Отчёт по лабораторной работе №1

Дисциплина: Основы информационной безопасности

Кузьмина Мария Константиновна

Table of contents

List of Figures

Цель работы

Знакомство с командами для получения информации об аппаратном обеспечении и ядре операционной системы Linux

Задание

1. Установить и настроить виртуальную машину с ОС Rocky Linux
2. Ознакомиться с выводом команды ‘dmesg’
3. Выполнить фильтрацию вывода ‘dmesg’ с помощью ‘grep’ для поиска информации о конкретных устройствах
4. Ответить на контрольные вопросы

Выполнение лабораторной работы

Подготовка виртуального окружения

Для выполнения работы была установлена виртуальная машина с операционной системой Rocky. На скриншоте ниже представлен процесс настройки параметров виртуальной машины (имя, тип ОС, объем памяти и размер диска) (рис.1)

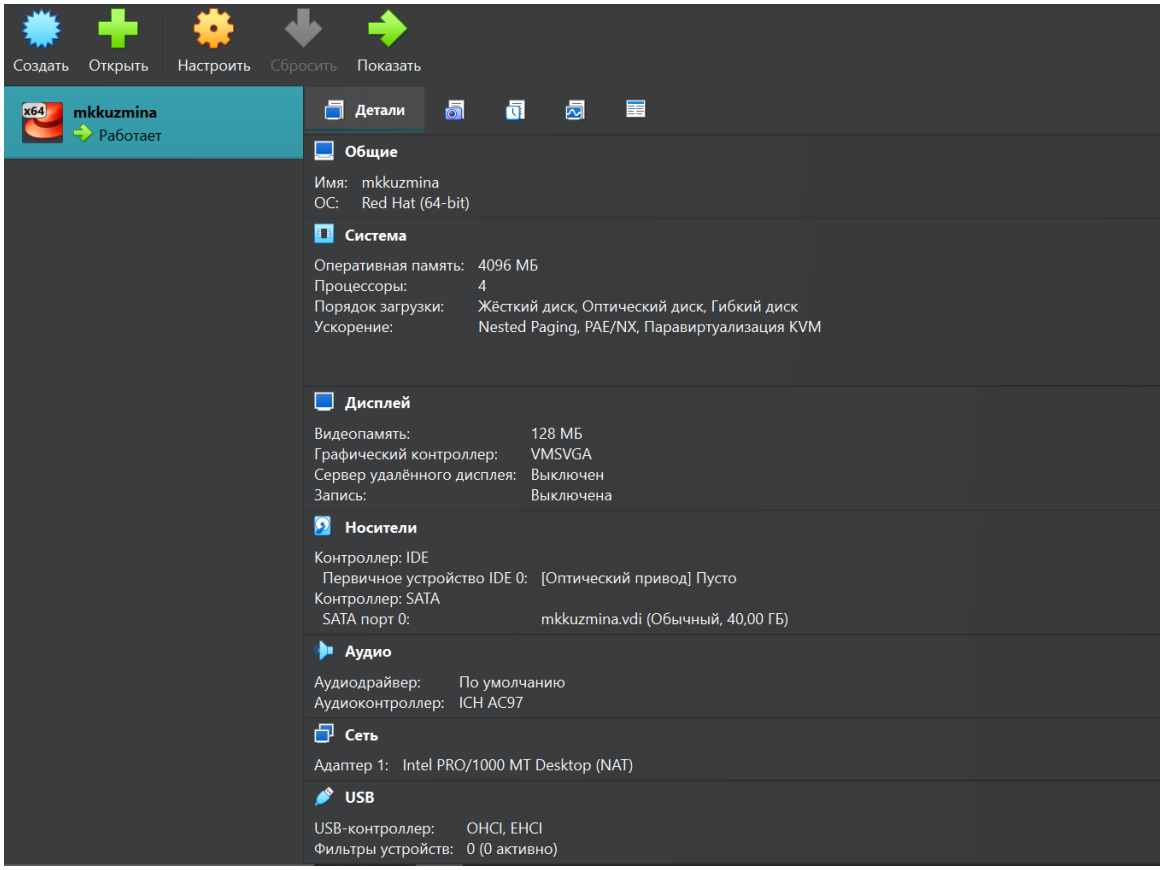

Figure 1: снимок экрана

Использование команды dmesg

Команда используется для просмотра кольцевого буфера сообщений ядра. Она позволяет увидеть информацию об обнаруженных устройствах, драйверах и ошибках при загрузке системы

Был выполнен базовый вызов команды ‘dmesg’, который выводит все сообщения ядра с момента загрузки (рис.2)

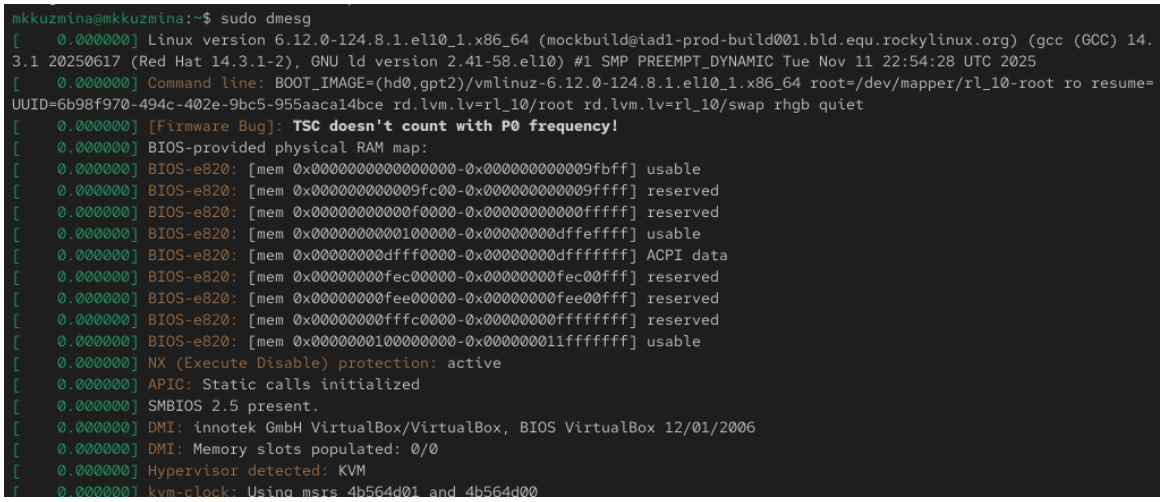

Figure 2: снимок экрана

Фильтрация вывода dmesg

Для поиска конкретной информации, вывод команды ‘dmesg’ был отфильтрован с помощью утилиты ‘grep’. Это позволяет, например, найти сообщения, связанные с конкретным оборудованием.

На скриншоте показан результат выполнения команды ‘dmesg | grep -i “CPU0” ’, отображающий только строки, содержащие информацию о процессоре (рис.3)

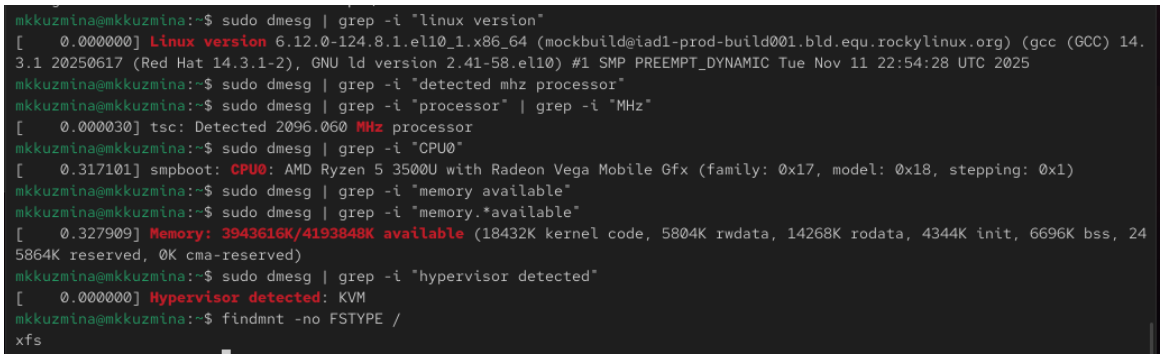

Figure 3: снимок экрана

Контрольные вопросы

1. **Какую информацию содержит учётная запись пользователя?** Учётная запись пользователя в Linux содержит следующую информацию:

   - **Имя пользователя (username):** уникальное имя для входа в систему.
   - **Пароль (password):** хранится в зашифрованном виде (обычно в файле `/etc/shadow`).
   - **UID (User ID):** уникальный числовой идентификатор пользователя.
   - **GID (Group ID):** идентификатор основной группы пользователя.
   - **Домашний каталог (home directory):** путь к личной папке пользователя (например, `/home/username`).
   - **Командная оболочка (shell):** программа-интерпретатор, запускаемая после входа (например, `/bin/bash`).

2. **Укажите команды терминала и приведите примеры:**

   - **Для получения справки по команде:**
     - `man <команда>` — выводит подробное руководство.
       - *Пример:* `man ls`
     - `<команда> --help` — выводит краткую справку по использованию.
       - *Пример:* `ls --help`
   - **Для перемещения по файловой системе:**
     - `cd <путь>` — переход в указанный каталог.
       - *Пример:* `cd /home/user/documents`

  - `cd ..` — переход на уровень выше.
  - `cd ~` или просто `cd` — переход в домашний каталог.

- **Для просмотра содержимого каталога:**
  - `ls` — выводит список файлов и папок в текущем каталоге.
  - `ls -l` — выводит подробный список (права, владелец, размер, дата).
    - *Пример:* `ls -l /etc`
  - `ls -a` — показывает также скрытые файлы (начинающиеся с точки).

- **Для определения объёма каталога:**
  - `du -sh <каталог>` — показывает общий размер каталога в удобочитаемом виде.
    - *Пример:* `du -sh /home/user`

- **Для создания / удаления каталогов / файлов:**
  - Создание каталога: `mkdir <имя_каталога>`
    - *Пример:* `mkdir new_folder`
  - Создание файла: `touch <имя_файла>` или `> <имя_файла>`
    - *Пример:* `touch readme.txt`
  - Удаление файла: `rm <имя_файла>`
    - *Пример:* `rm readme.txt`
  - Удаление пустого каталога: `rmdir <имя_каталога>`
  - Удаление каталога с содержимым: `rm -r <имя_каталога>`
    - *Пример:* `rm -r new_folder`

- **Для задания определённых прав на файл / каталог:**
  - Команда: `chmod <права> <файл/каталог>`
  - Права можно задавать символьно или цифрами.
    - *Пример (символьный):* `chmod u+x script.sh` — добавить право на выполнение владельцу.

    - *Пример (цифровой):* `chmod 755 script.sh` — владелец может читать/писать/выполнять, остальные — только читать/выполнять.

- **Для просмотра истории команд:**
  - `history` — показывает список ранее введённых команд.
  - `!!` — повторяет последнюю выполненную команду.
  - `!<номер>` — выполняет команду с указанным номером из истории.

3. **Что такое файловая система? Приведите примеры с краткой характеристикой.** Файловая система (ФС) — это способ организации, хранения и именования данных на носителях информации (жестких дисках, SSD, флеш-накопителях). Она определяет структуру каталогов, правила доступа к файлам и методы их размещения.

   Примеры:

   - **ext4 (Fourth Extended Filesystem):** стандартная файловая система для Linux. Поддерживает журналирование (защита от сбоев), большие файлы и разделы, высокую производительность.
   - **NTFS (New Technology File System):** основная ФС для Windows. Поддерживает журналирование, шифрование, разграничение прав доступа. Linux умеет читать и писать на NTFS.
   - **FAT32 (File Allocation Table):** старая ФС, совместимая со всеми ОС. Не поддерживает файлы больше 4 ГБ. Часто используется на флешках для совместимости.
   - **XFS:** высокопроизводительная журналируемая ФС, хорошо работает с большими файлами. Часто используется на серверах.

4. **Как посмотреть, какие файловые системы подмонтированы в ОС?** Для просмотра смонтированных файловых систем используются команды:

   - `mount` — выводит список всех смонтированных ФС.

- `df -h` — показывает список смонтированных ФС, их размер, занятое и свободное место в удобочитаемом формате.
- `findmnt` — выводит список смонтированных ФС в древовидном формате.

5. **Как удалить зависший процесс?** Для удаления (завершения) зависшего процесса используется команда `kill`. Сначала нужно найти идентификатор процесса (PID):

   1. Найти PID процесса: `ps aux | grep <имя_процесса>` или `top`.
   2. Завершить процесс:
      - `kill <PID>` — отправляет сигнал `SIGTERM` (мягкое завершение, процесс может попытаться закрыться корректно).
      - `kill -9 <PID>` — отправляет сигнал `SIGKILL` (немедленное принудительное завершение, если обычный `kill` не помогает).

   Пример: `kill -9 1234` (где 1234 — PID зависшего процесса).

Выводы

В ходе выполнения лабораторной работы были изучены основные команды для диагностики системы Linux. На практике освоено использование команды ‘dmesg’ и фильтрация ее вывода с помощью ‘grep’.