Chattr To Prevent File Alteration On Linux

Hello readers,

Some of you already know that chattr is the command in the Linux operating system that allows a user to set certain attributes of a file residing on a Linux file system. lsattr is the command that displays the attributes of a file.

For security purposes there are specific files that should be locked down using this method to prevent system access from non root users. (Or unauthorized users)

Setting the immutable attribute on files **/etc/passwd** or **/etc/shadow**, makes them secure from an accidental removal and also will disable user account creation.

Protecting important files

You can protect important files such as:

- /etc/php.ini
- /etc/passwd
- /etc/shadow
- /etc/group and more

Protecting SSH keys using chattr

You can use chattr to lockdown /home/ .ssh/id_rsa If you follow the steps outlined here.

If it prevents you from adding new users you can revoke the chattr using chattr -i for example if the public key was locked using chattr it would look like

sudo chattr + /home/ .ssh/id_rsa.pub

and to revoke it would simply be

sudo chattr -i /home/ .ssh/id_rsa.pub

Firewall rules and chattr

Even from simple firewalls in Linux like ufw (view using gufw) a table has a location and that location can be locked to prevent lsattr from viewing it. This will not prevent sniffing but will prevent altering the table from a lower level account.

Documents and chattr

From command line cd into the directory of the document i.e. cd/Documents then ls to see which documents are there and if the sudo command followed by chattr, followed by the document name i.e.

sudo chattr example.pdf

Security on Linux can often use IDS like Samain, Suricata, Snort, all of which have writable tables all of which could theoretically be encrypted, use chattr, or both.