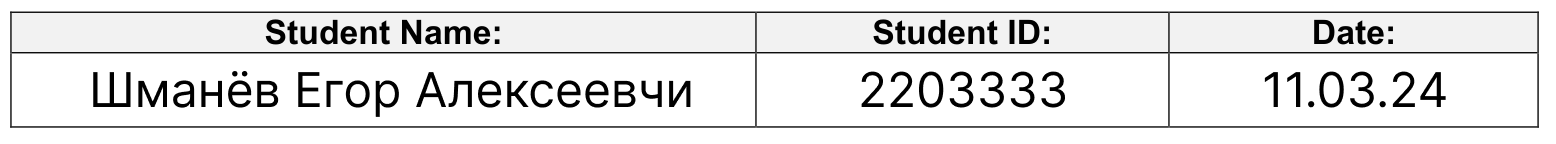
Отчет по лабораторной работе №2

Дисциплина: Информационная безопасноть

# Выполнил студент группы БИВТ-22-2 Шманёв Егор



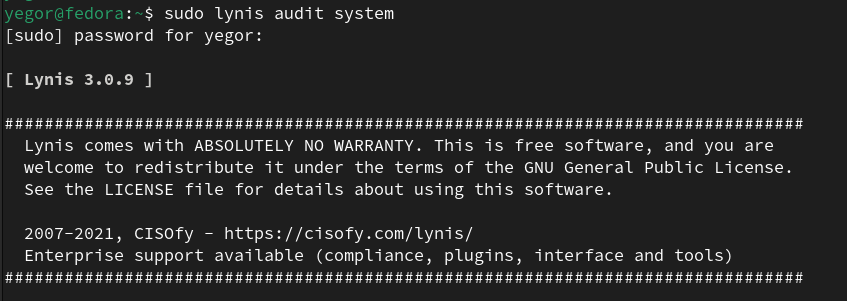
Рис. 1 – Запуск **lynis**

Рис. 2 – Предупреждение о уязвимости в службе сбора и управления журналами сбоев.

**Возможные причны уязвимости:**

**1. Несанкционированный доступ:**

* Возможно получить несанкционированный доступ к журналу ABRT, который содержит конфиденциальную информацию.

**2. Повышение привилегий:**

* Есть возможность использовать уязвимость в службе для повышения своих привилегий в системе.

**Рис. 3 — Предупреждение о уязвимости в службе **Postgresql 16****

****Возможные причины уязвимости:****

**Возможные уязвимости:**

**1. Несанкционированный доступ:**

* + - Есть возможность получить несанкционированный доступ к базе данных PostgreSQL, если она не корректна настроена.

**2. Повышение привилегий:**

* + - **Злоумышленник может использовать уязвимость в службе для повышения своих привилегий в системе.**

**Рис. 4 — Предупреждение о уязвимости в группе служб запроса паролей у пользователей**

**1. Служба Console запрашивает пароли при работе в консоли**

**2. Служба Plymouth запрашивает пароли при работе в графической среде**

**3. Служба Wall запрошивает пароли при авторизации в системе**

****Возможные причины уязвимости:****

**1. Пароль слишком простой**

* **При задании пароля система не всегда дает создать простой пароль, соответсвенно считает его ненадежным**

**2. Уязвимости в самом systemd или его зависимостях могут быть использованы для обхода службы**

**Рис. 4 — Предупреждение о уязвимости в службе **Firewall****

****Возможные причины уязвимости:****

**1. Неправильная конфигурация:**

* Ошибки в правилах брандмауэра могут привести к тому, что служба будет блокировать легитимный трафик или разрешать несанкционированный доступ.

**2. Уязвимости в программном обеспечении:**

* **Уязвимости в самом firewall или его зависимостях могут быть использованы для обхода правил брандмауэра.**

**Рис. 5 — Предкпреждение о уязвимости в службе sshd**

**Возможные уязвимости:**

**1. Неправильная конфигурация:**

* Ошибки в конфигурации SSH могут привести к тому, что служба будет:
* Разрешать доступ к серверу SSH несанкционированным пользователям.
* Использовать небезопасные протоколы аутентификации.
* Не шифровать трафик SSH.

**2. Уязвимости в программном обеспечении:**

* + Уязвимости в самом SSH-сервере или его зависимостях могут быть использованы для:
    - Обхода аутентификации.
    - Выполнения произвольных команд на сервере.
    - Перехвата трафика SSH.