INTROSEC ASSIGNMENT 2
AppArmor

Group 35

Volkan Sahin
Achyut Jagini

Experiment

We decided to create an Apparmor profile for nano editor.
We used the Xubuntu VM used for assignment 1.

We logged in as user lab and create folders such that there is directory home/lab/student/group35. After loading the apparmor profile ,nano will only be able to write to and create files in this directory.

To arrive at a solution first we looked at documentation available on internet .The links https://wiki.ubuntu.com/AppArmor and https://ubuntu.com/server/docs/security-apparmor gave us a good idea. We learned the necessary commands to use apparmor and how to write rules.

We also looked at apparmor man pages.

https://gitlab.com/apparmor/apparmor/-/wikis/Profiling_by_hand
also helped to understand the process of writing a profile.

We first created a preliminary profile file usr.bin.nano in the /etc/apparmor.d/ directory.

```
#include <tunables/global>
/usr/bin/nano {
}
```

tunables/global is the global preamble (to pull in variables for HOME and use system aliases.[3]

After this we start writing the lines into the profile file.

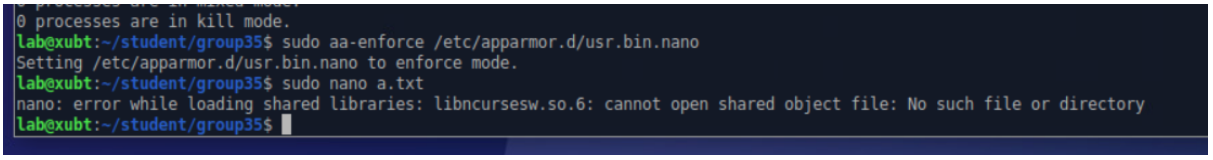
Steps for arriving at the solution

To see location of nano system files

Rules are added in profile to allow access to nano system files

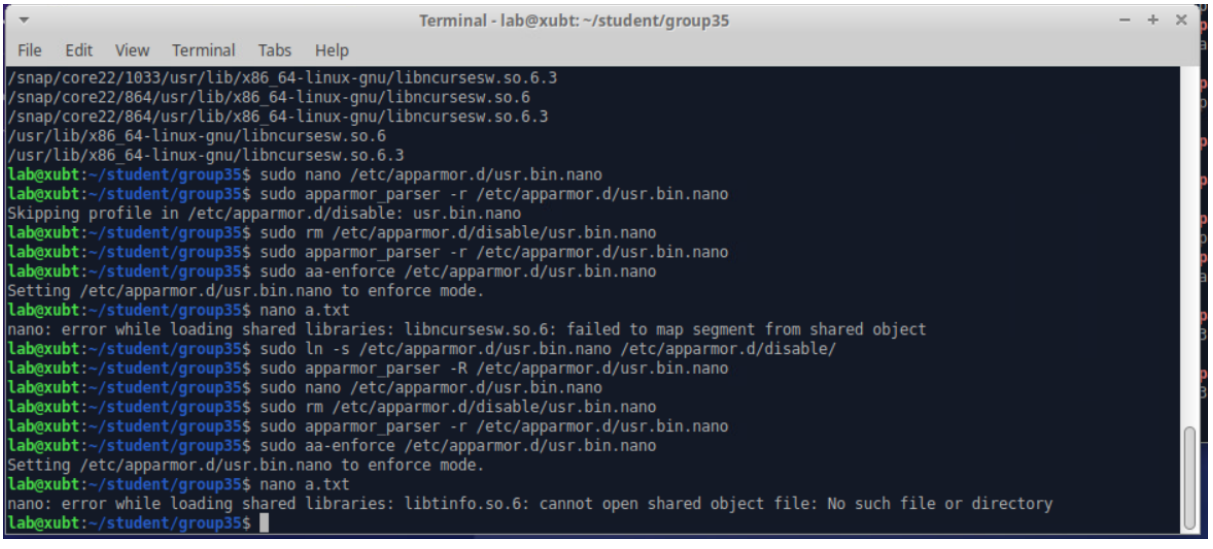
In between creating profile we see nano requires access to various libraries for interacting with terminal such as libncurses ,libc, libtinfo, terminfo.If access to these libraries is not included as rules in profile ,cannot use nano.

libncurses

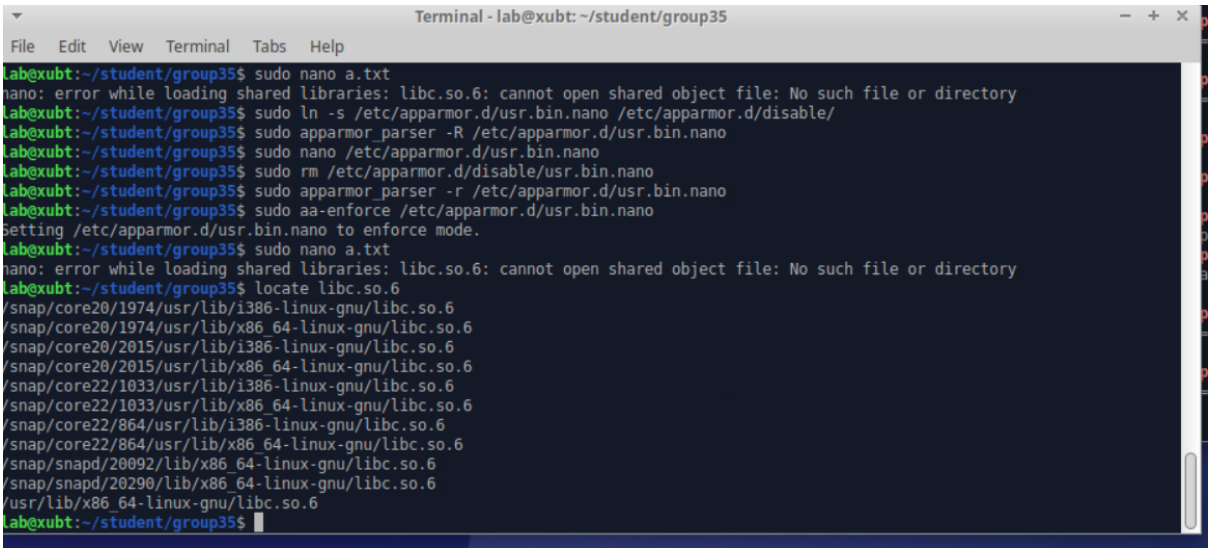


rules are added to allow access to these libraries

libtinfo



libc



The logs are opened in another terminal .
When viewing the apparmor logs after writing the incomplete profile and loading the profile to check it .

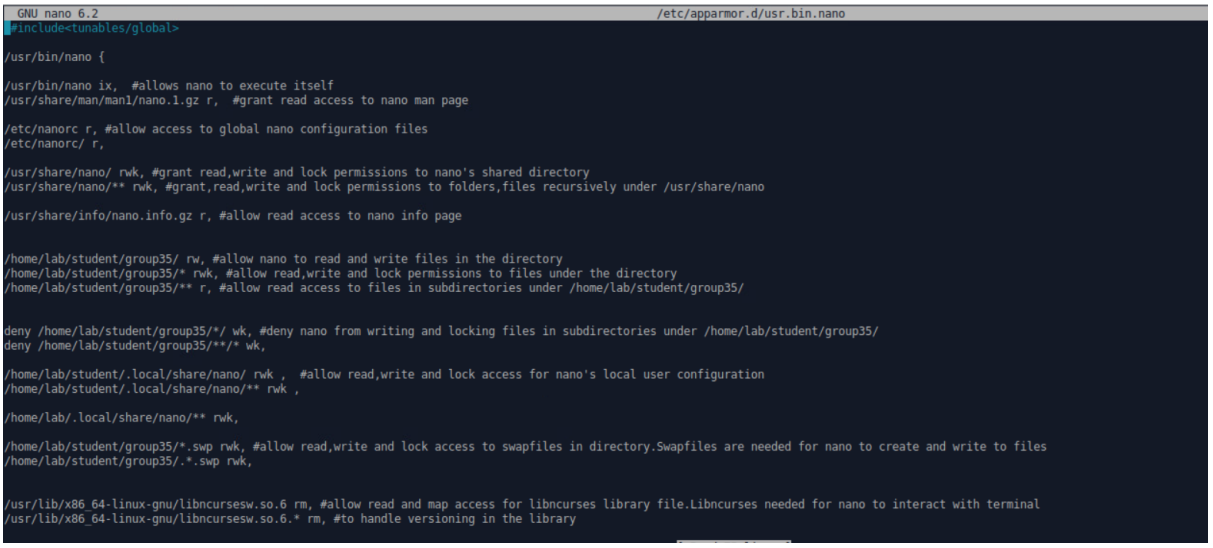
When trying to test nano , trying to use nano is not possible without some more access rules.
These file paths are also in the logs with apparmor=”DENIED” message

Hence rules need to be added to allow access to these so nano can be used

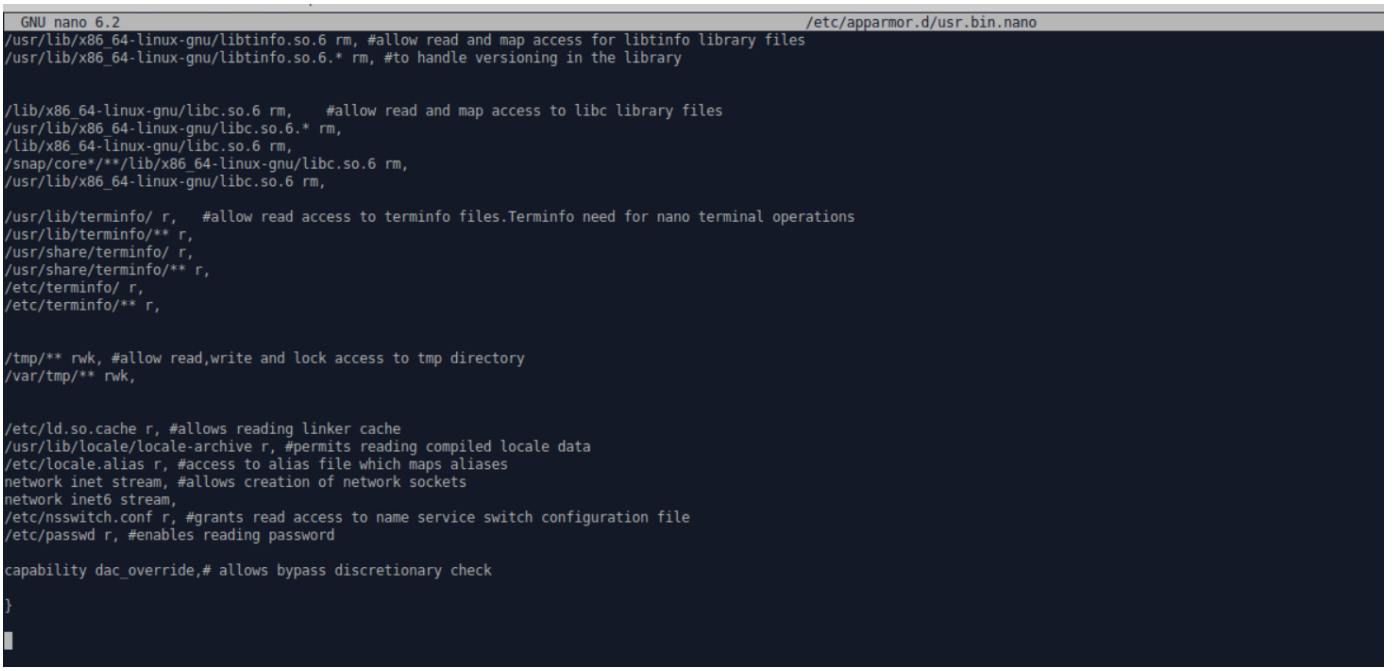
/etc/ld.so.cache r, #allows reading linker cache
/usr/lib/locale/locale-archive r, #permits reading compiled locale data
/etc/locale.alias r, #access to alias file which maps aliases
network inet stream, #allows creation of network sockets
network inet6 stream,

/etc/nsswitch.conf r, #grants read access to name service switch configuration file
/etc/passwd r, #enables reading system's password file

Final profile



```
 GNU nano 6.2                                                    /etc/apparmor.d/usr.bin.nano
#include<tunables/global>

/usr/bin/nano {

/usr/bin/nano ix,  #allows nano to execute itself
/usr/share/man/man1/nano.1.gz r,  #grant read access to nano man page

/etc/nanorc r, #allow access to global nano configuration files
/etc/nanorc/ r,

/usr/share/nano/ rwk, #grant read,write and lock permissions to nano's shared directory
/usr/share/nano/** rwk, #grant,read,write and lock permissions to folders,files recursively under /usr/share/nano

/usr/share/info/nano.info.gz r, #allow read access to nano info page


/home/lab/student/group35/ rw, #allow nano to read and write files in the directory
/home/lab/student/group35/* rwk, #allow read,write and lock permissions to files under the directory
/home/lab/student/group35/** r, #allow read access to files in subdirectories under /home/lab/student/group35/


deny /home/lab/student/group35/*/ wk, #deny nano from writing and locking files in subdirectories under /home/lab/student/group35/
deny /home/lab/student/group35/**/* wk,

/home/lab/student/.local/share/nano/ rwk ,  #allow read,write and lock access for nano's local user configuration
/home/lab/student/.local/share/nano/** rwk ,

/home/lab/.local/share/nano/** rwk,

/home/lab/student/group35/*.swp rwk, #allow read,write and lock access to swapfiles in directory.Swapfiles are needed for nano to create and write to files
/home/lab/student/group35/.*.swp rwk,


/usr/lib/x86_64-linux-gnu/libncursesw.so.6 rm, #allow read and map access for libncurses library file.Libncurses needed for nano to interact with terminal
/usr/lib/x86_64-linux-gnu/libncursesw.so.6.* rm, #to handle versioning in the library
```



```
 GNU nano 6.2                                                    /etc/apparmor.d/usr.bin.nano
/usr/lib/x86_64-linux-gnu/libtinfo.so.6 rm, #allow read and map access for libtinfo library files
/usr/lib/x86_64-linux-gnu/libtinfo.so.6.* rm, #to handle versioning in the library


/lib/x86_64-linux-gnu/libc.so.6 rm,    #allow read and map access to libc library files
/usr/lib/x86_64-linux-gnu/libc.so.6.* rm,
/lib/x86_64-linux-gnu/libc.so.6 rm,
/snap/core*/**/lib/x86_64-linux-gnu/libc.so.6 rm,
/usr/lib/x86_64-linux-gnu/libc.so.6 rm,

/usr/lib/terminfo/ r,   #allow read access to terminfo files.Terminfo need for nano terminal operations
/usr/lib/terminfo/** r,
/usr/share/terminfo/ r,
/usr/share/terminfo/** r,
/etc/terminfo/ r,
/etc/terminfo/** r,


/tmp/** rwk, #allow read,write and lock access to tmp directory
/var/tmp/** rwk,


/etc/ld.so.cache r, #allows reading linker cache
/usr/lib/locale/locale-archive r, #permits reading compiled locale data
/etc/locale.alias r, #access to alias file which maps aliases
network inet stream, #allows creation of network sockets
network inet6 stream,
/etc/nsswitch.conf r, #grants read access to name service switch configuration file
/etc/passwd r, #enables reading password

capability dac_override,# allows bypass discretionary check

}
```

Profile code (For testing use file included with submission)

```
 #include<tunables/global>

/usr/bin/nano {

/usr/bin/nano ix,  #allows nano to execute itself
/usr/share/man/man1/nano.1.gz r,  #grant read access to nano man page

/etc/nanorc r,  #allow access to global nano configuration files
/etc/nanorc/ r

/usr/share/nano/ rwk, #grant read,write and lock permissions to nano's shared directory
/usr/share/nano/** rwk, #grant,read,write and lock permissions to folders,files recursively under /usr/share/nano

/usr/share/info/nano.info.gz r, #allow read access to nano info page


/home/lab/student/group35/ rw, #allow nano to read and write files in the directory
/home/lab/student/group35/* rwk, #allow read,write and lock permissions to files under the directory
/home/lab/student/group35/** r, #allow read access to files in subdirectories under /home/lab/student/group35/


deny /home/lab/student/group35/*/ wk, #deny nano from writing and locking files in subdirectories under /home/lab/student/group35/
deny /home/lab/student/group35/**/* wk,

/home/lab/student/.local/share/nano/ rwk ,  #allow read,write and lock access for nano's local user configuration
/home/lab/student/.local/share/nano/** rwk ,

/home/lab/.local/share/nano/** rwk,
```

/home/lab/student/group35/*.swp rwk, #allow read,write and lock access to swapfiles in directory .Swapfiles are needed for nano to create and write to files.

/home/lab/student/group35/.*.swp rwk,

/usr/lib/x86_64-linux-gnu/libncursesw.so.6 rm, #allow read and map access for libncurses library file.Libncurses needed for nano to interact with terminal
/usr/lib/x86_64-linux-gnu/libncursesw.so.6.* rm, #to handle versioning in the library

/usr/lib/x86_64-linux-gnu/libtinfo.so.6 rm, #allow read and map access for libtinfo library files
/usr/lib/x86_64-linux-gnu/libtinfo.so.6.* rm, #to handle versioning in the library

/lib/x86_64-linux-gnu/libc.so.6 rm, #allow read and map access to libc library files
/usr/lib/x86_64-linux-gnu/libc.so.6.* rm,
/lib/x86_64-linux-gnu/libc.so.6 rm,
/snap/core*/**/lib/x86_64-linux-gnu/libc.so.6 rm,
/usr/lib/x86_64-linux-gnu/libc.so.6 rm,

/usr/lib/terminfo/ r, #allow read access to terminfo files.Terminfo need for nano terminal operations
/usr/lib/terminfo/** r,
/usr/share/terminfo/ r,
/usr/share/terminfo/** r,
/etc/terminfo/ r,
/etc/terminfo/** r,

/tmp/** rwk, #allow read,write and lock access to tmp directory
/var/tmp/** rwk,

/etc/ld.so.cache r, #allows reading linker cache
/usr/lib/locale/locale-archive r, #permits reading compiled locale data
/etc/locale.alias r, #access to alias file which maps aliases

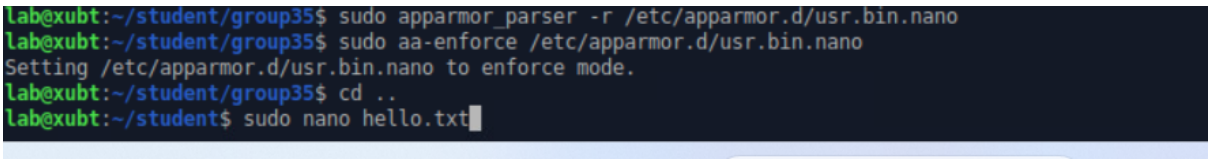
network inet stream, #allows creation of network sockets
network inet6 stream,
/etc/nsswitch.conf r, #grants read access to name service switch configuration file
/etc/passwd r, #enables reading system's password file

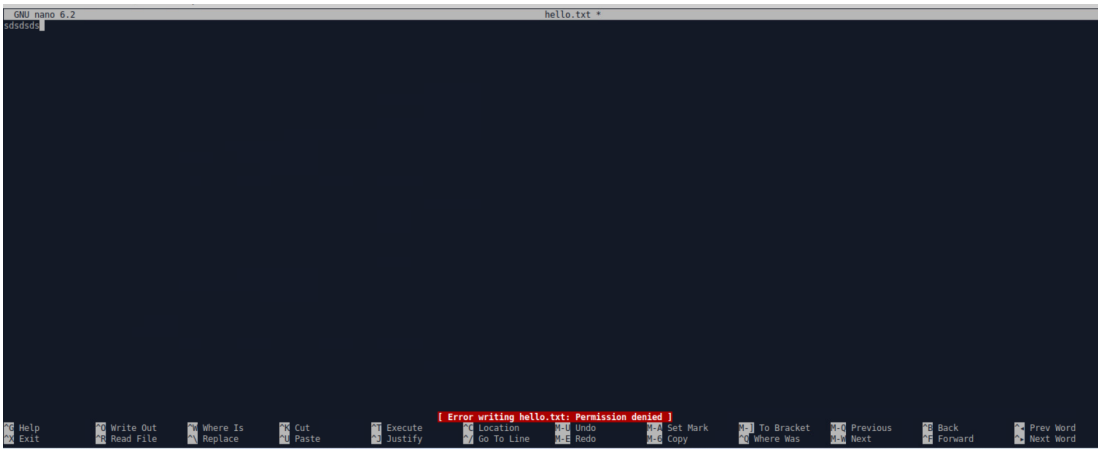
capability dac_override,# allows bypass discretionary check

}

Results

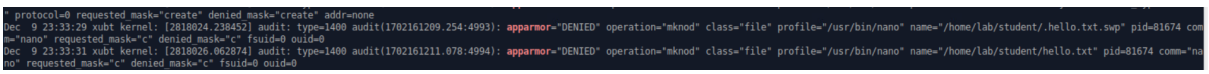
After, the profile is loaded and in enforce mode
creating and writing files outside directory after loading profile is denied



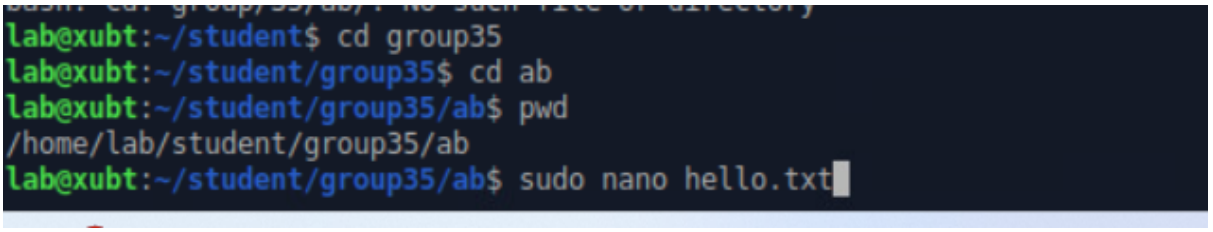


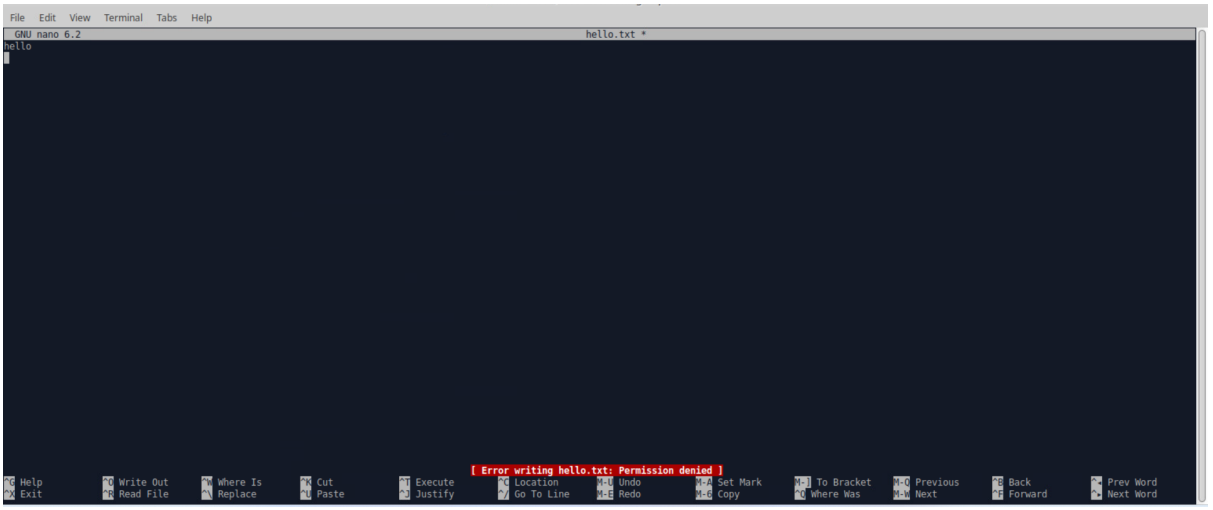
System log

apparmor=”DENIED” name= “home/lab/student/hello.txt”



It is also not possible to create and write files to subfolders within folder such as /home/lab/student/group35/ab as can be seen in below images





Only writing files within /home/lab/student/group35 directory is permitted after the apparmor profile is loaded and in enforce mode.

Time summary

Sl No	Task	Time (hours)
1	Reading documentations	8
2	Writing profile	18
3	Testing and Debugging errors	12
4	Report	6

Report on how can behaviour of Apparmor’s MAC be used to improve system security in a real - life situation

AppArmor can be used to protect sensitive data by restricting how applications can access it. For example, an application handling confidential information can be confined so it doesn't unintentionally or maliciously transmit this data elsewhere.

Strengths and Weakness of Apparmor use

Strengths

- AppArmor allows for precise control over the resources that applications can access.
- By confining applications ,it can minimise vulnerabilities.

Weakness

- Setting up AppArmor profiles can take time and it is a complex process.
- Apparmor profiles may need to be updated from time to time if there are changes to the application.

Conclusion

From this assignment we learn how apparmor can be used to restrict access of certain applications.
In our case the text editor was only able to perform a write operation in a specific directory.
Hence it can be used as an important tool to enforce security and can be useful in many different situations.

One other usecase is that it can help to improve security of a system by preventing access of applications to confidential files.

References

[1]https://wiki.ubuntu.com/AppArmor
[2]https://ubuntu.com/server/docs/security-apparmor
[3]https://gitlab.com/apparmor/apparmor/-/wikis/Profiling_by_hand
[4]https://manpages.ubuntu.com/manpages/xenial/man5/apparmor.d.5.html