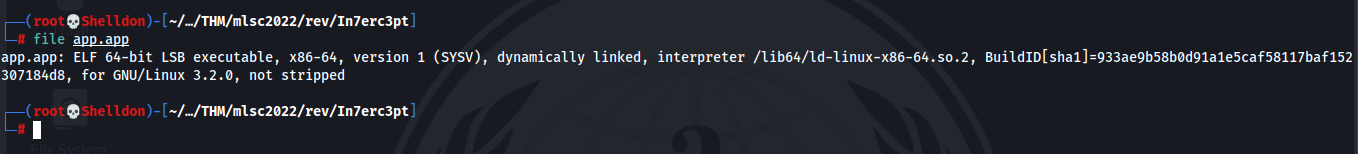
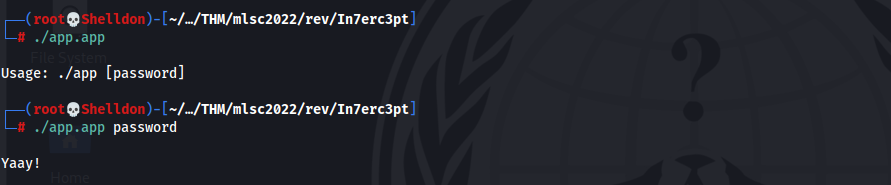
MLSC CTF 2022 -> reverse -> In7erc3pt

Firstly, I checked what type of file it is. Command: **file <file name>**

****

So, it is ELF 64 bits, LSB executable. Let’s run app



As we can see I must have a password so that get a flag.

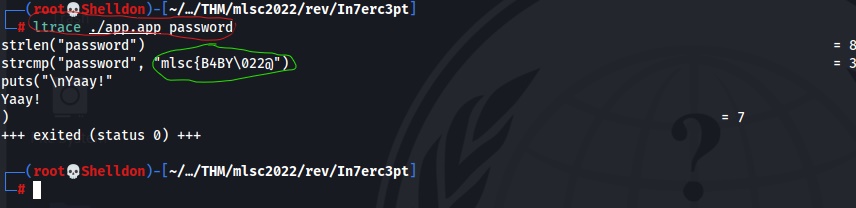
If I try type password or any strings, I get message **Yaay!** But it is not right. **I just changed values in app with radar2. In original app we have error message.**

****

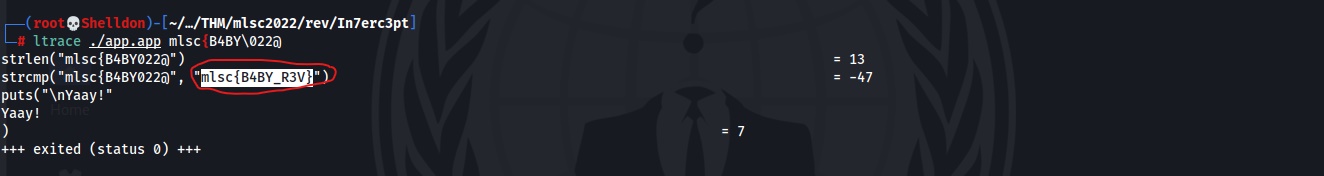
There is function **strmp()**. This function check two strings and if it will be false, we jump to another function. For example **sym.imp.puts()**. I just remove check and jump modules in app. In original app we get another message.

So, let’s find correct password.

I run app with ltrace. **ltrace** is a debugging utility in Linux, used to display the calls a userspace application makes to shared libraries.



In red is **command**. In green is **correct password** or correct value. Let’s try use this value.



Yes with this value we got flag