TCS332 Fundamental of Information Security and Blockchain

B. Tech CSE III Semester

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE

Head of Cyber security and IoT research group

Graphic Era (Deemed to be University), Dehradun, India

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

Unit-II
Linux basic commands

pwd

- When you first open the terminal, you are in the home directory of your user. To know which directory you are in, you can use the “pwd” command.

ls

Use the "ls" command to know what files are in the directory you are in. You can see all the hidden files by using the command “ls -a”.

cd

- Use the "cd" command to go to a directory. For example, if you are in the home folder, and you want to go to the downloads folder, then you can type in “cd Downloads”.
- To go back from a folder to the folder before that, you can type “cd ..” The two dots represent back.

mkdir & rmdir

- Use the mkdir command when you need to create a folder or a directory.
- For example, if you want to make a directory called “DIY”, then you can type “mkdir DIY”.
- Remember, as told before, if you want to create a directory named “DIY Hacking”, then you can type “mkdir DIY\ Hacking”.
- Use rmdir to delete a directory.
- But rmdir can only be used to delete an empty directory.
- To delete a directory containing files, use rm.

rm

- Use the rm command to delete files and directories. Use "rm -r" to delete just the directory.
- It deletes both the folder and the files it contains when using only the rm command.

touch

- The touch command is used to create a file.
- It can be anything, from an empty txt file to an empty zip file. For example, “touch new.txt”.

man

- To know more about a command and how to use it, use the man command.
- It shows the manual pages of the command.
- For example, “man touch” shows the manual pages of the touch command.

cp

- Use the cp command to copy files through the command line.
- It takes two arguments: The first is the location of the file to be copied, the second is where to copy.

Example:

cp waz.txt /home/mwazid/waz1

In another way:

cp /home/kali/Documents/myfolder2/file.txt /home/kali/Documents/myfolder3

mv

- Use the mv command to move files through the command line.
- We can also use the mv command to rename a file.

For example,

mv waz23.txt /home/mwazid/waz1

locate

- Is used to locate a file in a Linux system, just like the search command in Windows.
- This command is useful when you don’t know where a file is saved or the actual name of the file.
- Using the -i argument with the command helps to ignore the case (it doesn't matter if it is uppercase or lowercase).

locate

Example:

- locate waz.txt

Output:

- /home/mwazid/waz/waz.txt

echo

- The “echo” command helps us move some data, usually text into a file.
- For example, if you want add text to an already made text file, you just need to type in, “echo text >> filename.extension”.

Example:

- mwazid@mwazid:~/waz$ echo hello, my name is wazid >> waz.txt

cat

- Use the cat command to display the contents of a file. It is usually used to easily view programs.

sudo

- A widely used command in the Linux command line, sudo stands for “SuperUser Do”.
- So, if you want any command to be done with administrative or root privileges, you can use the sudo command.
- you can use the command “sudo passwd”. Then type in the new root password.
- **Example:** sudo apt-get update (to update OS)

df

- Use the df command to see the available disk space in each of the partitions in your system.
- If you want it to be shown in megabytes, you can use the command “df -m”.

- **Example: mwazid@mwazid:~$ df -m**

- Filesystem 1M-blocks Used Available Use% Mounted on
- /dev/sda1 467837 3670 440381 1% /
- none 1 0 1 0% /sys/fs/cgroup
- udev 727 1 727 1% /dev
- tmpfs 148 2 147 1% /run
- none 5 0 5 0% /run/lock
- none 738 3 736 1% /run/shm
- none 100 1 100 1% /run/user

du

- Use du to know the disk usage of a file in your system.
- If you want to know the disk usage for a particular folder or file in Linux, you can type in the command du and the name of the folder or file.
- Example: mwazid@mwazid:~/waz$ du waz.txt

Output:

4 waz.txt

Create tar Archive File

- Use tar to work with tarballs (or files compressed in a tarball archive) in the Linux command line.
- It works on the basis of the arguments given to it.
- For example, “tar -cvf” for creating a .tar archive, -xvf to untar a tar archive

Example: mwazid@mwazid:~$ tar -cvf waz.tar /home/mwazid/waz/

uname

- Use uname to show the information about the system your Linux distro is running.
- Using the command “uname -a” prints most of the information about the system.

Example: mwazid@mwazid:~$ uname –a

Output:

Linux mwazid 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:16:20 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux

apt-get

- Use apt to work with packages in the Linux command line. Use apt-get to install packages.
- For example, if you want to install the text editor jed, we can type in the command

sudo apt-get install jed

chmod

- Use chmod to make a file executable and to change the permissions granted to it.
- Suppose you have a python code named numbers.py.
- You'll need to run "python numbers.py" every time you need to run it.
- Instead of that, when you make it executable, you'll just need to run "numbers.py" in the terminal to run the file.
- To make a file executable, you can use the command "chmod +x numbers.py" in this case.
- You can use "chmod 755 numbers.py" to give it root permissions or "sudo chmod +x numbers.py" for root executable.

hostname

- Use hostname to know your name in your host or network.
- Basically, it displays your hostname and IP address.
- Just typing “hostname” gives the output.
- Typing in “hostname -I” gives you your IP address in your network.

Example: mwazid@mwazid:~$ hostname

Output: mwazid

- mwazid@mwazid:~$ hostname -I
- 192.168.43.252 2402:8100:2063:314a:a443:154a:de2:c5d0 2402:8100:2063:314a:26fd:52ff:fe9e:b5b9

To know about the addresses of your machine

- **mwazid@mwazid:~$ ifconfig**
- eth0 Link encap:Ethernet HWaddr d4:c9:ef:68:3e:1f
- UP BROADCAST MULTICAST MTU:1500 Metric:1
- RX packets:0 errors:0 dropped:0 overruns:0 frame:0
- TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
- collisions:0 txqueuelen:1000
- RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

To know about the addresses of your machine

- **mwazid@mwazid:~$ ifconfig**
-
- lo Link encap:Local Loopback
- inet addr:127.0.0.1 Mask:255.0.0.0
- inet6 addr: ::1/128 Scope:Host
- UP LOOPBACK RUNNING MTU:65536 Metric:1
- RX packets:4344 errors:0 dropped:0 overruns:0 frame:0
- TX packets:4344 errors:0 dropped:0 overruns:0 carrier:0
- collisions:0 txqueuelen:0
- RX bytes:382314 (382.3 KB) TX bytes:382314 (382.3 KB)
-

To know about the addresses of your machine

- **mwazid@mwazid:~$ ifconfig**
-
- wlan0 Link encap:Ethernet HWaddr 24:fd:52:9e:b5:b9
- inet addr:192.168.43.252 Bcast:192.168.43.255 Mask:255.255.255.0
- inet6 addr: 2402:8100:2063:314a:26fd:52ff:fe9e:b5b9/64 Scope:Global
- inet6 addr: fe80::26fd:52ff:fe9e:b5b9/64 Scope:Link
- inet6 addr: 2402:8100:2063:314a:a443:154a:de2:c5d0/64 Scope:Global
- UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
- RX packets:38214 errors:0 dropped:0 overruns:0 frame:0
- TX packets:30393 errors:0 dropped:0 overruns:0 carrier:0
- collisions:0 txqueuelen:1000
- RX bytes:44333600 (44.3 MB) TX bytes:3874177 (3.8 MB)

ping

- Use ping to check your connection to a servers

Example: mwazid@mwazid:~$ ping google.com

Output:

- PING google.com (172.217.166.174) 56(84) bytes of data.
- 64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=1 ttl=53 time=119 ms
- 64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=2 ttl=53 time=118 ms
- 64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=3 ttl=53 time=236 ms

- **Create a new user account.**
- Create a new user account using the adduser command.

Example: mwazid@mwazid:~$ adduser john

Adduser: Only root may add a user or group to the system

- **mwazid@mwazid:~$ sudo**

- usage: sudo -h | -K | -k | -V
- usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
- usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
- [command]
- usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
- prompt] [-u user] [VAR=value] [-i|-s] [<command>]
- usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
- prompt] [-u user] file ...

- **mwazid@mwazid:~$ sudo su**
- **[sudo] password for mwazid:**
- **root@mwazid:/home/mwazid# adduser john**
- Adding user `john' ...
- Adding new group `john' (1001) ...
- Adding new user `john' (1001) with group `john' ...
- Creating home directory `/home/john' ...
- Copying files from `/etc/skel' ...
- Enter new UNIX password:
- Retype new UNIX password:
- passwd: password updated successfully
- Changing the user information for john
- Enter the new value, or press ENTER for the default
- Full Name []: john j
- Room Number []: 12
- Work Phone []: 0120687655
- Home Phone []: 0120889966
- Other []: 0120123456
- Is the information correct? [Y/n] y

Add the new user to the sudo group

- By default on Ubuntu systems, members of the group sudo are granted with sudo access.
- To add the user you created to the sudo group use the usermod command:

Example: usermod -aG sudo username

Test the sudo access

- Switch to the newly created user:

su - username

For example:

root@mwazid:/home/mwazid# usermod -aG sudo john

root@mwazid:/home/mwazid# su - john

john@mwazid:~$

- Use the sudo command to run the whoami command:

sudo whoami

- Is the user have sudo access then the output of the whoami command will be root:

Example: john@mwazid:~$ sudo whoami

Output:

[sudo] password for john:

root

grep

- grep filter searches a file for a particular pattern of characters, and displays all lines that contain that pattern.
- The pattern that is searched in the file is referred to as the regular expression.
- **1. Case insensitive search:** The -i option enables to search for a string case insensitively in the given file.

Output:

- mwazid@mwazid:~/waz$ grep -i “Wazid” waz.txt
- hello, my name is wazid

- **Displaying the count of number of matches :**
- We can find the number of lines **(count)** that matches the given string/pattern

Example: mwazid@mwazid:~/waz$ grep -c "wazid" waz.txt

Output:

1

- **Checking for the whole words in a file:**
- By default grep matches the given string/pattern (line) even if it found as a substring in a file.
- The -w option to grep makes it match only the whole words.

Example: mwazid@mwazid:~/waz$ grep -w "wazid" waz.txt

Output: hello, my name is wazid

- **Displaying only the matched pattern:**
- We can make the grep to display only the matched string by using the -o option.

Example: mwazid@mwazid:~/waz$ grep -o "wazid" waz.txt

Output: wazid

- **Starting and stopping services**

systemctl usage

- The stopping|starting|restarting of services on Linux is now quite simple.
- Suppose we want to stop the Apache server on linux.
- To do this we’d open up a terminal window and issue the command:

sudo systemctl stop httpd

- The Apache server would stop and you'd be returned to the bash prompt. To start the same service:

sudo systemctl start httpd

- The service would start and you’d be returned to your bash prompt. To restart the same service:

sudo systemctl restart httpd

- **service usage**
- service command still works -even for those distributions that have migrated to systemd and systemctl.
- **sudo service httpd start**
- **sudo service httpd stop**
- **sudo service httpd restart**
- To check the status of a service
- Here we are requesting the current status of the ‘sshd’ daemon

[root@linux etc]# service sshd status

End of lectures

References

- 1. The Linux Command Line: A Complete Introduction Book by William E. Shotts Jr. and William E. Shotts, Jr.
- 2. The Linux Programming Interface Book by Michael Kerrisk