- What is the name and the UID of the administrator user?
    - root, 0
- How to list all files, including hidden ones, in a directory?
    - ls -a or find .
- What is the Unix/Linux command to remove a directory and its contents?
    - rm -R
- Which command will show you free/used memory? Does free memory exist on Linux?
    - free
    - Sure exists, but the Linux kernel creates file caches in ram, so when we see the output from free command, sometimes can show us that we are without memory but this memory is cached by the OS.
- How to search for the string "my konfi is the best" in files of a directory recursively?
    - grep -Rin "my konfi is the best" /folder
- How to connect to a remote server or what is SSH?
    - ssh user@server - simple way
    - SSH (secure shell) it's a cryptographic network protocol, used for remote login to computer systems by users.
- How to get all environment variables and how can you use them?
    - env, set or printenv, will show every variable that login session, we can use setting as variables ex.: TEST=something or using export the variable will be global (can be used by all system users)
- I get "command not found" when I run ifconfig -a. What can be wrong?
    - your PATH variable doesn't have the full path for the ifconfig command.
- What happens if I type TAB-TAB?
    - It depends which program the user is trying to complete
- What command will show the available disk space on the Unix/Linux system?
    - df -h
- What commands do you know that can be used to check DNS records?
    - dig +trace
    - nslookup
    - whois
    - host
- What Unix/Linux commands will alter a files ownership, files permissions?

    - chmod, chown, chattr
- What does chmod +x FILENAMEdo?
    - Add a execute permission to a file for all users
- What does the permission 0750 on a file mean?
    - Add a permission to the owner of the file write, execute and read, the group of the owner execute and read, and others do nothing
- What does the permission 0750 on a directory mean?
    - Add a permission to the owner of the folder, create, get access and list the directory files,for the group of the owner only enter and list the directory, and nothing for others.
    - +r - User can list the files
    - +w - User can create a file inside the directory
    - +x - User can get into the folder
- How to add a new system user without login permissions?
    - useradd username -s /bin/false
- How to add/remove a group from a user?
    - usermod -a -G groupname username #to add a user in a new group
    - usermod -G [all groups that you want the user into] username #You don't remove the user from a group, you add the user in all groups that this user is suppose to be.
    - newgrp - Updates shell session with new group permissions
- What is a bash alias?
    - It's a shortcut for some bash command
- How do you set the mail address of the root/a user?
    - creating a file called .forward in the user folder
    - editing the file /etc/aliases
- What does CTRL-c do?
    - send a SIGINT to the terminal (it's a polite kill)
- What is in /etc/services?
    - A mapping for services and ports, when a service call a function getportbyname() usually this function goes in this file to check.
    - Example the command netstat or ss without the -n parameter
- How to redirect STDOUT and STDERR in bash? (> /dev/null 2>&1)
    - 1> redirect the STDOUT

    - 1>> redirect the STDOUT in append mode
    - 2> redirect the STDERR
    - 2>> redirect the STDERR in append mode
    - &> redirect both STDERR and STDOUT
    - &>> redirect both STDERR and STDOUT in append mode
    - 2>&1 redirect STDERR to STDOUT
- What is the difference between UNIX and Linux.
    - Linux it's a UNIX "clone" using the same POSIX(Portable Operating System Interface) standards, but UNIX it's a brand, has different copyrights and tools.
- What is the diference between Telnet and SSH?
    - SSH it's encrypted and telnet isn't.
    - Telnet can ommit authentication
    - SSH adds overhead to the bandwidth
- Explain the three load averages and what do they indicate. What command can be used to view the load averages?
    - The three load averages indicate the processor usage estimated in 1 minute, estimated in 5 minutes and 15 minutes.
    - top or uptime
- Can you name a lower-case letter that is not a valid option for GNU ls?
    - z

####[⬆] Medium Linux Questions:

- What do the following commands do and how would you use them?
- tee
- copies the STDOUT to a file, but continues to show the STDOUT.
- awk
- awk it's a programming language designed for text processing.
- tr
    - tr or translate, it's a command to substitute characters.
- cut
    - cut is a command for text processing and extracts a portion of a text
- tac
- tac it's a reverse cat, pritting the file bottom to up.

- curl
- curl or cURL is a tool to transfer data from or to a server, using one of the supported protocols. cURL can be called a CLI browser, you can use to authenticate, change the HEADER, and do a lot of stuffs with it.
- wget
- wget is a tool for retrieving files using HTTP, HTTPS , or FTP.
- watch
- Watch it's a tool that runs a specified command repeatedly and displays the result on standard output.
- head
    - It's a command that shows the first lines of a file, the default it's 10 lines
- tail
    - It's a command that shows the last lines of a file, the default it's 10 lines
- What does an & after a command do?
    - Makes the command run in a background sub shell, and becomes a job.
- What does & disown after a command do?
    - disown control jobs that are running in the system, without any paramenter or ID removes the last job on the job table.
- What is a packet filter, and how does it work?
    - Packet filter it's the process of passing or blocking packets at a network interface based on source and destination address, port or protocols. The packet filter examines, the header of every packet who passed through and based in the rules, ACCEPT, DROP or REJECT the packet, it's well know as firewall.
- What is Virtual Memory?
    - Virtual memory it's the amount of memory available for the system, physical memory + swap memory (hard disk memory).
- What is swap and what is it used for?
    - Swap it's a disk partition used by the Linux when the physical memory is full, if the system needs more memory resources some inactive pages are copied to swap, it was a common way to increase the computer/server memory using the disk.
- What is an A record, an NS record, a PTR record, a CNAME record, an MX record?
    - A record stands for address, indicates an IP address for a domain
    - NS stands for Name Server record indicates which DNS server is authoritative for that domain (Where the actual DNS entries are)

    - CNAME stands for canonical name and servers to make one domain to another domain name.
    - MX stands for mail exchange, it's a list of mail exchange servers used by the domain.
- Are there any other RRs and what are they used for?
    - Yes.
    - PRT record stands for pointer record and maps an IPV4 address to a CNAME
    - SOA record stands for State of Authority and is easily one of the most important DNS records because stores information like when the domain was last updated.
    - SRV record stands for Service Record, is a record that specifies hostname and port number for a specific service, it can be used for service discovery.
    - TXT record stands for Text Information, used by various purposes, as domain ownership for example.
- What is a Split-Horizon DNS?
    - It's the feature/configuration of the DNS server answer a different resolution to a query based on the source of the query. A common use it's when the DNS server needs to diferentiate internal and external queries, for the same domain. We can use views to configure this.
- What is the sticky bit?
    - It's a permission bit that is set on a file or a directory that let only the owner of the file/directory or the root user to delete or rename the file.
- What does the immutable bit do to a file?
    - It makes the file immutable, any user can change the state of the file or create hard links.
- What is the difference between hardlinks and symlinks? What happens when you remove the source to a symlink/hardlink?
    - All files in the linux filesystem are a link to a inode, a hard link is a new link to the same inode (if you remove or rename the old or the new link, the file will be intact, but any change in the data on the inode is reflected in all files that refer to that inode), the file system will only delete the inode if you don't have any link for this inode. Because of this characteristic a hardlink only works on files that are in the same file system.
    - A softlink, it's a link that points the link from the inode, so it's a link from a link if the first link change the name or be deleted, the soft link will break, but can be used between differents filesystems.
- What is an inode and what fields are stored in an inode?
    - Each object in the filesystem is represented by a inode that stores all the information about the file, like file type, permissions, owner, group, file size, file access, change and modification time (never birth time), file deletion time, number of links,

extended attributes. Each inode has a unique number and it can acessed using stat filename

- How to force/trigger a file system check on next reboot?
    - Create a file named forcefsck in the root folder
- What is SNMP and what is it used for?
    - SNMP stands for simple network monitoring protocol, it's a protocol to monitor devices, works in the application layer, has 3 versions now, they are not compatible between each other, and V3 introduced encryption. Messages are transported via UDP.
- What is a runlevel and how to get the current runlevel?
    - Runlevel it's a preset operational system state, so based in this level, the OS starts the corresponding services, or scripts. To get the current runlevel uses the command runlevel, or who -r
- What is SSH port forwarding?
    - SSH Port forwarding it's a way to create a tunnel between your machine in a destination using ssh.
- What is the difference between local and remote port forwarding?
    - Local port forwarding creates a tunnel between a local server and a local client, a remote port uses a local server but with internet IP address to connect a internal service that doesn't have access in the internet.
- What are the steps to add a user to a system without using useradd/adduser?
    - Edit /etc/passwd with the new username, configure the home, and shell
    - Edit /etc/groups add this new username to some groups
    - Create the user home folder and set the right permissions
    - Reset the user password with passwd username
- What is MAJOR and MINOR numbers of special files?
    - The MAJOR number will set to the kernel with kind of device it is, and MINOR number will set a special characteristics of the device, example if a machine have 2 disks, the MAJOR number will be the same for both, but the MINOR doesn't.
- Describe the mknod command and when you'd use it.
    - mknod command creates a new device in /dev but actually udev creates automatically each device, if something very terrible happen we can recreate some devices using mknod to fix or make some backup.
- Describe a scenario when you get a "filesystem is full" error, but df shows there is free space.
    - When a filesystem it's out of inode, it can happen when you have a huge amount of small files, in a small filesystem. df -i will show.

- Describe a scenario when deleting a file, but 'df' not showing the space being freed.
    - when a process it's still appending that file. We can use lsof to check it.
- Describe how 'ps' works.
    - the ps command read files from /proc and the content of these files are generated by the kernel.
- What happens to a child process that dies and has no parent process to wait for it and what's bad about this?
    - creates a zombie process, one zombie process it's not a big problem, but each process uses a little size of ram, and uses a PID that's a finite number of it.
- Explain briefly each one of the process states and all signals
    - CREATED or NEW STATE, in this moment the process wait the admission to the ready state, by the scheduler
    - RUNNING/RUNNABLE (R) the process has been loaded into main memory and is awaiting execution by the CPU, or it's using CPU core right now
    - SLEEPING a sleeping process is a process waiting for a resource to be available, I/O operation to complete for example, or an event to happen. There is two states of SLEEPING process
        - Interrruptible Sleep (S) - Process that can be terminated before the wake up condition is fulfilled without any consequences.
        - Uninterruptible Sleep (D) - Process that can't be killed, in the example of I/O operation, the act the process it's in uniterruptible sleep (D) until a the I/O operation to complete and wake up.
    - STOPPED (T) - A process becomes stopped when it receives the SIGSTOP signal, when stopped the process execution is suspended and only signals it will handle are SIGKILL and SIGCONT
    - Zombie (Z) it's a state after completing the execution or being explicitly killed, but the process remains as a zombie until the parent process call the wait system call to read its exit status, and finally ending the process lifetime.
    - Process SIGNALS are one of the ways process communicate among themselves and with the kernel. Exceptionally SIGKILL and SIGSTOP signals cannot be handled or blocked.
        - SIGTERM - the default signal sent by kill command, Asks the process to terminate voluntarily
        - SIGKILL - unlike SIGTERM, forces the process to terminate, can't be blocked or handled
        - SIGSTOP - suspend the process execution, putting in stopped state. In this state, the process will do nothing but accept SIGKILL or SIGCONT.

        - SIGSTP - almost identical to SIGSTOP, the only difference is it can be blocked or handled, this is the signal sent when you type <ctrl>+z in the terminal
        - SIGCONT - if a process is in stopped state, it will put it back in the RUNNING/RUNNABLE state and resume it execution. If the process is in any other state, it's silently ignored.
        - SIGINT - generated when the user type <ctrl>+c in the terminal, it interrupts the current command processing and wait for user's next command.
        - SIGQUIT - generated when eht user type <ctrl>+\ in the terminal, normally it will force the process to produce a core dump and terminate.
        - SIGALARM - signal used to wake up sleeping process, normally scheduled by alarm system call.
        - SIGCHLD - sinal send from a child process to its parent process when its state changes.
        - SIGHUP - the signal indicates the terminal handling the process has been disconnected and/or parent process terminated. To run a process that won't terminate when the terminal disconnects, you can start it using the command nohup.
- How to know which process listens on a specific port?
    - lsof -i :$PORT or netstat -lp | grep $port or ss -lp | grep $port
- What is a zombie process and what could be the cause of it?
    - A zombie process is a process whose execution is completed but it still has an entry in the process table. Zombie process usually occurs for child process, as the parent process still needs to read its child exit status.
- You run a bash script and you want to see its output on your terminal and save it to a file at the same time. How could you do it?
- Use the tee command
- script | tee file
- Explain what echo "1" > /proc/sys/net/ipv4/ip_forward does.
- Disable ipv4 ip_forward function from the kernel, as well the IPV4 routing function
- Describe briefly the steps you need to take in order to create and install a valid certificate for the site https://foo.example.com.
    - Create a key file
    - Uses this key file to create a csr file
    - Send this csr file to a ssl certificate provider
    - Get the crt from the certificate provider with the CA chain and configure into the webserver

    - Or you can use certbot to simplify.
- Can you have several HTTPS virtual hosts sharing the same IP?
    - Yes using virtualhosts, but the client needs to support http/1.1, to use name-based virtual host configuration.
- What is a wildcard certificate?
    - It's a certificate that can be used by differents hostnames from a single domain.
- Which Linux file types do you know?
    - Regular file
    - Directory file
    - Special files
        - Block file
        - character file
        - named pipe file
        - symbolic link file
        - socket file
- What is the difference between a process and a thread? And parent and child processes after a fork system call?
    - A fork it's an identical process as the parent but with new PID, it has a own memory share, and runs independently from the parent. A thread it's a lightweight process and usually it's just a CPU state with the process containing the remainings. A threads require less overhead then forking or spawning a new process, because doesn't have a new system virtual memory space and environment.
    - Both child and parent process have different PIDs, neither process access the variables of each other, the child process ctime, uptime, stime, cutime and cstime subrotines are set to 0.
- What is the difference between exec and fork?
    - A fork in a simple way, it's a process copy only changing the pid and resource limits, a exec it's a call that basically replaces the entire current process with a new program. It loads the program into the current process space and runs it from the entry point. Example, when we call the find command, our bash forks itself, and in this new fork context, uses exec call to execute the find program.
- What is "nohup" used for?
    - It's used to create process that are independent from user login, starting a process with nohup it's telling the process to ignore SIGHUP calls, that the signal sent by the kernel when the parent shell is closed.
- What is the difference between these two commands?

- myvar=hello
- export myvar=hello
- The first one create the variable only in the user context, the second in a global context, so this variable can be used by all users.
- How many NTP servers would you configure in your local ntp.conf?
    - 4 it's minimum recommended by RedHat
- What does the column 'reach' mean in ntpq -p output?
    - It's a octal number, that show the last 8 transactions with the ntp server, this number is a FIFO log, so if the same packet doesn't arrive (it's UDP), this number can be different based in the order of the checks.
- You need to upgrade kernel at 100-1000 servers, how you would do this?
    - I would be using Ansible, but before I would test in a controled group to check if something bad can happen.
- How can you get Host, Channel, ID, LUN of SCSI disk?
    - cat /proc/scsi/scsi
- How can you limit process memory usage?
    - Calling the program with limit command, or set the ulimit in the console, or in the /etc/security/limits.d, or in the systemd init script.
- What is bash quick substitution/caret replace(^x^y)?
    - sed -e 's/^x/^y/g'
- Do you know of any alternative shells? If so, have you used any?
    - I use zsh, it's 100% bash compatible
- What is a tarpipe (or, how would you go about copying everything, including hardlinks and special files, from one server to another)?
    - It's a way to copy a directory to a server from another preserving permissions and the files, usually I don't copy files from a server to another, I use automation to do the job to recreate the server for me, but if I really need to copy, we could use a tarpipe, or dd.