CSci 4271W (011 and 012 sections) Lab Instructions

Lab 1 **January 27, 2025**

0.1 Labs, an intro

The labs in this class are intended to be short introductions to a variety of tools that could be useful as a starting point for project reports or in applying some of the ideas from this course to other projects. You can work with up to two other people on any lab assignment, and when you complete it there will typically be a short writeup to submit on Gradescope.

However, for this particular lab, while you can still work in a group of up to three, *every* student should follow the procedure with their own VM, to make sure they can access the resources needed for labs and projects. Instead of a Gradescope submission, each student should demonstrate that they have completed the tasks to the lab instructor (TA).

1 Virtual Machines

A *virtual machine* (VM) is a (partially) software-based emulation of a computer, complete with its own operating system, storage, and network access. VMs are frequently used in connection with security for a variety of reasons, including:

- Reproducing attacks that depend on the configuration of hardware or software a program is running on
- Testing with some security features turned off
- Isolating the effects of a potentially harmful piece of software
- Misleading a network attacker into attacking a VM rather than some other asset

And certainly others, as well! In this class, you will complete all labs and some parts of the project work on a VM so that we can give you "root" access to a machine with a known configuration, and allow you to do things like monitor network connections between VMs that would not be acceptable on the live network.

Each student's VM is accessible over SSH from University networks, but is not routed outside the U. To SSH in, you should be connected to a CSE Labs machine first or another computer on a U network, including wireless. You can also visit a CSE Lab to login in person or SSH to a workstation in an Ubuntu lab.

The purpose of this lab is for each student to make sure they can connect to and navigate the VM, and transfer files back and forth to the VM as will be required for future labs and projects. So let's get started!

1.1 Login, install an ssh key

Sign in to your lab workstation. Open a terminal window, such as by right-clicking on the desktop and selecting "Open Terminal Here."

If you haven't already received it via email, obtain your password and VM hostname from the lab instructor (the hostname will be of the form `csel-xsme-s25-csci4271-NNN.cselabs.umn.edu`).

Your account on the VM is named `student` and has "root" access via sudo. Verify that you can connect to the VM from a CSELabs terminal by typing:

```
$ ssh student@csel-xsme-s25-csci4271-NNN.cselabs.umn.edu
student@csel-xsme-s25-csci4271-NNN.cselabs.umn.edu's password:
```

(Be sure to replace `NNN` with the appropriate digits for your VM; let's just agree to remember to keep doing that from now on. Also, in examples like this don't type the `$` at the beginning of the line, it indicates the terminal prompt.)

Enter your (VM) password at the prompt, and you should see the login message and then a shell prompt:

```
student@csel-xsme-s25-csci4271-NNN:~$
```

Open another **CSELabs** terminal window, and from your CSELabs home directory, create and install an SSH key as follows. (When prompted for a passphrase, we recommend you just press enter for an empty passphrase. A passphrase on your SSH key would provide an additional level of protection if the private key file were compromised, but it would require additional steps to keep from having to retype the passphrase frequently. You can also change or add a passphrase later.)

```
$ cd
$ ssh-keygen -t ed25519 -f id4271
$ mkdir .ssh
$ mv id4271 .ssh/
$ scp id4271.pub student@csel-xsme-s25-csci4271-NNN.cselabs.umn.edu:/home/student/
```

Next you should edit or create the file `~/.ssh/config` in your CSELabs account with an entry for your VM. If you've never done this before, it should work to type `gedit .ssh/config` in your CSELabs terminal (**not** the VM terminal) and add the following lines:

```
Host csel-xsme*4271*
User student
IdentityFile ~/.ssh/id4271
```

The line `User student` saves you from typing `student@` in front of the host name in future commands.

Finally, in the terminal window **connected to your VM session** you need to install your public key:

```
student@csel-xsme-s25-csci4271-NNN:~$ mkdir .ssh
student@csel-xsme-s25-csci4271-NNN:~$ cp id4271.pub .ssh/authorized_keys
```

Now you can ssh to and from your VM from your CSELabs account without having to enter your password. Try it by exiting from your ssh connection and re-connecting:

```
student@csel-xsme-s25-csci4271-NNN:~$ exit
$ ssh student@csel-xsme-s25-csci4271-NNN.cselabs.umn.edu
```

(You may wish to do this again, both on your VM and a personal machine, to upload a ssh key to the UMN github instance, where we'll be hosting some code related to labs, homeworks, and projects this semester.)

1.2 Use the shell to transfer files

We can transfer files between a regular CSELabs machine and the VMs using `scp`, a network file transfer protocol that is encrypted by building on top of SSH.

In a **CSELabs** terminal window, create a file with your name and favorite color:

```
$ echo "SirLancelot blue" >name_and_color.txt
```

Then securely copy it to your VM as follows (replacing `NNN` with the appropriate digits):

```
$ scp name_and_color.txt csel-xsme-s25-csci4271-NNN:/home/student/
```

In your VM terminal window, you should be able to see this file now by running the command `ls` from your home directory.

You can also use `scp` in the other direction to grab files from your VM to your CSELabs directory. In your CSELabs terminal window type:

```
$ scp csel-xsme-s25-csci4271-NNN:/etc/hostname .
```

(Note the `.` at the end of the line, which is a Unix abbreviation for "the current directory my shell is in.") This will copy the `/etc/hostname` file to your CSELabs account. (When you're using this command in the future, replace `/etc/hostname` with the path to the file you want to copy.)

On the VM we can also download files from an external network using typical download commands such as `wget`. In your VM terminal, use `wget` to fetch the file `example.c` from `cs4271.org` as follows:

```
student@csel-xsme-s25-csci4271-NNN:~$ wget http://cs4271.org/example.c
```

This will create the file `example.c` in your VM home directory.

1.3 All Set!

If you've done all this, you're all set for Lab 1! Get the TA's attention and show them that:

- You can ssh to your VM without entering a password.
- Your VM has the file `name_and_color.txt` in your home directory.
- Your CSELabs account has the `hostname` file you copied *from* the VM.

Make sure the instructor knows your UMN internet ID.