

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
root@ubuntuVM:/home/nick# cd gb
root@ubuntuVM:/home/nick/gb# ls -l
total 4
drwxr-xr-x 2 root root 4096 Feb 14 21:03 bin
root@ubuntuVM:/home/nick/gb# cd ..
Files ubuntuVM:/home/nick# cp /bin/bash gb/bin/
root@ubuntuVM:/home/nick# chroot gb
chroot: failed to run command '/bin/bash': No such file or directory
root@ubuntuVM:/home/nick# ldd /bin/bash
        linux-vdso.so.1 (0x00007ffe4ff86000)
        libtinfo.so.6 => /lib/x86_64-linux-gnu/libtinfo.so.6 (0x00007fc761093000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fc760e00000)
        /lib64/ld-linux-x86-64.so.2 (0x00007fc761243000)
root@ubuntuVM:/home/nick# mkdir gb/lib/
root@ubuntuVM:/home/nick# mkdir gb/lib64/
root@ubuntuVM:/home/nick# ls -l gb
total 12
drwxr-xr-x 2 root root 4096 Feb 14 21:04 bin
drwxr-xr-x 2 root root 4096 Feb 14 21:07 lib
drwxr-xr-x 2 root root 4096 Feb 14 21:07 lib64
root@ubuntuVM:/home/nick# cp /lib/x86_64-linux-gnu/libtinfo.so.6 gb/lib/
cp: cannot stat '/lib/x86_64-linux-gnu/libtinfo.so.6': No such file or directory
root@ubuntuVM:/home/nick# cp /lib/x86_64-linux-gnu/libtinfo.so.6 gb/lib/
root@ubuntuVM:/home/nick# cp /lib/x86_64-linux-gnu/libc.so.6 gb/lib/
root@ubuntuVM:/home/nick# cp /lib64/ld-linux-x86-64.so.2 gb/lib64
root@ubuntuVM:/home/nick# chroot gb
bash-5.2# ls
bash: ls: command not found
bash-5.2# ip -a
bash: ip: command not found
bash-5.2# exit
exit
root@ubuntuVM:/home/nick# ldd /bin/ls
        linux-vdso.so.1 (0x00007ffe25f20000)
        libselinux.so.1 => /lib/x86_64-linux-gnu/libselinux.so.1 (0x00007f9153864000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f9153600000)
        libpcre2-8.so.0 => /lib/x86_64-linux-gnu/libpcre2-8.so.0 (0x00007f9153565000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f91538c8000)
root@ubuntuVM:/home/nick#
```

Изоляция файловой системы.

```
root@ubuntuVM:/home/nick# unshare --net --pid --fork --mount-proc /bin/bash
root@ubuntuVM:/home/nick# ls -l
total 116
-rw-rw-r-- 1 nick nick 10000 Feb 15 2023 2to3_3.11.2-1_all.deb
drwxr-xr-x 2 nick nick 4096 Jan 24 18:55 Desktop
drwxr-xr-x 2 nick nick 4096 Jan 24 18:55 Documents
-rw-rw-r-- 1 nick nick 12379 Jan 29 18:06 download
-rw-rw-r-- 1 nick nick 12379 Jan 29 18:06 download.1
drwxr-xr-x 2 nick nick 4096 Jan 24 18:55 Downloads
drwxrwxr-x 5 nick nick 4096 Feb 14 21:07 gb
drwxr-xr-x 2 nick nick 4096 Jan 24 18:55 Music
drwxr-xr-x 3 nick nick 4096 Jan 25 18:12 Pictures
drwxr-xr-x 2 nick nick 4096 Jan 24 18:55 Public
-rw-rw-r-- 1 nick nick 14791 Jan 29 18:06 python
-rw-rw-r-- 1 nick nick 11953 Jan 29 18:06 python3-acoustid
drwxrwxr-x 2 nick nick 4096 Feb 12 00:53 send
drwx----- 6 nick nick 4096 Jan 29 22:49 snap
drwxr-xr-x 2 nick nick 4096 Jan 24 18:55 Templates
drwxr-xr-x 2 nick nick 4096 Jan 24 18:55 Videos
root@ubuntuVM:/home/nick# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
root@ubuntuVM:/home/nick# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.1 18832  4224 pts/1    S   22:04   0:00 /bin/bash
root         9  0.0  0.1  22544  4864 pts/1    R+  22:05   0:00 ps aux
root@ubuntuVM:/home/nick#
```

команда:

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

`ps aux`

`unshare` Утилита которая позволяет это разграничивать –

`--net` – ограничивает 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`.

```
root@ubuntuVM:/home/nick# ip netns add testns
root@ubuntuVM:/home/nick# ip netns exec testns bash
root@ubuntuVM:/home/nick# ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
root@ubuntuVM:/home/nick#
```

Пространство имён.

`# ip a`

посмотреть доступные сетевые интерфейсы и их состояние.