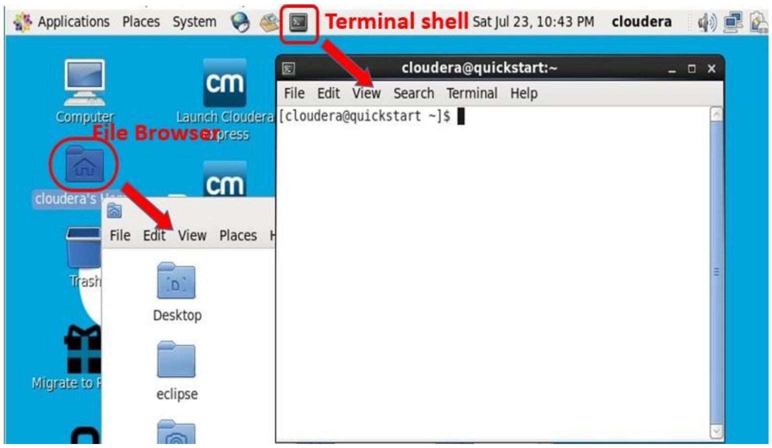
Lab 2
Intro to Linux and Kali Linux

1 Lab Preparation

The major distributions of Linux (Linux distros) such as Ubuntu, Debian, SUSE, RedHat, Fedora, CentOs, etc. provide various forms of GUI facilities and desktop environments that are similar in functionality and look-and-feel to Windows. The major ones include GNOME, Unity, KDE and XFce. However, to obtain the full functionality and power of Linux, it is necessary to learn how to work by typing Linux commands in to the shell terminal. Linux commands work like self-contained blocks which can be combined together in a wide variety of ways to accomplish complex functionality that would be impossible, or would take a very long time, to accomplish using a point-and-click approach through a GUI.

The Linux distro that is running as the guest OS in the VM is CentOS. You can start up a Linux shell terminal and also the File Browser by clicking on the appropriate icons in the desktop display.



Terminal shell

File Browser

```
[cloudera@quickstart ~]$
```

You can increase and decrease the shell terminal size by pressing Ctrl + and Ctrl – respectively.

For interaction with the Linux shell, the following conventions will be used in this lab tutorial:

- The `Dejavu Sans Mono` font will be used for commands to be typed in the Linux shell prompt. *Italics* will be used to denote expressions that can assume any suitable value.
- The `Courier New` font will be used for output in the Linux shell in response to these commands.

2 Basic Linux tutorial

To obtain the current directory that the shell is in, type in the open shell terminal:

```
pwd
```

```
/home/cloudera
```

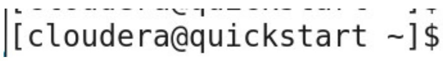
All user accounts in Linux have a home directory associated with them for each user to store files to work with. This home directory is usually found at /home/*username*.

To determine the current active account:

```
whoami
```

```
cloudera
```

This is the default user account which the OS boots up with when is containing VM is started. Typically the current active account is also shown in the prompt for most Linux shells, which takes the form of *username@machinename*



```
[cloudera@quickstart ~]$
```

To see a listing of all subdirectories and files in the current directory in a long list form, type:

```
ls -l
```

```
total 188
-rwxrwxr-x 1 cloudera cloudera  5387 Aug 10 19:52 cloudera-manager
-rwxrwxr-x 1 cloudera cloudera  9964 Aug 10 19:52 cm_api.py
drwxrwxr-x 2 cloudera cloudera  4096 Aug 10 19:52 Desktop
drwxrwxr-x 4 cloudera cloudera  4096 Aug 10 19:52 Documents
drwxr-xr-x 2 cloudera cloudera  4096 Jan 13 22:02 Downloads
drwxrwsr-x 9 cloudera cloudera  4096 Feb 19  2015 eclipse
-rw-rw-r-- 1 cloudera cloudera 53653 Aug 10 19:52 enterprise-
deployment.json
-rw-rw-r-- 1 cloudera cloudera 50513 Aug 10 19:52 express-
deployment.json
-rwxrwxr-x 1 cloudera cloudera  5007 Aug 10 19:52 kerberos
drwxrwxr-x 2 cloudera cloudera  4096 Aug 10 19:52 lib
drwxr-xr-x 2 cloudera cloudera  4096 Jan 13 22:02 Music
-rwxrwxr-x 1 cloudera cloudera  4226 Aug 10 19:52 parcels
drwxr-xr-x 2 cloudera cloudera  4096 Jan 13 22:02 Pictures
```

```
drwxr-xr-x 2 cloudera cloudera  4096 Jan 13 22:02 Public
drwxr-xr-x 2 cloudera cloudera  4096 Jan 13 22:02 Templates
drwxr-xr-x 2 cloudera cloudera  4096 Jan 13 22:02 Videos
drwxrwxr-x 4 cloudera cloudera  4096 Aug 10 19:52 workspace
```

The file entries shown in the listed are color coded to indicate their type, for e.g.

- Light blue – indicates directories
- Light green – indicates program files or executable scripts

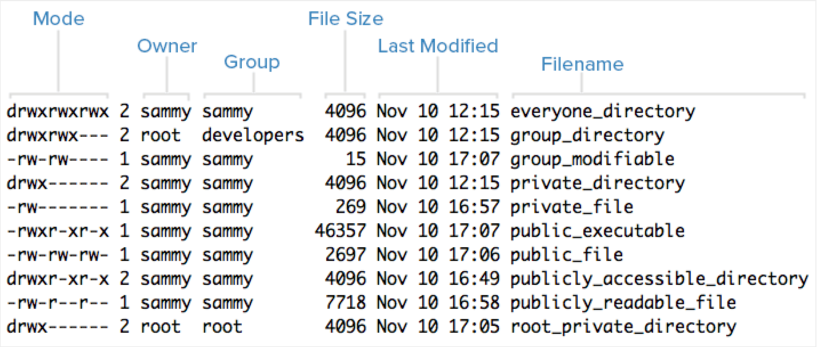
There are hidden files in a directory which typically do not show up in a listing as they are system files that could affect OS functionality if they were unintentionally deleted or modified. To see these hidden files, type:

```
ls -la
```

```
total 284
drwxrwxr-x  27 cloudera cloudera  4096 Jan 13 22:04 .
drwxrwxr-x.  3 root     root      4096 Aug 10 19:52 ..
-rw-r--r--   1 cloudera cloudera    18 Aug 10 14:33 .bash_logout
-rw-r--r--   1 cloudera cloudera   176 Aug 10 14:33 .bash_profile
-rw-r--r--   1 cloudera cloudera   176 Aug 10 14:33 .bashrc
…. .
……
```

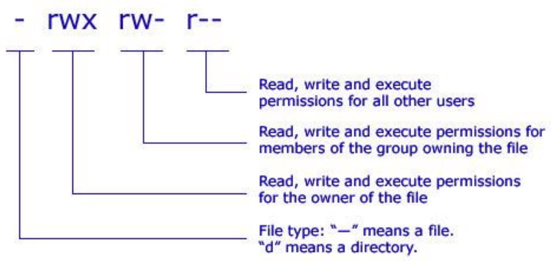
You should be able to see several files with only an extension name following the starting dot. These are the various scripts and files used by the Bash shell (the current active shell) when it starts up.

The entries in a Linux directory listing can be broken down into several portions:



```
drwxrwxrwx 2 sammy sammy       4096 Nov 10 12:15 everyone_directory
drwxrwx--- 2 root  developers  4096 Nov 10 12:15 group_directory
-rw-rw---- 1 sammy sammy         15 Nov 10 17:07 group_modifiable
drwx------ 2 sammy sammy       4096 Nov 10 12:15 private_directory
-rw------- 1 sammy sammy        269 Nov 10 16:57 private_file
-rwxr-xr-x 1 sammy sammy      46357 Nov 10 17:07 public_executable
-rw-rw-rw- 1 sammy sammy       2697 Nov 10 17:06 public_file
drwxr-xr-x 2 sammy sammy       4096 Nov 10 16:49 publicly_accessible_directory
-rw-r--r-- 1 sammy sammy       7718 Nov 10 16:58 publicly_readable_file
drwx------ 2 root  root        4096 Nov 10 17:05 root_private_directory
```

The mode portion denotes whether the item is a directory (d) or ordinary file (-), and also the permissions rights for each item. We will not go into detail here of the meaning and how to set or change the permissions of a particular item, but this knowledge will be relevant if you are working with Hadoop administration and operations.


- rwx rw- r--
Read, write and execute permissions for all other users
Read, write and execute permissions for members of the group owning the file
Read, write and execute permissions for the owner of the file
File type: "—" means a file. "d" means a directory.

There is no subdirectory in the current directory. To navigate to the parent directory, type:

```
cd ..
pwd
```

```
/home
```

The `..` means to move to the parent directory from whichever current directory the shell is in.

```
ls -l
```

```
total 4
drwxrwxr-x 34 cloudera cloudera 4096 Jan 13 19:08 cloudera
```

Go back up again to reach the top level root directory:

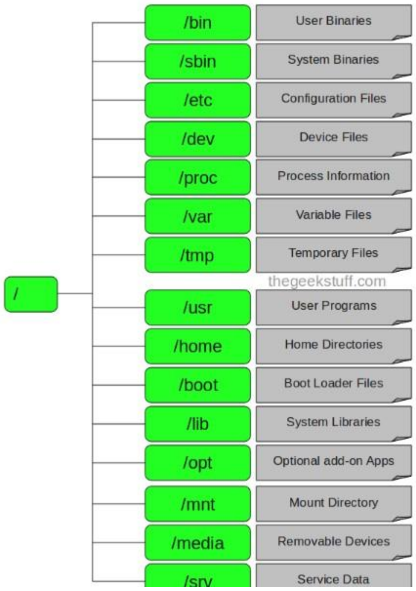
```
cd ..
pwd
```

```
/
```

```
ls -l
```

```
total 102
dr-xr-xr-x.   2 root root  4096 Jul  6  2016 bin
dr-xr-xr-x.   5 root root  1024 Apr  6  2016 boot
drwxr-xr-x   17 root root  3660 Jan 13 19:08 dev
drwxr-xr-x. 119 root root 12288 Jan 13 19:06 etc
drwxrwxr-x.   3 root root  4096 Apr  5  2016 home
dr-xr-xr-x.  11 root root  4096 Apr  6  2016 lib
dr-xr-xr-x.   9 root root 12288 Jul  6  2016 lib64
…….
…….
```

Each of the directories in the main root directory have specific purposes and store certain types of files and subdirectories. These directories differ between different Linux distros and their customizations; a brief explanation is shown below.



To navigate into a child or subdirectory from the current directory, type: `cd` *`nameofdirectory.`* This is known as a relative path as it is specified with regards to the current directory location.

```
cd etc
cd hadoop
cd conf
pwd
/etc/hadoop/conf
```

```
ls -l
```

```
total 40
-rw-rw-r-- 1 root root  1915 Jul  8  2016 core-site.xml
-rwxr-xr-x 1 root root  1366 Feb 23  2016 hadoop-env.sh
-rwxr-xr-x 1 root root  2890 Feb 23  2016 hadoop-metrics.properties
-rw-rw-r-- 1 root root  3739 Apr  5  2016 hdfs-site.xml
-rwxr-xr-x 1 root root 11291 Mar 23  2016 log4j.properties
-rw-rw-r-- 1 root root  1546 Apr  5  2016 mapred-site.xml
-rwxr-xr-x 1 root root  1104 Feb 23  2016 README
-rwxr-xr-x 1 root root  2375 Feb 23  2016 yarn-site.xml
```

To return back to our home directory, type:

```
cd
pwd
```

```
/home/cloudera
```

To go directly to particular directory, we can use its absolute path (this always starts with a / indicating the Linux root directory) in the `cd` command:

```
cd /etc/hadoop/conf
pwd
```

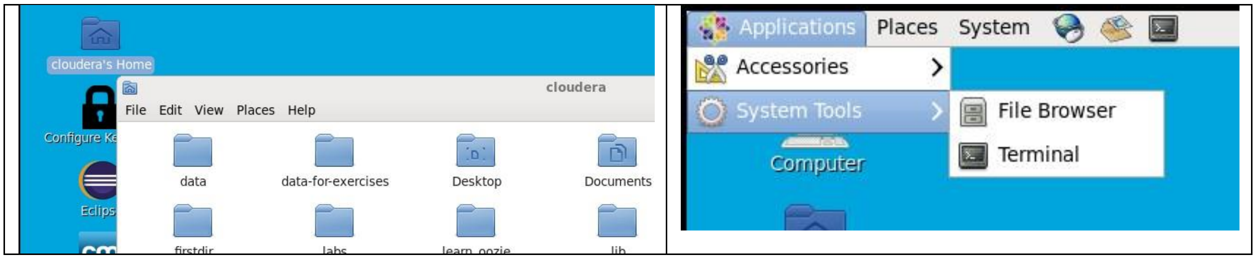
```
/hadoop/hdfs/namenode
```

We can chain the `..` to go navigate back out through several levels of directories in a single command:

```
cd ../../..
pwd
```

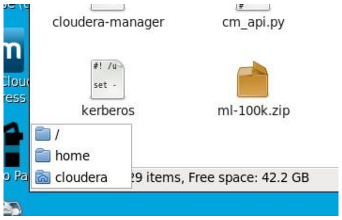
```
/
```

Most Linux distros also provide a File Browser that supports a graphical browsing functionality similar to Windows Explorer. This can be accessed by clicking on the Cloudera's Home icon on the desktop or using Applications -> System Tools -> File Browser from the desktop main menu.

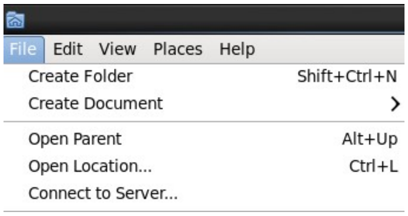


You should be able to see a listing of the various files and directories in the home directory of the active user account (`/home/cloudera)`. Various icons represent the different directory and file types. For example, notice that different icons are employed to depict files that contain program code (`cm_api.py`), json files (`enterprise-deployment.json` and `express-deployment.json`) and script files (`cloudera-manager`).

To navigate to a lower level directory, simply double click on the required folder. To navigate to a higher level directory, use the drop down menu at the bottom left corner.



There are also options to open a new File Browser window in the immediate parent directory, or at a specified absolute file path: using the Open Parent and Open Location options from the File option in the File Browser main menu.



You can practice using the File Browser to navigate and view the contents of the previous directories that we previously navigated using commands at the shell terminal.

Switch back to the shell terminal and return to the home directory and create a nested subdirectory structure with this command:

```
cd
mkdir firstdir
cd firstdir
mkdir seconddir
cd seconddir
mkdir thirddir
cd thirddir
pwd
```

```
/home/cloudera/firstdir/seconddir/thirddir
```

We return back to the home directory to verify the creation of the first directory `firstdir` in the nested directory structure.

```
cd
ls -l
```

```
total 192
-rwxrwxr-x 1 cloudera cloudera  5387 Aug 10 19:52 cloudera-manager
-rwxrwxr-x 1 cloudera cloudera  9964 Aug 10 19:52 cm_api.py
drwxrwxr-x 2 cloudera cloudera  4096 Aug 10 19:52 Desktop
drwxrwxr-x 4 cloudera cloudera  4096 Aug 10 19:52 Documents
drwxr-xr-x 2 cloudera cloudera  4096 Jan 13 22:02 Downloads
drwxrwsr-x 9 cloudera cloudera  4096 Feb 19  2015 eclipse
-rw-rw-r--  1  cloudera  cloudera  53653  Aug  10  19:52  enterprise-
deployment.json
-rw-rw-r--  1  cloudera  cloudera  50513  Aug  10  19:52  express-
deployment.json
drwxrwxr-x 3 cloudera cloudera  4096 Jan 13 23:50 firstdir
…….
…….
```

To remove a directory and all its nested subdirectories, type the command below. Notice that you will be prompted for each nested subdirectory to be deleted as a precaution.

```
rm -r firstdir
rm: descend into directory `firstdir'? y
```

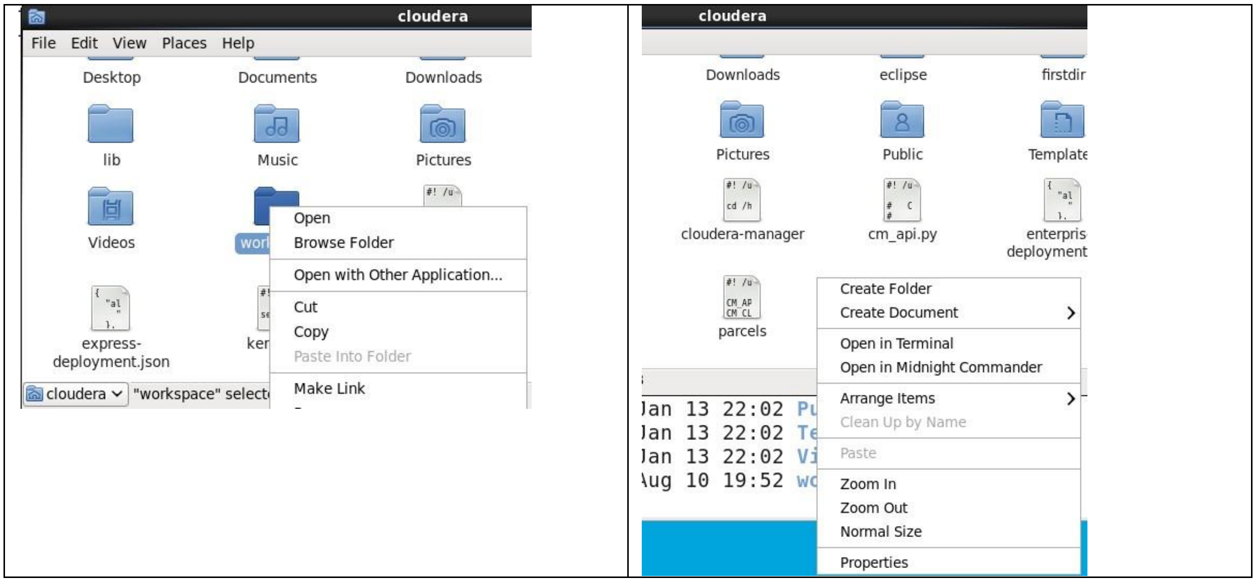
```
rm: descend into directory `firstdir/seconddir'? y
rm: remove directory `firstdir/seconddir/thirddir'? y
rm: remove directory `firstdir/seconddir'? y
rm: remove directory `firstdir'? y
```

Verify now that `firstdir` has been removed by listing the directory contents:

```
ls -l
```

```
total 5440
-rwxrwxr-x  1 cloudera cloudera    5387 Apr  5  2016 cloudera-manager
-rwxrwxr-x  1 cloudera cloudera    9964 Apr  5  2016 cm_api.py
drwxrwxr-x  2 cloudera cloudera    4096 Nov 25 04:48 data
drwxrwxr-x  3 cloudera cloudera    4096 Jul 23 07:17 data-for-exercises
-rw-rw-r--  1 cloudera cloudera   20136 Aug  6 06:21 derby.log
drwxrwxr-x  2 cloudera cloudera    4096 Jan 13 20:53 Desktop
drwxrwxr-x  4 cloudera cloudera    4096 Apr  5  2016 Documents
drwxr-xr-x  2 cloudera cloudera    4096 Jul  8  2016 Downloads
drwxrwsr-x  9 cloudera cloudera    4096 Jul  7  2016 eclipse
-rw-rw-r--  1 cloudera cloudera   53653 Apr  5  2016 enterprise-
deployment.json
-rw-rw-r--  1 cloudera cloudera   50513 Apr  5  2016 express-
deployment.json
…….
…….
```

The File Browser provides the standard facility of creating new folders and files (or documents), as well as deleting, copying and renaming existing folders and files. There are accessible via the File and Edit options in the Main Menu bar, as well as through the drop down menu presented when right clicking on a file, directory or empty space in the window.



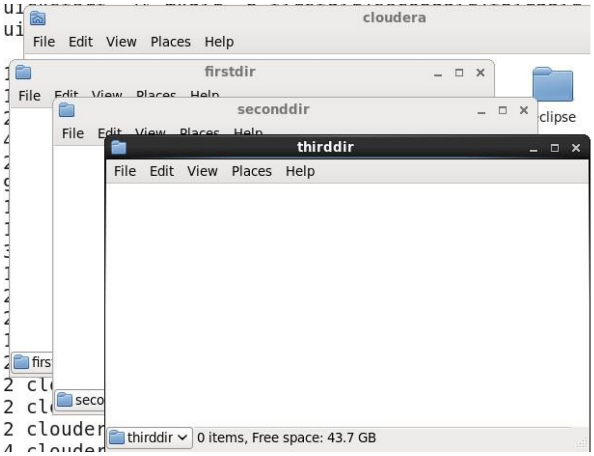
Repeat the previous sequence of creating and deleting the nested directory structure, but this time using the File Browser instead.

Return back to the shell terminal and recreate this nested subdirectory structure with a single command:

```
mkdir -p firstdir/seconddir/thirddir
ls -l
```

```
total 192
-rwxrwxr-x 1 cloudera cloudera  5387 Aug 10 19:52 cloudera-manager
-rwxrwxr-x 1 cloudera cloudera  9964 Aug 10 19:52 cm_api.py
drwxrwxr-x 2 cloudera cloudera  4096 Aug 10 19:52 Desktop
drwxrwxr-x 4 cloudera cloudera  4096 Aug 10 19:52 Documents
drwxr-xr-x 2 cloudera cloudera  4096 Jan 13 22:02 Downloads
drwxrwsr-x 9 cloudera cloudera  4096 Feb 19  2015 eclipse
-rw-rw-r--  1  cloudera  cloudera  53653  Aug  10  19:52  enterprise-
deployment.json
-rw-rw-r--  1  cloudera  cloudera  50513  Aug  10  19:52  express-
deployment.json
drwxrwxr-x 3 cloudera cloudera  4096 Jan 13 23:50 firstdir
…….
…….
```

VMWare Workstation supports drag-and-drop functionality to transfer files between the guest OS within an active VM and the host OS. Open a File Browser window (or use an existing one) and navigate to: `/home/cloudera/firstdir/seconddir/thirddir`.



Create a file named `file1.txt` in the Windows guest system using a text editor (for e.g. Notepad++) and fill it with random text. Then drag and drop this file into the File Browser view.

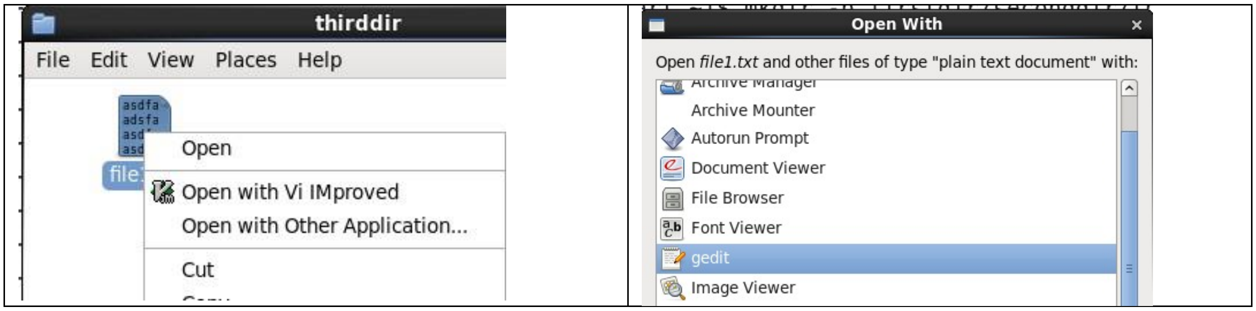
To view the contents of this file from the Linux shell:

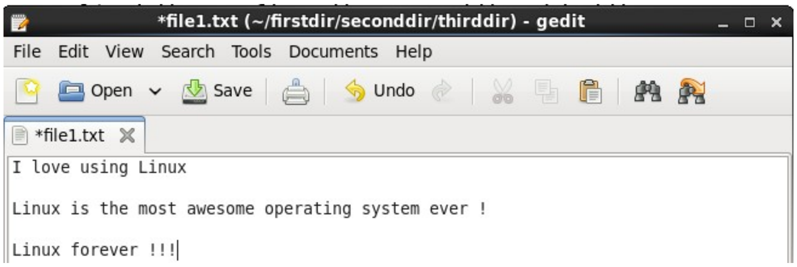
```
cd firstdir/seconddir/thirddir
less file1.txt
```

A listing of the file contents appears. Use the arrow keys to scroll through the output (the word END appears to indicate the end of the file) and press Q to quit the display and return to the shell prompt

The guest CentOS Linux comes with two text editors (`gedit` and `Vi Improved`) that allow you to view and modify the contents of files in the Linux file system. The first one, `gedit`, provides sufficient functionality to do some basic editing and formatting and will be the one that we will use for the remaining labs as it is simpler to work with compared to `Vi Improved` (although you are free to use any editor of your choice). For heavy duty editing or code work, work with a Windows-based editor or IDE and transfer the file to the Linux file system when you are done.

Right click on `file1.txt` in the File Browser window and select Open with Other Application. In the Dialog box that appears, select gedit.




*file1.txt (~/firstdir/seconddir/thirddir) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
*file1.txt

```
I love using Linux

Linux is the most awesome operating system ever !

Linux forever !!!
```

Make some changes to `file1.txt` and save it. Return to the shell terminal to view its contents and verify that the changes were saved:

```
less file1.txt
```

Notice that when we work with gedit, saving a file automatically creates a back up file with a tilde (~) appended to it.

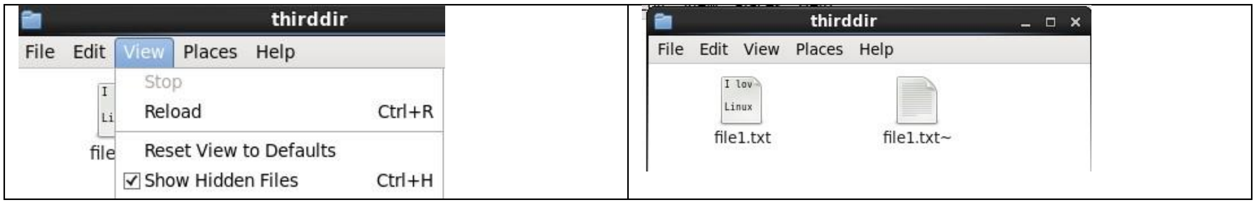
```
ls -l
```

```
total 8
-rwxrw-rw- 1 cloudera cloudera 95 Jan 14 00:15 file1.txt
-rw-rw-rw- 1 cloudera cloudera 54 Jan 14 00:04 file1.txt~
```

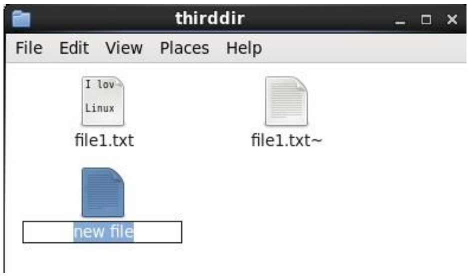
Notice also that `file1.txt` is in green font; this indicates it is a file transferred from the host OS. Verify that the contents of `file1.txt~` are the previous version of `file1.txt` prior to the changes that you made to it.

```
less file1.txt~
```

Currently, this backup file is not viewable from the File Browser window. To do this, you need to enable the Show Hidden Files option from View in the Main Menu.

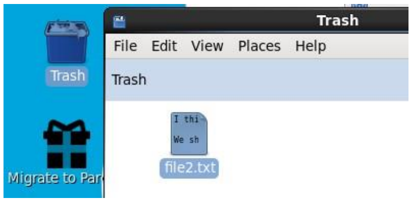


Right click anywhere in the empty space in the open File Browser window and select Create Document -> Empty File, and rename the newly created file to `file2.txt`.



Right click on it and choose to edit with `gedit` from the drop down menu. Then populate this file with some random text and save it. Right click on it again and choose Copy from the drop down menu. Switch back to the Windows host system, and right click on any open Explorer window and select Paste. The file will now be copied into the directory of that Explorer window. You can also use the drag-and-drop functionality that we saw earlier to transfer the file.

There are two ways to delete a file in Linux: using the File Browser or from the shell terminal. We will start with the first approach. Right click on `file2.txt` and select Move to Trash from the drop down menu. The Trash facility here is conceptually identical to the Windows Recycle Bin: it allows temporary storage of deleted files in case you need to recover them. Open the Trash folder by double clicking on its icon on the Desktop.



Right click on `file2.txt`. The drop down menu offers the usual options associated with a File Browser, and additionally the option of either deleting the file permanently or restoring it to its original location. Choose to restore it, and verify that `file2.txt` is now returned to its original location.

Return back to the shell terminal and repeat the deletion using a Linux command instead:

```
ls -l
```

```
total 12
-rwxrw-rw- 1 cloudera cloudera 95 Jan 14 00:15 file1.txt
-rw-rw-rw- 1 cloudera cloudera 54 Jan 14 00:04 file1.txt~
-rw-rw-r-- 1 cloudera cloudera 79 Jan 14 00:30 file2.txt
-rw-rw-r-- 1 cloudera cloudera  0 Jan 14 00:27 file2.txt~
```

```
rm -f file2.txt
ls -l
```

```
total 8
-rwxrw-rw- 1 cloudera cloudera 95 Jan 14 00:15 file1.txt
-rw-rw-rw- 1 cloudera cloudera 54 Jan 14 00:04 file1.txt~
-rw-rw-r-- 1 cloudera cloudera  0 Jan 14 00:27 file2.txt
```

The `-f` option parameter allows the deletion operation to proceed without any prompting from the shell.

Open the Trash folder again. Notice that `file2.txt` is not found in it. This illustrates a very important point: deleting using `rm` from the shell is permanent; there is no way to recover the files. Thus be very careful when using `rm`, especially with wildcard characters like *.

Remove the two backup files with:

```
rm -f *.txt~
```

The * is a wildcard character which allows the selection of multiple files (or directories) simultaneously. In this case, it selects all files that end with the extension `txt~` for deletion.

We can make a copy of the single file left in the directory:

```
cp file1.txt file1copy.txt
ls -l
```

```
total 8
-rwxrw-r-- 1 cloudera cloudera 95 Jan 14 00:53 file1copy.txt
-rwxrw-rw- 1 cloudera cloudera 95 Jan 14 00:15 file1.txt
```

We can copy the file to other directories as well:

```
cp file1.txt ../../
cp file1.txt ~
```

The first command copies the file up two directories into `firstdir`. The second command copies the file into the home directory (`/home/cloudera`). The ~ symbol is used as a shortcut to refer to the absolute path for the home directory. Verify the existence of the copied file at these two locations either through Linux shell commands (`cd, ls -l`) or navigating through the File Browser view.

We can move files as well. Moving files within the same directory renames them.

```
mv file1copy.txt dog.txt
ls -l
```

```
total 8
-rwxrw-r-- 1 cloudera cloudera 95 Jan 14 00:53 dog.txt
-rwxrw-rw- 1 cloudera cloudera 95 Jan 14 00:15 file1.txt
```

To move to a different directory, specify the directory location:

```
mv dog.txt ../
```

This moves the dog.txt up to the parent directory. Note that we could have used an absolute path here by typing: `mv dog.txt /home/cloudera/firstdir/seconddir/` instead. Either approach is fine (absolute or relative path) but it is important to be clear which one you are using to avoid unintentional errors particuarly when moving or deleting files and directories.

When specifying file or directory names in conjunction with commands, we often use wildcard characters to select more than one file or directory at a time. The most common wildcard character is *. For e.g.

```
mv *.txt newdirectory
```

Will move all files ending with the extension .txt in the current directory to *`newdirectory`*

```
rm *
```

will remove all files in the current directory. If there are directories in here, they will need to be removed first before running this command.

The previous copying, moving and renaming operations can also be accomplished via the File Browser. Repeat them using the File Browser as an exercise.

2.1 Additional Linux tutorials

Now that you are familiar with the Linux environment, you should go through a few detailed tutorials available on the Internet to acquaint yourself with some of the other basic Linux commands. When going through these tutorials, keep in mind that for this particular Linux installation, the active user account is `cloudera` and the machine name is `quickstart` (hence the shell prompt `cloudera@quickstart`). The tutorials will use different user account and machine names, so perform a substitution where appropriate. Try to confine your operations to the `/home/cloudera` directory as adding or deleting items in other directories may unintentionally affect the operation of some of the Hadoop components that we will be working with later.

http://linuxcommand.org/lc3_learning_the_shell.php
Go through the following parts:
1. What Is "The Shell"?
2. Navigation
3. Looking Around
4. A Guided Tour
5. Manipulating Files
6. Working With Commands
7. I/O Redirection
8. Expansion

http://www.ee.surrey.ac.uk/Teaching/Unix/
Go through Tutorial One to Four:

3 Kali Linux

Kali Linux is the next evolution and successor to the popular BackTrack Linux, an open source Debian-based distribution that comes with a plethora of penetration testing tools preinstalled and preconfigured. This simplifies the process of penetration testing as these tools can be used immediately and in combination with each other. Kali includes open source versions of numerous commercial security products which is a great incentive to use it, and it also provides options of upgrading to the fully featured versions which can be used directly through Kali. Kali also runs on a wide range of hardware devices (for e.g. a Raspberry PI), thus increasing the options available for pen testing many systems.

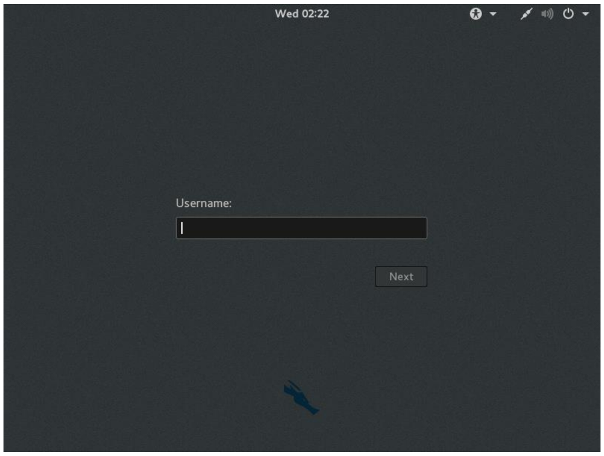
The various distributions of Kali can be downloaded in the form of an ISO file from:

https://www.kali.org/downloads/

This ISO can subsequently be burned as an installation image on a CD which can be used to install directly on a physical machine, or alternatively to create a VM using virtualization platforms such as Oracle VirtualBox or VMWare Workstation.

3.1 Basic Intro

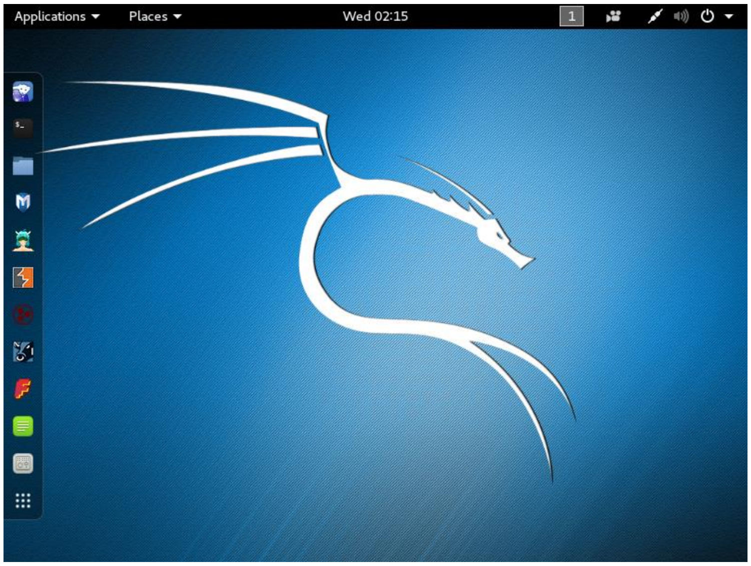
For the security labs, we will be running Kali Linux in a VM. Make sure to allocate at least 1GB of RAM (and 2 processors, if possible) to it from the VM settings in VMWare Workstation before starting the VM. After several boot up messages, you will be prompted for a user name and password.



Use the following credentials to allow you to login as root or superuser account.

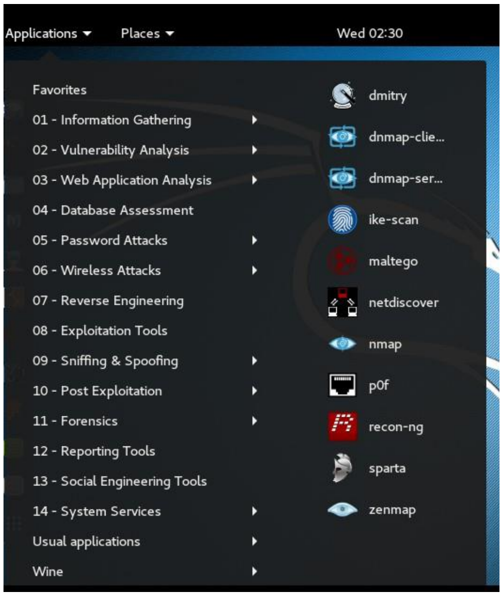
Username: `root`
Password: `toor`

You will then reach the main Desktop screen.

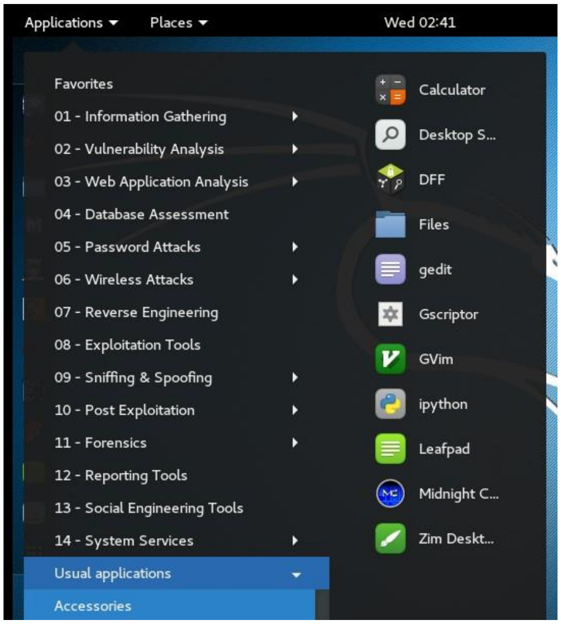


The various icons on the left panel provide a quick start to the corresponding applications. The first 3 icons start IceWeasel (the default browser for Kali), a shell terminal and the native File Browser. The remaining icons start common pen testing applications such as Metasploit, Armitage, Burpsuite, etc.

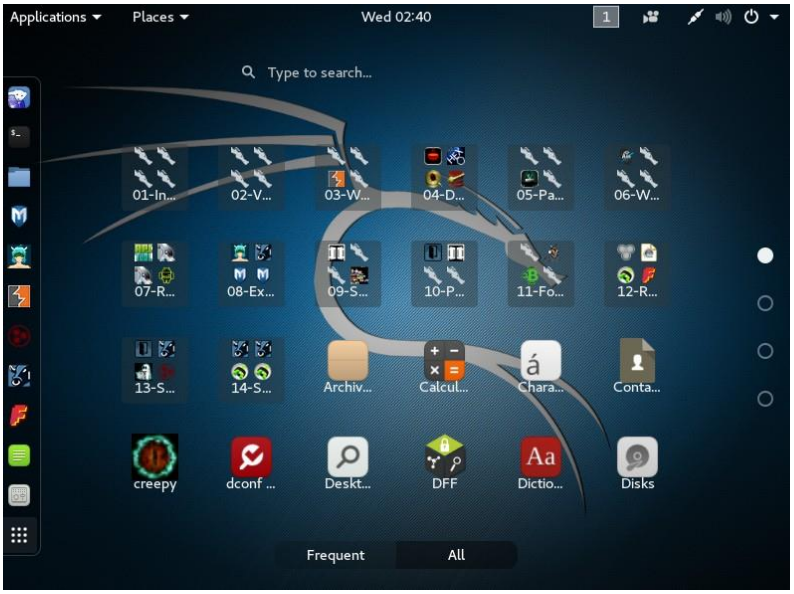
Clicking on Applications provides a list of numbered options that categorize tools for various phases and functionality of pen testing (e.g. 01 – Information gathering, 02 - Vulnerability Analysis, 03 - Web Application Analysis, etc). Sliding the mouse pointer down the various numbered options gives a side menu of application icons that fall into each respective category:



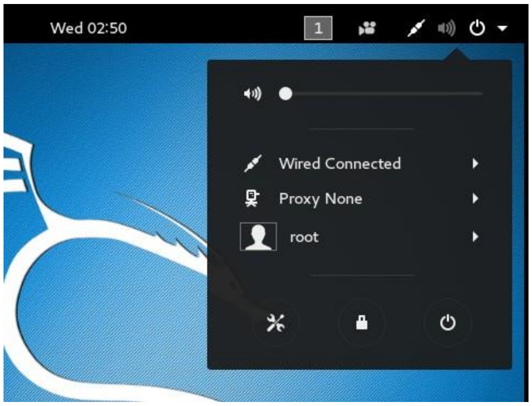
Clicking on Usual Applications -> Accessories gives you the list of common applications that are useful for general operations such as text file editors (gedit, Leafpad and GVim), calculator, Desktop search.



To get a full list of all applications installed on the Kali OS, click on the last icon on the left panel, and then click on the radio buttons on the right to scroll through the various applications.



Clicking on the arrow at the upper right hand corner gives you access to account and network settings, which will be useful for certain lab sessions. It also allows you to power down and restart the VM when you are done working in it.


Wed 02:50
1
Wired Connected
Proxy None
root