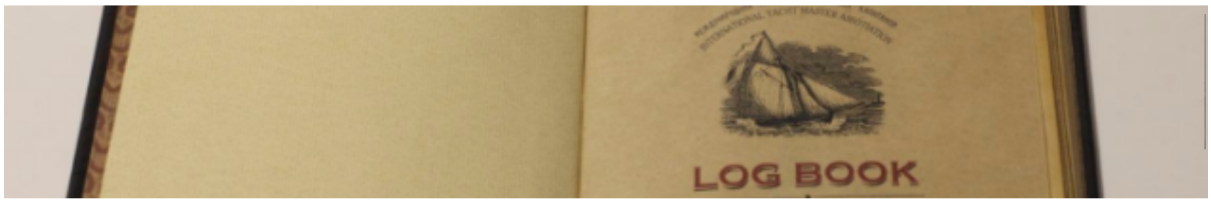

Server_log

Лог-файл - документ с последовательной записью всех событий, происходящих на веб-сайте или удаленном сервере. Термин происходит от английского Log - бревно с зарубками, которое в средневековье использовалось в качестве своеобразного журнала событий.

Зачем нужен лог-файл

В журнале фиксируется абсолютно все происходящее, изучение лога позволяет использовать накопленные данные в различных важных для продвижения и обслуживания сайтов целях.

- При возникновении технических проблем, недоступности сайта, вирусном заражении, хакерских атаках и DDoS, администратор ресурса может по зафиксированным в логе сведениям выяснить причину, что облегчит и ускорит устранение нежелательных явлений;
- С помощь сведений из лога интернет-маркетолог может изучать поведение посетителей на сайте, оценивать качество целевого трафика, формировать рекомендации по улучшению, выбирать оптимальные стратегии продвижения и раскрутки сайта.

Данные логов используются интернет-магазинами для отслеживания пути пользователя в направлении покупки, а также применяются в ретаргетинге - привлечении клиентов, сразу не совершивших покупку, но проявивших заинтересованность.

Вопрос	**Ответ**
Какой файл логов поможет при проверке безопасности при авторизации в систему?	**/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.

Вопрос	Ответ
В каком файле смотреть логи неудачных попыток авторизации?	**/var/log/faillog** — Неудачные попытки входа в систему. Очень полезно при проверке угроз в системе безопасности, хакерских атаках, попыток взлома методом перебора. Прочитать содержимое можно с помощью команды `faillog`.
Что делает команда ls/var/log?	**ls -** сокращение от list, при добавлении **/var/log** - отобразится директория, с большинством логов системы.
Какой командой посмотреть логи журнала сообщений от ядра в реальном времени?	**var/log/kern.log** - Журнал содержит сообщения от ядра и предупреждения, которые могут быть полезны при устранении ошибок пользовательских модулей встроенных в ядро.
Какая команда покажет, кто из пользователей сейчас залогинен в системе и когда он зашел?	**who** - выводит набор данных по умолчанию, об учетных записях подключенных пользователей - имя пользователя, название пользовательского терминала, время подключения.
Какая команда дает понять, когда пользователь заходил в систему и сколько времени в ней находился?	Каждый раз, когда пользователь входит в систему, запись для этого сеанса записывается в файл **/var/log/wtmp**. Команда **last** читает файл wtmp и печатает информацию о входах и выходах пользователей. Записи печатаются в обратном порядке времени, начиная с самых последних.
Какой самый простой способ посмотреть логи (открыть лог файл) syslog?	**cat/var/log/syslog** - команда просто открывает файл лога указанного в директории.