**Министерство науки и высшего образования Российской Федерации** ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий Дисциплина:**

«Организация и обеспечение аудита настроек средств защиты информации»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6**

«**Методическая ЗИ с помощью специализированных программных средств.**»

**Выполнили:**

Молитвин Илья Алексеевич, студент группы N3345

(подпись)

**Проверил:**

Пенин Андрей Семенович

(отметка о выполнении)

(подпись)

Содержание

[Ход работы 3](#_Toc199676225)

[Этап 1 4](#_Toc199676226)

[Этап 2 6](#_Toc199676227)

[Этап 3 10](#_Toc199676228)

[Заключение 12](#_Toc199676229)

Ход работы

**Цели:**

**Цели работы:**

Необходимо установить и настроить систему предотвращения утечек данных (DLP), систему управления информацией и событиями безопасности (SIEM), а также систему резервного копирования данных. Работа выполняется на виртуальной машине (рекомендуется использовать ту же, что и в предыдущих ПР) и включает три этапа. Результаты оформляются в отчёт.

**Этапы работы:** Этап 1. Установка и настройка DLP-системы (до 3 баллов)

- Установите программное обеспечение для предотвращения утечек данных (например, OpenDLP, MyDLP или аналоги).

- Настройте параметры мониторинга: определите защищаемые данные (например, текстовые файлы с заданным шаблоном, такие как номера кредитных карт или паспортов); установите правила блокировки или журналирования попыток копирования данных (например, на USB или через сеть).

- Проведите тестирование: попробуйте скопировать защищённые данные на внешний носитель или передать через сеть; зафиксируйте срабатывание DLP (логи, уведомления).

Этап 2. Установка и настройка SIEM-системы (до 4 баллов)

- Установите программное обеспечение для SIEM (например, ELK Stack с Elastic SIEM, Splunk Free, Graylog или аналоги).

- Настройте сбор и анализ событий: подключите источник логов (например, системные логи ОС или приложения); создайте правило обнаружения подозрительной активности (например, многократные неудачные попытки входа).

- Проведите тестирование: сгенерируйте тестовые события (например, несколько раз введите неверный пароль); продемонстрируйте, что SIEM зафиксировала событие и выдала уведомление или отчёт.

Этап 3. Установка и настройка системы резервного копирования (до 3 баллов)

- Установите программное обеспечение для резервного копирования (например, Bacula, Duplicati, rsync или встроенные средства Windows).

- Настройте параметры: задайте расписание автоматического создания резервных копий (например, ежедневно); выберите каталог для копирования (например, /important или C:\Data) и место хранения копий.

- Проведите тестирование: создайте резервную копию тестовых данных; удалите или измените исходные файлы и восстановите их из копии.

Отчёт должен содержать описание действий, скриншоты и выводы по каждому этапу.

Кроме того, быть готовым к демонстрации ВМ на защите работы.

Этап 1

Этап 1. Установка и настройка DLP-системы  
Выбираем auditd, устанавливаем, включаем службы,добавляем правила на папку, проверяем логи, после создания файла в папке.

Изображение выглядит как текст, электроника, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 1 – настройка и тест auditd

Создаем файл с иммитацией защищенных данных, echo "Секретный номер: 1234-5678-9012-3456" > /opt/secret\_data/credit\_card.txt

chmod 600 /opt/secret\_data/credit\_card.txt,  
воспользуемся еще сервером для тестировок webhook,и попробуем передать наш файл на наш айпи.

Изображение выглядит как текст, программное обеспечение, веб-страница, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 2 – Фиксируем передачу файлаИзображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.  
Рисунок 3 – передача файла

Проверяем логи и фиксируем, что DLP эмуляция работате, факт утечки зафиксирован, файл использовался.

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 4 – Логи

Этап 2

Этап 2. Установка и настройка SIEM-системы

Установить Docker и Docker Compose

sudo apt update

sudo apt install -y docker.io docker-compose sudo systemctl enable docker

sudo systemctl start docker

Развертывание Wazuh с помощью Docker Загрузка исходного кода Docker Compose:

git clone https://github.com/wazuh/wazuh-docker.git -b v4.12.0 cd wazuh-docker/single-node

Создание SSL-сертификатов:

docker-compose -f generate-indexer-certs.yml run --rm generator

Эта команда создаст сертификаты в каталоге config/wazuh\_indexer\_ssl\_certs. Запуск системы Wazuh:

docker-compose up -d

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 5 - вход

Установка Wazuh Agent на Ubuntu Установка Wazuh Agent

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --dearmor

-o /etc/apt/trusted.gpg.d/wazuh.gpg

echo "deb https://packages.wazuh.com/4.x/apt stable main" | sudo tee

/etc/apt/sources.list.d/wazuh.list sudo apt update

sudo apt install wazuh-agent -y

Настройка отправки логов на Wazuh Manager Открыть файл конфигурации:

sudo nano /var/ossec/etc/ossec.conf

Найти блок <server> и изменить его на следующий:

<server>

<address>127.0.0.1</address>

</server>

Запуск и проверка состояния агента sudo systemctl enable wazuh-agent sudo systemctl start wazuh-agent

sudo systemctl status wazuh-agent

Установка и активация SSH-сервера на Ubuntu Установка OpenSSH-сервера:

sudo apt update

sudo apt install openssh-server -y

Запуск и активация SSH-сервиса:

sudo systemctl enable ssh sudo systemctl start ssh

(Необязательно) Создание тестового пользователя:

sudo adduser testuser

→ Введите пароль и любые данные по запросу.

Проверка работы и генерация события:

Подключитесь по SSH к localhost:

ssh [testuser@127.0.0.1](mailto:testuser@127.0.0.1)

Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 6 - Подключитесь по SSH к localhost

→ Введите несколько раз неправильный пароль, чтобы сгенерировать предупреждение "Failed password".

Проверка события в Wazuh Dashboard:

Перейдите в Security Events и отфильтруйте по ключевым словам:

sshd

authentication failure

Изображение выглядит как текст, снимок экрана, число, линия

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 7 - Результат

Этап 3

Этап 3. Установка и настройка системы резервного копирования

Устанавливаем rsync, подготавливаем директории и тестовые файлы, создаем скрипт,  
 #!/bin/bash

# Резервное копирование директории ~/important в ~/backups/important\_bkp с логом

rsync -av --delete ~/important/ ~/backups/important\_bkp/ >> ~/backup.log,  
делаем его испольняемым, открываем планировщик, устанавливаем на ежедневно в 02:00,тестируем, создаем бекап вручну, потом удаляем или изменяем файл, и восстанавливаем, смотрим логи и убеждаемся, что всё получилось

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

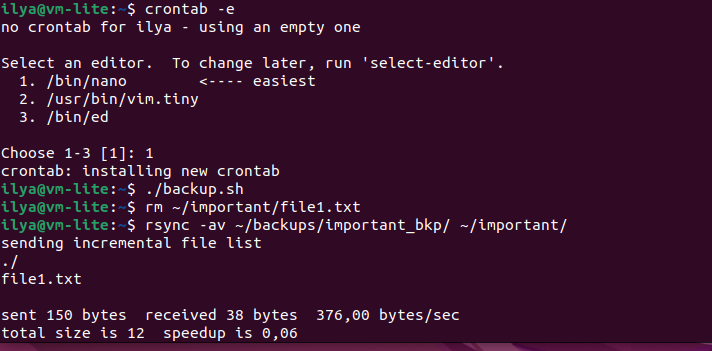
Рисунок 8 – Подготовка каталогов и файлов, создание скрипта.  


Рисунок 9 – Установка расписания,тестирование

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 10 – устанавливаем расписание на 02:00  
Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.  
Рисунок 11 – Смотрим логи.

Заключение

В рамках выполнения лабораторной работы были реализованы три этапа, направленные на повышение уровня информационной безопасности посредством предотвращения утечек данных, выявления инцидентов и обеспечения сохранности информации.

На **первом этапе** была установлена и настроена DLP-система с использованием встроенных средств мониторинга и аудита Linux (в частности, auditd), имитирующих функции DLP. Настроены правила для отслеживания доступа к защищённым данным, содержащим чувствительную информацию. Проведено тестирование путём попытки копирования таких данных на внешний носитель, что успешно зафиксировалось в логах системы. Это позволило продемонстрировать возможность базового предотвращения утечек и фиксации инцидентов.

На **втором этапе** была установлена и сконфигурирована SIEM-система **Wazuh** в одновузловой конфигурации с применением Docker. Подключён агент безопасности на контролируемом узле, проведено моделирование инцидента — многократные неудачные попытки входа в систему по SSH. Система успешно зарегистрировала события и отобразила их в веб-интерфейсе, что подтвердило её работоспособность. Wazuh показал эффективность в агрегации, анализе и визуализации событий безопасности.

На **третьем этапе** была настроена система резервного копирования с помощью **rsync** и cron. Задано ежедневное автоматическое копирование содержимого выбранного каталога в указанный резервный репозиторий. Проведено тестирование: после удаления тестовых данных они были успешно восстановлены из резервной копии, что подтверждает надёжность настроенного решения.

Таким образом, все поставленные цели лабораторной работы были достигнуты. Полученные практические навыки и знания формируют основу для дальнейшего освоения методов защиты информации и построения комплексных решений обеспечения безопасности в корпоративной среде.