Практика 1. Wireshark: HTTP (сдать до 23.02.2022)

Эта работа исследует несколько аспектов протокола HTTP: базовое взаимодействие GET/ответ, форматы сообщений HTTP, получение больших файлов HTML, получение файлов HTML со встроенными объектами, а также проверку подлинности и безопасность HTTP.

Во всех заданиях предполагается, что вы к своему ответу приложите подтверждающий скрин программы Wireshark (достаточно одного скрина на задание).

Задание 1. Базовое взаимодействие HTTP GET/response (2 балла)

Подготовка:

1. Запустите веб-браузер.
2. Запустите анализатор пакетов Wireshark, но пока не начинайте захват пакетов. Введите «http» в окне фильтра, чтобы позже в окне списка пакетов отображались только захваченные сообщения HTTP.
3. Подождите несколько секунд, а затем начните захват пакетов Wireshark.
4. Введите в браузере адрес: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
5. Ваш браузер должен отобразить очень простой однострочный HTML-файл.
6. Остановите захват пакетов Wireshark.

Вопросы:

1. Использует ли ваш браузер HTTP версии 1.0 или 1.1? Какая версия HTTP работает на сервере?
2. Какие языки (если есть) ваш браузер может принимать? В захваченном сеансе какую еще информацию (если есть) браузер предоставляет серверу относительно пользователя/браузера?
3. Какой IP-адрес вашего компьютера? Какой адрес сервера gaia.cs.umass.edu?
4. Какой код состояния возвращается с сервера на ваш браузер?
5. Когда HTML-файл, который вы извлекаете, последний раз модифицировался на сервере?
6. Сколько байтов контента возвращается вашему браузеру?

Задание 2. HTTP CONDITIONAL GET/response (2 балла)

Большинство веб-браузеров выполняют кэширование объектов и, таким образом, выполняют условный GET при извлечении объекта HTTP. Прежде чем выполнять описанные ниже шаги, убедитесь, что кеш вашего браузера пуст.

Подготовка:

1. Запустите веб-браузер и убедитесь, что кэш браузера очищен.
2. Запустите анализатор пакетов Wireshark.
3. Введите следующий URL-адрес в адресную строку браузера:
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html .
   Ваш браузер должен отобразить очень простой пятистрочный HTML-файл.
4. Введите тот же URL-адрес в браузер еще раз (или просто нажмите кнопку обновления в браузере).

5. Остановите захват пакетов Wireshark и введите «http» в окне фильтра, чтобы в окне списка пакетов отображались только захваченные HTTP-сообщения.

Вопросы:

1. Проверьте содержимое первого HTTP-запроса GET. Видите ли вы строку «IF-MODIFIED-SINCE» в HTTP GET?
2. Проверьте содержимое ответа сервера. Вернул ли сервер содержимое файла явно? Как вы это можете увидеть?
3. Теперь проверьте содержимое второго HTTP-запроса GET (из вашего браузера на сторону сервера). Видите ли вы строку «IF-MODIFIED-SINCE:» в HTTP GET? Если да, то какая информация следует за заголовком «IF-MODIFIED-SINCE:»?
4. Какой код состояния HTTP и фраза возвращаются сервером в ответ на этот второй запрос HTTP GET? Вернул ли сервер явно содержимое файла?

Задание 3. Получение длинных документов (2 балла)

Подготовка:

1. Запустите веб-браузер и убедитесь, что кэш браузера очищен.
2. Запустите анализатор пакетов Wireshark.
3. Введите следующий URL-адрес в адресную строку браузера:
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html
   В браузере должен отобразиться довольно длинный текст.
4. Остановите захват пакетов Wireshark и введите «http» в окне фильтра.

Вопросы:

1. Сколько сообщений HTTP GET отправил ваш браузер? Какой номер пакета в трассировке содержит сообщение GET?
2. Какой номер пакета в трассировке содержит код состояния и фразу, связанные с ответом на HTTP-запрос GET?
3. Сколько сегментов TCP, содержащих данные, потребовалось для передачи одного HTTP-ответа?
4. Есть ли в передаваемых данных какая-либо информация заголовка HTTP, связанная с сегментацией TCP?

Задание 4. HTML-документы со встроенными объектами (2 балла)

Исследуйте, что происходит, когда ваш браузер загружает файл со встроенными объектами, т. е. файл, который включает в себя другие объекты (в данном примере это файлы м картинками), которые хранятся на другом сервере (серверах).

Подготовка:

1. Запустите веб-браузер и убедитесь, что кэш браузера очищен.
2. Запустите анализатор пакетов Wireshark.
3. Введите следующий URL-адрес в адресную строку браузера:
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html . Ваш браузер должен отобразить HTML-файл с двумя изображениями. На эти два изображения есть ссылки в базовом файле HTML. То есть сами изображения не содержатся в HTML; вместо этого URL-

адреса изображений содержатся в загруженном файле HTML. Ваш браузер должен получить эти изображения с указанных веб-сайтов.

4. Остановите захват пакетов Wireshark и введите «http» в окне фильтра.

Вопросы:

1. Сколько HTTP GET запросов было отправлено вашим браузером? На какие Интернет-адреса были отправлены эти GET-запросы?
2. Можете ли вы сказать, загрузил ли ваш браузер два изображения последовательно или они были загружены с веб-сайтов параллельно? Объясните

Задание 5. HTTP-аутентификация (2 балла)

Запустите веб-сайт, защищенный паролем, и исследуйте последовательность HTTP-сообщений, которыми обмениваются такие сайты.

Подготовка:

1. Убедитесь, что кеш вашего браузера очищен.
2. Запустите анализатор пакетов Wireshark.
3. Введите следующий URL-адрес в адресную строку браузера: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html
4. Введите требуемые имя пользователя и пароль во всплывающем окне (Имя пользователя — «wireshark-students», пароль — «network»).
5. Остановите захват пакетов Wireshark и введите «http» в окне фильтра

Вопросы:

1. Каков ответ сервера (код состояния и фраза) в ответ на начальное HTTP-сообщение GET от вашего браузера?
2. Когда ваш браузер отправляет сообщение HTTP GET во второй раз, какое новое поле включается в сообщение HTTP GET?