ПРАКТИЧЕСКАЯ РАБОТА №3

# Мониторинг сетевого трафика на хосте

**Цель работы:** получить практические навыки по работе с анализаторами сетевого трафика. На практике ознакомиться с различиями в принципах работы активного сетевого оборудования. Уяснить особенности взаимодействия сетевого и канального уровней на примере стека TCP/IP. Выяснить отличия форматов кадров Ethernet. Познакомиться с консольными утилитами диагностики и анализа сетевых соединений.

**Необходимо:** Компьютер с установленной средой виртуализации Virtual Box. Виртуальные машины Linux. Административные учетные записи на виртуальных машинах. Сетевое подключение по протоколу IP. Доступ к глобальной сети Интернет. Программный пакет Wireshark.

**Краткие теоретические сведения**

Для перехвата и анализа трафика на отдельном хосте используются программы «Анализаторы трафика», или «снифферы». Эти программы позволяют осуществить перехват всего трафика по выбранному сетевому интерфейсу и его деинкапсуляцию до прикладного уровня. Как правило, они обладают средствами фильтрации и поиска в перехваченном наборе кадров. Наиболее известным кроссплатформенным решением является Wireshark.

Кроме них существуют стандартные консольные утилиты arp, netstat (Windows, Linux), ss, lsof и tcpdump (Linux).

К назначению средств анализа начального уровня относятся анализ текущих соединений на хосте и поиск неисправностей при сетевом взаимодействии.

**Инструментальные средства:**

Утилиты работы с оборудованием: ip, ss, lsof, ping, mtr

Утилиты работы с текстом: echo, grep, sed

Редакторы: vi, nano

**Порядок выполнения работы:**

**Часть 1. Подготовка и проверка сетевой конфигурации**

1. Установите на реальном хосте программу Wireshark (<https://www.wireshark.org>). Если вы используете WiFi при инсталляции npcap включите поддержку IEEE 802.11 .
2. Настройте виртуализацию сети в VirtualBox так, чтобы виртуальная машина оказалась в локальной сети (если это невозможно, то используйте режим NAT).
3. Зайдите в ОС на виртуальной машине с правами root.
4. Определите ip адрес хоста, адрес DNS и имя хоста на виртуальной машине **(!)**.
5. С помощью утилиты ping проверьте доступность внешней сети, послав 5 эхо-запросов на сервер 8.8.8.8 или 1.1.1.1 **(!)**
6. Проверьте наличие утилиты mtr, при ее отсутствии установите ее.

**Часть 2. Работа с Wireshark**

1. Настройте перехват трафика на реальном интерфейсе, так чтобы он завершился после сбора 15 Мб (для увеличения интенсивности генерации кадров открыть любой сайт в браузере).
2. **Используя инструментарий статистики, определите (!):**
   1. Узел с максимальной активностью (по объему переданных данных),
   2. Узел осуществивший наибольшее количество широковещательных рассылок,
   3. Самый активный TCP-порт на хосте (по количеству переданных пакетов)
   4. Постройте на одной координатной сетке постройте графики интенсивности TCP и UDP трафика (пункт Io Graphs).
   5. Постройте диаграму связей только для пакетов, содержащих сообщения протокола HTTPS (пункт Flow Graph)
3. **Напишите фильтры, которые выделяют из общего числа пакеты (!):**
   1. Относящиеся к работе протоколов HTTP и FTP и относящиеся только к взаимодействию локальных клиентов и внешнего сервера. То есть в случае, если на вашем компьютере запущен и Web-броузер и Web-сервер, фильтр должен отбирать только трафик от и к Web-браузеру, игнорируя трафик от и к Web-серверу.
   2. Все кадры Ethernet, отправленные с сетевого интерфейса хоста.
   3. Напишите фильтр, отбирающий только широковещательные сообщения. Определите назначение как минимум 3-х широковещательных рассылок разных протоколов.
   4. Определить адреса, на которые поступают данные кадры и пакеты для канального и сетевого уровня
   5. Напишите фильтры для каждой из трех широковещательных рассылок, выбранных в пункте 3-с.
   6. На основании собранной статистики определить, к какому типу коммутационного оборудования подключен используемый компьютер (концентратор, коммутатор или маршрутизатор).
4. В виртуальной машине с помощью утилиты mtr выведите статистику передачи трафика до хоста ya.ru, отправив 111 запросов и выводя на экран, как имена, так и ip адреса промежуточных устройств **(!)**.
5. С помощью Wireshark определите, с помощью какого протокола осуществляется проверка доступности.

**Часть 3. Консольные утилиты**

1. Подключитесь с реального хоста на виртуальную машину через протокол ssh. Для Программа putty доступна на <http://www.putty.org/>.
2. С Windows с помощью терминального клиента Putty подключитесь к SSH серверу на Linux.
3. Используя утилиту netstat или lsof (для Linux) вывести все активные (прослушиваемые) порты на обоих платформах. Используя утилиту netstat или ss (для Linux) все открытые соединения на обоих платформах. **(!)**.
4. С помощью команды tcpdump на Linux настроить вывод на экран содержимого пакетов от Windows-хоста по протоколу ssh. **(!)**.

**Содержание отчета**

Требуется подготовить отчеты в формате DOC\DOCX или PDF. Отчет содержит титульный лист, артефакты выполнения и ответы на вопросы и задания.

Артефакты:

* 1. Тексты команд и консольный вывод из Части 1, п.4-5.
  2. Скриншоты окон Wireshark с необходимыми данными заданий Части 2, п.2.
  3. Текст фильтров Части 2, п.3.
  4. Тексты команд и консольный вывод из Части 3, п.3-4.

Вопросы и задания:

1. По какому протоколу работает утилита mtr? Как вы это определили?
2. Опишите значения столбцов статистики, выводимой утилитой mtr.
3. Какие типы кадров Ethernet бывают, в чем их отличия?
4. Какой тип кадров Ethernet используется в анализируемой сети? Почему именно он?
5. Как можно определить тип используемого коммутационного оборудования, используя сетевую статистику? Какой тип коммутационного оборудования использовался в сети?
6. На какие адреса сетевого уровня осуществляются широковещательные рассылки?
7. На какой канальный адрес осуществляются широковещательные рассылки?
8. Для чего применяются перехваченные широковещательные рассылки в Части 2 п. 3-e?
9. Как с помощью утилиты ip просмотреть arp-кэш и как его очистить. В каких случаях может понадобиться последняя операция?
10. Напишите команду tcpdump, выводящую все пакеты с хоста 192.168.0.254 и содержащего udp или идущего на tcp порт 80.

Отчет выслать в течение 4-х недель на адрес [edu-net@yandex.ru](mailto:edu-net@yandex.ru).

В теме письма: №группы ФИО (латинскими буквами) №работы (например: 5555 Fedor Sumkin 3)

**Поддержка работы**

Дополнительные материалы по теме курса публикуются на Telegram-канале ITSMDao (t.me/itsmdao). Обсуждать работу и задавать вопросы можно в чате ITSMDaoChat (t.me/itsmdaochat).