Tutorial Lab 4 (Acces Control List)

Unix Permissions

Unix Permissions - `rwx`:

- `r` **Read** allows
  - Opening a file for reading
  - Listing the contents of directories (ex. `ls`)
- `w` **Write** allows
  - Opening a file for writing
  - Creating and deleting directories children
- `x` **Execute** allows
  - Executing a file
  - Changing working directory (ex. `cd`)

Symbol	Perimmission	Value
`-`	None	0
`r`	Read	1
`w`	Write	2
`x`	Execute	4

Symbol	Permissions	Numeric Value
`---`	None	0
`--x`	Execute	1
`-w-`	Write	2
`-wx`	Write+Execute	3
`r--`	Read	4
`r-x`	Read+Execute	5
`rw-`	Read+Write	6
`rwx`	Read+Write+Execute	7

```
# Read The Friendly Manuals:
$ man chmod
$ man chown
```

Special Permissions

```
SETUID - set user ID on execute
SETGID - set group ID on execute
StickyBit - puts the directory in sticky mode
```

The `SETUID` and `SETGID` permissions allow users and groups who are not the owner or group of a file to execute that file as though they were.

When the `Sticky Bit` is set on a **directory**, only that directory's owner or root can **delete or rename** the directory's files.

Special Permission	Value
None	0
`Sticky Bit`	1
`Setgid`	2
`Setuid`	4

```
$ chmod 4762 file
```

translates to

```
setuid = on
setgid = off
sticky bit = off
user = read + write + execute
group = read + write
other = write
```

Structure of a 4-Digit `chmod` command:

- 1. First Digit: **Special permissions** (setuid, setgid, sticky bit)
- 2. Second Digit: **Owner**'s permissions (read, write, execute)
- 3. Third Digit: **Group**'s permissions (read, write, execute)
- 4. Fourth Digit: **Others**' permissions (read, write, execute)

```
# Add write to *user*
$ chmod u+w

chmod g-rw = remove read and write from *group*
chmod o-rwx = remove read, write and execute from *other*
chmod u+s = add setuid
chmod g-s = remove setgid
chmod o+t = add sticky bit

chmod a+w = add write to *all*
chmod a-wx = remove write and execute from *all*
```

Tasks

Task 01

```
❯ docker run --rm --name acl-lab -it ghcr.io/cs-pub-ro/isc-acl-lab
hacker@f1dfd7d9b35d:/$ cd /etc/secret/
hacker@f1dfd7d9b35d:/etc/secret$ ls
ls: cannot open directory '.': Permission denied
hacker@f1dfd7d9b35d:/etc/secret$ cd /usr/local/isc/
hacker@f1dfd7d9b35d:/usr/local/isc$ ls -a
.  ..  .hidden
hacker@f1dfd7d9b35d:/usr/local/isc$ ls -alh
total 12K
drwxr-xr-x 3 root root 4.0K Oct 30  2023 .
drwxr-xr-x 1 root root 4.0K Oct 30  2023 ..
d--x--x--x 2 root root 4.0K Oct 30  2023 .hidden
hacker@f1dfd7d9b35d:/usr/local/isc$ cd .hidden/
hacker@f1dfd7d9b35d:/usr/local/isc/.hidden$ ls
ls: cannot open directory '.': Permission denied
hacker@f1dfd7d9b35d:/usr/local/isc/.hidden$ ls -a
ls: cannot open directory '.': Permission denied
hacker@f1dfd7d9b35d:/usr/local/isc/.hidden$ for i in {100..10000} ; do ls
".$i" 2> /dev/null ; done
.1338
hacker@f1dfd7d9b35d:/usr/local/isc/.hidden$ ls .1338
.1338
hacker@f1dfd7d9b35d:/usr/local/isc/.hidden$ cat .1338
ISC{14mt3h31337}
```

> Flag 1: `ISC{14mt3h31337}`

```
❯ docker cp 2e98c240a231:/usr/local/bin/giff-me-flag giff-me-flag
Successfully copied 20kB to /home/bogdan/giff-me-flag
```

Asa zice `Chat GPT` ca arata `/usr/local/bin/giff-me-flag giff-me-flag`

```
#include <stdio.h>
#include <string.h>
```

```
int main() {
    char input[50];
    printf("What do you say? ");
    fgets(input, 50, stdin);

    if (strcmp(input, "PLEASE!!!11oneone") == 0) {
        printf("Okay, here's your flag: %s\n", "FLAG_GOES_HERE");
    } else {
        printf("Wrong answer!\n");
    }

    return 0;
}
```

TODO: ce fac mai departe?

Task 02

```
hacker@2e98c240a231:/$ ls /home/
.not_for_your_eyes  decanu/             flagz0wner/         mihai/
student/
an0th3r0n3/         dujm3n/             hacker/             rekt0r/
t4l3nt/
hacker@2e98c240a231:/$ ls /home/decanu/
hacker@2e98c240a231:/$ ls -a /home/decanu/
.  ..  .secret
hacker@2e98c240a231:/$ ls -a /home/decanu/.secret/
ls: cannot open directory '/home/decanu/.secret/': Permission denied
hacker@2e98c240a231:/$ ls -a /home/decanu/.secret/
ls: cannot open directory '/home/decanu/.secret/': Permission denied
hacker@2e98c240a231:/$ ls -a /home/decanu/.mihai
ls: cannot access '/home/decanu/.mihai': No such file or directory
hacker@2e98c240a231:/$ ls -a /home/mihai
.  ..
hacker@2e98c240a231:/$ ls -a /home/student
.  ..
hacker@2e98c240a231:/$ ls -a /home/.not_for_your_eyes
/home/.not_for_your_eyes
hacker@2e98c240a231:/$ ls -a /home/flagz0wner/
ls: cannot open directory '/home/flagz0wner/': Permission denied
hacker@2e98c240a231:/$ ls -a /home/student
.  ..
hacker@2e98c240a231:/$ ls -a /home/an0th3r0n3/
.  ..
hacker@2e98c240a231:/$ ls -a /home/dujm3n/
.  ..
hacker@2e98c240a231:/$ ls -a /home/hacker/
.  ..
hacker@2e98c240a231:/$ ls -a /home/rekt0r/
.  ..  money  read-bank-accounts  tutorial.txt
```

```
hacker@2e98c240a231:/$ ls -a /home/rekt0r/
.  ..  money  read-bank-accounts  tutorial.txt
hacker@2e98c240a231:/$ ls -a /home/t4l3nt/
.  ..  .flags  calculator.c  sant_calculator
hacker@2e98c240a231:/$ cat /home/rekt0r/money/
cat: /home/rekt0r/money/: Permission denied
hacker@2e98c240a231:/$ cat /home/rekt0r/tutorial.txt
Decanu, you are allowed use 'sudo' on my behalf to execute 'read-bank-accounts'! Use man if you don't know how to control its behavior, google, anything but don't bother me!
hacker@2e98c240a231:/$ cd /home/rekt0r/
hacker@2e98c240a231:/home/rekt0r$ ls
money  read-bank-accounts  tutorial.txt
hacker@2e98c240a231:/home/rekt0r$ cat read-bank-accounts
#!/bin/bash
set -e

cat "/home/rekt0r/money/$1"

hacker@2e98c240a231:/home/rekt0r$
```

```
hacker@2e98c240a231:/home/rekt0r$ ls -1 /home/
an0th3r0n3
decanu
dujm3n
flagz0wner
hacker
mihai
rekt0r
student
t4l3nt
```

```
hacker@2e98c240a231:/home/rekt0r$ ls -a
.  ..  money  read-bank-accounts  tutorial.txt
hacker@2e98c240a231:/home/rekt0r$ ls -alh
total 20K
drwxr-xr-x 3 rekt0r rekt0r 4.0K Oct 30  2023 .
drwxr-xr-x 1 root   root   4.0K Oct 30  2023 ..
drwxr-x--- 2 rekt0r rekt0r 4.0K Oct 30  2023 money
-rwxr-xr-x 1 rekt0r rekt0r   49 Oct 30  2023 read-bank-accounts
-rwxr-xr-x 1 rekt0r rekt0r  174 Oct 30  2023 tutorial.txt
hacker@2e98c240a231:/home/rekt0r$ cat tutorial.txt
Decanu, you are allowed use 'sudo' on my behalf to execute 'read-bank-accounts'! Use man if you don't know how to control its behavior, google, anything but don't bother me!
```

```
hacker@2e98c240a231:/home/decanu$ ls -alh
total 12K
drwxr-xr-x 3 decanu decanu 4.0K Oct 30  2023 .
drwxr-xr-x 1 root   root   4.0K Oct 30  2023 ..
drwxr-x--- 2 decanu unstpb 4.0K Oct 30  2023 .secret
```

```
hacker@2e98c240a231:/home/rekt0r$ su decanu
Password:

# I don't know :(((
```

TODO: ce fac mai departe?

Task 03

```
hacker@2e98c240a231:/$ cd /home/t4l3nt/
hacker@2e98c240a231:/home/t4l3nt$ ls -alh
total 36K
drwxr-xr-x 3 t4l3nt t4l3nt 4.0K Oct 30  2023 .
drwxr-xr-x 1 root   root   4.0K Oct 30  2023 ..
drwx------ 2 t4l3nt t4l3nt 4.0K Oct 30  2023 .flags
-rwxr-xr-x 1 t4l3nt t4l3nt  642 Oct 30  2023 calculator.c
-rwsr-sr-x 1 t4l3nt t4l3nt  18K Oct 30  2023 sant_calculator
hacker@2e98c240a231:/home/t4l3nt$ cat calculator.c
#include <stdio.h>
#include <string.h>
#include <unistd.h>

#define TEST_MODE_FILE "/tmp/.TEST_MODE_ENABLED"


int main(int argc, char **argv) {
    if (argc < 2) {
        puts("Please supply a Python expression as argument!\n");
        return 1;
    }
    setreuid(geteuid(), geteuid());
    char expr[1024];
    snprintf(expr, sizeof(expr), "import math; print(%s);", argv[1]);
    if (access(TEST_MODE_FILE, F_OK) == 0) {
        snprintf(expr, sizeof(expr), "import math; print(\"TEST MODE! 
Here's a PI:\", math.pi);");
    }
    char *const exec_args[] = {"python3", "-c", expr, 0};
    return execv("/usr/bin/python3", exec_args);
}
```

```c
// talent.c
#include <stdio.h>
#include <string.h>
#include <unistd.h>

#define TEST_MODE_FILE "/tmp/.TEST_MODE_ENABLED"


int main(int argc, char **argv) {
    if (argc < 2) {
        puts("Please supply a Python expression as argument!\n");
        return 1;
    }
    setreuid(geteuid(), geteuid());
    char expr[1024];
    snprintf(expr, sizeof(expr), "import math; print(%s);", argv[1]);
    if (access(TEST_MODE_FILE, F_OK) == 0) {
        snprintf(expr, sizeof(expr), "import math; print(\"TEST MODE! Here's a PI:\", math.pi);");
    }
    char *const exec_args[] = {"python3", "-c", expr, 0};
    return execv("/usr/bin/python3", exec_args);
}
```

```
hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator
Please supply a Python expression as argument!
```

```
hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator 2
TEST MODE! Here's a PI: 3.141592653589793
hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator "2+2"
TEST MODE! Here's a PI: 3.141592653589793
hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator "2+2"
TEST MODE! Here's a PI: 3.141592653589793
hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator "2+2"
TEST MODE! Here's a PI: 3.141592653589793
hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator "2+2"
TEST MODE! Here's a PI: 3.141592653589793
hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator "2+2"
TEST MODE! Here's a PI: 3.141592653589793
hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator "2+2"
TEST MODE! Here's a PI: 3.141592653589793
hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator "2+2"
TEST MODE! Here's a PI: 3.141592653589793
hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator "pi"
TEST MODE! Here's a PI: 3.141592653589793
```

```
hacker@2e98c240a231:/home/t4l3nt$ cat /tmp/.TEST_MODE_ENABLED
hacker@2e98c240a231:/home/t4l3nt$
```

```
hacker@2e98c240a231:/home/t4l3nt$ rm /tmp/.TEST_MODE_ENABLED

# Ma ia capu'

hacker@2e98c240a231:/home/t4l3nt$ ./sant_calculator "import os;
print(os.listdir('.flags'))"
  File "<string>", line 1
    import math; print(import os; print(os.listdir('.flags')));
                       ^^^^^^
SyntaxError: invalid syntax
```

TODO: ce fac mai departe?

Task 04

```
# Parola: student
hacker@2e98c240a231:/home/t4l3nt$ su student
Password:

student@2e98c240a231:~$ copy-t3h-fl4gz
cp: cannot create regular file '/home/student/givemeflagz/': Not a
directory
Copy 1 failed!
student@2e98c240a231:~$ which copy-t3h-fl4gz
/usr/local/bin/copy-t3h-fl4gz


# Arata a binar
student@2e98c240a231:~$ cat $(which copy-t3h-fl4gz)
```

`Chat GPT` says: From the provided output, we can see that the binary contains a shell script. Here's the relevant portion extracted from the binary:

```
#!/bin/bash
set -e
umask 000
DEST=/home/student/givemeflagz

su -c 'ls -l /home/student/' dujm3n >/dev/null 2>&1 || { echo "Test
failed!" >&2; exit 1; }
! su -c 'ls -l '$DEST'/' dujm3n >/dev/null 2>&1 || { echo "Test failed!"
>&2; exit 2; }
```

```
! su -c 'ls -l '$DEST'/' an0th3r0n3 >/dev/null 2>&1 || { echo "Test
failed!" >&2; exit 3; }

su -c 'bash -c "umask 000; cp -f /home/flagz0wner/lastflag1.txt '$DEST'/"'
flagz0wner || { echo 'Copy 1 failed!'; exit 4; }
echo "First flag successfully copied!"

DEST=/home/student/givemeflagz/second
! su -c 'ls -l '$DEST'/' flagz0wner >/dev/null 2>&1 || { echo "Test
failed!" >&2; exit 5; }

su -c 'bash -c "umask 006; mkdir -p "'$DEST'"; umask 000; cat
/home/flagz0wner/lastflag2.txt > '$DEST'/lastflag2.txt"' flagz0wner || {
echo 'Copy 2 failed!'; exit 6; }
echo "Second flag successfully copied!"
```

```
student@2e98c240a231:~$ getfacl $(which copy-t3h-fl4gz)
getfacl: Removing leading '/' from absolute path names
# file: usr/local/bin/copy-t3h-fl4gz
# owner: root
# group: root
# flags: ss-
user::rwx
group::r-x
other::r-x
```

TODO: ce fac mai departe?