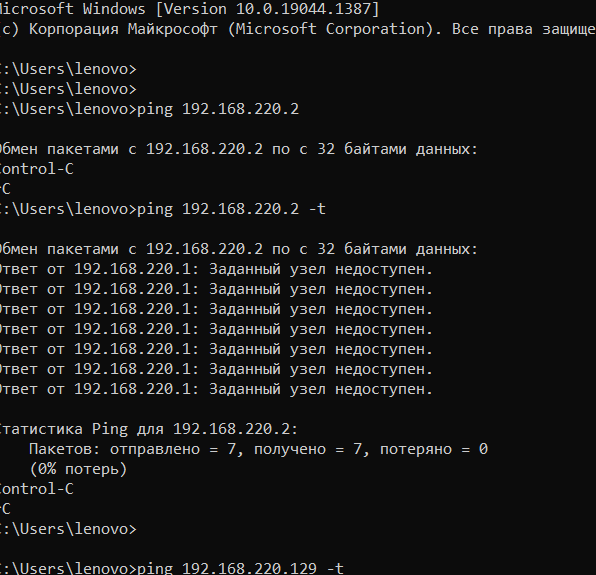
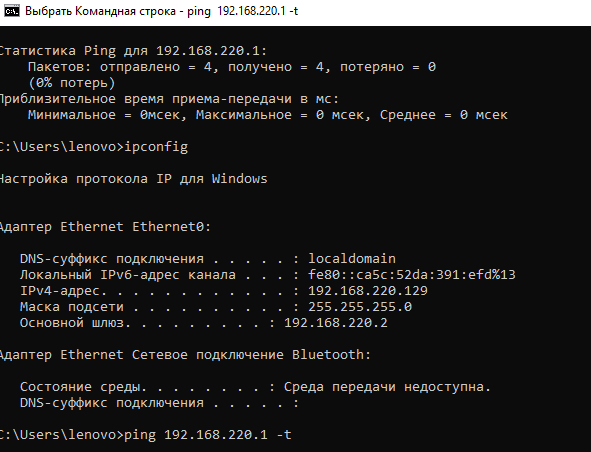
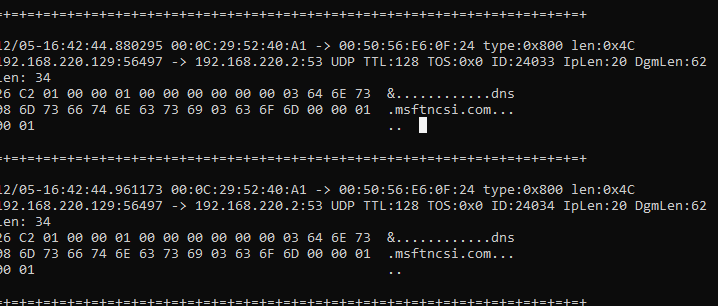


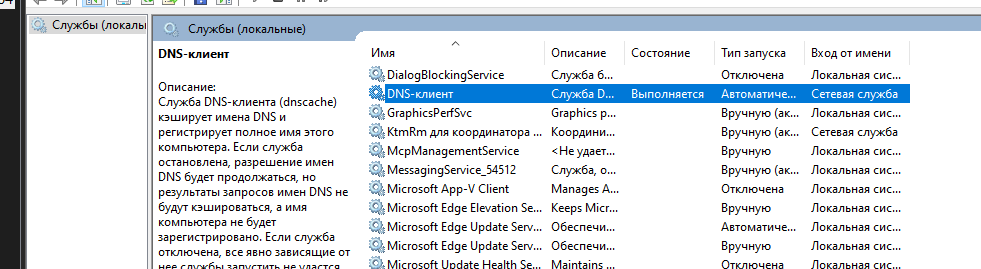
1. Запустите Snort в режиме Sniffer пакетов или протоколирования с различными параметрами детализации.





1. Обратитесь к локальной сети. Выполните команду ping, запустите броузер или проводник. Сохраните какой либо файл (не большой) на материнской машине.
2. Остановите Snort. Определите к каким IP-портам и адресам были выполнены обращения.





Отчет:

Запуск виртуальной машины и изменение имени компьютера:

- Запустил виртуальную машину на основном компьютере.

- Изменил имя компьютера на "UniqueVM".

Установка Snort:

- Скачал последнюю версию Snort с официального сайта.

- Запустил установочный файл и следовал инструкциям мастера установки.

- Проверил успешность установки, выполнив команду "snort -V" в командной строке.

Запуск Snort в режиме Sniffer пакетов:

- Запустил Snort в режиме Sniffer с различными параметрами детализации.

- Настроил Snort на отслеживание и регистрацию сетевых пакетов в реальном времени.

Обращение к локальной сети и сохранение файла:

- Взаимодействовал с локальной сетью, выполнив команду "ping" на другой компьютер.

- Запустил веб-браузер и проводник для обращения к различным ресурсам в сети.

- Сохранил небольшой файл на материнской машине.

Остановка Snort и определение обращений к IP-портам и адресам:

- Остановил работу Snort и получил лог-файл с информацией о пакетах.

- Изучил лог-файл и определил, к каким IP-портам и адресам были выполнены обращения.

Использование файла \windows\system32\etc\service для определения системных служб:

- Открыл файл \windows\system32\etc\service и изучил его содержимое.

- Определил, какие системные службы использовались во время работы Snort.