Министерство образования

Республики Беларусь

Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

Кафедра: интеллектуальных информационных технологий

Отчёт

По дисциплине

«Средства и методы защиты информации в интеллектуальных системах»

Тема: «Наблюдение за стеком TCP/IP»

Написал: Проверил

Германенко В.В., гр. 321701 Сальников Д. А.

Минск 2025

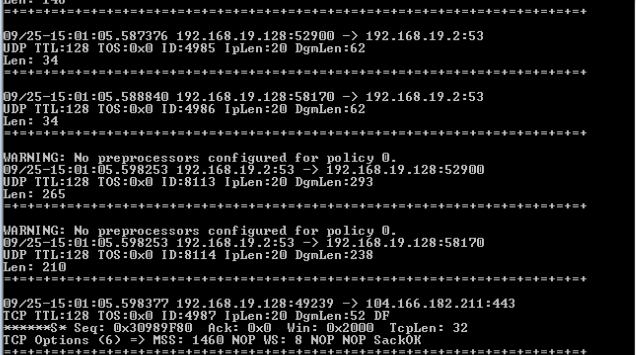
Задача:

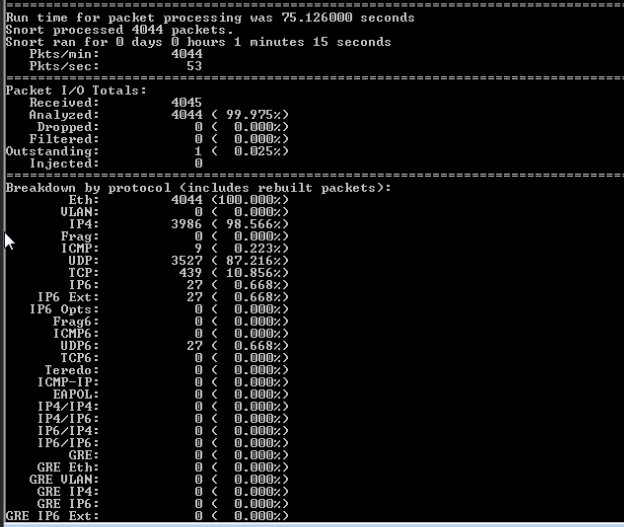
1. На основном компьютере запустить Виртуальную машину. Измените имя компьютера на уникальное.
2. Установить Snort.
3. Запустите Snort в режиме Sniffer пакетов или протоколирования с различными параметрами детализации.
4. Обратитесь к локальной сети. Выполните команду ping, запустите броузер или проводник. Сохраните какой либо файл (не большой) на материнской машине.
5. Остановите Snort. Определите к каким IP-портам и адресам были выполнены обращения.
6. Пользуясь \windows\system32\etc\service, определите какие системные службы использовались.
7. Просмотрите содержимое перехваченных пакетов.
8. **Используя дополнительную литературу расшифруйте содержание вывода заголовка.** Оформите отчет. В отчет обязательно поместите примеры пакетов и список обнаруженных протоколов и служб.

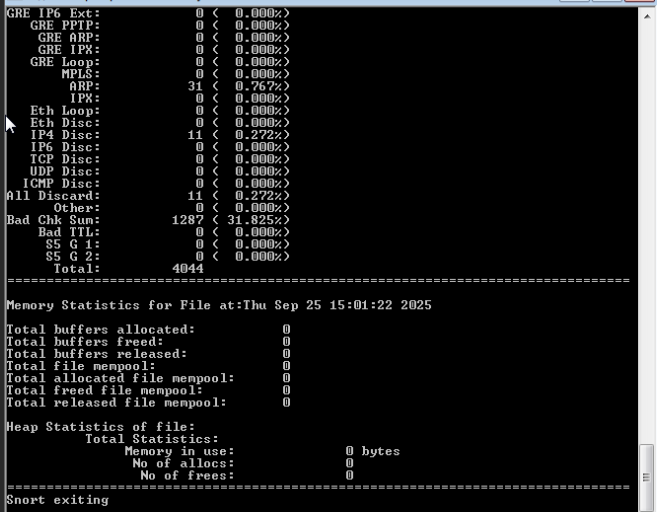
Реализация:

Использовал команду snort -v -i 5 -N что бы запустить режим sniffer, выполнил несколько ping команд: ping 8.8.8.8 -n 3, ping 192.168.19.1 -n 3

Примеры вывода snort:







Службы:



Вывод: Освоил принципы работы со стеком TCP/IP, команды и особенности snort.