

Tutorial No. : 2

**Title: Report on basic commands and scripting
in Kali Linux**



(A Constituent College of Somaiya Vidyavihar University)

Roll No.: 16010420075

Tutorial No.: 2

Aim: Report on commands in Linux and writing scripts

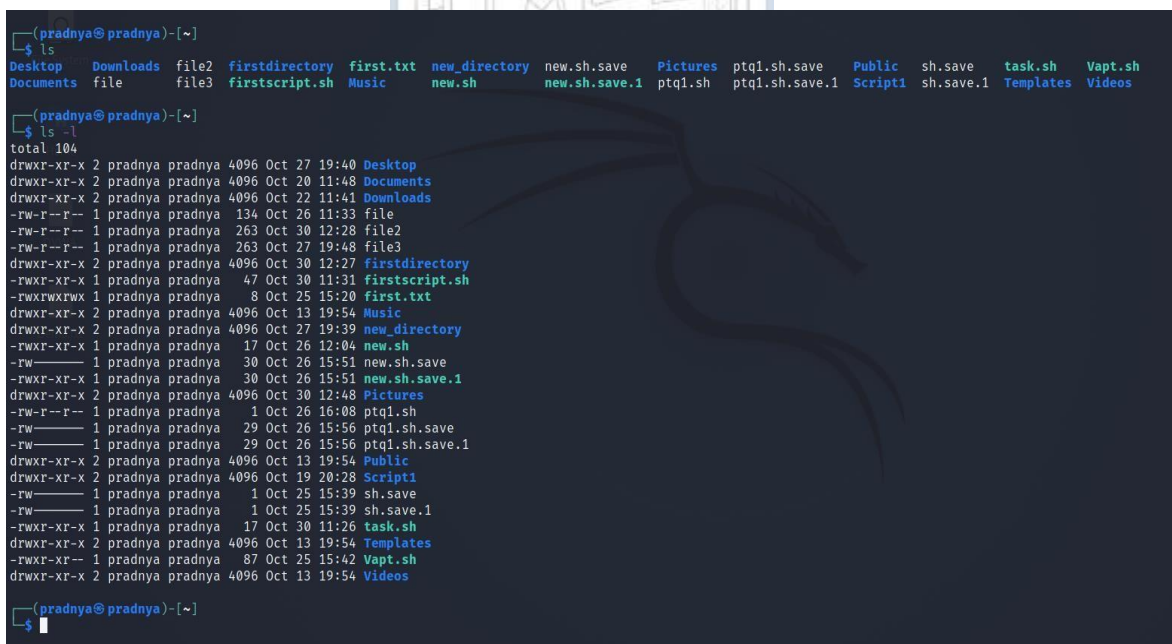
Resources: Kali Linux OS, Any editor for documentation

Theory

Kali Linux Commands is an advanced penetration testing distribution by offensive security. Its features allow users to create custom complex images with ease. Following are the must know Linux basic commands with examples:

1. Listing files (ls):

- If you want to see the list of files on your UNIX or Linux system, use the 'ls' command. It shows the files /directories in your current directory.
- Directories are denoted in blue color. Files are denoted in white. You will find similar color schemes in different flavors of Linux.
- You can use 'ls -l' to shows all the files not only in directories but also subdirectories



```
(pradnya@pradnya)~$ ls
Desktop  Downloads  file2  firstdirectory  first.txt  new_directory  new.sh.save  Pictures  ptq1.sh.save  Public  sh.save  task.sh  Vapt.sh
Documents file      file3  firstscript.sh  Music      new.sh         new.sh.save.1  ptq1.sh  ptq1.sh.save.1  Script1  sh.save.1  Templates  Videos

(pradnya@pradnya)~$ ls -l
total 104
drwxr-xr-x 2 pradnya pradnya 4096 Oct 27 19:40 Desktop
drwxr-xr-x 2 pradnya pradnya 4096 Oct 20 11:48 Documents
drwxr-xr-x 2 pradnya pradnya 4096 Oct 22 11:41 Downloads
-rw-r--r-- 1 pradnya pradnya 134 Oct 26 11:33 file
-rw-r--r-- 1 pradnya pradnya 263 Oct 30 12:28 file2
-rw-r--r-- 1 pradnya pradnya 263 Oct 27 19:48 file3
drwxr-xr-x 2 pradnya pradnya 4096 Oct 30 12:27 firstdirectory
-rwxr-xr-x 1 pradnya pradnya 47 Oct 30 11:31 firstscript.sh
-rwxrwxrwx 1 pradnya pradnya 8 Oct 25 15:20 first.txt
drwxr-xr-x 2 pradnya pradnya 4096 Oct 13 19:54 Music
drwxr-xr-x 2 pradnya pradnya 4096 Oct 27 19:39 new_directory
-rwxr-xr-x 1 pradnya pradnya 17 Oct 26 12:04 new.sh
-rw-r--r-- 1 pradnya pradnya 30 Oct 26 15:51 new.sh.save
-rwxr-xr-x 1 pradnya pradnya 30 Oct 26 15:51 new.sh.save.1
drwxr-xr-x 2 pradnya pradnya 4096 Oct 30 12:48 Pictures
-rw-r--r-- 1 pradnya pradnya 1 Oct 26 16:08 ptq1.sh
-rw-r--r-- 1 pradnya pradnya 29 Oct 26 15:56 ptq1.sh.save
-rw-r--r-- 1 pradnya pradnya 29 Oct 26 15:56 ptq1.sh.save.1
drwxr-xr-x 2 pradnya pradnya 4096 Oct 13 19:54 Public
drwxr-xr-x 2 pradnya pradnya 4096 Oct 19 20:28 Script1
-rw-r--r-- 1 pradnya pradnya 1 Oct 25 15:39 sh.save
-rw-r--r-- 1 pradnya pradnya 1 Oct 25 15:39 sh.save.1
-rwxr-xr-x 1 pradnya pradnya 17 Oct 30 11:26 task.sh
drwxr-xr-x 2 pradnya pradnya 4096 Oct 13 19:54 Templates
-rwxr-xr-x 1 pradnya pradnya 87 Oct 25 15:42 Vapt.sh
drwxr-xr-x 2 pradnya pradnya 4096 Oct 13 19:54 Videos

(pradnya@pradnya)~$
```

- ### 2. pwd (Print working directory):
- pwd stands for “Print Working Directory” which simply prints the name of the working directory

(A Constituent College of Somaiya Vidyavihar University)

```
(pradnya@pradnya)-[~]
$ pwd
/home/pradnya
(pradnya@pradnya)-[~]
$
```

3. Date: This command is generally used to display the system date and time.

```
(pradnya@pradnya)-[~]
$ date
Saturday 30 October 2021 12:26:43 PM IST
```

4. whoami: The whoami command simply prints the effective user ID whereas who command prints the information about users who are currently logged in.

```
(pradnya@pradnya)-[~]
$ whoami
pradnya
```

5. mkdir: The command used for creating directories is mkdir. For e.g. mkdir /root/Desktop/yeahhub

```
(pradnya@pradnya)-[~]
$ mkdir firstdirectory
```

6. cat (concatenate): Command is one of the most frequently used command in Kali Linux which allows us to create single or multiple files, view contain of file, concatenate files and redirect output in terminal or files. E.g. \$cat file1> file2

```
(pradnya@pradnya)-[~]
$ cat file1>file2
```

cat file1 file2>file2: Joins two files 1 and 2 and stores output of them in a new file3

7. cp (copy): This command is used to copy files or group of files or directory which creates an exact image of a file on a disk with different file name.

```
(pradnya@pradnya)-[~]
$ cp file1 file3
```

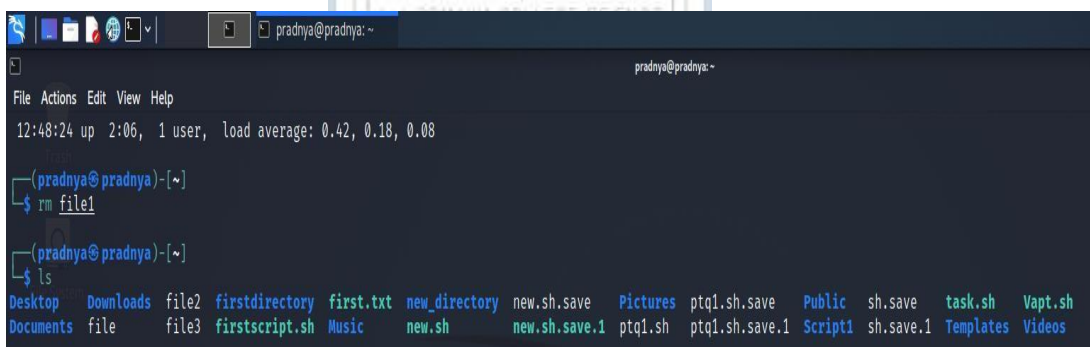
8. mv: The mv command moves, or renames, files and directories on your file system.

```
(pradnya@pradnya)-[~]
$ mv file file3

(pradnya@pradnya)-[~]
$
```

9. rm (remove):

- Command is used to delete files. When used recursively, it may be used to delete directories.
- The removal process unlinks a file name in a file system from its associated data, and marks that space on the storage device as usable by future writes.
- In other words, when you remove a file, the data in the file isn't changed, but it's no longer associated with a filename.



```
pradnya@pradnya: ~
File Actions Edit View Help
12:48:24 up 2:06, 1 user, load average: 0.42, 0.18, 0.08

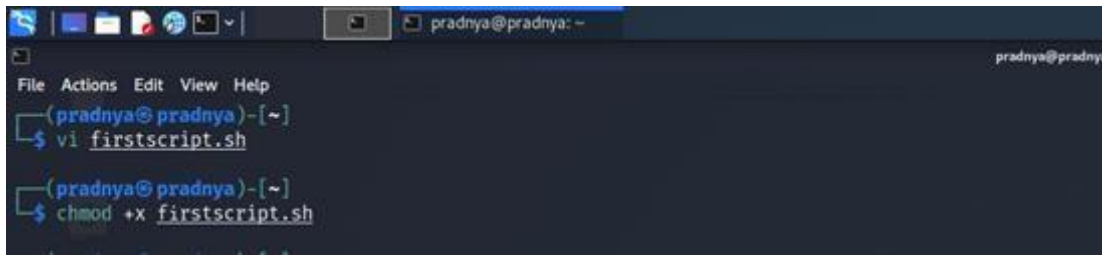
(pradnya@pradnya)-[~]
$ rm file1

(pradnya@pradnya)-[~]
$ ls
Desktop  Downloads  file2  firstdirectory  first.txt  new_directory  new.sh.save  Pictures  ptq1.sh.save  Public  sh.save  task.sh  Vapt.sh
Documents  file  file3  firstscript.sh  Music  new.sh  new.sh.save.1  ptq1.sh  ptq1.sh.save.1  Script1  sh.save.1  Templates  Videos
```

10. vi:

- The vi editor is a screen editor which is available on almost all UNIX systems. In general, vi has two modes: the command mode and the insert mode.
- To begin entering text in an empty file, you must first change from the command mode to the insert mode. To do this, type the letter i. When you start typing, anything you type will be entered into the file.
- Type a few short lines and hit Return at the end of each of line. Unlike word processors, vi does not use word wrap. It will break a line at the edge of the screen.

- If you make a mistake, you can use the Backspace key to remove your errors. If the Backspace key doesn't work properly on your system, try using the Ctrl h key combination.



```

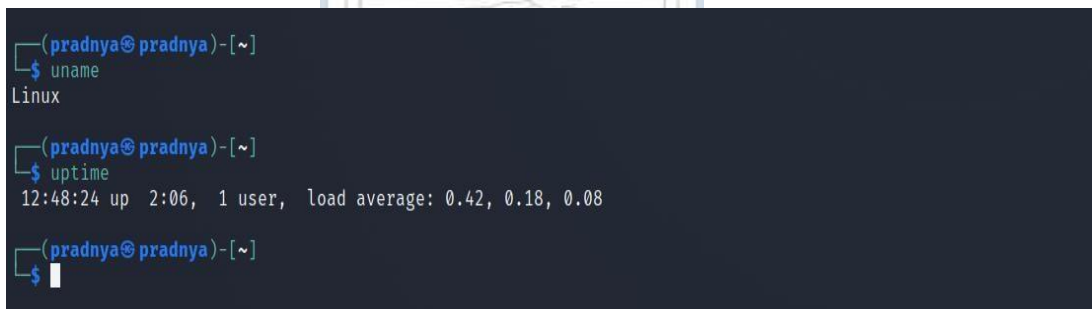
pradnya@pradnya: ~
File Actions Edit View Help
(pradnya@pradnya)-[~]
$ vi firstscript.sh
(pradnya@pradnya)-[~]
$ chmod +x firstscript.sh

```

11. uname:

- This command prints the information about the current system. The uname command within Linux allows you to view system information about your Linux environment.
- With `uname -a` command, which gives you more information about the system like Kernel Name, Node Name, Kernel Release, Kernel Version, Machine, Processor, Hardware Platform and Operating system.

12. uptime: The uptime command gives you the time for which the system has been up (or running). Uptime's basic usage is very easy – just write the command's name and press enter.

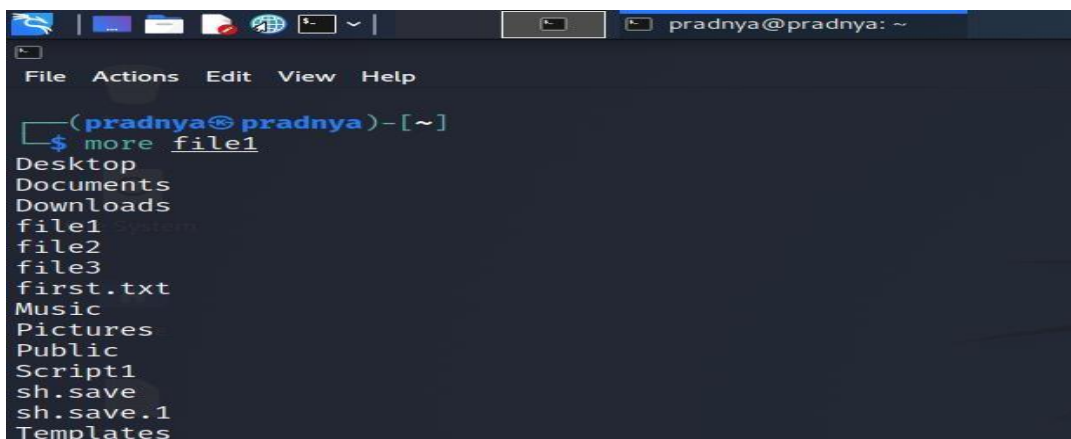


```

(pradnya@pradnya)-[~]
$ uname
Linux
(pradnya@pradnya)-[~]
$ uptime
12:48:24 up 2:06, 1 user, load average: 0.42, 0.18, 0.08
(pradnya@pradnya)-[~]
$

```

13. more: it is filter for paging through text one screenful at a time e.g. `more myfile`



```

pradnya@pradnya: ~
File Actions Edit View Help
(pradnya@pradnya)-[~]
$ more file1
Desktop
Documents
Downloads
file1
file2
file3
first.txt
Music
Pictures
Public
Script1
sh.save
sh.save.1
Templates

```

14. less: less command is used to view files instead of opening the file. The less command is considered to be a more powerful version of the “more” command which is used to display information to the terminal one page at a time.

15. chmod: To change file access permissions

- u- user who owns the file, g- group file owner, o- user classified as others, a- all other system user , + set permissions, - remove permission, r - read permission, w- write permission, x- execute permission
- e.g. \$chmod x myfile

```
(pradnya@pradnya)-[~]
$ chmod +x firstscript.sh
```

16. wc (word count): To count lines, words and characters of the given files. E.g. \$wc -r myfile

```
(pradnya@pradnya)-[~]
$ wc file1
33 33 263 file1
```

17. head: Used to print the first N lines of a file. It accepts N as a input and the default value of N is 10. E.g. \$head -6 myfile

18. tail: used to print last N-1 lines of a file. It accepts n as input and default value of N is 10. E.g. \$tail-5 myfile

```
(pradnya@pradnya)-[~]
$ head -3 file1
Desktop
Documents
Downloads

(pradnya@pradnya)-[~]
$ tail -1 file1
Videos
```

19. cmp: This command is used to compare the files. E.g. \$cmp file1 file2

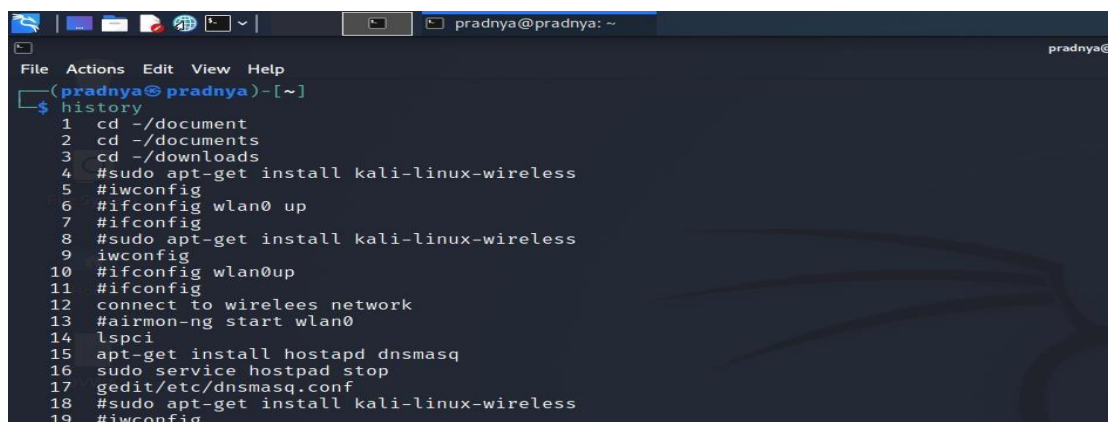
```
(pradnya@pradnya)-[~]
$ cmp file1 file2
```

20. pr: this command is used to print the file. E.g. \$pr file1
21. sort: Sort command sorts the contents of a text file, line by line. Sort is a standard command line program that print the lines of its input or concatenation of all files listed in its argument list in sorted order.



```
(pradnya@pradnya)-[~]
$ sort file1
Desktop
Desktop
Documents
Documents
Downloads
Downloads
file
file1
file1
file2
file2
file3
file3
first.txt
first.txt
Music
Music
Pictures
Pictures
Public
Public
Script1
Script1
sh.save
sh.save
sh.save.1
sh.save.1
Templates
Templates
Vapt.sh
Vapt.sh
Videos
Videos
(pradnya@pradnya)-[~]
$
```

22. free: free is a command which can give us valuable information on available RAM in Linux machine. It also gives information about total used and available space of physical memory and swap memory with buffers used by kernel. E.g. \$free
23. history: One of the extensively used command in Kali Linux is history command. The bash shell stores a history of commands entered, which can be used to repeat commands by using the history command. In simple manner, you can run the history command by itself and will simply print out the bash history of current user to the screen.

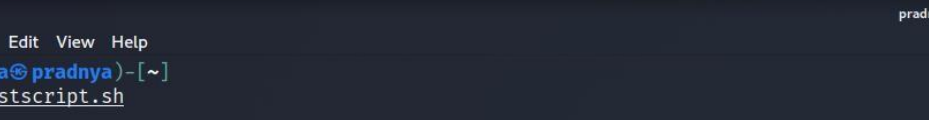


```
(pradnya@pradnya)-[~]
$ history
1 cd ~/document
2 cd ~/documents
3 cd ~/downloads
4 #sudo apt-get install kali-linux-wireless
5 #iwconfig
6 #ifconfig wlan0 up
7 #ifconfig
8 #sudo apt-get install kali-linux-wireless
9 iwconfig
10 #ifconfig wlan0up
11 #ifconfig
12 connect to wirelees network
13 #airmon-ng start wlan0
14 lspci
15 apt-get installl hostapd dnsmasq
16 sudo service hostpad stop
17 gedit/etc/dnsmasq.conf
18 #sudo apt-get install kali-linux-wireless
19 #iwconfig

```


Scripting in Kali Linux:

- Scripting allows for an automatic commands execution that would otherwise be executed interactively one-by-one. Shell is a macro processor which allows for an interactive or non-interactive command execution. Scripting is a way to execute all given commands together.
- Bash is a command language interpreter. It is widely available on various operating systems and is a default command interpreter on most GNU/Linux systems. The name is an acronym for the 'Bourne-Again SHell'.
- A shell script is a file that contains ASCII text. To create a shell script, we use a text editor. A text editor is a program, like a word processor, that reads and writes ASCII text files. There are many text editors available for Linux systems, both for the command line and GUI environments. Some common ones are vi, gedit, nano, emacs, kwrite.
- Let's create a new shell script for that open vi editor to create new file firstscript.sh. Once ready, make your new file executable using chmod command with an option +x. Lastly, execute your new script by prefixing its name with ./



The screenshot shows a terminal window with a dark background. The title bar at the top indicates the user is 'pradnya@pradnya' in the home directory. The terminal content shows a series of commands and their output:

```
(pradnya@pradnya)-[~]  
$ vi firstscript.sh  
  
(pradnya@pradnya)-[~]  
$ chmod +x firstscript.sh  
  
(pradnya@pradnya)-[~]  
$ ./firstscript.sh  
hello world!  
  
(pradnya@pradnya)-[~]  
$
```

The prompt changes from '(pradnya@pradnya)-[~]' to '\$' after each command. The output 'hello world!' is displayed on the line following the execution of './firstscript.sh'. A cursor is visible on the line following the final '\$' prompt.

The screenshot shows a terminal window with a dark background. The title bar at the top indicates the user is 'pradnya' on a machine named 'pradnya', in the home directory '~'. The terminal content shows a shell script being executed. The first line is a comment: `#this is my first script`. The second line is an echo command: `echo "hello world!"`. The output of the command, `hello world!`, is printed on the following line. The prompt character is a simple box.

- The first line is a comment. Everything that appears after a "#" symbol is ignored by bash. As our scripts become bigger and more complicated, comments become vital. They are used by programmers to explain what is going on so that others can figure it out. The last line is the echo command. This command simply prints its arguments on the display.
- The next thing we have to do is give the shell permission to execute our script. This is done with the chmod command as \$ chmod +x firstscript.sh. We can also give command as \$chmod 777 firstscript.sh. The "777" will give us read, write, and execute permission. Everybody else will get only read and execute permission. To make the script private, (i.e., only we can read and execute), use "700" instead.
- Now to run our script give command as \$./firstscript.sh. We should see "Hello World!" displayed. By use of scripting, any shell interaction can be automated and scripted.

IMPLEMENTATION AND RESULTS:

1. whoami

```
(kali㉿kali)-[~]
└─$ whoami
kali

(kali㉿kali)-[~]
└─$ who: user ID whereas the who command print
kali      tty7      2022-02-01 09:06 (:0)
```

2. ls

```
(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

3. uname

```
(kali㉿kali)-[~]
└─$ uname -a
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64
GNU/Linux
```

4. uptime

```
(kali㉿kali)-[~]
└─$ uptime
09:17:32 up 11 min,  1 user,  load average: 0.96, 0.76, 0.48
```

5. free

```
(kali㉿kali)-[~]
$ free
```

	total	used	free	shared	buff/cache	availa
ble						
Mem:	2029520	1317948	84828	102232	626744	461
100						
Swap:	998396	2060	996336			

Outcomes: We have successfully created first script in Kali Linux called as “hello world!” There are many more commands related to kali Linux which can be used for ease of vulnerability assessment and penetration testing.

Conclusion:

The Linux commands were successfully reported and executed in it's terminal.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- [1] Scripting tutorial for beginners: <https://www.linuxconfig.com>
- [2] Kali Linux commands: <https://www.javatpoint.com>
- [3] Top 20 Kali Linux commands: <https://www.jigsawacademy.com>
- [4] Top 20 basic kali Linux commands: <https://www.yeahhub.com>