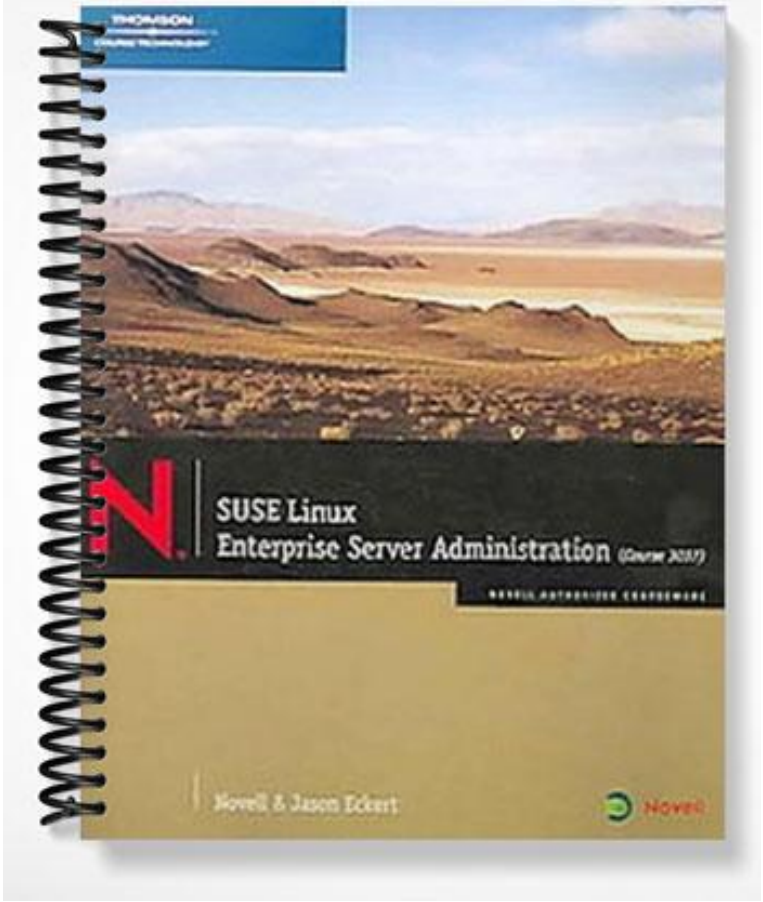
TEST BANK


SUSE Linux
Enterprise Server Administration
Novell & Jason Eckert
Novell

ch02

True/False
Indicate whether the statement is true or false.

____ 1. One of the main characteristics of a Linux operating system is its ability to handle several users at the same time (multiuser).

____ 2. Root can change to any user ID without knowing the password of the user.

____ 3. Every file and directory in a Linux system has a numerical permission value assigned to it. This value has five digits.

____ 4. If the default settings are not changed, files are created with the access mode 333 and directories with 444 by default.

____ 5. PAM recognizes four types of modules: auth, account, session, and password.

Multiple Choice
Identify the choice that best completes the statement or answers the question.

____ 6. The number that a user receives is called a ____.
a. group ID (GID)
b. system ID (SID)
c. user ID (UID)
d. login ID (LID)

____ 7. Groups are internally allocated a number, called the ____.
a. group ID (GID)
b. user ID (UID)
c. login ID (LID)
d. system ID (SID)

____ 8. You can use the command ____ to display information about a user's UID and the groups to which she is assigned.
a. ls
b. id
c. uname
d. user

____ 9. As part of Linux security measures, each user in the system has her own directory in the directory ____.
a. /var/
b. /etc/
c. /usr/
d. /home/

____ 10. The ____ file stores encrypted user passwords and password expiration information.
a. /usr/home
b. /etc/shadow
c. /home/passwd
d. /var/shadow

____ 11. You can use the ____ command to change the password for a user account.
a. useradd
b. groupadd
c. userpwd
d. passwd

____ 12. The ____ command lets you delete an existing user account.
a. userdel
b. useradd
c. groupadd
d. passwd

____ 13. You can create a new group by entering ____ *group_name*.
a. useradd
b. groupdel
c. groupadd
d. passwd

____ 14. You can delete a group by entering ____ *group_name*.
a. userdel
b. passwd
c. groupmod
d. groupdel

____ 15. The ____ file contains an initial message for users logging into the system.
a. /etc/welcome
b. /etc/welmsg
c. /etc/issue
d. /etc/inimsg

____ 16. You can change the effective group GID with the command ____ or sg.
a. newgrp
b. newusr
c. adduser
d. grpchg

____ 17. To enable a command to be run by a normal user, you can use the command ____.
a. su
b. sudo
c. newgrp
d. sg

____ 18. ____ is the Linux default password encryption method.
a. DES
b. Blowfish
c. MD5
d. RSA

____ 19. You can use the command ____ to display the contents of the current directory with the assigned permissions for each file or subdirectory.
a. ps -p
b. su
c. ls -l
d. sudo

____ 20. As user root, you can use the command ____ to change the user and group affiliation of a file.
a. chmod
b. chown
c. grpmod
d. usrmod

____ 21. As user root, you can change the group affiliation of a file with the command ____.
a. usrmod
b. grpmod
c. grpadd
d. chgrp

____ 22. To modify (restrict) the file and directory default access mode settings, you can use the command ____.
a. uname
b. su
c. umask
d. visudo

____ 23. The PAM configuration file ____ column contains control flags that influence the behavior of PAM modules.
a. Module type
b. Module
c. Arguments
d. Control flag

____ 24. Open ports, with the socket in state LISTEN, can be found with the program ____.
a. netstat
b. uname
c. umask
d. listen

____ 25. The ____ command shows who is currently logged in to the system and information such as the time of the last login.
a. last
b. who
c. faillog
d. finger

____ 26. The ____ command formats and prints the contents of the last login log file (/var/log/lastlog).
a. faillog
b. who
c. finger
d. lastlog

Completion
Complete each statement.

27. You can create a new user account with the _____ command.

28. You can use the command _____ (switch user) to assume the UID of root or of other users.

29. The updatedb command generates a database (_____) in which the location of each file on your computer is stored.

30. Every program that relies on the PAM modules has its own configuration file in the directory _____.

31. The _____ command displays a listing of the last logged-in users.

Matching

Match each term with the correct statement below.

a. The groups command
b. The file /etc/passwd
c. The file /etc/group
d. The usermod command
e. The groupmod command
f. The visudo command
g. The chmod command
h. The chattr command
i. The pam_securetty.so module

____ 32. modify the settings (such as GID, group name, and users) for an existing group.
____ 33. displays information on the groups in which you are a member.
____ 34. lets you modify settings for an existing user account.
____ 35. allows you to set the ext2 file attributes.
____ 36. allows you to add, remove, or assign permissions assigned to a file or directory.
____ 37. determines which terminals can be regarded as secure.
____ 38. modifies the sudo configuration file /etc/sudoers.
____ 39. stores information for each user such as the user name, the UID, the home directory, and the standard shell.
____ 40. stores group information.

Short Answer

41. What are the four file system security components?

42. What is the difference between regular and system users?

43. What is the difference between public and private group schemes?

44. What is the structure of each line in the file /etc/passwd?

45. Name and briefly describe the three file system access permission levels in SUSE Linux.

46. Explain how to use the passwd command.

47. What security settings can you modify using YaST?

48. What boot settings can you configure using YaST?

49. What are the permissions that you can assign to a file or directory?

50. What is PAM?

ch02
Answer Section

TRUE/FALSE

1. ANS: T PTS: 1 REF: 52
2. ANS: T PTS: 1 REF: 84
3. ANS: F PTS: 1 REF: 103
4. ANS: F PTS: 1 REF: 107
5. ANS: T PTS: 1 REF: 114

MULTIPLE CHOICE

6. ANS: C PTS: 1 REF: 53
7. ANS: A PTS: 1 REF: 53
8. ANS: B PTS: 1 REF: 53
9. ANS: D PTS: 1 REF: 55
10. ANS: B PTS: 1 REF: 57
11. ANS: D PTS: 1 REF: 72
12. ANS: A PTS: 1 REF: 72
13. ANS: C PTS: 1 REF: 74
14. ANS: D PTS: 1 REF: 74
15. ANS: C PTS: 1 REF: 74
16. ANS: A PTS: 1 REF: 85
17. ANS: B PTS: 1 REF: 87
18. ANS: A PTS: 1 REF: 93
19. ANS: C PTS: 1 REF: 101
20. ANS: B PTS: 1 REF: 104
21. ANS: D PTS: 1 REF: 105
22. ANS: C PTS: 1 REF: 107
23. ANS: D PTS: 1 REF: 115
24. ANS: A PTS: 1 REF: 122
25. ANS: B PTS: 1 REF: 123
26. ANS: D PTS: 1 REF: 125

COMPLETION

27. ANS: useradd

    PTS: 1 REF: 72
28. ANS: su

    PTS: 1 REF: 84
29. ANS: locatedb

PTS: 1 REF: 99

30. ANS: /etc/pam.d/*program_name*

PTS: 1 REF: 112

31. ANS: last

PTS: 1 REF: 124

MATCHING

32. ANS: E PTS: 1 REF: 74
33. ANS: A PTS: 1 REF: 53
34. ANS: D PTS: 1 REF: 72
35. ANS: H PTS: 1 REF: 110
36. ANS: G PTS: 1 REF: 102
37. ANS: I PTS: 1 REF: 115
38. ANS: F PTS: 1 REF: 87
39. ANS: B PTS: 1 REF: 56
40. ANS: C PTS: 1 REF: 59

SHORT ANSWER

41. ANS:
As with other operating systems, you control access to files in a Linux file system by implementing the following types of components:
* Users. Users are individual accounts on the Linux system.
* Groups. Groups are collections of users. Users are assigned to a group when they are created. Only root or the owner can change the group to which the file or directory is assigned. Every user must belong to at least one group.
* Ownership.The user who creates a file or directory is automatically assigned as its owner. Ownership can only be changed manually by root.
* Permissions. Permissions determine user access to a file or directory.

PTS: 1 REF: 52

42. ANS:
In a Linux operating system, there are two basic kinds of user accounts:
* Regular (normal) users. These are user accounts you create that allow employees and others to log in to the Linux environment. This type of login gives people a secure environment for accessing data and applications. These user accounts are managed by the system administrator.
* System users.These are user accounts created during installation that are used by services, utilities, and other applications to run effectively on the server.

Regular users are stored in the files /etc/passwd and /etc/shadow; system users are created by scripts that are part of rpm packages.

PTS: 1 REF: 54

43. ANS:

When you create a user in a Linux (or UNIX) environment, that user is assigned a default group using one of two basic methods (schemes):
* Private scheme. In this scheme, the user is assigned his own group that he can manage. For example, if you create the user cgrayson, a group cgrayson is also created.
* Public scheme. In this scheme, the user is assigned to a general,public group such as users. Because the group includes all new users, the group is normally managed by the system administrator.

SUSE Linux Enterprise Server uses the public scheme for assigning new users to a group.

PTS: 1 REF: 54

44. ANS:
Each line in the file /etc/password represents one user, and contains the following information:
* User name. This is the name a user enters to log in to the system (login name). Although Linux can handle longer user names, in this file they should be restricted to a maximum of 8 characters for backward compatibility with older programs.
* Password. The x in this field means that the password is stored in the file /etc/shadow.
* UID. In compliance with the Linux standards, there are two number ranges which are reserved:
  - 0–99 for the system itself
  - 100–499 for special system users (such as services and programs)
  - Normal users start from UID 1000.
* Comments field. Normally, the full name of the user is stored here. Information such as a room number or telephone number can also be stored here.
* Home directory. The personal directory of a user is normally in the directory /home/ and is the same name as the user (login) name.
* Standard shell. This is the shell that is started for a user after he or she has successfully logged in. In Linux this is normally bash (Bourne Again Shell). The shell must be listed in the file /etc/shells. Each user can change his standard shell with the command chsh.

PTS: 1 REF: 57

45. ANS:
Each file and directory in the file system is assigned access permissions. The permissions assigned determine the level of access a given user has. Permissions are assigned at 3 levels:
* Owner. The permissions assigned to a file or directory's owner determine the owner's level of access.
* Group. Permissions assigned to the group determine the level of access group members have to the file or directory.
* Others. Permissions assigned to this entity apply to authenticated users who are not members of the group that has been associated with the file or directory.

PTS: 1 REF: 61

46. ANS:
When logged in, any user can change his password by entering passwd without options; root can change the password of any user by entering passwd *username*.
Besides changing a user's password, you can also use the command to do the following:
* Lock a user account.With the option -l (lock), you can deactivate a user account, and then reactivate the account with the option -*u* (unlock). For example, to deactivate the user account geeko, enter passwd -l geeko.
* Display the password status of a user account. The option -S lets you display the status of a user account. For example, entering passwd -S geeko might display the following:
geeko L 09/04/2007 0 99999 7 0

The status follows directly after the username. L means that the user is locked out. Other options are NP (no password) or P (valid password).
This is followed by the date of the last password change, the minimum length
of validity, the maximum length of validity, and the warning periods and inactivity periods when a password expires.
* Change password times. You can use options such as -n and -w to change expiration times for user passwords.
For example, entering passwd -x 30 -w 5 geeko changes the maximum number of days to 30 for which the password is valid and warns the user 5 days in advance of the password expiration.

PTS: 1 REF: 73

47. ANS:
YaST provides a Security Settings module that lets you configure the following local security settings for your SUSE Linux Enterprise Server:
* Password settings
* Boot configuration
* Login settings
* User creation settings
* File permissions
You can select from (or modify) three preset levels of security, or create your own customized security settings to meet the requirements of your enterprise security policies and procedures.

PTS: 1 REF: 90

48. ANS:
You can select the following boot settings (which update the file /etc/inittab):
* Interpretation of Ctrl + Alt + Del. When someone at the console presses the Ctrl+Alt+Del keystroke combination, the system usually reboots.
Sometimes you want to have the system ignore this keystroke combination, especially when the system serves as both workstation and server.
You can select from Ignore, Reboot, or Halt. If you select Halt, the system shuts down.
* Shutdown Behavior of KDM.You use this option to set who is allowed to shut down the computer from KDM.
You can select from Only root, All users, Nobody, Local users, and Automatic.
If you select Nobody, you can only shut down the system from a text console.

PTS: 1 REF: 95

49. ANS:
You can assign the following three permissions to a file or directory:
* Read (r). This permission allows the file to be read or the contents of a directory to be listed.
* Write (w). This permission allows a file to be modified. It allows files to be created or deleted within a directory.
* Execute (x). This permission allows a file to be executed. It allows access to a directory.

PTS: 1 REF: 101

50. ANS:

Linux uses PAM(Pluggable Authentication Modules) in the authentication process as a layer that communicates between users and applications. By providing systemwide access to applications through its authentication modules, PAM lets you configure and change authentication methods between users and individual applications from centrally managed modules. Whenever a new authentication method is needed (such as a fingerprint scan instead of a username/password) for an application, you simply reconfigure or create a PAM module for use by the application.

PTS: 1 REF: 112