Lab 3: Symbolic Execution for Backdoor Discovery

Lab Overview

The goal of this lab is to understand how to perform symbolic execution on binary code to explore program logic. In particular, you need to implement an analysis script based upon angr, a symbolic execution framework (https://angr.io/), to discover a backdoor in a given binary program.

Requirement

You are required to submit your source code and a written lab report. In this brief report, you need to use screenshots to explain your implementation and present your analysis result.

Lab Environment

This lab needs to be conducted in an angr docker container. To install docker and angr image, you can use the following commands:

```
# install docker
curl -sSL https://get.docker.com/ | sudo sh

# pull the docker image
sudo docker pull angr/angr

# run it
sudo docker run -it angr/angr
```

Please refer to the following link for detailed install instructions:
https://docs.angr.io/introductory-errata/install

Task: Find the Backdoor in Binary

`login` is a binary executable which is used to authenticate users. When `login` runs, it asks a user to provide credentials, an 8-character username and an 8-character password. Once it receives the user inputs, it will check them against credential files stored in the same directory. Each user account is stored in a separate file: the filename is the username and the file content is the password. If a user provides the correct credential, `login` will display a message: “Access granted! You are now in the admin console!”; otherwise, it will say “Access denied!”

However, aside from the normal authentication procedure, `login` also has a backdoor. Anyone who uses a secret password can bypass the authentication regardless of what username she gives. Our goal is to find out this hardcoded password.

You can find the binary file `login` and a credential file `gooduser` at:
https://drive.google.com/open?id=1dOKZgD6PZTcFUXusG9edNUTMMkGkWjMB

You can copy these files into the docker container using `docker cp` command:
https://til.codes/copy-file-from-host-machine-to-docker-container/

To exchange files between the host and a docker container, you need to find container IDs using this command: `sudo docker ps`

Hints:

1) You may learn how to write your analysis Python script from this angr example:
https://github.com/angr/angr-doc/tree/master/examples/fauxware

2) We've already known that the backdoor is at the beginning of this executable. As a result, you can leverage this knowledge to limit the depth of symbolic exploration.