МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

МАТЕРИАЛЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Технологии хранения в системах кибербезопасности

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень	специалитет
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление(-я) подготовки	10.05.04 Информационно-аналитические системы безопасности
	(код(-ы) и наименование(-я))
Институт	Кибербезопасности и цифровых технологий (ИКБ)
	(полное и краткое наименование)
Кафедра	КБ-2 «Информационно-аналитические системы кибербезопасности»
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))
Лектор	к.т.н., Селин Андрей Александрович, Бугаев Александр Александрович
	(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2024/2025

(учебный год цифрами)

Проверено и согласовано «____» _____2024 г. _____ А.А. Бакаев

(подпись директора Института/Филиала с расшифровкой)

Москва 2024 г.

ПРАКТИЧЕСКАЯ РАБОТА № 5

«Знакомство с инструментами анализа данных. Использование стека OpenSearch»

Цель работы – получение практических навыков развертывания кластера OpenSearch и анализа данных в OpenSearch Dashboards.

Задание:

1. Запустите Unix-подобную систему (например, Debian 12.6.0 64-bit[1]).

2. Создайте пользователя с именем формата **fio_nn**,
где f – первая буква фамилии на латинице;
i – первая буква имени на латинице;
o – первая буква отчества на латинице (при наличии),
nn – двузначный номер по списку в группе.

Добавьте его в группу sudo. **Все дальнейшие действия необходимо выполнять от имени созданного пользователя.**

3. Запустите терминал и установите Docker и Docker Compose.

4. Установите значение параметра **vm.max_map_count** равным **262144**. Это параметр ядра, который определяет максимальное количество областей памяти, доступных процессу. OpenSearch (Elasticsearch) рекомендует устанавливать значение данного параметра как минимум 262144.

Пример временного изменения параметра (будет сброшено после перезагрузки системы):
sudo sysctl -w vm.max_map_count=262144

Чтобы сделать изменение постоянным, нужно добавить в файл **/etc/sysctl.conf** строку следующего формата:
vm.max_map_count=262144

[1] Можно скачать готовый образ виртуальной машины по ссылке https://sourceforge.net/projects/osboxes/files/v/vb/14-D-b/12.6.0/64bit.7z/download

5. Изучите:

– основные понятия для Elasticsearch/OpenSearch (документ, кластер, узел, индекс, шард, реплика) – https://opensearch.org/docs/latest/getting-started/intro;

– формат шаблона индекса (https://opensearch.org/docs/latest/im-plugin/index-templates);

– основные возможности Opensearch Dashboards (https://opensearch.org/docs/latest/dashboards/quickstart);

– примеры дашбордов для Opensearch Dashboards (https://playground.opensearch.org/app/home#/tutorial_directory).

6. Разверните OpenSearch и OpenSearch Dashboards с помощью Docker Compose. Образец файла docker-compose.yml можно найти на официальном сайте: https://opensearch.org/docs/latest/install-and-configure/install-opensearch/docker.

Требования к запускаемым сервисам:

– последние 2 цифры номера порта, на котором будет развернут сервис, должны соответствовать номеру по списку в группе (например, для 3 – 12303, 8003, 9903 и т.п.);

– имя контейнера должно заканчиваться на символ подчеркивания и инициалы ФИО (например, для Иванова Петра Дмитриевича – opensearch_ipd, dashboards_ipd).

6.1. В переменной **OPENSEARCH_INITIAL_ADMIN_PASSWORD** задайте сложный пароль, иначе контейнеры OpenSearch не будут работать. При простом пароле будет выведено сообщение:
«Password does not match validation regex. Please re-try with a minimum 8 character password and must contain at least one uppercase letter, one lowercase letter, one digit, and one special character that is strong. Password strength can be tested here: https://lowe.github.io/tryzxcvbn».

6.2. Для контейнеров OpenSearch в разделе environment добавьте параметр:
plugins.security.disabled=true

6.3. Для контейнера OpenSearch Dashboards в разделе environment добавьте параметр:
DISABLE_SECURITY_DASHBOARDS_PLUGIN: true

7. Установите ПО TShark (инструмент для сетевого анализа пакетов):
sudo apt-get install tshark

Проверьте работоспособность, запустив захват пакетов:
sudo tshark

Для просмотра списка сетевых интерфейсов используется команда:
sudo tshark -D

Для захвата пакетов с конкретного интерейса (например, enp0) используется команда:
sudo tshark -i enp0

Документация для TShark:
https://www.wireshark.org/docs/man-pages/tshark.html

8. Скачайте не менее 5 образцов трафика от вредоносного программного обеспечения (https://www.malware-traffic-analysis.net) по следующему правилу:
202A-BB-CC, где **A** – номер группы, **BB** – результат деления номера по списку по модулю 10 (например, для 23 – 3). Если для вас нет подходящих файлов, то используйте соседние значения **BB** (+/- 1).

9. Соберите статистические данные от скачанных PCAP-файлов с помощью TShark.
Минимальный набор полей:

- Дата и время пакета (frame.time_epoch);
- IP-адрес отправителя (ip.src);
- IP-адрес получателя (ip.dst);
- Стек используемых протоколов (frame.protocols);
- Имя хоста по протоколу HTTP (http.host);
- Порты отправителя и получателя для протоколов TCP и UDP (4 поля);
- Имя хоста по протоколу TLS;
- Размер пакета.

Обязательно добавьте еще несколько полей по вашему усмотрению. Выберите их при анализе образцов вредоносного трафика. **Поясните, почему выбрали их**.

Точные названия полей необходимо посмотреть в ПО Wireshark (некоторые представлены выше).

Пример команды для сбора статистических данных, в которых поле «http.host» содержит значение:

sudo tshark -r example_malware.pcap -Y "http.host" -T fields -e frame.time_epoch -e ip.src -e ip.dst -e tcp.srcport -e tcp.dstport -e http.host -e frame.protocols -E header=y -E separator=\; -E aggregator=, > result_ipd.csv

```
frame.time_epoch;ip.src;ip.dst;tcp.srcport;tcp.dstport;http.host;frame.protocols
1533323180.363204000;192.168.10.195;192.0.79.32;49714;80;college.usatoday.com;eth:ethertype:ip:tcp:http
1533323180.919913000;192.168.10.195;52.84.125.10;49727;80;dl5krst4gi8g86.cloudfront.net;eth:ethertype:ip:tcp:http
1533323180.924848000;192.168.10.195;52.84.125.10;49729;80;dl5krst4gi8g86.cloudfront.net;eth:ethertype:ip:tcp:http
1533323180.930780000;192.168.10.195;52.84.125.10;49728;80;dl5krst4gi8g86.cloudfront.net;eth:ethertype:ip:tcp:http
1533323180.936368000;192.168.10.195;52.84.125.10;49730;80;dl5krst4gi8g86.cloudfront.net;eth:ethertype:ip:tcp:http
1533323180.941713000;192.168.10.195;52.84.125.10;49731;80;dl5krst4gi8g86.cloudfront.net;eth:ethertype:ip:tcp:http
1533323180.952938000;192.168.10.195;52.84.125.10;49732;80;dl5krst4gi8g86.cloudfront.net;eth:ethertype:ip:tcp:http
1533323180.958849000;192.168.10.195;192.0.72.22;49735;80;usatcollege.files.wordpress.com;eth:ethertype:ip:tcp:http
1533323180.964495000;192.168.10.195;192.0.72.22;49736;80;usatcollege.files.wordpress.com;eth:ethertype:ip:tcp:http
1533323180.975407000;192.168.10.195;23.211.124.129;49733;80;admin.brightcove.com;eth:ethertype:ip:tcp:http
1533323180.991825000;192.168.10.195;192.0.72.22;49740;80;usatcollege.files.wordpress.com;eth:ethertype:ip:tcp:http
1533323181.003250000;192.168.10.195;192.0.77.32;49744;80;s0.wp.com;eth:ethertype:ip:tcp:http
1533323181.059316000;192.168.10.195;192.229.163.25;49752;80;platform.twitter.com;eth:ethertype:ip:tcp:http
1533323181.064263000;192.168.10.195;192.229.163.25;49753;80;platform.twitter.com;eth:ethertype:ip:tcp:http
1533323181.081571000;192.168.10.195;192.0.73.2;49756;80;0.gravatar.com;eth:ethertype:ip:tcp:http
1533323181.102741000;192.168.10.195;192.0.76.3;49760;80;stats.wp.com;eth:ethertype:ip:tcp:http
1533323181.280043000;192.168.10.195;72.21.91.29;49777;80;ocsp.digicert.com;eth:ethertype:ip:tcp:http
1533323181.285919000;192.168.10.195;216.58.218.238;49778;80;ocsp.pki.goog;eth:ethertype:ip:tcp:http
1533323181.346526000;192.168.10.195;216.58.218.238;49778;80;ocsp.pki.goog;eth:ethertype:ip:tcp:http
1533323181.355726000;192.168.10.195;72.167.239.239;49779;80;ocsp.godaddy.com;eth:ethertype:ip:tcp:http
1533323181.362754000;192.168.10.195;72.167.239.239;49780;80;ocsp.godaddy.com;eth:ethertype:ip:tcp:http
1533323181.408617000;192.168.10.195;216.58.218.238;49781;80;ocsp.pki.goog;eth:ethertype:ip:tcp:http
1533323181.629762000;192.168.10.195;72.167.239.239;49784;80;ocsp.godaddy.com;eth:ethertype:ip:tcp:http
```

Пояснения по параметрам:

-r – считывание данных из файла;

-Y – использование фильтра (аналогично строке фильтра в ПО Wireshark);

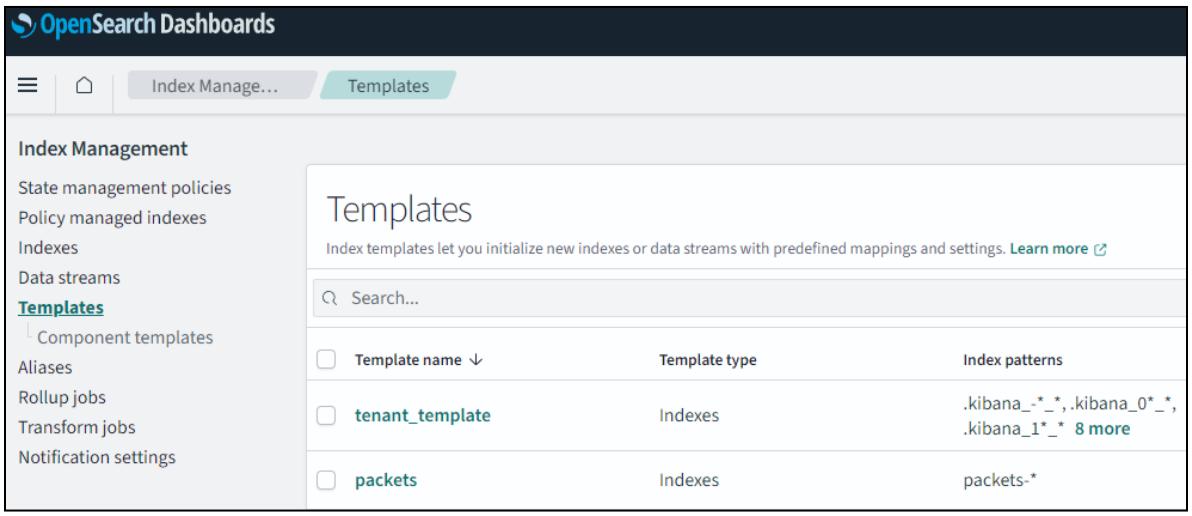
-T – формат выходных данных;

-e – указание требуемого поля (столбца в CSV-файле);

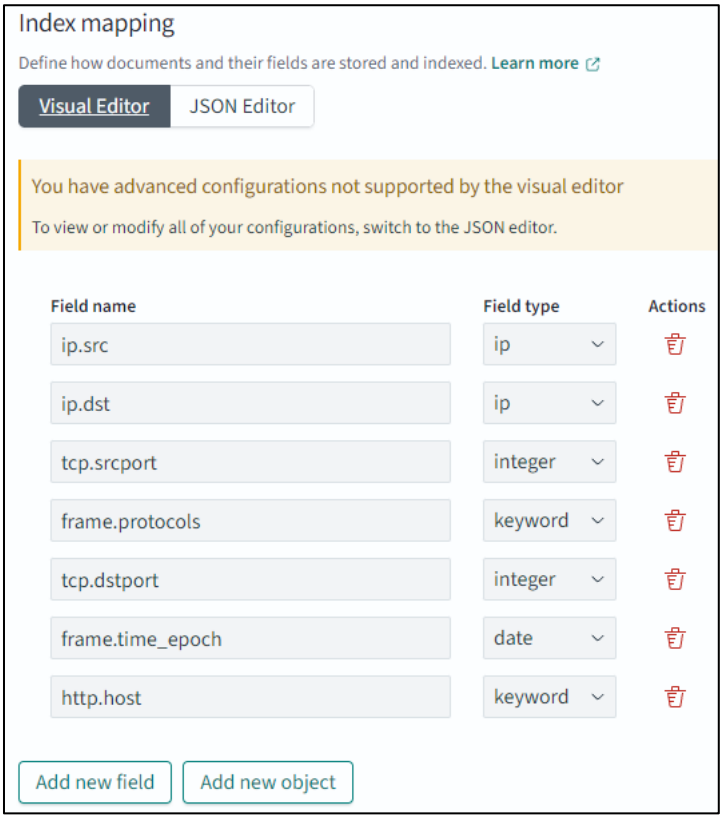
-E – указание параметров CSV-файла (**header=y** – указывает, что в выходном файле требуются заголовки; **separator=\;** – указывает, что разделителем значений в строке будет точка с запятой; **aggregator=,** – указывает, каким символом разделять значения в одном поле, если в пакете их будет несколько).

Сформируйте команду, содержащую **все требуемые поля**. Задайте корректный фильтр, чтобы сохранить наиболее важные и минимизировать неинформативные строки в результирующем файле.

10. Сформируйте шаблон индекса в OpenSearch Dashboards. В конце названия шаблона должны содержаться инициалы (например, packets_ipd).



Пример простого маппинга в настройках шаблона индекса:



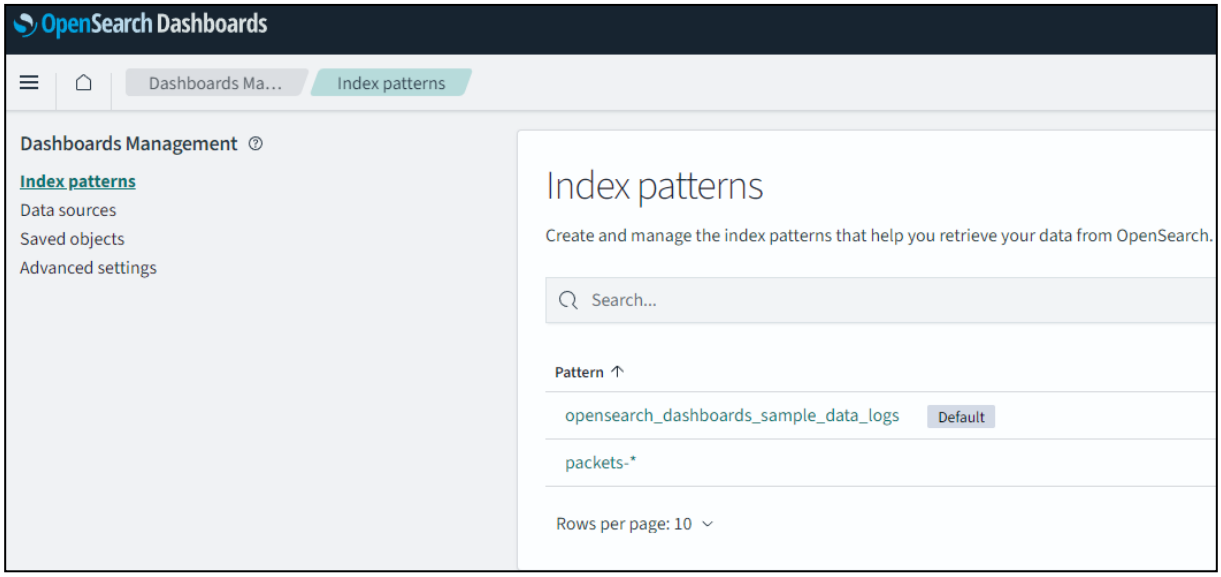
В «JSON Editor» обязательно укажите формат даты «epoch_second» для поля «frame.time_epoch»:

```
"frame.time_epoch": {
  "format": "epoch_second",
  "type": "date"
}
```

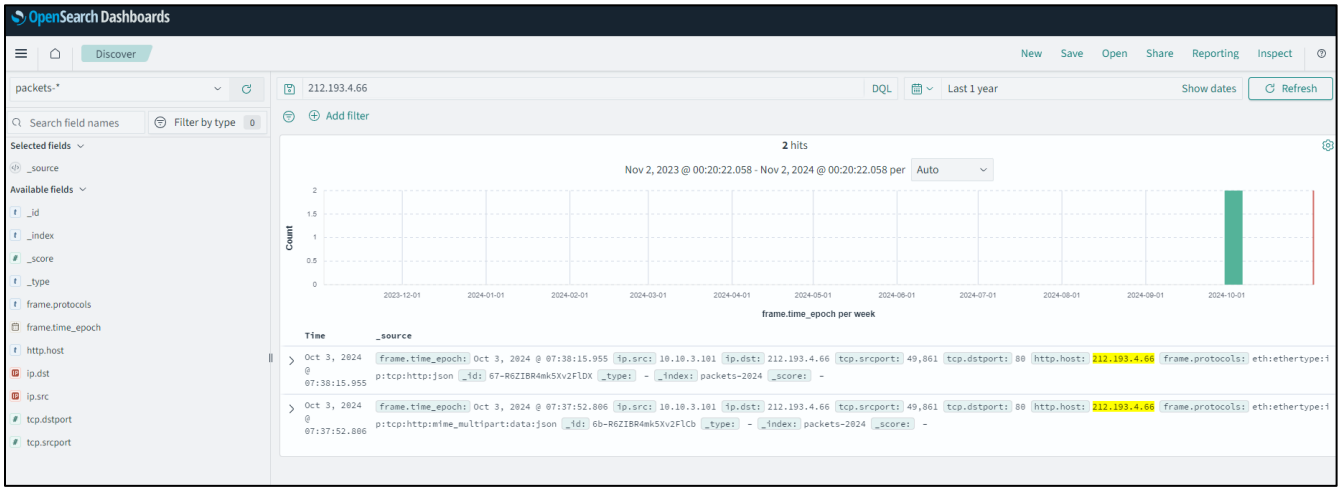
11. Загрузите полученные статистические данные в OpenSearch любым удобным способом. Ниже представлен пример на языке Python.

```python
from opensearchpy import OpenSearch
import pandas as pd

# Создание соединения с OpenSearch
client = OpenSearch(
hosts=["http://localhost:9200"]
)

# Чтение CSV-файла
df = pd.read_csv("result_ipd.csv", sep=';')

# Преобразование DataFrame в список словарей
data = df.to_dict(orient='records')

# Отправка документов в индекс
for doc in data:
  try:
    response = client.index(
      index = 'packets-2024',
      body = doc,
      refresh = True
  )
  except:
    continue
```

12. Для возможности анализа данных создайте Index Pattern в OpenSearch Dashboards.



13. Изучите возможности поиска и анализа данных в разделе «Discover» (не менее 5 различных запросов).



14. Сформируйте не менее 5 **различных** дашбордов (раздел «Dashboards»). Каждый должен иметь уникальное значение. **Поясните их назначение и какие выводы вы сделали по результатам анализа данных**.

15. **Дополнительно:** изучите и протестируйте **OpenSearch Alerting**. С помощью этой функции пользователи могут создавать оповещения для отслеживания данных в реальном времени или на основе запланированных интервалов.