Exam Report: 8.11.4 Practice Questions

Date: 1/27/2020 8:21:38 pm
Time Spent: 10:04

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 20%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

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 it expires.
- Sets the password for *jsmith* to expire after 6 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.
- Sets the password for *jsmith* to expire after 6 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 change before a user can change the password again.

References

LabSim for Security Pro, Section 8.11.
[All Questions SecPro2017_v6.exm LINUX_USRSEC_01]

Question 2: Incorrect

What **chage** command should you use to set the password for *jsmith* to expire after 60 days and give a warning 10 days before it expires? (Tip: Enter the command as if at the command prompt.)

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 changed before a user can change the password again.

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

References

LabSim for Security Pro, Section 8.11.
[All Questions SecPro2017_v6.exm LINUX_USRSEC_02]

Question 3: Incorrect

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

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

Explanation

chage -m 33 forces the user to keep his 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.

chage -a is not a valid option.

References

LabSim for Security Pro, Section 8.11.
[All Questions SecPro2017_v6.exm LINUX_USRSEC_03]

Question 4: Incorrect

Which file should you edit to limit the amount of concurrent logins for a specific user? (Tip: Enter the full path to the file.)

[ ] /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 the following:

Entity Type Limit Value

References

LabSim for Security Pro, Section 8.11.
[All Questions SecPro2017_v6.exm LINUX_USRSEC_04]

Question 5: Correct

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 number of logins from the Guest group to three.
- Limits the total amount of memory used by the Guest group to 3 MB
- Limits concurrent logins from the same user to three.
- Limits the maximum file size that the Guest group can create to 3GB.

Explanation

@guests hard maxlogins 3 limits the number of 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

LabSim for Security Pro, Section 8.11.
[All Questions SecPro2017_v6.exm LINUX_USRSEC_05]