In the name of God

Sharif University of Technology
Department of Computer Engineering

CE 815: Secure Software Systems

Mehdi Kharrazi *Aban 2^{th}, 1402*

Homework 1*

1 Get Familiar with Git

You should submit all your HWs at S4lab's Git distributed revision control system named Tarasht. To access Tarasht, your account and personal repositories will be emailed.

1.1 Git Config

In order to use Git, we recommend using a Linux machine or using a Linux virtual machine. Git uses a username to associate commits with an identity, and your username is like **ce815-021-student-id**. Using following commands, you can specify Git configuration settings with the git config command. One of the first things you should do is to set up your name, username and email address:

```
git config –global user.name "Your name"
git config –global user.username "ce815-021-student-id"
git config –global user.email "you@sharif.edu"
```

1.2 SSH Key

You can generate a new SSH key (or use an existing SSH key) for authentication, then add it to your Tarasht account to modify your repositories without entering passwords every time. Using following commands, you can generate a new pair of ssh key:

```
ssh-keygen -t rsa -b 4096 -C "you@sharif.edu"
eval "$(ssh-agent -s)"
ssh-add ~/.ssh/id_rsa
```

After key generation, log in at Tarasht, open your account's setting and add your public key. Your public key should start with **ssh-rsa**.

1.3 HW Submission

You can find your personal repo at Tarasht, and its name is exactly like your username; therefore your personal repo URL address is `https://tarasht.ce.sharif.edu/ce815-021-students/ce815-021-student-id`.

First clone your repository with the following command:

*Acknowledgement: This homework was orginally developed by Iman Hosseini and Solmaz Salimi, and edited By Razieh Eskandari and Parisa Ezzatpanah

```
git clone https://tarasht.ce.sharif.edu/ce815-021-students/ce815-021-student-id.git
```

For each HW, you should create a new folder with the name of HW id, i.e., **HW1**. We need a pdf file as HW's report, codes and related data to be added to this folder.

After adding your HW's directory, use the following command to submit your data:

```
git add HW1
gitt commit -m "Finished HW1"
git push
```

1.4 HW Handouts

All handouts can be found at handouts repository `https://tarasht.ce.sharif.edu/ce815-021-students/ce815-021-handouts`. You should first clone this repository:

```
git clone https://tarasht.ce.sharif.edu/ce815-021-students/ce815-021-handouts.git
```

2 Simple Memory Corruption Attack

Your first assignment is easy buffer Overflow , Format String and ROP attacks. We have a vulnerable binary program, which for the sake of simplicity, we have also released its C source code. You should first find the vulnerability and then write a simple script (bash, Python,Perl, etc.) to smash the stack and make it spawn a shell. The Aleph One tutorial, **Smashing The Stack For Fun And Profit**, and also Stanford's **Exploiting Format String Vulnerabilities** are your friend.

The vulnerable program and its source code is available at handouts repository.

- **prog_vuln0:** this program is a 32bit executable, use buffer Overflow to access shell. Accessing the shell in gdb is enough and you don't need to access it in terminal.
- **prog_vuln1:** this program is a 32bit executable, so with crafted input you can reach the shell.
- **prog_vuln2:** this program is a 32bit executable that has NX (Non-eXecutable) security feature on, so instead of putting the shell code into stack you should use ROP attack and find proper gadgets.

2.1 Delivery

You should submit a report, explaining your script, and the steps to find the return address. You should also submit your script and explain how to run it. We should note that you are not allowed to use libraries to find return address but you can use tools like pwntools and ROPgadget for automatically find gadgets and build ROP chain.