|  |  |  |
| --- | --- | --- |
|  |  |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | | |
| Институт кибербезопасности и цифровых технологий  Кафедра КБ-4 «Интеллектуальные системы информационной безопасности» | | |

**Отчёт по практической работе №3**

**по дисциплине «Система для сбора событий и логов»**

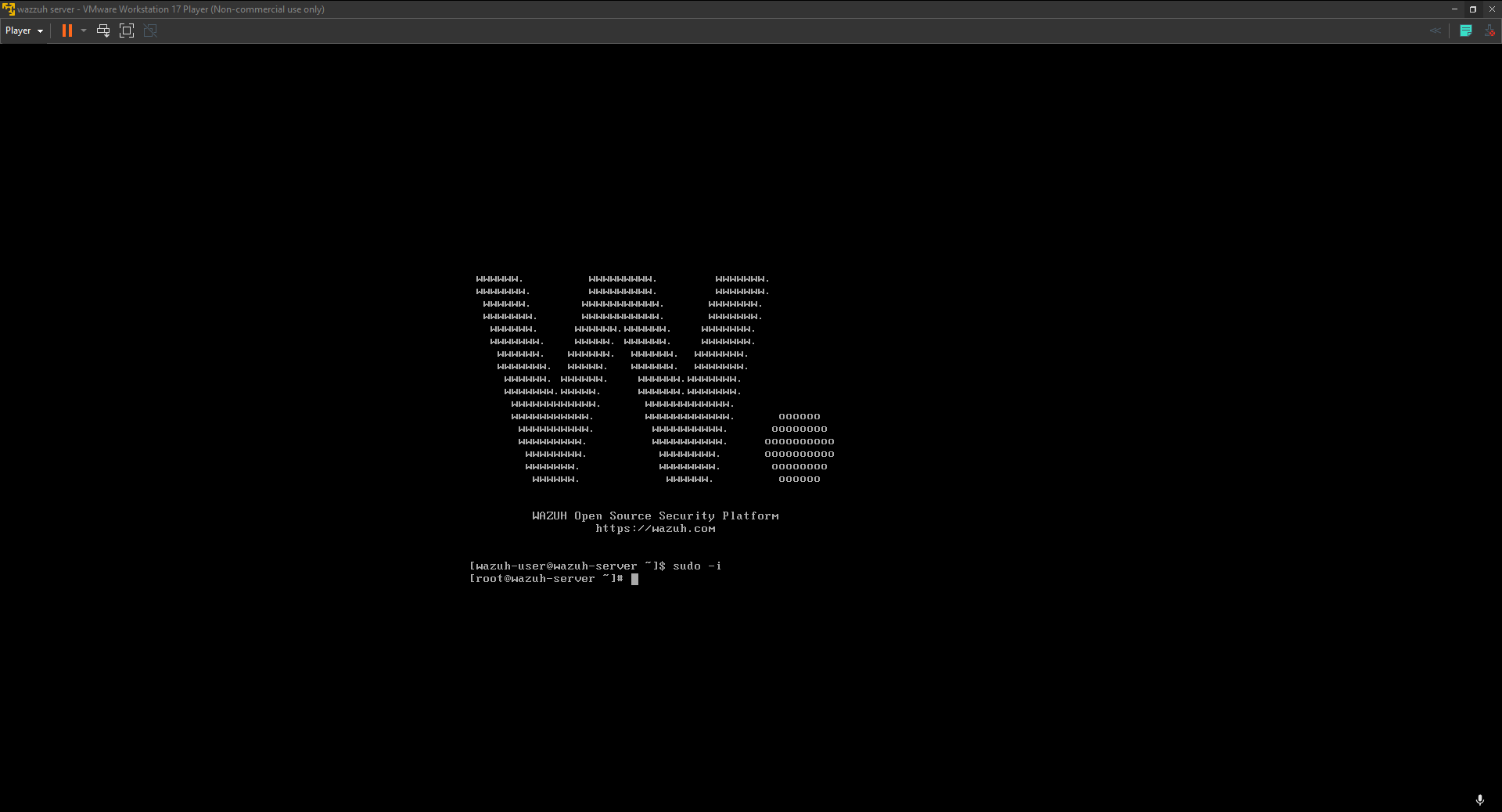
Выполнил:

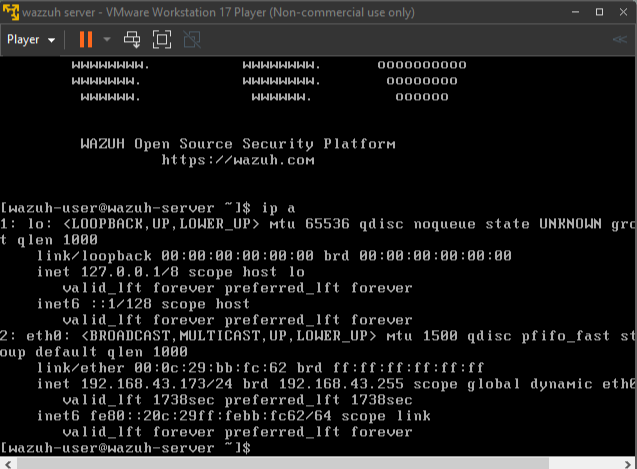
Евдокимов А.М.

Группа: ББМО-02-23

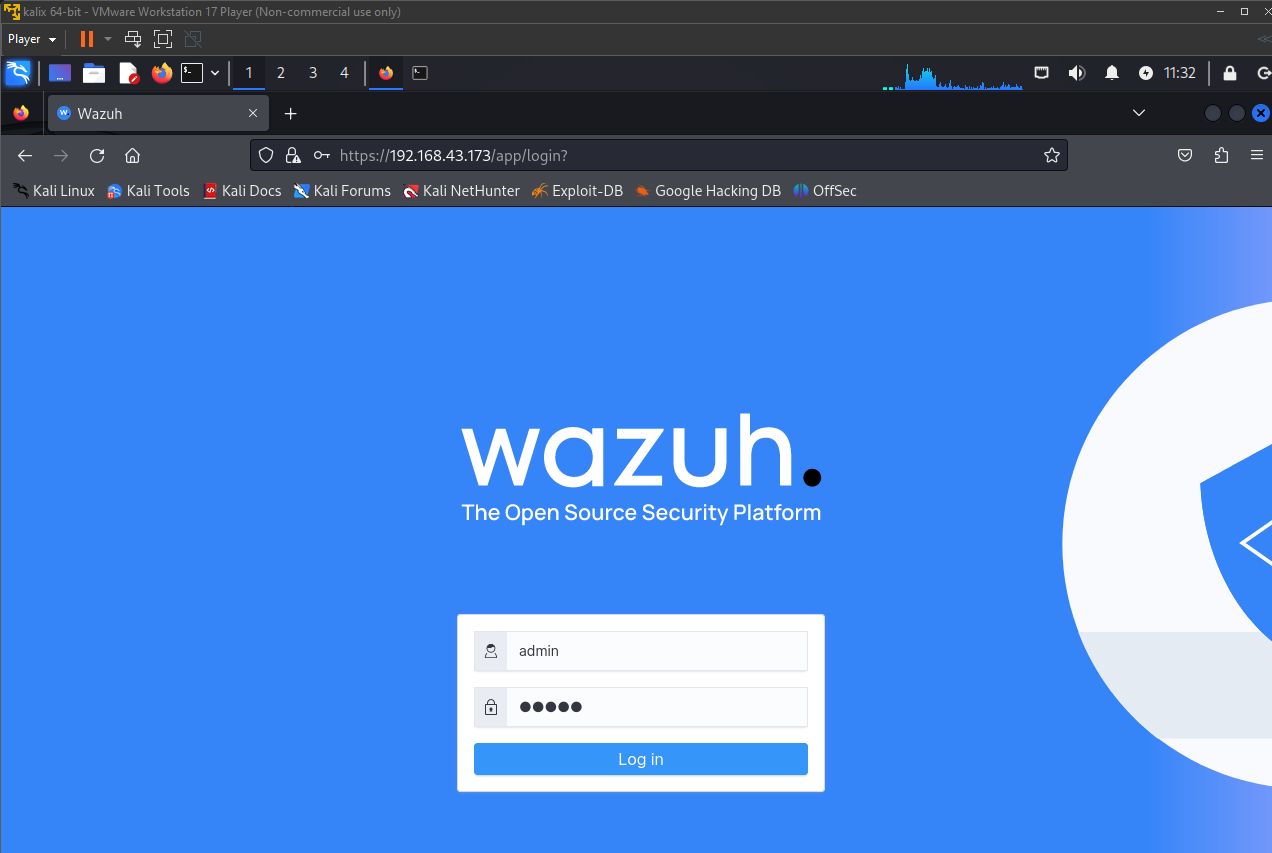
Москва - 2024

В данной практике я выбрал готовый вариант Wazuh Server

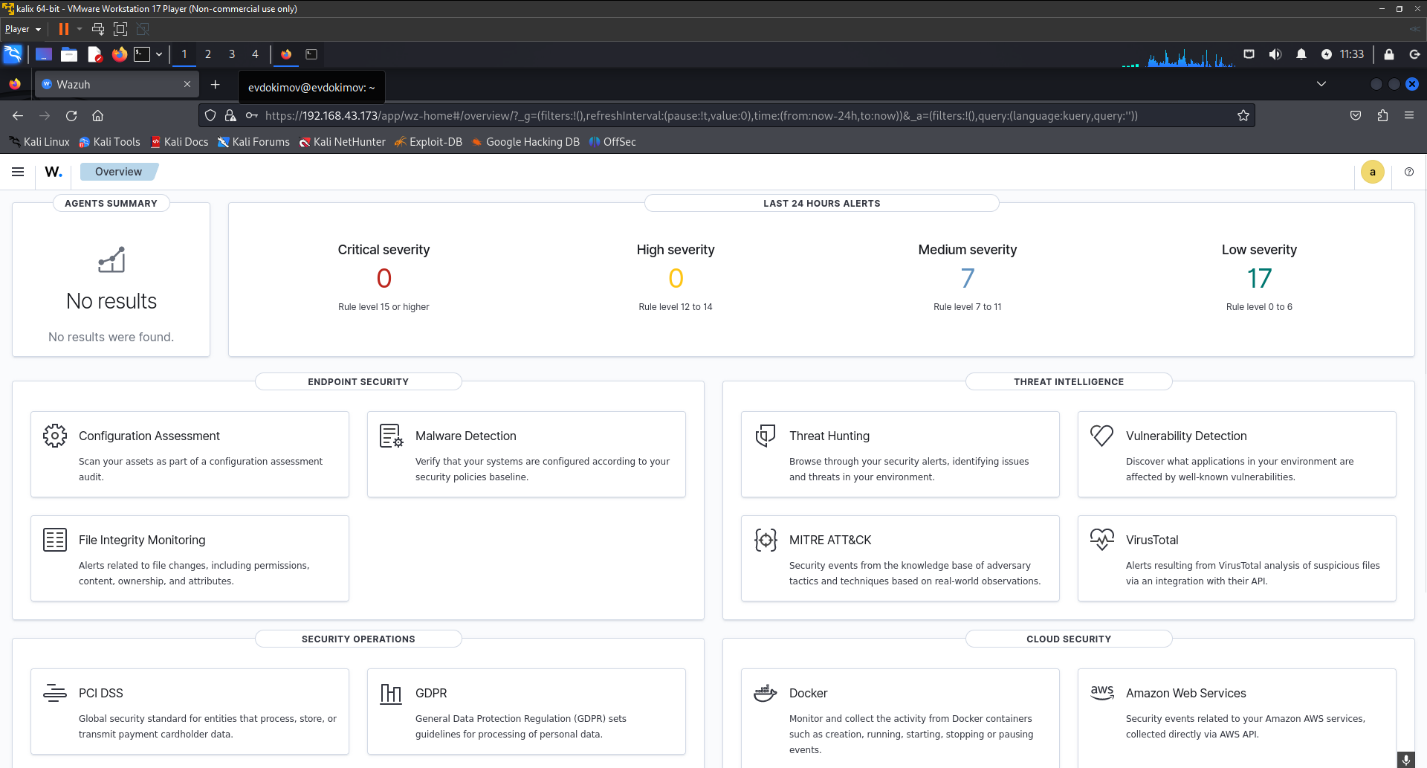




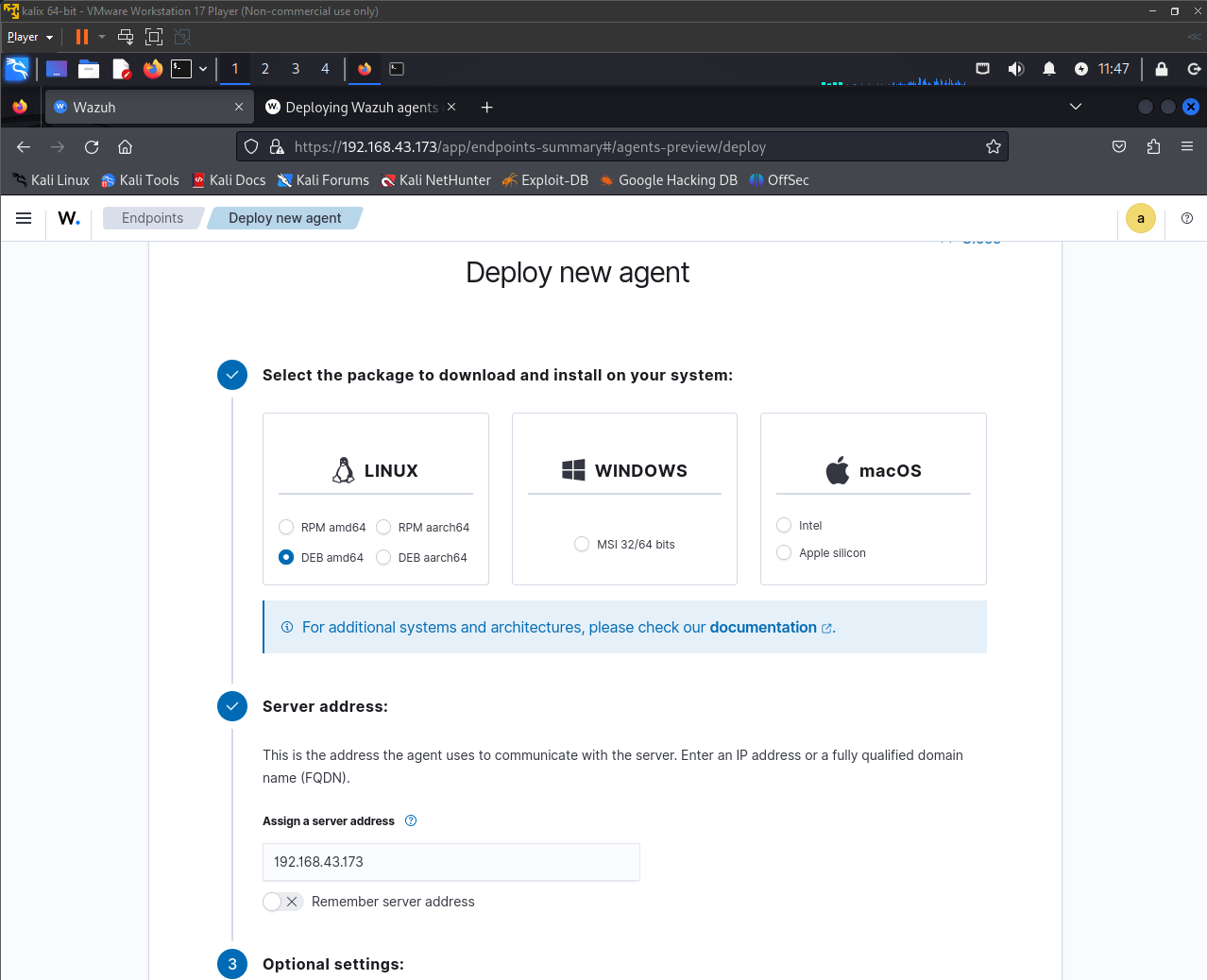
Авторизация

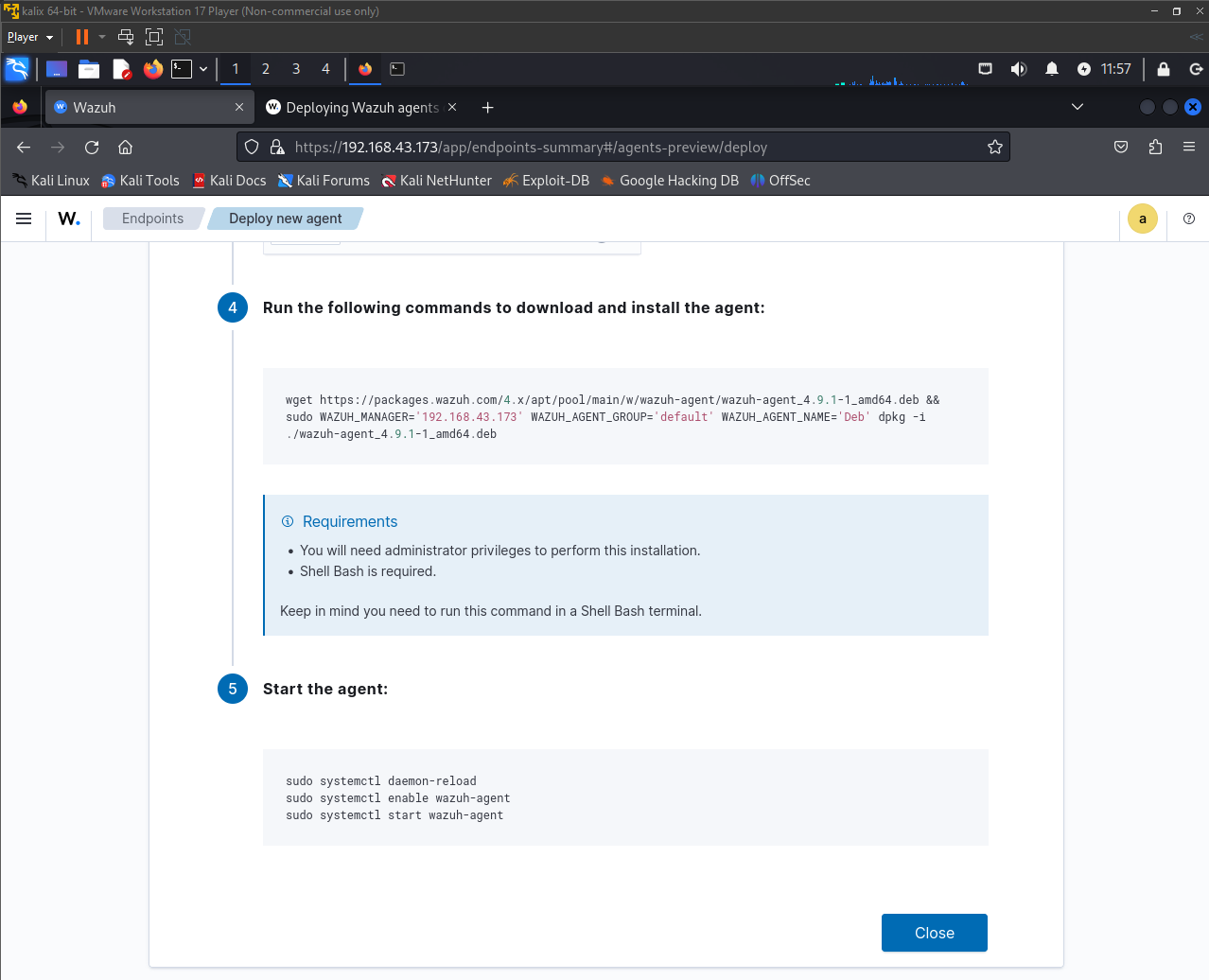


Веб-интерфейс Wazuh

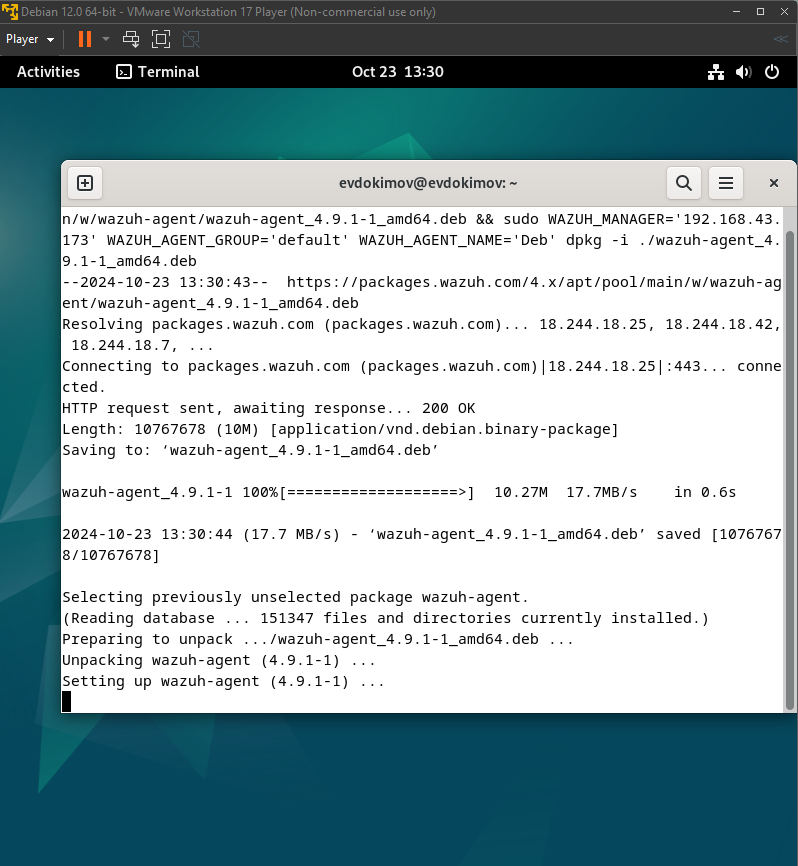


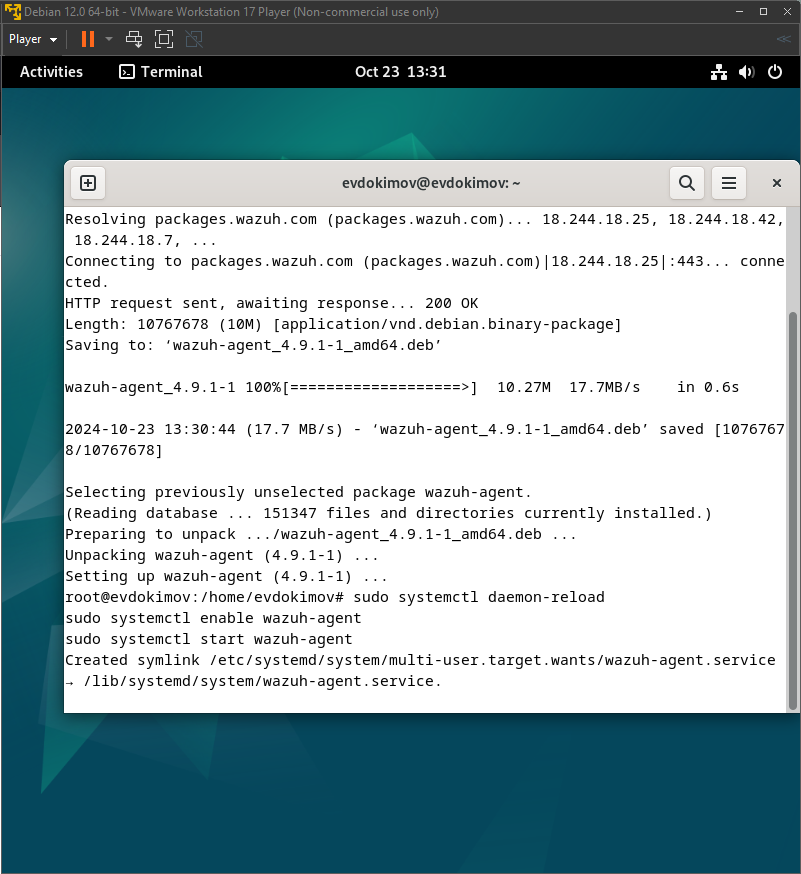
Теперь готовимся установить агент на другой ВМ



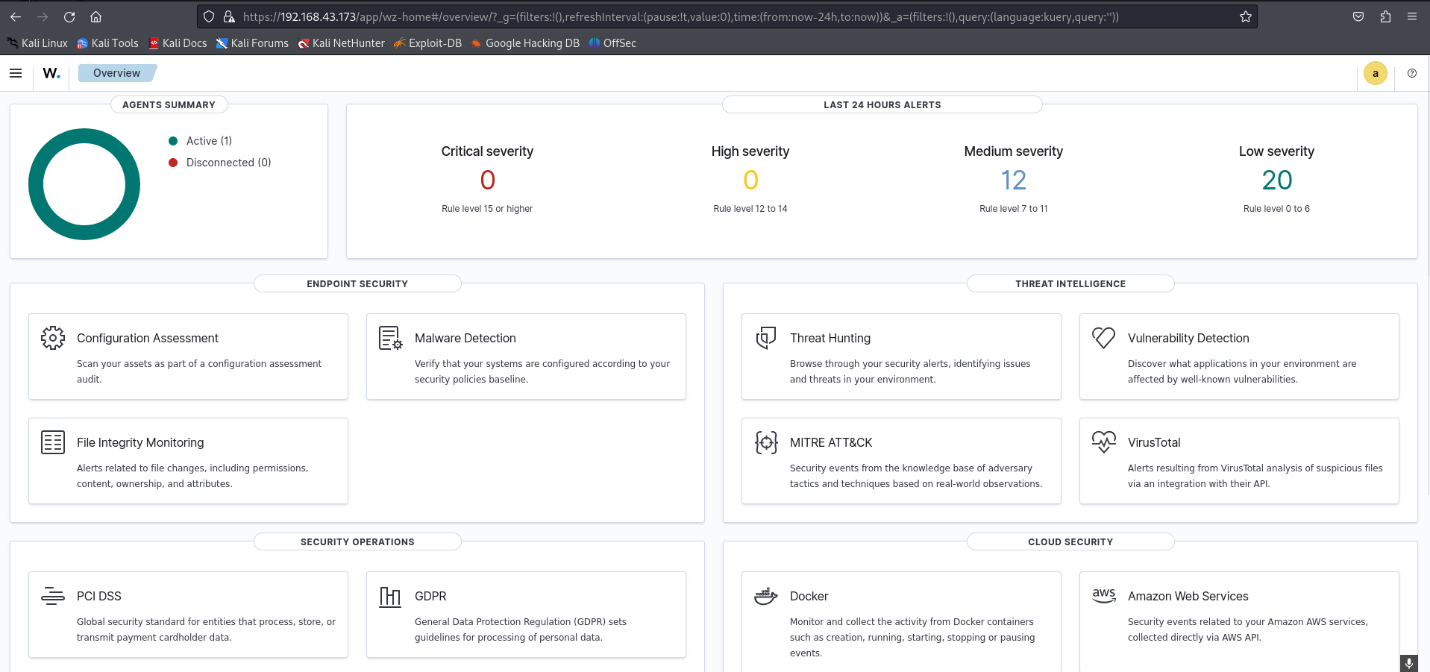


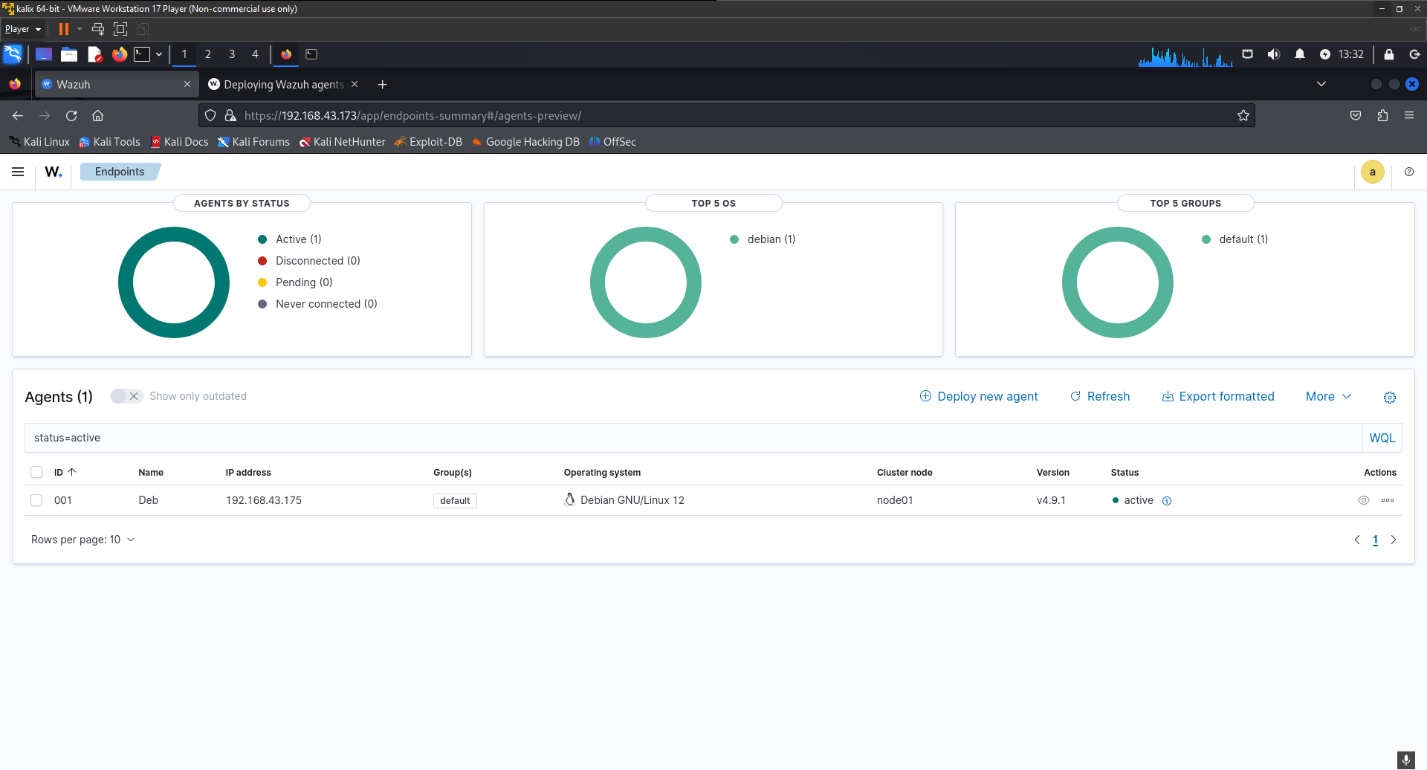
Разворачиваем агент на второй ВМ



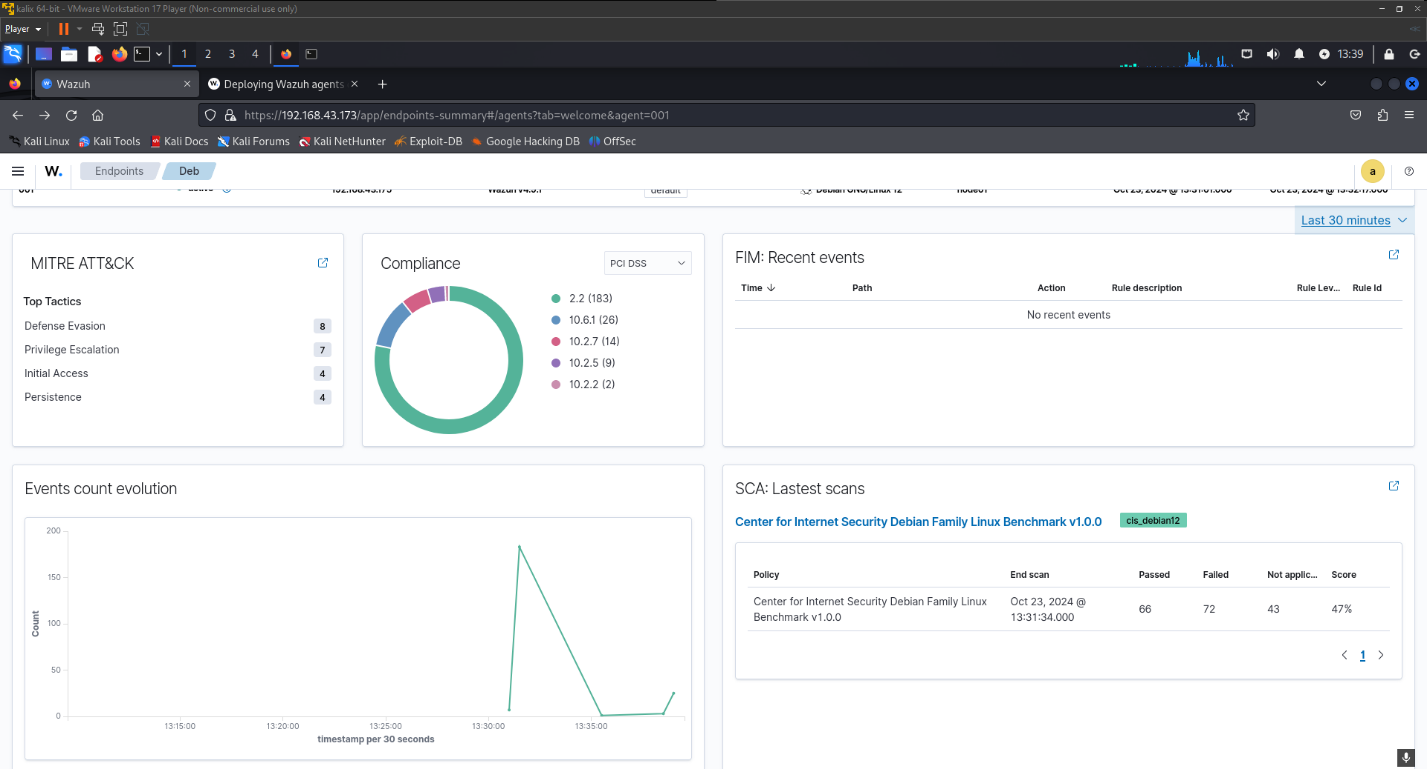


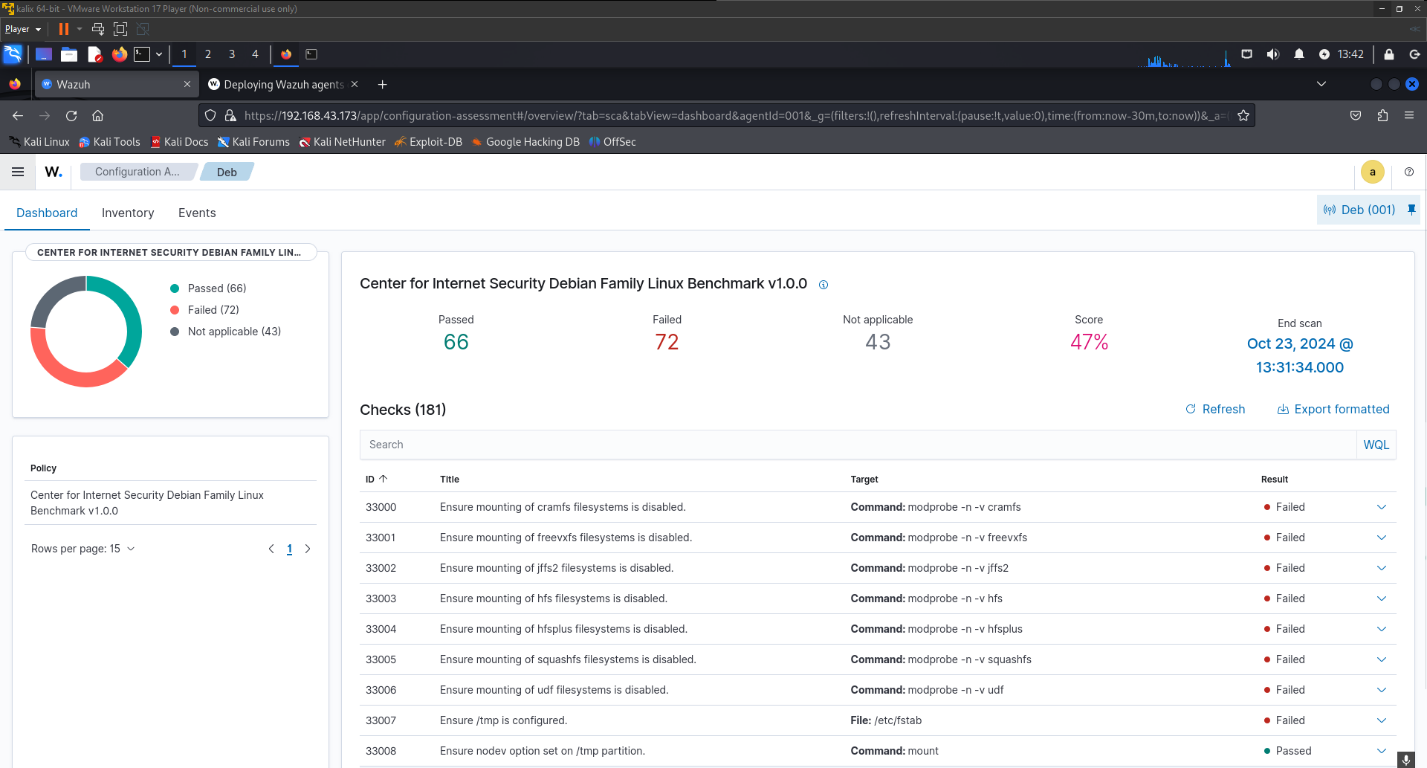
После настройки убедились, что агент настроен. И доступна машина для мониторинга

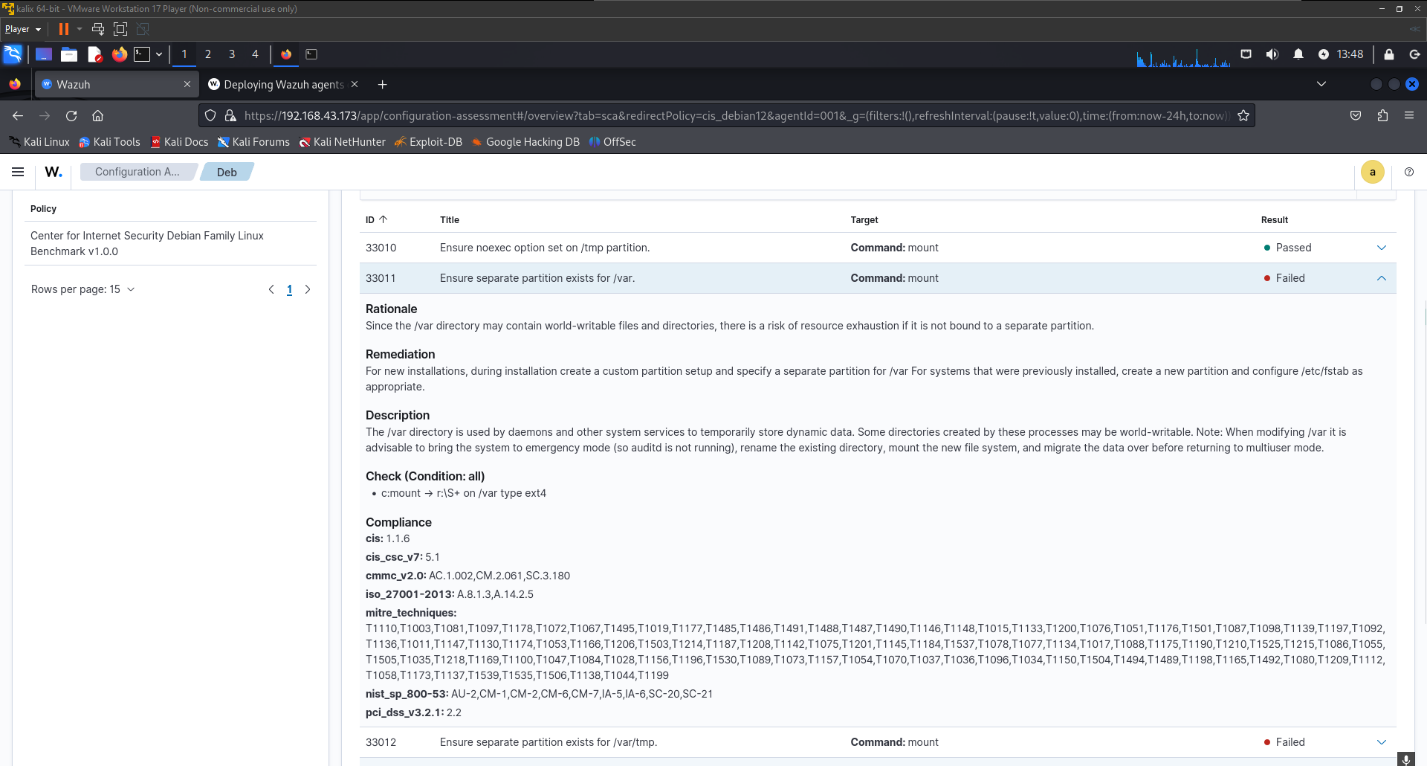


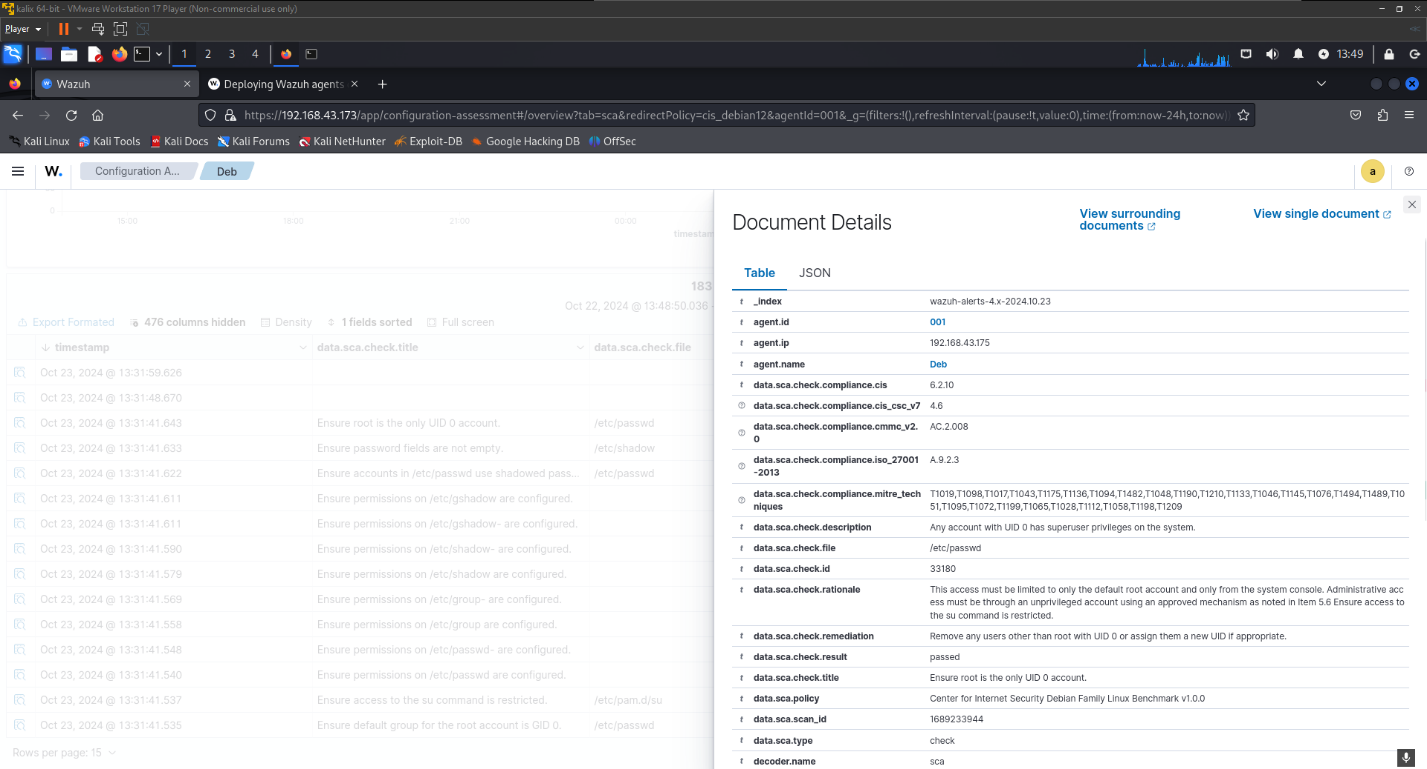


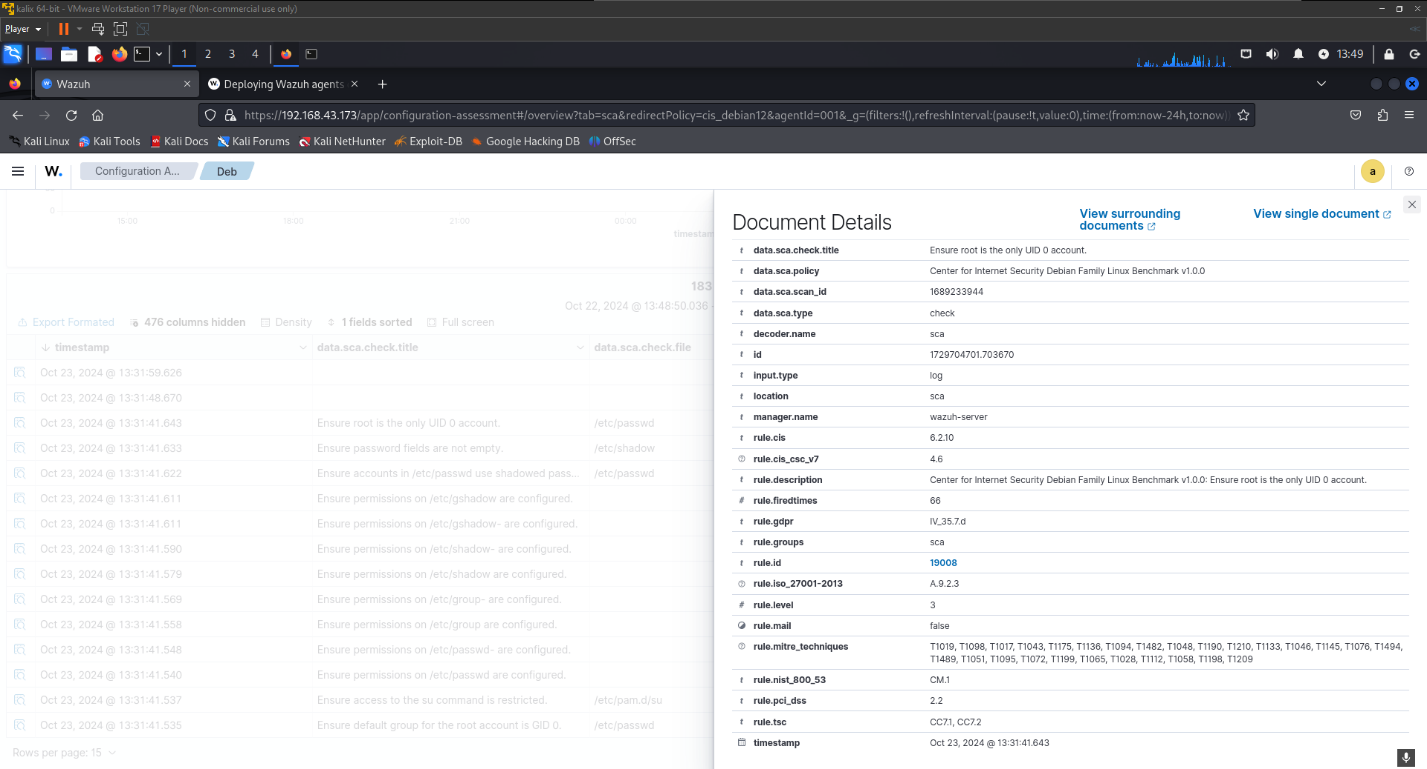
Система имеет встроенный детектор уязвимостей



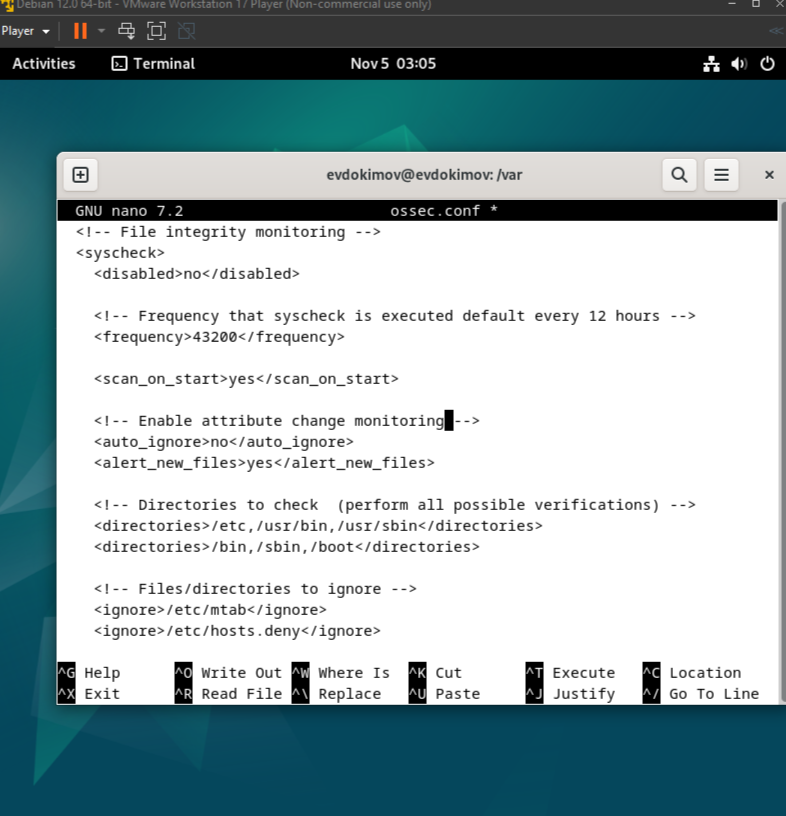




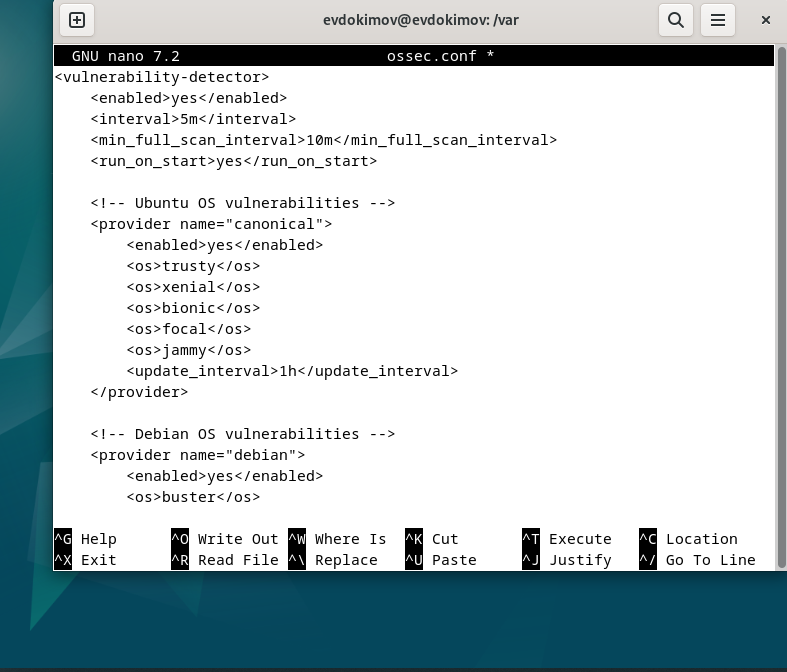




Создание проверки целостности файлов



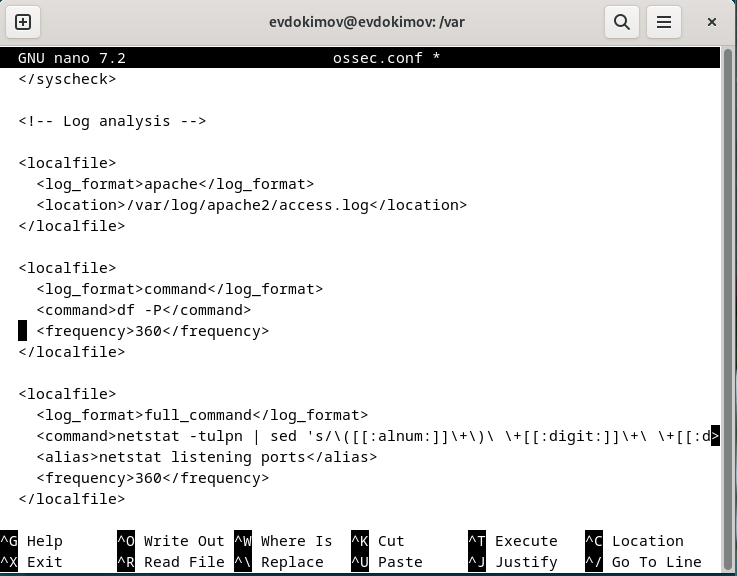
Настройка выявлений уязвимостей в соответствии с документацией



Выявление скрытых процессов



Выявление SQL-инъекций



Проверка работы настроенных механизмов

SQL injection

