Nitin Nagavel

CPRE 431

M03 HW

Assignments will be submitted in PDF format via Canvas.

Please submit your homework online through Canvas. Late homework will not be accepted.
Please ensure that you support all your answers with the correct screenshots showing your solutions.

1. In this "lab" problem, you will be working on a Linux Server Virtual Machine (VM). An image of this VM is available on Canvas (attached with the HW). The VM is having an administrator and 5 users, as shown in the figure below. You don't have access to any of the users of the Server, to be able to access the Server, you will need to perform password cracking! You were given a line of password hash from (/etc/shadow) for the administrator (admin1) of the Server (attached with the HW).
    a. Determine the used hash type of the password.
       SHA-512
    b. Determine the salt value of the password.
       $xgLS35s6
    c. Crack the passwords of all users using OpenSSL tool.
       Admin1:P@ssw0rd

    Hints:

    - It would be useful if you search for Linux shadow file password format.
    - You must use the latest OpenSSL version 1.1.1x for this problem. It would be helpful to read about creating Linux password hashes using OpenSSL.
    - You can use a password list for your cracking. There is a password list of most used 100K passwords, according to NIST attached with the HW.
    - You will need to write some code to iterate through the password list (feel free to use any language you prefer).
    - After cracking the password, ensure that you can access the Server.

2. The given Server users are managed as follows:
    - There are 5 users: user1, user2, …, user5. The first four users are staff members, but user5 is an external consultant.
    - User1 and user2 are programmers only, user4 is a manager only, and user3 is both programmer and manager.

    a. You are now the administrator of the server, and you are responsible for managing users and groups. Create 3 groups named “allstaff”, “prog” (short for programmers) and “mgmt” (short for management). Add users to the corresponding groups. List the users and groups to ensure the correct previous setup of system users and groups. Explain with screenshots how you applied this.

```
allstaff:x:1006:user1,user2,user3,user4,user5
prog:x:1007:user1,user2,user3
mgmt:x:1008:user3,user4
admin1@CPRE-431:~$
```

```
drw------- 2 user1 prog     4096 Sep 30  2019 Desktop
drwxr-x--- 2 user1 allstaff 4096 Sep 30  2019 documentation
drw------- 2 user1 prog     4096 Sep 30  2019 Documents
drw------- 2 user1 prog     4096 Sep 30  2019 Downloads
drw------- 2 user1 prog     4096 Sep 30  2019 Music
drw------- 2 user1 prog     4096 Sep 30  2019 Pictures
drw------- 2 user1 prog     4096 Sep 30  2019 Public
-rwxr----- 1 user1 allstaff    0 Sep 30  2019 schedule.txt
drw------- 2 user1 prog     4096 Sep 30  2019 Templates
drw------- 2 user1 prog     4096 Sep 30  2019 Videos
```

```
user2@CPRE-431:~$ ls
code     documentation  Downloads  Pictures  schedule.txt  Videos
Desktop  Documents      Music      Public    Templates
user2@CPRE-431:~$ ls -l
total 40
drwxrwx--- 2 user2 prog     4096 Sep 26 18:58 code
drwx------ 2 user2 prog     4096 Sep 30  2019 Desktop
drwxr-x--- 2 user2 allstaff 4096 Sep 30  2019 documentation
drwx------ 2 user2 prog     4096 Sep 30  2019 Documents
drwx------ 2 user2 prog     4096 Sep 30  2019 Downloads
drwx------ 2 user2 prog     4096 Sep 30  2019 Music
drwx------ 2 user2 prog     4096 Sep 30  2019 Pictures
drwx------ 2 user2 prog     4096 Sep 30  2019 Public
-rwxr----- 1 user2 allstaff    0 Sep 30  2019 schedule.txt
drwx------ 2 user2 prog     4096 Sep 30  2019 Templates
drwx------ 2 user2 prog     4096 Sep 30  2019 Videos
```

- Inside their home directory, each programmer has a directory called code and a directory called documentation. Inside the code directory, there is a file called source_code.txt, as well as one application called myapp.exe. Inside the documentation directory, there is a file called notes.txt.

```
user1@CPRE-431:/home/user2/documentation$ ls
notes.txt
user1@CPRE-431:/home/user2/documentation$ cat notes.txt
user1@CPRE-431:/home/user2/documentation$
```

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                  source_code.txt

Never gonna give you up

                        [ Wrote 1 line ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

- Each manager has a directory called finance (for financial information) including a confidential business.txt file.

```
user3@CPRE-431:~$ cd finance/
user3@CPRE-431:~/finance$ ls
business.txt
user3@CPRE-431:~/finance$ nano business.txt
user3@CPRE-431:~/finance$ ls
business.txt
user3@CPRE-431:~/finance$ cat business.txt
you know the rules and so do I!!!!!!!
```

- Each user also has a file called schedule.txt in their home directory.

```
user1@CPRE-431:/home/user2$ cat schedule.txt
user1@CPRE-431:/home/user2$
```

b. Configure file access controls so that it explicitly applies only the following:
   - All users can view each other's schedules, but not other files in their home directory (except for as stated in the following).

```
rwx------ 2 user2 prog     4096 Sep 30  2019 Desktop
rwxr-x--- 2 user2 allstaff 4096 Sep 30  2019 documentation
rwx------ 2 user2 prog     4096 Sep 30  2019 Documents
rwx------ 2 user2 prog     4096 Sep 30  2019 Downloads
rwx------ 2 user2 prog     4096 Sep 30  2019 Music
rwx------ 2 user2 prog     4096 Sep 30  2019 Pictures
rwx------ 2 user2 prog     4096 Sep 30  2019 Public
rwxr----- 1 user2 allstaff    0 Sep 30  2019 schedule.txt
rwx------ 2 user2 prog     4096 Sep 30  2019 Templates
rwx------ 2 user2 prog     4096 Sep 30  2019 Videos
ser2@CPRE-431:~$
```

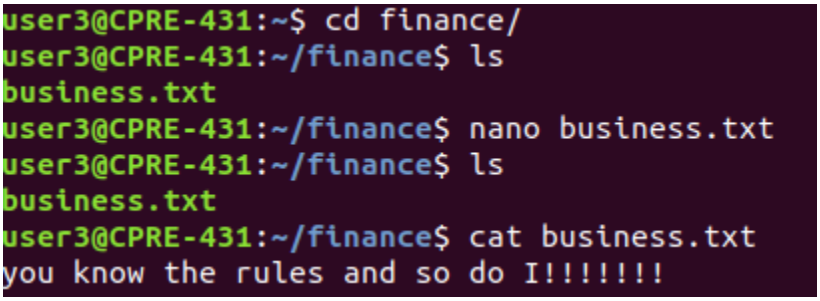
   - All staff can view files in the documentation directory of other staff.
     All users can view the documentation folder shown below:

```
ser2@CPRE-431:/home/user3/code$ ./myapp.exe
ser2@CPRE-431:/home/user3/code$ cd ..
ser2@CPRE-431:/home/user3$ ls
ode      documentation  Downloads  Music     Public        Templates
esktop   Documents      finance    Pictures  schedule.txt  Videos
ser2@CPRE-431:/home/user3$ cd documentation/
ser2@CPRE-431:/home/user3/documentation$ ls
otes.txt
```

   - Programmers can view and edit each other's source code files, create new files in any code directory, as well as run each other's myapp.exe files.
     Same for other users in the Prog group:

```
user2@CPRE-431:/home/user3/code$ cat source_code.txt
never gonna let you down!!!!!
user2@CPRE-431:/home/user3/code$ ./myapp.exe
user2@CPRE-431:/home/user3/code$
```

- Financial information (in the finance directory) is only viewable by the manager that owns the files, not by any other user.
  User below is the manager that owns the files



Hints:

- Take screenshots of setting the access and listing it using (ls -l). Also, take screenshots of testing that the access control works by logging in as each user and checking they can(not) access the specified files/directories.
- Use only the basic Linux permissions. Do NOT use advanced permissions such as setfacl or getfacl.
- Use the "Introduction to Linux" Page to help you in the needed commands for this Homework.