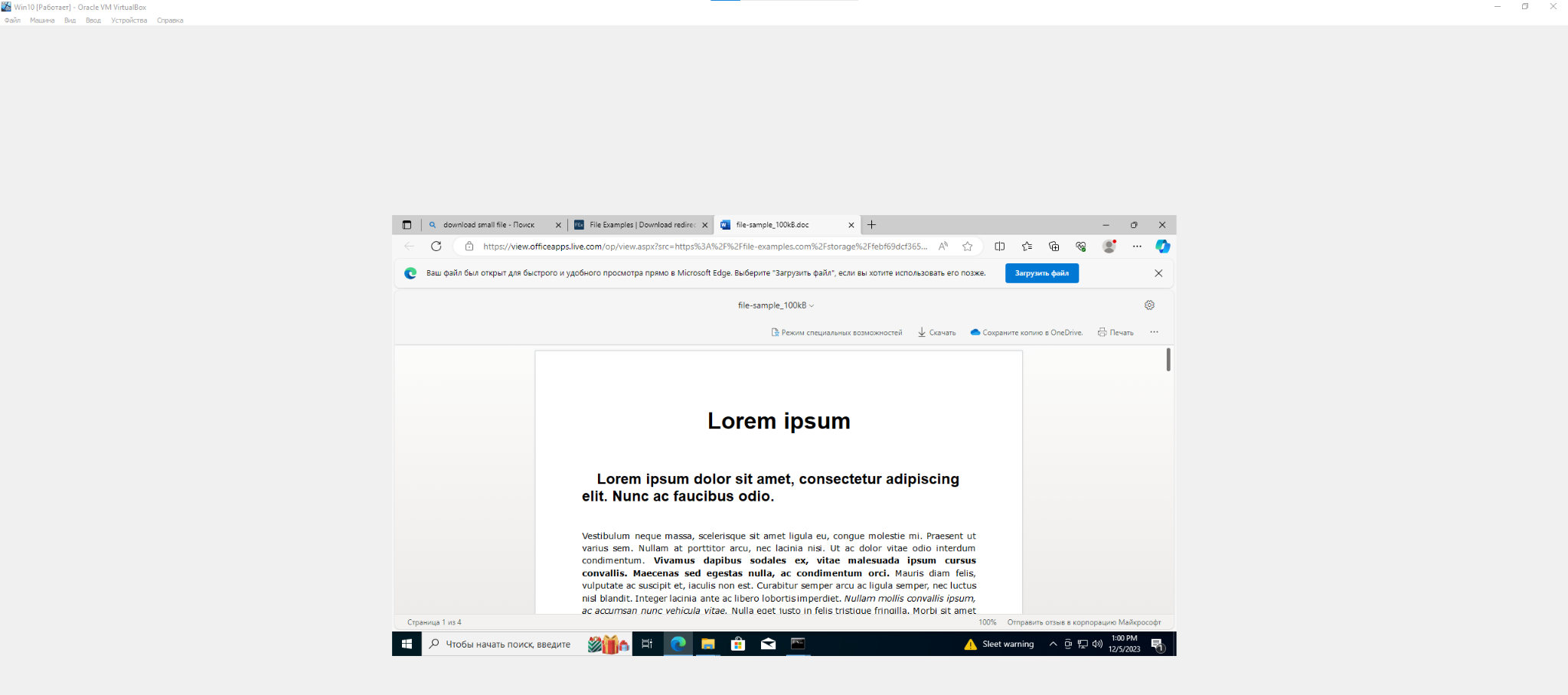
Наблюдение за стеком TCP/IP

**Задание**

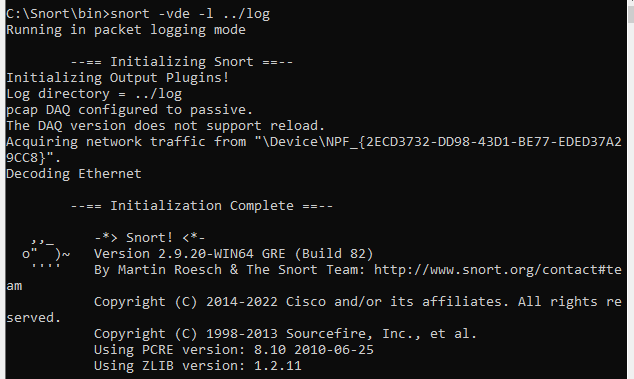
1. На основном компьютере запустить виртуальную машину.
2. Установить Snort.
3. Запустить Snort в режиме Sniffer пакетов или протоколирования с различными параметрами детализации.
4. Обратится к локальной сети. Выполнить команду ping, запустить браузер или проводник. Сохранить какой либо файл (не большой) на материнской машине.
5. Остановить Snort. Определить к каким IP-портам и адресам были выполнены обращения.
6. Пользуясь \windows\system32\etc\service, определить какие системные службы использовались.
7. Просмотреть содержимое перехваченных пакетов.
8. Используя дополнительную литературу расшифровать содержание вывода заголовка.

**Выполнение задания**

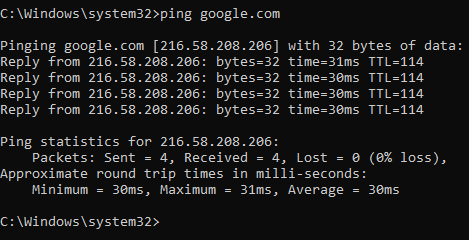
В качестве виртуальной машины использовалась виртуальная машина VirtualBox на базе операционной системы Windows 10.



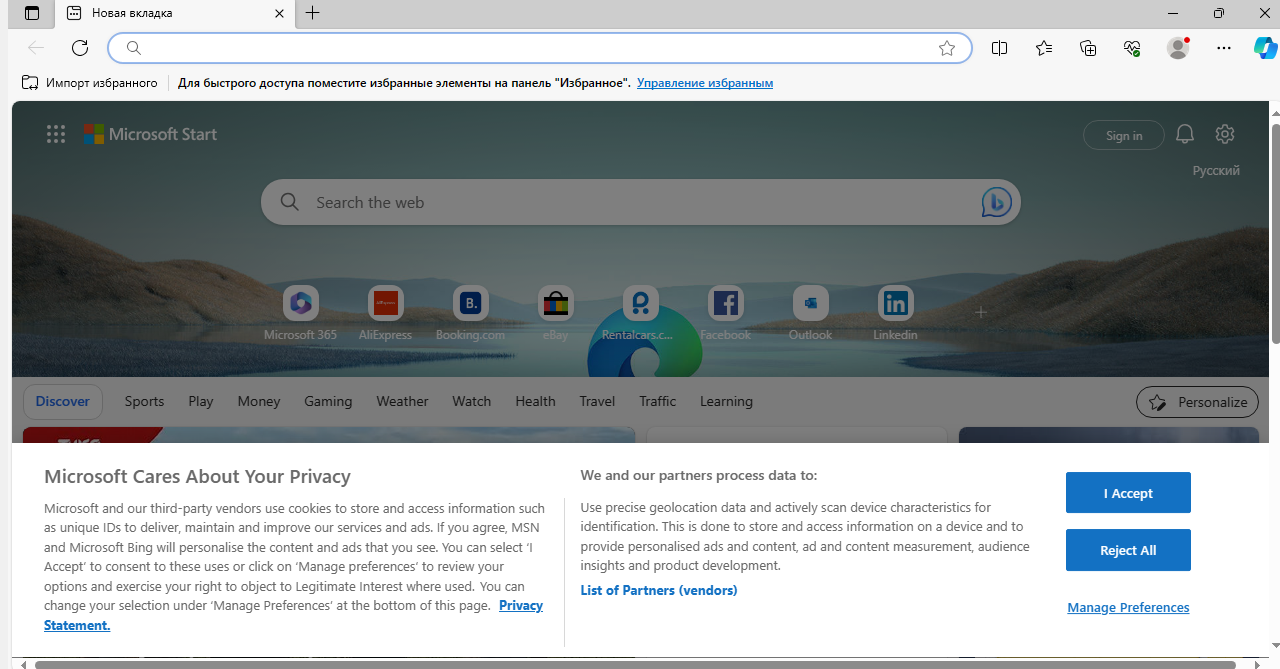
Запуск Snort и выполнение различных действий, связанных с сетевым взаимодействием

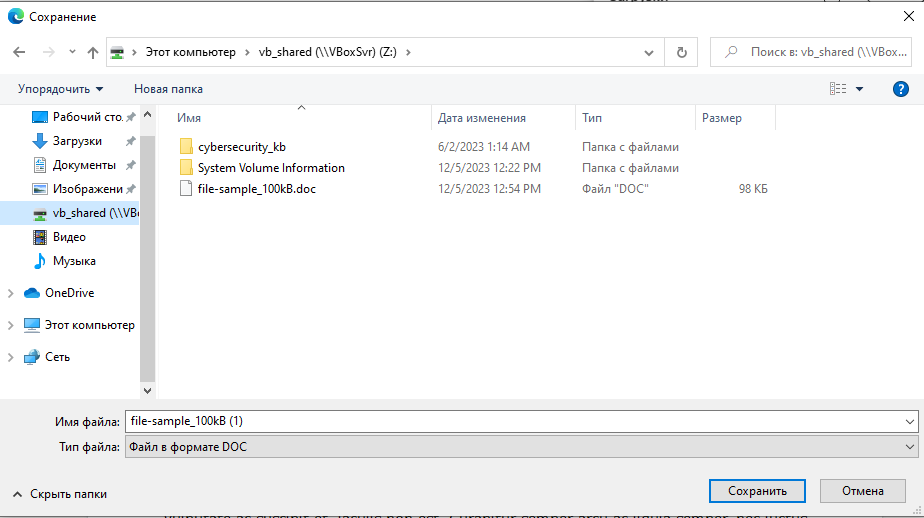
Запуск Snort  
  


Выполнение команды Ping

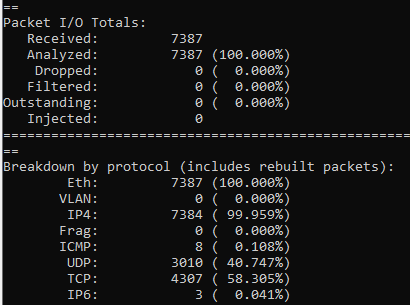


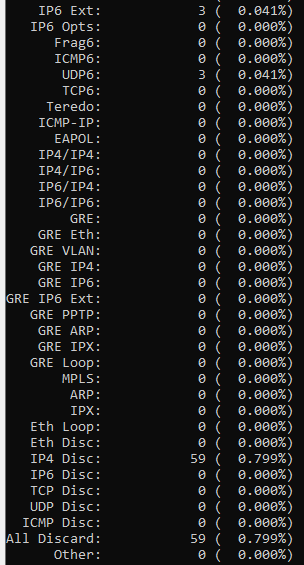
Открытие браузера



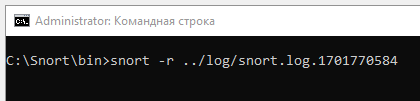
Сохранение файла в общую с материнской машиной папку  


Завершение работы и статистика

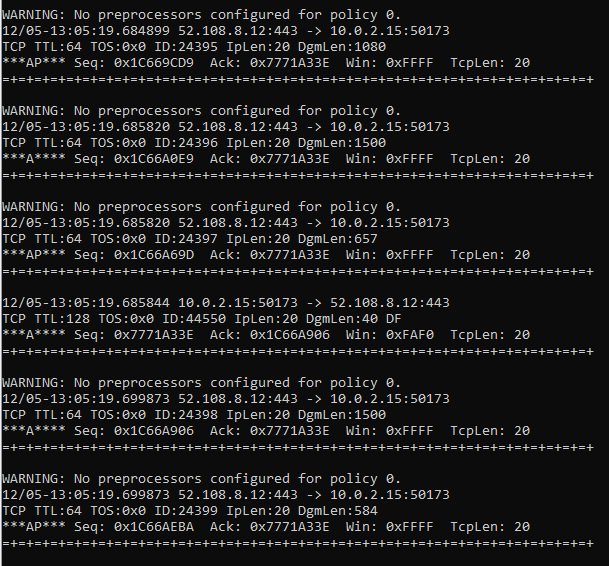




Просмотр логов

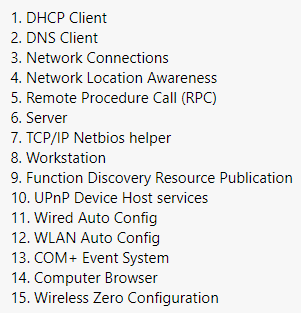


Пример вывода

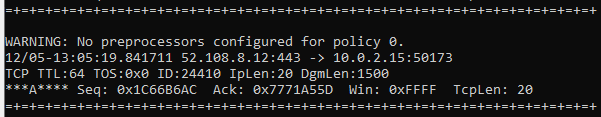


Определить IP/Port отправителя и получателя можно следующим методом - из отдельно выведенной строки с информацией о пакете взять вторую строку (если исключить строку с WARNING, то нужно взять первую строку) и рассмотреть значения, находящиеся по разные стороны от стрелки. Например, возьмём строку: 10.0.2.15:50173 -> 52.108.8.12:443. Здесь 10.0.2.15 - IP отправителя; 50173 - порт отправителя; 52.108.8.12 - IP получателя; 443 - порт получателя (443 - порт, по которому работает протокол HTTPS).

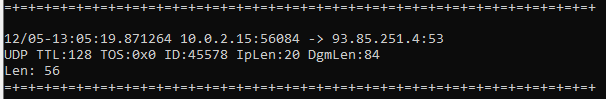
Для работы с сетью в Windows необходима работа следующих сервисов, которые автоматически запускаются фаерволом Windows



Рассмотрим несколько пакетов и опишем характеристики, которые можно узнать из информации о нём:



IP-отправителя: 52.108.8.12  
IP-получателя: 10.0.2.15  
Порт отправителя: 443  
Порт получателя: 50173  
Протокол транспортного уровня: TCP  
Время жизни (TTL): 64  
Тип обслуживания (TOS): 0x0  
Идентификатор пакета (ID): 24410  
Длина IP-заголовка (IpLen): 20 байт  
Общая длина пакета (DmgLen): 1500 байт  
Номер первого байта передаваемого сегмента (Seq): 0x1C66B6AC  
Номер следующего байта, ожидаемого к получению (Ack): 0x7771A55D  
Размер скользящего окна (Win): 0xFFFF  
Длина TCP-заголовка (TcpLen): 20 байт

****

IP-отправителя: 10.0.2.15  
IP-получателя: 93.85.251.4  
Порт отправителя: 56084  
Порт получателя: 53  
Протокол транспортного уровня: UDP  
Время жизни (TTL): 128  
Тип обслуживания (TOS): 0x0  
Идентификатор пакета (ID): 45578  
Длина IP-заголовка (IpLen): 20 байт  
Общая длина пакета (DmgLen): 84 байта  
Длина полезной нагрузки (Len): 56 байт  
Длина UDP-заголовка: DmgLen - IpLen - Len = 84 - 20 - 56 = 8 байт

Стоит отметить, что пакеты, протоколом транспортного уровня которых является UDP, содержат меньше информации, чем пакеты с транспортным протоколом TCP. Это объясняется спецификой данных протоколов: UDP предназначен для быстрого обмена информацией, TCP - для надёжного обмена информацией. По протоколу TCP отслеживается установление соединения между устройствами, проверка целостности полученных данных, проверка факта получения данных, порядок полученных данных. Это объясняет увеличение количества отправляемой вместе с пакетом информации.

**Вывод**

В ходе лабораторной работы были рассмотрены принципы работы с программой отслеживания сетевых пакетов Snort. Посредством различных действий (выполнение команды ping, открытие браузера, обмен файлом в общей папке виртуальной и материнской машин) был произведён обмен сетевыми пакетами между различными системами. Данные пакеты были обнаружены ПО Snort. Впоследствии был произведён анализ информации, полученной из отловленных сетевых пакетов.