МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
 РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

Институт радиоэлектроники и информационной безопасности

Кафедра «Информационная безопасность»

**ОТЧЁТ**

по лабораторной работе № 1

на тему: «Поиск и работа с уязвимостями c использованием программных средств»

по дисциплине

«Программно-аппаратные средства защиты информации»

Выполнил: студент гр. ИБ/б-21-2-о

Филатов Роман Александрович

Защитил с оценкой: \_\_\_\_\_\_

Принял: доцент Голиков

Севастополь

2023

**Цель работы**: Изучение особенностей работы с программным обеспечением ScanOVAL и Lynis. Сбор, анализ выявленных уязвимостей, поиск решения по закрытию уязвимостей.

**Ход работы:**

Первоначально было скачано ПО ScanOVAL, с оффициального сайта БДУ «ФСТЭК России».

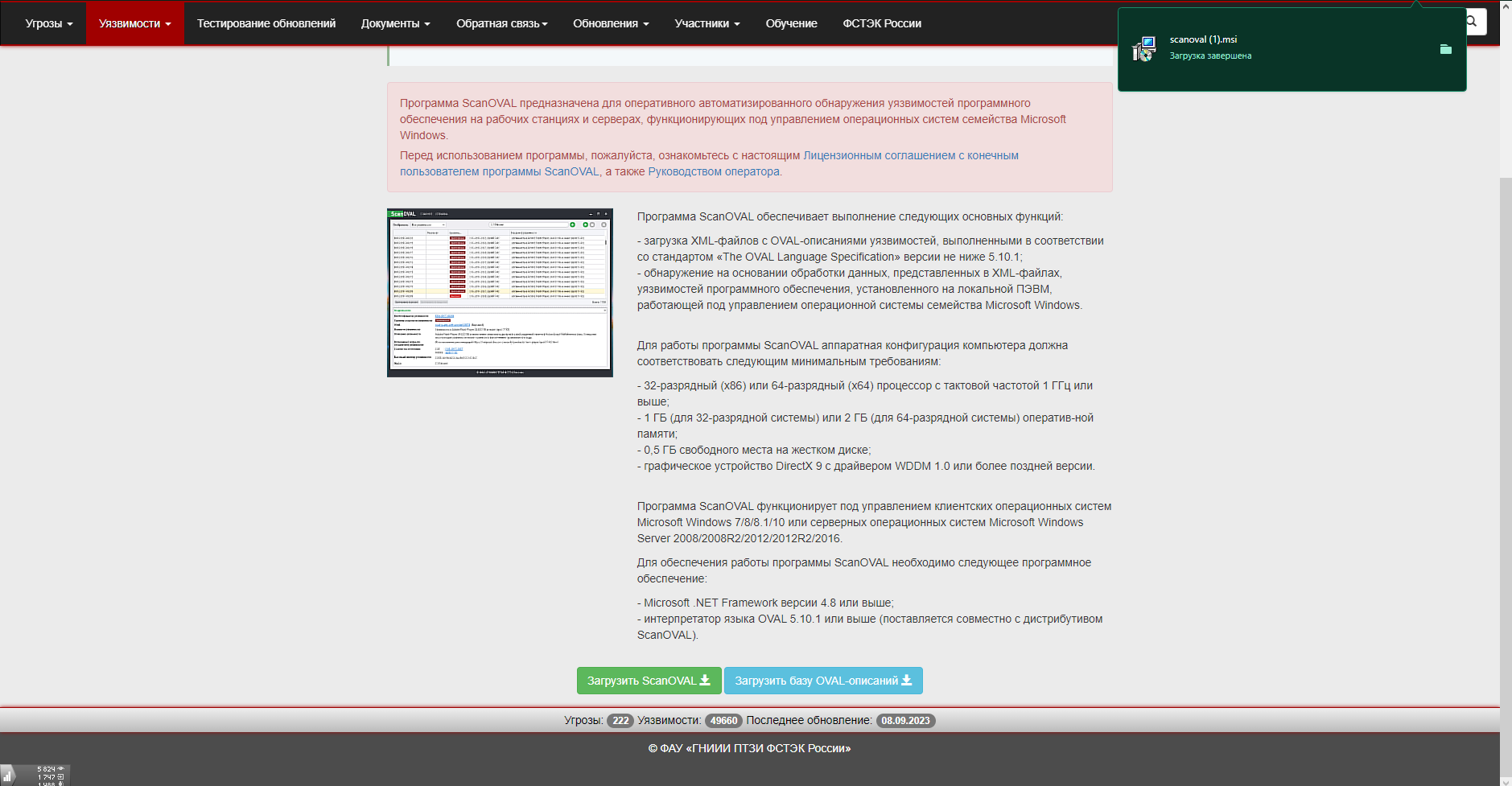


Рисунок 1 — Скачивание программы и базы данных

Далее база данных была скопирована в удобную папку — «Загрузки»

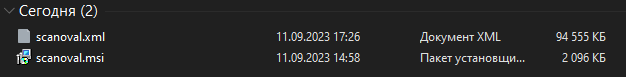


Рисунок 2 — Копирование базы данных и установщика программы

На следующем этапе, в программе была выбрана база данных и запущено сканирование.

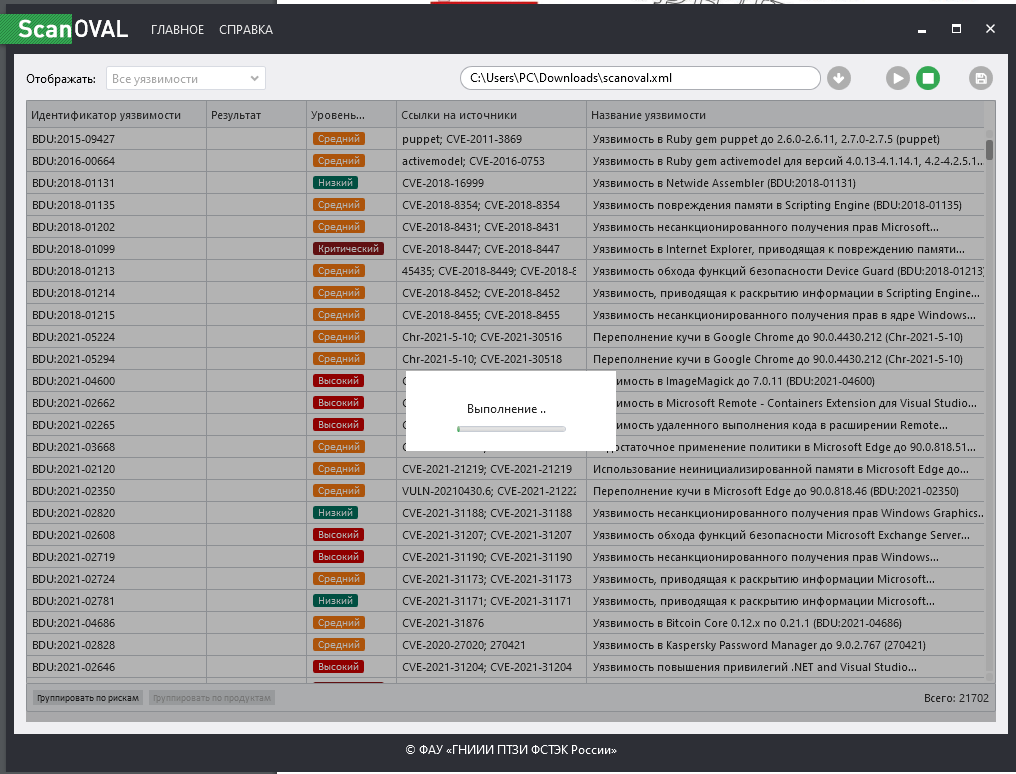


Рисунок 3 — Выбор базы данных в программе и старт сканирования

После выполнения сканирования, был сохранен отчет

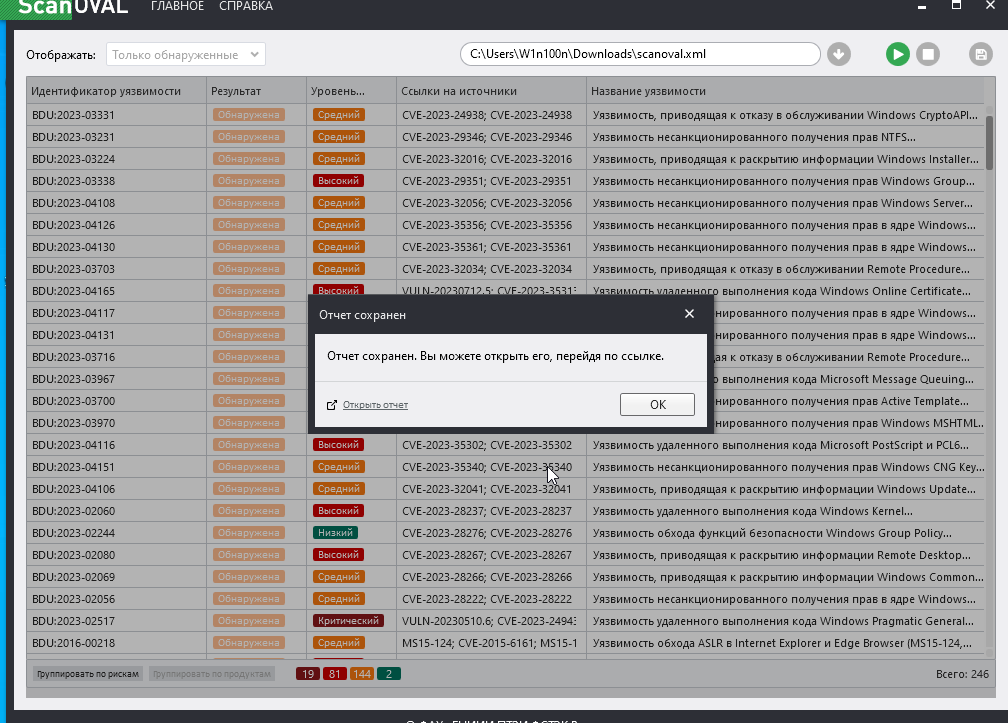


Рисунок 4 — Сохранение отчета сканирования

Далее были устранены несколько уязвимостей и снова проведено сканирование и сохранен отчет.

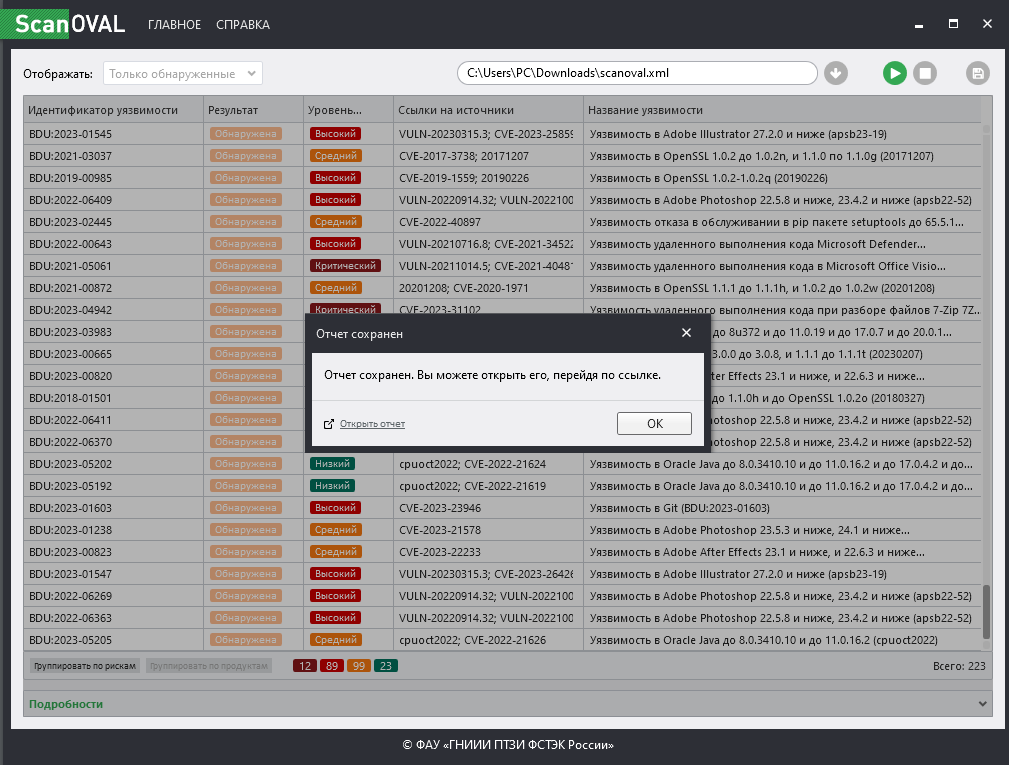


Рисунок 5 — Сохранение отчета сканирования после устранения уязвимостей

Как стало заметно после устранения уязвимостей стало на 23 меньше. Все уязвимости были устранены с помощью обновления Windows.

**Часть 2. Lynis**

Первоначально была скачана программа Lynis на Kali Linux.

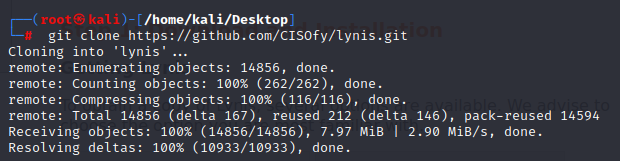


Рисунок 6— Скачивание Lynis на KaliLinux

Далее был запущен аудит системы, командой «lynis audit system».

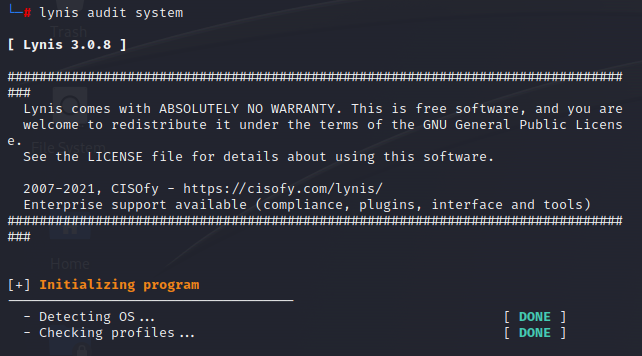


Рисунок 7 — Запуск аудита системы KaliLinux

Далее были открыты файлы с данными аудита — lynis.log и lynis-report.dat

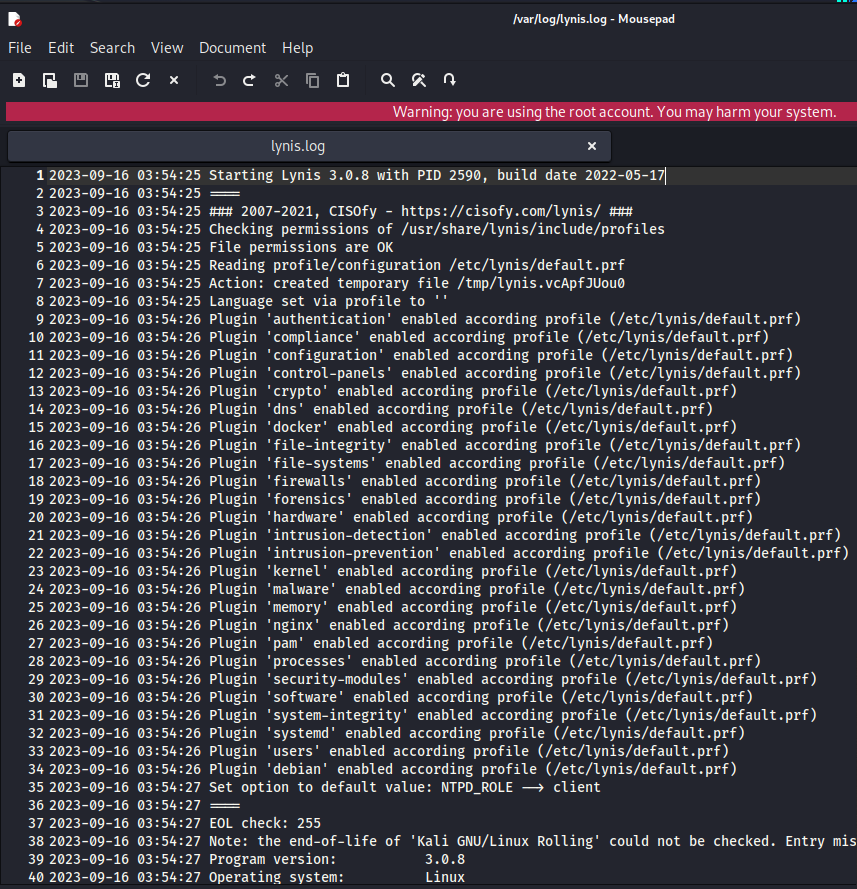
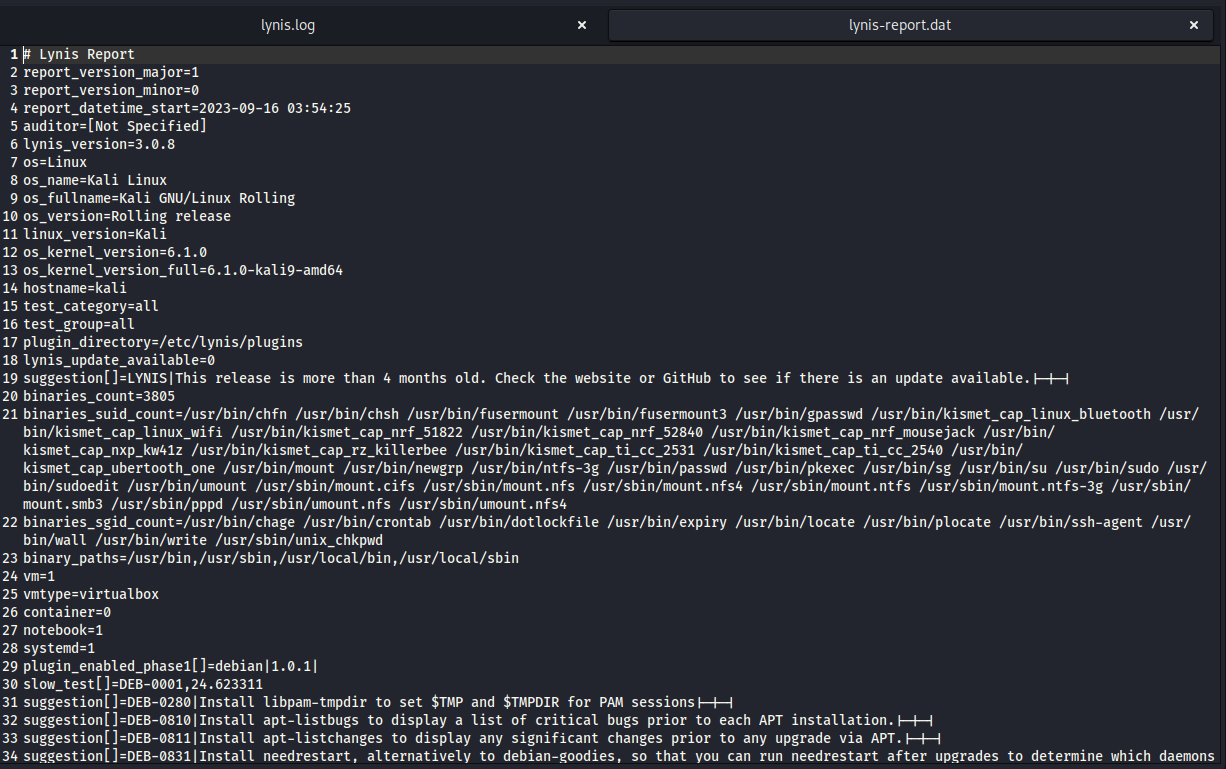


Рисунок 8 — Файл Lynis.log

Рисунок 9 — Файл lynis-report.dat

Далее был изучен отчет аудита. В результате изучения отчета были найдены ответы на вопросы по лабораторной работе. Вопросы и ответы представлены далее.

**Ответы на вопросы:**

1. *Какие цвета и для чего используются в отчетах?*

Отчет делиться на различные разделы, которые начинаются с — [+]. В каждом разделе указывается уязвимость и ее статус. В отчете статусы разделяются по цветам — зеленый, желтый и красный.

Зеленый — возможность эксплуатации уязвимости отсутствует, все хорошо;

Желтый — возникновение спорной ситуации или не найдены нужные файлы, неизвестно;

Красный — возможность эксплуатации присутствует, необходимо срочно исправить.

1. *Какой командой можно найти дополнительную информацию по исправлению?*

Информация по поводу уязвимостей и их устранения хранится в конце отчета, но для того, чтобы получить расширенную информацию по устранению, необходимо использовать команду: [./lynis show details «Идентификатор уязвимости»].

1. *Какие уязвимости вы нашли — их точно будет не менее 5.*

В результате аудита системы KaliLinux были найдены следующие уязвимости:

* Обнаружен один или несколько уязвимых пакетов [PKGS-7392];
* сервер имен 192.168.8.205 не отвечает [NETW-2704];
* модули iptables загружены, но правила не активны [FIRE-4512];

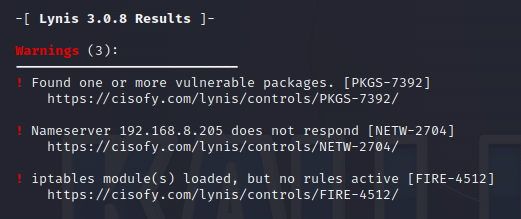


Рисунок 10 — Уязвимости, обнаруженные аудитом

1. *Какие рекомендации вы можете дать по их устранению?*

Для решения проблемы с id PKGS-7392, необходимо обновить свою систему с помощью apt-get update, apt-get upgrade, apt-get dist-upgrade и/или автоматических обновлений.

Для решения NETW-2704 необходимо проверить подключение к этому серверу имен и убедиться, что исходящие DNS-запросы не заблокированы (порт 53 UDP и TCP).

Для решения FIRE-4512 необходимо активировать правила для iptables.

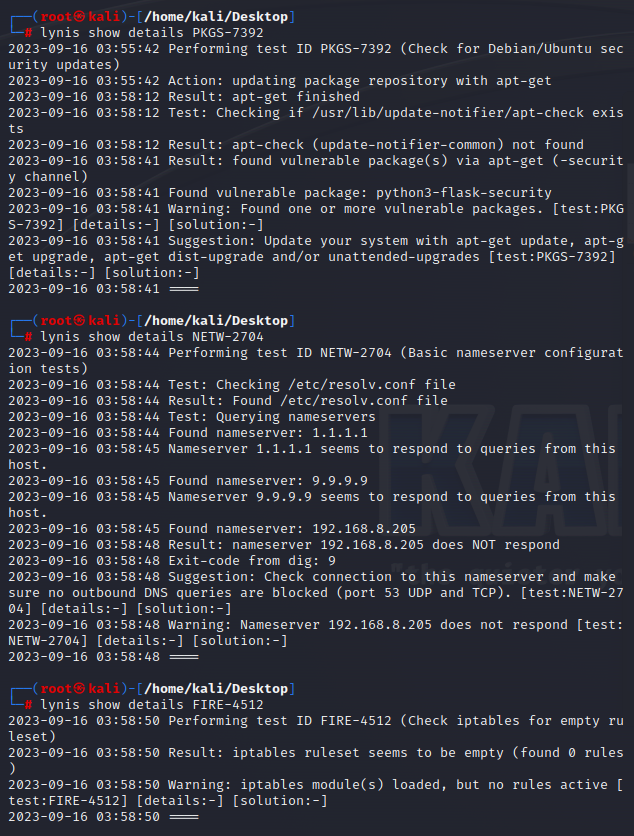


Рисунок 11 — Предложения по устранению уязвимостей Kali

1. *Сделайте выводы по степени защищённости операционной системы.*

В результате проведения аудита системы было определено, что KaliLinux хорошо защищенная ОС, имеющая малое количество критических уязвимостей, в отличии от Windows.