**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет ИКСС f

Кафедра ЗСС р

*Допустить к защите*

Заведующий кафедрой

\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(подпись)*  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

Разработка комплекса лабораторных работ по обнаружению компьютерных атак при помощи анализатора сетевых пакетов Packetbeat

*(тема ВКР)*

Направление/специальность подготовки

10.03.01 - Информационная безопасность л

*(код и наименование направления/специальности)*

Направленность (профиль)

Информационная безопасность л

*(наименование)*

Квалификация Бакалавр л

*(наименование квалификации в соответствии с ФГОС ВО)*

Студент:

Шестакова В.А., ИКБ-81 д \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Научный руководитель:

Скорых М.А. б \_\_\_\_\_\_\_\_\_

*(учёная степень, учёное звание, Ф.И.О.)(подпись)*

Санкт-Петербург, 2022

*Оборотная сторона титульного листа*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*работа написана мною самостоятельно*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*работа не содержит неправомерных заимствований*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*работа может быть размещена в электронно-библиотечной системе университета*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(дата) (подпись) (ФИО студента)*

Текст ВКР размещен в электронно-библиотечной системе университета.

Руководитель отдела комплектования библиотеки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(Ф.И.О.)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(дата) (подпись)*

Коэффициент оригинальности ВКР \_\_\_\_\_\_\_\_ % .

Проверил: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(Должность, Ф.И.О.)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(дата) (подпись)*

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет ИКСС д Кафедра ЗСС л

Направление (специальность) 10.03.01 - Информационная безопасность р

(код и наименование)

**Утверждаю:**

Зав. кафедрой\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О., подпись)

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ г.

**ЗАДАНИЕ**

**на выполнение выпускной квалификационной работы (ВКР)**

1. Студент Шестакова Валерия Алексеевна № группы ИКБ-81 л

(фамилия, имя, отчество)

2. Руководитель Скорых Марк Андреевич, ассистент кафедры ЗСС д

(фамилия, имя, отчество, должность, уч. степень и звание)

3. Квалификация Бакалавр д

(наименование в соответствии с ФГОС ВО)

4. Тема ВКР Разработка комплекса лабораторных работ по обнаружению компьютерных атак при помощи анализатора сетевых пакетов Packetbeat л

h h

утверждена приказом ректора университета от « 15 » 04 2022 г. № 418/кс

5. Исходные данные (технические требования): виртуальная машина с предустановленной операционной системой Ubuntu, доступ в Интернет, VPN, CPU 4+, RAM 8 Gb l

;

6. Содержание работы (анализ состояния проблемы, проведение исследований, разработка, расчеты параметров, экономическое обоснование и др.)

КОМПЬЮТЕРНЫЕ АТАКИ И СРЕДСТВА АНАЛИЗА ТРАФИКА k

РЕАЛИЗАЦИЯ ЛАБОРАТОРНОГО СТЕНДА k

РАЗРАБОТКА ЛАБОРАТОРНЫХ РАБОТ k

7. Вид отчетных материалов, представляемых в ГЭК (пояснительная записка, перечень, графического материала, отчет о НИР, технический проект, образцы и др.):

1. Пояснительная записка п

2. Презентация а

3. Диск с электронным вариантом ВКР р

8. Консультанты по ВКР с указанием относящихся к ним разделов

|  |  |  |  |
| --- | --- | --- | --- |
| Раздел | Консультант | Подпись дата | |
| Задание  выдал | Задание  принял |
| 1. Компьютерные атаки и средства анализа трафика | Скорых М.А. | 20.04.2022 | 01.05.2022 |
| 2. Реализация лабораторного стенда | Скорых М.А. | 01.05.2022 | 15.05.2022 |
| 3. Разработка лабораторных работ | Скорых М.А. | 15.05.2022 | 01.06.2022 |

Дата выдачи задания « 20 » 04 2022 г.

Дата представления ВКР к защите « 08 » 06 2022 г.

*Руководитель* *ВКР\_*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

*Студент*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

**КАЛЕНДАРНЫЙ ПЛАН[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Наименование этапов выпускной квалификационной работы (ВКР) | Срок выполнения этапов ВКР | Примечание |
| 1. | Постановка цели выполнения ВКР и задач | 20.04.2022 |  |
| 2. | Работа с теоретическим материалом | 20.04.2022  –  01.06.2022 |  |
| 3. | Сбор информации, необходимой для написания работы |  |
| 4. | Систематизация и обработка материалов ВКР |  |
| 5. | Анализ полученных в работе результатов, обобщение |  |
| 6. | Подготовка отчетных материалов, представляемых в государственную экзаменационную комиссию, доклада к защите и презентации | 01.06.2022  *-*  08.06.2022 |  |
| 7. | Консультации с руководителем ВКР |  |
| 8. | Представление выполненной ВКР руководителю для подготовки отзыва |  |
| 9. | Подготовка к защите ВКР, включая подготовку к процедуре защиты и процедуру защиты |  |

*Студент*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

*Руководитель ВКР*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

###### РЕФЕРАТ

В данной дипломной работе рассмотрена тема «Разработка лабораторных работ по обнаружению компьютерных атак при помощи анализатора сетевых пакетов Packetbeat».

Дипломная работа содержит: 72 страницы, 27 рисунков, 3 таблицы, 3 приложения.

Ключевые слова: Packetbeat, Kibana, Elasticsearch, стек, компьютерные атаки, средства анализа

Целью данной работы является реализация алгоритма сбора сетевого трафика с удаленного устройства для последующего анализа этих данных.

В выпускной квалификационной работе представлены основные компоненты стека ELK для анализа сети, описана настройка программных продуктов и разработаны лабораторные работы. Приведен вариант разбора компьютерной атаки типа «Сетевое сканирование».

**СОДЕРЖАНИЕ**

[ПРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ 9](#_Toc104486954)

[ВВЕДЕНИЕ 11](#_Toc104486955)

[1 КОМПЬЮТЕРНЫЕ АТАКИ И СРЕДСТВА АНАЛИЗА ТРАФИКА 13](#_Toc104486956)

[1.1 Классификация компьютерных атак 13](#_Toc104486957)

[1.2 Современные решения для обнаружения компьютерных атак 16](#_Toc104486958)

[1.3 Средства анализа трафика 21](#_Toc104486959)

[1.4 Packetbeat инструмент анализа трафика 26](#_Toc104486960)

[2 РЕАЛИЗАЦИЯ ЛАБОРАТОРНОГО СТЕНДА 30](#_Toc104486961)

[2.1 Общее описание разработанного стенда 30](#_Toc104486962)

[2.2 Установка ELK – стека 34](#_Toc104486963)

[2.2.1 Установка распределённой поисковой системы 34](#_Toc104486964)

[2.2.2 Установка системы визуализации информации 35](#_Toc104486965)

[2.2.3 Установка и настройка анализатора сетевых пакетов 35](#_Toc104486966)

[2.3 Настройка Dashboard в Kibana 36](#_Toc104486967)

[2.3.1 Создание Index Pattern 36](#_Toc104486968)

[2.3.2 Создание карты 39](#_Toc104486969)

[2.3.3 Создание dashboard «Total Events» 42](#_Toc104486970)

[2.4 Разработка сценария автоматического анализа сетевого трафика с помощью Packetbeat 44](#_Toc104486971)

[3 РАЗРАБОТКА ЛАБОРАТОРНЫХ РАБОТ 48](#_Toc104486972)

[3.1 Описание лабораторной работы №1 «Установка ELK - стека» 48](#_Toc104486973)

[3.2 Описание лабораторной работы №2 «Определение IP адресов и стран участников сетевой сессии» 50](#_Toc104486974)

[3.3 Описание лабораторной работы №3 «Обнаружения сканирования узлов» 52](#_Toc104486975)

[ЗАКЛЮЧЕНИЕ 55](#_Toc104486976)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 56](#_Toc104486977)

[ПРИЛОЖЕНИЕ А 59](#_Toc104486978)

[ПРИЛОЖЕНИЕ Б 66](#_Toc104486979)

[ПРИЛОЖЕНИЕ В 72](#_Toc104486980)

# ПРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

AMQP (Advanced Message Queuing Protocol) - открытый протокол прикладного уровня для передачи сообщений между компонентами системы

Cassandra - распределённая система управления базами данных

DHCP (Dynamic Host Configuration Protocol) - протокол динамической настройки узла

DNS (Domain Name System) - система доменных имён

EDR - средства обнаружения компьютерных атак на конечных устройствах

ELK - это аббревиатура, используемая для описания стека из трех популярных проектов: Elasticsearch, Logstash и Kibana

HTTP (HyperText Transfer Protocol) - протокол передачи гипертекста

ICMP (Internet Control Message Protocol) - протокол межсетевых управляющих сообщений

IP (Internet Protocol) - никальный адрес, идентифицирующий устройство в интернете или локальной сети

MAC (Media Access Control) - уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet

Memcache - программное обеспечение, реализующее сервис кэширования данных в оперативной памяти на основе хеш-таблицы

MongoDB - документоориентированная система управления базами данных, не требующая описания схемы таблиц

Mysql (Structured Query Language) - свободная реляционная система управления базами данных

NDR - система анализа сетевого трафика нового поколения

NFS (Network File System) - протокол сетевого доступа к файловым системам

NGFW - межсетевые экраны нового поколения

NTA - системы анализа сетевого трафика

OSI (The Open Systems Interconnection model) — сетевая модель стека сетевых протоколов

PostgreSQL - свободная объектно-реляционная система управления базами данных

Redis (Remote Dictionary Server) - быстрое хранилище данных типа «ключ‑значение» в памяти с открытым исходным кодом

SDP (Session Description Protocol) - сетевой протокол прикладного уровня, предназначенный для описания сессии передачи потоковых данных

SIEM - системы мониторинга событий безопасности

SIP (Session Initiation Protoco) - протокол установления сеанса

TCP (Transmission Control Protocol) - протокол управления передачей

TLS (Transport Layer Security) - протокол защиты транспортного уровня

## **ВВЕДЕНИЕ**

Еще несколько десятилетий тому назад компьютерные системы были преимущественно однопользовательскими и обменивались информацией по несколько довольным ограниченным каналам.

Разработка нового принципа построения сети на основе коммутации пакетов позволили значительно повысить гибкость и живучесть систем. Жизнь в настоящее время невозможно представить без использования интернета и сетевого взаимодействия, в частности. Современные сети передачи данных объединяют различные технологические и информационные ресурсы организаций, а также представляют доступ к внешним ресурсам. Инфокоммуникационные технологии применяются повсеместно практически каждым человеком. Деятельность многих компаний зависит от глобальной сети Интернет.

Информация, передаваемая по каналам связи, и ресурсы систем ежедневно подвергаются нападению со стороны злоумышленников. Используемые сетевые атаки имеют различные направления воздействия. Существующие разнообразие программного обеспечения и операционных систем, имеющих в своем исполнении, может не явные, но уязвимости, дают злоумышленникам пространства для создания и воплощения своих идей. Количество и множество способов реализации сетевых атак невероятно велико, в связи с этим встает вопрос о безопасности информации на ресурсах и защите сети.

Актуальность темы обусловлена резко выросшей в последние годы атак на информационные ресурсы, что требует разработки эффективных способов защиты от них. Предотвращение атак - одна из самых сложных задач в области информационной безопасности. Большинство современных систем имеет распределённую структуру, в основе их архитектуры лежит использование сетевых технологий. И обеспечение работоспособности таких систем зависит от способности противостоять злонамеренным действиям, которые направлены на нарушение работы как самой сети, так и информационной системы, функционирующей ее рамках. В тоже время современные системы обнаружения вторжений и атак еще не совершены и недостаточно эффективны с точки зрения безопасности решений. Поэтому методы работы в это направление необходимы и актуальны.

Целью данной работы является реализация алгоритма сбора сетевого трафика с удаленного устройства для последующего анализа этих данных. Помимо этого, целью является написания программы скрипта, которая позволяет автоматизировать и упростить процесс обработки сетевого трафика. Выявление нежелательных событий позволяет своевременно уменьшить пагубность влияния или вовсе устранить проблему.

Задачами дипломной работы в связи с указанной целью являются:

* Изучить классификацию компьютерных атак
* Проанализировать средства анализа сетевого трафика
* Разработать стенд, реализующий захват и анализ сетевого трафика
* Автоматизировать процесс анализа данных

Практическая и теоретическая значимость работы обусловлена тем, что стенд, реализованный в процессе, может быть использован для получения полной картины обо всех событиях, происходящих в сети и выявления возможных компьютерных атак.

## **КОМПЬЮТЕРНЫЕ АТАКИ И СРЕДСТВА АНАЛИЗА ТРАФИКА**

## **Классификация компьютерных атак**

Универсальной классификации угроз не существует, потому что нет предела творческим способностям человека, и каждые день применяются новые способы проникновения в сеть, появляются новые вирусы, находятся новые изъяны в существующих программных и аппаратных сетевых продуктах.

Виды атак и их результат имеют значительные отличия друг от друга. Рисунок 1 иллюстрирует классификацию компьютерных угроз по категориям [5].

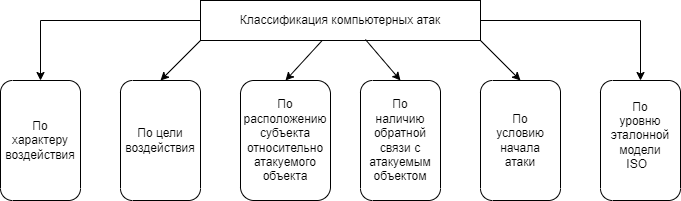


Рисунок 1 – Классификация компьютерных атак

Рассмотрим подробнее основные виды компьютерных атак по этим категориям.

**По характеру воздействия на сеть.**

Так различают пассивное и активное воздействие. Пассивное воздействие не оказывает прямого влияния на работу системы, но может нарушить ее политику безопасности [4]. Выявить пассивную атаку гораздо труднее как раз по причине недоступности прямого влияния. Примером такого воздействия может послужить компьютерная атака «ARP-spoofing».

Активное воздействие противоположно и оказывает прямое воздействие, нарушая работоспособность системы. Явным отличием активного воздействия от пассивного является возможность его обнаружить, так как происходят изменения в системе. На рисунке 2 представлены категории активных атак.

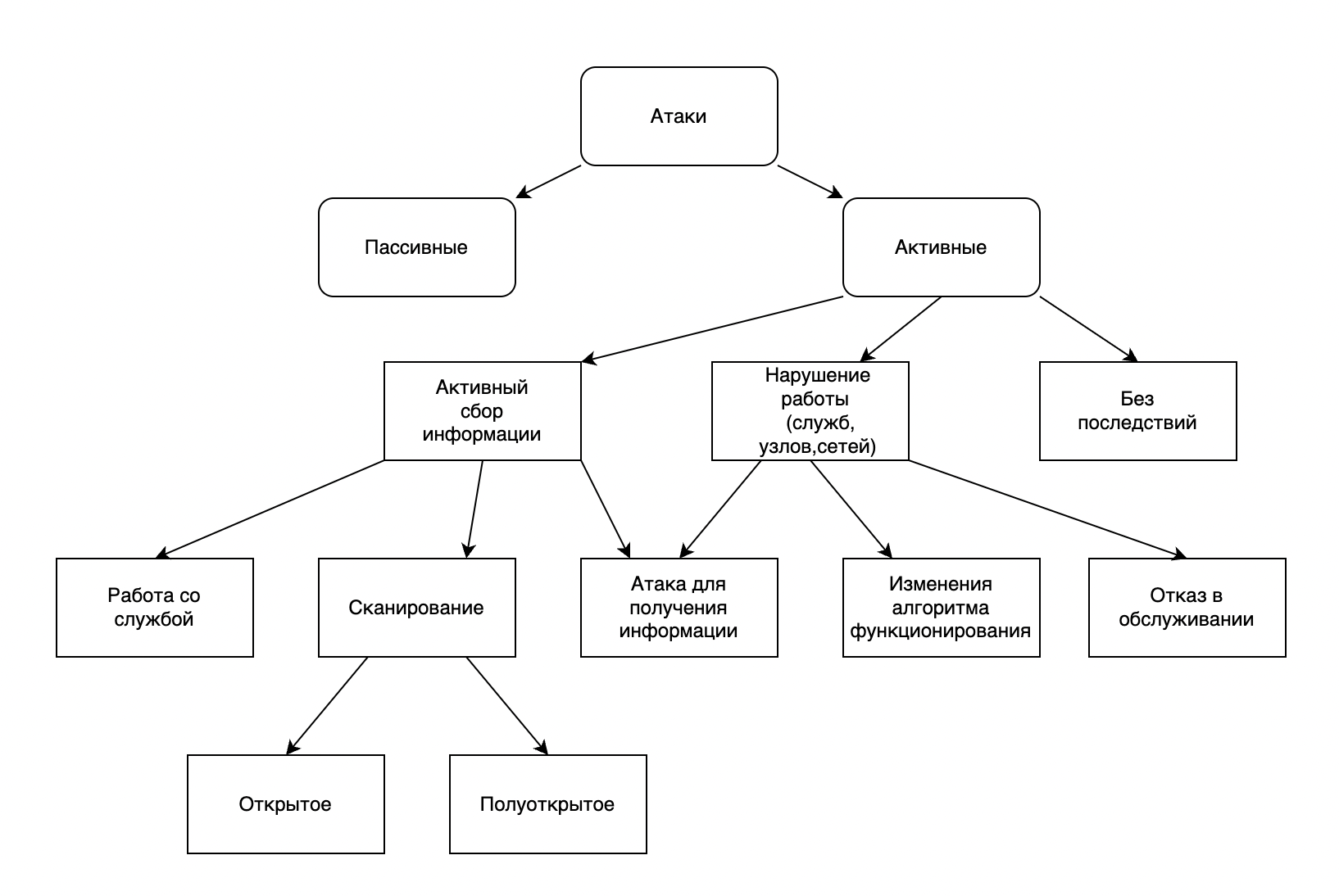
****

Рисунок 2 – Категории активных атак

**По цели воздействия.**

Данный признак описывает основные разновидности угроз:

* отказ в обслуживании;
* раскрытие целостности информации;
* нарушение целостности информации.

Одни нарушают функционирование системы и непосредственно сам доступ к ней, другие конфиденциальность и целостность информационных ресурсов, основной целью которых служит получение несанкционированного доступа к информации методом искажения или перехвата. В первом случае такое информационное нарушение имеет характер активного воздействия, так как сведения могут быть изменены. Во втором – доступ выполняется без изменения данных и поэтому имеет характер пассивного воздействия.

**По расположению субъекта относительно атакуемого объекта.**

По этому критерию различают атаки межсегментного и внутрисегментного типа. Особенностью категории межсегментного типа является расположение субъекта и объекта в различных разделах сети. Внутрисегментный тип характеризуется их расположением в одном разделе. Данный классификационный признак дает возможность судить о степени удаленности атаки. Намного легче осуществить внутрисегментную атаку, чем межсегментную, но вторая представляет куда большую опасность, чем первая, так как физическое расстояние между объектом атаки и атакующим может быть значительным, что сыграет отрицательную роль в отражении атаки.

**По наличию обратной связи с атакуемой сетью.**

Так же атаки можно классифицировать по наличию обратной связи с атакуемым объектом. Можно разделить атаки: с обратной связью и без обратной связи (однонаправленные атаки). Злоумышленник отправляет запросы на атакуемый объект и получает актуальные данные о состоянии сети.

Атаки без обратной связи отличительны тем, что им не требуется реагировать на изменения. Обычно они осуществляются отправкой одиночных запросов, ответы на которые не нужны.

**По условию начала компьютерной атаки.**

Существуют разные условия начала воздействия. Выделяют три критерия:

* По запросу от атакуемого объекта

В данной атаке воздействие со стороны злоумышленника начнется при передаче запроса определенного типа со стороны атакуемого.

* По выполнению на стороне объекта определенного действия

В данной ситуации злоумышленник наблюдает за состоянием операционной системы своей цели атаки и начинает осуществлять воздействие при появлении определенного события.

* Безусловные атаки.

Безусловные атаки происходят медленно и не опираются на состояние операционной системы и атакуемого объекта.

**По уровню эталонной модели OSI.**

Каждый сетевой протокол или сетевую программу можно спроецировать на эталонную семиуровневую модель взаимодействия открытых систем, что дает описание функций сетевого протокола или программы. Удаленная атака является сетевой программой, следовательно, можно рассмотреть ее по уровням эталонной модели OSI, на котором осуществляется взаимодействие. Данная модель включает в себя следующие уровни и виды атак:

* Физический уровень – повреждение кабеля, шум по всей полосе пропускания, электромагнитные помехи, импульсы напряжения, приводят к отказу в сервисе;
* Канальный уровень – переполнение таблиц коммутации, прослушивание, несанкционированная смена MAC – адреса и тд.;
* Сетевой уровень – подмена IP – адресов, модификация маршрутной таблицы, фрагментация и тд.;
* Транспортный уровень – подмена порта отправителя, перехват TCP – соединений, использование нестандартных комбинаций флагов и параметров TCP;
* Прикладной уровень – отправление кеша DNS, подмена идентификатора пользователя, подбор пароля, использование ошибок программного обеспечения.

## **Современные решения для обнаружения компьютерных атак**

Если бы не было уязвимостей в компонентах информационных сетей, то нельзя было бы реализовать множество атак и традиционные средства защиты справлялись бы с возможными угрозами. Скоординированные атаки сильно понижают эффективность межсетевых экранов и других защитных систем. Появляются новые технологии обнаружения и предотвращения атак, работа которых состоит в постоянной диагностике активности информационной системы. При обнаружении подозрительной активности определенные механизмы начинают свою работу по предотвращению и подаче сигналов определенным лицам [21].

Технология обнаружения атак должна решать задачи по распознанию известных атак и предупреждению соответствующего персонала. Таким образом, освобождаются или происходит снижение нагрузки на специалистов, отвечающих за безопасность, от рутинных операций по контролю за пользователями, системами и сетями.

В настоящее время технологии обнаружения компьютерных атак активно разрабатываются производителями различного программного обеспечения. Основными инструментами, которые разработчики программного обеспечения закладывают в свои продукты, являются мониторинг, обнаружение и анализ изменений, происходящих в информационных системах. Решения усложняются и объединяют разные инструменты.

Рассмотрим классы средств обнаружения, которые появились за последнее время [8].

**Межсетевые экраны нового поколения (NGFW)**

Традиционные межсетевые экраны, принцип которых заключался в основном в фильтрации пакетов и контроле сетевых подключений, были заменены решениями нового поколения. Класс решений появился давно, но и его стоит учитывать в стеке современных технологий обнаружения. Межсетевые экраны нового поколения сочетают в себе функции классического межсетевого экрана и более передовые технологии, которые можно использовать в различных сочетаниях в NGFW:

* функции межсетевого экрана прикладного уровня (WAF);
* сигнатурный анализ трафика для обнаружения блокирования угроз(IPS);
* полнотекстовый анализ (проверка) трафика, зашифрованного многоуровневыми протоколами;
* возможности ограничения и приоритезации трафика - Quality of Service (QoS);
* поведенческий анализ файлов в изолированной среде («песочницы»);
* регулярное пополнение данными о текущих угрозах (репутационные списки, индикаторы компрометации и т.п.).

Кроме того, в зависимости от производителя и конфигурации NGFW может включать в себя функции защиты от атак на DNS, защиты от программ-шпионов (программ-шпионов для несанкционированного сбора информации или изменения настроек), контроля соединений с ботнетами и другие дополнительные функции.

Таким образом, NGFW — это устройство с управлением трафиком на уровне приложений, встроенными средствами обнаружения вторжений и идентификацией трафика.

**Системы мониторинга событий безопасности (SIEM)**

Решения класса Security Information and Event Management (SIEM) предназначены для мониторинга событий, поступающих от различных информационных систем и приложений. Решения по информационной безопасности данного класса позволяют решать следующие задачи:

* собирать и анализировать большие объемы событий безопасности;
* следить за текущим состоянием средств защиты ИТ-инфраструктуры;
* обнаружение ИТ-инцидентов в режиме реального времени;
* получить полное представление о том, что происходит в ИТ-инфраструктуре;
* обнаружение и реагирование на сбои компьютеров и систем информационной безопасности;
* построить карту сети для прогнозирования цепочек атак;
* получать данные для оперативного анализа и оценки рисков;
* соблюдение отдельных требований и норм законодательства Российской Федерации в области обеспечения информационной безопасности (ИБ) мониторинга событий.

SIEM позволяет получить более полную картину происходящего в ИТ-инфраструктуре и дополнительно проанализировать сетевую доступность конкретных узлов. Тщательно анализируя и собирая данные из нескольких источников, SIEM обнаруживает инциденты, когда традиционные инструменты обнаружения, работающие изолированно, не всегда эффективны. Принцип работы решений класса SIEM заключается в сборе всех типов журналов (событий) с различных устройств, как на программном, так и на уровне аппаратной составляющей. Кроме того, все события приведены в единый формат для дальнейшего анализа. Набор событий (корреляция), связанных с одним и тем же элементом инфраструктуры, может свидетельствовать о кибератаке.

**Системы анализа сетевого трафика (NTA)**

Решения класса Network Traffic Analysis (NTA) предназначены для обнаружения сетевых атак, перехвата и анализа сетевого трафика. Этот класс систем помогает обнаруживать присутствие злоумышленников на ранней стадии атаки, быстро локализовать угрозы и обеспечивать соблюдение правил информационной безопасности.

Кроме того, с появлением актуальных сигнатур решения класса NTA должны иметь возможность запускать анализ сетевого трафика, хранящегося в архиве (ретроспективный анализ).

На практике такие решения позволяют, например, обнаружить подозрительную попытку подключения неавторизованного хоста к контроллеру домена, проанализировать исторические данные о сетевой активности хоста и проверить, были ли другие подобные попытки. Если это произошло, это свидетельствует о целенаправленной атаке или как минимум о попытках взлома.

**Средства обнаружения компьютерных атак на конечных устройствах (EDR).**

Решения класса Endpoint Detection and Response (EDR) позволяют выявлять компьютерные атаки на конечные устройства и предоставлять необходимые метрики для реагирования специалистов по информационной безопасности.

Этот класс решений обычно использует специальный агент, который устанавливается на конечное устройство. В его функции входит сбор информации о действиях пользователей и программного обеспечения, обнаружение индикаторов компрометации (IoC), помощь в идентификации и обнаружении скомпрометированных устройств и т. д.

В зависимости от реализации решение EDR может включать в себя различные сенсорные технологии. Например, помимо агента для сбора и анализа данных, это может быть средство антивирусной защиты с поведенческим анализом, анализом индикаторов компрометации, а также автоматическим взаимодействием с SIEM-системами и системами класса Threat Intelligence для обогащения данных об угрозах и, совместно с другими системами дают специалистам по информационной безопасности более полную картину произошедшего для проведения качественного расследования.

Вся собранная информация способствует расследованию компьютерных инцидентов. Использование решений класса EDR позволяет организациям выявлять изощренные угрозы, направленные на обход традиционных средств защиты на конечных точках.

**Система анализа сетевого трафика нового поколения (NDR)**

Класс решений NDR (Network Detection & Response) был недавно сформирован исследовательским центром Gartner. Решения NDR включают следующие технологии:

* анализ сетевого трафика;
* поведенческая аналитика (машинное обучение для быстрого обнаружения, расследования и реагирования на угрозы).

По сути, NDR включает в себя технологии NTA, также добавляются исторические метаданные для расследования и поиска угроз, а также автоматического реагирования на угрозы за счет интеграции с различными инструментами управления ИТ и информационной безопасностью (брандмауэры, средства контроля доступа к сети и т. д.).

Решения NDR обеспечивают полную видимость сети с обнаружением угроз в реальном времени, а интеграция с продуктами EDR и SIEM обеспечивает дополнительную, более точную корреляцию данных для обнаружения инцидентов.

## **Средства анализа трафика**

В терминологии системных администраторов и специалистов по информационной безопасности часто встречается понятие «анализаторы трафика». Анализатор трафика — это устройство или программа, которая перехватывает трафик, а затем анализирует его.

Задача анализа сетевого трафика становится все более актуальной в связи с развитием и внедрением новых сетевых технологий (и, соответственно, увеличением объема данных, передаваемых по сети), а также появлением большого количества новых сетевых протоколов прикладного уровня. К наиболее популярным областям практического применения относятся:

* анализ трафика для выявления проблем в сети (включая несанкционированные действия);
* восстановление потоков данных («прослушивание»);
* предотвращение различных видов сетевых атак;
* сбор статистики.

Если говорить о комплексном решении задачи анализа сетевого трафика, то в первую очередь ее следует разделить на три достаточно самостоятельных подзадачи (Рисунок 3).



Рисунок 3 – Подзадачи системы анализа сетевого трафика

Перед тем, как перейти к непосредственному рассмотрению сетевых анализаторов, отметим, что есть два режима работы:

* в реальном времени;
* по предварительно сохраненному трафику.

Анализ в реальном времени требует поддержки инструмента в непрерывном режиме с достаточной производительностью для анализа поступающего на вход трафика. Должна быть возможность обрабатывать потенциально бесконечный поток входных данных.

В случае отложенного анализа инструмент получает входные данные из файла, что позволяет более детально проанализировать сетевой маршрут по сравнению с анализом аналогичного трафика в реальном времени [9].

**Wireshark**

Wireshark – это программа – анализатор сетевых протоколов, задача которого состоит в мониторинге сетевого трафика в режиме реального времени, детальном отображении принятых и отправленных пакетов данных, а также сохранении собранных данных для последующего анализа. Является одним из самых известных и распространённых инструментов в данной области [10].

Работа программы основана на классической библиотеке libpcap, отвечающей за непосредственный сбор пакетов. Wireshark осуществляет мониторинг огромного числа сетевых протоколов: TCP, UDP, SIP, RTP и т.д. Также поддерживает такие технологии физического и канального уровней, как Ethernet, Token Ring и FDDI, ATM.

Непосредственно Wireshark предоставляет графический интерфейс для проведения анализа, обеспечивая инструменты просмотра содержимого, фильтрации, группировки, построения графиков и так далее (Рисунок 4).

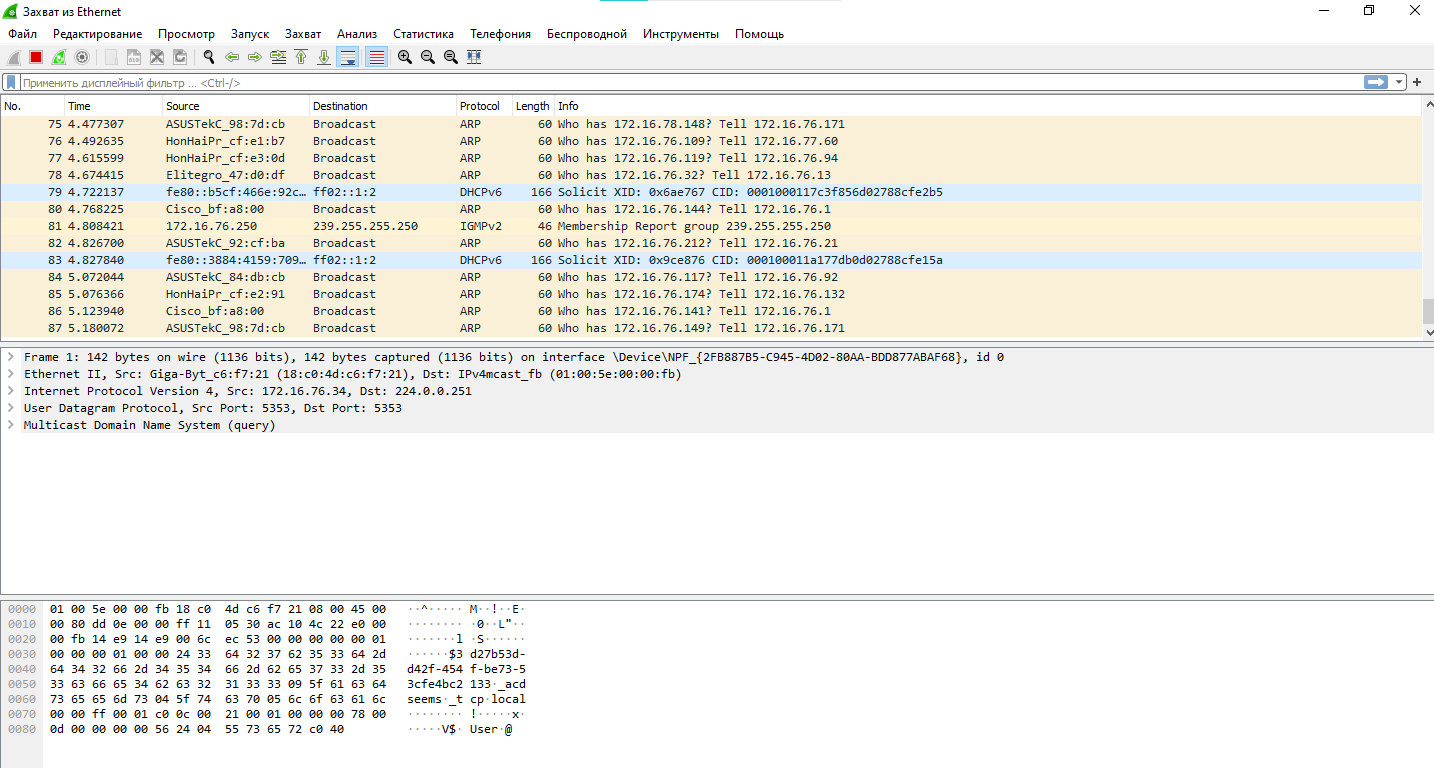


Рисунок 4 – Интерфейс Wireshark

Отличительными чертами продукта можно назвать простоту установки, а также легкость и удобство использования. Также WireShark является бесплатным и открытым исходным кодом и без проблем работает с любым из трех самых популярных семейств операционных систем: \* NIX, Windows и macOS.

**Tcpdump**

TCPdump – утилита анализа трафика, предназначенная в первую очередь для UNIX систем, хотя имеются реализации и для Windows. TCPdump основан на библиотеке libpcap, поэтому, как и WireShark, обладает теми же возможностями захвата и анализа трафика.

Работа с утилитой tcpdump осуществляется благодаря использованию команд с определённым синтаксисом [17]:

*$ tcpdump <опции> -i <интерфейс> <фильтры>*

*<Опции> – настраивают отображение и основные возможности утилиты;*

*<Интерфейс> – сетевой интрфейс, с которого следует принимать данные;*

*<Фильтры> – отсеивают те типы пакетов, которые не подходят под заданные пользователем параметры перехвата трафика.*

В соответствии с подходами UNIX, утилита предназначена для работы из командной строки и не имеет графического интерфейса (Рисунок 5).

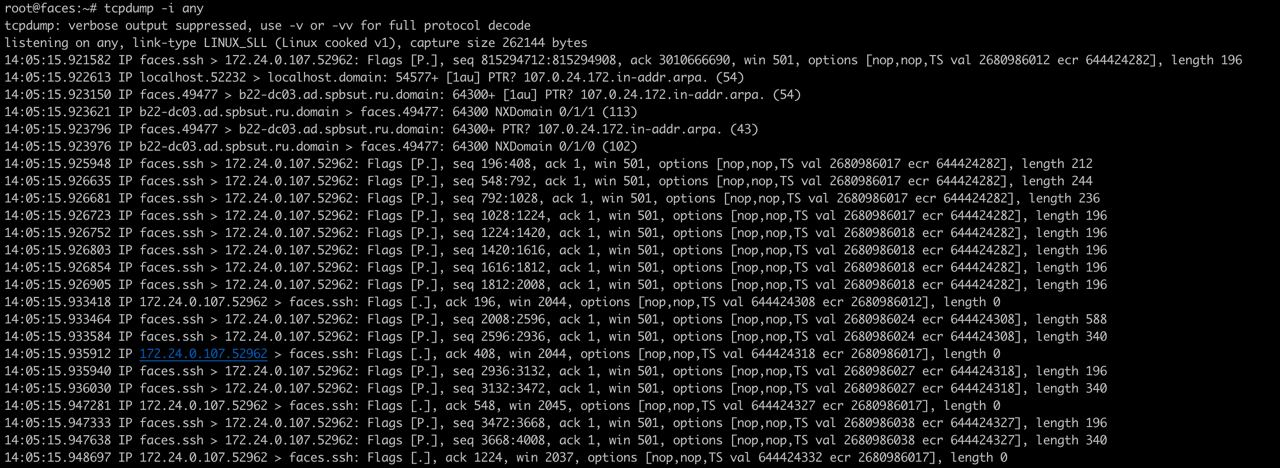


Рисунок 5 – вывод данных утилитой tcpdump

Главным преимуществом tcpdump является возможность захвата пакетных данных и их запись в файл с расширением .pcap для дальнейшего пост-анализа.

**Snort**

Snort – это система предотвращения вторжений с открытым исходным кодом, способная выполнять анализ трафика в реальном времени и протоколирование пакетов в IP – сетях.

Эта система также предназначена для использования в UNIX и является инструментом командной строки, однако существуют другие открытые продукты, добавляющие web – интерфейс [10].

Snort постоянно следит за трафиком и способен отправлять уведомления в случае обнаружение подозрительной активности. Кроме того, система собирает статистику и позволяет строить различные отчеты. На рисунке 6 приведен пример отчета.

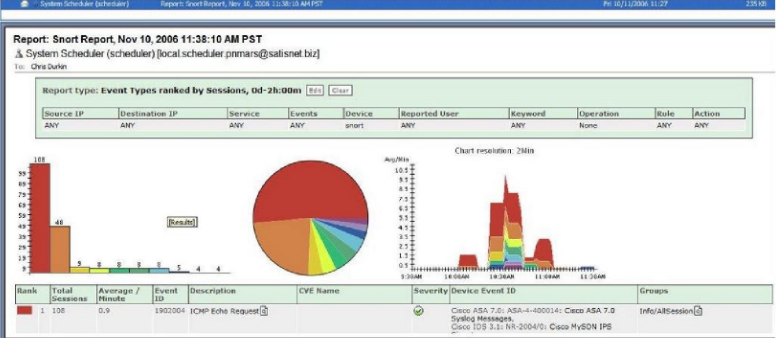


Рисунок 6 – Отчет об активности сети (Snort)

**Brim**

Утилита Brim выглядит как настольное приложение и состоит из набора следующих подсистем: фреймворка Zeek, системы обнаружения атак Suricata, поисковой системы Zed и графического пользовательского интерфейса на основе Electron и React (Рисунок 7).

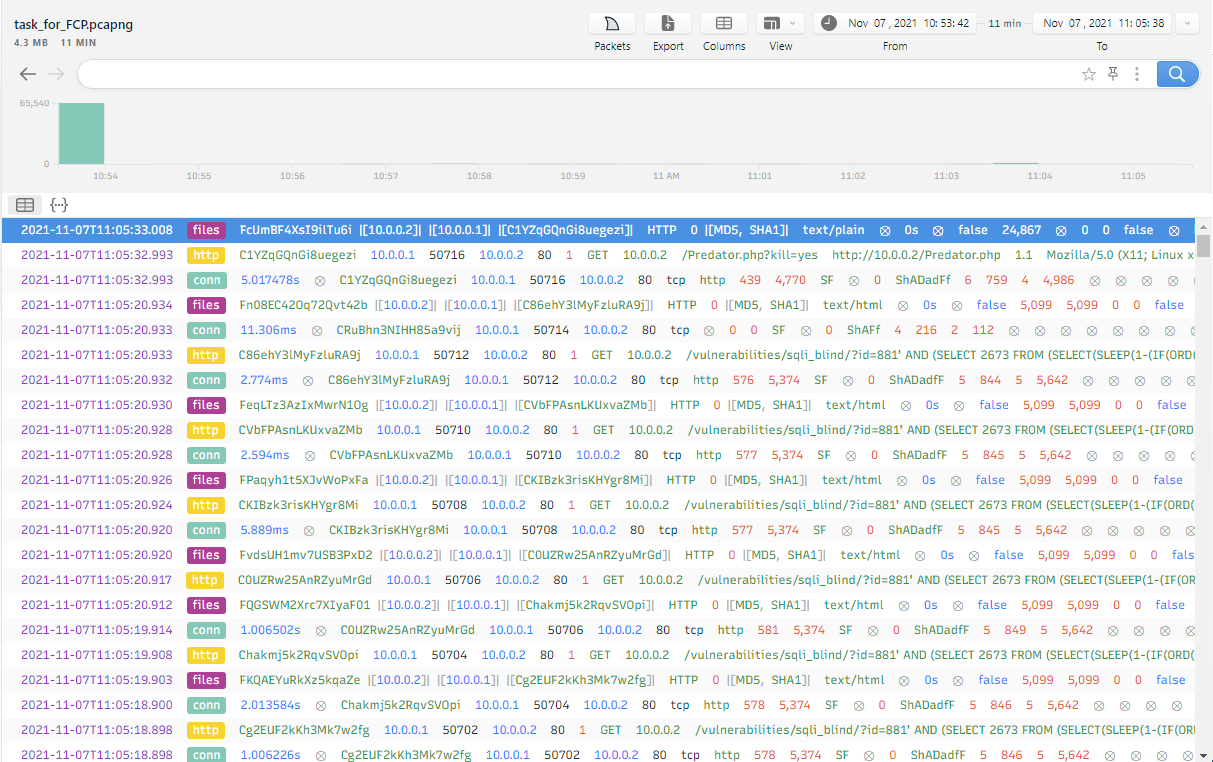


Рисунок 7 – Интерфейс утилиты Brim

Сочетая в себе сильные стороны вышеперечисленных подсистем, инструмент позволяет быстро анализировать сетевой трафик с целью анализа его безопасности [2].

## **Packetbeat инструмент анализа трафика**

Packetbeat — это анализатор сетевых пакетов в режиме реального времени, который можно использовать с Elasticsearch для обеспечения системы мониторинга приложений и анализа производительности.

После установки Packetbeat в клиентской системе служба начнет собирать и передавать все сетевые данные, которые можно использовать для анализа аномального сетевого трафика. Данные, собранные Packetbeat, показывают все пользовательские события в выбранной сети. Это полезно для обнаружения вторжения между внутренней и внешней сетью.

Существует множество доступных инструментов анализа пакетов, каждый из которых имеет свои преимущества и недостатки при устранении неполадок в сети. Среди них продукт с открытым исходным кодом, интегрированный в стек ELK. ELK — это комбинация трех разных сервисов, таких как Elasticsearch, Logstash и Kibana.

Объединенные и используемые вместе, они образуют инструмент анализа данных в реальном времени, который предоставляет надежную информацию из любого типа структурированных и неструктурированных источников данных.

Elasticsearch похож на базу данных и поисковую систему, которая может хранить много данных. Logstash используется для обработки данных, отправки событий и журналов в Elasticsearch. Kibana работает с данными Elasticsearch, этот сервис может быть полезен для визуализации данных.С помощью ELK вы можете настраивать информационные панели Kibana в соответствии со своими потребностями и создавать новые шаблоны индексов.

Сервисы Beats — это поставщики данных с открытым исходным кодом, которые можно установить в качестве агентов в клиентской системе для сбора журналов и отправки данных непосредственно в Elasticsearch или для передачи через Logstash в Elasticsearch. По сути, существует 5 типов сервисов Beats, необходимых для сбора журналов [13]:

1. Packetbeat - предназначен для сбора всех сетевых данных с клиентских систем. Использование Packetbeat позволяет отслеживать и анализировать сетевые пакеты.
2. Winlogbeat - позволяет собирать журналы событий в операционной системе Windows с клиентских систем. Его можно развернуть только в операционных системах Windows.
3. Metricbeat - используется для сбора различных метрик системного уровня для разных систем и платформ.
4. Filebeat - предназначен для сбора файлов из лога. Он имеет различные модули для сбора, анализа и визуализации лог-файлов.
5. Auditbeat - требуется для мониторинга действий пользователей и процессов, происходящих на серверах Linux. Его можно использовать для обнаружения различных нарушений безопасности и контроля целостности данных.

Каждый сервис Beats — это отдельно устанавливаемый продукт. Перед установкой Beats необходимо установить и настроить стек ELK.

На рисунке 8 представлена схема работы ELK стека с сервисами Beats.

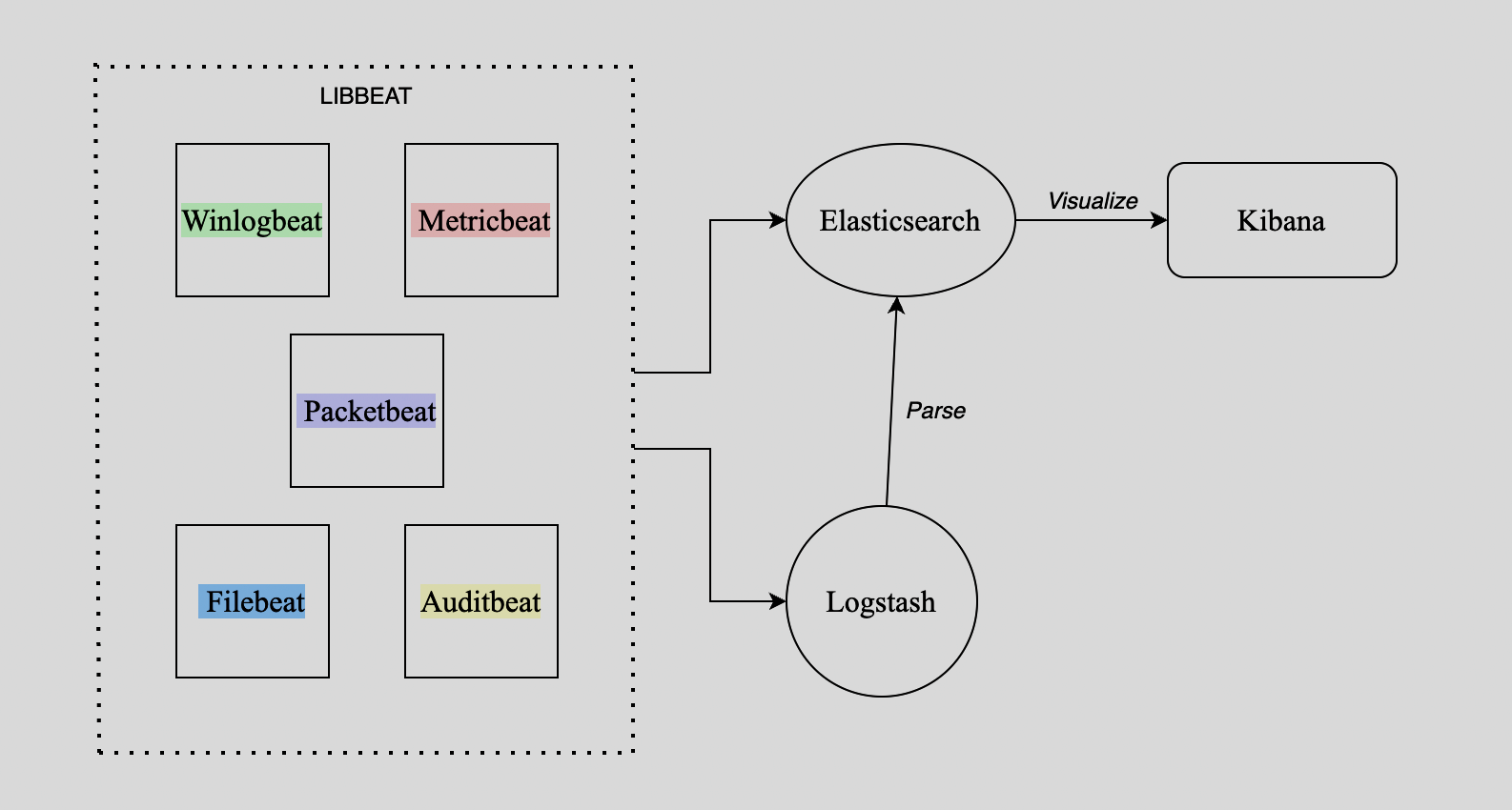


Рисунок 8 – Архитектура ELK - стека

**Преимущества Packetbeat**

Packetbeat реализован для сбора сетевых данных с клиентских систем. Это одновременно источник сетевых данных и анализатор сетевых пакетов с открытым исходным кодом, который можно интегрировать в стек ELK.

Packetbeat обеспечивает мониторинг различных показателей в сети, базе данных или любом другом протоколе в режиме реального времени путем мониторинга пакетов. Мониторинг пакетов данных с помощью стека ELK полезен для выявления вредоносного сетевого трафика и поведения сетевых пакетов, а также для определения источника и назначения пакета и при поиске определенных последовательностей данных в пакетах.

Packetbeat может перехватывать сетевой трафик между серверами и использоваться для мониторинга производительности веб-приложений.

Packetbeat можно установить в клиентской системе и управлять им на выделенном сервере. При работе на выделенных серверах Packetbeat может получать трафик с зеркальных портов коммутатора или прослушивающих устройств. При таком развертывании отслеживаемое приложение не требует дополнительной нагрузки.

Packetbeat отслеживает сетевой трафик и декодирует протоколы, а затем записывает данные в транзакцию. Для каждой транзакции Packetbeat вставляет документ JSON в Elasticsearch.

Packetbeat анализирует трафик между вашими серверами, анализирует журналы прикладного уровня на лету и сопоставляет сообщения с транзакциями [14]. В настоящее время Packetbeat поддерживает следующие протоколы:

* ICMP (v4 and v6)
* DHCP (v4)
* DNS
* HTTP
* AMQP 0.9.1
* Cassandra
* Mysql
* PostgreSQL
* Redis
* Thrift-RPC
* MongoDB
* Memcache
* NFS
* TLS
* SIP/SDP (beta)

Packetbeat может помочь вам легко определить проблемы с вашим серверным приложением, такие как ошибки или проблемы с производительностью, и значительно ускорить их устранение и, следовательно, исправить их.

## **РЕАЛИЗАЦИЯ ЛАБОРАТОРНОГО СТЕНДА**

## **Общее описание разработанного стенда**

Для проведения практической части на сервер Ubuntu версии 20.04 был установлен ELK-стек для сбора и визуализации сетевых данных с помощью Packetbeat.

ELK Stack представляет собой коллекцию из трех продуктов с открытым исходным кодом как Elasticsearch, Logstash и Kibana – от Elastic.

Основными достоинствами ELK-стека считаются следующие [3]:

* *Масштабируемость.* Кластер Elasticsearch быстро расширяется за счет добавления новых серверов. В этом случае распределение нагрузки между узлами происходит автоматически.
* *Отказоустойчивость.* В случае выхода из строя узла кластера данные не будут потеряны, а будут перераспределены, а поисковая система продолжит работу самостоятельно. Стабильность работы достигается за счет ведения журналов по каждому изменению данных в хранилище одновременно на нескольких узлах кластера.
* *Гибкость поисковых фильтров*, в том числе нечеткий поиск, возможность работы с восточными языками (китайский, японский, корейский) и мультиарендность, когда в рамках одного объекта можно динамически организовать несколько разных поисковых систем. Благодаря встроенным анализаторам текста Elasticsearch автоматически выполняет токенизацию, лемматизацию, стемминг и другие преобразования текста для решения задач NLP, связанных с поиском данных.
* *Управляемость* Elasticsearch по HTTP с помощью JSON-запросов за счет REST API и визуального веб-интерфейса Kibana.
* *Универсальность*. Logsatsh в потоковом режиме работает одновременно с множеством различных источников данных (СУБД, файлы, системные журналы, веб-приложения и т.д.), фильтруя их и преобразовывая для отправки в хранилище Elasticsearch. А NoSQL (безсхемный) характер Elasticsearch позволяет загружать в него JSON-объекты, которые автоматически индексируются и добавляются в базу поиска. Это позволяет ускорить прототипирование исследовательских решений для работы с большими данными.

ELK — cтек состоит из 3-х программных продуктов Elasticsearch, Logstash и Kibana. На нашем стенде были использованы только 2 программных продукта: Elasticsearch и Kibana, так как с помощью Packetbeat мы отправляем данные напрямую в Elasticsearch. Стенд также включает Nginx в качестве обратного прокси-сервера для приложения Kibana (Рисунок 9).

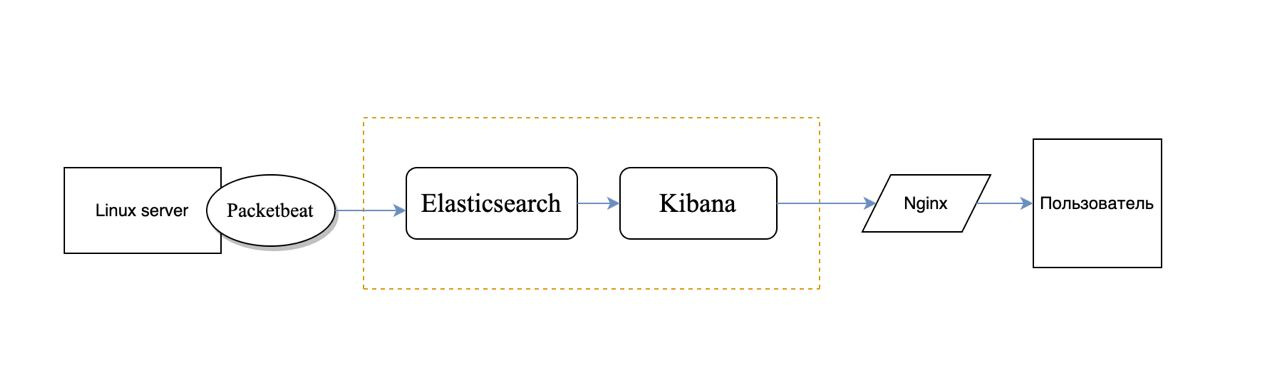


Рисунок 9 – Архитектура реализуемого стенда

Рассмотрим компоненты стенда подробнее.

**Kibana**

Kibana – это веб-интерфейс, который соединяет пользователей с базой данных Elasticsearch. Данный продукт дает возможность интерактивной визуализации данных проиндексированных страниц в кластере Elasticsearch и поиска пользователям системы. Результатом графического вывода может быть как текстовая информация, так и различные диаграммы, гистограммы, графики.

Официальный разработчик описывает ряд преимуществ в использование продукта [18]:

* Визуализация

Kibana предлагает множество способов простой визуализации данных. Некоторые из них широко используются: вертикальная гистограмма, горизонтальная гистограмма, круговая диаграмма, линейная диаграмма, тепловая карта и т. д.

* Приборная доска

Когда у нас есть готовые визуализации, их можно поместить на одну вкладку: панель инструментов. Глядя на разные разделы вместе, вы получаете четкое общее представление о том, что именно происходит.

* Dev Tools

Вы можете работать со своими индексами, используя инструменты разработки. Новички могут добавлять фиктивные индексы из инструментов разработчика, а также добавлять, обновлять, удалять данные и использовать индексы для создания визуализаций.

* Отчеты

Все данные в форме просмотра и панели мониторинга можно преобразовать в отчеты (в формате CSV), внедрить в код или в виде URL-адреса для совместного использования с другими.

* Фильтры и поисковый запрос

Вы можете использовать фильтры и поисковые запросы, чтобы получить информацию, необходимую для конкретных входных данных, с информационной панели или инструмента визуализации.

* Плагины

Вы можете добавить сторонние плагины, чтобы добавить новую визуализацию или другое дополнение пользовательского интерфейса в Kibana.

* Карты координат и регионов

Карта координат и регионов в Kibana помогает отображать визуализацию на географической карте, обеспечивая реалистичное представление данных.

* Timelion

Timelion, также называемый временной шкалой, — это еще один инструмент визуализации, который в основном используется для анализа данных на основе времени. Для работы с временной шкалой нам нужно использовать простой язык выражений, который помогает нам подключаться к индексу, а также выполнять вычисления с данными для получения желаемых результатов. Это больше помогает в сравнении данных с предыдущим циклом по неделям, месяцам и т.д.

* Холст

Canvas — еще одна мощная функция Kibana. Используя представление холста, вы можете представлять свои данные в различных сочетаниях цветов, форм, текстов на нескольких страницах, обычно называемых информационными панелями.

**Elasticsearch**

Elasticsearch – это широко используемый сервер базы данных и поиска основанный на Apache Lucence. Он является основным компонентом установки ELK. Elasticsearch является базой данных NoSQL, это означает, что он хранит данные неструктурированным способом. Elasticsearch позволяет вам выполнять и комбинировать множество типов запросов – структурированных, неструктурированных, географических, метрических. В отличие от большинства баз данных NoSQL, Elasticsearch уделяет большое внимание поисковым возможностям и функциям.

Официальный разработчик на своем сайте описывает ряд преимуществ в использование продукта [3]:

* Скорость

Разработчики увеличили скорость за счет инвертирования индексов с преобразователями конечного состояния для полнотекстового запроса, BKD trees для хранения числовых геоданных и хранилище столбцов для аналитики.

* Запрос и анализ

Elasticsearch позволяет ранжировать результаты поиска, основываясь на множестве факторов, от частоты использования термина или возраста до популярности и многого другого. Смешивать и сочетать их вместе с функциями, чтобы оптимизировать то, как ваши результаты отображаются для ваших пользователей.

* Безопасность и мониторинг

С помощью X – Рack у пользователя есть возможность установить защиту для своего кластера и наблюдать за работой Elasticsearch.

* Масштабируемость

Elasticsearch запущенный на одном узле работает, точно так же, как и в кластере из 300 узлов.

## **Установка ELK – стека**

Далее были установлены основные элементы стека. Для этого был загружен и установлен публичный ключ компании Elastic. После этого возникла необходимость добавления репозитория для пакетного менеджера. Далее была проведена активация репозитория для полноценной работы пакетного менеджера репозиторием компании [7].

После добавления необходимых репозиториев с помощью пакетного менеджера были установлены следующие пакеты:

1. Elasticsearch
2. Kibana
3. Packetbeat

После установки каждый из этих элементов требует настройки и накладки работоспособности.

## Установка распределённой поисковой системы

После установки Elasticsearch был отредактирован главный конфигурационный файл Elasticsearch, elasticsearch.yml.

Файл elasticsearch.yml предоставляет параметры конфигурации для кластера, узлов, путей, памяти, сети, обнаружения и шлюзов. Большинство этих параметров имеют значения по умолчанию, но можно изменить их в соответствии потребностями. Для кластера, состоящего из одного сервера, мы изменили настройки только для сетевого хоста.

При изначальной настройки к Elasticsearch внешний доступ имеет любой пользователь. С точки зрения безопасности — это не практично, поэтому нужно ограничить внешний доступ Elasticsearch (порт 9200), чтобы посторонние пользователи не смогли прочитать данные.

Затем добавили сервис в автозагрузку, чтобы Elasticsearch запускался при каждой загрузке вашего сервера

## Установка системы визуализации информации

После была произведена установка компонента для визуального интерфейса Kibana, он необходим для визуализации получаемой информации в Elasticsearch.

Установка это элемента происходила с помощью добавления репозитория в пакетный менеджер. После установки необходимо добавить Kibana в автозагрузку и указать, адрес устройства на котором работает Elasticsearch и Packetbeat. В нашем случае мы работаем одним и тем же узлом, как и сама Kibana, поэтому направляем сбор данных Kibana на внешний IP адрес машины, на котором будет запущен ElasticStack.

Также есть необходимость указать какой конкретно адрес должна слушать сама Kibana для ответа на запросы, в нашем случае мы используем IP-адрес 0.0.0.0, используя этот адрес, мы слушаем все возможные запросы, приходящие на это устройство.

Веб – интерфейс продукта Kibana, в отличии от других сайтов, доступен не по 80 или 443 порту, а по порту 5601. Данный порт был выбран разработчиками качестве еще одного ограничения, которое уменьшает возможность случайного попадания в панель управления Kibana.

## Установка и настройка анализатора сетевых пакетов

Так как в нашем стеке не используется Logstash, производим настройку инструмента Packetbeat. После установки и обновления пакета Packetbeat, необходимо добавить его в автоматический запуск системы, чтобы при возможных проблемах с электричеством или появившийся необходимости перезагрузке машины в максимально короткие сроки продолжился сбор информации и минимизировалось время простаивания машины [12].

Далее, для настройки Packetbeat следует редактировать файл конфигурации. В первую очередь в файле конфигурации указываем сетевой интерфейс, с которого следует вести захват трафика. После, в секции протоколов указываем, какие протоколы и на каких портах должен обнаружить Packetbeat. Таже выполняем настройки вывода. Packetbeat поддерживает множество способов вывода, но чаще всего используется передача в Elasticsearch или в Logstash для дополнительной обработки. В -разработанном стенде настраиваем передачу трафика напрямую в Elasticsearch.

## **Настройка Dashboard в Kibana**

## Создание Index Pattern

В первую очередь нужно создать Index Pattern для Kibana с информацией о том, какие данные надо отображать [11].

Для настройки выбираем раздел Discover в левом меню и переходим на страницу создания Index pattern (Рисунок 10).

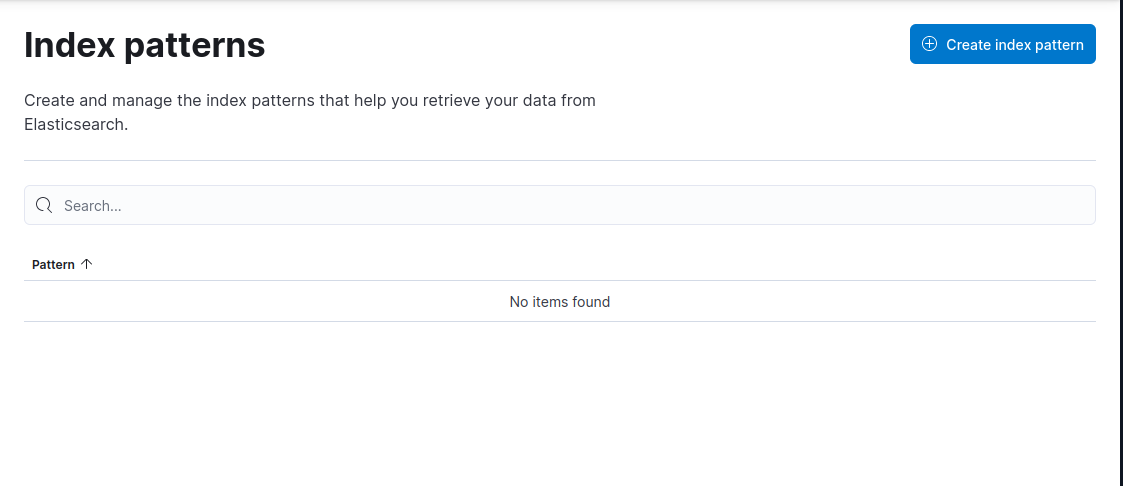


Рисунок 10 – Начальная страница Index pattern

Нажав на кнопку «Create index pattern», попадаем на страницу создания индекса. В поле «Name» вводим «packetbeat \*», а в поле «Timestamp field» выбираем ключевое поле с временной отметкой, в нашем случае это @timestamp (Рисунок 11).

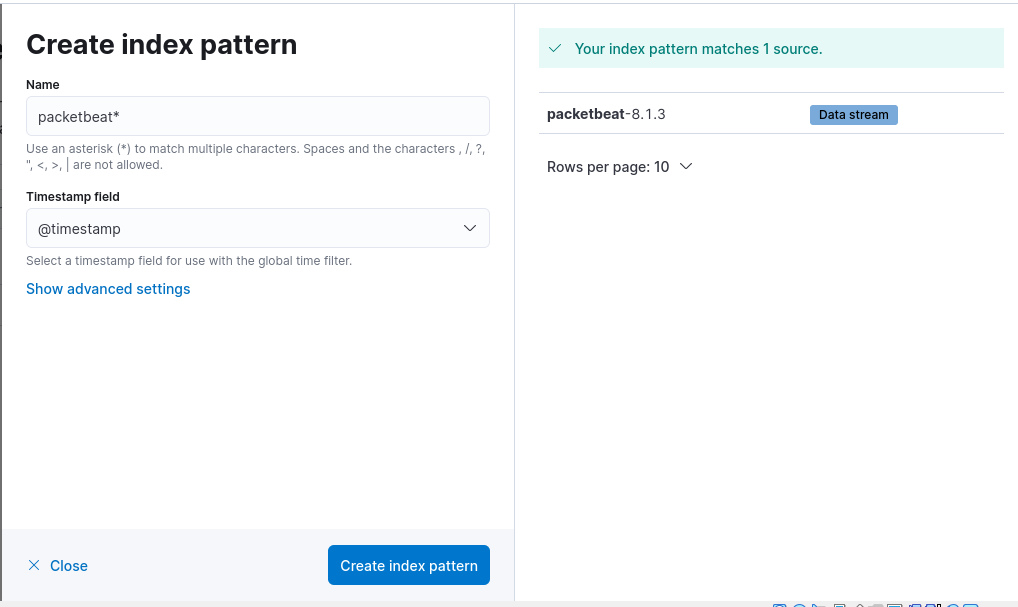


Рисунок 11 – Страница создания Index pattern

На рисунке 12 изображена страница настроек индекса, в результате выполненных инструкций.

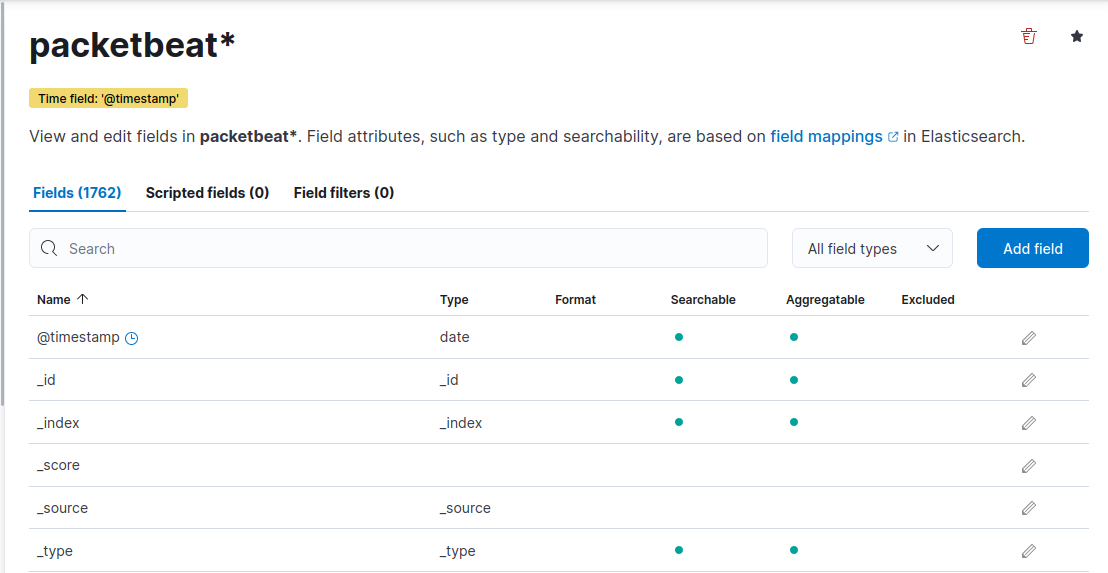


Рисунок 12 – Страница настроек индекса

Перейдя в раздел Discover, увидим записи логов (Рисунок 13).

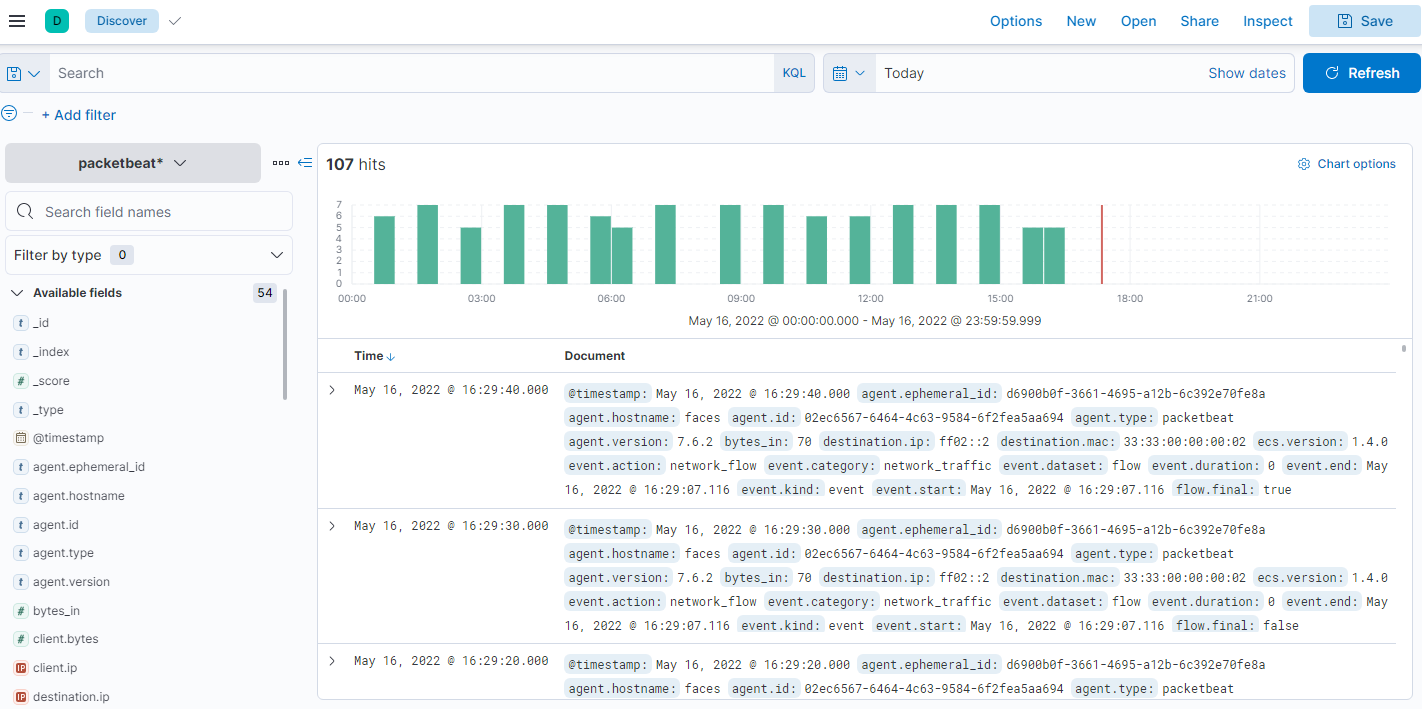


Рисунок 13 – Записи логов

Страница Discover содержит следующие элементы [16]:

* **Панель поиска:** расположена непосредственно под главным меню навигации и позволяет выполнять поиск по собранным сообщениям журнала.
* **Фильтр времени:** расположен в правом верхнем углу. Используйте эту функцию для фильтрации журналов на основе различных относительных и абсолютных интервалов времени.
* **Список полей:** расположен слева, чуть ниже строки поиска. Здесь вы можете выбрать поля для визуализации.
* **Гистограмма:** график, который находится в центре страницы под строкой поиска. По умолчанию он отображает количество всех журналов в зависимости от времени (ось X).
* **Просмотр журналов:** список под гистограммой, содержащий сообщения журнала и данные, отфильтрованные по полям. Если поле не заполнено, сообщение отображается полностью.

## Создание карты

Для настройки карты, в разделе «Analytics» выбираем вкладку «Maps» (Рисунок 14).

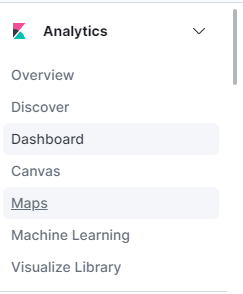


Рисунок 14 – Раздел «Analytics»

Далее добавляем слой, нажимая на «Add layer» (Рисунок 15).

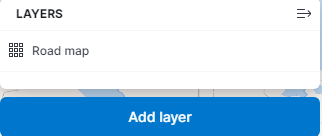


Рисунок 15 – Добавление слоя

После выбираем вид слоя из представленных (Рисунок 16). В нашем случае был выбран «Heat map».

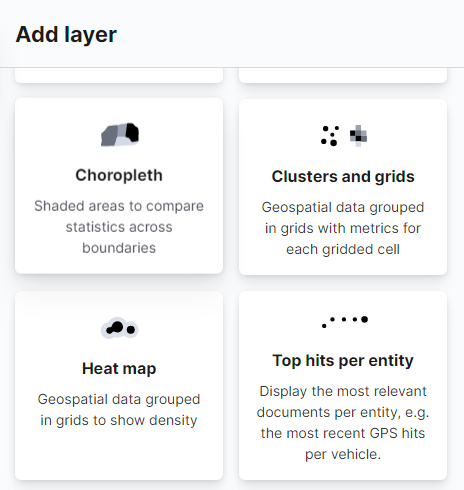


Рисунок 16 – Некоторые виды слоев

Настраиваем слой, выбирая в «Index pattern» packetbeat\* (Рисунок 17).

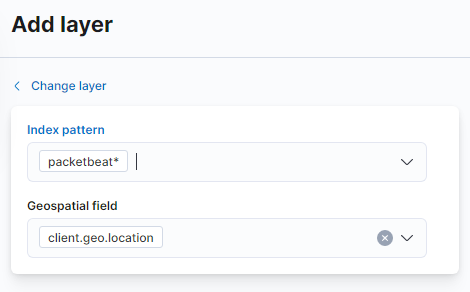


Рисунок 17 – Настройки слоя

Присваиваем имя панели и сохраняем (Рисунок 18).

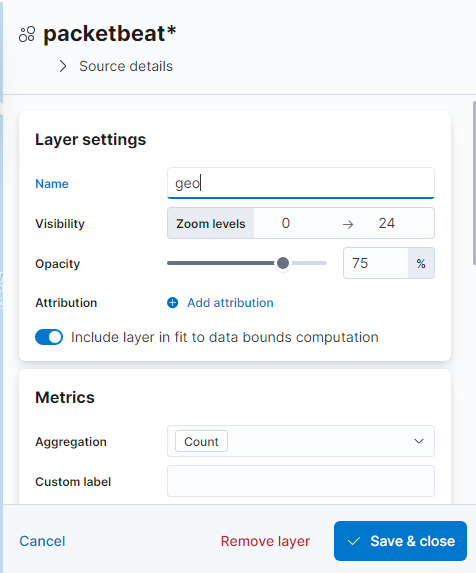


Рисунок 18 – Сохранение настроек слоя

Получаем dashboard с геопозицией клиента (Рисунок 19).

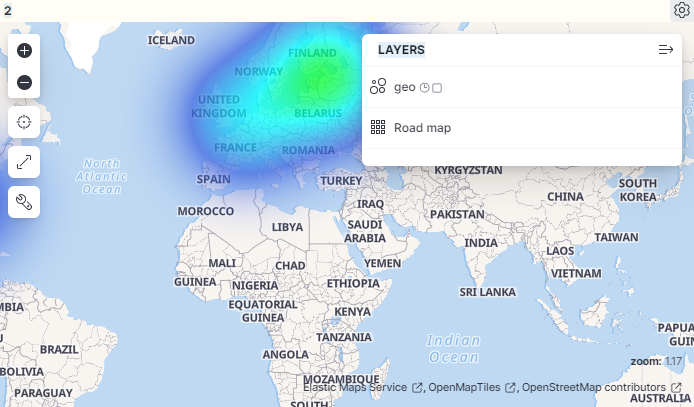


Рисунок 19 – Готовый dashboard карты

## Создание dashboard «Total Events»

Далее мы проанализируем общее количество запросов и ответов с указанного http-порта.

В разделе «Analytics» выбираем вкладку «Dashboard», попадаем на страницу создания dashboard (Рисунок 20).

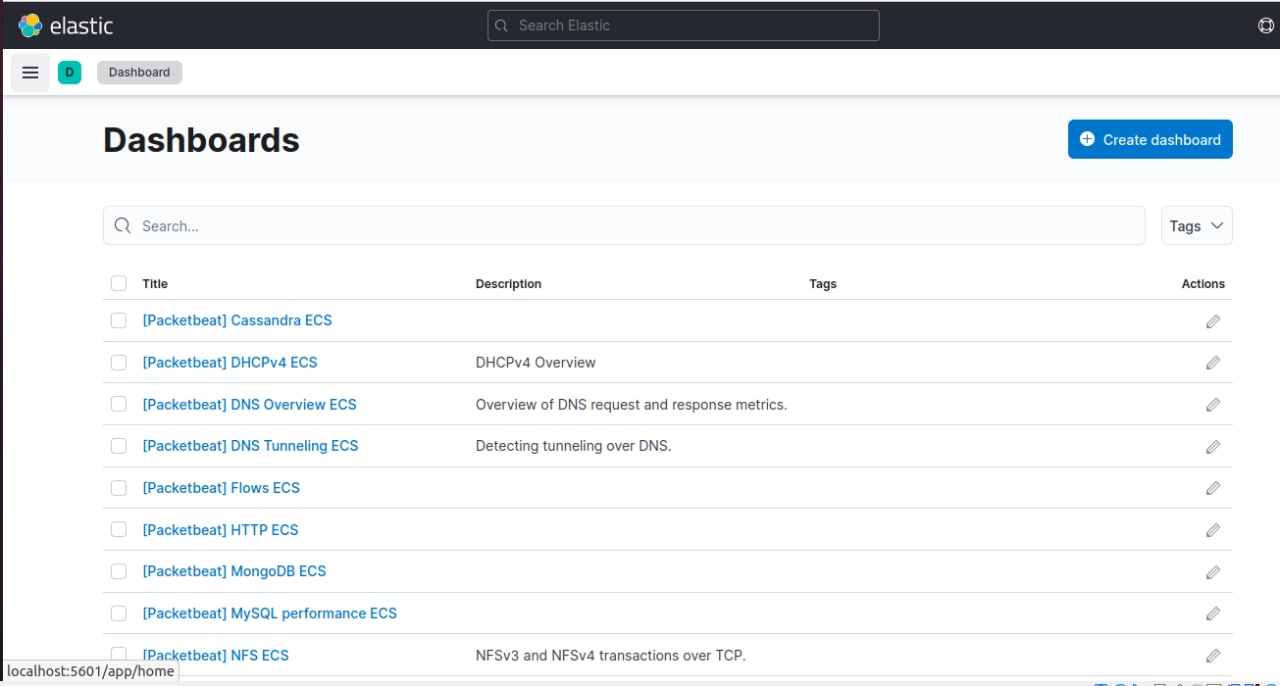


Рисунок 20 – Начальная страница создания Dashboard

Создаем дашборд с помощью кнопки «Create dashboard».

Далее переключаемся на представление диаграммы с областями, и выбираем вкладку «Area» (Рисунок 21).



Рисунок 21 – Выбор типа дашборда

В параметрах визуализации задаем настройки как на рисунке 22.



Рисунок 22 – Настройки диаграммы

В результате получаем дашборд с диаграммой, где отображаются общее количество запросов (Рисунок 23).

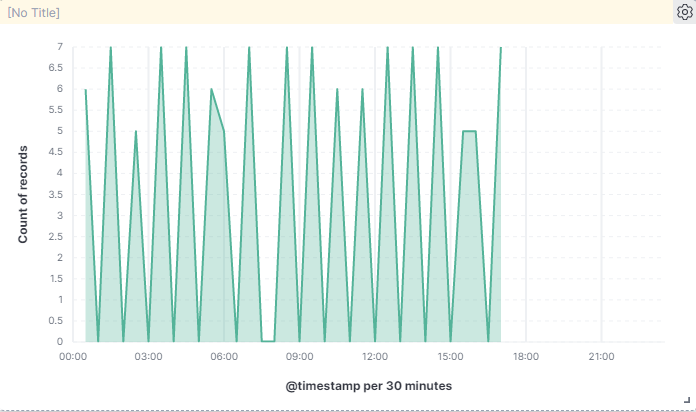


Рисунок 23 - Диаграмма «Total Events»

## **Разработка скрипта автоматического анализа сетевого трафика с помощью Packetbeat**

При анализе трафика используются PCAP файлы, которые являются ценным ресурсом для анализа файлов и мониторинга сетевого трафика. Инструменты захвата пакетов, такие как Wireshark, позволяют захватывать сетевой трафик и переводить его в удобочитаемый формат. Есть много причин, по которым PCAP используется для мониторинга сетей. Некоторые из наиболее распространенных включают мониторинг использования полосы пропускания, обнаружение мошеннических DHCP-серверов, обнаружение вредоносных программ, разрешение DNS и реагирование на инциденты [17].

Для сетевых администраторов и исследователей безопасности анализ файлов трафика является хорошим способом обнаружения сетевых вторжений и других подозрительных действий.

Для быстрой и удобной работы с данными файлами был написан bash скрипт, который автоматизирует процесс обработки дампов сетевого трафика (Рисунок 24).

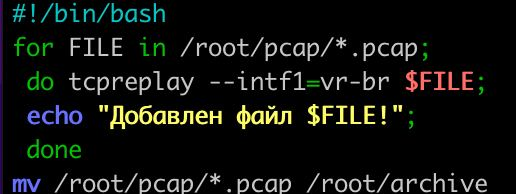
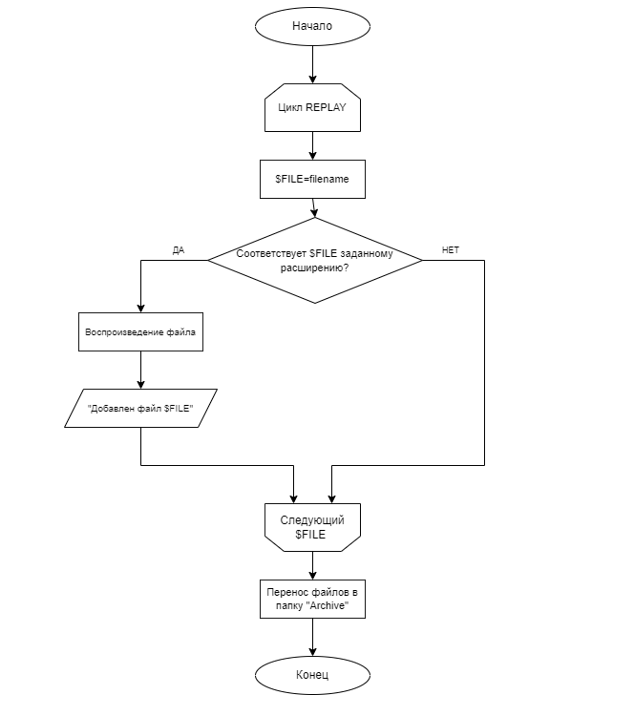


Рисунок 24 - bash скрипт

Скрипт выполняет следующие функции: из целевой папки поочередно берет каждый содержащийся в ней файл в формате pcap, и направляет трафик, записанный в нем на виртуальный интерфейс, созданный при конфигурации стенда, после чего перемещает все файлы в папку архив, которая создана для возможности последующего использования наших PCAP файлов (Рисунок 25).



.

Рисунок 24 – Блок-схема скрипта

Тестирование bash скрипта выявило проблему недоступности хоста, при воспроизведение pcap файла. Это связано с тем, что утилита tcp-replay на время обработки файла полностью блокирует остальной трафик, направленный на данный интерфейс. Для решения данной трудности было принято решение создать дополнительный виртуальный интерфейс и настроить Packetbeat для его прослушивания. Благодаря данному решению мы можем беспрепятственно осуществлять воспроизведение любого объема сетевого трафика без потери доступности сервера.

## **РАЗРАБОТКА ЛАБОРАТОРНЫХ РАБОТ**

## **Описание лабораторной работы №1 «Установка ELK - стека»**

Данная лабораторная работа направлена на изучение продуктов компании Elastic. В частности, их решений [6]:

* elasticsearch (поисковая система с открытым исходным кодом. Горизонтально масштабируется, поддерживает многопоточность и обладает хорошей производительностью.)
* kibana (инструмент визуализации и изучения данных, который применяется для таких задач, как анализ журналов и временных рядов, мониторинг приложений и текущих процессов.)
* packetbeat (инструмент мониторинга, который работает как анализатор сетевых пакетов, парсит различные, получает нужные данные, и отсылает их либо напрямую в Elasticsearch, либо в Redis, из которого данные будет забирать Logstash и класть их все в тот же Elasticsearch.)

Данные элементы единой экосистемы Elactic замечательно интегрируется друг с другом. После их настройки мы получаем готовую систему мониторинга Сетевого трафика в нашей информационной инфраструктуре.

Для выполнения лабораторной работы понадобится:

* Виртуальная машина с предустановленной операционной системой семейства UNIX (в нашем случае используется Ubuntu 20.04) и следующими характеристиками:

Таблица 1 – Характеристики виртуальной машины

|  |  |
| --- | --- |
| CPU | 4+ |
| Memory | 8 Gb |
| Disk | 20 Gb |

* Базовые знания работы с командной строкой UNIX-подобных операционных систем
* Понимание принципов работы сетевых протоколов модели OSI

Для успешного выполнения лабораторной работы необходимо следовать инструкции, описанной в лабораторной работе.

Описание шагов лабораторной работы:

1. Был установлен веб-сервер Nginx (Рисунок 25 ).



Рисунок 25 - Приветственное сообщение от nginx

1. Далее была произведена установка программного пакета JVM и JDK.
2. После был загружен и установлен публичный ключ компании Elastic. Затем добавлен репозиторий для пакетного менеджера. Далее была проведена активация репозитория для полноценной работы пакетного менеджера.
3. После добавления необходимых репозиториев с помощью пакетного менеджера были установлены и настроены следующие пакеты:

* Elasticsearch
* Kibana
* Packetbeat

По окончании выполнения всех шагов, описанных в Приложении 1, выполняющий лабораторную работу получит готовое решение для мониторинга сетевой нагрузки инфраструктуры.

Решение, предоставляемое компанией Elastic позволяет в наглядном и удобном виде отслеживать текущее состояние информационной структуры предприятия, а также быстро реагировать на инциденты, связанные с обеспечением информационной безопасности.

По итогу выполнения лабораторной работы, студенты научатся работать с программным решением Elasticsearch, освоят базовые приемы и принципы построения системы мониторинга в информационной инфраструктуре предприятия.

## **Описание лабораторной работы №2 «Определение IP адресов и стран участников сетевой сессии»**

Лабораторная работа направленна на изучение и работу с интерфейсом программного обеспечения компании Elasctic.

Для выполнения лабораторной работы понадобится:

* Виртуальная машина с предустановленной операционной системой семейства UNIX (в нашем случае используется Ubuntu 20.04) и следующими характеристиками:

Таблица 2 - Характеристики виртуальной машины

|  |  |
| --- | --- |
| CPU | 4+ |
| Memory | 8 Gb |
| Disk | 20 Gb |

* Предустановленное и настроенное программное обеспечение компании elastic:
  + elasticsearch (поисковая система с открытым исходным кодом. Горизонтально масштабируется, поддерживает многопоточность и обладает хорошей производительностью.)
  + kibana (инструмент визуализации и изучения данных, который применяется для таких задач, как анализ журналов и временных рядов, мониторинг приложений и текущих процессов.)
  + packetbeat (инструмент мониторинга, который работает как анализатор сетевых пакетов, парсит различные, получает нужные данные, и отсылает их либо напрямую в Elasticsearch, либо в Redis, из которого данные будет забирать Logstash и класть их все в тот же Elasticsearch.)
* Базовые знания работы с командной строкой UNIX-подобных операционных систем
* Понимание принципов работы сетевой маршрутизации в глобальной сети Интернет
* Понимание принципов работы сетевых протоколов модели OSI

Для успешного выполнения лабораторной работы необходимо следовать инструкции, описанной в лабораторной работе.

Описание шагов лабораторной работы:

1. В первую очередь был скачен дамп трафика.
2. Воспроизведен данный трафик.
3. Выбран нужный промежуток времени.
4. Настроена панель для определения IP адресов и стран участников сетевой сессии. Пример визуализации представлен на рисунке 26.

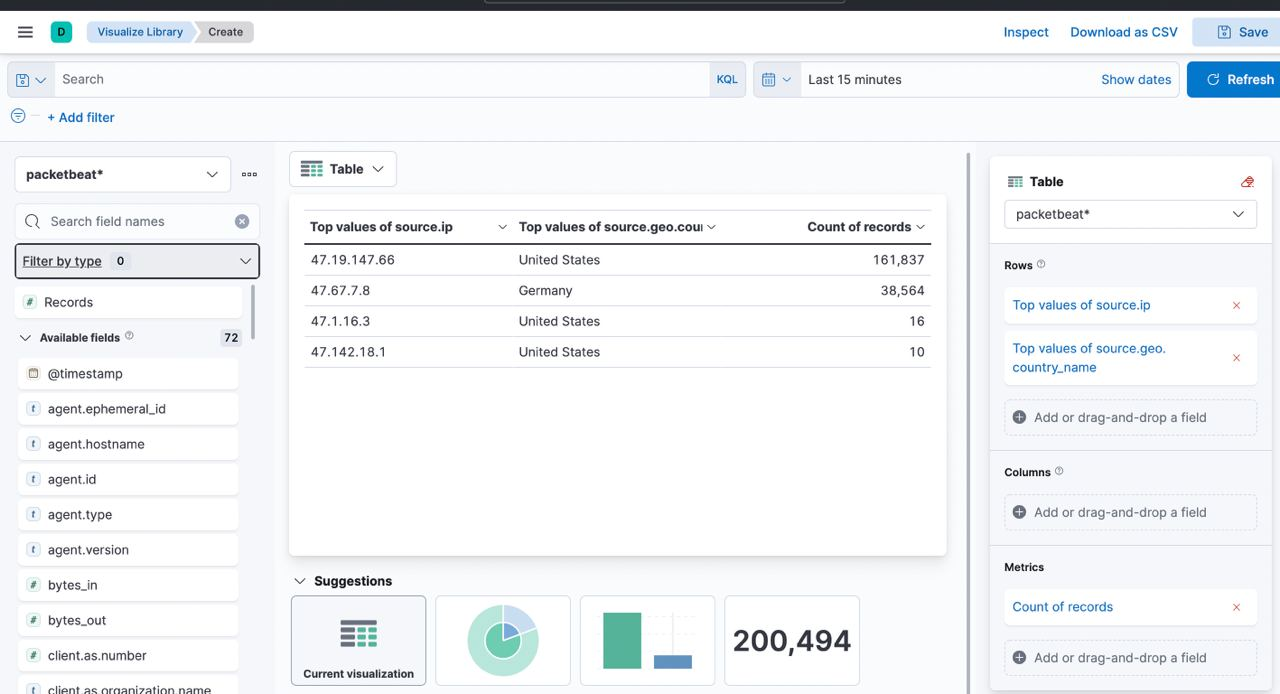


Рисунок 26 – Пример визуализации IP адресов и стран участников сетевой сессии

Во время выполнения лабораторной работы студент настроит свои панели для визуального представления данных, определит гео-позицию адресов, с которых отправлялись запросы в тестовом дампе трафика.

По окончании выполнения всех шагов, описанных в Приложении 2, выполняющий лабораторную получит знания по настройке программного обеспечения компании Elastic, научится представлять необработанные данные в виде таблиц, графиков и др., с целью более быстрого и безошибочного анализа данных.

## **Описание лабораторной работы №3 «Обнаружения сканирования узлов»**

Лабораторная работа направленна на изучение и работу с интерфейсом программного обеспечения компании Elasctic, а также на использование этого интерфейса для обнаружения сетевых атак на нашу инфраструктуру.

Для выполнения лабораторной работы понадобится:

* Виртуальная машина с предустановелнной операционной системой семейства UNIX (в нашем случае используется Ubuntu 20.04) и следующими характеристиками:

Таблица 3 - Характеристики виртуальной машины

|  |  |
| --- | --- |
| CPU | 4+ |
| Memory | 8 Gb |
| Disk | 20 Gb |

* Предустановленное и настроенное программное обеспечение компании elastic:
* elasticsearch (поисковая система с открытым исходным кодом. Горизонтально масштабируется, поддерживает многопоточность и обладает хорошей производительностью.)
* kibana (инструмент визуализации и изучения данных, который применяется для таких задач, как анализ журналов и временных рядов, мониторинг приложений и текущих процессов.)
* packetbeat (инструмент мониторинга, который работает как анализатор сетевых пакетов, парсит различные, получает нужные данные, и отсылает их либо напрямую в Elasticsearch, либо в Redis, из которого данные будет забирать Logstash и класть их все в тот же Elasticsearch.)Базовые знания работы с командной строкой UNIX-подобных операционных систем
* Понимание принципов работы сетевой маршрутизации в глобальной сети Интернет
* Понимание принципов работы сетевых протоколов модели OSI

Для успешного выполнения лабораторной работы необходимо следовать инструкции, описанной в лабораторной работе.

Описание шагов лабораторной работы:

1. В первую очередь был скачен дамп трафика.
2. Воспроизведен данный трафик.
3. Выбран нужный промежуток времени.
4. Настроена панель для обнаружения сканирования узлов. Пример визуализации представлен на рисунке 27.

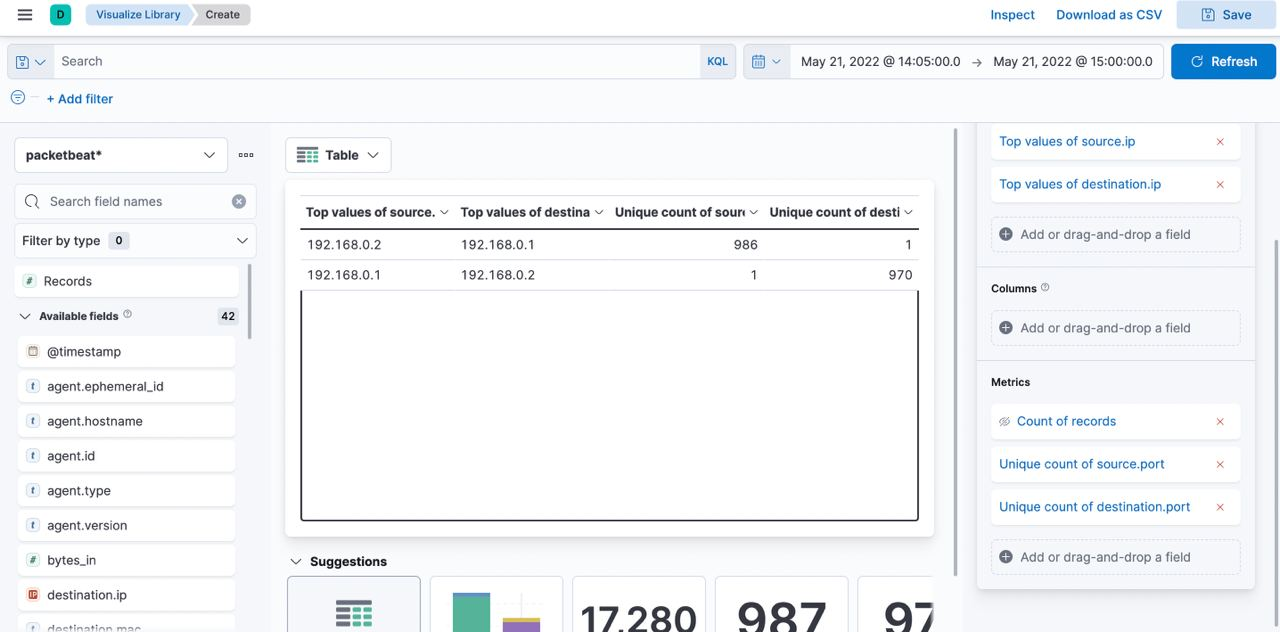


Рисунок 27 - Пример визуализации сканирования

Во время выполнения лабораторной работы студент настроит свои панели для визуального представления данных и с помощью тестового дампа обнаружит сканирование портов.

По окончании выполнения всех шагов, описанных в Приложении 3, выполняющий лабораторную работу получит знания по настройке программного обеспечения компании Elastic, научится представлять необработанные данные в виде таблиц, графиков и др., с целью более быстрого и безошибочного анализа данных. Научится находить и анализировать атаки, производимые на сетевую инфраструктуру.

## **ЗАКЛЮЧЕНИЕ**

Основной целью, данной выпускной квалификационной работы являлась разработка лабораторных работ по обнаружению компьютерных атак при помощи анализатора сетевых пакетов Packetbeat.

Для достижения этой цели были выполнены следующие задачи:

* Изучить классификацию компьютерные атака
* Проанализировать средства анализа трафика
* Разработать стенд, реализующий захват и анализ трафика
* Автоматизировать процесс анализа данных

В теоретической части были рассмотрены важные особенности по работе с программами Elasticsearch, Kibana и Packetbeat.

Рассмотренный материал позволяет сделать вывод о существенных достоинствах программного компонента, выделяющих его среди других – централизованный сбор логов, работающий в одной связке и способный представить логов в графическом виде, кот который читабелен обычному пользователю. Стек программ Elasticsearch, Kibana и Packetbeat ориентирован на сбор сетевых логов, позволяющий контролировать используемый ресурс.

Стек ELK можно использовать для развертывания больших информационных ресурсов и для личного пользования.

В практической части был реализован алгоритм сбора сетевого трафика с удаленного устройства для последующего анализа этих данных. Помимо этого, бала написана программа скрипта, которая позволяет автоматизировать и упростить процесс обработки сетевого трафика.

На основе данного стенда разработаны следующие лабораторные работы:

* 1. Лабораторная работа №1 «Установка ELK - стека»
  2. Лабораторная работа №2 «Определение IP адресов и стран участников сетевой сессии»
  3. Лабораторная работа №3 «Обнаружения сканирования узлов»

## **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Скорых, М.А. Применение фреймворка Zeek и ELK-СТЕКА для анализа рассылок вредоносного программного обеспечения / М.А. Скорых // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021): сборник научных статей X международной научно-технической и научно-методической конференции "Актуальные Проблемы Инфотелекоммуникаций в Науке и Образовании". – 2021. – С. 658-661.
2. Башмаков А.В., Израилов К.Е., Скорых М.А. Задачаориентированное сравнение средств анализа сетевого трафика // Сборник трудов по материалам всероссийской научно-теоретической конференции «ТиПОИБ-2021».
3. Elastic [Электронный ресурс]. – Режим доступа: <https://www.elastic.co/>
4. Типы сетевых атак и способы борьбы с ними [Электронный ресурс]. – Режим доступа: <https://www.smart-soft.ru/blog/tipy_setevyh_atak_i_sposoby_borjby_s_nimi/>
5. Атака на Internet [Электронный ресурс]. – Режим доступа: https://it.wikireading.ru/6317
6. Что такое стек ELK [Электронный ресурс]. – Режим доступа: <https://gitinsky.com/elkstack>
7. Установка стека ELK на операционную систему Ubuntu 18.04 [Электронный ресурс]. – Режим доступа: <https://mcs.mail.ru/docs/additionals/cases/cases-elk/elk-u18>
8. Технологии обнаружения компьютерных атак [Электронный ресурс]. – Режим доступа: <https://safe-surf.ru/specialists/article/5274/656701/>
9. Обзор методов и средств анализа сетевого трафика [Электронный ресурс]. – Режим доступа: <https://www.evkova.org/kursovye-raboty/obzor-metodov-i-sredstv-analiza-setevogo-trafika>
10. 8 лучших программ для анализа сетевого трафика [Электронный ресурс]. – Режим доступа: <https://networkguru.ru/8-luchshikh-programm-dlia-analiza-setevogo-trafika/>
11. Создание Dashboard в Kibana для мониторинга логов [Электронный ресурс].– Режим доступа: <https://habr.com/ru/company/citymobil/blog/521802/>
12. Сбор метрик инфраструктуры с помощью Packetbeat и ELK в Ubuntu 16.04 [Электронный ресурс]. – Режим доступа: <https://www.8host.com/blog/sbor-metrik-infrastruktury-s-pomoshhyu-packetbeat-i-elk-v-ubuntu-16-04/>
13. Lightweight data shippers [Электронный ресурс]. – Режим доступа: <https://www.elastic.co/beats/>
14. Lightweight shipper for network data [Электронный ресурс]. – Режим доступа: <https://www.elastic.co/beats/packetbeat>
15. Визуализация данных с помощью kibana [Электронный ресурс]. – Режим доступа: <https://www.8host.com/blog/vizualizaciya-dannyx-s-pomoshhyu-kibana/>
16. Расширение файла PCAP kibana [Электронный ресурс]. – Режим доступа: <https://www.file-extension.info/ru/format/pcap>
17. Утилита tcpdump для анализа сети [Электронный ресурс]. – Режим доступа: <https://sysadminium.ru/tcpdump/>
18. Kibana [Электронный ресурс]. – Режим доступа:https://www.elastic.co/kibana/
19. Сканирование портов [Электронный ресурс]. – Режим доступа: <https://encyclopedia.kaspersky.ru/glossary/port-scanning/>
20. Настройка обратного прокси Nginx на Linux [Электронный ресурс]. – Режим доступа: <https://andreyex.ru/operacionnaya-sistema-linux/nastrojka-obratnogo-proksi-nginx-na-linux/>
21. Компьютерные атаки: что это такое и как защититься от них [Электронный ресурс]. – Режим доступа: <http://citforum.ru/security/internet/secatt.shtml>

## **ПРИЛОЖЕНИЕ А**

Лабораторная работа №1

«Установка стека ELK»

**Цель работы:**

Изучить компоненты стека ELK с помощью их установки и настройки. Определить функции каждого из компонент стека. Изучить типы сервисов Beats, необходимых для сбора журналов.

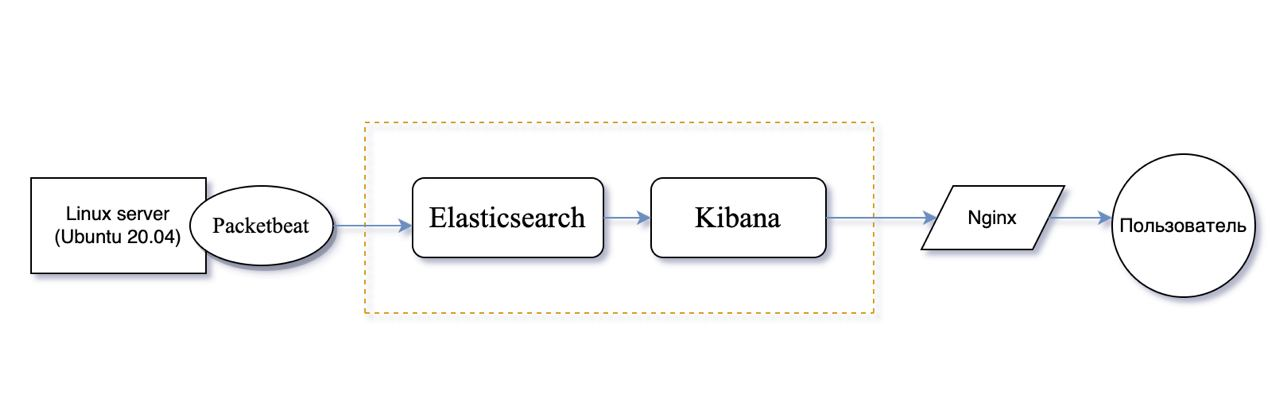


Рисунок 1 – Схема лабораторной работы

**Описания лабораторной работы:**

В данной лабораторной работе будет использован ELK-стек для сбора и визуализации сетевых данных с помощью Packetbeat. Будет произведена установка и базовая настройка Elasticsearch, Kibana и Packetbeat на одном хосте.

Для установки одиночного инстанса с набором компонентов ELK необходимы следующие системные ресурсы:

* Виртуальная машина с предустановленной операционной системой семейства UNIX (в нашем случае используется Ubuntu 20.04) и следующими характеристиками:

Таблица 1 – Характеристики виртуальной машины

|  |  |
| --- | --- |
| CPU | 4+ |
| Memory | 8 Gb |
| Disk | 20 Gb |

* Базовые знания работы с командной строкой UNIX-подобных операционных систем
* Понимание принципов работы сетевых протоколов модели OSI

**Порядок выполнения:**

***Установка веб-сервера Nginx***

1. Откройте окно терминала.
2. Обновите индексы пакетов, выполнив команду:

***sudo apt update***

1. Установите веб-сервер Nginx, выполнив команду:

***sudo apt install nginx***

*Дожидаемся окончания процесса установки.*

1. Разрешим автозапуск сервера:

***systemctl enable nginx***

1. Проверяем результат:

***systemctl is-enabled nginx***

*Если в ответ получили «enabled», значит nginx успешно добавлен в автозагрузку.*

1. Запускаем наш веб-сервер:

***service nginx start***

1. Проверяем статус:

***service nginx status***

*Если в статусе присутствует строка Active: active (running), значит сервер работает. Также в этом можно убедиться, набрав в адресной строке браузера IP адрес сервера, будет отображено приветственное сообщение от nginx, которое выглядит так:*

****

Рисунок 2 - Приветственное сообщение от nginx

***Установка виртуальной машины Java***

Для работы стека ELK требуется виртуальная машина Java. Чтобы установить JVM:

1. Откройте окно терминала.
2. Установите программный пакет JVM, выполнив команду:

***sudo apt install default-jre -y***

*В результате будет установлен пакет Java Runtime Environment (JRE).*

1. Установите программный пакет JDK, включающий компилятор Java, стандартные библиотеки классов Java, примеры, документацию и различные утилиты. Для этого выполните команду:

***sudo apt install default-jdk –y***

***Установка и настройка Elasticsearch***

Чтобы установить и выполнить первичную настройку Elasticsearch:

1. Откройте окно терминала.
2. Импортируете открытый ключ GPG Elasticsearch, с использованием которого защищаются пакеты Elastic, выполнив команду:

***sudo wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add***

1. Добавьте пакеты Elastic в каталог системных репозиториев sources.list.d, выполнив команду:

***sudo echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list***

1. Обновите индексы пакетов, выполнив команду:

***sudo apt update***

1. Установите Elasticsearch, выполнив команду:

***sudo apt install elasticsearch***

1. Внесите изменения в конфигурационный файл elasticsearch.yml.

Для этого:

* Откройте этот файл для редактирования, выполнив команду:

***sudo nano /etc/elasticsearch/elasticsearch.yml***

* Найдите строку:

***#network.host: 192.168.0.1***

И замените ее на строку:

***network.host: localhost***

*Для поиска по файлу используйте сочетание клавиш CTRL+W.*

*После редактирования конфигурационного файла \*.yml убедитесь, что в нем нет лишних пробелов и/или отступов!*

*Сохраните изменения, используя сочетание клавиш CTRL+O, и завершите редактирование, используя сочетание клавиш CTRL+X.*

1. Запустите сервис Elasticsearch, выполнив команду:

***sudo systemctl start elasticsearch***

1. Проверьте статус запуска сервиса Elasticsearch, выполнив команду:

***sudo systemctl status elasticsearch***

1. Чтобы при перезагрузке операционной системы сервис Elasticsearch запускался автоматически, выполните команду:

***sudo systemctl enable elasticsearch***

1. Для проверки доступа к сервису Elasticsearch отправьте HTTP-запрос, выполнив команду:

***curl -X GET localhost:9200***

*Если установка Elasticsearch выполнена успешно, отобразится следующая информация:*

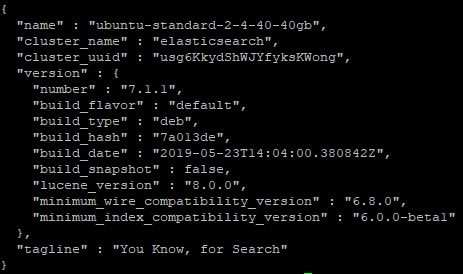
****

Рисунок 3 – Успешная установка Elasticsearch

***Установка и настройка Kibana***

Чтобы установить и выполнить первичную настройку Kibana, выполните следующее:

1. Убедитесь, что вы успешно установили Elasticsearch.
2. Откройте окно терминала.
3. Установите Kibana, выполнив команду:

***sudo apt install kibana***

1. Внесите изменения в конфигурационный файл kibana.yml. Для этого:

* Откройте этот файл, выполнив команду:

***sudo nano /etc/kibana/kibana.yml***

* Найдите строку:

***#server.port: 5601***

* И замените ее на строку:

***server.port: 5601***

* Найдите строку

***#server.host: "localhost"***

* и замените ее на строку:

***server.host: "localhost"***

* Найдите строку:

***#elasticsearch.hosts: ["http://localhost:9200"]***

* И замените ее на строку:

***elasticsearch.hosts: ["http://localhost:9200"]***

1. Запустите Kibana, выполнив команду:

***sudo systemctl start kibana***

1. Чтобы при перезагрузке операционной системы сервис Kibana запускался автоматически, выполните команду:

***sudo systemctl enable kibana***

1. Для проверки статуса работы Kibana, выполните команду:

***sudo systemctl status kibana***

***Установка и настройка Packetbeat***

1. Установите необходимые пакеты, выполнив команду:

***sudo apt-get install libpcap0.8***

1. Для загрузки и установки Packetbeat используйте команды:

***curl -L -O https://artifacts.elastic.co/downloads/beats/packetbeat/packetbeat-7.6.1-amd64.deb***

***sudo dpkg -i packetbeat-7.6.1-amd64.deb***

1. Откройте файл конфигурации Packetbeat под названием packetbeat.yml.

***nano /etc/packetbeat/packetbeat.yml***

1. Внесите изменения в конфигурационный файл packetbeat.yml:

* Найдите строку:

***setup.kibana***

* И замените ее на строку:

***setup.kibana:***

***host: "localhost:5601"***

1. Используйте следующую команду для создания панелей мониторинга Packetbeat на сервере Kibana:

***packetbeat setup***

1. Запустите службу Packetbeat:

***sudo systemctl start packetbeat***

1. Настройте службу Packetbeat для запуска во время загрузки.

***sudo systemctl enable packetbeat***

***Кибана - Доступ к панели мониторинга Packetbeat***

1. Откройте браузер и введите IP-адрес вашего сервера Kibana плюс: 5601.

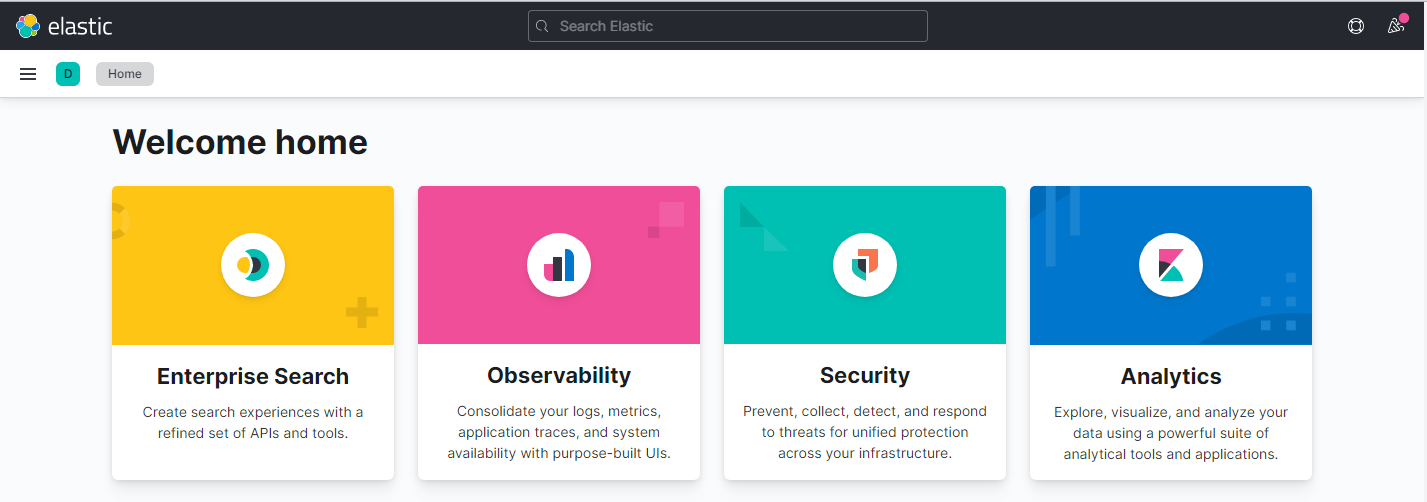


Рисунок 4 - Веб-интерфейс Kibana

1. Откройте вкладку Settings. Выберите packetbeat-\* в меню Index Patterns.
2. Затем откройте вкладку Discover. Здесь вы можете просматривать и фильтровать различные записи Packetbeat, добавлять в просмотр новые поля и визуализировать их.

## **ПРИЛОЖЕНИЕ Б**

Лабораторная работа №2

«Определение IP адресов и стран участников сетевой сессии»

**Цель работы:**

Изучить интерфейс Kibana. Настроить геопозицию адресов, с которых отправлялись запросы с тестовом дампе трафика.

**Схема:**

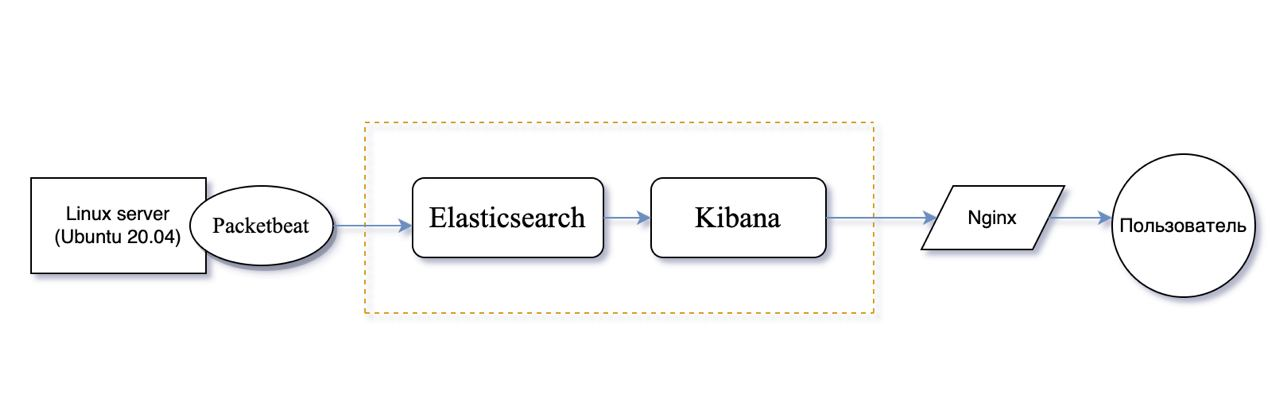


Рисунок 1 - Схема лабораторной работы

**Описание лабораторной работы:**

Даная лабораторная работа направленна на изучение и работу с интерфейсом программного обеспечения компании Elasctic.

Для выполнения лабораторной работы понадобится:

* Виртуальная машина с предустановленной операционной системой семейства UNIX (в нашем случае используется Ubuntu 20.04) и следующими характеристиками:

Таблица 2 - Характеристики виртуальной машины

|  |  |
| --- | --- |
| CPU | 4+ |
| Memory | 8 Gb |
| Disk | 20 Gb |

* Предустановленное и настроенное программное обеспечение компании elastic:
  + elasticsearch
  + kibana
* packetbeat Базовые знания работы с командной строкой UNIX-подобных операционных систем
* Понимание принципов работы сетевой маршрутизации в глобальной сети Интернет
* Понимание принципов работы сетевых протоколов модели OSI

**Порядок выполнения:**

1. Скачайте трафик на ваш сервер [ссылка](https://drive.google.com/file/d/1ElfYq1EFRv2j8moXIAcm0OEaTVRU35Xq/view?usp=sharing)
2. Откройте окно терминала.
3. Воспроизведите данный трафик с помощью команды:

***tcpreplay --intf1=ens192 lb2.pcap***

1. Откройте браузер и введите IP-адрес вашего сервера Kibana плюс: 5601
2. В разделе «Analytics» выберите вкладку «Discover»

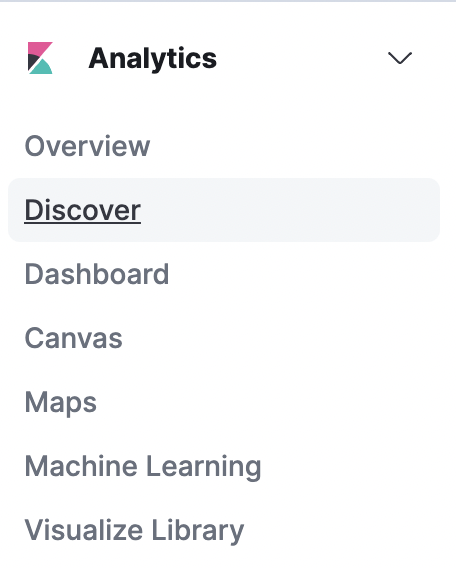


Рисунок 2 – Раздел «Analytics»

1. Далее верхнем правом углу страницы выберите нужный промежуток времени

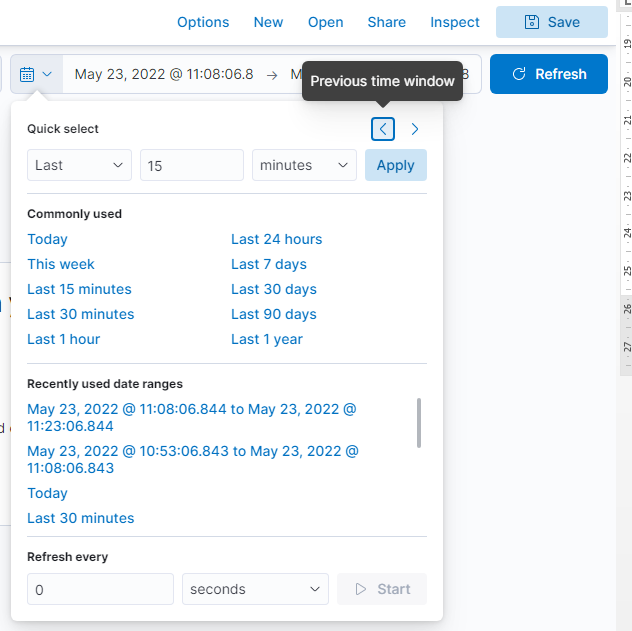


Рисунок 3 – Выбор промежутка времени

1. Убедитесь в появление логов

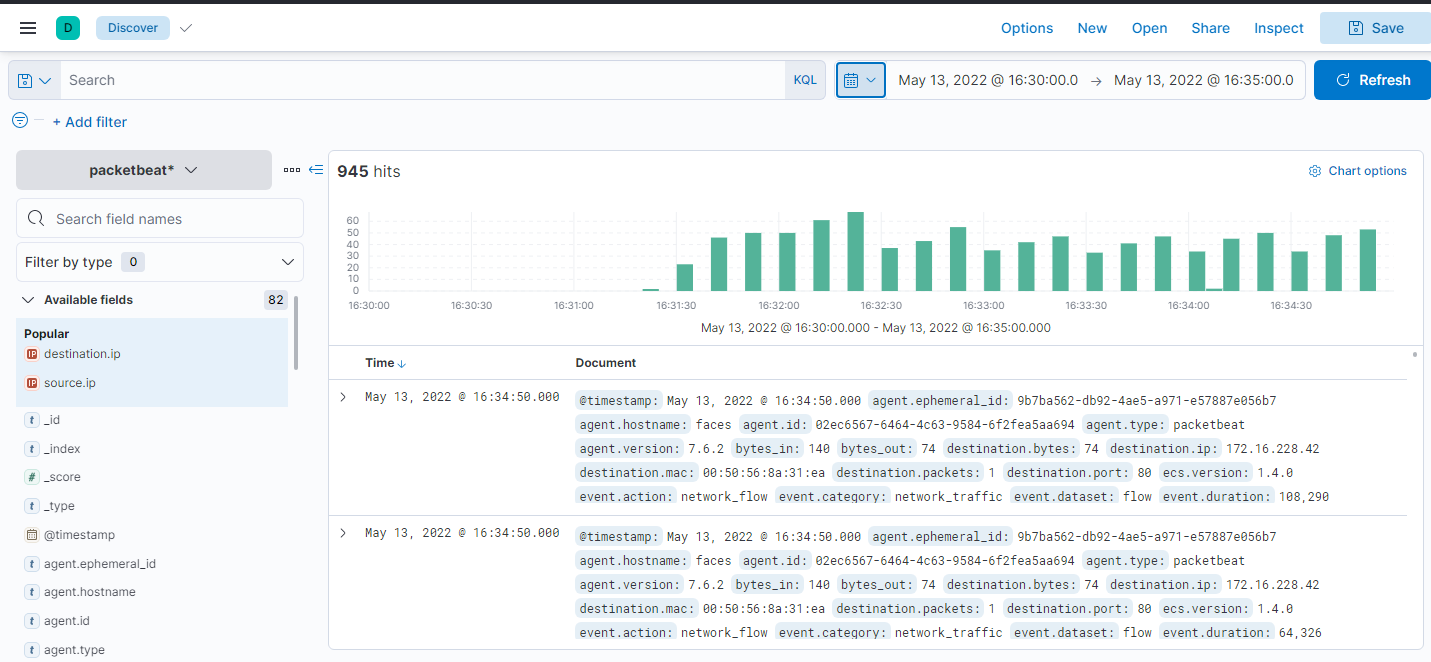


Рисунок 4 - Логи

1. В разделе «Analytics» выберите вкладку «Visualize Library»
2. Нажмите на «Create Visualization»

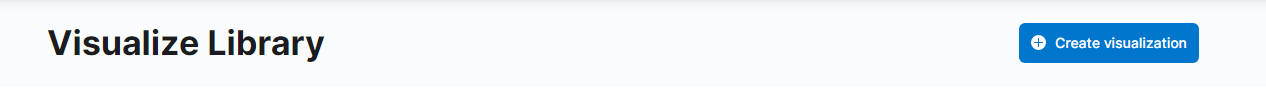


Рисунок 5 - Вкладка «Visualize Library»

1. Далее выберете «lens»

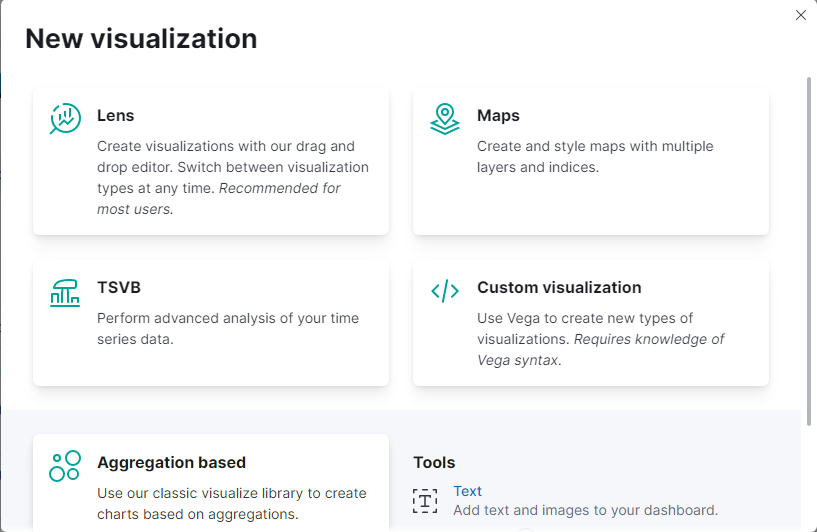


Рисунок 6 -Визуализация

1. Выберите тип визуализации «Table»

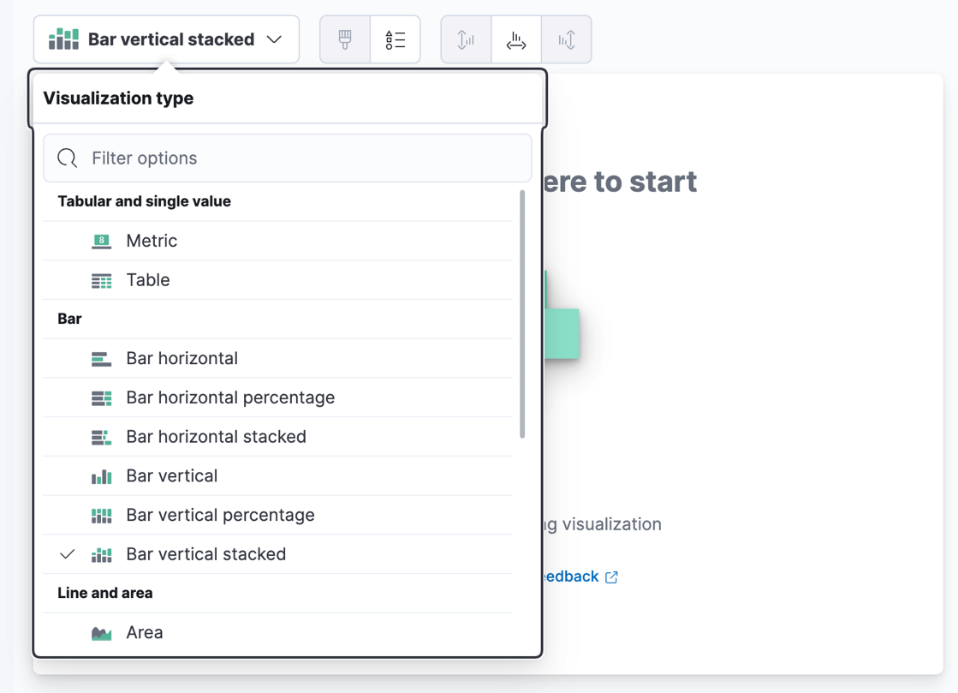


Рисунок 7- Тип визуализации

1. Настройте визуализацию. Для этого перетащите поля «source.ip» и «source.geo.country\_name» в центр страницы.

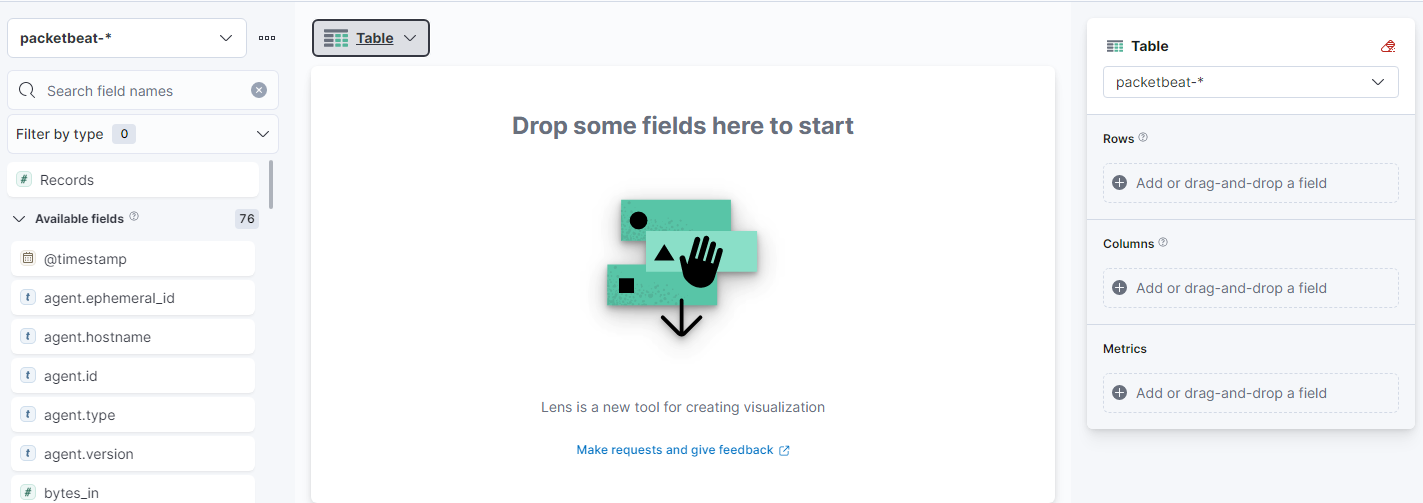


Рисунок 8 – Настройка визуализации

1. Далее сохраните и добавьте визуализацию в панель управления, нажав на кнопку «Save».

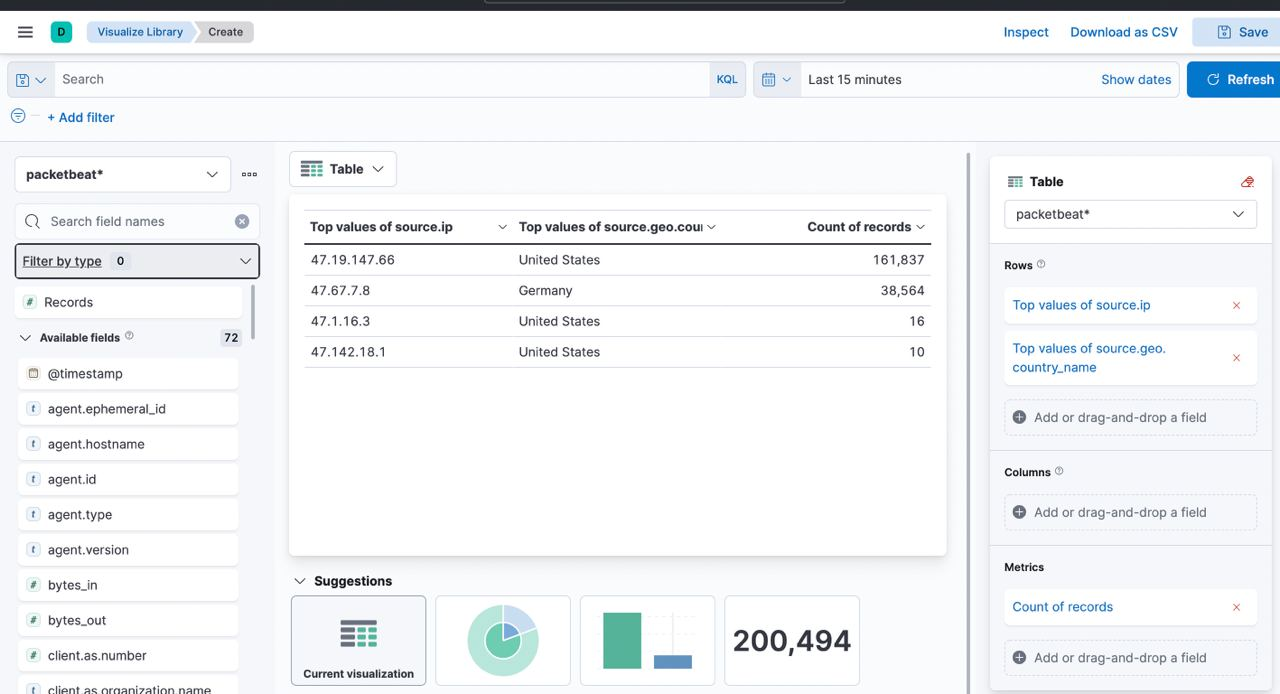


Рисунок 9 – Готовый dashboard

## **ПРИЛОЖЕНИЕ В**

Лабораторная работа №3

«Обнаружения сканирования узлов»

**Цель работы:**

Изучить интерфейс Kibana. Научится использовать интерфейс для обнаружения сетевых атак.

**Схема:**

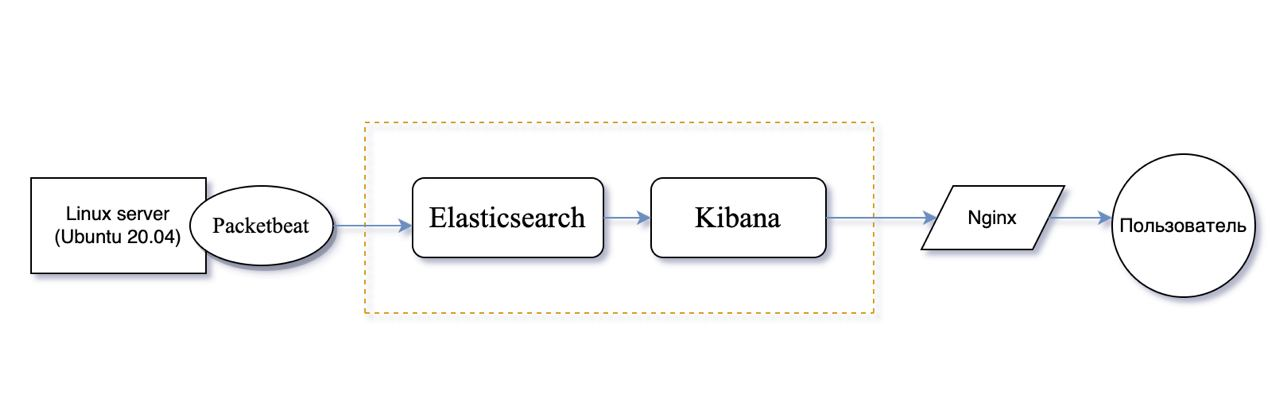


Рисунок 1 – Схема лабораторной рабы

**Описание лабораторной работы:**

Данная лабораторная работа направленна на изучение и работу с интерфейсом программного обеспечения компании Elasctic

Для выполнения лабораторной работы понадобится:

* Виртуальная машина с предустановленной операционной системой семейства UNIX (в нашем случае используется Ubuntu 20.04) и следующими характеристиками:

Таблица 3 - Характеристики виртуальной машины

|  |  |
| --- | --- |
| CPU | 4+ |
| Memory | 8 Gb |
| Disk | 20 Gb |

* Предустановленное и настроенное программное обеспечение компании elastic:
* elasticsearch
* kibana
* packetbeat
* Понимание принципов работы сетевой маршрутизации в глобальной сети Интернет
* Понимание принципов работы сетевых протоколов модели OSI

**Порядок выполнения:**

* 1. Скачайте трафик на ваш сервер [ссылка](https://drive.google.com/file/d/1IOiiKnrD6Xn8J1odMXrd8q1ViI8VzLHS/view?usp=sharing)
  2. Откройте окно терминала.
  3. Воспроизведите данный трафик с помощью команды:

***tcpreplay --intf1=ens192 lb3.pcap***

* 1. Откройте браузер и введите IP-адрес вашего сервера Kibana плюс: 5601
  2. В разделе «Analytics» выберите вкладку «Discover»

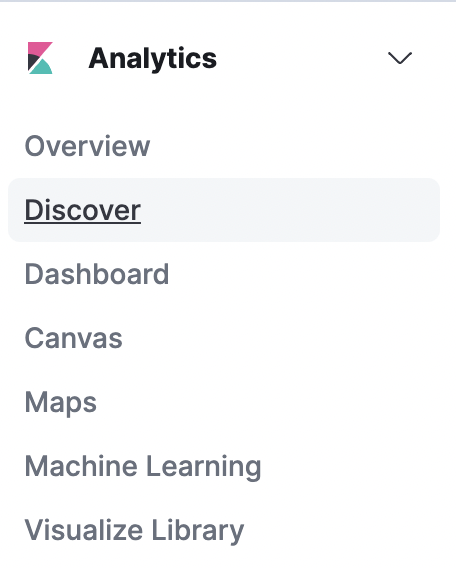


Рисунок 2 – Раздел «Analytics»

* 1. Далее верхнем правом углу страницы выберите нужный промежуток времени

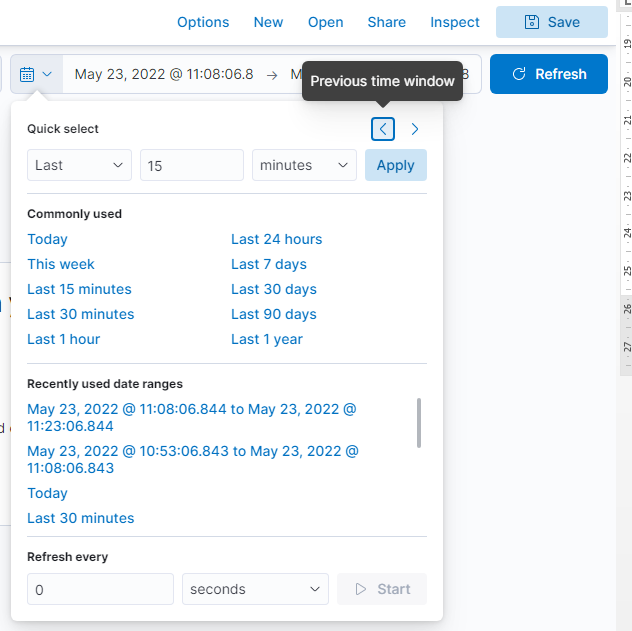


Рисунок 3 – Выбор промежутка времени

* 1. Убедитесь в появление логов

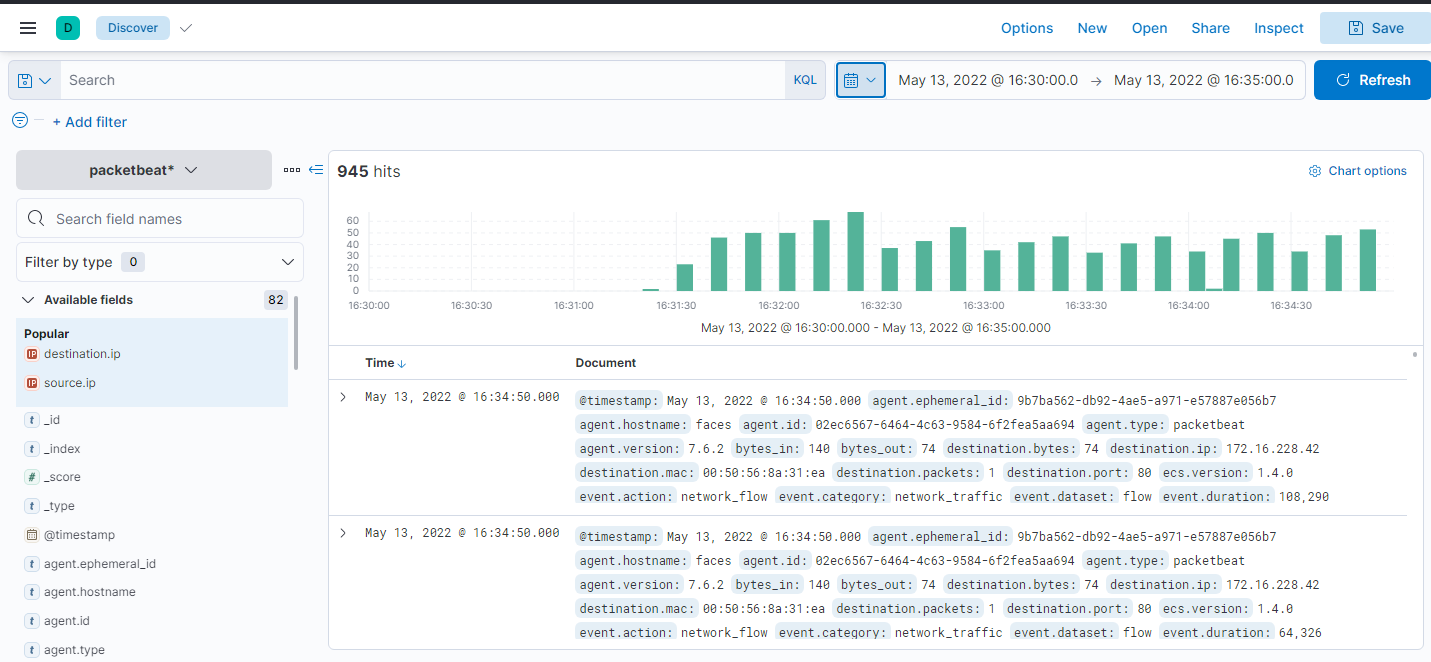


Рисунок 4 –Логи

* 1. В разделе «Analytics» выберите вкладку «Visualize Library»
  2. Нажмите на «Create Visualization»

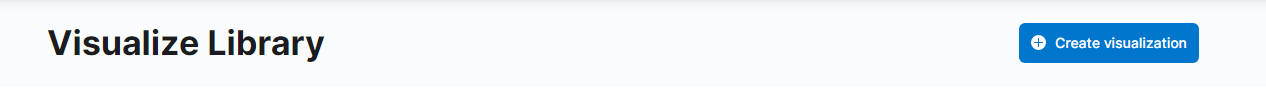


Рисунок 5 - Вкладка «Visualize Library»

* 1. Далее выберете «lens»

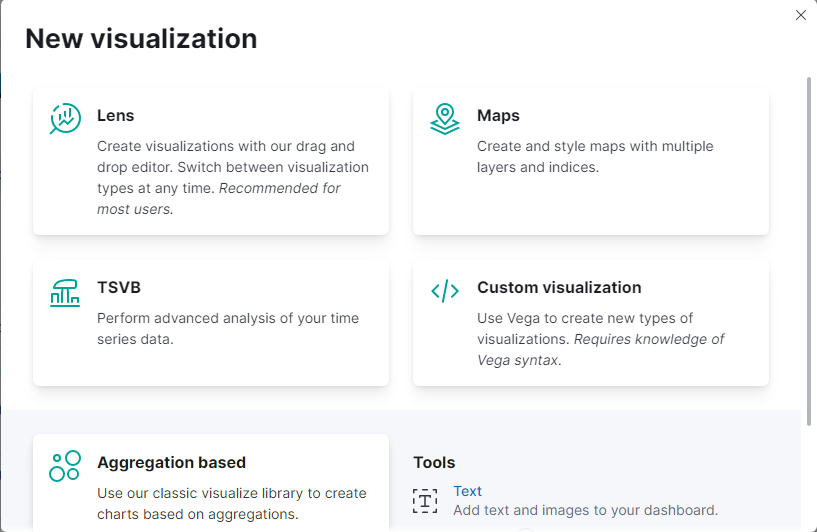


Рисунок 6 - Визуализауция

* 1. Выберите тип визуализации «Table»

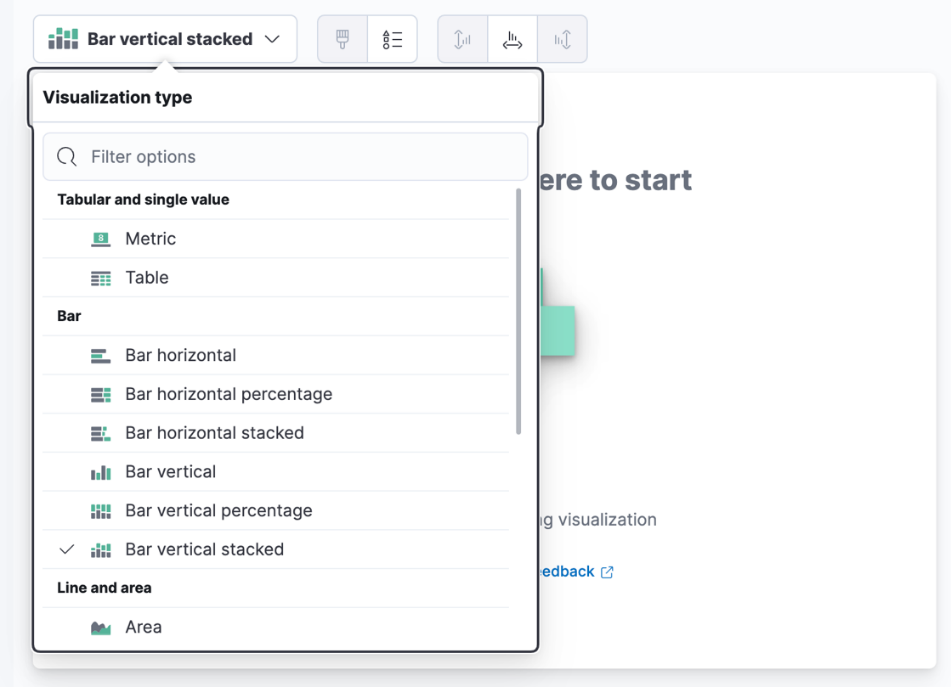


Рисунок 7 – Тип визуализации

* 1. Настройте визуализацию. Для этого перетащите поля «source.ip», «source.port», «destination.ip» и «destination.port» в центр страницы.

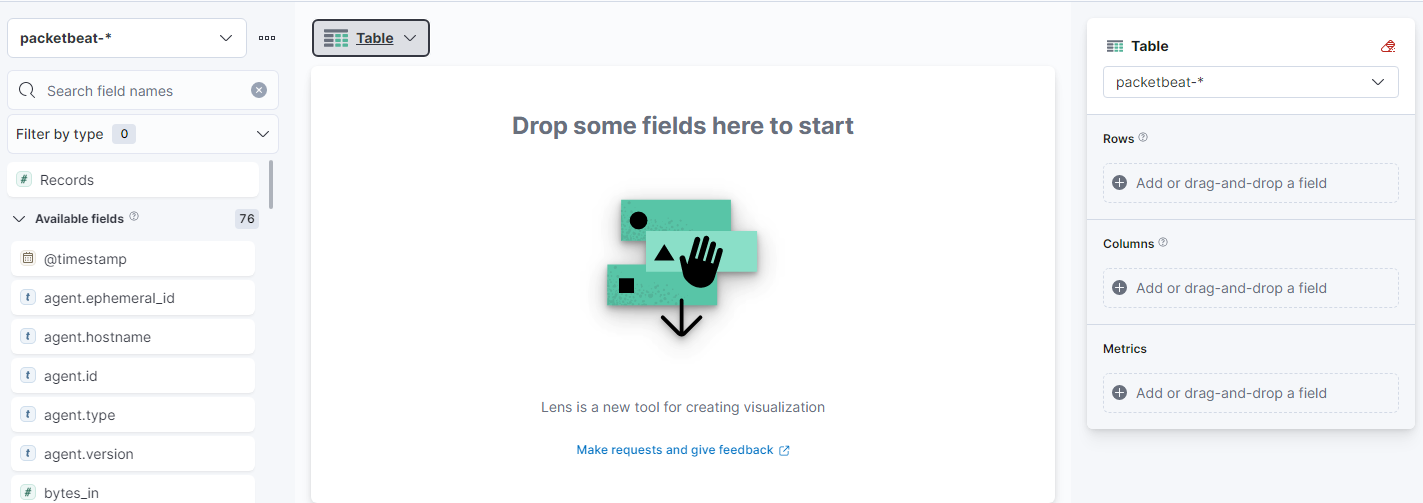


Рисунок 8 – Настройка визуализации

* 1. В разделе «Metrics» выбираем *Median of source.port*

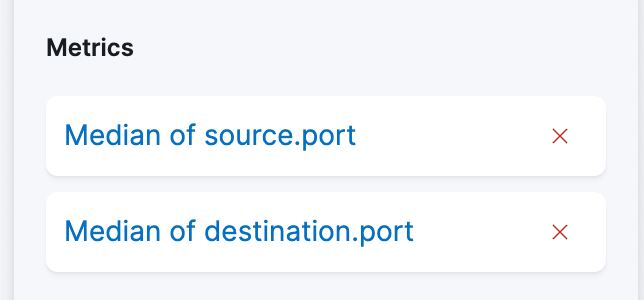


Рисунок 9 – Раздел «Metrics»

* 1. Далее выбираем функцию «Unique count»

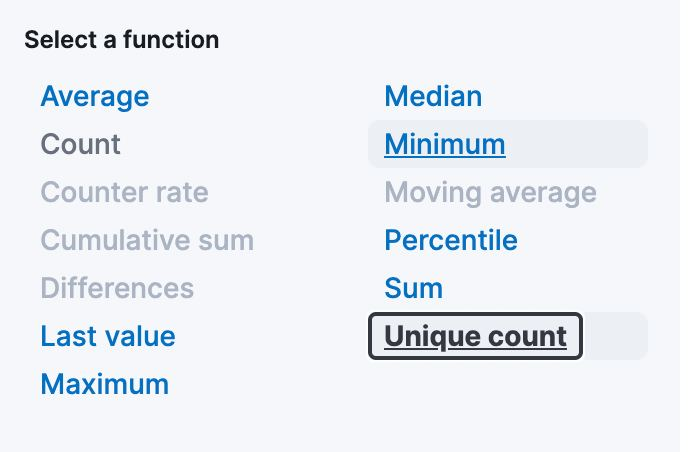


Рисунок 10 – Выбор функции

* 1. Пункты повторяем для *Median of destination.port*
  2. Далее сохраните и добавьте визуализацию в панель управления, нажав на кнопку «Save».

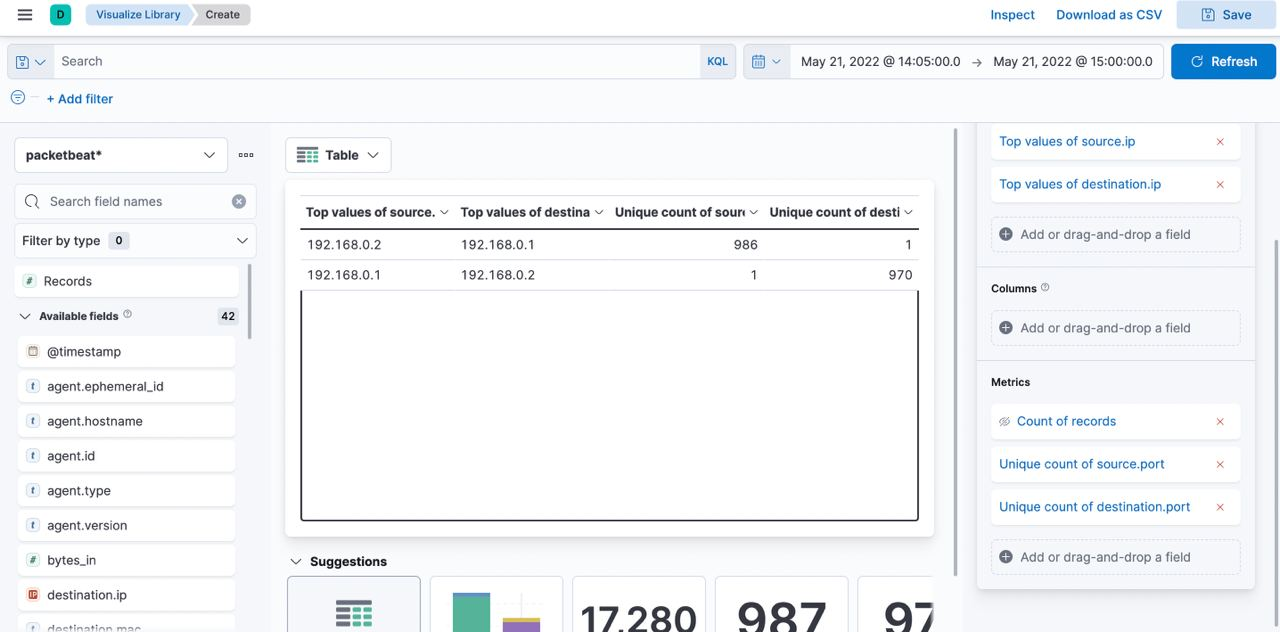


Рисунок 11 – Готовый dashbord

1. Дата начала работы по плану должна совпадать с началом преддипломной практики в календарном графике учебного процесса по соответствующему направлению подготовки, а дата окончания работы по плану – с окончанием государственной итоговой аттестации [↑](#footnote-ref-1)