**Linux Learning**

**FILE SYSTEM HIRARCHY**

/ represent root 🡪 equal to C drive in Windows

/etc contain system and any application configuration

/var contain log file and database files

/run contain process for running OS

/home contain each user directory

/bin contain binary files

/sbin contain system binary

/usr contain installed application and shared libraries

/tmp contain temporary files

/dev contain hardware

/boot contain kernel and boot file for OS

**LAB CREATION**

We will create a lab by installing Ubuntu 18.0 in VirtualBox using Vagrant

LISTING FILES AND DIRECTORIES

1. We are using **ls** command to show files and directories
2. **ls -a** this command will show hidden directories
3. **ls -l** this command will show detail information about files & directories
4. **ls -h** this command will show detail info about files & directories & size in MB
5. **ls -t** this command will show detail info about files & directories in ascd order
6. **ls -r** this command will show detail info about files & directories in reverse order

CD , PWD

HOW TO CREATE DIRECTRIES IN LINUX

1. use mkdir directory\_name1 directory\_name2

above command is used to create directory

1. use mkdir -p dir1/dir2/dir3

above command will create dir2 inside dir2 inside dir1

HOW TO CREATE FILES IN LINUX

1. use touch file1 file2 file2

above touch command is used to create file in linux

HOW TO DELETE FILES & DIRECTORIES

1. use rm and rmdir to delete files and directories
2. rmdir dir1

rmdir will delete dir1 directory. rmdir will delete empty directory only

1. rm command is used to delete both files and directories with contents

rm file\_name

rm -rfv directory\_name

above command will delete directory without asking yes and show summary as well

HOW TO COPY FILES & DIRECTORIES

1. use cp command to copy files and directories
2. cp source destination this command is used to copy files
3. cp -r source destination this command is used to copy directories

HOW TO COPY FILES / DIRECTORY TO / FROM REMOTE SERVER

scp command is used to copy files to and from server

1. dd if=/dev/zero of=file1.txt bs=1 count=0 seek=1G

above command will create a file of 1GB size

1. scp file1.txt root@ip\_address\_server:/home/root

above command will copy file1.txt file from local server to remote server

1. scp root@ip\_address\_server:/home/root/file1.zip /local\_user/home

above command will copy file1.zip from remote server to local system

1. scp -r /local\_directory\_path root@ip\_address\_server:/root

above command will copy directory from local system to remote server

1. scp -r root@ip\_address\_server:/root/downloads /local\_system/directory

above command will copy directory from remote server to local system

HOW TO USE SFTP IN LINUX

SFTP is same like SCP command

1. sftp roo@ip\_address\_server

above command will used to connect to remote server

1. if we enter pwd command after connect to server using sftp will give remote directory location
2. if we enter lpwd command after connect to server using sftp will give local directory location
3. entering l letter before any command, then command is executed for local system otherwise will execute for remote server
4. put file1.txt

above command will transfer file1.txt to remote server

1. mget file1.txt

above command will transfer file1.txt to local system from remote server

HOW TO MOVE FILES & DIRECTORIES

1. use mv command to move files and directories
2. mv source destination this command is used to move files
3. mv -rvf source destination this command is used to move directories

HOW TO RENAME FILES & DIRECTORIES

1. use mv command to rename files and directories as well
2. mv existing\_file\_name new\_file\_name this command is used to rename files & directories

HOW TO PRINT FILE CONTENT ON SCREEN

1. use cat command to print content on screen
2. cat file\_name
3. cat > file\_name.txt

above command will create a file and allow to enter some text in it

1. cat file\_name1 > file\_name2.txt

above command will copy file1 in to file2

HOW TO PRINT FILE CONTENT ON SCREEN

1. use less command to print content on screen like cat command but file open its self
2. less file\_name

HOW TO CREATE ARCHIVE / ZIP DIRECTORIES LINUX

1. use tar command to archive / zip the files and directories
2. tar -rvf backup\_file.tar source\_directory\_or\_files

above command will archive the directory

1. tar -xvf backup\_file.tar

above command will unzip the file

1. tar -tvf backup\_file.tar

above command will show files inside zip file

1. tar -rvf backup\_file.tar another\_file\_name

above command will add another file in zip file

1. gzip file\_name

above command will convert file in compressed file

1. gzip -d file\_name or gunzip file\_name

above both command will uncompress the files

1. bzip2. File\_name

above command is also used to compress files

bunzip2 file\_name command is used to unzip files

HOW TO CREATE SOFT LINK / HARD LINK (SHORTCUTS ) IN LINUX

1. ln -s path\_of\_file destination\_location\_short\_cut

above command will create shortcut on desktop for a file

above same command is used to create directory shortcut as well

1. unlink shortcut\_link\_name

above command will remove the linking

1. ls path\_of\_file destination\_location\_short\_cut

above command will create hard link

hard link create copy of file and make connection between both file

we can not create directory hard link

HOW TO CREATE USER AND GROUP IN LINUX

1. useradd user\_name
2. adduser user\_name

both above command is to create user in linux

1. to check all user vi /etc/passwd
2. passwd user\_name

above command to allow us to reset the username password

1. vi /etc/login\_defs

using above file we can setup min , max number of days

1. userdel -r user\_name

above command will delete user with user home directory as well

1. chage -l user\_name

above command will show change in user\_name

1. check chage command help
2. chage -l user\_name

above command is used to modify user properties

1. vi /etc/group

above command will show all groups in system

1. groupadd group\_name
2. id username

above command will give user related info

1. usermod -aG group\_name username

above command is used to add user to a group

HOW TO SETUP PERMISSIONS IN LINUX

1. permission in linux consist on 10 bits
   1. first bit represent file or directory
   2. then next three bits represent user permission
   3. then next three bits represent group permission
   4. then next three bits represent everyone permission
2. one bit can have value
   1. r read 4
   2. w write 2
   3. x execute 1
3. chmod 646 file\_name

above command will set or change permission on file

1. chown -R username file\_name

above command will change the file owner

1. chown -R :group\_name file\_name

above command will change group of file\_name

VI EDITIOR IN LINUX

1. type vi
2. press arrow keys will move cursor
3. press w key will move cursor forward by one word
4. press b key will move cursor backward by one word
5. press 0 key will move cursor to beginning of line
6. press cmd+ key will move cursor by end of line
7. press shift+L key will move cursor down by page by some paragaph
8. press shift+h key will move cursor Up by page by some paragaph
9. press Ctrl+f key will move cursor down by page
10. press ctrl+b key will move cursor Up by page
11. press capital G key will move cursor to end of file
12. press small g key will move cursor to begining of file
13. press capital 5G key will move cursor to 5th line of file
14. press O key will insert line
15. press :q key will quit file without save
16. press :wq key will save file
17. press :q! key will quit file without save by force
18. press x key will delete one character at a time from cursor position
19. press 6x key will delete six characters at a time from cursor position include spaces
20. press dw key will delete one word at a time from cursor position
21. press d0 key will delete complete line from cursor to line beginning
22. press shift d+$ key will delete complete line from cursor to line end
23. press dd key twice will delete complete line
24. press 3dd key twice will delete complete 3 lines
25. press cc key twice will delete complete line and put in insert mode
26. press shift+R will put in replace mode
27. press shift s key will delete complete line and put in insert mode
28. press yy key twice will copy complete line
29. press shift+p or only p key will paste the copy content complete line
30. press / and then type word to search (downword )
31. press ? and then type word to search (upword)
32. press n to search next occurrence of work

STRING PROCESSING IN LINUX

1. head command is used to display first ten lines
2. tail command is used to display last ten lines
3. wc command is used to display no of word in file
4. sort command is used to display info in sorted order

SEARCHING / FINDING IN LINUX

1. grep command is used for searching in file

grep bash /etc/passwd

above command will search bash in passwd file

we can enter any search cretira using regular expression

1. awk command is also used for searching as well
2. sed is command is also used to display file content like cat or less command
3. we are using locate command to find string in linux

locate -i message

above command will search all files & directories contain word messages

locate \*example\*

above command will search example but case sensitive

1. find command is also used for searching in linux

find /home -name “example.txt”

above command search for example.txt file in home directory

find /home -name -empty

above command search for empty file in home directory

find . -type f -exec ls -s {} \; | sort -n -r | head -5

above command will find largest 5 file in current directory

-type f 0r d

-size. +1MB

-name

NETWORK CONFIGURATION IN LINU,X

1. open /etc/sysconfig/network-scripts location in centoos

PROCESS MANAGEMENT IN LINUX

Process is instance of program running in linux

1. ps -aux command will give all te
2. kill process\_id

above command is used to kill the process

1. top command is also used to list all running process
2. pkill -u username or pkill process\_name is also used to kill process
3. bg process\_id and fg process\_id are used to bring process in backgroup or front
4. vmstate -a command is used to system & disk statistic
5. iostate command also give system & disk statistic like vmstate
6. lsof stand for list open file

above command will list all open file and processes

SERVICES MANAGER / SYSTEMD IN LINUX

Systemd is new services manager in Linux

1. systemctl is the basic commad for system
2. systemctl status httpd.service -l

above command will show the status of apache services

1. systemctl command\_name services\_name
2. command\_name can have values

status

is\_active

is\_enable

start

stop

restart

enable /disable

Making Partition and Mounting to Directory

1. CREATING PARTION USING FDISK
   1. Run fdisk -l command to see all the partition
   2. This will show /dev/sd(partition\_number)

Like /dev/sda , /dev/sdb / /dev/sdbc ( three disk a , b , c attached to VM)

Harddisk are represented with SDA , SDB & SDC lable

Partition in Harddisk are represented with SDA1, SDA2 labels

* 1. fdisk /dev/sdc and press enter, we are create a partition in harddisk no. 3
  2. type n for new partition 🡪 type p for primary 🡪 type 2 for partition no. 🡪 Enter for first sector default value 🡪 Enter partition size (+2G) 🡪 type w to save

1. CREATING FILE SYSTEM ON NEWLY CREATED PARTITION
   1. mkfs.ext4 /dev/sdc1
2. MOUNT PARTITION TO DIRECTORY
   1. Create a directory using mkdir directory name
   2. Now mount partition to directory using below command

mount /dev/sdc1 /partition1

* 1. Type df -h to display mounted directories
  2. To make the mounting parmenent, open file fstab file located in etc directory

vim /etc/fstab and enter following record

/dev/sdc1 /partition1 ext4 default

Save file and exit

* 1. Run command mount -a

CREATING SWAP PARTITION

1. Run the free -m command to see memory information
2. Now create a partition like above instruction but change the type to Linux swap using l option
3. Save and exit
4. Now format / or create file system using below command

mkswap /dev/sdc3

1. Now edit /etc/fstab and enter the partition information to make it permanent
2. Now run the below command to enable swap partition

swapon -v /dev/sdc3

1. swapon -s to show all the swap partition in system
2. to remove the swap partition using below command

swapoff /dev/sdc3

CREATING SWAP USING FILE

1. enter below command to create swap using file

dd if=/dev/zero of=/swap1G bs=1024 count=1048576

above command will create a file with name swap1G at / level of 1GB size

1. enable swap on above file using below command

mkswap /swap1G

swapon -v /swap1G

1. edit the /etc/fstab file to make it permanent

LOGICAL DISK MANAGEMENT

Using LVM we can join two partition from two different hard disk in to one logical

volume

Step No. 1 create partition on first hard disk

1. run the command parted -l

above command will give information about harddisk and partitions

1. parted /dev/sdd 🡪 mklabel msdos 🡪 q

above command will give label to hard disk no. 3

1. to create partion in hard disk issue parted /dev/sdd 🡪 p

mkpart primary start finish press enter

1. set partition\_number lvm on

Step No. 2 create partition on second hard disk

Same step as above

Step No. 3 create physical volume partition

1. pvcreate /dev/first\_partition /dev/second\_partition and press enter
2. pvdisplay command will physical volume partition

Step No. 4 create volume group and add these partition in it

1. vgcreate vol\_group\_name /dev/partition\_1 /dev/partition\_2
2. vgdispaly

Step No. 5 create logical volume inside logical Volume Group

1. lvcreate -L 8GB -n logical\_vol\_name vol\_group\_name
2. lvdisplay

Step No. 6 format the logical volume create at step 5

1. mke2fs -t ext4 -j /dev/volume\_group/logical\_volume
2. get path from fdisk command

Step No. 7

1. mount the logical volume to directory
2. mount /dev/volume\_group/logical\_volume /directory\_name
3. add information /etc/fstab
4. mount -a

Step No. 8 Extending the Logical Volume Group by adding new partition

1. create new partition by step no. 1
2. convert newly created partition in physical partition by below command

pvcreate /dev/partition\_name

1. vgextend logical\_volume\_group\_name /dev/new\_partition\_name
2. now we can increase the logical volume by following command

lvresize -L new\_size /dev/logical\_volume\_group/logical\_volume\_name

1. resize2fs /dev/logical\_volume\_group/logical\_volume\_name new\_size
2. df -h

Step No. 8 to rename the logical volume

1. lvrename name\_of\_volume\_group name\_of\_logical\_volume new\_name\_of\_logical\_volume
2. unmount the logical\_volume then change in /etc/fstab and mount again

Step No. 9 to rename volume\_group\_name

1. vgrename name\_of\_volume\_group. New\_name\_of\_volume\_group
2. unmount the directory firstv
3. update /etc/fstab as well accordingly

CREATING SOFTWARE RAID

WE ARE CREATING RAID 0, FOR THIS WE NEED TWO HARD DISKS

Step No. 1 Enter below command to create RAID zero

1. mdadm --create /dev/md0 –level=0 --raid-devices=2 /dev/harddisk1

/dev/harddisk2 and press enter

1. mke2fs -t ext4 -j /dev/md0

above command will format the newly created RAID 0

1. now we can mount the RAID 0 to Directory
2. add to /etc/fstab to make it parament

WE ARE CREATING RAID 1, FOR THIS WE NEED TWO HARD DISKS

Enter below command to create RAID ONE (Mirror)

1. mdadm --create /dev/md1 –level=1 --raid-devices=2 /dev/harddisk1

/dev/harddisk2 and press enter

1. mke2fs -t ext4 -j /dev/md1

above command will format the newly created RAID 1

1. now we can mount the RAID 0 to Directory
2. add to /etc/fstab to make it parament

WE ARE CREATING RAID 1, FOR THIS WE NEED THREE OR MORE HARD DISKS

Enter below command to create RAID FIVE

1. mdadm --create /dev/md5 –level=5 --raid-devices=3 /dev/harddisk1

/dev/harddisk2 /dev/harddisk3 and press enter

1. mke2fs -t ext4 -j /dev/md5

above command will format the newly created RAID 5

1. now we can mount the RAID 0 to Directory
2. add to /etc/fstab to make it parament
3. mdadm –detail /dev/md5

above command will give detail of RAID 5

1. mdadm --detail –scan

above command will show all array configured on system

1. mdadm --detail –scan >> /etc/mdadm.conf

above command will save RAID configuration and will not lost if system reboot

DEGRADING A Harddisk in array, removing the hard disk and add another hard disk

1. mdadm /dev/md1 -f /dev/partition\_number
2. mdadm --detail
3. mdadm /dev/md1 -r /dev/partition\_number
4. mdadm --manage /dev/md1 --add /dev/new\_partition\_number
5. mdadm --grow /dev/md1 --raid-device=3 --add /dev/new\_partition

above command will add additional partition to array

SSH SETUP & CONFIGURATION IN LINUX

SSH is used to connect to remote server securely

1. to check ssh is install or not run below command

ssh -V

1. to install ssh run below command

apt-get install openssh-server openssh-client

1. ssh root@ip\_address\_server or ssh -p port\_num root@ip\_address\_server

ssh root@ip\_address\_server “cd /home/directory ; bash “

above command is used to connect to server using root

SECURING SHELL

HOW TO CHANGE DEFAULT PORT OF SHELL AND RESTRICT ROOT ACCESS

1. open vim /etc/ssh/sshd\_config
2. look for port and change from 22 to any i.e. 3212
3. uncomment rootpermision login and set to no
4. save file
5. /etc/init.d/sshd restart
6. Above command will restart shell services
7. Open vi /etc/sysconfig/iptables

Change the ssh port from 22 to 3212 and save

1. Restart iptables services
2. Now try to connect ssh using new port

SECURING SHELL USING PUBLIC AND PRIVATE KEYS

1. Generated private and public key using below command first

ssh-keygen -t rsa and press enter

1. Above command will show the path of both files
2. cd /home/login\_user/.ssh
3. cp id\_rsa.pub authorized\_keys
4. cat id\_rsa and copy the content and paste in notepad file and give any name with ppk (private.ppk)
5. download putty gen to convert private key
6. open file 🡪 load private key 🡪 select key 🡪 enter pass prash 🡪 save key with name id\_rsa.ppk
7. open putty 🡪 enter IP 🡪 port 🡪 click ssh 🡪 auth 🡪 browse 🡪 select id\_rsa 🡪 click session 🡪 save 🡪 click contact 🡪 enter pass pharse 🡪

SECURING SHELL ACCESS FROM SPECIFIC IP ADDRESS OR DENY IP ADDRESS

1. open vi /etc/ssh/sshd\_config file
2. at end of file enter below line

AllowUsers. [\*@192.168.1.15](mailto:*@192.168.1.15) user@192.168.1.\*

Above command will only allow connection from IP 192.168.1.15

But user with any IP address allow to connect

1. open /etc/host.config and add following line

sshd : 192.168.1.15 : allow

sshd : ALL : deny

above command will allow IP and deny other IP, SSHD is a service name.

INSTALLING AND CONFIGURING ANTIVIRUS CLAMAV LINUX

1. apt-get install clamav clamd

above command will clamav antivirus

1. to update the database run the below command

freshclam

if you got error, restart the service clamav-freshclam

then r un the command

1. clamscan -ir /home

above command will scan home directory, i parameter will show infacted file

1. clamscan -riI /home /clamav.log

above command scan home directory and log in /clamav.log file

1. clamscan –remove /home

above command will remove infected files

INSTALLING AND CONFIGURING LINUX MALWARE DEDECT IN LINUX

1. download from follow location
2. wget <http://www.rfxn.com/downloads/maldetect-current-tar.gz>
3. tar -zxvf maldetect-current.tar.gz
4. cd maldetect-1.4.2 🡪 sh install.sh
5. check installation path cand configuration file
6. now edit the configuration file
7. look for email alert, change to 1 from zero, next chack quar\_hits = 1 , next check for email\_addr and give emailaddress option , save it
8. install perl using command apt-get install perl
9. maldet -a /home

above command will scan the home directory

1o. maldet --report

INSTALLING LINUX FIREWALL OR IPTABLE

Linux firewall is refer as IPTable

1. iptables -V / iptables --version

above command will give iptables information

1. iptables -L

above command will give information

1. iptables –line-numbers -n -L

above command will shows all rules

1. vi /etc/systconfig/iptables

deny IP to access shell using iptables

1. iptables -I INPUT 4 -s 192.168.1.9 -p tcp --dport 22 -j DROP

above command will drop

1. service iptables save

above command will save the above command in configuration file

how to delete rule from iptables

1. iptables -D INPUT 4

above command delete the rule from iptables

how to backup iptables and restore if we want

1. go to iptables location first
2. cp iptables iptables.backup

above command will create copy of iptables, which we can restore later

1. iptables-restore < /etc/sysconfig/iptables-backup

above command will restore the backup

How to block IP using iptables

1. iptables -A INPUT -s 192.168.13.17 -j DROP

above command will block the mention IP

How to block outgoing traffic / or block a website [www.facebook.com](http://www.facebook.com)

1. first find the ip of facebook.com
2. ping [www.facebook.com](http://www.facebook.com)
3. which will give 31.13.86.49
4. iptables -A OUTPUT -p tcp -d 31.13.86.49 -j DROP

above command will block facebook.com

1. iptables -A OUTPUT -p tcp -d www.facebook.com -j DROP
2. iptables -A OUTPUT -p tcp -d facebook.com -j DROP

INSTALLING AND CONFIGURING LINUX FIREWALL D

1. Install firewall d using apt-get install firewalld
2. First enable firewall using command firewall enable
3. systemctl start firewalld
4. systemctl enable firewalld
5. firewalld-cmd --get-zones

above command will show all zone

1. firewalld-cmd --get-default-zones

above command will show default zone

1. firewalld-cmd –help
2. firewalld-cmd –list-all

above command will show all active zone and services for that zone

1. firewalld-cmd –list-all --zone=home

how to add IP as trusted IP in firewall

1. firewalld-cmd --zone=home –add-source=192.168.13.0/24 --permanent
2. firewalld-cmd --relaod
3. firewalld-cmd --zone=home –add-port=21/tcp --permanent
4. firewalld-cmd --zone=home --remove-port=21/tcp --permanent
5. firewalld-cmd --set-default-zone=home

above command will change default zone from publich to home

CORN JOBS IN LINUX

Corn is used to run schedule jobs in Linux

1. we are adding all corn jobs in file, to add corn job run below command
2. crontab -e
3. crontab has six fields

1st Field 2nd Field 3rd Field 4th Field 5th Field 6th Field

Minutes Hours day of month month day of week command

1-60 1-24 1-31 1-12 1-6 command

**10 19 \* \* \* rm -rvf /tmp/\***

**@reboot command (this will run command at reboot)**

**@yearly command**

**@monthly command**

**@daily command**

**@hourly command**

Above job will run on 07:10 pm daily and remove all tmp content

1. after entering the record and restart the corn job service
2. service cornd restart
3. all corn job results are store in file
4. vi /var/spool/mail/root

corn job will save result in above file

1. 10 19 \* \* \* rm -rvf /tmp/\* MAILTO=”rizwan.khan@magrudy.com”
2. Above command will send report to email id
3. corn -l

above command will show all corn jobs

1. crontab -r

above command will delete all corn jobs

1. /etc/cron.daily/

If we create any cron job in above directory, will run daily