ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«Национальный исследовательский университет ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

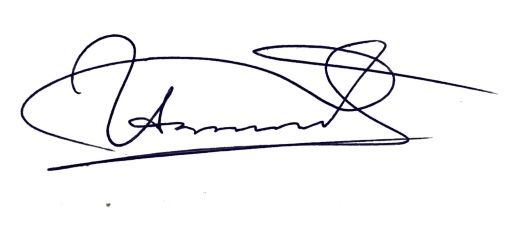
«Система мониторинга и управление информационной безопасностью»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

**Ручной труд**

**Выполнил:**

Студент группы N33451

Галюкшев И. А.

**Проверил:**

Попков И. А.

Санкт-Петербург

2023г.

**Цель**

Познакомиться с основными принципами мониторинга информационной безопасности без использования специализированного программного обеспечения.

**Задачи**

1. Подготовить среду;
2. Сгенерировать записи журналов;
3. Собрать и проанализировать сгенерированные записи.

**Выполнение**

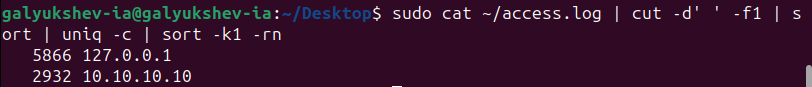
****

Рисунок 1 – Вывод уникальных адресов и их количества

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 2 – Результат работы скрипта histogram.sh

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 3 – Вывод строк, содержащих заданный адрес и соответствующих заданному времени

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Рисунок 4 – Топ-10 самых популярных имен пользователей, под которыми была произведена попытка логика

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 5 – Уникальные ip-адреса, для которых аутентификация была произведена успешно

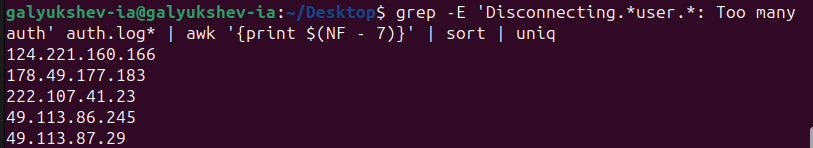


Рисунок 6 – Адреса, аутентификация которых была отброшена по причине превышения максимального количества попыток

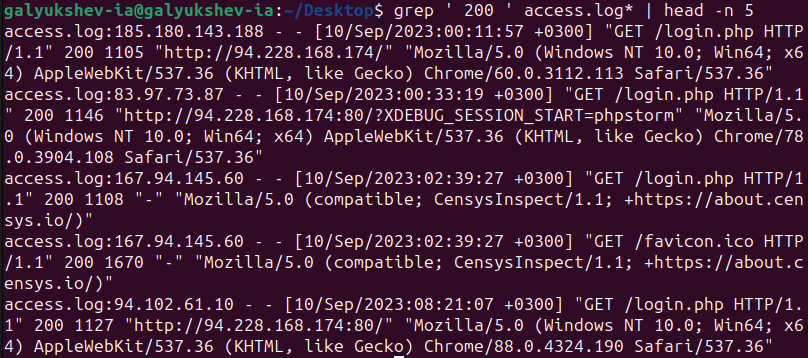
Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание Рисунок 7 – Количество отброшенных подключений по дням

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 8 – Уникальные User-Agent из журналов access.log, не соответствующие распространенным пользовательским браузерам

 Рисунок 9 – Запросы, код возврата которых соответствует 200

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 10 – Адрес, метод и запрос, если http-метод не соответствует GET или POST

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 11 – Строки журнала, если адрес источника – ipv6

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Рисунок 12 – Журналы access.log, совпадающие по времени с отличающейся строкой журнала mycustom.log

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 13 – Запросы, которые делали адреса, упомянутые в журнале ошибок

**Вывод**

В ходе работы я познакомиться с основными принципами мониторинга информационной безопасности без использования специализированного программного обеспечения и научился генерировать записи журналов, а также собирать и анализировать уже сгенерированные записи.