Лабораторная работа №7

Управление журналами событий в системе

Ко А.Г.

18 февраля 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Ко Антон Геннадьевич
- Студент
- Российский университет дружбы народов
- 1132221551@pfur.ru
- https://github.com/SenDerMen04

Цель работы

Целью данной работы является получение навыков работы с журналами мониторинга различных событий в системе.

Мониторинг журнала системных событий в реальном времени

Для начала запустим три вкладки терминала и в каждом из них получим полномочия администратора:

```
su -
```

На второй вкладке терминала запустим мониторинг системных событий в реальном времени:

```
tail -f /var/log/messages
```

В третьей вкладке терминала:

1. Вернёмся к учётной записи своего пользователя:

```
Ctrl + d
```

2. Попробуем получить полномочия администратора, но при этом вводим неправильный пароль.

Ответы на контрольные вопросы:

1. Какой файл используется для настройки rsyslogd?
   `/etc/rsyslog.conf`
2. В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?
   `/var/log/secure`
3. Сколько времени потребуется для ротации файлов журналов по умолчанию?
   Неделя
4. Как записать все сообщения с приоритетом info в файл /var/log/messages.info?
   `info.* - /var/log/messages.info`
5. Какая команда позволяет видеть сообщения журнала в режиме реального времени?
   `tail -f /var/log/messages`
6. Какая команда позволяет видеть все сообщения журнала для PID 1 между 9:00 и 15:00?

Вывод

В ходе выполнения лабораторной работы были получены навыки работы с журналами мониторинга различных событий в системе.