**Лабораторная работа 4**

**Suricata и ELK**

**Индивидуальность отчетов:**

* имя пользователя и компьютера на скриншотах в соответствии с фамилией студента;
* индивидуальный график в Kibana.

**Источники:**

1. Часть 1:

<https://kifarunix.com/install-and-setup-suricata-on-ubuntu-18-04/>

<https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Ubuntu_Installation_-_Personal_Package_Archives_(PPA)>

2. Часть 2:

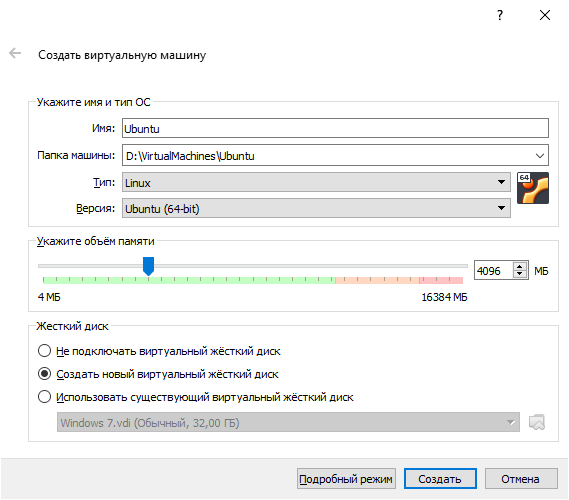
<https://www.elastic.co/guide/en/elasticsearch/reference/current/deb.html>

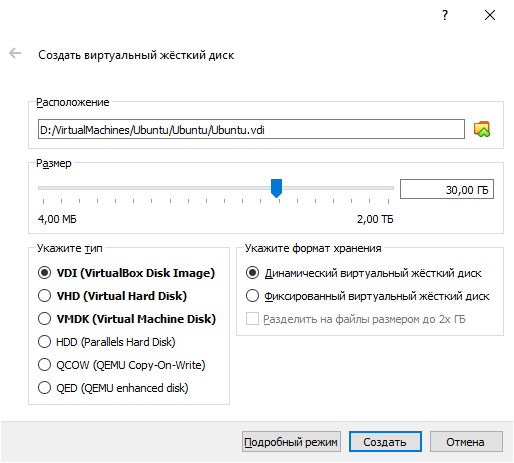
<https://www.howtoforge.com/tutorial/suricata-with-elk-and-web-front-ends-on-ubuntu-bionic-beaver-1804-lts/>

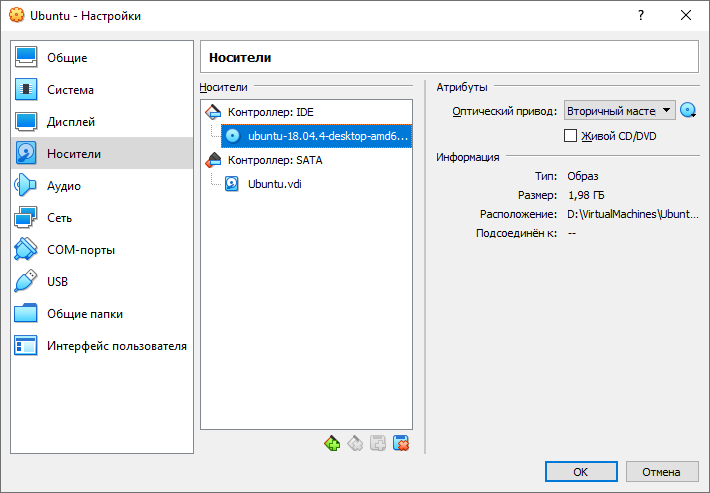
**Часть 1**

1. Создать виртуальную машину Ubuntu 18.04 LTS

<https://ubuntu.com/download/desktop>

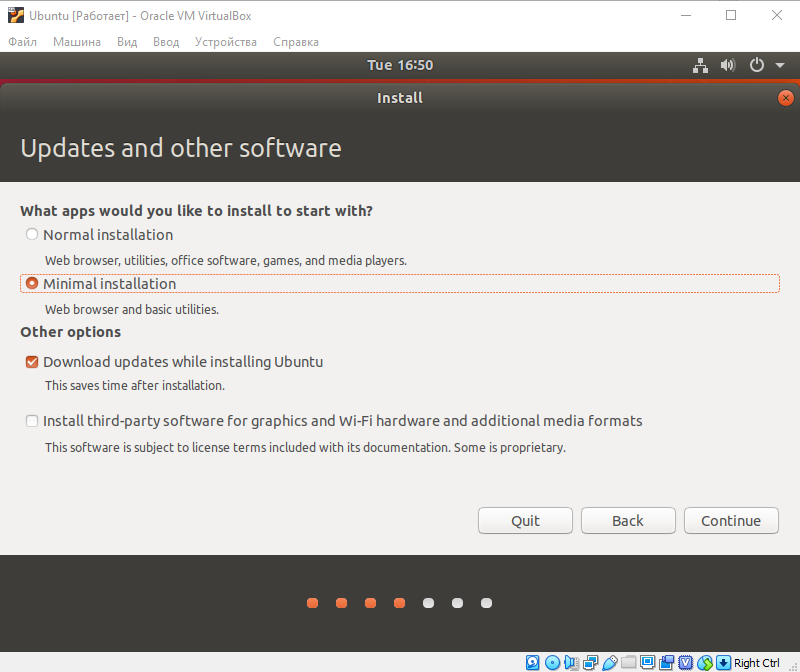






2. Установить Ubuntu

Имя пользователя – ваша фамилия на латинице. Если имя пользователя не будет соответствовать вашей фамилии – работа не засчтиывается.



3. Обновить ПО

sudo apt update

sudo apt upgrade

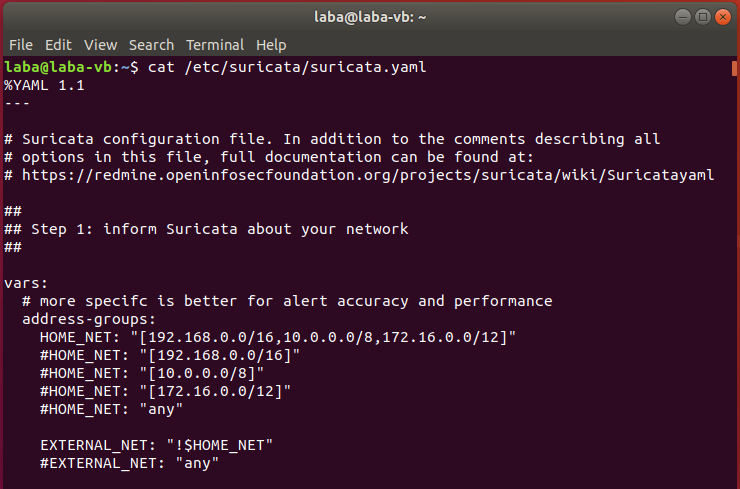
4. Установить Suricata

sudo apt install suricata

sudo apt autoremove

5. Проверить наличие файла suricata.yaml

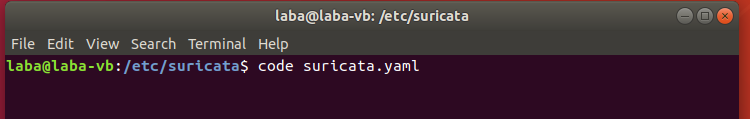
cat /etc/suricata/suricata.yaml

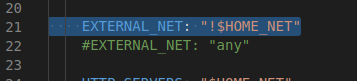


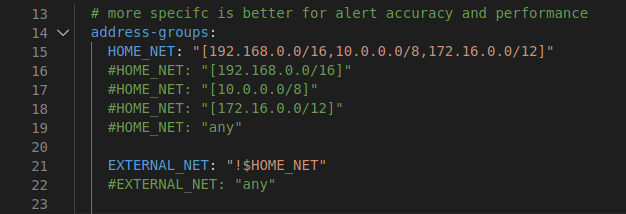
*По желанию можно поставить любой редактор*

*Я, например, ставлю Visual Studio Code прямо из Ubuntu Software*

6. Редактируем suricata.yaml







7. Ставим ifconfig

sudo apt install net-tools

ifconfig

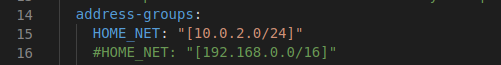


*Для справки:*

*255.0.0.0 - Class A (8-bit netmask)*

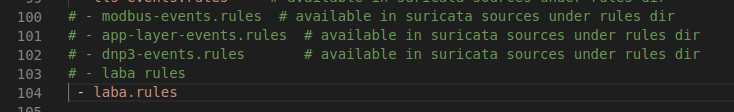
*255.255.0.0 - Class B (16-bit netmask)*

*255.255.255.0 - Class A (24-bit netmask)*

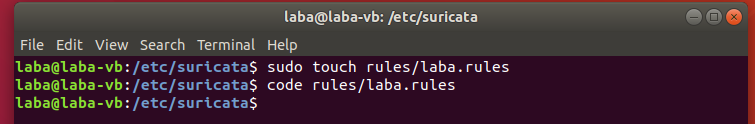


**Visual Studio Code попросит root права на сохранения**

8. Добавляем наш будущий файлик с нашими правилами



9. Создаем наши правила



Добавить туда правило:

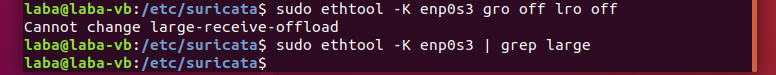
alert tcp any any -> $HOME\_NET 80 (msg: "Test possible ddos attack"; flags: S; flow: stateless; threshold: type both, track by\_dst, count 200, seconds 1; sid: 1000001; rev:1;)

10. Настраиваем сетевой интерфейс

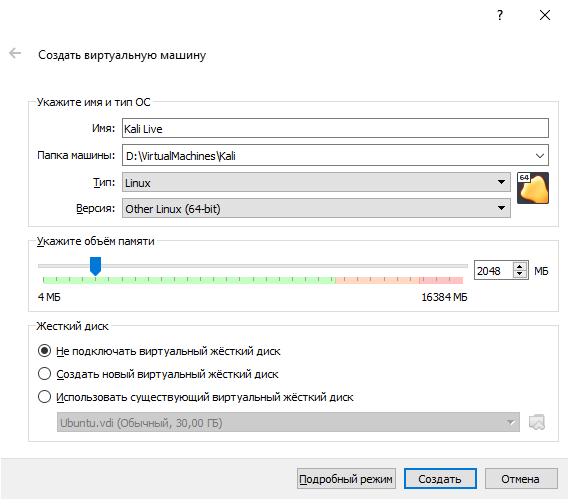
sudo apt install ethtool

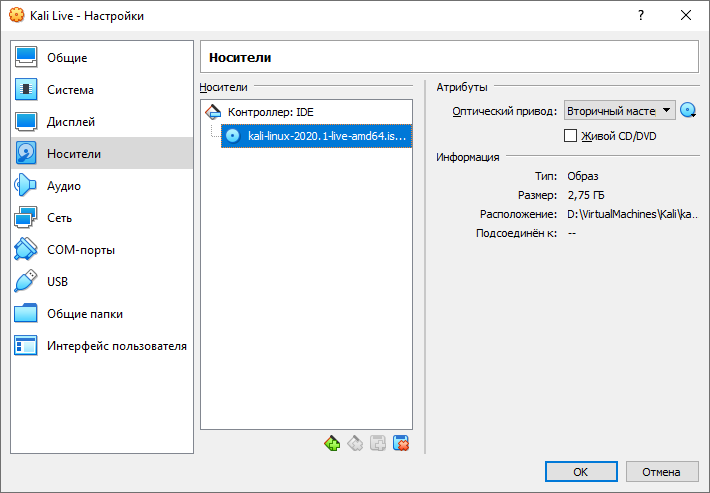
ethtool -K enp0s3 gro off lro off

*Это отключает large-receive-offload*

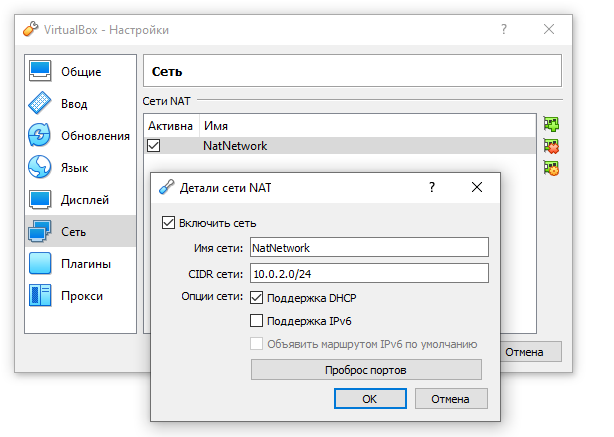


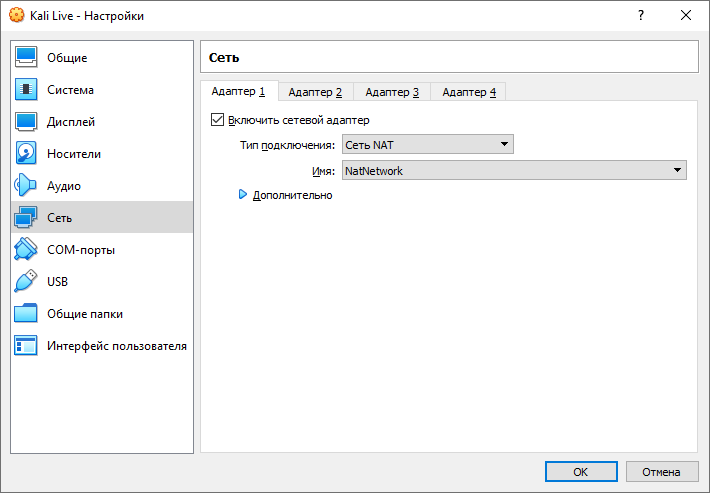
11. Создаём виртуальную машину Kali

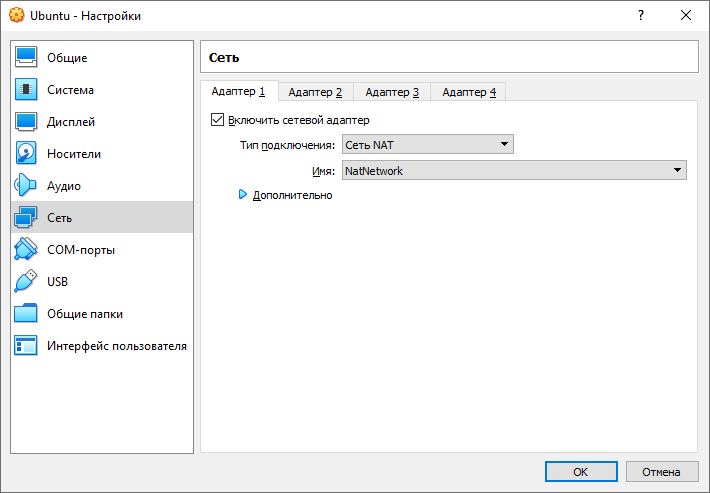




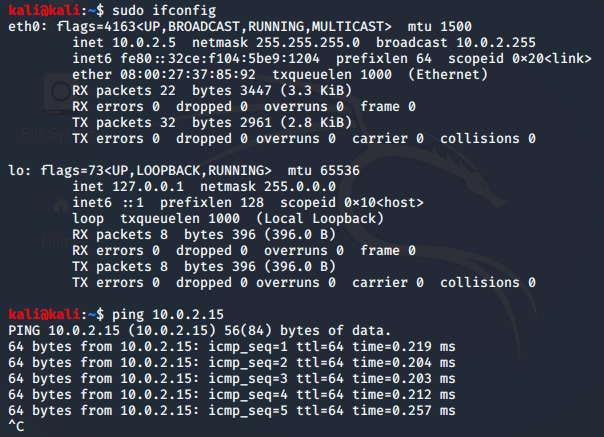
12. Настраиваем локальную сеть между компьютерами

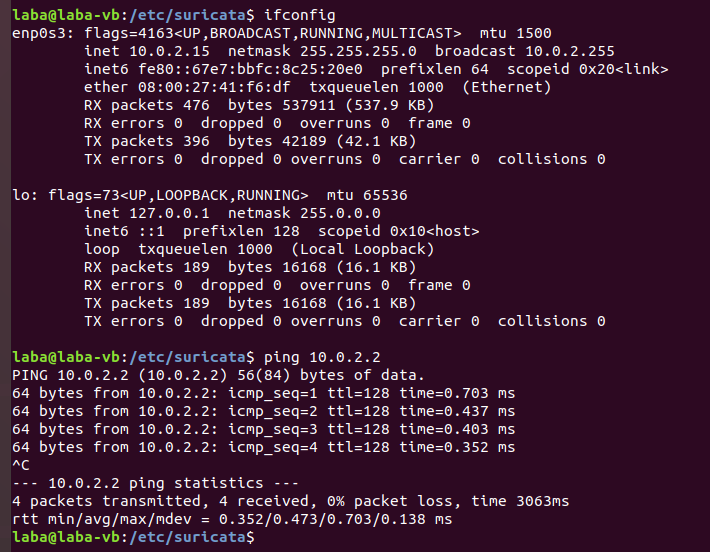






13. Проверяем пинги в обе стороны





14. Запускаем Suricata

sudo service suricata restart

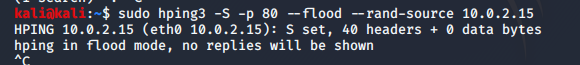
sudo suricata -c /etc/suricata/suricata.yaml -i enp0s3



15. На Kali

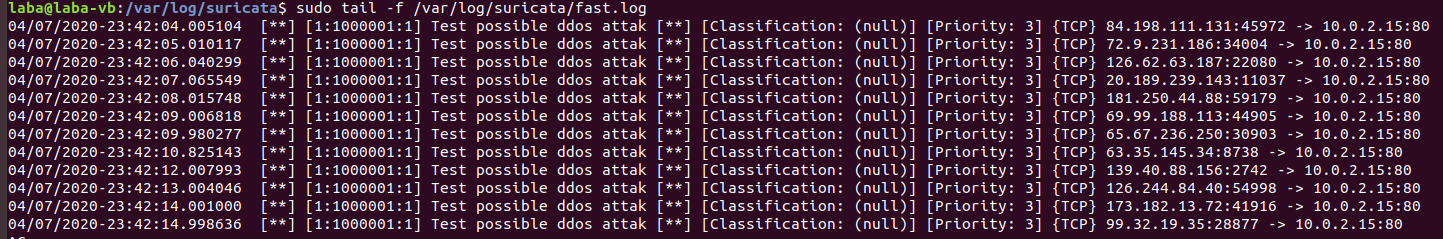
sudo apt install hping3

sudo hping3 -S -p 80 --flood --rand-source 10.0.2.15



16. Посмотри наши логи Suricata

sudo tail -f /var/log/suricata/fast.log



*Если обновить, то тогда будут ещё и встроенные правила срабатывать, но строчки с “Test possible ddos attack” тоже буду присутствовать*

**Часть 2**

1. Установим Java и зависимости

sudo apt-get install default-jre

sudo apt -y install libpcre3 libpcre3-dev build-essential autoconf automake libtool libpcap-dev libnet1-dev libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libmagic-dev libcap-ng-dev libjansson-dev pkg-config libnetfilter-queue-dev geoip-bin geoip-database geoipupdate apt-transport-https

2. Установим ELK

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

sudo apt-get install apt-transport-https

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

sudo apt-get update && sudo apt-get install elasticsearch

sudo apt install kibana

sudo apt install logstash

sudo /bin/systemctl daemon-reload

sudo /bin/systemctl enable elasticsearch.service

sudo /bin/systemctl enable kibana.service

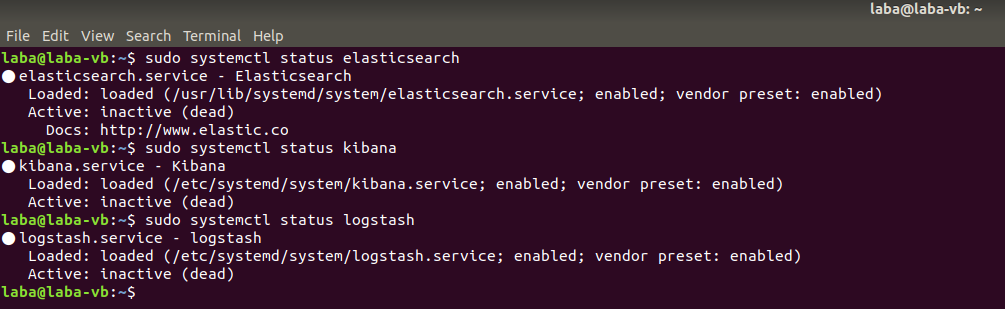
sudo /bin/systemctl enable logstash.service

Проверим статус служб

sudo systemctl status elasticsearch

sudo systemctl status kibana

sudo systemctl status logstash



3. Дадим права, чтобы Logstash мог читать логи

sudo usermod -a -G adm logstash

sudo chmod 777 /usr/share/logstash/data/

4. Обновим плагины

sudo /usr/share/logstash/bin/logstash-plugin update

5. Настроим logstash

cd /etc/logstash/

sudo mkdir /conf.d/

sudo touch /etc/logstash/conf.d/logstash.conf

code /etc/logstash/conf.d/logstash.conf

**Содержимое logstash.conf**

input {

file {

path => ["/var/log/suricata/eve.json"]

sincedb\_path => ["/dev/null"]

codec => json

type => "SuricataIDPS"

}

}

filter {

if [type] == "SuricataIDPS" {

date {

match => [ "timestamp", "ISO8601" ]

}

}

if [src\_ip] {

geoip {

source => "src\_ip"

target => "geoip"

#database => "/opt/logstash/vendor/geoip/GeoLiteCity.dat"

add\_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]

add\_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]

}

mutate {

convert => [ "[geoip][coordinates]", "float" ]

}

if ![geoip.ip] {

if [dest\_ip] {

geoip {

source => "dest\_ip"

target => "geoip"

#database => "/opt/logstash/vendor/geoip/GeoLiteCity.dat"

add\_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]

add\_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]

}

mutate {

convert => [ "[geoip][coordinates]", "float" ]

}

}

}

}

}

output {

elasticsearch {

hosts => ["localhost:9200"]

}

#stdout {codec => rubydebug }

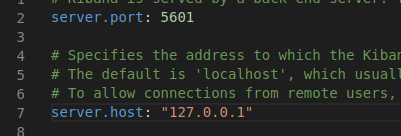
}

6. Отредактируем конфиг kibana

code /etc/kibana/kibana.yml



Разкомментируем строчки



7. Запустим службы

sudo systemctl start elasticsearch

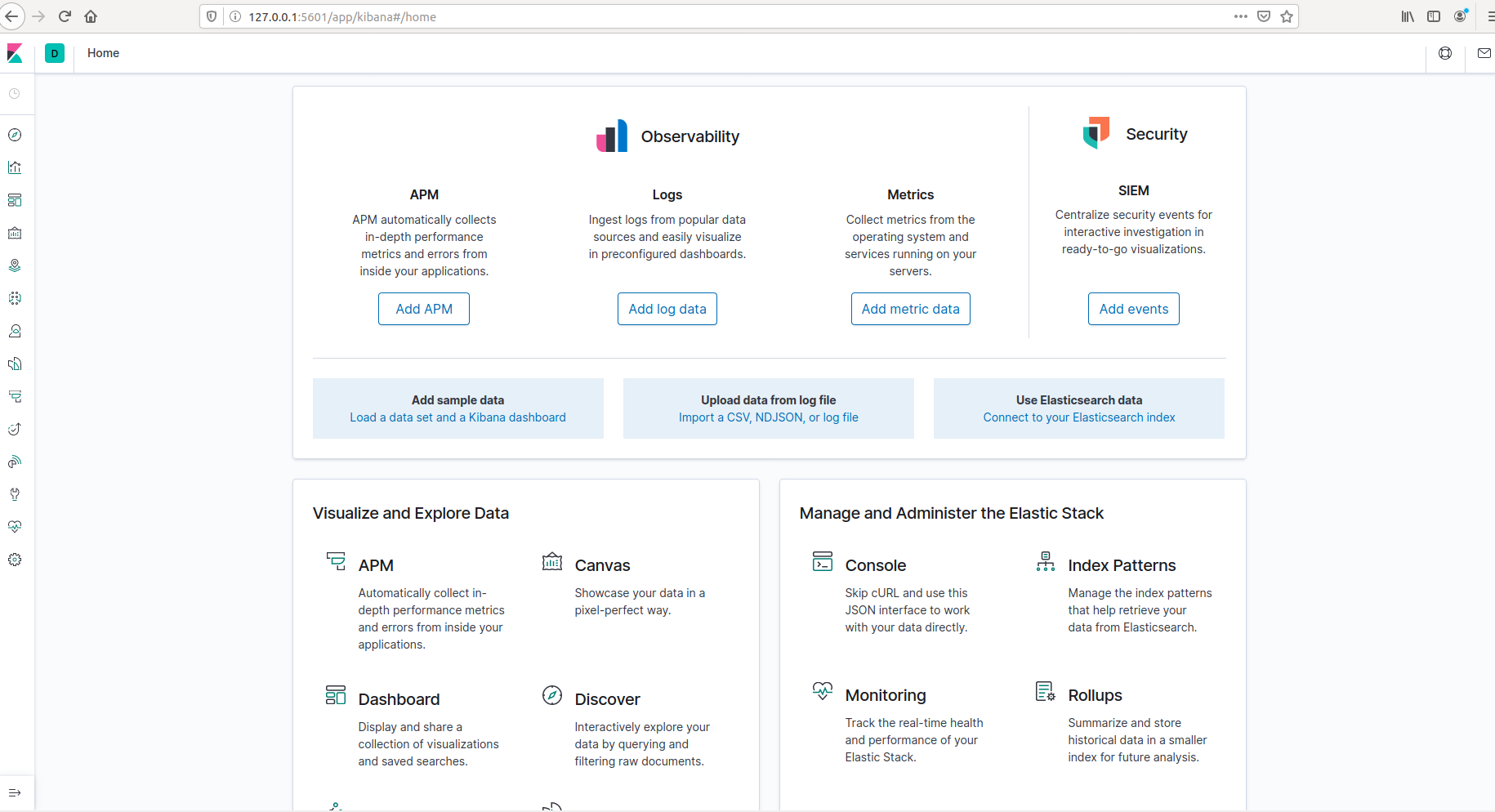
sudo systemctl status elasticsearch

sudo systemctl start kibana

sudo systemctl status kibana

sudo /usr/share/logstash/bin/logstash -f /etc/logstash/conf.d

8. Откроем в браузере 127.0.0.1:5601 и увидим интерфейс Kibana



**Часть 3**

1. Опять запустить Suricata

sudo suricata -c /etc/suricata/suricata.yaml -i enp0s3

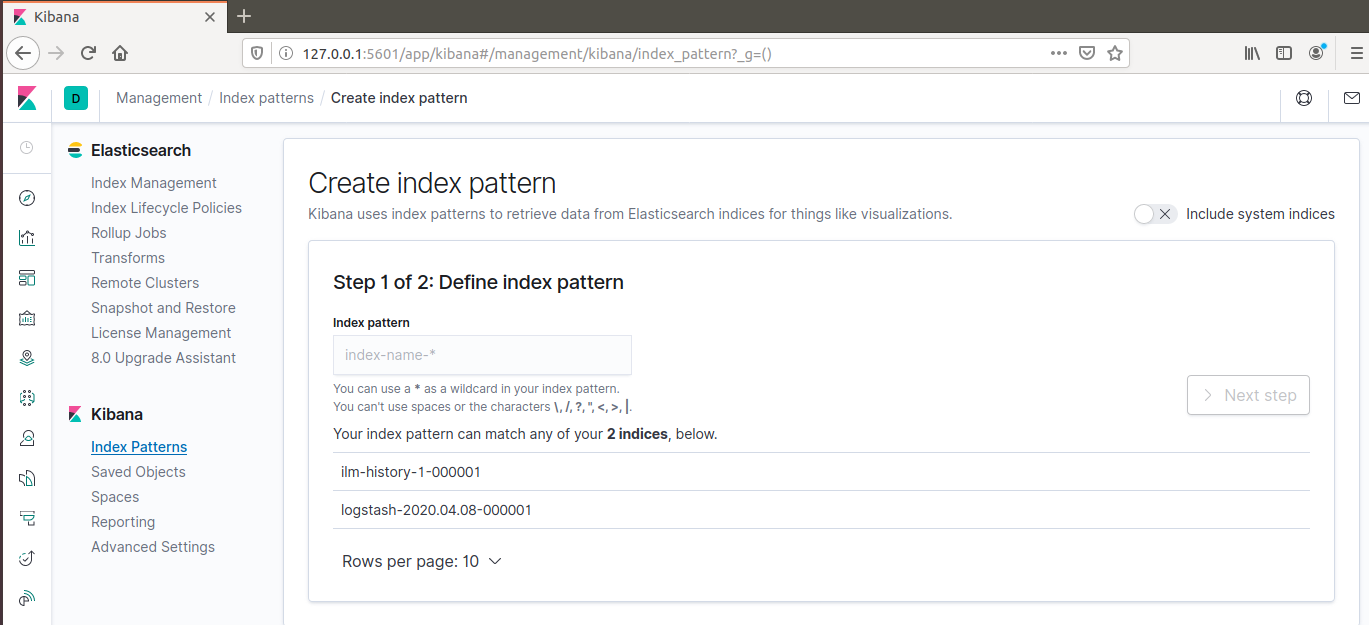
2. Немного пропинговать с Kali

sudo hping3 -S -p 80 --flood --rand-source 10.0.2.15

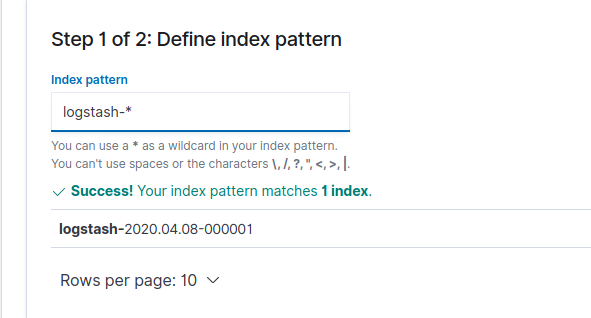
3. Открыть Kibana

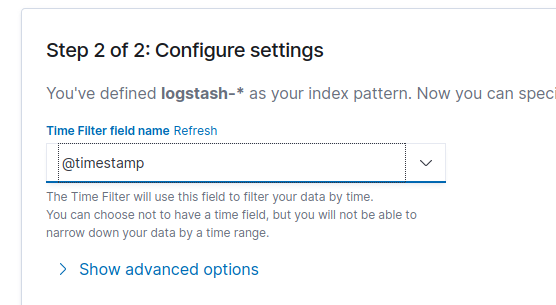
Перейти в Management – Index patterns – Create index pattern

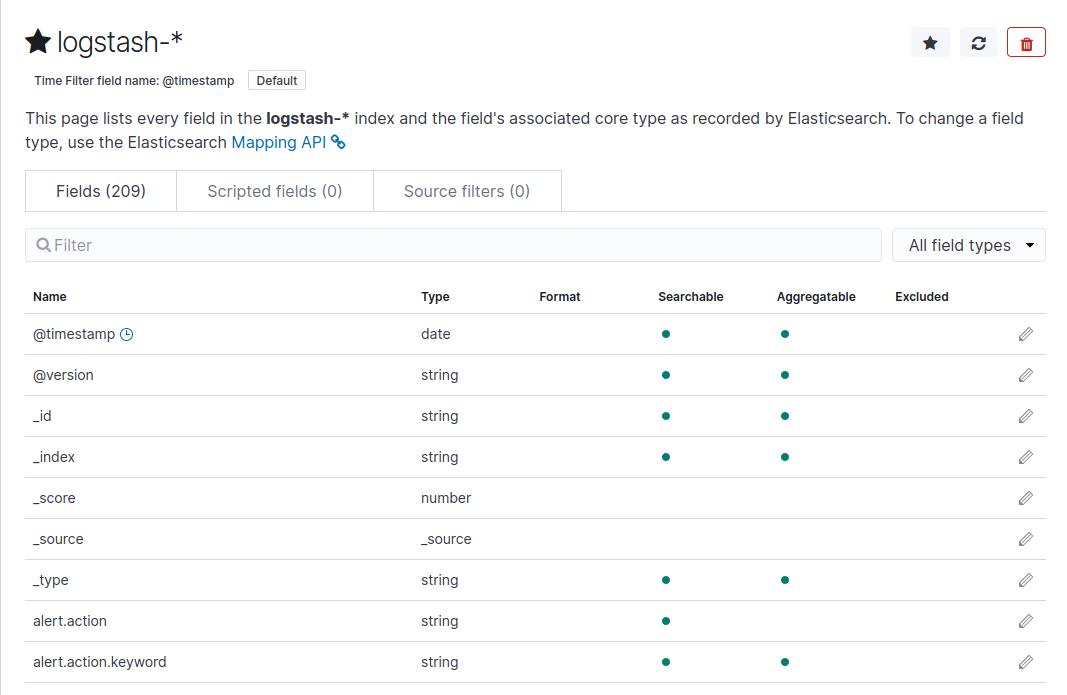
Увидеть, что там теперь есть logstash



4. Создать простой индекс

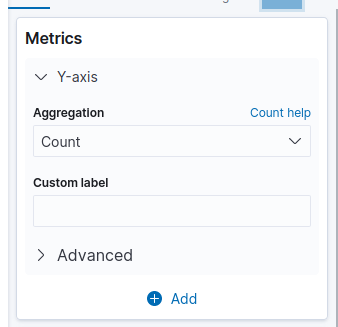


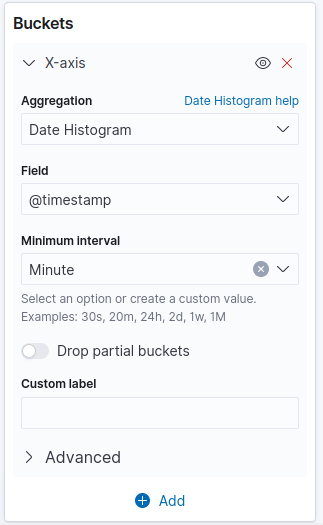




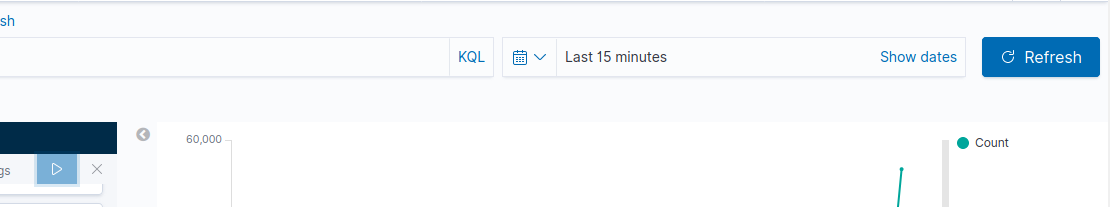
5. Открыть вкладку Visualize

6. Создать график Line



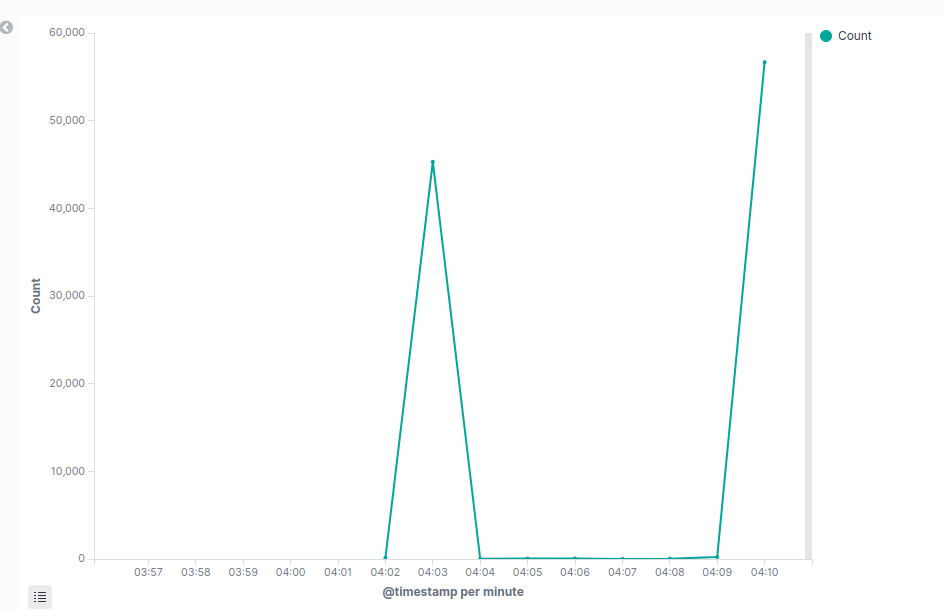


7. Применить настройки (стрелочка и refresh)



8. Для наглядности ещё пару раз запустить ненадолго пинги с Kali

9. Нажать на refresh, получить индивидуальный для каждого студента график



10. Сохранить график, нажав Save

**Что ещё можно посмотреть?**

1. Evebox

2. Filebeat

3. Обновление Suricata (suricata-update)

4. Ротация логов

/var/log/suricata/\*.log /var/log/suricata/\*.json

{

rotate 3

missingok

nocompress

create

sharedscripts

postrotate

/bin/kill -HUP $(cat /var/run/suricata.pid)

endscript

}