# 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 --mount --root=HomeWork01 /bin/zsh

unshare -- команда, запускающая программу в новом пространстве имён.

--mount -- опция указывает, что требуется изолировать пространство имен монтирования файловой системы (Unshare the mount namespace, согласно man unshare)

--root=<dir> -- опция указывает какая директория должна быть смонтирована как корневая.

/bin/zsh -- Командный интерпретатор zsh; процесс, который будет запущен в изолированном пространстве имён.

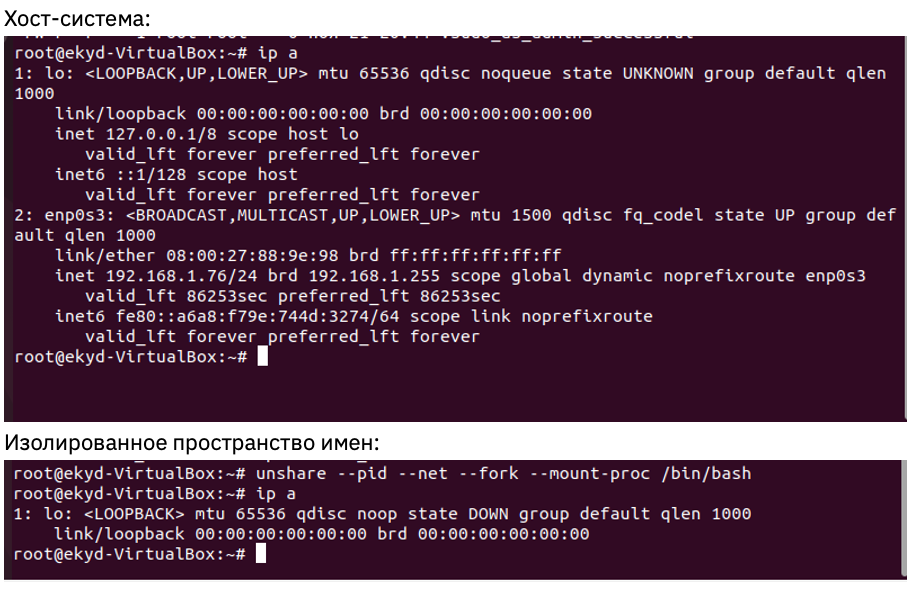
В новый корневой каталог были скопированы утилиты ls, rm, mount и др., а также библиотеки, требующиеся для работы этих утилит.

Вызов 'mount' без параметров неудачен в связи с отсутствием файла mtab, который ссылается на /proc/self/mounts.

Вызов 'rm -rf --no-preserve-root /' привел к ожидаемому результату -- уничтожению корневой файловой системы пространства имён, host-система не затронута.

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.

Хост-система.

# ip link add virt0 type veth peer name virt1

добавить виртуальный сетевой интерфейс virt0 типа veth связанный с сетевым интерфейсом virt1

# ip addr add 10.0.0.1/24 dev virt0

назначить сетевой адрес интерфейсу virt0

# ip addr add 10.0.0.2/24 dev virt1

назначить сетевой адрес интерфейсу virt1

# ip link set virt1 netns testns

назначить сетевой интерфейс virt1 пространству имён "testns"

Пространство имён.

# ip addr add 10.0.0.3/24 dev virt1

назначить сетевой адрес интерфейсу virt1

# ip link set dev virt1 up

включить (поднять) сетевой интефейс virt1

Хост-система.

# ip link set dev virt0 up

включить (поднять) сетевой интефейс virt0

# ping 10.0.0.3 -c2

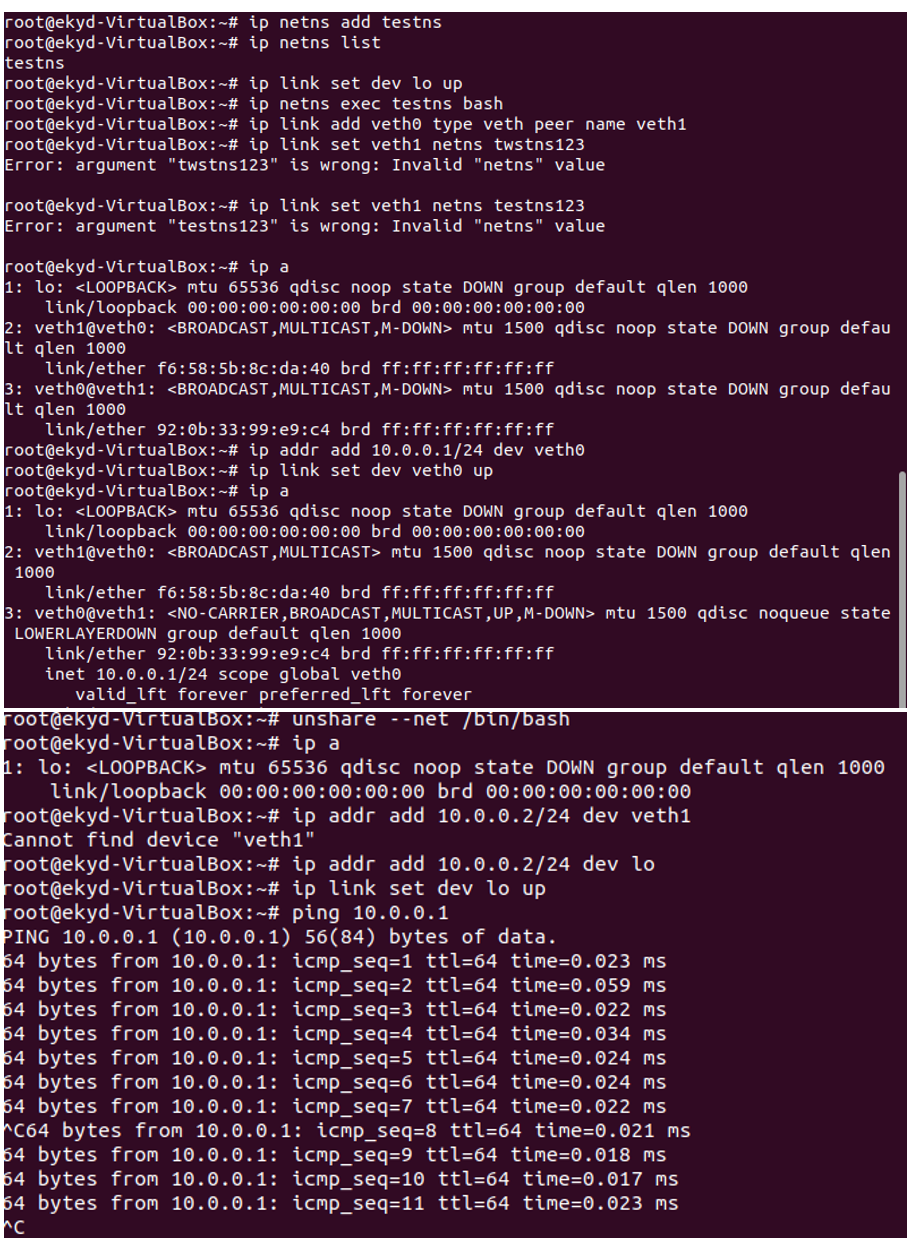
опросить интерфейс пространства имен.

Пространство имён.

# ping 10.0.0.1 -c2

опросить интерфейс хост-системы.

Результат выглядит следующим образом:



Отдельно можно отобразить изоляцию сразу нескольких пространств имен:

PID, network, mount и UTS

root@ubuntu2004:~# unshare --pid --net --fork --mount-proc --mount --uts /bin/bash