

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет» РТУ МИРЭА**

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Отчёт по практической работе №3

по дисциплине: «Система для сбора событий и логов»

Группа: ББМО-02-22

Выполнил: Давыдов И.Д.

Проверил: Козачок А.В.

Москва, 2024

содержание

[Введение 3](#_Toc157696772)

[Ход выполнения работы 4](#_Toc157696773)

[Шаг 1. Разворачиваем 2 виртуальные машины 4](#_Toc157696774)

[Шаг 2. Настройка сетевого обмена 4](#_Toc157696775)

[Шаг 3. Установка сервера Wazuh 5](#_Toc157696776)

[Шаг 4. Установка агента Wazuh 6](#_Toc157696777)

[Шаг 5. Изучим меню сканирования wazuh 6](#_Toc157696778)

[Шаг 6. Создадим проверку целостности файлов 13](#_Toc157696779)

[Шаг 7. Создадим настройку выявления уязвимостей 14](#_Toc157696780)

[Шаг 8. Создадим выявление скрытых процессов 17](#_Toc157696781)

[Шаг 10. Настройка выявления web shell attack 22](#_Toc157696782)

[Заключение 23](#_Toc157696783)

# Введение

**Цель практической работы:** Выполнить установку и настройку Wazuh.

**Задачи:**

1. Разверните виртуальные машины (минимум 2 – сервер и агенты);
2. Обеспечить между ними сетевой обмен;
3. Развернуть на одной из ВМ сервер Wazuh;
4. Подключите агента используя документацию;
5. Убедившись, что агент установлен, зайдите на веб-интерфейс сервера wazuh и изучите предлагаемые пункты меню сканирования ресурса, доступные из коробки. Проанализируйте обнаруженные уязвимости;
6. Создайте проверку целостности файлов;
7. Настройте выявление уязвимостей в соответствии с документацией;
8. Настройте выявление скрытых процессов;
9. Настройте выявление SQL-инъекций;
10. Изучить выявление web shell attack;
11. Продемонстрируйте работу настроенных механизмов в отчете со скриншотами.

# Ход выполнения работы

# Шаг 1. Разворачиваем 2 виртуальные машины

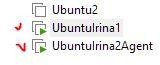
Самым привычным образом создадим две виртуальные машины и установим на них ОС Ubuntu (рисунок 1.1).

Рисунок 1.1 – Созданные виртуальные машины

# Шаг 2. Настройка сетевого обмена

Для настройки сетевого обмена включим режим моста в настройках сети виртуальных машин. Проверим, что ВМ пингуются между собой (рисунок 1.2).

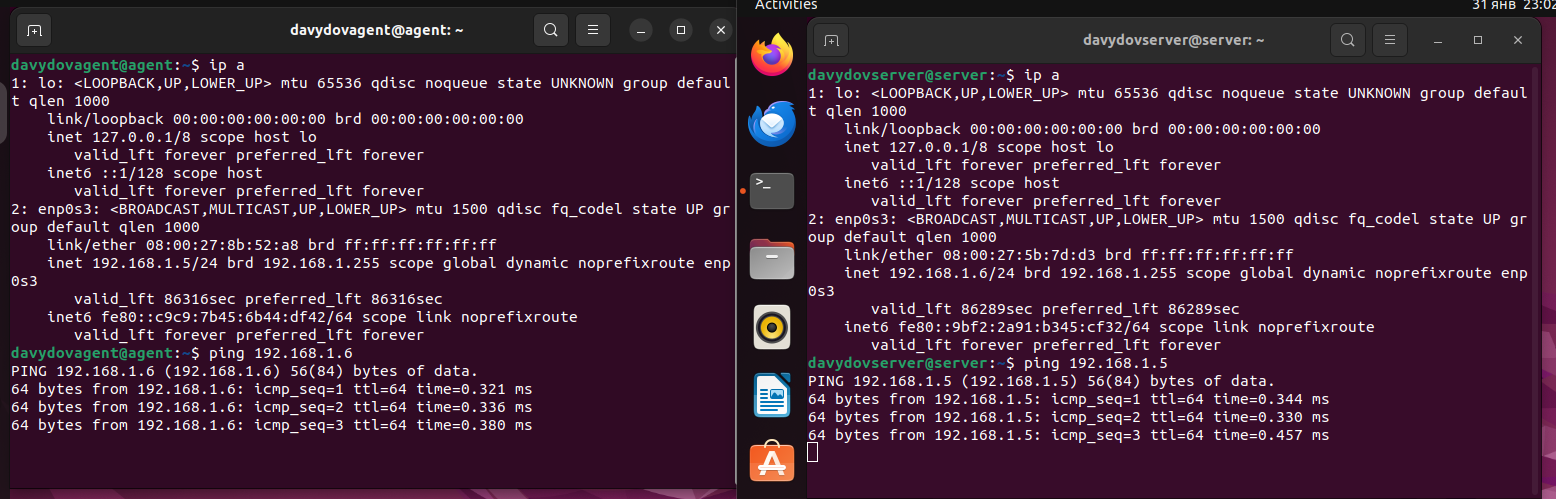


Рисунок 1.2 – Проверка сетевого обмена

# Шаг 3. Установка сервера Wazuh

Установка сервер wazuh через помощника установки. Для этого сначала скачиваем установочный скрипт и запускаем его командой «curl -sO https://packages.wazuh.com/4.5/wazuh-install.sh && sudo bash ./wazuh-install.sh -a» (рисунок 3.1).

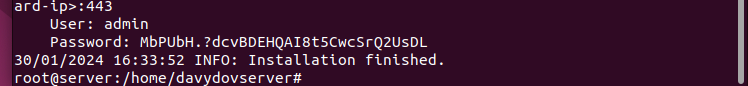
=

Рисунок 3.1 – Установка сервера Wazuh, видно Логин(admin) и Пароль(MbPUbH.?dcvBDEHQAI8t5CwcSrQ2UsDL)

# Шаг 4. Установка агента Wazuh

Для установки агента нам потребутся подключить репозиторий Wazuh, а затем уже задеплоить сам агент (рисунок 4.1).



Рисунок 4.1 – Установка агента Wazuh

# Шаг 5. Изучим меню сканирования wazuh

Логин и пароль нам был предоставлен в терминале по окончанию выполнения скрипта. Авторизуемся. Подключимся к веб-интерфейсу Wazuh по адресу https://192.168.1.7 (рисунок 5.1).

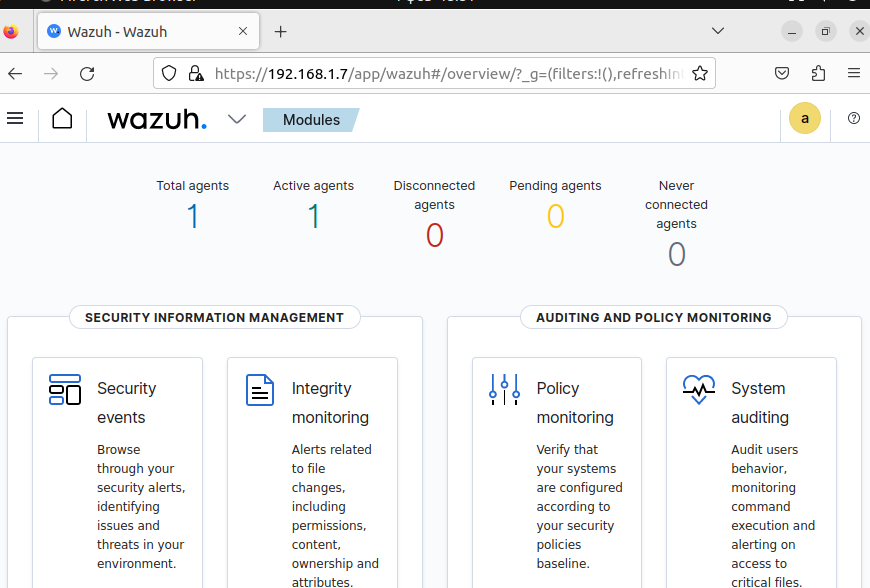


Рисунок 5.1 – Веб-интерфейс Wazuh

Видим подключённые агенты (рисунок 5.2).

Рисунок 5.2 – Агенты

Изучим предлагаемые пункты меню сканирования ресурса по умолчанию:

**Security events.**

В этом разделе мы можем увидеть предупреждения системы безопасности в виде дашбордов и в виде таблицы.

Cобытия безопасности (рис. 5.3-5.5).

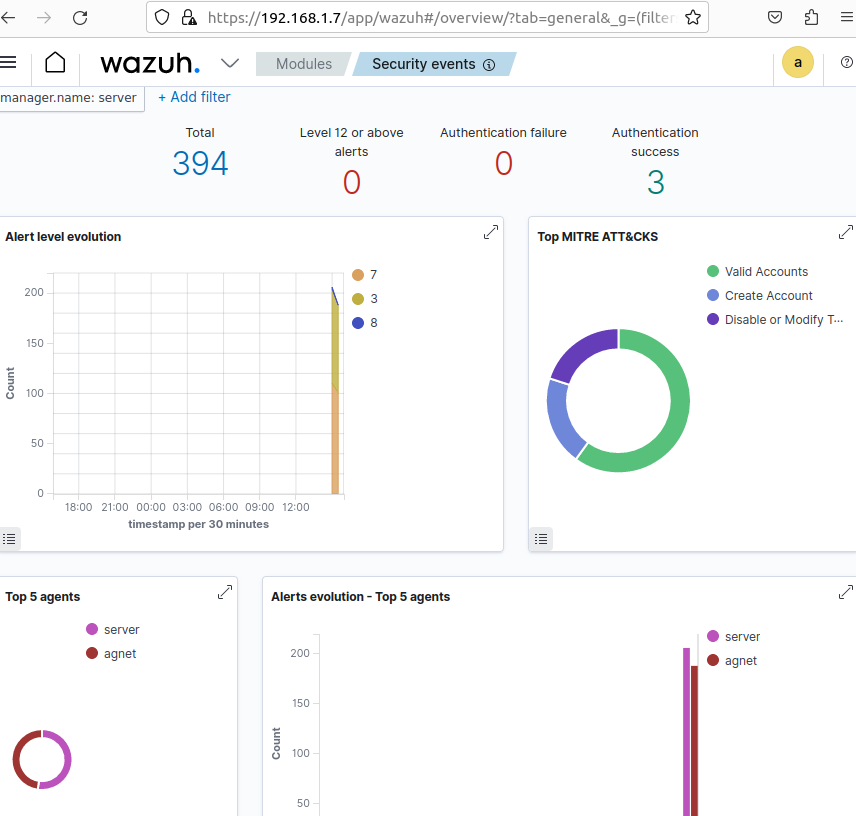


Рисунок 5.3 – Дашборд по событиям безопасности

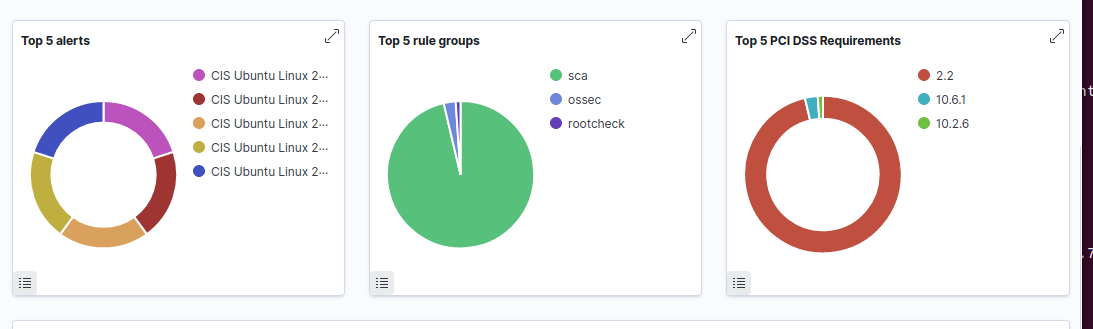


Рисунок 5.4 – Дашборд по событиям безопасности

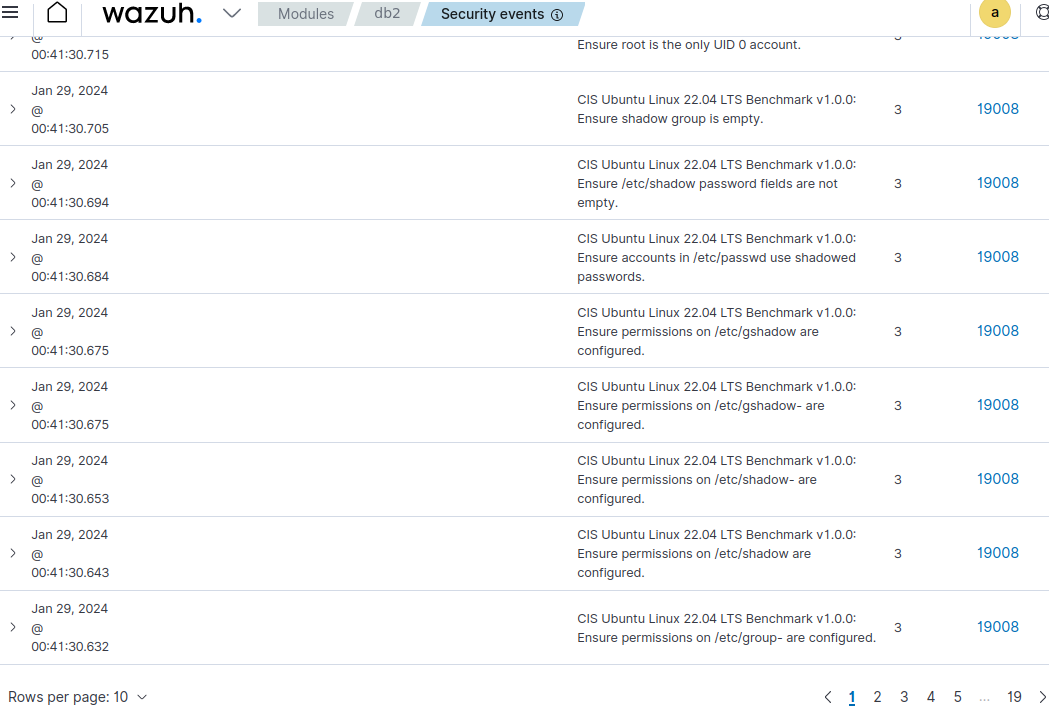


Рисунок 5.5 – Таблица по событиям безопасности

**Mitre Attack.**

Этот модуль сравнивает события безопасности с базой изученных тактик и техник злоумышленников, так называемой базой MITRE ATT&CK (рис. 5.6).

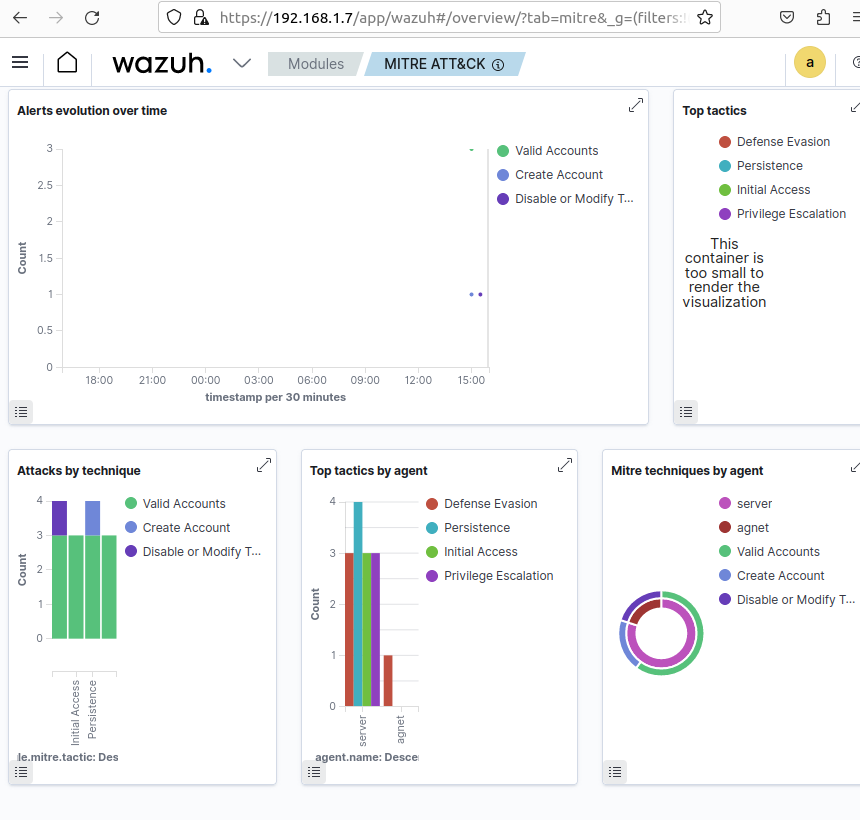


Рисунок 5.6 – Общий дашборд

**NIST 800-53.**

Этот модуль проводит проверку на соответствие требованиям стандарта NIST 800-53. NIST 800-53 – это стандарт информационной безопасности, который предоставляет перечень мер безопасности для федеральных информационных систем (рис. 5.7).

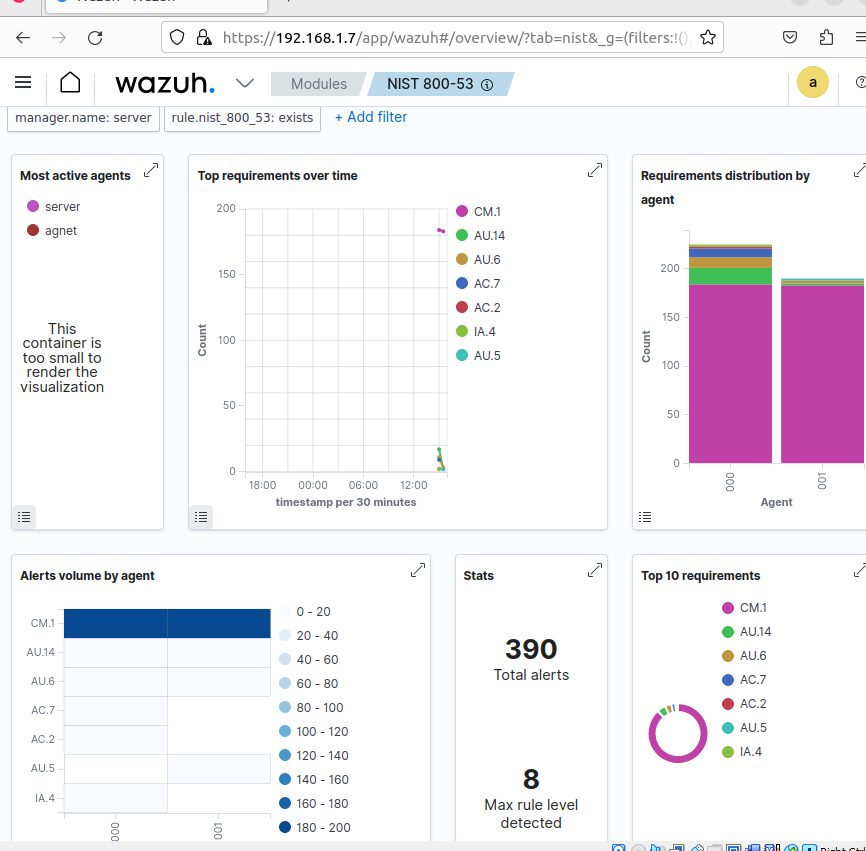


Рисунок 5.7 – Модуль NIST 800-53

**Security configuration assessment.**

Этот модуль сканирует активы в рамках аудита оценки конфигурации. В этом разделе мы можем увидеть алерты по событиям безопасности ОС в виде общей сводки (рисунок 5.8).

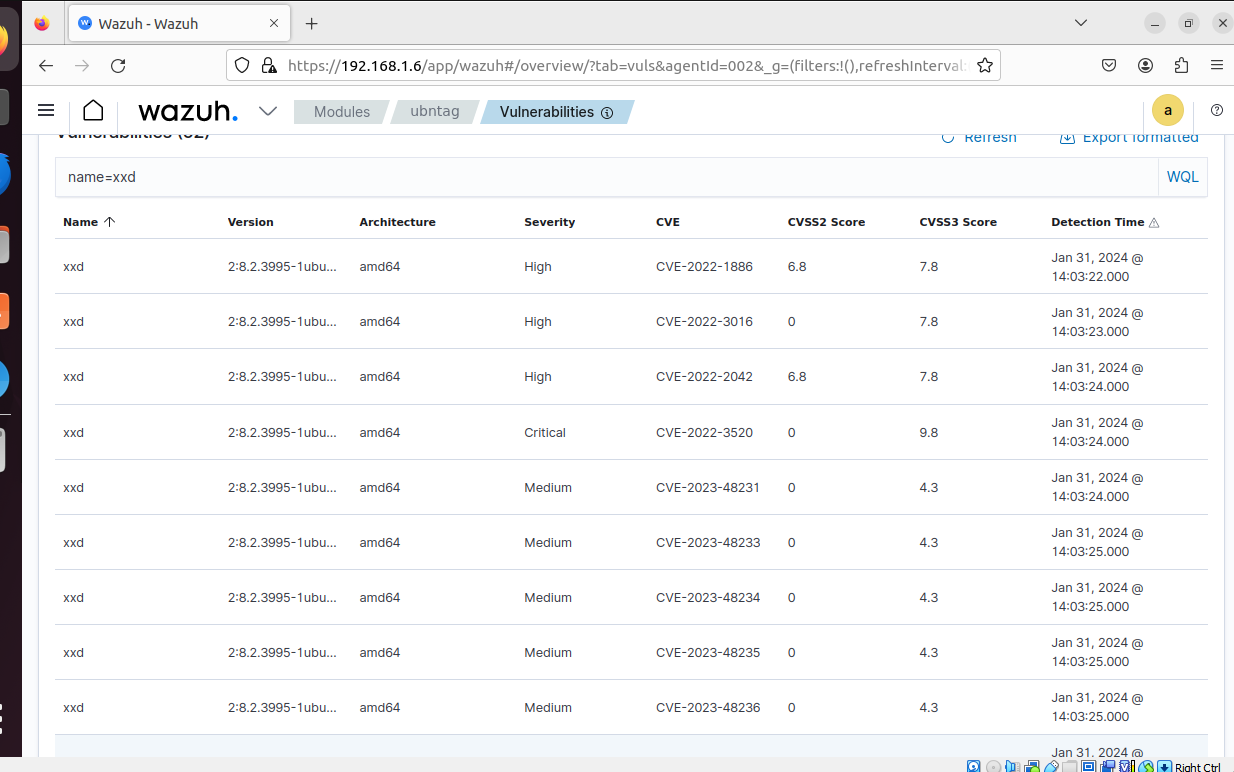


Рисунок 5.8 – vulnerabilities

**TSC (Regulatory compliance).**

Этот модуль проводит проверку на соответствие критериям доверенных служб для безопасности, доступности, целостности обработки, конфиденциальности и секретности.

**GDPR (Regulatory compliance).**

Этот модуль проводит проверку на соответствие общему регламент по защите данных (GDPR), который устанавливает правила обработки персональных данных.

**HIPAA (Regulatory compliance).**

Этот модуль проводит проверку на соответствие закону о переносимости и подотчетности медицинского страхования 1996 года (HIPAA), который обеспечивает конфиденциальность и безопасность данных для защиты медицинской информации.

**PCI DSS (Regulatory compliance).**

Этот модуль проводит проверку на соответствие требованиям стандарта PCI DSS. PCI DSS (Payment Card Industry Data Security Standard) – это стандарт безопасности данных платёжных карт, учреждённый международными платёжными системами Visa, MasterCard, American Express, JCB и Discover.

# Шаг 6. Создадим проверку целостности файлов

Отредактируем конфигурацию агента /var/ossec/etc/ossec.conf добавив в список проверяемых папок /home (рис. 6.1).

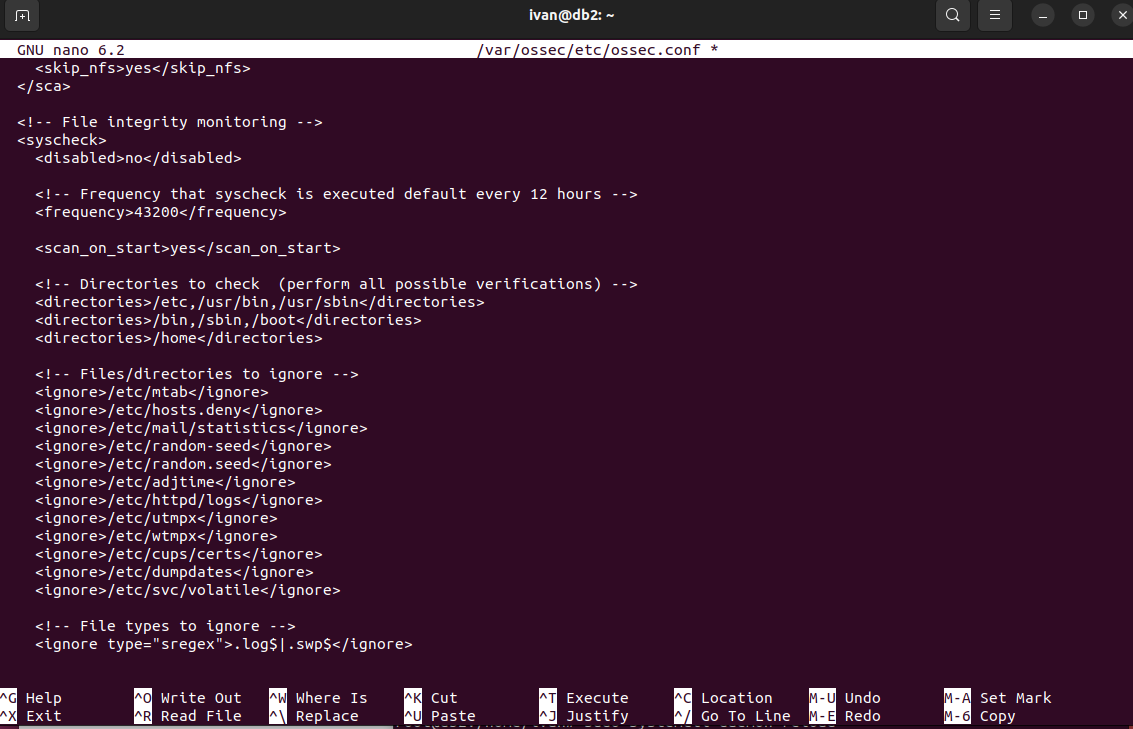


Рисунок 6.1 – Добавление директорий и файлов к мониторингу файловой системы

Видим добавленные файлы из папки /home (рис. 6.2).

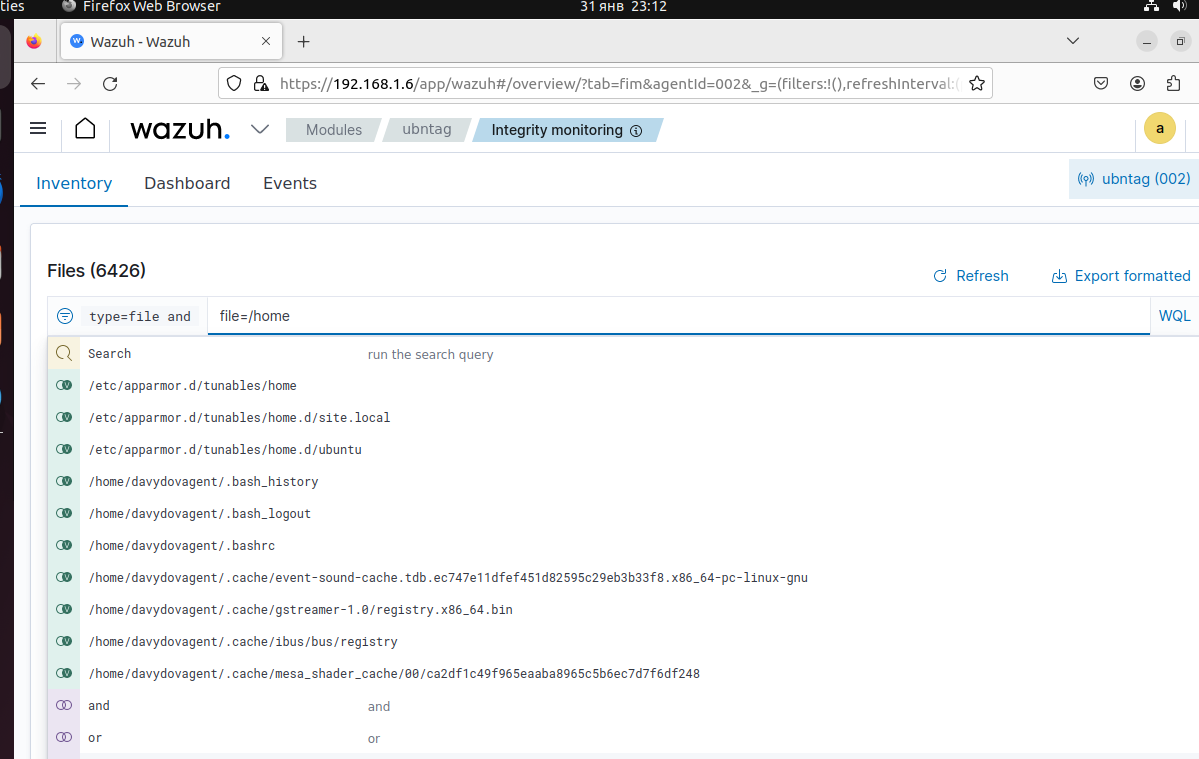


Рисунок 6.2 – Добавленная директория

# Шаг 7. Создадим настройку выявления уязвимостей

Сконфигурируем общего агента на сервере. Добавление раздела, отвечающего за syscollector в конфигурационный файл агента или сервера представлен на рисунке 7.1.

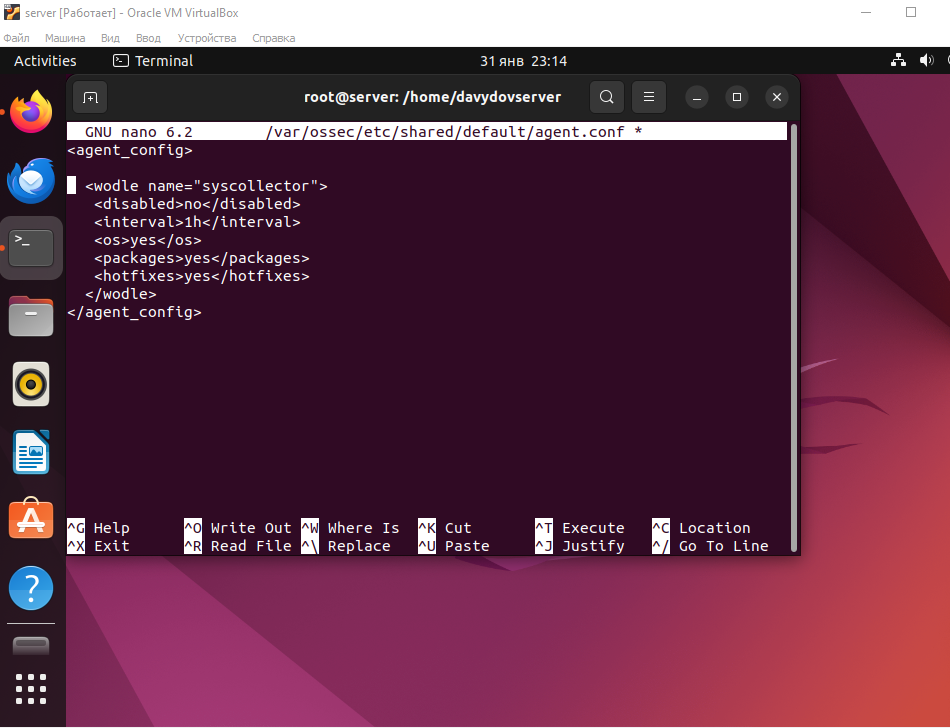
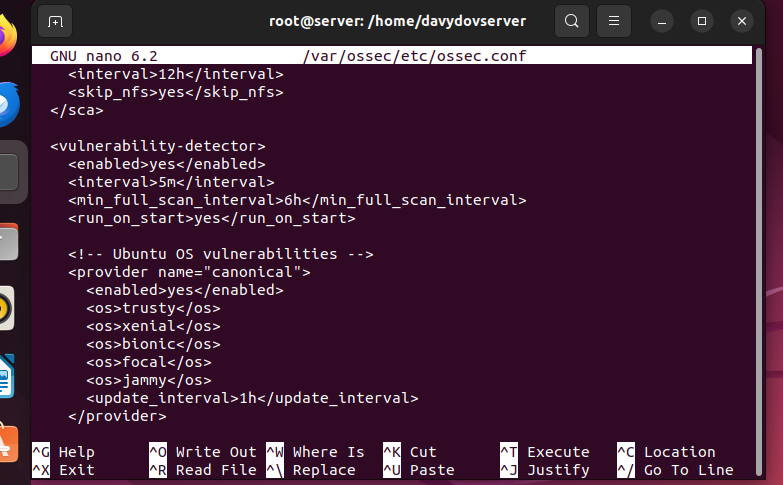


Рисунок 7.1 – Подключаем syscollector

Активация модуля детектора уязвимостей и указание операционных систем агентов в конфигурационном файле сервера. Включим обнаружение уязвимостей для Ubuntu (рис. 7.2).

Рисунок 7.2 – Активация детектора и подключение ОС агентов

Перезапуск сервиса агента и/или сервера для применения изменений (рис.

7.3).

Рисунок 7.3 – Перезапуск сервиса сервера Видим список уязвимостей (рис. 7.4).

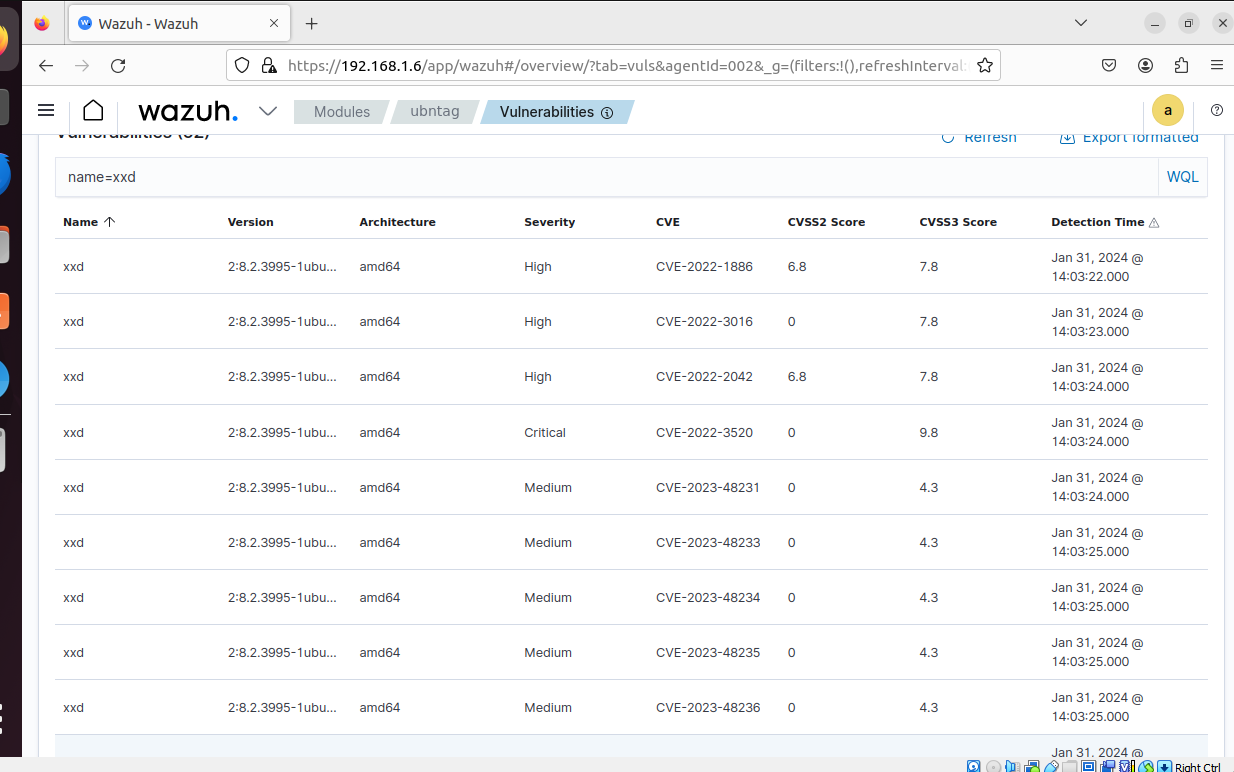


Рисунок 7.4 – События детектора уязвимостей

# Шаг 8. Создадим выявление скрытых процессов

Установим rootkit.

Изменим частоту проверок агента до 60 секунд с целью уменьшения таймаута срабатывания рутчекера (рис. 8.1).

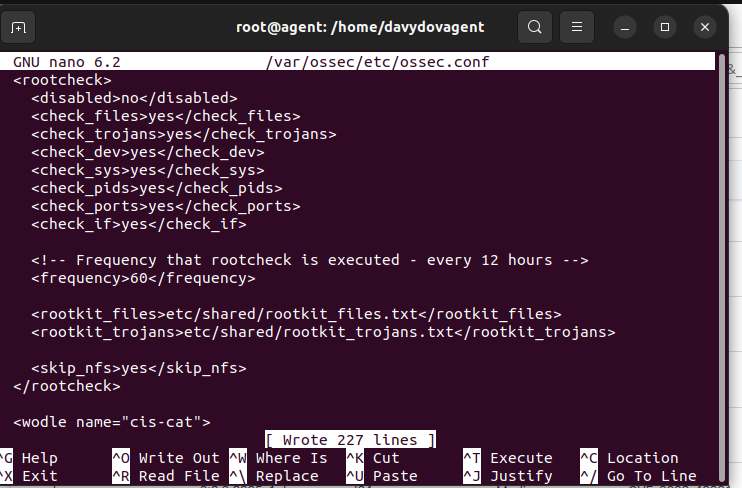


Рисунок 8.1 – Настройка частоты срабатывая рутчекера Перезапуск сервиса агента для применения изменений (рисунок 8.2).

Рисунок 8.2 – Перезапуск агента Эмуляция атаки представляет из себя следующий алгоритм:

* Клонирование репозитория с руткитом (рис. 8.3);
* Компиляция руткита;
* Загрузка руткита в ядро;
* Отправка сигнала KILL -63 со случайным PID для обнаружения руткита. Имитация атаки (рис. 8.4):



Рисунок 8.3 – Клонирование исходного кода руткита

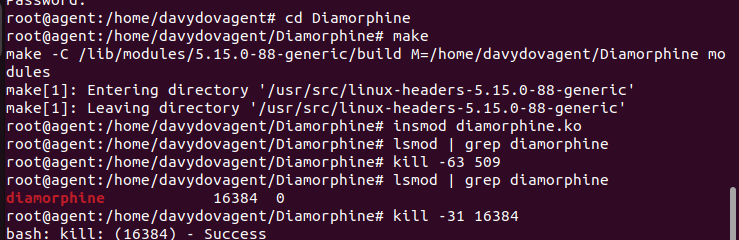


Рисунок 8.4 – Компиляция, загрузка руткита, который создает скрытый процесс Скроем процесс rsyslogd с помощью руткита. Для этого нужно отправить

сигнал KILL -31 с PID rsyslogd (рис. 8.5 (команды видно в 8.4)).

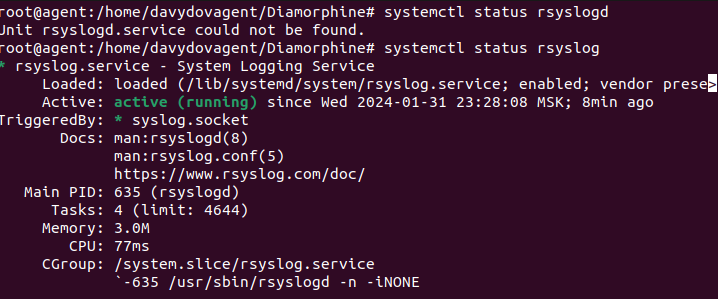


Рисунок 8.5 – Сокрытие процесса rsyslogd Посмотрим результат (рис. 8.6).

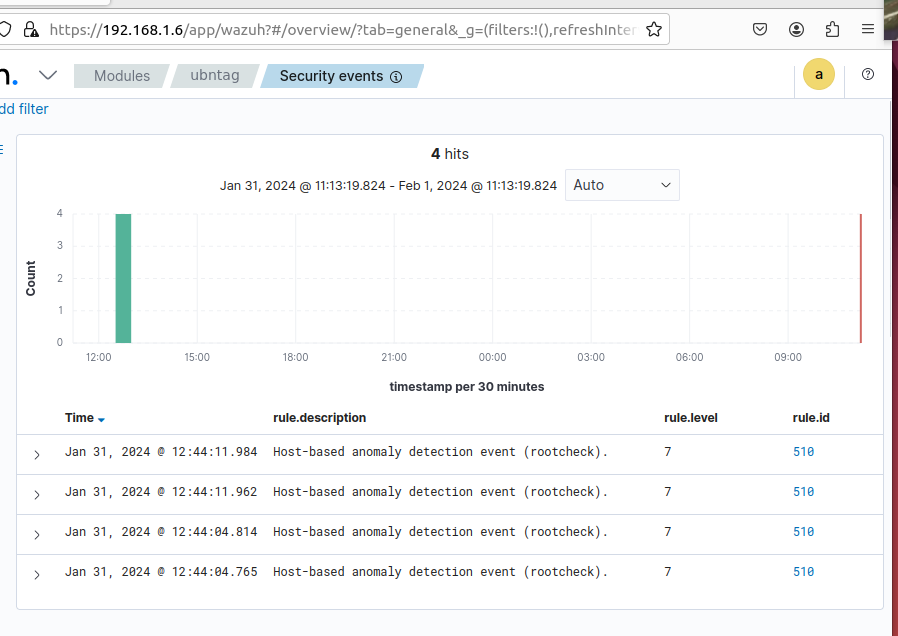
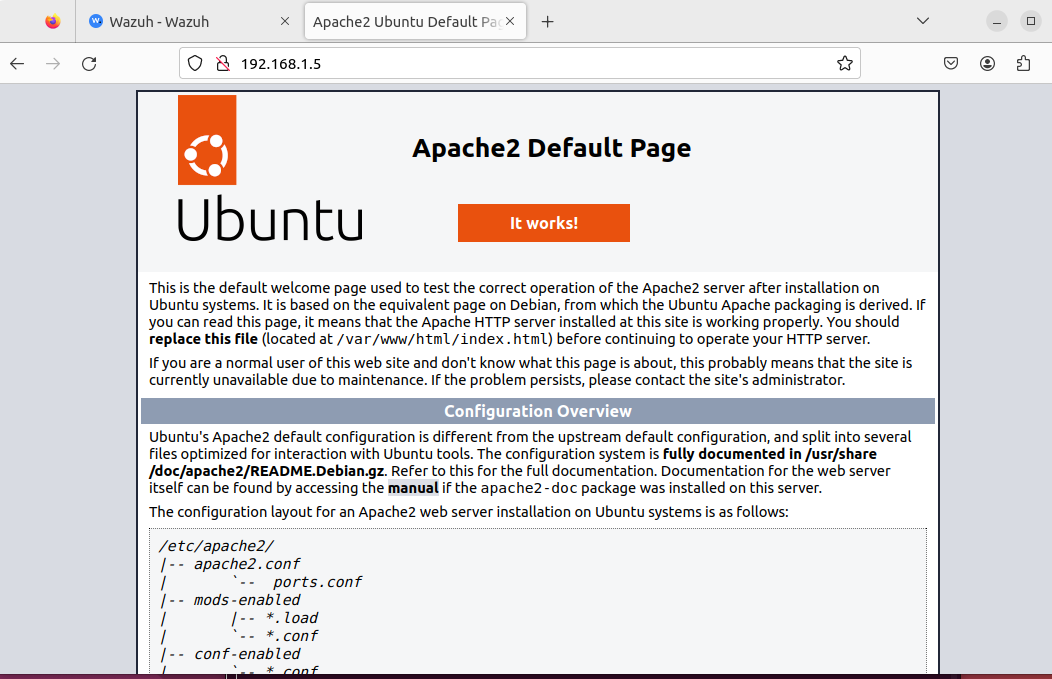


Рисунок 8.6 – Результат скрытого процесса

**Шаг 9. Создадим выявление sql иньекций Установим apache.**

Настройка выявления SQL-инъекций: Для этого установим Apache и настроим агент. Установка веб-сервера (рис. 9.1).

Рисунок 9.1 – Приветственное окно веб-сервера

Настройка конфигурационного файла агента для подключения веб- сервера к мониторингу. Добавим отслеживание apache (рис. 9.2).

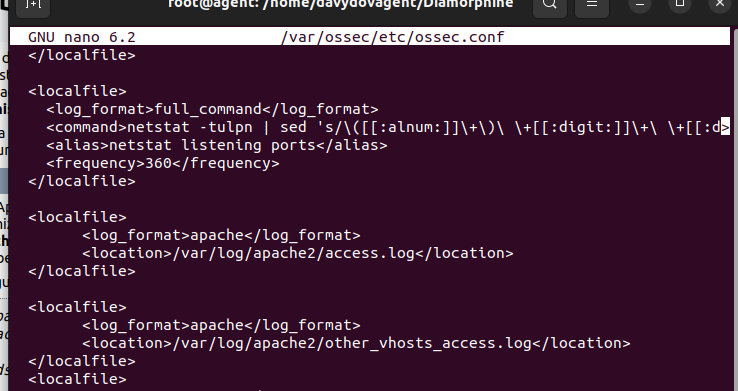


Рисунок 9.2 – Настройка конфига агента

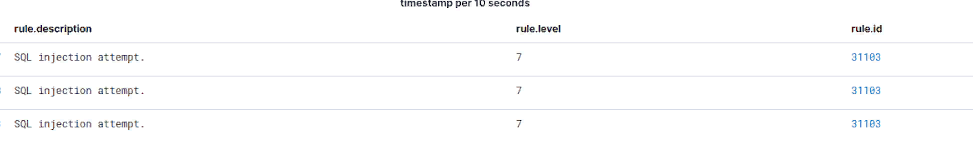
Список команд: sudo apt install apache2 sudo ufw app list

sudo ufw allow 'Apache'

sudo systemctl status apache2 curl http://192.168.1.5

Сэмулируем атаку. Для этого выполним команду:

curl -XGET "http://<192.168.1.5>/users/?id=SELECT+\*+FROM+users"; Посмотрим на sql иньекцию (рис. 9.3).

Рисунок 9.3 – Результат

# Шаг 10. Настройка выявления web shell attack

Настройка выявления web shell attack может быть проведена следующими вариантами:

* Использование Integrity monitoring (FIM) для обнаружения создания и модификации web shell файлов.
* Использование своих правил Wazuh для обнаружения действий web shell.
* Использование мониторинга команд для отслеживания сетевых подключений и попыток атак.

# Заключение

В процессе выполнения данной работы был изучен функционал Wazuh, настроены и показаны механизмы его работы.