РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 11

Управление загрузкой системы (GRUB2)

Студент: Эйвази Мани

Группа: НПИбд-03-24

Студенческий билет №: 1032245107

Цель работы

Получить практические навыки работы с загрузчиком системы GRUB2. Освоить методы модификации параметров загрузки, устранения неполадок на этапе загрузки (включение в режимах rescue и emergency), а также выполнения критических административных задач, таких как сброс пароля суперпользователя (root) без знания старого пароля.

Первый шаг: Изменение времени отображения меню загрузки. Находим строку GRUB_TIMEOUT и устанавливаем значение, например, GRUB_TIMEOUT=10. Это задает время в секундах, в течение которого меню загрузки будет ждать выбора пользователя перед автоматическим запуском системы по умолчанию. Изменение сохранено в конфигурационном файле /etc/default/grub.

- Команда: grub2-mkconfig-o /boot/grub2/grub.cfg

Второй шаг: Применение изменений, внесенных в /etc/default/grub, путем генерации основного файла конфигурации загрузчика. Создан обновленный файл /boot/grub2/grub.cfg, в который включены изменения (время ожидания 10 секунд). При следующей перезагрузке меню загрузки будет отображаться в течение заданного времени.

- Команда: grub2-mkconfig-o /boot/grub2/grub.cfg

Третий шаг: Принудительная загрузка системы в режиме для восстановления.

- Перезагрузка системы.
- В меню GRUB нажатие клавиши e для редактирования параметров загрузки выбранного ядра.
- В строке, начинающейся с linux или linux16, в конце (после ro quiet или аналогичных параметров) добавляется параметр systemd.unit=rescue.target.
- Удаление параметров rhgb и quiet, если они присутствуют (для отображения подробных сообщений).
- Нажатие Ctrl+X или F10 для загрузки с измененными параметрами.

Система загружается в однопользовательский режим с ограниченным набором служб, но с доступной сетью. Требуется ввод пароля пользователя root. Это позволяет выполнять восстановительные работы, например,

Четвертый шаг: Загрузка в минимальном режиме для устранения критических сбоев.

Аналогичен предыдущему, но в строке параметров ядра указывается systemd.unit=emergency.target.

Система загружает абсолютный минимум служб, необходимых для работы ядра. Доступ к сети отсутствует. Требуется пароль root. Этот режим используется в самых тяжелых случаях, когда даже rescue.target не загружается.

Пятый шаг: Проверка возможности выгрузки модулей ext4 и xfs.

- Модуль ext4 может быть успешно выгружен (rmmod ext4 также работает), если в данный момент не используется (нет смонтированных разделов ext4).
- Модуль xfs выгрузить не удается. Система выдает ошибку: modprobe: FATAL: Module xfs is in use.. Это означает, что в данный момент есть смонтированная файловая система XFS (скорее всего, корневой раздел /), поэтому ядро не позволяет выгрузить необходимый для её работы драйвер.

Шестой шаг: Прерывание процесса загрузки до момента монтирования корневой файловой системы в режим чтения-записи.

- Перезагрузка, вход в редактор параметров GRUB (e).
- В строке параметров ядра в конце добавляется rd.break.
- Загрузка с этими параметрами (Ctrl+X).

Загрузка останавливается, и пользователь попадает в оболочку (sh) внутри временной корневой файловой системы (initramfs). Корневой раздел (/) системы смонтирован в /sysroot в режиме только для чтения.

Седьмой шаг: Получение доступа к файлу с паролями для его изменения.

Команды в оболочке initramfs:

 # Перемонтируем /sysroot в режим чтения-записи

mount-o remount,rw /sysroot

 # "Переключаемся" в настоящую корневую файловую систему

chroot /sysroot

 # Меняем пароль пользователя root

passwd root

 # Вводим новый пароль дважды.

Пароль для пользователя root успешно изменен.

Восьмой шаг: При активном SELinux изменение
файла /etc/shadow может привести к неправильному контексту безопасности, что заблокирует вход. Необходимо это исправить.

Команда (внутри chroot): touch /.autorelabel

Создан скрытый файл-триггер. При следующей перезагрузке система автоматически выполнит полное восстановление меток SELinux для всей файловой системы, что гарантирует корректную работу политик безопасности.

девяти шаг: Выход из окружений и перезагрузка в нормальном режиме.

Команды:

bash

exit *(Выход из chroot)*

exit *(Выход из оболочки initramfs (или нажать Ctrl+D))*

Система продолжает обычную загрузку. После входа можно использовать новый пароль root. Если был создан файл /.autorelabel, процесс загрузки займет больше времени из-за перемаркировки файлов SELinux.

заключение

В ходе лабораторной работы были успешно освоены ключевые навыки управления процессом загрузки Linux-системы с использованием загрузчика GRUB2:

1. Настройка GRUB2: Освоен базовый процесс конфигурации через редактирование файла /etc/default/grub и последующую генерацию основного конфигурационного файла командой grub2-mkconfig. Это позволяет гибко настраивать параметры, такие как таймаут меню, аргументы ядра по умолчанию и внешний вид.
2. Диагностика и восстановление: Получены практические навыки загрузки в специальных режимах для восстановления работы системы:
    - rescue.target: Режим спасения с работающей сетью для устранения менее критичных проблем (ошибки в конфигурации, проблемы с драйверами).
    - emergency.target: Аварийный режим с минимальным окружением для решения самых серьезных сбоев (повреждение критичных системных файлов).
    - rd.break: Мощнейший инструмент, позволяющий получить контроль над системой до полной загрузки, обходя стандартные механизмы аутентификации. Критически важен для восстановления доступа при утере пароля root.
3. Безопасность и SELinux: Процедура сброса пароля с помощью rd.break наглядно продемонстрировала уязвимость физического доступа к серверу. Одновременно было показано, как правильно работать в таких условиях с учетом мандатного контроля доступа (SELinux), используя touch /.autorelabel для предотвращения последующих проблем с безопасностью.

Работа подчеркнула важность понимания этапов загрузки Linux и владения инструментами GRUB2 для любого системного администратора. Эти навыки являются незаменимыми как для тонкой настройки, так и для экстренного восстановления работоспособности серверов.

1. Какой файл является основным конфигурационным для GRUB2?
   Финальный файл конфигурации, который читает загрузчик: /boot/grub2/grub.cfg. Основной файл для редактирования параметров: /etc/default/grub.

2. Какая команда применяет изменения, внесенные в /etc/default/grub?
   grub2-mkconfig-o /boot/grub2/grub.cfg.

3. Какой параметр загрузки ядра используется для входа в однопользовательский режим (режим восстановления) с минимальным набором служб?
   systemd.unit=rescue.target

4. Какой параметр передать ядру, чтобы прервать загрузку на этапе initramfs и получить оболочку для сброса пароля root?
   rd.break

5. Почему после сброса пароля через rd.break может потребоваться создать файл /.autorelabel?
   Потому что при изменении файла /etc/shadow в обход обычных механизмов системы его контекст безопасности SELinux может стать некорректным (unlabeled_t), что приведет к блокировке входа после включения SELinux. Файл /.autorelabel инициирует полное восстановление всех меток SELinux при следующей загрузке.