

# CSci 5271: Introduction to Computer Security

## Virtual Machine Instructions

## Homework 1

In order to complete the homework, each group has been given access to a VMWare-based virtual machine running on the ITLabs cluster machines, `itclusN.itlabs.umn.edu`, where  $N \in \{1, 2, \dots, 12\}$ . Each of you will receive an email informing you which physical machine your VM is running on, and your group number.

**Logging in to VMs.** Once you've received this email, you can access your VM from any ITLabs or CS machine as follows:

1. To load the vmware module, type `module load vmware/server-console` (and hit return).
2. Next, run the vmware application with the command `vmware-server-console`.
3. In the vmware dialog box, under host name, enter the name of the physical machine your VM is hosted on, for example `itclus7.itlabs.umn.edu`. The user name and password for this dialog box should be your itlabs account name and password.
4. You will then get a list of virtual machines that your account can access. For this homework, the only machine you will need is the `attacker` instance for your group.
5. You can log into the VM using the account "student" with password "pass".

**Installing FCVS.** Aside from the VMWare console, these VMs have no network access to the outside world, but they CAN be accessed from the itclus machine they are hosted on. So to transfer FCVS and your exploits between your ITLabs account and your VM (and back), you can use `scp` from the appropriate itclus machine. You can do this as follows:

1. Connect to your VM as in the previous section.
2. You will need to learn what your VM thinks its IP address is. You can do this by typing, at the VM command prompt: `sudo ifconfig eth0`. The result will contain a private IP address on the second line of output, like `172.16.68.128`.
3. Log in to the physical machine associated to your VM, say `itclus7.itlabs.umn.edu`, using your ITLabs account and password.
4. Use `scp` to copy data from your local directory to your VM. For example, if you download `fcvs.tgz` to your home directory, and want to copy it into the home directory on your VM, you would type: `scp ~/fcvs.tgz student@172.16.68.128:~/` at the prompt on `itclus7`. (Substitute the appropriate IP address for your machine, and the appropriate path for other files)

To copy files back from the VM to your ITLabs account, reverse the order of the arguments, e.g. to copy `~/sploit1.sh` from the VM to your home directory, type `scp student@172.16.68.128:~/sploit1.sh ~/`.

Once you've copied over FCVS to your virtual machine, you can install it on the VM by typing (in the home directory, or wherever you've placed the `.tgz` file) `tar -vzxf fcvs.tgz` to untar the file and `./install.sh` to make and install FCVS. After that you can `cd /opt/fcvs` and checkout a copy of the source code using `./fcvs checkout fcvs.c`.

**A Few Words of Caution.** You have `sudo` access on your VM, meaning that you can do anything to the machine that an administrator can - including wipe the hard disk, etc. If you make an unrecoverable error, you can restore the VM to its original state as follows:

1. Login to the itclus machine that your VM is hosted on.
2. Do `cd /export/scratch/vmware/cs5271-groupN-attacker/`, where N is your group number.
3. Run `./revert-to-old-attacker-disk.sh`.

This will restore your VM to its original state, and wipe out any changes you have made, including any work you saved to the VM disk. Thus it is a good idea to backup your work to an ITLabs machine regularly.

You also have access to shutdown or reboot your VM. The best way to do this is with `sudo`, from the command prompt, e.g. `sudo halt` or `sudo reboot`. You can also shut down your VM using the "Shut Down Guest" option in VMWare's VM -> Power menu. Unless all of these options fail, you should *not* use the red power button on the VMWare server console, or the "Shut Down" command in the VM -> Power menu, as these send a hard power off signal, just like pulling the power plug on a running computer. Doing this will create a strong chance of irretrievably corrupting the VM's disk image.

Finally, if you halt, restore, or reboot your VM you will have to manually turn off address space randomization again. You can do this by typing

```
sudo sysctl -w kernel.randomize_va_space=0
```

at your VM's command prompt.

**Hacking from Home.** You may also access the default VM images on personal machines, by downloading them from either:

- [http://www.cs.umn.edu/cs\\_files/cs5271/cs5271-VMs.tar.gz](http://www.cs.umn.edu/cs_files/cs5271/cs5271-VMs.tar.gz) or
- [http://www.cs.umn.edu/cs\\_files/cs5271/cs5271-VMs.exe](http://www.cs.umn.edu/cs_files/cs5271/cs5271-VMs.exe) (for Windows users)

These contain the three identical VMs that are currently available on the itclus machines. Each file is 1.5GB in size. You can download VMware Player to access these VMs at <http://www.vmware.com/download/player/>. Suggested bare-minimum system specs for running all three VMs at once is 1.5GHz proc, 1GB RAM, and 6GB hard drive space. You'll need a broadband connection for the download, otherwise we can provide DVD burns to those who want them. Contact Landon Thomas ([lthomas@cs.umn.edu](mailto:lthomas@cs.umn.edu)) for those requests. You can expect a one business day turn-around.

If you choose to do this, you should know that ITLabs will not provide any support for users to run these VMs on your home machines, and the VMs at home will not have access to the files you upload at school.