

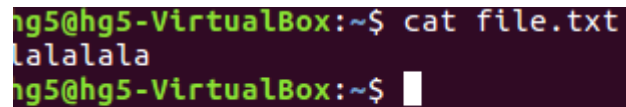
README

1. In this MP, I designed the mp4 security module, when booting with this kernel, user can assign security attribute to files to enforce access control as they want.

2. My module can successfully compile and works good when rebooting.

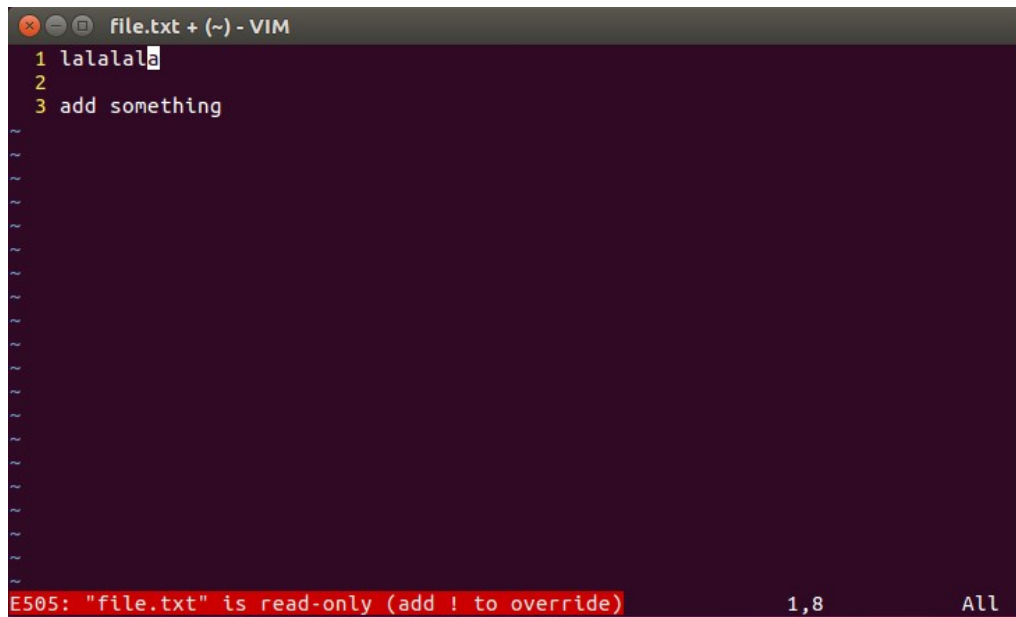
I also tested the kernel with test.perm and test.perm.unload. They results are corrent.

(1) . The original file.txt is like this:

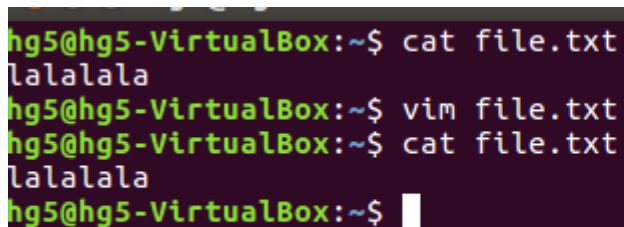


```
hg5@hg5-VirtualBox:~$ cat file.txt
lalalala
hg5@hg5-VirtualBox:~$
```

(2). After enforcing the test.perm. I tried to edit the file, but I failed because the access control (read-only)

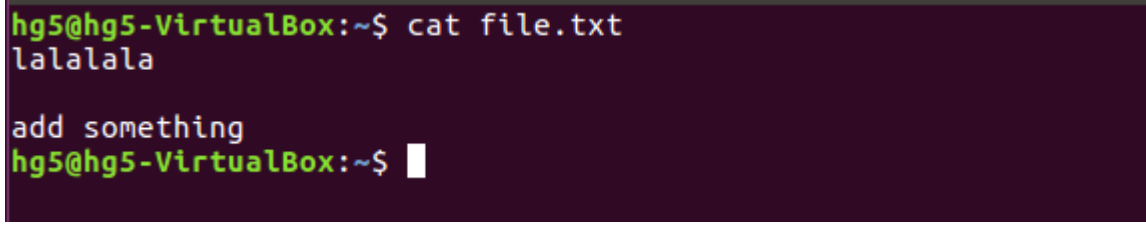


(3). I cannot change the file for access control.



```
hg5@hg5-VirtualBox:~$ cat file.txt
lalalala
hg5@hg5-VirtualBox:~$ vim file.txt
hg5@hg5-VirtualBox:~$ cat file.txt
lalalala
hg5@hg5-VirtualBox:~$
```

(4). After “source test.perm.unload” I can edit the file now.

A terminal window with a dark purple background. The prompt is 'hg5@hg5-VirtualBox:~\$'. The user enters 'cat file.txt' and the output is 'lalalala'. Then the user enters 'add something' and the prompt returns to 'hg5@hg5-VirtualBox:~\$' with a white cursor.

```
hg5@hg5-VirtualBox:~$ cat file.txt
lalalala

add something
hg5@hg5-VirtualBox:~$
```

3. For the least privilege policy. I use strace on /usr/bin/passwd. I got all the permission denied file accesses. And then, apply our security policies on these files to grant accesses.

The least privilege should be:

```
sudo setfattr -n security.mp4 -v target /usr/bin/passwd
sudo setfattr -n security.mp4 -v read-only /etc/shadow
sudo setfattr -n security.mp4 -v read-write /etc/.pwd.lock
```