LINUX CIS 37.1 By Ruban LABS

26 October 2024 12:06

LINUX

To Show All the Processes

```
pstree
```

Get Process Id

```
Pidof processname

Pgrep processname
```

User Management

```
useradd <your_user_name>

tail -1 /etc/passwd

usermod -c "Your_Comment" <your_user_name>
```

Logonname- Spiderman
Uid- 5000
Shell /bin/sh
Comment-"Peter Parker"

```
useradd -u 5000 -s /bin/sh -c "Peter Parker" spiderman
```

Delete A User

```
userdel -r <your_user_name>
```

Creating A Sudo User

Switch to another user
```
su - <your_user_name>
sudo useradd <your_sudo_user_name>
```

Switch to the root user
```
visudo
```
go to 101 line
```
<sudo_user_name> TABSPACE  ALL=(ALL) TABSPACE ALL
```

Add user with your last name

And provide "STORAGE" admin access to this user
Make user equivalent to root user
Make user storage admin
Add custom root level commands for user

Create a sudo user
Open visudo
Add username ALL=(ALL) STORAGE,NETWORK
Uncomment Storage and network
Go to that user
sudo -l

To bypass password use NOPASSWD:

ADD CUSTOM PERMISSIONS COMMANDS

visudo
username ALL=(ALL) NOPASSWD: CUSTOMCMDS <- This will be any name

Go to upper bellow networking

```
##########################################
######THIS IS MY CUSTOM COMMANDS########
```

cmnd_Alias CUSTOMCMDS = /usr/sbin/useradd [in terminal use this cmd to get this path which cmdname]

Now go to the terminal
Switch to the user
sudo -l

Groups In Linux

ADDING GROUP : groupadd <your_group_name>
SEE YOUR GROUP: getent group <your_group_name>
cat /etc/group | grep <your_group_name>

Add group member

usermod -G <your_group_name> username
CHECK
cat /etc/group | grep <your_group_name>

Add custom command to group user

```
visudo
%yourgroupname ALL=(ALL) NOPASSWD:CUSTOMCMDS<- This will be any name
```

Disable the storage line by uncommenting all

Permissions

Create a new directory "/LTIMindtree" and give Read-Write access to group LTIB372 only. Access this folder with a new user (not part of LTIB372 group) with your last name and ensure you get permission denied while accessing it.

```
touch /salary.txt
ls -l /salary.txt
groupadd governance
useradd -G governance u1
useradd -G governance u2
useradd u3
chgrp gov /salary.txt
chmod 660 /salary.txt
```

Access Control List(ACL)

```
getfacl /salary.txt
groupadd hr;
useradd -G hr hr1
useradd -G hr hr2
setfacl -m g:hr:r-- /salary.txt
Getfacl /salary.txt
```

Package Management(RPM)

Add your offlinepackages.iso files
Media->dvd drive->insertdisc->offlinepackages.iso

```
df -h
cd /run/media/root/<package_date>
ls
ls | wc -l
rpm -qa package_name   <- Querrying a package
rpm -ivh <full_package_name>.rpm <- Installing a package
rpm -uvh <full_package_name>.rpm<- updating a package
rpm -e <full_package_name>.rpm<- uninstalling a package
```

Installing A Package With No Dependencies

```
rpm -ivh --nodeps <full_package_name>.rpm
```

Foreground Process

```
firefox
```

Background Process

```
firefox &
```

Configuring LVM(Logical Volume Management)

```
lsblk
```

Add the virtual hard discs of 5 GB of 2

```
fdisk /dev/sda<-your vhd
```

Select n
Primary
Press enter
Press enter
Press enter
Press t
Choose 8e
Choose w

```
pvcreate /dev/sda1 /dev/sdb1
vgcreate <add_vol_group_name> /dev/sda1 /dev/sdb1
vgdisplay
vgs
lvcreate -n <add_lvm_name> -l 100%FREE <your_vol_group_name>
lvdisplay
```

Create a filesystem

mkfs. [2 tabs]
Go with XFS

```
mkfs.xfs /dev/<your_vol_group_name>/<your_lvm_name>
```

Mount Temporary

```
mkdir /lvm
mount /dev/<your_vol_group_name>/<your_lvm_name> /lvm
df -hT
```

Mount Permanently

```
cp /etc/fstab /fstab_backup
vim /etc/fstab
```

In that fstab file do this

```
/dev/<your_vol_group_name>/<your_lvm_name> /lvm xfs defaults 0 0
mount -a
systemctl daemon-reload
df -h
```

Configuring FTP Server(File Transfer Protocol)

```
rpm -qa | grep ftp
rpm -qa | grep vsftpd
```

If ftp is not installed install it

```
cp /etc/vsftpd/vsftpd.conf /root/vsftpd.conf-backup
vim /etc/vsftpd/vsftpf.conf
```

In that file make sure anonymus_enable=NO

```
ftpd_banner = Write Some Text Here
```

In the last 2 lines

```
userlist_file=/etc/vsftpd/userlist
userlist_deny=NO
```

```
su - <your_user_name>
```

Create a text file in it

```
cat > /etc/vsftpd/userlist
systemctl stop firewalld; systemctl status firewalld
systemctl enable vsftpd; systemctl start vsftpd; systemctl status vsftpd
```

```
nmcli networking off && nmcli networking on
```

```
ifconfig | grep inet
```

```
systemctl start firewalld
systemctl status firewalld
ftp 192.168.10.10
```

Type your username and it should be added in userlist

Write password

```
ls
```

Download that readme file

```
get Readme.txt
put Readme.txt
```

```
ls -l
```

Configuring NFS SERVER

```
rpm -qa | grep nfs
rpm -qa | grep rpcbind
```

Nfs Shared Folder

```
mkdir /nfsserver
touch /nfsserver /t{1..10}.txt
ls /nfsserver /
```

```
getenforce
```

```
vim /etc/selinux/config
```

Go to line 22 and make it disabled

Save it

Reboot

Edit the config file

```
vim /etc/exports
```

In that file

```
/nfsserver <tabspace> *(no_root_squash,rw,sync)
```

Save it

```
systemctl enable nfs-server rpcbind
systemctl start nfs-server rpcbind
systemctl status nfs-server rpcbind
```

```
exportfs
```

Go to client

Make sure your selinux is disabled

Disable firewall both client and server

```
systemctl  stop firewalld; systemctl disable firewalld
```

Check for nfs and rpcbind package

```
systemctl enable nfs-server rpcbind;
systemctl start nfs-server rpcbind;
systemctl status nfs-server rpcbind;


showmount -e 192.168.10.10;

mkdir /nfsclient
mount 192.168.10.10:/nfsserver /nfsclient

df -h

ls /nfsclient
```

Apache WEB SERVER

```
updatedb
locate httpd.conf

cd /var/www/html/
vim index.html
Write some html code
systemctl enable httpd; systemctl start httpd; systemctl status httpd
Open firefox
Type in url localhost
Pwd
cd ..
ls
mkdir www.ruban.in

ls
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf_backup
cp html/index.html www.ruban.in/
cd www.ruban.in
vim index.html
Change the code
Save and quit

cd /var/www/www.ruban.in
ls
vim /etc/httpd/conf/httpd.conf
Go to line 47
Listen 80
In the last line add this
<VirtualHost 192.168.10.10:80>
	DocumentRoot /var/www/www.ruban.in
	ServerName www.ruban.in
</VirtualHost>

Save and quit
```

```
vim /etc/hosts
```

Add this line

```
192.168.10.10 www.ruban.in
```

```
ping www.ruban.in
```

```
systemctl enable httpd; systemctl start httpd; systemctl status httpd
```

```
firefox &
```

www.ruban.in

See the magic!!

Linux Bind (DNS)

```
ip a
```

```
cat /etc/resolv.conf
```

```
nmtui
```

Set the host name

server.ruban.in

```
getenforce
```

```
systemctl stop firewalld
```

```
rpm -qa | grep bind
```

```
cp /etc/named.conf /etc/named.conf-backup
vim /etc/named.conf
```

Go to line 11

After ';' add one space and another space in the middle write this

```
53 { 127.0.0.1; 192.168.10.10; };
```

Go to line 20

```
{ localhost; any; }
systemctl enable named; systemctl start named; systemctl status named;
vim /etc/named.conf
```

Go to line 56

Press o

```
zone "ruban.in" IN{
type master;
file "forward.ruban.in";
allow-update {none;};
};

zone "10.168.192.in-adda-arpa" IN {
type master;
file "reverse.ruban.in";
allow-update {none;};
};
```

Save & exit

```
cd /var/named
ls
cp named.localhost forward.ruban.in
vim forward.ruban.in
```

In line 2

```
IN SOA @ server.ruban.in. (
```

```
Go to line 8 and press dd
                 9  and press dd
                10 and press dd
press o
```

```
@ <tab> IN <tab> NS <tab> server.ruban.in.
@ <tab> IN <tab> A   <tab>  192.168.10.10
server <tab> IN <tab> A <tab> 192.168.10.10
client <tab> IN <tab> A <tab> 192.168.10.11
```

```
cp forward.ruban.in reverse.ruban.in
vim reverse.ruban.in
```

GO to line 8 and press o

```
@ tab IN tab PTR tab ruban.in.
```

Go to line 13

```
10 tab IN tab PTR tab server.ruban.in
11 tab IN tab PTR tab client.ruban.in
```

Save & exit

```
ls -l *.ruban.in
chown root:named *.ruban.in
named-checkconf -z /etc/named.conf
named-checkzone forward forward.ruban.in
named-checkzone reverse reverse.ruban.in
systemctl restart named; systemctl status named
```

Go to client

ip a
hostname (set the hostname)
cat /etc/resolv.conf
ping 192.168.10.10
dig ruban.in
nslookup ruban.in
ping server

Linux Mail Server

vim /var/named/forward.ruban.in
Go to line 8
Press shift + o
server tab IN tab MX tab 10 tab server.ruban.in
systemctl restart named; systemctl status enabled
cp /etc/postfix/main.cf /etc/postfix/main.cf-backup
vim /etc/postfix/main.cf
Go to line 94
server.ruban.in (addit in myhostname)
Go to line 102
Mydomain=ruban.in
Go to line 117 and uncomment it
Go to line 132 uncomment
Comment 135
Go line 183
In my destinition add this
, $mydomain
Go to line 284 and add
192.168.10.10/24, 127.0.0.0/8
Go to 438 line
home_mailbox= Mailbox
systemctl enable postfix
systemctl start postfix
systemctl status postfix
rpm -qa | grep telnet
If not installed installed both
systemctl enable telnet.socket;systemctl start telnet.socket;
systemctl status telnet.socket
useradd username
Set password
Add another user
telnet localhost smtp
ehlo localhost
mail from: <soumita>
rcpt to: <sreema>
data
Write anything as mail

. Put that dot to close mail
Quit

```
cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf-backup
vim /etc/dovecot/dovecot/dovecot.conf
```

Go to line 24 and uncomment it
Save and quit

```
vim /etc/dovecot/conf.d/10-mail.conf
```

Uncomment 24
Save

```
vim /etc/dovecot/conf.d/10-auth.conf
```

Uncomment line 10
Line 100

```
auth_mechanisms=plain login
```

Save

```
vim /etc/dovecot/conf.d/10-master.conf
```

Go to line 102
Uncomment user and group
Assign postfix both of it

```
systemctl enable dovecot;systemctl start dovecot;systemctl status dovecot
telnet localhost pop3
user <reciever_user_name>
pass <password>
List
retr
```

SORRY IT WILL NOT WORK THANK YOU FOR YOUR UNDERSTANDING DO SUBSCRIBE MY CHANNEL