Links to security news sites are as follows:

- Packet Storm Security: `https://packetstormsecurity.com/`
- The Hacker News: `http://thehackernews.com/`

Links to general tech news sites are as follows:

- The INQUIRER: `https://www.theinquirer.net/`
- The Register: `http://www.theregister.co.uk/`
- ZDNet: `http://www.zdnet.com/`

You can check out some general Linux learning resources as well. Linux News Site:

- LXer: `http://lxer.com/`
- *BeginLinux Guru* on YouTube: `https://www.youtube.com/channel/UC88eard_2sz89an6unmlbeA`

(Full disclosure: I am the *BeginLinux Guru*.)

One thing to always remember as you go through this book is that the only operating system you'll ever see that's totally, 100% secure will be installed on a computer that never gets turned on.

Introduction to VirtualBox and Cygwin

Whenever I write or teach, I try very hard not to provide students with a cure for insomnia. Throughout this book, you'll see a bit of theory whenever it's necessary, but I mainly like to provide good, practical information. There will also be plenty of step-by-step hands-on labs.

The best way to do the labs is to use Linux virtual machines. Most of what we'll do can apply to any Linux distribution, but we will also do some things that are specific to either Red Hat Enterprise Linux or Ubuntu Linux. (Red Hat Enterprise Linux is the most popular for enterprise use, while Ubuntu is most popular for cloud deployments.)

Red Hat is a billion-dollar company, so there's no doubt about where they stand in the Linux market. But, since Ubuntu Server is free-of-charge, we can't judge its popularity strictly on the basis of its parent company's worth. The reality is that Ubuntu Server is the most widely-used Linux distribution for deploying cloud-based applications.

See here for details: `http://www.zdnet.com/article/ubuntu-linux-continues-to-dominate-openstack-and-other-clouds/`.

Since Red Hat is a fee-based product, we'll substitute CentOS 7, which is built from Red Hat source code and is free-of-charge. There are several different virtualization platforms that you can use, but my own preferred choice is VirtualBox.

VirtualBox is available for Windows, Linux, and Mac hosts, and is free of charge for all of them. It has features that you have to pay for on other platforms, such as the ability to create snapshots of virtual machines.

Some of the labs that we'll be doing will require you to simulate creating a connection from your host machine to a remote Linux server. If your host machine is either a Linux or a Mac machine, you'll just be able to open the Terminal and use the built-in Secure Shell tools. If your host machine is running Windows, you'll need to install some sort of Bash shell, which we'll do by installing Cygwin.

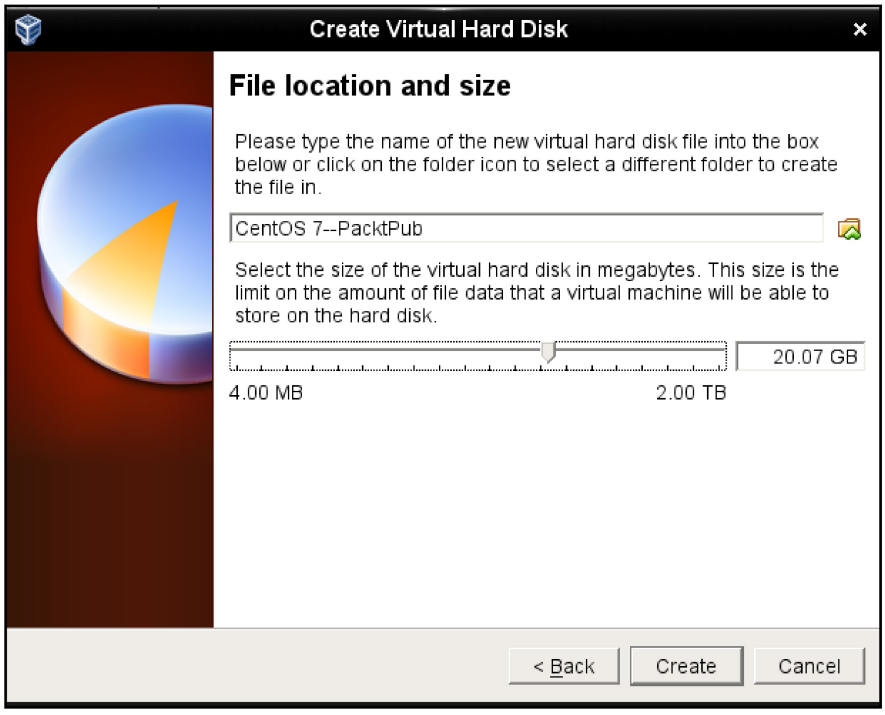
Installing a virtual machine in VirtualBox

For those of you who've never used VirtualBox, here's a quick how-to to get you going:

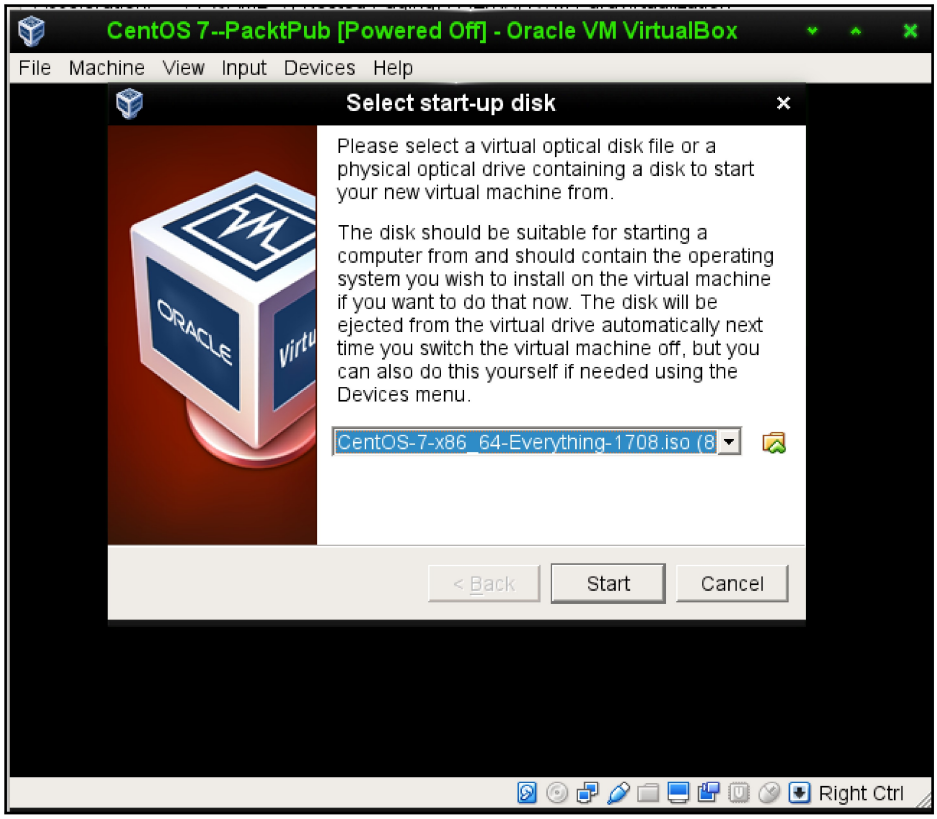
1. Download and install VirtualBox and the VirtualBox Extension Pack. You can get them from: `https://www.virtualbox.org/`.

2. Download the installation `.iso` files for Ubuntu Server and CentOS 7. You can get them from: `https://www.ubuntu.com/` and `https://www.centos.org/`.

3. Start VirtualBox and click the **New** icon at the top of the screen. Fill out the information where requested. Increase the virtual drive size to 20 GB, but leave everything else as the default settings:



4. Start the new virtual machine. Click on the folder icon at the bottom-left corner of the dialog box and navigate to the directory where you stored the `.iso` files that you downloaded. Choose either the Ubuntu `.iso` file or the CentOS `.iso` file as shown in the following screenshot:



5. Click the **Start** button on the dialog box to start installing the operating system. Note that, for Ubuntu Server, you won't be installing a desktop interface. For the CentOS virtual machine, choose either the KDE desktop or the Gnome desktop, as you desire. (We'll go through at least one exercise that will require a desktop interface for the CentOS machine.)
6. Repeat the procedure for the other Linux distribution.
7. Update the Ubuntu virtual machine by entering:

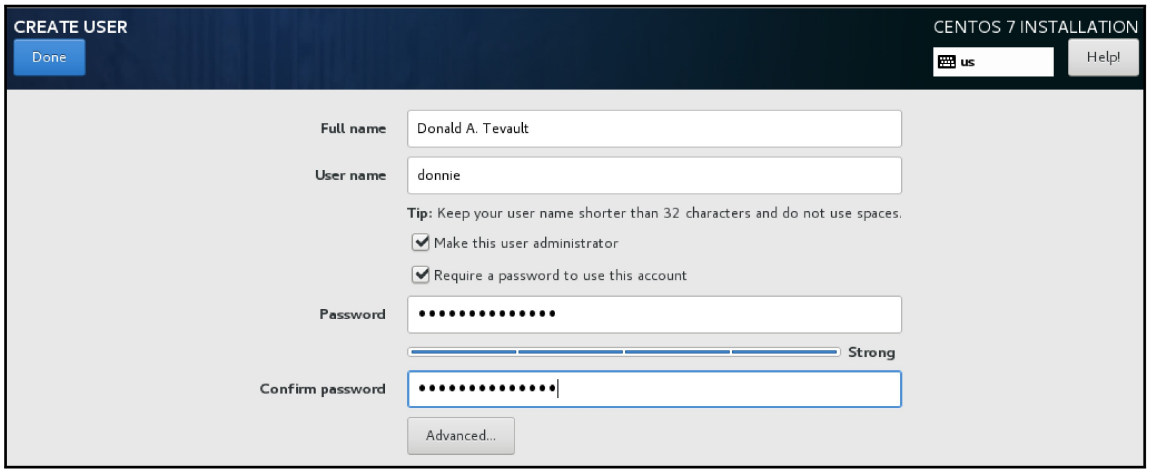
```
sudo apt update
sudo apt dist-upgrade
```

8. Hold off on updating the CentOS virtual machine because we'll do that in the next exercise.

When installing Ubuntu, you'll be asked to create a normal user account and password for yourself. It won't ask you to create a root user password, but will instead automatically add you to the sudo group so that you'll have admin privileges.

When you get to the user account creation screen of the CentOS installer, be sure to check the **Make this user administrator** box for your own user account, since it isn't checked by default. It will offer you the chance to create a password for the root user, but that's entirely optional—in fact, I never do.

The user account creation screen of CentOS installer is shown as follows:



The EPEL repository on the CentOS virtual machine

While the Ubuntu package repositories have pretty much everything that you need for this course, the CentOS package repositories are—shall we say—lacking. To have the packages that you'll need for the CentOS hands-on labs, you'll need to install the **EPEL** (**Extra Packages for Enterprise Linux**) repository. (The EPEL project is run by the Fedora team.) When you install third-party repositories on Red Hat and CentOS systems, you'll also need to install a `priorities` package, and edit the `.repo` files to set the proper priorities for each repository. This will prevent packages from the third-party repository from overwriting official Red Hat and CentOS packages if they just happen to have the same name. The following steps will help you install the required packages and edit `.repo` file:

1. The two packages that you'll need to install EPEL are in the normal CentOS repositories. Run the command:

   ```
   sudo yum install yum-plugin-priorities epel-release
   ```

2. When the installation completes, navigate to the `/etc/yum.repos.d` directory, and open the `CentOS-Base.repo` file in your favorite text editor. After the last line of the `base`, `updates`, and `extras` sections, add the line, `priority=1`. After the last line of the `centosplus` section, add the line, `priority=2`. Save the file and close the editor. Each of the sections that you've edited should look something like this (except with the appropriate name and priority number):

   ```
   [base]
   name=CentOS-$releasever - Base
   mirrorlist=http://mirrorlist.centos.org/?
   release=$releasever&arch=$basearch&repo=os&infra=$infra
     #baseurl=http://mirror.centos.org/centos/
      $releasever/os/$basearch/
   gpgcheck=1
   gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
   priority=1
   ```

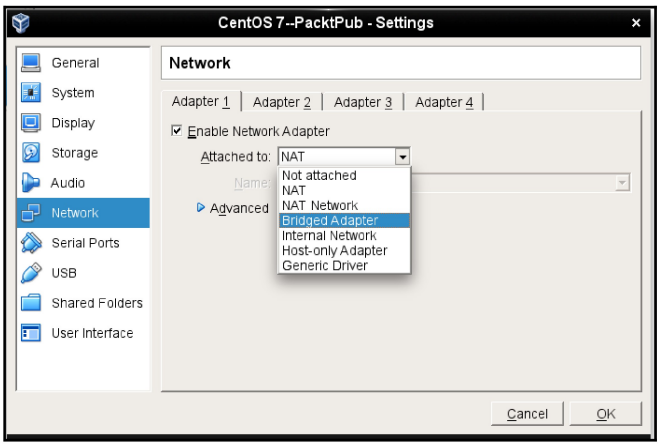
3. Open the `epel.repo` file for editing. After the last line of the `epel` section, add the line, `priority=10`. After the last line of each remaining section, add the line, `priority=11`.
4. Update the system and then create a list of the installed and available packages by running:

```
sudo yum upgrade
sudo yum list > yum_list.txt
```

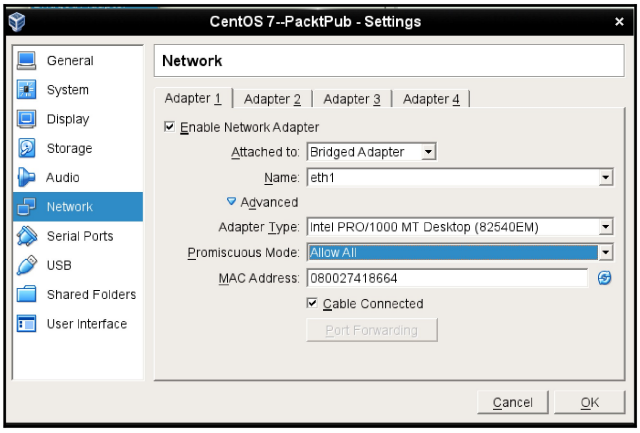
Configuring a network for VirtualBox virtual machines

Some of our training scenarios will require you to simulate creating a connection to a remote server. You would do this by using your host machine to connect to a virtual machine. When you first create a virtual machine on VirtualBox, the networking is set to **NAT** mode. In order to connect to the virtual machine from the host, you'll need to set the virtual machine's network adapter to **Bridged Adapter** mode. Here's how you can do this:

1. Shut down any virtual machines that you've already created.
2. On the VirtualBox manager screen, open the **Settings** dialog for a virtual machine.
3. Click the **Network** menu item, and change the **Attached to** setting from **NAT** to **Bridged Adapter**:



4. Expand the **Advanced** item, and change the **Promiscuous Mode** setting to **Allow All**:



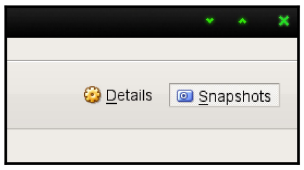
5. Restart the virtual machine and set it to use a static IP address.

If you assign static IP addresses from the high end of your subnet range, it will be easier to prevent conflicts with low-number IP addresses that get handed out from your internet gateway.

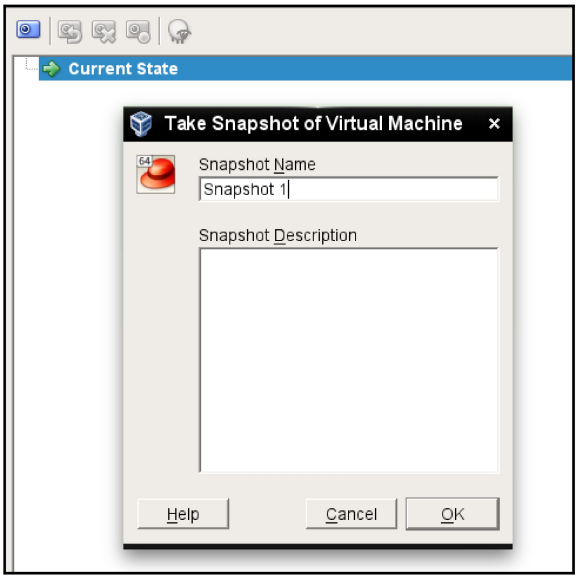
Creating a virtual machine snapshot with VirtualBox

One of the beautiful things about working with virtual machines is that you can create a snapshot and roll back to it if you mess something up. With VirtualBox, that's easy to do.

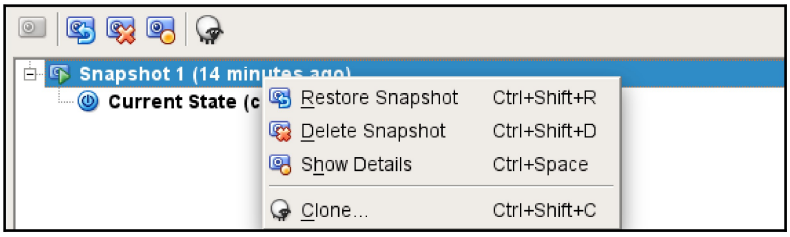
1. At the top, right-hand corner of the VirtualBox manager screen, click the **Snapshots** button:



2. Just left of mid-screen, you'll see a camera icon. Click on that to bring up the snapshot dialog box. Either fill in the desired **Snapshot Name**, or accept the default name. Optionally, you can create a description:



3. After you've made changes to the virtual machine, you can roll back to the snapshot by shutting down the virtual machine, then right-clicking on the snapshot name, and selecting the proper menu item:



Using Cygwin to connect to your virtual machines

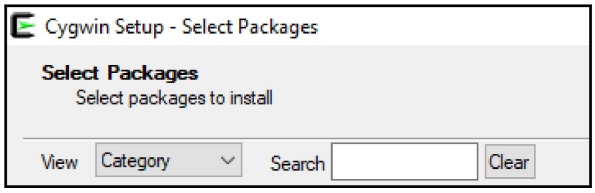
If your host machine is either a Linux or Mac machine, you'll simply open the host's Terminal and use the tools that are already there to connect to the virtual machine. But, if you're running a Windows machine, you'll want to install some sort of Bash shell and use its networking tools. Windows 10 Pro now comes with a Bash shell that's been provided by the Ubuntu folk and you can use that if you desire. But, if you don't have Windows 10 Pro, or if you prefer to use something else, you might consider Cygwin.

Cygwin, a project of the Red Hat company, is a free open source Bash shell that's built for Windows. It's free-of-charge, and easy to install.

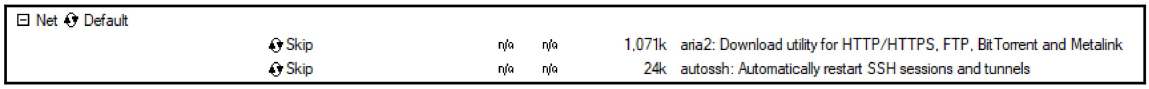
Installing Cygwin on your Windows host

Here's a quick how-to to get you going with Cygwin:

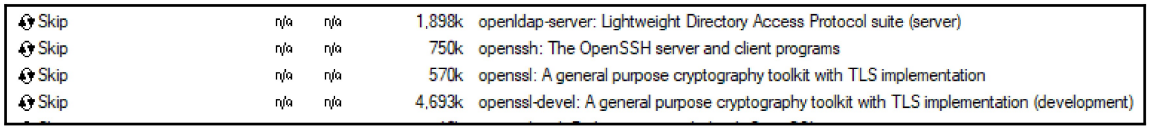
1. In your host machine's browser, download the appropriate `setup*.exe` file for your version of Windows from: `http://www.cygwin.com/`.
2. Double-click on the setup icon to begin the installation. For the most part, just accept the defaults until you get to the package selection screen. (The one exception will be the screen where you select a download mirror.)
3. At the top of the package selection screen, select **Category** from the **View** menu:



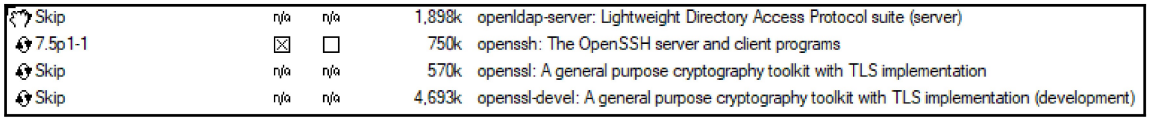
4. Expand the **Net** category:



5. Scroll down until you see the openssh package. Under the **New** column, click on **Skip**. (This causes a version number to appear in place of the **Skip**.):



6. After you have selected the proper package, your screen should look like this:



7. In the bottom right-hand corner, click **Next**. If a **Resolving Dependencies** screen pops up, click **Next** on it as well.
8. Keep the setup file that you downloaded, because you'll use it later to either install more software packages, or to update Cygwin. (When you open Cygwin, any updated packages will show up on the **Pending** view on **View** menu.)
9. Once you open Cygwin from the Windows Start menu, you can resize it as you desire, and use either the *Ctrl* + + or *Ctrl* + - key combinations to resize the font: