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   
«Безопасность компьютерных сетей»

Лабораторная работа №7  
«Suricata»

Студенты: Клоченко И.Е., Юсупов Д.А.

Преподаватель: Ваулин С.С.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[Ход работы: 3](#_Toc136263825)

[Вывод 5](#_Toc136263826)

**Цель работы:**

Знакомство с сигнатурами Suricata.

## Ход работы:

Используются две виртуальные машины Kali Linux (клиент, сервер).

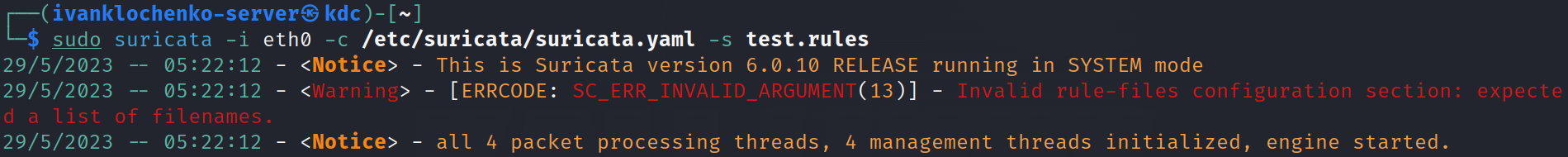
1. На серверную машину устанавливаем Suricata.
2. Создаем в текущей (домашней) директории файл test.rules, который будем в дальнейшем использовать в качестве правила для Suricata, со следующим содержимым.



**Рисунок 1.** Правило для Suricata

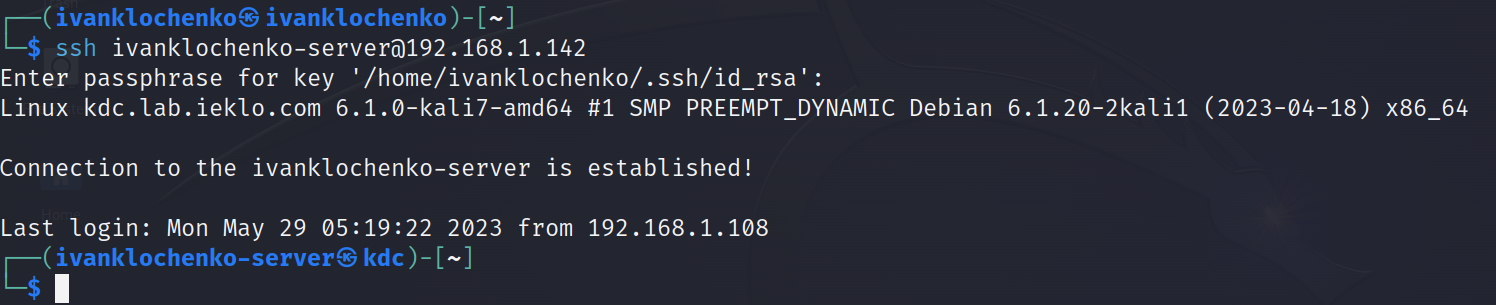
Идея правила в том, чтобы детектировать пакеты, которые относятся к подключению к серверной машине посредством SSH. Указан протокол TCP, чтобы детектировать все пакеты, которые принадлежат этому процессу. Порт 22 указан для конкретизации детектирования пакетов (именно SSH/SFTP). При сработке правила в файл fast.log будет выведено сообщение «SSH login attempt!».

1. Запускаем на серверной машине Suricata с использованием созданного правила.



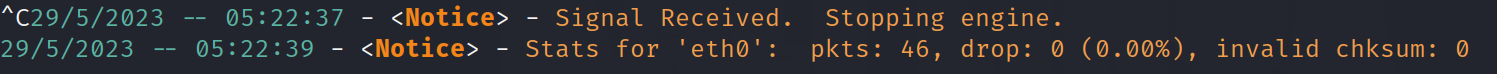
**Рисунок 2.** Запуск Suricata

1. С клиентской машины инициируем подключение по SSH.



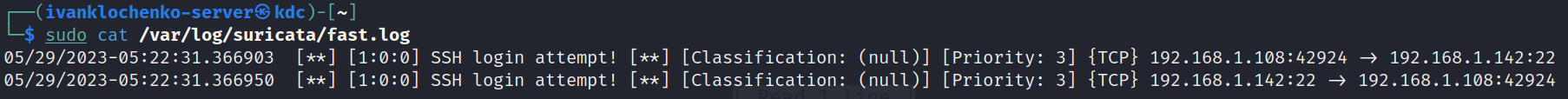
**Рисунок 3.** Подключение к серверной машине по SSH

1. На серверной машине останавливаем работу Suricata комбинацией клавиш Ctrl+C. Suricata сообщит нам, сколько пакетов было детектировано.



**Рисунок 4.** Остановка работы Suricata

1. Просматриваем файл fast.log.



**Рисунок 5.** Содержимое файла fast.log

Как видим, правило успешно детектирует пакеты SSH подключения.

## Вывод

В ходе выполнения лабораторной работы, были освоены принципы построения правил (сигнатур) для IDS/IPS Suricata.

Написано простое правило, детектирующее пакеты, относящиеся к процессу подключения по SSH к серверной машине.