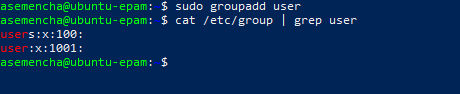
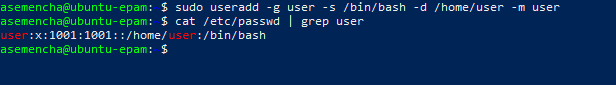
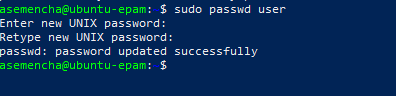
1. User management. Here we suppose there are at least two users - root and guest.
   1. Create a new user user

groupadd - create a new group

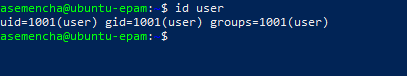


useradd - create a new user or update default new user information



passwd - change user password

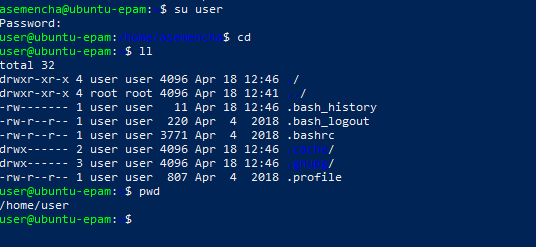
id - print real and effective user and group IDs



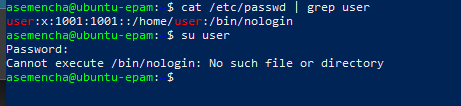


* 1. Log in to the system as “user”

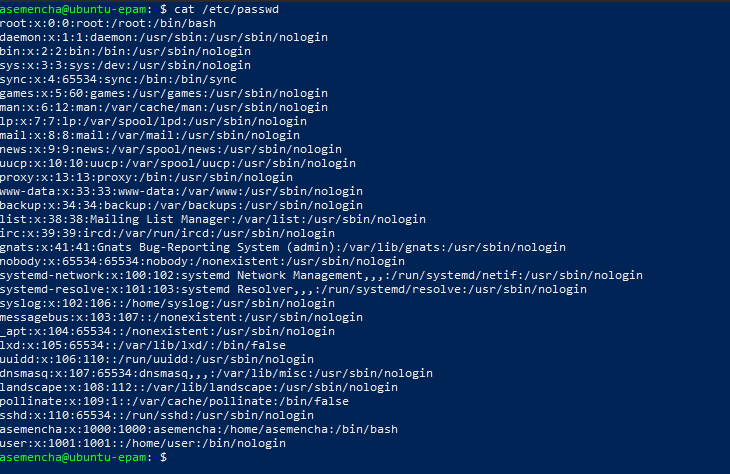
su - change user ID or become superuser

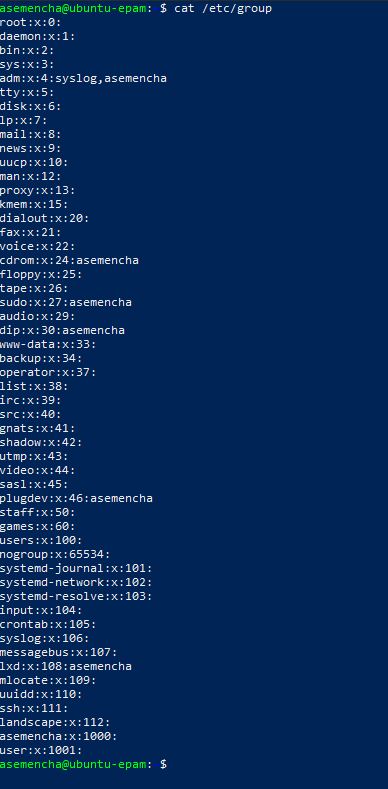


* 1. Edit /etc/passwd to prevent user user from logging in to the system.

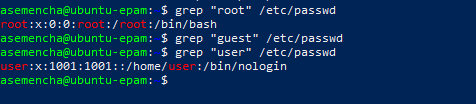


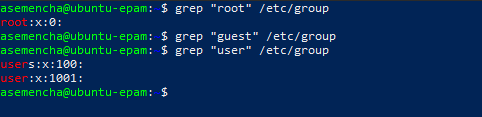
1. Content of /etc/passwd and /etc/group.
   1. Look through /etc/passwd and /etc/group



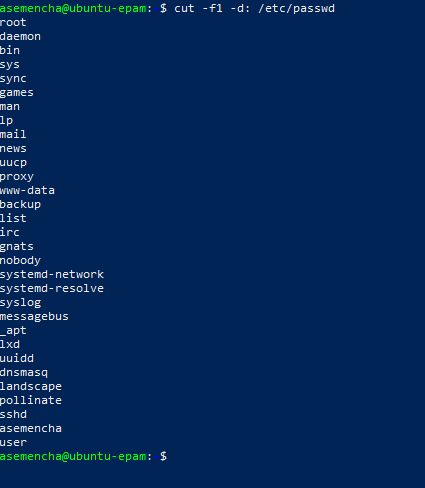


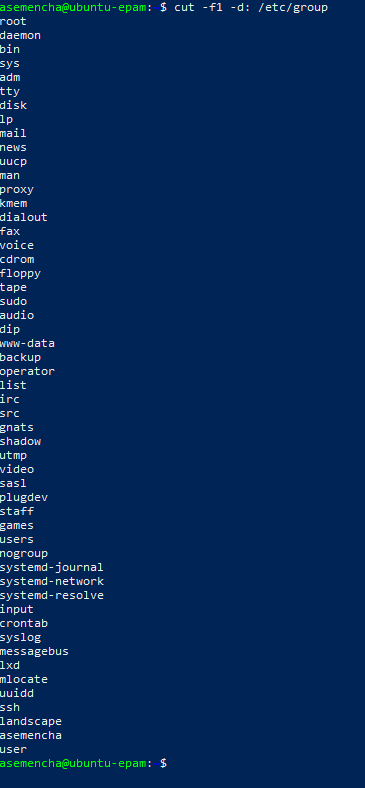
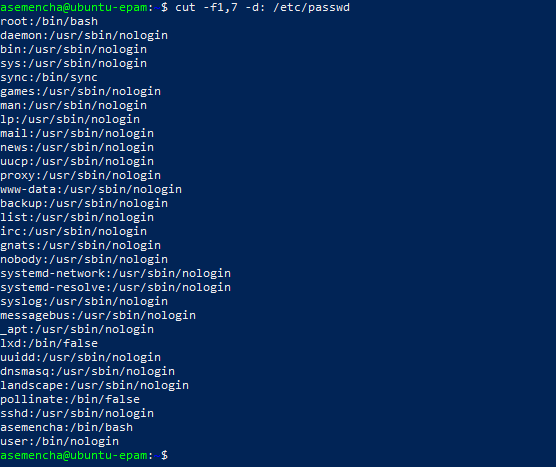
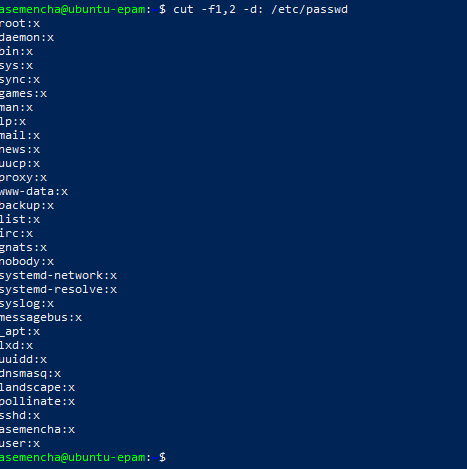
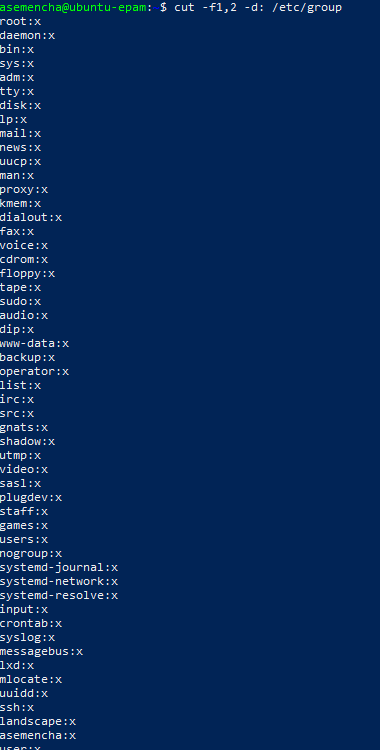
* 1. Get data from /etc/passwd and /etc/group about users: root, guest, user



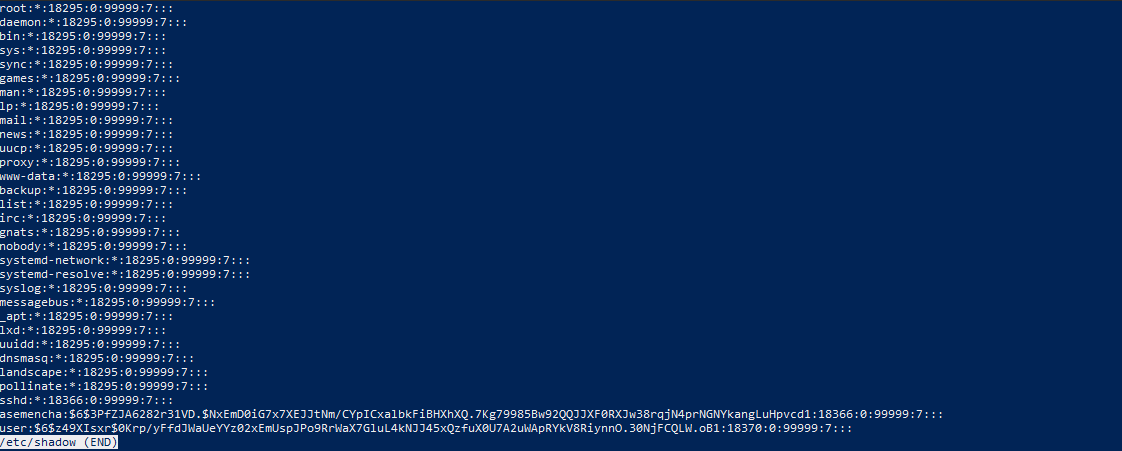


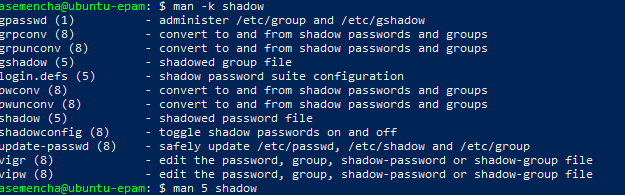
* 1. Parse /etc/passwd and /etc/group with cut.

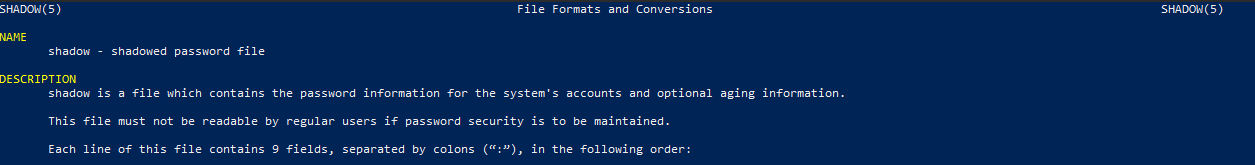


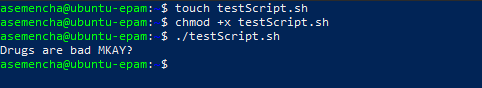
 

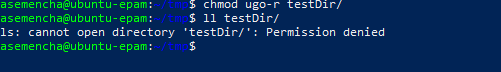
* 1. Try to call less on /etc/shadow and invoke







1. Dealing with chmod.
   1. An executable script. Open your favorite editor and put these lines into a file
   2. Suppose you have logged in to the system as guest. Create directory “testDir” in the /tmp; put some file into testDir and prohibit user user from visiting this directory

chmod - change file mode bits

* 1. Test, if it possible to forbid an owner of some file to read to or write from this file.

