Course Project Update 1

Our course project aims to solve three challenges. The challenge binaries are on our course website at http://columbus.cse.eng.auburn.edu

Links to an external site.

You need to be in the engineering college network, e.g., the lab on the first floor of Shelby Center. Or, you need to login to some remote machine on: rdp.eng.auburn.edu

Links to an external site.

to access our course website.

To login to the our course website, the username is your Auburn user name (the email address before @) and the password is 1 for every student.

Once you login, please go to the front page to read the instructions. There, you will need to run:

```
ssh-keygen -f key -N ''
```

to generate a key pair. Paste the content of the public key to

Settings > SSH Key

on the course website so that you can login to the server.

Then, you can start a challenge by clicking the challenge Start button on the website. After the challenge is started, you can connect to the server with the following (assuming your private key file is in the current directory).

```
ssh -i key hacker@columbus.cse.eng.auburn.edu
```

After you successfully login to the server with ssh, you are in your home directory /home/hacker , where you can add/delete/modify files. The challenge binary is in the directory of /challenge . The challenge binary is owned by the root user and has the privilege of reading the /flag file. /flag file is also owned by root user. Only if you hack the challenge binary and the challenge binary will be hijacked to read the content of /flag file. Then, you can paste the content of the /flag file, which is the "flag" to the website and click Submit.

Welcome to COMP5700/6700 Course Project Website!

Launching Challenges

At the core of the course project is flags. How do you get those flags? Solve challenges. You can start a challenge by clicking on the `Challenges` tab at the top, selecting our course module, clicking on a particular challenge, and hitting `Start`. In order to access that challenge, you can connect with ssh as follows:

Connecting using `ssh`. In order to ssh into your challenge instances, you must add a public ssh key to `Settings` > `SSH Key`. You can quickly generate an ssh key by running `ssh-keygen -f key -N ''` in a terminal on your (unix-friendly) host machine. This will generate files `key` and `key.pub`, which are your private and public keys respectively. Once you have linked your ssh public key to your account, you can run `ssh -i key hacker@columbus.cse.eng.auburn.edu` to connect into your challenge instance.

Once you are in a challenge instance, your goal is to get the contents of the `/flag` file. Unfortunately for you, you are executing as the `hacker` user, but `/flag` is only readable by the `root` user. Fortunately, however, there are challenge programs located inside of the `/challenge` directory, which when run, will run with the privileges of the `root` user. Solve the challenge to get the `/flag`, and then submit it in order to complete the challenge!

A few things to note. Your home directory `/home/hacker` is persistent. This means that when you start a new challenge, all of the files you have saved in there will still be there.

For our particular three challenges this semester, we recommand using the pwntools library to write the exploitation script.