МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 24

КОНТРОЛЬНАЯ РАБОТА ЗАЩИЩЕН С ОЦЕНКОЙ ПРЕПОДАВАТЕЛЬ

Доцент, канд. Техн. наук А.З. Яфаров

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

**ЛАБОРАТОРНАЯ РАБОТА № 2**

**«Технологии анализа трафика компьютерной сети»**

по курсу: **Информационные технологии**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № 2213 |  | 29.02.2024 |  | Калинин А. А. . |
| номер группы |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2024

**Цель работы:** закрепление знаний по анализу и оптимизации трафика компьютерной сети.  
**Основные навыки:** определение процесса и программы по номеру идентификатора процесса; определение программ, которые занимают каналы передачи данных (открытые порты); проведение анализа трафика по протоколам и программам, выявление доли широковещательного трафика.

**Общая информация о компьютере:**

Имя компьютера: DESKTOP-2H26PMC

MAC адрес:74-56-3C-66-F1-9E

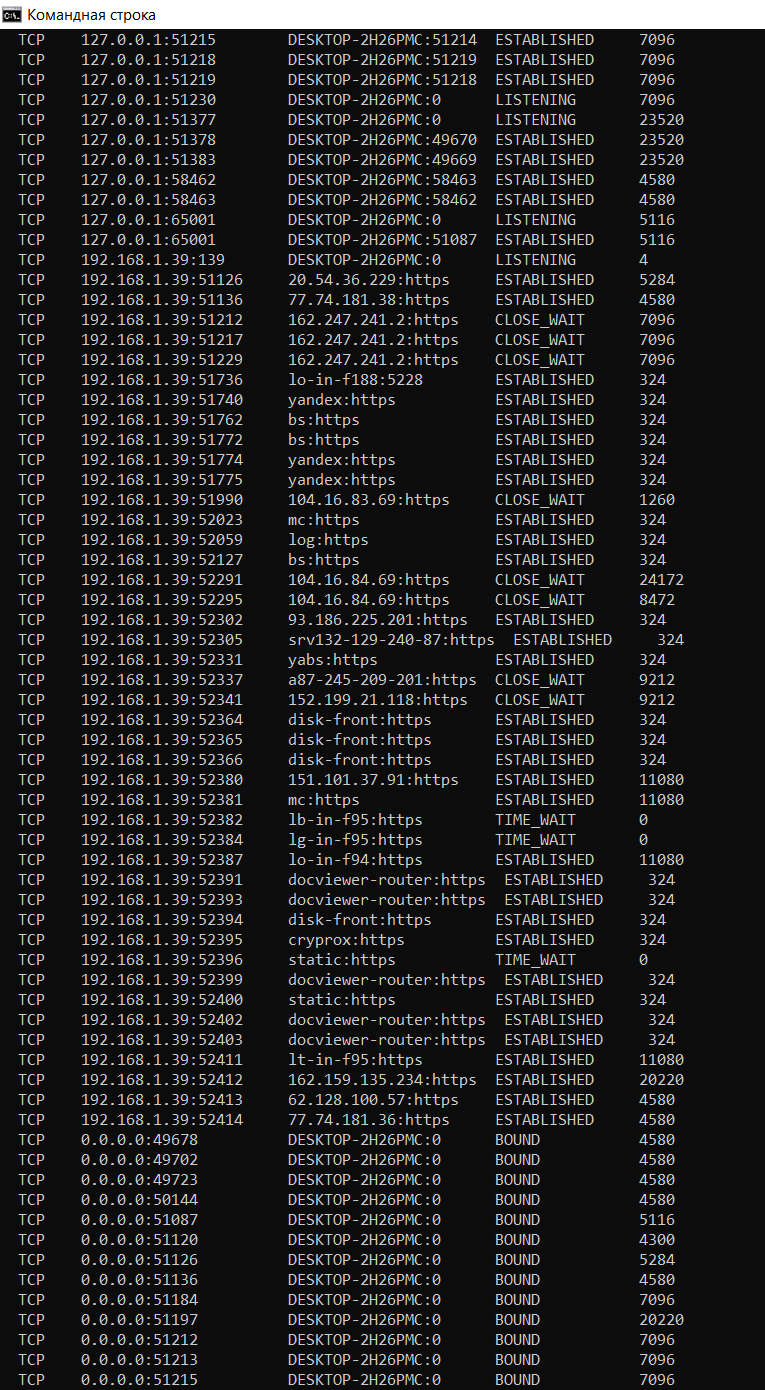
IPv4-адрес: 192.168.1.39(Основной)

**«Часть 1 Анализ состояния компьютера»**

**Анализ 1.**

Блок 1.1 необходимость определить список активных портов.

Список состояния портов



Используя утилиту netstat -qo, я получил список активных портов. Большинство из них установило соединение TCP для передачи данных. Лишь некоторые порты(0.0.0.0) был определен под UPD.

Состояние порта Listening – означает, что приложение, контролирующее этот

порт, находится в состоянии ожидания получения какого-либо пакета.

Состояние порта Estblished – означает, что приложение, контролирующее

этот порт, находится в состоянии активной передачи данных.

Для каждого такого соединения известен уникальный PID процесса. По

этому номеру можно найти имя процесса.

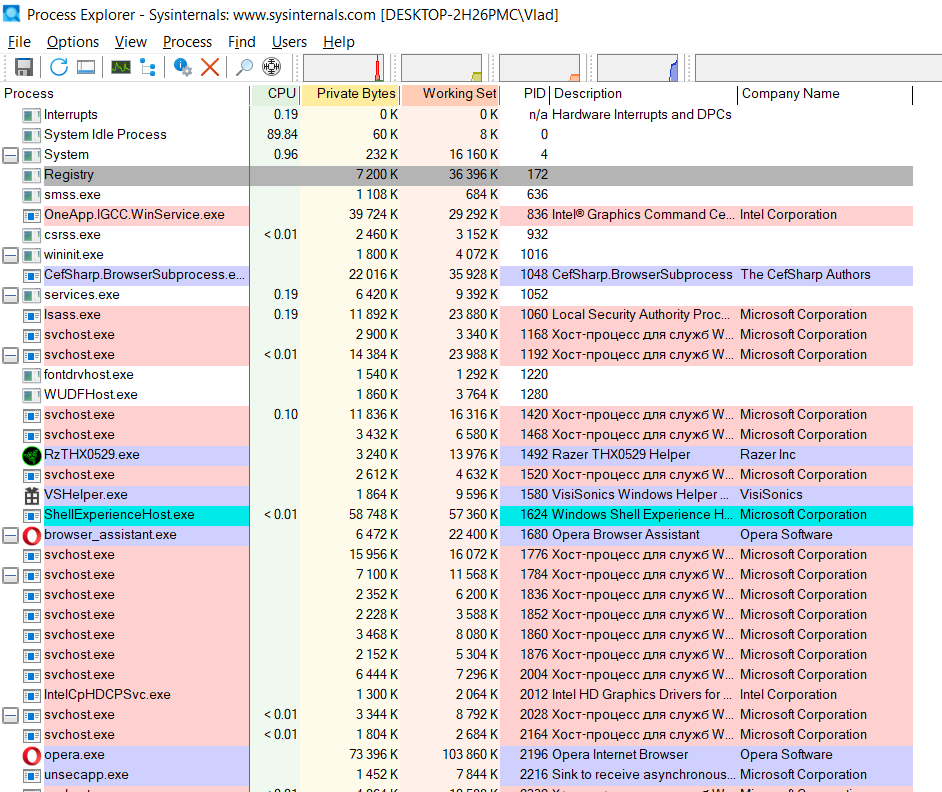
Состояние порта Bound — это переходное состояние перед состоянием listening.

Состояние порта Time\_wait — означает, что приложение или процесс находятся

в очереди.

Состояние порта Close\_wait — это состояние, когда одна сторона узла TCP

больше не имеет данных для отправки, но может получать данные с другого конца.



Отображение процессов и программ компьютера в Process explorer

**Отчёт «Анализ 2».**

Блок 1.2. Список программ

Были составлены таблицы с соотношением портов и программ.

По PID отображенном в Process Explorer мы находили порт, определенный под данную программу и заносили информацию в таблицу.

Практически все программы использовали порты с протоколом TCP, но некоторые неизвестные мне программы(вероятно системные) распределены в порты с протоколом UPD.

Таблица 1.1.Системные программы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование | PID | Порт | Состояние порта | Протокол |
| System | 4 | 0.0.0.0:445 | LISTENING | TCP |
| Svchost.exe | 1400 | 0.0.0.0:135 | LISTENING | TCP |
| VSSr.exe | 5268 | 127.0.0.1:49669 | LISTENING | TCP |
| Svchost.exe | 4928 | 0.0.0.0:500 | - | UDP |
| Service.exe | 1040 | [::]:49676 | LISTENING | TCP |
| Svchost.exe | 7616 | 0.0.0.0:5040 | LISTENING | TCP |
| System Idle Process | 0 | 192.168.1.39:52396 | TIME\_WAIT | TCP |

Таблица 1.2.Известные программы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование | PID | Порт | Состояние порта | Протокол |
| Discord | 7518 | 127.0.0.1:6463 | LISTENING | TCP |
| NVIDIA Web Helper.exe | 10488 | 127.0.0.1:51149 | LISTENING | TCP |
| Wps.exe | 8472 | 0.0.0.0:52295 | BOUND | TCP |
| Opera.exe | 324 | 192.168.1.39:52302 | ESTABLISHED | TCP |
| Avp.exe | 4580 | 192.168.1.39:51136 | ESTABLISHED | TCP |
| RiotClientService.exe | 7096 | 127.0.0.1:51184 | ESTABLISHED | TCP |
| RzTHX0529.exe | 23520 | 127.0.0.1:51377 | ESTABLISHED | TCP |

Таблица 1.3.Неизвестные программы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование | PID | Порт | Состояние порта | Протокол |
| Search.App | 9212 | 192.168.1.39:52337 | CLOSE\_WAIT | TCP |
| winnit | 960 | 0.0.0.0:49665 | LISTENING | TCP |
| Das.Host | 5404 | [::]:4500 | - | UPD |
| fontdrvhost.exe | 3232 | 0.0.0.0:49312 | ESTABLISHED | TCP |
| WUDFHost | 1288 | 0.0.0.0:49668 | LISTENING | TCP |
| Dmw.exe | 3312 | 0.0.0.0:51197 | ESTABLISHED | TCP |
| WmiPrv SE.exe | 4576 | 0.0.0.0:52395 | ESTABLISHED | TCP |

**«Часть 2. Анализ трафика локальной сети»**

Блок 2.1. Формирование тестового набора пакетов

Было произведено три захвата пакетов: в режиме «Idle» (компьютер работает без каких либо программ), в режиме «Копирование большого файла», и в режиме «Доступ в интернет к веб сайту». Все три файла сохраняются для дальнейшей работы и формировании статистики пакетов.

Таблица 2.1. Режим «Idle»

|  |  |
| --- | --- |
| Параметр | Значение |
| Время захвата трафика, мин | 11,5 минут |
| Количество захваченных пакетов | 782 |
| Объем, Мб | 0,019 |
| Средн.размер пакета, КБ | 0,025 |
| Средняя скорость, для пакетов / сек | 1,1 |
| Средняя скорость, Мбит / сек | 0,001874 |

Таблица 2.2. Режим «Копирования большого файла»

|  |  |
| --- | --- |
| Параметр | Значение |
| Время захвата трафика, мин | 3,1 минут |
| Количество захваченных пакетов | 227 |
| Объем, Мб | 0,155 |
| Средн.размер пакета, КБ | 0,026 |
| Средняя скорость, для пакетов / сек | 1,2 |
| Средняя скорость, Мбит / сек | 0,002079 |

Таблица 2.3. Режим «доступ к Web-сайту»

|  |  |
| --- | --- |
| Параметр | Значение |
| Время захвата трафика, мин | 2,16 |
| Количество захваченных пакетов | 19999 |
| Объем, Мб | 1,93 |
| Средн.размер пакета, КБ | 0,0988 |
| Средняя скорость, для пакетов / сек | 149 |
| Средняя скорость, Мбит / сек | 0,965 |

**Анализ 3.**

Составили таблицу распределения трафика по протоколам, которые использовались пи выполнении захвата. Наиболее частые протоколы TCP и SSDP. Появились ранее неизвестные протоколы LLMNR (позволяет компьютерам выполнять разрешение имен хостов в локальной сети.) ,LLDP (протокол [канального уровня](https://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%83%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C" \o "Канальный уровень), позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения.) и SSL-certificate — это криптографический протокол, который отвечает за безопасную передачу данных на сеансовом уровне.

Таблица 2.4. Режим IDLE

|  |  |  |
| --- | --- | --- |
| Протокол | Трафик, бит | Трафик, % |
| UDP | 16512 | 10,13 |
| ARP | 11460 | 7,03 |
| Browser | 6561 | 4,027 |
| DHCP | 700 | 0,43 |
| DNS | 1880 | 1,15 |
| HTTP | 498 | 0,3 |
| ICMPv6/ICMPv2 | 4292 | 2,63 |
| LLMNR | 170 | 0,1 |
| MDNS | 14897 | 9,14 |
| SSDP | 72855 | 44,7 |
| SSL | 2572 | 1,578 |
| TCP | 18105 | 11,1 |
| TLSv1.2 | 12303 | 7,55 |
| HIP | 102 | 0,062 |
| LLDP | 58 | 0,035 |
| Итого | 162965 | 100 |

Фрагмент таблицы 2.4 для режима копирования файла

|  |  |  |
| --- | --- | --- |
| Протокол | Трафик, бит | Трафик, % |
| ARP | 852 | 1,74 |
| BROWSER | 1458 | 2,48 |
| IGMPv6 | 540 | 1,1 |
| IGMPv2 | 834 | 1,7 |
| MDNS | ... | |
| SSDP |
| SSL |
| TCP |
| TLSv1.2 |
| UDP | 48947 | 100 |

Фрагмент таблицы 2.4 для режима доступа к Web сайту

|  |  |  |
| --- | --- | --- |
| Протокол | Трафик, бит | Трафик, % |
| TCP | 11367350 | 70,16 |
| BROWSER | ... | |
| IGMPv6 |
| IGMPv2 |
| MDNS |
| SSDP |
| SSL |
| ARP |
| TLSv1.2 |
| UDP | 16201463 | 100 |

Также была составлена таблица распределения Ethernet-трафика по узлам сети(Табл. 2.5)

Таблица 2.5 для режима доступа к Web сайту

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| MAC-адресы | IP-адресы | Трафик | | | | | |
| Входной | | Выходной | | общий | |
| Кб | % | Кб | % | Кб | % |
| 01:00:5e:00:00:fc | 224.0.0.252 | 0,09 | 4 | 0 | 0 | 0,09 | 0,34 |
| 01:00:5e:00:00:01 | 224.0.0.1 | 0,117 | 5,3 | 0 | 0 | 0,117 | 0,45 |
| ff:ff:ff:ff:ff:ff | 192.168.1.255 | 1 | 45,3 | 0 | 0 | 1 | 3,81 |
| 48:e7:da:c7:07:2d | 64.233.164.94 | 0 | 0 | 9 | 37,5 | 9 | 34,34 |
| 1e4:18:6b:7b:db:ac | 192.168.1.39 | 1 | 45,3 | 15 | 62,5 | 16 | 61,05 |
|  |  | 2,207 | 100 | 24 | 100 | 26,207 | 100 |

Фрагмент таблицы 2.5 для режима Idle

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| MAC-адресы | IP-адресы | Трафик | | | | | |
| Входной | | Выходной | | общий | |
| Кб | % | Кб | % | Кб | % |
| 01:00:5e:00:00:02 | 87.245.209.201 | 0,44 |  | 0 |  | 0,44 |  |
| ... | | | | | | | |
|  |  |  | 100 |  | 100 |  | 100 |

Фрагмент таблицы 2.5 для режима копирования файла

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| MAC-адресы | IP-адресы | Трафик | | | | | |
| Входной | | Выходной | | общий | |
| Кб | % | Кб | % | Кб | % |
| 01:00:5e:00:00:fc | 224.0.0.252 | 0,13 |  | 0 |  | 0,13 |  |
| ... | | | | | | | |
|  |  |  | 100 |  | 100 |  | 100 |

Сформировали распределение пакетов по программам в выборке. % от

трафика (статистика).

|  |  |  |
| --- | --- | --- |
| Search.App | Кб | % |
| winnit | 1,76 | 0,94 |
| Das.Host | 4,86 | 2,6 |
| fontdrvhost.exe | 10,08 | 5,4 |
| WUDFHost | 1,82 | 0,97 |
| Dmw.exe | 164,4 | 87,75 |
| WmiPrv SE.exe | 4,43 | 2,36 |
|  | 187,35 | 100 |

Пункт 2.4.5 Определение эффективной пропускной способности выполнен не был из-за отсутствия возможности передачи файла.

Блок 2.3. Анализ трафика Broadcast и специальных протоколов

**Анализ 4-5.**

Пакеты категории Broadcast (широковещательный) могут значительно

засорять компьютерную сеть. Эти пакеты в большинстве своем относятся к

служебным. Признаком этих пакетов являются пакеты с IP адресами в

хостовой части имеющие 255.255,

либо имеющие адрес MAC - FF:FF:FF:FF:FF:FF.

Эти пакеты выявляются в трафике с помощью фильтров.

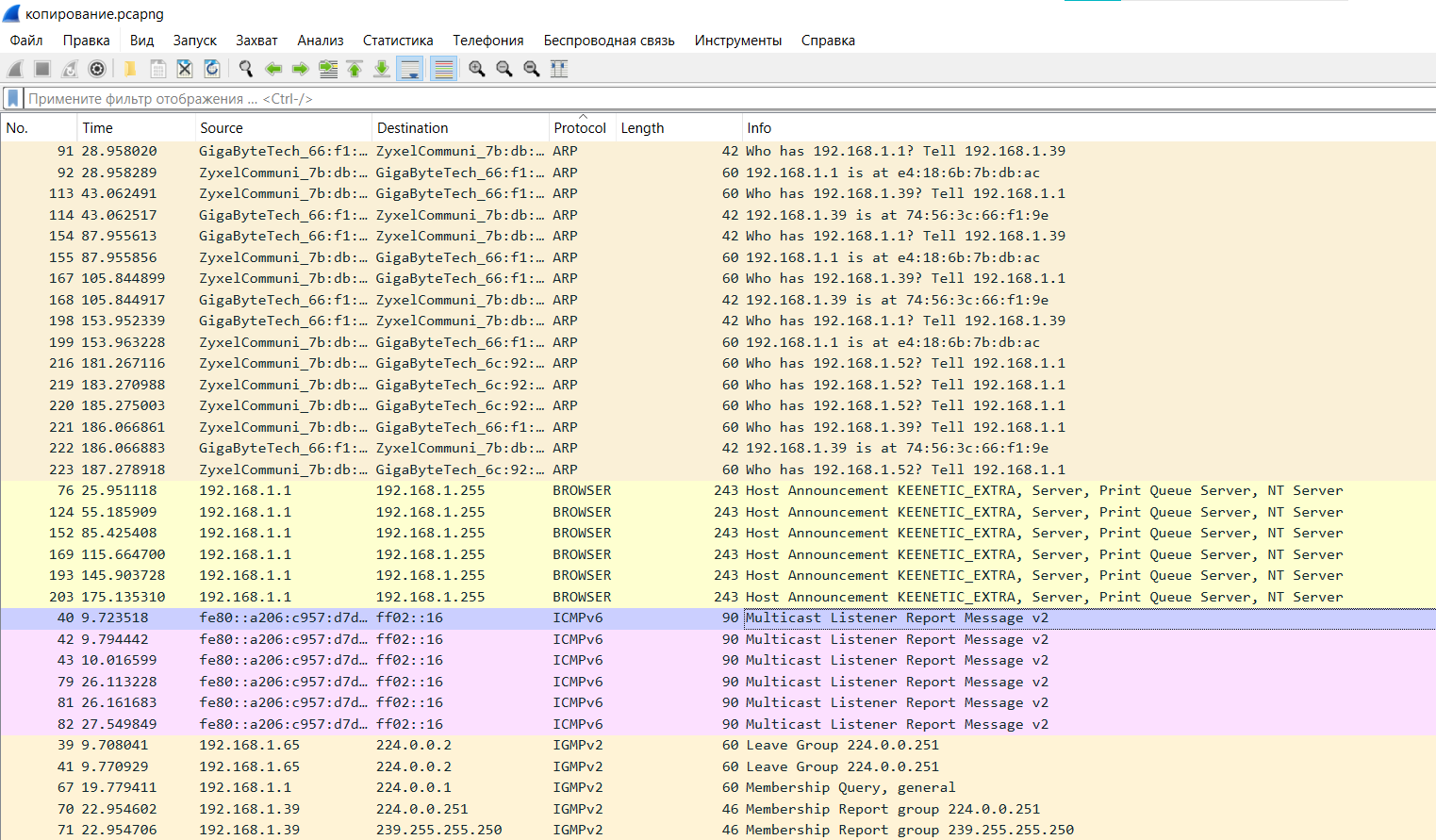
К полезным служебным пакетам относятся пакеты ARP, идущие со своего

компьютера. Остальные (если есть, относятся к категории «чужой») .

В режиме Idle 221 из 782 пакетов специальные пакеты с последним байтом 255 (Protocol Browser) и протоколы ARP.

В режиме копирования файла 22 из 227 пакетов специальные пакеты с последним байтом 255 (Protocol Browser) и протоколы ARP.

В режиме доступа к Web сайту 8 из 19999 специальные пакеты с последним байтом 255 (Protocol Browser) и протоколы ARP.

Трафик Broadcost и специальных протоколов.