Семинар 1

Решение

Смена корневого каталога (полноценной изоляцией не является).

При создании новой корневой директории нужно копировать все исполняемые файлы - рост объема дискового пространства.

----------------

mkdir GB

cd GB

mkdir bin

cp /bin/bash GB/bin

ldd /bin/bash

mkdir GB/lib

mkdir GB/lib64

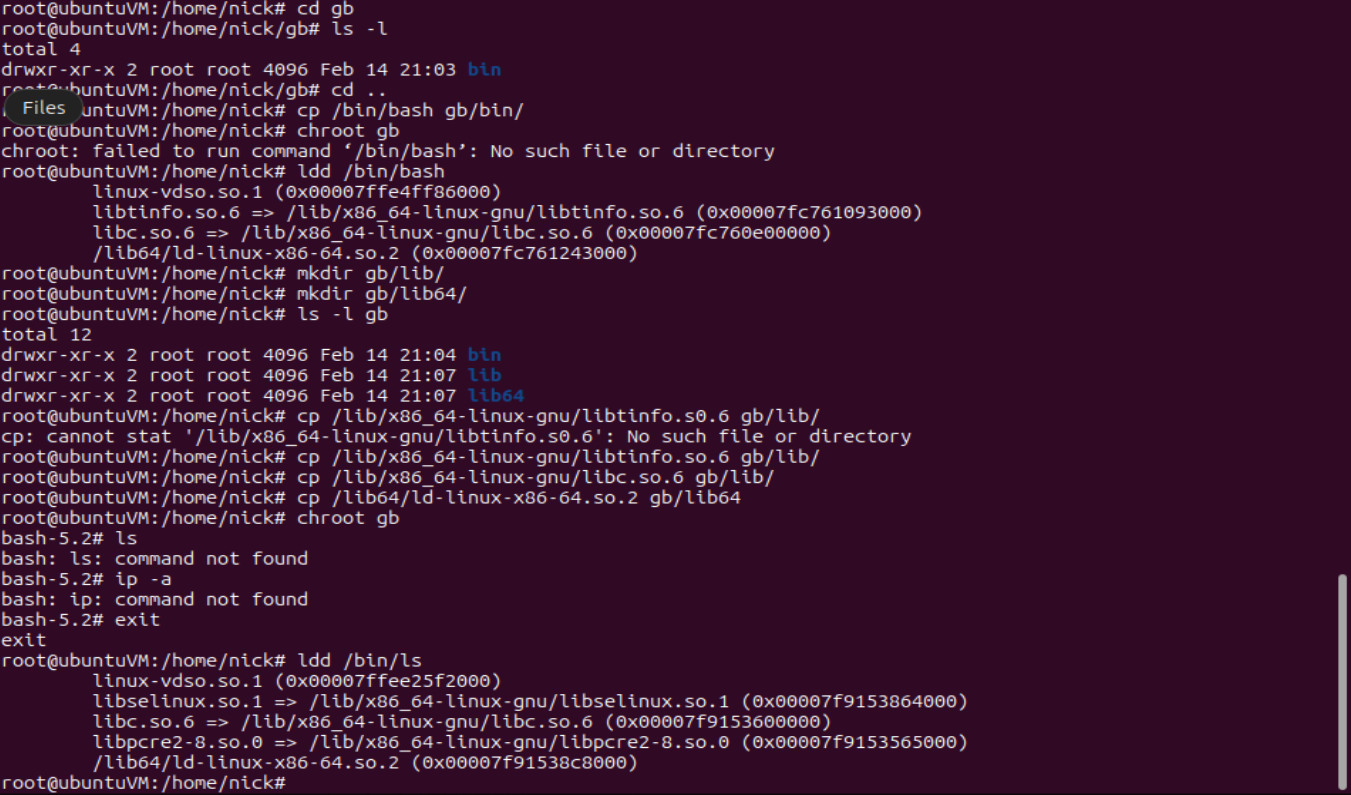
cp /lib/x86\_64-linux-gnu/libtinfo.so.6 GB/lib

cp /lib/x86\_64-linux-gnu/libc.so GB/lib

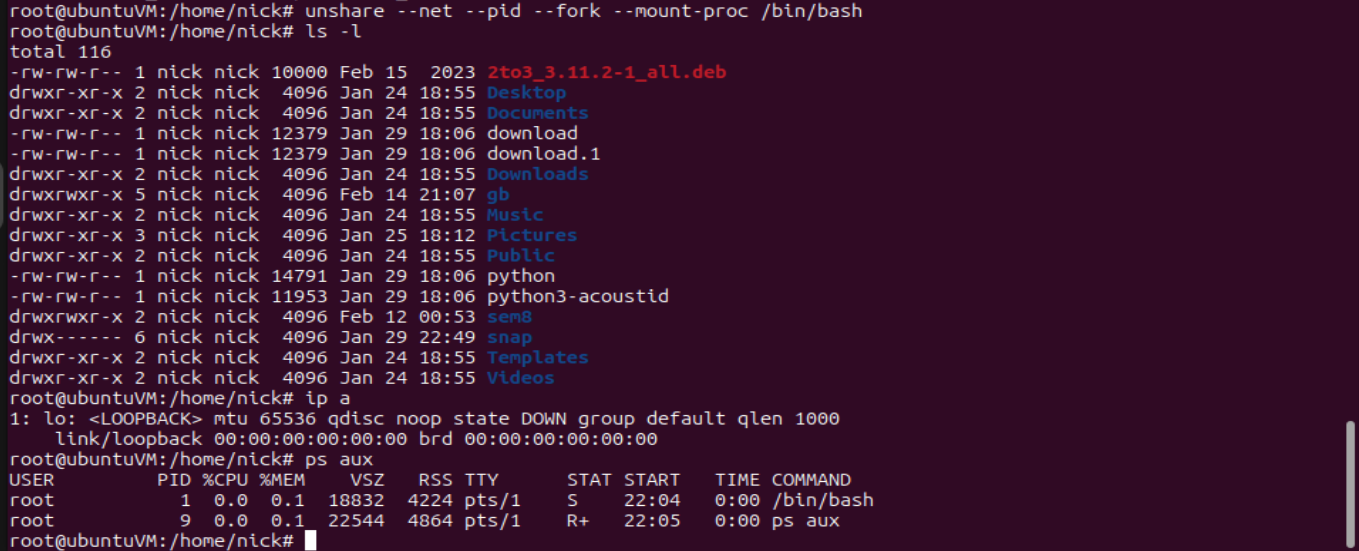
cp /lib/x86\_64-linux-gnu/libc.so.6 GB/lib

cp /lib64/ld-linux-x86-64.so.2 GB/lib64

sudo chroot GB



Изоляция файловой системы.



команда:

unshare --net --pid --fork --mount-proc /bin/bash

ps aux

unshare Утилита которая позволяет это разграничивать –

--net — ограничевает сетевое пространство имен

ip a

-mount-proc — разграничивает процессы

ps aux

--fork — изолирует память

--pid — изолирует дерево процессов Формально мы внутри контейнера

ls

ls /

ps aux

Изоляция сетевого пространства имён.

Сама изоляция демонстрируется путем запуска команды ip a на хост-системе и в изолированном пространстве имен:

Далее идет создание интерфейса в пространстве имен и демонстрация взаимодействия с хост-системой.

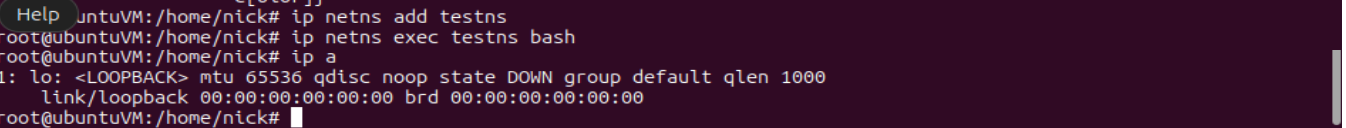
Хост-система.

# ip netns add testns

Добавляет сетевое пространство имен с именем testns

# ip netns exec testns bash

запуск командного интерпретатора bash в пространстве имен testns.



Пространство имён.

# ip a

просмотреть доступные сетевые интерфейсы и их состояние.