

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ компьютерной безопасности и криптографии

**ОБНАРУЖЕНИЕ СЕТЕВОГО RDP ТРАФИКА МЕТОДОМ АНАЛИЗА
ЕГО ПОВЕДЕНИЯ**

КУРСОВАЯ РАБОТА

студента 3 курса 331 группы
направления 10.05.01 — Компьютерная безопасность
факультета КНиИТ
Токарева Никиты Сергеевича

Научный руководитель
доцент

Гортинский А. В.

Заведующий кафедрой

Абросимов М. Б.

Саратов 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 Определение RDP	4
1.1 Место протокола RDP в структуре OSI.....	4
2 Принцип работы протокола RDP и анализ его поведения	9
3 Обнаружение сеанса удаленного управления с помощью разработан- ной программы	13
3.1 Описание работы программы «sniffer.py»	13
3.2 Описание работы программы «data-analysis.py»	15
4 Демонстрация работы программ	18
ЗАКЛЮЧЕНИЕ	25
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	26
Приложение А Код sniffer.py	28
Приложение Б Код data-analysis.py	32

ВВЕДЕНИЕ

Информация – это сведения об окружающем мире и протекающих в нём процессах, которые зафиксированы на каком-либо носителе. Благодаря протоколам удаленного доступа можно распоряжаться базами данных, информацией, которая хранится на другом устройстве. В недавнем прошлом большинство схем удаленного доступа характеризовалось высокой стоимостью, низкой производительностью, небольшой скоростью передачи данных, недостаточным уровнем защищенности передаваемой информации [1].

Сейчас, когда практически все предприятия перешли на дистанционный формат работы, компании выбирают протокол RDP, так как он прост в настройке и в использовании. Но далеко не все уделяют особое внимание безопасности собственных рабочих мест. Поэтому предприятия могут быть атакованы злоумышленниками.

В данной работе будут разобраны принцип работы RDP, анализ его поведения, а также методы обнаружения данного протокола.

1 Определение RDP

Протокол RDP (от англ. Remote Desktop Protocol — протокол удалённого рабочего стола) — патентованный протокол прикладного уровня компании Microsoft и приобретен ею у другой компании Polycom, который предоставляет пользователю графический интерфейс для подключения к другому компьютеру через сетевое соединение. Для этого пользователь запускает клиентское программное обеспечение RDP, а на другом компьютере должно быть запущено программное обеспечение сервера RDP [2].

Стоит отметить, что RDP позволяет работать с удаленным компьютером, почти как с локальным. При успешном создании RDP-сессии пользователь может двигать мышкой, открывать файлы, диски, документы, программы, без каких-либо проблем использовать буфер обмена (Ctrl+C, Ctrl+V) не только для текста, но и для файлов. Также отлично работает передача сочетаний клавиш, переключения языков.

1.1 Место протокола RDP в структуре OSI

Эталонная модель OSI представляет собой 7-уровневую иерархическую сетевую иерархию, разработанную международной организацией по стандартам (International Standardization Organization — ISO). В рамках модели, любой протокол может взаимодействовать либо с протоколами своего уровня (горизонтальные взаимодействия), либо с протоколами уровня на единицу выше/ниже своего уровня (вертикальные взаимодействия). Каждый из семи уровней характеризуется типом данных, которым данный уровень оперирует и функционалом, который он предоставляет слою, находящемуся выше него [11]. Модель OSI включает в себя следующие уровни:

1. Физический уровень, который отвечает за передачу последовательности битов через канал связи;
2. Канальный уровень, где осуществляется разбиение данных на «кадры», размер которых обычно достигает от несколько сотен до нескольких тысяч байтов;
3. Сетевой уровень, на котором осуществляется структуризация и маршрутизация пакетов от отправителя к получателю;
4. Транспортный уровень, функцией которого является передача надежных последовательностей данных произвольной длины через коммуникацион-

- ную сеть от отправителя к получателю;
5. Сеансовый уровень, на котором происходит поддержка сессии связи, управление взаимодействием между приложениями;
 6. Уровень представления, который представляет данные в понятном для какой-либо конкретной машины виде;
 7. Прикладной уровень, предоставляющий набор интерфейсов для взаимодействия пользовательских процессов с сетью.

Вследствие этого, RDP является непосредственно протоколом прикладного уровня модели OSI, наряду с SMTP, HTTP, FTP и многими другими. Протоколы седьмого уровня используют TCP или UDP в качестве передачи информации. Поэтому данные протокола RDP хранятся в заголовках TCP и UDP.

Далее для понимания того, в каком виде информация передается от отправителя к получателю необходимо разобрать структуру пакета. Согласно вышесказанному с помощью протоколов TCP и UDP отправитель передает данные, принадлежащие RDP, получателю. Они хранятся в специальном поле данных. Его можно увидеть на рисунке 1, где изображена структура TCP-заголовка.

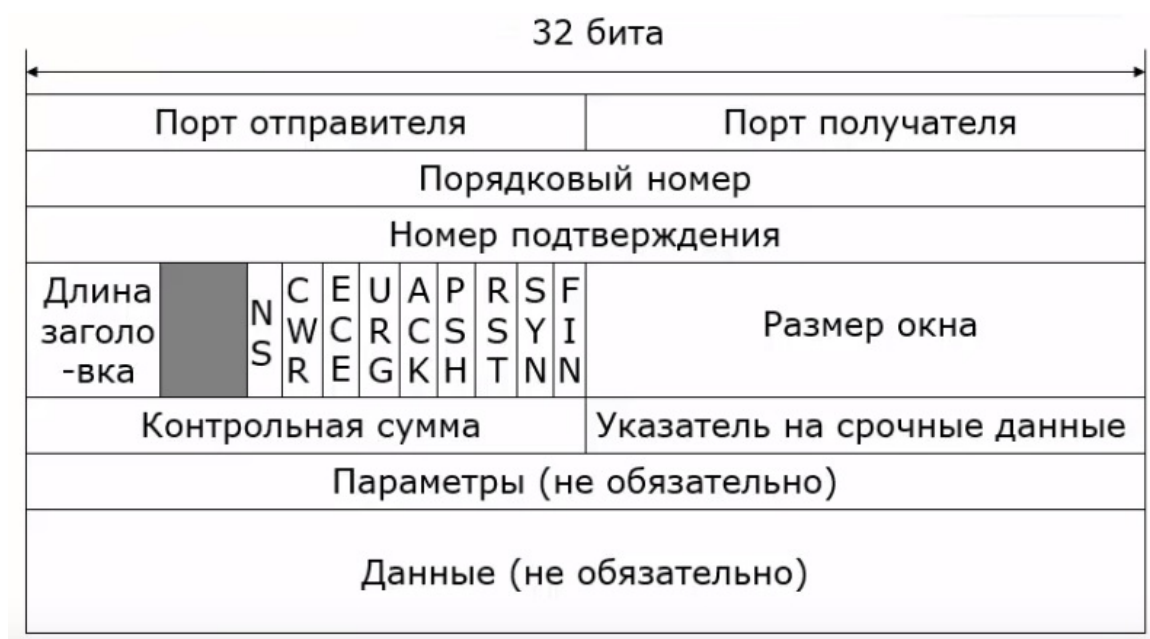


Рисунок 1 – Структура TCP-заголовка

Помимо поля данных в TCP-заголовке для дальнейшего анализа будут интересными поля, в которых хранится информация о портах отправителя и получателя. Стоит отметить, что при подключении к удаленному рабочему столу по умолчанию используется порт 3389. Поэтому для обнаружения RDP-сессии информация о портах будет достаточно полезной.

Также не менее интересной информацией являются установленные флаги, хранящиеся в поле флагов. В нем хранятся следующие управляющие биты:

1. NS — одноразовая сумма (Nonce Sum). По-прежнему является экспериментальным флагом, используемым для защиты от случайного злонамеренного сокрытия пакетов от отправителя [10]. Используется для улучшения работы механизма явного уведомления о перегрузке (Explicit Congestion Notification, ECN);
2. CWR — окно перегрузки уменьшено (Congestion Window Reduced). Данный флаг устанавливается (принимает значение равной единице) отправителем, чтобы показать, что TCP-фрагмент был получен с установленным полем ECE;
3. ECE — ECN-Эхо (ECN-Echo). Этот флаг показывает, поддерживает ли TCP-отправитель ECN;
4. URG — устанавливается, если необходимо передать ссылку на поле указателя срочности (Urgent pointer);
5. ACK — флаг подтверждения используется для подтверждения успешного получения пакета;
6. PSN — инструктирует получателя протолкнуть данные, накопившиеся в приемном буфере, в приложение пользователя;
7. RST — флаг сброса отправляется от получателя к отправителю, когда пакет отправляется на конкретный хост, который этого не ожидал;
8. SYN — начинает соединение и синхронизирует порядковые номера. Первый пакет, отправленный с каждой стороны, должен в обязательном порядке иметь установленным этот флаг;
9. FIN — означает, что данных от отправителя больше нет. Поэтому он используется в последнем пакете, отправленном отправителем.

Благодаря вышеописанным флагам можно узнать информацию о конкретном состоянии соединения.

IP пакет представляет собой отформатированную информацию в блоке, которая передается в сети. В настоящее время применяются две версии IP пакетов: IPv4 и IPv6. В данной работе будут рассматриваться пакеты IP версии 4, так как для анализа данных этого вполне достаточно. Поэтому далее необходимо рассмотреть IPv4-заголовок, который показан на рисунке 2.

Октет	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Версия			IHL			Тип обслуживания						Длина пакета																			
4	Идентификатор																Флаги		Смещение фрагмента													
8	Время жизни						Протокол						Контрольная сумма заголовка																			
12	IP-адрес отправителя																															
16	IP-адрес получателя																															
20	Параметры от 0-я до 10-и 32-х битовых слов																															
	Данные																															

Рисунок 2 – Структура IPv4-заголовка

IPv4 используется на сетевом уровне модели OSI для осуществления передачи пакетов между сетями.

В его заголовке достаточно важной информацией являются поля, в которых записаны IP-адреса отправителя и получателя. Ведь благодаря этой информации можно определить, между какими устройствами происходит обмен данными.

Также необходимо обратить внимание на 8-разрядное поле протокола. На рисунке оно обозначено как «Протокол». С помощью него можно идентифицировать протоколы следующего уровня (TCP, UDP, ICMP и другие) по его номеру. Например, если в IPv4-заголовке в поле «Протокол» будет задан номер 6, значит в поле данных хранится информация о протоколе TCP.

Согласно модели OSI, если перейти на один уровень ниже, а именно на канальный, то на нем осуществляется инкапсуляция пакета, полученного на сетевом уровне, где добавляется дополнительный заголовок, кадр Ethernet, к сегменту данных. Его структура показана на рисунке 3.



Рисунок 3 – Структура Ethernet кадра

Здесь достаточно важной информацией считаются поля адресов отправителя и получателя. Ведь в них содержатся MAC-адреса источника и назначения

соответственно. В поле «Тип», содержится номер, идентифицирующий тип сетевого протокола. Также в поле данных содержатся данные от более высокого уровня согласно модели OSI, а именно инкапсулированные данные о пакете.

Далее необходимо разобрать, опираясь на практическую часть, поведение протокола RDP при подключении к удаленному рабочему столу.

2 Принцип работы протокола RDP и анализ его поведения

Принцип работы RDP базируется на протоколе TCP. Соединение клиент-сервер происходит на транспортном уровне. После инициализации пользователь проходит аутентификацию. В случае успешного подтверждения сервер передает клиенту управление. Стоит отметить, что под понятием слова «клиент» подразумевается любое устройство (персональный компьютер, планшет или смартфон), а «сервер» — удаленный компьютер, к которому оно подключается.

Протокол RDP внутри себя поддерживает виртуальные каналы, через которые пользователю передаются дополнительные функции операционной системы, например, можно распечатать документ, воспроизвести видео или скопировать файл в буфер обмена.

Далее в работе будет описан процесс подключения к удаленному рабочему столу, во время которого осуществлялся захват трафика с помощью одной известной программы Wireshark. С помощью нее можно достаточно подробно рассмотреть структуру сообщений протоколов, поддерживающих RDP-сессию.

Для начала будет произведено подключение с помощью «Удаленного рабочего стола». Это средство представляет собой встроенную в Windows программу, предназначенную для удалённого доступа. При его использовании предполагается, что пользователь будет подключаться к одному компьютеру с другого устройства, находящегося в той же локальной сети. В качестве клиента и сервера будут выступать компьютеры с операционной системой Windows 10 Professional версии 21H2.

Для подключения к удаленному рабочему столу были заданы статические IP-адреса. Клиенту был присвоен статический IP-адрес 192.168.10.254, а серверу — 192.168.10.229, соответственно маска сети 255.255.255.0. После того, как были заданы IP-адреса, необходимо зайти в настройки Windows, чтобы включить возможность подключения к удаленному рабочему столу. Об этом более подробно описано в статьях [3] и [4]. Далее на сервере был произведен запуск анализа трафика с помощью приложения Wireshark. После подключения к удаленному компьютеру программа-анализатор трафика начала «захватывать» пакеты, как показано на рисунке 4, принадлежащие следующим протоколам:

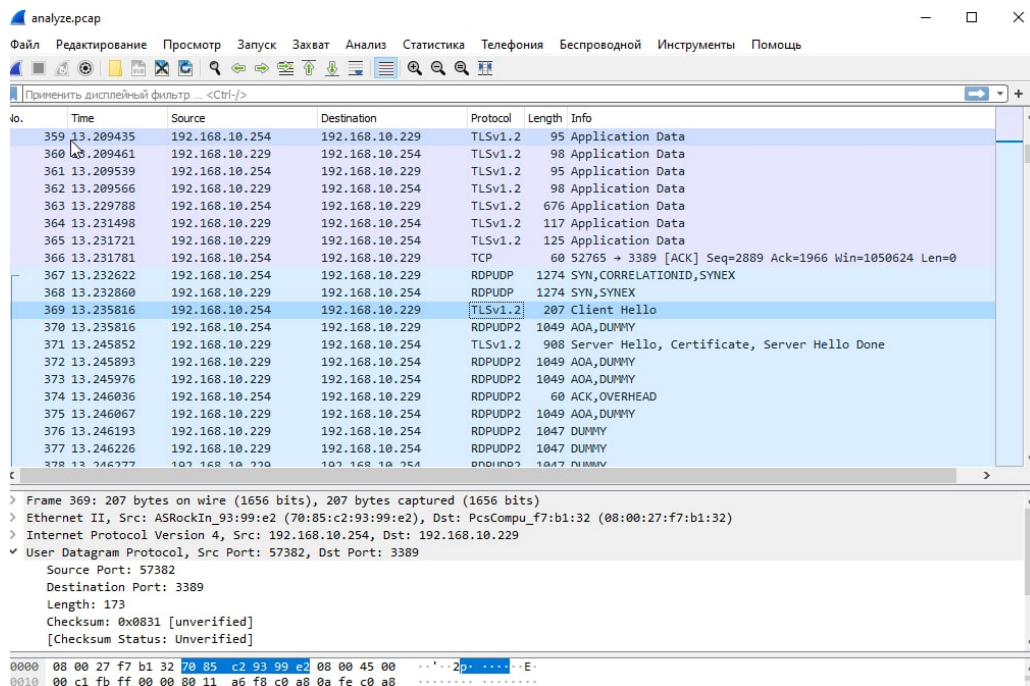


Рисунок 4 – Окно программы Wireshark после захвата трафика

- RDPUDP — протокол RDP, использующий для передачи данных UDP-протокол.
- RDPUDP2 также относится к протоколу RDP. Он был разработан для повышения производительности сетевого соединения по сравнению с соответствующим соединением RDP-UDP [8].
- TLSv1.2 — протокол защиты транспортного уровня, обеспечивающий защищенную передачу между узлами в сети интернет. В данном случае обеспечивает безопасность RDP-сессии.

Во время работы программы Wireshark было найдено достаточное количество пакетов, принадлежащих RDP, которые содержат в себе достаточно интересную информацию. Поэтому стоит рассказать о том, как происходит стандартный способ защиты RDP, осуществляемый в момент аутентификации. Это можно представить в несколько этапов:

1. Клиент объявляет серверу о своем намерении использовать стандартный протокол RDP.
2. Сервер соглашается с этим и отправляет клиенту свой собственный открытый ключ, полученный при шифровании алгоритмом RSA, а также некоторую строку случайных байтов (обычно её называют «random сервером»), генерируемую сервером. На рисунке 5 можно увидеть запись random сервера.

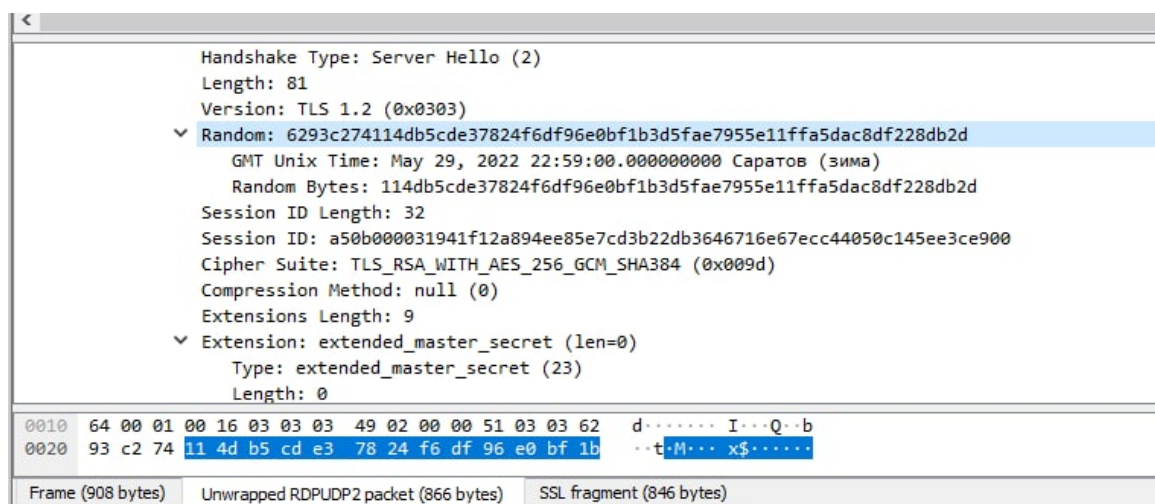


Рисунок 5 – Содержимое пакета, посылаемого от сервера клиенту (запись random сервера)

Совокупность открытого ключа и некоторая строка случайных байтов называется «сертификатом». Данная запись изображена на рисунке 6.

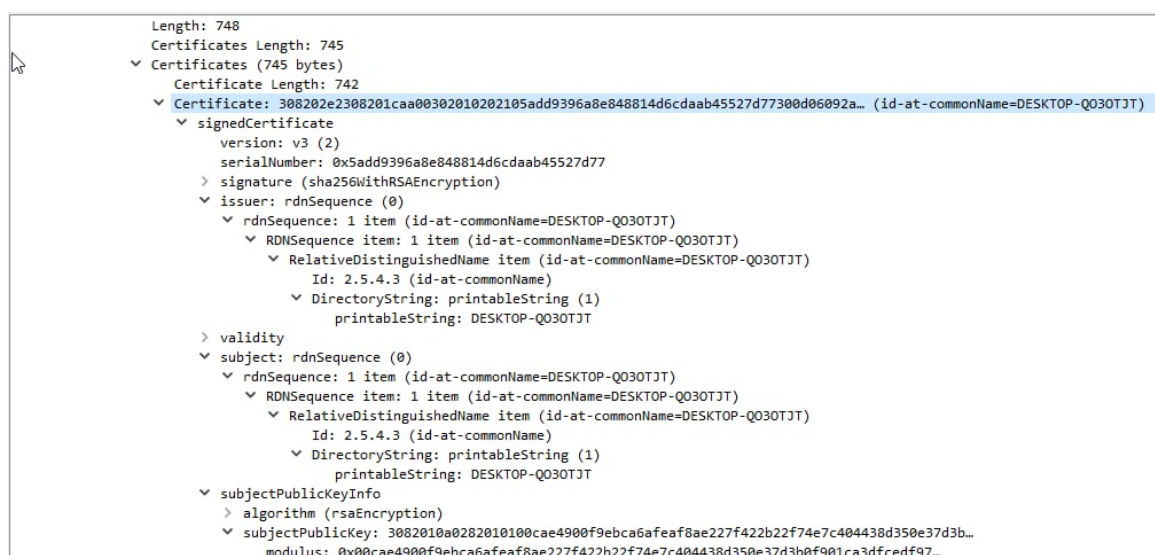


Рисунок 6 – Содержимое пакета, посылаемого от сервера клиенту (запись сертификата)

Сертификат подписывается службой терминалов, например, RDS, с использованием закрытого ключа для обеспечения подлинности.

3. Теперь клиент посылает некоторую строку случайных байтов, которая называется «premaster secret», показанная на рисунке 7.

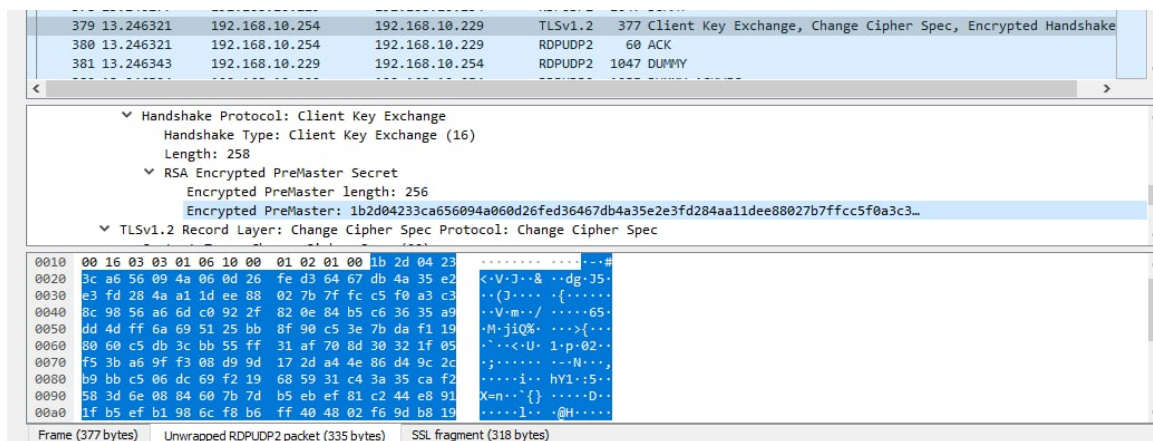


Рисунок 7 – Содержимое пакета, посылаемого от клиента серверу (запись premaster secret)

Данная запись шифруется открытым ключом, которая может быть расшифрована сервером только с помощью закрытого ключа службы терминалов.

4. Сервер расшифровывает premaster secret с помощью собственного закрытого ключа.
5. В случае успеха клиент и сервер получают свои сеансовые ключи из random сервера и premaster secret. Далее они используются для симметричного шифрования остальной части сеанса.

После того, как всё настроено, сессия RDP готова к работе. На ПК клиента от сервера поступает графическое изображение (результат операций), которое происходит в результате отправки команд с клавиатуры или мыши. Стоит отметить, что для такого вида отправки сообщений подходит протокол UDP. Ведь область применения UDP заключается в обмене короткими сообщениями в режиме запрос-ответ, и этот протокол часто используется для передачи потоковых данных, например, аудио или видео. Поэтому неслучайно при RDP-сессии используется протокол UDP.

Осталось только понять, как обнаружить передачу информации, характерную для подключения к удаленному рабочему столу.

3 Обнаружение сеанса удаленного управления с помощью разработанной программы

Одним из методов выявления сообщений, передаваемых по сети, является сниффер — это программное обеспечение, которое анализирует входящий и исходящий трафик с компьютера, подключенного к интернету. Для данной работы была написана на языке Python программа «sniffer.py», перехватывающая трафик сети.

Данный сниффер принимает пакеты четвертой версии интернет-протокола, пакеты IPv4, содержащие в поле данных сообщения протоколов других уровней. В этом случае здесь будут рассматриваться сообщения протоколов транспортного уровня, а именно TCP- и UDP-протоколы.

Для успешного перехвата трафика, необходимо установить неразборчивый режим на сетевой интерфейс, чтобы сетевая плата принимала все пакеты независимо от того, кому они адресованы. Данный выбор зависит от способа подключения устройства к сети. Например, в Linux есть виртуальный интерфейс («lo»), который ваш компьютер использует для связи с самим собой, также существуют интерфейсы, относящиеся к проводному соединению («enp0s3») и беспроводному («wlp2s0»). В данном случае все устройства будут подключены к сети через Ethernet.

После выбора сетевого интерфейса сниффер начнет перехватывать трафик. В этот момент информация о перехваченных пакетах будет отображаться в консоли, а также будет записываться необходимая информация каждого пакета для анализа в текстовый файл. В результате работы программы «sniffer.py» будет получен файл data.log. Для обработки содержимого данного файла была написана программа «data-analysis», реализованная также на языке Python. С помощью нее можно проанализировать весь перехваченный трафик относительно каждого IP-адреса, полученного из файла. Описание этих программ будет представлено ниже.

3.1 Описание работы программы «sniffer.py»

Для анализа трафика в сети был создан сокет — программный интерфейс для обеспечения обмена данными между процессами. В силу заданных параметров он получал данные, представленные в виде некоторой последовательности чисел, записанных в шестнадцатеричной системе счисления. По сути, сокет

перехватывает сообщения, получаемые на канальном уровне модели OSI.

Опираясь на вышеизложенную информацию, чтобы раскодировать данную последовательность чисел, необходимо разобрать кадр Ethernet, представленный на рисунке 3. Стоит отметить, что в данном заголовке нужно раскодировать 14 байт, 12 из которых MAC-адреса получателя и отправителя и 2 байта, идентифицирующие протокол сетевого уровня. К примеру, 0x0800 – IPv4, 0x86DD – IPv6 и т.д. С помощью функций *get_ethernet_frame* и *get_mac_addr* производится получение всех необходимых данных заголовка Ethernet.

После получения информации об Ethernet кадре идет раскодирование данных, принадлежащих сетевому уровню модели OSI.

Обычно длина заголовка IP равна 20 байт, т.е. пять 32-битных слов, однако при увеличении объема служебной информации эта длина может быть увеличена за счет использования дополнительных байт в поле параметров и выравниваний. Благодаря полю, где содержится длина заголовка, можно правильно раскодировать оставшуюся последовательность байт. С помощью функций *get_ipv4_data* и *ipv4_dec* будет получена информация о времени жизни текущего пакета, о номере транспортного протокола, об IP-адресах отправителя и получателя.

После того, как был получен номер транспортного протокола, можно раскодировать их данные. Как уже упоминалось ранее, в качестве транспортных протоколов будут рассматриваться TCP и UDP протоколы.

С помощью функции *get_tcp_segment* производится получение информации, содержащейся в TCP-протоколе. Таким образом, теперь программе известны порт получателя, порт отправителя, порядковый номер, номер подтверждения, флаги и данные, которые содержат в себе TCP-заголовок.

Аналогично получается раскодирование данных UDP-заголовка с помощью функции *get_udp_segment*.

Вся необходимая информация о пакетах для дальнейшего анализа записывается в файл *data.log* с помощью функции *write_to_file*.

Практически все выше перечисленные функции вызываются в *start_to_listen*, где осуществляется сбор информации о получаемых пакетах и вывод ее в консоль. Стоит отметить, что все выше описанные функции приведены в приложении А, где показан непосредственно сам код программы «sniffer.py». Соответственно код программы «data-analysis.py» представлен в приложении Б.

3.2 Описание работы программы «data-analysis.py»

При запуске программа попросит пользователя ввести название файла. Далее производится считывание файла с помощью функции *read_from_file*, где в это время сохраняется информация о каждом пакете, перехваченном во время работы программы «sniffer.py».

После считывания собирается некоторая общая информация о перехваченном трафике. Под общей информацией подразумевается: время начала и завершения перехвата трафика, количество пакетов, среднее количество пакетов в секунду, средний размер пакетов. Вместе с этим в консоль выводится список IP-адресов, участвующих в передаче пакетов по сети, в момент работы программы «sniffer.py». Пользователю предоставляется возможность выбрать интересующий его IP-адрес для дальнейшего анализа пакетов, связанных с ним. После выбора конкретного IP-адреса осуществляется вывод опять же общей информации, но уже только относительно выбранного IP-адреса. Т.е. выводится время первого и последнего перехваченных пакетов, где в качестве отправителя или получателя выступает данный IP-адрес.

Таким образом можно понять, в какой конкретно момент времени начался обмен информацией с тем или иным IP-адресом. Также рассчитываются количество пакетов, среднее количество пакетов в секунду и средний размер пакетов для определения общего объема информации, передаваемой в данный отрезок времени. Помимо этого, пользователю предоставляются некоторые опции, которые будут описаны ниже:

1. Пользователю предоставляется возможность вывести весь сетевой трафик, где в качестве отправителя или получателя выступает выбранный IP-адрес.
2. При выборе второй опции строится график отношения входящего и исходящего трафиков в единицу времени. Данное отношение рассчитывается по формуле

$$r_{ip} = \frac{V_{dest}}{V_{src}},$$

где V_{dest} и V_{src} — объемы соответственно входящего и исходящего трафика в единицу времени.

При большой величине входящего трафика, можно узнать в какой момент времени происходит обмен информацией с каким-либо другим IP-адресом.

3. При выборе третьей опции строится график отношения V_{udp} — объема входящего UDP-трафика и V_{tcp} объема входящего TCP-трафика. Отношение рассчитывается по формуле

$$r_{udp} = \frac{V_{udp}}{V_{tcp}}.$$

Так как во время RDP-сессии осуществляется передача пакетов по протоколу UDP и TCP, то анализируя полученную информацию исходя из этого графика, можно установить признаки RDP-сессии. Ведь превышение объема входящего UDP-трафика над объемом TCP-трафика может стать одним из признаков установки RDP-сессии, когда одному устройству нужно обменяться большим количеством сообщений с другим устройством в режиме запрос-ответ.

4. При выборе данной опции строится график разности количества исходящих и входящих TCP-пакетов, в которых флаг ACK имеет значение равное единице.

$$r_{ack} = V_{A_{out}} - V_{A_{in}},$$

где $V_{A_{in}}$ и $V_{A_{out}}$ — число входящих и исходящих ACK-флагов в TCP-трафике в единицу времени. При подключении к удаленному рабочему столу сервер отправляет клиенту TCP-пакеты с установленным флагом ACK, указывающим, что поле номера подтверждения задействовано. В таком случае с помощью графика, анализируя изменение величины r_{ack} в разные промежутки времени, можно идентифицировать устройство, совершающее подключение к удаленному рабочему столу.

5. При выборе пятой опции строятся два графика, показывающие частоту SYN-флагов и RST-флагов в TCP-трафике. Частота SYN-флагов находится по формуле

$$r_{syn} = \frac{V_{S_{in}}}{V_{tcp}},$$

где $V_{S_{in}}$ число входящих TCP-пакетов, в которых установлен флаг SYN = 1, V_{tcp} — число входящих TCP-пакетов в единицу времени. Пакеты с флагом SYN пересылаются между клиентом и сервером в ходе установления TCP-соединения, после чего начинается обмен данными с помощью пакетов без SYN-флага. Таким образом, число SYN-флагов, пришедших на сервер,

равно числу запросов на соединение, а частота SYN-флагов определяет долю служебных пакетов этого типа в ТСП-трафике.

Частота PSH-флагов вычисляется по формуле

$$r_{psh} = \frac{V_{P_{in}}}{V_{tcp}},$$

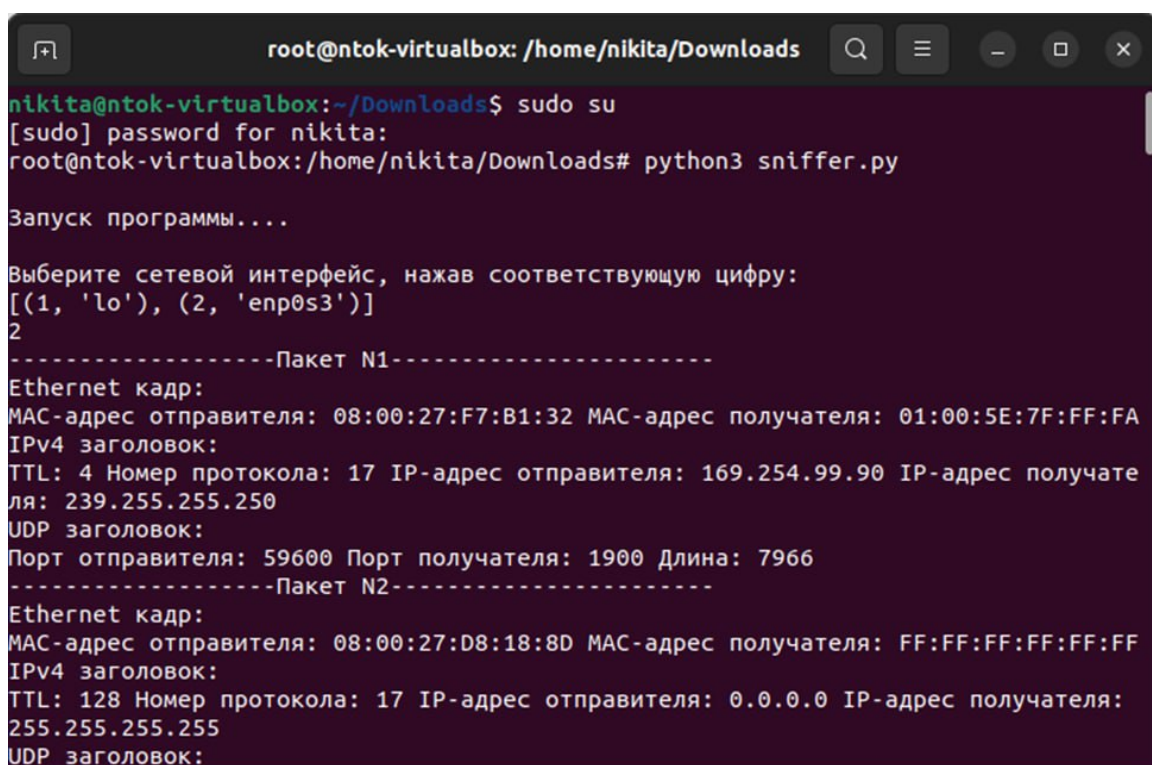
где $V_{P_{in}}$ число входящих ТСП-пакетов, в которых установлен флаг PSH = 1, V_{tcp} — число входящих ТСП-пакетов в единицу времени. Опираясь на вышеописанную информацию, PSH-флаг инструктирует получателя, чтобы он отправил накопившиеся в приемном буфере данные в приложение отправителя. Таким образом, если значение величины r_{psh} резко возросло в некоторый промежуток времени, значит за это время одно устройство успело передать получателю большое количество пакетов.

После описания всех опций данной программы остается только показать, как это будет выглядеть на практике.

4 Демонстрация работы программ

Для тестирования данных программ было запущено три виртуальных машины. Две из них (ПК-1 и ПК-2) имеют операционную систему Windows 10 Professional версии 21H2. И у одной машины (ПК-3) поставлена операционная система Linux Ubuntu 22.04 LTS. Все устройства не имеют доступа к интернету, однако каждая виртуальная машина может взаимодействовать друг с другом.

Запустив программу «sniffer.py», был произведен захват трафика, как показано на рисунке 8.



```
root@ntok-virtualbox: /home/nikita/Downloads
nikita@ntok-virtualbox:~/Downloads$ sudo su
[sudo] password for nikita:
root@ntok-virtualbox:/home/nikita/Downloads# python3 sniffer.py

Запуск программы....

Выберите сетевой интерфейс, нажав соответствующую цифру:
[(1, 'lo'), (2, 'enp0s3')]
2
-----Пакет N1-----
Ethernet кадр:
MAC-адрес отправителя: 08:00:27:F7:B1:32 MAC-адрес получателя: 01:00:5E:7F:FF:FA
IPv4 заголовок:
TTL: 4 Номер протокола: 17 IP-адрес отправителя: 169.254.99.90 IP-адрес получателя: 239.255.255.250
UDP заголовок:
Порт отправителя: 59600 Порт получателя: 1900 Длина: 7966
-----Пакет N2-----
Ethernet кадр:
MAC-адрес отправителя: 08:00:27:D8:18:8D MAC-адрес получателя: FF:FF:FF:FF:FF:FF
IPv4 заголовок:
TTL: 128 Номер протокола: 17 IP-адрес отправителя: 0.0.0.0 IP-адрес получателя: 255.255.255.255
UDP заголовок:
```

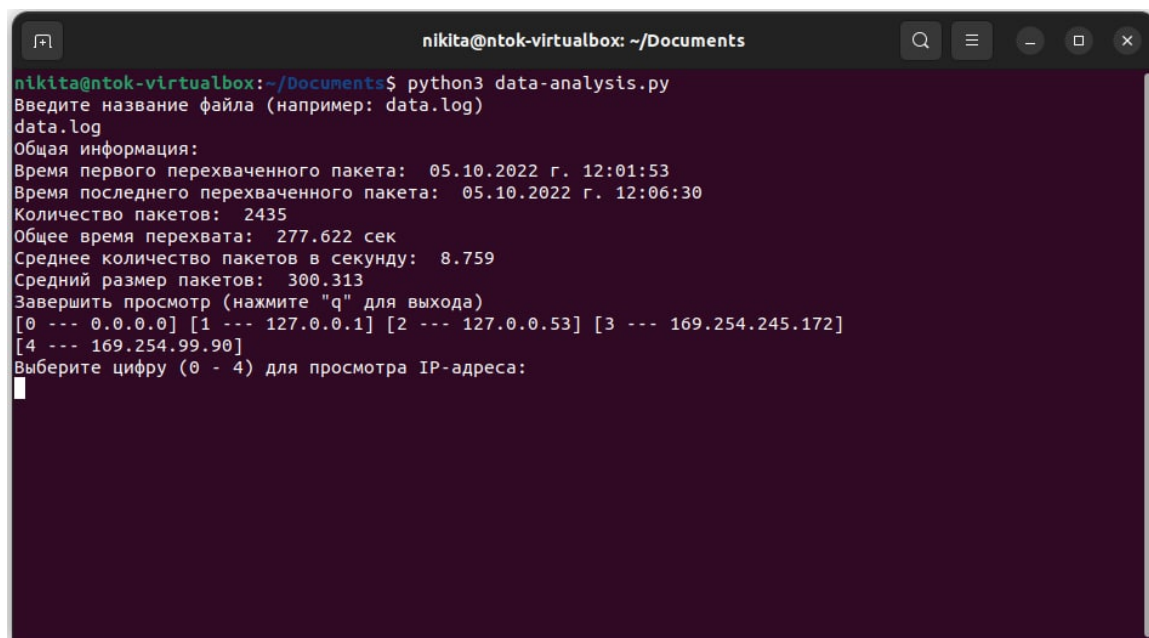
Рисунок 8 – Вид консоли при работе программы «sniffer.py»

Во время работы программы совершались следующие действия:

1. В 12:03 на ПК2 была запущена программа «Подключение к удаленному рабочему столу».
2. Примерно через 15 секунд было совершено подключение ПК2 к ПК1 по протоколу RDP.
3. Начиная с 12:03:50 производилось движение мышкой по рабочему столу, открытие текстовых файлов, лежащих на рабочем столе ПК1.
4. В 12:04:51 было завершено подключение к удаленному рабочему столу ПК1.

После завершения программы «sniffer.py» был получен файл data.log, в

котором хранится вся необходимая информация о каждом перехваченном пакете. Запустив программу «data-analysis.py» и введя название анализируемого файла, в консоли отображаются общие сведения о перехваченном трафике, как показано на рисунке 9.



```
nikita@ntok-virtualbox: ~/Documents
nikita@ntok-virtualbox:~/Documents$ python3 data-analysis.py
Введите название файла (например: data.log)
data.log
Общая информация:
Время первого перехваченного пакета: 05.10.2022 г. 12:01:53
Время последнего перехваченного пакета: 05.10.2022 г. 12:06:30
Количество пакетов: 2435
Общее время перехвата: 277.622 сек
Среднее количество пакетов в секунду: 8.759
Средний размер пакетов: 300.313
Завершить просмотр (нажмите "q" для выхода)
[0 --- 0.0.0.0] [1 --- 127.0.0.1] [2 --- 127.0.0.53] [3 --- 169.254.245.172]
[4 --- 169.254.99.90]
Выберите цифру (0 - 4) для просмотра IP-адреса:
█
```

Рисунок 9 – Вид консоли при работе программы «data-analysis.py»

Из рисунка 9 видно, что в данном промежутке времени в обмене данными принимали участие всего 5 IP-адресов, первые три из которых рассылает устройство ПК3. А последние два принадлежат ПК1 и ПК2. Осталось только определить какой IP-адрес принадлежит серверу, а какой — клиенту. Конечно, больше всего сейчас интересны последние два IP-адреса, поэтому далее пользователь введет значение 3, чтобы выбрать IP-адрес 169.254.245.172.

На рисунке 10 показана информация, связанная с IP-адресом 169.254.245.172.

```
nikita@ntok-virtualbox: ~/Documents
Общая информация:
Время первого перехваченного пакета: 05.10.2022 г. 12:01:53
Время последнего перехваченного пакета: 05.10.2022 г. 12:06:30
Количество пакетов: 2435
Общее время перехвата: 277.622 сек
Среднее количество пакетов в секунду: 8.759
Средний размер пакетов: 300.313
Завершить просмотр (нажмите "q" для выхода)
[0 --- 0.0.0.0] [1 --- 127.0.0.1] [2 --- 127.0.0.53] [3 --- 169.254.245.172]
[4 --- 169.254.99.90]
Выберите цифру (0 - 4) для просмотра IP-адреса:
3
Общая информация о трафике, связанном с 169.254.245.172
Время первого перехваченного пакета: 05.10.2022 г. 12:02:31
Время последнего перехваченного пакета: 05.10.2022 г. 12:04:50
Количество пакетов: 2278
Среднее количество пакетов в секунду: 16.296
Средний размер пакетов: 262.049
Выберите опцию:
1. Вывести весь трафик, связанный с 169.254.245.172
2. Построить график отношения входящего и исходящего трафиков
3. Построить график отношения объема входящего UDP-трафика и объема входящего TCP-трафика
4. Построить график разности числа исходящих и числа входящих ACK-флагов в единицу времени
5. Построить график частоты SYN и PSN флагов во входящих пакетах
6. Вернуться к выбору IP-адреса
```

Рисунок 10 – Вид консоли при выборе IP-адреса 169.254.245.172

При выборе второй опции будет построен график, изображенный на рисунке 11.



Рисунок 11 – График отношения входящего и исходящего трафиков относительно 169.254.245.172

Из рисунка 11 видно, что значение переменной V_{dest} начинает возрастать с 12:03:18, а на 12:03:20 эта величина достигает своего максимального значения.

Теперь для сравнения на следующем рисунке будет показан график отношения входящего и исходящего трафиков, но уже относительно IP-адреса 169.254.99.90.

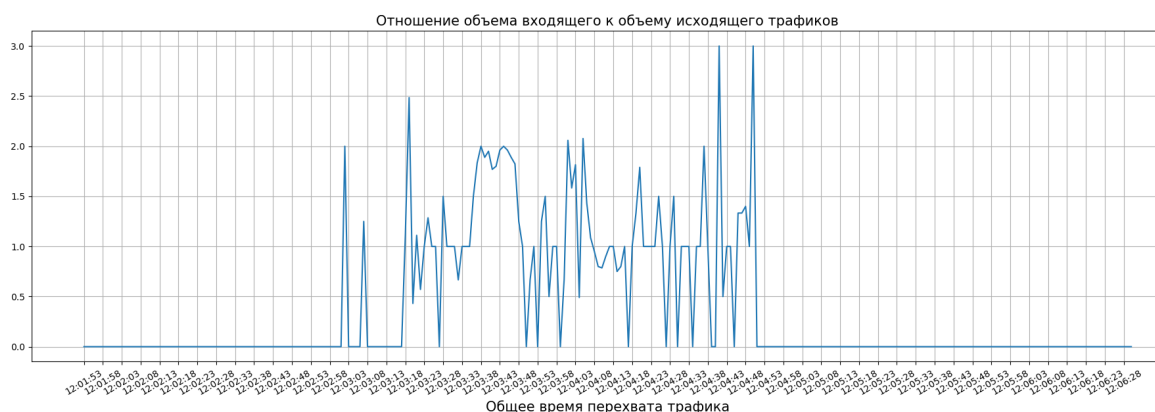


Рисунок 12 – График отношения входящего и исходящего трафиков относительно 169.254.99.90

Если посмотреть на следующий рисунок, то можно увидеть в данном трафике, что первый пакет был передан по порту 3389 в 12:03:02. Это также видно из графиков, показанных на рисунках 11 и 12. Тогда начиная с 12:03:18 произошла установка RDP-сессии.



Рисунок 13 – Просмотр трафика, связанного с 169.254.245.172

Исходя из рисунков 14 и 15, можно сделать вывод, что в промежутке 12:03:18 – 12:03:25 передается большой объем UDP-пакетов и скорее всего это произошло в момент подтверждения сертификата клиента сервером.



Рисунок 14 – График, построенный по формуле $r_{udp} = \frac{V_{udp}}{V_{tcp}}$ относительно 169.254.245.172

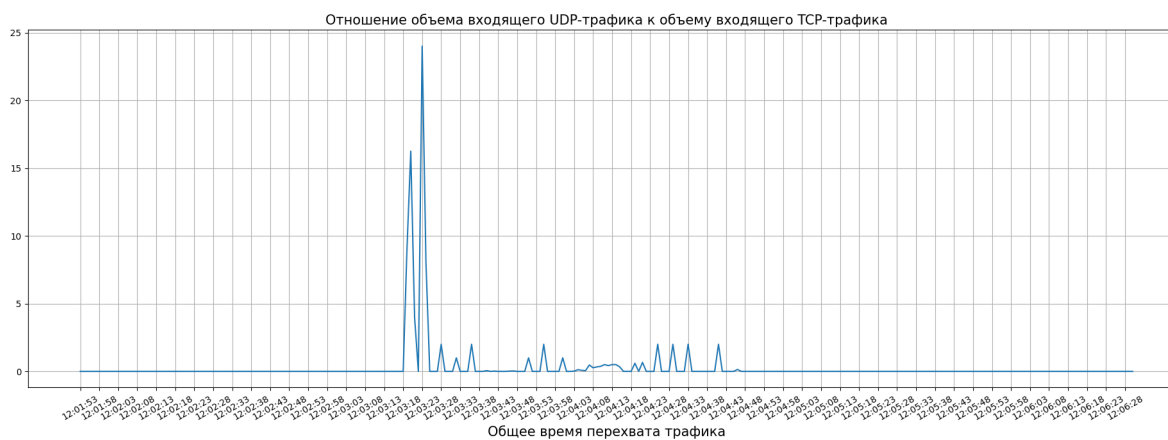


Рисунок 15 – График, построенный по формуле $r_{udp} = \frac{V_{udp}}{V_{tcp}}$ относительно 169.254.99.90

На рисунках 16 и 17 изображены графики разности числа исходящих и входящих АСК-флагов в единицу времени.



Рисунок 16 – График, построенный по формуле $r_{ack} = V_{ack_out} - V_{ack_in}$ относительно 169.254.245.172

Величина V_{ack_in} показывает, как часто сервер отказывает клиенту из-за перегрузки. На промежутке 12:03:36 – 12:03:49 видно, что осуществляется обмен

данными между клиентом и сервером. Как показано на рисунке 17 отрицательное значение величины r_{ack} показывает, что на данном промежутке времени сервер, получая от клиента ТСР-пакеты с установленным АСК-флагом, теряет возможность отвечать на запросы клиента.



Рисунок 17 – График, построенный по формуле $r_{ack} = V_{Aout} - V_{Ain}$ относительно 169.254.99.90

Получается, что ПК1 (серверу) соответствует адрес 169.254.99.90, а ПК2 (клиенту) — 169.254.245.172.

На рисунках 18 и 19 изображены графики частот SYN- и PSH-флагов.

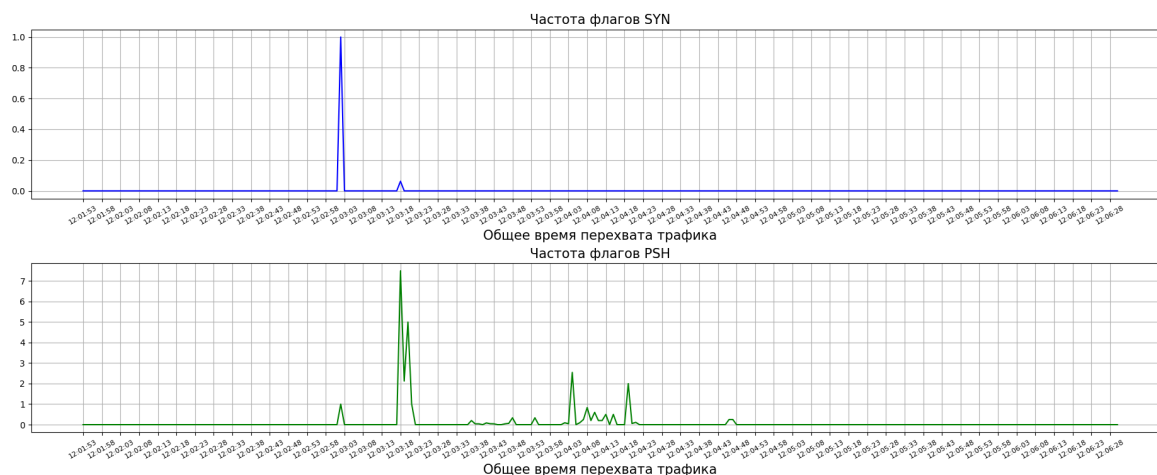


Рисунок 18 – График, построенный по формуле $r_{syn} = \frac{V_{Sin}}{V_{tcp}}$ относительно 169.254.245.172



Рисунок 19 – График, построенный по формуле $r_{psh} = \frac{V_{Pin}}{V_{tcp}}$ относительно 169.254.99.90

Исходя из количества PSN-флагов в момент времени 12:03:17 – 12:03:22, как показано на рисунке 18, на этом отрезке времени передаются также TCP-пакеты с установленным PSN-флагом, сигнализируя протоколу TCP отправить все данные, независимо от того, где и сколько их было уже передано.

По построенным графикам можно сделать несколько выводов. Например, из рисунка 14 отчетливо видно, что с 12:03:50 начинается рост значения V_{udp} , а значит увеличивается объем входящего UDP-трафика ПК2. Это можно аргументировать тем, что в этот момент времени происходят различные операции, сделанные на рабочем столе ПК1. В данном случае были произведены движения мышкой.

Также из рисунков 11 и 12 видно, что обмен данными между ПК1 и ПК2 прерывается в 12:04:51. Тогда можно предположить, что именно в это время закончилась RDP-сессия.

ЗАКЛЮЧЕНИЕ

В результате проделанной работы были разобраны методы обнаружения подключения к удаленному рабочему столу по протоколу RDP, где с помощью различных программ удалось рассмотреть принцип работы RDP-протокола. Стоит отметить, что хоть RDP далеко не самый защищенный протокол, его обнаружение может стать затруднительным, особенно когда производится подключение к удаленному рабочему столу в реальных условиях с выходом в интернет. И для его анализа обычного перехвата трафика будет недостаточно. Однако, благодаря различным метрикам и построенным по ним графикам, по которым анализируют сетевые атаки, можно получить полезную информацию. Поэтому в дальнейшем, опираясь на проделанную работу, будут совершены попытки выявления протокола RDP от всех прочих протоколов сети интернет путем анализа данных по построенным графикам.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Книга Ибе О.С. «Компьютерные сети и службы удаленного доступа» / пер. с англ. - Москва, издательство: «ДМК Пресс», Яз. рус.
- 2 Удалённый рабочий стол RDP: как включить и как подключиться по RDP [Электронный ресурс] / URL:<https://hackware.ru/?p=11835> (дата обращения 03.05.2022), Яз. рус.
- 3 How to use remote desktop [Электронный ресурс] / URL: <https://support.microsoft.com/en-us/windows/how-to-use-remote-desktop-5fe128d5-8fb1-7a23-3b8a-41e636865e8c> (дата обращения 27.05.2022), Яз. англ.
- 4 Статья «Как исправить ошибку удаленного рабочего стола не удастся подключиться к удаленному компьютеру» [Электронный ресурс] / URL: <https://okdk.ru/kak-ispravit-oshibku-udalennogo-rabochego-stola-ne-udaetsya-podkljuchitsya-k-udalennomu-kompjuteru/> (дата обращения 27.05.2022), Яз. рус.
- 5 Документация Remote Utilities «RDP» [Электронный ресурс] / URL: <https://www.remoteutilities.com/support/docs/rdp/> (дата обращения 27.05.2022), Яз. англ.
- 6 Документация по стандартным библиотекам языка Python [Электронный ресурс] / URL: <https://docs.python.org/3/library/socket.html> (дата обращения 25.06.2022), Яз. англ.
- 7 Статья «Интерактивная система просмотра системных руководств (man-ов)» [Электронный ресурс] / URL: <https://www.opennet.ru/cgi-bin/opennet/man.cgi?topic=socket&category=2> (дата обращения 25.06.2022), Яз. англ.
- 8 Документация Microsoft «Протоколы» [Электронный ресурс] / URL: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpeudp2/d8bf9a56-90f3-4608-8f98-9600ed69876b (дата обращения 28.05.2022), Яз. рус.
- 9 Статья «Wireshark Tutorial: Decrypting RDP Traffic» [Электронный ресурс] / URL: <https://unit42-paloaltonetworks-com.translate.goog/wireshark->

tutorial-decrypting-rdp-traffic/?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=op,wapp (дата обращения 28.05.2022), Яз. англ.

- 10 Статья «TCP flags» [Электронный ресурс] / URL: <https://www.keycdn.com/support/tcp-flags#:~:text=ACK> (дата обращения 02.10.2022), Яз. англ.
- 11 Статья «Модель OSI» [Электронный ресурс] / URL: http://neerc.ifmo.ru/wiki/index.php?title=OSI_Model (дата обращения 13.10.2022), Яз. рус.

ПРИЛОЖЕНИЕ А

Код sniffer.py

```
1  import socket, struct
2  import os, time
3  import keyboard
4
5
6  # Получение ethernet-кадра
7  def get_ethernet_frame(data):
8      dest_mac, src_mac, proto = struct.unpack('!6s6sH', data[:14])
9      return get_mac_addr(dest_mac), get_mac_addr(src_mac), socket.htons(proto)
10
11
12  # Получение MAC-адреса
13  def get_mac_addr(mac_bytes):
14      mac_str = ''
15      for el in mac_bytes:
16          mac_str += format(el, '02x').upper() + ':'
17      return mac_str[:len(mac_str) - 1]
18
19
20  # Получение IPv4-заголовка
21  def get_ipv4_data(data):
22      version_header_length = data[0]
23      header_length = (version_header_length & 15) * 4
24      ttl, proto, src, dest = struct.unpack('!8xBB2x4s4s', data[:20])
25      return str(ttl), proto, ipv4_dec(src), ipv4_dec(dest), data[header_length:]
26
27
28  # Получение IP-адреса формата X.X.X.X
29  def ipv4_dec(ip_bytes):
30      ip_str = ''
31      for el in ip_bytes:
32          ip_str += str(el) + '.'
33      return ip_str[:-1]
34
35
36  # Получение UDP-сегмента данных
37  def get_udp_segment(data):
38      src_port, dest_port, size = struct.unpack('!HH2xH', data[:8])
39      return str(src_port), str(dest_port), str(size), data[8:]
40
41
42  # Получение TCP-сегмента данных
43  def get_tcp_segment(data):
44      src_port, dest_port, sequence, ack, some_block = struct.unpack('!HLLH', data[:14])
45      return str(src_port), str(dest_port), str(sequence), str(ack), \
46          some_block, data[(some_block >> 12) * 4:]
```

```

47
48
49 # Форматирование данных для корректного представления
50 def format_data(data):
51     if isinstance(data, bytes):
52         data = ''.join(r'\x{:02x}'.format(el) for el in data)
53     return data
54
55
56 # Перехват трафика и вывод информации в консоль
57 def start_to_listen(s_listen):
58     NumPacket = 1
59     while True:
60         # Получение пакетов в виде набора hex-чисел
61         raw_data, _ = s_listen.recvfrom(65565)
62         arr_data = [''] * 17
63         arr_data[0], arr_data[1] = str(NumPacket), str(time.time())
64         arr_data[2] = str(len(raw_data))
65         # Если это интернет-протокол четвертой версии
66         arr_data[4], arr_data[3], protocol = get_ethernet_frame(raw_data)
67         if protocol == 8:
68             print(f'-----Пакет N{NumPacket}-----')
69             NumPacket += 1
70             print('Ethernet кадр: ')
71             print( 'MAC-адрес отправителя: ' + arr_data[3]
72                   , 'MAC-адрес получателя: ' + arr_data[4] )
73             ttl, proto, arr_data[6], arr_data[7], data_ipv4 = get_ipv4_data(raw_data[14:])
74             print('IPv4 заголовок:')
75             print( 'TTL: ' + ttl
76                   , 'Номер протокола: ' + str(proto)
77                   , 'IP-адрес отправителя: ' + arr_data[6]
78                   , 'IP-адрес получателя: ' + arr_data[7])
79             # Если это UDP-протокол
80             if proto == 17:
81                 arr_data[5] = 'UDP'
82                 arr_data[8], arr_data[9], length, data_udp = get_udp_segment(data_ipv4)
83                 print('UDP заголовок:')
84                 print( 'Порт отправителя: ' + arr_data[8], 'Порт получателя: ' +
85                       arr_data[9], 'Длина: ' + length )
86                 arr_data[10], arr_data[11] = str(len(data_udp)), format_data(data_udp)
87                 write_to_file(arr_data)
88             # Если это TCP-протокол
89             if proto == 6:
90                 arr_data[5] = 'TCP'
91                 arr_data[8], arr_data[9], arr_data[10], \
92                 arr_data[11], flags, data_tcp = get_tcp_segment(data_ipv4)
93                 fl_urg = str((flags & 32) >> 5)
94                 fl_ack = str((flags & 16) >> 4)

```

```

95     fl_psh = str((flags & 8) >> 3)
96     fl_rst = str((flags & 4) >> 2)
97     fl_syn = str((flags & 2) >> 1)
98     fl_fin = str(flags & 1)
99     print('TCP заголовок:')
100    print( 'Порт отправителя: ' + arr_data[8]
101           , 'Порт получателя: ' + arr_data[9]
102           , 'Порядковый номер: ' + arr_data[10]
103           , 'Номер подтверждения: ' + arr_data[11] )
104    print('Флаги:')
105    print( 'URG: ' + fl_urg, 'ACK: ' + fl_ack, 'PSH: ' + fl_psh
106           , 'RST: ' + fl_rst, 'SYN: ' + fl_syn, 'FIN: ' + fl_fin )
107    arr_data[12], arr_data[13], arr_data[14] = fl_ack, fl_psh, fl_syn
108    arr_data[15], arr_data[16] = str(len(data_tcp)), format_data(data_tcp)
109    write_to_file(arr_data)
110    if keyboard.is_pressed('space'):
111        s_listen.close()
112        print('Завершение программы...')
113        break
114
115
116    # Запись в файл
117    def write_to_file(a):
118        try:
119            with open('data.log', 'a') as f:
120                if a[5] == 'TCP':
121                    f.write( 'No: ' + a[0] + ';' + 'Time: ' + a[1] + ';' +
122                             'Pac-size: ' + a[2] + ';' + 'MAC-src: ' + a[3] + ';' +
123                             'MAC-dest: ' + a[4] + ';' + 'Type: ' + a[5] + ';' +
124                             'IP-src: ' + a[6] + ';' + 'IP-dest: ' + a[7] + ';' +
125                             'Port-src: ' + a[8] + ';' + 'Port-dest: ' + a[9] + ';' +
126                             'Seq: ' + a[10] + ';' + 'Ack: ' + a[11] + ';' +
127                             'Fl-ack: ' + a[12] + ';' + 'Fl-psh: ' + a[13] + ';' +
128                             'Fl-syn: ' + a[14] + ';' + 'Len-data: ' + a[15] + ';' +
129                             'Data: ' + a[16] + ';\n')
130                else:
131                    f.write( 'No: ' + a[0] + ';' + 'Time: ' + a[1] + ';' +
132                             'Pac-size: ' + a[2] + ';' + 'MAC-src: ' + a[3] + ';' +
133                             'MAC-dest: ' + a[4] + ';' + 'Type: ' + a[5] + ';' +
134                             'IP-src: ' + a[6] + ';' + 'IP-dest: ' + a[7] + ';' +
135                             'Port-src: ' + a[8] + ';' + 'Port-dest: ' + a[9] + ';' +
136                             'Len-data: ' + a[10] + ';' + 'Data: ' + a[11] + ';\n')
137            f.close()
138        except:
139            print('Ошибка записи в файл...')
140            pass
141
142

```

```
143 # Осуществление запуска программы
144 if __name__ == '__main__':
145     print('\nЗапуск программы....\n')
146
147     print('Выберите сетевой интерфейс, нажав соответствующую цифру:')
148     print(socket.if_nameindex())
149     interface = int(input())
150     os.system(f'ip link set {socket.if_indextoname(interface)} promisc on')
151     s_listen = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.ntohs(3))
152     start_to_listen(s_listen)
```

ПРИЛОЖЕНИЕ Б

Код data-analysis.py

```
1  import matplotlib.pyplot as plt
2  import matplotlib.gridspec as gridspec
3  import time
4  from colorama import init, Back, Fore
5
6  init(autoreset=True)
7  FileName = ''
8  Packet_list = []
9  Object_list = []
10 Labels_list = []
11 x_axisLabels = []
12
13 # Класс, содержащий информацию о каком-либо пакете
14 class PacketInf:
15
16     def __init__( self, numPacket, timePacket, packetSize, mac_src, mac_dest, protoType
17                   , ip_src, ip_dest, port_src, port_dest, len_data, data
18                   , seq=None, ack=None, fl_ack=None, fl_psh=None, fl_syn=None):
19         self.numPacket = int(numPacket)
20         self.timePacket = float(timePacket)
21         self.packetSize = int(packetSize)
22         self.mac_src = mac_src
23         self.mac_dest = mac_dest
24         self.ip_src = ip_src
25         self.ip_dest = ip_dest
26         self.port_src = port_src
27         self.port_dest = port_dest
28         self.len_data = int(len_data)
29         self.data = data
30         self.protoType = protoType
31         self.seq = seq
32         self.ack = ack
33         self.fl_ack = fl_ack
34         self.fl_psh = fl_psh
35         self.fl_syn = fl_syn
36
37
38 # Класс, содержащий информацию относительно какого-либо IP-адреса
39 class ExploreObject:
40
41     def __init__(self, ip):
42         self.ip = ip
43         self.strt_time = None
44         self.fin_time = None
45         self.amnt_packet = None
46         self.avg_packet_num = None
```



```

47     self.avg_packet_size = None
48
49     self.in_out_rel_data = None
50     self.ack_flags_diff_data = None
51     self.udp_tcp_rel_data = None
52     self.syn_flags_freq_data = None
53     self.psh_flags_freq_data = None
54     self.adjcIPList = None
55     self.adjcPacketList = None
56
57
58 # Считывание с файла и заполнение массива
59 # Packet_list объектами класса PacketInf
60 def read_from_file(inf):
61     a = []
62     while True:
63         beg = inf.find(':')
64         end = inf.find(';')
65         if beg == -1 and end == -1:
66             break
67         else:
68             a.append(inf[beg + 1: end])
69             inf = inf[end + 1:]
70     try:
71         if a[5] == 'TCP':
72             Packet_list.append(PacketInf( a[0], a[1], a[2], a[3], a[4], a[5]
73                                           , a[6], a[7], a[8], a[9], a[15], a[16]
74                                           , a[10], a[11], a[12], a[13], a[14] ))
75         elif a[5] == 'UDP':
76             Packet_list.append(PacketInf( a[0], a[1], a[2], a[3], a[4], a[5]
77                                           , a[6], a[7], a[8], a[9], a[10], a[11] ))
78     except:
79         print('Ошибка при считывании файла...')
80         exit(0)
81
82 # Получение общей информации о текущей
83 # попытке перехвата трафика
84 def get_common_data():
85     IPList = []
86     numPacketsPerSec = []
87     curTime = Packet_list[0].timePacket + 1
88     fin = Packet_list[-1].timePacket + 1
89     Labels_list.append(time.strftime('%H:%M:%S', time.localtime(Packet_list[0].timePacket)))
90     cntPacket = 0
91     i = 0
92     while curTime < fin:
93         for k in range(i, len(Packet_list)):
94             if Packet_list[k].timePacket > curTime:

```

```

95         numPacketsPerSec.append(cntPacket)
96         Labels_list.append(time.strftime('%H:%M:%S', time.localtime(curTime)))
97         cntPacket = 0
98         i = k
99         break
100     cntPacket += 1
101     curTime += 1
102     numPacketsPerSec.append(cntPacket)
103     for p in Packet_list:
104         CurIP = p.ip_src
105         if CurIP not in IPList:
106             IPList.append(CurIP)
107     return IPList, numPacketsPerSec
108
109
110 # Получение данных об отношении входящего
111 # трафика к исходящему в единицу времени
112 def get_in_out_rel(exploreIP, strt, fin):
113     cntInput = 0
114     cntOutput = 0
115     rel_list = []
116     curTime = strt + 1
117     fin += 1
118     pos = 0
119     while curTime < fin:
120         for k in range(pos, len(Packet_list)):
121             if Packet_list[k].timePacket > curTime:
122                 if cntOutput != 0:
123                     rel_list.append(cntInput / cntOutput)
124                 else:
125                     rel_list.append(0.0)
126                 cntInput = 0
127                 cntOutput = 0
128                 pos = k
129                 break
130             if Packet_list[k].ip_src == exploreIP:
131                 cntOutput += 1
132             if Packet_list[k].ip_dest == exploreIP:
133                 cntInput += 1
134         curTime += 1
135     if cntOutput != 0:
136         rel_list.append(cntInput / cntOutput)
137     else:
138         rel_list.append(0.0)
139     return rel_list
140
141
142 # Получение данных о разности количества

```

```

143 # исходящих ACK-флагов и количества входящих
144 # ACK-флагов
145 def get_ack_flags_diff(exploreIP, strt, fin):
146     cntInput = 0
147     cntOutput = 0
148     diff_list = []
149     curTime = strt + 1
150     fin += 1
151     pos = 0
152     while curTime < fin:
153         for k in range(pos, len(Packet_list)):
154             if Packet_list[k].timePacket > curTime:
155                 diff_list.append(cntOutput - cntInput)
156                 cntInput = 0
157                 cntOutput = 0
158                 pos = k
159                 break
160             if Packet_list[k].protoType == 'TCP' and Packet_list[k].fl_ack == '1':
161                 if Packet_list[k].ip_src == exploreIP:
162                     cntOutput += 1
163                 if Packet_list[k].ip_dest == exploreIP:
164                     cntInput += 1
165             curTime += 1
166     diff_list.append(cntOutput - cntInput)
167     return diff_list
168
169
170 # Получение данных об отношении количества
171 # входящего UDP-трафика на количество
172 # исходящего TCP-трафика в единицу времени
173 def get_udp_tcp_rel(exploreIP, strt, fin):
174     cntUDP = 0
175     cntTCP = 0
176     curTime = strt + 1
177     fin += 1
178     pos = 0
179     rel_list = []
180     while curTime < fin:
181         for k in range(pos, len(Packet_list)):
182             if Packet_list[k].timePacket > curTime:
183                 if cntTCP != 0:
184                     rel_list.append(cntUDP / cntTCP)
185                 else:
186                     rel_list.append(0.0)
187                 cntTCP = 0
188                 cntUDP = 0
189                 pos = k
190                 break

```

```

191         if Packet_list[k].ip_dest == exploreIP:
192             if Packet_list[k].protoType == 'TCP':
193                 cntTCP += 1
194             if Packet_list[k].protoType == 'UDP':
195                 cntUDP += 1
196         curTime += 1
197     if cntTCP != 0:
198         rel_list.append(cntUDP / cntTCP)
199     else:
200         rel_list.append(0.0)
201     return rel_list
202
203
204     # Получение данных о частоте SYN-флагов
205 def get_syn_flags_freq(exploreIP, strt, fin):
206     cntSynTCP = 0
207     cntTCP = 0
208     rel_list = []
209     curTime = strt + 1
210     fin += 1
211     pos = 0
212     while curTime < fin:
213         for k in range(pos, len(Packet_list)):
214             if Packet_list[k].timePacket > curTime:
215                 if cntTCP != 0:
216                     rel_list.append(cntSynTCP / cntTCP)
217                 else:
218                     rel_list.append(0.0)
219                 cntSynTCP = 0
220                 cntTCP = 0
221                 pos = k
222                 break
223             if Packet_list[k].ip_dest == exploreIP and Packet_list[k].protoType == 'TCP':
224                 if Packet_list[k].fl_syn == '1':
225                     cntSynTCP += 1
226                 else:
227                     cntTCP += 1
228             curTime += 1
229     if cntTCP != 0:
230         rel_list.append(cntSynTCP / cntTCP)
231     else:
232         rel_list.append(0.0)
233     return rel_list
234
235
236     # Получение данных о частоте PSH-флагов
237 def get_psh_flags_freq(exploreIP, strt, fin):
238     cntPshTCP = 0

```

```

239     cntTCP = 0
240     rel_list = []
241     curTime = strt + 1
242     fin += 1
243     pos = 0
244     while curTime < fin:
245         for k in range(pos, len(Packet_list)):
246             if Packet_list[k].timePacket > curTime:
247                 if cntTCP != 0:
248                     rel_list.append(cntPshTCP / cntTCP)
249                 else:
250                     rel_list.append(0.0)
251                 cntPshTCP = 0
252                 cntTCP = 0
253                 pos = k
254                 break
255             if Packet_list[k].ip_dest == exploreIP and Packet_list[k].protoType == 'TCP':
256                 if Packet_list[k].fl_psh == '1':
257                     cntPshTCP += 1
258                 else:
259                     cntTCP += 1
260             curTime += 1
261         if cntTCP != 0:
262             rel_list.append(cntPshTCP / cntTCP)
263         else:
264             rel_list.append(0.0)
265     return rel_list
266
267
268     # Получение общей информации о трафике,
269     # связанном с выбранным IP-адресом
270     def get_inf_about_IP(exploreIP):
271         adjcPacketList = []
272         adjcIPList = []
273         for p in Packet_list:
274             if p.ip_src == exploreIP:
275                 adjcPacketList.append(p)
276                 adjcIPList.append(p.ip_dest)
277             if p.ip_dest == exploreIP:
278                 adjcPacketList.append(p)
279                 adjcIPList.append(p.ip_src)
280         return adjcPacketList, adjcIPList
281
282
283     # Вывод пакетов, связанных с выбранным IP-адресом
284     def print_adjacent_packets(adjcPacketList):
285         cnt = 0
286         for p in adjcPacketList:

```

```

287     t = time.strftime('%H:%M:%S', time.localtime(p.timePacket))
288     if cnt % 2 == 1:
289         print( f'Номер пакета: {p.numPacket};', f'Время: {t};'
290             , f'Размер: {p.packetSize};', f'MAC-адрес отправителя: {p.mac_src};'
291             , f'MAC-адрес получателя: {p.mac_dest};'
292             , f'IP-адрес отправителя: {p.ip_src};', f'IP-адрес получателя: {p.ip_dest};'
293             , f'Протокол: {p.protoType};', f'Порт отправителя: {p.port_src};'
294             , f'Порт получателя: {p.port_dest};', f'Количество байт: {p.len_data};' )
295     else:
296         print( Back.CYAN + Fore.BLACK + f'Номер пакета: {p.numPacket};' + f' Время: {t};' +
297             f' Размер: {p.packetSize};' + f' MAC-адрес отправителя: {p.mac_src};' +
298             f' MAC-адрес получателя: {p.mac_dest};' +
299             f' IP-адрес отправителя: {p.ip_src};' + f' IP-адрес получателя: {p.ip_dest};' +
300             f' Протокол: {p.protoType};' + f' Порт отправителя: {p.port_src};' +
301             f' Порт получателя: {p.port_dest};' + f' Количество байт: {p.len_data};' )
302     cnt += 1
303
304
305     # Вывод пар (число, IP-адрес) для
306     # предоставления выбора IP-адреса
307     # пользователю
308     def print_IP_list(IPList):
309         num = 0
310         cnt = 1
311         for el in IPList:
312             if cnt > 3:
313                 cnt = 0
314                 print ( '[' + str(num), '---', el, end=']\n' )
315             else:
316                 print ( '[' + str(num), '---', el, end='] ' )
317             cnt += 1
318             num += 1
319
320
321     # Получение меток и "шага" для оси абсцисс
322     def get_x_labels(total_time):
323         step = 1
324         if total_time > 500:
325             step = 8
326         elif total_time > 100:
327             step = 5
328         elif total_time > 50:
329             step = 2
330         for i in range(0, len(Labels_list), step):
331             x_axisLabels.append(Labels_list[i])
332         return step
333
334

```

```

335 # Выбор опций для выбранного IP-адреса
336 def choose_options(k, strt, fin, step):
337     curIP = Object_list[k].ip
338     if Object_list[k].adjcPacketList == None:
339         Object_list[k].adjcPacketList, Object_list[k].adjcIPList = get_inf_about_IP(curIP)
340     if Object_list[k].strt_time == None:
341         Object_list[k].strt_time = time.localtime(Object_list[k].adjcPacketList[0].timePacket)
342     if Object_list[k].fin_time == None:
343         Object_list[k].fin_time = time.localtime(Object_list[k].adjcPacketList[-1].timePacket)
344     if Object_list[k].amnt_packet == None:
345         Object_list[k].amnt_packet = len(Object_list[k].adjcPacketList)
346     if Object_list[k].avg_packet_num == None:
347         tmp = Object_list[k].adjcPacketList[-1].timePacket - \
348             Object_list[k].adjcPacketList[0].timePacket
349         if tmp == 0:
350             tmp = 1
351         Object_list[k].avg_packet_num = round(Object_list[k].amnt_packet / tmp, 3)
352     if Object_list[k].avg_packet_size == None:
353         avgSize = 0
354         for p in Object_list[k].adjcPacketList:
355             avgSize += p.len_data
356         Object_list[k].avg_packet_size = round(avgSize / Object_list[k].amnt_packet, 3)
357     while True:
358         print(f'Общая информация о трафике, связанном с {curIP}')
359         print( 'Время первого перехваченного пакета: '
360             , time.strftime('%d.%m.%Y г. %H:%M:%S', Object_list[k].strt_time) )
361         print( 'Время последнего перехваченного пакета: '
362             , time.strftime('%d.%m.%Y г. %H:%M:%S', Object_list[k].fin_time) )
363         print('Количество пакетов: ', Object_list[k].amnt_packet)
364         print('Среднее количество пакетов в секунду: ', Object_list[k].avg_packet_num)
365         print('Средний размер пакетов: ', Object_list[k].avg_packet_size)
366         print(f""""Выберите опцию:
367         1. Вывести весь трафик, связанный с {curIP}
368         2. Построить график отношения входящего и исходящего трафиков
369         3. Построить график отношения объема входящего UDP-трафика и объема входящего TCP-трафика
370         4. Построить график разности числа исходящих и числа входящих ACK-флагов в единицу времени
371         5. Построить график частоты SYN и PSN флагов во входящих пакетах
372         6. Вернуться к выбору IP-адреса """)
373         b1 = input()
374         if b1 == '1':
375             print_adjacent_packets(Object_list[k].adjcPacketList)
376         elif b1 == '2':
377             if Object_list[k].in_out_rel_data == None:
378                 data = get_in_out_rel(curIP, strt, fin)
379                 Object_list[k].in_out_rel_data = data
380             x = [i for i in range(0, len(Object_list[k].in_out_rel_data))]
381             x_labels = [i for i in range(0, len(x), step)]
382             fig = plt.figure(figsize=(16, 6), constrained_layout=True)

```

```

383     f = fig.add_subplot()
384     f.grid()
385     f.set_title('Отношение объема входящего к объему исходящего трафика', fontsize=15)
386     f.set_xlabel('Общее время перехвата трафика', fontsize=15)
387     plt.plot(x, Object_list[k].in_out_rel_data)
388     plt.xticks(x_labels, x_axisLabels, rotation=30)
389     plt.show()
390 elif bl == '3':
391     if Object_list[k].udp_tcp_rel_data == None:
392         data = get_udp_tcp_rel(curIP, strt, fin)
393         Object_list[k].udp_tcp_rel_data = data
394     x = [i for i in range(0, len(Object_list[k].udp_tcp_rel_data))]
395     x_labels = [i for i in range(0, len(x), step)]
396     fig = plt.figure(figsize=(16, 6), constrained_layout=True)
397     f = fig.add_subplot()
398     f.grid()
399     f.set_title('Отношение объема входящего UDP-трафика к объему входящего TCP-трафика'
400               , fontsize=15)
401     f.set_xlabel('Общее время перехвата трафика', fontsize=15)
402     plt.plot(x, Object_list[k].udp_tcp_rel_data)
403     plt.xticks(x_labels, x_axisLabels, rotation=30)
404     plt.show()
405 elif bl == '4':
406     if Object_list[k].ack_flags_diff_data == None:
407         data = get_ack_flags_diff(curIP, strt, fin)
408         Object_list[k].ack_flags_diff_data = data
409     x = [i for i in range(0, len(Object_list[k].ack_flags_diff_data))]
410     x_labels = [i for i in range(0, len(x), step)]
411     fig = plt.figure(figsize=(16, 6), constrained_layout=True)
412     f = fig.add_subplot()
413     plt.plot(x, Object_list[k].ack_flags_diff_data)
414     f.grid()
415     f.set_title('Разность числа исходящих и числа входящих АСК-флагов', fontsize=15)
416     f.set_xlabel('Общее время перехвата трафика', fontsize=15)
417     plt.xticks(x_labels, x_axisLabels, rotation=30)
418     plt.show()
419 elif bl == '5':
420     if Object_list[k].syn_flags_freq_data == None:
421         data = get_syn_flags_freq(curIP, strt, fin)
422         Object_list[k].syn_flags_freq_data = data
423     if Object_list[k].psh_flags_freq_data == None:
424         data = get_psh_flags_freq(curIP, strt, fin)
425         Object_list[k].psh_flags_freq_data = data
426     x = [i for i in range(0, len(Object_list[k].syn_flags_freq_data))]
427     x_labels = [i for i in range(0, len(x), step)]
428     fig = plt.figure(figsize=(16, 6), constrained_layout=True)
429     gs = gridspec.GridSpec(ncols=1, nrows=2, figure=fig)
430     fig_1 = fig.add_subplot(gs[0, 0])

```



```

431     fig_1.grid()
432     plt.plot(x, Object_list[k].syn_flags_freq_data, 'b')
433     plt.xticks(x_labels, x_axisLabels, rotation=30, fontsize=8)
434     fig_2 = fig.add_subplot(gs[1, 0])
435     fig_2.grid()
436     plt.plot(x, Object_list[k].psh_flags_freq_data, 'g')
437     plt.xticks(x_labels, x_axisLabels, rotation=30, fontsize=8)
438     fig_1.set_title('Частота флагов SYN', fontsize=15)
439     fig_1.set_xlabel('Общее время перехвата трафика', fontsize=15)
440     fig_2.set_title('Частота флагов PSH', fontsize=15)
441     fig_2.set_xlabel('Общее время перехвата трафика', fontsize=15)
442     plt.show()
443     elif bl == '6':
444         break
445
446
447 if __name__ == '__main__':
448     print('Введите название файла (например: data.log)')
449     FileName = input()
450     while True:
451         if not Packet_list:
452             try:
453                 f = open(FileName, 'r')
454             except:
455                 print('Некорректное название файла!')
456                 exit(0)
457             while True:
458                 inf = f.readline()
459                 if not inf:
460                     break
461                 read_from_file(inf)
462             f.close()
463             IPList, numPacketsPerSec = get_common_data()
464             strt = Packet_list[0].timePacket
465             fin = Packet_list[-1].timePacket
466             strt_time = time.localtime(strt)
467             fin_time = time.localtime(fin)
468             avgNumPacket = 0
469             for el in numPacketsPerSec:
470                 avgNumPacket += el
471             avgNumPacket /= len(numPacketsPerSec)
472             avgSizePacket = 0
473             for p in Packet_list:
474                 avgSizePacket += p.packetSize
475             avgSizePacket /= len(Packet_list)
476             step = get_x_labels(int(fin - strt))
477
478     print('Общая информация:')

```

```

479     print( 'Время первого перехваченного пакета: '
480           , time.strftime('%d.%m.%Y г. %H:%M:%S', strt_time) )
481     print( 'Время последнего перехваченного пакета: '
482           , time.strftime('%d.%m.%Y г. %H:%M:%S', fin_time) )
483     print('Количество пакетов: ', len(Packet_list))
484     print('Общее время перехвата: ', round(fin - strt, 3), 'сек')
485     print('Среднее количество пакетов в секунду: ', round(avgNumPacket, 3))
486     print('Средний размер пакетов: ', round(avgSizePacket, 3))
487     print('Завершить просмотр (нажмите \"q\" для выхода)')
488     for k in range(0, len(IPList)):
489         Object_list.append(ExploreObject(IPList[k]))
490     print_IP_list(IPList)
491     print(f'\nВыберите цифру (0 - {len(IPList) - 1}) для просмотра IP-адреса:')
492     k = input()
493     if k == 'q':
494         break
495     try:
496         k = int(k)
497     except:
498         print('Некорректный ввод')
499     else:
500         if 0 <= k < len(IPList):
501             choose_options(k, strt, fin, step)
502         else:
503             print(f'Введите число в пределах 0 - {len(IPList) - 1}')

```