Wireshark

Порядок выполнения

1. Перейти по ссылке github-classroom: сгенерируется репозиторий для сдачи работы
2. Ознакомиться с заданием (в ReadMe на всякий случай продублировано то, что ниже идёт под заголовком «Задание»)
3. Создать ветку wireshark и переключиться на неё
4. Выполнить задание в ветке (закоммитить/залить изменения в ветку)
5. Запросить Pull Request (в имени PR должна присутствовать фамилия, инициалы и группа для идентификации студента)
6. После создания PR начнут проходить автоматизированные тесты
7. Добиться прохождения тестов стандартным образом через дополнительные коммиты в ветку (запускаются по каждому коммиту в ветку после создания PR)
8. Назначить reviewer PR на eugenyk
9. Дождаться проведения обзора и принятия PR в master-ветку. После слияния работа считается сделанной успешно

Задание

Содержимое файла

В каталоге file-content выложен трафик в формате (сжатом zip), пригодном для загрузки в wireshark. Мы знаем, что в предпоследней коммуникации по порту 6789 по протоколу HTTP был передан файл. Необходимо узнать содержимое этого файла и заполнить им файл answer, находящийся в директории file-content

Анализ коммуникации

В каталоге communication выложен трафик в формате (сжатом zip), пригодном для загрузки в wireshark. Мы знаем, что на порту 3389 по адресу 192.168.1.101 был поднят TCP-сервер, к которому последовательно соединялись и отсоединялись клиенты из подсети 192.168. Необходимо перечислить в файле connect IP-адреса клиентов в порядке их соединения и в файле disconnect в порядке отсоединения (по 1 адресу в строке)

Подсказки

Могут пригодиться команды и функции:

- Decode as
- Show packet bytes
- Flow Graph (в том числе в внутренней фильтрацией по display filter)
- Фильтры:

- tcp.port