Getting comfortable with linux

28 April 2021

17:32

**kali linux file system**

Kali linux adhere to the filesystem hierarchy standard (FHS) which provide a familiar and universal layout for all linux users. The directories you will find most useful are:

* /bin - basic program (ls, cd, cat, etc.) (binary files)
* /sbin - system programs ( fdisk, mkfs, sysctl, etc)
* /etc - configuration files
* /tmp - tempotaty files (typically deleted on boot)
* /usr/bin - application (apt, ncat, nmap, etc.)

This is the primary directory for executable programs. Most

programs executed by normal users which are not needed for

booting or for repairing the system and which are not

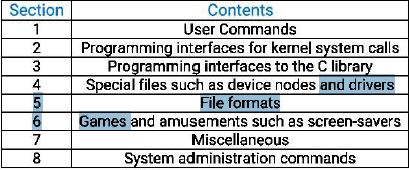
installed locally should be placed in this directory.

* /usr/share - application support and data files

**Man page**

Man ls (for manual)

Man -k passwd



**Apropos**

With apropos command we can search the list of the man page description for a possible based on a keyword. Example : suppose that we want to partition a a hard drive but can't remember the name of the command we can figure out with an apropos search for partition

**Listing file**

**Ls**

-a (display all files hidden also)

-1 (each file on a single line)

**Moving around**

Cd

**Creating directories**

**Mkdir**

Mkdir one two (make 2 dir)

Mkdir "one two" (make one folder)

Mkdir -p test/{recon,test,uu} (create dir test within test create 2 sub dir)

**Finding the files**

Which, locate, find

**Which:** the which command search through the directories that are defined in the **$path** environment variable for a given file name.

-echo $path (to who path variable)

Which python (to search)

**Locate:** the locate command is the quickest way to find the locations of files and directories in kali in order to provide a much shorter search time. Locate searches built-in-database name **locate.db** rather than entire hard disk. Database automatically update .to manual update locate.db database, you can use **updatedb** command.

Sudo updatedb (update locatedb)

**Find:** the find command is the most complex and flexible search tool. Find command preform recursive search starting from the root file system directory and look for any file that start the the letters "sbd"

Sudo find / -name snd

**Managing kali linux services**

**Ssh service**

The secure shell(ssh) serivce is most commonly used to remotely access a computer, using a secure, encryption protocol. The SSH is TCP-based and listens by default on port 22.

-->Sudo systemctl start ssh (to start ssh service)

-->Sudo ss -antl | greo sshd (to check ssh is on or not)

-->Sudo systemctl enable ssh (to start automatically at boot time)

-->We can use systemctl to enable and disable most service in kali linux.

**HTTP service**

The apache HTTP service is often used during a penetration test either for hosting a asite, or providing a platform for download files on a victim machine. The HTTP service is TCP-based and listing by default on port 80.

-->sudo systemctl start apache2 (to start spache service)

--> sudo ss -antlp | grep apache (to check HTTP start or not)

---> sudo systemctl enable apache2 (to start automatically)

most services in kali linux are operated in much the same way as SSH and HTTP, through their service ir init scripts. To see a table of all available.

-->systemctl list-unit-files

**Searching, installing, and removing tools**

APT is a set of tools that manage packages, or applications, on a Dabian-based system. We can use use APT to install and remove applications, updates packages, and even upgrade the entire system.

Apt update

Apt upgrade

Apt upgrade metasploit-framework

Apt install pure-ftpd

Apt remove pure-ftpd (leave some small user configuration files behind

Apt remove -purge (remove completely)

**DPKG**

Package manager

**Command line fun**

**Environment variables**

When opening a terminal window, a new bash process, which has its own **environment variables,** in initialized. One of the most commonly-referenced environment variables is PTH, which is colon-separated list of directory [aths that bash will search through whenever a command is run without a full path.

Export ip=10.0.2.2 (to make variable)

Echo %ip (to check)

Unsent ip (ip=variable name) (to delete variable)

Export -p (to list all exported variables)

**Alias command**

As a Linux user, you will tend to use the same commands time and time again. This will often tend to negatively impact your productivity. To save yourself from this inconvenience , alias command comes in handy. An alias is a custom shortcut that represents another command. It’s a shell command that allows you to define your own command based on a predefined set of pre-existing commands.

--> Alias (To list all predefined aliases)

To types of Alias

1. Temporary
2. Permanent

--> alias net='ping 10.0.2.2' (to make alias)

--> net (it will ping 10.0.2.2)

It will remove after you restart linux

To make in parmanent add alias in **bashrc** file

--> vim ~/.bashrc

Add alias in this

--> :wq! (to exit from bashrc file)

**To remove alias**

--> unalias net (it will remove net alias)

**Bash history tricks**

Bash maintain a history of commands that have benn entered which can be displayed with history command

-->history (to see history of commands)

-->!22 (to run command no. on 22 ) (! Line no, 22 run command on 22 no)

--> !! (repeats the last command that was executed during out terminal)

By default, the command history is saved to the **.bash\_history** file in the home directory. Two environment variable control the history size: HISTSIZE and HISTFILESIZE

HISTSIZE control the number of commands stored in memory for the current session and

HISTFILESIZE configures how many commands are kept in the history files. These variable can edited according to our needs and saved to the Bash configuration file(.bashrc).

**Ctrl+r** will invoke the reverse-i-search facility. Type a letter, for example, c and you will get a match for the most recent command I your history that contains the latter "c" keep typing to narrow down your match and when you find the desired command press enter to execute it

--> ctrl+r (to invoke a reverse-i-search)

**Piping and Redirection**

**< redirect standard input**

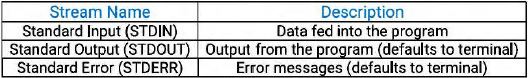
**> redirect standard output**

**2> redirect standard error**

**&> file redirect standard out and standard srror**

**>> appand the file**

Every program run from the command line has three streams connected to it that serve as communication channels with external environment. These streams are defined as foolow.



**Redirection to a New File**

We can use the > to save the output to a file to keep it for future.

-->echo "this is a file" > test1.txt (save data in test1.txt)

If we save the file output to a file that already exists, that files content will be replaced. And There is no undo function..

To append additional data to an existing file use >> operator.

>> to append the file

**Redirection from a file**

Wc -m < test1.txt (to count characters in file)

**Redirecting STDERR**

To save error in file

ls .test (give error)

Ls .test 2>error.txt (save error in error.txt file)

**Piping**

Cat error.txt

Cat error.txt | wc -m (count characters)

Cat error.txt | wc m > count.txt (save output in count.txt)

We used pipe character (|) to redirect the output to the cat command to the input of wc command.

**Text searching and manipulation**

**Grep**

Grep searches text files for the occurrence of a given regular expression and outputs any line containing a match to the standard output, which is usually the terminal screen.

-->cat /etc/passwd | grep kali

**Sed**

Sed is powerfull stream editor.

Pattern sed 's/word/change word/' (s=substitute)

--> echo this is my first day > bob.txt

--> sed 's/first/harder/' bob.txt

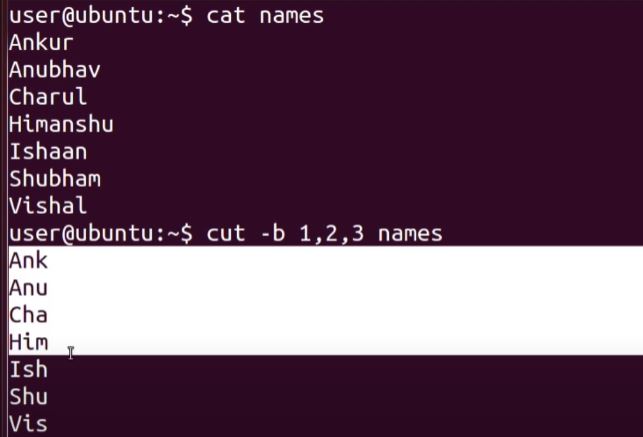
Change first with second and show output but nothing change in file.

**CUT**

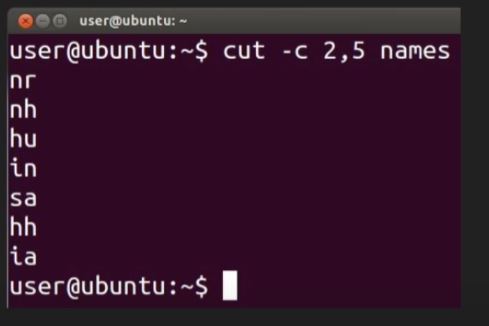
The cut command in linux is a command for cutting out the section from each line of files an writing the result to standard output.

The cut command slices a line and extracts the text.

--> cut -b 1,2,3 filename , cut -b 1-3,5,7 (-b= to extract the specific bytes)



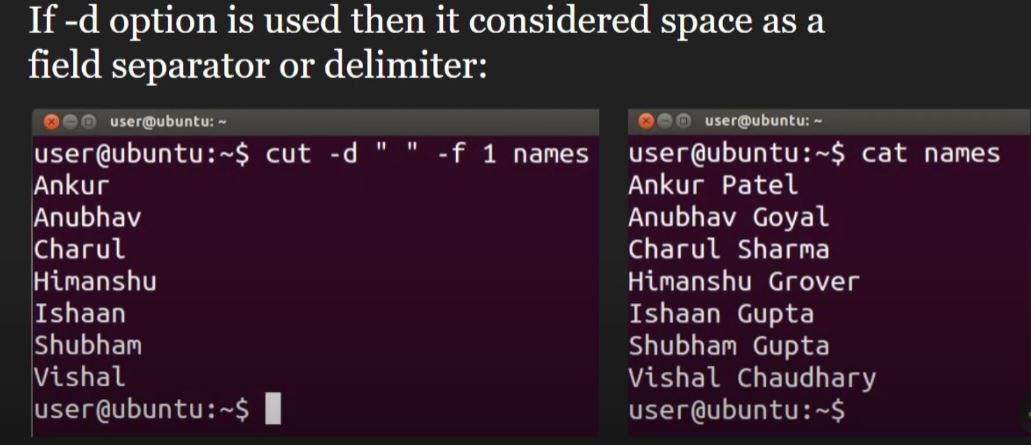
--> cut -c 2-5 (-c = to cut by character)



-->cut -d ":" -f 1 filename

-f = to extract the usefull information you need to but by fields rather than columns

cut use tab as a default field delimiter but can also work with other delimiter by using -d options



**AWK**

AWK is a programing language designed for text processing and is typically used as a data extraction and reporting tool.



