Exam Report: 15.2.8 Practice Questions
_____

Date: 4/4/28 6:01:12 pm   Candidate: Garsteck, Matthew
Time Spent: 1:00   Login: mGarsteck
_____

Overall Performance

Your Score: 31%

Passing Score: 80%

View results by: ◯ Objective Analysis   ⦿ Individual Responses
_____

Individual Responses

▼ **Question 1:**   <u>Correct</u>

What is the effect of the following command?

chage -M 60 -W 10 jsmith

◯ Sets the password for *jsmith* to expire after 6 days and gives a warning 10 days before it expires.

◯ Sets the password for *jsmith* to expire after 6 days and gives a warning 10 days before it expires.

➡ ⦿ Sets the password for *jsmith* to expire after 60 days and gives a warning 10 days before it expires.

◯ Forces *jsmith* to keep the password 60 days before changing it and gives a warning 10 days before changing it.

◯ Deletes the *jsmith* user account after 60 days and gives a warning 10 days before it expires.

Explanation

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

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 has been changes before a user can change the password again.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_01]

▼ **Question 2:**   <u>Incorrect</u>

What **chage** command should you enter at the command prompt to set the password for *jsmith* to expire after 60 days and give a warning 10 days before it expires?

[   ]   chage -M 60 -W 10 jsmith

Explanation

chage -M 60 -W 10 jsmith sets the password for *jsmith* to expire after 60 days and gives a warning 10 days before it expires. Use **chage** to set 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 has been changes before a user can change the password again.

Look in the /etc/shadow file to see current limits for users.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_02]

▼ **Question 3:**　　　　　　　　<u>Correct</u>

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

　　　⚪ **-a 33**

➡　　⦿ **-m 33**

　　　⚪ **-M 33**

　　　⚪ **-W 33**

Explanation

chage -m 33 prohibits the user fromchanging his password for 33 days. This sets the minimum number of days that must pass after a password has been changes 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.

chage -a is not a valid option.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_03]

▼ **Question 4:**　　　　　　　　<u>Incorrect</u>

What do you enter at the command prompt to prevent the shell from using too much of the system's resources?

[　　　　　　　　　　　　　　　]　　　ulimit

Explanation

Use **ulimit** to limit computer resources used for applications launched from the shell. Limits can be hard or soft limits. Soft limits can be temporarily exceeded up to the hard limit setting. Users can modify soft limits, but only root can modify hard limits. Options include the following:

- **-c** limits the size of a core dump file. The value is in blocks.
- **-f** limits the file size of files created using the shell session. The value is in blocks.
- **-n** limits the maximum number of open files.
- **-t** limits the amount of CPU time a process can use. This is set in seconds.
- **-u** limits the number of concurrent processes a user can run.
- **-d** limits the maximum amount of memory a process can use. The value is in kilobytes.
- **-H** sets a hard resource limit.
- **-S** sets a soft resource limit.
- **-a** displays current limits. The default shows soft limits.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_04]

▼ **Question 5:**　　　　　　　　<u>Correct</u>

What effect does the **ulimit -t 600** command have on a Linux system?

　　　⚪ Limits the concurrent processes a user can run to 10.

　　　⚪ Limits the maximum number of processes to 600.

➡ ⦿ Limits CPU time for a process to 10 minutes.

○ Limits CPU time for a process to 600 minutes.

Explanation

ulimit -t 600 limits CPU time for a process to 10 minutes. The value is set in seconds. This sets both hard and soft limits.

Use **ulimit** to limit computer resources used for applications launched from the shell. Limits can be hard of soft limits. Soft limits can be temporarily exceeded up to the hard limit setting. Users can modify soft limits, but only root can modify hard limits. Be aware of the other **ulimit** options:

- **-c** limits the size of a core dump file. The value is in blocks.
- **-f** limits the file size of files created using the shell session. The value is in blocks. **-n** limits the maximum number of open files.
- **-u** limits the number of concurrent processes a user can run.
- **-d** limits the maximum amount of memory a process can use. The value is in kilobytes.
- **-H** sets a hard resource limit.
- **-S** sets a soft resource limit.
- **-a** displays current limits. The default shows soft limits.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_05]

▼ **Question 6:**   <u>Incorrect</u>

What is the full path and filename of the file you should edit to limit the amount of concurrent logins for a specific user?

[   ]   /etc/security/limits.conf

Explanation

Use the /etc/security/limits.conf file to limit resource use for all applications. This is from the pam_limits module of the Plugable Authentication Modules (PAM) module set. Entries in /etc/security/limits.conf contain *Entity Type Limit Value.*

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_06]

▼ **Question 7:**   <u>Incorrect</u>

Within the /etc/security/limits.conf file, you notice the following entry:

@guests hard maxlogins 3

What effect does this line have on the Linux system?

○ Limits the maximum file size that the guest group can create to 3GB.

⦿ ~~Limits concurrent logins from the same user to three.~~

➡ ○ Limits the number of maximum logins from the guest group to three.

○ Limits the total amount of memory used by the guest group to 3 MB

Explanation

@guests hard maxlogins 3 limits the number of max logins from the guest group to three. Use the /etc/security/limits.conf file to limit resource use for all applications. Entries in /etc/security/limits.conf contain the following *Entity Type Limit Value.*

jsmith hard fsize 1024 limits the maximum file size that jsmith can create to 1024 KB.

* hard maxlogins 1 limits concurrent logins from the same user to one.

* soft cpu 10 sets a soft limit of 10 minutes on the amount of CPU time any single process for any user can take.

rss hard rss 5000 limits the total amount of memory available to a single user to 5 MB

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_07]

▼ **Question 8:**   Incorrect

You are limiting the total amount of memory a user can take up when they use the X Windows System. Which of the following limit keywords should you use?

◯ **nproc**

◉ ~~**cpu**~~

◯ **data**

➡ ◯ **rss**

Explanation

Use the /etc/security/limits.conf file to limit resource use for all applications. Entries in /etc/security/limits.conf contain *Entity Type Limit Value.*

Limits in the /etc/security/limits.conf file include the following:

   • **rss** limits the total amount of memory a user can use. The value uses kilobytes.
   • **core** limits the size of core dump files. The value uses kilobytes.
   • **data** limits the amount of ram an application can use. The value uses kilobytes.
   • **fsize** limits maximum file size. The value uses kilobytes.
   • **nofile** limits the number of concurrently open data files.
   • **cpu** limits the amount of CPU time a process can use. The value uses minutes.
   • **nproc** limits the number of concurrent processes a user can have.
   • **maxlogins** limits the number of concurrent logins.
   • **priority** sets process priority limits. The value range is from -20 (highest priority) to 19 (lowest priority) with 0 being the default.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_08]

▼ **Question 9:**   Correct

Which of the following is a pair of virtual character devices that provide a bidirectional communication channel? (One end of the channel is called the master; the other end is called the slave.)

◯ virtual terminal (tty)

◯ /dev/console

➡ ◉ pseudo-terminal (pty)

◯ /dev/null

Explanation

pseudo-terminal (pty) is a pair of virtual character devices that provide a bidirectional communication channel. One end of the channel is called the master, and the other end is called the slave.

virtual terminal (tty) is a tty device.

/dev/null is a device file that is associate with a null device that is commonly used for disposing unwanted output streams.

/dev/console is the system console.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_PTY]

▼ **Question 10:**   _Incorrect_

Which of the following is the associated device file for that terminal?

○ /dev/null

◉ ~~/dev/port~~

○ /dev/lp0

➡ ○ /dev/tty5

Explanation

/dev/tty5 is a device file that is associated with the computer's controlling terminal or the shell's window.

/dev/lp0 is a device file associated to the first parallel port.

/dev/null is a device file that is associate with a null device that is commonly used for disposing unwanted output streams.

/dev/port is a device associated with system ports.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_RESTRICT_TTY]

▼ **Question 11:**   _Incorrect_

The root user attempted to log in to the system using tty and was denied access. The pam_securetty module uses a configuration file to determine which virtual terminals (tty#) that root is allowed to log in from. Which of the following files would the root user check to see which terminals are permitted?

○ pam_securetty

○ /etc/pam.d/password-auth

◉ ~~pam_ldap.conf~~

➡ ○ /etc/securetty

Explanation

When a root user attempts to log in to a system using tty, the pam_securetty module uses the /etc/securetty file to decide which virtual terminals (tty#) root is allowed to log in from.

Pam_ldap stores its configuration in the pam_ldap.conf file.

/etc/pam.d/password-auth is a pam configuration file that is used to configure settings such as the number of incorrect password attempts before locking the account.

pam_securetty is a module, not a configuration file.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_USR_RESTRICT_LP5_TTY]

▼ **Question 12:**   _Incorrect_

What is the purpose of the **find / type f -perm -o=x -ls** command?

○ Audit files in the root directory that have execute permissions for group owners.

➡ ○ Audit files in the root directory that have execute permissions for others.

○ Audit files in the root directory that have execute permissions for the owner.

Explanation

find / type f -perm -o=x -ls audits and displays files in the root directory that have execute permissions for others. Use the **find / type f -perm** command with the following options to audit for files that pose a security risk:

- **-o=x** audits for the execute permission for others.
- **-o=w** audits for the write permission for others.
- **-g=x** audits for the execute permissions for group owners.
- **-u=x** audits for the execute permission for the owner.
- **-u=s** audits for the SUID bit.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_FILE_AUD_F_LP5_01]

▼ **Question 13:**   Incorrect

What is the purpose of the **find / type f -perm -u=s -ls** command?

➡ ○ Audit files in the root directory that have the SUID bit set.

○ Audit files in the root directory that have execute permissions for the owner.

○ Audit files in the root directory that have execute permissions for others.

○ Audit files in the root directory that have execute permissions for group owners.

Explanation

find / type f -perm -u=s -ls audits and displays files in the root directory that have the SUID bit set. Use the **find / type f -perm** command with the following options to audit for files that pose a security risk:

- **-o=x** audits for the execute permission for others.
- **-o=w** audits for the write permission for others.
- **-g=x** audits for the execute permissions for group owners.
- **-u=x** audits for the execute permission for the owner.
- **-u=s** audits for the SUID bit.

References

Linux Pro - 15.2 User Security and Restriction
[e_usrsec_lp5.exam.xml Q_FILE_AUD_F_LP5_02]