6.7.12 Linux User Security and Restriction Facts

This lesson covers the following topics:

- User security
- User security commands

User Security

When considering user security, keep the following in mind:

- Users should be trained to use secure passwords. Secure passwords use numbers and letters and are more than seven characters in length.
- Passwords should expire periodically but not too often.
- Administrators can limit the resources that the user can access.

User Security Commands

The following table describes Linux commands used to promote user security and restrictions:

Command	Description
chage	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.
ulimit	Limits 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 the root user can modify hard limits. Options include: - **-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 files that can be open. - **-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.