RHCE FINAL PAPER

IMP NOTES:
1)PLZ 1ST REBOOT YOUR SERVER ,THEN DESKTOP, IF U WANT TO DO SO
2)DO NOT USE ANY LAB(e.g. lab nfskrb5 setup) @ EXAM TIME.

1. Selinux should be in enforcing mode on your both systems.
Ans:]# getenforce
enforcing
IF NOT SO,THEN
]# vim /etc/selinux/config
SELINUX=enforcing
:wq!
]#reboot

---

*2. Configure yum client side repository using a following url:
http://classroom.example.com/content/rhel7.0/x86_64/dvd
(THIS IS NOT QUESTION BUT YOU NEED TO CONFIGURE YUM SERVER OTHERWISE NOT POSSIBLE TO SOLVE PAPER. USE GIVEN LINK)
Ans:]# yum repolist (TO CHECK)
]# cd /etc/yum.repos.d/
]#vim sangram.repo
[rhce_123]
gpgcheck = 0
enabled = 1
baseurl = http://classroom.example.com/content/rhel7.0/x86_64/dvd
name = sangram12
:wq!
]#yum repolist

---

2. Configure SSH access on your both syatems as follows.
a. Users should have SSH access on your systems from remotely.
b. Clients within my133t.org should not have SSH access on your systems.
Ans: (ON YOUR BOTH SYSTEM SSH SERVICE IS ALREADY ENABLED AND WE ARE USING IT,SO NO NEED TO CONFIGURE SSH)
]#systemctl status sshd.service(TO CHECK)
]#firewall-cmd --list-all(TO CHECK)
(YOU HAVE PROVIDED WITH ADDRESS OF my133t.org(192.168.12.23))
]#firewall-cmd --add-rich-rule 'rule family="ipv4" source address="192.168.12.23/24" service name="ssh" reject' --permanent
]#firewall-cmd --reload
(NO NEED TO REMEMBER ABOVE RULE. USE man page of firewalld.richlanguage. USE example no.3. MAKE CHANGES AS ABOVE.)
]#firewall-cmd --list-all (TO CHECK)
(APPLY ABOVE RULE ON YOUR BOTH SYSTEMS @ EXAM TIME)

---

3. Create a new customized envoirment for your users.
a. Create a new custom command called "userstat" whos output should be similar to "/bin/ps -Ao pid,tt,user,fname,rsz"
b. Make sure "userstat" command should available by-default for all users on both systems.

```
Ans: ]#vim /etc/bashrc
      AT END OF FILE
      alias userstat="/bin/ps -Ao pid,tt,user,fname,rsz"
       :wq!
     ]#logout
     ]#ssh root@serverX -X
     ]#userstat (TO CHECK)
     (MAKE ABOVE CHANGES ON BOTH SYSTEMS)
-------------------------------------------------------------------------
-------------------------------------------------
4.    Configure port forwarding on your server.
       a. The traffic coming from desktop on port 415/tcp should be
forwarded to port 22/tcp on your system1.
Ans:  ]# firewall-cmd --add-rich-rule 'rule family="ipv4" source
address="172.25.5.10" forward-port to-addr="172.25.5.11" to-
               port="22"protocol="tcp"  port="415"' --permanent
      ]# firewall-cmd --reload
      ]# firewall-cmd --list-all (TO CHECK)
DESKTOPX]# ssh -p 415 root@serverX (TO CHECK)
      (NO NEED TO REMEMBER ABOVE RULE. USE man page of
firewalld.richlanguage. USE example no.5. MAKE CHANGES AS ABOVE.)
-------------------------------------------------------------------------
-------------------------------------------------
5.    Configure a new network teaming link on both systems. (## use #lab
teambridge setup)
       a. Both systems has a network interfaces "eno1" and "eno2"
       b. These two interface should be Slaved for new teaming device
called "team1". (Make sure "team1" should remain active even if one of
the          interfaces goes down)
       c. Assign the given IP address for "team1" on 1st system -
192.168.XX.111
       d. Assign the given IP address for "team1" on 2nd system -
192.168.XX.222
Ans:  ]# lab teambridge setup (USE ONLY WHEN PRACTICING. IT WORKS ONLY ON
SERVER. BUT @ EXAM TIME U NEED TO CONFIGURE ON BOTH SYSTEMS.)
      ]# nmcli con add con-name sam ifname team1 type team config
'{"runner": {"name": "activebackup"}}'
      ]# nmcli con add con-name team-slave1 ifname eno1 type team-slave
master team1
      ]# nmcli con add con-name team-slave2 ifname eno2 type team-slave
master team1
      ]# nmcli con modify sam ipv4.addresses "192.168.X.111/24"
ipv4.method manual
      ]# teamdctl team1 state (TO CHECK)
      ]# systemctl restart network
      ]# ifconfig (TO CHECK)
-------------------------------------------------------------------------
-------------------------------------------------------------
6.    Configure the following IPV6 ip address for interface eth0 on your
both systems.
       a. IPV6 address for system1 - "fddb:fe2a:ab1e::c0a8:1/64"
       b. IPV6 address for system2 - "fddb:fe2a:ab1e::c0a8:fe/64"
Ans:    (FOR SYSTEM1)
      ]#  nmcli con modify "System eth0" ipv6.addresses
"fddb:fe2a:ab1e::c0a8:1/64" ipv6.method manual
      ]#  systemctl restart network
      ]#  ifconfig
      ------------------------------------------------
```

```
      ]#  nmcli con modify "System eth0" ipv6.addresses
"fddb:fe2a:ab1e::c0a8:fe/64" ipv6.method manual
      ]#  systemctl restart network
      ]#  ifconfig
-------------------------------------------------------------------------
-------------------------------------------------------------
7.    Implement a web server for the site http://serverX.example.com,
      then perform the following steps:
        - Download http://classroom.example.com/pub/server.html
        - Rename the downloaded file to index.html
        - Copy this index.html to the DocumentRoot of your web server
        - Do NOT make any modifications to the content of index.html
Ans:    (ON SERVERX SIDE)
     ]# yum groupinstall 'basic web server' -y
     ]# cd /var/www/html/
     ]# wget -O index.html http://classroom.example.com/pub/server.html
     ]# firewall-cmd --add-service=http --permanent
     ]# firewall-cmd --reload
     ]# firewall-cmd --list-all (TO CHECK IF HTTP SERVICE IS ADDED OR
NOT)
     ]# systemctl enable httpd.service
     ]# systemctl restart httpd.service
     ]# cd /etc/httpd/conf.d/
     ]# ll
     ]# vim exam.conf
        #1ST QUESTION-------------------------------------------
           <virtualhost *:80>
                 servername server5.example.com
                 documentroot /var/www/html
                 directoryindex index.html
           </virtualhost>
      #-----------------------------------------------------
        :wq!
     ]# systemctl restart httpd.service
     ]# firefox (TO CHECK: http://serverX.example.com)
-------------------------------------------------------------------------
-------------------------------------------------------------
8.   Extend your web server to include a virtual host for the site
     http://wwwX.example.com
     then perform the following steps:
           - where X would be replaced by domain number.
           - Set the DocumentRoot to /var/www/virtual
           - Download http://classroom.example.com/pub/www.html
           - Rename the downloaded file to index.html
           - Copy this index.html to the DocumentRoot of the virtual host
           - Do NOT make any modifications to the content of index.html
           - Ensure that harry is able to create content in
/var/www/virtual
Ans:  ]#  mkdir /var/www/virtual
      ]#  cd /var/www/virtual/
      ]#  wget -O index.html http://classroom.example.com/pub/www.html
      ]#  ll
      ]#  useradd harry
      ]#  setfacl -m u:harry:rwx /var/www/virtual/
      ]#  vim /etc/httpd/conf.d/exam.conf
     #8TH QUESTION-----------------------------------------------------
-----------
           <virtualhost *:80>
```

```
                servername www5.example.com
                documentroot /var/www/virtual
                directoryindex index.html
          </virtualhost>
     #-------------------------------------------------------------
     :wq!
     ]#  httpd -t (TO CHECK SYNTAX OF CONFIG FILE)
     ]#  systemctl restart httpd.service
     ]#  firefox (TO CHECK: http://wwwX.example.com)
-------------------------------------------------------------------------
-------------------------------------------------------------
9.   Secure web service.
     - Configure TLS encryption for the web server
"http://serverX.example.com"
     - A signed certificate for web server is available at
http://classroom.example.com/pub/tls/certs/serverX.crt
     - Required key for this certificate file is available at
http://classroom.example.com/pub/tls/private/serverX.key
     - The certificate for signing authority is provided at
http://classroom.example.com/pub/example-ca.crt
Ans:  ]#cd /etc/pki/tls/certs/
     ]#  wget http://classroom.example.com/pub/tls/certs/server5.crt
     ]#  wget http://classroom.example.com/pub/example-ca.crt
     ]#  cd ..
     ]#  cd private/
     ]#  wget http://classroom.example.com/pub/tls/private/server5.key
     ]#  cd /etc/httpd/conf.d/
     ]#  vim exam.conf
          #9TH QUESTION-----------------------------------------------
----
          <virtualhost *:443>
                servername server5.example.com
                documentroot /var/www/html
                directoryindex index.html
                SSLEngine on
                SSLProtocol all -SSLv2
                SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
                SSLCertificateFile /etc/pki/tls/certs/server5.crt
                SSLCertificateKeyFile /etc/pki/tls/private/server5.key
                SSLCertificateChainFile /etc/pki/tls/certs/example-
ca.crt
          </virtualhost>
          #-------------------------------------------------------------
-----------------------
     :wq!
     ]#  httpd -t (TO CHECK SYNTAX)
     ]#  firewall-cmd --add-service=https --permanent
     ]#  firewall-cmd --reload
     ]#  firewall-cmd --add-port=443/tcp --permanent
     ]#  firewall-cmd --reload
     ]#  systemctl restart httpd.service
     ]#  firefox (TO CHECK: https://server5.example.com,If u get page
showing untrusted connection or page then ur config is OK.)
-------------------------------------------------------------------------
-----------------------------------------------
10.  Create a directory named as secret in default DocumentRoot of your
default web server.
```

```
      - Download a file - http://classroom.example.com/pub/private.html
to secret directory.
      - Rename this file as index.html
      - The secret directory should be only available to localhost.
Ans:  ]# mkdir /var/www/html/secret
      ]# wget -O /var/www/html/secret/index.html
http://classroom.example.com/pub/private.html
      ]#  ll /var/www/html/secret/
      ]#  vim exam.conf
            #10TH QUESTION-----------------------------------------------
----------------------
                  <virtualhost *:80>
                        servername server5.example.com/secret
                        documentroot /var/www/html/secret
                        directoryindex index.html
                  <directory /var/www/html/secret>
                        order deny,allow
                        deny from all
                        allow from 172.25.5.11
                  </directory>
                  </virtualhost>
            #-------------------------------------------------------------
-----------------------------------
      :wq!
      ]#  httpd -t
      ]#  systemctl restart httpd.service
      ]#  firefox (TO CHECK: http://server5.example.com/secret)
-------------------------------------------------------------------------
-----------------------------------------------------
11.  Configure your web server to display the dynamic web contents.
       - Dynamic content is provided by a virtual host named as
http://webappX.example.com
       - This host should listen on port no 8877
       - Download a copy of script from
http://classroom.example.com/pub/webapp.wsgi and place it on appropriate
location for virtual host so that        it generates dynamic web
contents.
       - Do not make any changes in webapp.wsgi file
       - Clients connecting to http://webappX.example.com:8877 should get
the output of dynamic web contents.
       - This virtual host must be accessible to all the systems in
example.com.
Ans:  ]# mkdir /var/www/dynamic
      ]#  cd /var/www/dynamic/
      ]#  wget http://classroom.example.com/pub/webapp.wsgi
      ]#  ll (TO CHECK)
      ]#  firewall-cmd --add-port=8877/tcp --permanent
      ]#  firewall-cmd --reload
      ]#  semanage port -a -t http_port_t -p tcp 8877
      ]#  yum install mod_wsgi.x86_64
      ]#  vim /etc/httpd/conf.d/exam.conf
                  #11TH QUESTION-----------------------------------------
----------------------------
                  listen 8877
                  <virtualhost *:8877>
                        servername webapp5.example.com
                        documentroot /var/www/dynamic
                        wsgiscriptalias / /var/www/dynamic/webapp.wsgi
```

```
                </virtualhost>
            #-------------------------------------------------------------
-------------------------
      :wq!
      ]#  httpd -t
      ]#  systemctl restart httpd.service
      ]#  firefox (TO CHECK: http://webapp5.example.com:8877)
-------------------------------------------------------------------------
-------------------------------------------------------------
12.  Write a script nameing as bar.sh in root directory
        - If we give redhat as input it should print  fedora.
      - If we give fedora as input it should print  redhat.
      - If we give other than redhat or fedora it should print
"./root/bar.sh redhat|fedora" as an standerd error.
Ans:  ]# vim bar.sh
                #!/bin/bash

            if [ "$1" = 'redhat' ];then
                  echo "fedora"
            elif [ "$1" = 'fedora' ];then
                  echo "redhat"
            else
                  echo "./root/bar.sh redhat|fedora" > /dev/stderr
            fi

      :wq!
      ]# bash bar.sh
      ]# bash bar.sh redhat
      ]# bash bar.sh fedora
-------------------------------------------------------------------------
-------------------------------------------------------------
13. Configure NFS on serverX as follow
       - export /public directory with read only acess to desktopX
machine.
       - export /protected directory with read write acess to desktopX
       -Acess to /protected is authenticate by using Kerborse.You can use
keytab file from http://classroom.example.com/pub/keytabs/
            serverX.keytab
      - Create a  secure directory  inside the /protected directory
      - User ldapuserX have read and write acess on secure directory
Ans:    (ON SERVERX SIDE)
      ]#  mkdir /public /protected
      ]#  wget -O /etc/krb5.keytab
http://classroom.example.com/pub/keytabs/server5.keytab
      ]#  lab nfskrb5 setup (DO NOT RUN THIS LAB @ EXAM TIME)
      ]#  vim /etc/exports
            /public 172.25.5.10(ro,sec=sys,sync)
            /protected 172.25.5.10(rw,sec=krb5p,sync)
        :wq!
      ]#  exportfs -avr
      ]#  firewall-cmd --add-service=nfs --permanent
      ]#  firewall-cmd --reload
      ]#  mkdir /protected/secure
      ]#  getent passwd ldapuser5
      ]#  chown ldapuser5:ldapuser5 /protected/secure
      ]#  systemctl enable nfs-secure-server.service
      ]#  systemctl enable nfs-server.service
      ]#  systemctl restart nfs-secure-server.service
```

```
      ]#  systemctl restart nfs-server.service
-------------------------------------------------------------------------
-------------------------------------------------------------------
14.  Mount nfs on following Directory
       - public Directory exported by ServerX should be  mounted across
reboot  on /mnt/data
       - protected Directory exported by ServerX should be mounted
across reboot on /protected
Ans:     (ON DESKTOPX SIDE)
      ]# lab nfskrb5 setup
      ]# mkdir /mnt/data /protected
      ]# wget -O /etc/krb5.keytab
http://classroom.example.com/pub/keytabs/desktop5.keytab
      ]# vim /etc/fstab
            172.25.5.11:/public   /mnt/data  nfs  defaults,sec=sys,sync 0
0
            172.25.5.11:/protected  /protected  nfs
defaults,sec=krb5p,sync 0 0
      :wq!
      ]# systemctl enable nfs-secure.service
      ]# systemctl restart nfs-secure.service
      ]# mount -a
      ]# df -h
      ]# getent passwd ldapuser5
      (TO CROSS-CHECK)
      ]# cd /protected/secure/
      ]# touch 12 (IT SHOWS MSG: PERMISSION DENIED)
      ]# ssh ldapuser5@localhost(USE PASSWD:kerberos)
ldapuserhomedir]$ cd /protected/secure/
               ]$ touch 12 (IF FILE IS CREATED THEN CONFIG IS OK)
             ]$ logout
      ]#df -h
-------------------------------------------------------------------------
-------------------------------------------------------------------
15.   Share /common directory via smb from your serverX
      - Share name must be samba.
      - Samba share must browseable.
      - User natasha should have read access on it and authenticate with
the password "postroll".
      - sarah should have read and write access on share and authenticate
with the  "postroll" .
Ans:    (ON SERVERX SIDE)
      ]# yum install samba samba-client.x86_64 -y
      ]# mkdir /common
      ]# semanage fcontext -a -t samba_share_t '/common(/.*)?'
      ]# restorecon -Rv /common
      ]# useradd natasha
      ]# useradd sarah
      ]# setfacl -m u:natasha:r-x /common
      ]# setfacl -m u:sarah:rwx /common
      ]# getfacl /common
      ]# vim /etc/samba/smb.conf (IN THE END OF FILE(shift+g))
            [samba]
            path = /common
            writable = no
            write list = sarah
            valid users = natasha , sarah
            browseable = yes
```

```
      :wq!
       ]# testparm (TO CHECK SYNTAX OF CONFIG FILE)
       ]# smbpasswd -a natasha (USE PASSWD:postroll)
       ]# smbpasswd -a sarah (USE PASSWD:postroll)
       ]# firewall-cmd --add-service=samba --permanent
       ]# firewall-cmd --reload
       ]# systemctl enable smb nmb
       ]# systemctl restart smb nmb
--------------------------------------------------------------------------
--------------------------------------------------------------------------
16.  The samba share must be permanently mounted on DesktopX machine on
/mnt/samba directory and this share must allow anyone who can
authenticate     as sarah.
Ans:   (ON DESKTOPX SIDE)
       ]# mkdir /mnt/samba
       ]# yum install cifs-utils.x86_64 -y
       ]# vim /tmp/pass
           username=sarah
           password=postroll
       ]# vim /etc/fstab (FOR PERMANENT MOUNTING)
           //172.25.5.11/samba /mnt/samba cifs
defaults,sec=ntlmssp,multiuser,creds=/tmp/pass 0 0
        :wq!
       ]# mount -a
       ]# df -h
            (FOR TEMPERORY MOUNTING)
       ]# mount -o username=sarah //172.25.5.11/samba /mnt/samba(PASSWD:
postroll)
--------------------------------------------------------------------------
--------------------------------------------------------------------------
-
17.  Configure iscsi target on ServerX machine.
      - iscsi disk name is iqn.2014-06.com.example:serverX
      - iscsi should use default port as 3260.
      - target should use 3G backing volume nameing as datavol.
      - target should available to only desktopX machine.
Ans:      (ON SERVERX SIDE)
      ]# fdisk /dev/vdb
             :n
           :+5G
           :t
           :8e(lvm)
           :w
      ]# partprobe
      ]# pvcreate /dev/vdb1
      ]# vgcreate focus /dev/vdb1
      ]# lvcreate -n redhat -L 3G focus
      ]# yum install targetcli.noarch -y
      ]# targetcli
        /> cd
      o- /
.....................................................................
.....................................[...]
        o- backstores
.....................................................................
.....................................[...]
```

```
        | o- block
.....................................................................
.....................[Storage Objects: 0]
        | o- fileio
.....................................................................
.....................[Storage Objects: 0]
        | o- pscsi
.....................................................................
.....................[Storage Objects: 0]
        | o- ramdisk
.....................................................................
.....................[Storage Objects: 0]
        o- iscsi
.....................................................................
.............................[Targets: 0]
        o- loopback
.....................................................................
.............................[Targets: 0]
      /backstores/block> create datavol /dev/focus/redhat
      /backstores/block> cd
      /iscsi> create iqn.2014-06.com.example:server5
      /iscsi> cd
      /iscsi/iqn.20...er5/tpg1/acls> create iqn.2014-
06.com.example:desktop5
      /iscsi/iqn.20...er5/tpg1/acls> cd
      /iscsi/iqn.20...er5/tpg1/luns> create /backstores/block/datavol
      /iscsi/iqn.20...er5/tpg1/luns> cd
      /iscsi/iqn.20.../tpg1/portals> create 172.25.5.11 ip_port=3260
      /iscsi/iqn.20.../tpg1/portals> cd
      o- /
.....................................................................
.............................................[...]
      /> saveconfig
      /> exit
     ]# firewall-cmd --add-port=3260/tcp --permanent
     ]# firewall-cmd --reload
     ]# systemctl enable target.service
     ]# systemctl restart target.service
---------------------------------------------------------------------
---------------------------------------------------------------------
18.   Configure DesktopX machine for iscsi intiator.
      - Iscsi device should be automatically mounted at booting time.
      - Iscsi should contain a block of 2000MB and should have xfs file
system on it.
      - The partion must be mounted on /mnt/iscsi and it should be
automatically mounted.
Ans:      (ON DESKTOPX SIDE)
     ]# yum install iscsi-initiator-utils.i686 -y
     ]#  vim /etc/iscsi/initiatorname.iscsi
           InitiatorName=iqn.2014-06.com.example:desktop5
      :wq!
     ]#  systemctl enable iscsid.service
     ]#  systemctl restart iscsid.service
     ]#  iscsiadm --mode discoverydb --type sendtargets --portal
172.25.5.11 --discover (U will get this cmd from example section ofman
page of     iscscadm )
     ]#  iscsiadm --mode node --targetname iqn.2014-
06.com.example:server5 --portal 172.25.5.11:3260 --login
```

```
     ]#  lsblk
      NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
      sda      8:0    0   3G  0 disk
     ]# fdisk /dev/sda
           :p
           :n
           :+2000M
           :w
     ]#  partprobe
     ]#  mkfs.xfs /dev/sda1
     ]#  blkid
     ]#  vim /etc/fstab
          UUID=712cc38d-b14e-4951-b335-f5478497c30b /mnt/iscsi xfs
defaults,_netdev 0 0
     ]#  mkdir /mnt/iscsi
     ]#  mount -a
     ]#  df -h
      (BEFORE U REBOOT UR SYSTEMS,PLZ LOGOUT FROM ISCSI SERVER AS
FOLLOWS)
     ]# iscsiadm --mode node --targetname iqn.2014-06.com.example:server5
--portal 172.25.5.11:3260 --logout
--------------------------------------------------------------------------
--------------------------------------------------------------------------
19. create A MariaDB database by using the dump file.
    - create database named as legacy and import dump file into database.
    - dump file is provided by
http://classroom.example.com/pub/mariadb.dump
    - create user smith and grant select access on legacy database.
Ans: ]#  yum groupinstall mariadb mariadb-client -y
     ]#  systemctl enable mariadb.service
     ]#  systemctl restart mariadb.service
     ]#  mysql_secure_installation (Set passwd:redhat,use y(yes))
     ]#  mysql -u root -predhat
           MariaDB [(none)]> show databases;
           MariaDB [(none)]> create database legacy;
           MariaDB [(none)]> exit (ctrl+d)
     ]#  wget http://classroom.example.com/pub/mariadb.dump
     ]#  mysql -u root -predhat legacy < mariadb.dump
     ]#  mysql -u root -predhat
           MariaDB [(none)]> use legacy;
           MariaDB [legacy]> show tables;
           MariaDB [legacy]> create user smith@"localhost" identified by
"redhat";
           MariaDB [legacy]> grant select on legacy.* to
smith@'localhost';
           MariaDB [legacy]> exit (ctrl+d)
--------------------------------------------------------------------------
--------------------------------------------------------------------------
20.  Ans the following question in the file /root/mariadb.txt
   - count the number of product which are having id_catagory=2
Ans: ]# mysql -u root -predhat
           MariaDB [(none)]> use legacy;
           MariaDB [legacy]> select count(*) from product where
id_category=2;
           MariaDB [legacy]> exit(ctrl+d)
      ans is 2
     ]# vim /root/mariadb.txt
         ans=2
```

```
        :wq!
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
21.   Write a script nameing as foo.sh in root directory
        - create users provide by the file
http://classroom.example.com/pub/users
        - if appropriate file is not provide then it should return error
/root/foo.sh [Valid File]
         and return with appropirate error status
Ans:  ]# vim /root/foo.sh
            #!/bin/bash

            b=`basename $1`
            a=`cat $1`
                  if [ -s $1 -a "$b" = "user.txt" ];then
                        for i in $a
                              do
                                    useradd $i -s /sbin/nologin
                                    echo "$i"|passwd $i --stdin
                                    echo "$i is added"
                        done
                  else
                        echo "/root/foo.sh [Valid File]" > /dev/stderr
                  exit 2
                  fi
      :wq!
      ]# vim user.txt(USE FILE provide by the file
http://classroom.example.com/pub/users @ EXAM TIME )
            sam
            ram
            rani
            mahesh
      ]# bash foo.sh user.txt
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
-
22.   Configure mail access on both the systems as follows
      - system should not accept mail from external sources.
      - mail sent locally  from both systems get routed through
example.com
      - mail send from systems shows up as coming from
serverX.example.com.
Ans:  ]# lab smtp-nullclient setup
      ]# yum install postfix
      ]# vim /etc/postfix/main.cf
      LINE NO          CHANGES
      75          myhostname = server5.example.com
      83          mydomain = example.com
      98          myorigin = $mydomain
      116         inet_interfaces = all
      119         inet_protocols = all
        164       mydestination =
      264         mynetworks = 172.25.0.0/16, 127.0.0.0/8
      314         relayhost = [smtp5.example.com]
      @END        local_transport = error: local delivery disabled
     ]#  systemctl enable postfix
     ]#  systemctl restart postfix
     ]#  mail -s 'test' student@desktop5.example.com
```

(WHILE PRACTICING IF MAIL IS SENT THEN CHECK FOR HOSTNAME AS FOLLOWS)

(@ EXAM TIME PLZ GIVE mynetworks CAREFULLY)

```
]#  hostname
]#  hostname -d
]#  hostnamectl set-hostname server5.example.com
]#  systemctl enable postfix
]#  systemctl restart postfix
]#  mail -s 'test22' student@desktop5.example.com
```
