CIS 418/518 – Secure Software Engineering
Linux Security Basics (Chapter 1)

1. The following is an entry inside the `/etc/passwd` file. What is the user ID (numeric) of the user `bob`?

   ```
   bob:x:2000:3000:SEED,,,:/home/bob:/bin/bash
   ```

   `User ID of bob: 2000`

2. What is the root user's user ID? The root user has special privileges than normal user. Is it because its username is root?

   0 The user ID, not the username, of an account determines its privileges.

3. Which of these files contains user account details? **`/etc/passwd`** `/etc/shadow`

4. Which of these files contains user password details? `/etc/passwd` **`/etc/shadow`**

5. Which of these files is readable to all? **`/etc/passwd`** `/etc/shadow`

6. Which Linux command(s) can be used to see what groups a user belongs to?

   ```
   $ id
   $ groups
   ```

7. In Linux, which file stores all the groups and their members? **`/etc/group`**

8. In systems, resources need to be protected so only authorized users can access them. What are the four common access control methods?
   - **Permission-based (rwx) access control**
   - **Access Control Lists (ACLs)**
   - **Capability-base access control**
   - **Role-based access control**

9. Alice belongs to the `abc` group. What permission does Alice have on file `xyz`?

   ```
   -rwxr--r-- seed abc 1802 Feb 6 11:39 xyz
   ```

   Alice has only read access to file xyz

10. What will be the file `xyz`'s permissions after running the following command?

    ```
    $ chmod 543 xyz
    ```

```
owner:  r-r
group:  r--
others: -wx
```

11. If the system's default initial permission for a non-executable file is 666 and the *umask* value is 0427, what will be the final permissions of this file?

Default initial file permission: 0666	`110 110 110`
umask value: 0427	`100 010 111`
Final file permission with *umask* 0427:	`010 100 000 (-w-,r--,---)`

12. The account `bob` is a normal user account. The root user wants to grant bob the power to run commands using the superuser privilege, but without giving bob the password of the root account. How can the root user achieve this?

    Add account bob to the sudo group.

13. Assume we are allowed to run commands using the superuser privilege (via `sudo`). List ways we can get a root shell to launch. After getting a root shell, what do you expect the `id` command to show for UID?

    You can use one of the following commands to get a root shell:

    ```
    $ sudo -s
    $ sudo bash
    $ sudo su
    ```

    The `id` command will show 0 for UID.

14. What is the purpose of the salt in the `/etc/shadow` file?

    It prevents two users with the same password from having duplicate entries in the shadow file.

15. The `/etc/passwd` file is called password file, but in reality, it does not contain account passwords. Explain why?

    Since the `/etc/passwd` file is world-readable, the password details are kept in `/etc/shadow` file.

16. What is the meaning of "execute" permission on directories?

    "execute" permission allows a user to "cd" into the directory.