Linux Security Basics

S1.1. 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
```

S1.2. What is the root user's user ID? Why does root have special privilege than normal user? Is it because its user name is root?

S1.3. Alice belongs to the abc group. What permission does Alice have on the following file?

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

S1.4. What will be the file xyz's permission after running the following command?

```
$ chmod 543 xyz
```

S1.5. If the umask value is 0427, when we create a non-executable file, what will be its permission?

S1.6. 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?

S1.7. We are allowed to run commands using the superuser privilege (via sudo). How do we get a root shell?

S1.8. By exploiting a vulnerability in the system, an attacker gets a chance to modify any arbitrary file in the system. What file can the attacker modify, such that after modifying the file, the attacker can gain the root privilege on the system. Please name two files. Assume that the attacker has a normal-user account on the system.

S1.9. What are the main objectives of the POSIX capabilities?

S1.10. We run the following sequence of commands. What are the results at ① and ②?

```
$ cp /usr/bin/cat mycat
$ mycat /etc/shadow       ①
$ sudo setcap CAP_DAC_READ_SEARCH=ep mycat
$ mycat /etc/shadow       ②
```

S1.11. The /etc/passwd file is called password file, but in reality, it does not contain account passwords. Please explain why?

S1.12. What is the purpose of the salt in the shadow file?