King's Ransom 2

The initial process of getting a shell is the same as in king's ransom 1. After obtaining a shell on the target box, we looked around for ways to recover the original key file.

Recon

We took a look at the `entrypoint.sh` file which presumly was the entry point for the Dockercontainer. There we found the line `echo ${FLAG} > /challenge/bank/flag2.txt`, which prepares the second flag to be encrypted.

Docker init process environment shenanigans

Here the bash process uses the flag string, which is saved in the environment of the bash process, to write the flag into a file. Since the bash process is the entrypoint of the Dockercontainer, the process hasn't exited yet. This in turn means, that the environment of the initial process is still around in the container.

Getting the flag

We can access the env of the init process by running `cat /proc/1/environ | sed -e 's/\x00/\n/g'`. That command yields something like

```
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
HOSTNAME=f8a0d3f24283
FLAG=TESTFLAG
SERVICE_HOST=localhost
SERVICE_PORT=54321
HOME=/home/challenge
```

The `FLAG=TESTFLAG` would be the flag in the challenge.