Restrict SSH User Access to Certain Directory Using Chrooted Jail

In order to lock SSH users in a certain directory, we can use chroot mechanism.

change root (chroot) in Unix-like systems such as Linux, is a means of separating specific user operations from the rest of the Linux system; changes the apparent root directory for the current running user process and its child process with new root directory called a chrooted jail.

In this tutorial, we'll show you how to restrict a SSH user access to a given directory in Linux. Note that we'll run the all the commands as root, use the sudo command if you are logged into server as a normal user.

Step 1: Create SSH Chroot Jail

1. Start by creating the chroot jail using the mkdir command below:

```
# mkdir -p /home/test
```

2. Next, identify required files, according to the **sshd_config** man page, the `ChrootDirectory` option specifies the pathname of the directory to chroot to after authentication. The directory must contain the necessary files and directories to support a user's session.

For an interactive session, this requires at least a shell, commonly `sh`, and basic `/dev` nodes such as null, zero, stdin, stdout, stderr, and tty devices:

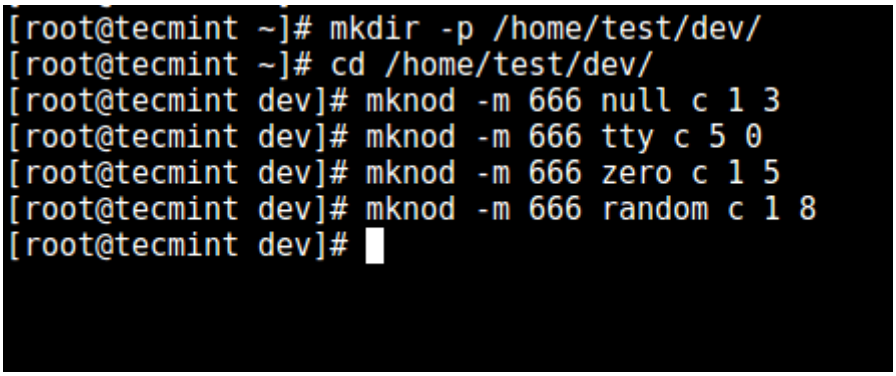
```
# ls -l /dev/{null,zero,stdin,stdout,stderr,random,tty}
```

```
[root@tecmint ~]# ls -l /dev/{null,zero,stdin,stdout,stderr,random,tty}
crw-rw-rw- 1 root root 1, 3 Mar  3 15:51 /dev/null
crw-rw-rw- 1 root root 1, 8 Mar  3 15:51 /dev/random
lrwxrwxrwx 1 root root   15 Mar  3 15:50 /dev/stderr -> /proc/self/fd/2
lrwxrwxrwx 1 root root   15 Mar  3 15:50 /dev/stdin -> /proc/self/fd/0
lrwxrwxrwx 1 root root   15 Mar  3 15:50 /dev/stdout -> /proc/self/fd/1
crw-rw-rw- 1 root tty  5, 0 Mar  3 15:51 /dev/tty
crw-rw-rw- 1 root root 1, 5 Mar  3 15:51 /dev/zero
[root@tecmint ~]#
```

3. Now, create the `/dev` files as follows using the **mknod command**. In the command below, the `-m` flag is used to specify the file permissions bits, `c` means character file and the two numbers are major and minor numbers that the files point to.

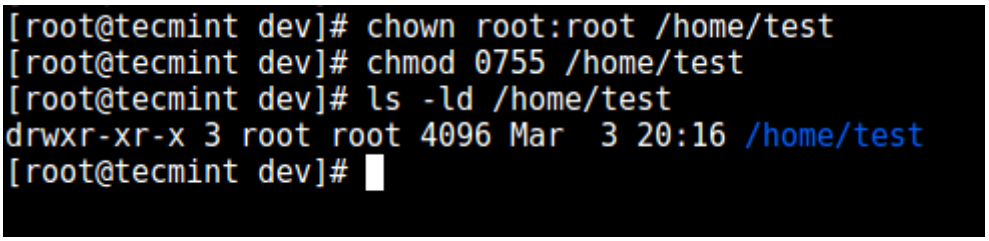
```
# mkdir -p /home/test/dev/
# cd /home/test/dev/
# mknod -m 666 null c 1 3
```

```
# mknod -m 666 tty c 5 0
# mknod -m 666 zero c 1 5
# mknod -m 666 random c 1 8
```



4. Afterwards, set the appropriate permission on the chroot jail. Note that the chroot jail and its subdirectories and subfiles must be owned by **root** user, and not writable by any normal user or group:

```
# chown root:root /home/test
# chmod 0755 /home/test
# ls -ld /home/test
```



Step 2: Setup Interactive Shell for SSH Chroot Jail