Введение в аудит

Чтобы контролировать процессы, проводить аудит операционной системы и расследовать инциденты в ОС Linux, используют утилиту **audit**.

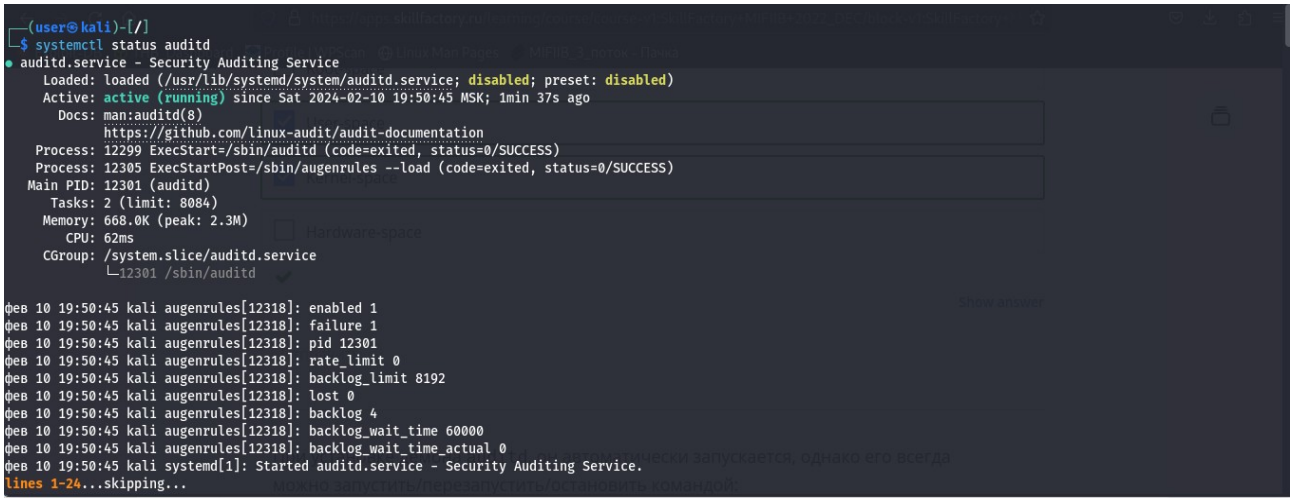
Для установки user-space сервиса воспользуемся командой:
sudo apt install auditd

При работе с аудитом у нас есть несколько основных компонентов, с которыми мы будем взаимодействовать:

- /etc/audit/auditd.conf — файл конфигурации демона, настраивает то, *как* будет происходить логирование;
- /etc/audit/audit.rules — файл конфигурации аудита, настраивает то, *что* будет логироваться;
- /var/log/audit/audit.log — файл логов, куда собирается вся информация.

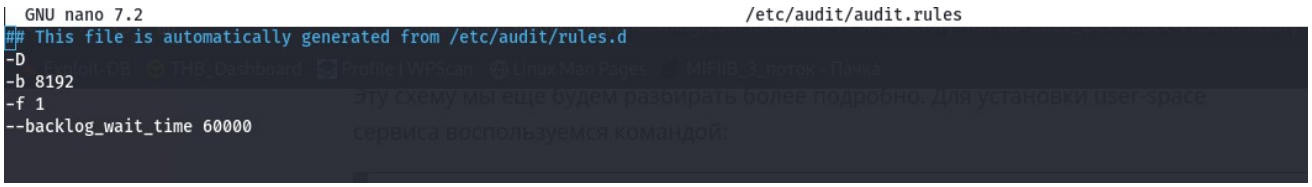
При установке демона auditd, он автоматически запускается, однако его всегда можно запустить/перезапустить/остановить командой:

sudo systemctl start/restart/stop auditd



Чтобы управлять аудитом, используют команду **auditctl**. Она и позволяет добавлять новые параметры и правила в audit.rules.

Откроем файл конфигурации аудита командой:
sudo nano /etc/audit/audit.rules



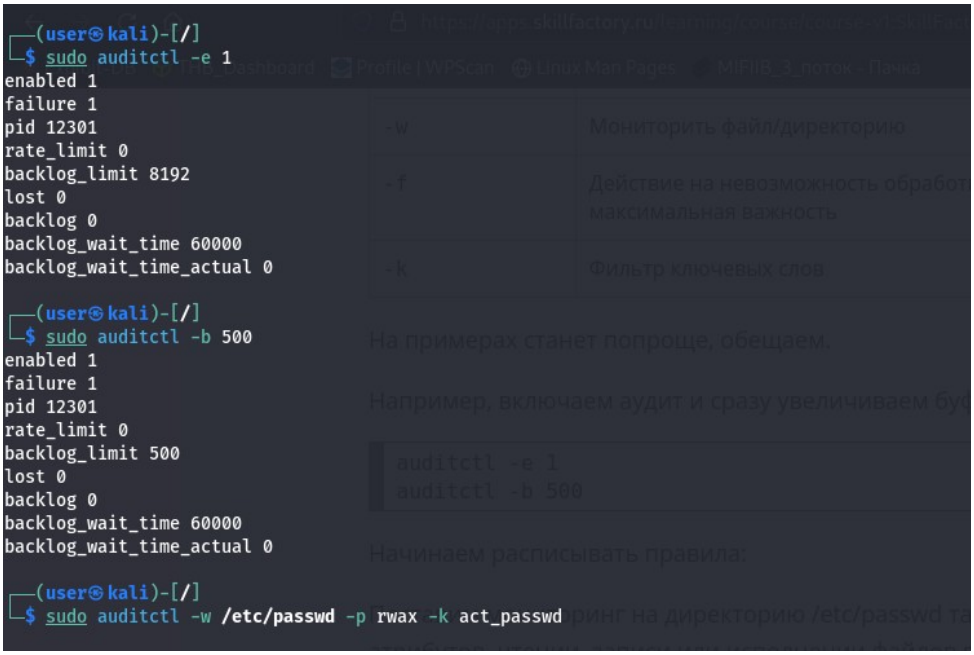
Включаем аудит и сразу увеличиваем буфер логов до 500:

auditctl -e 1

auditctl -b 500

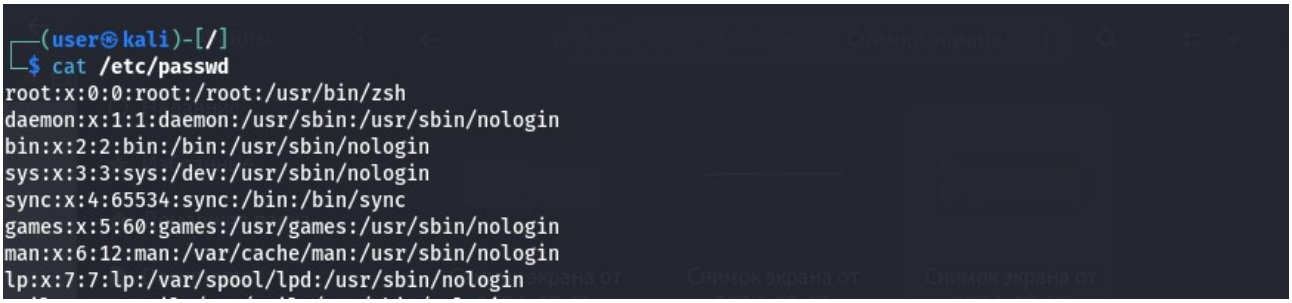
Поставим мониторинг на директорию /etc/passwd так, чтобы при любом изменении атрибутов, чтении, записи или исполнении файлов в этой директории, мы получали об этом информацию. Опцией -k мы задаем как бы лейбл для данного действия, чтобы потом в логах смогли быстро его найти:

auditctl -w /etc/passwd -p rwax -k act_passwd



В качестве примера посмотрим содержимое файла командой:

cat /etc/passwd



Команда **ausearch** — один из способов быстрого просмотра логов. Вводим:

ausearch -k act_passwd