Assignment 0: Software environment and Arm review

Due date: none

Nothing is required to be turned in for this assignment, but everyone should have the software environment for the course configured and tested by next class.

1   Ubuntu 21.10 VM

Instructions for software configuration will be given assuming an operating system of Ubuntu 21.10. While you may elect to use whatever operating system you prefer, it is recommended to install a virtual machine with Ubuntu 21.10 for use in this course.

1.1   Install virtualization software

There are multiple virtualization software products that are sufficient to host the virtual machine. Some examples are:

- VirtualBox: https://www.virtualbox.org/

- VMWare Workstation Player:
  https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html

- Hypervisors provided by your host OS (QEMU/KVM on Linux; Hyper-V on Windows)

1.2   Install Ubuntu 21.10

The Ubuntu 21.10 installation ISO is available here:
https://releases.ubuntu.com/21.10/ubuntu-21.10-desktop-amd64.iso
The following parameters should be sufficient for your VM:

- Memory: 4 GB

- Disk space: 20 GB

- NATed network adapter, so that the virtual machine can access the Internet

- 'Minimal installation' within the Ubuntu installer

Students are free to provide the VM with more resources or install additional software if desired.

2   Ghidra

Many of the projects in this course will use Ghidra for software reverse engineering. Install Ghidra and take the opportunity to familiarize yourself with the user interface by importing and analyzing some executable files.

2.1   Installation

To install Ghidra within your Ubuntu VM:

- Install the Ghidra dependencies:

```
apt-get install openjdk-11-jre openjdk-11-jre-headless openjdk-11-jdk \
openjdk-11-jdk-headless
```

- Download the latest version of Ghidra from https://github.com/NationalSecurityAgency/ghidra/releases

- Unzip the Ghidra installation in your location of choice

- Run the `ghidraRun` script in the unzipped directory to launch the application

2.2   References

- In the Ghidra installation directory: `docs/CheatSheet.html`

- In the Ghidra installation directory: `docs/GhidraClass/`

3   Arm review

If you are unfamiliar with the Arm instruction set, it is strongly encouraged that you read through the first reference below. Some Arm executables have been provided in the `resources` directory so that you can compare the disassembled output to the associated source files. A recorded lecture will provide an introduction to the Arm instruction set and will provide walkthroughs of analyzing some example Arm executables. Listed below are some useful references for analyzing Arm assembly code:

- Azeria Labs Arm assembly overview:
  https://azeria-labs.com/writing-arm-assembly-part-1/

- Arm Assembler Guide:
  https://developer.arm.com/documentation/dui0068/b/

- Armv7-A Architecture Reference Manual:
  https://developer.arm.com/documentation/ddi0406/latest

If you would like to execute the binaries in the `resources` directory, install the `libc6-armel-cross` and `qemu-user` packages. You can then execute them in QEMU's userspace emulation mode:

```
qemu-arm -L /usr/arm-linux-gnueabi/ ./arm-hello-world
```