ДЗ 17 — Логи

Цель: *Изучение команд анализа и просмотра логов*
Поработать со встроенными средствами просмотра логов.

1) Приведите пример не менее 12 встроенных программ просмотра логов.

less, more, cat, head, grep, tail, zcat, zgrep, zmore, vi, vim, nano, mcedit

2) Приведите пример не менее 5 из них с возможностью поиска по шаблону.

Для записи результата поиска и замены по шаблону, по завершении выполнения команды sed в обратно в файл,
можно использовать стандартный оператор перенаправления вывода ">" или утилиту "**tee**":

*$ sudo sed '/^#\|^$\| *#/d' /etc/apache2/apache2.conf | sudo tee /etc/apache2/apache2.conf*

Пример использования стандартного инструмента для анализа log-файлов tail:

$ sudo tail -n 100 /var/log/secure | grep "polkitd"

Анализ логов с использованием не стандартного инструмента **petit**

$ sudo cat /var/log/messages | grep error | petit --mgraph

$ sudo cat squid.conf.bak | grep -v "^#" | grep -v "^$" > squid.conf

Пример поиска журналов проверки подлинности для «user hoover» в системе Ubuntu:

$ grep «user hoover» /var/log/auth.log

Пример извлечения имени пользователя, которому не удалось войти в систему, с использованием команды **awk**:

*$ awk '/sshd.*invalid user/ { print $9 }' /var/log/auth.log*

Команда "**cut**" позволяет вам анализировать поля из разделенных журналов.
пример получения текста после восьмого знака равенства:

$ grep «authentication failure» /var/log/auth.log | cut —d '=' —f 8

xargs довольно часто используется в сочетании с командой **cut**, позволяющей вырезать строки из текстовых файлов. Рассмотрим некоторые практические примеры. С помощью приведённой
ниже команды на консоль будет выведен список всех пользователей системы:

$ cut -d: -f1 < /etc/passwd | sort | xargs echo

3) Написать пример команды, которая будет анализировать файл авторизаций пользователей и подсчитывать кол-во попыток входа в систему с неверным именем пользователя.

Для решения этой задачи будем использовать стороннее программное обеспечение -- petit. Устанавливается в ОС семейства Ubuntu командой:

$ sudo apt install petit

Отслеживание отдельных слов в файле журнала:

$ sudo cat /var/log/auth.log | grep «authentication failure» | petit --mgraph