1. Study the following situations. In each of them, which of the main security objectives are probably not fulfilled?
    a. You have selected your favourite red filament for 3D printing in an e-shop, now entering your payment data and receiving an error message: "The transaction could not be completed, your bank is not responding, try later". Confidentiality
    b. You are sitting at a conference, listening to presentations of other researchers in the area you are keen on. You see one of them explaining your breakthrough ideas you never shared with anyone except that you have submitted them with a recent EU project proposal that happened to be rejected. Confidentiality and integrity
    c. Yesterday, you have completed the design of your new 3D model with Tinkercad. When you have logged into Tinkercad today, you found your model to be modified for unknown reasons. Integrity

2. An employee in the bank has been preparing 10 years for this beautiful day. The plan was perfect. Some large sum of money has been forgotten on some unused account- probably of a victim of a mafia war. Now they are safely moved to his private account in Belize. Unfortunately, a day after, the police knock on the door. You know why because you have programmed the information system for this bank. Which property does it have?
    - Non-repudiation property -> evidence that they transferred money from an unused account to private one.

3. System calls are a typical example of a weak point of operating systems. They can be used by an adversary to take control over otherwise protected parts of memory, hardware, or other resources. It can be done, because an adversary program can offer a substitute routine to be called when user programs trap to system calls. Your comments.
    - System calls are potential weak point in OS-> they can be exploited by adversaries to gain control over protected resources-> significant security risk

4. Under linux, a user sometimes cannot hear anything when playing music with his favorite music player (mplayer program) even though it has speakers connected and volume up. This can happen for instance when that user is not member of the audio user group. We give him this privilege by adding him to that group. Fill in the following generic concepts with entities for this particular situation:
    a. Principal -> the user who needs access to the audio functionality (ex. “John Doe”)
    b. Agent -> administrative command or action that adds “John Doe” to “audio” user group.
    c. Object -> “audio” user group, resource that “John Doe” needs access to in order to use audio functionality
    d. Credential -> privileges associated with the “audio” user group (OS checks begore gaining access to audio resources)

5. A citizen who was banned from getting certain kind of permission from regulators notices that when the clerk in the office gives this permission to others, they always use certain URL address in this format: https://permission-server.gov/give_permission?personal_id=####&type_of_permission=#### Therefore he tried to enter this URL to his web browser with his personal_id, and the type of permission that he would like to have, but does not. Fortunately, it did not work out, because systems obey one of the core security principles? Which one?
    - principle of least privilege (users and processes should only be given the minimum levels of access and permissions necessary to perform their tasks)

6. What is the purpose of salt in hashing passwords process on a typical Linux system?
    - Linux systems can improve overall security and confidentiality of user credentials.

7. Provide 6 (in total) meaningful, useful, true and informative sentences about *advantages and/or disadvantages* of the three authentication methods:
    a. by what you know:
        - +: easily remembered and cheap passwords to implement, quick and easy authentication for users

- -: Easy to guess password, dictionary attacks and social engineering, weak or reused passwords

b. by what you have:
   - +: additional security (not only usernames and passwords), physical tokens
   - -: impractical to use physical tokens-> can be lost or stolen

c. by what you are:
   - +: fingerprints, iris patterns, faceid, difficult to replicate
   - -: cannot be changed like passwords or tokens, harder to use on multiple devices

8. When a user is logging in to a Linux desktop system on a text terminal, it sees the login: prompt first. After the user provides his username and password, the login process that runs with superuser privileges verifies the entered hashed password against a hashed password stored in /etc/shadow file. If they match, it forks a new process, changes the owner of that process to the user that is just logging in and starts a login shell as specified in /etc/passwd file. Your comments.
   - Most important part is proper authentication and access control in the OS. If it is done correctly, it ensures the security and integrity of the system

9. Why do we typically start a webserver as some user and not as a root?
   - If webserver would have full root privileges, some system-wide damage or unauthorised changes could occur

10. Somebody wanted to enter a hairdresser during pandemic and pulled out her covid-pass so that they let her in. Will her entry permission be based on capabilities or on access control list? Explain why.
    - Based on capabilities-> capabilities work like key in a lock
    - Covid-pass-> capability that grants permission for entry based on certain criteria (test results, vaccination)

11. What is the relation between SSL and TLS and between HTTPS and SSL?
    - SSL (Secure Socket Layer) and TLS (Transport Layer Security):

    - SSL: cryptographic protection to communications between processes in modern systems
    - TSL: more secure and updated version of SSL, standard method for providing secure communication over a network
- HTTPS (Hypertext Transfer Protocol Secure) and SSL:
    - HTTPS: protocol that supports WWW, takes existing HTTP and connects it to SSL or TLS-> ensuring that sensitive information transmitted over the web is protected from potential security threads

12. What are the different ways to authenticate when using SSH?
    - Password-based, public-key, A. servers (f.ex Kerberos)

13. A process P on a typical Linux system opens a file F, then reads from it 3 times, and finally closes it. Which of the following was used:
    a. Capabilities
    b. ACL

14. Suppose you have a family bakery, and different people are working there: bakers, juniors, cleaning staff and others. Juniors have access to the flour, while bakers can get into the cabinet that contains hereditary recipes. In a corona crisis, some bakers were ill and trustful juniors temporarily received the privileges of the bakers until they could return. How is this access control method called and what basic security principle does this preserve?
    - Role-based access control (RBAC) and basic security principle of least privilege

15. Can a similar access control be achieved somehow in Linux system? Using which technique and how does it work?
    - It can, by Access Control Lists and groups-> feature: privilege escalation-> allows small extensions of privileges

16. What command on Linux could we use to start a process under a different user?
    - sudo -u <username> <command>

17. You have installed some new program on your mobile phone and it asks you to let it use your microphone. What data structure will hold the decision of your approval?
    - Permissions label

18. A browser is accessing a webserver that is providing the content in encrypted form to increase security. Why does the server need a certificate?
    - the server needs a certificate to authenticate its identity, establish a secure encrypted connection, ensure data integrity, and build trust with the client browser

19. How can that webserver obtain such certificate?
    - Generate certificate signing request (CSR)
    - submit the CSR to Certificate authority (CA)
    - validation process
    - certificate insurance
    - installation on the web server

20. Suppose an adversary would like to cheat the web browser by recording a traffic between the webserver and the browser first and then reusing this recorded communication to modify the content of the following communication. How is such a wrongdoing called? What is done to prevent it?
    - “man-in-the-middle attack”
    - The adversary positions themselves between the client and server intercepts the communication and can alter the data being exchanged
    - We can take some measures:
        - Encrypt the communication between the client and server
        - Certificate validation-> client can detect unauthorised or forget certificates
        - A framework for secure communication by using digital certificates and public private key pairs
        - SSL/ TLS->secure communication channels by encrypting data and ensuring data integrity

21. you have files A, B, C and users X, Y, Z, W. You would like to give read and write access to these files to the users as follows (other users should not have it):

file	users to have read access	users who have write access
A	X Y	X W
B	X Z	Y X
C	Y Z	Z W

Can this be done in traditional 9-bit POSIX-like access control? If yes, how, if not why?

- It cannot be done, because the access control requirements involve specific combinations of users having read and write access to each file which cannot be directly achieved with traditional POSIX model

22. One of the customers of a system you developed has ordered a Christmas tree to be brought right to his door using that system. Now he is refusing to pay for it, claiming he has not placed the order. However, you are 100% sure that he did that and you can provide a proof. It means that your system has the following property: (fill in)
    - Non-repudiation

23. You have opened your program and commented-out lines 10-20 in it. Then you saved it, compiled it, and run it, surprisingly finding out that the program still executes those instructions at lines 10-20. You open the file and you see the lines are NOT commented-out. Which property is the system you are using lacking? (fill in)
    - Integrity property

24. A teacher has developed a special program to tacitly subscribe students to his elective course that nobody wanted to register for. Somehow he managed to start and keep that program running on a student computer, waiting until the student will have logged in to AIS. After that his program would just issue a few needed requests to AIS and the student would be silently registered. If this was possible, which core security principle was not obeyed by such AIS?
    - Authorization

25. Under Linux, when you are trying to send a program to Arduino over serial cable, you run into a difficulty- you are missing the rights to file /dev/ttyUSB0 or similar. When we give a user this right, fill in the following generic concepts with entities in this situation:
    a. Principal-> user
    b. Agent->program / tool
    c. Object-> file /dev/ttyUSB0 or serial port
    d. Credential-> permissions or rights
26. Why does an experienced attacker who has stolen password file from a machine you use, and who wants to guess your password has an easier job if the "salt" is not used?
    - By not using a salt when hashing passwords, the security of the passwords is weakened, making it easier for attackers to guess passwords through various techniques like dictionary attacks, rainbow table lookups, and identifying common passwords across multiple users. Salting passwords adds randomness and uniqueness to each hashed password, making it significantly harder for attackers to crack passwords even if they have access to the hashed passwords

27. When a user is logging in to a Linux desktop system on a text terminal, it sees the login: prompt first. After the user provides his username and password, the login process changes its own user to the provided one so that it can read and verify the hashed password from a file, which is stored in an area that is readable only to that user. Your comments.
    - the process of changing the user to the provided one during login in a Linux system enhances security by ensuring secure access to hashed password files, following the principle of least privilege, isolating user data, and facilitating the authentication verification process

28. What is the main advantage and main disadvantage of using capabilities instead of ACL?
    - +: Fine-grained control and flexibility in managing access to resources
    - -: they require careful design and handling to ensure that the right set if privileges is assigned to each process or entry

29. Capabilities allow both mandatory and discretionary access control, whereas ACL allow only mandatory. True?
    - False-> it depends on specific security requirements and policies of the system

30. Suppose you have a family bakery, and different people are working there: bakers, juniors, cleaning staff and others. Juniors have access to the flour, while bakers can get into the cabinet that contains hereditary recipes. In a corona crisis, some bakers were ill and trustful juniors temporarily received the privileges of the bakers until they could return. How is this access control method called and what basic security principle does this preserve?
    - Role-based access control, principle of least privilege