Reverseing

Challenge = “ find the password”

FILE = “pass"

FILE TYPE

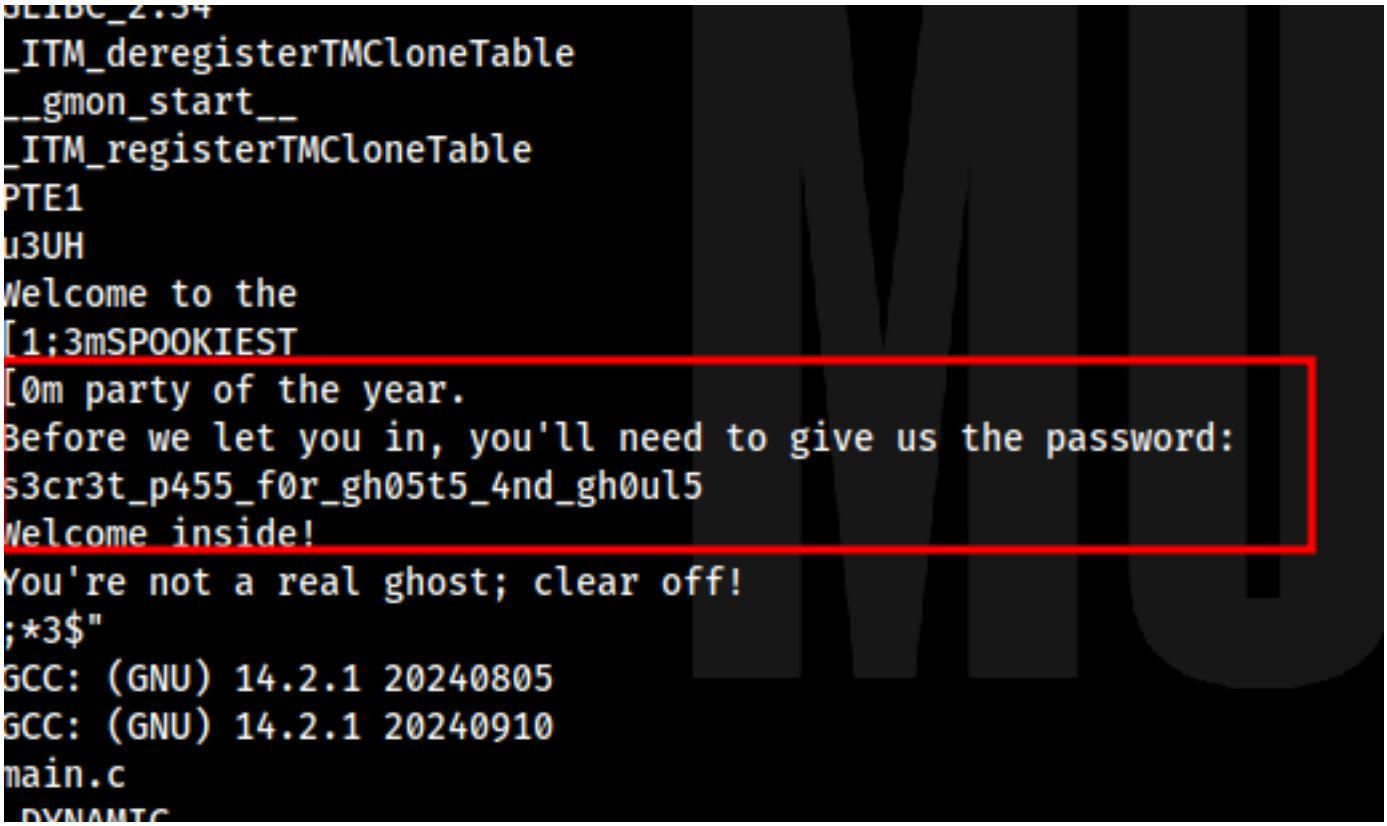
```
pass: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=3008217772cc2426c643d69b80a96c715490dd91, for GNU/Linux 4.4.0, not stripped
```

Running the binary

```
./pass
Welcome to the SPOOKIEST party of the year.
Before we let you in, you'll need to give us the password: password
You're not a real ghost; clear off!
```

Trying password gave me that response Time for some basic reverse engineering

STRINGS



PASSWORD FOUND

s3cr3t_p455_f0r_gh05t5_4nd_gh0ul5

Running binary with correct password

```
 ./pass
Welcome to the SPOOKIEST party of the year.
Before we let you in, you'll need to give us the password: s3cr3t_p455_f0r_gh05t5_4nd_gh0ul5
Welcome inside!
HTB{un0bfu5c4t3d_5tr1ng5}
```

password and flag found