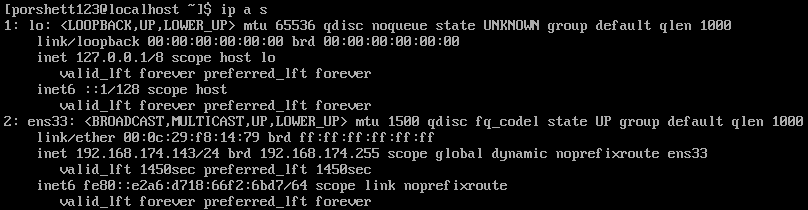
**Name, Surname: Kamil Kangarli**

You can add print screen

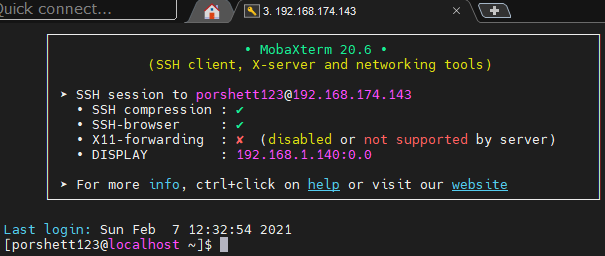
1. What is IP address of your Linux machine? Write command and result.

Answer here: ip a s

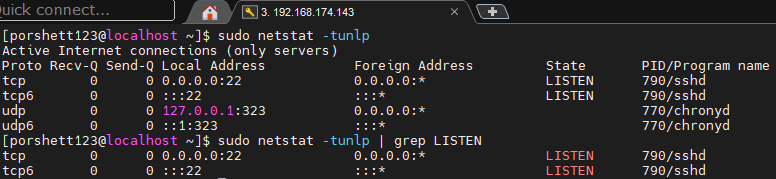


1. Connect from windows host to your Linux machine with putty via ssh protocol

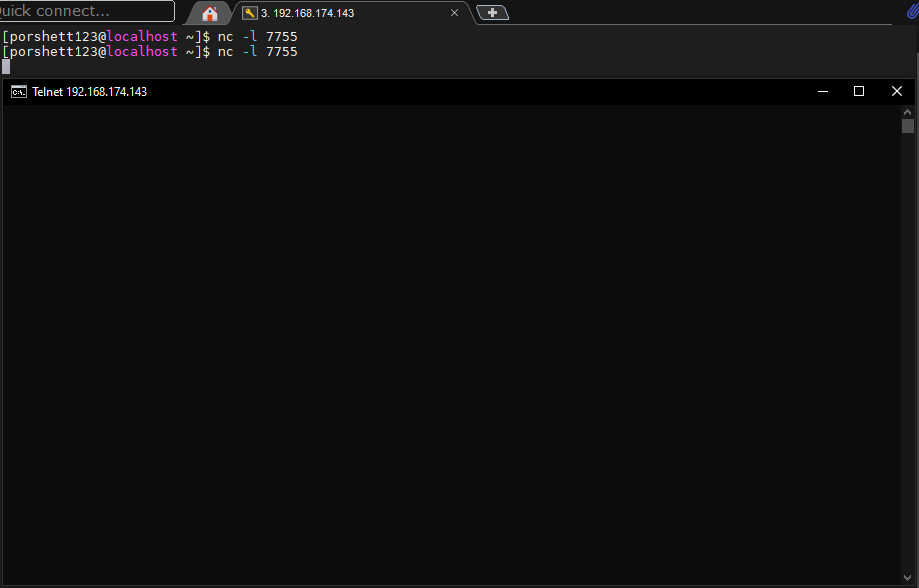
Answer here:



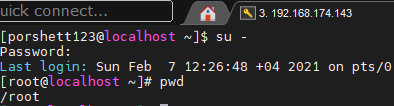
1. Show open ports with netstat command (you need to grep LISTEN ports)



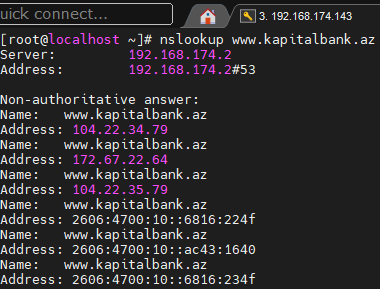
1. Telnet one of open (LISTEN) ports from windows machine.



1. After you login with root user look which directory you are in. Which command did you use?

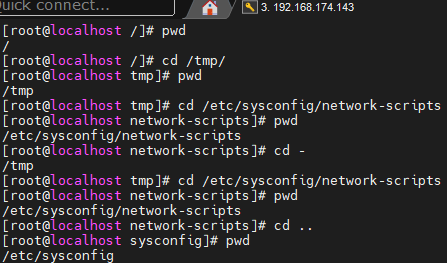


1. Check if #nslookup command is available on your linux machine. (you can use #which command to check)
2. If nslookup is not available try to install it.
3. #yum whatprovides nslookup
4. #yum install <write\_here\_result\_of\_”b”\_command>
5. Run #nslookup www.kapitalbank.az and show the result.



1. What can happen if you run #rm –rf /\* command on you linux machine. (don’t run it on production machine !!! )  
   Deleting all data and killing your machine
2. Change directory to /tmp directory. Now run #cd /etc/sysconfig/network-scripts.
3. What is the difference between #cd - and #cd .. commnds.

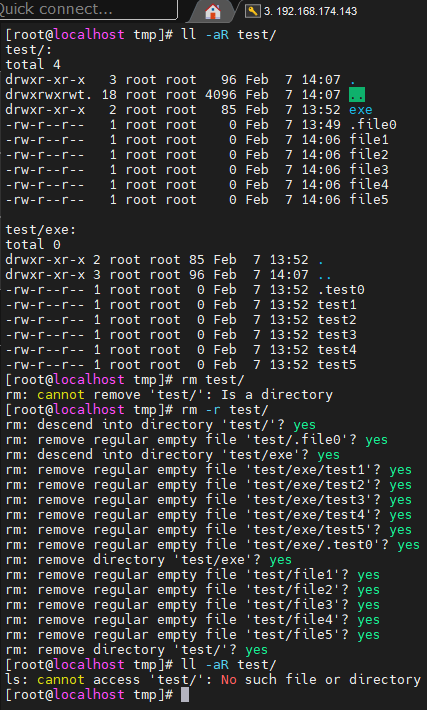
cd - : move to previous working directory but cd .. : move to one level up from the current working directory

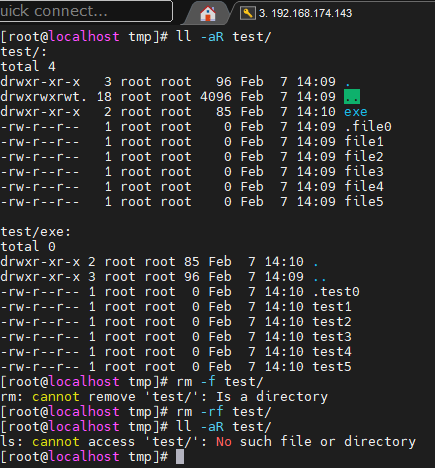


1. #rm commands –r and –f options meanings.

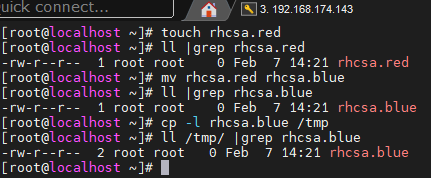
-f: ignore nonexistent files and arguments, never prompt

-r: remove directories and their contents recursively

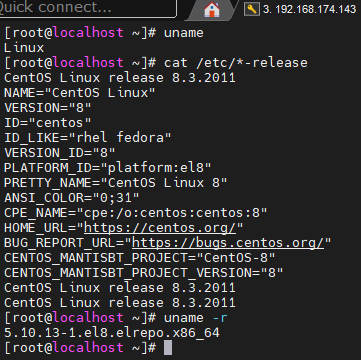




1. Create new file with name rhcsa.red under home directory of root user.
2. Now change name of file rhcsa.blue
3. Copy file to /tmp directory. Pay attention not to change files permissions while copying. Use cp commands one option to save permissions.



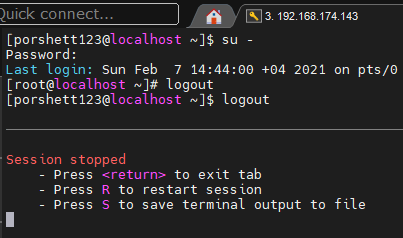
1. Show name of operating system which you are using.
2. Distro name?
3. Kernel version?



1. Write commnd which shows kernel version of linux.

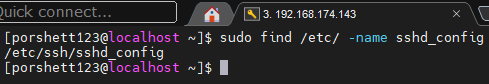
uname -r

1. How do you logout from current user in linux OS (in ssh terminal)

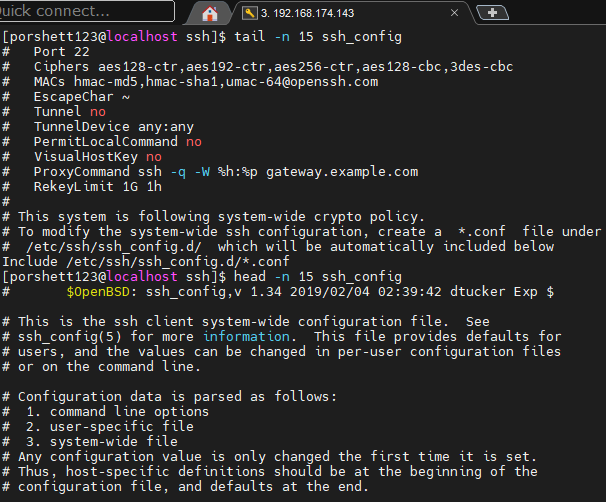


1. Using find command find sshd\_config file under /etc directory. Write down command.

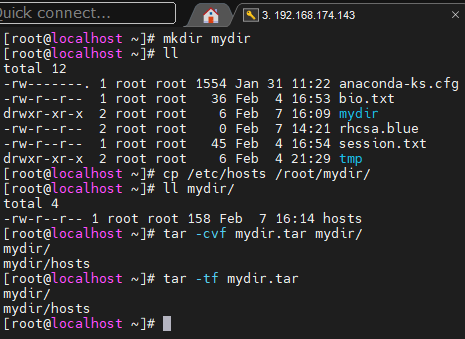
sudo find /etc/ -name sshd\_config



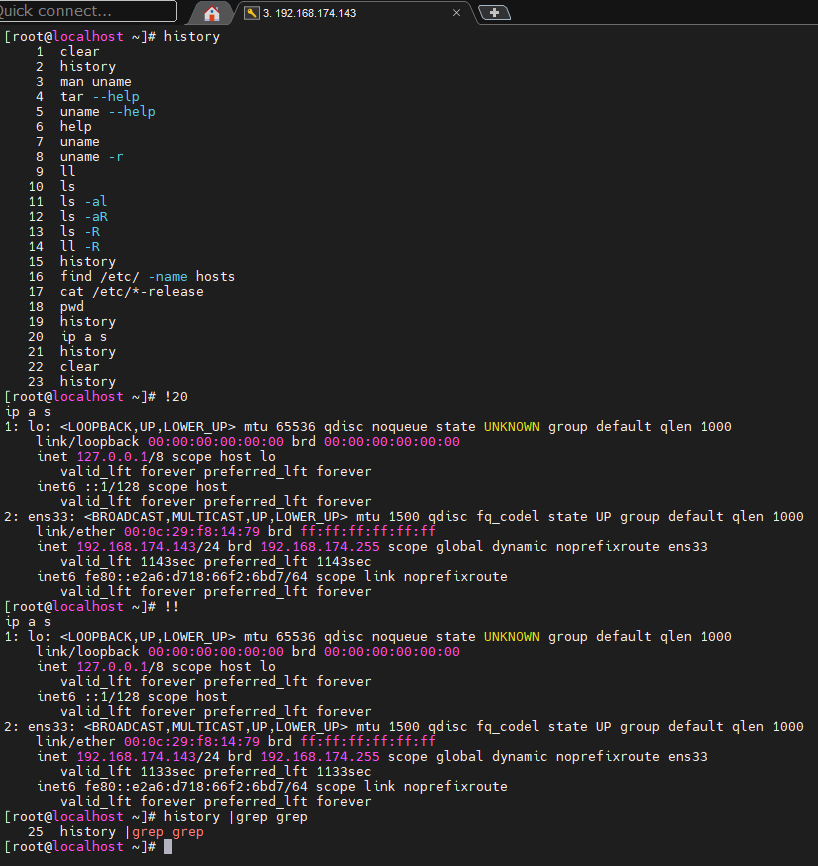
1. Using tail and head command write down 15th line of sshd\_config file.



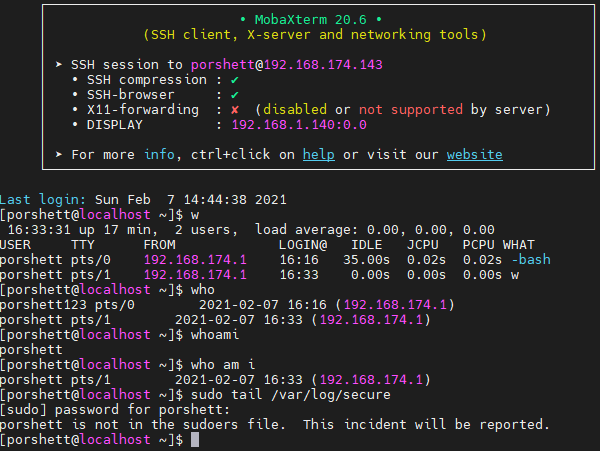
1. Cp /etc/hosts file to /root/mydir directory. (create mydir). Archive newly created folder and then show which content of new created tar file. (tar –t)



1. Run history command. 20th command run it again #!20
2. Run #!! Command what happened?
3. #history | grep grep --- what happened?



1. Connect to linux from windows with another ssh session using putty.
2. Run commands. #w , #who #whoami #who am i . Try to memorize different results.



1. Try to monitor /var/log/secure file with tail command while on another ssh(putty) session

