

Лабораторная работа №11

Отчет

Славинский Владислав Вадимович

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	12
4	Ответы на контрольные вопросы	13

Список иллюстраций

2.1	Установка таймера загрузки	6
2.2	Запись изменений в GRUB2	6
2.3	Проверка изменений	7
2.4	Редактирование	7
2.5	Список всех файлов модулей	8
2.6	Задействованные переменные среды оболочки	8
2.7	Редактирование	8
2.8	Просмотр списка всех загруженных файлов модулей и перезагрузка	9
2.9	Редактирование	9
2.10	Получение доступа к системному образу для чтения и записи	10
2.11	Новый корневой каталог	10
2.12	Создание нового пароля root	10
2.13	Исправление контекста	11
2.14	Установка правильного типа контекста	11
2.15	Перезагрузка и проверка изменений	11

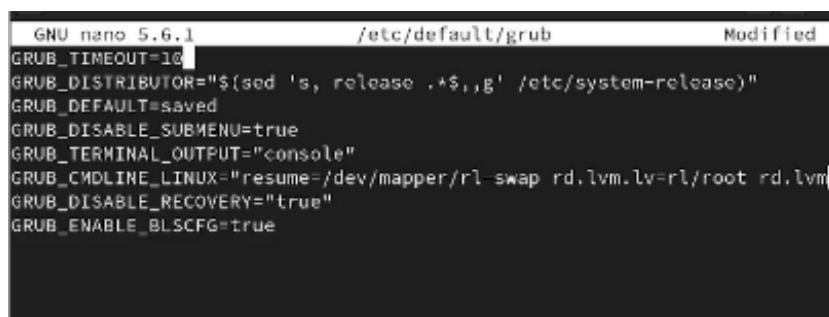
Список таблиц

1 Цель работы

Получить навыки работы с загрузчиком системы GRUB2.

2 Выполнение лабораторной работы

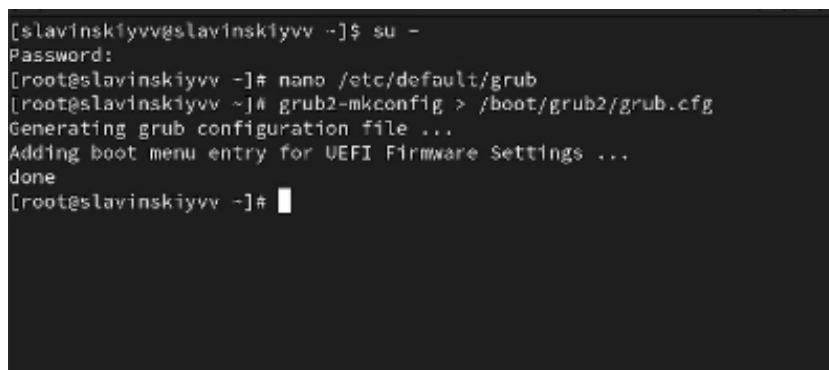
В терминале получим права администратора, после в файле /etc/default/grub установим параметр отображения меню загрузки в течение 10 секунд: GRUB_TIMEOUT=10. (рис. 2.1)



```
GNU nano 5.6.1 /etc/default/grub Modified
GRUB_TIMEOUT=10
GRUB_DISTRIBUTOR="$(sed 's, release .*$,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="resume=/dev/mapper/rl-swap rd.lvm.lv=rl/root rd.lvm"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
```

Рис. 2.1: Установка таймера загрузки

Запишем изменения в GRUB2, введя в командной строке: grub2-mkconfig > /boot/grub2/grub.cfg.(рис. 2.2)



```
[slavinskiyvv@slavinskiyvv ~]$ su -
Password:
[root@slavinskiyvv ~]# nano /etc/default/grub
[root@slavinskiyvv ~]# grub2-mkconfig > /boot/grub2/grub.cfg
Generating grub configuration file ...
Adding boot menu entry for UEFI Firmware Settings ...
done
[root@slavinskiyvv ~]#
```

Рис. 2.2: Запись изменений в GRUB2

Перезагрузим систему и посмотрим изменения. (рис. 2.3)

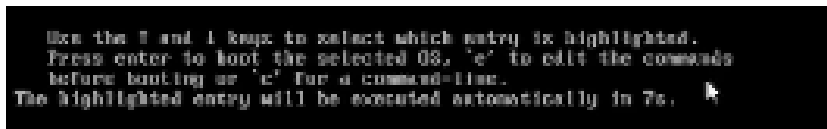


Рис. 2.3: Проверка изменений

Перезагрузим систему. Как только появляется меню GRUB входим в режим редактирования. После чего находим строку, которая начинается с linux (\$root)/vmlinuz-, в ней мы удаляем rhgb и quit и в конце добавляем systemd.unit=rescue.target. (рис. 2.4)

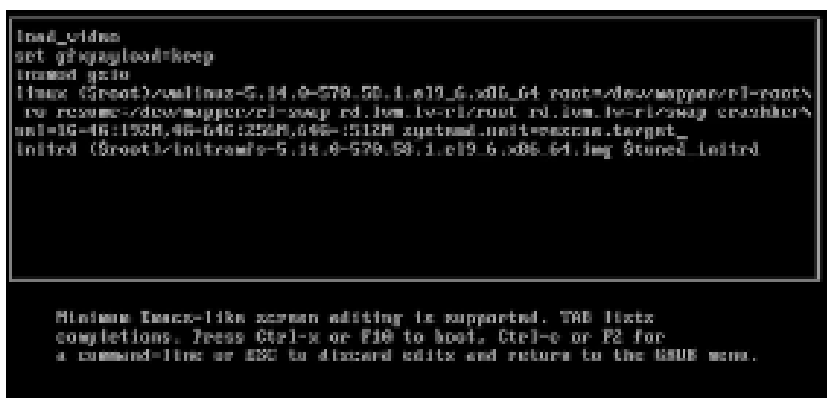


Рис. 2.4: Редактирование

Нажмем ctrl+x для продолжения загрузки. Введем root пароль и посмотрим список всех файлов модулей, которые загружены в настоящее время: systemctl list-units. У нас загружена базовая системная среда. (рис. 2.5)

[illegible]

Посмотрим задействованные переменные среды оболочки: `systemctl show-environment`. (рис. 2.6)

Перезагрузим систему через `systemctl reboot`. Дальше опять зайдём в режим редактирования, удалим `rhgb` и `quit`, и введём в конце другую строку `systemd.unit=emergency.target`. (рис. 2.7)

Этап загрузки системы у нас остановится в момент загрузки `initramfs` непосредственно перед монтированием корневой файловой системы в каталоге `/`. Чтобы получить доступ к системному образу для чтения и записи, наберем `mount -o remount,rw /sysroot`. (рис. 2.10)

```
switch_root:/# mount -o remount,rw /sysroot
switch_root:/# _
```

Рис. 2.10: Получение доступа к системному образу для чтения и записи

Сделаем содержимое каталога `/sysimage` новым корневым каталогом, набрав `chroot /sysroot`. (рис. 2.11)

```
switch_root:/# mount -o remount,rw /sysroot
switch_root:/# chroot /sysroot
sh-5.1# _
```

Рис. 2.11: Новый корневой каталог

Введем команду `passwd` и дальше зададим новый пароль `root`. (рис. 2.12)

```
Changing password for user root:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
sh-5.1#
```

Рис. 2.12: Создание нового пароля root

Поскольку на этом очень раннем этапе загрузки SELinux ещё не активирован, то тип контекста SELinux для файла `/etc/shadow` будет испорчен. Если мы перезагрузимся в этот момент, то никто не сможет зайти в систему. Нам нужно убедиться, что тип контекста задан правильно, поэтому нам нужно загрузить политику SELinux: `load_policy -i`. (рис. 2.13)

```

kernel: all initialization taken updated successfully.
sh-5.14 # find_policy -l
[ 223.344595] audit: type=1404 audit(1576314228.165:1): enforcing=0 old_enforcing=0 auid=4294967295 ses=4294967295 enabled=1 old-enabled=1 lowreslinux rev=1
[ 223.472287] SELinux: policy capability enforce_selinux=1
[ 223.472563] SELinux: policy capability open_perms=1
[ 223.472791] SELinux: policy capability extended_object_class=1
[ 223.472860] SELinux: policy capability always_check_status=0
[ 223.473173] SELinux: policy capability group_context=1
[ 223.473280] SELinux: policy capability app_context_transitions=1
[ 223.473793] SELinux: policy capability sysfs_context_label=1
[ 223.884999] audit: type=1403 audit(1576314238.215:2): auid=4294967295 ses=4294967295 lowreslinux rev=1
sh-5.14 #

```

Рис. 2.13: Исправление контекста

Теперь устанавливаем правильный тип контекста для /etc/shadow: `chcon -t shadow_t /etc/shadow`. (рис. 2.14)

```

[ 223.472599] SELinux: policy capability sysfs_context_label=1
[ 223.884999] audit: type=1403 audit(1576314238.215:2): auid=4294967295
sh-5.14 # chcon -t shadow_t /etc/shadow
sh-5.14 #

```

Рис. 2.14: Установка правильного типа контекста

Перезагружаем систему с помощью команды `reboot -f`. Когда загрузились, войдем в консоль и получим root права, введя новый пароль. Пароль успешно изменился. (рис. 2.15)

```

root@salavimakiyov:~
[salavimakiyov@salavimakiyov ~]$ su -
Password:
[salavimakiyov ~]$

```

Рис. 2.15: Перезагрузка и проверка изменений

3 Выводы

В ходе выполнения лабораторной работы были получены навыки работы с загрузчиком системы GRUB2.

4 Ответы на контрольные вопросы

1. `/etc/default/grub`
2. `/etc/default/grub`
3. `grub-mkconfig > /boot/grub/grub.cfg`