Section 8 – User Management

Questions

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

1. A login name can be duplicated in a Linux system
   a. True
   b. False
2. The following character can be put in a login name:
   a. –
   b. :
   c. ;
   d. .
3. The maximum number of character allowed for a user name in Linux is:
   a. 8
   b. 10
   c. 20
   d. 32
4. You can use capitals letters in a login name:
   a. True
   b. False
5. Encrypted passwords are stored by default in /etc/passwd file
   a. True
   b. False
6. You can set the password hashing (encryption) algorithm using the following file:
   a. /etc/passwd
   b. /etc/shadow
   c. /etc/default/useradd
   d. /etc/login.defs
7. What happens if the x placeholder was left empty in the /etc/passwd file?
   a. Users will not be able to login to the system
   b. Users will be able to login to the system without entering passwords
   c. User accounts will get locked
   d. Users will login normally by entering the correct passwords, as passwords are read from the /etc/shadow file
8. If more than one user chose the same password, that does not mean that you'll find identical password strings in /etc/shadow file
   a. True
   b. False
9. Multiple user id's (UID) are allowed in Linux
   a. True

b. False

10. The GECOS field can hold the account real name only

    a. True
    b. False

11. c

12. b

    Although chsh can be used to change the login shell, the executable must be in the /etc/shells file. So users are confined by the number of shells available in this file

13. b

14. b

15. a,c, and d

16. a

17. b

    However, .profile gets executed before any other environment file does

18. b

    The adduser command is just a wrapper for useradd. It is a Perl script that provides more convenience for the administrator when creating new users. Yet it still uses useradd command behind the scenes.

19. d

20. a

21. a

22. b

    But make sure you replace the x in the password placeholder field with the real, unencrypted password

23. a,b, and c

24. a

    Yet it's better it use usermod –L and usermod –U to avoid any errors