Анализатор сетевого трафика Wireshark

- Установите и запустите в привилегированном режиме анализатор сетевого трафика *Wireshark* . О базовой функциональности снифера *Wireshark* можно узнать, например, из учебных роликов, выложенных на ресурсах:

https://www.youtube.com/watch?v=r0l_54thSYU
http://www.youtube.com/watch?v=6X5TwvGXHP0
http://www.youtube.com/watch?v=r0l_54thSYU
http://www.youtube.com/watch?v=qs_DqMdlKHY

- Отфильтруйте трафик протокола ICMP (трафик порождается, например, утилитами ping , traceroute). Приведите в отчете подробный формат пакета, содержащего ICMP сообщение с пояснением назначения каждого из полей.
Воспроизведите различные режимы работы утилит и приведите снятые снифером дампы пакетов с соответствующими этим режимам кодами сообщений или ошибок в полях пакетов.

- Проанализируйте трафик ARP (протокола преобразования адресов). поясните предназначение ARP-таблиц и приведите (с пояснениями) дампы ARP-сообщений, снятые снифером.

- Установите на компьютере лаборатории FTP-сервер или воспользуйтесь имеющимся.
- Продемонстрируйте уязвимость протокола FTP (имена и пароли пользователей передаются по незащищённым сетям в открытом виде) путем извлечения информации из пакетов с помощью анализатора трафика.
- Выполните, по возможности, настройки, повышающие уровень защиты ftp-сервера (измените текст приветствия, организуйте отправку баннеров соединений, обезопасьте анонимный доступ) и проверьте работу настроек ftp-сервера, соединяясь с ним с клиентского приложения.

- Сопоставьте защищенность протоколов удаленного доступа Telnet и SSH.
Действуйте по схеме, аналогичной демонстрации уязвимости протокола FTP.

- Проанализируйте сообщение транспортного уровня: UDP-дейтаграммы и TCP-сегменты.