Daniele Romanini – 598897

Information Security – Assignment 2 (Part C)

Exercise C1
Files attached are in folder "linux".
The file "infosec.sh" is a shell script, with the following code:

```
cd /home
mkdir /home/assignment
cd assignment
touch textfile.txt
mkdir /home/assignment/confidential
cd confidential
touch textfileconf.txt
groupadd project2016
usermod -G project2016 daniele
useradd -G project2016 testuser
chown daniele /home/assignment -R
chmod 770 /home/assignment -R
chmod 700 /home/assignment/confidential -R
```

Note: we must change, the name "daniele" with your favourite username logged in the system.

The code above creates a directory called assignment, in which a file called textfile.txt (empty) and a folder (confidential) is contained. The folder confidential contains another file called textconf.txt.
Then, it creates a group called project2016 and add user daniele to that. It creates alsoa new user called "testuser", and add it to the same group project2016.

After that, it makes the user "daniele") owner of the directory "assignment" with:

```
chown daniele /home/assignment -R
```

And set all the permission to him and the group for *assignment* (and respective contained file(s)) and just to *him* for the directory confidential:

```
chmod 770 /home/assignment -R
chmod 700 /home/assignment/confidential -R
```

The file "infosec2.c" is a wrapper written in C. Here the code:

```
include <stdio.h>
#include <unistd.h>
#include <sys/types.h>

int main (void) {

setuid (0);
clearenv();
system("/home/daniele/Desktop/infosec.sh"); //change the parameter

return 0;
}
```

Note: the directory passed as a parameter to system must be changed with the directory of the file

“infosec.sh” on your own machine (if it is different).

The setuid(0) allow to set the user identifier, so a user can ran the programme as he was administrator.

To install the program the first time, we must login as a root (with *sudo -i*, then type the password), move into the directory of the C file and compile it with the following command (make sure to have a gcc compiler installed in your machine, otherwise install it with *sudo apt-get install gcc*):

gcc infosec2.c -o i

Note*:* “i” will be the name of the executable output. You can change it if you wish.

After that, staying logged in as a root, type:

chmod 4775 i

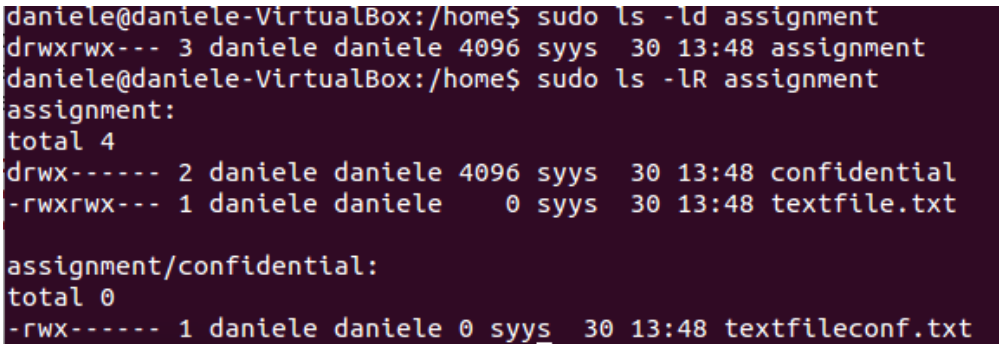
With this command you give the permission to other user to run the programme with administrator privileges.
After that, log out from the root terminal typing *exit*.
In that way you return to your user space (daniele in this case) and you can move in the directory where the file “i”(the executable) is (normally it is in the same directory of the file “infosec2.c”).
(We can also log off and login with daniele, or other user if we change the name)
At this point launch the executable typing:

./i

Now you have obtained the same result as in part A. Thus, if you type *sudo ls -ld /assignment* , and then *sudo ls -lR /assignment ,* the result will be the same as in the first image of this document.

Note: the programme can be modified putting *$USER* instead of “daniele”. In this case we must also modify the directory in the system call, for example passing it as a parameter to the programme, using argv[1].
In this way everyone, once the root user has compiled the programme, can run it.

If you type *sudo ls -ld /assignment* , and then *sudo ls -lR /assignment ,* here is the results:



Exercise C2
The program is “infowin.bat” (in the folder “windows” attached).
It is a bat script (the code is readable from “infowin2.txt” file).
Every user can run it and create a group called “project 2016”, add himself to that group, create a user called testuser (with a password testuser). The program creates also a directory called “assignment” containing a txt file, and another folder “confidential”(containing another text file).
The members of project2016 can access to the assignment folder, but not the confidential one (taht can be accessed just from the user that has run the program).

Just double click on the bat file in a Windows environment to run it.

Following the code is explained:

Create a group called project2016 and add the current user to the group:

net localgroup project2016 /add
net localgroup project2016 %USERNAME% /add

Go to the root directory and create a folder called “assignment”:

CD
mkdir assignment

Move into that directory, create an empty file called “EmpyFile.txt”:

CD assignment
copy NUL EmptyFile.txt

Now, inside assignment, create a directory called confidential and inside another file:

mkdir confidential
CD confidential
copy NUL EmptyFileConf.txt

Now it assigns the privileges at the files and folder.
After each command, from now, it stop inehirtance in order to avoid that user authenticad can have access to the directories or files created:

icacls C:\assignment\confidential\EmptyFileConf.txt /inheritance:r
icacls C:\assignment\confidential\EmptyFileConf.txt /grant %USERNAME%:f
icacls C:\assignment\confidential\ /inheritance:r
icacls C:\assignment\confidential /grant %USERNAME%:f
icacls C:\assignment\EmptyFile.txt /inheritance:r
icacls C:\assignment\EmptyFile.txt /grant project2016:f
icacls C:\assignment\ /inheritance:r
icacls C:\assignment /grant project2016:f

[**]Before the command explained above, there is a piece of code to run the script as an administrator (the command above could be launched without a script, just typing one by one in the command prompt. In order to be useful, the command prompt must be launched as administrator, with a right click of mouse and selecting “run as an administrator”).
The code used is from Evan Greene: https://sites.google.com/site/eneerge/home/BatchGotAdmin

Note: Windows can take some time to change permissions to the directories and files, so it may be necessary to wait a bit in order to see the permission changed.
After , you can log off and log in as another users (also the testuser created) to see effectively what it is changed.
Now, if we type *ICACLS \assignment /T* , the result is (IEUser is the username with which we were logged in):