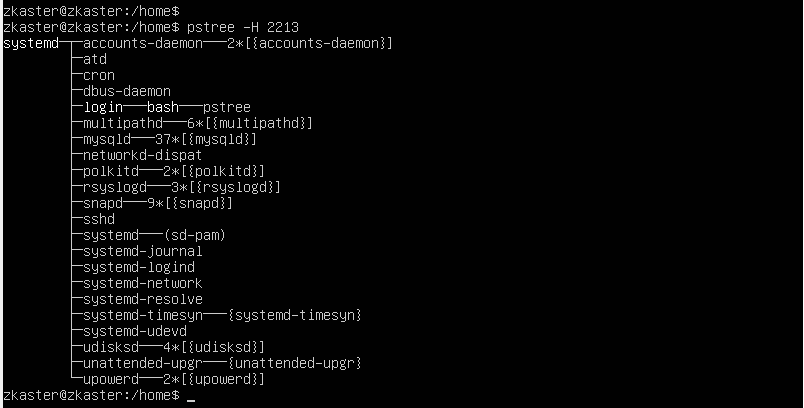
Task 3

# Part1

1. How many states could has a process in Linux?

* Running or Runnable (R)
* Uninterruptible Sleep (D)
* Interruptable Sleep (S)
* Stopped (T)
* Zombie (Z)

1. Examine the pstree command. Make output (highlight) the chain (ancestors) of the current process.



1. What is a proc file system?

The proc filesystem (procfs) is a special filesystem in Unix-like operating systems that presents information about processes and other system information in a hierarchical file-like structure, providing a more convenient and standardized method for dynamically accessing process data held in the kernel than traditional tracing methods or direct access to kernel memory. Typically, it is mapped to a mount point named /proc at boot time. The proc file system acts as an interface to internal data structures about running processes in the kernel. In Linux, it can also be used to obtain information about the kernel and to change certain kernel parameters at runtime (sysctl).

1. Print information about the processor (its type, supported technologies, etc.).

**lscpu**

or

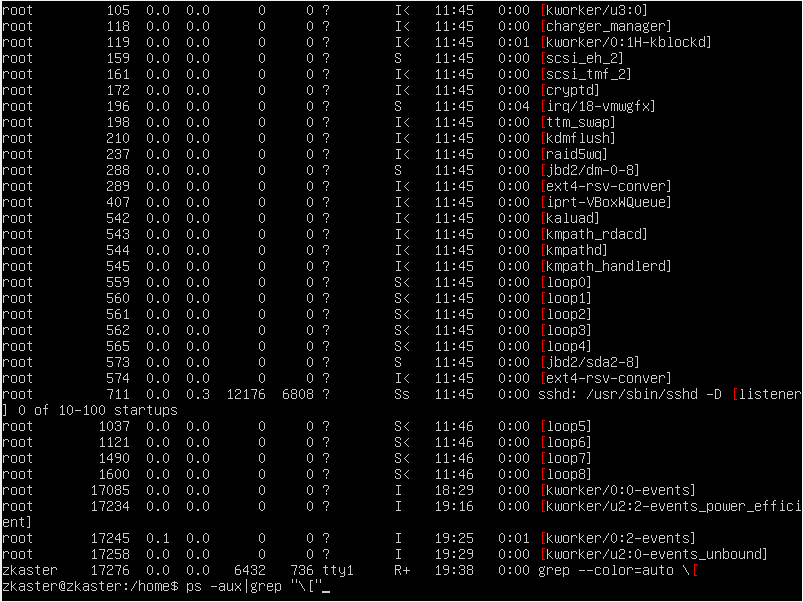
**cat /proc/cpuinfo**

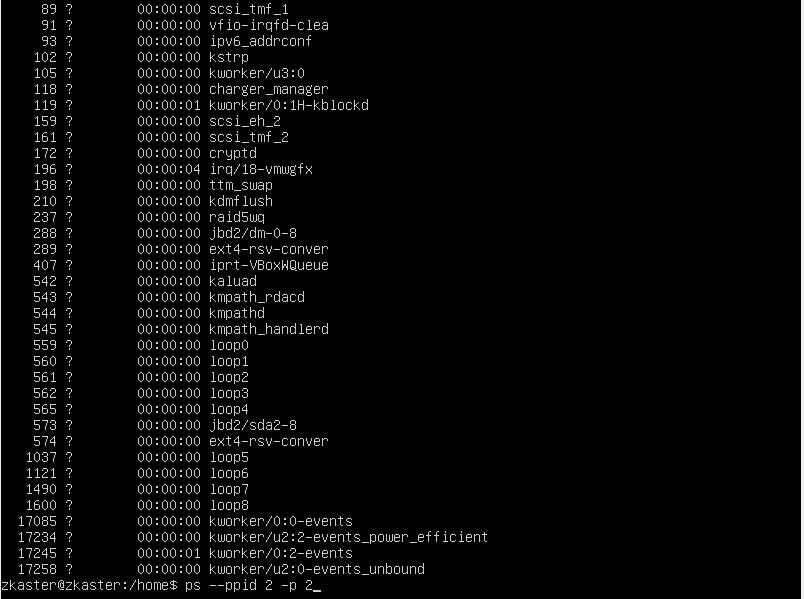
1. Use the ps command to get information about the process. The information should be as follows: the owner of the process, the arguments with which the process was launched for execution, the group owner of this process, etc.

**ps -au** or **ps -aux**

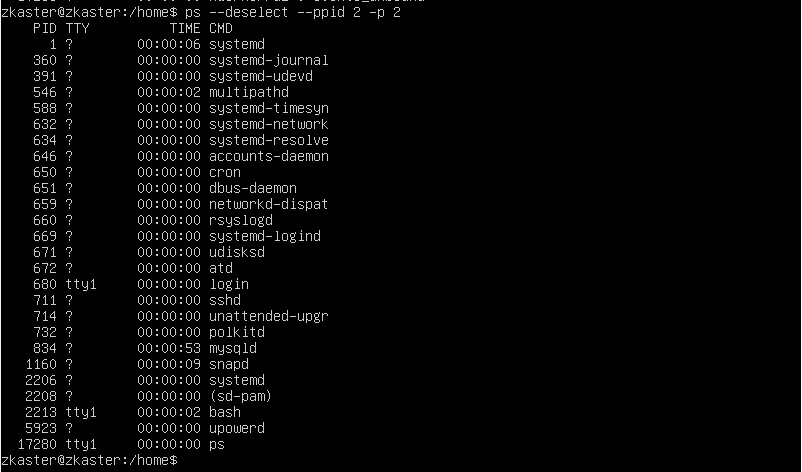
1. How to define kernel processes and user processes?

Kernel process showed with “[ …]”,



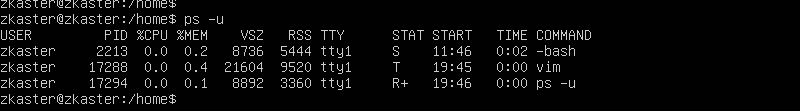


User processes



1. Print the list of processes to the terminal. Briefly describe the statuses of the processes.

What condition are they in, or can they be arriving in?

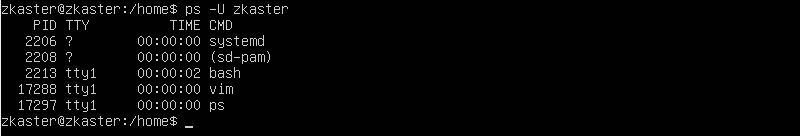


2213 – S-sleep

17288 – T-Stopped

17294 – R-Running

1. Display only the processes of a specific user.



1. What utilities can be used to analyze existing running tasks (by analyzing the help for the ps command)?

ps

ps -A or ps -e (all active)

ps -au or ps -aux (BSD like format)

ps – eF (more info)

ps -x (processes of current/active user)

ps -fU <RUID>

ps -fU <username>

ps -f <EUID>

ps -fG <groupname or groupRUID>

ps -fg <groupname or groupEUID>

ps -f -ppid <PPID> (PPID – parent process ID)

ps -ft tty2 (process by TTY)

ps -t pts/0 (process by TTY)

ps -e --forest

ps -C <name> (parent and children)

Other commands for active monitoring: htop, top, glances

1. What information does top command display?

top – is a real-time command, which shows used resources

11. Display the processes of the specific user using the top command.

top -u <username>

1. What interactive commands can be used to control the top command? Give a couple of examples.

After top started next command can be used:

M – memory sort

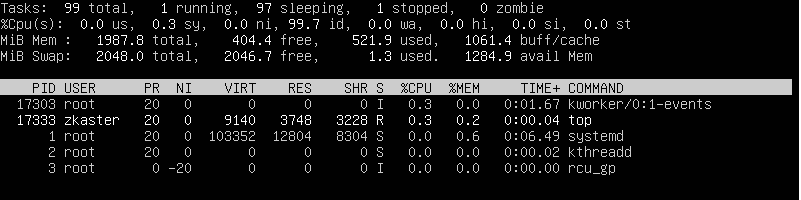
P – processor sort

u -user sort

n – number of displayed processes

z -highlight processes

1. Sort the contents of the processes window using various parameters (for example, the amount of processor time taken up, etc.)

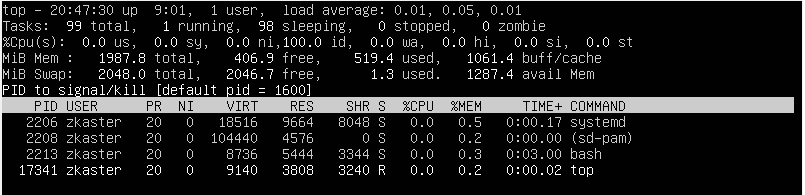


n=5

1. Concept of priority, what commands are used to set priority?

htop: when running press **r** to set up priority, chose proc number and set priority.

1. Can I change the priority of a process using the top command? If so, how? 16. Examine the kill command. How to send with the kill command process control signal? Give an example of commonly used signals.



9 - SIGKILL - terminate immediately/hard kill

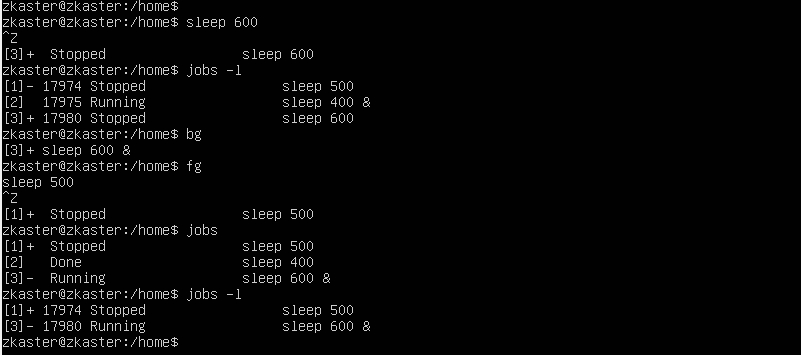
17,19,23 - SIGSTOP - to pause the process. “hold on”.

19,18,25 - SIGCONT - to continue the process. “pick up where you left off”

2 - SIGINT - interupt process stream, ctrl-C

15 - SIGTERM - terminate whenever/soft kill

16. Commands jobs, fg, bg, nohup. What are they for? Use the sleep, yes command to demonstrate the process control mechanism with fg, bg.



# Part2

1. Check the implementability of the most frequently used OPENSSH commands in the MS Windows operating system. (Description of the expected result of the commands + screenshots: command – result should be presented)
2. Implement basic SSH settings to increase the security of the client-server connection (at least

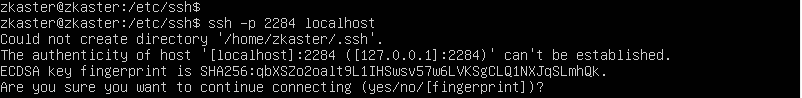
Copy default config: sudo cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.factory-defaults

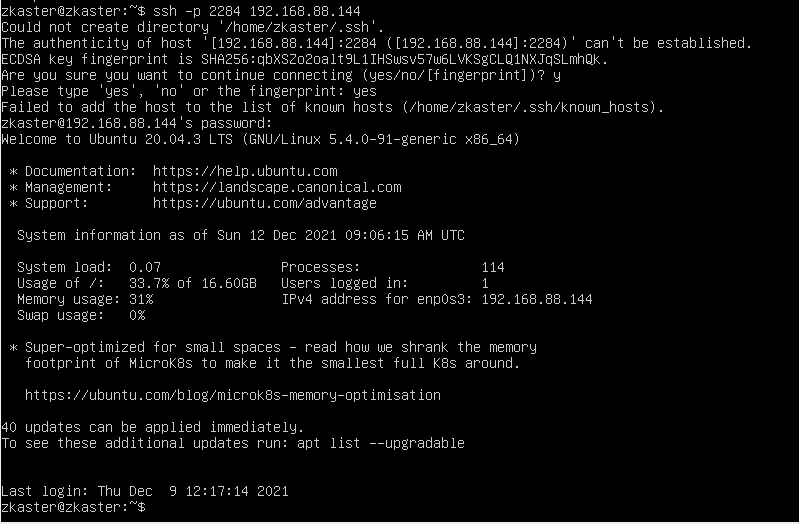
Change config : sudo nano /etc/ssh/sshd\_config

Change standart port : Port 2284

Activate auth by key : PubkeyAuthentication yes

Save changes  
Restart ssh server: sudo systemctl restart ssh



From other VM:  


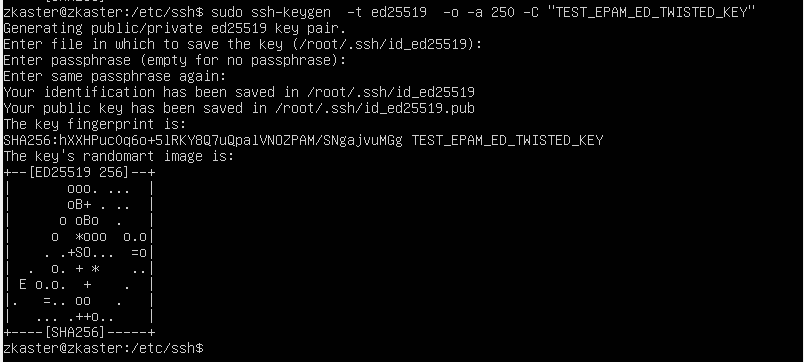
1. List the options for choosing keys for encryption in SSH. Implement 3 of them.

1)To generate RSA 2048 : sudo ssh-keygen -t rsa

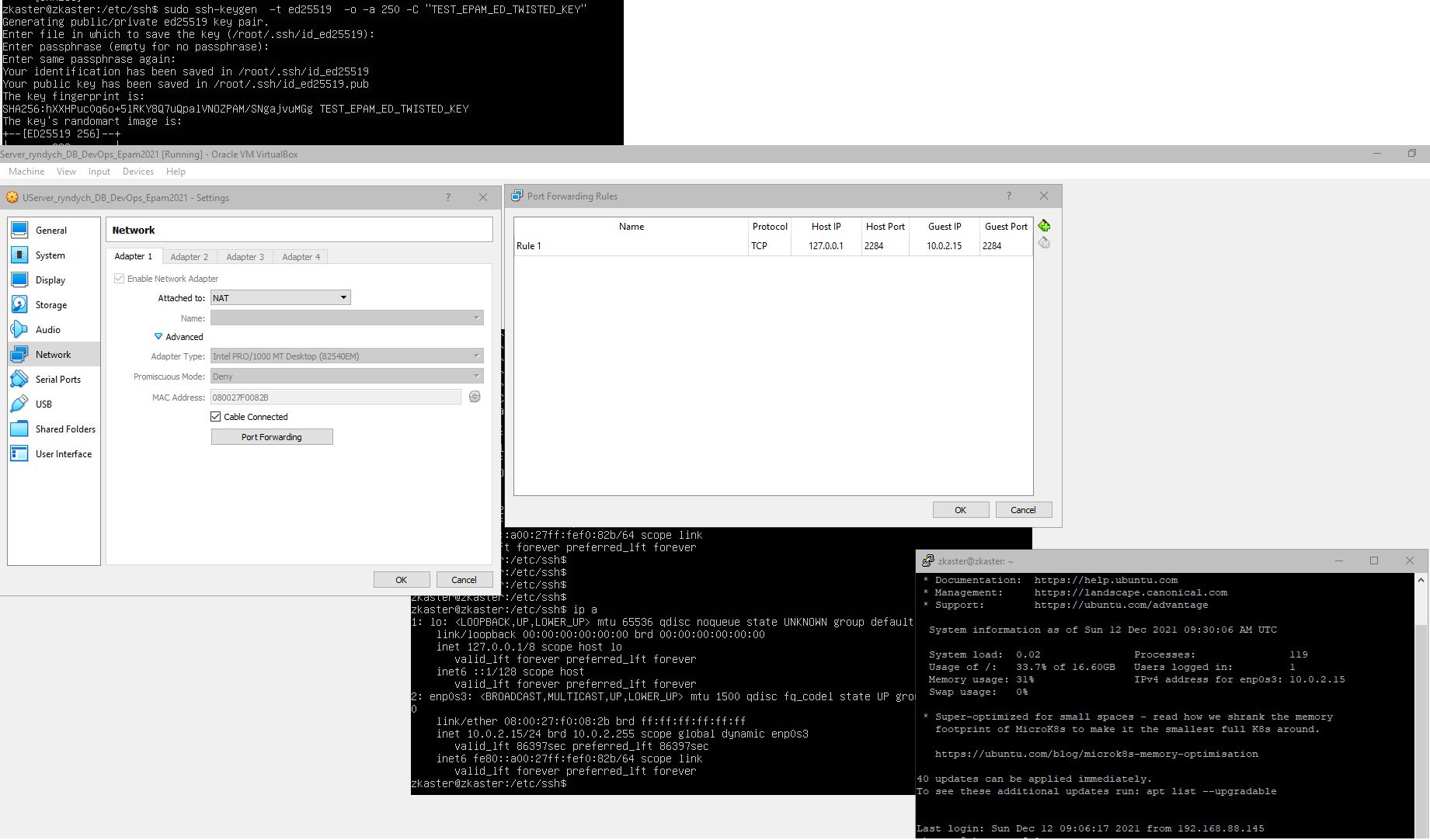
2)To generate RSA 4096 : ssh-keygen -t rsa -b 4096



3) Using the Edwards Twisted Curve algorithm



1. Implement port forwarding for the SSH client from the host machine to the guest Linux virtual machine behind NAT.



5\*. Intercept (capture) traffic (tcpdump, wireshark) while authorizing the remote client on the server using ssh, telnet, rlogin. Analyze the result.

ssh send encrypted password, telnet sends login and password as cleartext by 1 symbol. Login symbols send back, password symbols just to server. Rlogin also doesn’t use encryption.

