МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)

Факультет Среднего профессионального образования

Дисциплина Операционные системы и среды
наименование дисциплины

ЛАБОРАТОРНАЯ РАБОТА №4
номер (при наличии)

Диагностика сетевых технологий
при наличии указать тему лабораторной работы и (или) номер варианта

ОБУЧАЮЩИЙСЯ

группы 09С51

_____ Куманов Д.В
подпись фамилия и инициалы

_____
дата сдачи

ПРОВЕРИЛ

_____ Шарипова Э.Р.
подпись фамилия и инициалы

Оценка / балльная оценка _____

_____
дата проверки

г. Санкт-Петербург
2025 г.

Задание 1.

Пользователь сообщает, что не открывается поисковая система Yandex.ru, при этом другие сайты работают нормально.

1. **Проверка базовой связности:**

– С помощью ipconfig определите IP-адрес вашего компьютера, шлюза по умолчанию.

Команды: ipconfig

Показывает текущие сетевые настройки компьютера. На рисунке 1 представлен IP-адрес и результат команды ipconfig.

```
даптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::cc0f:4b8d:61c8:738b%18
   IPv4-адрес. . . . . . . . . . . . : 172.20.10.5
   Маска подсети . . . . . . . . . . : 255.255.255.240
   Основной шлюз. . . . . . . . . . : 172.20.10.1

уннельный адаптер Teredo Tunneling Pseudo-Interface:

   DNS-суффикс подключения . . . . . :
   IPv6-адрес. . . . . . . . . . . . : 2001:0:14c9:d804:2c39:345d:53eb:f5fa
   Локальный IPv6-адрес канала . . . : fe80::2c39:345d:53eb:f5fa%13
   Основной шлюз. . . . . . . . . . :
```

Рисунок 1 – Результат команды ipconfig

2. **Проверка DNS-разрешения:**

— Используя nslookup, узнайте IP-адрес домена yandex.ru.

IP-адрес Yandex.ru представлен на рисунке 2.

```
╤xËтxË:  UnKnown
Address:  fe80::7cec:b1ff:fe51:9564

Не заслуживающий доверия ответ:
╚ь :     YANDEX.ru
Addresses:  2a02:6b8:a::a
          77.88.55.88
          77.88.44.55
          5.255.255.77
```

Рисунок 3 – IP-адрес yandex.ru

— Удалось ли получить IP-адрес? Что это может означать?

Получить IP-адрес получилось из-за того, что DNS-серверы разрешают доменное имя в IP-адрес, что позволяет устройству найти сервер, на котором расположен yandex.ru.

3. **Проверка доступности сайта:**

— Попробуйте пропинговать полученный IP-адрес сайта yandex.ru.

Команды: ping

Используя команду ping можно скорость подключение к yandex.ru. На рисунке 3 представлен результат команды ping.

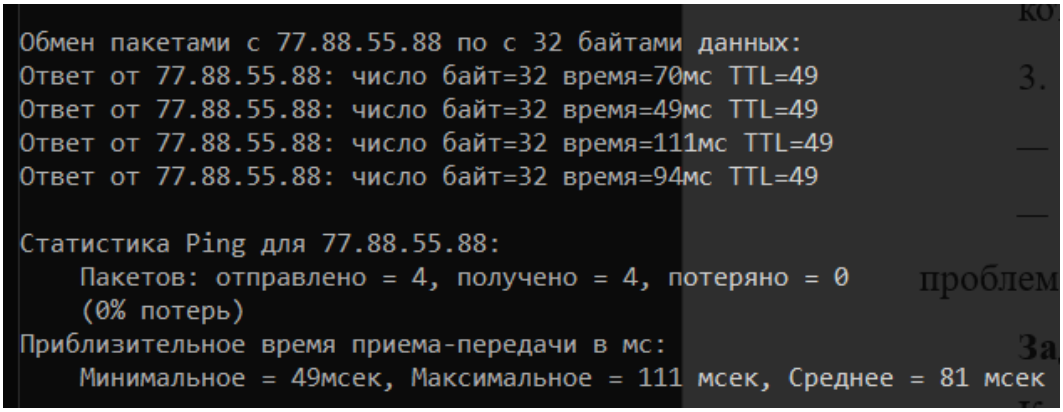


Рисунок 3 – Результат команды ping

— На основе результатов (доступен ли IP) сформулируйте гипотезу: проблема скорее всего в DNS или в блокировке на сетевом уровне?

Смотря на результат рисунка 3, IP-адрес (77.88.55.88) доступен, происходит обмен пакетами без потерь.

Задание 2.

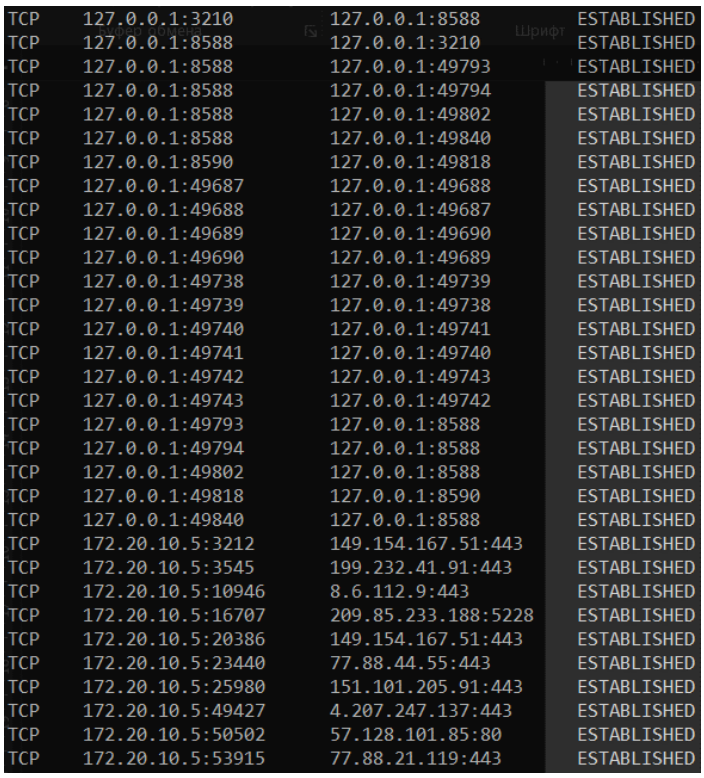
К вам поступила информация о возможной нежелательной активности на компьютере.

1. **Анализ установленных соединений:**

– Запустите команду netstat -abn | findstr ESTABLISHED.

Команды: netstat -abn | findstr ESTABLISHED

Выводит список всех TCP-соединений в состоянии ESTABLISHED. На рисунке 4 представлен результат команды netstat.



TCP	127.0.0.1:3210	127.0.0.1:8588	ESTABLISHED
TCP	127.0.0.1:8588	127.0.0.1:3210	ESTABLISHED
TCP	127.0.0.1:8588	127.0.0.1:49793	ESTABLISHED
TCP	127.0.0.1:8588	127.0.0.1:49794	ESTABLISHED
TCP	127.0.0.1:8588	127.0.0.1:49802	ESTABLISHED
TCP	127.0.0.1:8588	127.0.0.1:49840	ESTABLISHED
TCP	127.0.0.1:8590	127.0.0.1:49818	ESTABLISHED
TCP	127.0.0.1:49687	127.0.0.1:49688	ESTABLISHED
TCP	127.0.0.1:49688	127.0.0.1:49687	ESTABLISHED
TCP	127.0.0.1:49689	127.0.0.1:49690	ESTABLISHED
TCP	127.0.0.1:49690	127.0.0.1:49689	ESTABLISHED
TCP	127.0.0.1:49738	127.0.0.1:49739	ESTABLISHED
TCP	127.0.0.1:49739	127.0.0.1:49738	ESTABLISHED
TCP	127.0.0.1:49740	127.0.0.1:49741	ESTABLISHED
TCP	127.0.0.1:49741	127.0.0.1:49740	ESTABLISHED
TCP	127.0.0.1:49742	127.0.0.1:49743	ESTABLISHED
TCP	127.0.0.1:49743	127.0.0.1:49742	ESTABLISHED
TCP	127.0.0.1:49793	127.0.0.1:8588	ESTABLISHED
TCP	127.0.0.1:49794	127.0.0.1:8588	ESTABLISHED
TCP	127.0.0.1:49802	127.0.0.1:8588	ESTABLISHED
TCP	127.0.0.1:49818	127.0.0.1:8590	ESTABLISHED
TCP	127.0.0.1:49840	127.0.0.1:8588	ESTABLISHED
TCP	172.20.10.5:3212	149.154.167.51:443	ESTABLISHED
TCP	172.20.10.5:3545	199.232.41.91:443	ESTABLISHED
TCP	172.20.10.5:10946	8.6.112.9:443	ESTABLISHED
TCP	172.20.10.5:16707	209.85.233.188:5228	ESTABLISHED
TCP	172.20.10.5:20386	149.154.167.51:443	ESTABLISHED
TCP	172.20.10.5:23440	77.88.44.55:443	ESTABLISHED
TCP	172.20.10.5:25980	151.101.205.91:443	ESTABLISHED
TCP	172.20.10.5:49427	4.207.247.137:443	ESTABLISHED
TCP	172.20.10.5:50502	57.128.101.85:80	ESTABLISHED
TCP	172.20.10.5:53915	77.88.21.119:443	ESTABLISHED

Рисунок 4 – Результат команды netstat

– Внимательно просмотрите список. Попробуйте определить, к каким известным вам адресам и портам (например, 443 — HTTPS, 5222 — мессенджеры) установлены соединения. Есть ли в списке незнакомые IP-адреса или нетипичные порты?

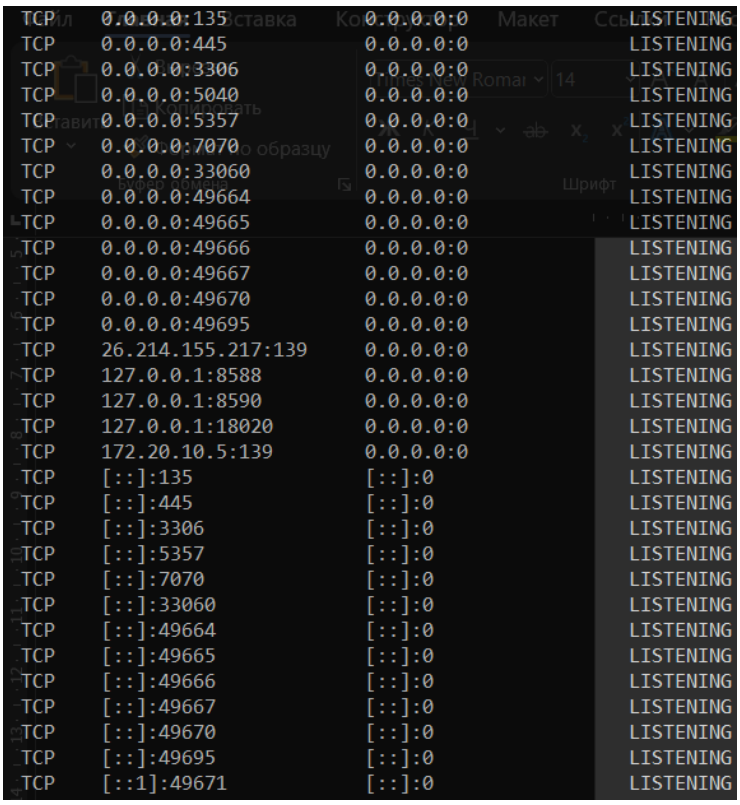
На рисунке 4 можно видеть IP-адреса типа 172.20.10.5 которые относятся к внутренней/локальной сети.

2. **Просмотр ожидающих портов:**

– Запустите команду netstat -an | findstr LISTENING.

Команды: netstat -an | findstr LISTENING

Выводит список всех портов на компьютере, которые в данный момент ожидают входящих подключений. На рисунке 5 представлен результат команды netstat.



TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7070	0.0.0.0:0	LISTENING
TCP	0.0.0.0:33060	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49695	0.0.0.0:0	LISTENING
TCP	26.214.155.217:139	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8588	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8590	0.0.0.0:0	LISTENING
TCP	127.0.0.1:18020	0.0.0.0:0	LISTENING
TCP	172.20.10.5:139	0.0.0.0:0	LISTENING
TCP	[::]:135	[::]:0	LISTENING
TCP	[::]:445	[::]:0	LISTENING
TCP	[::]:3306	[::]:0	LISTENING
TCP	[::]:5357	[::]:0	LISTENING
TCP	[::]:7070	[::]:0	LISTENING
TCP	[::]:33060	[::]:0	LISTENING
TCP	[::]:49664	[::]:0	LISTENING
TCP	[::]:49665	[::]:0	LISTENING
TCP	[::]:49666	[::]:0	LISTENING
TCP	[::]:49667	[::]:0	LISTENING
TCP	[::]:49670	[::]:0	LISTENING
TCP	[::]:49695	[::]:0	LISTENING
TCP	[::1]:49671	[::]:0	LISTENING

Рисунок 5 – Результат команды netstat

– Изучите, какие порты на вашем компьютере открыты и ожидают подключений. Какие из них являются стандартными для системных служб Windows?

135 (TCP) — Microsoft RPC службы удалённого вызова процедур, который так же важен для работы сетевых функций

139 (TCP) — NetBIOS Session Service используется для передачи файлов/папок и совместного доступа

445 (TCP) — Microsoft-DS, используемый для доступа к файлам и печати.

5040, 5357, 49664–49671 (TCP) — динамически выделяемые порты для внутренних служб.

3306 (TCP) — стандартный порт MySQL

7070 (TCP) — не является стандартным системным портом, чаще используется для потокового вещания.