server_log

Что такое логи?

Все что происходит в системе записывается в логи, в том числе действия пользователей, работа приложений, системы и т.д. Этот процесс называется журналирование. И это основной источник информации о событиях в системе, в том числе и об ошибках.

Вопрос	Ответ
Какой файл логов поможет при проверке безопасности при авторизации в систему, в каком файле смотреть логи неудачных попыток авторизации?	`/var/log/btmp` - неудачные попытки входа `/var/run/utmp` - кто в данный момент залогинен `/var/log/wtmp` - список всех сессий входа в систему Для просмотра данных файлов используется команда `last` (`last -10` # *чтобы отобразить только 10 последних строк*)
Что делает команда ls /var/log ?	Команда `ls` выводит содержимое директории, в который мы находимся. Таким образом, команда отображает все файлы логов Linux
Какой командой посмотреть логи журнала сообщений от ядра в реальном времени?	`sudo dmesg` (`tail -f /var/log/kern.log` или `cat /var/log/kern.log` * *данные варианты найдены в интернете, но они не работают для MacOS*)
Какая команда покажет, кто из пользователей сейчас залогинен в системе и когда он зашел?	`w` - получаем список залогиненных пользователей `who` - получаем список пользователей, залогиненных в системе `whoami` или `id -un` - узнать под каким именем залогинены мы сами `last` - показывает историю подключений для всех пользователей
Какая команда дает понять, когда пользователь заходил в систему и сколько времени в ней находился?	`last`
Какой самый простой способ посмотреть логи (открыть лог файл) syslog?	`less /var/log/system.log`