Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/2/2022 8:52:19 pm • Time spent: 03:20

Score: 70% Passing Score: 80%

Question 1: ✔ Correct

You have performed an audit and found an active account for an employee with the username *joer*. This user no longer works for the company.

Which command can you use to disable this account?

- **usermod -L joer**
- **usermod -d joer**
- **usermod -u joer**
- **usermod -l joer**

EXPLANATION

Use **usermod -L joer** to lock the user's password. Doing so disables the account.

The **usermod -l joer** command changes the account's login name.

The **-d** flag is used for changing the account's home directory.

The **-u** flag is used for changing the account's numeric ID.

REFERENCES

6.7.3 Linux User Commands and Files

q_linux_usr_cmds_audit_secp7.question.fex

Question 2: ✔ Correct

One of your users, Karen Scott, has recently married and is now Karen Jones. She has requested that her username be changed from kscott to kjones with no other values changed. Which of the following commands would accomplish this?

- **usermod -l kjones kscott**
- **usermod -l kscott kjones**
- **usermod -u kscott kjones**
- **usermod -u kjones kscott**

EXPLANATION

Use the **usermod** command to modify user settings. Use the **-l** flag to signal a change to the username. The correct syntax requires the new username value be given, followed by the old username. The **-u** flag changes the UID number.

REFERENCES

6.7.3 Linux User Commands and Files

q_linux_usr_cmds_user_01_secp7.question.fex

Question 3: ✔ Correct

An employee named Bob Smith, whose username is bsmith, has left the company. You have been instructed to delete his user account and home directory.

Which of the following commands would produce the required outcome? (Select two.)

- [ ] **userdel -h bsmith**
- [ ] **userdel -x bsmith**
- [x] **userdel -r bsmith**
- [ ] **userdel bsmith**
- [x] **userdel bsmith;rm -rf /home/bsmith**

EXPLANATION

The **userdel -r** command deletes a user's home directory and user account. The **userdel** command by itself does not delete a user's home directory and user account. Executing **rm -rf** on the user's home directory after executing **userdel** removes the home directory. The **userdel -h** command displays the syntax and options for the **userdel** command.

REFERENCES

6.7.3 Linux User Commands and Files

q_linux_usr_cmds_user_02_secp7.question.fex

Question 4: ✔ Correct

In the /etc/shadow file, which character in the password field indicates that a standard user account is locked?

!

EXPLANATION

! or *!!* in the password field of /etc/shadow indicates that the account is locked and cannot be used to log in. The /etc/shadow file holds passwords and password expiration information for user accounts.

$ preceding the password identifies the password as an encrypted entry. * indicates a system user account entry (which cannot be used to log in).

REFERENCES

6.7.3 Linux User Commands and Files

q_linux_usr_cmd_lockout_01_secp7.question.fex

Question 5: ✕ Incorrect

Which of the following utilities could you use to lock a user account? (Select two.)

- [x] ~~**ulimit**~~
- [ ] **useradd**
- [ ] **passwd**
- [ ] **userdel**
- [x] **usermod**

EXPLANATION

Use the following utilities to lock a user account:

- **passwd -l** disables (locks) an account. This command inserts *!!* before the password in the /etc/shadow file.
- **usermod -L** disables (locks) an account. This command inserts *!* before the password in the /etc/shadow file.

The **useradd** command creates new user accounts, and **userdel** deletes user accounts from the system.

The **ulimit** command is used to limit computer resources.

REFERENCES

6.7.3 Linux User Commands and Files

q_linux_usr_cmd_lockout_02_secp7.question.fex

Question 6: ✕ Incorrect

You suspect that the gshant user account is locked.

Enter the command you would use in a shell to show the status of the user account.

~~cat /etc/passwd~~ passwd -S gshant

EXPLANATION

Use **passwd -S gshant** to display the status of the gshant user account.

- LK indicates that the user account is locked.
- PS indicates that the user account has a password.

Viewing the /etc/shadow file also displays whether the user account is disabled. The second field for each entry in the /etc/password file is the password field:

- *$* preceding the password identifies the password as an encrypted entry.
- *!* or *!!* indicates the account is locked and cannot be used to log in.
- * indicates a system account entry, which cannot be used to log in.

REFERENCES

6.7.3 Linux User Commands and Files

q_linux_usr_cmd_lockout_03_secp7.question.fex

Question 7: ✔ Correct

What is the effect of the following command?

chage -M 60 -W 10 jsmith

- ➡ Sets the password for jsmith to expire after 60 days and gives a warning 10 days before expiration.
- Sets the password for jsmith to expire after 60 days and sets a minimum of 10 days before a user can change the password again.
- Forces jsmith to keep the password for 60 days before changing it while also giving a warning 10 days before expiration.
- Sets the password for jsmith to expire after 10 days and gives a warning 60 days before expiration.
- Deletes the jsmith user account after 60 days and gives a warning 10 days before expiration.

EXPLANATION

Using **chage -M 60 -W 10 jsmith** sets the password for jsmith to expire after 60 days and gives a warning 10 days before expiration.

Using **chage** sets user passwords to expire. Be aware of the following options:

- **-M** sets the maximum number of days before the password expires.
- **-W** sets the number of days before the password expires that a warning message displays.
- **-m** sets the minimum number of days that must pass after a password change before a user can change the password again.

REFERENCES

6.7.12 Linux User Security and Restriction Facts

q_linux_sec_history_secp7.question.fex

Question 8: ✔ Correct

Which **chage** option keeps a user from changing their password every two weeks?

- **-m 33**
- **-M 33**
- **-a 33**
- **-W 33**

EXPLANATION

Using **chage -m 33** forces a user to keep his or her password for 33 days. This sets the minimum number of days that must pass after a password change before a user can change the password again. Be aware of the other **chage** options:

- **-M** sets the maximum number of days before the password expires.
- **-W** sets the number of days before the password expires that a warning message displays.

The **chage -a** option is not a valid option.

REFERENCES

6.7.12 Linux User Security and Restriction Facts

q_linux_sec_reuse_secp7.question.fex

Question 9: ✔ Correct

Which account type in Linux can modify hard limits using the **ulimit** command?

- Standard
- Administrator
- Root
- User

EXPLANATION

Only the root user in Linux can modify hard limits using the **ulimit** command.

Standard and administrator are Windows user types.

Users can modify soft limits but not hard limits using the **ulimit** command.

REFERENCES

6.7.12 Linux User Security and Restriction Facts

q_linux_sec_root_secp7.question.fex

Question 10: ✕ Incorrect

Which of the following commands would you use to view the current soft limits on a Linux machine?

- ~~**ulimit -u**~~
- **ulimit -a**
- **ulimit -n**
- **ulimit -c**

EXPLANATION

The **ulimit -a** command displays the current limits. The default shows soft limits.

The **ulimit -c** command limits the size of a core dump file.

The **ulimit -n** command limits the maximum number of files that can be open.

The **ulimit -u** command limits the number of concurrent processes a user can run.

REFERENCES

6.7.12 Linux User Security and Restriction Facts

q_linux_sec_ulimit_secp7.question.fex