Getting Started

There are two options to set up the vulnerable server for the project. All functionality is the same between the two options, and you can switch between the two options without losing your progress as long as you manually copy any files over.

Option 1: Local Setup

You may choose to run the virtual machine on your local computer. The vulnerable server will be run as a virtual machine on your local device, and you can access the machine via SSH. **This is the recommended setup for most students.**

Windows Installation (VirtualBox)

Note: Students with x86-64 Macs may also use the VirtualBox setup, but students with M1 Macs can only use the QEMU setup in the next section.

For Windows, we recommend using VirtualBox to run the virtual machine. You can download the installer from the website and run the installer to install VirtualBox.

You will also need a client that supports SSH. The Windows Command Prompt or PowerShell may already have an SSH client installed, in which case you do not need to install anything else. Many students also already have Git Bash installed from previous classes, which will also work for this project.

After that, follow these instructions to set up the virtual machine:

1. Download the VirtualBox VM image pwnable-sp24.ova.
2. Open VirtualBox and import the downloaded VM image via `File -> Import Applicance...`.
3. Start the virtual machine you just imported. It should be pre-configured with the correct networking settings needed to access the machine.

We do **not** recommend interacting with the virtual machine using the virtual terminal that appears when you start the machine, because it does not support features such as copy-paste and mouse interaction. See the Accessing the Machine section below to find SSH access instructions.

If you run into VirtualBox issues, try locating your error in the VM debugging page and following the instructions to resolve it.

macOS and Linux Installation (QEMU)

On macOS and Linux, we recommend using QEMU to run the virtual machine.

On macOS, if you have the Homebrew package manager installed, you can install QEMU using `brew install qemu`. On Linux, you can install `qemu-system` through your distribution's package manager (`apt`, or `yum`) (if you use `pacman` the package is called `qemu-base`).

After that, follow these instructions to set up the virtual machine:

1. Download the QEMU VM image pwnable-sp24.qcow2.
2. `cd` to the folder containing the downloaded image and run the following command in your terminal:

```
$ qemu-system-x86_64 -accel kvm -accel hvf -accel tcg -m 512M -drive if=virtio,format=qcow2,file=pwnab
```

We do **not** recommend interacting with the virtual machine using the virtual terminal that appears when you start the machine, because it does not support features such as copy-paste and mouse interaction. See the Accessing the Machine section below to find SSH access instructions.

If you run into QEMU issues, try locating your error in the VM debugging page and following the instructions to resolve it.

Note: You may safely ignore any messages of the form `qemu-system-x86_64: -accel XXX: invalid accelerator XXX`, `qemu-system-x86_64: falling back to XXX`, or `qemu-system-x86_64: warning: host doesn't support requested feature: XXX`. As long as the virtual machine is started (the terminal appears, and the QEMU command doesn't immediately exit), you should be fine.

Accessing the Machine

You will be accessing the machine via SSH. Each question (and the customization step) will provide a `USERNAME` for accessing the machine. You can SSH into the virtual machine with the following command, replacing `USERNAME` with the username for the question:

```
$ ssh -p 16122 USERNAME@127.0.0.1
```

It will prompt you for a password to the vulnerable server. If the `USERNAME` and the password are correct, you should see a prompt starting with `pwnable:~$`. You are now ready to begin the project!

Option 2: Hive Setup

You should have already set up a hive account before running the steps in this section.

All steps in this section should be performed on the hive machine. Before starting this section, connect to the hive machine first by running `ssh hiveX`, replacing X with a number between 1 and 30.

SSH to hive troubleshooting:

- If you're getting "Connection refused" or "Connection timeout" or other connection errors, try using a different hive between hive1 and hive30 (e.g. run `ssh hive7` instead). Note: the Hivemind website used to be used to check which hive machines are busy or offline. It is now broken, please do not refer to it anymore.
- If you're getting "Connection timeout" or other connection errors, make sure you're not on the Berkeley-Visitor Wi-Fi network, which blocks SSH connections. If you're on Berkeley-Visitor, switch to eduroam or turn on the Berkeley VPN.

1. On the hive machine terminal, run this command to start the VM:

   ```
   ~cs161/proj1/start
   ```

   This command will take about a minute. If it worked, you should see "The virtual machine has been started."

2. Each question (and the customization step) will provide a username and password for logging into the VM. You can SSH into the VM by running the following command on the hive machine terminal, replacing USERNAME with the username for the question:

   ```
   ~cs161/proj1/ssh USERNAME@pwnable
   ```

   It will prompt you for a password to the vulnerable server. If the `USERNAME` and the password are correct, you should see a prompt starting with `pwnable:~$`.

You are now ready to begin the project!

Whenever you're finished with a work session on the project, remember to shut down the VM before logging out of the SSH session by running:

```
~cs161/proj1/stop
```

Do not close the terminal window without running the stop command; this could cause setup issues later.
