Лабораторная работа № 2

Корпоративная сеть

Перед началом выполнения работы запустите браузер (откройте какой-нибудь сайт), установите сетевые соединения по другим протоколам (`smb`, `ssh`, `ftp`, `webdav`, ...).

Задание 1. Сетевые настройки

Используя интерфейс ОС или системные сетевые утилиты (`ipconfig`, `ifconfig`), узнайте и поместите в отчёт сетевые настройки Вашего *хост-компьютера* (с ОС Windows) и *виртуальной машины* (гостевой ОС GNU/Linux):

1. Имя компьютера.
2. Маску сети.
3. IP-адрес, номер сети и номер узла.
4. Какой используется адрес: статический или динамический?
5. MAC-адрес.
6. Какая сетевая карта используется (производитель, чипсет)?
7. Сетевой шлюз.

   В Linux (кроме графических инструментов рабочего стола) можно получить подробные сведения с помощью утилиты `lshw`, например:

   ```
   lshw -class network
   ```

   А вся информация о сетевых соединениях записана в текстовых файлах в папке `/etc/sysconfig/network-scripts`

Задание 2. Работа в сети

Используя системные сетевые утилиты, узнайте и поместите в отчёт следующую информацию:

1. *Среднее время* обмена пакетами с узлом `portal.edu.asu.ru` и `www.securitylab.ru` (`ping`).
2. Маршрут к произвольному доступному удалённому узлу в глобальной сети Интернет (например, `portal.edu.asu.ru`, `www.securitylab.ru`) (`traceroute`).
3. *В ОС Windows* с помощью утилиты `net` посмотрите список сетевых подключений.

   Подключите любой общий сетевой ресурс как диск `Y:`. Снова посмотрите список сетевых подключений и добавьте его в отчёт.
4. С помощью утилиты `netstat` посмотрите:

   4.1. Активные подключения (имя, локальный и внешний адреса, состояние), если имеются (`netstat`).

   4.2. Статистику Ethernet (`netstat -s`).

   4.3. Таблицу маршрутов (`netstat -r`).

   4.4. Вывести список всех открытых TCP-портов (`netstat -at` или `netstat -ant` (`n` — без преобразования имён, так быстрее)). По какому количеству портов Ваша машина слушает сеть? Сколько соединений установлено?

   4.5. Какие процессы связаны с конкретными портами? (`netstat -anp`)

Задание 3. Слушаем сеть

1. С помощью утилиты `netstat` посмотрите информацию о сетевых интерфейсах TCP в реальном времени (`netstat -ic`).

2. С помощью утилиты `lsof` посмотрите все открытые объекты и процессы, открывшие их.

3. С помощью утилиты `lsof` посмотрите все открытые порты и процессы, открывшие их (`lsof -i`).

4. С помощью утилиты `tcpdump` посмотрите:

4.1. Информацию о всех перехваченных сетевых пакетах.

4.2. Информацию о всех перехваченных сетевых пакетах по сетевым интерфейсам, связанным с первым и вторым сетевым адаптером (`tcpdump -i<интерфейс>`).

4.3. Информацию о всех сетевых пакетах определённого узла (например, `proxy.asu.ru`) в сети (`tcpdump -i<интерфейс> -vvvv host <адрес>`). Рассмотрите варианты различной детализации информации (ключ `v`).

4.4. Информацию о всех сетевых пакетах обмена между определёнными двумя (соседними) узлами в сети (`tcpdump -i<интерфейс> -vvvv host <адрес1> and <адрес2>`).

Задание 4. Сканирование чужой сети

Используйте для сканирования утилиту `nmap` (можно в командной строке, можно через графический интерфейс). Изучите работу с `nmap`. Просканируйте сетевые узлы `10.0.12.15`, `10.0.12.224`, `scanme.nmap.org` и `demo.testfire.net`.

По результатам сканирования узнайте:

1. операционную систему хостов;

2. псевдонимы хостов (если есть);

3. IP-адрес хостов;

4. открытые порты хостов;

5. количество закрытых портов;

6. какое ПО используется хостом (использует доступные порты);

7. маршрут к хосту;

8. состояние хостов (включен или выключен).

Можно для отчёта сделать скриншоты.

Сохраните отчёт в файл и выложите его на Moodle.