Exam Report: 7.1.7 Practice Questions

Date: 4/22/2020 9:55:00 am
Time Spent: 2:25

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 4%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

During installation, you must create a root user account for the system.

Which of the following user account number does this account use?

- 0
- ~~1~~
- 10
- 100

Explanation

The root user has an account number of 0 and belongs to group 1.

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_01]

Question 2: Incorrect

You have been asked to temporarily fill in for an administrator who has just been fired. This administrator was known to have lax security standards, and you suspect that passwords are still kept in the /etc/passwd file.

Which of the following entry within the passwd file would indicate that the passwords are stored there?

- eddie:x:100:100::/users/eddie:
- kolton:34uyx:431:0:Back Door:/root:/bin/bash
- adam:x:341:52:Adam Fox:/users/adam:/bin/bash
- ~~clifford:x:687:301:non secure user:/root:~~

Explanation

The second field of the /etc/passwd file holds the password values. If the passwords are stored elsewhere (in /etc/shadow), then an x will appear in this field. If the values are stored in this file, then they will appear in the second field in hashed form.

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_02]

Question 3: Incorrect

During a Fedora distribution installation, you choose to add a regular user account. The only other user that has been added to the system was root.

Which of the following user IDs is MOST likely to be associated with the new user?

- 0
- ~~1~~
- 2
- 101
- 400
- 1000

Explanation

On Fedora (and in most modern distributions of Linux), accounts below 100 or 500 are used for system accounts, and user accounts begin with 1000.

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_03]

Question 4: Incorrect

Given this entry in the /etc/passwd file:

pmallory:x:1001:1050:Paul Mallory:/home/pmallory:/bin/bash

Which of the following is the user ID associated with this entry.

- pmallory
- x
- 1001
- ~~1050~~

Explanation

The user ID (UID) is in the third field of the line for the user. In this question, that value is 1001.

The format for the /etc/passwd file is as follows:

name:password:UID:GID:GECOS:homedirectory:shell

(GECOS is a field that allows a text description of the user account.)

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_04]

Question 5: Incorrect

A file contains the following entry:
sales:x:1001:pclark,mmckay,hsamson

Which of the following files contains similar enties?

- ~~/etc/gshadow~~
- /etc/shadow
-

/etc/group

/etc/passwd

Explanation

The following line is a sample entry in the /etc/group file:

sales:x:1001:pclark,mmckay,hsamson

The /etc/group file holds group information, including the group name, group password, group ID, and group membership information. Be aware of the following details:

- Each entry in the group file identifies a group.
- Each entry contains multiple fields, and fields are separated by colons.

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_05]

Question 6: Incorrect

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 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

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_06]

Question 7: Incorrect

In the /etc/shadow file, which character in the password field indicates that the password is an encrypted entry?

$

!!

!

*

Explanation

In the password field of the /etc/shadow file,*$* preceding the password identifies the password as an encrypted entry. The /etc/shadow file holds passwords and password expiration information for user accounts.

! or *!!* indicates that the account is locked and cannot be used to log in. * indicates a system user account entry (which cannot be used to log in).

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_07]

Question 8: Incorrect

You are an IT consultant for a small company. The company wants to increase the security of their small network. You want to move their passwords from the /etc/passwd file to the /etc/shadow file.

Which of the following utilities will BEST accomplish this task?

- **pwconv**
- ~~**pwck**~~
- **shadow**
- **sync**
- **cp**

Explanation

Use the **pwconv** utility to move passwords from the less-secure /etc/passwd file to the more secure /etc/shadow file. You can execute the opposite of this action with the **pwunconv** utility. Today, however, virtually all Linux distributions ship with shadow files enabled by default.

The **cp** command copies files an directories. The **pwck** command verifies entry in the passwd and shadow files. The **Shadow** command manipulates the contents of the shadow password file. The **sync** command synchronizes cached writes to persistent storage.

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_08]

Question 9: Incorrect

You are viewing the /etc/passwd file, and you notice the following entry:

pclark:x:1001:1001:Petunia Clark:/home/pclark:/bin/bash

What statement BEST describes this entry?

- ~~The pclark user account has not set a password.~~
- The pclark user account is locked.
- The pclark password is stored in the /etc/shadow file.
- The pclark password is the letter *x*.

Explanation

In this case, the x in the password field indicates that the pclark password is stored in the /etc/shadow file. The /etc/shadow file holds passwords and password expiration information for user accounts.

The /etc/passwd file holds user account information. Be aware of the following details:

- Each entry identifies a user account.
- Each entry contains multiple fields, with each field separated by a colon.

Be aware of the following details about the /etc/shadow file:

- Using the /etc/shadow file to separate usernames from passwords increases the security of the users' passwords.
- Each entry corresponds to a user account, and each entry contains multiple fields separated by colons.

An *x* in the password field does not indicate whether the password has been set for the user. An *!*, *!!*, or * in the password field of the /etc/shadow indicates that the corresponding user account is locked and cannot be used to log in.

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_09]

Question 10: Incorrect

You need to identify which user accounts on the Linux system have encrypted passwords.

Which character in the password field of the /etc/shadow file indicates that an encrypted password is set for the user account?

& $

Explanation

The *$* preceding the password identifies the password as an encrypted entry. The following example indicates that the user account has an encrypted password:

pclark:$ab7Y56gu9bs:12567:0:99999:7:::

Be aware of the following details about the /etc/shadow file:

- Using the /etc/shadow file to separate usernames from passwords increases the security of the user passwords.
- Each entry corresponds to a user account, and each entry contains multiple fields, with each field separated by a colon.

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_10]

Question 11: Incorrect

The graphics driver was recently updated on a system. Now, the graphical user interface (GUI) is not displaying, preventing the user from logging in. You need to access the system locally. Which of the following commands will access the tty2 terminal?

- **Ctrl+Alt+F2**
- ~~**tty**~~
- /dev/tty2
- **ssh localhost tty**

Explanation

On most Linux systems, tty2 can be accessed using **Ctrl+Alt+F2**.

ssh localhost tty will not access tty2, but returns "Not a tty."

tty will display "/dev/pts/0".

/dev/tty2 represents tty2.

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_LOCAL_ACCESS]

Question 12: Incorrect

A user is trying to access a system using SSH, but can't connect. The user has verified the correct hostname and IP address.

Which of the following should the user check to troubleshoot the issue? (Choose TWO).

- Verify that the vncd.services is running and listening on the default port.
- ~~Check that encryption is not enabled on the local SSH client.~~
- Check the firewall to see if the default SSH port 22 is blocked.
- Check whether the SSH daemon is running.

- [ ] Confirm that access is available for all virtual terminals.

Explanation

In order to access a Linux computer using SSH, the SSH daemon must be running. SSH uses TCP port 22, which must not be blocked by the network.

Access to the virtual terminals is independent of SSH access.

VNC can ride over SSH, but the vnc daemon is not required. for SSH connectivity.

Encryption is part of the SSH protocol.

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_REMOTE_ACCESS]

Question 13: Incorrect

A user type has the following qualities:

- Created by default during the Linux installation
- Used by the system for specific roles
- Not used to log into the system

Which of the following user types has these qualities?

- [ ] System or service user
- [x] ~~Root user~~
- [ ] Guest user
- [ ] Standard user

Explanation

A system or service user is created by default during the Linux installation and used by the system for specific roles.

A standard user account can log into the system.

A root user can log into the system and perform administrative tasks.

A guest user account is not created on a Linux system. Other operating systems, such as Windows, create a guest account that can log in to the system.

References

Linux Pro - 7.1 User and Group Overview
[e_usrgrp_lp5.exam.xml Q_USERS_LP5_SERVICE_USER]