Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РтФ

Школа профессионального и академического образования

Отчет по дисциплине   
«Криптографические методы защиты информации»

Лабораторная работа №7  
«IDS Suricata. Развертывание системы. Возможности. Реагирование на инциденты ИБ. Как работать с зашифрованным трафиком.»

Студенты: Клоченко И.Е.

Преподаватель: Соколов И.П.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[Ход работы 3](#_Toc136443041)

[Вывод 9](#_Toc136443042)

**Цель работы:**

Знакомство с IDS Suricata. Работа с зашифрованным трафиком.

## Ход работы

В лабораторной работе используется операционная система Kali Linux. В связи с этим некоторые команды для конфигурации отличаются.

1. Устанавливаем необходимые пакеты для сборки Suricata по исходникам.

apt-get install libpcre3 libpcre3-dbg libpcre3-dev build-essential autoconf automake libtool libpcap-dev libnet1-dev libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libcap-ng-dev libcap-ng0 make libmagic-dev libjansson-dev libjansson4 pkg-config rustc cargo

1. Далее скачиваем архив с Suricata.

wget <https://openinfosecfoundation.org/download/suricata-6.0.12.tar.gz>

1. Распаковываем архив и переходим в директорию распакованной папки.
2. Нас интересует сборка для режима работы IDS, поэтому пишем следующие строки.

./configure –prefix=/usr –sysconfdir=/etc – localstatedir=/var–enable-lua

1. Собираем пакет командой «make» и устанавливаем командой «make install». Затем устанавливаем конфигурационные файлы «make install-conf».
2. Устанавливаем пакеты для установки и обновления Suricata.
3. Формируем кэш динамических библиотек «ldconfig».
4. После установки Suricata находится по пути «/usr/bin/suricata».
5. Главный конфигурационный файл Suricata – это suricata.yaml (пользовательские настройки). Также есть файл конфигурации «/etc/default/suricata (настройки по умолчанию)» Логи хранятся в директориях /var/log/suricata/. Файлы fast.log, eve.json.

Параметры, которые сейчас активны (или не активны), можно посмотреть выполнив следующую команду (часть вывода).

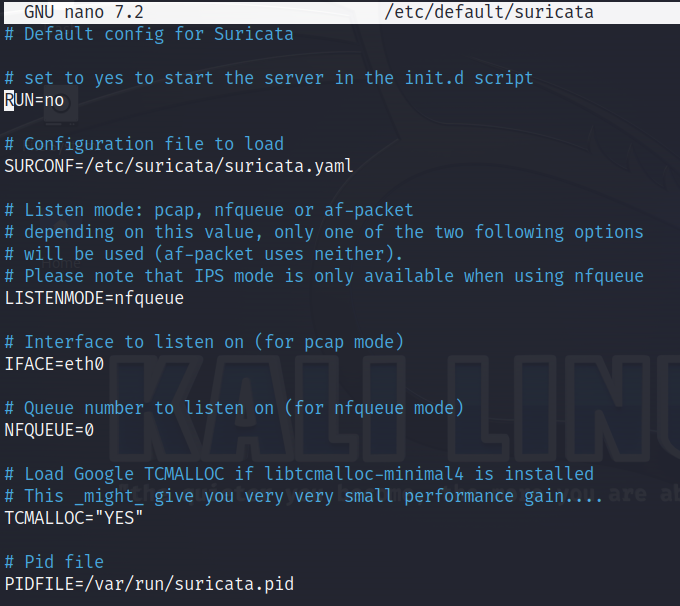


Рисунок 1. Параметры Suricata

1. Для IDS необходимы те параметры, которые сейчас активны, так как изначально мы собирали Suricata для работы в режиме IDS.
2. Посмотрим текущие установки и переменные.

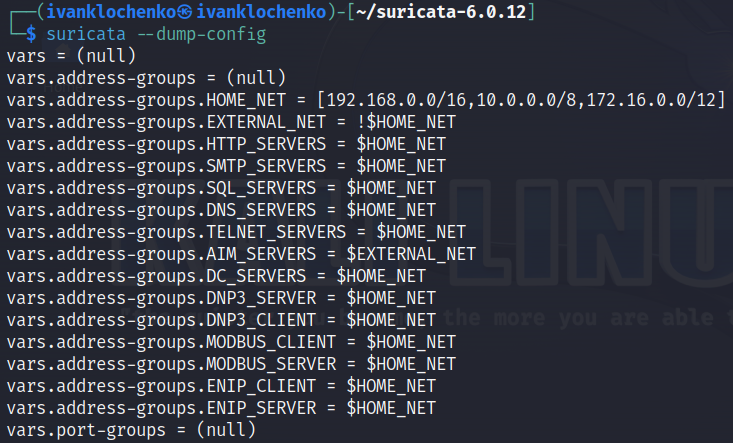


Рисунок 2. Текущие установки и переменные (не полный вывод)

1. Проверяем значение переменных в файле конфигурации suricata.yaml. Они совпадают с переменными SNORT.
2. В файле suricata.yaml значения переменных уже указаны.
3. Попробуем настроить переменные threading и detect-threat-ratio.

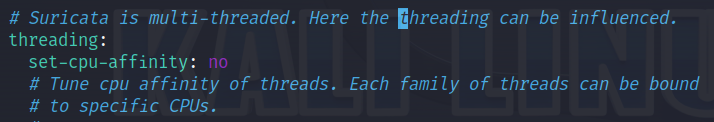


Рисунок 3. Настройка переменной threading



Рисунок 4. Настройка переменной detect-thread-ratio

1. Посмотрим возможные режимы реализации Suricata.

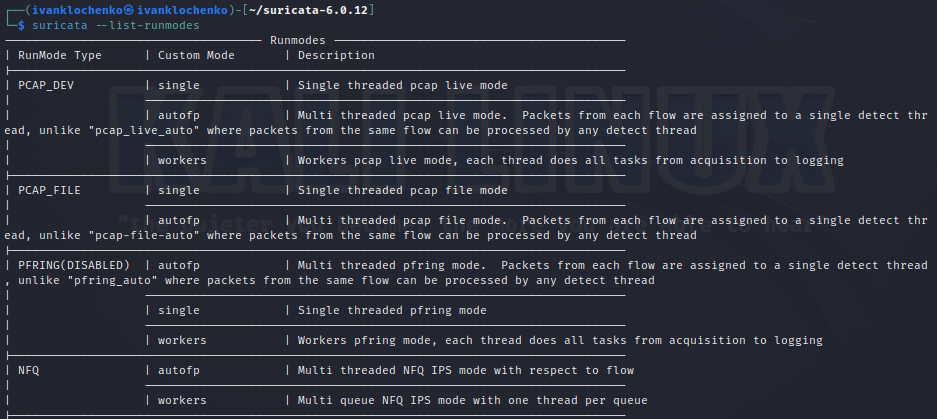


Рисунок 5. Возможности различных режимов реализации Suricata (неполный вывод)

1. Применены режимы реализации auto и workers.
2. Указываем значение для host-mode.



Рисунок 6. Присвоение значение параметру host-mode

1. Узнаем MTU своей сети.

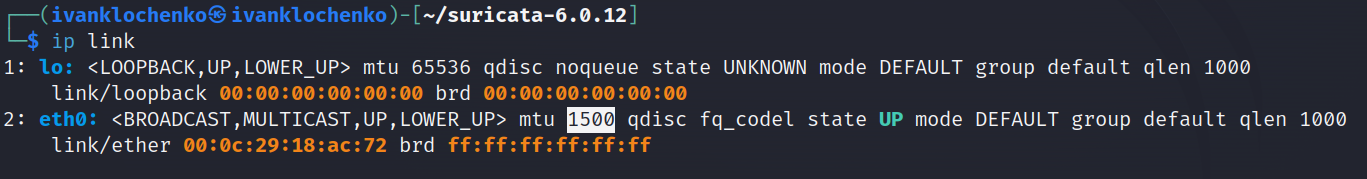


Рисунок 7. Просмотр MTU сети

1. Устанавливаем оптимальное значение default-packet-size, указав MTU своей сети.



Рисунок 8. Установка размера пакета по умолчанию

1. Получаем список настроенных для проверки протоколов уровня приложения.

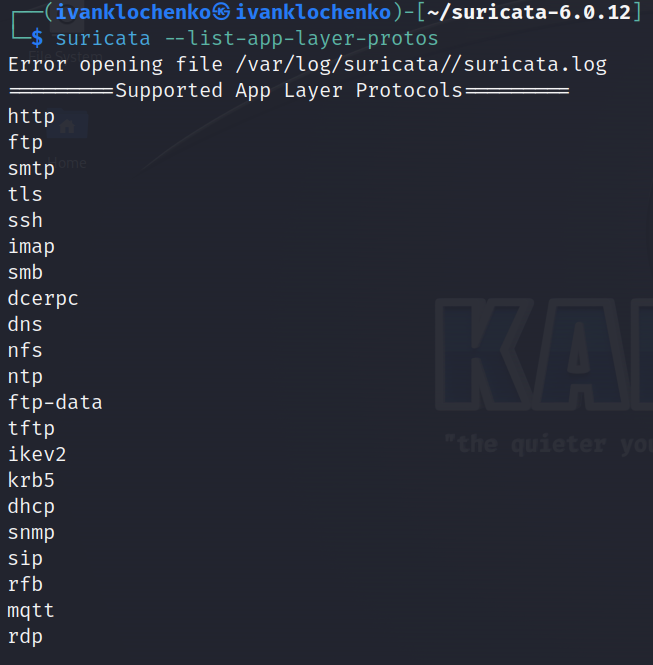


Рисунок 9. Настроенные для проверки протоколы уровня приложения

1. Просмотрим подключенные правила.

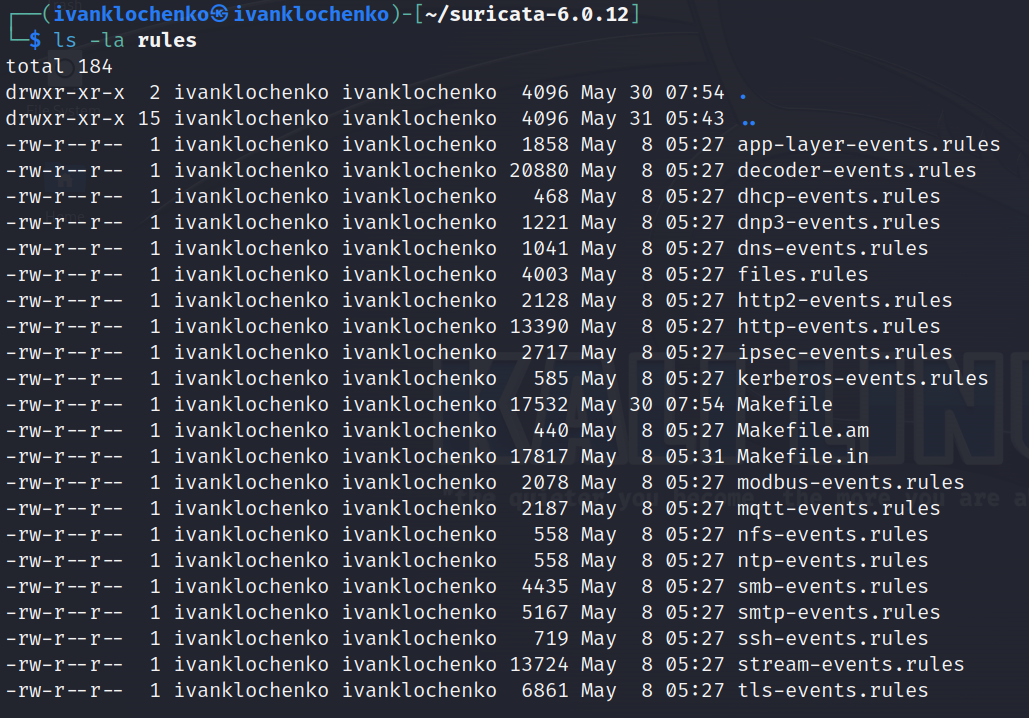


Рисунок 10. Подключенные правила

1. Политика для ОС Linux, которую можно изменить, следующая.

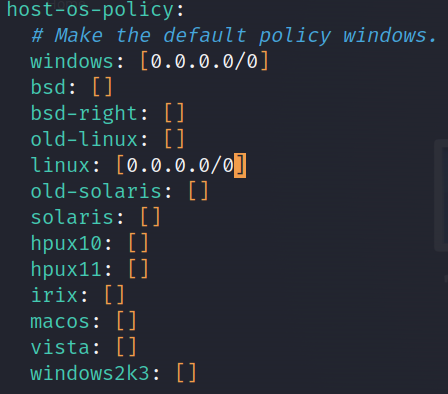


Рисунок 11. Политика для ОС Linux.

1. Определим ошибки в конфигурационном файле.

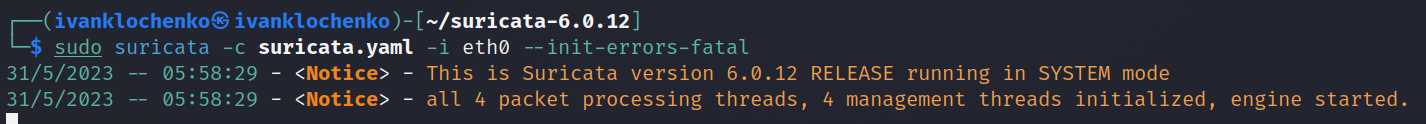


Рисунок 12. Проверка на ошибки в конфигурационном файле

Как видим, ошибок нет.

1. Запускаем Suricata в данном режиме.

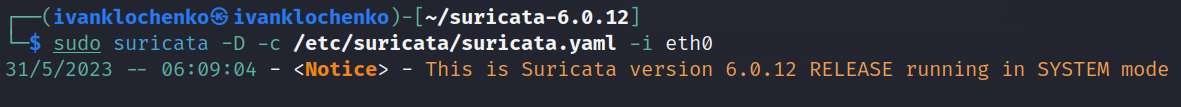


Рисунок 13. Запуск Suricata в данном режиме

1. Заходим на сайт Google.com. Сработок в терминале нет.
2. Используем в качестве второй виртуальной машины, машину с образом Kali Linux.
3. Запускаем ping со второй виртуальной машины.
4. Переходим на первую виртуальную машину и смотрим, как реагирует Suricata. Никак.
5. Переходим в каталог /var/log/suricata. Находим там файл с информацией о трафике. 5 из 5 ICMP пакетов было пройдено.
6. Оценим производительность CPU при тестировании Suricata в режиме IDS.

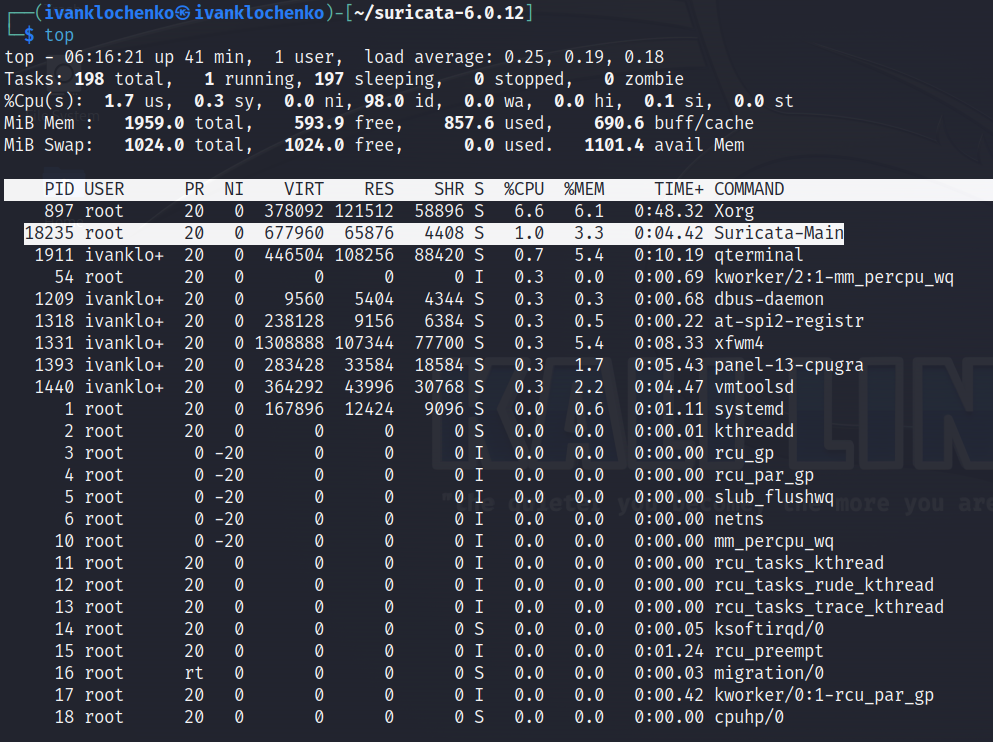


Рисунок 14. Загрузка системы процессами

1. Файл /etc/log/suricata/fast.log отвечает за логирование работы IDS Suricata.
2. Перезапускаем виртуальную машину.
3. Запускаем тестирование на 3 часа. В это время скачиваем файл объемом 3 ГБ. Графика загрузки при этом увеличивается, но не значительно. Это может быть связано с тем, что во время загрузки Suricata выступает фильтром-анализатором, и для выполнения своих функций она должна проверять все пакеты, проходящие в сеть и из нее. Это лишние процессы, что может сказываться на загрузке системы.

## Вывод

В ходе выполнения лабораторной работы я научился собирать из исходных файлов IDS/IPS Suricata. Научился конфигурировать эту утилиту. Никакой области, где бы применялись криптографические методы, шифрование, не было отражено в методических указаниях к работе. С точки зрения освоения предмета «Криптографические методы защиты информации» эта лабораторная работа была бесполезна. Для общего развития, научиться собирать программу с нуля – да, прекрасно, но для освоения предмета это не подходит.