**327.1 Discretionary Access Control**

**Description:**

Candidates are required to understand Discretionary Access Control and know how to implement it using Access Control Lists. Additionally, candidates are required to understand and know how to use Extended Attributes.

**Key Knowledge Areas:**

* Understand and manage file ownership and permissions, including SUID and SGID
* Understand and manage access control lists
* Understand and manage extended attributes and attribute classes

**Terms and Utilities:**

* getfacl
* setfacl
* getfattr
* setfattr

**Understand and manage file ownership and permissions, including SUID and SGID**

blablabla

|  |  |  |  |
| --- | --- | --- | --- |
|  | Character | Effect on files | Effect on dirs |
|  |  |  |  |
|  |  |  |  |

**chown**

**chown** - change file owner and group.

Synopsis:

**chown** [OPTION]... [OWNER][:[GROUP]] FILE...

**chown** [OPTION]... --reference=RFILE FILE...

Description:

1) **chown** changes the user and/or group ownership of each given file.

2) If only an owner (a user name/UID) is given, that user is made the owner of each given file, and the files' group is not changed.

3) If the owner is followed by a colon and a group name/GID, with no spaces between them, the group ownership of the files is changed as well.

4) If a colon but no group name follows the user name, that user is made the owner of the files and the group of the files is changed to that user's login group.

5) If the colon and group are given, but the owner is omitted, only the group of the files is changed; in this case, **chown** performs the same function as **chgrp**.

6) If only a colon is given, or if the entire operand is empty, neither the owner nor the group is changed.

Options:

**-c, --changes**

like verbose but report only when a change is made

**--dereference**

affect the referent of each symbolic link (this is the default), rather than the symbolic link itself

**-h, --no-dereference**

affect each symbolic link instead of any referenced file (useful only on systems that can change the ownership of a symlink)

**--from=CURRENT\_OWNER:CURRENT\_GROUP**

change the owner and/or group of each file only if its current owner and/or group match those specified here. Either may be omitted, in which case a match is not required for the omitted attribute.

**--no-preserve-root**

do not treat '/' specially (the default)

**--preserve-root**

fail to operate recursively on '/'

**-f, --silent, --quiet**

suppress most error messages

**--reference=RFILE**

use RFILE's owner and group rather than specifying OWNER:GROUP values

**-R, --recursive**

operate on files and directories recursively

**-v, --verbose**

output a diagnostic for every file processed

The following options modify how a hierarchy is traversed when the **-R** option is also specified. If more than one is specified, only the final one takes effect:

**-H**

if a command line argument is a symbolic link to a directory, traverse it

**-L**

traverse every symbolic link to a directory encountered

**-P**

do not traverse any symbolic links (default)

**--help**

**--version**

**chgrp**

**chgrp** - change group ownership

Synopsis:

**chgrp** [OPTION]... GROUP FILE...

**chgrp** [OPTION]... --reference=RFILE FILE...

Description:

1) Change the group of each *FILE* to *GROUP*.

2) With **--reference**, change the group of each *FILE* to that of *RFILE*.

Options:

**-c, --changes**

like verbose but report only when a change is made

**-f, --silent, --quiet**

suppress most error messages

**-v, --verbose**

output a diagnostic for every file processed

**--dereference**

affect the referent of each symbolic link (this is the default), rather than the symbolic link itself

**-h, --no-dereference**

affect symbolic links instead of any referenced file (useful only on systems that can change the ownership of a symlink)

**--no-preserve-root**

do not treat '/' specially (the default)

**--preserve-root**

fail to operate recursively on '/'

**--reference=RFILE**

use RFILE's group rather than specifying a GROUP value

**-R, --recursive**

operate on files and directories recursively

The following options modify how a hierarchy is traversed when the -R option is also specified. If more than one is specified, only the final one takes effect:

**-H**

if a command line argument is a symbolic link to a directory, traverse it

**-L**

traverse every symbolic link to a directory encountered

**-P**

do not traverse any symbolic links (default)

**--help**

**--version**

**chmod**

**chmod** - change file mode bits

Synopsis:

**chmod** [OPTION]... MODE[,MODE]... FILE...

**chmod** [OPTION]... OCTAL-MODE FILE...

**chmod** [OPTION]... --reference=RFILE FILE...

Description:

1) **chmod** changes the file mode bits of each given file according to mode, which can be either a symbolic representation of changes to make, or an octal number representing the bit pattern for the new mode bits.

2) The format of a symbolic mode is *[****ugoa...****][[****+-=****][perms...]...]*, where *perms* is either zero or more letters from the set ***rwxXst***, or a single letter from the set ***ugo***.

3) ***ugoa***: ***u*** - user, ***g*** - group, ***o*** - other users, ***a*** - all users. If none of these are given, the effect is as if ***a*** were given, but bits that are set in the **umask** are not affected.

4) ***+***: selected file mode to be added to the existing file mode; ***-***: selected file mode to be removed from the existing file mode; ***=***: selected file mode to be added and causes unmentioned bits to be removed except that a directory's unmentioned set user and group ID bits are not affected.

5) ***rwxXst***: ***r*** - read, ***w*** - write, ***x*** - execute (or search for directories), ***X*** - execute/search only if the file is a directory or already has execute permission for some user, ***s*** - set user or group ID on execution, ***t*** - restricted deletion flag or sticky bit. Instead of one or more of these letters, you can specify exactly one of the letters ***ugo***: ***u*** - for user, ***g*** - for group, ***o*** – for other users.

6) A numeric mode is from one to four octal digits (0-7), derived by adding up the bits with values 4, 2, and 1. Omitted digits are assumed to be leading zeros. The first digit selects the set user ID (4) and set group ID (2) and restricted deletion or sticky (1) attributes. The second digit selects permissions for the user: read (4), write (2), and execute (1); the third selects permissions group; the fourth for other users.

7) **chmod** never changes the permissions of symbolic links: for each symbolic link listed on the command line, **chmod** changes the permissions of the pointed-to file. In contrast, **chmod** ignores symbolic links encountered during recursive directory traversals.

8) **Setuid and Setgid Bits**: **chmod** clears the set-group-ID bit of a regular file if the file's group ID does not match the user's effective group ID or one of the user's supplementary group IDs, unless the user has appropriate privileges. Additional restrictions may cause the set-user-ID and set-group-ID bits of MODE or RFILE to be ignored. **chmod** preserves a directory's set-user-ID and set-group-ID bits unless you explicitly specify otherwise. You can set or clear the bits with symbolic modes like ***u+s*** and ***g-s***, and you can set (but not clear) the bits with a numeric mode.

9) **Restricted Deletion Flag or Sticky Bit**: The restricted deletion flag or sticky bit is a single bit, whose interpretation depends on the file type. For directories, it prevents unprivileged users from removing or renaming a file in the directory unless they own the file or the directory; this is called the restricted deletion flag for the directory, and is commonly found on world-writable directories like /tmp. For regular files on some older systems, the bit saves the program's text image on the swap device so it will load more quickly when run; this is called the sticky bit.

Options:

Change the mode of each *FILE* to *MODE*.

**-c, --changes**

like verbose but report only when a change is made

**--no-preserve-root**

do not treat '/' specially (the default)

**--preserve-root**

fail to operate recursively on '/'

**-f, --silent, --quiet**

suppress most error messages

**-v, --verbose**

output a diagnostic for every file processed

**--reference=RFILE**

use RFILE's mode instead of MODE values

**-R, --recursive**

change files and directories recursively

**--help**

**--version**

Each *MODE* is of the form '*[ugoa]\*([-+=]([rwxXst]\*|[ugo]))+*'.

**umask**

**Understand and manage access control lists**

blablabla

**Understand and manage extended attributes and attribute classes**

blablabla