|  |  |
| --- | --- |
| Используя «Меню», можно выбрать сетевой интерфейс, «прослушивание» которого будет осуществлять Wireshark (кнопка «Параметры захвата»). Как правило, по умолчанию используется только один из них, и именно с него Wireshark должен «захватывать» проходящие пакеты.  В поле “Фильтр” пользователь может указать булево выражение (в стиле языка С), которое используется для выборочного отображения захваченных пакетов в “Списке захваченных пакетов”. Например, если в “Фильтре” указать строку “(ip.src==192.168.12.1) && (tcp.srcport==3128)” (без кавычек), то в “Списке захваченных пакетов” будут отображаться только те пакеты, которые были отправлены с IP-адреса 192.168.12.1 и при этом в поле “порт источника” протокола TCP содержат число 3128. Если фильтр принимает значение “http”, то будут отображаться только пакеты, переданные с использованием протокола http.  Дальнейшее выполнение лабораторной работы состоит из следующих шагов:  1. Запустить Wireshark (иногда для этого требуются права Администратора). В появившемся окне выбрать интерфейс для которого необходимо осуществлять анализ проходящих через него пакетов. В качестве интерфейса, используемого для захвата трафика, выбрать физический адаптер, через который компьютер подключён к Интернету (обычно этот адаптер называется Local или “Подключение по локальной сети”). Если меню для выбора адаптера не появляется при запуске Wireshark, нужно запустить из “Меню” команду “Capture->Options”. После выбора адаптеру, нужно запустить процесс захвата трафика (кнопка Start).  2. Инициировать процесс передачи трафика по сети (например, в браузере открыть сайт, заданный по варианту, или запустить соответствующую сетевую утилиту – см. ниже);  3. Установить значение “Фильтра”, чтобы из всего множества перехватываемых пакетов Wireshark отобразил только те, которые имеют отношение к выполняемому заданию. Для корректного создания фильтра следует пользоваться всплывающими подсказками Wireshark, которые активизируются при наборе фильтра. В качестве альтернативного способа можно использовать интерактивный конструктор фильтра, нажав на кнопку “Expression” в правой части элемента “Фильтр”.  4. Дождаться появления данных в списке захваченных пакетов и убедиться, что количество пакетов достаточно для выполнения задания.  5. Сохранить захваченный трафик в файл-трассу (pcap). Указанный файл нужно предъявить по первому требованию преподавателя во время защиты, если в этом возникнет необходимость.  6. Описать в отчёте структуру наблюдаемых PDU (т.е. протокольных блоков данных: кадров, пакетов, сегментов) как для запросов, так и ответов. Указать название и назначение всех заголовков всех уровней OSI-модели в пакетах с учётом порядка инкапсуляции (для этого нужно раскрывать соответствующие значки «+» в поле с детальной информацией о выбранном пакете).  7. Написать в отчёте ответы на вопросы задания (для этого может потребоваться самостоятельно изучить назначение соответствующей заданию сетевой утилиты, использованной для создания трафика).  8. Поместить в отчёт скриншоты окна Wireshark, иллюстрирующие ответы из вышеуказанных п.6 и п.7 | Using the "Menu", you can select the network interface, which Wireshark will listen to (the "Capture Settings" button). As a rule, by default, only one of them is used, and it is from it that Wireshark should “capture” passing packets.  In the “Filter” field, the user can specify a Boolean expression (in the C language style), which is used to selectively display the captured packets in the “List of captured packets”. For example, if you specify the line “(ip.src == 192.168.12.1) && (tcp.srcport == 3128)” (without quotes) in the “Filter”, then only packets that were displayed in the “List of captured packets” will be displayed sent from the IP address 192.168.12.1 and at the same time the TCP source field contains the number 3128. If the filter is set to “http”, only packets transmitted using the http protocol will be displayed.  Further laboratory work consists of the following steps:  1. Launch Wireshark (sometimes this requires Administrator rights). In the window that appears, select the interface for which you want to analyze the packets passing through it. As the interface used to capture traffic, select the physical adapter through which the computer is connected to the Internet (usually this adapter is called Local or “Local Area Connection”). If the menu for selecting an adapter does not appear when starting Wireshark, you need to run the “Capture-> Options” command from the “Menu”. After choosing an adapter, you need to start the process of capturing traffic (Start button).  2. Initiate the process of transmitting traffic over the network (for example, in the browser, open the site specified by the option, or start the corresponding network utility - see below);  3. Set the “Filter” value so that of the entire set of intercepted packets, Wireshark displays only those that are related to the task being performed. To correctly create a filter, use Wireshark tooltips that are activated when a filter is set. As an alternative way, you can use the interactive filter constructor by clicking on the “Expression” button on the right side of the “Filter” element.  4. Wait until the data appears in the list of captured packets and make sure that the number of packets is sufficient to complete the task.  5. Save the captured traffic to a trace file (pcap). The specified file must be presented at the first request of the teacher during the defense, if necessary.  6. Describe in the report the structure of the observed PDUs (ie, protocol data units: frames, packets, segments) for both requests and responses. Indicate the name and purpose of all the headers of all levels of the OSI model in packages, taking into account the encapsulation order (for this you need to open the corresponding “+” icons in the field with detailed information about the selected package).  7. Write answers to the questions of the assignment in the report (for this you may need to independently study the purpose of the network utility corresponding to the assignment used to create traffic).   8. Put screenshots of the Wireshark window in the report, illustrating the answers from the above clauses 6 and 7 |
| В качестве адреса сайта в заданиях следует использовать один из следующих URL (следует выбрать один из пунктов в порядке перечисления):  ● Адрес, выбранный по явному указанию преподавателя. Если преподаватель не давал соответствующих указаний, нужно использовать следующие пункты.  ● Адрес сайта с домашней страницей студента. Автор страницы должен легко идентифицироваться с этой страницей по содержимому сайта.  ● Адрес сайта, в название которого лексически входит фамилия студента (например: www.sidorovivan.ru).  ● Адрес сайта, в котором по очереди встречаются инициалы (ФИО) студента в латинской транскрипции (например, для имени Иванов Фёдор Михайлович подойдёт адрес сайта http://ifmo.ru).  Примечание 1. При выполнении анализа HTTP-трафика не принимать во внимание HTTP-запрос и HTTP-ответ для файла favicon.ico. Появление ссылки на данный файл означает, что браузер автоматически запрашивает сервер о наличии значка веб-сайта, который отображается браузером в адресной строке перед адресом страницы (и в некоторых других местах).  Примечание 2. Все используемые в УИР утилиты доступны как в ОС MS Windows, так и Linux, однако в примерах к заданию указывается синтаксис и ключи командной строки для MS Windows. В Linux команды будут иметь несколько иной синтаксис. | As the site address in the tasks, use one of the following URLs (you should select one of the items in the order listed):  ● Address chosen by explicit instruction from the teacher. If the teacher did not give the appropriate instructions, the following points should be used.   ● Website address with student homepage. The author of the page should be easily identified with this page by the content of the site.   ● The address of the site, the name of which includes the student’s last name (for example: www.sidorovivan.ru).  ● The address of the site in which the initials (full name) of the student meet in Latin transcription (for example, the name of the site http://ifmo.ru is suitable for the name Ivan Fyodor Mikhailovich).  Note 1. When performing HTTP traffic analysis, do not take into account the HTTP request and HTTP response for favicon.ico file. The appearance of a link to this file means that the browser automatically asks the server for the presence of the website icon, which is displayed by the browser in the address bar in front of the page address (and in some other places).  Note 2. All utilities used in the OIR are available both in MS Windows and Linux, however, the examples for the task specify the syntax and command line keys for MS Windows. On Linux, commands will have slightly different syntax. |