Задание: необходимо продемонстрировать изоляцию одного и того же приложения (как решено на семинаре - командного интерпретатора) в различных пространствах имен.

1. Изолированное выполнение процессов с помощью *chroot*.

Создаем каталог "testfolder"

*mkdir ~/testfolder*

Копируем необходимые исполняемые файлы и библиотеки в этот каталог

*cp /bin/bash ~/testfolder/bin*

*mkdir ~/testfolder/lib ~/testfolder/lib64*

*cp /lib/x86\_64-linux-gnu/libtinfo.so.6 ~/testfolder/lib*

*cp /lib/x86\_64-linux-gnu/libc.so.6 ~/testfolder/lib*

*cp /lib64/ld-linux-x86-64.so.2 ~/testfolder/lib64/*

Запускаем команду *chroot* для изменения корневой папки нашей текущей среды

*sudo chroot ~/testfolder /bin/bash*

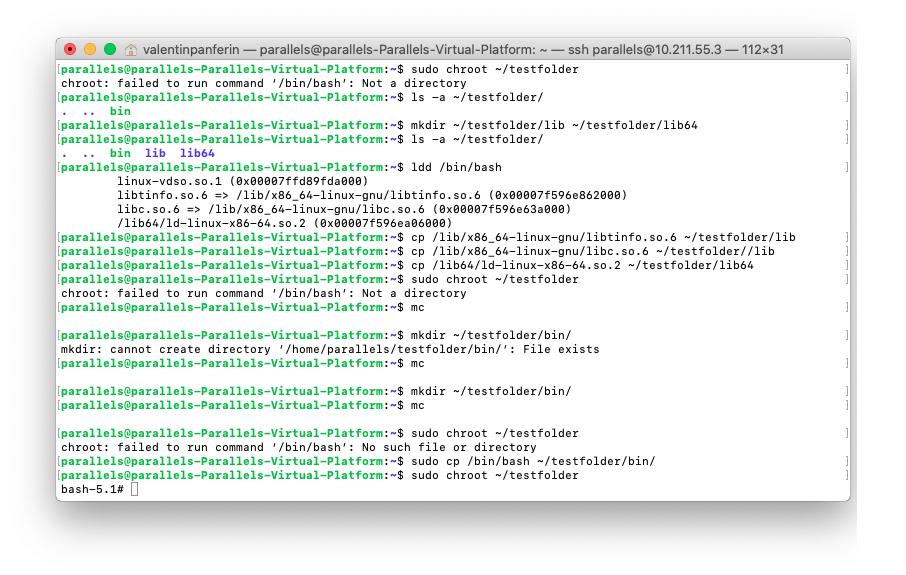
Необходимо также скопировать исполняемые файлы, такие как "ls", и связанные с ними библиотеки в созданный каталог. Копируем необходимые файлы

*сp /bin/ls ~/testfolder/bin/*

*cp /lib/x86\_64-linux-gnu/libselinux.so.1 ~/testfolder/lib/*

*cp /lib/x86\_64-linux-gnu/libpcre2-8.so.0 ~/testfolder/lib/*

Пример выполнения:



1. Сетевая изоляция, сетевое пространство имен *ip netns*.

Воспользуемся командой *ip* для создания сетевого пространства имен. Создаем пространство имен с именем "*testns*", к которому можно подключить процессы

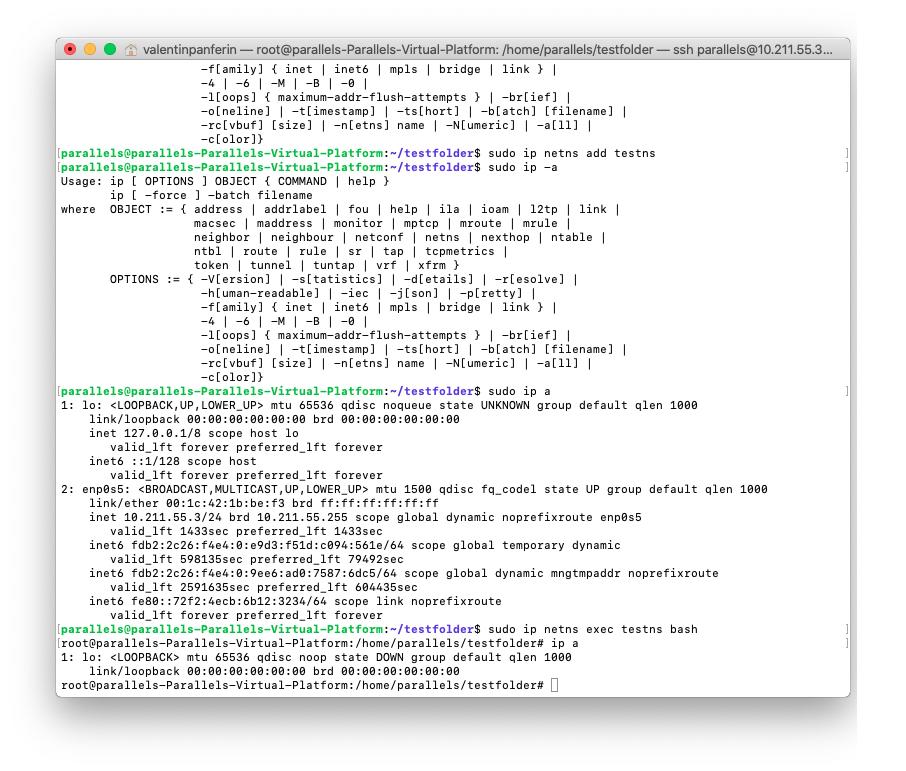
*ip netns add testns*

Запускаем процесс в пространстве имен используя команду ip, мы можем выполнить процесс в созданном пространстве имен

*ip netns exec testns bash*

При выполнении команды *ip* a мы можем увидеть только виртуальные настройки

Пример выполнения:



1. Изоляция процесса и файловой системы *unshare*.

*Unshare* это утилита которая позволяет это разграничивать.

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

*--net* — ограничивает сетевое пространство имен

*--pid* — изолирует дерево процессов

*--fork* — изолирует память

*--mount-proc* — разграничивает процессы

Пример выполнения:

