LX0-104/102-400 Exam Questions

1. Your Linux system is configured to boot into runlevel 3 by default. After starting the system, you authenticate as the tux user. Which shell configuration files may have been used to configure the current session? (Choose two.)
    a. /etc/profile
    b. ~/.bash_login
    c. ~/.bashrc
    d. /etc/bashrc
    e. /etc/bash.bashrc

2. When a login shell is run, the bash shell program searches for configuration files to configure the current session. Which file has the lowest priority in the search order?
    a. ~/.profile
    b. ~/.bash_login
    c. ~/.bash_profile
    d. ~/.bashrc

3. You want to create an alias on your Linux system named update that will first test to see if the user running the command is the root user. If so, the alias should run the /var/opt/db/updatemydb command. If not, the alias should use su to run the /var/opt/db/updatemydb command. Which command will create this alias?
    a. alias update='/var/opt/db/updatemydb'
    b. alias update='if test "$EUID" = 0 ; then /var/opt/db/updatemydb ; else su - -c "/var/opt/db/updatemydb" ; fi'

c. alias update='su - -c "/var/opt/db/updatemydb"'

d. alias update='if "$EUID" = 0 ; then /var/opt/db/updatemydb ; else su - "/var/opt/db/updatemydb" ; fi'

4. Which command can be used at the shell prompt to display a list of currently defined aliases on your system?

   a. aliases –l

   b. alias –l

   c. aliases

   d. alias

5. Which locale value specifies the United States English locale with Unicode encoding?

   a. en_US.UTF-8

   b. en_US.iso885915

   c. fr_CA.ASCII

   d. en_CA.UTF-8

6. Which locale variable overrides all other locale variables?

   a. LANG

   b. LANGUAGE

   c. LC_CTYPE

   d. LC_ALL

7. Which commands can be used to view a list of locales and encodings available on a Linux system? (Choose two.)
    a. echo $LC_CTYPE
    b. locale –c
    c. locale –a
    d. locale charmap
    e. locale –m

8. Which directive in the /etc/sysconfig/clock file configures a Linux system to use local time instead of UTC?
    a. SYSTOHC="yes"
    b. TIMEZONE
    c. HWCLOCK –-localtime
    d. HWCLOCK –u

9. Which commands can be used on a Linux system to change the time zone? (Choose two.)
    a. tzselect
    b. tzconfig
    c. zoneinfo
    d. time
    e. date

10. You've just installed a new font on your Linux system. Which section of the xorg.conf file do you need to edit to configure the X server to use the new font?
    a. ServerFlags
    b. Files
    c. Fonts
    d. Screen

11. You've just used the Xorg –configure command at the shell prompt, which generated a video configuration proposal for you named /root/xorg.conf.new. Which command can you use to test the video configuration settings in the file before committing them?
    a. X –config /root/xorg.conf.new
    b. xorgconfig
    c. XFree-86 –config /root/xorg.conf.new
    d. system-config-display

12. Which command can be used to display information about open windows on your graphical desktop?
    a. xhost
    b. xwininfo
    c. X
    d. xorgcfg

13. Which command can be used to view information about the X server software on your Linux system?

a. XFree-86 –configure

b. Xorg –configure

c. xwininfo

d. xdpyinfo

14. Your Linux system boots into runlevel 3 by default. You start your graphical environment using the startx command. Which file can you edit to manually specify which display manager you want loaded by default when the X server starts?

    a. ~/.xinitrc

    b. /etc/xattr.conf

    c. /etc/X11/xdm/xdm-config

    d. ~/.xdm

15. You boot your Linux system every morning and shut it down at the end of the work day. Yesterday, you made some configuration changes to your Linux system that you suspect are causing issues. You need to view the system boot messages from two days ago so you can see how the system behaved prior to the configuration changes. Given that your system uses systemd instead of the init daemon, what command should you use?

    a. journalctl –b 2

    b. logger –p 2

    c. journalctl –b

    d. journalctl –b -2

16. You recently created a script file named isethup.sh, which contains a single function statement that tests to see if an Ethernet interface is up. It expects to be passed an argument that contains the name of the network interface to test. You want to call the function in this file from another script file named updatedata.sh to see if the ens32 interface is up. Which statement should you add to the second script file to do this?
    a. include isethup.sh ens32
    b. source isethup.sh ens32
    c. call isethup.sh ens32
    d. run isethup.sh ens32

17. Which keyboard accessibility option inserts a slight delay between keystrokes to prevent the keyboard from sending unintentional keystrokes?
    a. RepeatKeys
    b. SlowKeys
    c. ToggleKeys
    d. BounceKeys

18. Which mouse accessibility option sends a mouse click whenever the mouse pointer stops moving for a specified amount of time?
    a. Simulated secondary click
    b. Dwell click
    c. Mouse gestures
    d. MouseKeys

19. Which entry from the /etc/shadow file is a special-purpose system user account?
    a. geeko:$2a$05$57is82BUSDNJ1TzZzMpFo:15101:0:99999:7:::
    b. sysadm:$2a$10$0fLoXnbIjtr:15108:0:99999:7:::
    c. rtracy:$2a$05$Kscqfv3nRNV2rDD:15094:0:99999:7:::
    d. fjohnson:*:14312::::::

20. Which of the following entries from the /etc/passwd file is a system user account?
    a. mwilliams:x:30:8:Mary Williams:/var/lib/mwilliams:/bin/false
    b. sysadm:x:1001:100:System Admin:/home/sysadm:/bin/bash
    c. pmgr:x:1002:100:Program Manager:/home/pmgr:/bin/bash
    d. rtracy:x:1000:100:Robb Tracy:/home/rtracy:/bin/bash

21. Which files contain default values used by the useradd command if no corresponding parameters are included using command-line options? (Choose two.)
    a. /etc/login.defs
    b. /etc/default/passwd
    c. /etc/default/rmt
    d. /etc/default/su
    e. /etc/default/useradd

22. Which passwd command option sets the maximum number of days before a password must be changed?
    a. –l
    b. –u

c. –x

d. –n

23. Which file stores group passwords, if assigned?

    a. /etc/group

    b. /etc/passwd

    c. /etc/gshadow

    d. /etc/shadow

    e. /etc/gpasswd

24. Which file contains default values used by the groupadd command if no corresponding parameters are included using command-line options?

    a. /etc/login.defs

    b. /etc/default/passwd

    c. /etc/default/groupadd

    d. /etc/default/useradd

25. Your organization uses private IP addresses using the 172.16.0.0 addressing scheme. You need to divide your IP address space into multiple subnets, so you decide to use an 18-bit subnet mask instead of the default Class B subnet mask. Which of the following is a valid address that could be assigned to a host on the second subnet created using this subnet mask?

    a. 172.16.64.1/18

    b. 172.16.127.251/16

c. 172.16.2.1/18

d. 172.16.128.1/18

26. Which files are used to restrict user access to the at daemon? (Choose two.)

    a. hosts.deny

    b. at.deny

    c. hosts.allow

    d. at.allow

    e. cron.deny

    f. cron.allow

27. It's currently 1:00 in the afternoon. You want to schedule the compilemyapp program to run automatically tomorrow afternoon at 2:00. Which at commands could you use to do this? (Choose two.)

    a. at 2pm tomorrow

    b. at tomorrow +1 hour

    c. at now + 1 day

    d. at today +25 hours

    e. at now +25 hours

28. Which crontab file entry will cause the /usr/bin/compilejob process to run at 5:05 p.m. Monday through Thursday?

    a. 5 17 * * 1-4 /usr/bin/compilejob

    b. 17 5 1-4 * * /usr/bin/ compilejob

c. * * 5 17 0-3 /usr/bin/myappcleanup

d. 5 5 * * 0-3 /usr/bin/compilejob

29. Which commands can be used to view your user's crontab file? (Choose two.)

a. crontab –r

b. crontab –e

c. crontab –v

d. crontab –l

e. crontab –u

30. You've created a shell script in your home directory (~) named killerapp. How can you execute it? (Choose two.)

a. Enter /bin/bash ~/killerapp at the shell prompt.

b. Enter cd ~ at the shell prompt; then enter killerapp.

c. Select Computer | Run in the graphical desktop; then enter ~/killerapp and select Run.

d. Enter exec ~/killerapp at the shell prompt.

e. Enter chmod u+x ~/killerapp; then enter ~/killerapp at the shell prompt.

31. You need to use the tail command to view the last few lines of all the files in /var/log that contain the text "login". Which command will do this?

a. fgrep –l login /var/log/* | tail

b. tail $(fgrep –l login /var/log/*)

c. tail /var/log/* | grep –l login

d. fgrep –l login /var/log/* $(tail)

32. Which test command option checks to see if a specified file exists and tests whether or not that file is a symbolic link?

    a. –e

    b. –f

    c. –L

    d. –O

33. Which control structure processes over and over as long as a specified condition evaluates to false?

    a. while

    b. until

    c. for

    d. case

34. Which protocol sends IP packets without requiring acknowledgment of receipt of those packets from the destination host?

    a. TCP

    b. UDP

    c. RDP

    d. SPX

35. A service you are configuring on your Linux system transfers data on port 3708. What kind of port is this?
    a. Well-known
    b. Registered
    c. Dynamic
    d. Private

36. Which IP address is a private Class B address?
    a. 10.0.0.3
    b. 178.7.8.44
    c. 172.17.8.1
    d. 192.168.1.4

37. Which of the following is a valid IPv6 address?
    a. 35BC:FA77:4898:DAFC:200C:FBBC:A007:8973
    b. 35BC:FP77:4898:DAFC:200C:FBBC:A007:8973
    c. 35BC:FA77:4898:DAFC
    d. 35BC:FA77:4898:DAFC:200C:FBBC:A007

38. You needed to add a route to the 192.168.2.0/24 network through the router with an IP address of 192.168.1.254. Which command will do this?
    a. route add –net 192.168.2.0 netmask 255.255.255.0 192.168.1.254
    b. route add netmask 255.255.255.0 gw 192.168.1.254
    c. route add –net 192.168.2.0 subnetmask 255.255.255.0 gw 192.168.1.254

d. route add –net 192.168.2.0 netmask 255.255.255.0 gw 192.168.1.254

39. You need to use the dig command to perform an MX record lookup for the mail.mydom.com hostname. You need to run the dig command against a DNS server with an IP address of 137.65.10.1. Which command will do this?

    a. dig @137.65.10.1 mail.mydom.com
    b. dig mail.mydom.com 137.65.10.1 –t MX
    c. dig mail.mydom.com –t A
    d. dig @137.65.10.1 mail.mydom.com –t MX

40. You need to restrict access to the CUPS printing service on a Linux server to specific network hosts. Which of the options that follow can you use to do this? (Choose two.)

    a. The BrowseAllow parameter in /etc/cups/cupsd.conf
    b. The /etc/hosts.allow file
    c. The /etc/cups.allow file
    d. The /etc/cups.deny file
    e. The BrowseDeny parameter in the /etc/cups/cupsd.conf
    f. The /etc/hosts.deny file

41. Which file in /etc/cups stores CUPS printer definitions on a Linux system?

    a. printers.conf
    b. client.conf
    c. cupsd.conf

d. command.types

42. One of your users mistakenly sent an 800-page print job to the shared CUPS printer daemon on your Linux server. You need to delete the job. Which commands will do this? (Choose two.)

    a. lpc
    b. cupsreject
    c. cancel
    d. lprm
    e. lpq

43. Which hwclock command options can be used to set the motherboard clock to the current system time? (Choose two.)

    a. –r
    b. –s
    c. –hctosys
    d. –w
    e. –systohc

44. Which NTP concept refers to the estimated time difference between the consumer and the provider since the last time poll?

    a. Jitter
    b. Drift
    c. Stepping

d. Slewing

45. Your Linux system uses the postfix MTA. Where is your incoming mail queue?

    a. /var/spool/mail/incoming

    b. /var/spool/postfix/incoming

    c. /var/spool/postfix/active

    d. /var/spool/mail/active

46. Which file can be used to configure e-mail forwarding to a different e-mail address for your user account?

    a. ~/.forward

    b. /etc/forward

    c. ~/.profile

    d. /etc/postfix/main.cf

47. You need to view all records from the customers table in the mydom database that contains a value of “active” in the status column. Which SQL command will do this?

    a. SELECT status='active' FROM customers;

    b. RETRIEVE * FROM customers WHERE status='active';

    c. SELECT * FROM customers WHERE status='active';

    d. SELECT * FROM mydom WHERE status='active';

48. Which SQL statement can be used to consolidate the results from a SELECT statement by one or more columns?

a. UPDATE

b. JOIN

c. INSERT INTO

d. GROUP BY

49. Which su command option can be used to create a login shell session instead of a non-login shell?

a. –l

b. –c

c. –g

d. –m

50. Which chage command option can be used to set a fixed expiration date for a user account?

a. –m

b. –M

c. –W

d. –E

51. Which entry in the /etc/security/limits.conf file would limit the tux user to only one login at a time?

a. tux hard locks 1

b. tux hard priority 1

c. tux hard maxlogins 1

d. tux soft maxlogins 1

52. You need to scan your Linux file system to locate all files that have the SUID permission set. Which commands can you use to do this? (Choose two.)

    a. find / –type f –perm –g=s –ls

    b. find / –type f –perm –u=s –ls

    c. find / –type f –perm –2000 –ls

    d. find / –type f –perm –1000 –ls

    e. find / –type f –perm –4000 –ls

53. Which netstat command options can be used to display open ports on a Linux system? (Choose two.)

    a. –a

    b. –i

    c. –l

    d. –s

    e. –r

54. Which system log file contains a list of unsuccessful authentication attempts to a Linux system?

    a. lastlog

    b. warn

    c. wtmp

    d. faillog

55. You want to reconfigure the vsftpd service (managed by the xinetd super-daemon) to use TCP Wrappers. What changes do you need to make to the vsftpd configuration file in /etc/xinetd.d? (Choose two.)
    a. server = /usr/sbin/vsftpd
    b. server_args = /usr/sbin/tcpd
    c. server = /usr/sbin/tcpd
    d. server_args = /usr/sbin/vsftpd
    e. wait = yes

56. Where does the ssh client store keys received from the various sshd server hosts it connects to? (Choose two.)
    a. /etc/ssh/ssh_known_hosts
    b. /etc/ssh/ssh_host_key
    c. /etc/ssh/ssh_host_rsa_key
    d. ~/.ssh/known_hosts
    e. ~/.ssh/authorized_keys

57. Which files are the public keys used by the sshd daemon using the SSH version 2 protocol? (Choose two.)
    a. /etc/ssh/ssh_known_hosts
    b. /etc/ssh/ssh_host_key.pub
    c. /etc/ssh/ssh_host_rsa_key.pub
    d. /etc/ssh/ssh_host_dsa_key.pub

e. ~/.ssh/authorized_keys

58. Which parameter in /etc/ssh/ssh_config can be used to specify that it use SSH version 1 when connecting to an sshd server host?

    a. Port

    b. Protocol

    c. Version

    d. StrictHostKeyChecking

59. You want to encrypt a file named sensitive.odt in your user's home directory using the gpg command. Given that you specified a real name of tuxuser when you initially generated your GPG keys, which command can you use to encrypt this file?

    a. gpg –e ~/sensitive.odt

    b. gpg –e tuxuser ~/sensitive.odt

    c. gpg –e –r tuxuser ~/sensitive.odt

    d. gpg –d –r tuxuser ~/sensitive.odt

60. You want to configure public key authentication to an SSH server host. Which commands can you use to create the public keys for your user on your SSH client system that can be copied over to the SSH server host to enable this functionality? (Choose two.)

    a. ssh –-key-gen –t rsa

    b. ssh-keygen –t rsa

    c. ssh –-key-gen –t dsa

    d. ssh-keygen –t dsa

e. ssh –-gen-key –t rsa,dsa

Quick Answer Key

1. A, B
2. A
3. B
4. D
5. A
6. D
7. C, E
8. C
9. A, B
10. B
11. A
12. B
13. D
14. A
15. D
16. B
17. D
18. B
19. D
20. A
21. A, E
22. C

23. C
24. A
25. A
26. B, D
27. A, E
28. A
29. B, D
30. A, E
31. B
32. C
33. B
34. B
35. B
36. C
37. A
38. D
39. D
40. A, E
41. A
42. C, D
43. D, E
44. A
45. B

46. A

47. C

48. D

49. A

50. D

51. C

52. A, E

53. A, C

54. D

55. C, D

56. A, D

57. C, D

58. B

59. C

60. B, D

Answer Explanations

1. A and B are correct. Because the system booted into a text-based environment (runlevel 3), the shell session used to authenticate the tux user is a login shell. As a result, the /etc/profile file or the ~/.bash_login file may have been used to configure the session, depending on the distribution.

   C, D, and E are incorrect. The ~/.bashrc, /etc/bashrc, and /etc/bash.bashrc files are used to configure non-login shell sessions, such as when you open a terminal session within the X graphical environment.

2. A is correct. When a login shell is run, the bash shell program searches for configuration files in the following order: 1) ~/.bash_profile, 2) ~/.bash_login, 3) ~/.profile. It uses the first file it finds and ignores all the rest.

   B, C, and D are incorrect. The ~/.profile file has a higher search priority than ~/.bash_profile and ~/.bash_login. The ~/.bashrc file is used to configure non-login shell sessions.

3. B is correct. The alias update='if test "$EUID" = 0 ; then /var/opt/db/updatemydb ; else su - -c "/var/opt/db/updatemydb" ; fi' command creates an alias on your Linux system named update that uses an if/then/else control structure to test to see if the user running the command is the root user (whose EUID is 0). If so, the alias runs the /var/opt/db/updatemydb command. If not, the alias runs su – to execute the /var/opt/db/updatemydb command using the –c option. The –c option allows su – to run the specified command as root.

   A, C, and D are incorrect. A and C are incorrect because they fail to test whether the user is root before running the commands. D is incorrect because it omits the test command in the if/then/else statement that is required to evaluate whether the current user is root.

4. D is correct. The alias command can be used at the shell prompt to display a list of currently defined aliases on your system.

   A, B, and C are incorrect. The aliases command is an invalid shell command. The alias command does not have a –l option defined.

5. A is correct. A value of en_US.UTF-8 can be used for the LC_CTYPE locale environment variable to configure the system to use the United States English (en_US) local with Unicode (UTF-8) encoding.

   B, C, and D are incorrect. B is incorrect because it configures the system to use the U.S. English locale with Latin-9 encoding, which is designed for Western European languages. C is incorrect because it configures the system to use the French Canadian locale with ASCII encoding. D is incorrect because it configures the system to use the English Canadian locale with UTF-8 encoding.

6. D is correct. The LC_ALL locale environment variable overrides all other LC environment variables.

   A, B, and C are incorrect. The LANG environment variable specifies the default locale value for all LC_ variables but has a lower precedence than LC_ALL. The LANGUAGE environment variable only overrides LC_MESSAGES. LC_CTYPE is only used to configure the default character type and encoding.

7. C and E are correct. The local –a command displays a list of all available locales whereas the locale –m command displays a list of available encodings.

   A, B, and D are incorrect. The echo $LC_CTYPE command only displays the current locale and encoding in use on the system. The locale –c command is used to display

names of specified categories. The locale charmap command only displays the type of encoding currently in use.

8. C is correct. The HWCLOCK –localtime directive configures a Linux system to use local time instead of UTC.

   A, B, and D are incorrect. The SYSTOHC="yes" directive writes the system time to the hardware clock when the system is started or shut down. The TIMEZONE directive sets the system's time zone. The HWCLOCK –u directive configures the system to use UTC instead of local time.

9. A and B are correct. The tzselect and tzconfig commands are used on various Linux distributions to set the time zone.

   C, D, and E are incorrect. C (zoneinfo) is a directory (not a command) in /usr/share that contains your time zone files. The time command is used to time a simple command or display resource usage. The date command can be used to display the current time zone, but it can't be used to set it.

10. B is correct. You need to edit the Files section of the xorg.conf file and add a FontPath directive that points to the directory where the new font is installed.

    A, C, and D are incorrect. The ServerFlags section specifies global X server options. There is no Fonts section in the xorg.conf file; this is a distracter. The Screen section binds your video board configuration to your monitor configuration.

11. A is correct. The X –config /root/xorg.conf.new command will test the video settings in the /root/xorg.conf.new file.

B, C, and D are incorrect. The xorgconfig command is used to display a text-based X server configuration menu. The XFree-86 –config /root/xorg.conf.new command is used to test configuration settings on an XFree-86 X server system. The system-config-display utility is a Red Hat–specific command that runs the Display Settings utility that you can use to configure your video board, monitor type, resolution, and color depth.

12. B is correct. The xwininfo command can be used to display information about open windows on your graphical desktop. You can click the window you want to get information about, or you can specify the window ID of the window you want to get information about using the –id option with the command.

    A, C, and D are incorrect. The xhost command is a server access control program for X. The X command can be used to start the X server from the command line. The xorgcfg utility is a graphical version of the xorgconfig X server configuration utility.

13. D is correct. The xdpyinfo command displays the capabilities of a server, the various parameters used when communicating between clients and the server, and the different screen modes available.

    A, B, and C are incorrect. The XFree-86 –configure command is used with the XFree86 X server and is used to detect your hardware and create a file named /etc/X11/XF86Config.new. The Xorg –configure command is used with the X.org X server and also automatically detects all of your hardware and creates a configuration file named /root/xorg.conf.new for you. The xwininfo command is used to display information about open windows on your graphical desktop.

14. A is correct. You can specify the path to the display manager you want to use in the ~/.xinitrc file in your home directory.

B, C, and D are incorrect. The /etc/xattr.conf file configures how extended file attributes are handled when copying files. The /etc/X11/xdm/xdm-config file is used to configure the xdm display manager itself. The ~/.xdm file doesn't exist by default and is a distracter.

15. D is correct. The journalctl –b -2 command displays system messages that were logged two boot events ago.

    A, B, and C are incorrect. The journalctl –b 2 command will display messages created during the second boot event found at the beginning of the journal. The logger command is used to send test log events to the logging daemon. The journalctl –b command displays boot messages that were logged in the most recent boot event.

16. B is correct. You can call a function from a script file using the source statement. The syntax is source <filename> <arguments>. In this example, you would include the source isethup.sh ens32 statement in your script.

    A, C, and D are incorrect. The commands used in these statements can't be used to load a function from a file.

17. D is correct. The BounceKeys option inserts a slight delay between keystrokes to prevent the keyboard from sending unintentional keystrokes.

    A, B, and C are incorrect. RepeatKeys configures the keyboard to allow the user extra time to release a pressed key before sending multiple keystrokes. SlowKeys configures the keyboard such that the user must hold a key down for a specified period of time before the keystroke is actually sent. ToggleKeys sounds an audible alert if either the Caps Lock key or the Num Lock key is on.

18. B is correct. Dwell click sends a mouse click whenever the mouse pointer stops moving for a specified amount of time.

    A, C, and D are incorrect. Simulated secondary click allows you to send a double-click by holding down the primary mouse button for a specified amount of time. Mouse gestures allow you to complete a certain task when you move the mouse in a specific way. MouseKeys configures key sequences to move the mouse cursor on the screen and to send mouse clicks.

19. D is correct. The fjohnson:*:14312:::::: entry in the /etc/shadow file is a system user account because it has an asterisk (*) in the password field of the record and can't be used for login.

    A, B, and C are incorrect. Each of these user accounts has a password assigned in the password field of each record and is available for login.

20. A is correct. Because the UID assigned to the mwilliams user account is less than 100, it is a system user account.

    B, C, and D are incorrect. Each of these user accounts has a UID greater than 1000 and is therefore a standard user account.

21. A and E are correct. The /etc/login.defs file contains values you can use for the GID and UID parameters when creating an account with useradd. It also contains defaults for creating passwords in /etc/shadow. The /etc/default/useradd file contains defaults used by the useradd utility.

    B, C, and D are incorrect. The /etc/default/passwd file contains defaults used by the passwd command. The /etc/default/rmt file configures defaults for the remote magnetic tape protocol server. The /etc/default/su file contains defaults used by the su command.

22. C is correct. The passwd –x command can be used to set the maximum number of days before a password must be changed.

    A, B, and D are incorrect. The –l option locks the user's account. The –u option unlocks a user's account. The –n option sets the minimum number of days required before a password can be changed.

23. C is correct. Passwords for Linux groups are stored in the /etc/gshadow file.

    A, B, D, and E are incorrect. The /etc/group file contains group account definitions, but it shouldn't be used to store passwords. The /etc/passwd file stores user account definitions. The /etc/shadow file stores user passwords, but not group passwords. The /etc/gpasswd file doesn't exist by default and is a distracter.

24. A is correct. The /etc/login.defs file contains values you can use for the GID and UID parameters when creating a user account with useradd or a group account with groupadd.

    B, C, and D are incorrect. The /etc/default/passwd file contains defaults used by the passwd command. The /etc/default/groupadd file doesn't exist by default and is a distracter. The /etc/default/useradd file contains defaults used by the useradd command.

25. A is correct. Using an 18-bit subnet mask allows you to divide this Class B network into four subnets. The valid host address range for the second subnet is 172.16.64.1/18–172.16.127.254/18.

    B, C, and D are incorrect. B is incorrect because it uses the default Class B subnet mask, instead of the custom 18-bit mask required in the scenario. C is incorrect

because it is a valid address for the first subnet. D is incorrect because it is a valid address for the third subnet.

26. B and D are correct. The at.deny file is used to specify which users are not allowed to configure at jobs, whereas the at.allow file is used to specify which users can configure at jobs.

    A, C, E, and F are incorrect. The hosts.allow and hosts.deny files are used to restrict access to the xinetd daemon. The cron.allow and cron.deny files are used to restrict access to the cron daemon.

27. A and E are correct. The at 2pm tomorrow command and the at now +25 hours command will schedule the command to run automatically tomorrow afternoon at 2:00.

    B, C, and D are incorrect. C is incorrect because it uses correct syntax but schedules the command to run tomorrow at 1 p.m. B and D are incorrect because they do not use the correct at syntax.

28. A is correct. The 5 17 * * 1-4 /usr/bin/compilejob entry in a crontab file will cause the /usr/bin/compilejob process to run at 5:05 p.m., Monday through Thursday.

    B, C, and D are incorrect. B is incorrect because it reverses the hour and minute fields. It also misplaces the day of the week field. C is incorrect because it reverses the hour and minute fields with the day and month fields. It also specifies the job run on Sunday through Wednesday. D is incorrect because it specifies the job to run at 5:05 a.m. on Sunday through Wednesday.

29. B and D are correct. The crontab –e command opens your user's crontab file in the vi editor. The crontab –l command displays your user's crontab file onscreen.

A, C, and E are incorrect. The –r option removes your user's crontab file. The crontab command doesn't use a –v option, so this is a distracter. The –u option allows the root user to view any user's crontab file.

30. A and E are correct. A is correct because it will run the killerapp as a script even though it doesn't have the execute permission set. E is correct because it will set the execute permission for the file's owner, thus allowing it to be run from the command line.

    B, C, and D are incorrect. B is incorrect because it won't work—the file doesn't reside in a directory in the PATH environment variable and it doesn't have the execute permission set. C and D are incorrect because they won't work for the same reasons.

31. B is correct. The tail $(fgrep –l login /var/log/*) command will use the fgrep command to generate a list of files in /var/log that contain the term "login". Then the list will be substituted as arguments for the tail command, displaying the contents of each file sent to it by fgrep.

    A, C, and D are incorrect. A is incorrect because it uses piping and only displays the output of the fgrep command on the screen. C is incorrect because it also uses pipes but generates a "no such file" error as the incorrect information is sent to the input of grep. D is incorrect because it reverses the order of the commands required to use command substitution in this scenario.

32. C is correct. The –L option tells the test command to test whether or not a specified file exists and whether or not it is a symbolic link.

    A, B, and D are incorrect. The –e option just checks to see if the specified file exists. The –f option checks to see if the specified file exists and if it is a regular file. The –O

option checks to see if the specified file exists and if it is owned by the specified user ID.

33. B is correct. An until loop runs over and over as long as the condition is false. As soon as the condition is true, it stops.

    A, C, and D are incorrect. A while loop executes over and over until a specified condition is no longer true. A for loop processes a specific number of time. A case statement is not a looping structure.

34. B is correct. With UDP, IP packets are sent unacknowledged. It is usually implemented with applications that send very small amounts of data at a time. It assumes that error checking and correction is either not necessary or will be performed by the application, thus avoiding the processing overhead.

    A, C, and D are incorrect. The TCP, RDP, and SPX protocols all require acknowledgment of packet receipt.

35. B is correct. Port 3708 is a registered port. ICANN has reserved ports 1024 through 49151 for special implementations. Organizations can create their own network service and then apply for a registered port number to be assigned to it.

    A, C, and D are incorrect. Well-known ports are those numbered from 0 to 1023. Dynamic and private ports are the same and are designated as ports 49152 through 65535.

36. C is correct. The Class B private address range is 172.16.0.0–172.31.255.255.

A, B, and D are incorrect. A is incorrect because it is a private Class A address. B is incorrect because it is not a private IP address. D is incorrect because it is a private Class C address.

37. A is correct. 35BC:FA77:4898:DAFC:200C:FBBC:A007:8973 is a valid IPv6 address.

    B, C, and D are incorrect. B is incorrect because it uses an invalid hexadecimal number (FP77). C and D are incorrect because they use addresses that are too short.

38. D is correct. The route add –net 192.168.2.0 netmask 255.255.255.0 gw 192.168.1.254 command will add a route to the 192.168.2.0/24 network through the router with an IP address of 192.168.1.254.

    A, B, and C are incorrect. A is incorrect because it omits the gw option. B is incorrect because it omits the –net option. C is incorrect because it uses an invalid option (subnetmask).

39. D is correct. The dig @137.65.10.1 mail.mydom.com –t MX command will perform an MX record lookup for the mail.mydom.com hostname on the DNS server with an IP address of 137.65.10.1.

    A, B, and C are incorrect. A is incorrect because it omits the type parameter of MX. B is incorrect because it reverses the order of the name server to be used and the hostname to resolve. C is incorrect because it performs an A record lookup using whatever DNS server is configured in the /etc/resolv.conf file.

40. A and E are correct. You can use the BrowseAllow and BrowseDeny parameters in the /etc/cups/cupsd.conf file to restrict network printing to specific network hosts.

B, C, D, and F are incorrect. The /etc/hosts.allow and /etc/hosts.deny files are used to restrict access to the xinetd daemon. The /etc/cups.allow and /etc/cups.deny files don't exist by default and are distracters.

41. A is correct. All CUPS printers are defined in the /etc/cups/printers.conf file.

    B, C, and D are incorrect. The client.conf file is the CUPS client configuration file. The cupsd.conf file configures the CUPS daemon itself. The command.types file is the MIME types file for the CUPS drivers.

42. C and D are correct. The cancel and lprm commands can be used to remove a print job from the print queue.

    A, B, and E are incorrect. The lpc command is used to view the status of a printer. The cupsreject command is used to enable or disable a print queue. The lpq command is used to view pending print jobs.

43. D and E are correct. The –w and --systohc options can be used with the hwclock command to set the motherboard clock to the current system time.

    A, B, and C are incorrect. The –r option simply displays the time from the hardware clock. The –s and --hctosys options set the system time to the hardware clock.

44. A is correct. Jitter refers to the estimated time difference between the consumer and the provider since the last time poll.

    B, C, and D are incorrect. Drift measures and corrects for incidental clock frequency errors. Stepping refers to larger time adjustments NTP makes when the time difference between the time provider and consumer is more than 128 milliseconds.

Slewing refers to smaller time adjustments NTP makes when the time offset is less than 128 milliseconds.

45. B is correct. The postfix incoming mail queue is /var/spool/postfix/incoming.

    A, C, and D are incorrect. The postfix daemon doesn't use the /var/spool/mail directory for incoming mail messages. The /var/spool/postfix/active directory contains messages that arrived intact, were processed correctly, and are ready to be forwarded on to the next MTA or MDA.

46. A is correct. The ~/.forward file can be used to configure e-mail forwarding to a different e-mail address for your user account. Most Linux MTAs check for the existence of this file to configure forwarding of messages.

    B, C, and D are incorrect. The /etc/forward file doesn't exist by default and is a distracter. The ~/.profile file is used to configure the user's shell environment. The /etc/postfix/main.cf file is used to configure the postfix daemon itself.

47. C is correct. The SELECT * FROM customers WHERE status='active'; command will display all records from the customers table that contain a value of "active" in the status column.

    A, B, and D are incorrect. A is incorrect because it places "status='active'" in the wrong place in the command. B is incorrect because it uses an incorrect command (RETRIEVE). D is incorrect because it specifies the database (mydom) instead of the table in the database (customers).

48. D is correct. You can use the GROUP BY statement to consolidate the results from a SELECT statement by one or more columns. It is commonly used with the SUM() statement.

A, B, and C are incorrect. The UPDATE statement is used to modify data in an existing record in the table. The JOIN statement is used to merge fields from two different tables. The INSERT INTO statement is used to add new records to the table.

49. A is correct. The –l option causes the su command to create a login shell session instead of a non-login shell.

    B, C, and D are incorrect. The –c option tells the su command to switch to the specified user account and run a specified command as that user. The –g option sets the primary group. The –m option preserves the existing environment variables.

50. D is correct. The –E option causes the chage command to set a fixed expiration date for the specified user account.

    A, B, and C are incorrect. The –m option sets the minimum number of days between password changes. The –M option sets the maximum number of days during which the user's password is valid. The –W option sets the number of days of warning before a password change is required.

51. C is correct. The tux hard maxlogins 1 directive in the /etc/security/limits.conf file would limit the tux user to only one login at a time.

    A, B, and D are incorrect. A is incorrect because it sets the maximum number of locked files for the user. B is incorrect because it sets the priority to run user processes with. D is incorrect because although it does set a limit on user logins, it sets a soft limit that can be temporarily exceeded.

52. A and E are correct. Both the find / –type f –perm –g=s –ls and the find / –type f –perm –4000 –ls commands can be used to locate all files that have the SUID permission set. (Remember the SUID special permission has a value of 4.)

B, C, and D are incorrect. B and C are incorrect because they search for files with the SGID special permission set. (Remember the SGID special permission has a value of 2.) D is incorrect because it searches for files with the Sticky Bit special permission set (which has a value of 1).

53. A and C are correct. The –a option displays all listening and nonlistening sockets, whereas the –l option only displays listening sockets.

    B, D, and E are incorrect. The –i option causes netstat to display statistics for your network interfaces. The –s option displays summary information for each protocol. The –r option displays your routing table.

54. D is correct. The /var/log/faillog file contains a list of unsuccessful authentication attempts to a Linux system. It must be viewed with the faillog command at the shell prompt.

    A, B, and C are incorrect. The lastlog file contains last login information for users. The warn file contains warning messages. The wtmp file contains a list of users who have authenticated to the system.

55. C and D are correct. C is incorrect because it causes the TCP Wrapper daemon (tcpd) to be started when a client tries to connect to the FTP service on the system. D is incorrect because it tells tcpd to start the vsftpd daemon to service the request.

    A, B, and E are incorrect. A is incorrect because it will allow the FTP service to work, but it will be started directly by xinetd without the benefit and protection provided by TCP Wrappers. B is incorrect because it does not correctly pass the tcpd executable path to the server daemon as a server argument. E is incorrect because the vsftpd configuration file sets the socket_type directive to a value of “stream”, which requires that the wait directive be set to a value of “no”.

56. A and D are correct. When the ssh client connects to an sshd server host, it stores the keys it receives in the /etc/ssh/ssh_known_hosts and ~/.ssh/known_hosts files.

    B, C, and E are incorrect. The /etc/ssh/ssh_host_key and /etc/ssh/ssh_host_rsa_key files are the private keys used by the ssh v1 and ssh v2 daemons, respectively. The ~/.ssh/authorized_keys file is used to configure public key authentication to the sshd server host.

57. C and D are correct. The /etc/ssh/ssh_host_rsa_key.pub and /etc/ssh/ssh_host_dsa_key.pub files are the public keys used by the sshd daemon using the SSH version 2 protocol.

    A, B, and E are incorrect. The /etc/ssh/ssh_known_hosts file is used by the ssh client to store public keys received from sshd server hosts. The /etc/ssh/ssh_host_key.pub is an sshd server public key file, but it's only used when the daemon is using version 1 of the SSH protocol. The ~/.ssh/authorized_keys file is used to configure public key authentication to the sshd server host.

58. B is correct. The Protocol parameter in /etc/ssh/ssh_config can be used to specify that it use SSH version 1 (or version 2) when connecting to an sshd server host.

    A, C, and D are incorrect. The Port parameter configures which port the ssh client should establish SSH connections on. There is no parameter named Version used in the ssh_config file. This response is a distracter. The StrictHostKeyChecking parameter can be used to restrict the ssh client to connections only with SSH servers whose public keys have been added to either the ~/.ssh/known_hosts file or the /etc/ssh/ssh_known_hosts file.

59. C is correct. The gpg –e –r tuxuser ~/sensitive.odt command can be used to encrypt the file.

    A, B, and D are incorrect. A and B are incorrect because they both omit the –r <user_name> option required to use your GPG key file. D is incorrect because it uses the –d (decrypt) option instead of –e (encrypt).

60. B and D are correct. You can use the ssh-keygen –t rsa or the ssh-keygen –t dsa command to create a public/private key pair on the client system so that you can send the public key to the SSH server to enable public key authentication.

    A, C, and E are incorrect. The --key-gen and --gen-key options are invalid ssh command options and are distracters.

Objectives

1. 105.1 Customize and use the shell environment.
2. 105.1 Customize and use the shell environment.
3. 105.1 Customize and use the shell environment.
4. 105.1 Customize and use the shell environment
5. 107.3 Localization and internationalization: Locale settings
6. 107.3 Localization and internationalization: Locale settings
7. 107.3 Localization and internationalization: Locale settings
8. 107.3 Localization and internationalization: Time zone settings
9. 107.3 Localization and internationalization: Time zone settings
10. 106.1 Install and configure X11: Basic understanding and knowledge of the X Window configuration file
11. 106.1 Install and configure X11: Basic understanding and knowledge of the X Window configuration file
12. 106.1 Install and configure X11
13. 106.1 Install and configure X11
14. 106.2 Set up a display manager: Turn the display manager on or off
15. 108.2 System logging
16. 105.1 Customize and use the shell environment
17. 106.3 Accessibility: Keyboard accessibility settings
18. 106.3 Accessibility
19. 107.1 Manage user and group accounts and related system files: Create and manage special-purpose and limited accounts

20. 107.1 Manage user and group accounts and related system files: Create and manage special-purpose and limited accounts
21. 107.1 Manage user and group accounts and related system files: Manage user/group info in password/group databases
22. 107.1 Manage user and group accounts and related system files: Manage user/group info in password/group databases
23. 107.1 Manage user and group accounts and related system files: Manage user/group info in password/group databases
24. 107.1 Manage user and group accounts and related system files: Manage user/group info in password/group databases
25. 109.1 Fundamentals of Internet protocols: Demonstrate an understanding of network masks and CIDR notation
26. 107.2 Automate system administration tasks by scheduling jobs: Configure user access to cron and at services
27. 107.2 Automate system administration tasks by scheduling jobs: Manage cron and at jobs
28. 107.2 Automate system administration tasks by scheduling jobs: Manage cron and at jobs
29. 107.2 Automate system administration tasks by scheduling jobs: Manage cron and at jobs
30. 105.2 Customize or write simple scripts: Use standard sh syntax (loops, tests)
31. 105.2 Customize or write simple scripts: Use command substitution
32. 105.2 Customize or write simple scripts: Test return values for success or failure or other information provided by a command
33. 105.2 Customize or write simple scripts: Use standard sh syntax (loops, tests)

34. 109.1 Fundamentals of Internet protocols: Knowledge about the differences and major features of UDP, TCP, and ICMP
35. 109.1 Fundamentals of Internet protocols: Knowledge about common TCP and UDP ports (20, 21, 22, 23, 25, 53, 80, 110, 119, 139, 143, 161, 443, 465, 993, 995)
36. 109.1 Fundamentals of Internet protocols: Knowledge of the differences between private and public "dotted quad" IP addresses.
37. 109.1 Fundamentals of Internet protocols: Knowledge of the major differences between IPv4 and IPV6
38. 109.3 Basic network troubleshooting: Manually and automatically configure network interfaces and routing tables to include adding, starting, stopping, restarting, deleting, or reconfiguring network interfaces
39. 109.3 Basic network troubleshooting: Debug problems associated with the network configuration
40. 108.4 Manage printers and printing: Basic CUPS configuration (for local and remote printers)
41. 108.4 Manage printers and printing: Manage user print queues
42. 108.4 Manage printers and printing: Manage user print queues
43. 108.1 Maintain system time: Set the hardware clock to the correct time in UTC
44. 108.1 Maintain system time: Basic NTP configuration
45. 108.3 Mail Transfer Agent (MTA) basics: Knowledge of commonly available MTA programs (postfix, sendmail, qmail, exim) (no configuration)
46. 108.3 Mail Transfer Agent (MTA) basics: Configure e-mail forwarding
47. 105.3 SQL data management: Use of basic SQL commands
48. 105.3 SQL data management: Perform basic data manipulation
49. 110.1 Perform security administration tasks

50. 110.1 Perform security administration tasks: Set or change user passwords and password aging information
51. 110.1 Perform security administration tasks: Set up limits on user logins, processes, and memory usage
52. 110.1 Perform security administration tasks: Audit a system to find files with the suid/sgid bit set
53. 110.1 Perform security administration tasks: Being able to use nmap and netstat to discover open ports on a system
54. 108.2 System logging
55. 110.2 Set up host security: Understand the role of TCP wrappers
56. 110.3 Securing data with encryption: Understand the role of OpenSSH 2 server host keys
57. 110.3 Securing data with encryption: Understand the role of OpenSSH 2 server host keys
58. 110.3 Securing data with encryption: Perform basic OpenSSH 2 client configuration and usage
59. 110.3 Securing data with encryption: Perform basic GnuPG configuration and usage
60. 110.3 Securing data with encryption: Perform basic OpenSSH 2 client configuration and usage