- What is a tunnel and how you can bypass a http proxy?
    - We can create a ssh tunnel with ssh -R and redirect the http proxy to a server that has access to the internet.
- What is the difference between IDS and IPS?
    - IDS detect the problem inspecting the packet header and payload and creates a log.
    - IPS detect the problem inspecting the packet header and payload and drops the packet if finds something problematic, based in some pre defined rules.
- What shortcuts do you use on a regular basis?
    - ai package - sudo apt install package
    - ll - ls -lha
    - gitcm - git commit -m
    - gl - git pull
    - gp - git push
    - .. - cd ..
    - ... - cd ../..
    - .... - cd ../../../
- What is the Linux Standard Base?
    - It's a joint project projected by several Linux distributions under the organizational structure of the Linux Foundation to standardize the sofware system structure, including filesystem hierarchy.
- What is an atomic operation?
    - Atomic operations are program operations that run until completion independently from any other process.
- Your freshly configured HTTP server is not running after a restart, what can you do?
    - I would try to see the logs and check what's the problem. jounalctl -xe systemctl status httpd
- What kind of keys are in ~/.ssh/authorized_keys and what it is this file used for?
    - Public keys, they are used to authenticate users in the server.
- I've added my public ssh key into authorized_keys but I'm still getting a password prompt, what can be wrong?
    - The permission for authorized_keys file, and .ssh folder, as the path from authorized_keys file needs to be /home/user/.ssh/authorized_keys and right spelled, or your private key has the wrong permission.
- Did you ever create RPM's, DEB's or solaris pkg's?

    - yes using fpm, and using dpkg or rpm.
- What does :(){ :|:& };: do on your system?
    - creates a forkbomb
- How do you catch a Linux signal on a script?
    - using the command trap inside the script
- Can you catch a SIGKILL?
    - No, by security proposes
- What's happening when the Linux kernel is starting the OOM killer and how does it choose which process to kill first?
    - OOM will kill the process that will free more memory and the least important for the OS.
- Describe the linux boot process with as much detail as possible, starting from when the system is powered on and ending when you get a prompt.
    - BIOS/UEFI
        - BIOS performs startup based in the hardware, POST (Power On Self Test) processs to initiallize the hardware, after complete, and calls the bootloader.
    - bootloader
        - The bootloader (GRUB2) present options to the user select, GRUB supports unix-like OS, and chain-load Windows OS, and loads the kernel into memory and supplies it with some parameters.
    - kernel
        - The kernel will decompress itself and will setup essential hardware and memory paging, and calls start_kernel() function, and it will perform the majority of system setups like device and driver initialization, scheduler, idle process and then starts separately in the user space the init process (pid 1).
    - init -The init it's scripts executed by shell (sysV, runit) or configuration files that are executed by binaries (upstart, systemd), init has specific levels, that are passed as variables at the call, with consists of specifics set of daemons. These will provide various non-operating system services and structures and form the user environment.
    - User environment
        - The typical desktop environment begins with a daemon that calls everything needed. To shutdown, it's the inverse, the kernel kills every process, and shutdown.
- What's a chroot jail?
    - Chroot jail it's a way to isolate a process and its children from the rest of the system. The idea is that you create a directory tree where you copy or link in all the system

files needed for a process to run, usually we use bind to mount some folder inside a chroot.

- When trying to umount a directory it says it's busy, how to find out which PID holds the directory?
    - lsof directory
- What's LD_PRELOAD and when it's used?
    - LD_PRELOAD it's a variable that can be used to load some library before the default C library, can be used to test a new version for a library, or for development proposes.
- You ran a binary and nothing happened. How would you debug this?
    - strace binary, and see what's happening.
- What are cgroups? Can you specify a scenario where you could use them?
    - Cgroups are a Linux kernel feature that allow limit the resource use for a group of process(CPU, memory, disk I/O). A scenario to use could be to test a software in a physical machine that has a big hardware, and make this software run a minimum configuration, a very common sofware that uses cgroups it's in containners (docker, crio).