Домашняя работа Модуль 3 урок 2. Управление паролями и выполнение от root.

При попытках выполнения пункта 2. Скрипты экспресс-аудита безопасности для Linux домашней работы наталкиваюсь на ошибку вида:

root@VBSTD:~# cat /etc/shadow | awk -F: ($2==””){print $1}’
-su: синтаксическая ошибка рядом с неожиданным маркером «(»

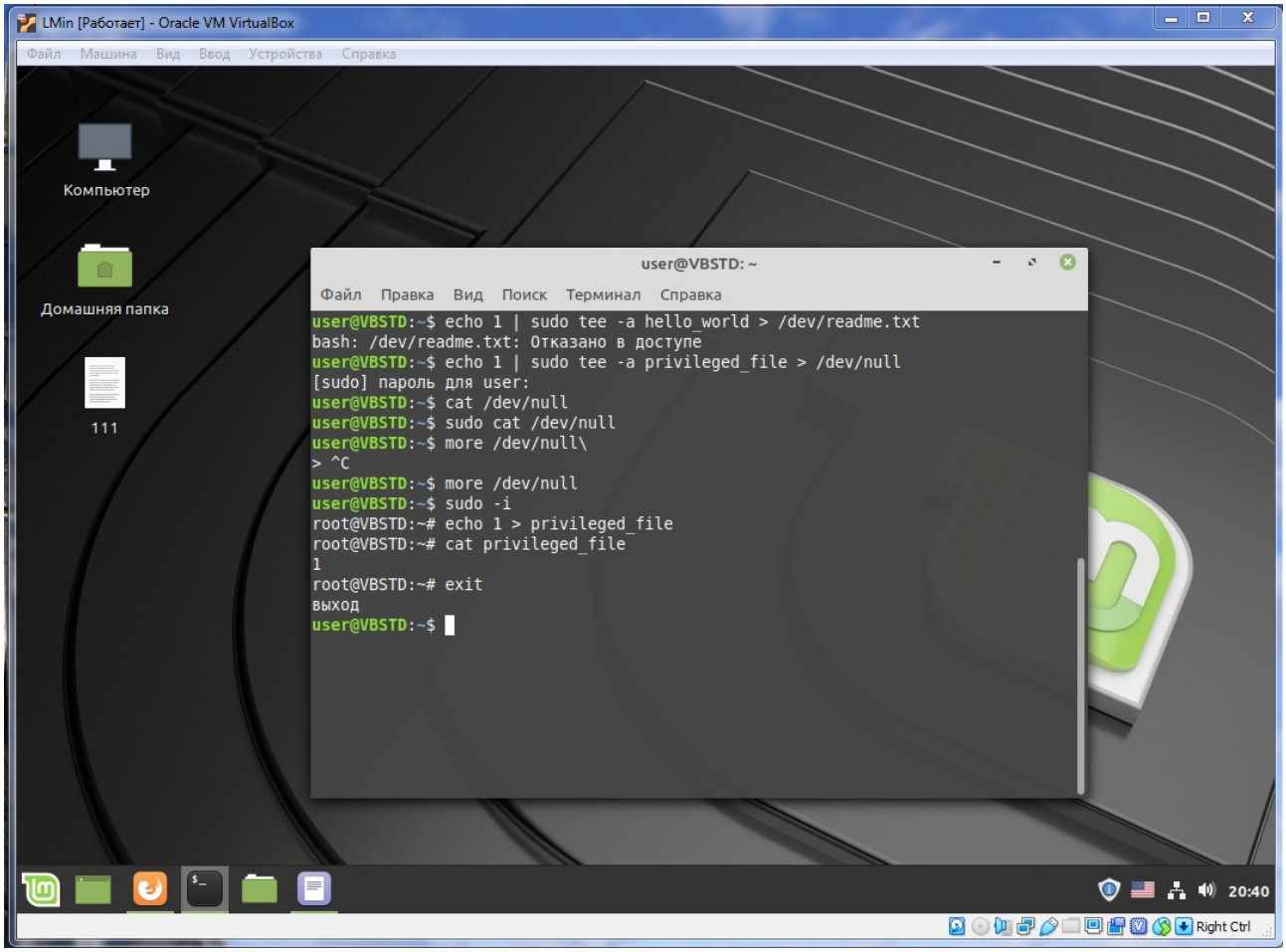
разобрался, поправил, не хватало одного апострофа:

root@VBSTD:~# cat /etc/shadow | awk -F:'($2==””){print $1}’
>

Проверки парольной политики работают:
root@VBSTD:~# chage -l user
Последний раз пароль был изменён : сен 10, 2019
Срок действия пароля истекает : никогда
Пароль будет деактивирован через : никогда
Срок действия учётной записи истекает : никогда
Минимальное количество дней между сменой пароля : 0
Максимальное количество дней между сменой пароля : 99999
Количество дней с предупреждением перед деактивацией пароля : 7

root@VBSTD:~# chage -M 60 -m 7 -W 3 user
root@VBSTD:~# chage -l user
Последний раз пароль был изменён : сен 10, 2019
Срок действия пароля истекает : ноя 09, 2019
Пароль будет деактивирован через : никогда
Срок действия учётной записи истекает : никогда
Минимальное количество дней между сменой пароля : 7
Максимальное количество дней между сменой пароля : 60
Количество дней с предупреждением перед деактивацией пароля : 3
root@VBSTD:~#

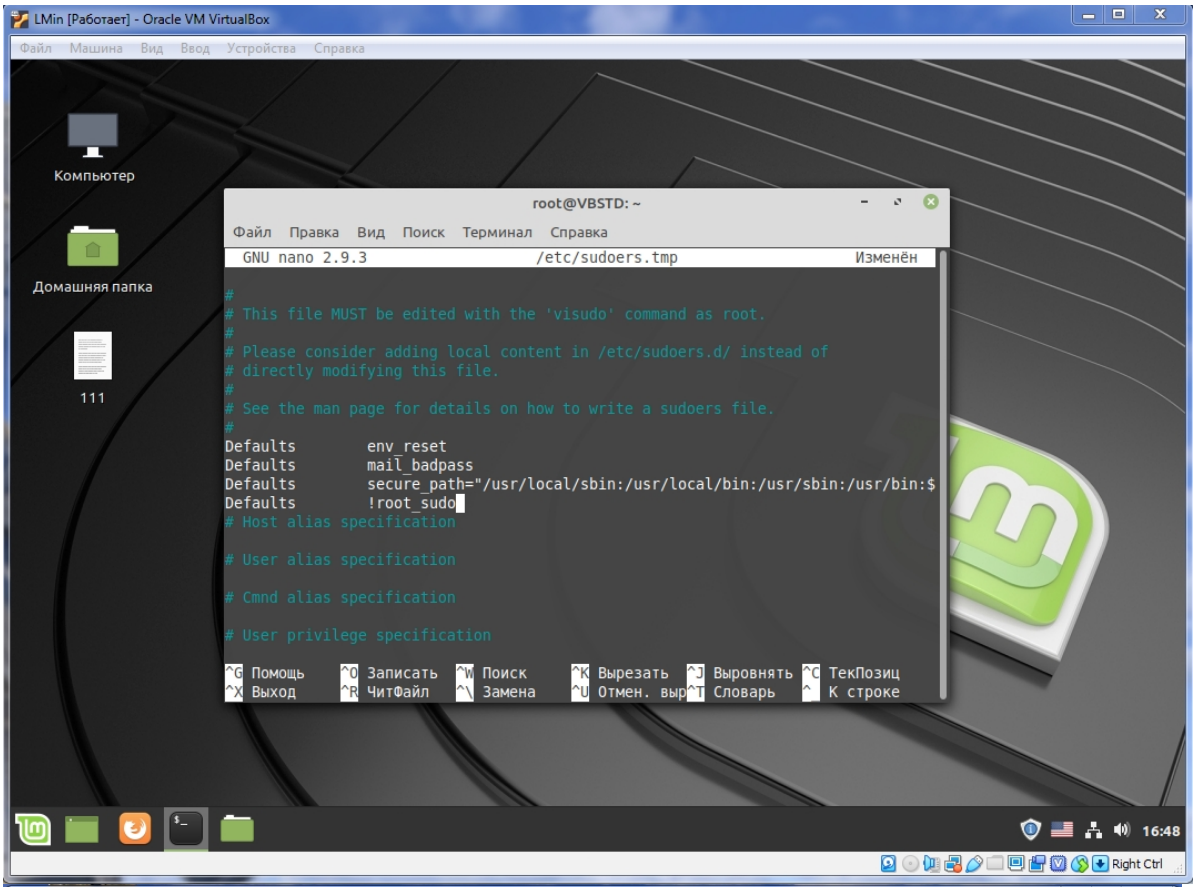
3. Права суперпользователя линукс

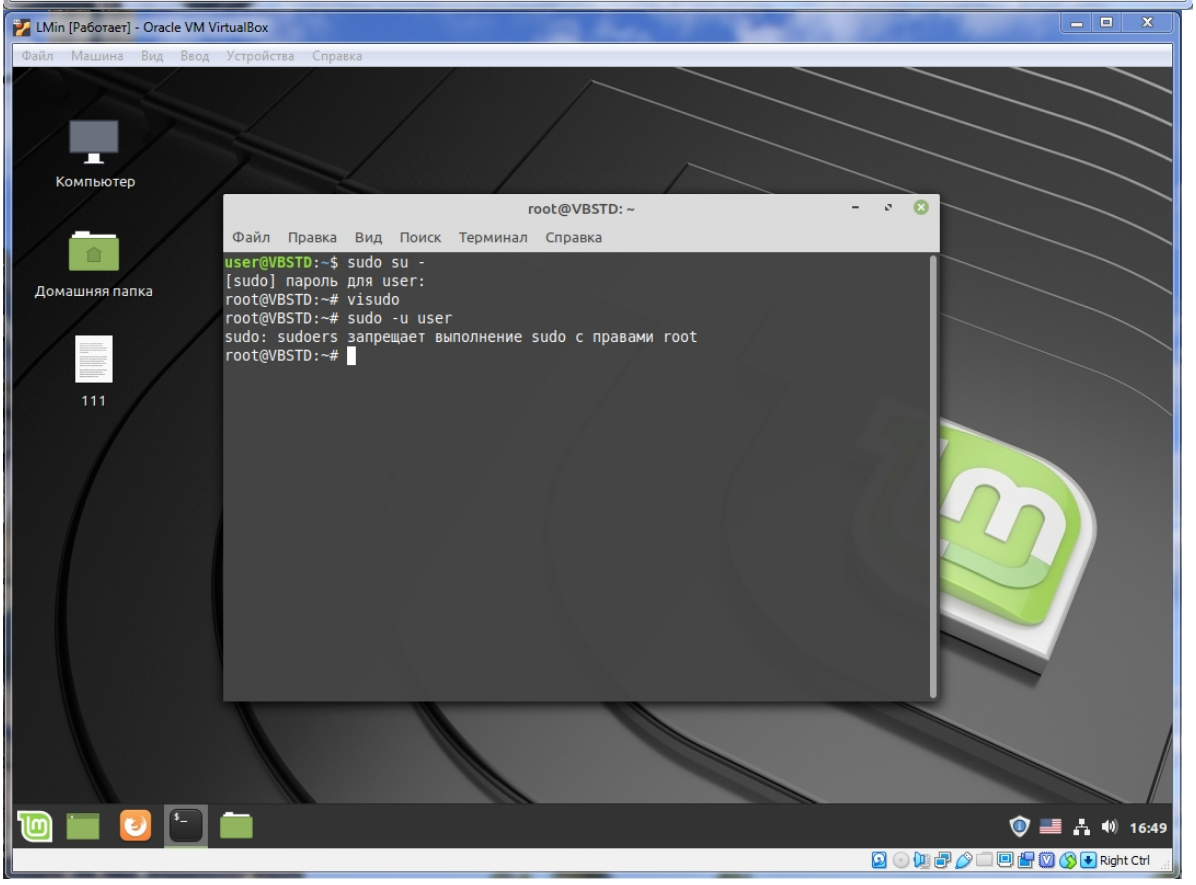


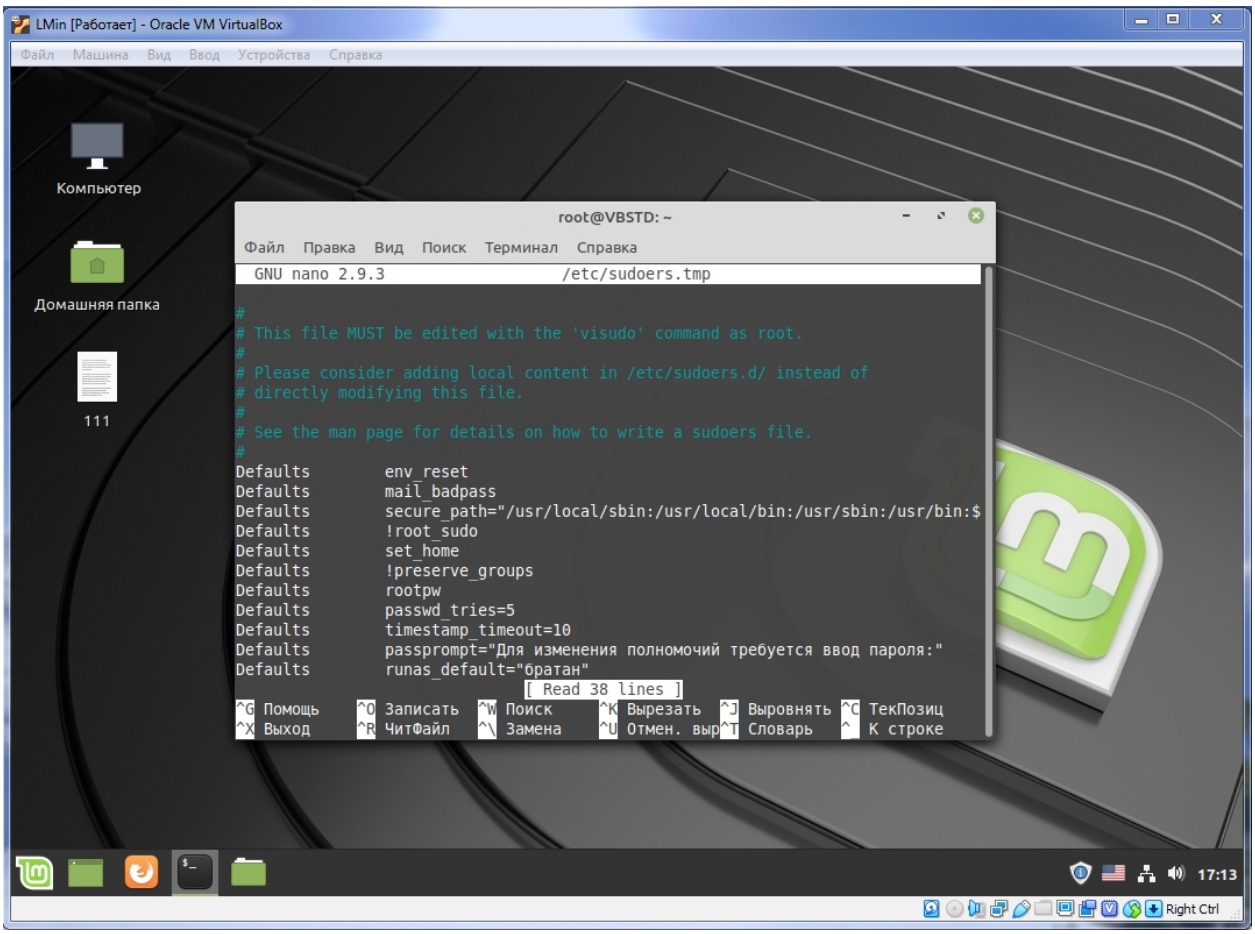
4. ***sudo*** выгоднее использовать, нежели чем ***su***, с точки зрения администрирования ОС:
У sudo есть несколько преимуществ, ради которых стоит потрудиться набрать несколько лишних символов: по умолчанию sudo записывает всю пользовательскую активность в syslog-канал authpriv (как правило, результат кладется в файл /var/log/auth.log), а в su подобную фичу надо включать с помошью задания специального параметра в файле настроек, различающемся от дистрибутива к дистрибутиву (SULOG_FILE в /etc/login.defs в Ubuntu Linux, /etc/login.conf и /etc/pam.d/su в FreeBSD и т.д.) в случае с su администратор системы не может ограничить команды, выполняемые пользователями, а в sudo — может если пользователь должен быть лишен права администрирования, в случае с su после удаления его из группы wheel он должен забыть пароль root'a; если используется sudo, достаточно вынести его из соответствующей группы (например, wheel или admin) и/или файла sudoers, если он был дополнительно настроен. Источник: https://habr.com/ru/post/44783/

5. Настройка sudo в Linux (источник: https://losst.ru/nastrojka-sudo-v-linux)

Основные параметры







Теперь попробуем проверить работу лога: