# 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.
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.

- Продемонстрируйте уязвимость протокола FTP (имена и пароли пользователей передаются по незащищённым сетям в открытом виде) путем извлечения информации из пакетов с помощью анализатора трафика.

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

- Попытайтесь проанализировать сообщения транспортного уровня: UDP-дейтаграммы и TCP-сегменты.

## *ТРЕБОВАНИЯ К ОТЧЕТАМ*

По результатам выполнения лабораторных работ необходимо составлять отчет. Рекомендуется составлять отчет параллельно с выполнением заданий лабораторных работ, не оставляя этот процесс на потом. Отчет должен быть оформлен с титульным листом с названием университета, института и высшей школы. На титульном листе указывается ф.и.о. студента исполнителя работы, номер студенческой группы и ф.и.о. преподавателя.

В отчете приводится информация, удостоверяющая выполнение студентом заданий лабораторных работ: скриншоты с результатами исполнения сценариев, команд и программ, командных файлов, дампы памяти и пакетов, составленные вами скрипты (*BASH* или др.), ответы на поставленные в заданиях вопросы и т.д.

Результаты выполнения каждого из  заданий должны предваряться в отчете фрагментом текста, формулирующим само задание (фрагменты копируются прямо из текста заданий).

Защита лабораторных работ происходит по предъявлению оформленного отчета и сопровождается демонстрацией исполнения программ и командных файлов, а также ответами на вопросы преподавателя.

Отчет можно создавать под *ОС Linux*, например, с помощью приложения *LibreOffice Writer* , сохраняя в *Home* каталоге вашего рабочего компьютера. Либо можете использовать офисные средства от MS Windows или MacOS.