

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО ИНСТИТУТ
КОМПЬЮТЕРНЫХ НАУК И КИБЕРБЕЗОПАСНОСТИ

ВЫСШАЯ ШКОЛА КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННЫХ СИСТЕМ

Отчёт по лабораторной работе №2

Курс: «Администрирование компьютерных сетей»

Тема: «Тестирование компьютерной сети на основе TCP/IP»

Выполнил студент:

Алешковский Александр Анатольевич

Росинский Александр Ильич

Группа: 5140901/31502

Проверил:

Малышев Игорь Алексеевич

Содержание

1	Лабораторная работа №2	2
1.1	Цели работы	2
1.2	Сведения о системе	2
1.3	Оценка пропускной способности	2
1.3.1	Установка	2
1.3.2	Тестирование	3
1.4	Карта сети	3
1.5	Поиск уязвимостей	3

Лабораторная работа №2

1.1 Цели работы

1. Изучение утилит и систем администрирования TCP/IP-сетей.
2. Мониторинг и анализ характеристик TCP/IP-сетей.

1.2 Сведения о системе

Работа производилась на реальной системе, со следующими характеристиками:

Элемент	Значение
Имя ОС	Майкрософт Windows 10 Pro (Registered Trademark)
Версия	10.0.16299 Сборка 16299
RAM	16 ГБ
Процессор	Intel(R) Core(TM) i5-7300HQ CPU @ 2.50GHz, 2496 МГц

Для выполнения работы использовалась **VMware Workstation**. В качестве сети для экспериментов, использовалась ККС из прошлой работы.

1.3 Оценка пропускной способности

В качестве утилиты для оценки пропускной способности была выбрана **iperf**. Iperf — кроссплатформенная консольная клиент-серверная программа, предназначена для тестирования пропускной способности интернет канала между двумя компьютерами.

Измерение осуществляется следующим образом, на одном ПК запускаем iperf в режиме «сервер», на втором в режиме «клиент» с указанием ip-адреса первого ПК («сервера»). Через заданное время показывается измеренная информация.

В работе использовалась **версия 2.0.5**

1.3.1 Установка

На **NetBsd**, были выполнены команды:

1. Загрузка iperf

- (a) Подключение к ftp серверу, к папке с пакетами для моей версии NetBSD

```
1 ftp -i ftp://ftp.netbsd.org/pub/pkgsrc/packages/NetBSD/x86_64/7.1.1/All/
```

- (b) Загрузка последней версии

```
1 mget iperf-2.0.5nb1.tgz
```

- (c) Завершение работы ftp

```
1 quit
```

2. Создаем папку и разархивируем туда архив

```
1 mkdir iperf
2 tar -xzf iperf-2.0.5nb1.tgz -C /root/iperf
```

3. Утилита для запуска находится по пути **/root/iperf/bin**

На **FreeBSD**, были выполнены команды:

```
1 cd /usr/ports/benchmarks/iperf
2 make install clean
```

На **Kali Linux**, была выполнена команда:

```
1 apt-get install iperf
```

На **Windows XP** были скачены бинарные файлы программы.

1.3.2 Тестирование

На хосте с FreeBSD запущен сервер iperf

```
1 iperf -s
```

На машинах(Kali Linux, NetBSD, Windows XP) iperf запущен в качестве клиента, командой:

```
1 iperf -c 192.168.40.2
```

В результате были получены следующие данные:

NetBSD	Kali Linux	Windows XP
1.47 Гбит/с	1.62 Гбит/с	5.81 Мбит/с

1.4 Карта сети

Для изучения сети использована программа **10-Страйк: Схема Сети**(версия 3.32), установленная на Windows XP.

При запуске программы, были указаны следующие диапазоны для сканирования:

- 192.168.32.1-192.168.32.254;
- 192.168.40.1-192.168.40.254;
- 192.168.80.1-192.168-80.254;
- 192.168.120.1-192.168.120.254.

В качестве параметров тестирования выбрать ICMP-ping.

После чего начнется сканирование данных диапазонов адресов. Программа построила следующую карту сети: Программа не смогла определить точную карту сети, типы операционных систем, она видит лишь

Рис. 1.1: Карта сети

ближайший маршрутизатор, в данном случае – это FreeBSD (хост 192.168.80.2).

1.5 Поиск уязвимостей

В качестве программы по поиску уязвимостей была выбрана **X-Spider**(версия 7.7), которая была установлена на Windows XP.

Перед сканированием были добавлены следующие адреса интерфейсов:

- 192.168.80.128(Windwos XP);
- 192.168.40.2(FreeBSD);
- 192.168.80.2(FreeBSD);
- 192.168.120.2(FreeBSD);
- 192.168.120.15(Windows 98);

- 192.168.40.32(Kali Linux);
- 192.168.40.57(NetBSD);
- 192.168.32.128(NetBSD).

По итогам работы, были выявлены следующие уязвимости:

- Windows XP
 - имя операционной системе;
 - сервисом NTP открыт порт 123 по UDP;
 - сервисом RPC Windows открыт порт 135 по TCP;
 - сервисом NBNS открыт порт 137 по UDP;
 - сервисом NetBIOS открыт порт 139 по TCP.
- Windows 98
 - имя операционной системе;
 - сервисом NetBIOS-SSN открыт порт 137 по UDP;
 - сервисом NetBIOS открыт порт 139 по TCP.

В системах unix слабых мест не обнаружено.

Вывод

В ходе данной лабораторной работы была протестирована сеть на основе TCP/IP.

Оценка пропускной способности показала очень высокую скорость для операционных систем семейства Unix и довольно медленную для Windows XP. Это может быть связано с кроссплатформенностью используемой утилиты для тестирования и различными настройками операционных систем.

Утилита для построения карты сети показала некорректную карту, что указывает на сложность создания точной карты сети.

Тестирование на уязвимости выявило, что операционные системы семейства Windows подвержены уязвимостям, тогда как на Unix-системах уязвимостей обнаружено не было.

Для предотвращения подобных уязвимостей необходимо использовать актуальные версии операционных систем (с последними обновлениями). Также рекомендуется наличие специализированного ПО для защиты системы.