МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

# ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №16
# «Системы виртуализации в среде ОС Linux. Наблюдение и аудит в ОС Linux»

Практическая работа
по дисциплине «Системное программное обеспечение»
студента 3 курса группы ИВТ-б-о-222(2)
Чудопалова Богдана Андреевича

09.03.01 «Информатика и вычислительная техника»

Симферополь, 2025

## Ход работы

**A)** 1) Изучите возможности команды qemu-img — выполнил с помощью команды qemu-img —help

```
QEMU-IMG(1)                          QEMU                          QEMU-IMG(1)

NAME
       qemu-img - QEMU disk image utility

SYNOPSIS
       qemu-img [standard options] command [command options]

DESCRIPTION
       qemu-img  allows  you  to create, convert and modify images offline. It
       can handle all image formats supported by QEMU.

       Warning: Never use qemu-img to modify images in use by a  running  vir-
       tual machine or any other process; this may destroy the image. Also, be
       aware  that querying an image that is being modified by another process
       may encounter inconsistent state.
```

(a) Создайте образ виртуального жёсткого диска в папке /tmp/ размером 1.5GB в формате vmdk с именем disk_base_$USER.vmdk — сделал с помощью команды qemu-img create -f vmdk /tmp/disk_base_$USER.vmdk 1.5G

```
→  ~ qemu-img create -f vmdk /tmp/disk_base_$USER.vmdk 1.5G
Formatting '/tmp/disk_base_bogdan.vmdk', fmt=vmdk size=1610612736 compat6=off hwver
→  ~ ls /tmp
disk_base_bogdan.vmdk
lu38561vyt.tmp
OSL_PIPE_1000_SingleOfficeIPC_5b44374ded4aec4786df5c6b41f1f73a
snap-private-tmp
```

(c) Измените формат образа на qcow2, изменив также расширение файла - сначала конвертирую образ из формата VMDK в QCOW2

```
→  ~ qemu-img convert -O qcow2 /tmp/disk_base_$USER.vmdk /tmp/disk_base_$USER.qcow2
→  ~ ls /tmp
disk_base_bogdan.qcow2
disk_base_bogdan.vmdk
lu38561vyt.tmp
OSL_PIPE_1000_SingleOfficeIPC_5b44374ded4aec4786df5c6b41f1f73a
snap-private-tmp
```

Затем удаляю исходный VMDK файл.

```
→  ~ rm /tmp/disk_base_$USER.vmdk
→  ~ ls /tmp
disk_base_bogdan.qcow2
lu38561vyt.tmp
OSL_PIPE_1000_SingleOfficeIPC_5b44374ded4aec4786df5c6b41f1f73a
snap-private-tmp
systemd-private-85e5cbc1c0b3489589b699683e9631fe-colord.service-2vkva9
```

(d) Увеличьте размер образа диска до 7Gb — сделал с помощью команды qemu-img resize /tmp/disk_base_$USER.qcow2 7G

```
bogdan@bogdan-laptop
→  ~ qemu-img resize /tmp/disk_base_$USER.qcow2 7G
Image resized.
→  ~
```

e) С помощью qemu-img создайте целевой (дочерний) образ диска, базирующийся на образе диска, созданном на предыдущем этапе. Образ в формате qcow2 должен называться disk_$USER.qcow2 и располагаться в директории /tmp/ - сделал с помощью команды qemu-img create -f qcow2 -o backing_fmt=qcow2 -b /tmp/disk_base_$USER.qcow2 /tmp/disk_$USER.qcow2

```
→  ~ qemu-img create -f qcow2 -o backing_fmt=qcow2 -b /tmp/disk_base_$USER.qcow2 /tmp/disk_$USER.qco
w2

Formatting '/tmp/disk_bogdan.qcow2', fmt=qcow2 cluster_size=65536 extended_l2=off compression_type=z
lib size=7516192768 backing_file=/tmp/disk_base_bogdan.qcow2 backing_fmt=qcow2 lazy_refcounts=off re
fcount_bits=16
→  ~ ls /tmp/
disk_base_bogdan.qcow2
disk_bogdan.qcow2
```

Новый диск будет хранить только различия между новым образом и базовым.

2) Определите поддерживается ли гипервизор KVM на вашем оборудовании как описано в предыдущей главе (для тестов можно использовать файл CD-ROM /var/qemu/OS/ubuntu14.iso). Если KVM поддерживается, в дальнейшем используйте его при работе с ВМ — выполнил с помощью команды egrep -c '(vmx|svm)' /proc/cpuinfo

```
bogdan@bogdan-laptop:~
→  ~ egrep -c '(vmx|svm)' /proc/cpuinfo
12
→  ~
```

Т.к. вывод команды больше 0, значит мой процессор поддерживает аппаратную виртуализацию.

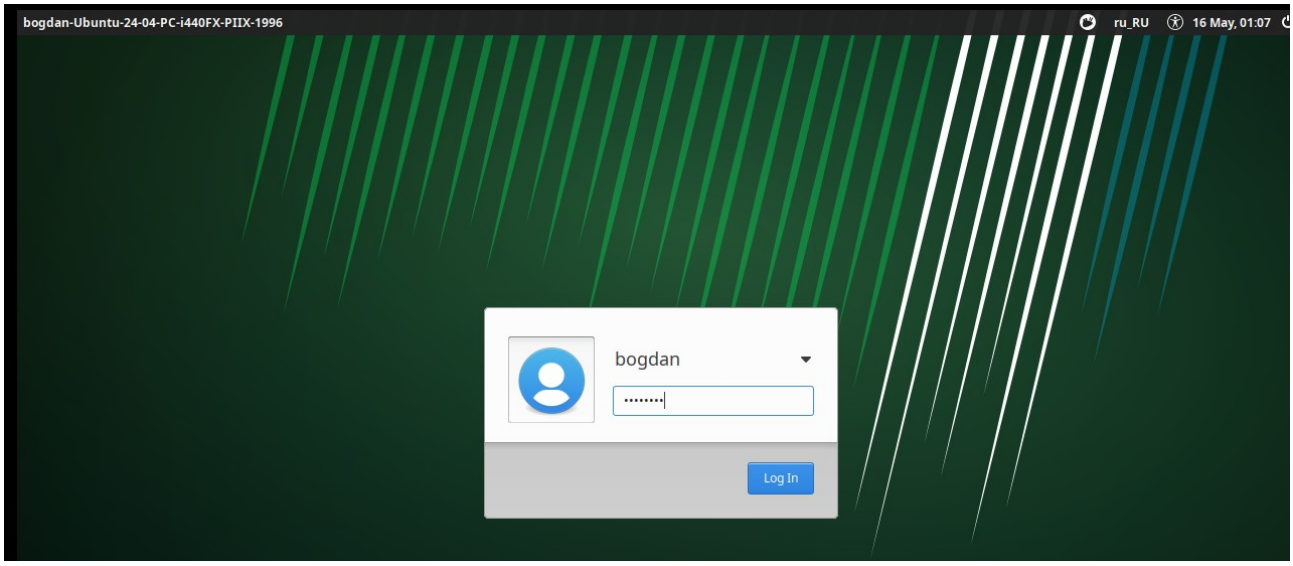
3) Запустите виртуальную машину qemu с необходимыми параметрами:
• Количество процессоров 1
• Оперативная память 512Mb
• Тип эмулируемой видеокарты std
• Образ жёсткого диска образ, созданный вами на предыдущем этапе лабораторной работы (целевой)
• Файл CD-ROM /var/qemu/OS/xubuntu14.iso

• Сеть пользовательская сеть
• Проброс портов: порт хост-компьютера = 8080) порт виртуальной машины = 80
• Включите отображение меню выбора устройства для загрузки
• Дополнительные опции:
-serial none -monitor telnet: 127.0.0.1:10023, server, nowait
Команда для решения

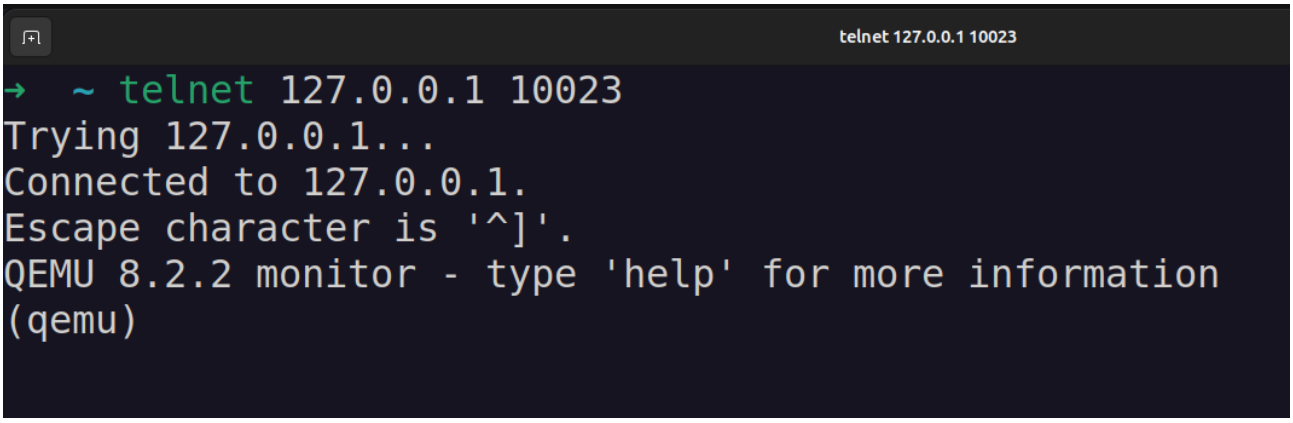
```
→  ~ qemu-system-x86_64 \
-enable-kvm \
-smp 1 \
-m 512 \
-vga std \
-hda /tmp/disk_$USER.qcow2 \
-cdrom /var/qemu/OS/xubuntu-24.04.2-desktop-amd64.iso \
-netdev user,id=usernet,hostfwd=tcp::8080-:80 \
-device e1000,netdev=usernet \
-boot menu=on \
-serial none \
-monitor telnet:127.0.0.1:10023,server,nowait
```

Начало установки


Установленная ОС

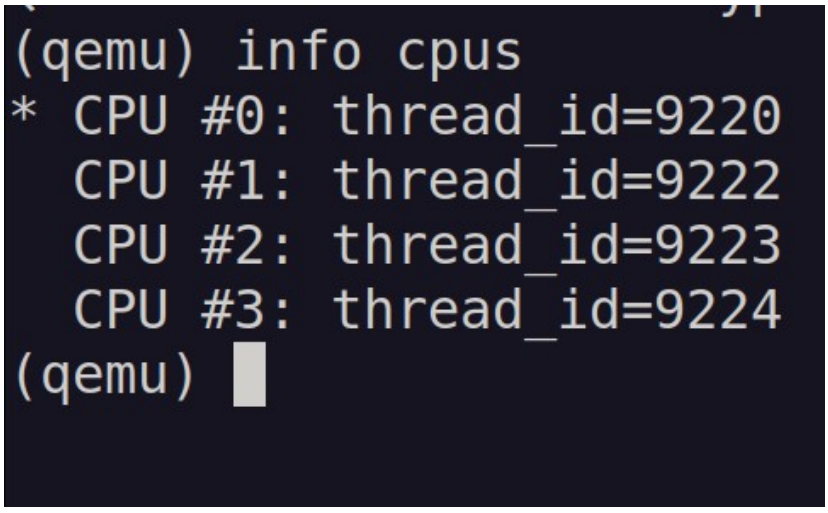



(b) Подключитесь к монитору ВМ по протоколу telnet с помощью команды - telnet 127.0.0.1 10023




(d) Получите информацию о:

• процессорах




• регистрах процессоров

```
(qemu) info registers

CPU#0
RAX=0000000000000000 RBX=0000000000000000 RCX=0000000000000000 RDX=0000000000000000
RSI=0000000000000000 RDI=0000000000000000 RBP=ffffffff86603df8 RSP=ffffffff86603df0
R8 =0000000000000000 R9 =0000000000000000 R10=0000000000000000 R11=0000000000000000
R12=ffffffff8660fec0 R13=0000000000000000 R14=0000000000000000 R15=000000000008a000
RIP=ffffffff852981ab RFL=00000246 [---Z-P-] CPL=0 II=0 A20=1 SMM=0 HLT=1
ES =0000 0000000000000000 00000000 00000000
CS =0010 0000000000000000 ffffffff 00a09b00 DPL=0 CS64 [-RA]
```

• сети

```
(qemu) info network
e1000.0: index=0,type=nic,model=e1000,macaddr=52:54:00:12:34:56
 \ usernet: index=0,type=user,net=10.0.2.0,restrict=off
(qemu)
```

• блочных устройствах

```
(qemu) info network
e1000.0: index=0,type=nic,model=e1000,macaddr=52:54:00:12:34:56
 \ usernet: index=0,type=user,net=10.0.2.0,restrict=off
(qemu) info block
ide0-hd0 (#block173): /tmp/disk_bogdan.qcow2 (qcow2)
    Attached to:      /machine/unattached/device[10]
    Cache mode:       writeback
    Backing file:     /tmp/disk_base_bogdan.qcow2 (chain depth: 1)

ide1-cd0 (#block564): /var/qemu/OS/xubuntu-24.04.2-desktop-amd64.iso (raw, read-only)
    Attached to:      /machine/unattached/device[11]
    Removable device: locked, tray closed
    Cache mode:       writeback

floppy0: [not inserted]
    Attached to:      /machine/unattached/device[20]
    Removable device: not locked, tray closed

sd0: [not inserted]
    Removable device: not locked, tray closed
(qemu)
```

(e) Удалите существующий проброс портов:
порт хост-компьютера = 8080 > порт виртуальной машины = 80, это можно сделать с помощью команды redir del tcp:8080, но в новых версиях она не работает
(f) Добавьте новый проброс портов к виртуальной машине - порт хост-компьютера = 2222 > порт виртуальной машины = 22, можно было сделать с помощью redir add tcp:2222::22, запускаем ВМ с новым параметром

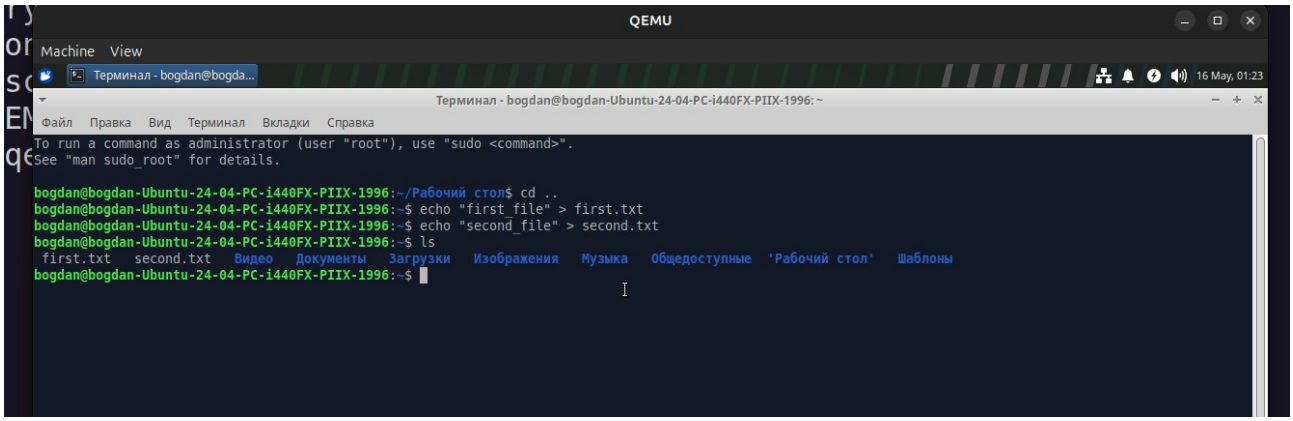
```
-hda /tmp/disk_$USER.qcow2 \
-cdrom /var/qemu/OS/xubuntu-24.04.2-desktop-amd64.iso \
-netdev user,id=usernet,hostfwd=tcp::2222-:22 \
-device e1000,netdev=usernet \
```

QEMU слушает необходимый порт

```
→  ~ sudo netstat -tulnp | grep 2222

tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN
10348/qemu-system-x
→  ~
```

(g) Выполните сохранение текущего состояния ВМ с тегом "running_state" — перед сохранением домашняя директория ВМ имеет вид




Сохраняем состояние

```
(qemu) savevm running_state
(qemu)
```

(h) Перезагрузите виртуальную систему

```
(qemu) system_reset
(qemu)
```

(i) Принудительно завершите работу ВМ исполнив команду quit

```
(qemu) quit
Connection closed by foreign host.
→  ~
```

j) Получите информацию об образах виртуальной машины, которые вы создавали и использовали во время работы ВМ. Какой объём они занимают в данный момент? Какие снимки состояния в них хранятся? — информация об образах и размерах

Первый

```
→  ~ qemu-img info /tmp/disk_base_$USER.qcow2
image: /tmp/disk_base_bogdan.qcow2
file format: qcow2
virtual size: 7 GiB (7516192768 bytes)
disk size: 200 KiB
cluster_size: 65536
Format specific information:
    compat: 1.1
    compression type: zlib
    lazy refcounts: false
    refcount bits: 16
    corrupt: false
    extended l2: false
Child node '/file':
    filename: /tmp/disk_base_bogdan.qcow2
    protocol type: file
    file length: 256 KiB (262656 bytes)
    disk size: 200 KiB
```

Второй

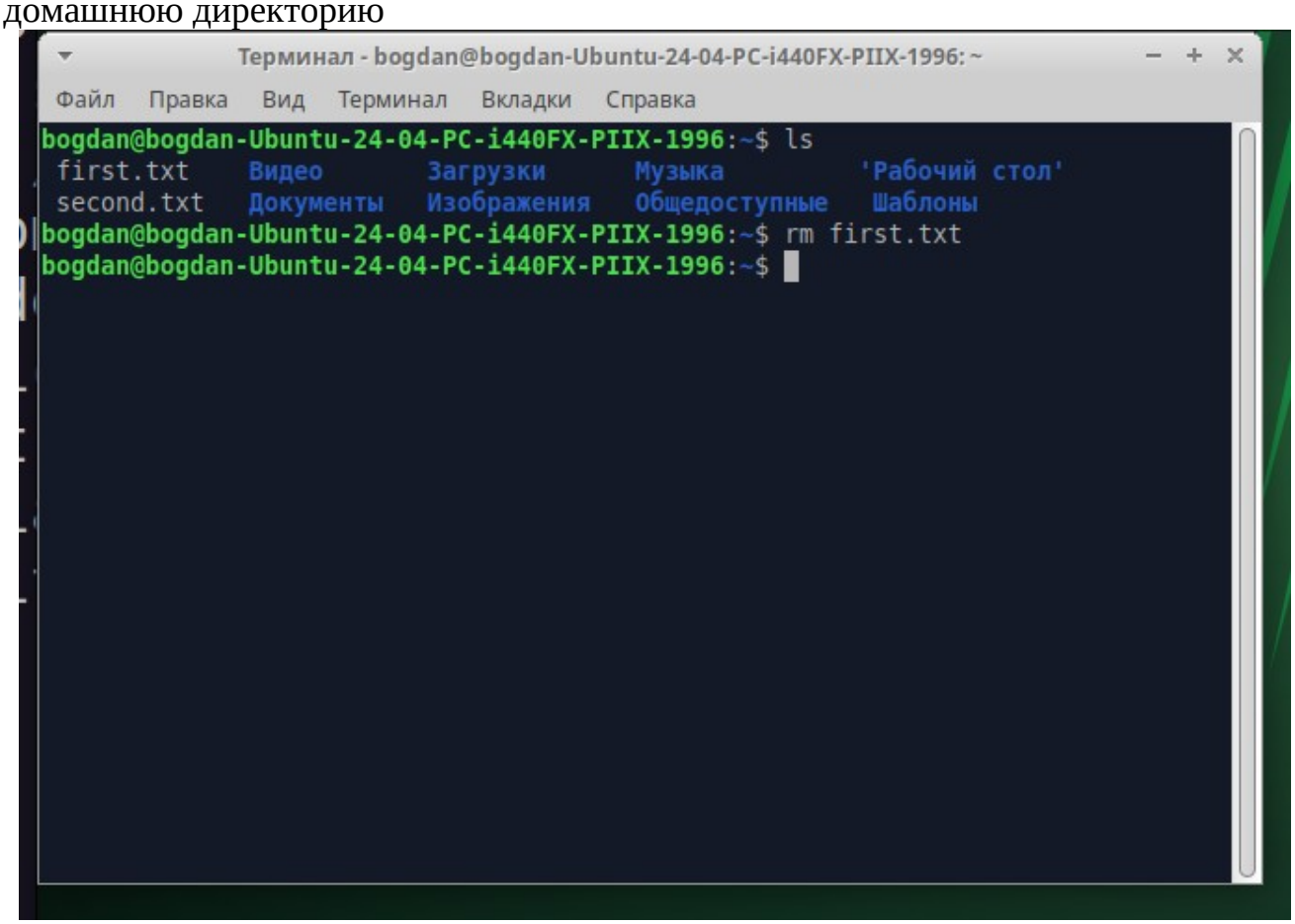
```
→  ~ qemu-img info /tmp/disk_$USER.qcow2
image: /tmp/disk_bogdan.qcow2
file format: qcow2
virtual size: 7 GiB (7516192768 bytes)
disk size: 5.97 GiB
cluster_size: 65536
backing file: /tmp/disk_base_bogdan.qcow2
backing file format: qcow2
Snapshot list:
ID        TAG               VM SIZE                DATE     VM CLOCK
1         running_state     892 MiB 2025-05-16 01:25:15 00:06:34.951
Format specific information:
    compat: 1.1
    compression type: zlib
    lazy refcounts: false
    refcount bits: 16
    corrupt: false
    extended l2: false
Child node '/file':
    filename: /tmp/disk_bogdan.qcow2
    protocol type: file
    file length: 5.97 GiB (6412173312 bytes)
    disk size: 5.97 GiB
→  ~
```

Информация о снимках состояния — командой qemu-img snapshot -l /tmp/disk_$USER.qcow2

```
→  ~ qemu-img snapshot -l /tmp/disk_$USER.qcow2

Snapshot list:
ID        TAG               VM SIZE                DATE     VM CLOCK     ICOUNT
1         running_state     892 MiB 2025-05-16 01:25:15 00:06:34.951
→  ~
```

(k) Восстановите работу ВМ из сохранённого снимка состояния — изменим домашнюю директорию

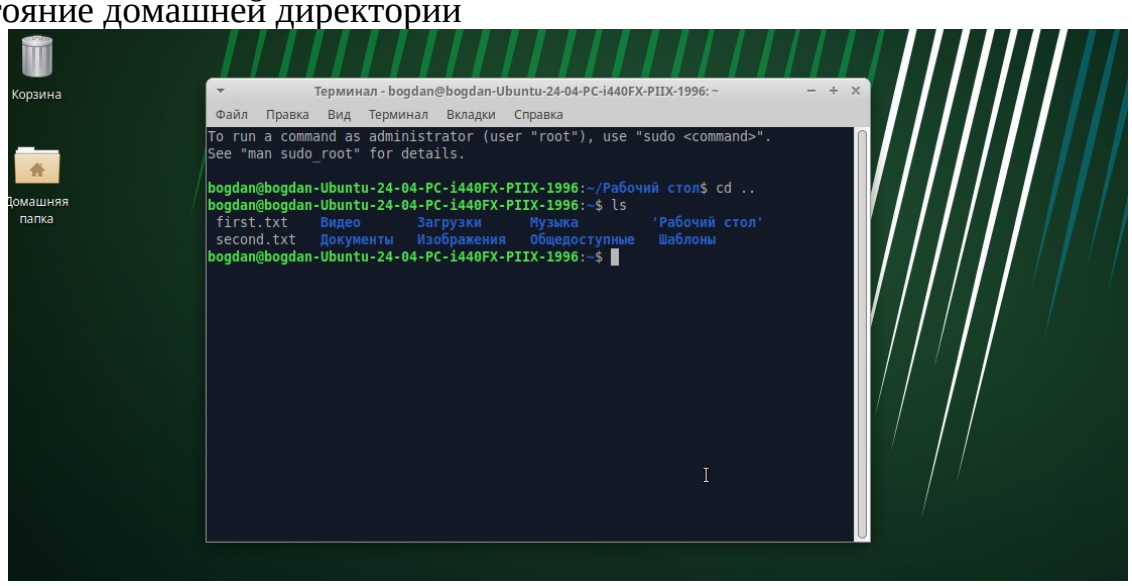



Далее запускаем ВМ с помощью команды

```
~ qemu-system-x86_64 \
-enable-kvm \
-smp 4 \
-m 2048 \
-vga std \
-hda /tmp/disk_$USER.qcow2 \
-cdrom /var/qemu/OS/xubuntu-24.04.2-desktop-amd64.iso \
-nic user,hostfwd=tcp::2222-:22 \
-boot menu=on \
-serial none \
-monitor telnet:127.0.0.1:10023,server,nowait \
-loadvm running_state
```

В конце добавил строчку -loadvm running_state

Состояние домашней директории




**B)** 1. Узнайте список всех пользователей — с помощью команды cat /etc/passwd

```
→  ~ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

2. Получите вывод только имён пользователей в системе

```
→  ~ cut -d':' -f1 /etc/passwd
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
```

3. Узнайте список всех подключенных пользователей к системе в данный момент времени

```
→  ~ who
bogdan   seat0        2025-05-15 23:28 (login screen)
bogdan   tty2         2025-05-15 23:28 (tty2)
→  ~
```

4. С помощью команды find найдите в корневом каталоге файлы:
a) имеющие атрибуты SUID;

```
→  ~ find / -perm -4000 -type f -ls 2>/dev/null
     1032     72 -rwsr-xr-x   1 root     root        72792 мая 30
n
     1038     44 -rwsr-xr-x   1 root     root        44760 мая 30
h
     1102     75 -rwsr-xr-x   1 root     root        76248 мая 30
sswd
     1186     51 -rwsr-xr-x   1 root     root        51584 дек  5
nt
     1195     40 -rwsr-xr-x   1 root     root        40664 мая 30
grp
     1210     63 -rwsr-xr-x   1 root     root        64152 мая 30
swd
     1323     55 -rwsr-xr-x   1 root     root        55680 дек  5
     1324    272 -rwsr-xr-x   1 root     root       277936 апр  8
```

b) имеющие атрибуты SGID;

```
→  ~ find / -perm -2000 -type f -ls 2>/dev/null
     1027     71 -rwxr-sr-x   1 root     shadow      72184 мая 30
ge
     1084     27 -rwxr-sr-x   1 root     shadow      27152 мая 30
iry
     1315    303 -rwxr-sr-x   1 root     pipewire   309688 фев 11
-agent
     7586     27 -rwxr-sr-x   1 root     shadow      26944 мая  3
m_extrausers_chkpwd
     7632     31 -rwxr-sr-x   1 root     shadow      31040 мая  3
ix_chkpwd
     1024     71 -rwxr-sr-x   1 root     shadow      72184 мая 30
ge
     1081     27 -rwxr-sr-x   1 root     shadow      27152 мая 30
iry
```

c) имеющие атрибуты SGID и SUID;

```
→  ~ find / -perm -6000 -type f -ls 2>/dev/null
 22020883     16 -rwsr-sr-x   1 root     root        14488 мар  4 07:58 /us
 22156636    140 -rwsr-sr-x   1 root     root       141632 авг 26  2024 /us
less
 22156652    140 -rwsr-sr-x   1 root     root       141632 авг 26  2024 /us
AT
 22157707    140 -rwsr-sr-x   1 root     root       141632 авг 26  2024 /us
oxVM
 22156648    140 -rwsr-sr-x   1 root     root       141632 авг 26  2024 /us
HCP
 22156646     36 -rwsr-sr-x   1 root     root        35304 авг 26  2024 /us
dpCtl
 22156662    140 -rwsr-sr-x   1 root     root       141632 авг 26  2024 /us
```

d) файлы, которые разрешено модифицировать всем — используем команду find / -perm -o+w -type f -ls 2>/dev/null

```
oc/13132/attr/apparmor/exec
    317158      0 -rw-rw-rw-   1 root                root
oc/13132/timerslack_ns
    345982      0 -rw-rw-rw-   1 bogdan               bogdan
oc/13217/task/13217/attr/current
    345984      0 -rw-rw-rw-   1 bogdan               bogdan
oc/13217/task/13217/attr/exec
    345985      0 -rw-rw-rw-   1 bogdan               bogdan
oc/13217/task/13217/attr/fscreate
    345986      0 -rw-rw-rw-   1 bogdan               bogdan
oc/13217/task/13217/attr/keycreate
    345987      0 -rw-rw-rw-   1 bogdan               bogdan
oc/13217/task/13217/attr/sockcreate
    345990      0 -rw-rw-rw-   1 bogdan               bogdan
```

e) файлы, не имеющие владельца

```
→  ~ sudo find / -nouser -type f -ls 2>/dev/null
→  ~
```

5. С помощью команды id user_name посмотрите список основной и дополнительных групп пользователей. Найдите дополнительные группы floppy, cdrom и plugdev, дающие право использовать сменные машинные носители /etc/cdrom, /etc/fd0 и т.д. для бесконтрольного блочного копирования данных — просмотрели список групп

```
→  ~ id $USER
uid=1000(bogdan) gid=1000(bogdan) группы=1000(bogdan),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),
100(users),114(lpadmin),128(libvirt)
→  ~
```

Дополнительные группы

```
→  ~ grep -E 'floppy|cdrom|plugdev' /etc/group
cdrom:x:24:bogdan
floppy:x:25:
plugdev:x:46:bogdan
```

6. Зарегистрируйте нового пользователя и добавьте его в разные группы, выведите список существующих пользователей и группы, проверьте наличие нового пользователя — добавили пользователя

```
→  ~ sudo adduser testuser
info: Добавляется пользователь «testuser» ...
info: Выбор UID/GID из диапазона от 1000 до 59999 ...
info: Добавляется новая группа «testuser» (1006) ...
info: Добавление нового пользователя `testuser' (1006) в группу `testuser (1006)' ...
info: Создаётся домашний каталог «/home/testuser» ...
info: Копирование файлов из «/etc/skel» ...
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: пароль успешно обновлён
Изменение информации о пользователе testuser
Введите новое значение или нажмите ENTER для выбора значения по умолчанию
        Полное имя []:
        Номер комнаты []:
        Рабочий телефон []:
        Домашний телефон []:
        Другое []:
Данная информация корректна? [Y/n]
info: Adding new user `testuser' to supplemental / extra groups `users' ...
info: Добавляется пользователь «testuser» в группу «users» ...
→  ~
```

Добавили его в группы

```
→  ~ sudo usermod -a -G audio testuser
→  ~ sudo usermod -a -G video testuser
```

Проверка

```
→  ~ grep '^testuser:' /etc/passwd
testuser:x:1006:1006:,,,:/home/testuser:/bin/bash
→  ~ cat /etc/group | grep audio
audio:x:29:testuser
→  ~ cat /etc/group | grep video
video:x:44:testuser
→  ~
```

7. С помощью команды md5sum вычислите и запишите контрольную сумму для одного из файлов в каталоге /home/

```
→  ~ md5sum /home/bogdan/2.txt > checksum.txt
→  ~ cat checksum.txt
2c1530bfc2e7979960bed84d23089e8b  /home/bogdan/2.txt
→  ~
```

8. С помощью команды md5sum вычислите и запишите в файл контрольную сумму всех файлов в каталоге /bin

```
→  ~ find /bin/ -type f -print0 | xargs -0 md5sum > bin_checksums.txt
→  ~ cat bin_checksums.txt
69da972b71f0e213ac3d57465e970f7e  /bin/file2brl
1b075af45d1d46ca7b4848fa2103bb69  /bin/x86_64-linux-gnu-gcov-dump-13
b9c137c2290f93cde749f25efd79f299  /bin/boltctl
5432fcbd6bf1b44600d5e0d602321137  /bin/systemd-creds
713dda5cc05ee9ac94409ad16bb2cc25  /bin/hbpldecode
822ce0a9838c93e13484a37bbfb5634a  /bin/pamedge
cd0fa54689e80ad3c9d18c9637f16ce9  /bin/pamtodjvurle
79e8285df8425d379af1a4d04dd307b3  /bin/oakdecode
c113b33dc57b887ce9ede95c7c20775d  /bin/evince-previewer
0cdf3af96780861139fc1ee4f87fe6b2  /bin/perli11ndoc
fadf743209d96f6c52bb4058e24a2f57  /bin/qtchooser
991d0cc19f26d45be146c3653c74ac3f  /bin/ln
```

9. Снова с помощью команды md5sum вычислите и запишите в файл контрольную сумму всех файлов в каталоге /bin и добавьте какие-нибудь символы в конце файла, после сравните обе суммы

```
→  ~ find /bin/ -type f -print0 | xargs -0 md5sum > bin_second_checksums.txt
→  ~ echo "дополнительный текст" >> bin_second_checksums.txt
```

Сравнение файлов

```
bogdan@bogdan-laptop:~
→  ~ diff ./bin_checksums.txt ./bin_second_checksums.txt
2016a2017
> дополнительный текст
→  ~
```

10. Найдите в папке /usr/share, включая подкаталоги, простые файлы “doc” и скопируйте найденное в папку /tmp/docs/

```
→  ~ find /tmp/test/usr/share -type f -name "doc" -exec sh -c 'for f; do cp "$f" /tmp/docs/"$(basena
me $(dirname "$f"))_doc"; done' sh {} +

→  ~ ls -l /tmp/docs
итого 0
-rw-rw-r-- 1 bogdan bogdan 0 мая 16 02:25 doc
-rw-rw-r-- 1 bogdan bogdan 0 мая 16 02:25 share_doc
-rw-rw-r-- 1 bogdan bogdan 0 мая 16 02:25 subdir_doc
→  ~
```

11. Установите пакет auditd для мониторинга событий операционной системы и записи их в журналы событий

```
→  ~ sudo apt install auditd
Чтение списков пакетов… Готово
Построение дерева зависимостей… Готово
Чтение информации о состоянии… Готово
Будут установлены следующие дополнительные пакеты:
  libauparse0t64
Предлагаемые пакеты:
  audispd-plugins
Следующие НОВЫЕ пакеты будут установлены:
  auditd libauparse0t64
Обновлено 0 пакетов, установлено 2 новых пакетов, для удаления отмечено 0 пакетов, и 21 пакетов не о
бновлено.
Необходимо скачать 274 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 893 kB.
Хотите продолжить? [Д/н]
```

12. Просмотрите статус службы auditd

```
→  ~ sudo systemctl status auditd
● auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-05-16 02:27:10 MSK; 46s ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
    Process: 15575 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
    Process: 15579 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
   Main PID: 15576 (auditd)
      Tasks: 2 (limit: 18324)
     Memory: 500.0K (peak: 2.3M)
        CPU: 32ms
     CGroup: /system.slice/auditd.service
             └─15576 /sbin/auditd
```

13. Запустите службу auditd — уже запущена

14. Выведите абсолютно все события аудита за день

```
→  ~ sudo ausearch -ts today
----
time->Fri May 16 02:27:10 2025
type=DAEMON_START msg=audit(1747351630.110:9399): op=start ver=3.1.2 format=enriched kerne
5-generic auid=4294967295 pid=15576 uid=0 ses=4294967295 subj=unconfined  res=success
----
time->Fri May 16 02:27:10 2025
type=PROCTITLE msg=audit(1747351630.127:372971): proctitle=2F7362696E2F617564697463746C002
4632F61756469742F61756469742E72756C6573
type=SYSCALL msg=audit(1747351630.127:372971): arch=c000003e syscall=44 success=yes exit=6
7ffce7d40070 a2=3c a3=0 items=0 ppid=15579 pid=15590 auid=4294967295 uid=0 gid=0 euid=0 su
=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="auditctl" exe="/usr/sbin/auditctl
onfined key=(null)
type=CONFIG_CHANGE msg=audit(1747351630.127:372971): op=set audit_backlog_limit=8192 old=6
```

15. Установите пакет figlet

```
sudo apt install figlet

Сущ:1 http://archive.ubuntu.com/ubuntu noble InRelease
Пол:2 https://dl.google.com/linux/chrome/deb stable InRelease [1 825 B]
Пол:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Пол:4 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Пол:5 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1 216 B]
Пол:6 https://packages.microsoft.com/ubuntu/22.04/prod jammy InRelease [3 632 B]
Пол:7 https://packages.microsoft.com/ubuntu/20.04/prod focal InRelease [3 632 B]
Сущ:8 https://download.mono-project.com/repo/ubuntu stable-bionic InRelease
Пол:9 https://packages.microsoft.com/ubuntu/22.04/prod jammy/main amd64 Packages [219 kB]
Пол:10 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Пол:11 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21,5 kB]
Пол:12 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B
```

16. Запустите figlet таким образом, чтобы на экране отобразилась ваша фамилия и группа