dr--r-xrwt 2 jon humans 4096 Mar 23 snacks

Directory, owner may read, group may read and execute, world may read and write and execute with sticky bits, the owner is jon, group is humans

dr-xr-xr-x 2 jon humans 4096 Mar 24 toys

Directory, owner may read and execute, group may read and execute, world may read and execute, the owner is jon, group is humans

----r--rw- 1 garfield pets 16384 Mar 12 lasagna.jpg

group may read, world may read and write, the owner is garfield, group is pets

-rw-rw-r-- 1 odie pets 4096 Mar 20 icecream.txt

owner may read and write, group may read and write, world may read, the owner is odie, group is pets

-rw-rw-r-- 1 odie pets 8192 Mar 18 bone.png

owner may read and write, group may read and write, world may read, the owner is odie, group is pets

1. Can user jon read the contents of file lasagna.jpg?

Yes, the 8th bit in lasagna.jpg allows everyone who isn’t the owner or in group pet (jon is human) to read the lasagna.jpg

2. Can user garfield read the contents of file lasagna.jpg?

No, the 2nd bit in lasagna.jpg does not allow the owner of the file to read the file

3. Can user odie modify the contents of file lasagna.jpg?

No, the 6th bit in lasagna.jpg does not allow odie who is in group pets to modify the lasagna.jpg

4. Can user jon list the names of the files within directory snacks?

Yes, the 2th bit in snacks allows the owner to have file’s names to be listed.

5. Can user jon read the contents of file icecream.txt in directory snacks?

No, the 4th bit in snacks does not allow the owner to access the directory snacks

6. Can user garfield delete the file icecream.txt in directory snacks?

No, the 10th bit in snacks is a sticky bit which does not allow anyone but the owner delete any files in the directory snacks including icecream.txt

7. Can user garfield modify the contents of file bone.png in directory toys?

Yes, the 10th bit in toys allows everyone who is not the owner or in group humans to open the directory toys and the 6th bit in bone.png allows those of group pets to modify the contents of bone.png

8. Can user odie delete the file bone.png in directory toys?

No, the 10th bit in toys allows everyone who is not the owner or in group humans to open the directory toys so odie can execute but the 9th bit in directory toys does not allow those who are not the owner or in group humans to modify the contents of the directory toys

Problem 2.1: You’ve got to crack a few eggs to make an omelet

Suppose that an attacker has stolen the password storage file users and would like to find the

users’ passwords.

1. Write a Java or Python program that brute-force searches for the first user’s password

using the list password\_dictionary, and measure how long it takes to find the

correct password on your computer. Please include the measured running time in your

answer to this question.

12601286400 nanoseconds or 12.6012864 seconds

2. Calculate how long it would take to find each and every user’s password if you performed

the same brute-force search for every user. Please include your calculation and result in

your answer.

12.6012864\*64849 = 817180.821754 seconds

3. Calculate how long it would take to find each and every user’s password with brute-force

search if the users’ passwords were 8-characters long and chosen uniformly at random

from lower- and upper-case letters and digits. Please include your calculation and result

in your answer.

( 62^8 ) \* (817180.821754) / 4717720 =3.7819825e+13 seconds,

Problem 2.2: All your passwords are belong to us

Since performing a brute-force search for every password takes a lot of time, attackers will try to

pre-compute the hashes if possible.

4. Write a Java or Python program (or extend the previous program) that computes the

hash value of every password in the list password\_dictionary, stores the hash1 Note that this is a small dictionary for demonstration purposes only, which consists of less than 5 million variants

of English words. Real attacks use larger dictionaries, which often include commonly used passwords and passwords that have been stolen in prior attacks. password pairs in a Java HashMap or Python dictionary (or similar data structure)2 , and finds each and every user’s password by simply looking up this data structure. Measure how long it takes to find every user’s password on your computer using this program. Please include the measured running time in your answer to this question.

16293334600 nanoseconds or 16.2933346 seconds

Problem 2.3: Why so salty?

Attacks based on pre-computed hashes can be prevented using password salting.

5. Select two users from users who have the same hash values (i.e., same passwords), and

verify that their hash values are different in users\_salted. Please include the selected

users’ usernames, password (recovered in the previous step), and hash values from

users\_salted in your answer.

Preston-Jay,7chiromantic,6c76b2f07d750088c5e3e892d6536890a0c0319ab51a9b7e2bea9a4e1a7fa3db

Kostandinos,7chiromantic,794cc51efe2b59af551500a806579d8cc6ddf6b09d562ec688ae8fc798886d69

6. Compute these users’ salted & hashed passwords using the salt values included in

users\_salted, and verify that the hash values in users\_salted are correct.

oblem 2