server_log

Что такое логи Логи (лог-файлы или журнал сервера) — это файлы, содержащие системную информацию работы сервера или компьютера, в которые заносятся определенные действия пользователя или программы. Иногда также употребляется русскоязычный аналог понятия — журнал.

Вопрос	Ответ
Какой файл логов поможет при проверке безопасности при авторизации в систему, в каком файле смотреть логи неудачных попыток авторизации?	**/var/log/auth.log или /var/log/secure** — информация об авторизации пользователей, включая удачные и неудачные попытки входа в систему, а также задействованные механизмы аутентификации.
Что делает команда ls /var/log?	Отображает все файлы логов для вашей системы Linux
Какой командой посмотреть логи журнала сообщений от ядра в реальном времени?	команда **tail -f /var/log/kern.log** логи ядра, где хранится информация из ядра Linux или **cat /var/log/kern.log**
Какая команда покажет, кто из пользователей сейчас залогинен в системе и когда он зашел?	команда **who** сообщает имя пользователя, имя терминальной линии, астрономическое время начала сеанса, продолжительность бездействия терминальной линии с момента последнего обмена, идентификатор процесса интерпретатора **команд shell** для каждого из пользователей, работающих в системе UNIX
Какая команда дает понять, когда пользователь заходил в систему и сколько времени в ней находился?	Для просмотра логов входа в систему используется команда **last**. По умолчанию команда **last** выводит информацию из файла **/var/log/wtmp**, в котором хранятся записи обо всех сессиях входа и времени пребывания
Какой самый простой способ посмотреть логи (открыть лог файл) syslog?	Команда **cat -f /var/log/syslog** позволит наблюдать запись **логов** в реальном времени