

Changing File Attributes

This tip explains how to use `chattr` to keep important system files secure. The "change attribute" command, or `chattr`, can be used to add or change existing file attributes for things such as synchronous updates, tighter file security, and more. However, this command is only available on `ext2` or `ext3` partitions.

A list of common attributes and their associated flags is listed below. For a more complete list see `man chattr`.

- (A) Don't update atime
- (S) synchronous updates
- (a) append only
- (d) no dump
- (i) immutable
- (j) data journalling
- (t) no tail-merging

Note: The 'j' option can only be used with `ext3`.

Note: The 'j', 'a' and 'i' options are only available to the superuser.

To set attributes on files, use the `chattr` command and to view attributes, use the `lsattr` command.

Code Listing 1: Examples of using `chattr` and `lsattr`

```
// Set the immutable bit on a file so it cannot be changed or removed
# chattr +i myfile
# lsattr myfile
----i----- myfile
// Testing the immutable flag by attempting to delete the file
# rm myfile
rm: cannot remove `myfile': Operation not permitted
// Set myfile to append-only
# chattr +a myfile
# lsattr myfile
-----a----- myfile
# echo testing > myfile
myfile: Operation not permitted
# echo testing >> myfile
// no errors - file was appended to
```

Some instances where this may be useful is keeping important files safe from deletion. Remember that even `root` can't delete a file that is immutable or append-only without first explicitly removing that attribute. Using this flag on `/etc/passwd` or `/etc/shadow` files keeps them safe from an accidental `rm -f` and also ensures no new accounts can be added in the event of an exploit. Keeping other files append-only means once they are written, that data can't be changed. Logs are a good candidate for this to keep them from being tampered with. With `chattr` and `lsattr`, you now have a few new tools to keep your system secure.

From <http://www.gentoo.org/news/en/gwn/20030407-newsletter.xml>