Санкт-Петербургский политехнический университет Петра Великого

Институт компьютерных наук и технологий

Высшая школа интеллектуальных систем и суперкомпьютерных технологий

**Лабораторной работе №2**

**Тестирование компьютерной сети на основе TCP/IP**

**Дисциплина:** Администрирование компьютерных сетей

Выполнил студент гр. 3540901/02001 Бараев Д.Р.

(подпись)

Руководитель Малышев И.А.

(подпись)

“\_\_\_” \_\_\_\_\_\_\_\_ 2021 г.

Санкт – Петербург

2021

**Содержание**

[1. Цели работы 3](#_Toc71289771)

[2. Программа работы 3](#_Toc71289772)

[3. Паспорт сети 3](#_Toc71289773)

[3.1 Схема сети 3](#_Toc71289774)

[3.2 Описание хостов 4](#_Toc71289775)

[4. Тестирование утилит на Ubuntu 4](#_Toc71289776)

[4.1. Ifconfig 5](#_Toc71289777)

[4.2. Arp 5](#_Toc71289778)

[4.3. Hostname 5](#_Toc71289779)

[4.4. Netstat -r 5](#_Toc71289780)

[4.6. Tracert 7](#_Toc71289781)

[5. Проверка пропускной способности сети 7](#_Toc71289782)

[6. Сканирование уязвимостей сети 8](#_Toc71289783)

[7. Карта сети 8](#_Toc71289784)

[Вывод 9](#_Toc71289785)

# Цели работы

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

# Программа работы

1. Составить паспорт сети, объединяющий карту сети (физическая и логическая топология с указанием числовых и символических имён хостов, номенклатур аппаратных и программных платформ хостов и сетевых компонентов), характеристики направления и интенсивности (для совокупного по всем типам пакетов и раздельного по каждому типу пакетов) сетевого трафика.
2. Представить и прокомментировать все конфигурационные файлы, определяющие состояние как отдельных хостов сети, так и подсетей/сетей.
3. Оценить производительность/загрузку сети в целом и её отдельных компонентов.
4. Оценить уязвимость системных (хосты) и сетевых (службы) ресурсов сети относительно внешних атак.

# Паспорт сети

# Схема сети

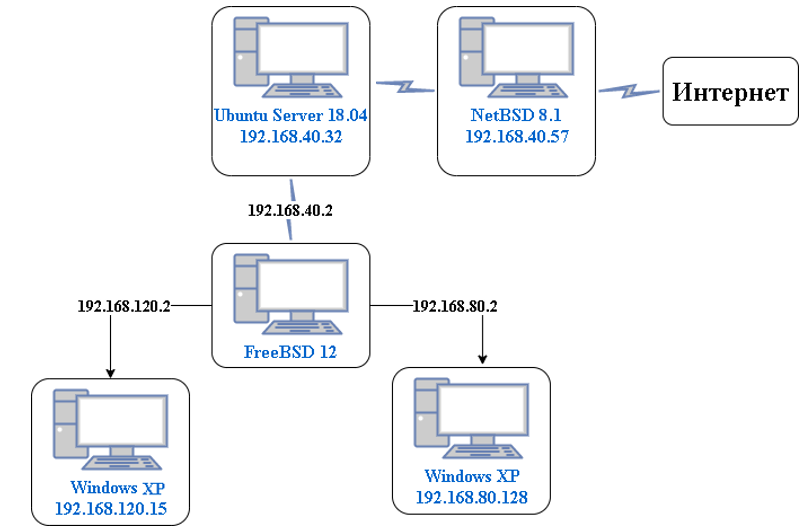
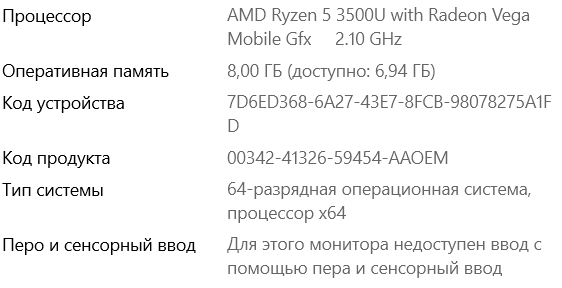
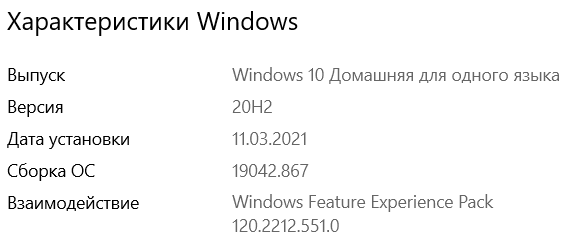


Рисунок 1 - Схема сети

# Описание хостов

Реальная система, используемая в проекте:





Для выполнения работы использовалась VMware Workstation.

С помощью средств VMware Workstation были созданы виртуальные машины, с использованием ниже представленных операционных систем, с соответствующим выделением оперативной памяти.

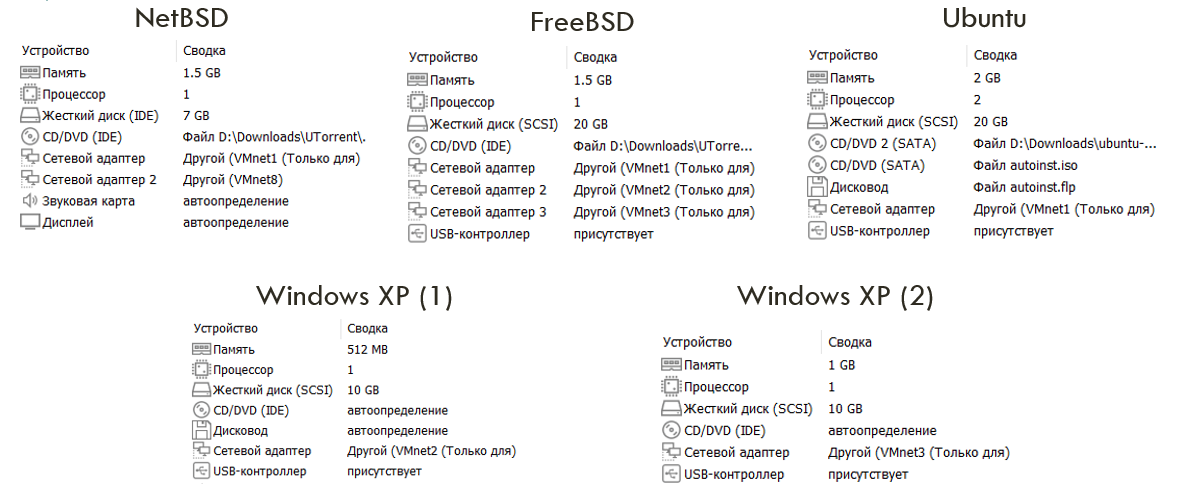


Рисунок 2 - Используемые ОС и их характеристики

# Тестирование утилит на Ubuntu

# Ifconfig

Выводит активные сетевые интерфейсы и их параметры.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3 - Результаты работы команды ifconfig

# Arp

Таблица Arp показывает соответствие между IP и MAC адресами.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 4 - Результат работы утилиты arp

# Hostname

Выводит имя хоста.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 5 - Утилита hostname

# Netstat -r

Просмотр таблицы маршрутизации.

Изображение выглядит как текст, табличка

Автоматически созданное описание

Рисунок 6 - Утилита netstat -r

1. **Netstat -i**

Просмотр статистики передачи пакетов по интерфейсам.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 7 - Утилита netstat -i

# Tracert

Определение пути пакетов.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 8 - Утилита tracert

# Проверка пропускной способности сети

Командой ***apt install iperf*** на хост Ubuntu была установлена утилита ***iperf***, которая генерирует трафик и тем самым позволяет тестировать пропускную способность сетей. Затем она была запущена как сервер.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 9 - Запуск утилиты iperf, как сервера

Также утилита была установлена на Windows XP. Там она была запущена как клиент слушающий сервер по адресу 192.168.40.32.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 10 - Запуск утилиты iperf, как клиента

# Сканирование уязвимостей сети

Поиск уязвимостей в сети осуществлялся через пробную версию утилиты

XSpider. Результаты поиска показали, что все обнаруженные уязвимости

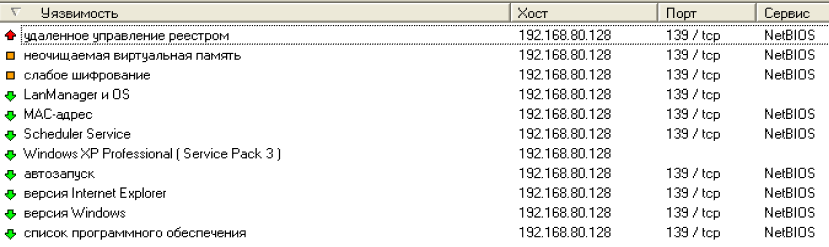
связаны с хостом Windows XP.

Рисунок 11 - Результат сканирования уязвимостей сети

# Карта сети

Карта сети строилась в пробной версии программы 10-Страйк: Схема Сети.

Схема не совсем соответствует действительности, однако утилита смогла обнаружить хосты компьютерной сети и связать их.

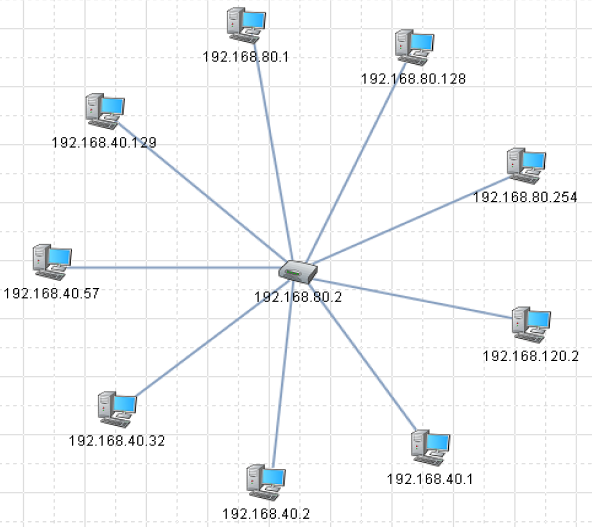


Рисунок 12 - Построенная схема сети

# Вывод

В ходе выполнения лабораторной работы были рассмотрены такие утилиты администрирования ККС как ifconfig, route, arp, hostname, ping и netstat. Они просты в использовании, и очень полезны для администратора.

Также было проведено знакомство с программами для мониторинга и анализа характеристик TCP/IP-сетей. Были обнаружены уязвимости, связанные с хостом на Windows XP, а также была построена карта с хостами сети. Утилитой iperf была протестирована пропускная способность сети.