Section 5 – Users Access Control

Questions

Please read the following questions carefully and try to answer them. You can find the correct answers, with an explanation where necessary, in the Answers.pdf file located in the same folder.

1. Group membership permissions can be applied to processes the same way they are applied to files and directories
    a. True
    b. False
2. The filesystem recognizes user and groups by their names rather than their UID and GID numbers
    a. True
    b. False
3. The real account UID/GID is what is used to grant the user/group non-elevated permissions on files and directories
    a. True
    b. False
4. The effect account UID/GID is the same as the real UID/GID even if in elevated mode:
    a. True
    b. False
5. The login process has the UID of 0 and it can change its own UID to the logged-user's, but this process in non-reversible
    a. True
    b. False
6. A strong password should have the following properties (choose all that apply):
    a. More than 8 characters long
    b. Contains numbers and symbols
    c. Contains upper and lower caps letters
    d. Easy to remember
7. A passphrase should be unpredictable to anyone other than you
    a. True
    b. False
8. Why isn't it a good idea to directly SSH login to a system as root? (choose all that apply):
    a. There'll be no user accountability
    b. You make it one step easier for intruders to attack the system
    c. It'd be difficult to trace changes that happened through the root account with the absence of logs
    d. There is no need to use root most of the time
9. The su – command will let you change your login to another user's account (or root), provided that you have the password. But using su – will also load the user's environment variables
    a. True

    b. False
10. You can edit /etc/sudoers with vi or emacs, and it's a good idea
    a. True
    b. False
11. The default number of minutes through which sudo will not ask the user again to enter the password for subsequent commands is:
    a. 10 minutes
    b. 5 minutes
    c. 1 minute
    d. 30 seconds
12. An /etc/sudoers file can be shared among many machines
    a. True
    b. False
13. How can you mitigate the risk of allowing the user to use programs that can spawn applications on their own (like vi, and less)?
    a. Restrict access to those commands
    b. Disable the user's login shell
    c. Add NOEXEC switch before the command
    d. Try to change the source code of those programs to make them reject spawning a shell
14. The system account have UID's that are generally under 100
    a. True
    b. False
15. To create a system account, you have to ensure the following (choose all that apply):
    a. The account shell is set to /bin/false or /sbin/nologin
    b. The account UID is less than 100
    c. It does not have a home directory
    d. It does not have a friendly name